Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins exigidos na legislação, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**01.432.068/0001-02**	DUNS®:	**902299932**
Razão Social:	**APIS SOLUCOES TECNOLOGIA DA INFORMACAO LTDA**		
Nome Fantasia:			
Situação do Fornecedor:	**Credenciado**	Data de Vencimento do Cadastro:	**25/07/2025**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**		
MEI:	**Não**		
Porte da Empresa:	**Empresa de Pequeno**		

Ocorrências e Impedimentos

Ocorrência:	**Consta**
Impedimento de Licitar:	**Nada Consta**
Ocorrências Impeditivas indiretas:	**Nada Consta**
Vínculo com "Serviço Público":	**Nada Consta**

Níveis cadastrados:

Documento(s) assinalado(s) com "*" está(ão) com prazo(s) vencido(s).

Automática: a certidão foi obtida através de integração direta com o sistema emissor. Manual: a certidão foi inserida manualmente pelo fornecedor.

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**01/04/2025**	**Automática**
FGTS		Validade:	**23/02/2025**	**Automática**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**18/05/2025**	**Automática**

IV - Regularidade Fiscal Estadual/Distrital e Municipal

Receita Estadual/Distrital		Validade:	**12/02/2025**
Receita Municipal	(Isento)		

VI - Qualificação Econômico-Financeira

Validade: **30/06/2025**

CPF: 752.XXX.XXX-20 Nome: RICHARD NIXON DO NASCIMENTO OLIVEIRA

Ass: _____

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Relatório de Credenciamento

Dados do Fornecedor

CNPJ: **01.432.068/0001-02** DUNS®: **902299932**
Razão Social: **APIS SOLUCOES TECNOLOGIA DA INFORMACAO LTDA**
Nome Fantasia:
Situação do Fornecedor: **Credenciado** Data de Vencimento do Cadastro: **25/07/2025**

Dados do Nível

Situação do Nível: **Cadastrado**

Dados do Fornecedor

Porte da Empresa: **Empresa de Pequeno Porte**
Natureza Jurídica: **SOCIEDADE EMPRESÁRIA LIMITADA** MEI: **Não**
Capital Social: **R$ 0,00** Data de Abertura da Empresa: **18/09/1996**
CNAE Primário: **4751-2/01 - COMÉRCIO VAREJISTA ESPECIALIZADO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMÁTICA**

CNAE Secundário 1: **6110-8/03 - SERVIÇOS DE COMUNICAÇÃO MULTIMÍDIA - SCM**
CNAE Secundário 2: **6190-6/01 - PROVEDORES DE ACESSO ÀS REDES DE COMUNICAÇÕES**
CNAE Secundário 3: **6201-5/01 - DESENVOLVIMENTO DE PROGRAMAS DE COMPUTADOR**

Dados para Contato

CEP: **70.711-903**
Endereço: **SETOR SCN QD 01 BLOCO E ED. CENTRAL PARK SALA 908 (PARTE), SN**
Município / UF: **BRASÍLIA / Distrito Federal**
Telefone: **(61) 32258956**
E-mail: **apis.pregao@gmail.com**

Dados do Responsável Legal

CPF: **443.997.661-15**
Nome: **EMERSON MENDES BATISTA**

Dados do Responsável pelo Cadastro

CPF: **443.997.661-15**
Nome: **EMERSON MENDES BATISTA**
E-mail: **emersonmendesb@gmail.com**

Relatório de Credenciamento

Sócios / Administradores

Dados do Sócio/Administrador 1

CPF:	**512.529.881-68**	Participação Societária:	**45,00%**
Nome:	**SERGIO SANTAREM TAVEIRA**		
Número do Documento:	**1070355**	Órgão Expedidor:	**SSPDF**
Data de Expedição:	**13/07/2015**	Data de Nascimento:	**16/12/1969**
Filiação Materna:	**CLEUZA SANTAREM TAVEIRA**		
Estado Civil:	**Divorciado(a)**		
CEP:	**70.730-703**		
Endereço:	**QUADRA HCGN 703 BLOCO C CASA 30, 30 - CASA - ASA NORTE**		
Município / UF:	**BRASÍLIA / Distrito Federal**		
Telefone:	**(61) 33404747**		
E-mail:	**sergio.pregao@gmail.com**		

Dados do Sócio/Administrador 2

CPF:	**443.997.661-15**	Participação Societária:	**55,00%**
Nome:	**EMERSON MENDES BATISTA**		
Número do Documento:	**535239**	Órgão Expedidor:	**SSPDF**
Data de Expedição:	**22/06/2004**	Data de Nascimento:	**25/06/1967**
Filiação Materna:	**AMELIA MENDES BATISTA**		
Estado Civil:	**Solteiro(a)**		
CEP:	**71.745-302**		
Endereço:	**QUADRA AV SMPW QUADRA 23 CONJUNTO 2, 5 - PARK WAY**		
Município / UF:	**BRASÍLIA / Distrito Federal**		
Telefone:	**(61) 82301111**		
E-mail:	**EMERSONMENDESB@GMAIL.COM**		

Linhas Fornecimento

Materiais

6940 - ACESSÓRIOS PARA TREINAMENTO DE COMUNICAÇÕES

7010 - COMPUTADORES

7020 - IMPRESSORAS

Serviços

582 - Estudos e Projetos de Telecomunicações - Transmissão

590 - Estudos e Projetos de Comutação Telefônica

604 - Estudos e Projetos de Comutação Telegráfica

612 - Estudos e Projetos de Comunicação de Dados

620 - Estudos e Projetos de Redes de Telecomunicações

736 - Auditoria em Área de Processamento de Dados

1279 - Informática - Programas Fechados (Software)

1589 - Instalações Prediais de Comunicação (Obras Civis)

1945 - Obras Civis de Redes de Telecomunicações

1988 - Manutenção / Instalação / Montagem / Ampliação - Equipamen-tos de Telecomunicações

2143 - Instalação e Montagem de Redes Aéreas - Telecomunicações

Relatório de Credenciamento

Serviços

2151 - Instalação e Montagem Redes Subterrâneas - Telecomunicações

2160 - Instalação e Montagem Redes Subaquáticas - Telecomunicações

2666 - Manutenção de Equipamentos de Comutação Telefônica

2674 - Manutenção de Equipamentos de Comutação Telegráfica

2682 - Manutenção de Equipamentos de Transmissão Multiplex Telefônica

2690 - Manutenção de Equipamentos de Transmissão Multiplex Telegrá-fica

2712 - Manutenção de Equipamentos de Comunicação de Dados

2887 - Manutenção de Redes Aéreas - Telecomunicações

2895 - Manutenção de Redes Subterrâneas de Telecomunicações

2909 - Manutenção de Redes Subaquáticas - Telecomunicações

3360 - Transporte Intermodal / Multimodal

3530 - Informática - Manutenção de Computadores

4006 - Locação de computadores / Periféricos

4065 - Locação de Equipamentos de Telecomunicações

4111 - Informática - Disquete Formatado (Software)

4251 - Comunicação Telefônica - Locação / Serviço

4260 - Comunicação - Telex / Telégrafo

4278 - Comunicação por Fac-Simile

4286 - Comunicação por Correio

5207 - Transporte Rodoviário - Substâncias Perigosas por VeículosComuns

5703 - Diagnose e Terapia - Tomografia Computadorizada

5800 - Instalação / Manutenção Vidro Comum - Porta / Janela

10740 - Exame por Tomografia Computadorizada

12637 - Tradução / Interpretação Simultânea / Consecutiva

13668 - Estudos e Projetos de Instalação de Rede Local de Microcomputador

13676 - Instalação de Rede Local de Microcomputador

13684 - Estudos e Projetos de Instalação de Rede Comunicação / Local

13935 - Disponibilização de Linha para Comunicação / Transmissão deDados

14737 - Estudo, Projeto - Multisetorial

15270 - Desenho / Produção - Multimídia

15601 - Consultoria e Assessoria - Comunicação

16195 - Recolhimento de Taxa / Imposto / Multa

16233 - Registro de Programa de Computador

16535 - Comunicação - Assinatura / Valor Adicionado

16608 - Oftalmologia / Diagnose - Ceratoscopia Computadorizada

16616 - Oftalmologia / Diagnose - Campimetria Computadorizada

16918 - Informática - Desenvolvimento / Implantação / Manutenção Re-de de Computador

17086 - Estudos e Projetos de Sistemas de Sinalização / ComunicaçãoVisual

17914 - Sinalização Visual Computadorizada

18104 - Consultoria e Assessoria - Telecomunicação

19615 - Informática - Instalação / Manutenção Comunicação Dados

21490 - Locação Equipamento - Tradução Simultânea / Sonorização

21750 - Locação Equipamento Radiocomunicação

21768 - Assistência Técnica / Prestação Serviço - Radiocomunicação

21873 - Telefonia Fixa Comutada / Convencional

Relatório de Credenciamento

Serviços

22357 - Comunicação de Dados e Frame Relay Com Roteadores

22365 - Serviços de Telecomunicações

23990 - Prestação de Serviços de Informática Operação de Computador

24988 - Serviços de Suporte de Divulgação em Comunicação Social.

25135 - Serviço Rede Comunicação Dados e Imagem

25739 - Prestação de Serviços de Técnico de Telecomunicações

CONTROLADORIA-GERAL DA UNIÃO

Certidão negativa correcional - Entes Privados (ePAD, CGU-PJ, CEIS, CNEP e CEPIM)

Consultado: **APIS SOLUCOES TECNOLOGIA DA INFORMACAO LTDA**

CPF/CNPJ: **01.432.068/0001-02**

Certifica-se que, em consulta aos sistemas ePAD e CGU-PJ e aos cadastros CEIS, CNEP e CEPIM mantidos pela Corregedoria-Geral da União, **NÃO CONSTAM** registros de penalidades vigentes relativas ao CNPJ/CPF consultado.

Destaca-se que, nos termos da legislação vigente, os referidos cadastros consolidam informações prestadas pelos entes públicos, de todos os Poderes e esferas de governo.

Os Sistemas ePAD e CGU-PJ consolidam os dados sobre o andamento dos processos administrativos de responsabilização de entes privados no Poder Executivo Federal.

O Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) apresenta a relação de empresas e pessoas físicas que sofreram sanções que implicaram a restrição de participar de licitações ou de celebrar contratos com a Administração Pública.

O Cadastro Nacional de Empresas Punidas (CNEP) apresenta a relação de empresas que sofreram qualquer das punições previstas na Lei nº 12.846/2013 (Lei Anticorrupção).

O Cadastro de Entidades Privadas sem Fins Lucrativos Impedidas (CEPIM) apresenta a relação de entidades privadas sem fins lucrativos que estão impedidas de celebrar novos convênios, contratos de repasse ou termos de parceria com a Administração Pública Federal, em função de irregularidades não resolvidas em convênios, contratos de repasse ou termos de parceria firmados anteriormente.

Certidão emitida às 15:47:23 do dia 11/02/2025 , com validade até o dia 13/03/2025.

Link para consulta da verificação da certidão https://certidoes.cgu.gov.br/

Código de controle da certidão: IRFs0c5iElSRStkxGQ2A

Qualquer rasura ou emenda invalidará este documento.

TRIBUNAL DE CONTAS DA UNIÃO

Consulta Consolidada de Pessoa Jurídica

Este relatório tem por objetivo apresentar os resultados consolidados de consultas eletrônicas realizadas diretamente nos bancos de dados dos respectivos cadastros. A responsabilidade pela veracidade do resultado da consulta é do Órgão gestor de cada cadastro consultado. A informação relativa à razão social da Pessoa Jurídica é extraída do Cadastro Nacional da Pessoa Jurídica, mantido pela Receita Federal do Brasil.

Consulta realizada em: 11/02/2025 15:47:56

Informações da Pessoa Jurídica:

Razão Social: **APIS SOLUÇÕES TECNOLOGIA DA INFORMAÇÃO LTDA.**
CNPJ: **01.432.068/0001-02**

Resultados da Consulta Eletrônica:

Órgão Gestor: **TCU**
Cadastro: **Licitantes Inidôneos**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **CNJ**
Cadastro: **CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **Cadastro Nacional de Empresas Inidôneas e Suspensas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **CNEP - Cadastro Nacional de Empresas Punidas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Obs: A consulta consolidada de pessoa jurídica visa atender aos princípios de simplificação e racionalização de serviços públicos digitais. Fundamento legal: Lei nº 12.965, de 23 de abril de 2014, Lei nº 13.460, de 26 de junho de 2017, Lei nº 13.726, de 8 de outubro de 2018, Decreto nº 8.638 de 15, de janeiro de 2016.

TRIBUNAL DE CONTAS DA UNIÃO

CERTIDÃO NEGATIVA

DE

LICITANTES INIDÔNEOS

Nome completo: **APIS SOLUÇÕES TECNOLOGIA DA INFORMAÇÃO LTDA.**

CPF/CNPJ: **01.432.068/0001-02**

O Tribunal de Contas da União CERTIFICA que, na presente data, o (a) requerente acima identificado(a) NÃO CONSTA da relação de responsáveis inidôneos para participar de licitação na administração pública federal, por decisão deste Tribunal, nos termos do art. 46 da Lei nº 8.443/92 (Lei Orgânica do TCU).

Não constam da relação consultada para emissão desta certidão os responsáveis ainda não notificados do teor dos acórdãos condenatórios, aqueles cujas condenações tenham tido seu prazo de vigência expirado, bem como aqueles cujas apreciações estejam suspensas em razão de interposição de recurso com efeito suspensivo ou de decisão judicial.

Certidão emitida às 15:47:26 do dia 11/02/2025, com validade de trinta dias a contar da emissão.

A veracidade das informações aqui prestadas podem ser confirmadas no sítio https://contas.tcu.gov.br/ords/f?p=1660:5

Código de controle da certidão: H1BP110225154726

Atenção: qualquer rasura ou emenda invalidará este documento.

Certidão Negativa

Certifico que nesta data (11/02/2025 às 15:48) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CNPJ nº 01.432.068/0001-02.

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle 67AB.9B63.6E2A.9683 no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

CONTROLADORIA-GERAL DA UNIÃO

Certidão negativa correcional - Entes Privados (ePAD, CGU-PJ, CEIS, CNEP e CEPIM)

Consultado: **EMERSON MENDES BATISTA**

CPF/CNPJ: **443.997.661-15**

Certifica-se que, em consulta aos sistemas ePAD e CGU-PJ e aos cadastros CEIS, CNEP e CEPIM mantidos pela Corregedoria-Geral da União, **NÃO CONSTAM** registros de penalidades vigentes relativas ao CNPJ/CPF consultado.

Destaca-se que, nos termos da legislação vigente, os referidos cadastros consolidam informações prestadas pelos entes públicos, de todos os Poderes e esferas de governo.

Os Sistemas ePAD e CGU-PJ consolidam os dados sobre o andamento dos processos administrativos de responsabilização de entes privados no Poder Executivo Federal.

O Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) apresenta a relação de empresas e pessoas físicas que sofreram sanções que implicaram a restrição de participar de licitações ou de celebrar contratos com a Administração Pública.

O Cadastro Nacional de Empresas Punidas (CNEP) apresenta a relação de empresas que sofreram qualquer das punições previstas na Lei nº 12.846/2013 (Lei Anticorrupção).

O Cadastro de Entidades Privadas sem Fins Lucrativos Impedidas (CEPIM) apresenta a relação de entidades privadas sem fins lucrativos que estão impedidas de celebrar novos convênios, contratos de repasse ou termos de parceria com a Administração Pública Federal, em função de irregularidades não resolvidas em convênios, contratos de repasse ou termos de parceria firmados anteriormente.

Certidão emitida às 15:50:28 do dia 11/02/2025 , com validade até o dia 13/03/2025.

Link para consulta da verificação da certidão https://certidoes.cgu.gov.br/

Código de controle da certidão: khoPsIeL0wd1sdb7pVVk

Qualquer rasura ou emenda invalidará este documento.

TRIBUNAL DE CONTAS DA UNIÃO

CERTIDÃO NEGATIVA

DE

LICITANTES INIDÔNEOS

(Válida somente com a apresentação do CPF)

Nome completo: **EMERSON MENDES BATISTA**

CPF/CNPJ: **443.997.661-15**

O Tribunal de Contas da União CERTIFICA que, na presente data, o (a) requerente acima identificado(a) NÃO CONSTA da relação de responsáveis inidôneos para participar de licitação na administração pública federal, por decisão deste Tribunal, nos termos do art. 46 da Lei nº 8.443/92 (Lei Orgânica do TCU).

Não constam da relação consultada para emissão desta certidão os responsáveis ainda não notificados do teor dos acórdãos condenatórios, aqueles cujas condenações tenham tido seu prazo de vigência expirado, bem como aqueles cujas apreciações estejam suspensas em razão de interposição de recurso com efeito suspensivo ou de decisão judicial.

Certidão emitida às 15:50:32 do dia 11/02/2025, com validade de trinta dias a contar da emissão.

A veracidade das informações aqui prestadas podem ser confirmadas no sítio https://contas.tcu.gov.br/ords/f?p=1660:5

Código de controle da certidão: HK25110225155032

Atenção: qualquer rasura ou emenda invalidará este documento.

Certidão Negativa

Certifico que nesta data (11/02/2025 às 15:50) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CPF nº 443.997.661-15.

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle 67AB.9C0E.0B68.1854 no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

Cliente
UNIVERSIDADE FEDERAL DO MARANHÃO

Proposta Comercial

Certame
PE 90003/2025

Data
04/02/2025

Brasilia 11 de fevereiro de 2025

E-Mail : apis.pregao@gmail.com
Site : www.apis.com.br

Endereço: SIBS Q.2 Conj.D Lote 3
Cidade: Núcleo Bandeirante – DF
CEP: 71.736-204

Prezados Senhores,

Pela presente, submetemos à apreciação da **UNIVERSIDADE FEDERAL DO MARANHÃO** e aos demais participantes deste certame, a nossa proposta de preço relativa a licitação **PE 90003/2025**, assumindo inteira responsabilidade por quaisquer erros ou omissões que venham a ser verificados na preparação da mesma, bem como concordamos com a totalidade das instruções e critérios de qualificação definidos no Edital e seus anexos, e declaramos, ainda, que temos pleno conhecimento das condições em que se desenvolverão o fornecimento.

A proposta comercial encontra-se em conformidade com as informações previstas no edital e seus anexos.

1. Identificação do licitante:

Nome	APIS Soluções Tecnologia da Informação Ltda				
CNPJ	01.432.068/0001-02				
Endereço	SCN Q.1 Bl.E Sl.910				
Cidade	Brasilia		Estado	Distrito Federal	
Bairro	Setor Comercial Norte		Cep	70.711-903	
Fone/Fax	61 3340-4747		E-Mail	apis.pregao@gmail.com	
Banco	001	Agencia	1230-0	Conta	41748-3

Representante Legal

Nome	Sergio Santarem Taveira – Analista de Sistemas
RG	1070355 – SSP/DF
CPF	512.529.881-68
Cargo	Sócio Diretor
Endereço	Cond. Lago Sul. Conj5 Casa 9
Cidade	Brasilia
Bairro	Jardim Botanico
Cep	71.680.361

Objeto : "Aquisição de equipamentos de rede local de computadores cabeada (LAN) e sem fio (WLAN), visando a manutenção e ampliação da rede de dados da UFMA."

PRODUTOS E SERVIÇOS

ITEM	DESCRIÇÃO	UN	QTD	Valor Uniario	Valor Total
01	Ponto de acesso interno - Tipo 1 **Marca**: Cambium **Modelo**: XV2-21X	Un	275	4.600,00	1.265.000,00
02	Ponto de acesso interno - Tipo 2 **Marca**: Cambium **Modelo**: XE3-4	Un	93	6.400,00	595.200,00
03	Ponto de acesso Externo **Marca**: Cambium **Modelo**: XV2-23T	Un	18	8.000,00	144.000,00
04	Licença para ponto de acesso **Marca**: Cambium	Un	386	740,00	285.640,00
05	Software de controladora de ponto de acesso **Marca**: Cambium **Modelo**: CnMaestro	Un	1	11.000,00	11.000,00
Valor Total					**2.300.840,00**

Informações Gerais

- **Simples Nacional? Sim (X) | Não ( )**
- **Prazo de Validade da Proposta:** será de 90 (noventa) dias corridos, a contar da data da sessao deste Pregão Eletrônico
- **Prazo de Garantia :** Conforme Edital
- **Prazo de Entrega :** Conforme Edital

Das Declarações e demais documentos:
A empresa APIS SOLUÇÕES TECNOLOGIA DA INFORMAÇÃO LTDA.,

DECLARA:

a) Declaramos expressamente que os preços contidos na proposta incluem todos os custos, tais como: salário, ônus tributários, fiscais, parafiscais, trabalhistas e sociais, seguro, transporte, embalagem, garantia e demais despesas de qualquer natureza que possam incidir, direta ou indiretamente, no cumprimento integral do objeto deste Termo de Referência;
b) Que as condições de pagamento são aquelas estabelecidas no ato convocatório do certame em epígrafe;
c) Declaração de elaboração independente de proposta, nos termos do disposto na Instrução Normativa MPOG/SLTI nº 2, de 16/09/2009;
d) Declaramos que entre os sócios que integram a composição societária do Licitante não há empregados do quadro de pessoal do Orgão, e nem exercem função de confiança, função de dirigente, ou que seja responsável pela presente licitação, nos termos do inciso III, do art. 9º da Lei nº 8.666, de 1993;
e) Declaramos expressamente que não alocaremos familiares de empregado do Orgão, que exerça cargo de confiança ou função de confiança, na execução do objeto deste Termo de Referência, nos termos do art. 7º do Decreto nº 7.203, de 2010;

f) Declaramos conhecer a legislação de regência do objeto a ser licitado e que o mesmo será executado e fornecido de acordo com as condições estabelecidas neste Termo de Referência;
g) Declaramos que o(s) item(ns) constante(s) desta proposta corresponde(m) exatamente às especificações descritas no Anexo do Edital, às quais aderimos formalmente.
h) Declaramos que 1/12 (um doze avos) do valor total dos contratos firmados com a Administração Pública e/ou com a iniciativa privada, vigentes na data da sessão pública de abertura deste Pregão, não é superior ao Patrimônio Líquido do licitante, podendo este ser atualizado na forma já disciplinada neste Edital;
i) Declaração de que não possui em seu quadro de pessoal empregado menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, ou menor de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do inciso XXXIII do art. 7º da Constituição Federal;
j) Que cumprimos os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, 14 de dezembro de 2006, e suas alterações posteriores, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;
k) Que nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;
l) Que estamos ciente e concordamos com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital;
m) Que inexistem fatos impeditivos para nossa habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;
n) Que não possuímos, em nossa cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
o) Que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

Brasília – DF, 11 de fevereiro de 2025.

Apis Soluções Tecnologia da Informação Ltda
Sergio Santarém Taveira
512.529.881-68
Sócio Proprietário

DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

APIS Soluções Tecnologia da Informação Ltda, CNPJ nº 01.432.068/0001-02, situado à SCN Q.1 Bl.E Sl.910, Setor Comercial Norte – Brasilia-DF, por intermédio de seu representante legal o Sr. Sergio Santarm Taveira, portador(a) da Carteira de Identidade nº 1070355 SSPDF e do CPF nº 512.529.881-68, DECLARA, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.

Estou ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes, quando solicitadas como requisito para habilitação, e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º da Instrução Normativa nº 01, de 19 de janeiro de 2010, do Ministério do Planejamento, Orçamento e Gestão – MPOG e o Decreto Federal nº 7.746, de 5 de junho de 2012. Declaramos também, em especial ao art. 299 do Código Penal Brasileiro, que a empresa está ciente de sua responsabilidade ambiental e que cumpri a legislação específica para a atividade que desenvolve e, adota práticas ecologicamente corretas, tomando todas as medidas necessárias para evitar, atenuar ou reparar os impactos resultantes de sua atividade, mantendo-se disponível à fiscalização pelos órgãos responsáveis. Estou ciente da obrigatoriedade da apresentação do registro no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais, caso minha empresa exerça uma das atividades constantes no Anexo I da Instrução Normativa nº 6, de 15 de março de 2013, do IBAMA.

A empresa abaixo qualificada, declara, sob as sanções cabíveis, de que não está sob pena de interdição temporária de direitos de que tr ata o art. 10 da Lei nº 9.605, de 12/02/98.

Declaramos, ainda, que inexiste qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com serviço ou dirigente do Ibama; e que foi (realizada a Vistoria nas instalações do Ibama, tomando conhecimento dos serviços a serem realizados / apresentada recusa formal de Vistoria), não sendo admitidas, em hipótese alguma, alegações posteriores de desenvolvimento dos serviços e de dificuldades técnicas não previstas.

Apis Soluções Tecnologia da Informação Ltda
Sergio Santarém Taveira
512.529.881-68
Sócio Proprietário

E-Mail : apis.pregao@gmail.com
Site : www.apis.com.br

Endereço: SIBS Q.2 Conj.D Lote 3
Cidade: Núcleo Bandeirante – DF
CEP: 71.736-204

DECLARAÇÃO DE RENÚNCIA DA VISTORIA

APIS Soluções Tecnologia da Informação Ltda, CNPJ nº 01.432.068/0001-02, situado à SCN Q.1 Bl.E Sl.910, Setor Comercial Norte – Brasilia-DF, por intermédio de seu representante legal o Sr. Sergio Santarm Taveira, portador(a) da Carteira de Identidade nº 1070355 SSPDF e do CPF nº 512.529.881-68, optamos pela NÃO REALIZAÇÃO DE VISTORIA, assumindo inteira responsabilidade ou consequências por essa omissão, mantendo as garantias que vincularem nossa proposta comercial processo licitatório, em nome da empresa que represento. Declaramos que o fato de não termos realizados a vistoria não será utilizado como argumento para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com a contratante. Estamos de acordo com todas as exigências do Edital, tendo ciência do ambiente operacional onde os equipamentos objeto do Termo de Referência serão utilizados e nos responsabilizamos pela elaboração da Proposta.

Apis Soluções Tecnologia da Informação Ltda
Sergio Santarém Taveira
512.529.881-68
Sócio Proprietário

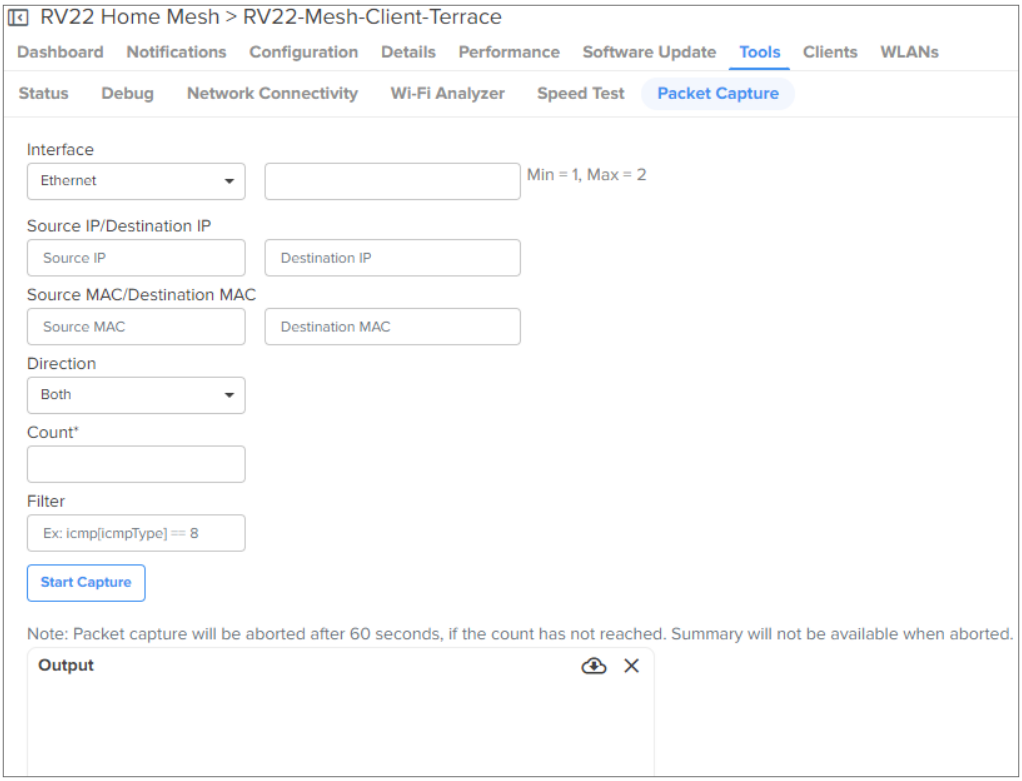
E-Mail : apis.pregao@gmail.com
Site : www.apis.com.br

Endereço: SIBS Q.2 Conj.D Lote 3
Cidade: Núcleo Bandeirante – DF
CEP: 71.736-204

To capture packet data:

1. Navigate to **Monitor and Manage >** <RV22-router-name> **> Tools** > **Packet Capture**.
2. Select the required interface and provide the source and destination IP address or MAC address.
3. Provide the number of packets to be captured.
4. Click **Start Capture**.

   cnMaestro displays the information in the **Ouput** window.
5. To download the PCAP file, click the download ( ) icon.



Wireless Intrusion Detection System (WIDS)

Note

This is a beta feature.

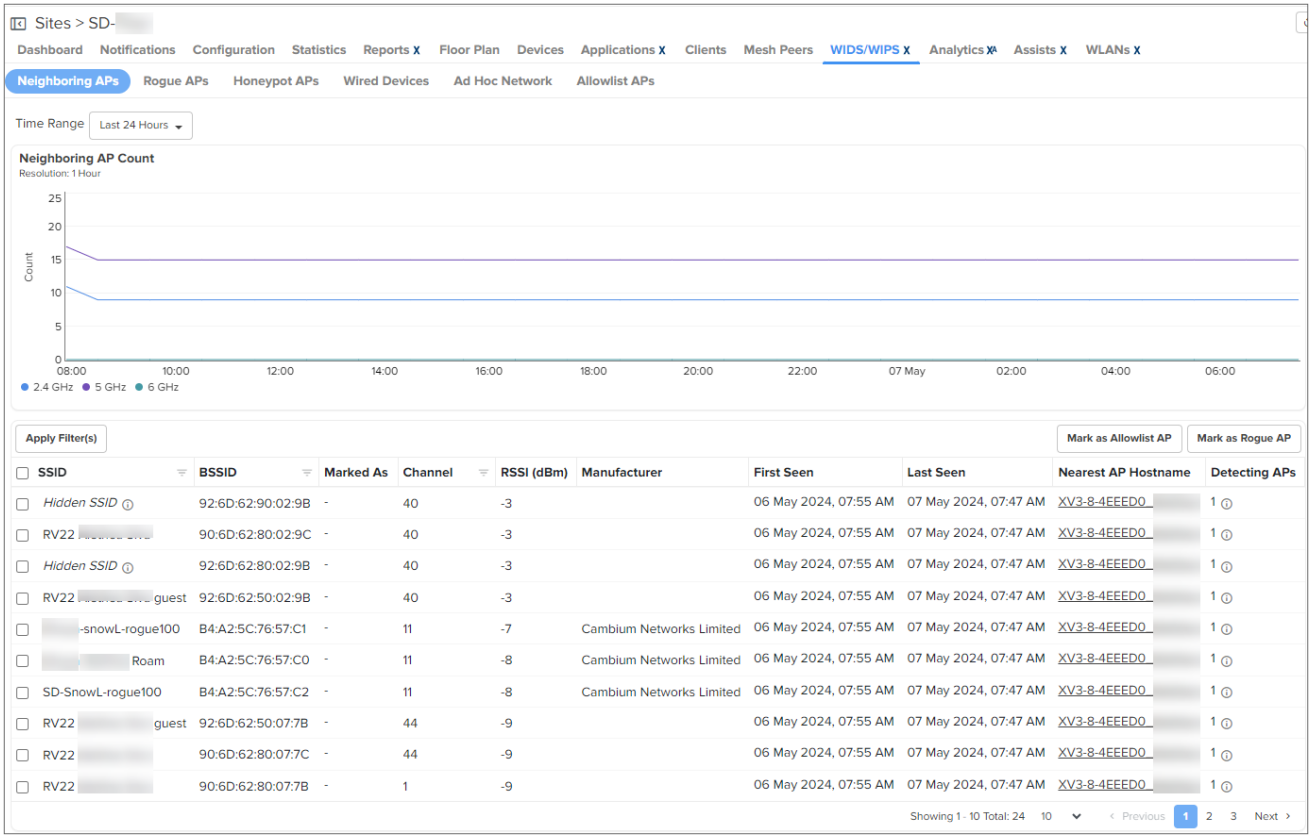
WIDS is a powerful feature within cnMaestro that helps administrators monitor and protect their wireless networks from unauthorized access and potential security threats. WIDS works by continuously scanning the wireless spectrum to detect and mitigate potential intrusions, ensuring the integrity and security of your network infrastructure.

This section provides detailed monitoring of various aspects including:

- Neighboring APs
- Rogue APs
- Honeypot APs
- Wired Devices

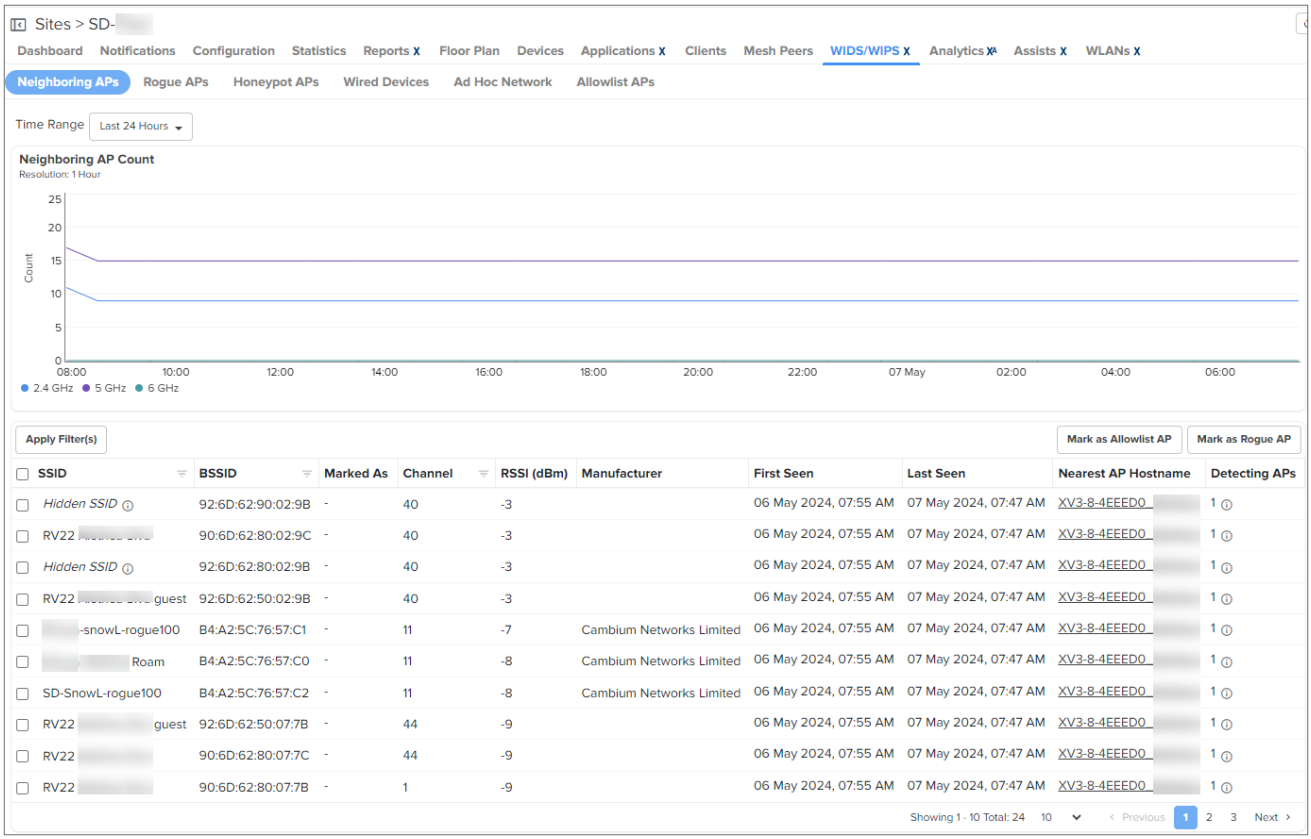
- Ad Hoc Network
- Allowlist APs

To view the WIDS page, navigate to **Network** > **Site** > **WIDS/WIPS** page.



Neighboring APs

This feature allows user to monitor and manage neighboring APs effectively to ensure optimal network performance and security.



User can selectively mark neighboring APs as **Allowlist APs** or **Rogue APs** directly from the Neighboring AP page. This functionality enables administrators to categorize neighboring APs based on their legitimacy and take appropriate actions to manage them.

The neighboring APs that are marked as allowlist or rogue APs are moved to the **Allowlist APs** and **Rogue APs** tabs respectively.

The Neighboring AP page offers flexibility in analyzing data by providing options to select the **Time Range**. User can choose between **Last 24 hours** and **Last 7 days** to view neighboring AP data within the specified time frame.

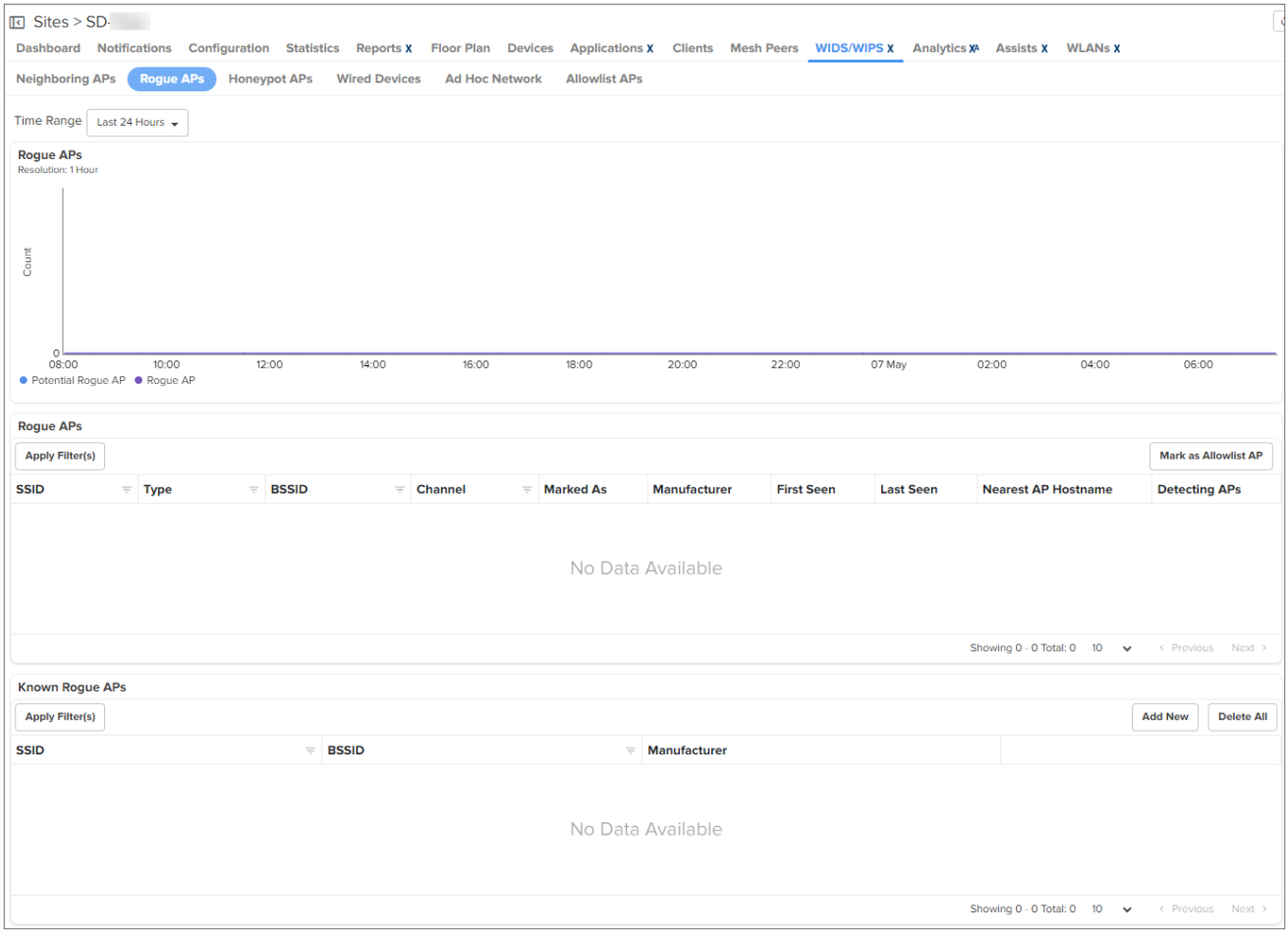
The following Neighboring APs parameters are displayed:

Table 36 *Neighboring APs parameters*

Field	Description
SSID	Name of the wireless network.
BSSID	MAC address of the AP.
Marked As	Indicates whether the neighboring AP is marked as an allowlist AP or a rogue AP.
Channel	Radio frequency channel on which the neighboring AP operates.
RSSI (dBm)	Received signal strength indication, measured in decibels relative to one milliwatt (dBm).
Manufacturer	Manufacturer name of the neighboring AP (For example, TP-Link, NETGEAR).
First Seen	Date and time when the neighboring AP was first detected.
Last Seen	Date and time when the neighboring AP was last detected.
Nearest AP Host name	Hostname of the nearest AP to the neighboring AP.
Detecting APs	Number of APs that have detected the neighboring AP.

Rogue APs

A Rogue AP is an unauthorized AP that is not onboarded to cnMaestro, which may include Cambium or non-Cambium devices causing interference. The authorized or onboarded APs scan all available channels and collect details about neighboring APs. They send this information to cnMaestro for monitoring and management.



The following Rogue AP parameters are displayed:

Table 37 *Rogue APs parameters*

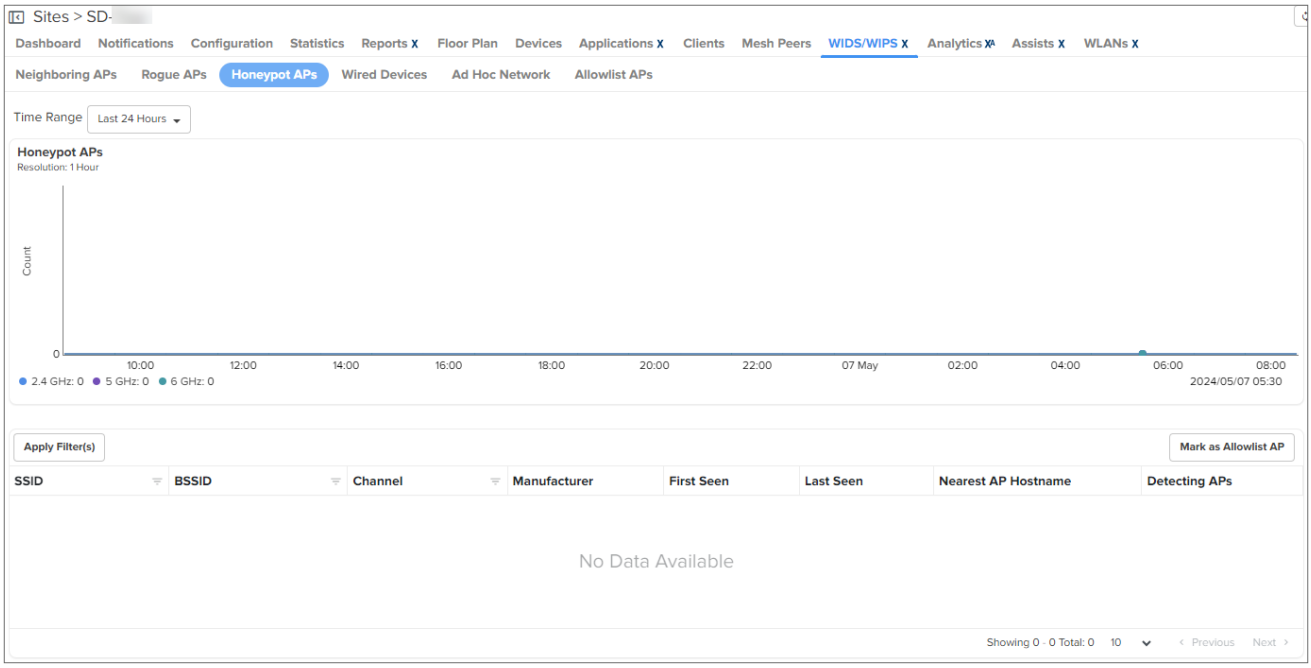
Field	Description
SSID	SSID of the rogue AP.
Type	Indicates the type of the rogue AP. Following are the supported values: • Rogue AP • Potential Rogue AP
BSSID	AP MAC address.
Channel	Channel in which the rogue AP operates.
Marked As	Indicates whether the rogue AP has been marked as an allowlist AP or a rogue AP.
Manufacturer	Manufacturer name of the neighboring AP (For example, TP-Link, NETGEAR).
First Seen	Time at which the rogue AP is detected for the first time.
Last Seen	Time at which the rogue AP was last detected.

Table 37 *Rogue APs parameters*

Field	Description
Nearest AP Hostname	Hostname of the nearest AP to the rogue AP.
Detecting APs	Number of APs that have detected the rogue AP.

Honeypot APs

Honeypot APs are unauthorized APs that advertise the same SSID as managed or onboarded APs. Detecting and monitoring these APs is crucial to prevent threats to the network infrastructure.



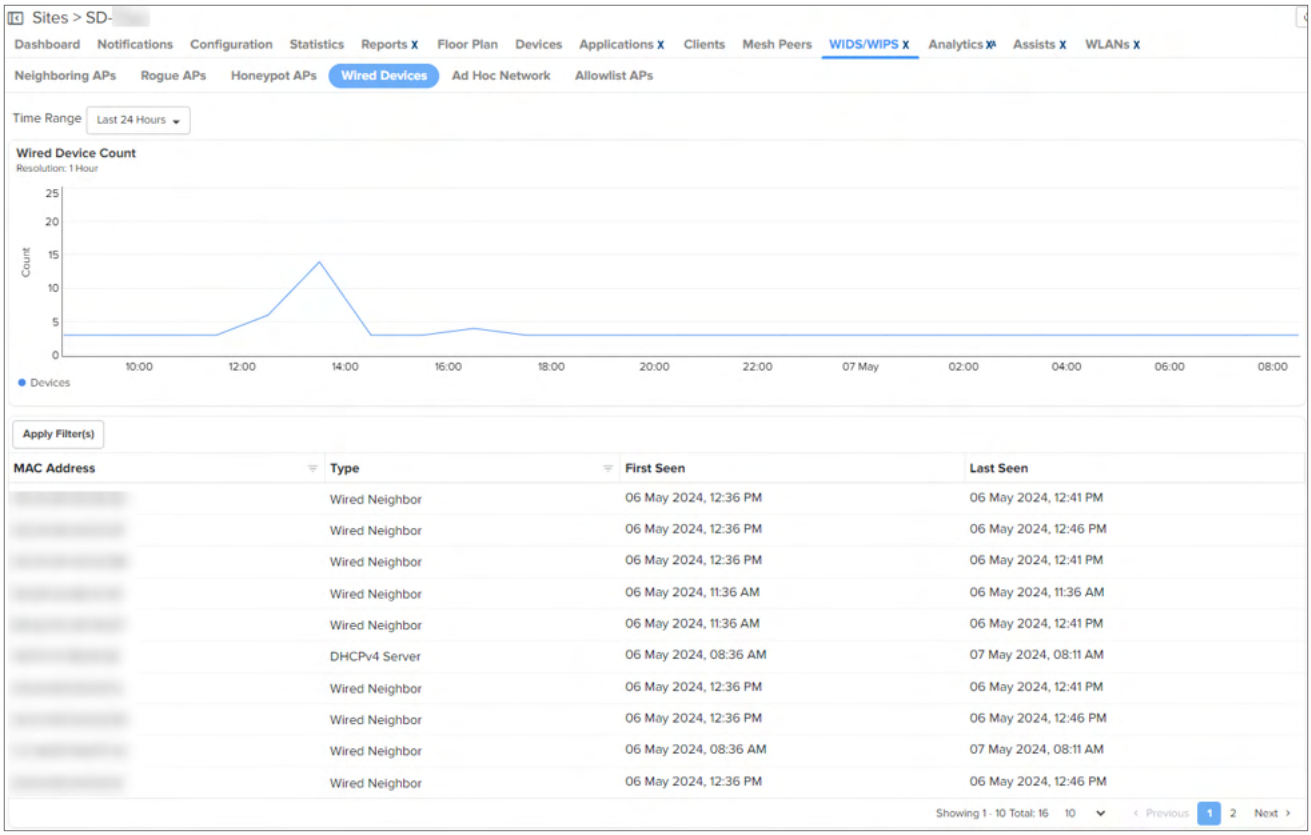
The following parameters related to Honeypot APs are displayed:

Table 38 *Honeypot APs parameters*

Field	Description
SSID	Name of the honeypot wireless network.
BSSID	AP MAC address.
Channel	Radio frequency channel on which the honeypot AP operates.
Manufacturer	Manufacturer name of the honeypot AP.
First Seen	Date and time when the honeypot AP was first detected.
Last Seen	Date and time when the honeypot AP was last detected.
Nearest AP Hostname	Hostname of the nearest AP to the honeypot AP.
Detecting APs	Number of APs that have detected the honeypot AP.

Wired Devices

The Wired Devices section within cnMaestro provides administrators with insights into the wired devices connected to the network infrastructure. This feature allows administrators to monitor and manage wired devices effectively to ensure optimal network performance and security.



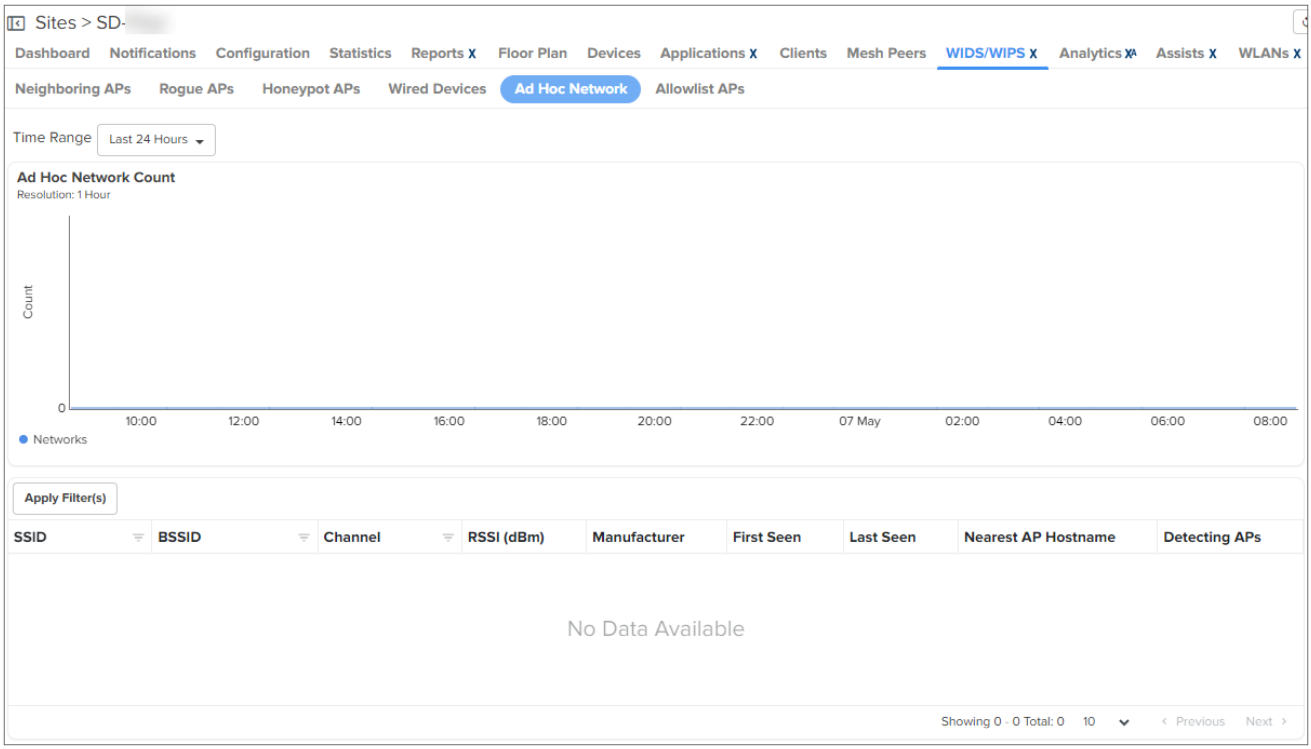
The following parameters related to Wired Devices are displayed:

Table 39 *Wired Devices parameters*

Field	Description
MAC Address	The MAC address of the wired device.
Type	The type or category of the wired device.
First Seen	The date and time when the wired device was first detected.
Last Seen	The date and time when the wired device was last detected.

Ad Hoc Networks

Ad hoc networks are temporary networks formed spontaneously by wireless devices for direct communication without the need for a central AP.



The following parameters related to Ad Hoc Networks are displayed:

Table 40 *Ad Hoc Networks parameters*

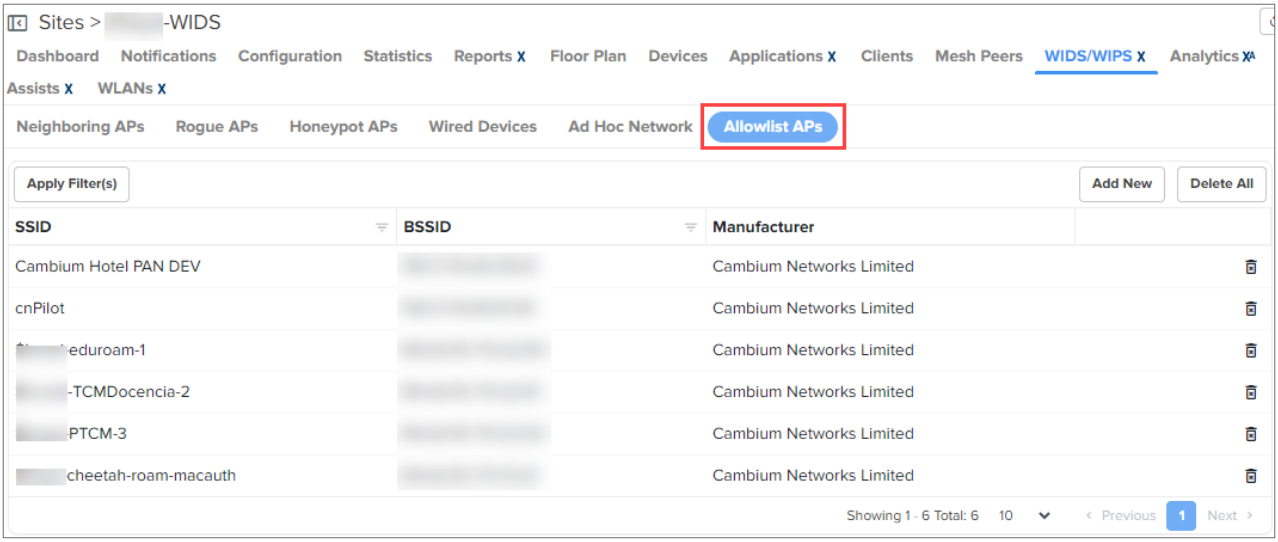
Field	Description
SSID	The name of the ad hoc wireless network.
BSSID	The MAC address of the ad hoc network.
Channel	The radio frequency channel on which the ad hoc network operates.
RSSI (dBm)	The received signal strength indication, measured in decibels relative to one milliwatt (dBm), of the ad hoc network.
Manufacturer	The manufacturer name of the device creating the ad hoc network.
First Seen	The date and time when the ad hoc network was first detected.
Last Seen	The date and time when the ad hoc network was last detected.
Nearest AP Hostname	The hostname of the nearest AP to the ad hoc network.
Detecting APs	The number of APs that have detected the ad hoc network.

Allowlist APs

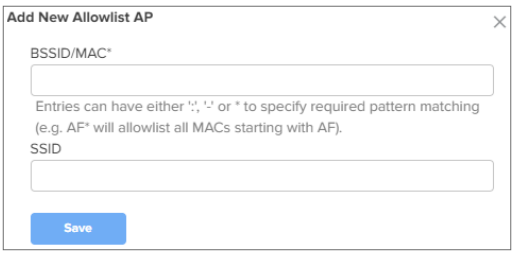
Allowlist APs allow administrators to configure the SSID and MAC addresses of authorized access points, providing control over permitted devices in the network infrastructure.

To add Allowlist APs, follow these steps:

1. Navigate to **WIDS** > **Allowlist APs**.



2. Click **Add New**. The **Add New Allowlist AP** windows appears.



3. Enter the **BSSID/MAC** address.
4. Enter **SSID.**
5. Click **Save**.

The following parameters related to Whiteilist APs are displayed:

Table 41 *Allowlist APs parameters*

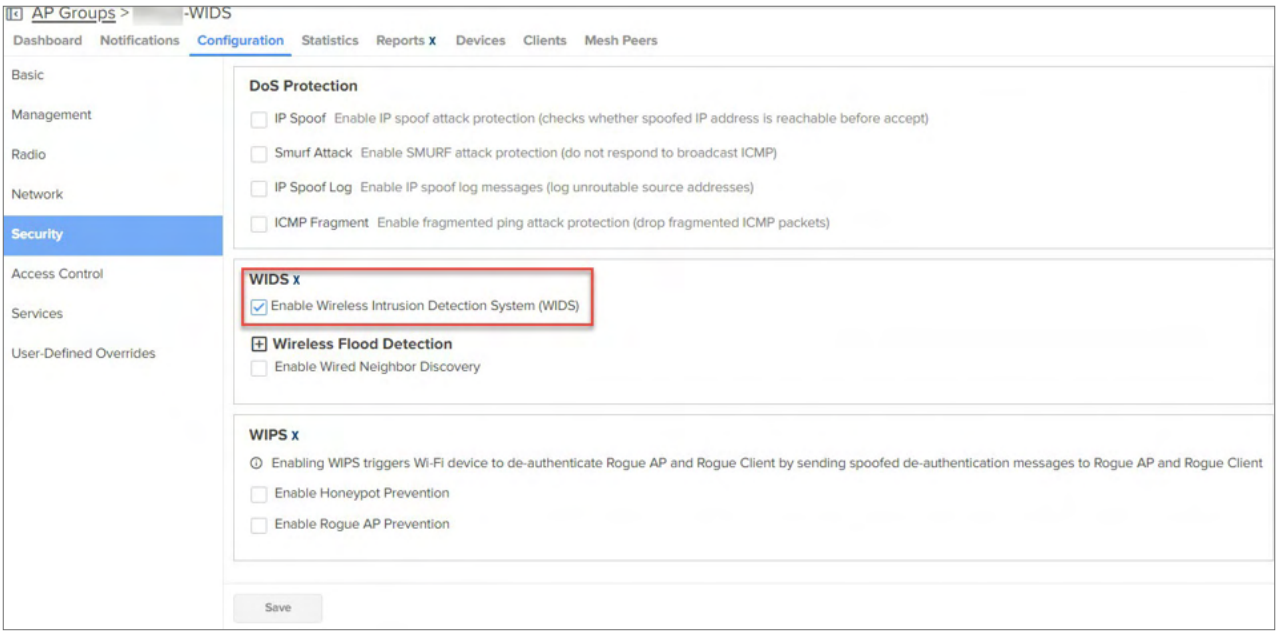
Field	Description
SSID	The name of the wireless network.
BSSID	The MAC address of the AP.
Manufacturer	The manufacturer of the AP.
Delete All	Allows to delete all Allowlist APs in the list.

Configuring WIDS

To enable WIDS feature perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** > **AP Groups** tab.
2. Select the **AP Group** and navigate to **Security** page.

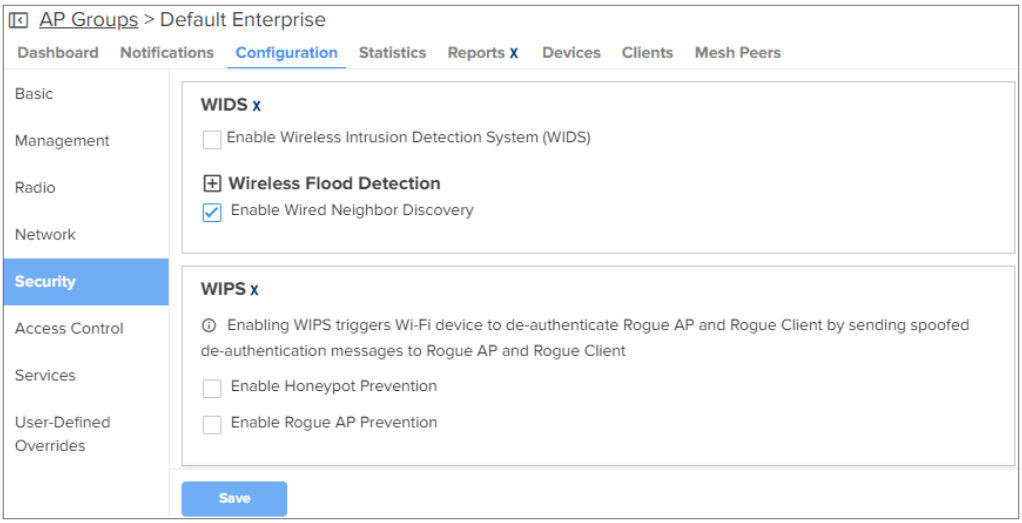
3. Select the **Wireless Intrusion Detection System (WIDS)** checkbox.



Configuring Wired Neighbor Discovery

To enable wired neighbor discovery, perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** tab.
2. Select the **AP Group** and navigate to the **Security** page.
3. Select the **Enable Wired Neighbor Discovery** checkbox.



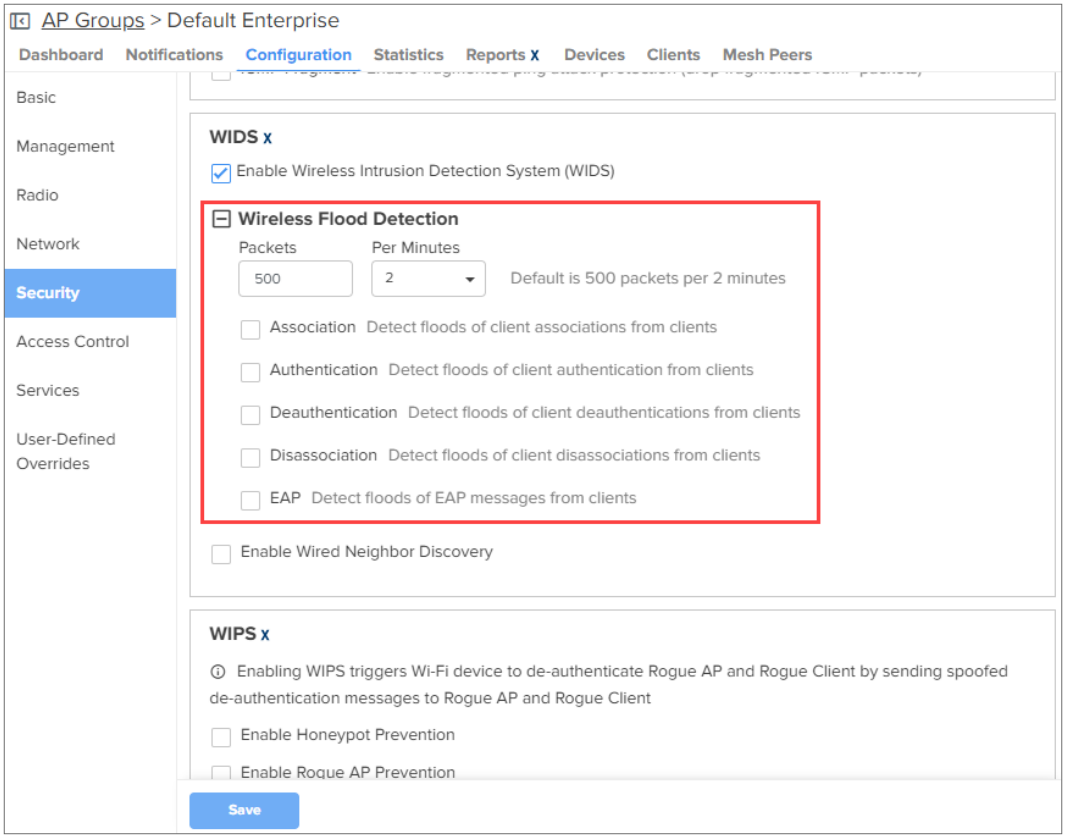
Wireless Flood Detection

Wireless Flood Detection in cnMaestro is crucial for identifying and mitigating flood attacks in wireless networks. This feature provides administrators with the ability to monitor various parameters to detect potential flood attacks and take appropriate actions.

Note

You need to enable the WIDS to configure the Wireless Flood Detection and Rouge AP detection.

Wireless Flood Detection is used to detect the flood attacks of Association, Authentication, Deauthentication, Disassociation, and EAP.



Wireless Flood Detection displays the following parameters:

Table 42 *Wireless Flood Detection parameters*

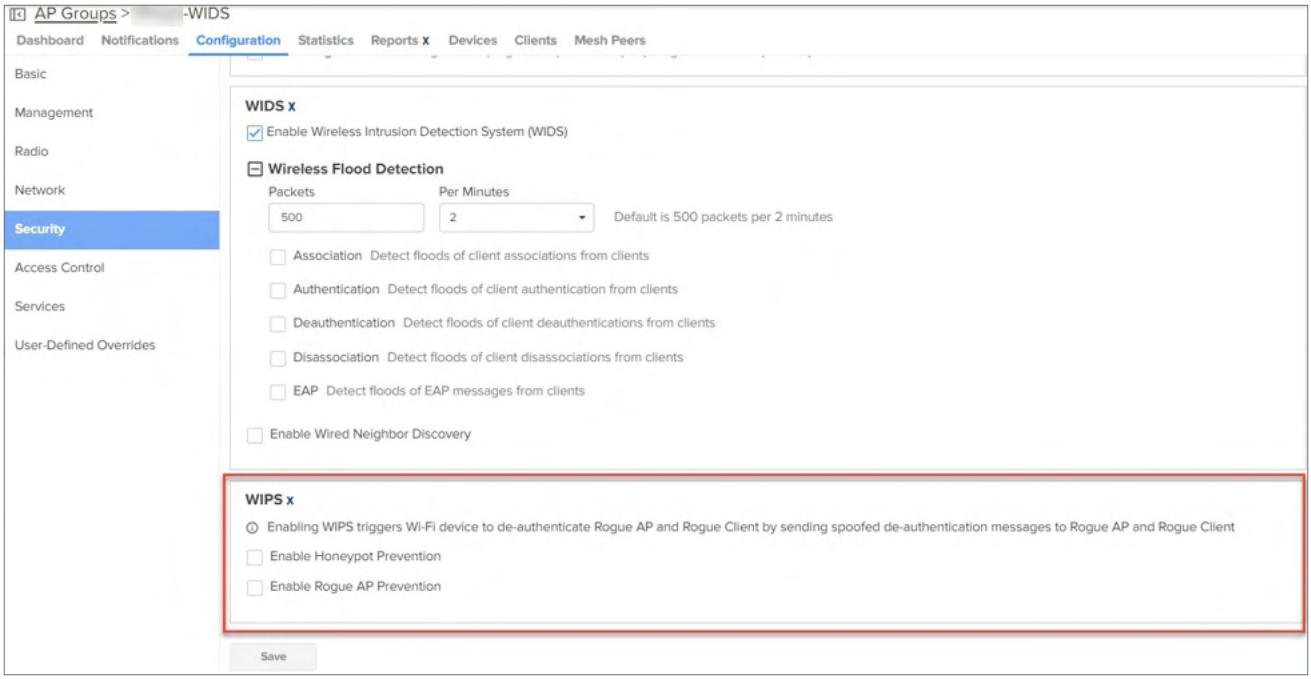
Field	Description
Association	Detect floods of client associations from clients.
Authentication	Detect floods of client authentication from clients.
Deauthentication	Detect floods of client deauthentications from clients.
Disassociation	Detect floods of client disassociations from clients.
EAP	Detect floods of EAP messages from clients.

Wireless Intrusion Prevention System (WIPS)

Note

This is a beta feature.

WIPS is a critical feature within cnMaestro designed to enhance the security of wireless networks. When enabled, WIPS triggers Wi-Fi devices to deauthenticate rogue APs and clients by sending spoofed deauthentication messages to the rogue APs and clients. You can also trigger Wi-Fi devices to deauthenticate honeypot APs and clients by enabling this feature.



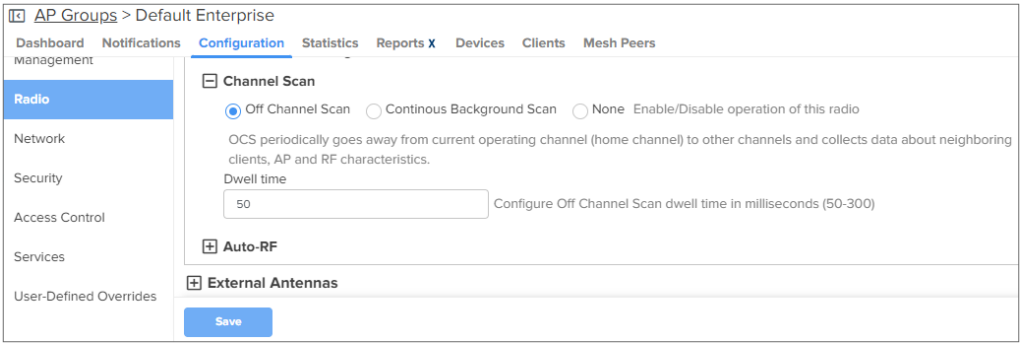
Off Channel Scan (OCS)

Note

- OCS (on 2.4 GHz, 5 GHz and 6 GHz) and Rogue AP detection should be enabled for WIDS option to work at Site level in cnMaestro.
- It will take 20 minutes to detect Rogue AP on AP boot up.

To enable OCS (Off Channel Scan):

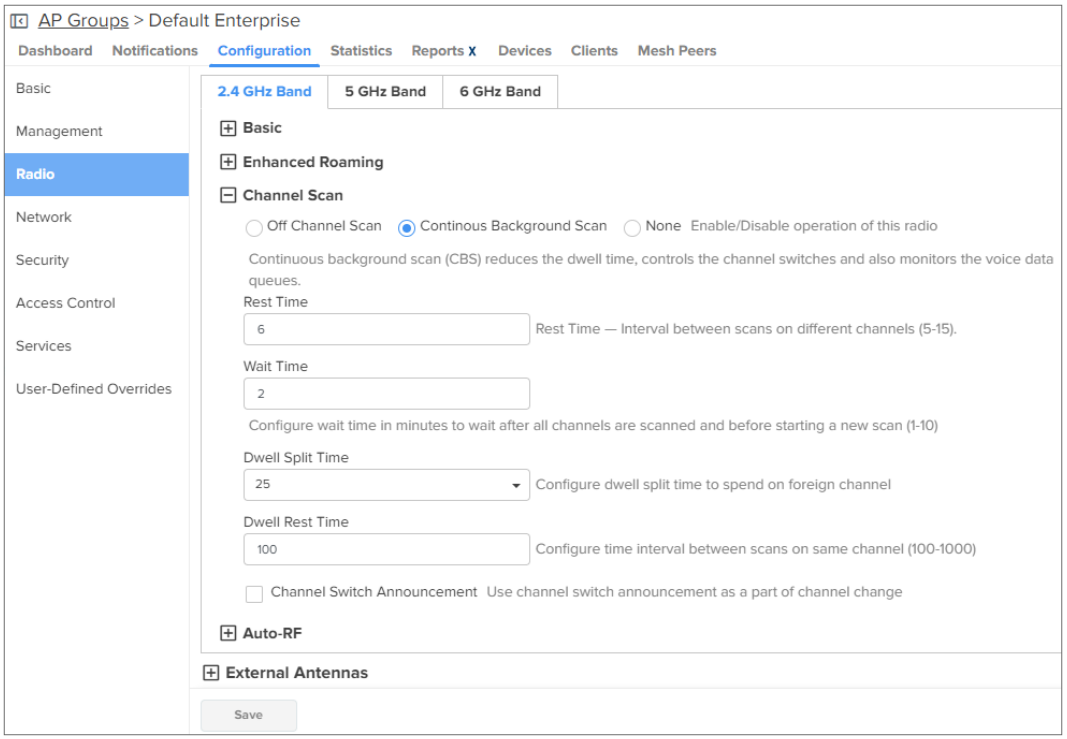
1. Navigate to **Configuration** > **Wi-Fi Profiles** > **AP Groups** > **Radio** (Available on all radios—2.4 GHz, 5 GHz, and 6 GHz) page.
2. Expand **Channel Scan** section and select **Off Channel Scan** option.
3. Click **Enable OCS** to periodically scan the network.



4. Enter **Dwell time** as required.
5. Click **Save**.

Continuous Background Scan (CBS)

CBS reduces the dwell time, controls the channel switches and also monitors the voice data queues.



To enable CBS:

1. Navigate to **Configuration** > **Wi-Fi Profiles** > **AP Groups** > **Radio** (Available on all radios—2.4 GHz, 5 GHz, and 6 GHz) page.
2. Expand **Channel Scan** section and select **Continuous Background Scan** option.
3. Configure rest time in seconds (5-15).
4. Configure wait time in minutes to wait after all channels are scanned and before starting a new scan (1-10).
5. Configure dwell split time to spend on foreign channel.
6. Configure time interval between scans on same channel (100-1000).
7. Enable Channel Switch Announcement.
8. Click **Save**.

Network Service Edge (NSE 3000)

The Network Service Edge (NSE 3000) delivers advanced security, routing and SD-WAN policies for small and medium enterprises. NSE 3000 model has two Gigabit WAN ports and four Gigabit LAN ports. It offers WAN throughputs of up to 1 Gbps. NSE 3000 is managed using the cloud-hosted cnMaestro (a management solution from Cambium Networks).

This section describes the following tabs available in cnMaestro for NSE 3000 model:

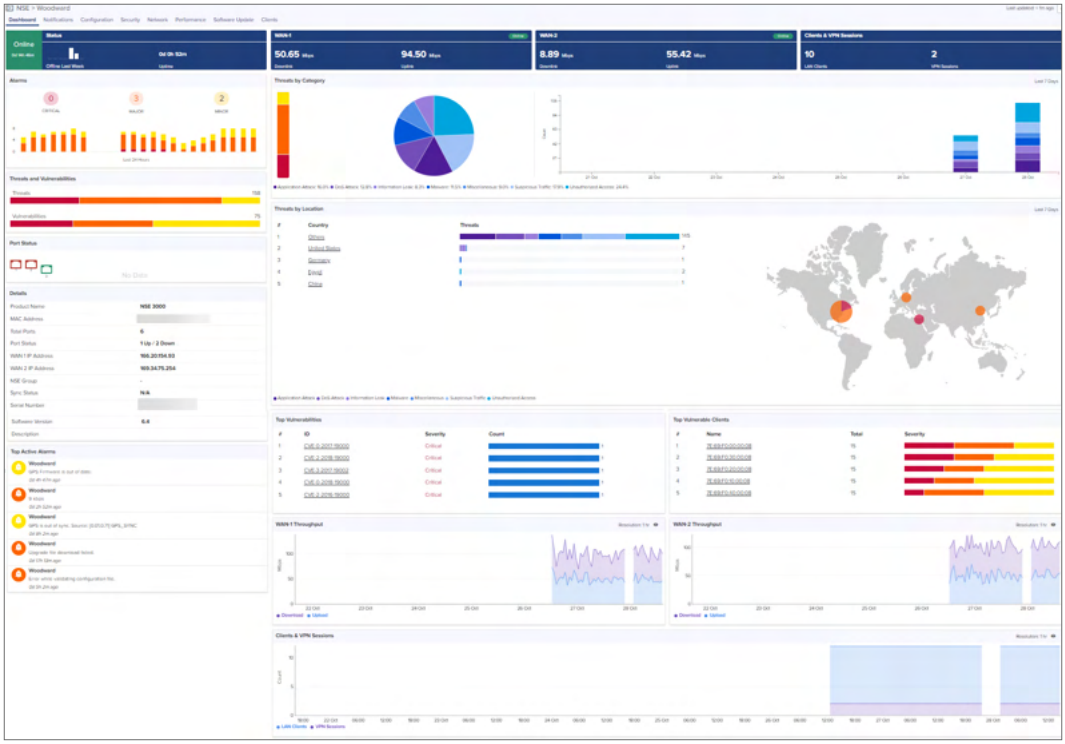
- Dashboard
- Notifications
- Configuration
- Security
- Network

- Tools
- Clients
- Certificate

Dashboard

Dashboard widgets provides you a comprehensive overview of NSE device and network health. The dashboard displays **Details** of NSE device, status of **WAN-1** and **WAN-2** usage, number of **LAN Clients & VPN Sessions**, **Alarms**, **Threats by Category**, **Threats and Vulnerabilities** categorized as **Critical, Major** and **Minor**, **Port Status**, **Top Vulnerabilities**, **Top Vulnerable Clients**, **Top Active Alarms**, **WAN-1 and WAN-2 Throughput**, and **Clients and VPN Sessions**.

Figure 180 *The NSE dashboard page*



Notifications

Notifications consist of Alarms, Alarms History, and Events. They are synchronous messages that provide real-time system status.

Figure 181 *The Notifications page*

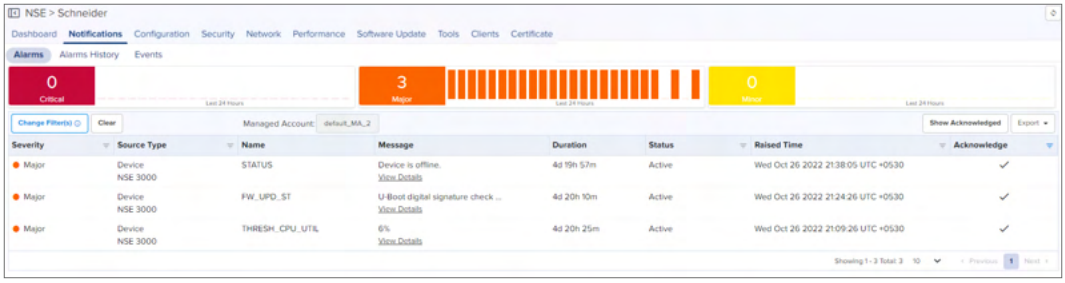


Table 43 *Notification overview*

Type	Description
Alarms	Alarms have a state and persist as long as the problematic activity continues; they reflect the current health of the devices in the network. The inactive alarms are removed from the alarms page after 10 minutes.
Alarms History	Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts. The history contains both the outstanding (active) and inactive alarms.
Events	Events are stateless, transient messages that occur in response to an input or action, such as if the CPU exceeds a threshold or a device association fails. Events are fire-and-forget; they are stored in an Event Table and provide a history of device activity.

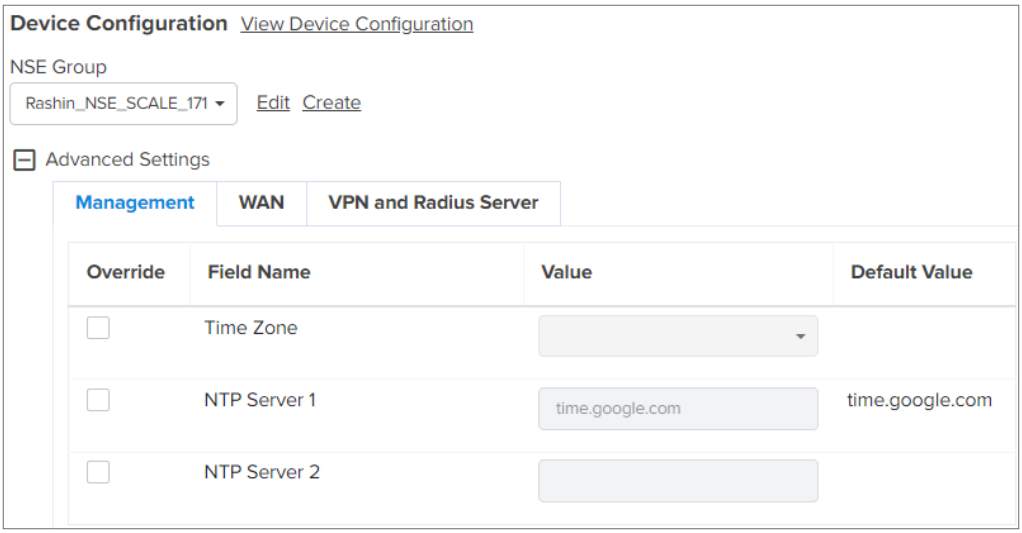
Configuration

The Configuration page allows you to configure the following for a device:

- Advanced Settings
- Factory Reset
- User-Defined Overrides
- Configuration Lock

To apply the Configuration Method, perform the following:

1. Navigate to the **Configuration** page.
2. In the **Device Configuration** section, select an NSE group from the **NSE Group** drop-down list.



To view the jobs, click **View Configuration Jobs** or navigate to **Administration** > **Jobs** > **Configuration Update**.

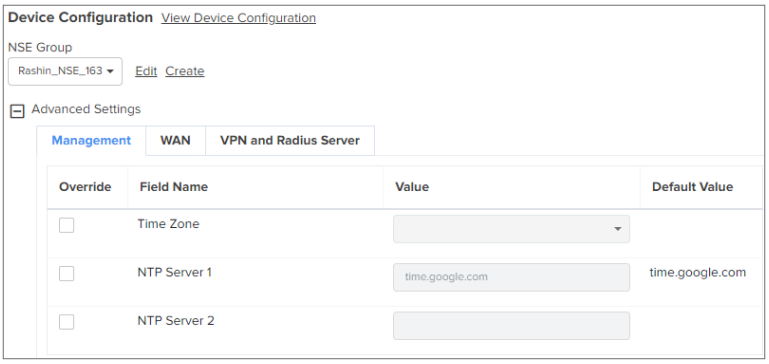
Advanced Settings

In the **Advanced Settings** you can configure the following tabs:

- Management
- WAN
- VPN and Radius Server

Management

1. In the **Management** tab, select the **Field Name** to override the settings.



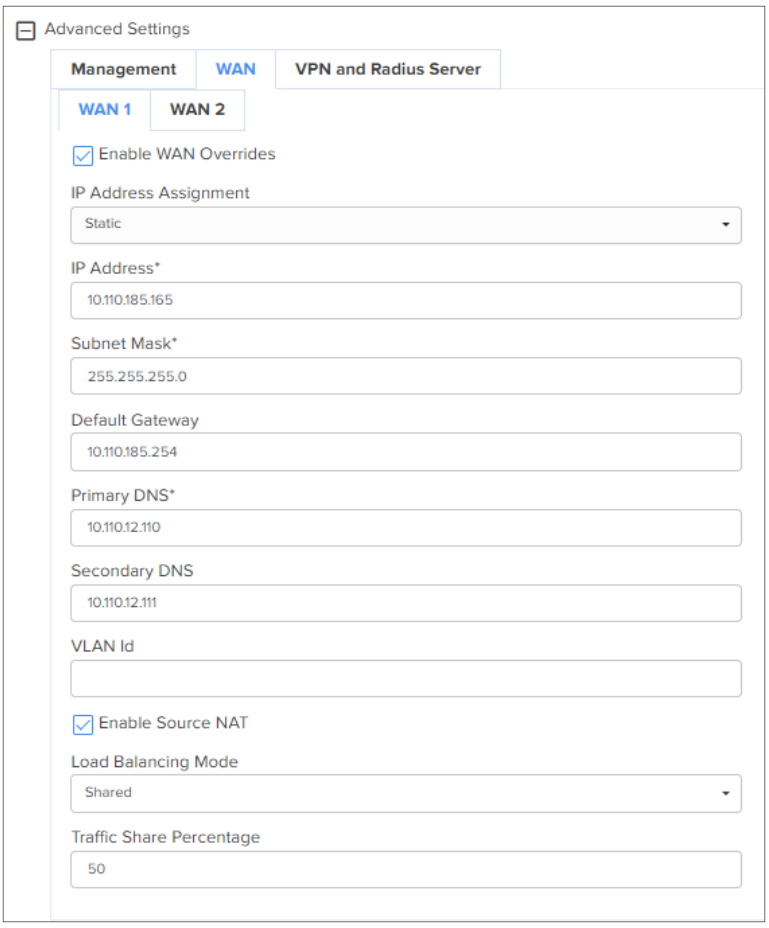
2. Click **Apply Configuration**.

WAN

In the **WAN**, you can override settings for **WAN 1** and **WAN 2.**

WAN 1

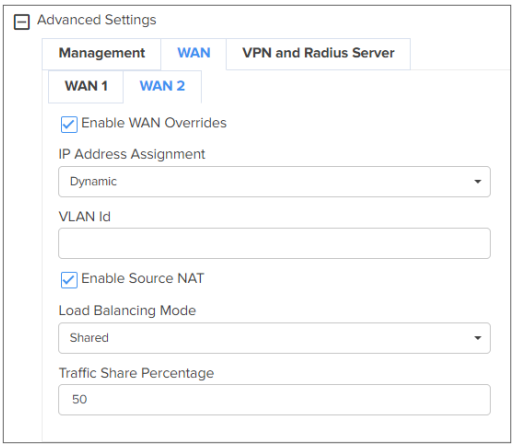
1. Select **Enable WAN Overrides** option.



2. Select the fields to override.
3. Click **Apply Configuration**.

WAN 2

1. Select **Enable WAN Overrides** option.

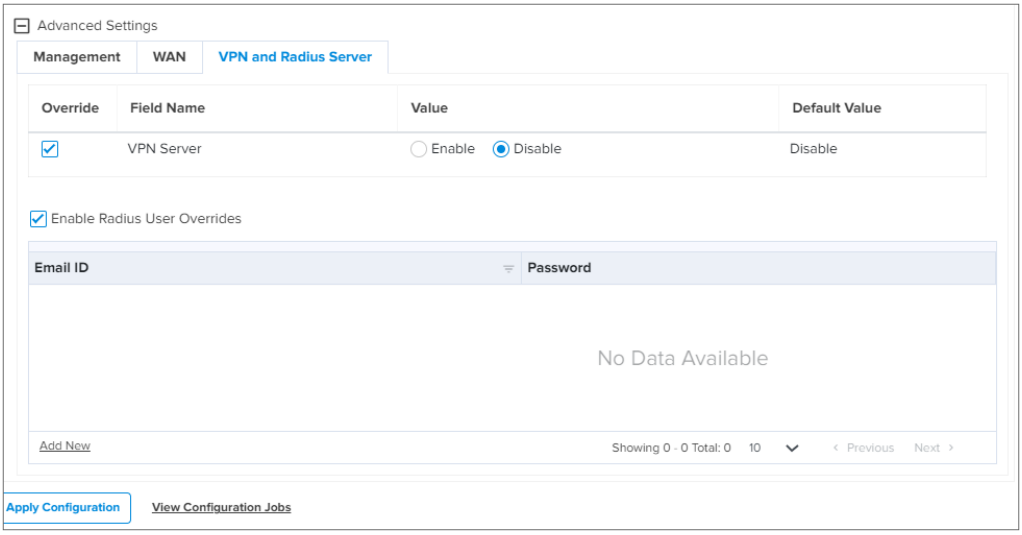


2. Select the fields to override.
3. Click **Apply Configuration**.

VPN and Radius Server

In the **VPN and Radius Server** tab you can override VPN and Radius Server settings.

1. Select VPN overrides field name.

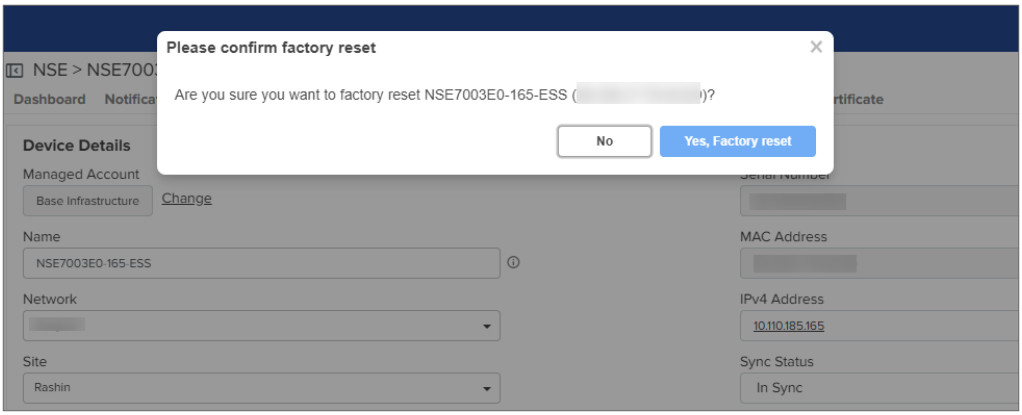


2. Select **Enable Radius User Overrides** option.
3. Click **Apply Configuration**.

Factory Reset

To erase all the configuration on the device and bring the device back to the default factory configuration, follow these steps:

1. Navigate to the **NSE > Configuration** page.
2. Click **Factory Reset**.



3. In the pop-up window that appears, Click **Yes, Factory Reset**.

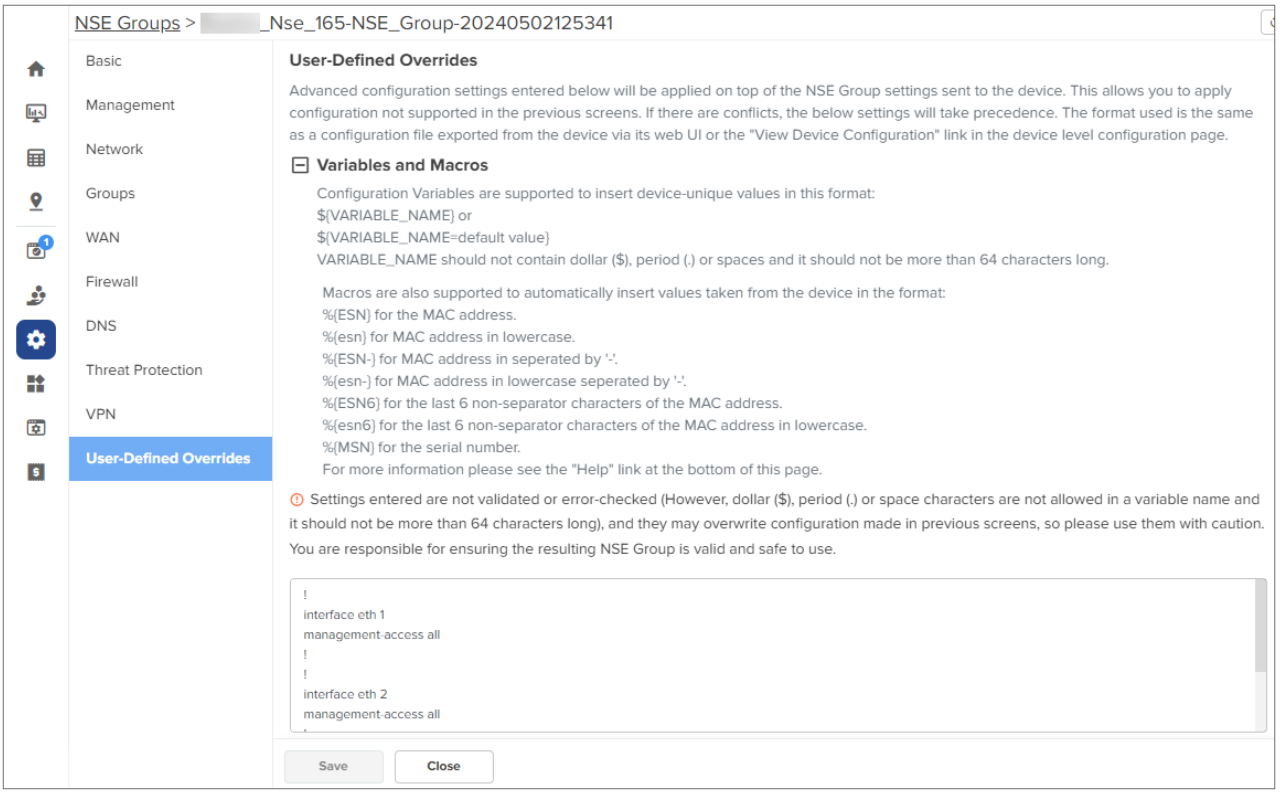
User-Defined Overrides

User-Defined Overrides are appended to the NSE groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI.

To configure overrides based on your customized requirements by using variables and macros, follow these steps:.

1. Navigate to the **NSE > configuration** page.
2. Define your overrides in the text box.

Figure 182 *The User-Defined Overrides page*



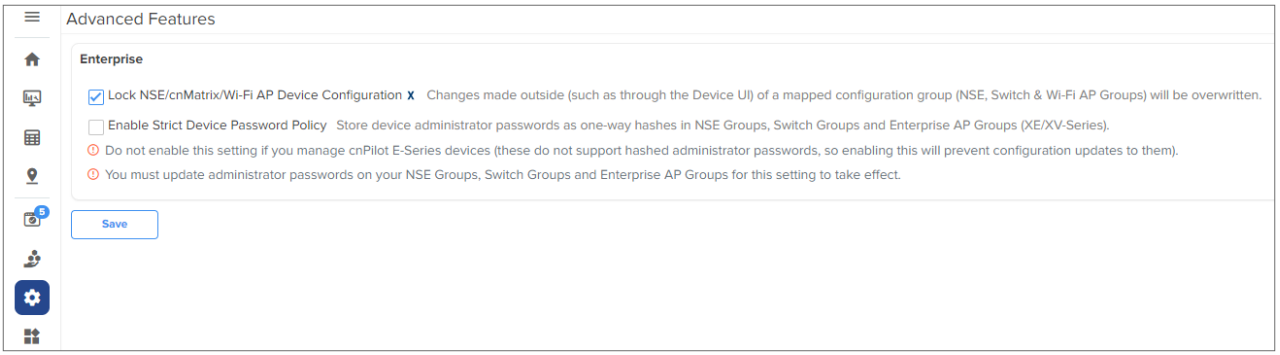
3. Click **Save**.

Configuration Lock

Configuration Lock forces the configuration on NSE and cnMaestro to be in sync always. If there is any configuration change done directly on the device, then cnMaestro tracks that device and triggers a configuration sync job to bring back the device to same configuration which is applied from the NSE Group.

To enable the configuration lock, follow these steps:

1. Navigate to the **Configuration** > **Advanced Features**.
2. Select the **Lock NSE/cnMatrix/Wi-Fi AP Device Configuration** check box.



3. Click **Save**.

Security

The **Security** page allows you to report the vulnerability and threats detected by the device.

Threats

1. Navigate to **NSE** > **Security** > **Threats**.
2. Select **Time Range** from the drop-down.
    - Last 24 hours
    - Last 7 Days
    - Last 30 Days

The threat page displays **Threat by Location, Total Threats,** and threat categories based on **Critical, Major, Minor,** and origin of the threat (country of origin). The bar graph on the left hand side displays the count based upon the threat **by Category**. The pie chart displays the percentage of threats with respect to other threats. The per day bar chart displays the threat count aggregated on per day basis.

Figure 183 *The Threats page*

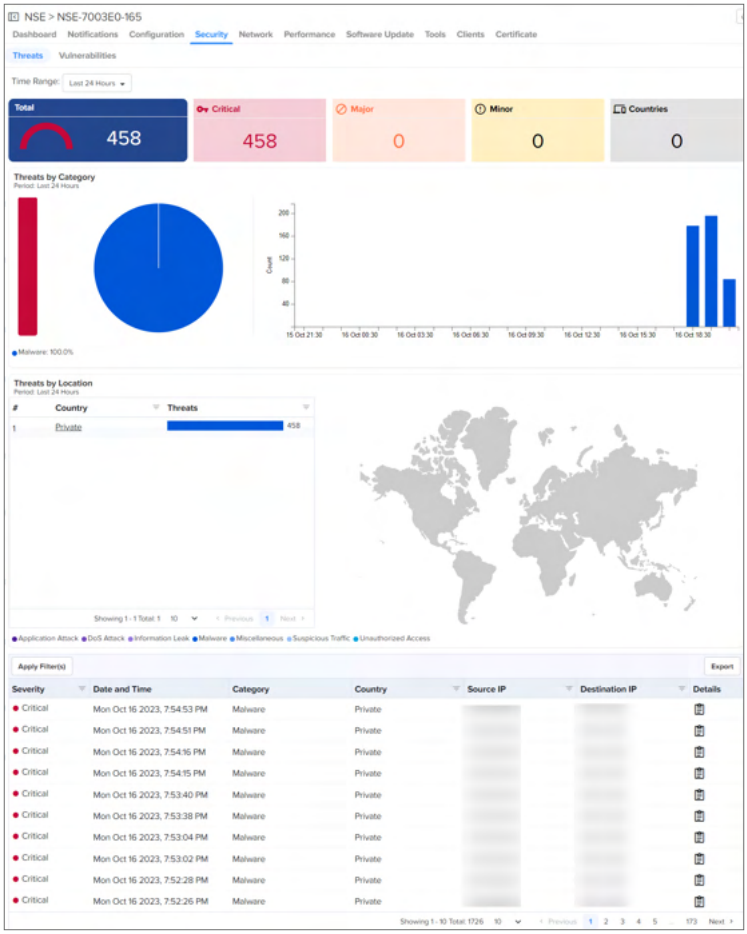
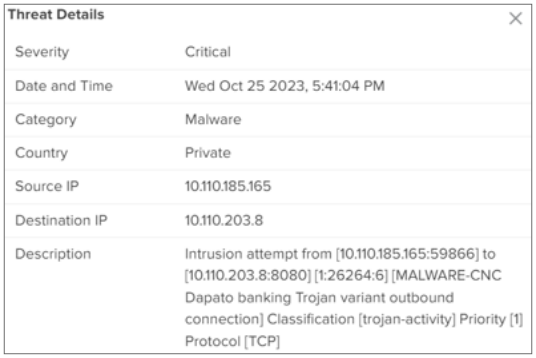


Table 44 *Parameters on the Threats page*

Parameter	Description
Severity	The severity of threat such as Critical, Major, and Minor.
Date and Time	The date and time of the threat occurrence.
Category	Displays any of the following categories of threat: • Application Attack • DoS Attack • Information Leak • Malware • Miscellaneous • Suspicious Traffic • Unauthorized Access
Country	The source country of the threat is displayed for threats that originate from WAN to LAN.
Source IP	Source IP address of the flow which is resulted in the threat.
Destination IP	Destination IP address of the flow which is resulted in the threat.
Details	Displays the above details in a single window in addition to a description of the threat. When you click the icon, the **Threat Details** window appears, as shown in Figure 184.

Figure 184 *The Threat Details window*



Vulnerabilities

The Vulnerabilities page displays **Total Vulnerabilities, Unique Critical, Unique Major, Unique Minor,** and **Vulnerable Clients.**

Figure 185 *The Vulnerabilities page*

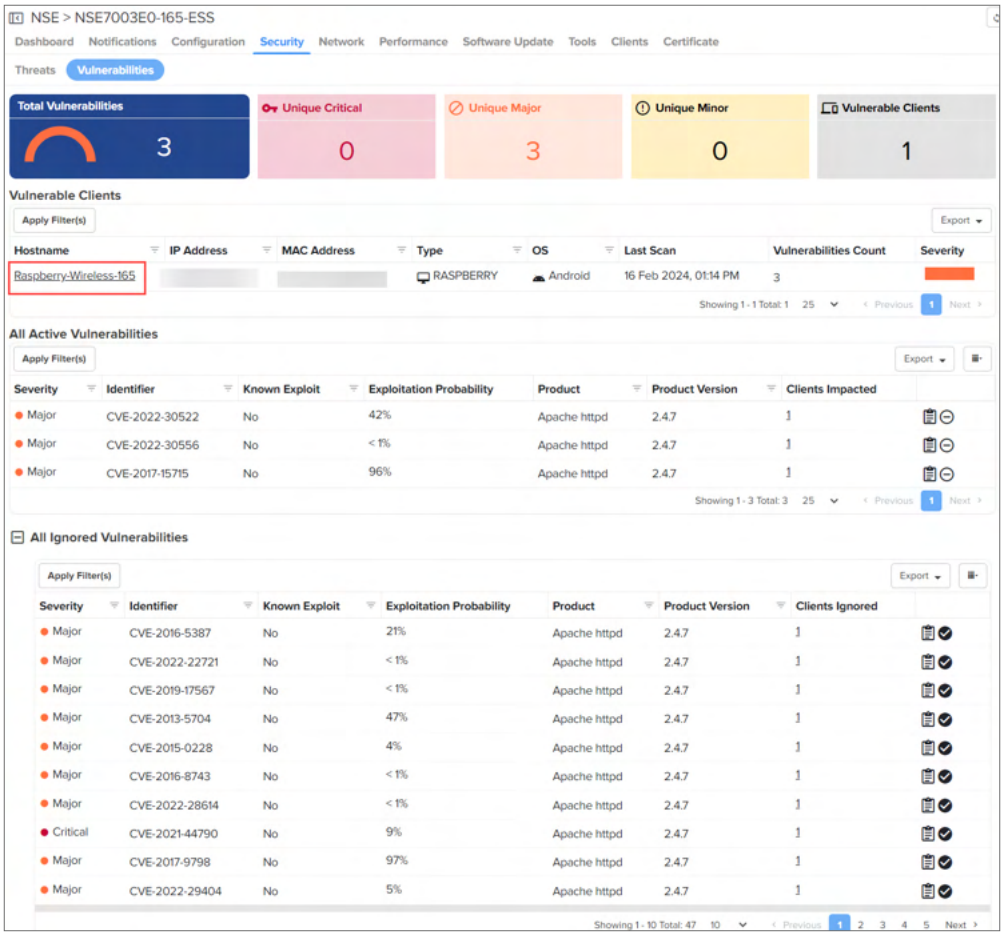


Table 45 *Parameters on the Vulnerabilities page*

Parameter	Description
Vulnerable Clients	
Hostname	Hostname of the client. When you click the hostname, you can view the vulnerabilities discovered by the NSE for the

Table 45 *Parameters on the Vulnerabilities page*

Parameter	Description
	client, as shown in Figure 201.
IP Address	Source IPv4 address of the vulnerable client.
MAC Address	MAC address of the client.
Type	Type of client. For example, Computer, or Switch.
OS	Operating system running on the client. For example, Windows, or macOS.
Last Scan	Date and time of the last security scan performed on the client.
Vulnerabilities Count	Number of vulnerabilities found on the client during the security scan.
Severity	Level of severity assigned to each vulnerability, such as Critical, Major, or Minor.
Export	Exports a list of vulnerable clients. The following options are supported: • **Export page as CSV** • **Export page as PDF** • **Export all as CSV**
All Active Vulnerabilities	
Severity	The severity level of the vulnerability: • Critical • Major • Minor
Identifier	CVE ID number for the discovered vulnerability.
Service	Service of the vulnerability.
Port	Port number of the service.
Known Exploit	Indicates whether the vulnerability is exploited in the wild and is present in the Known Exploited Vulnerabilities (KEV) catalog. For information on KEV catalog, see Known Exploited Vulnerabilities Catalog.
Exploitation Probability	The probability (in percentage) that a vulnerability will be exploited in the next 30 days. A higher value indicates a higher probability of the vulnerability being exploited. For information on Exploit Prediction Scoring System (EPSS), see Exploit Prediction Scoring System.
Product	Name of the product.
Product Version	Version of the product.
Clients Impacted	Number of clients impacted by the vulnerability. When you click the number in the **Clients Impacted** column, a window appears as shown in Figure 186.
Details	Displays the above details in a single window in addition to a short description of the vulnerability. A short description typically includes essential information, such as details on how an attacker can potentially exploit the vulnerability and which product versions are affected by it.

Table 45 *Parameters on the Vulnerabilities page*

Parameter	Description
	When you click the Details ( ) icon, the **Vulnerability Details** window appears, as shown in Figure 187. When you click the CVE Identifier link, you can access detailed information about a specific vulnerability in the National Vulnerability Database (NVD) page, as shown in Figure 188.
Ignore 	An option to ignore vulnerability(s). When you click the ignore ( ) icon, a window appears, as shown in Figure 190. To ignore vulnerability(s), select the required vulnerability(s), provide your reason in the **Reason** field, and then click **Ignore** button. The ignored vulnerability(s) are included in **All Ignored Vulnerabilities** section.
Export	Exports a list of all active vulnerabilities. The following options are supported: • **Export page as CSV** • **Export page as PDF** • **Export all as CSV**
All Ignored Vulnerabilities	
Severity	The severity level of the vulnerability: • Critical • Major • Minor
Identifier	CVE ID number for the discovered vulnerability.
Service	Service of the vulnerability.
Port	Port number of the service.
Known Exploit	Indicates whether the vulnerability is exploited in the wild and is present in the Known Exploited Vulnerabilities (KEV) catalog. For information on KEV catalog, see Known Exploited Vulnerabilities Catalog.
Exploitation Probability	The probability (in percentage) that a vulnerability will be exploited in the next 30 days. A higher value indicates a higher probability of the vulnerability being exploited. For information on Exploit Prediction Scoring System (EPSS), see Exploit Prediction Scoring System.
Product	Name of the product.
Product Version	Version of the product.
Clients Ignored	Number of clients ignored. When you click the number in the **Clients Ignored** column, a window appears as shown in Figure 191.
Details 	Displays the above details in a single window in addition to a short description of the vulnerability. A short description typically includes essential information, such as details on how an attacker can potentially exploit the vulnerability and which product versions are affected by it.

Table 45 *Parameters on the Vulnerabilities page*

Parameter	Description
	When you click the Details ( ) icon, the **Vulnerability Details** window appears, as shown in Figure 187. When you click the CVE Identifier link, you can access detailed information about the specific vulnerability in the National Vulnerability Database (NVD) page, as shown in Figure 188.
Re-activate	An option to reactivate the ignored vulnerability(s). When you click the Reactivate ( ) icon, a window appears, as shown in Figure 192. To reactivate an ignored vulnerability(s), select the vulnerability(s) and then click **Re-activate** button. The reactivated vulnerability(s) are included in **All Active Vulnerabilities** section.
Export	Exports a list of all ignored vulnerabilities. The following options are supported: • **Export page as CSV** • **Export page as PDF** • **Export all as CSV**

Figure 186 *A window with impacted clients*

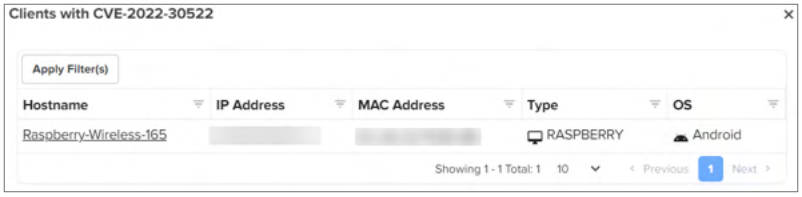


Figure 187 *The Vulnerability Details window*

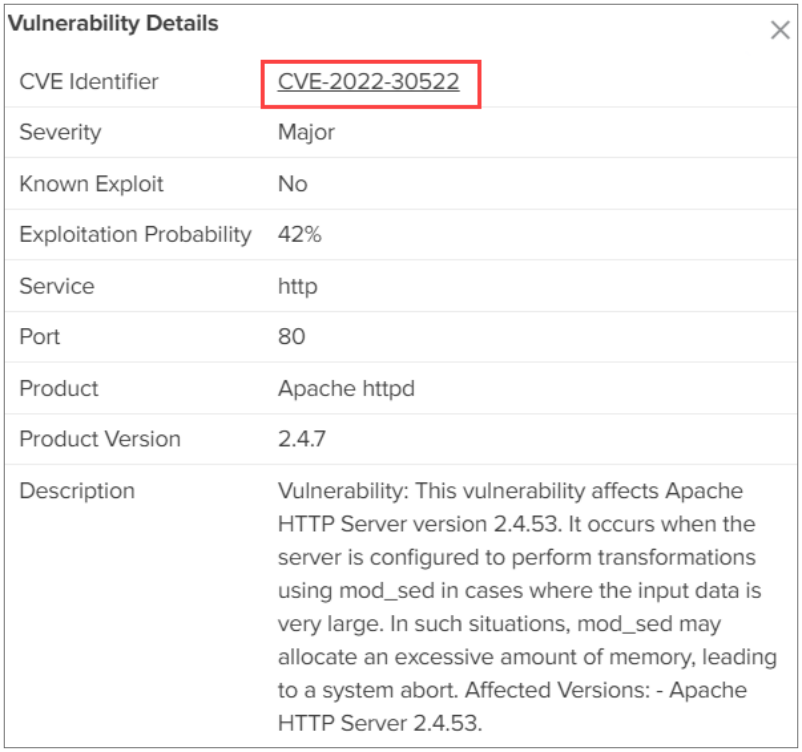
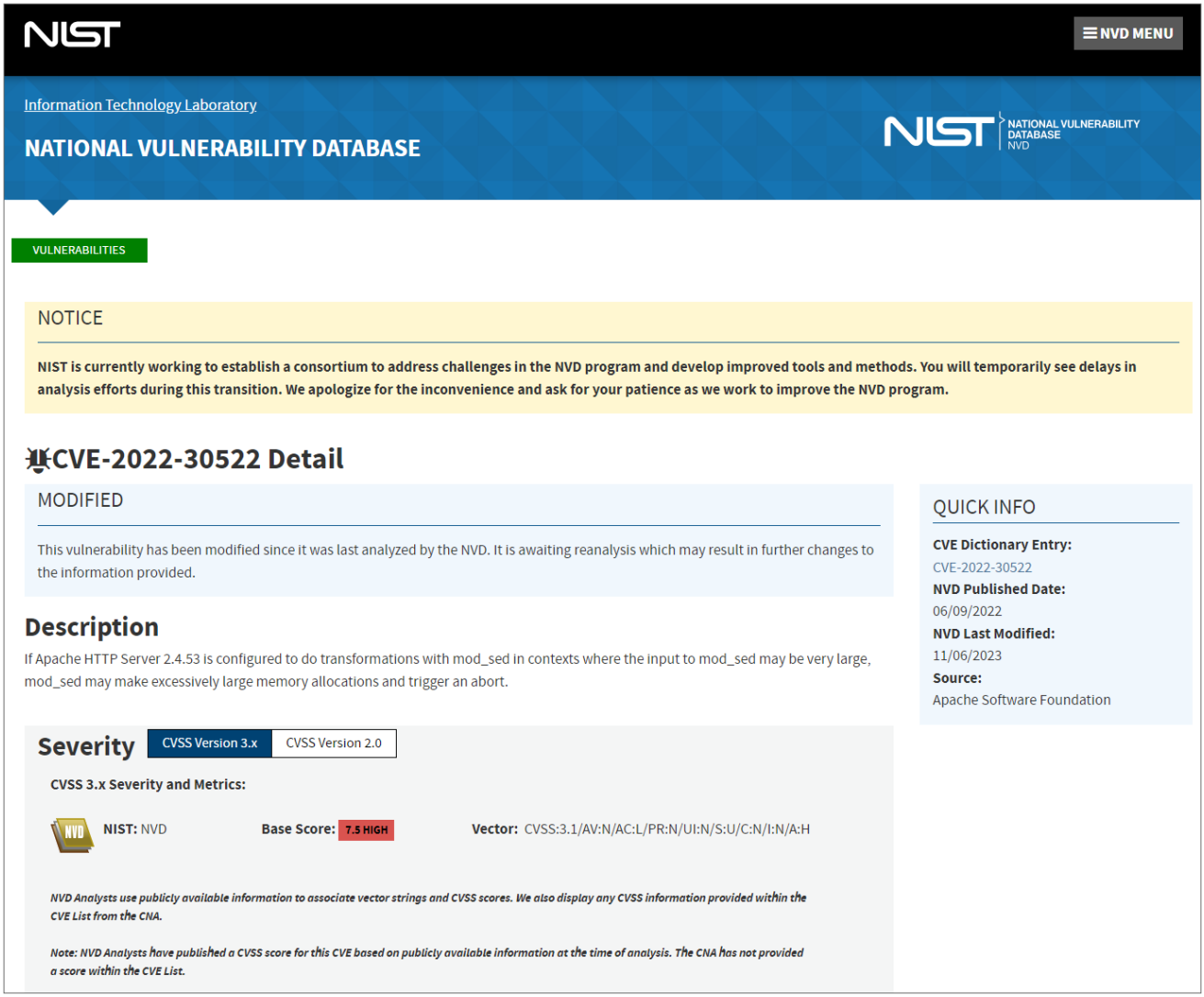


Figure 188 *The NVD page*



You can refine your search results using **Apply Filter(s)** option as shown in Figure 189.

Figure 189 *Apply Filter(s) option*

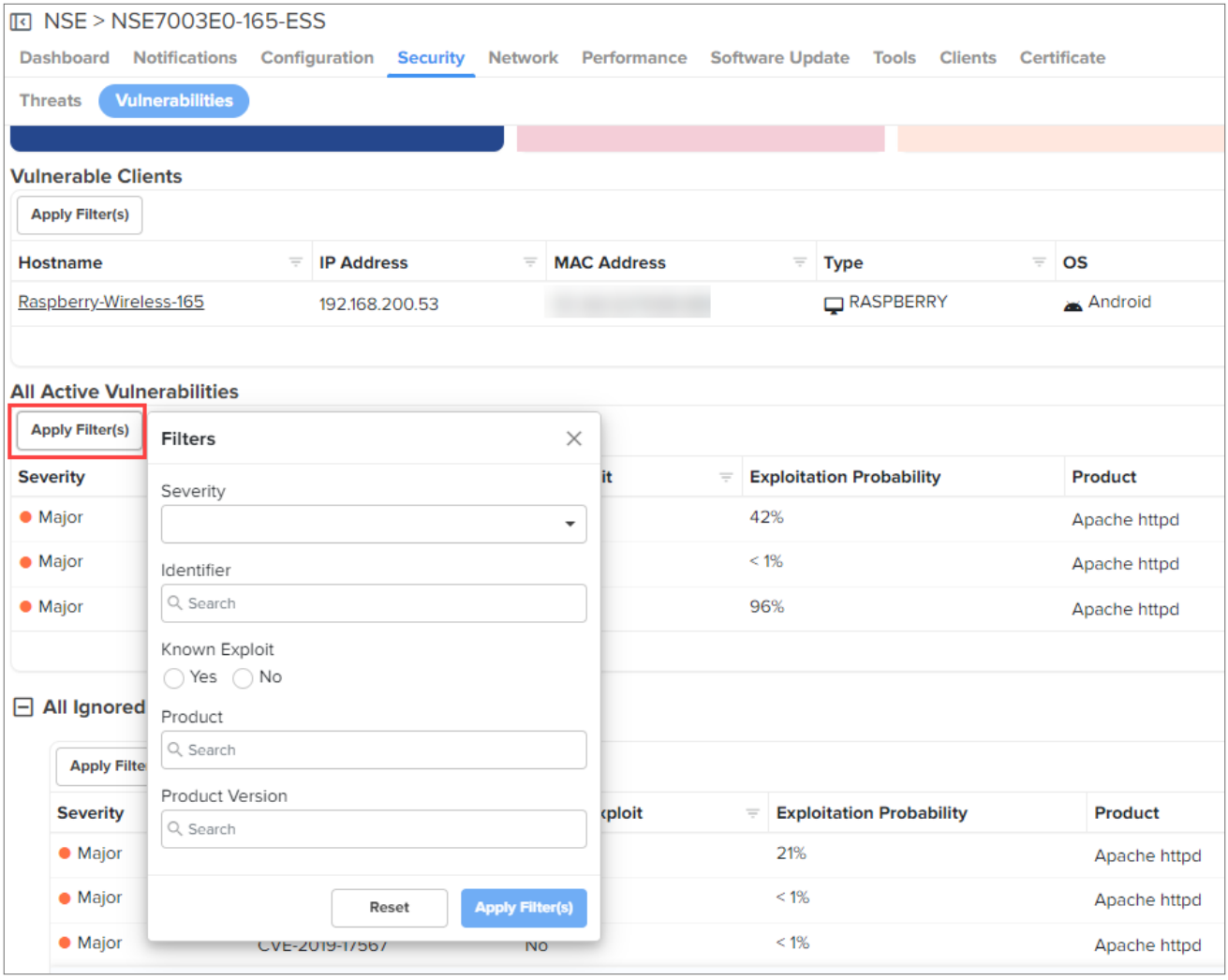


Figure 190 *A window with an option to ignore the client(s)*

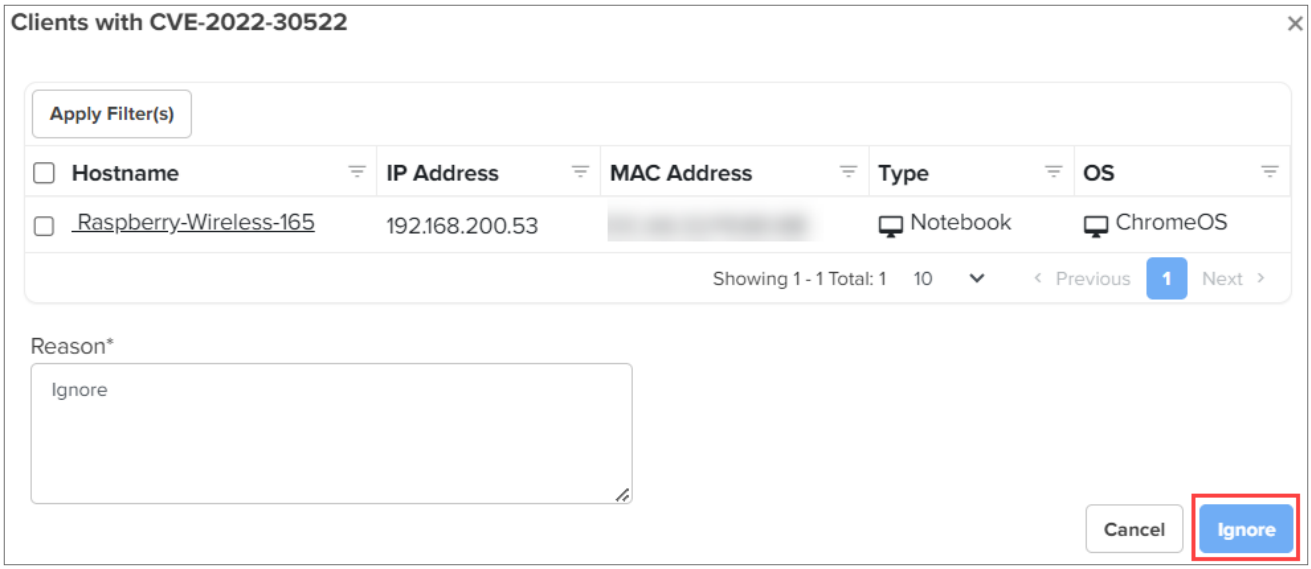


Figure 191 *A window with ignored clients*

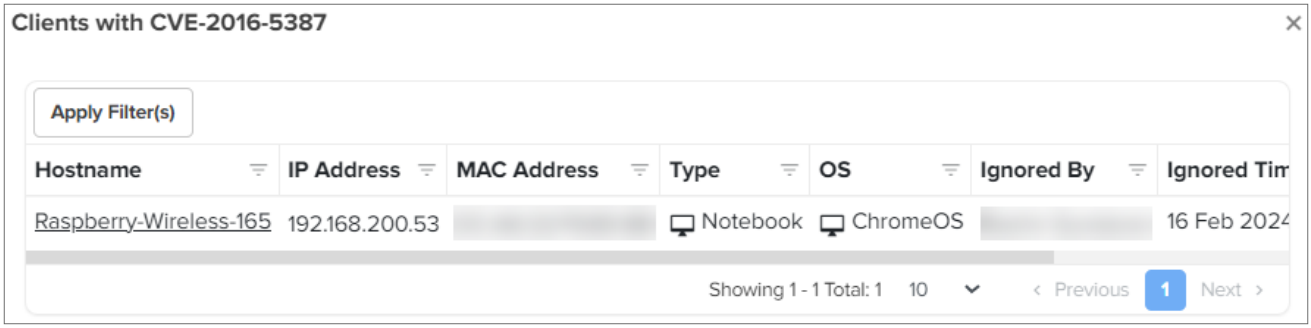
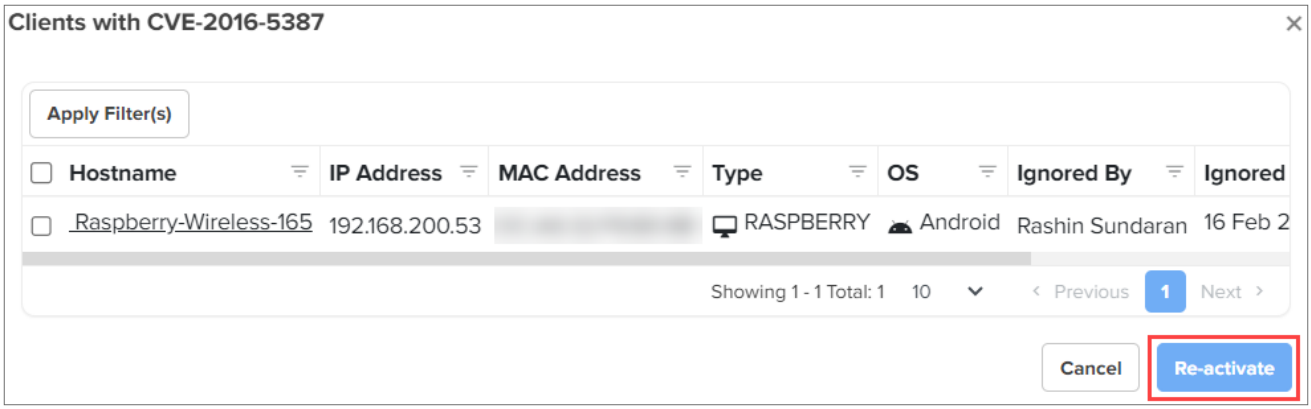


Figure 192 *A window with an option to reactivate*



Network

Network page displays information about onboard DHCP servers, Route table, and WAN statistics.

LAN

LAN page displays **Subnet** and **DHCP Leases**. You can **Apply Filters** for the table header to search for a specific parameter in the table.

Figure 193 *The LAN page*

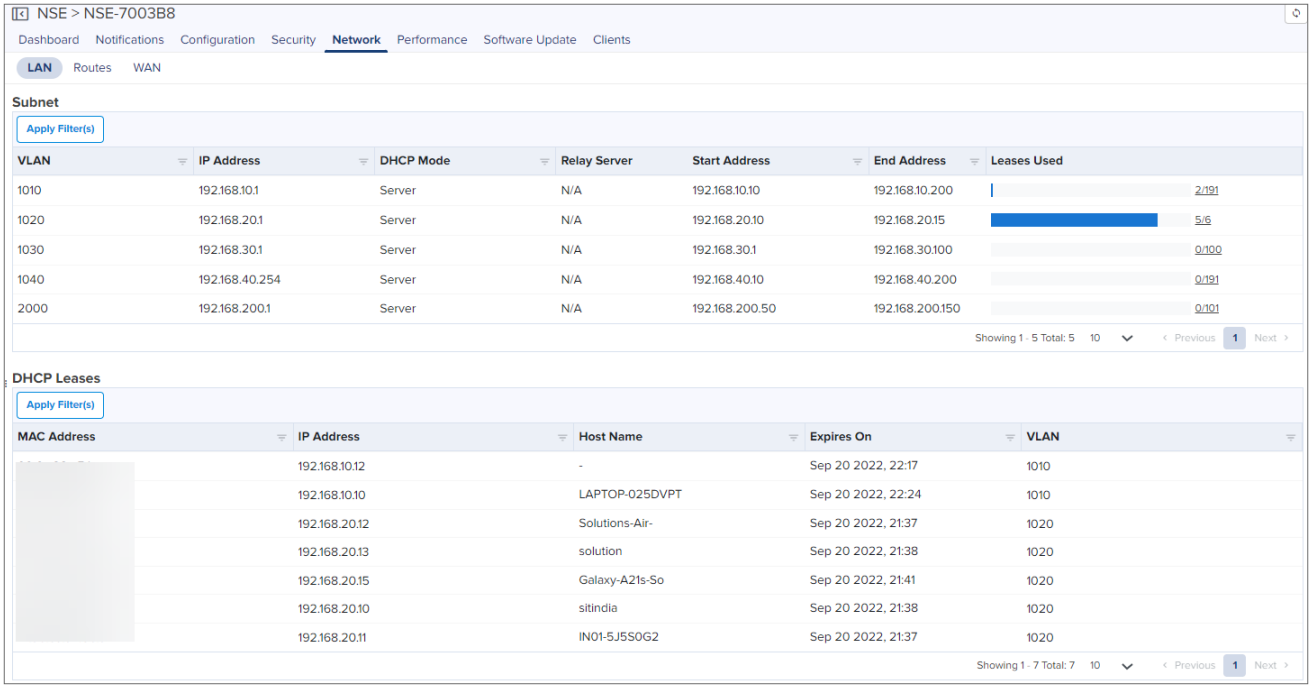


Table 46 *Parameters displayed in LAN*

Parameter	Description
Subnet	
VLAN	VLAN ID.
IP Address	Static IP address of the VLAN interface.
DHCP Mode	Status of the DHCP server mode enabled or disabled.
Relay Server	Status of the relay server mode enabled or disabled.
Start Address	DHCP pool start IP address.
End Address	DHCP pool end IP address.
Lease Used	Active IP address issued by the DHCP server.
DHCP Leases	
MAC Address	MAC address of the client.
IP Address	The leased IP address to the client.
Host Name	The hostname of the client.
Expires On	The duration for the leased IP.
VLAN	The VLAN ID assigned to the client.

Routes

Routes page displays layer 3 routing table of the device. You can **Apply Filters** for the table header to search for a specific parameter in the table.

Figure 194 *The Routes page*

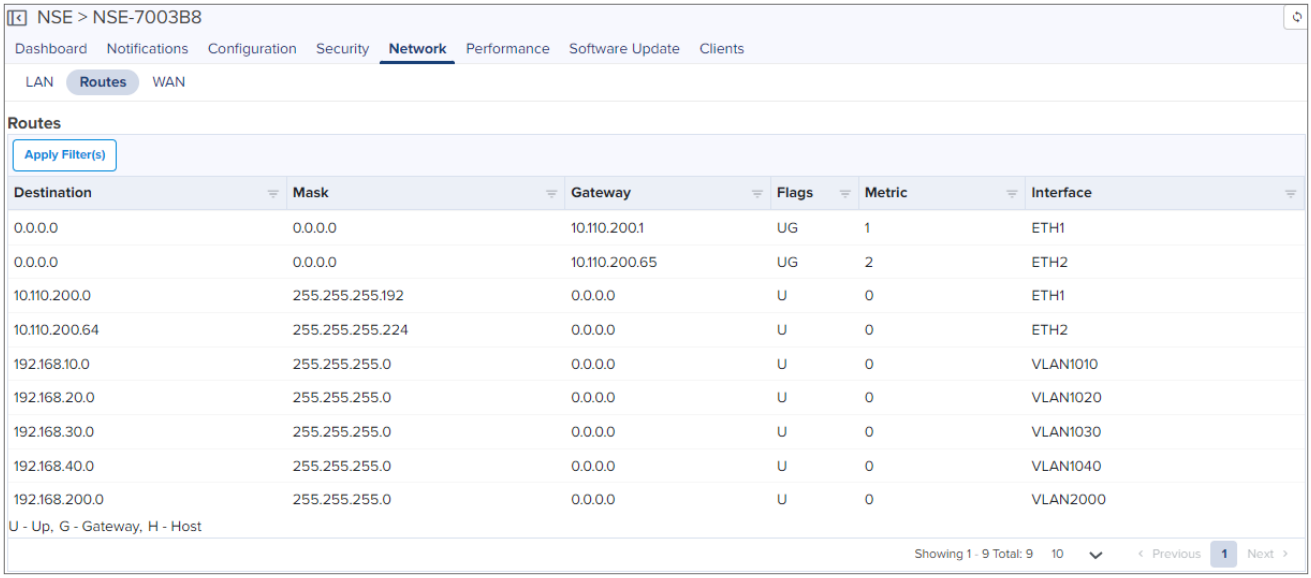


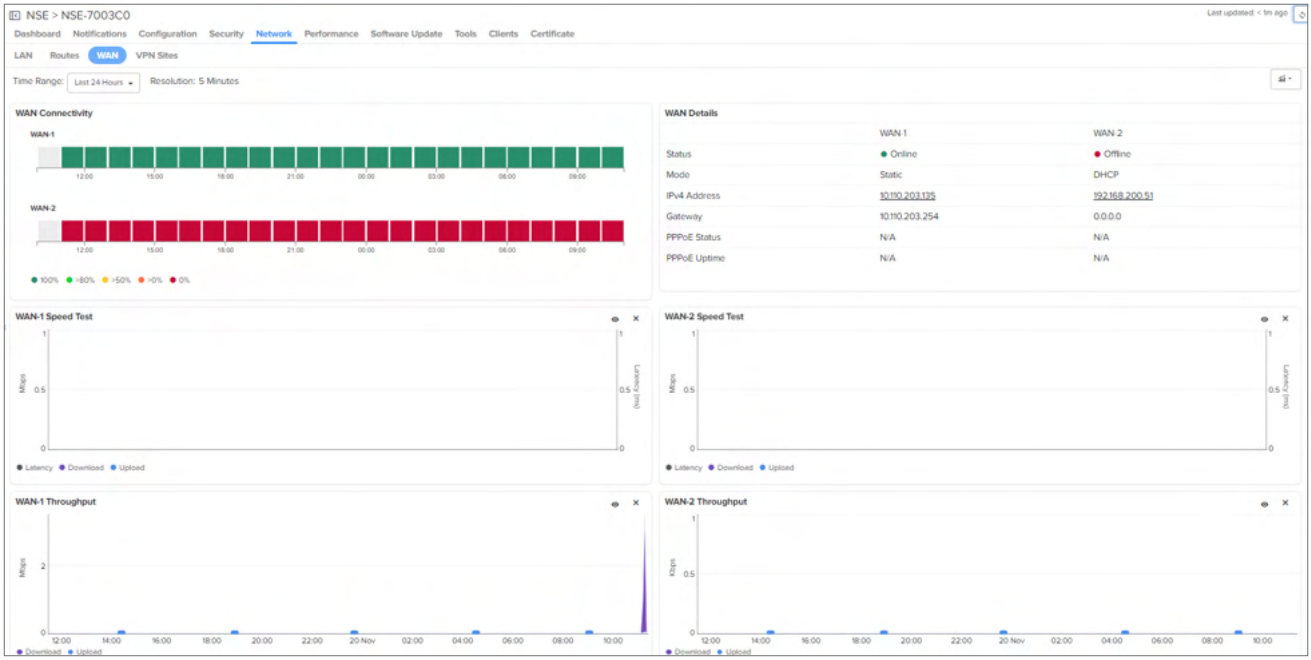
Table 47 *Parameters on the Routes page*

Parameter	Description
Routes	
Destination	Destination address of the routes.
Mask	Subnet mask of the specific route.
Gateway	Default gateway of the routes.
Flags	Flags of the routes.
Metric	Metric of the routes.
Interface	Interface of the routes.

WAN

WAN page displays **WAN Connectivity, WAN Details,** graphical representation of **Speed Test, Throughput** in **WAN-1** and **WAN-2** in selected **Time Range** (Last 24 hours or Last 7 Days)**.**

Figure 195 *The WAN page*



- **WAN connectivity**: Provides the status of the periodic health check of WAN links.
- **WAN speed test**: Provides the status of the MAX uplink and downlink bandwidth of the WAN link.
- **WAN throughput**: Provides the usage of WAN uplink and downlink over a period of time.

WAN Details

Table 48 *Parameters displayed on the WAN Details section*

Parameter	Description
WAN Details	
Status	Status (online or offline) based upon the periodic WAN link health check.
Refresh time	Last update of date and time.
IP mode	Mode as DHCP or Static.
IPv4 Address	IPv4 Address of the WAN.
Gateway	Default gateway of the WAN interface.

VPN Sites

The VPN Sites page displays the network traffic and connection details as shown in Figure 196.

Figure 196 *The VPN Sites page*

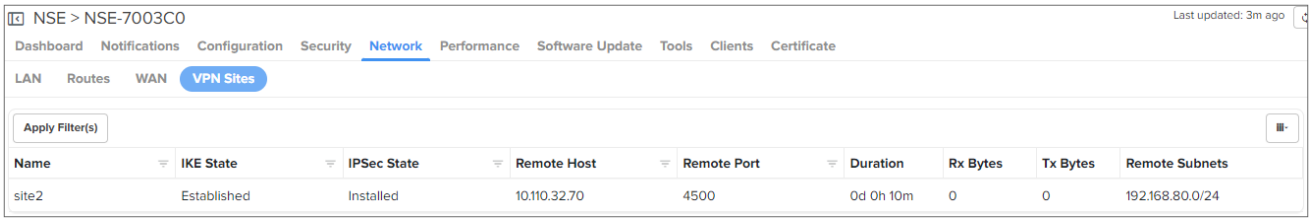


Table 49 *Parameters displayed on the VPN Sites page*

Parameter	Description
VPN Sites	
Name	Name of the VPN site.
IKE State	Current state of IKE protocol.
IPSec State	Current state of IPSec protocol.
Remote Host	IP address of the remote VPN endpoint.
Remote Port	Port number of the remote VPN endpoint.
Duration	Duration of the VPN connection.
Rx Bytes	Number of bytes received by the local VPN endpoint from the remote VPN endpoint.
Tx Bytes	Number of bytes transmitted by the local VPN endpoint to the remote VPN endpoint.
Remote Subnets	IP address ranges assigned to the remote VPN endpoint's network.

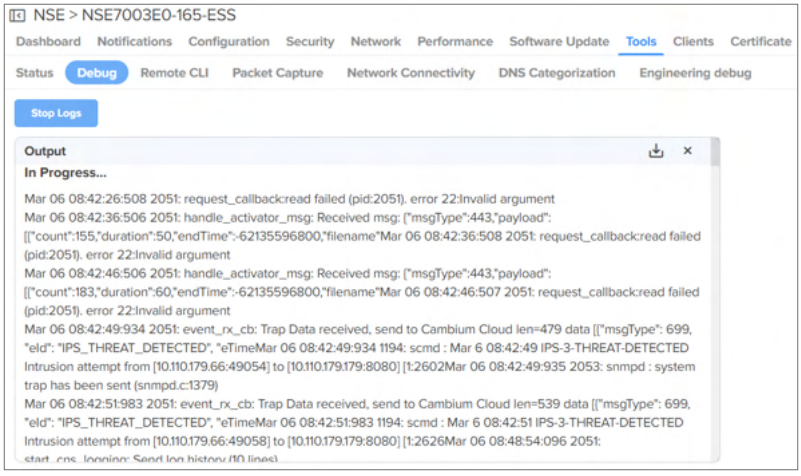
Debug Tools

You can capture logs, run remote CLI commands to see stats in real time, run traceroute, ping to check the reachability, and run live packet capture on the NSE devices on the selected interface.

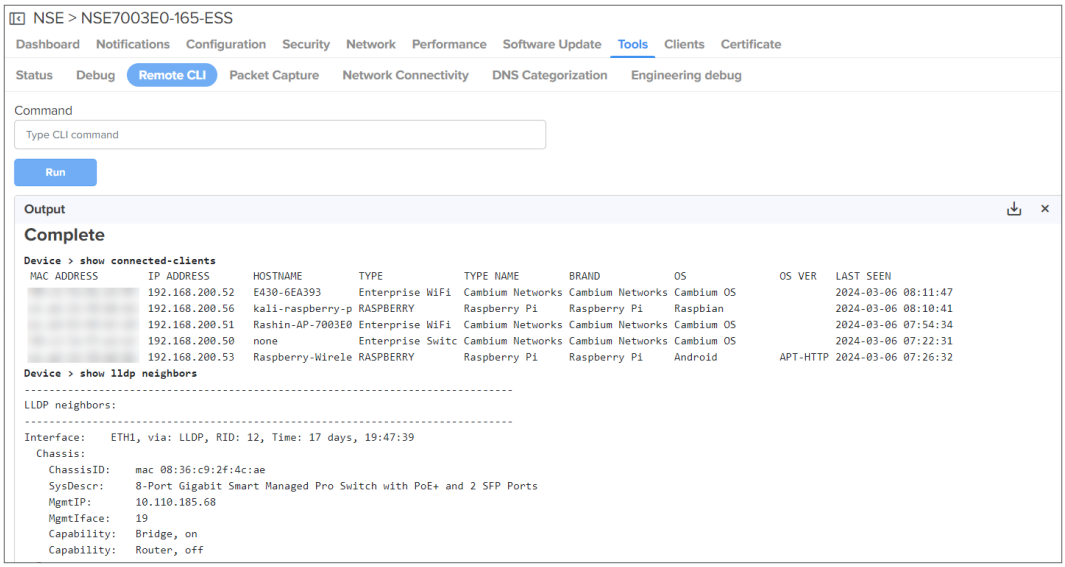
To display the NSE device status, navigate to **NSE** > **Tools** > **Status** page.



To access the logs, navigate to **NSE** > **Tools** > **Debug** tab and click **Start Logs**:

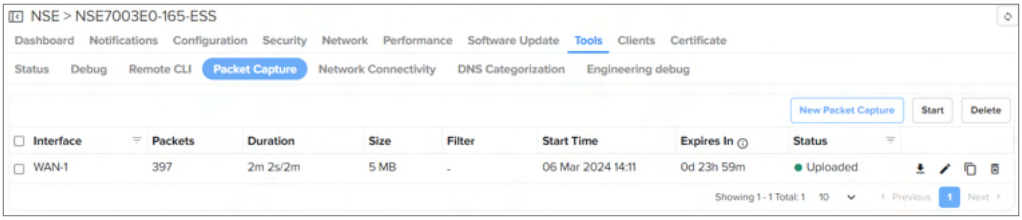


To run CLI commands, navigate to **NSE** > **Tools** > **Remote CLI** page, enter the **Command** and then click **Run**:

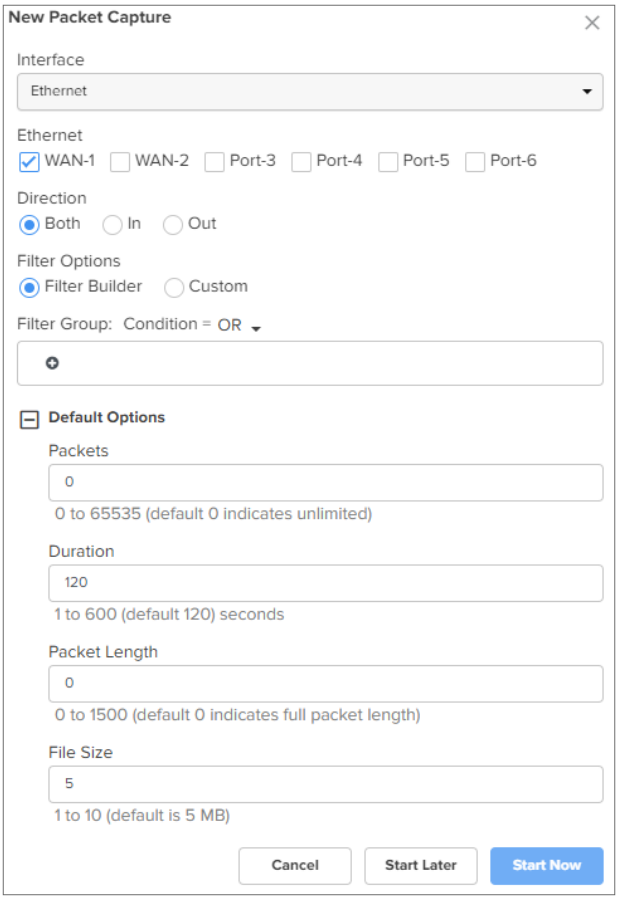


To run packet capture on the NSE device, navigate to **NSE > Tools > Packet Capture** page and follow these steps:

1. Click **New Packet Capture** and complete the details.

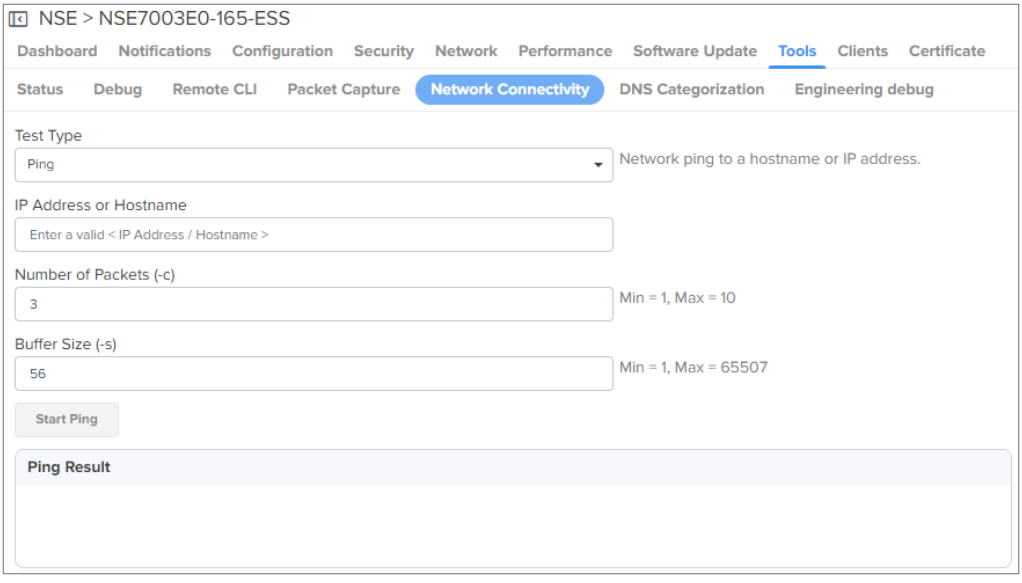


   The New Packet Capture window is displayed.



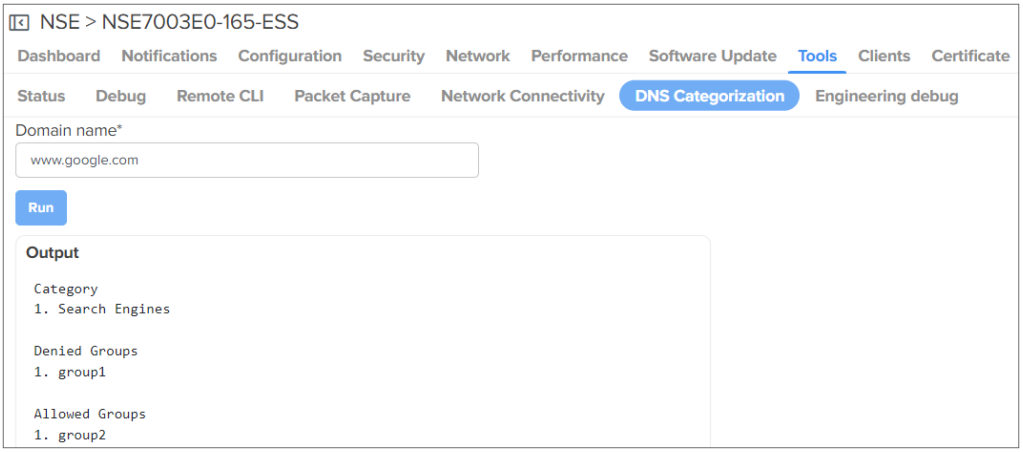
2. Click either **Start Now** or **Start Later** and then click **Close**.
3. If you had clicked **Start Later**, you can start the packet capture by clicking the right pointed triangle in the right most column of the interface details list.

   To check the network connectivity, navigate to **NSE > Tools > Network Connectivity** page, complete the details, and then click **Start Ping**:



   To access DNS categorization, navigate to **NSE** >**Tools** > **DNS Categorization.**

The DNS categorization tool is used to determine the category of the domain under which the queried domain falls. It is employed in scenarios where the administrator knows the specific domain and wants to ascertain which category to select while configuring the DNS filter. Additionally, it indicates whether the queried domain is permitted or denied for the specified group configured on the box.



Clients

The Clients page displays information depending on the system, network. or the device level from where you are accessing the page.

- Device-level information
- Network- and Site-level information
- Client Dashboard

Device-level information

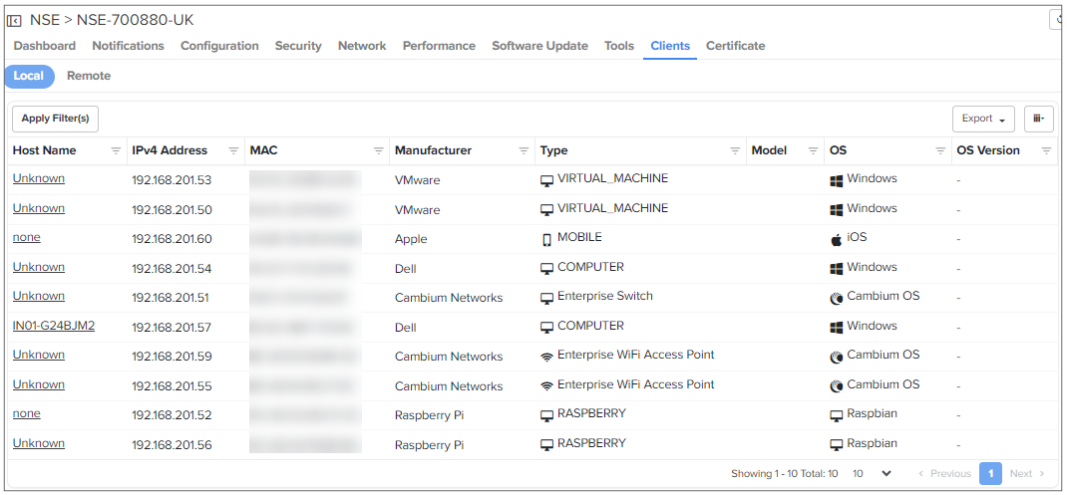
Clients page at the device-level displays the Local and Remote clients (VPN clients) connected to the NSE device.

Note

You can connect up to 1000 clients on the LAN side of NSE 3000. The clients can be either wired clients or wireless clients.

Local

The Local page displays the total client count which are connected to the NSE on the LAN side. Using device finger printing NSE provides **Device Type**, **Device OS**, and **OS Version**.



Click **Host Name**. It navigates to detailed Client Dashboard as shown in Figure 200.

Remote

The **Remote** page displays client count (vpn client) connected on the WAN side.

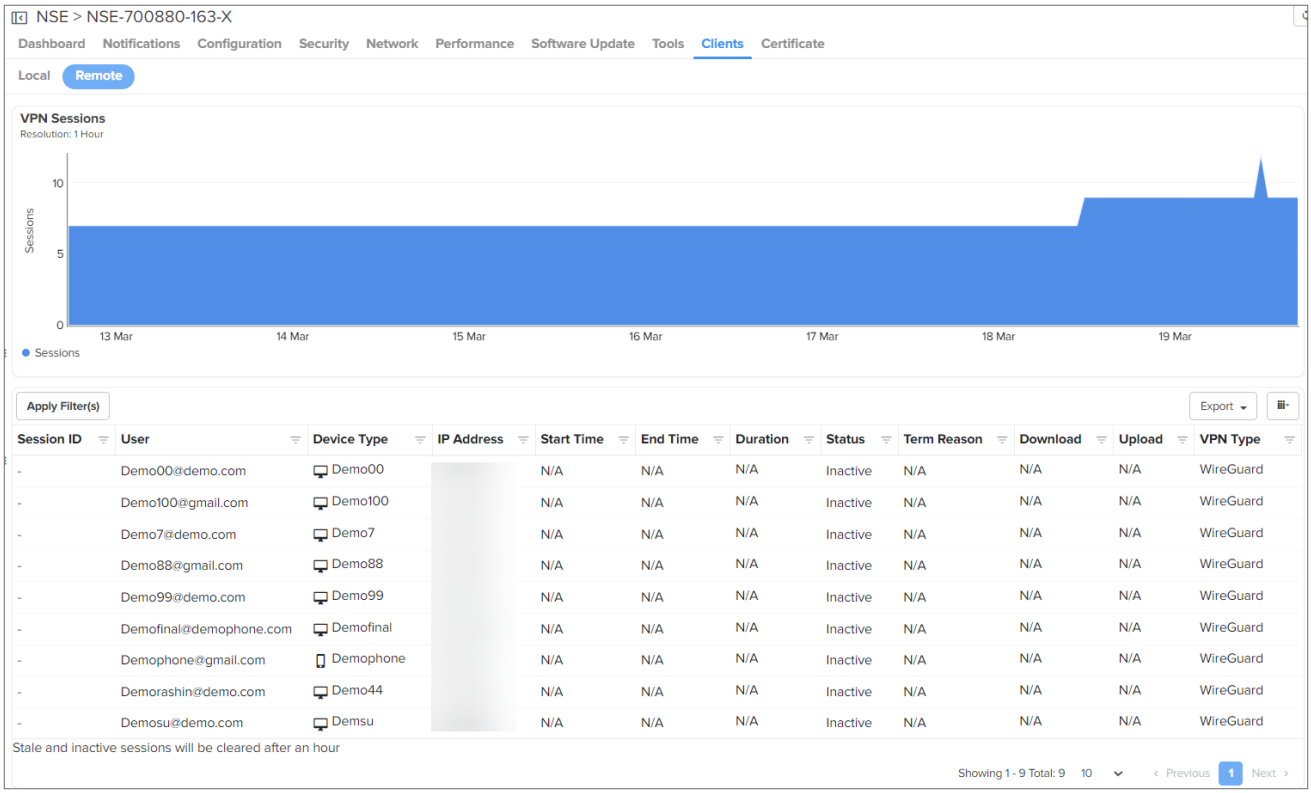


Table 50 *Parameters displayed in VPN sessions*

Parameter	Description
VPN Sessions	
Session ID	ID of the session. **Note**: The session ID is displayed only for **IPSec IKEV2** and **L2TP over IPSec** VPN types.
User	VPN user name.
Device Type	Type of device.

Table 50 *Parameters displayed in VPN sessions*

Parameter	Description
IP Address	IP Address assigned to the VPN client.
Start Time	VPN session start time.
End Time	VPN session end time.
Duration	Total session duration.
Status	Session status as active or inactive.
Term Reason	Terminated reason of the session disconnected or timeout.
Download	Total download by the VPN user.
Upload	Total upload by the VPN user.
VPN Type	Type of VPN. The following options are supported: • **WireGuard** • **IPSec IKEV2** • **L2TP over IPSec**

Network- and Site-level information

The Clients page at the Network- and Site-level displays the details of all the connected wireless and wired clients, and all unconnected clients.

- Wireless Clients
- Wired Clients
- Unconnected Clients

Wireless Clients

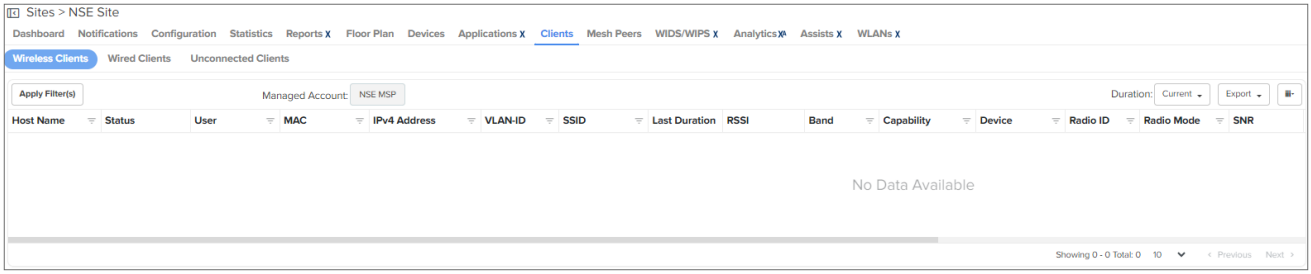
The **Clients** > **Wireless Clients** page at the Network- and Site-level displays the following details:

- **General**
  - Device
  - Device MAC
  - Host Name
  - Last Duration
  - Last Seen
  - Manufacturer
  - OS
  - Status
  - User
- **Guest Access**
  - Auth Status
  - Authentication Type

- Client Type
- Download Quota
- Download Quota Balance
- Guest Access Type
- Session Expiry
- Total Quota
- Total Quota Balance
- Upload Quota
- Upload Quota Balance

- **Network**
  - IPv4 Address
  - IPv6 Address
  - MAC
  - VLAN-ID
- **Wireless**
  - Band
  - Capability
  - Download
  - Radio ID
  - Radio Mode
  - RSSI
  - SNR
  - SSID
  - Upload

Figure 197 *Site > Clients > Wireless Clients*



Wired Clients

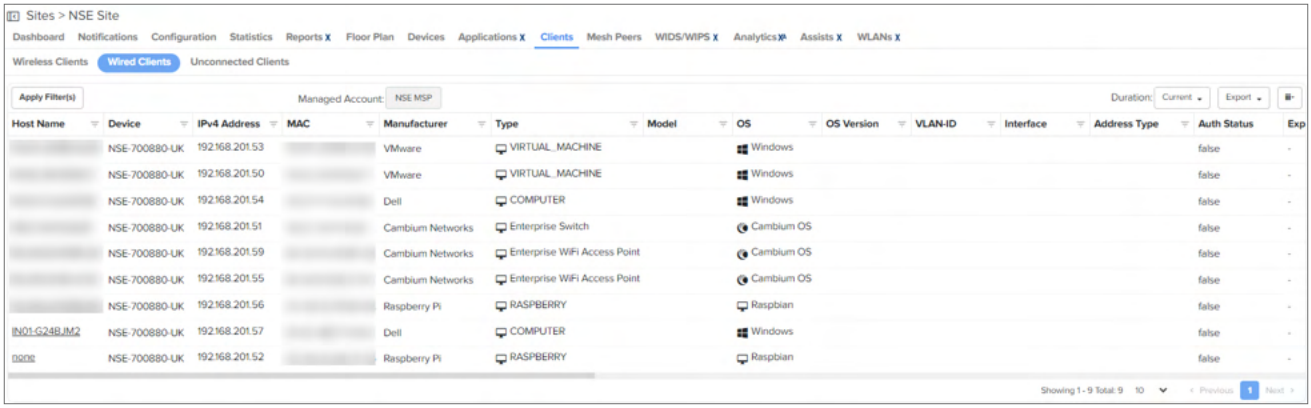
The **Clients** > **Wired Clients** page at the Network- and Site-level displays the following details:

- **General**
  - Address Type
  - Device

- Device MAC
- Download
- Expires
- Host Name
- Last Duration
- Manufacturer
- Model
- OS
- OS Version
- Type
- Upload

- **Guest Access**
  - Auth Status
  - Authentication Type
  - Client Type
  - Download Quota
  - Download Quota Balance
  - Guest Access Type
  - Portal Mode
  - Session Expiry
  - Total Quota
  - Total Quota Balance
  - Upload Quota
  - Upload Quota Balance
- **Network**
  - Interface
  - IPv4 Address
  - MAC
  - VLAN-ID

Figure 198 *Site > Clients > Wired Clients*

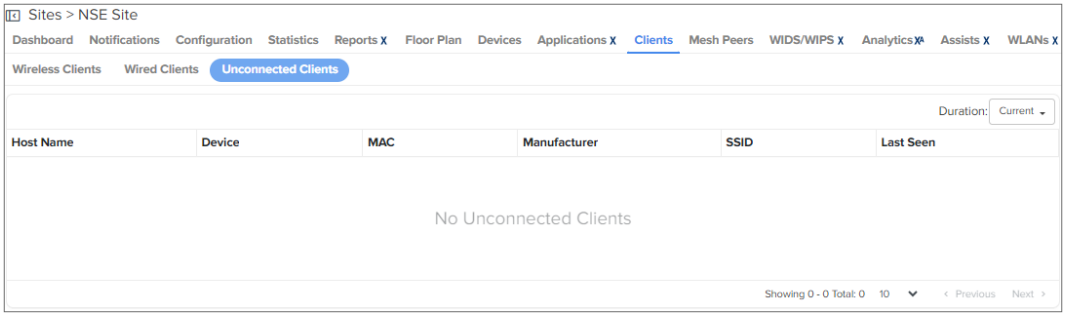


Unconnected Clients

The **Clients** > **Unconnected Clients** page at the Network- and Site-level displays the following details:

- Host Name
- Device
- Last Seen
- MAC (address)
- SSID
- Manufacturer

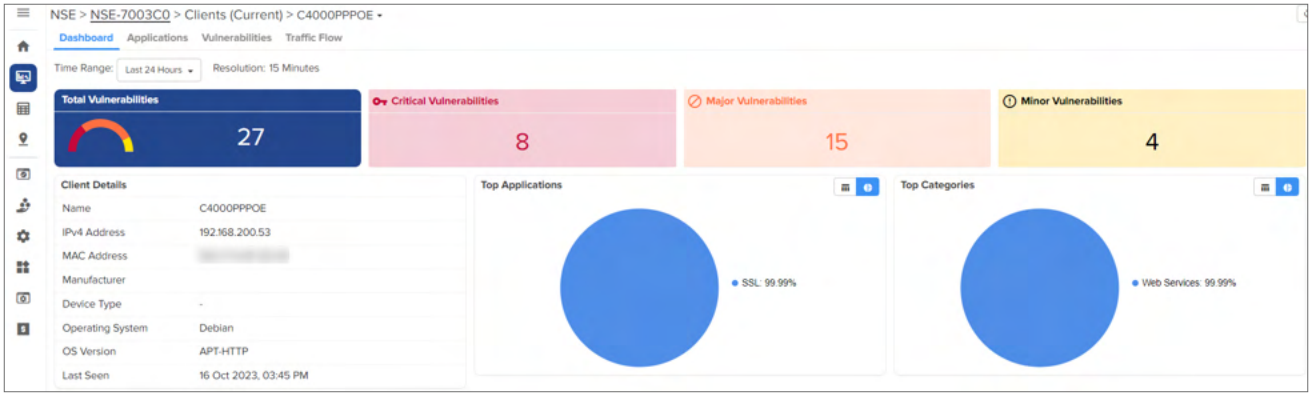
Figure 199 *Site > Clients > Unconnected Clients*



Client Dashboard

Dashboard provides overview of the wired and wireless clients usage. Click the pie chart to view specific application usage.

Figure 200 *Client Dashboard*



The following parameters are displayed for NSE Clients:

- Total Vulnerabilities
- Critical Vulnerabilities
- Major Vulnerabilities
- Minor Vulnerabilities
- Client Details
- Top Applications
- Top Categories

Applications

The Applications tab displays **Application History, Top Application**, **Top Category**, and **Total Bytes.**



The Application data can be presented most for 24 hours or 7 days.

- **Top Application**: Represent the most used application by the client.
- **Total Bytes**: Represents the sum of Uplink and Downlink traffic across all applications used by the client.
- **Top Category**: Category of the top application used by the client.

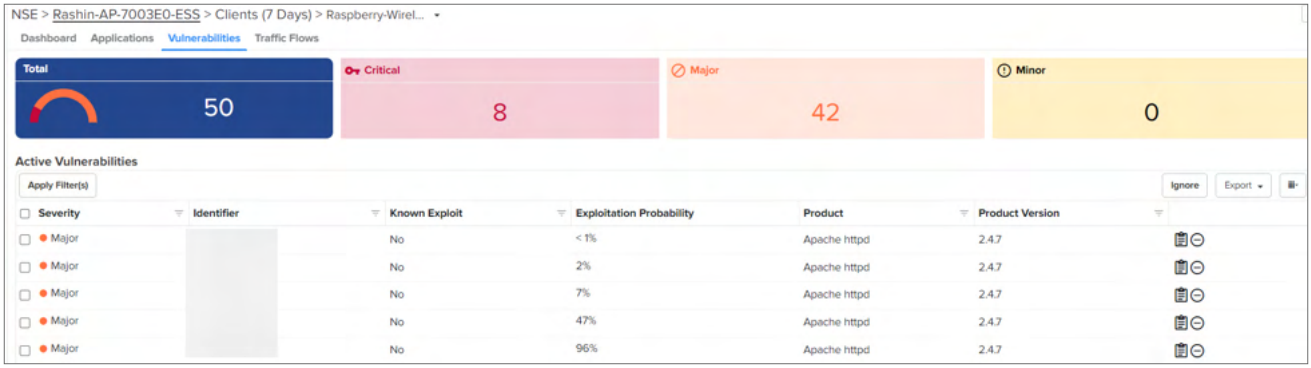
Table 51 *Parameters on the Applications page*

Field	Description
Application Name	Name of the application.
Category	Category of the application.
Downlink	Total number of downlink bytes during the period selected.
Uplink	Total number of uplink bytes during the period selected.
Total Bytes	Total amount of application data (uplink plus downlink).
Productivity Index	The estimate of the typical productivity of the application. A higher value means better productivity.
Risk Index	The estimate of the typical security risk of the application. A higher value means greater risk.
Usage	The percentage of usage by this application in comparison to all applications.

Vulnerabilities

The **Vulnerabilities** page displays the vulnerabilities discovered for the client by the NSE. Vulnerabilities are categorized as Minor, Major, and Critical.

Figure 201 *Vulnerabilities dashboard*



Traffic Flows

Traffic flows can be referred to as a current snapshot of existing flows. The flow direction can be either LAN to WAN or WAN to LAN.

Note

The NSE 3000 device supports up to 256000 concurrent connections.

The **Traffic Flows** page displays the active connections or flows of a client, as shown in Figure 202.

Figure 202 *The Traffic Flows page*



Table 52 *Parameters on the Traffic Flows page*

Parameter	Description
Source IP	Source IP address of the device or endpoint, based on the flow direction. If the flow direction is from LAN to WAN, the source IP address is the source IP address of the

Table 52 *Parameters on the Traffic Flows page*

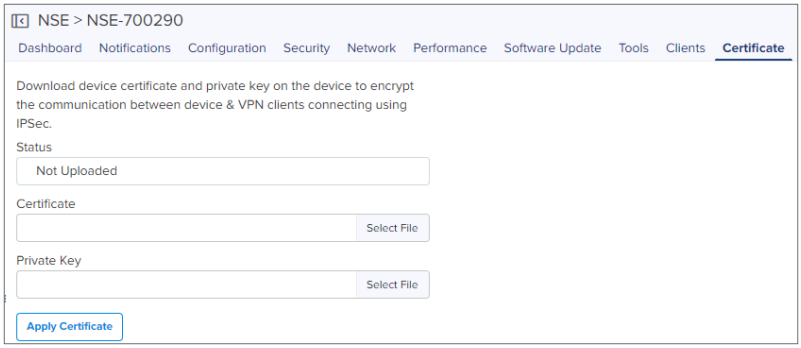
Parameter	Description
	device. If the flow direction is from WAN to LAN, the source IP address is the source IP address of the endpoint to which the device has connection to.
Source Port	Source port number.
Destination IP	Destination IP address of the device or endpoint, based on the flow direction. If the flow direction is from LAN to WAN, the destination IP address is the destination IP address of the endpoint. If the flow direction is from WAN to LAN, the destination IP address is the destination IP address of the device.
Destination Port	Destination port number.
Application	Name of the application.
Tx Packets	Transmitted packets.
Tx Bytes	Transmitted bytes.
Rx Packets	Received packets.
Rx Bytes	Received bytes.
TTL	Time to live. Time period during which a session or connection is active.
NAT'ed IP	IP address after the Network Address Translation (NAT) process.
NAT'ed Port	Port number after the NAT process.
Direction	Direction of the communication, indication whether it is incoming or outgoing. Outgoing: LAN to WAN Incoming: WAN to LAN
State	Current state of a connection. The following connection states are valid only if the protocol is TCP. • SYN_SENT • SYN_RECV • ESTABLISHED • FIN_WAIT • CLOSE_WAIT • LAST_ACK • TIME_WAIT • CLOSE
Protocol	Name of the protocol, such as TCP, UDP, ICMP, or any.

Certificate

To secure the communication between an NSE device and the VPN clients, you can encrypt the communication. To apply the encryption certificate, navigate to **NSE > Certificate**, upload the certificate and the key files, and then click **Apply Certificate**.

Note: Only certificates with "**.der**" and "**.pem**" file extensions are accepted.

Figure 203 *The Certificate page*



Wireless LAN Dashboards

This section describes the following topics:

- Wi-Fi Monitoring
- Site Dashboard
- WLANs Dashboard

Wi-Fi Monitoring

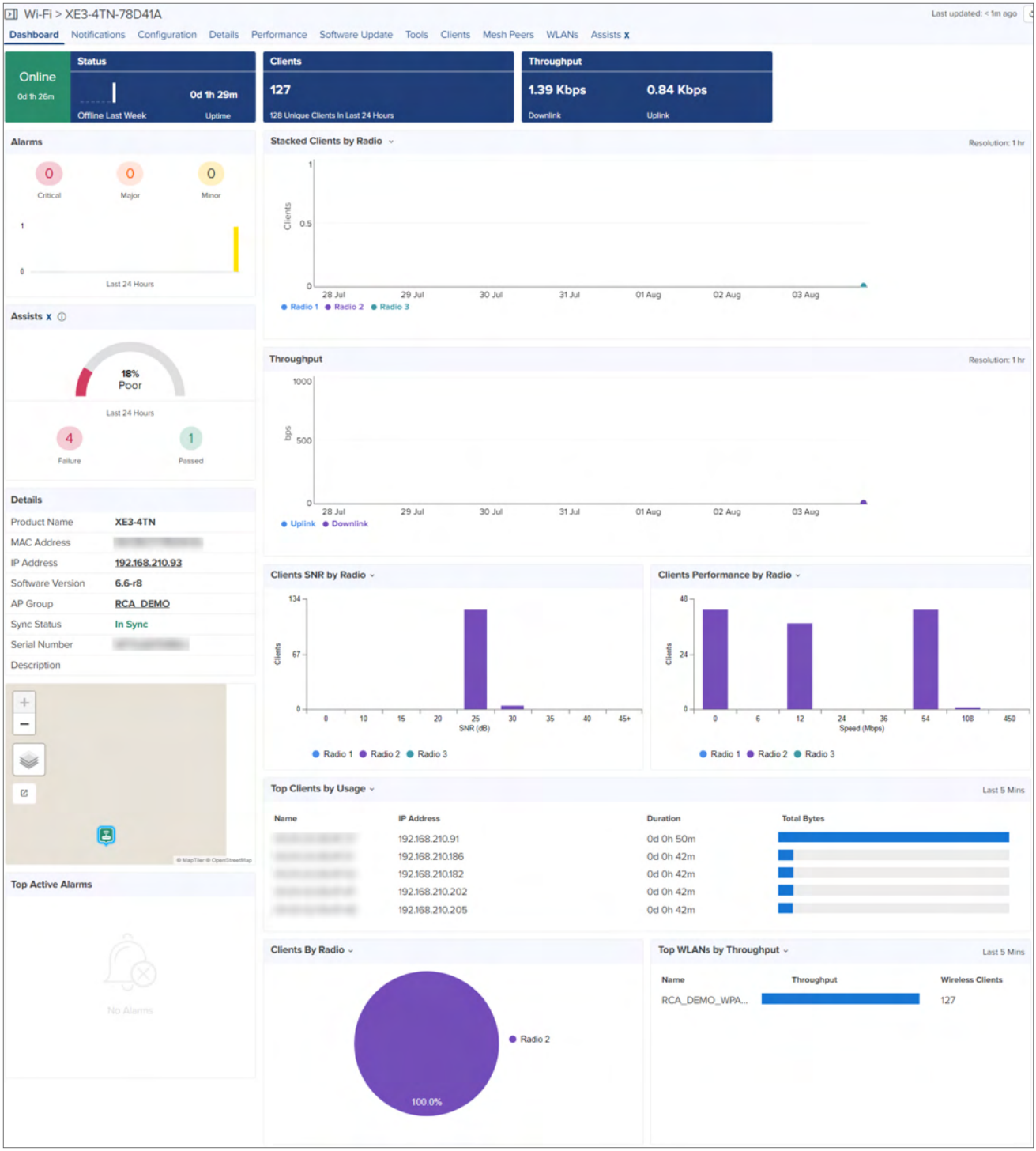
The Wi-Fi Monitoring pages include the following:

- Dashboard
- Clients
- Details
- Mesh Peers

Dashboard

The cnPilot Dashboard displays **Stacked Clients by Radio, Stacked Clients by Band, Clients by Radio, Clients by Band, Details, Status, Throughput, Top Active Alarms, Top Clients by Usage, Top Clients by Session, Top WLANs by Clients,** and **Top WLANs by Throughput**.

Figure 204 *Device > Dashboard*



Clients

The Clients tab displays the details of all the Wireless and Wired clients.

The following parameters are displayed for Wireless clients for cnPilot Home (R-Series):

- Actions
  - SSID
- Band

- Download
- Host Name
  - Edit Name
- IP Address
- MAC
- Managed Account
- Manufacturer
- RSSI
- Upload

Figure 205 *cnPilot Home: Device > Clients > Wireless Clients*

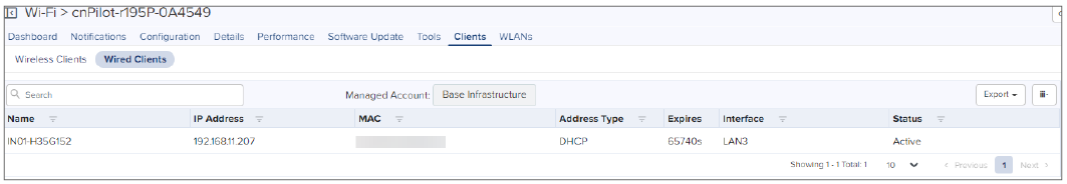


The following parameters are displayed for Wired Clients for cnPilot Home (R-Series):

Note

The historical clients are available for 24 Hours and 7 Days for cnMaestro X users.

Figure 206 *cnPilot Home (R-Series): Device > Wired Clients*



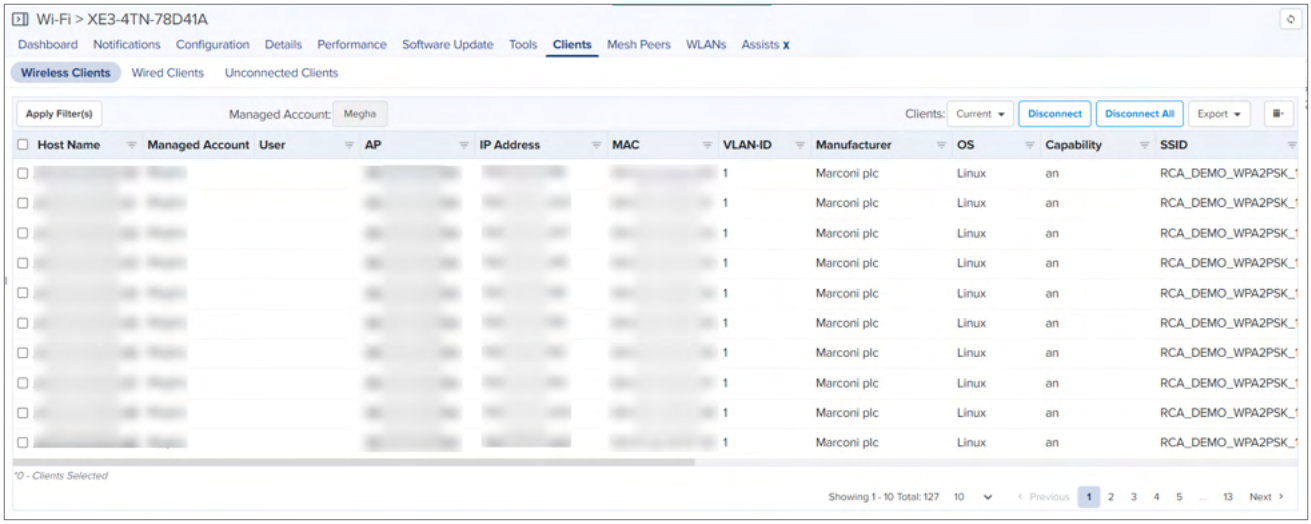
- Actions
  - Edit Name
- Address Type
- Expires
- Interface
- IP Address
- MAC Address
- Name
- Status

The following parameters are displayed for cnPilot E-Series Wireless Clients:

- Actions
- AP

- Auth Status
- Authentication Type
- Band
- Capability
- Client Type
- Download
- Download Quota
- Download Quota Balance
- Guest Access Type
- Host Name
- IP Address
- Last Duration
- Last seen
- MAC
- Managed Account
- Manufacturer
- OS
- Portal Mode
- Radio
- Radio ID
- Radio Mode
- RSSI
- Session Expiry
- SNR
- SSID
- Total Quota
- Total Quota Balance
- Upload
- Upload Quota
- Upload Quota Balance
- User
- VLAN-ID

Figure 207 *Enterprise Wi-Fi: Device Dashboard > Wireless Clients*



The following parameters are displayed for Wired clients for E-Series:

- Auth Status
- Client Type
- Download
- Download Quota
- Download Quota Balance
- Guest Access Type
- Host Name
- IP Address
- Last Duration
- MAC
- Manufacturer
- OS
- Portal Mode
- Total Quota
- Total Quota Balance
- Upload
- Upload Quota
- Upload Quota Balance
- VLAN-ID

Note

The historical clients are available for 24 Hours and 7 Days for cnMaestro X users in System/ Network/ Site and Device level.

Figure 208 *Enterprise Wi-Fi: Device Wired Clients*

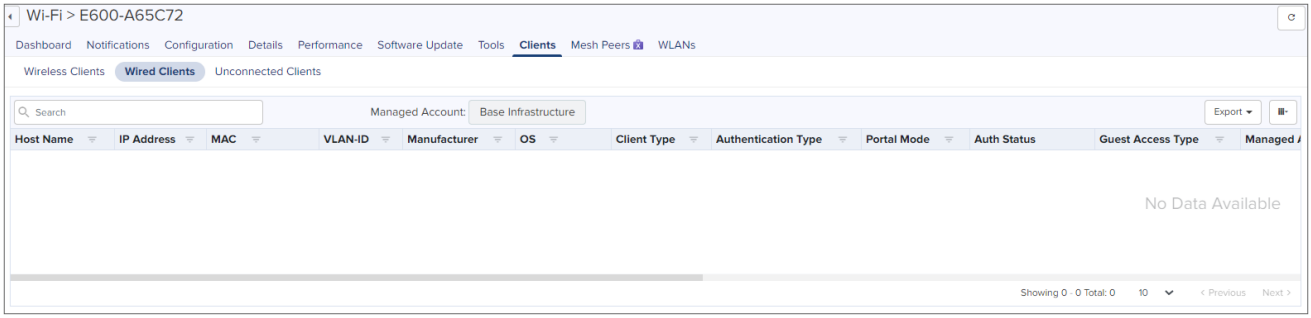
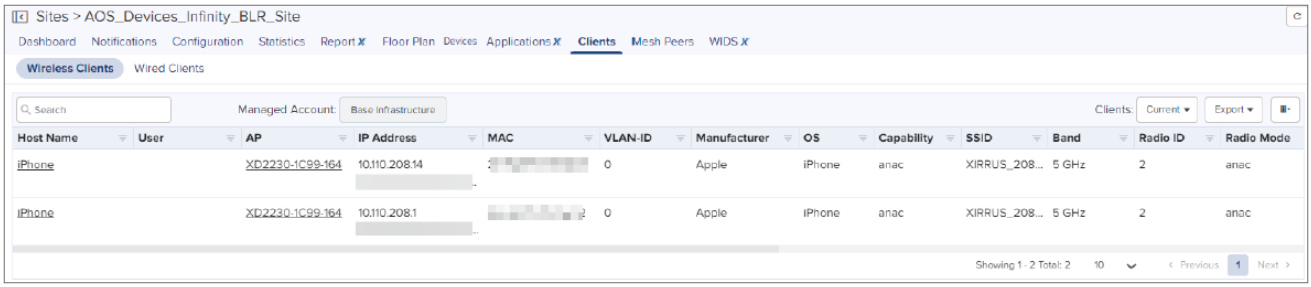


Figure 209 *Enterprise Wi-Fi (Xirrus-Series) Wireless Clients*

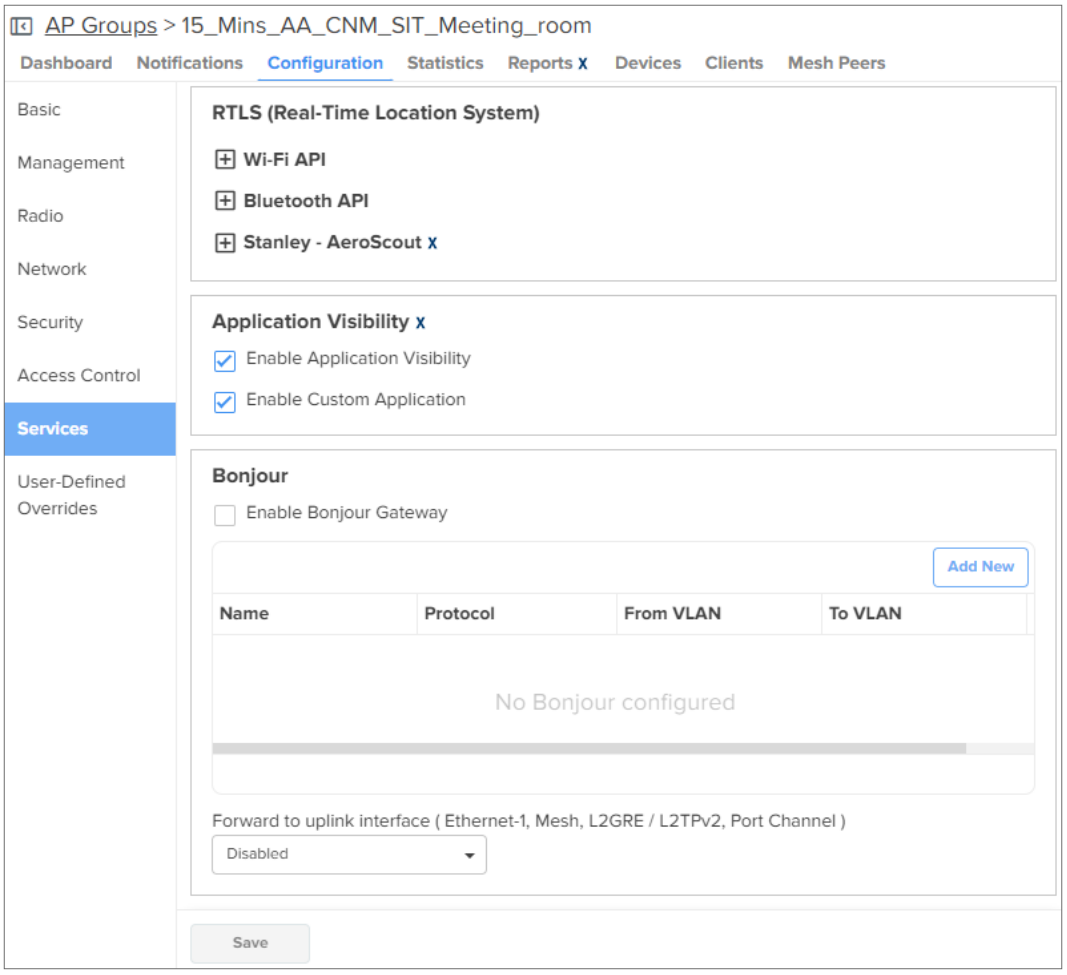


Note

Wired clients are not supported for Xirrus-Series.

Client Dashboard

The user can view the applications used by client when the **Application Visibility** option is enabled as shown below.

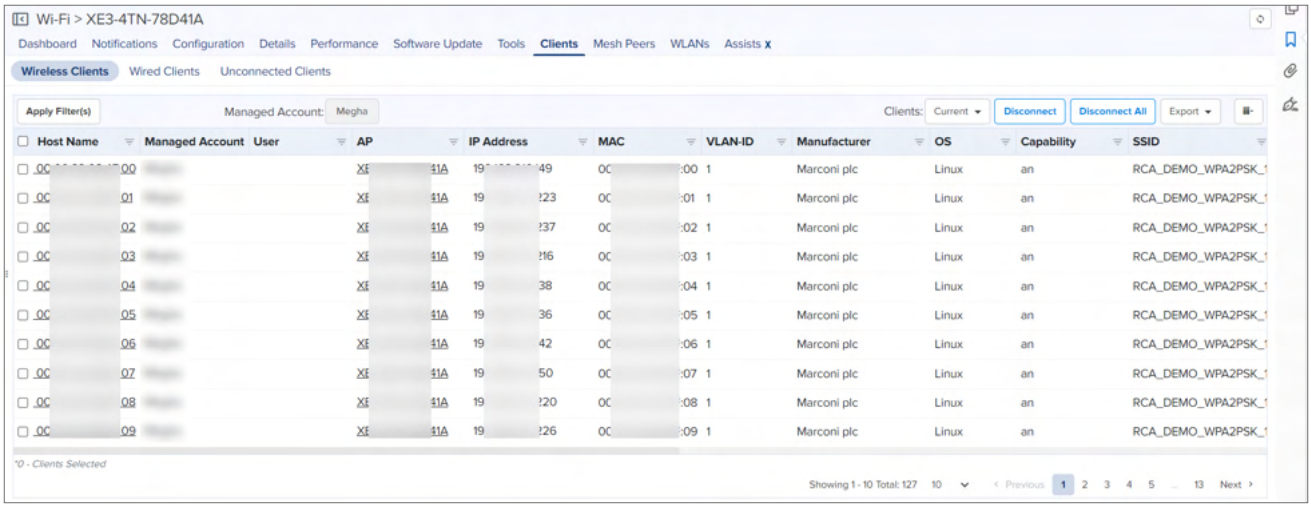


The Client Dashboard displays the details of the clients connected to the Wi-Fi device.

Note

- Enable the **Application Visibility** feature to view **Application** page. It is supported only for XE, XV, X7 series devices.
- **Dashboard** is supported for all cnPilot devices.
- The historical clients are available for 24 Hours and 7 Days for cnMaestro X users.

Figure 210 *XE, XV, and X7 Series: Device Dashboard Wireless Clients*



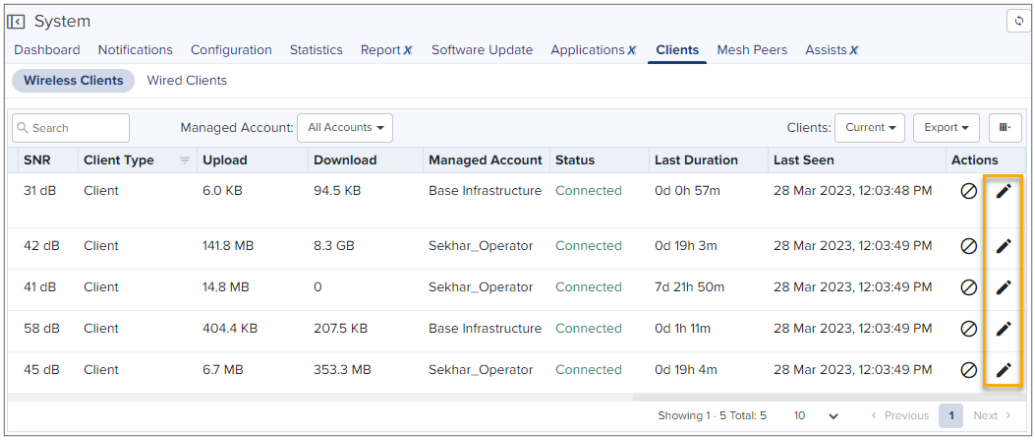
To view the **Dashboard**, navigate to **Clients** > **Wireless Clients** and click a value in the **Host Name** column.

A detailed **Client Dashboard** page is displayed. For more details, refer to

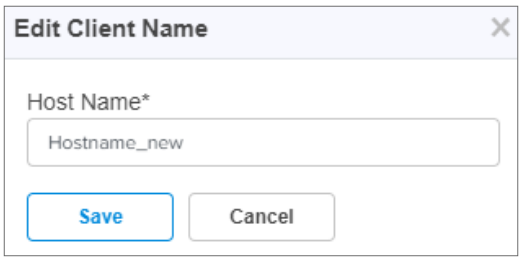
Renaming Client Host-names

You can assign friendly host-names for the clients. To edit the host-name of connected wired or wireless client, follow these steps:

1. Navigate to **Clients > Wireless Clients** or **Wired Clients** tab.



2. Scroll to the right most side of the clients list and click on the **Edit** icon under the **Actions** column.
3. In the **Edit Client Name** pop-up window, enter a friendly name for the client.

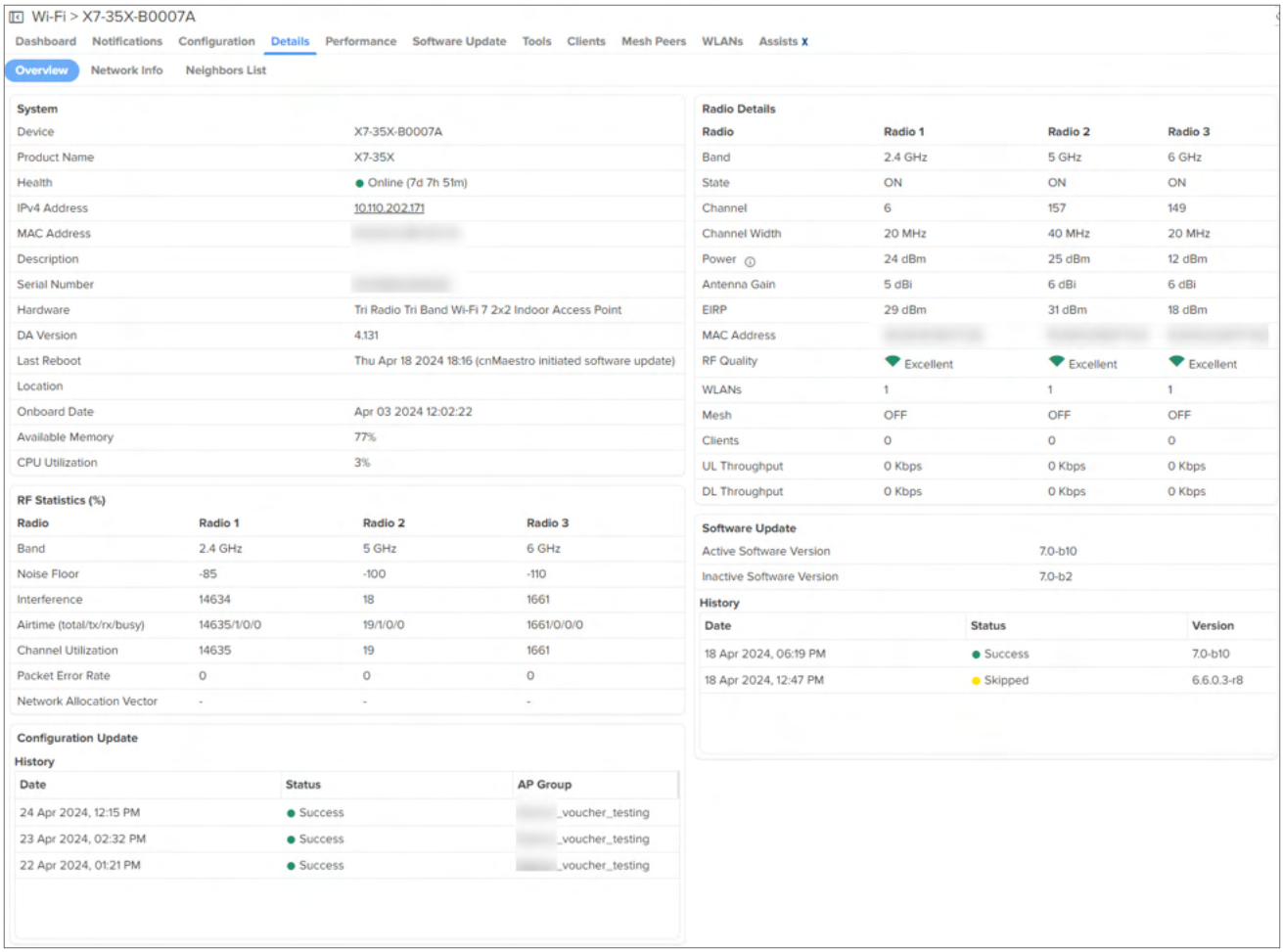


4. Click **Save**.

   The new host-name is displayed in all the places such as the Client Dashboards, Audit logs, and Reports.

Details

Details page displays the Overview, Network Info, and Neighbors List.



Overview

The **Details > Overview** page displays information, such as System, RF Statistics (%), Configuration Update, Radio Details, Software Update, and History.

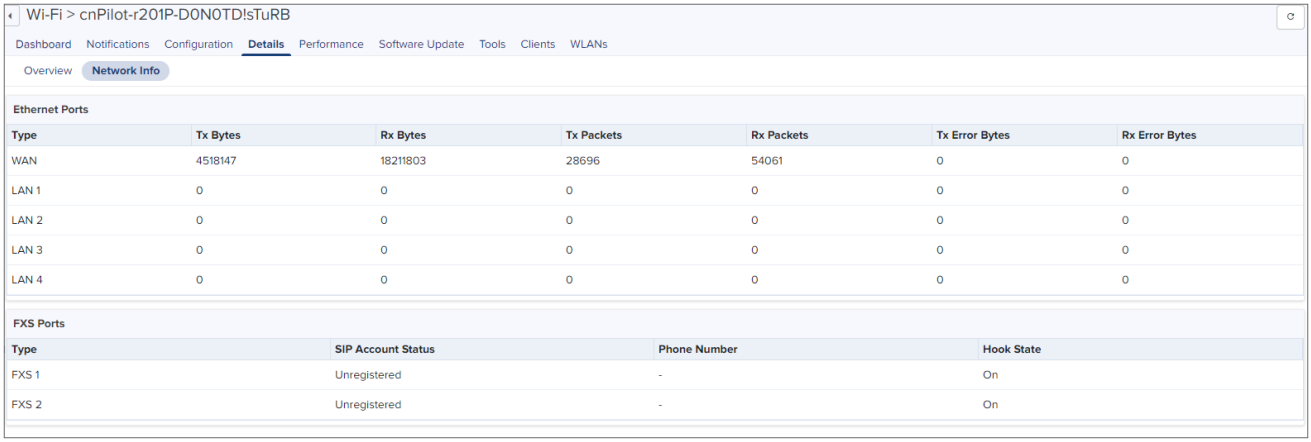
Network Info

The **Details > Network Info** page displays the following parameters for cnPilot Home (R-Series) router:

- Ethernet Ports
  - Rx Bytes
  - Rx Error Bytes
  - Rx Packets
  - Tx Bytes
  - Tx Error Bytes
  - Tx Packets
  - Type
- FXS Ports
  - Hook State
  - Phone Number

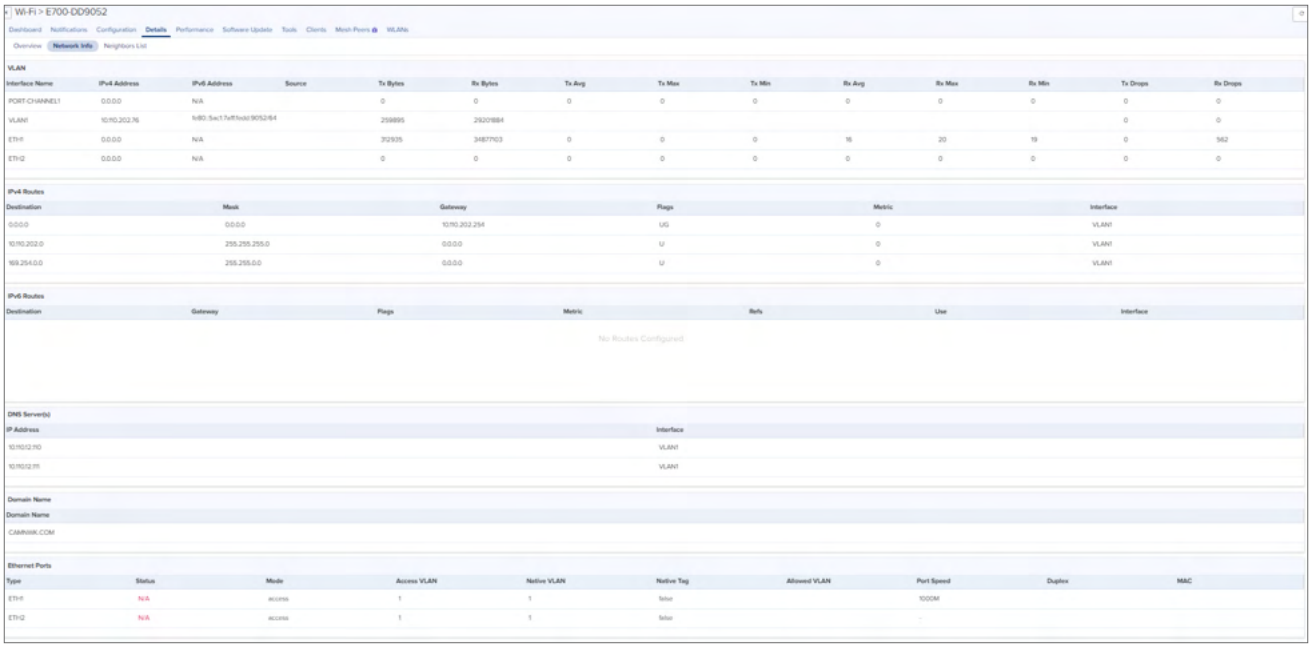
- SIP Account Status
- Type

Figure 211 *cnPilot Home: Device > Details > Network Info*

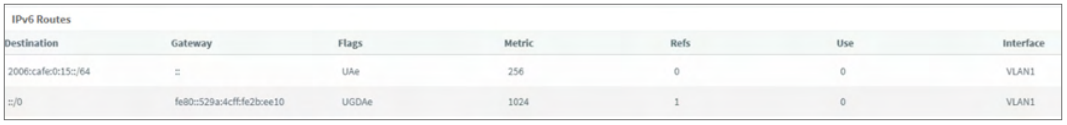


- Ethernet Ports
- PPPoE
- Routes
- Tunnels
- VLAN Pool

Figure 212 *Enterprise Wi-Fi: Device >Details > Network Info*



IPv6 Routes



DNS Servers

DNS Server(s)	
IP Address	Interface
10.110.12.110	VLAN1
10.110.12.111	VLAN1

The following parameter details are displayed in E-Series:

- Port
- Rx Broadcasts
- Rx Frames
- Rx Frames Oversize
- Rx Frames Undersize
- Rx Frames with Error
- Rx Octets
- Tx Broadcasts
- Tx Frames
- Tx Octets

Figure 213 *Enterprise Wi-Fi (Xirrus-Series): Device > Dashboard > Network Info*

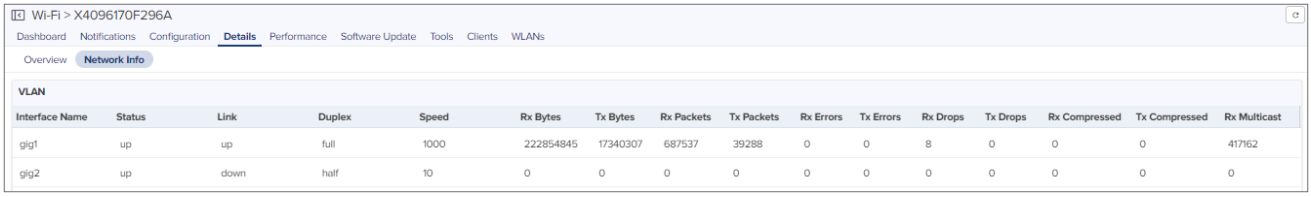


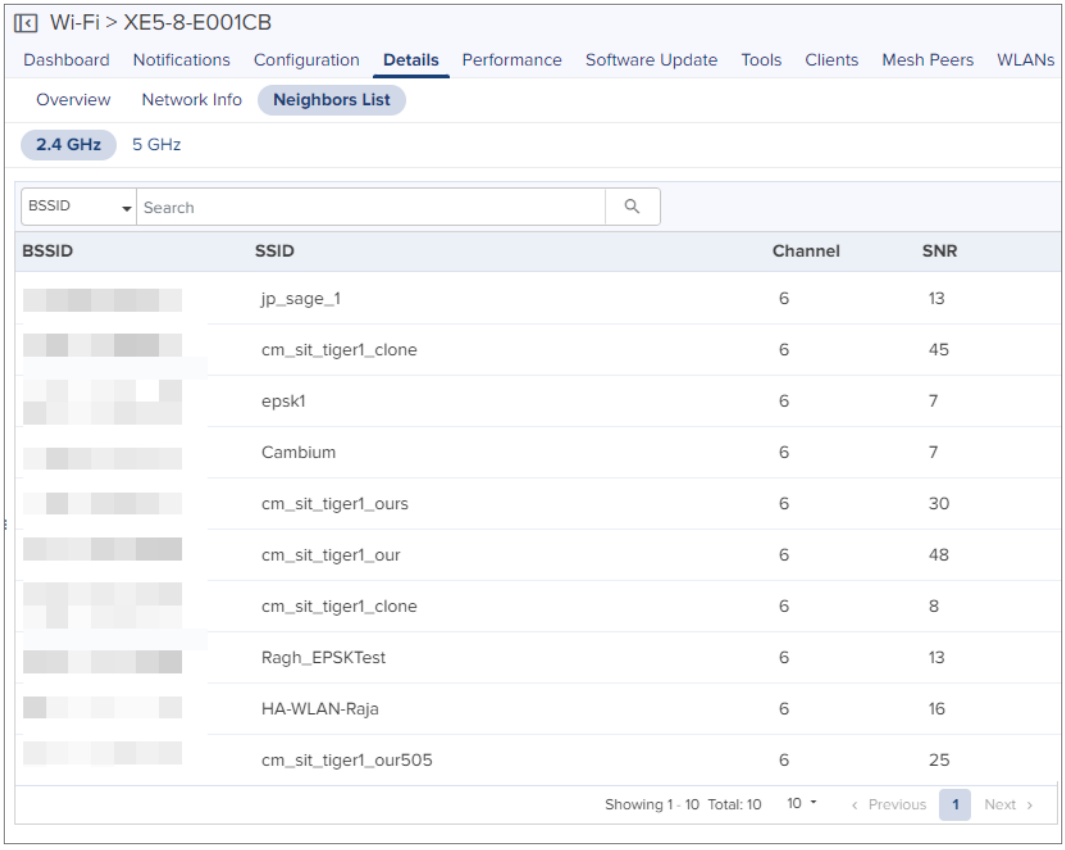
Figure 214 *PTP 650/670/700: Device >Details > Network Info*

Ethernet Ports									
Type	Status	Mode	Access VLAN	Native VLAN	Native Tag	Allowed VLAN	Port Speed	Duplex	MAC
ETH1	N/A	access	1	1	false		1000M		
ETH2	N/A	access	1	1	false		-		

Neighbors List

The **Neighbors List** displays the BSSID, SSID, Channel, and SNR details of neighboring 2.4 GHz and 5 GHz radios.

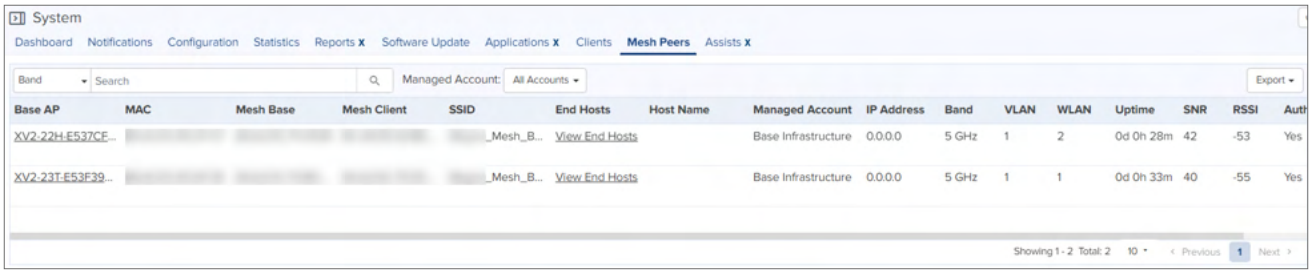
Figure 215 *Neighbors List*



Mesh Peers

The Mesh Peers tab displays information related to mesh such as SNR, RSSI, and Band. This provides insight to the performance between the Mesh Client and Mesh Base.

Figure 216 *Device > Mesh Peers*



Roaming History for Mesh Peers

To view the **Information** and **Roaming History,** perform the following**:**

In **the Mesh Peers** tab, click the **Host Name.**

A detailed Information and Roaming History window pops up.

Figure 217 *Mesh Peers > Host Name > Information*

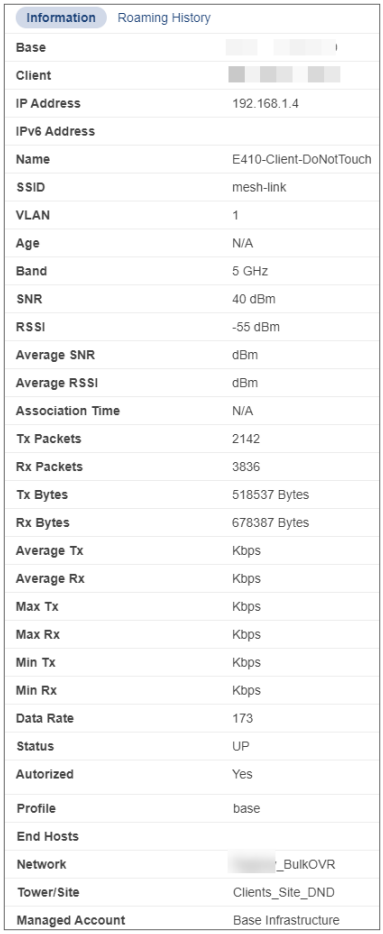
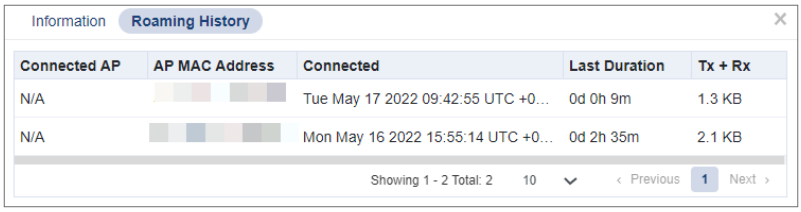
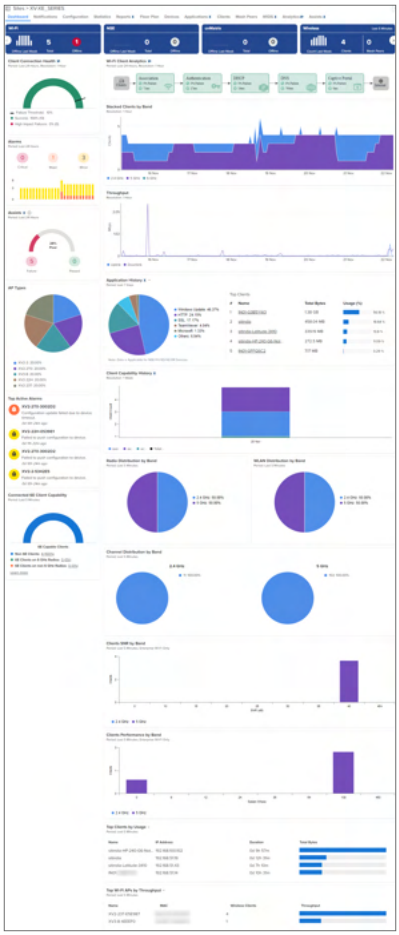


Figure 218 *Mesh Peers > Host Name > Roaming History*



Site Dashboard

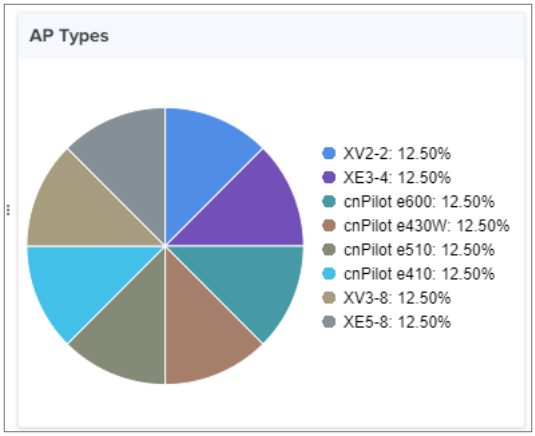
The Site Dashboard provides the overview of site-related parameters and devices.



The Site Dashboard displays the following graphics:

- AP Types
- Stacked Clients by Band
- Channel Distribution by Band
- Clients Performance by Band (Enterprise Wi-Fi)
- Clients SNR by Band (Enterprise Wi-Fi)
- Connected 6E Client Capability
- Client Capability History
- Radio Distribution by Band
- WLAN Distribution by Band
- RF Quality
- Wireless LAN Dashboards
- Wireless LAN Dashboards
- Floor Plan
- Wireless LAN Dashboards
- Wireless LAN Dashboards

AP Types

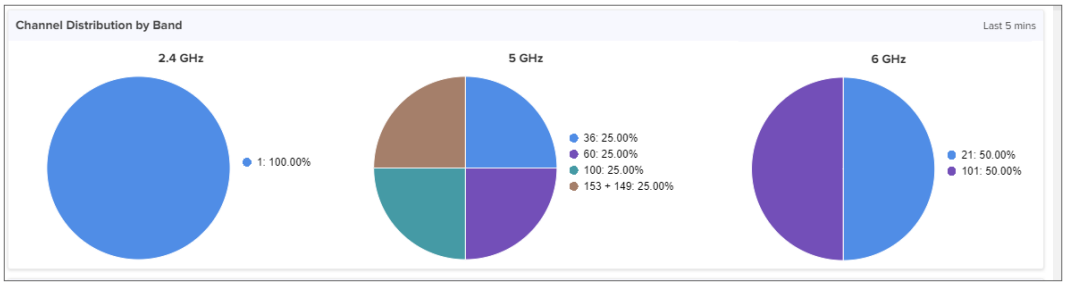


Stacked Clients by Band



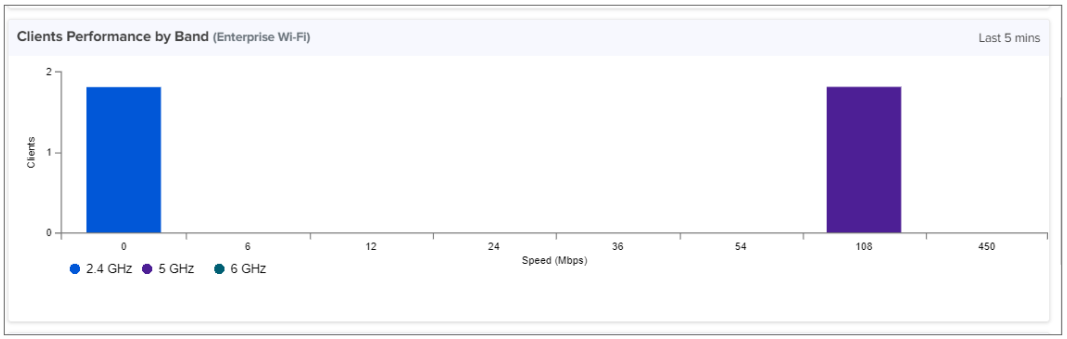
Channel Distribution by Band

Channel distribution displays usage of channels in 2.4 GHz, 5 GHz and 6 GHz. This helps in planning and implementing WLANs within a high-density environment. It displays the usage details for last 5 minutes.

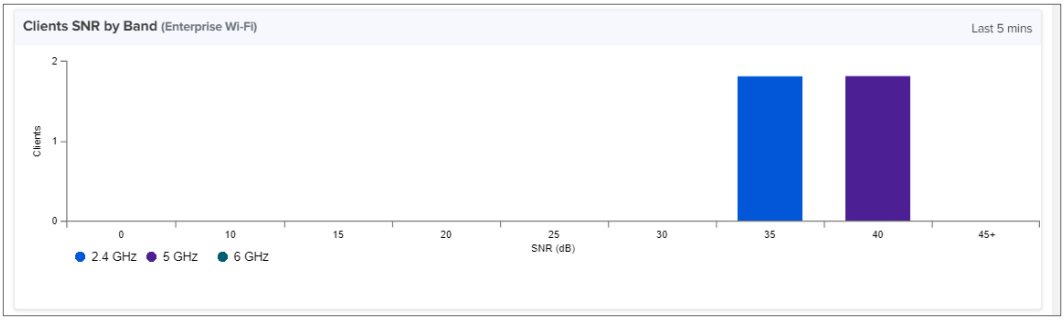


Clients Performance by Band (Enterprise Wi-Fi)

Clients performance details is displayed for last 5 minutes.



Clients SNR by Band (Enterprise Wi-Fi)



Connected 6E Client Capability

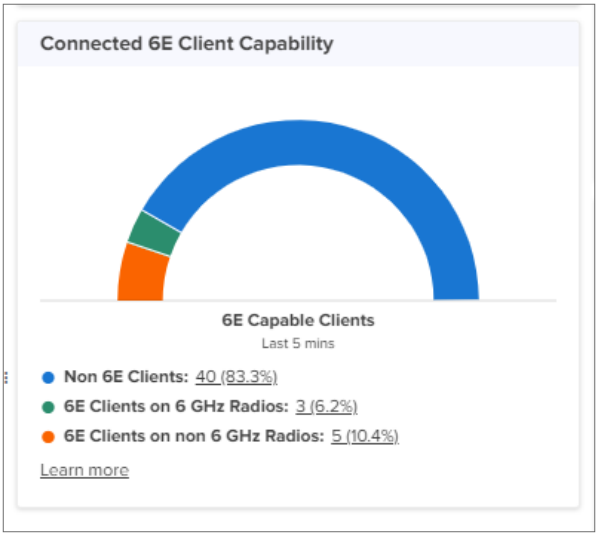
The Connected 6E Client Capability widget presents a point-in-time view of Wi-Fi 6E Clients associating to non-6E radios. These Clients may experience better service if SDR radios are upgraded from 5 GHz to 6 GHz. A high percentage of 6E Capable Clients connecting to non-6E radios is a signal to upgrade radios to 6 GHz. The Connected 6E Client Capability widget is represented using different colors and corresponding percentage values as described below:

- Non 6E Clients: represents non 6E clients connected across the devices at the Site level.
- 6E Clients on 6 GHz Radios: represents 6E clients connected across the devices at the Site level.
- 6E Clients on non 6 GHz Radios: represents 6E clients connected across the devices on non 6 GHz radios at the Site level.

Note

For best results, deploy a few radios in 6G mode in high traffic areas.

Figure 219 *Connected 6E Client Capability*



Clicking next to clients number navigates to **Wireless Clients** page.

Client Capability History

The Client Capability History graphic displays the highest detected Wi-Fi protocol for Clients active at a Site on weekly basis. Wi-Fi 6E devices are grouped into a single 6E category. A large number of 6E Capable Clients are a signal to expand infrastructure to include 6 GHz radios. If the period of evaluation extends more than a few weeks, the bar chart converts to a line chart.

Figure 220 *Clients History in line chart*

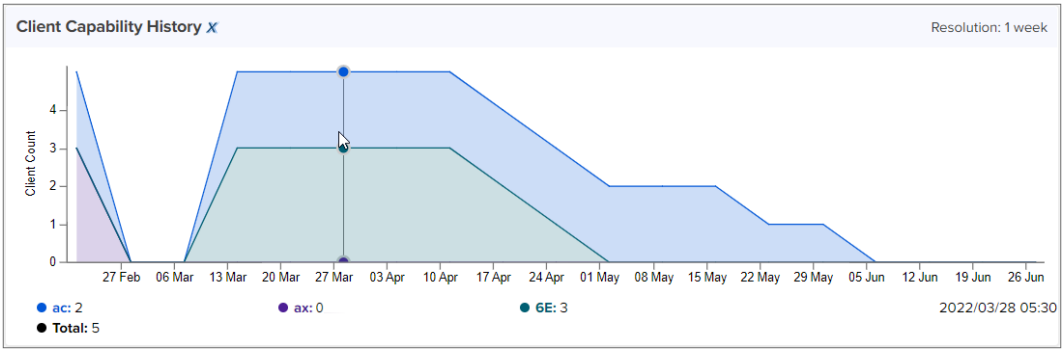
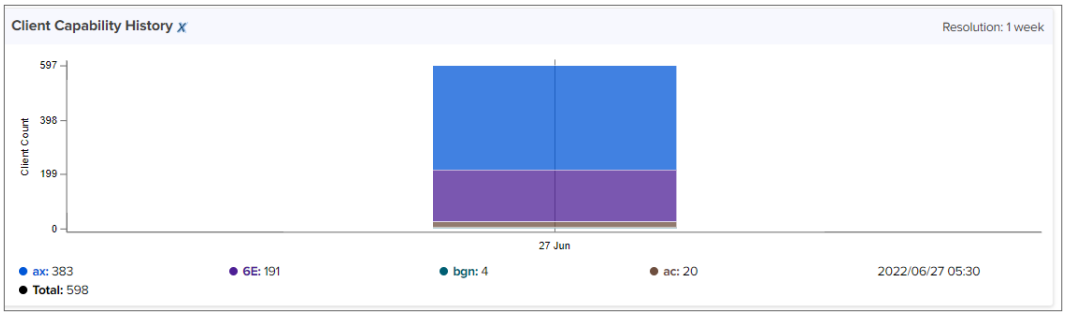
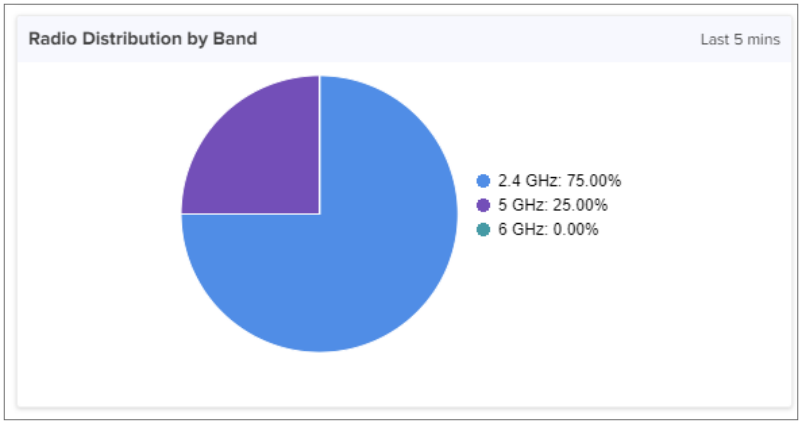


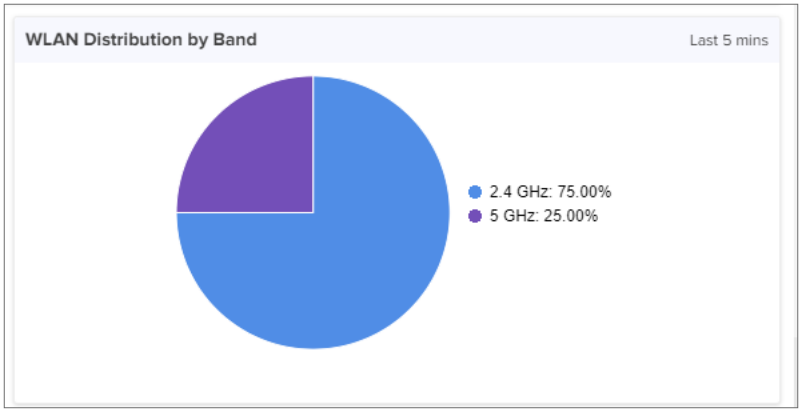
Figure 221 *Clients History in bar chart*



Radio Distribution by Band



WLAN Distribution by Band



RF Quality

Provides an indication of the current RF Quality across the Site.



Radio RF Quality Index is an indication of wireless clients and or MESH clients' RF link as seen by the access point radio (AP). It is the average of all the wireless clients and or mesh clients SNR.

- If aggregated SNR is more than 45: RF Quality Index is marked as Excellent
- If aggregated SNR is more than or equal to 35 and below 45: RF Quality Index is marked as Good
- If aggregated SNR is more than or equal to 25 and below 35: RF Quality Index is marked as Average
- If aggregated SNR is less than 25: RF Quality Index is marked as poor

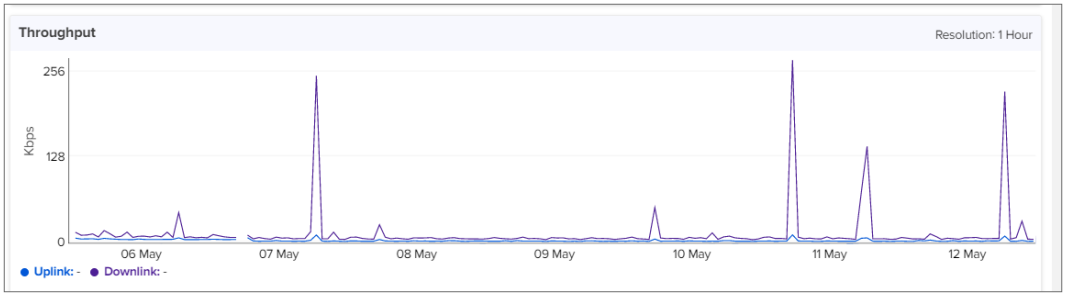
Throughput

Displays aggregated throughput for all the clients.

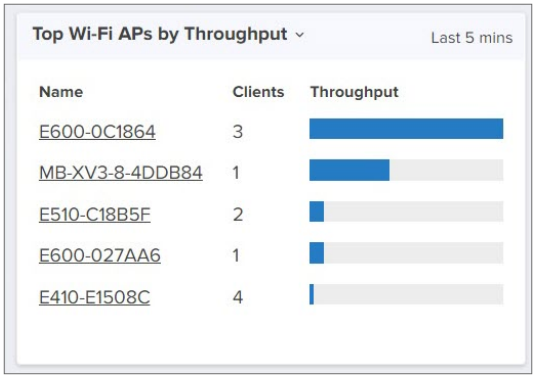


Throughput Graph

Throughput graph displays client traffic for the last week.



Top Wi-Fi APs by Throughput



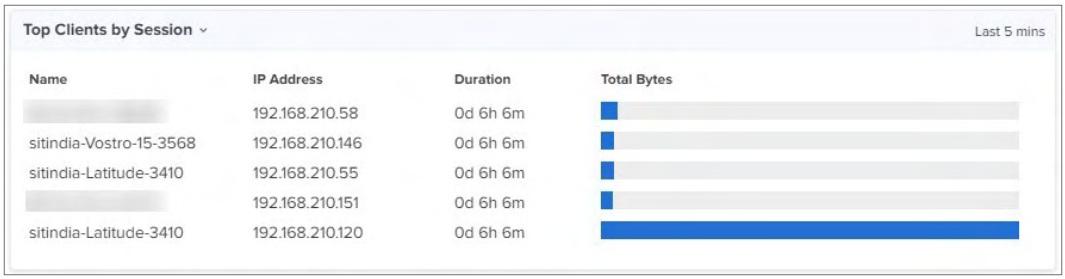
Wi-Fi Devices Availability (Total and Offline)

Displays total number of Access Points in the Site and the devices that are Offline.



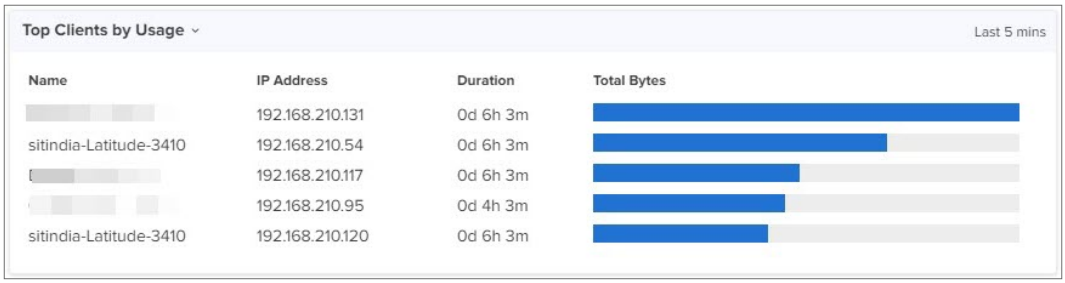
Top Clients by Session

Displays the top clients by session and the respective details.



Top Clients by Usage

Displays the top clients by usage and the respective details.



Wireless Clients Graph

Wireless clients graph displays clients that are connected in Radio 1 (2.4 GHz),Radio 2 (5 GHz), and Radio 3 (6 GHz).



Floor Plan

A Floor Plan is used to view APs, device status, connected clients, and transmit power. This is done by creating the floor plan and adding devices. You can upload a floor plan for each floor based on the selected environment type.

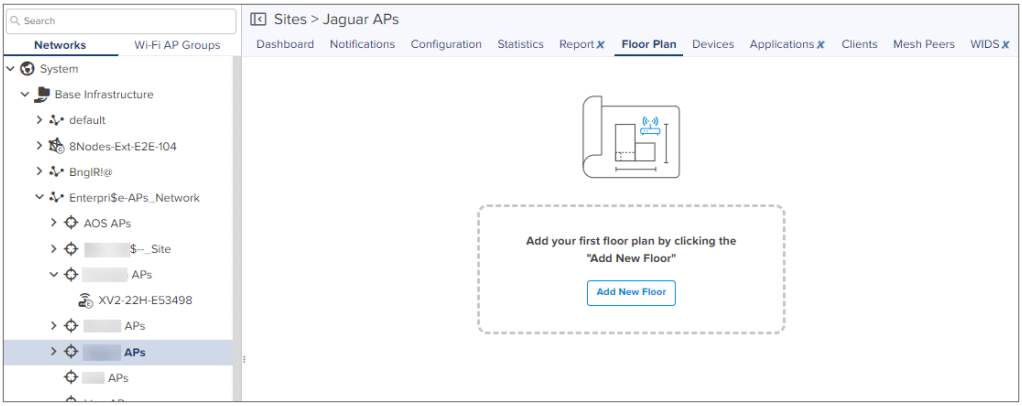
To create a floor plan, perform the following steps:

1. Navigate to **System > Network > Enterprise Site > Floor Plan.**

   Floor Plan can be uploaded when a **Site** is created.

2. Click **Add New Floor**.

The **Add New Floor** window appears.



3. Enter the parameters for a new floor plan.

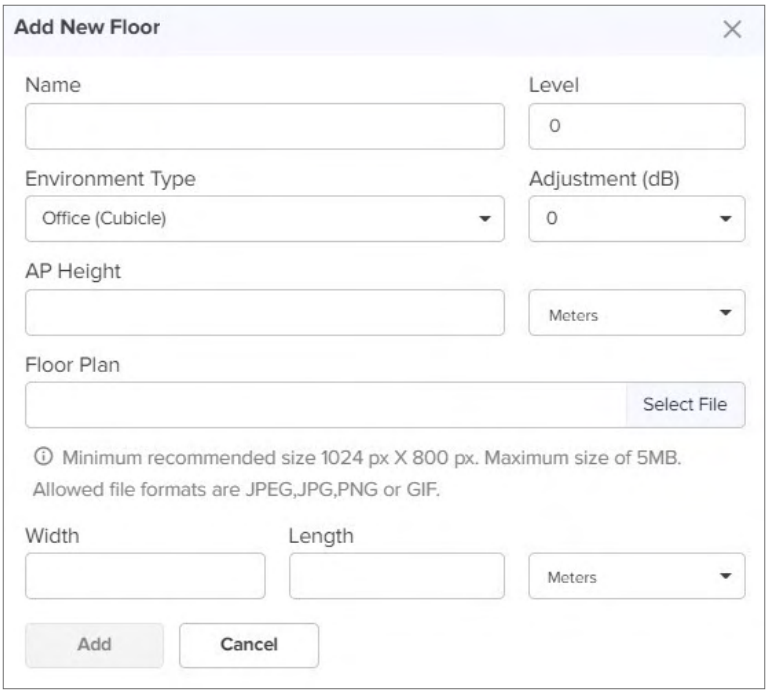


Table 53 *Fields in Floor Plan*

Field	Description
Name	Name of the floor.
Level	Level of the floor.
Environment Type	Floor type such as the following: • Apartment • Hospital • Hotel • Office (Cubicle) • Office (Walled) • Outdoors

Table 53 *Fields in Floor Plan*

Field	Description
	• School • University • Warehouse
Adjustment	Device adjustment in dB.
Height	Height of the ceiling in meters or feet.
Width	Width of the floor in meters or feet.
Length	Length of the floor in meters or feet.

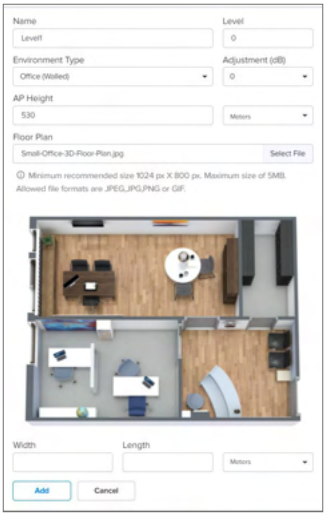
Note

Environment Type, Adjustment, and Height are currently unused by cnMaestro. They will become important when RF Heat Maps are added in a later release.

4. Click **Select File** and browse the required floor plan for uploading.

   A preview of the uploaded floor plan is shown below:

   Preview of Floor Plan

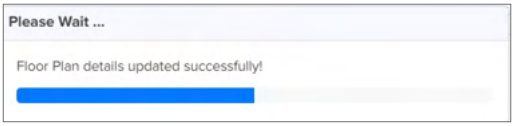


Note

- The minimum size of a floor plan is 1024 X 800 pixels.
- The maximum supported file size is 5 MB.
- The supported file formats are JPEG, JPG, PNG, and GIF.

5. Click **Add**.

   A successful message is displayed, as shown below:



The **Zoom** control allows you to zoom in and out of the floor plan.

Note

- Only cnMaestro X users can upload more than one floor plan.
- You cannot duplicate the floor level for other floor plans.
- If the devices are in a default location and upgraded to 3.1.1, the devices are moved to the **Unmapped Devices** option.

The right pane of the Floor Plan window provides details of uploaded floor plans, such as Floor View, Map Opacity, Radio Details, Filters, and the devices in the floor plan.

Figure 222 *Configure Floor Plan*

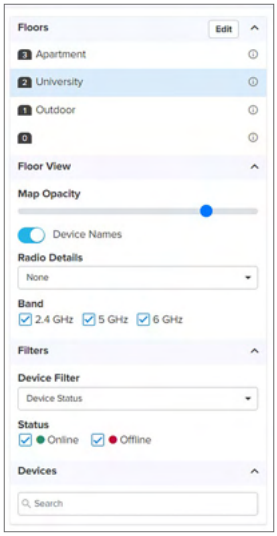


Table 54 *Fields to configure floor plan page*

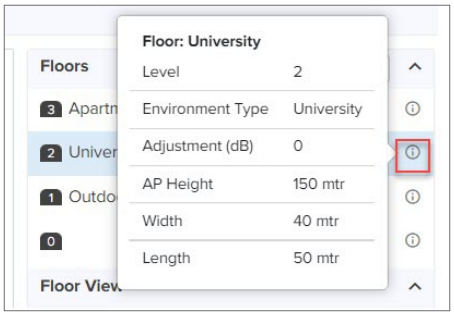
Field	Description
Floors	Indicates the floor level. The following actions are available: • Click **Add** to add new floor level. Drag and drop the selected devices from the right pane to the required floor level. If multiple floor levels are available, then select required floor level from the drop-down. • Select the floor level and click **Edit(**) icon to edit the uploaded floor level. • Click the **Delete** ( ) icon to delete a uploaded floor level. • Click on the info icon, next to floor level uploaded, to view the floor details.  • In the **Devices on this floor** drop-down, you can view the following options: ◦ Unmapped Devices: Devices not mapped to the floor plan.

Table 54 *Fields to configure floor plan page*

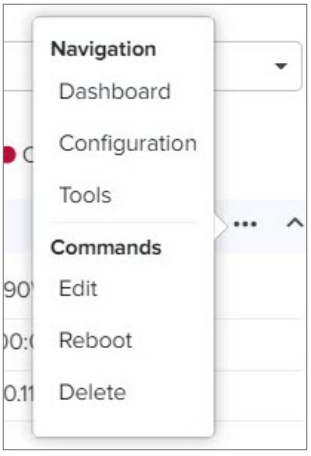
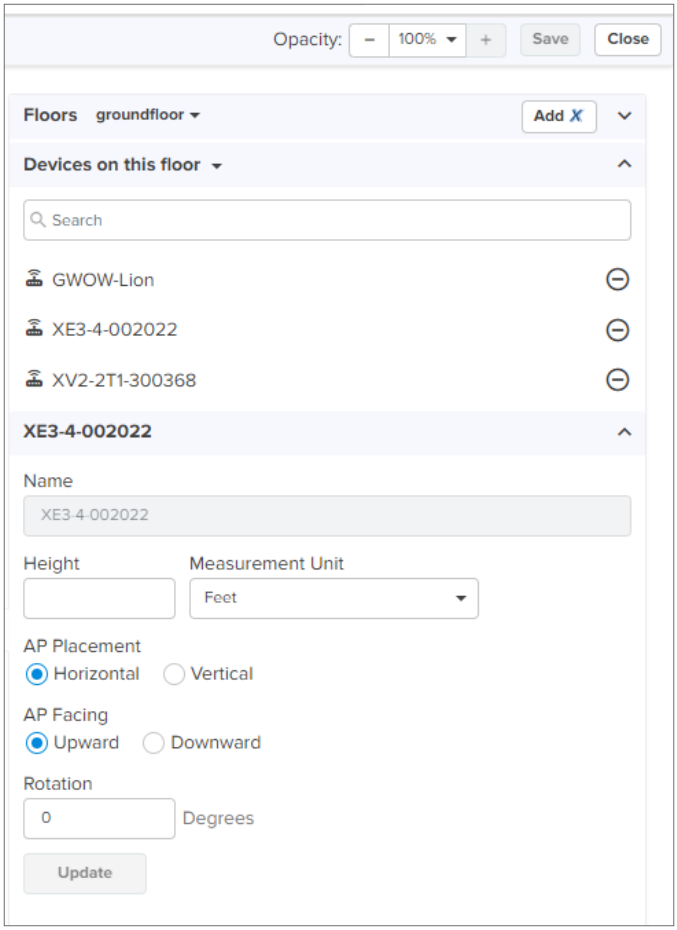
Field	Description
	◦ Devices on this floor: Devices available on the floor plan. ◦ Devices on other floors: Displays devices on the other floors. • Click **Remove** (⊖) icon to remove device from the floor level.
Floor View	Configure device presentation. The following options are available: • Map Opacity: Increase or decrease the opacity for the better visibility of uploaded floor plan. • Device Names: Toggle to view device names on the floor plan. • Radio Details: View the radio details such as Client Count, Channel, and Power. • Band: Select the desired band 2.4 GHz, 5 GHz, and 6 GHz (radio frequency).
Filter	Filter devices by Device Status, Channel, and Power.
Devices	View and edit the device details. The following actions are available: • Select the device on the floor plan or type the device name in the search field. • Click the eye icon (👁) to **Show** or **Hide** the device on the floor plan. • Click on the device name to view device details, as shown below:  • Click ellipsis (...) icon next to the device name, to navigate to the device homepage.  • Click **Edit** on the top right corner and select the device in the current floor.

Table 54 *Fields to configure floor plan page*

Field	Description
	 Edit the **AP Placement**, **AP Facing** and **Rotation** options. • Click **Update** and **Save.** • Click **Remove** (⊖) icon to remove device from the floor plan. • Click **Save**.

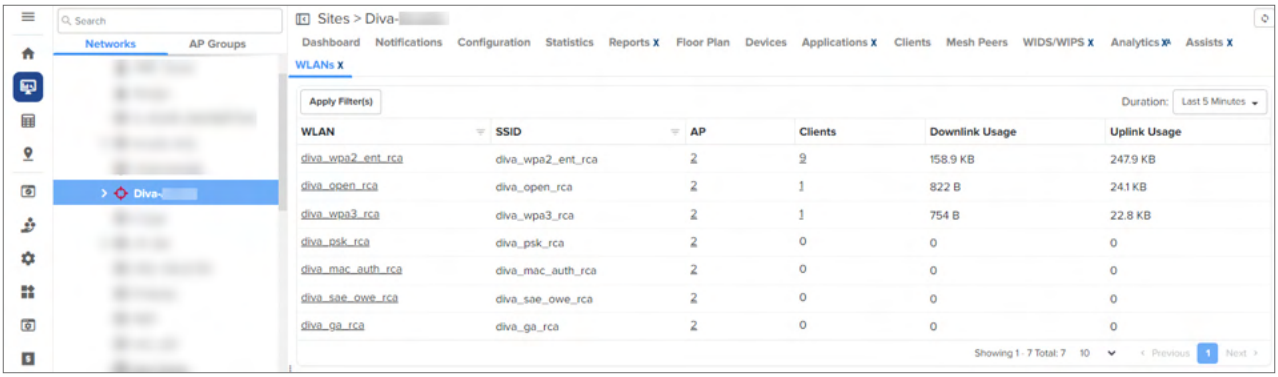
WLANs Dashboard

The **WLANs** dashboard displays details of all WLANs that are applied on devices at a given site. It also displays the number of APs on which the WLAN is applied, the SSID that is configured, and the number of clients that are currently connected to those SSIDs. It also displays the uplink and downlink throughput for that WLAN.

WLAN aggregation is performed only at the site-level. If no clients are connected to the APs, no WLAN data is aggregated.

- To view the WLANs dashboard, navigate to **Monitor and Manage** > ***<Site-Name>*** > **WLANs**[X] tab.

  Figure 223 *WLANs Dashboard*

  The WLANs data is available for the following durations:

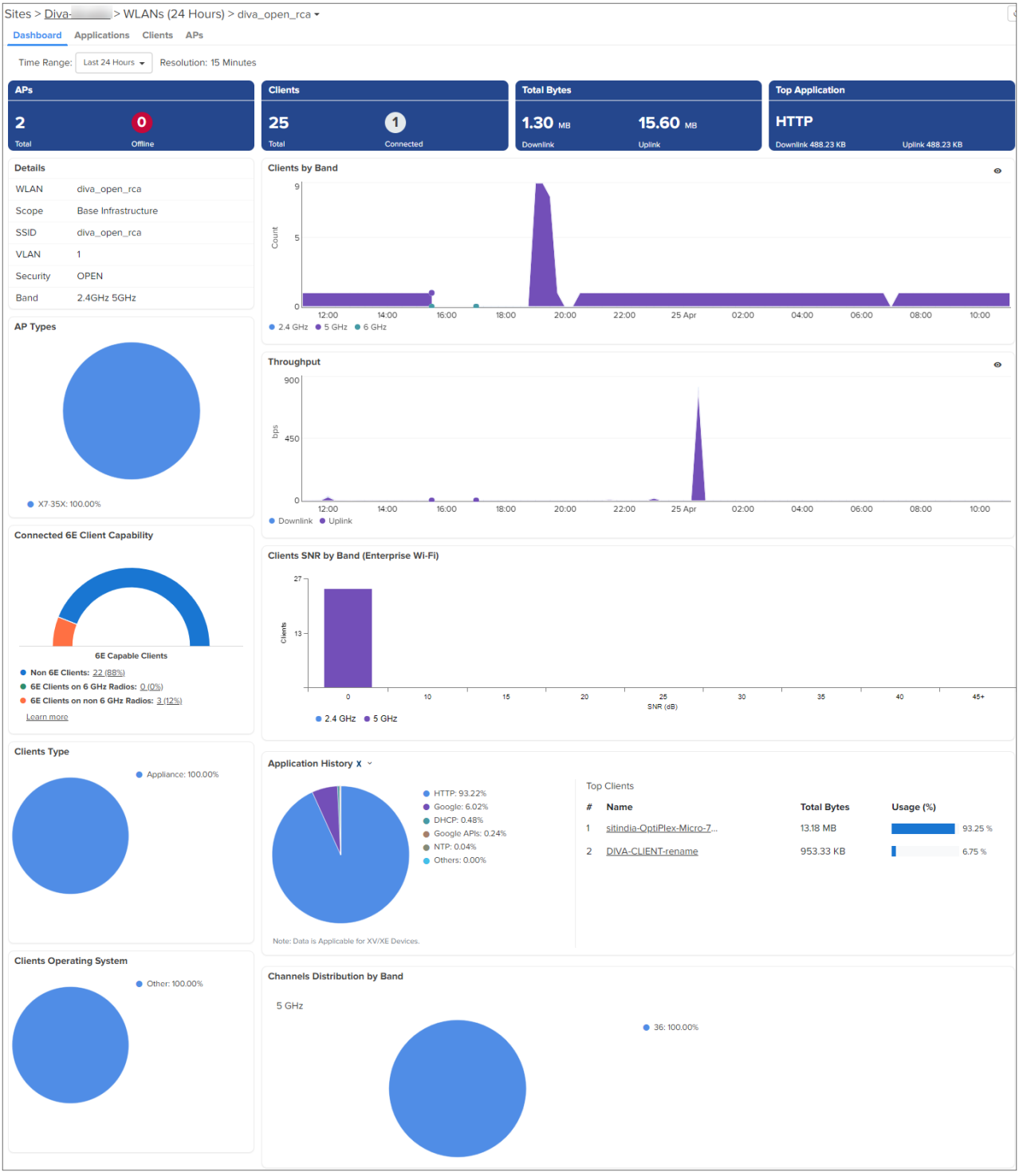
  - **Last 5 minutes**—Includes the most recent WLANs data (active clients and data traffic) for the last five minutes.
  - **24 hours**—Includes WLAN data aggregated every 15 minutes for the last 24 hours. This may include details of any active clients that are still connected to the APs.
  - **7 days**—Includes WLAN data that is aggregated every 1 hour for the last seven days.

- Click a WLAN in the WLANs page to view the WLAN-specific dashboard.

  You can view the data for last 24 hours or seven days by selecting the option from the **Time Range** drop-down list.

  - The dashboard displays the following data:
    - Details
    - AP Types
    - Connected 6E Client Capability
    - Client Type
    - Client Operating System
    - Clients By Band
    - Throughput
    - Clients SNR By Band (Enterprise (Wi-Fi)
    - Application History[X]
    - Channels Distribution By Band

Figure 224 *WLAN-specific Dashboard*



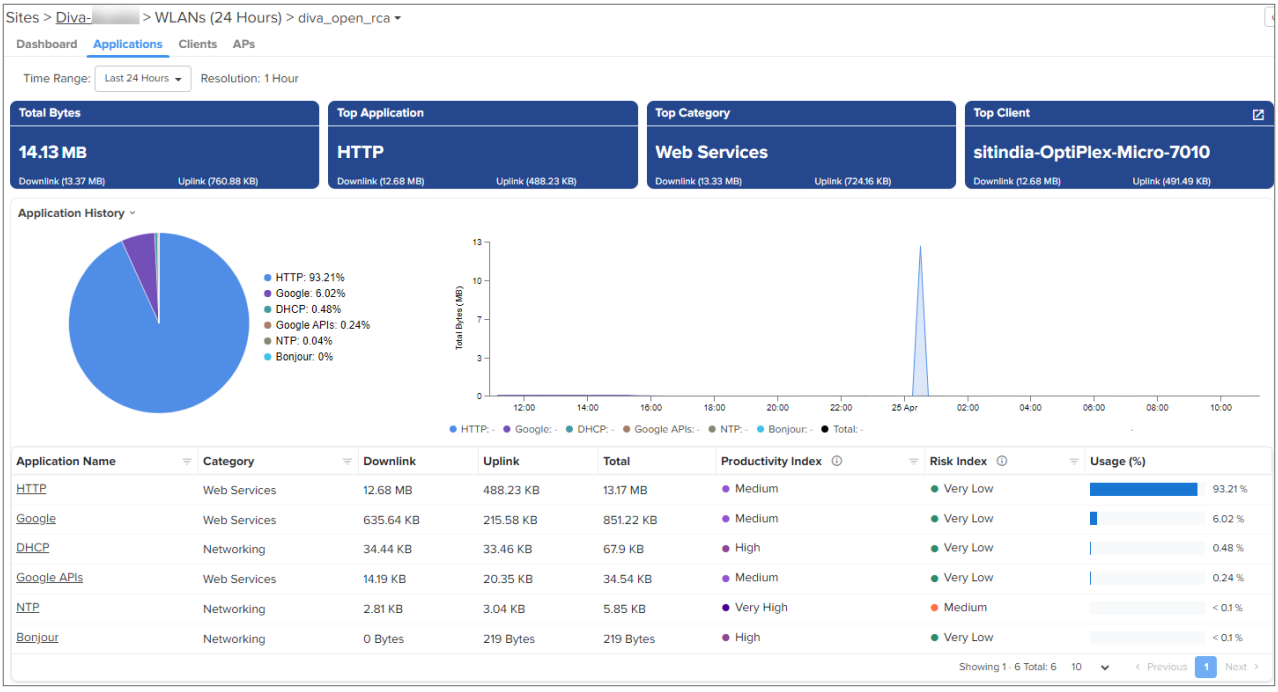
- To view the details of the applications accessed through this WLAN, click the **Monitor and Manage > *<Site-Name>* > WLANs^{X} >** <WLAN-Name> **> Applications** tab.

  The **Applications** dashboard displays both a graphical data and details in a table with the following fields:

Table 55 *Application fields*

Field	Description
Application Name	Name of the application.
Category	Category of the application.
Downlink	Total number of downlink bytes during the period selected.
Uplink	Total number of uplink bytes during the period selected.
Total	Total amount of application data (uplink plus downlink).
Productivity Index	Estimate of the typical productivity of the application. Following are the supported values: • Very Low • Low • Medium • High • Very High
Risk Index	Estimate of the typical security risk of the application. Following are the supported values: • Very Low • Low • Medium • High • Very High
Usage (%)	Percentage of usage by this application in comparison to all applications.

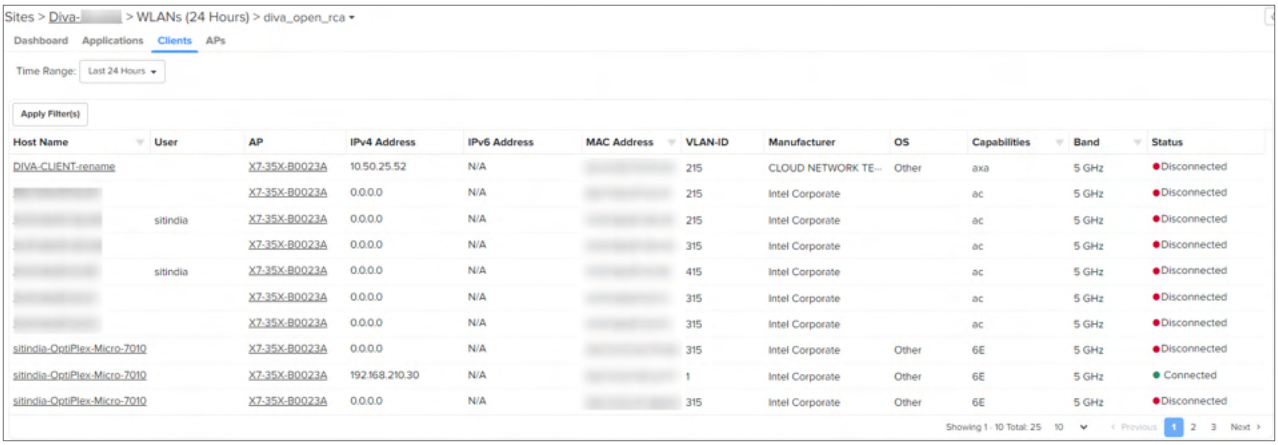
Figure 225 *WLAN-specific Application Dashboard*



- To view information about clients connected to the selected WLAN in the site, click the **Monitor and Manage** > ***<Site-Name>*** > **WLANs**[X] > <WLAN-Name> > **Clients** tab.

  The **Clients** dashboard displays information, such as the hostname of the client, AP to which client was connected, operating system, and radio capabilities.

  Figure 226 *WLAN-specific Clients Dashboard*



- To view information about the APs that are associated with the selected WLAN, click the **Monitor and Manage** > ***<Site-Name>*** > **WLANs**[X] > <WLAN-Name> > **APs** tab.

  The **APs** dashboard displays APs information, such as the device name, MAC address, the AP model, and the data usage..

  Figure 227 *WLAN-specific APs Dashboard*



Fiber OLT and ONU

The Fiber Optical Line Terminal (OLT) from Cambium Networks is a Passive Optical Network (PON) device that connects to a core switch using either an Ethernet cable or a fiber cable. It supports Gigabit Passive Optical Network (GPON), 10 Gigabit Symmetrical PON (XGS-PON), and combo-PON (GPON co-existing with XGS-PON) Optical Defined Networking (ODN) access. The Fiber OLT is available in 8 and 16 ports, including All-in-One (AIO) PON interfaces, allowing simultaneous support for multiple PON technologies. It is used for network development with GPON and User Network Interface (UNI) ports. The high-performance access design of the Fiber OLT focuses on Software-Defined Networking (SDN) deployments, providing open interfaces to all control management functions for seamless integration with SDN environments.

cnMaestro provides management, configuration, and monitoring services for Fiber OLT. It includes the following pages for Fiber OLT and ONU, providing comprehensive tools for efficient management and optimization:

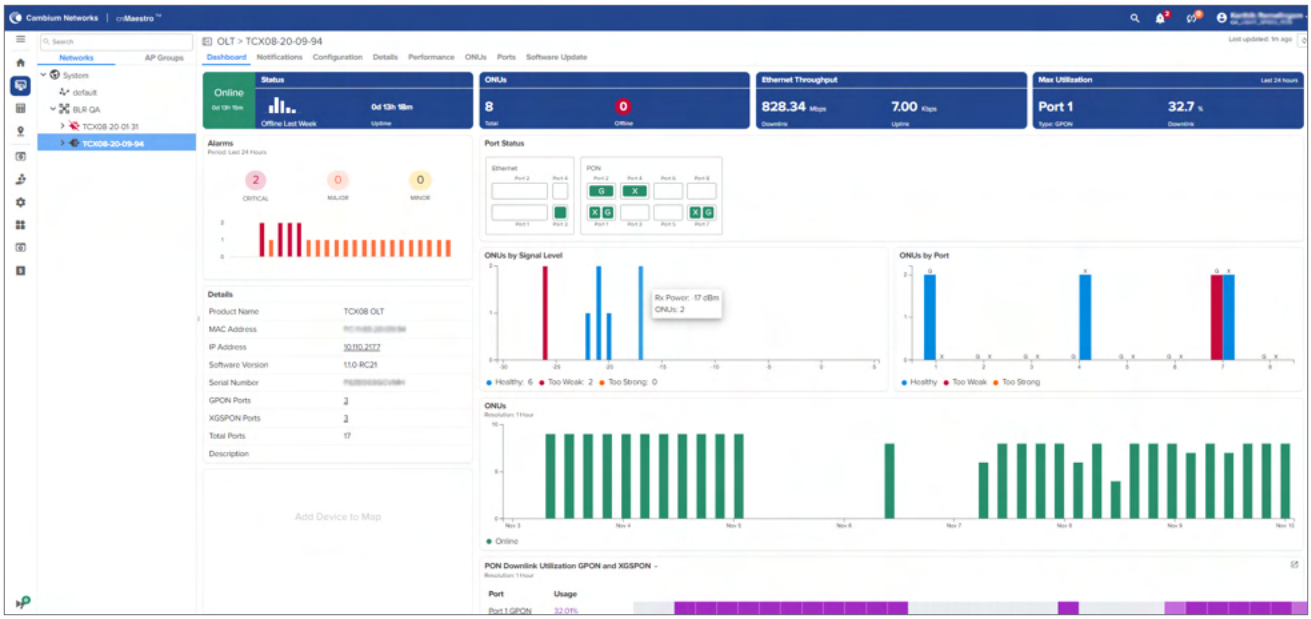
- Dashboard
- Notifications

- Configuration
- Details
- Performance
- ONU
- Ports
- Software Update

Dashboard

Displays the monitoring information of the OLT.

Figure 228 *Fiber OLT dashboard*



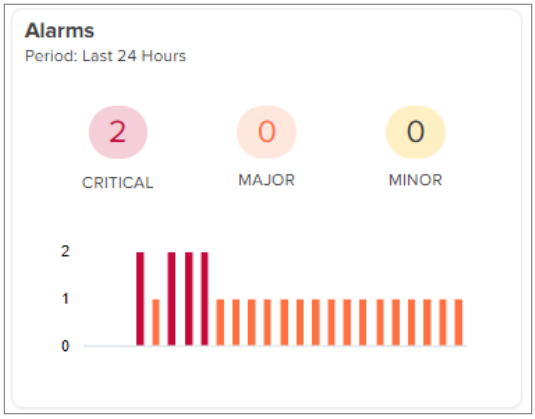
Dashboard has the following elements:

- Alarms
- Port Status
- ONU by Signal Level
- ONU by Signal Level per Port
- ONUs
- PON Downlink Utilization
- PON Downlink throughput
- PON Uplink throughput
- Ethernet Downlink throughput
- Ethernet Uplink throughput

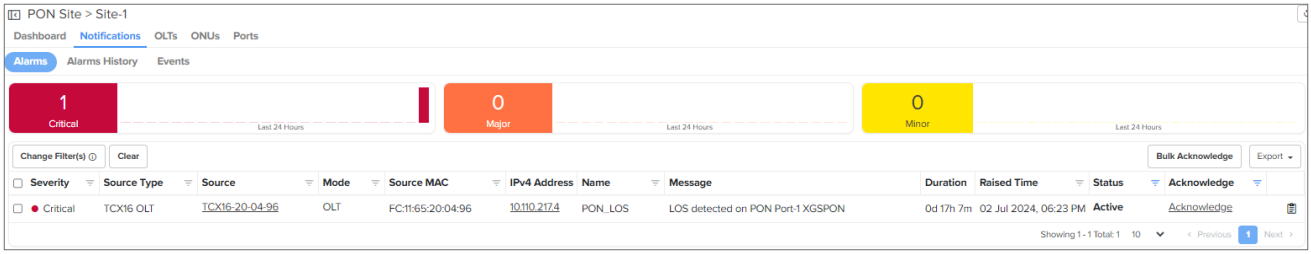
Alarms

Displays the critical, major, and minor alarms. Figure 229 shows the status of the alarms.

Figure 229 *Alarms*



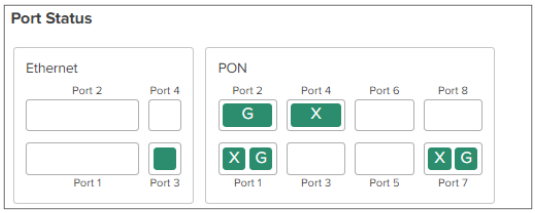
To view the detailed information, click on the respective alarm count.



Port Status

Displays the connection status for Network-to-Network Interface (NNI) or Ethernet (uplink) ports and PON ports (downlink). Small Form-Factor Pluggable (SFP) devices are connected to the Ethernet ports, and ONUs are connected to the PON ports. The uplink NNI has four ports. Port 1 and port 2 support 100 Gbps speed. Port 3 and port 4 support 10 Gbps speed. There are 16 downlink PON ports, with each port supporting both GPON and XGS-PON.

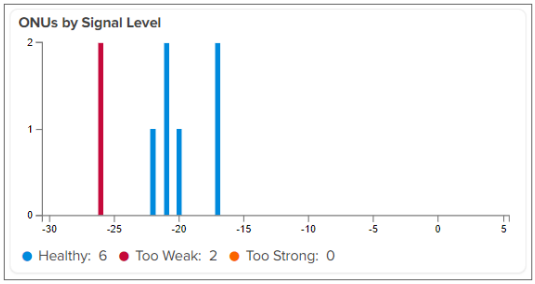
Figure 230 *Port status*



ONU by Signal Level

Displays the signal level received by the ONU.

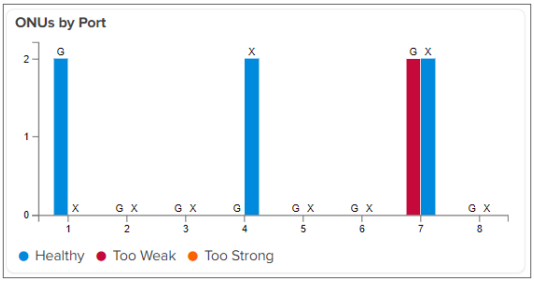
Figure 231 *ONU by signal level graph*



ONU by Signal Level per Port

Displays the number of ONU connected and their corresponding power levels.

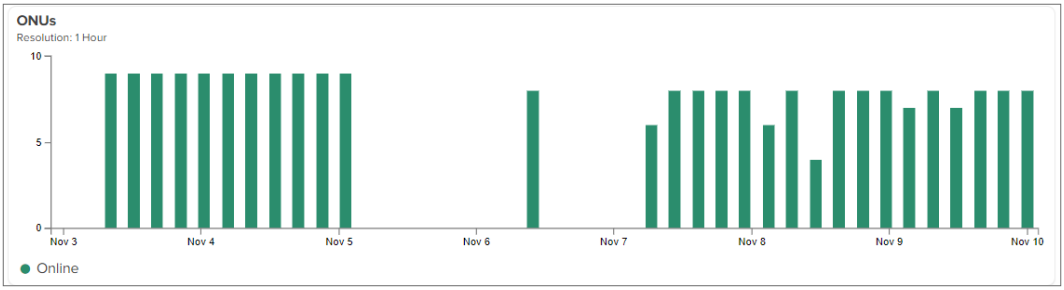
Figure 232 *ONU by signal level per port*



ONUs

Displays the number of ONUs connected to the OLT.

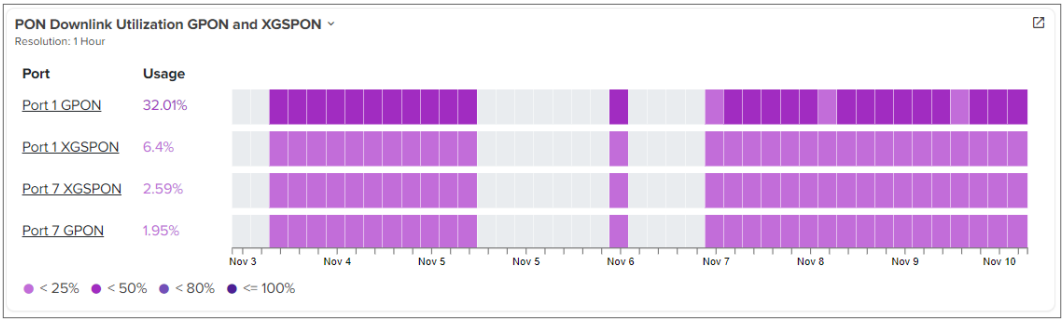
Figure 233 *ONU*



PON Downlink Utilization

Displays the utilization of GPON and XGS-PON.

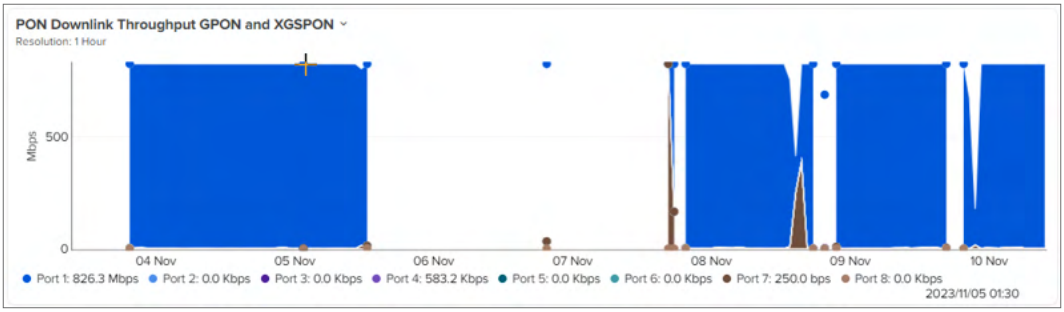
Figure 234 *PON Downlink Utilization*



PON Downlink Throughput

PON Downlink throughput displays the downlink throughput information of GPON and XGS-PON.

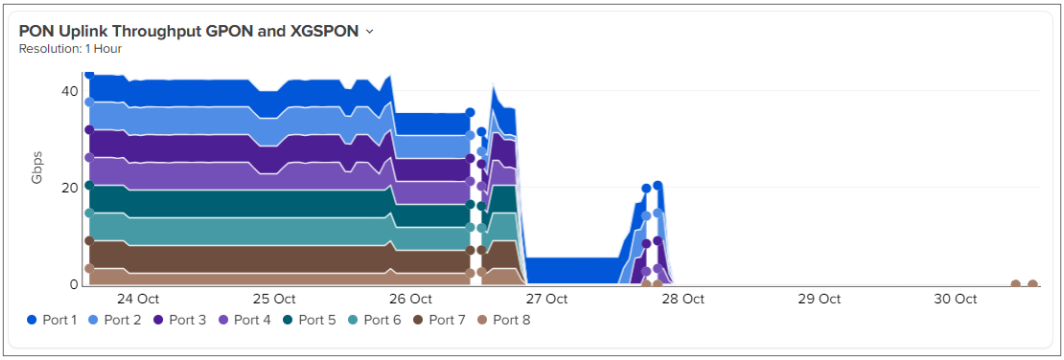
Figure 235 *PON Downlink Throughput*



PON Uplink Throughput

Displays the uplink throughput information of GPON and XGS-PON.

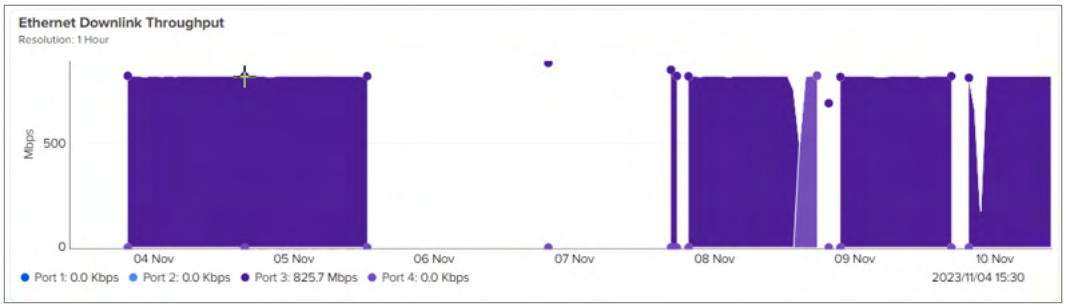
Figure 236 *PON Uplink Throughput*



Ethernet Downlink Throughput

Displays the Ethernet Downlink information of GPON and XGS-PON.

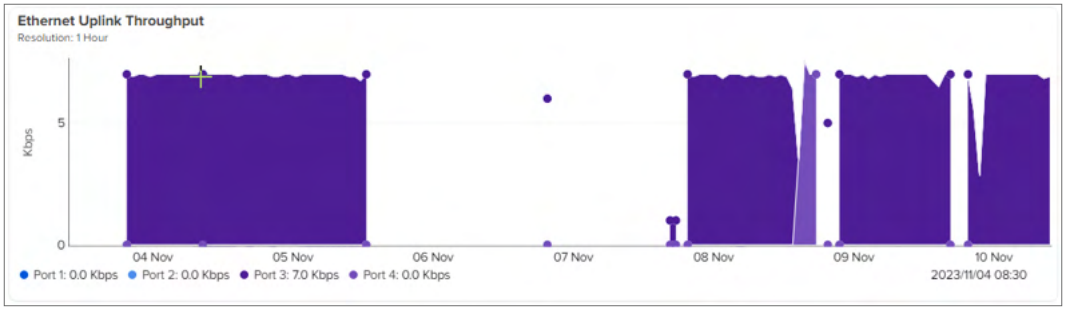
Figure 237 *Ethernet Downlink throughput*



Ethernet Uplink Throughput

Displays the Ethernet Uplink information of GPON and XGS-PON.

Figure 238 *Ethernet Uplink Throughput*



Notifications

Displays the alarm information of the OLT.

Figure 239 *Notifications*

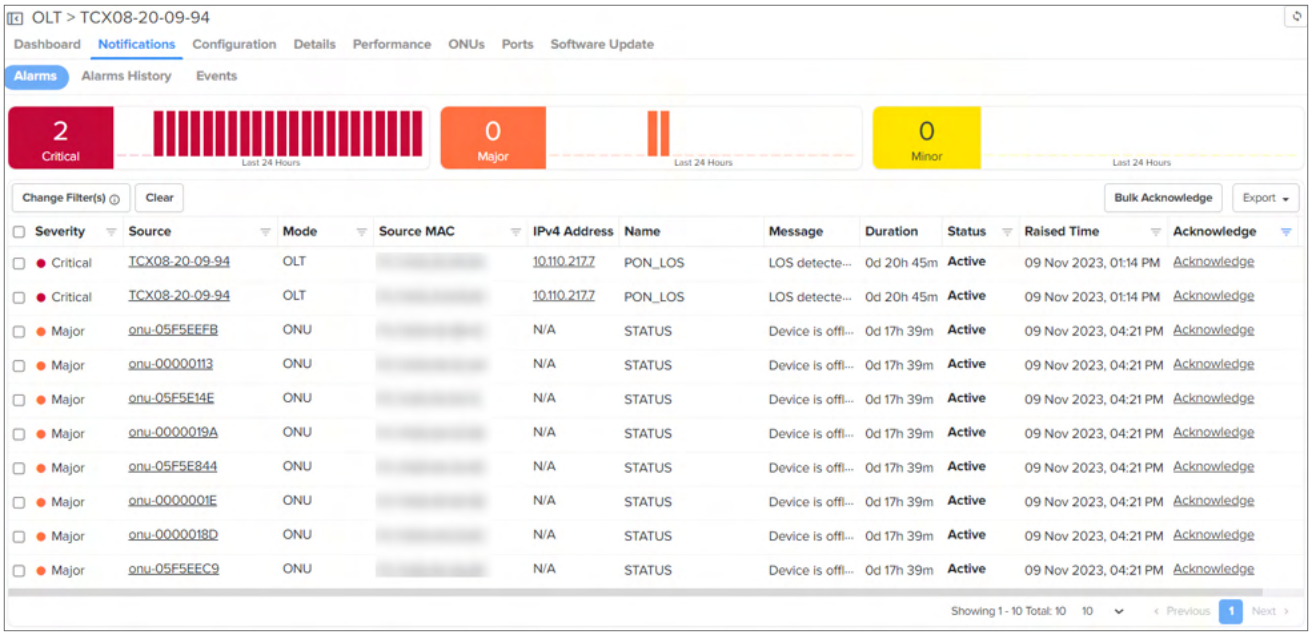


Table 56 *Parameters on the Notifications page*

Parameter	Description
Severity	Severity level of the alarm. This parameter supports the following severity levels: • Critical • Major • Minor
Source	Name of the OLT.
Mode	Type of the device. The following device types are supported: • OLT • ONU
Source MAC	MAC address of the OLT.
IPv4 address	IPv4 address of the OLT.

Parameter	Description
Name	Name of the ONU.
Message	A brief description of the alarm message.
Duration	Duration of the alarm.
Status	Status of the alarm. The following status values are supported: • Active • Inactive
Raised Time	Time when the alarm was raised.

Configuration

Users can configure the OLT using the Configuration tab. To sync the configuration with the E2E network, from the tree menu, click the **Actions** (⋮) icon corresponding to the OLT device and select **Sync Topology**

Figure 240 *Configuration*

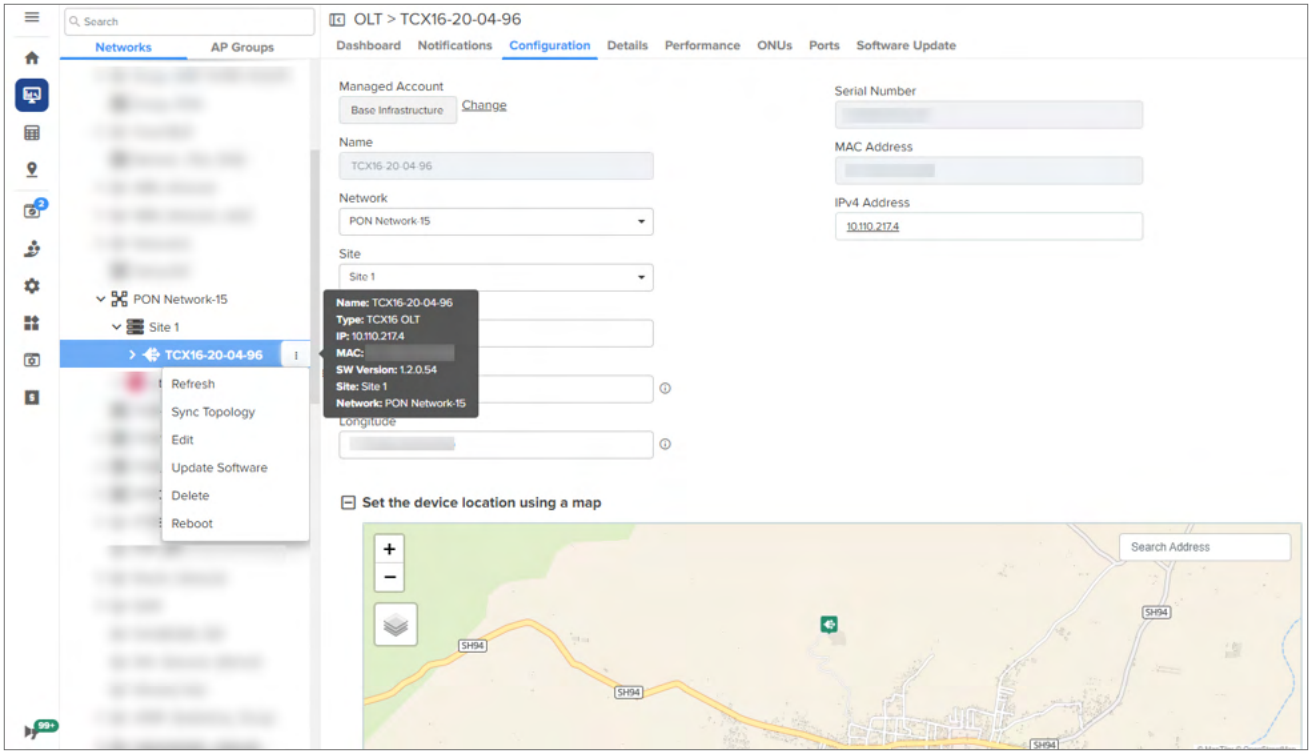


Table 57 *Parameters on the Configuration page*

Parameter	Description
Managed Account	Name of the site where OLT is configured.
Name	Name of the OLT.
Network	Name of the network where OLT is configured.
Site	Name of the site.
Description	A brief description of the OLT.
Latitude	Latitude of the OLT.
Longitude	Longitude of the OLT.

Parameter	Description
Serial Number	Serial Number (MSN) of the OLT.
MAC Address	MAC Address of the OLT.
IPv4 Address	IPv4 Address of the OLT.

Details

The Details page displays general configuration and runtime information of the OLT.

Figure 241 *Details*

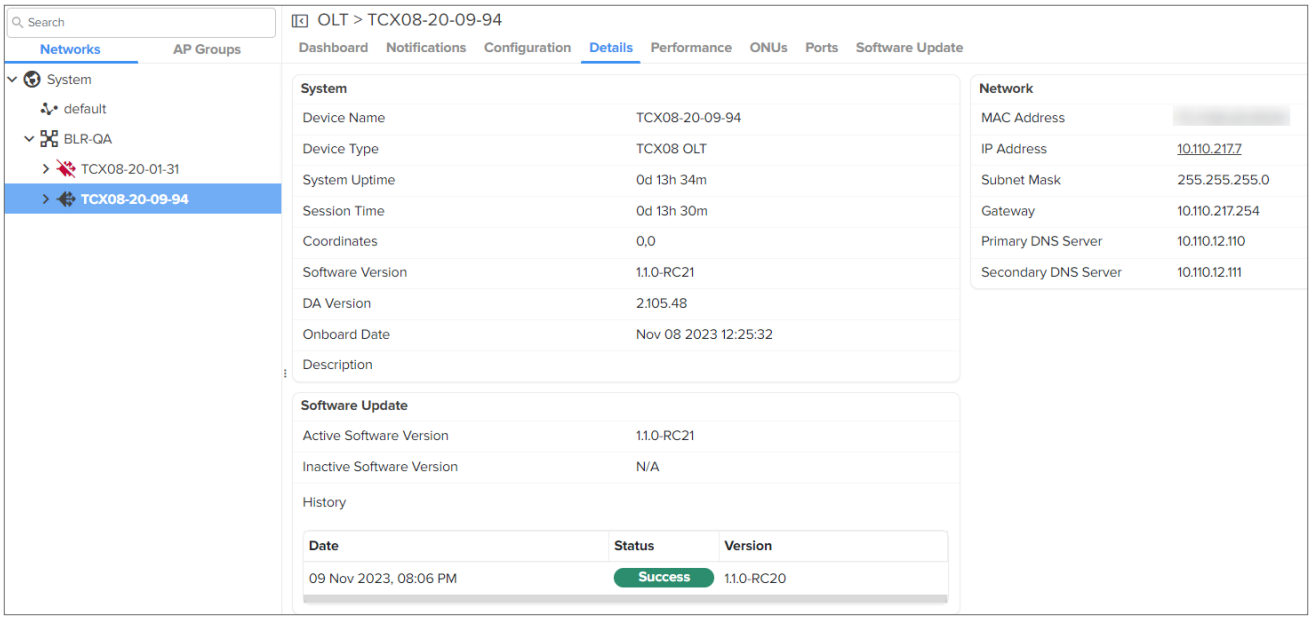


Table 58 *Parameters on the Details page*

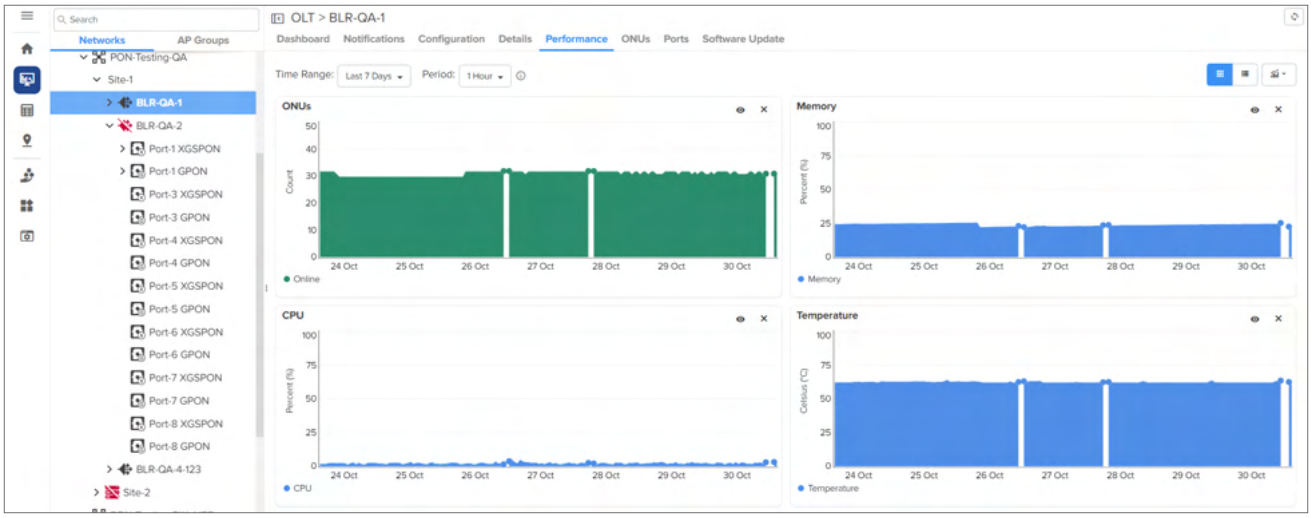
Parameter	Description
System	
Device Name	Name of the device.
Device Type	Type of the device. This parameter supports the following device types: • OLT • ONU
System Uptime	Date and time configured for the device.
Session Time	Duration of the session.
Coordinates	Latitude and longitude.
Software Version	The current software version used.
DA Version	Version of the device agent (DA).
Onboard Date	Onboard date of the device.
Description	A brief user-defined description of the onboarded device.
Software Update	
Active Software Version	Version of the active software.
Inactive Software Version	Version of the inactive software.

Parameter	Description
History	History of software version updates.
Network	
MAC Address	MAC Address of the device.
IP Address	IP Address of the device.
Subnet Mask	Subnet Mask of the device.
Gateway	Gateway address of the device.
Primary DNS Server	IP address of the primary DNS server.
Secondary DNS Server	IP address of the secondary DNS server.

Performance

Displays the performance graphs for ONU, CPU, memory, and temperature of the OLT and ONU.

Figure 242 *Performance*



ONU

Displays the number of ONUs connected to the OLT and their information.

Figure 243 *ONU*

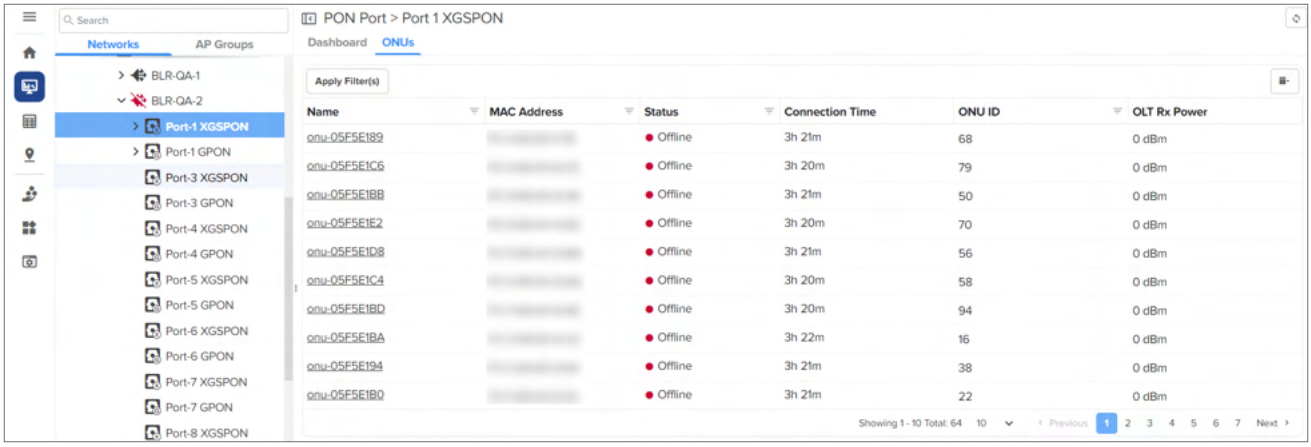


Table 59 *Parameters on the ONU page*

Parameter	Description
Name	Name of the OLT.
MAC Address	MAC address of the OLT.
Status	Status of the OLT.
OLT Port	Port number of the OLT to which ONU is connected.
Connection Time	Time during which ONU is connected to OLT.
ONU ID	ID of the ONU.
OLT Rx Power	Receive power of the OLT.

Ports

Displays the port details. Fiber OLT has 8 ports and 16 ports.

Figure 244 *Ports*

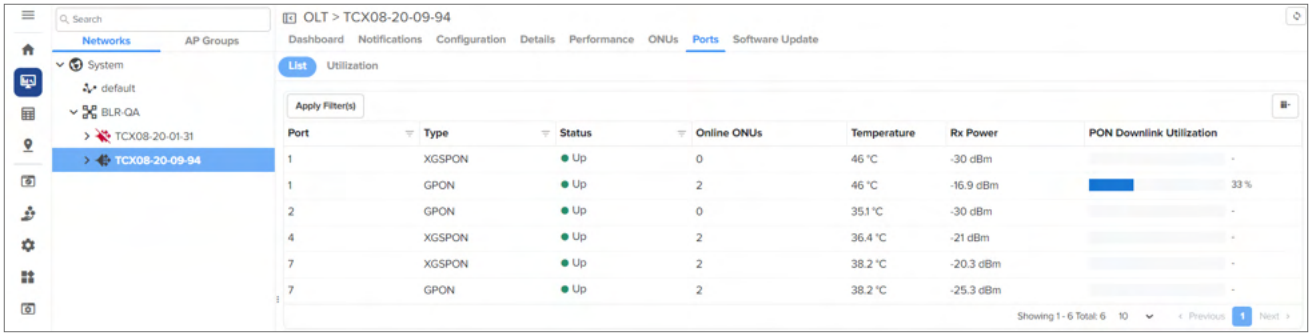
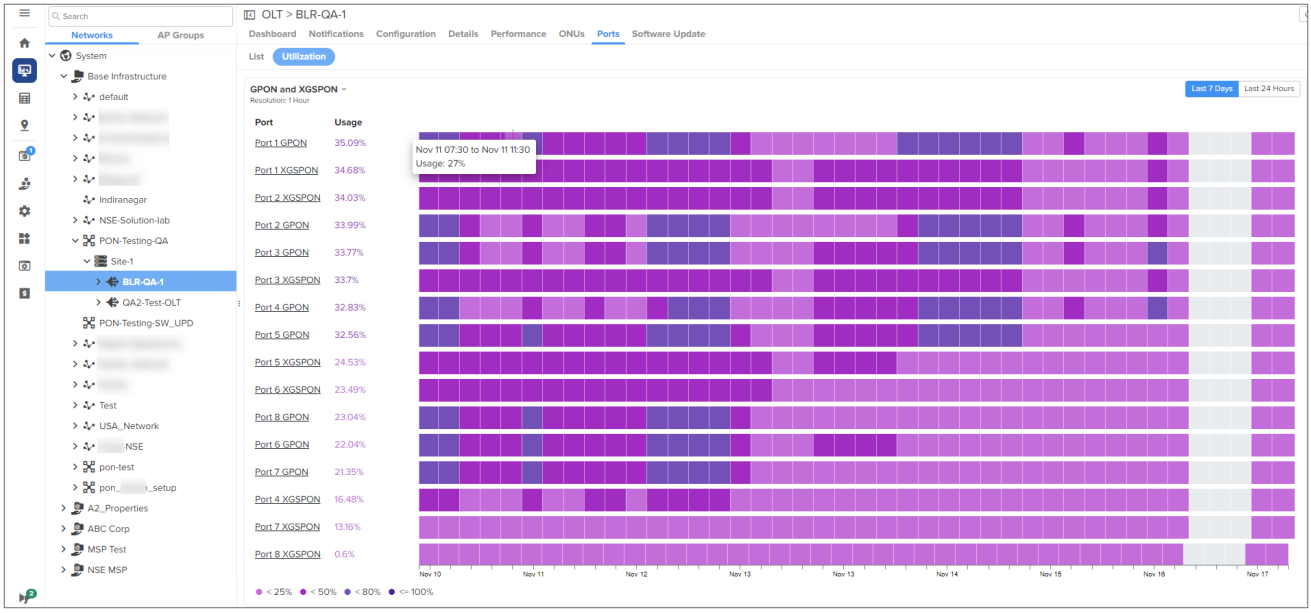


Figure 245 *Ports utilization*



To filter selected ports, perform the following steps:

1. Click **Apply Filter(s)**, type the port name.
2. Select the type of the OLT.
3. Select the status of the OLT and click **Apply Filter(s)**.

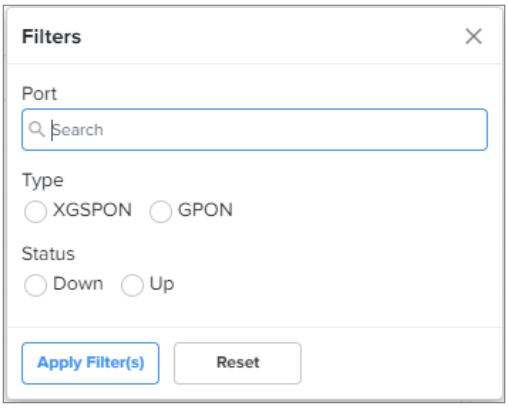


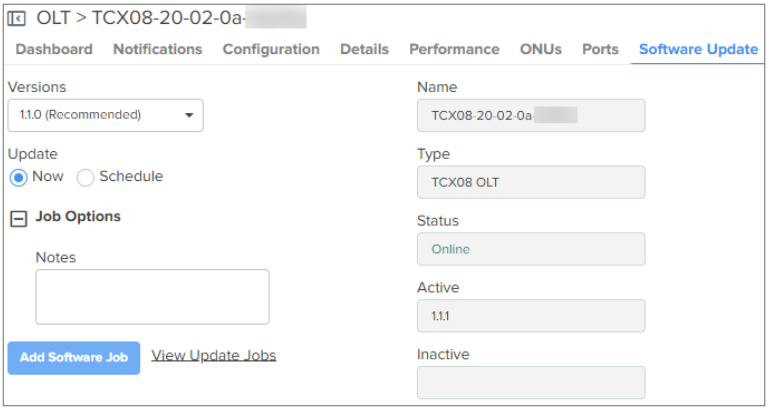
Table 60 *Parameters on the Ports page*

Parameter	Description
Port	Port number of the OLT.
Type	Type of the PON.
Status	Status of the ONU.
Online ONU	Number of ONUs online.
Temperature	Temperature of the ONU.
Rx Power	Receive power of the ONU.
PON Downlink Utilization	Utilization percentage of the PON Downlink.

Software Update

Users can upgrade the OLT firmware using the **Software Update** page. To upgrade the software, perform the following steps:

1. Download the latest firmware from Cambium Networks Support Site.
2. Select **OLT**.
3. Select the software version from the drop-down.
4. Click **Add Software Job** to upload the latest Firmware file.
5. Once the firmware file is uploaded, the software update job is added to the list of update jobs.
6. Click **View Update Jobs** to view the history of the software updates. This provides a record of all previous software update jobs.



Inventory

The Inventory page displays a list of devices under the selected Node. It presents health and maintenance information in a tabular view that allows for sorting and filtering. When selected for a single device, it presents a detailed customized page of that device.

Navigate to the **Inventory** tab on the left pane.

Figure 246 *Inventory page at the System-level*

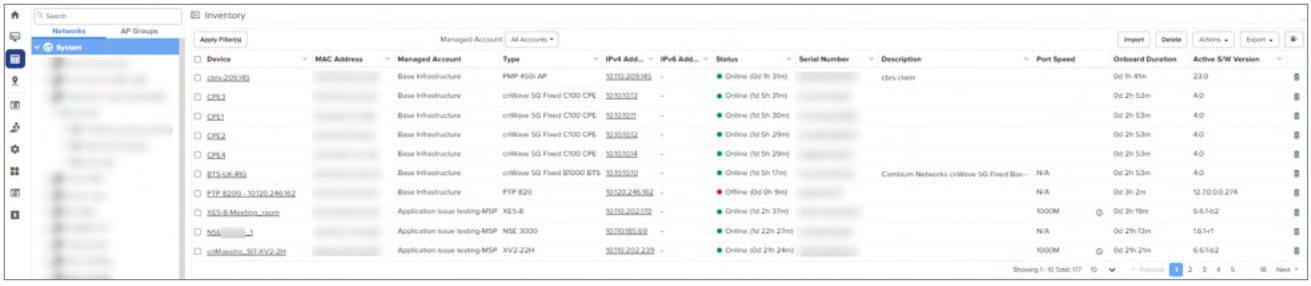
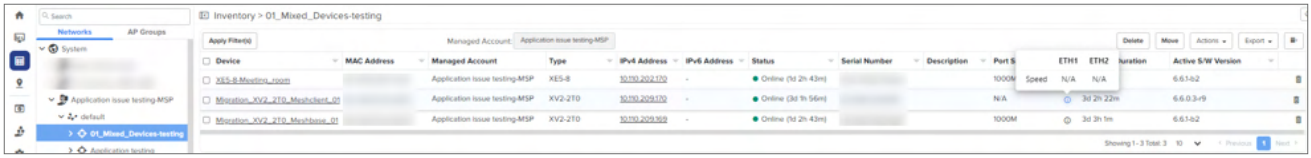


Figure 247 *Inventory page at the Site-level*



Note

The **Port Speed** column displays the port speed (in Mbps) for the Enterprise Wi-Fi devices only.

- At the System-level, you can enable the **Port Speed** column by selecting the **Port Speed** checkbox from the Column selector ( ).
- At the Site-level, the **Port Speed** column is displayed by default.

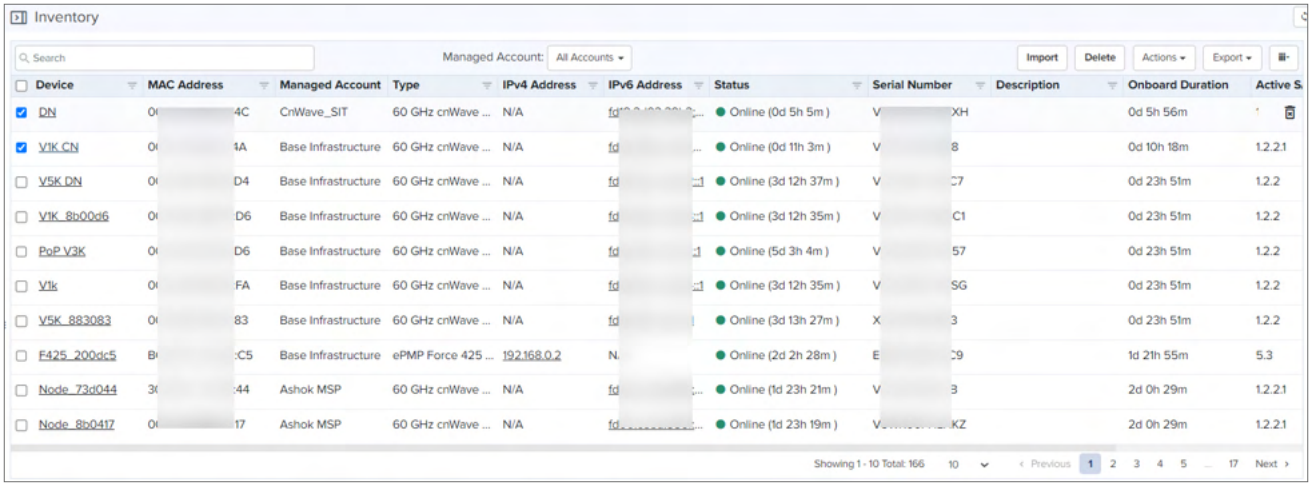
Inventory Export

The inventory table can be exported in either the CSV or the PDF format. The values exported will match those in the selected table columns. You can customize the health and maintenance views to add or delete columns.

Bulk Delete

The **Bulk Delete** option is available in the inventory page of System/MSP/Tower/Network/Site.

Figure 248 *Bulk Delete*



To delete devices using bulk delete, perform the following steps:

1. Navigate to the **Inventory** page of System/MSP/Network/Tower/Site.
2. Select one or multiple devices by selecting the corresponding checkboxes.
3. Click the **Delete** button.

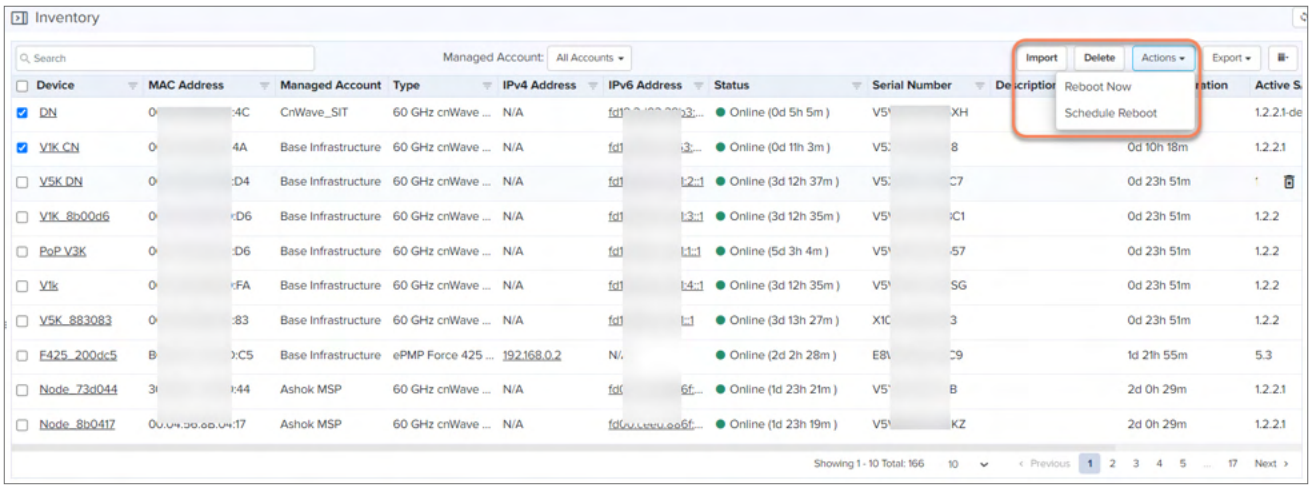
After deleting devices in bulk, you can view the status in the **Administration** > **Jobs** > **Actions** page.

For more information about deleting devices in bulk, see Deleting Devices in Bulk.

Bulk Reboot

The **Bulk Reboot** option is available on the inventory page of Tower/Network/Site. When the devices are rebooted using Bulk Reboot, all the Network/Tower/Site Dashboards, Graphs, Clients, Reports, and Mesh Peers will be updated accordingly.

Figure 249 *Bulk Reboot*



To reboot devices using bulk reboot, perform the following steps:

1. Navigate to **Inventory** page of Network/Tower/Site.
2. Select one or multiple devices.

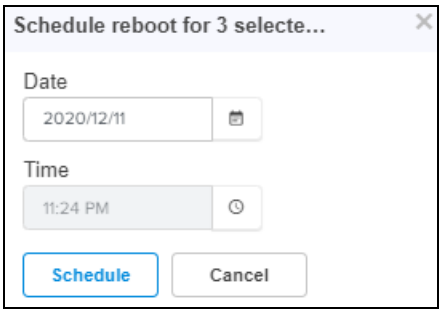
3. Click **Actions** and choose **Reboot Now**.

Schedule Reboot

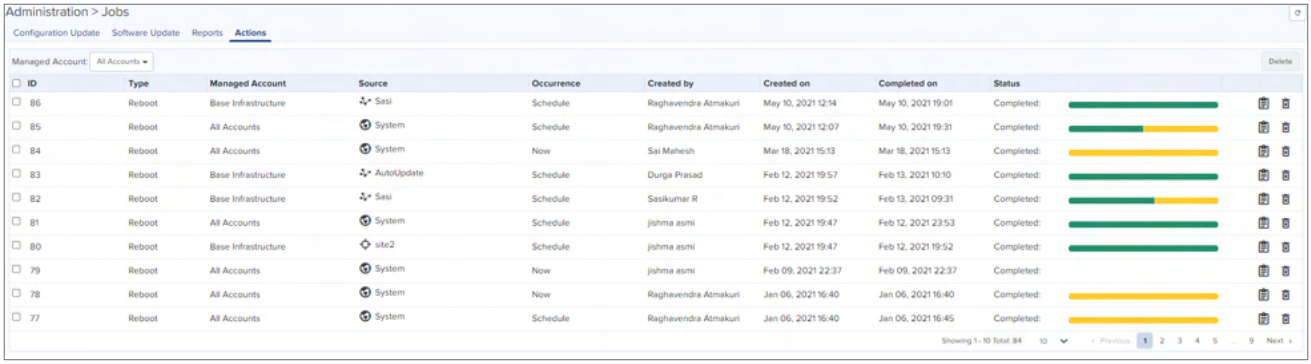
Schedule a reboot of the device(s) by selecting **Schedule Reboot** from **Actions** drop-down.

To reboot devices using schedule reboot, perform the following steps:

1. Navigate to **Inventory** page of Network/Tower/Site.
2. Select one or multiple devices.
3. Click **Actions** and choose **Schedule Reboot**.
4. Enter **Date** and **Time**.
5. Click **Schedule**.



After creating a scheduled reboot job, you can view the status in the **Administration > Jobs > Actions** page.



Import Device Configuration

Import device(s) configuration is available from the inventory page at System/Network/Managed Account/ePMP or PMP AP device levels.

Note

The Import Device configuration is supported only for the Access and Backhaul account and is applicable only on ePMP/PMP AP and SM devices.

The following parameters are supported for ePMP/PMP AP in the CSV file:

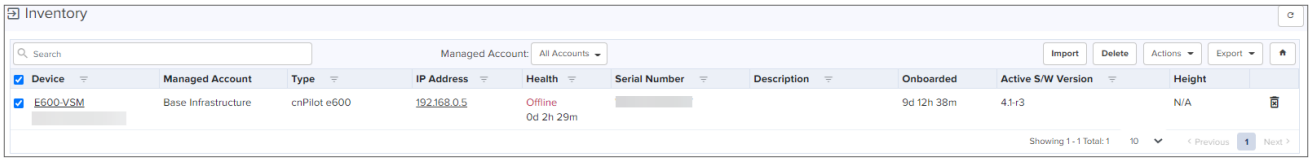
- Azhimuth
- Beamwidth
- Elevation
- Height

- Latitude
- Longitude

The following parameters are supported for ePMP/PMP SM is in the CSV file:

- Latitude
- Longitude

Figure 250 *Import Device Configuration*

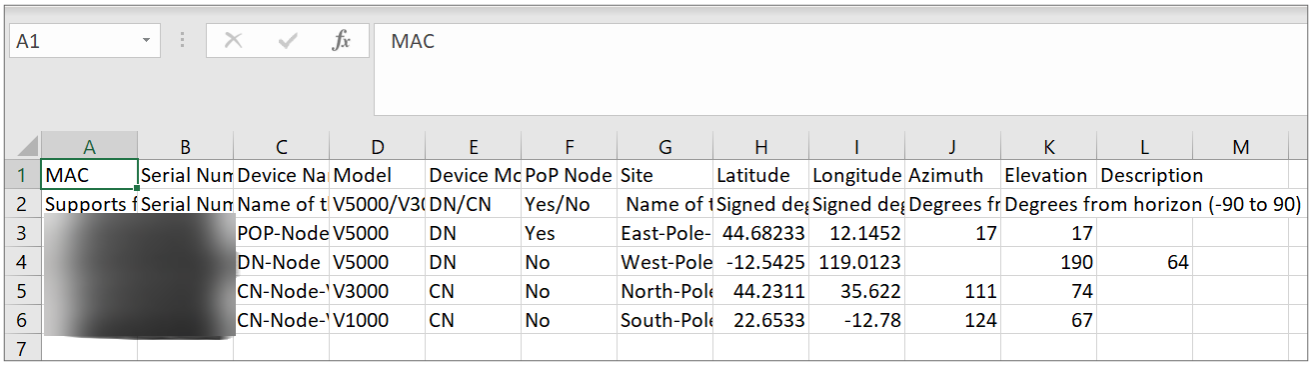


Sample Configuration File

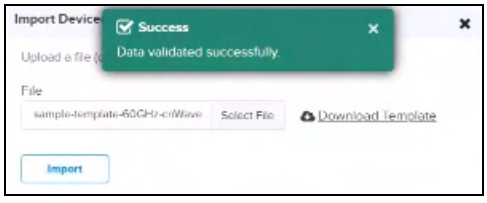
MAC	LATITUDE	LONGITUDE	AZIMUTH	ELEVATION	BEAM WIDTH	HEIGHT	HEIGHT UNIT
Supports formats with ':', '-', 'no space', upper and lower case.	Signed degrees format (DDD.ddd).	Signed degrees format (DDD.ddd).	Degrees from North (0 to 360)	Degrees from horizon (-90 to 90)	Degrees from 1 to 360	Min=0, Max=5	Meters/Feet
[redacted]	16	19	17	17	130	1500	Feet
[redacted]	-90	119.0123	190	64	120	1000	feet
[redacted]	79.0123	11	111	74	112	110	Meters
[redacted]	-44	-12.78	124	67	177	190	meters

Sample Configuration File (60 GHz cnWave)

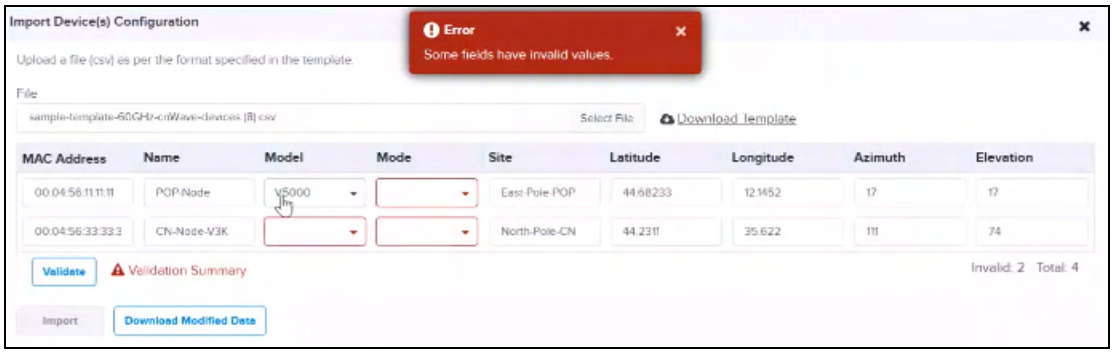
Figure 251 *Sample Configuration file: 60 GHz cnWave*



While importing the file, it automatically validates the data as shown below:



If any invalid fields are found, an error message pops up:



Uploading a Configuration File

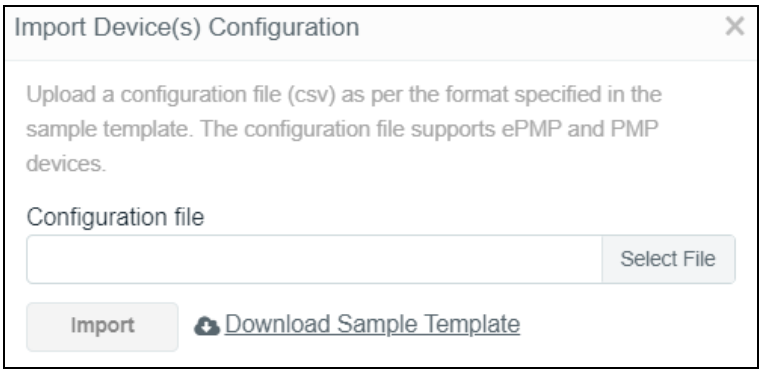
To upload a configuration file (CSV) using the format specified in the sample template, perform the following steps:

1. Click **Download Sample Template** or prepare a sheet in CSV file format with necessary column details.
2. Upload a configuration file (CSV) using the format specified in the sample template.

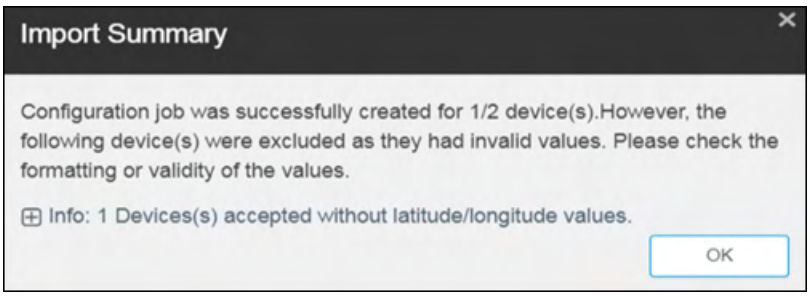
> **Note**
>
> You must know the MAC address of the device to push the configuration.

3. Click **Import**.

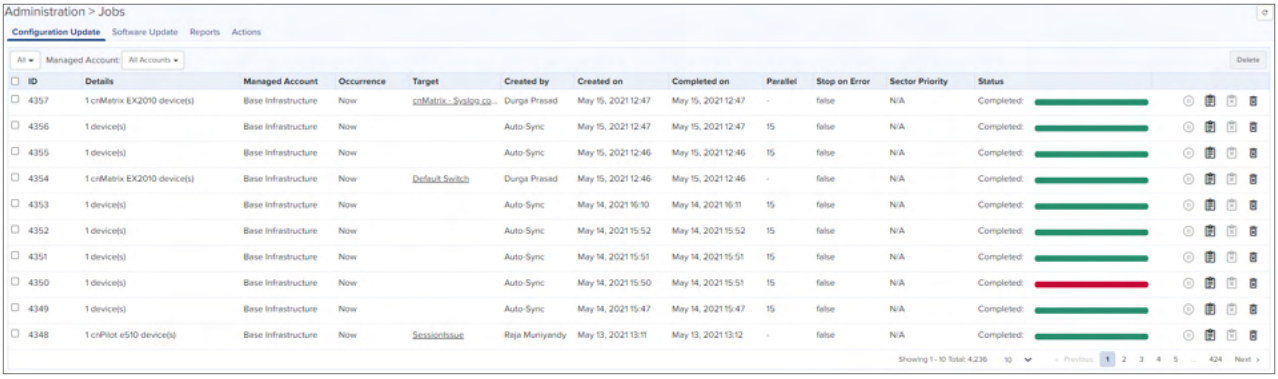
Figure 252 *Uploading Configuration file*



4. A configuration job will be created.



5. You can view the completed status of the configuration import in the configuration update page.



The following table provides details on different errors that might occur while importing a CSV file:

Table 61 *Importing Error*

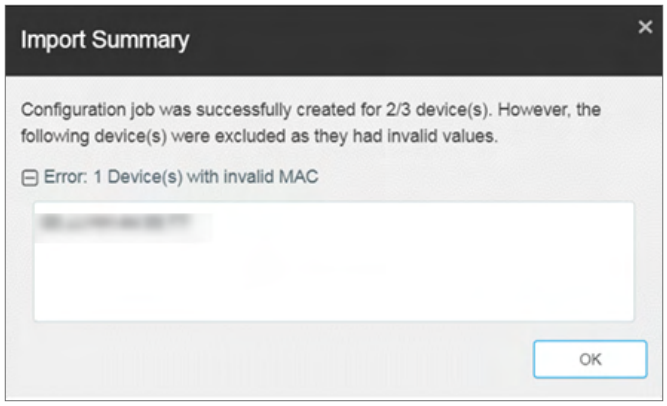
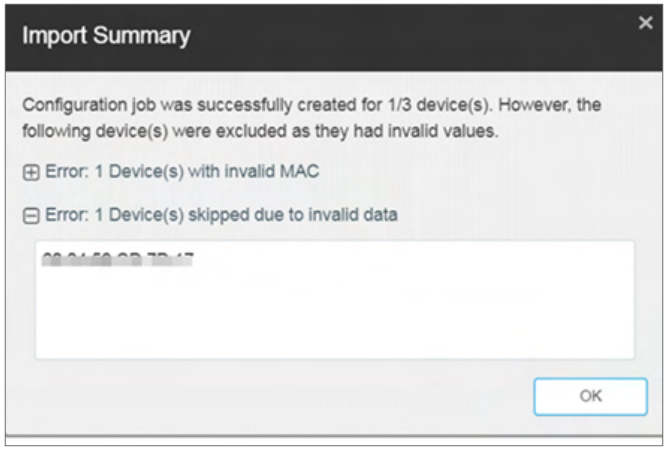
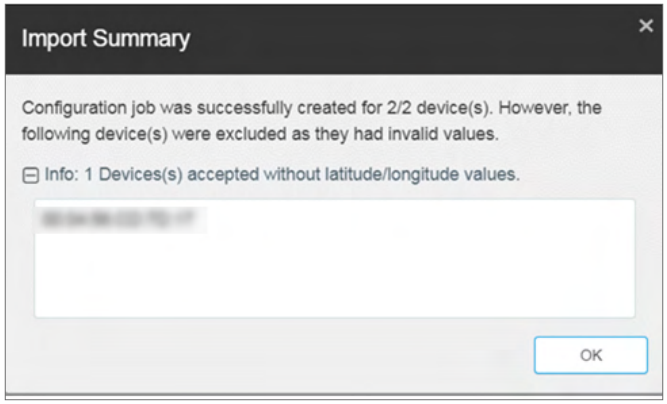
Error	Description
{Count of Devices} Device(s) with invalid MAC	This error is displayed if the uploaded CSV file contains an invalid MAC Address. 
{Count of Devices} Device(s) skipped due to invalid data	This error is displayed if the uploaded CSV file contains invalid Data or data not relevant for Latitude, Longitude, Azimuth, Height, and Elevation. 
Devices were not found for supplied MAC	This error message is displayed if the devices were not found with correct MAC address in the CSV file.

Table 61 *Importing Error*

Error	Description
Address	
Info: 1 Devices (s) accepted without latitude/longitude values	This error is displayed when the latitude and longitude values are tried to push on to ePMP AP or PMP AP which are under a Tower. 

Reports

There are two types of reports: Data Reports and Graphical Reports. Data Reports generate a CSV file and are meant to be read by Excel, Power BI, or a custom application. Graphical Reports generate a PDF file meant for human consumption.

The **Scheduled** tab displays reports that have not run. This includes reports executed periodically and those meant to run a single time. The **Completed** tab lists all reports that have finished and are available for download.

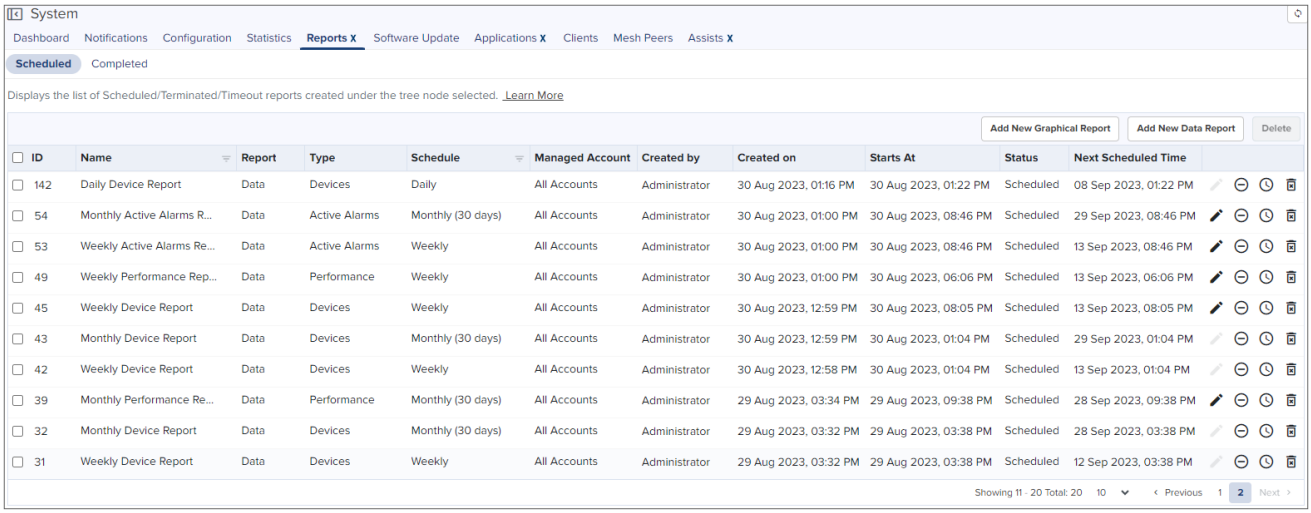
Scheduled Reports include the Scheduled, Terminated, and Timeout status in the Status column. **Completed Reports** include the Completed and Failed status is the Status column. Data reports are displayed only in a tabular format while graphical reports include charts and graphs.

Note

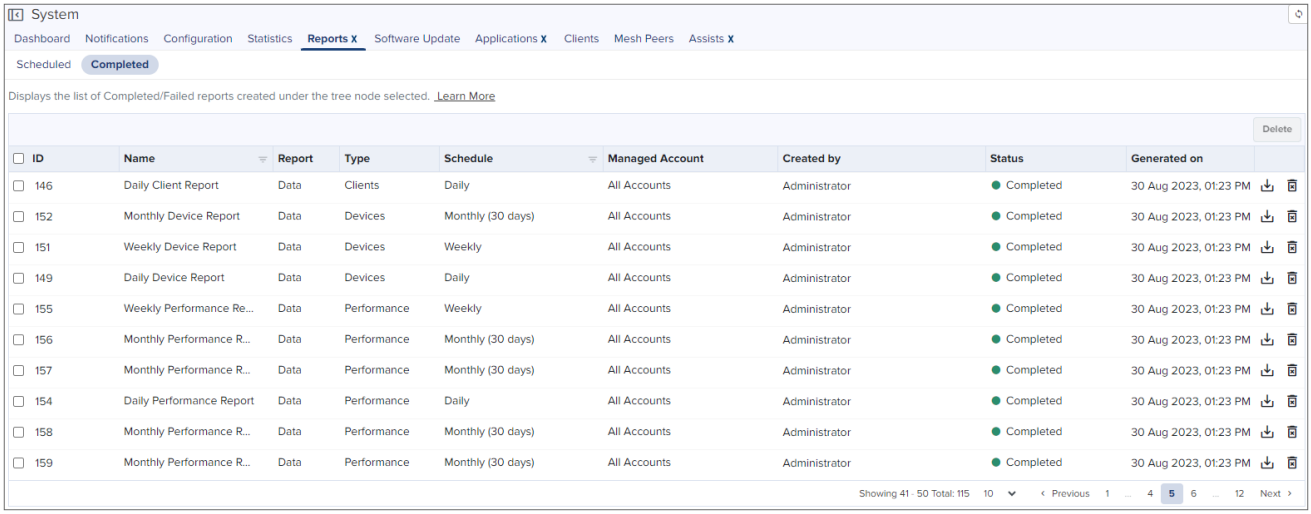
You can schedule and view reports (data and graphical) at the following levels in cnMaestro:

- System
- Network—Only data reports are available
- Site
- MSP

To view all scheduled data and graphical reports, navigate to **Monitor and Manage > System/<Nework-name>/<Site-name>/<MSP-name> > Reports** X **> Scheduled**.



To download completed reports, navigate to **System** > **Monitor and Manage** > **Reports X** > **Completed**.





Note

- You can have 50 reports in the **Scheduled** tab and any number in the **Completed** tab. Only 50 reports can be generated in parallel in a cnMaestro account.
- The completed reports are available for download for 30 days in the Cloud and for seven days in On-Premises.
- While generating Alarm History, Events, Performance, Clients, and Guest Access reports, there is a delay of up to 20-30 minutes for the recent entries to be available in the report.

Data Reports

Data Reports generate a CSV document that can be viewed in Excel, Power BI or other data analysis tools.

This section details how to schedule and generate different types of data reports in cnMaestro.

- Device Report
- Performance Report
- Active Alarms Report
- Alarm History Report

- Events Report
- Clients Report
- Guest Access Login Events

Note

cnMaestro supports 14 months of historical data for devices:

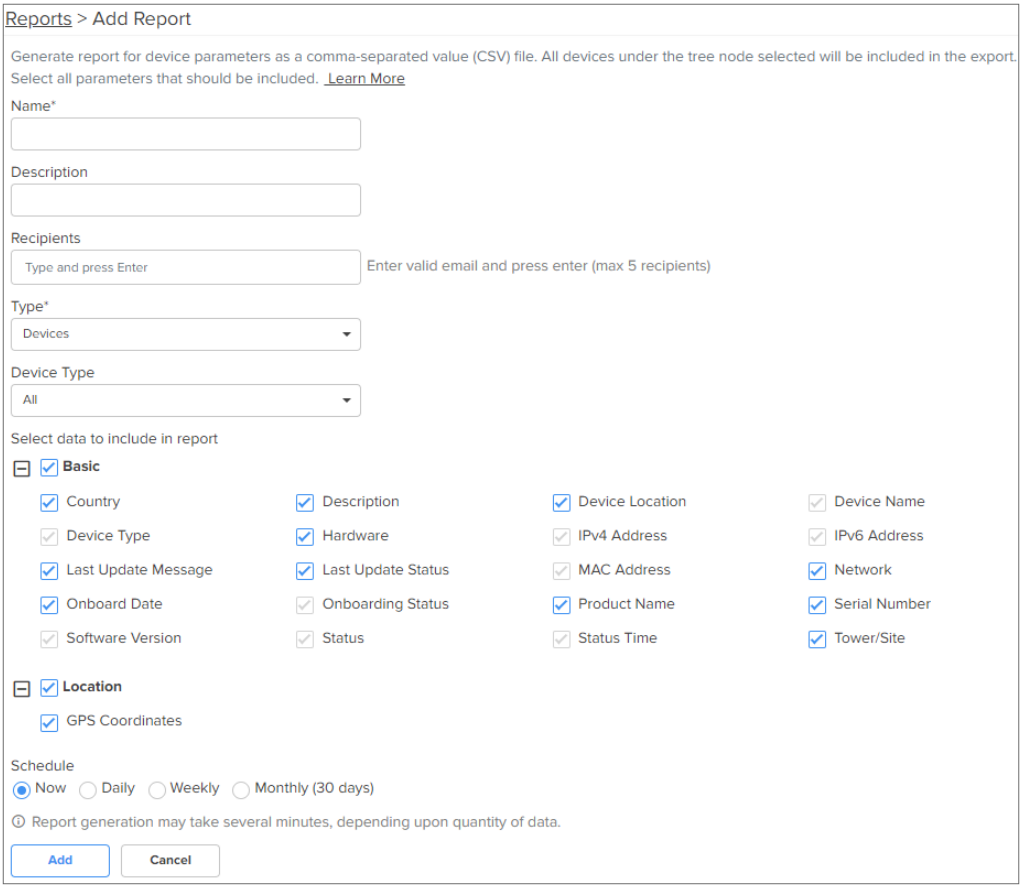
- cnPilot Home (R-Series)
- Enterprise devices (Enterprise Wi-Fi and cnMatrix)
- IIoT devices
- cnMaestro supports 26 months of historical data for devices:
- Fixed Wireless

Device Report

Device Reports are generated as CSV files and include all devices under the selected tree node.

To generate Device Reports, perform the following steps: X

1. Navigate to **Reports** X> **Scheduled** tab within System, MSP, Site, Network, or Tower nodes in the hierarchical tree.
2. Click **Add New Data Report**. The following window is displayed.



3. Enter a **Name** and **Description** for the report.

4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
5. Select the **Report Type** as **Devices**..
6. Select the **Device Type** such as cnMatrix, cnPilot Home, and cnRanger.
7. Select the data parameters to include in the report.
8. Select the **Schedule** such as Now, Daily, Weekly, or Monthly.
9. Click **Add**. The report is added to the **Scheduled Reports** page.

   If **Device Type** is **All**, then **Basic** data export parameters are available, rather than parameters specific to a device type.

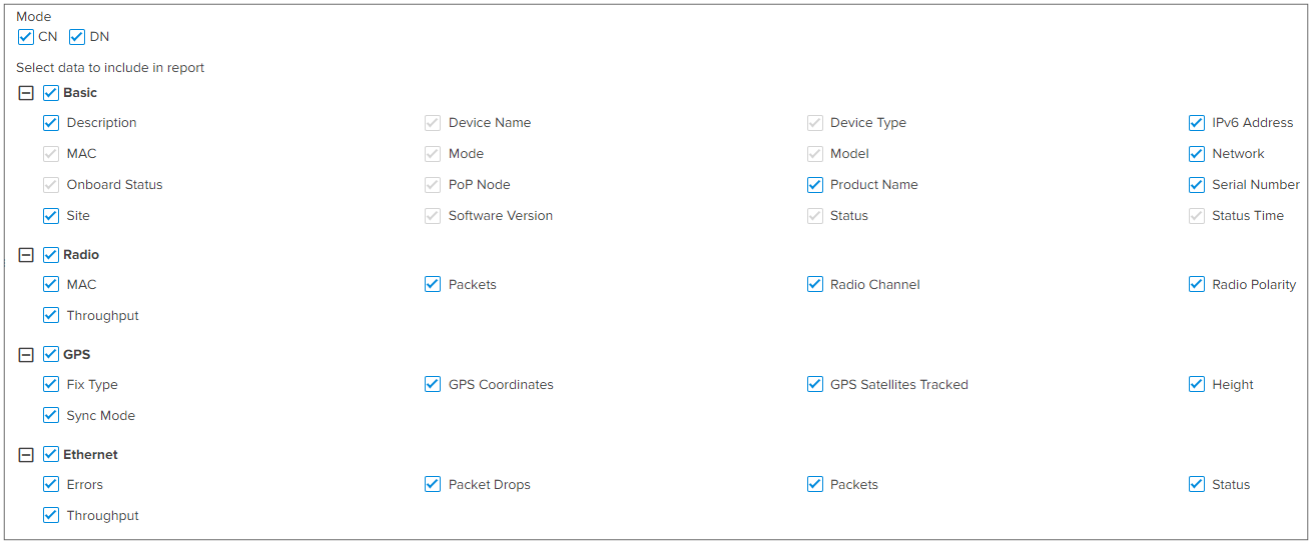
The device data parameters exported for the following devices are listed below:

- 60 GHz cnWave
- cnMatrix
- cnPilot Home (R-Series)
- cnRanger
- cnReach
- cnReach XIO
- cnVision
- cnWave 5G Fixed
- Enterprise Wi-Fi
- ePMP
- PMP
- PTP 650/670/700
- PTP 820/850
- RV22 Home Mesh

If 60 GHz cnWave device is selected as **Device Type**, then the following parameter sections are available:

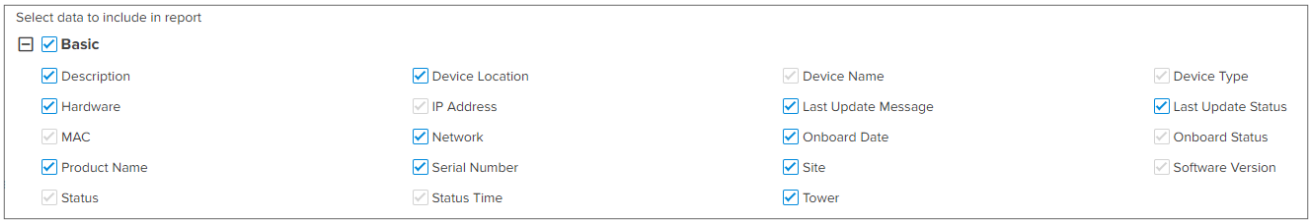
- Basic
- Ethernet
- GPS
- Mode (CN or DN)
- Radio

Figure 253 *Device Report: 60 GHz cnWave*



If cnMatrix is selected as the **Device Type**, then **Basic** data export parameters will be exported.

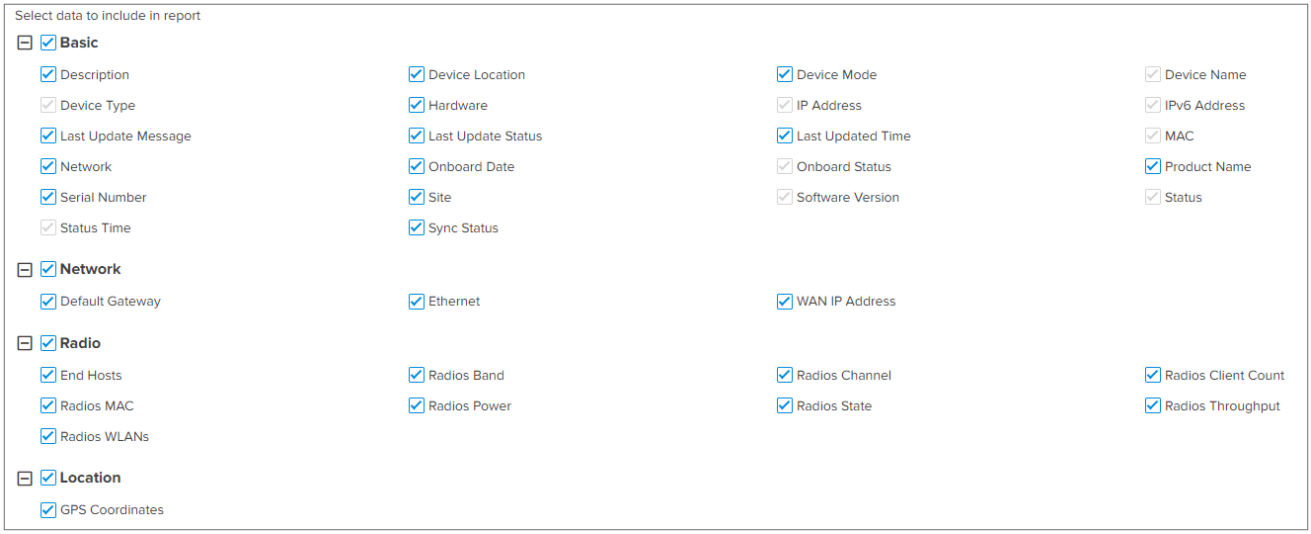
Figure 254 *Device Report: cnMatrix*



If cnPilot Home (R-Series) is selected as the **Device Type**, then the following parameter sections are available:

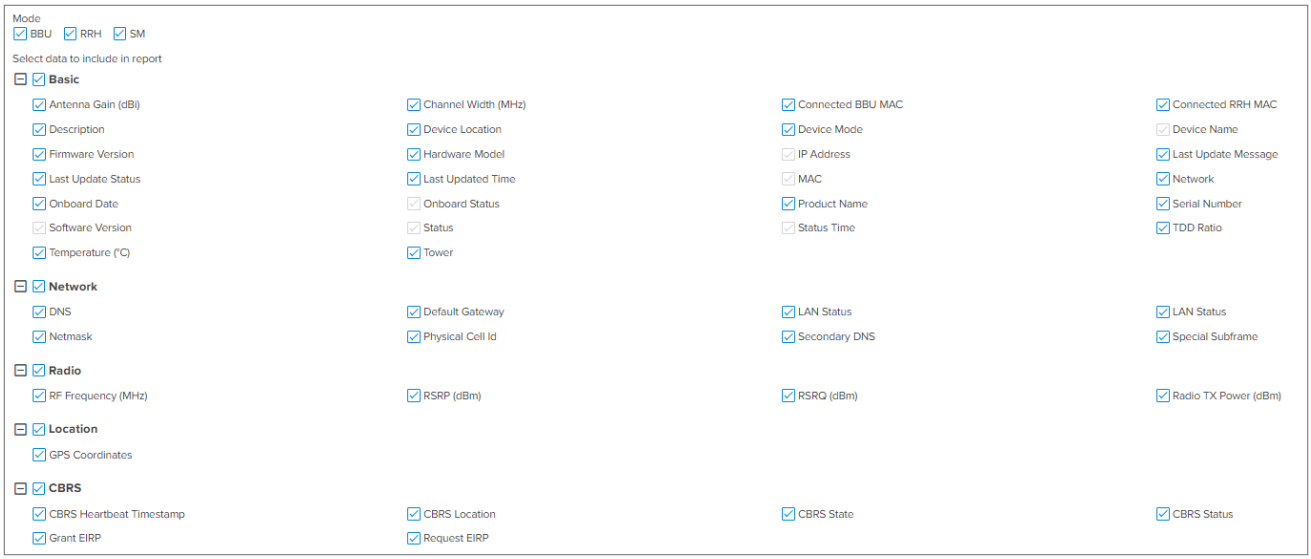
- Basic
- Location
- Network
- Radio

Figure 255 *Device Report: cnPilot Home (R-Series)*



If cnRanger is selected as the **Device Type**, then Basic, Network, Radio, Location, and CBRS parameter sections can be exported.

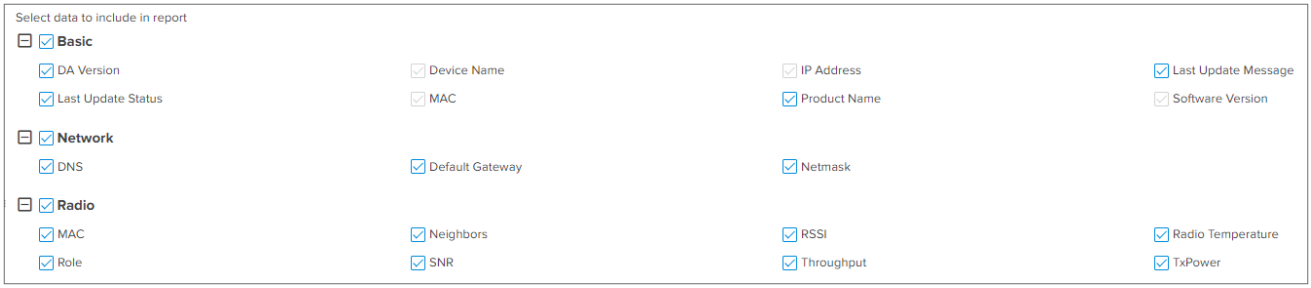
Figure 256 *Device Report: cnRanger*



If cnReach is selected as the **Device Type**, then the following sections are available:

- Basic
- Network
- Radio

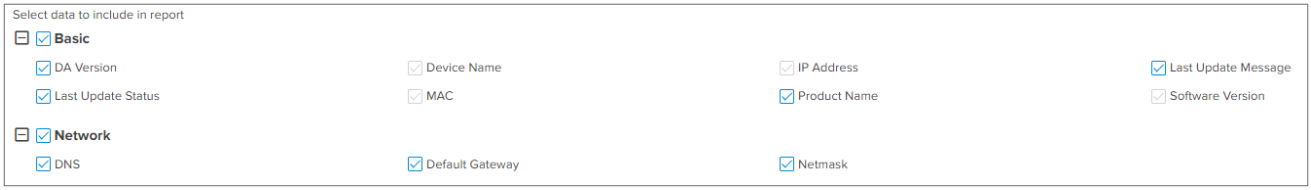
Figure 257 *Device Report: cnReach*



If cnReach XIO is selected as the **Device Type**, then the following sections are available:

- Basic
- Network
- Radio

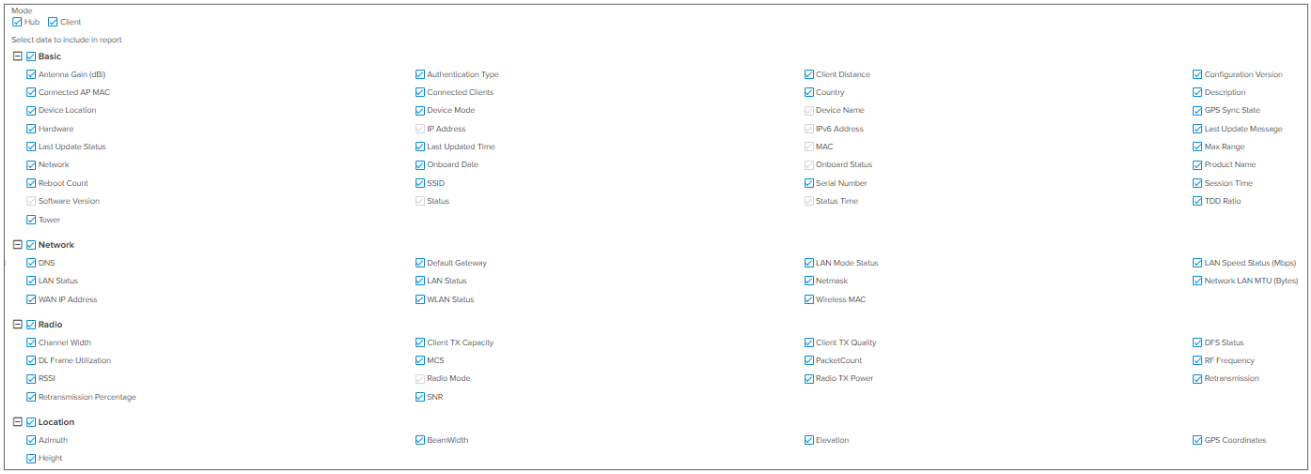
Figure 258 *Device Report: cnReach XIO*



If cnVision is selected as the **Device Type**, then the following sections are available:

- Basic
- Location
- Mode
- Network
- Radio

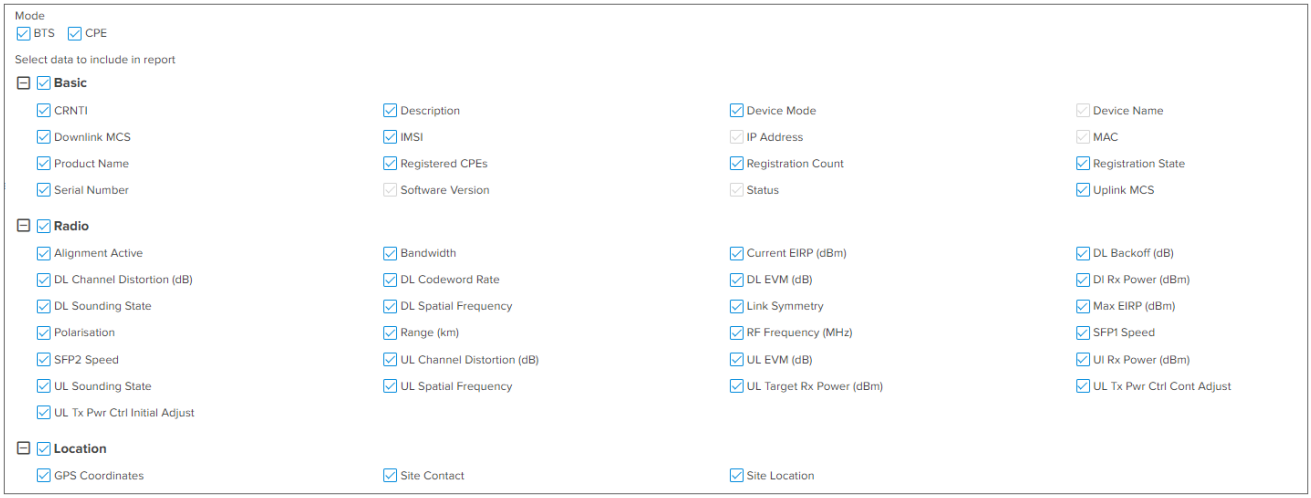
Figure 259 *Device Report: cnVision*



If cnWave 5G Fixed device is selected as **Device Type**, choose the type of **Mode** (BTS or CPE) then the following sections are available:

- Basic
- Location
- Radio

Figure 260 *Device Report: cnWave 5G Fixed*

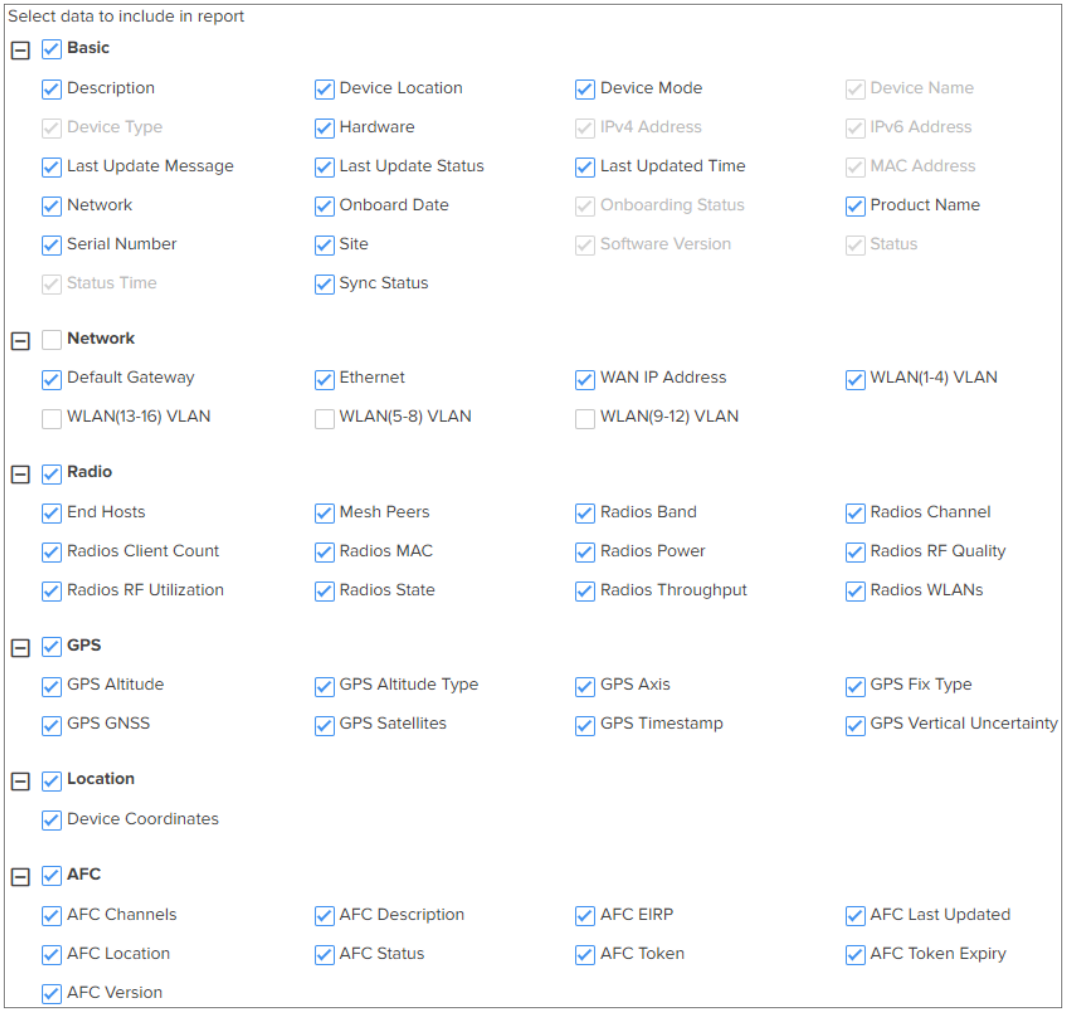


If Enterprise Wi-Fi is selected as the **Device Type**, then the following sections are available:

- Basic
- Location

- Network
- Radio

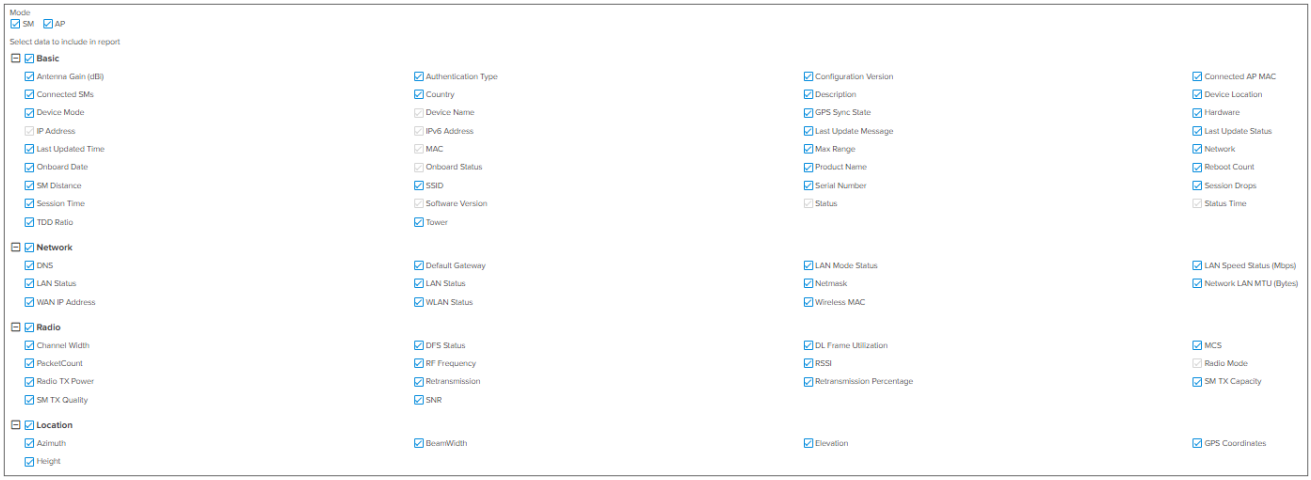
Figure 261 *Device Report: Enterprise(Wi-Fi)*



If ePMP is selected as the **Device Type** then the following sections are available:

- Basic
- Location
- Mode(s) (AP or SM)
- Network
- Radio

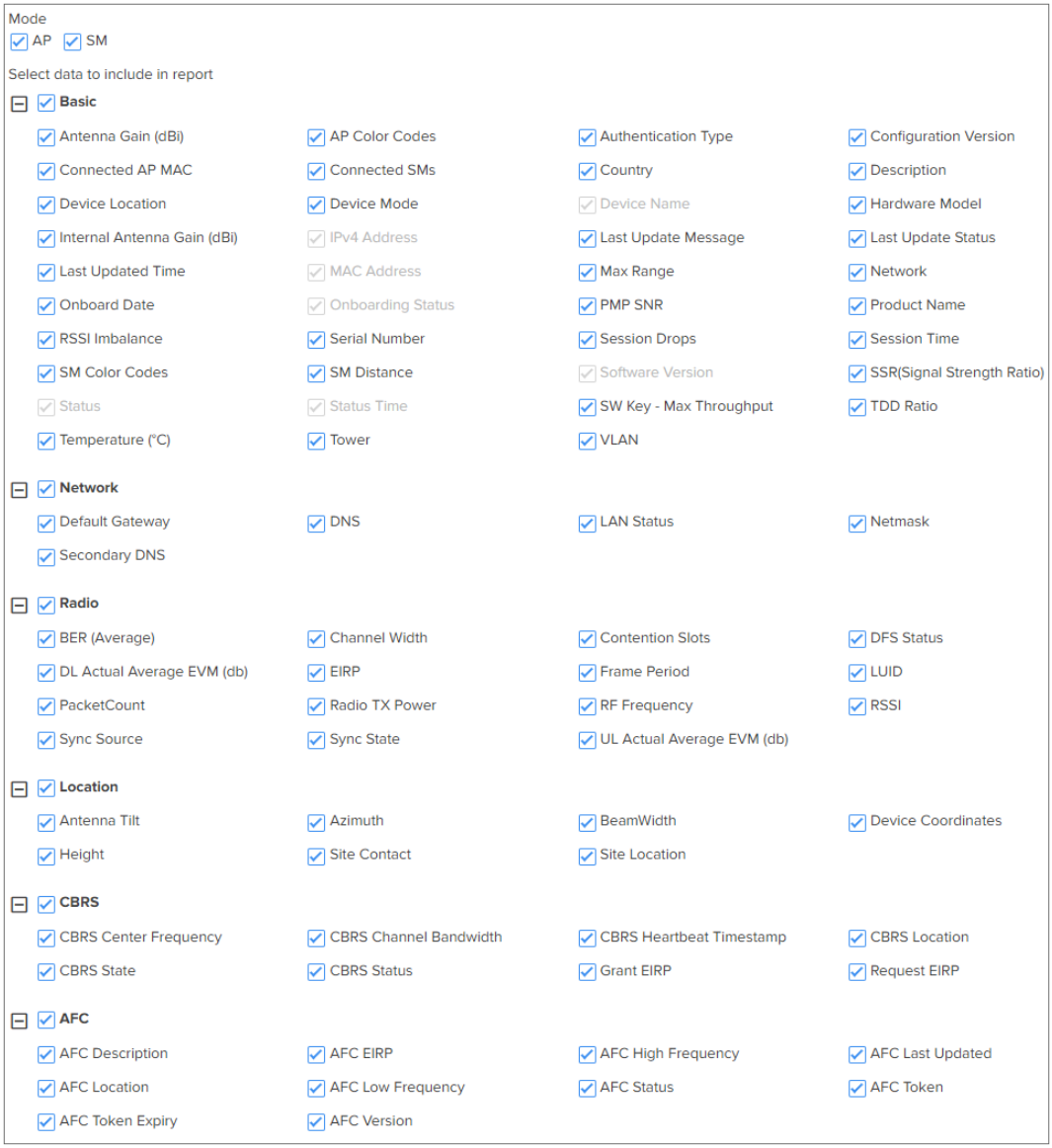
Figure 262 *Device Report: ePMP*



If PMP is selected as the **Device Type**, then the following sections are available:

- AFC
- Basic
- CBRS
- Location
- Mode(s) (AP or SM)
- Network
- Radio

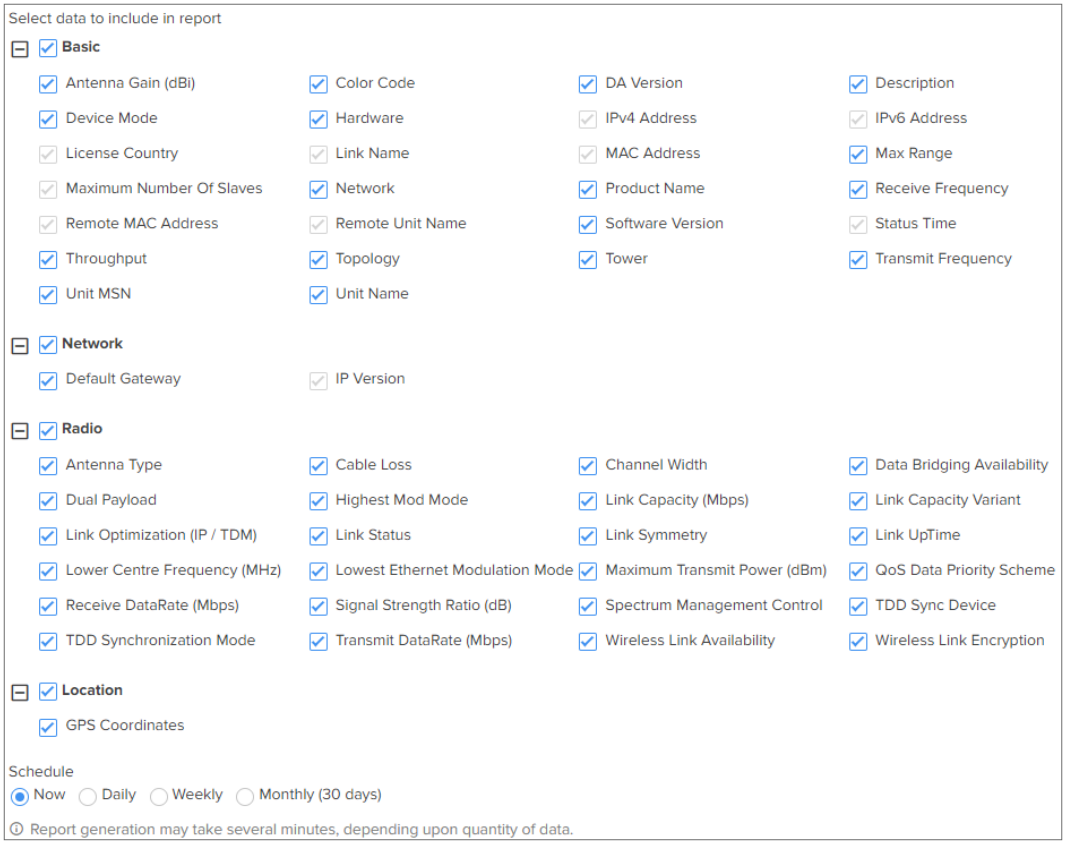
Figure 263 *Device Report: PMP*



If PTP 650/670/700 is selected as the **Device Type**, then the following sections are available:

- Basic
- Location
- Network
- Radio

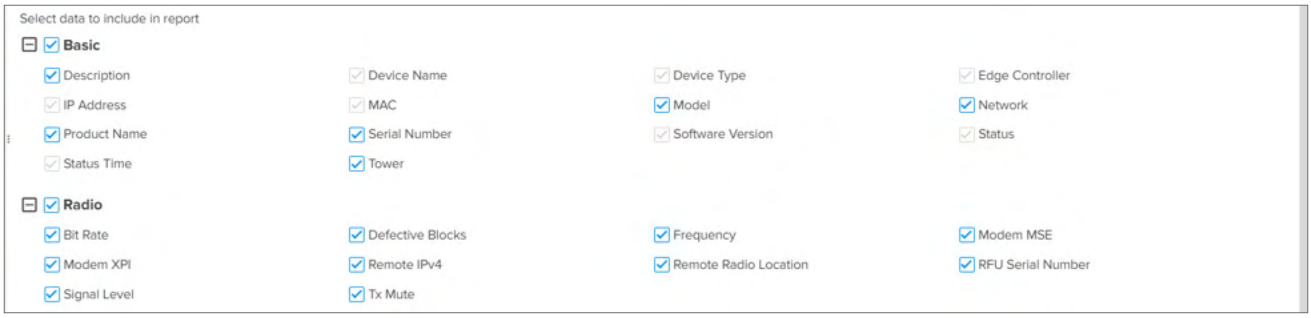
Figure 264 *Device Report: PTP 650/670/700*



If PTP 820/850 is selected as the **Device Type**, then the following sections are available:

- Basic
- Radio

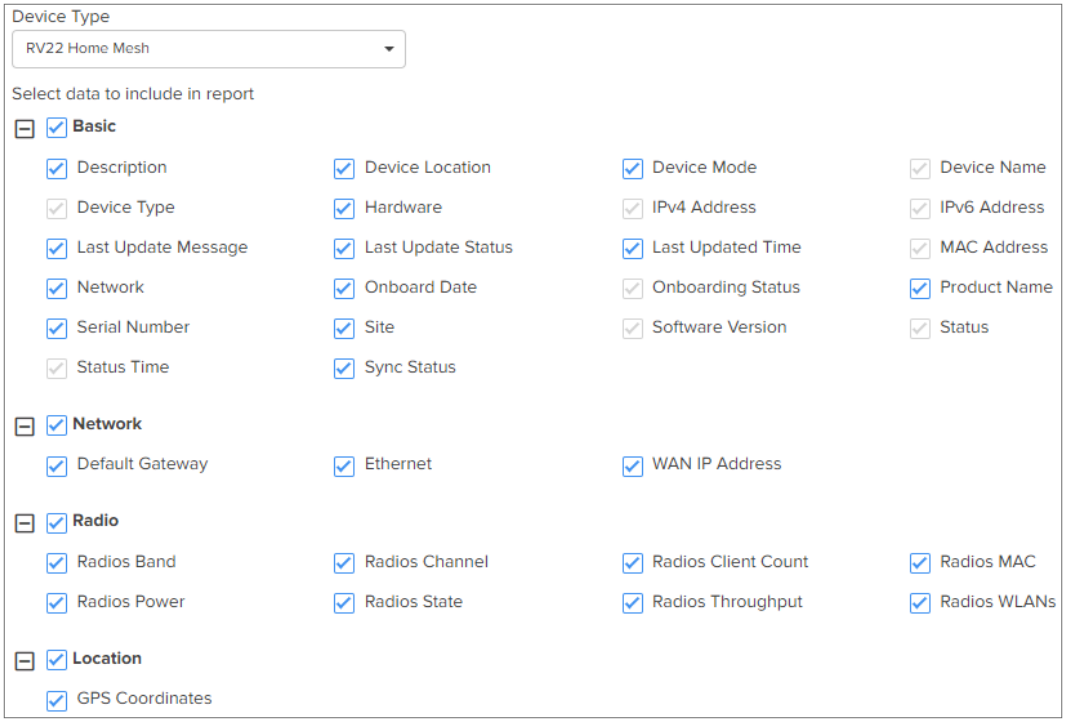
Figure 265 *Device Report: PTP 820/850*



The following sections are available for RV22 Home Mesh routers:

- Basic
- Location
- Network
- Radio

Figure 266 *Device Report: RV22 Home Mesh*



Note

Reports are available for each of the following hierarchical nodes in the tree:

- System
- Managed Account
- Network
- Tower
- Site
- AP Group

Performance Report

The Performance Report generates device time-series performance data as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export.

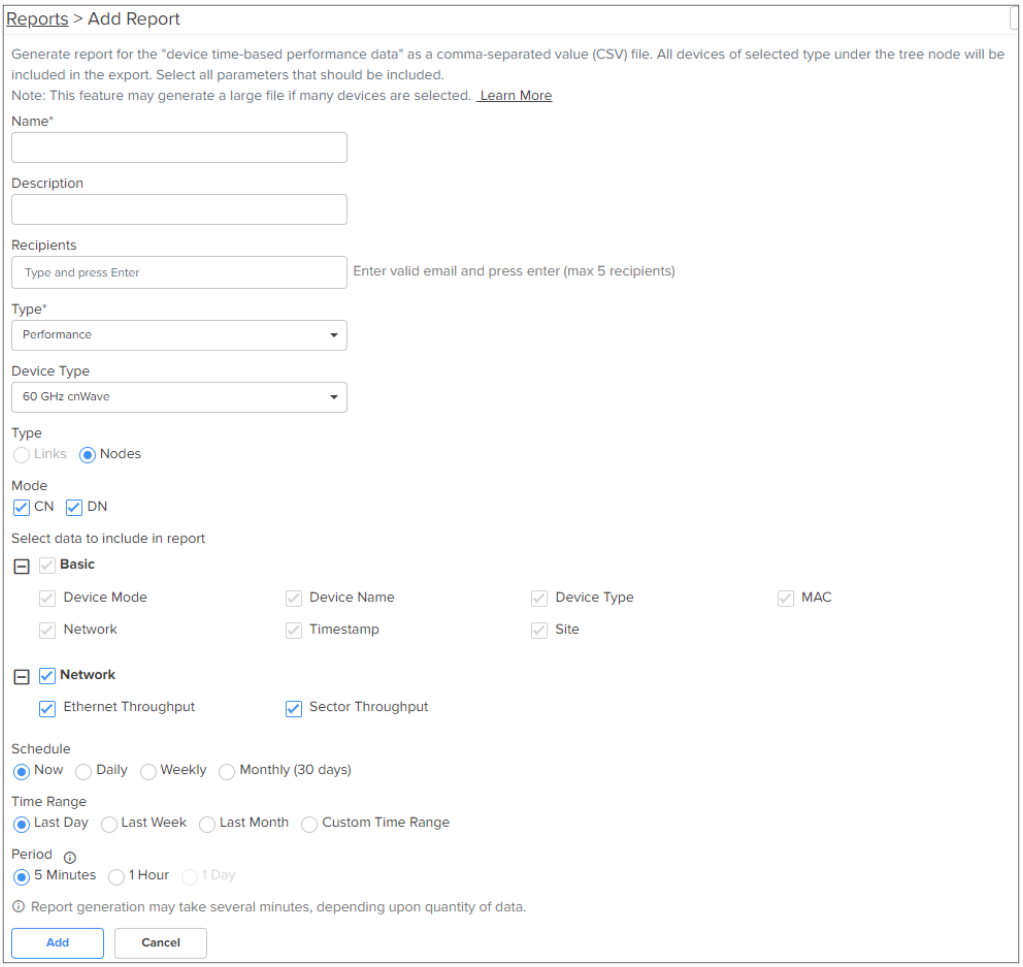
Note

- You must select the parameters.
- This feature may generate a large file if many devices are selected.

To generate Performance reports, perform the following steps:

1. Navigate to **Report X** > **Scheduled** tab.
2. Click **Add New Data Report**.
3. Enter a **Name** and **Description** for the report.
4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.

5. Select **Type** as **Performance**.
6. Select the **Device Type**.



7. Select the data parameters to include in the report.
8. Select the following options:
   - Schedule type (Now, Daily, Weekly, or Monthly)
   - Time Range (Last Day, Last Week, Last Month, Custom Time Range)
   - Period (5 Minutes, 1 Hour, or 1 Day)
9. Click **Add**. The report is added to the Scheduled Reports page.

60 GHz cnWave Performance Report

Figure 267 *Performance Report: 60 GHz cnWave (Links Type)*

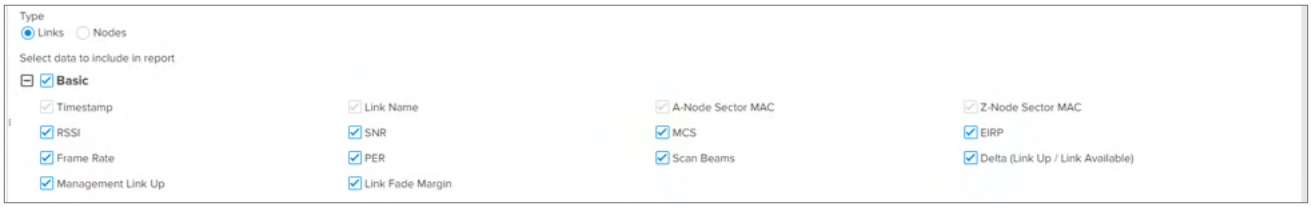
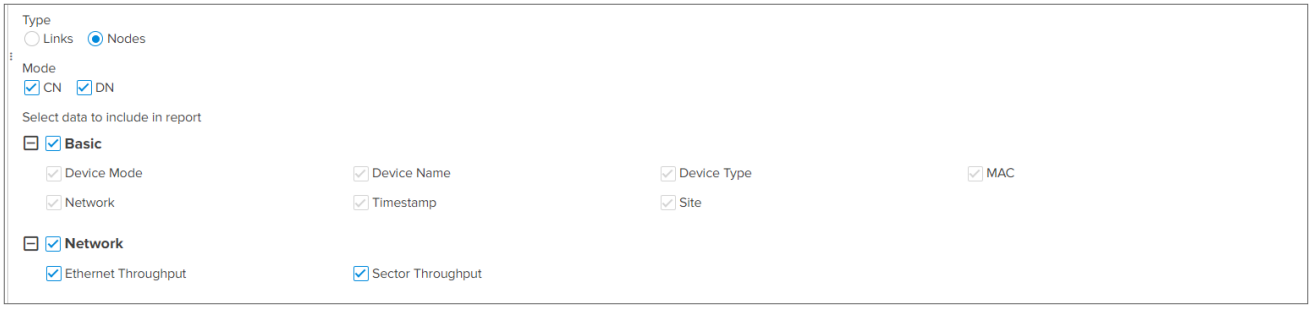


Figure 268 *Performance Report: 60 GHz cnWave (Node Type)*



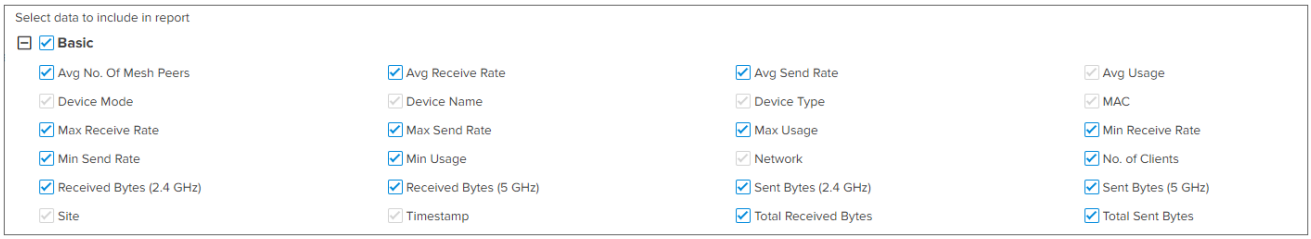
cnMatrix Performance Report

Figure 269 *Performance Report: cnMatrix*



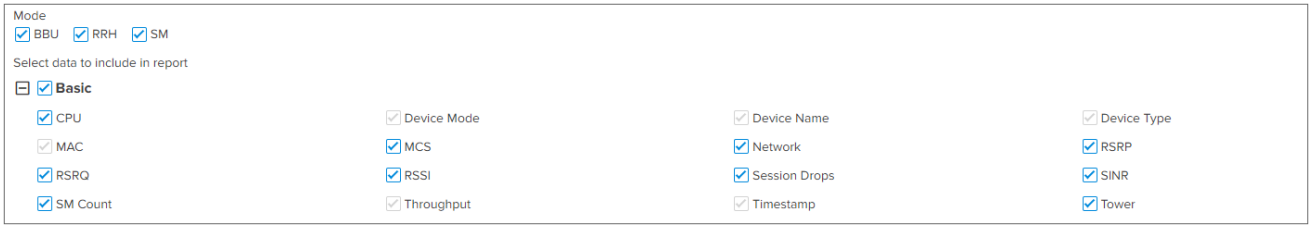
cnPilot Home (R-Series) Performance Report

Figure 270 *Performance Report: cnPilot Home (R-Series)*



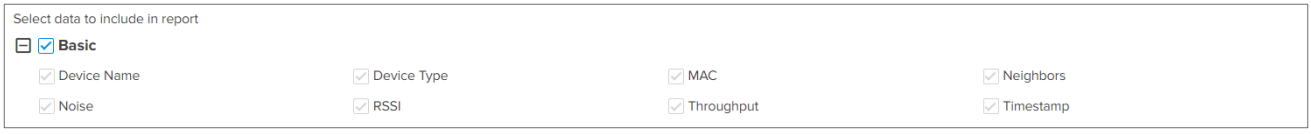
cnRanger Performance Report

Figure 271 *Performance Report: cnRanger*



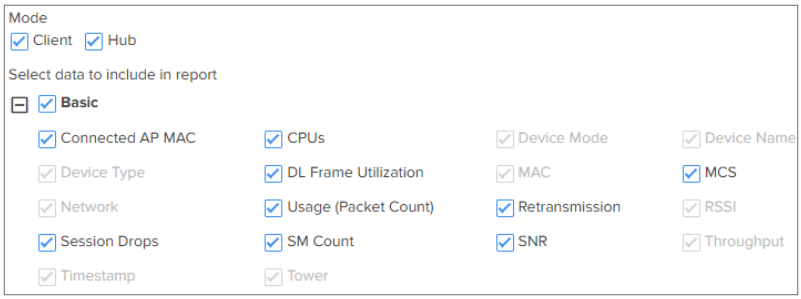
cnReach Performance Report

Figure 272 *Performance Report: cnReach*



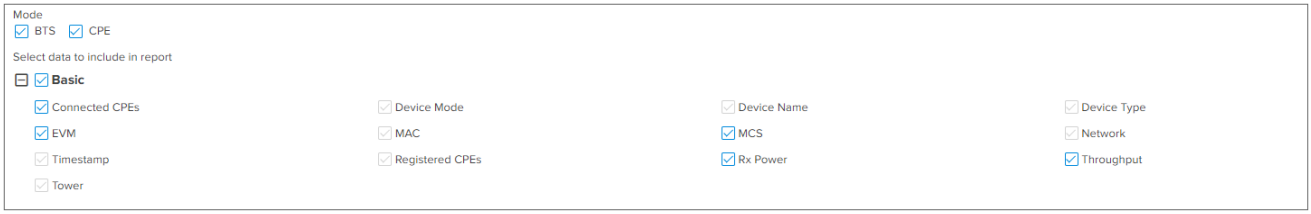
cnVision Performance Report

Figure 273 *Performance Report: cnVision*



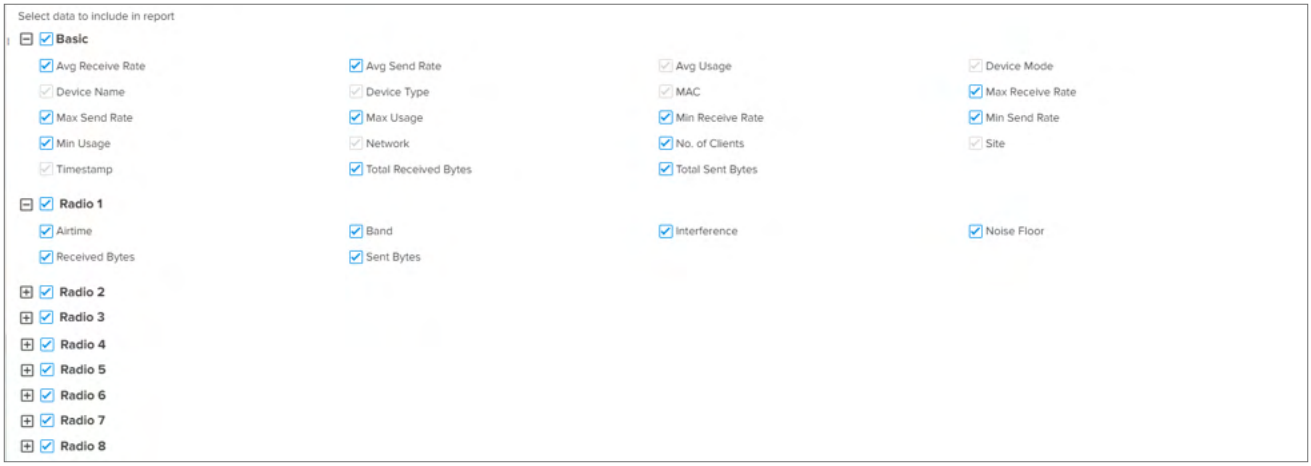
cnWave 5G Fixed Performance Report

Figure 274 *Performance Report: cnWave 5G Fixed*



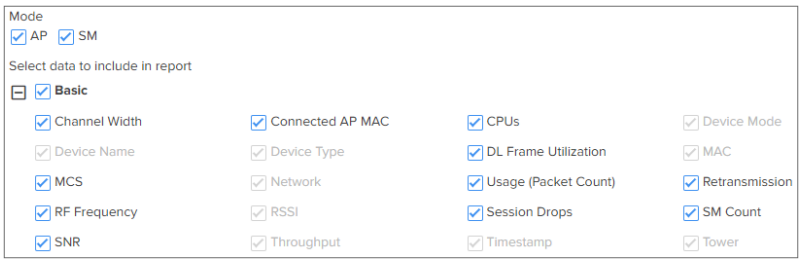
Enterprise Wi-Fi

Figure 275 *Performance Report: Enterprise Wi-Fi*



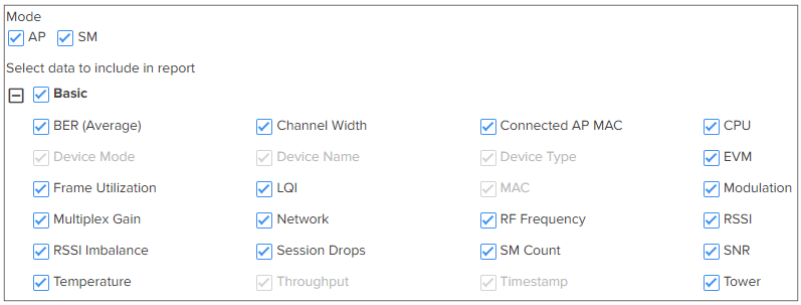
ePMP Performance Report

Figure 276 *Performance Report: ePMP*



PMP Performance Report

Figure 277 *Performance Report: PMP*



The modulation mappings for the PMP device are as follows:

Figure 278 *Mapping PMP*

Value	Description
-1	N/A
0	1X MIMO-A
1	2X MIMO-A
2	3X MIMO-A
3	4X MIMO-A
4	2X MIMO-B
5	3X MIMO-B
6	4X MIMO-B
7	5X MIMO-B
8	6X MIMO-B
9	7X MIMO-B
10	8X MIMO-B

Figure 279 *PMP 450m*

Value	Description
0	N/A
1	1X MIMO-A
2	2X MIMO-A
3	3X MIMO-A
4	4X MIMO-A

Figure 280 *PMP 450m*

Value	Description
0	N/A
2	2X MIMO-B
3	3X MIMO-B
4	4X MIMO-B

Value	Description
5	5X MIMO-B
6	6X MIMO-B
7	7X MIMO-B
8	8X MIMO-B

Figure 281 *PMP 430*

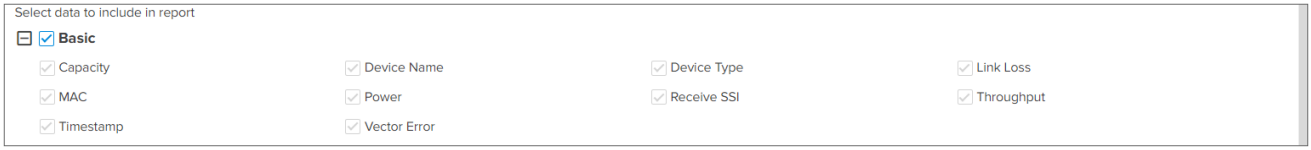
Value	Description
-1	N/A
0	1X SISO
1	2X SISO
2	3X SISO

Figure 282 *PMP 450v*

Value	Description
0	N/A
2	2X MIMO-B
3	3X MIMO-B
4	4X MIMO-B
5	5X MIMO-B
6	6X MIMO-B
7	7X MIMO-B
8	8X MIMO-B

PTP 650/670/700 Performance Report

Figure 283 *Performance Report: PTP 650/670/700*



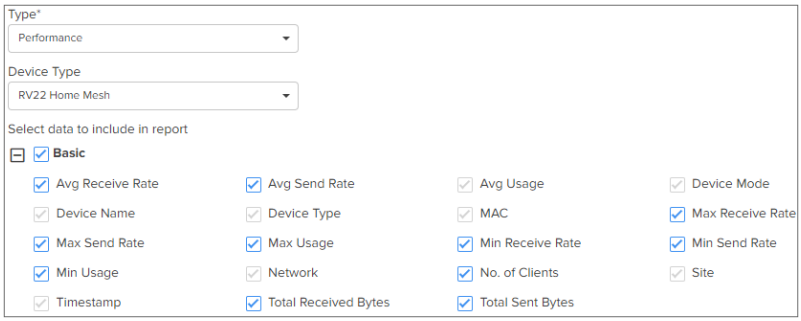
PTP 820/850 Performance Report

Figure 284 *Performance Report: PTP 820/850*



RV22 Home Mesh Performance Report

Figure 285 *Performance Report: RV22 Home Mesh*

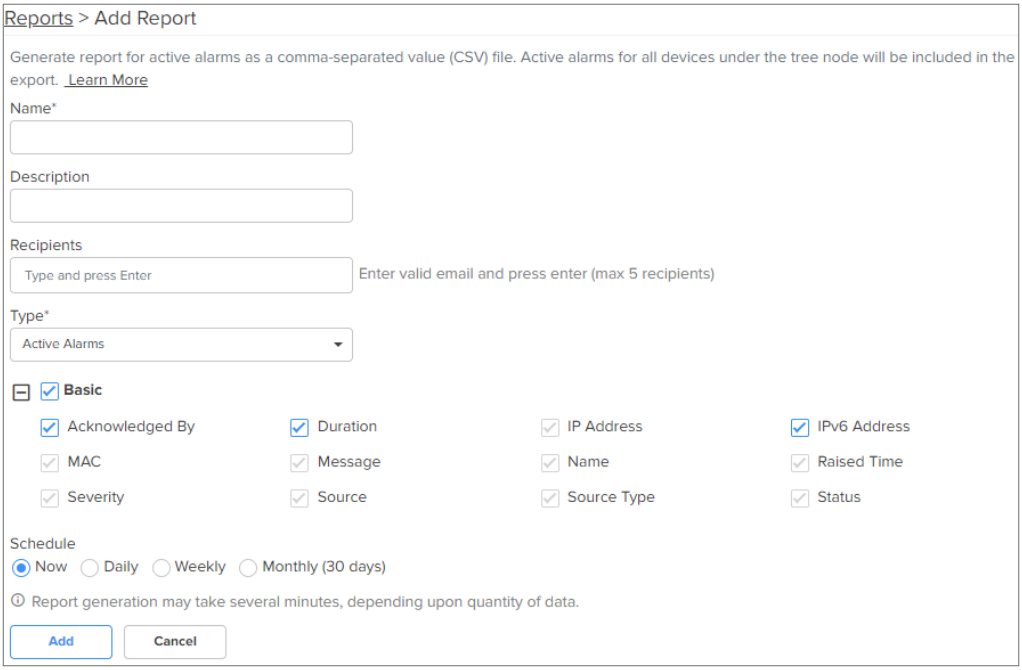


Active Alarms Report

The Active Alarms Report will export the data for the active alarms at the report generation time. Active alarms for all devices under the tree node will be included in the export.

To generate the Active Alarms reports, perform the following steps:

1. Navigate to **Reports** > **Scheduled** tab.
2. Enter a **Name** and **Description** for the report.
3. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
4. Select the **Report Type** as *Active Alarms*.
5. Select data parameters to include in the report.
6. Select the following options:
   - Schedule type (Now, Daily, Weekly, or Monthly)
7. Click **Add**. The report gets added to the Scheduled Reports page.

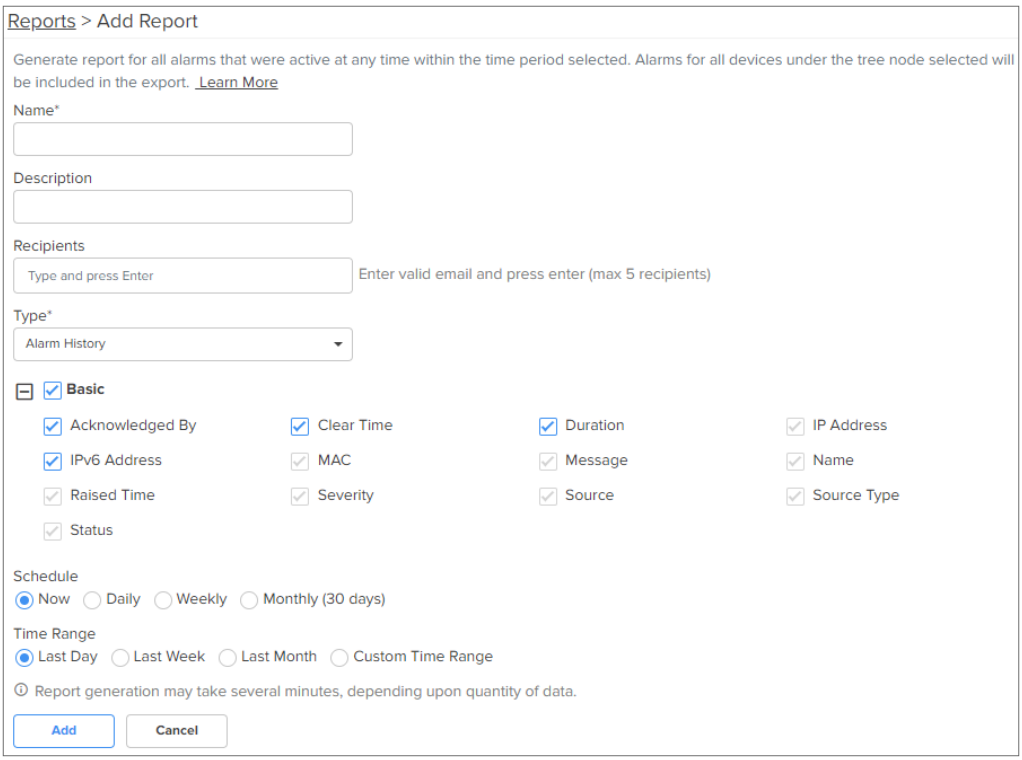


Alarm History Report

The Alarm History Report will generate data for all alarms that were active at any time within the time period. Alarms for all devices under the tree node selected will be included.

To generate the Alarms History reports, perform the following steps:

1. Navigate to **Reports** > **Scheduled** tab.
2. Enter a **Name** and **Description** for the report.
3. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
4. Select the **Report Type** as Alarms History.
5. Select data parameters to include in the report.
6. Select the following options:
   - Schedule type (Now, Daily, Weekly, or Monthly)
   - Time Range (Last Day, Last Week, Last Month, Custom Time Range)
7. Click **Add** . The report gets added to the **Scheduled Reports** page.
8. Click **View Jobs** to view the reports.



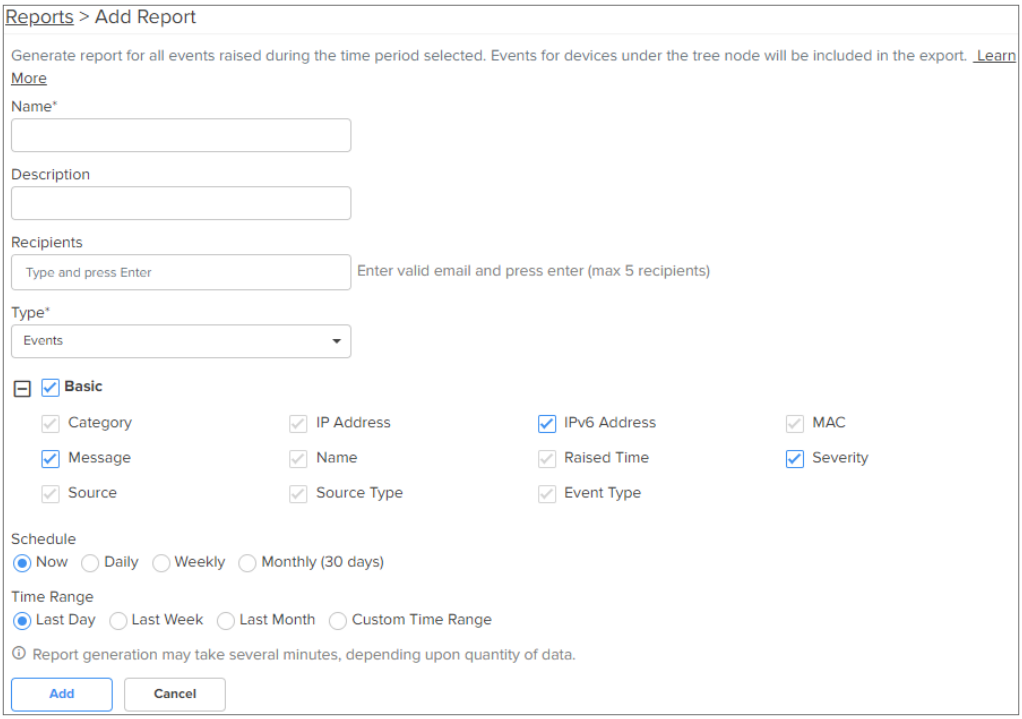
Events Report

The Events Report is generated for the events raised during the time period. Events for devices under the tree node will be included in the export.

To generate the Events reports, perform the following steps:

1. Navigate to **Reports** > **Scheduled** tab.
2. Enter a **Name** and **Description** for the report.
3. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.

4. Select the **Report Type** as Events.
5. Select data parameters to include in the report.
6. Select the following options:
    - Schedule type (Now, Daily, Weekly, or Monthly)
    - Time Range (Last Day, Last Week, Last Month, Custom Time Range)
7. Click **Add**. The report gets added to the **Scheduled Reports** page.



Clients Report

The clients report generates data for Wi-Fi clients.

Note

Client Data is available for the last day, last 24 hours, and last week.

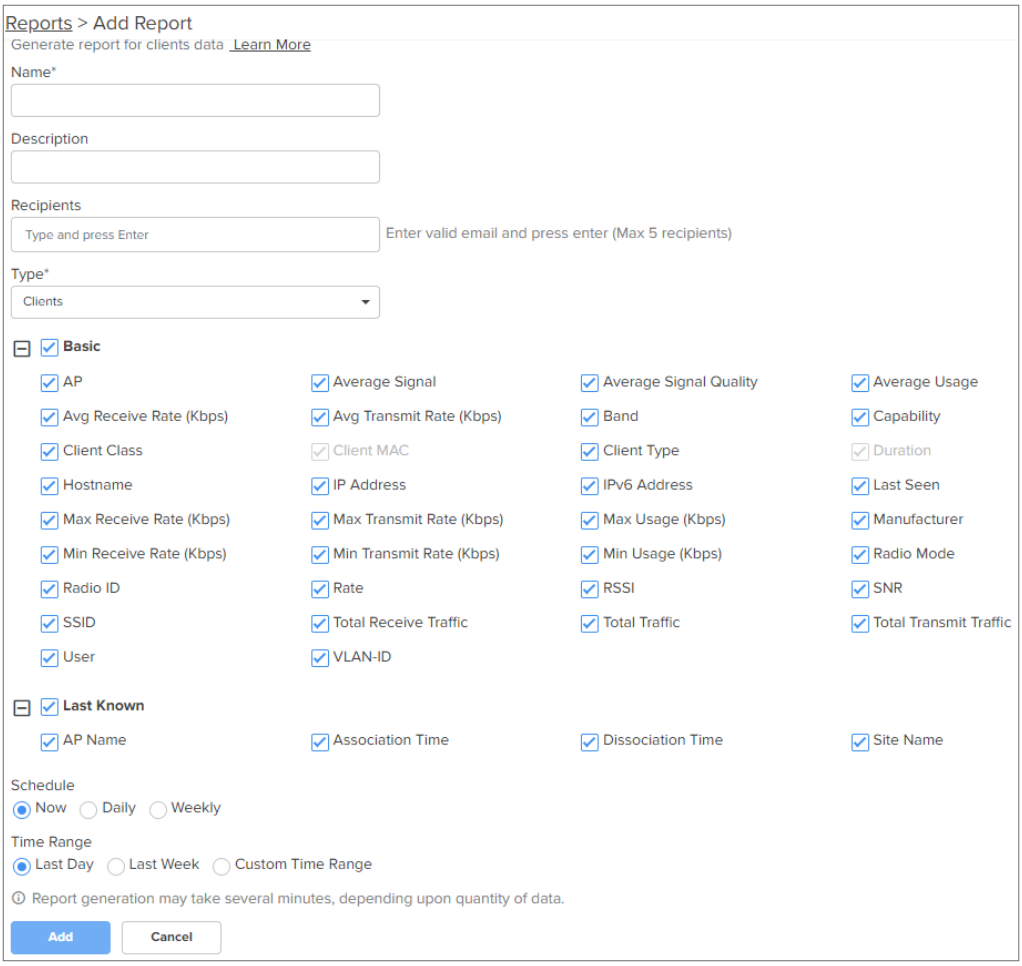
To generate the clients reports, perform the following steps:

1. Navigate to **Reports** > **Scheduled** tab.
2. Click **Add New Data Report**.

   The Add Report page appears.
3. Enter a **Name** and **Description** for the report.
4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
5. Select the **Report Type** as Clients.
6. Select data parameters to include in the report.
7. Select the following options:
    - Schedule type (Now, Daily, or Weekly)
    - Time Range (Last Day, Last Week. or Custom Range)

8. Click **Add**. The report is saved and listed in the **Scheduled Reports** page.

Figure 286 *Clients Report*



Guest Access Login Events

The Guest Access Login Events represent Wi-Fi Guest Access Logins.

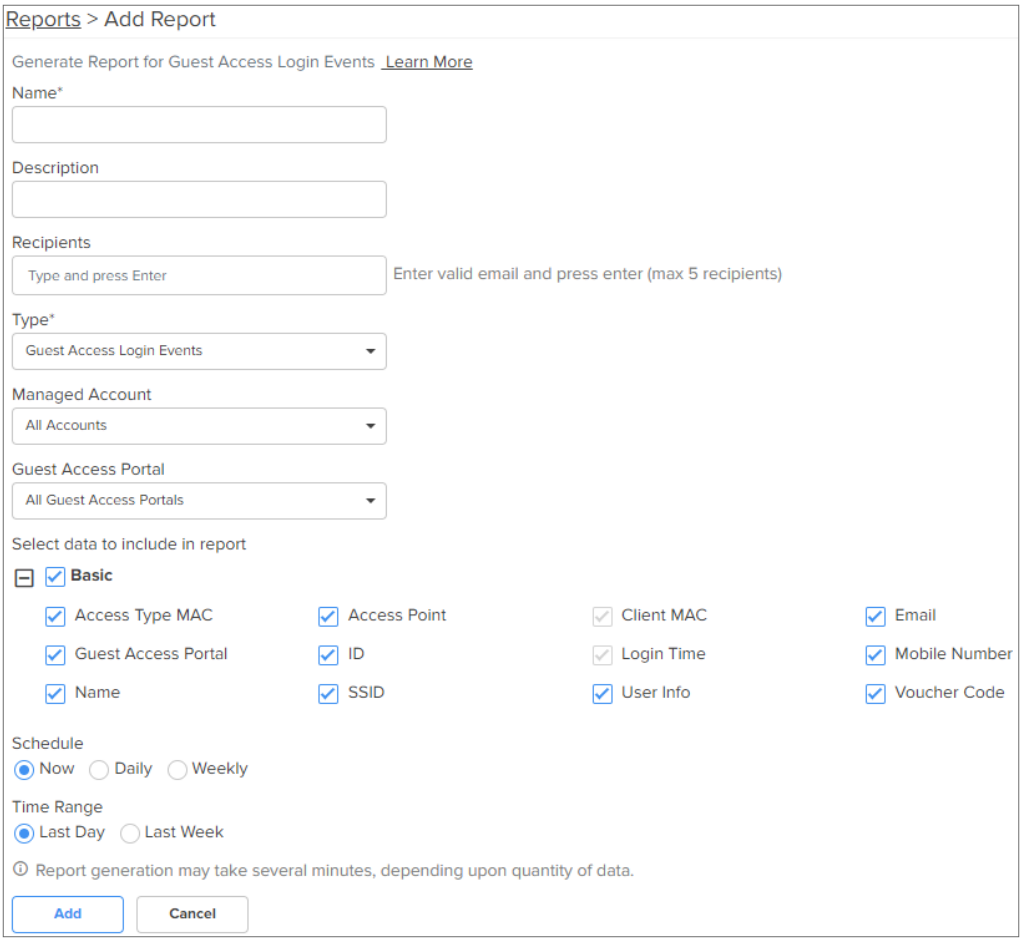
> **Note**
>
> Guest access report can be generated only at system level.

To generate the Guest Access Login Events report, perform the following steps:

1. Navigate to **Report X** > **Scheduled** tab.
2. Enter a **Name** and **Description** for the report.
3. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
4. Select the **Report Type** as Guest Access Login Events.
5. Select the **Managed Account**, if applicable.
6. Select the **Guest Access Portal**, if applicable.
7. Select data parameters to include in the report.
8. Select the following options:

- Schedule type (Now, Daily, or Weekly)
- Time Range (Last Day, Last Week).

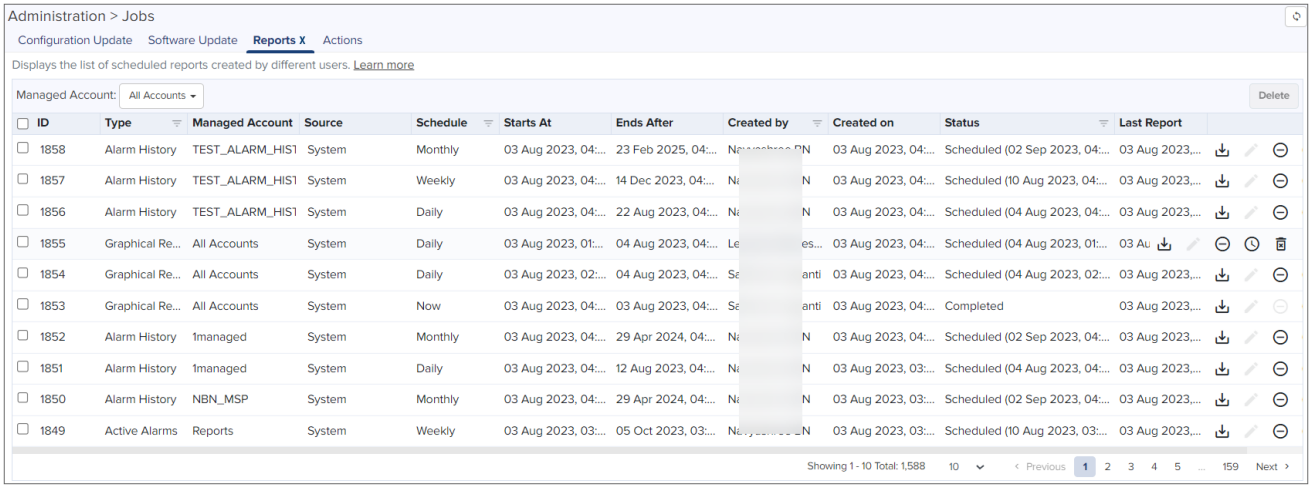
9. Click **Add**. The report gets added to the **Scheduled Reports** page.



Report Jobs

The report jobs displays the list of scheduled jobs created by different users. To view jobs, navigate to **Administration** > **Jobs** > **Reports**.

Figure 287 *Report Jobs*



A scheduled report job displays the following **Action** buttons:

- **Edit**: Visible only for **Active Jobs** which have not yet run. You can reschedule a job with this option.
- **Terminate**: Stop the **Active Jobs**.
- **Show History**: Display the detailed status of the generated reports and the file transfer status.
- **Delete**: Delete **Active** and **Completed Jobs**.
- **Instant Download**: Download the latest report without checking the **Show History**.

Graphical Reports

The data reports contain a lot of data that need to be represented graphically so that you can quickly summarize and get a better visualization. In such cases, you can use the Graphical Reports. Graphical Reports can be created by first building a template of the report you want to view, optionally with your own branding such as your logo and brand name. Then, apply the template at a level in the hierarchical tree in cnMaestro such managed service, system, or site. Each graphical report can consist of multiple pages called widgets. The following widgets are available with applicable type of graphs and charts based on context. Each widget has both a graphical and tabular representation of the data. The output is a PDF file.

Figure 288 lists the Graphical Reports widgets available in cnMaestro and the version they were introduced in.

Figure 288 *List of Graphical Reports widgets available*

Name of Widget	Version Introduced
Analytics	
Analytics: Top APs Reporting Client Disconnections—Top APs reporting client disconnections	4.1.0
Analytics: Top Client Connection Failures—Top client connection failure types by number of failures	4.1.0
Applications	
Top Access Points by Traffic Usage—Top APs by traffic usage	5.1.0
Clients	
6E Clients by Radio—Comparison between 6E Clients on 6 GHz radios and other radios	4.1.0
Client Capability Trend—Count of clients based on their Wi-Fi capabilities over time	4.1.0
Client Count by Band—Client count by band	4.1.0
Client Count by Manufacturers—Top manufacturers by number of clients	4.1.0
Client Count over Time—Connected clients by band over time	4.1.0
Client Traffic over Time—Client uplink and downlink speeds over time	4.1.0
Peak and Unique Clients—Total unique clients and peak time number of unique clients	4.1.0
Top Applications by Usage—Top applications by data usage	4.1.0
Top Access Points by Unique Clients—Top APs by unique clients	4.1.0
Top Category by Usage—Top applications category by data usage	4.1.0
Client Count by OS—Top client types by number of clients	5.1.0
Top Application Category by Client Count—Top application category by number of unique clients	5.1.0
Top Applications by Client Count—Top applications by number of clients	5.1.0
Top Client Types by Traffic Usage—Top client types by traffic usage	5.1.0

Name of Widget	Version Introduced
Top Sites by Client Count—Top sites by number of clients	5.1.0
Top Sites by Traffic Usage—Top sites by traffic usage	5.1.0
Top SSIDs by Client Count—Top SSIDs by number of clients	5.1.0
Top SSIDs by Traffic Usage—Top SSIDs by traffic usage	5.1.0
Top Clients by Traffic Usage—Top clients by traffic usage	5.1.0
Top Managed Accounts by Traffic Usage—Top managed accounts by traffic usage	5.1.0

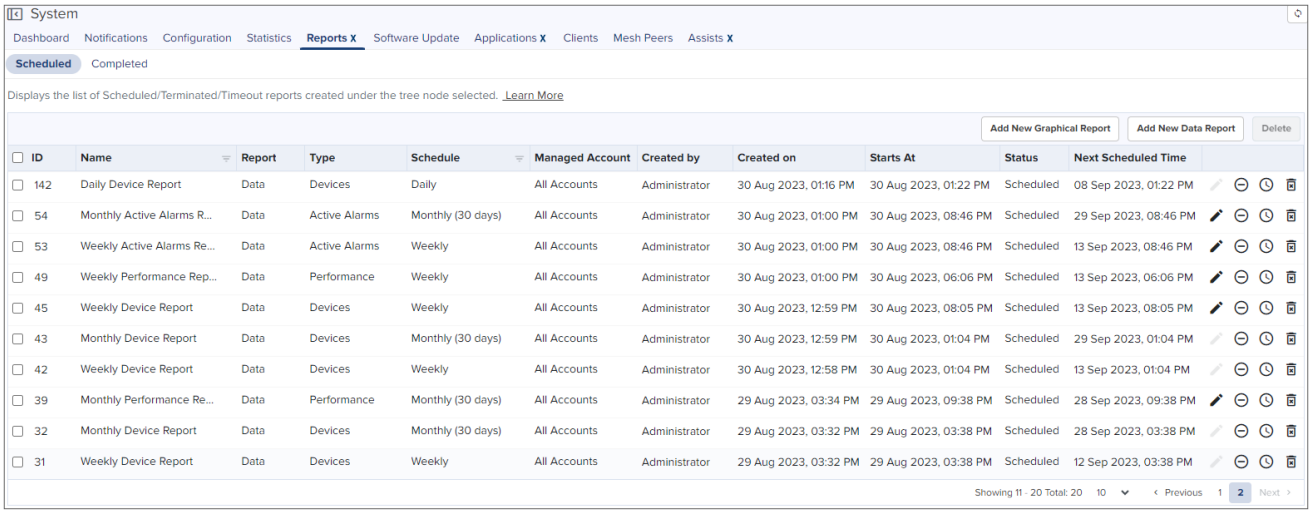
The standard process for graphical report generation includes the following:

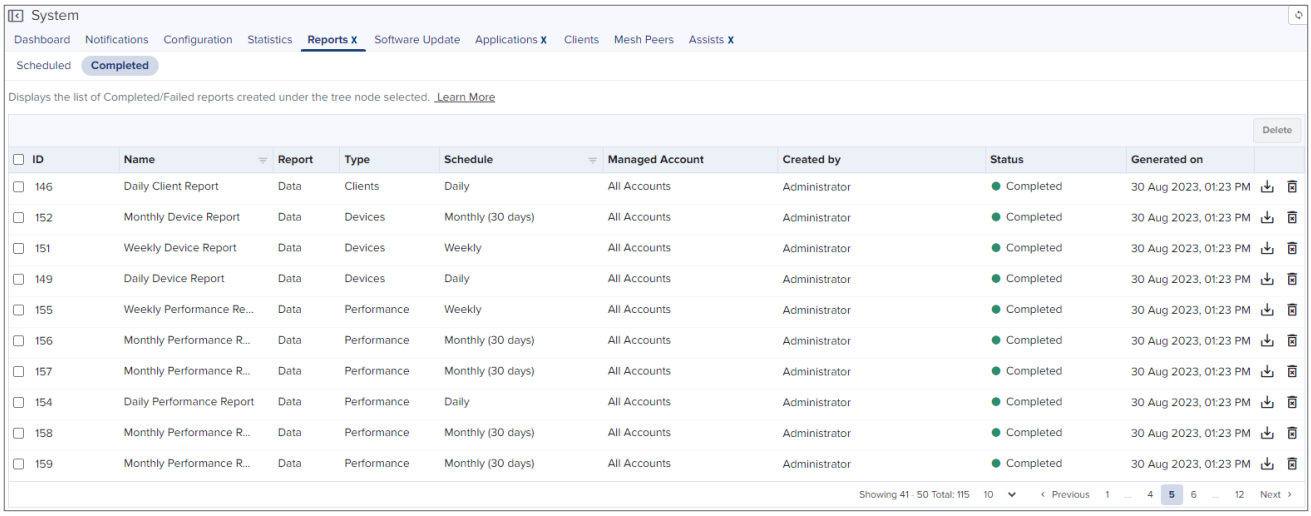
1. Create a template using the widgets listed above.
2. Select a level of the hierarchy on which to apply the template.
3. Schedule the report to either execute one-time or periodically.

Note

- Graphical reports are only supported for Wi-Fi APs and clients, and they can only be applied at the Managed Service, System, and Site levels.
- If there is no data for the specific period, then a blank page is displayed in the PDF.
- The title page of the PDF displays the date and time zone of the user who scheduled the report.

The **Scheduled** tab presents reports pending execution, and the **Completed** tab provides access to reports that have finished running. The already generated reports are listed as **Completed Reports** (includes Success and Failed status in the status column) and those that are not yet generated but scheduled for a future time are listed as **Scheduled reports** (includes and Future and Terminated status in the status column).





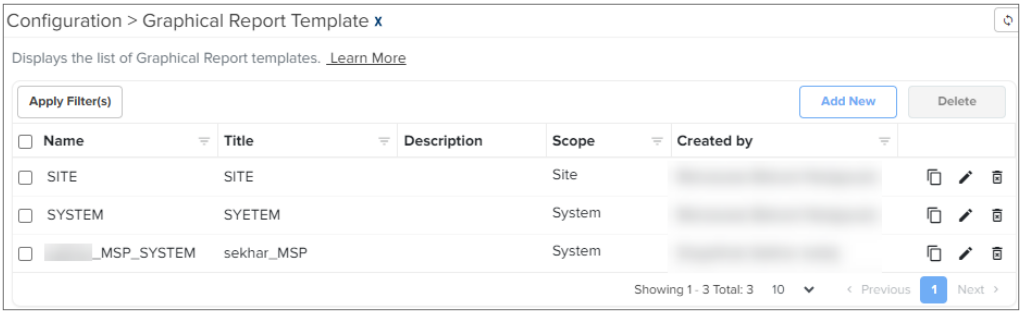
Refer to the following topics to create templates and schedule reports:

- Create Graphical Report Templates
- Generate Reports Based on Templates

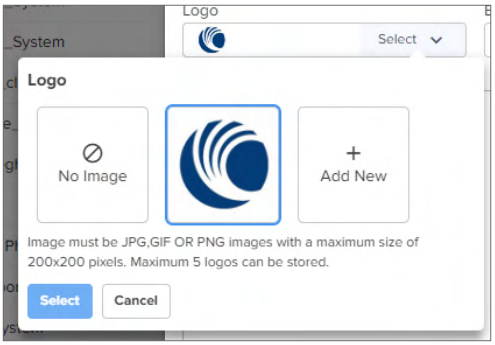
Create Graphical Report Templates

To create a graphical report template, complete the following steps:

1. Navigate to **Configuration** > **Graphical Report Template X** page.



2. Click **Add New** and complete the following details:
   - **Name**—Enter a meaningful name for the template.
   - **Scope**—Select the scope of the report such as **System**or **Site** from the drop-down list.
   - **Title**—Enter the title that you want to see in the Title page of the generated PDF document.
   - **Description**—Optionally, describe the report in details.
3. Optionally, brand the report as per your requirement.
   - **Logo**—To select an existing logo, click the down arrow and then click **Select**. You can also add a new logo by clicking **Add New**.



- **Brand Image**—To select an existing brand image, click the down arrow, and then click **Select**. You can also add a new brand image by clicking **Add New**.
- **Themes**—Select a theme for the title page of the report as either **Vertical Lines**, **Brand Box**, or **Plain**.

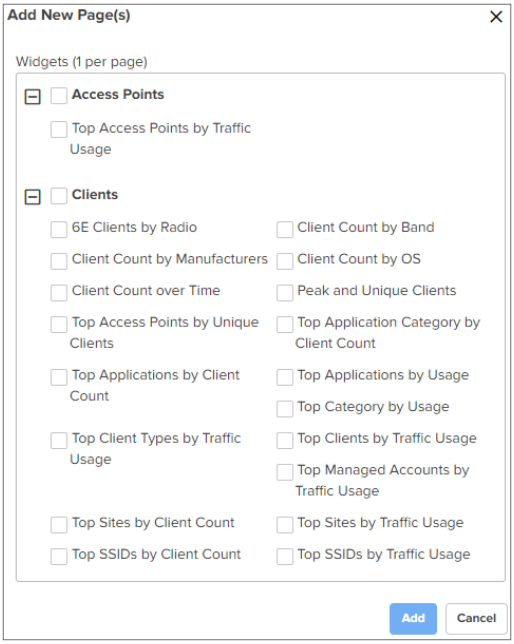


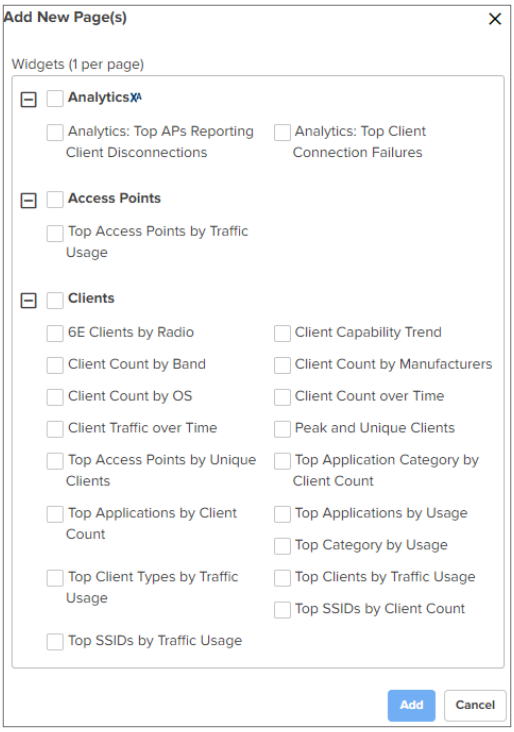
- **Theme Color**—Select the Theme Color by clicking the desired colored square.

4. Click **Add**.

   The report template design page is displayed. You can add one or more widgets to the report, one per page.

5. Click **Add New** in the left pane. The following widgets are available:

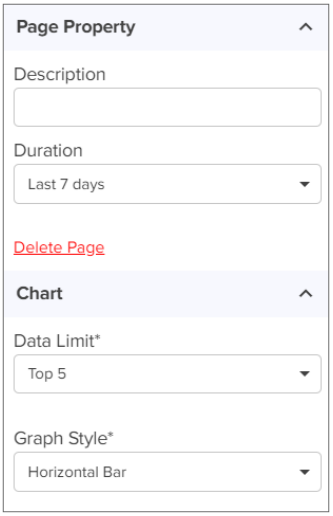




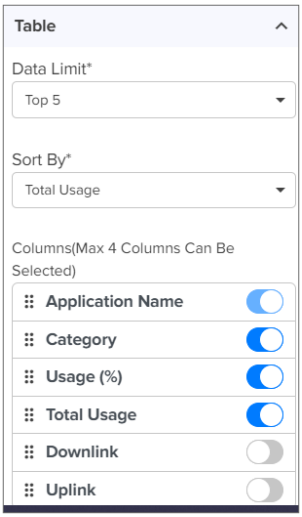
6. Select the check-box for one or more Widgets and click **Add**. Each page can have only one widget. The pages can be rearranged by drag and drop in the left pane.



7. For each page, select the page properties in the right pane. They differ based on widget and options that you have chosen.



8. You can also select the Table columns for each page.



The following options are available based on the page type:

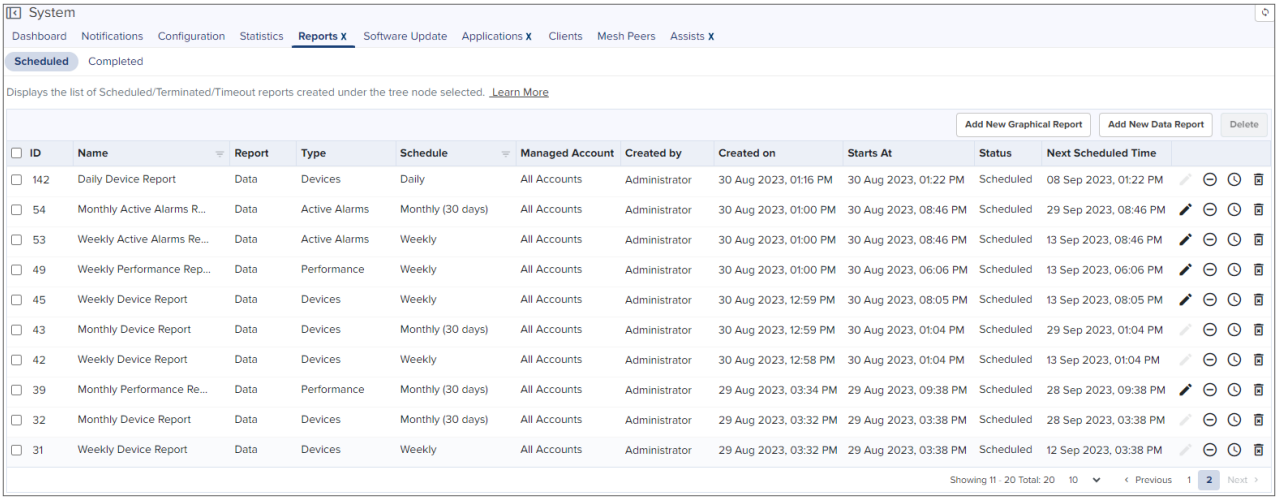
- **Title**—Title for the report.
- **Description**—Detailed information about the report criteria.
- **Duration**— Time interval. For example, **Last Day** or **Last 7 Days**.
- **Chart/Graph Style**— Type of graph. For example, **Horizontal Bar** or **Pie Chart**
- **Data Limit**—Volume of data to be filtered. For example, **Top 5** or **Top 10**.
- **Sort By**—Column name in the tabular format. For example, **Count**, or **Total Usage**.

9. Click **Save**.

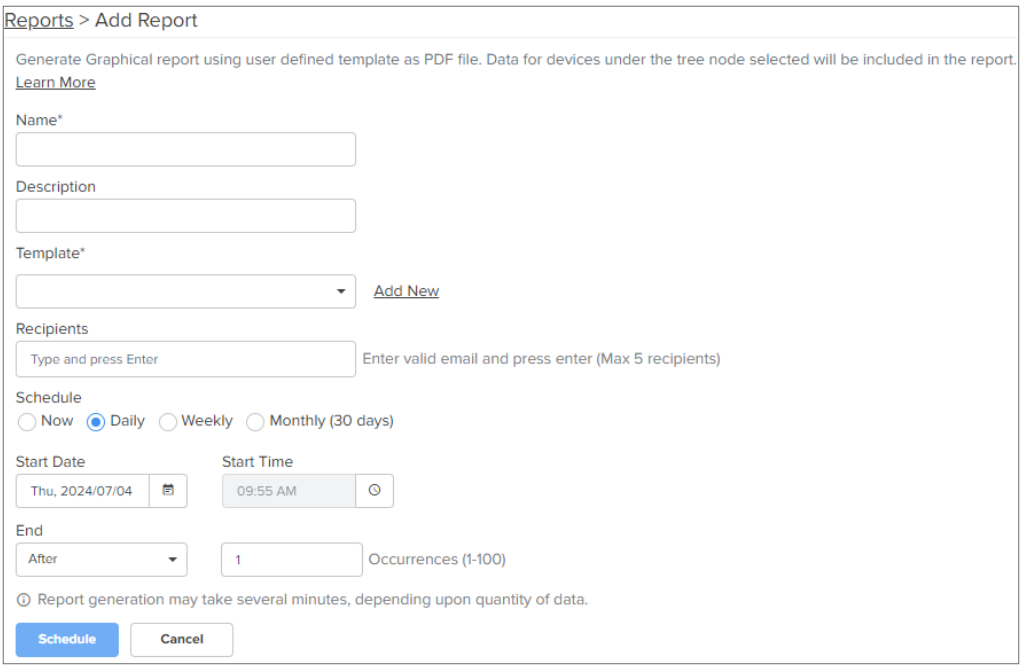
Generate Reports Based on Templates

To add a new report, follow the steps below:

1. Navigate to **Monitor and Manage** > **System** or **Site** > **Reports X** > **Scheduled** tab.



2. Click **Add New Graphical Report**.



3. Complete the following details:
   - **Name**—Enter a name for the report.
   - **Description**—Enter a detailed description for the report.
   - **Template**—Select the PDF template from the drop-down list. If there is no template listed, click **Add New** to create a new PDF template.
   - **Recipients**—Add email addresses of the recipients or requesters to whom the report is applicable.
   - **Schedule**—Select a schedule to generate the report from the following options:
     - **Now**—Generate the report immediately after you click **Add**.
     - **Daily**—Generate the report at the following interval:

        - **Start Date**—Select the date.
        - **Start Time**—Select the time.
        - **End**—Stop generating this report:
            - **After**—Enter the number of instances. The maximum is 100 instances.
            - **By**—Select the date when the report generations should be completely stopped.
    - **Weekly**—Generates the report at the following interval.
    - **Monthly**—Generates the report at the following interval.
4. Click **Schedule**. Adds the report to the list of Scheduled Reports.

Provisioning

The Provisioning chapter includes both Device Software Update and Configuration. It includes the following topics:

- Software Update
- Fixed Wireless Configuration
- Wireless LAN Configuration
- Switch Groups Configuration
- 60 GHz cnWave Configuration
- NSE 3000 Configuration
- Configuring Advanced Features

Software Update

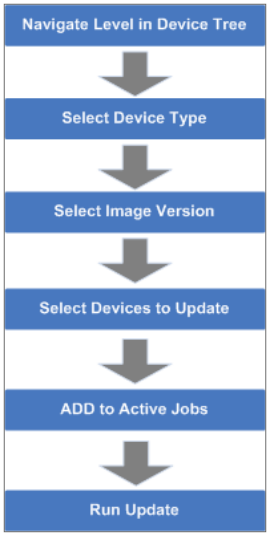
The **Software Update** tab displays the device update details. This section includes the following:

- Software Update Overview
- Create Software Update Job
- Software Update Jobs and Parameters
- Viewing Running Jobs in header

Software Update Overview

The Software Update feature allows users to deploy the latest software images to devices. Software updates can be started at any level in the Device Tree. Updates are created as Jobs and placed into the Jobs Queue. When the update is ready to run, it can be started. The process flow of Software Update is shown below:

Figure 289 *Software Update Overview*



When a Job completes, it is placed in the completed Jobs table. Jobs are available for one week before they are deleted.

Create Software Update Job

Device Selection

Navigate the Device Tree to an appropriate level for the devices to be updated. For example, selecting a Fixed Wireless AP will filter the devices to include the AP and its children.

Device Type

Software Updates are executed on one type of device at a time.

Software Update Dashboard

Once the device type is chosen, the UI displays the most recent software release version for that device type. It also displays a breakdown of the different software versions currently installed on the devices.

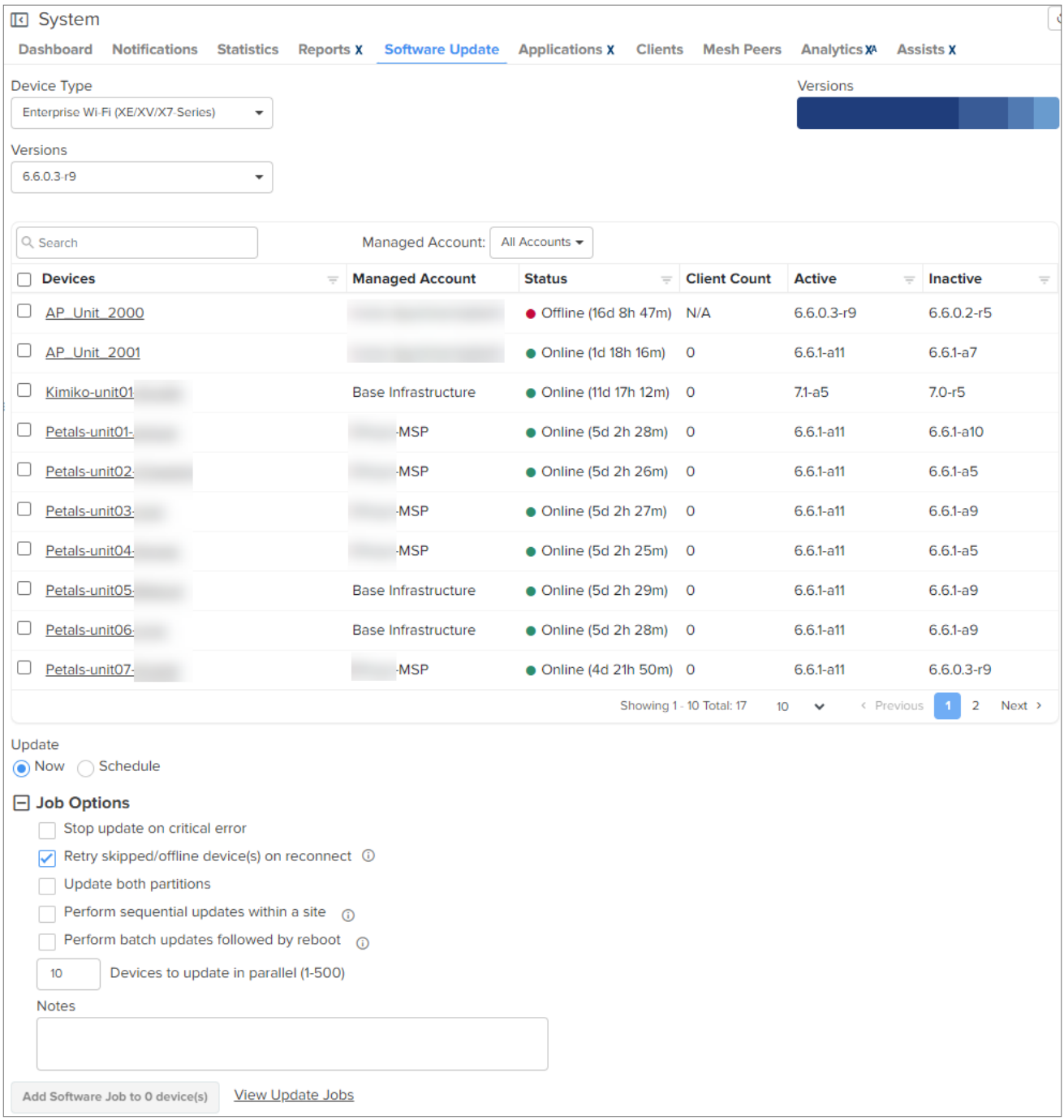


Note

Enterprise Wi-Fi shown below contains device types on the **Software Update** page:

- Enterprise Wi-Fi (E-Series)
- Enterprise Wi-Fi (XE/XV/X7-Series)
- Enterprise Wi-Fi (Xirrus-Series)

Figure 290 *Software Update: Enterprise Wi-Fi*



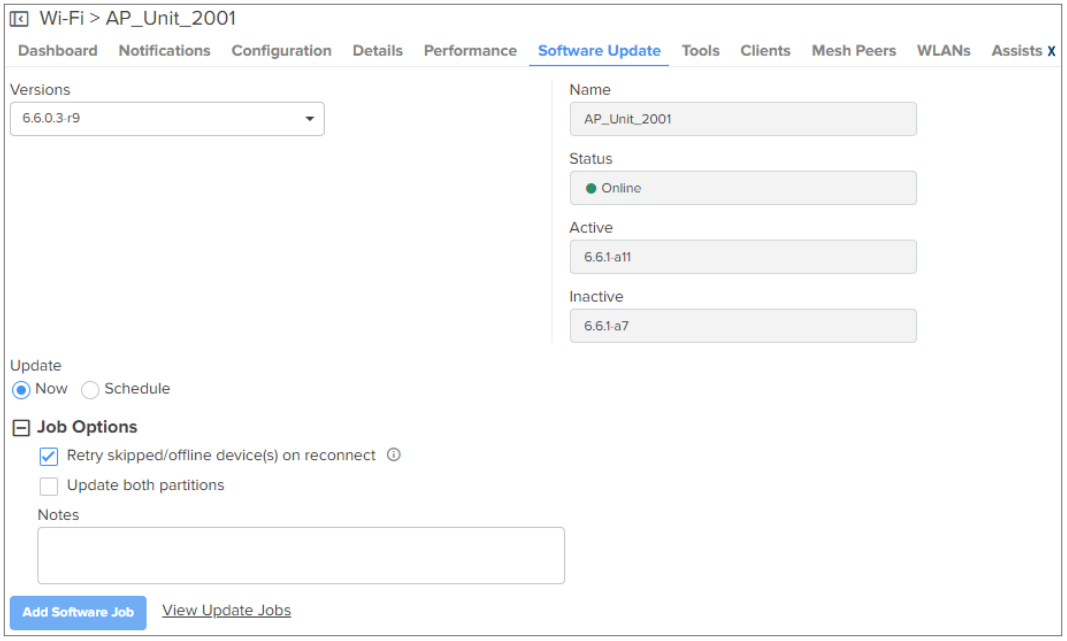
Note

- **Update both partitions** option is available at System/Network/Site/Device levels. It is only available for the devices that support it.
- **Perform sequential updates within a site** option is available at System/Network/Site level except the Device level.

If the **Update both partition** option is enabled/ disabled, the device level of the Software Update will be displayed as follows:

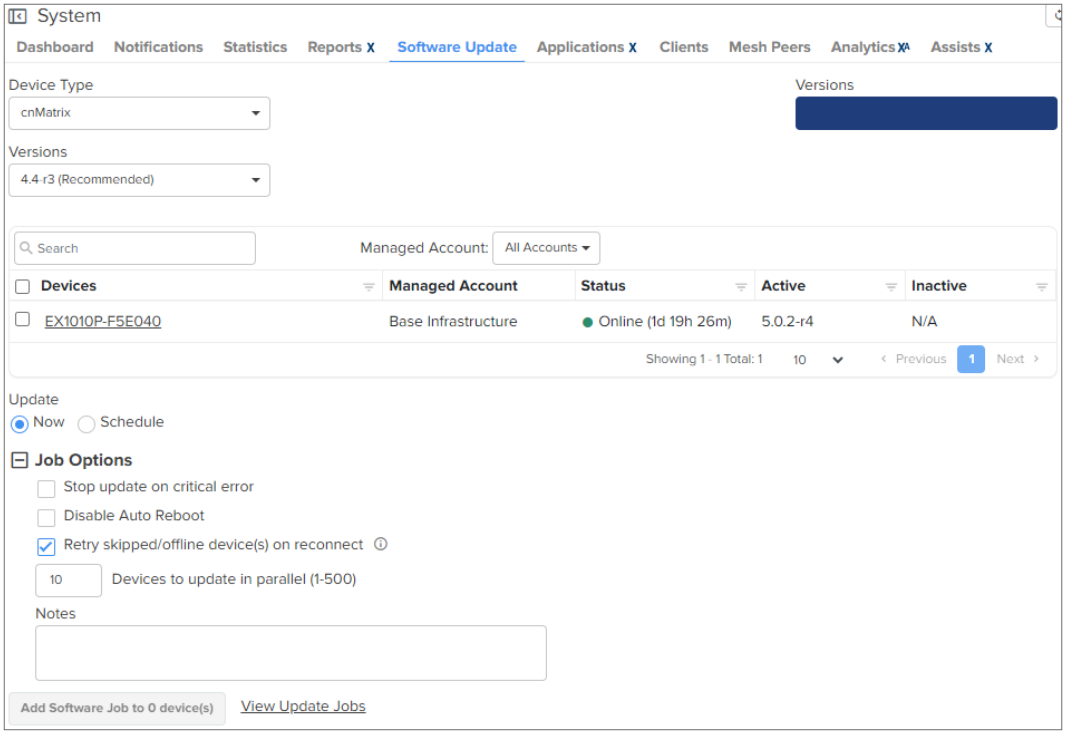
- **Enable**: Tp
- selected target image will be upgraded in only active portion of the device.

Figure 291 *Software Update: Device level*



If **Perform sequential updates within a site** is enabled, the image upgrade will happen only on one device at a time.

Figure 292 *Software Update: cnMatrix*



Disable Auto Reboot option disables reboot after applying the new software image. The user must manually reboot the device to complete the software update.

Figure 293 *Software Update: cnRanger*

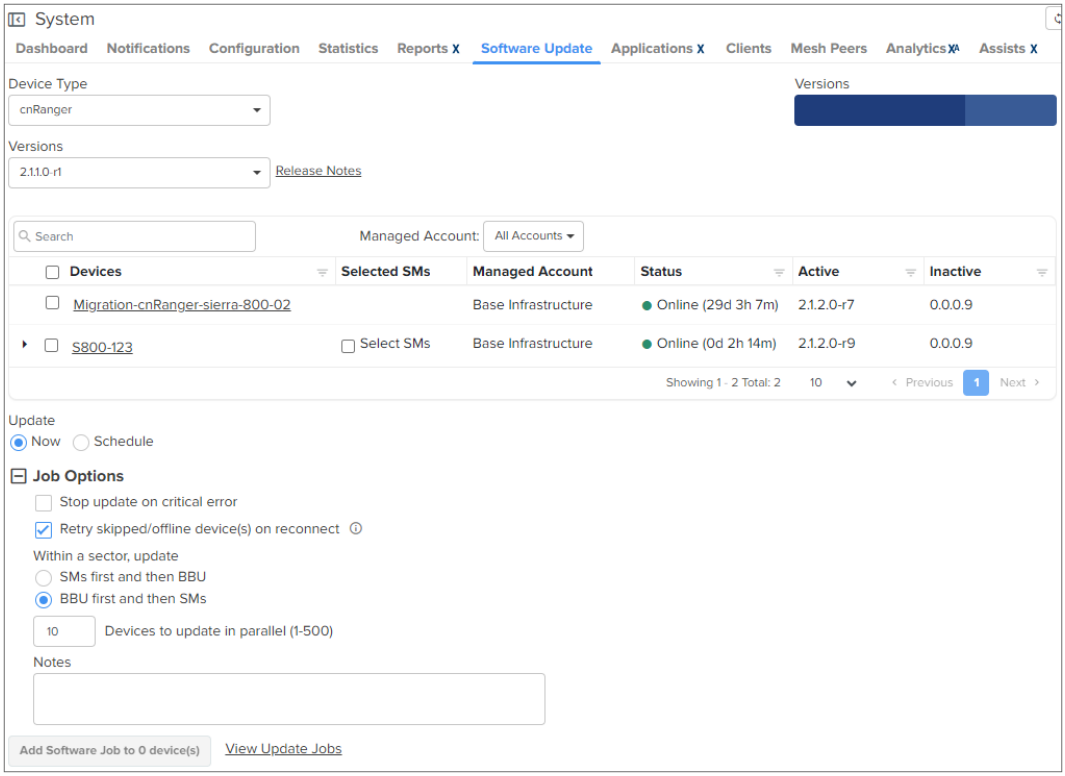


Figure 294 *Software Update: 60 GHz cnWave*

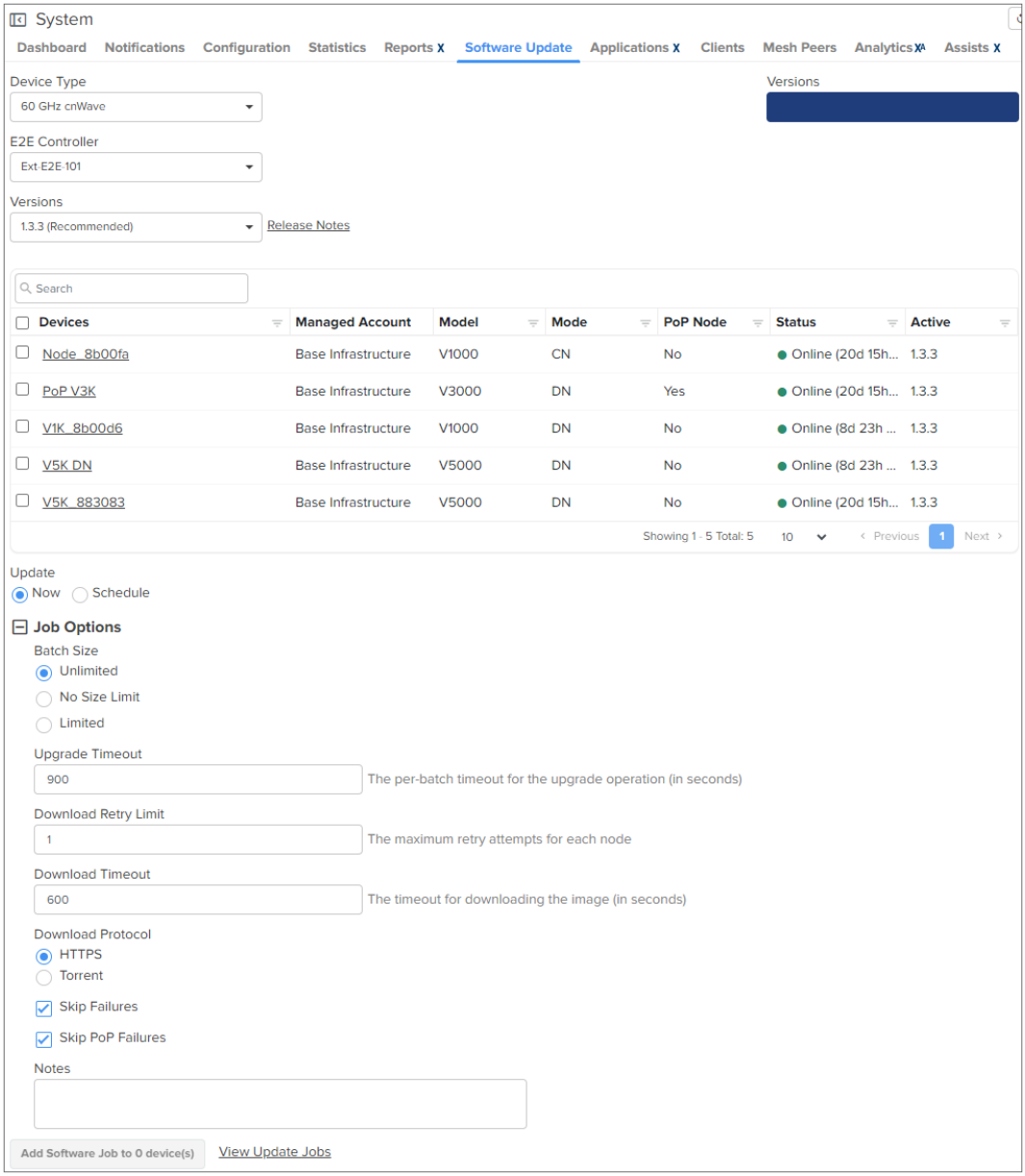
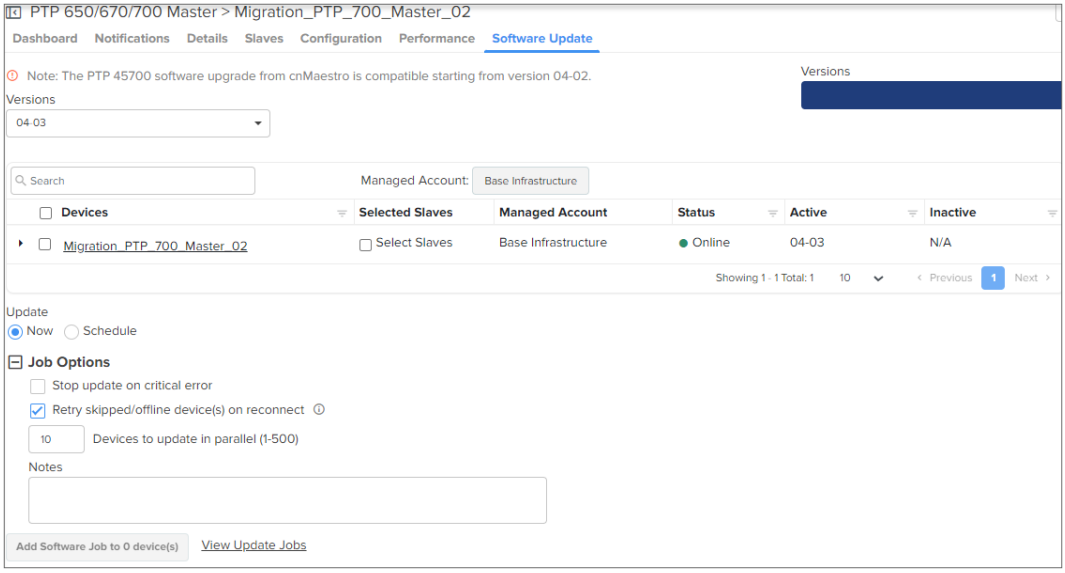


Figure 295 *Software Update: PTP 670/700*



Note

- Ensure that PTP 45700 devices are running the software version 04-02 or later before proceeding with the upgrade.
- Software update is supported on PTP devices from the following cnMaestro versions:
  - from cnMaestro 5.1.0 and later—PTP 78700 and PTP 50670 devices running software version 04-10 and later.
  - from cnMaestro 5.1.1 and later—PTP 48670 devices running software version 04-10 and later.

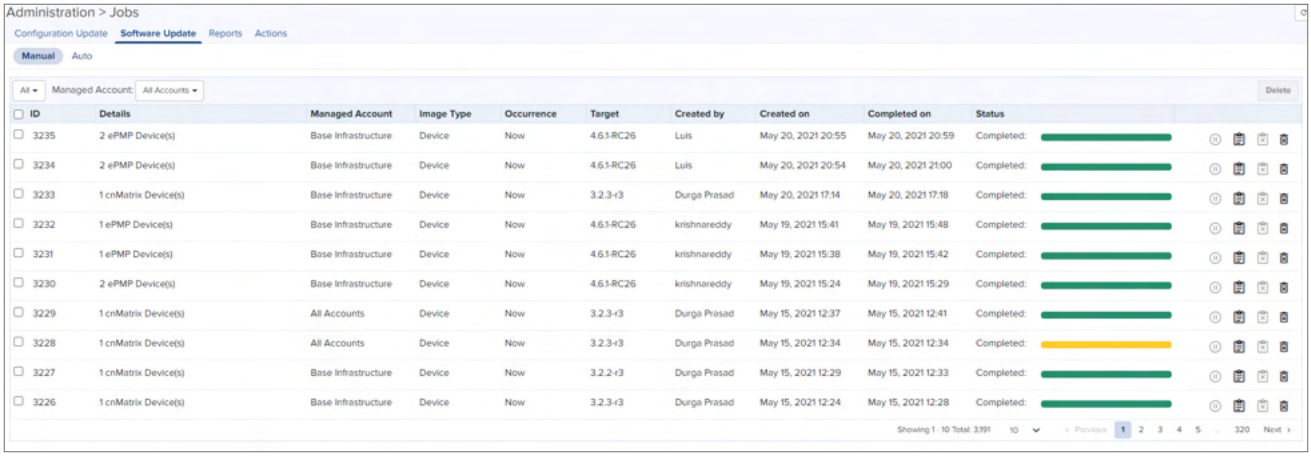
Software Update

The software version on the devices can be automatically updated to the preferred version when the device first contacts cnMaestro.

Enable the automatic update of device software as follows:

1. Navigate to **Administration** > **Jobs** > **Software Update** page**.**
2. Select the **Manual** or **Auto** page for updating the device software feature.
3. Choose the software version depending on the device type.
4. Click **Start.**

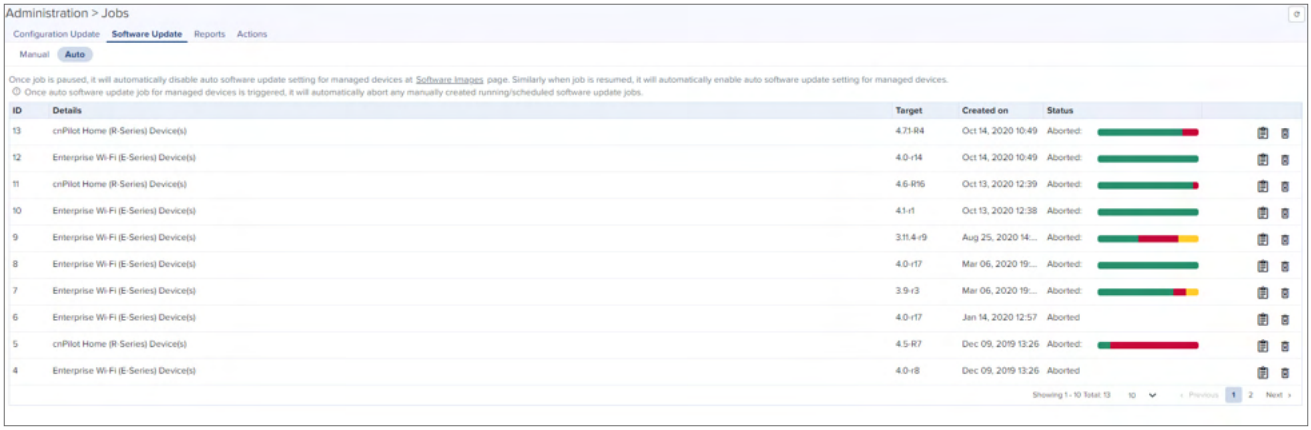
Figure 296 *Manual update*



Note

A Manual Update can be aborted at any point of time by clicking the Abort.

Figure 297 *Auto update*



Note

Auto update can't be manually aborted.

You need to download the new image version released from the Support Site. For more details refer to Managing Device Software Images.

Device Table

Select the devices to upgrade in the Devices Table.

Note

- You can upgrade a device only when status is Up. If you try to upgrade a device when it is Down, you will receive a message the selected device is down.
- If the device is under the Auto Software Upgrade, the manual software update is not possible.

The following parameters are visible (though some are only available for certain device types).

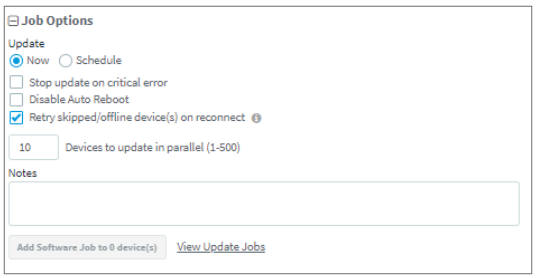
Table 62 *Parameters in Device Table*

Parameter	Description
Current Version	The version of the active software image running on the device.
Devices	The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree.
Selected SMs	If the AP is selected, the corresponding SMs will also be selected.
Status	The status of a particular device in a system. Devices that are not connected cannot updated.

Retry Software Update

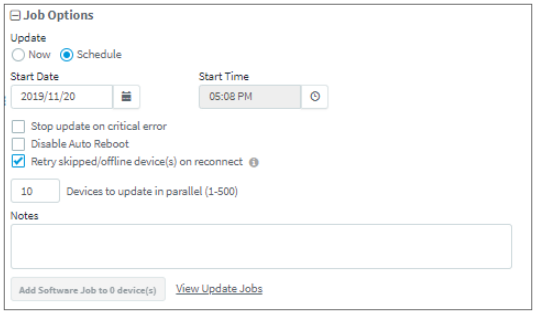
The **Retry Software Update** option is available in every **Software Update** tab; it is enabled by default.

Figure 298 *Retry Software Update*



When you select **Schedule** to update, the following options are available as shown below:

Figure 299 *Retry Software Update: Schedule*



If the Software Update Job was Skipped for a device because it was offline, an icon (⟳) appears next to the Active Software version of the device. This indicates the software update for the device will be done with the Target device version in the Job, whenever it reconnects to cnMaestro.

If the software update job was skipped while upgrading with the same version as the device active version, the icon will not be displayed, and the device will not update when it reconnects.

Note

The device which undergoes **Retry Software Update**, does not create a new Job.

Options

Stop Updates on Critical Error

If one of the updates fails, do not start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off if desired.

Sector Upgrade Order

The recommended update order for devices within a sector will be pre-configured according to the recommendations for the device. It can be changed if desired.



Note

Device update occurs sector-by-sector. One sector needs to complete before a second sector is started.

Parallel Upgrades

Specify how many device upgrades to perform in parallel to complete the upgrade faster. However if the job is configured to halt on an error, all concurrent sessions will still be allowed to complete.

Upgrade Steps

To upgrade an ePMP (Sectors) device, perform the following steps:

1. Navigate to System/Network/Tower/Device level. and select the device.
2. To update the device, navigate to **Manage** > **Software Update**.
3. Select the following **ePMP (Sectors)** from the **Device Type** drop-down:
   a. 60 GHz cnWave
   b. cnMatrix
   c. cnPilot Enterprise (ePMP Hotspot)
   d. cnPilot Home (R-Series)
   e. cnRanger
   f. cnReach
   g. cnVision
   h. cnWave 5G Fixed
   i. Enterprise Wi-Fi (E-Series)
   j. Enterprise Wi-Fi (XV-Series)
   k. ePMP (Sectors)
   l. NSE
   m. PMP (Sectors)
   n. PTP 670/700
   o. PTP 820/850
4. Select the software image to update from the **Version** drop-down.
5. Select checkbox for the devices to update.
6. Select **Job Options**.
7. Click **Add Software Job**.

Software Update Jobs and Parameters

The Software Update Jobs table lists all currently running, queued, and completed jobs. The jobs can be triggered immediately, or they can be run later.

(**Administration** > **Jobs** > **Software Update** tab.)

The following table displays the list of parameters in the **Software Update Jobs** tab:

Table 63 *Parameters in Software Update Jobs*

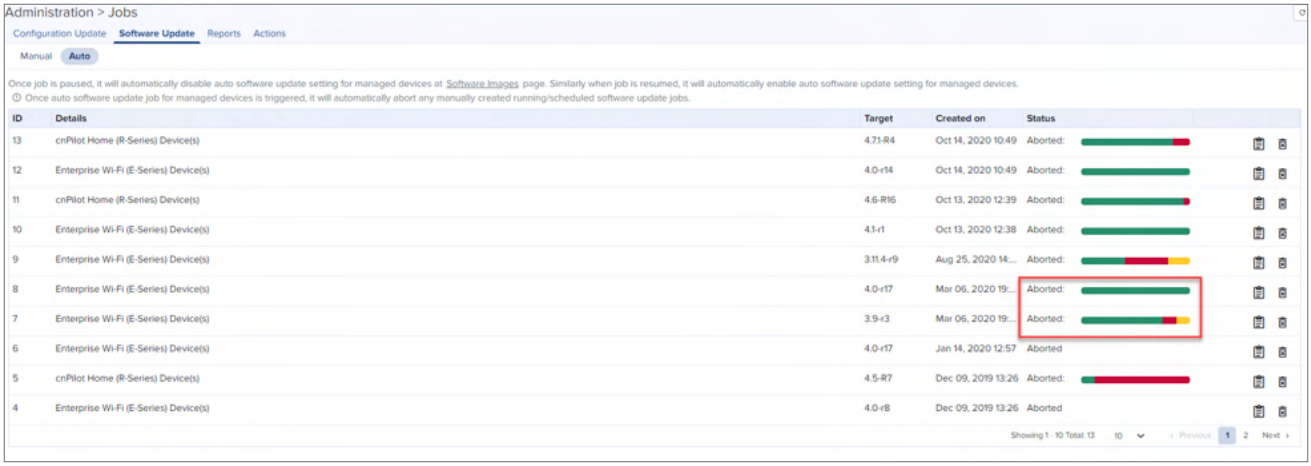
Parameter	Description
Action	Use the **Start** or **Delete** button to manage the upgrade process. After the upgrade has started, the **Pause** button will stop new upgrades from the beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the **Resume** button.
Created By	The user who has created this job.
Created On	Date and time the job is created.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Image Type	Displays **Device** for Device Firmware Upgrade.
Occurrence	Displays **Now** and **Scheduled** depending upon the job options selected during Software Update Job.
Parallel	Number of devices to start in parallel.
Sector Priority	For cnVision, ePMP/PMP, the priority of AP/SM to start.
Status	Status of update.
Stop on Error	Stop the job on an error in any device update.
Target	Target software version to upgrade.
By selecting the **Show More** icon, you can view the following parameters:	
Device	Device for which the upgrade is initiated.
Message	The message that is displayed after the update.
Original Version	The current software image version of the device.
Result	The upgrade status of the device.
Status	Status of the device.

The user can filter the jobs based on the running status. The user can also filter the devices in a particular job based on the parameters mentioned in the above table.

Abort Software Job

Abort operation will skip devices that are waiting for an update to begin. Devices already being updated may continue, but cnMaestro will stop tracking their progress. Aborting a Software Job puts the device into a "Completed" state that cannot be manually restarted by the user. The "pending" devices will not begin their updates.

Figure 300 *Abort Software Job*



Note

1. Devices which are already updated display as **Completed** with a message **Update Complete** along with the status as Completed.
2. Devices that are ongoing display as **Aborted** with a message **Manually Aborted** with the status as Aborted.
3. Devices that have not yet started display as **Skipped** with a message **Job was aborted** with the status as **Skipped**.
4. Software update jobs can be scheduled in parallel irrespective of other running jobs in cnMaestro X accounts.
5. Only **Configuration** or **Software Update Job** operation can be performed on the device, as the job locks the device.

Viewing Running Jobs in header

Click the icon in the top right corner of the UI. This navigates to the **Software Update** tab > **Jobs** page of the Software Update section. For more information, see Software Update

Fixed Wireless Configuration

This chapter provides the following information:

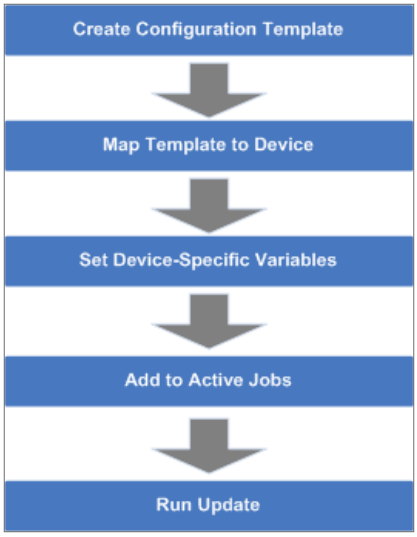
- Overview
- Configuration Templates
- Configuration Variables
- Configuration Update at Onboarding

Overview

Template configuration is supported for ePMP, PMP, cnWave 5G Fixed devices. Templates are textual representations of device settings that contain a full or partial configuration. When a template is applied to a device, the only parameters changed are those in the template.

The process flow of the basic template configuration is shown below:

Figure 301 *Basic Template Configuration Flow*



Configuration Templates

Templates can be pushed to a device manually through a configuration job. This is accomplished in the configuration management page. Templates can also be applied prior to onboarding, in which they would be provisioned in the Onboarding Queue.

Some sample templates are listed below. The ellipses (...) represents additional content that has been excised from the example to limit the size of the text. Each device type has its own template syntax, which can be examined by viewing the device configuration.

Sample ePMP Template

The ePMP template uses the exported ePMP configuration format, which is JSON-encoded.

Figure 302 *Sample ePMP Template*

```
"device_props": {
      "acsEnable":      "0",
      "acsScanMinDwellTime":  "200",
      "acsScanMaxDwellTime":  "300",
      "acsControl":      "0",
      "bcPriority":      "0",
      "cambiumInternetConnectionServerIP":      "",
      "centerFrequency":      "5670",
      "dataVLANEnable": "0",
      "dataVLANVID":    "",
      ...,
      "snmpTrapTable": [{
            "snmpTrapEntryIP":      "10.120.143.176",
            "snmpTrapEntryPort":    "162"
      }],
      ...
}
```

Configuration Variables

Administrators can embed variables into templates that will be replaced when the template is applied to a device. This allows one to leverage a shared, generic template, but to tailor it to individual devices when it is pushed. Template variables are added to a configuration file by replacing an existing parameter with a customer-defined string of the format ${VARIABLE}. An example configuration line with a single variable replacement is shown below:

“networkLanIPAddr”: ${IP ADDRESS}

The above variable is named IP_ADDRESS. When the template is pushed to a device, this variable will be replaced with a value specific to the device. This value needs to be set for the device prior to the template application, else the configuration will not be pushed. Default values can also be specified for variables, as shown below:

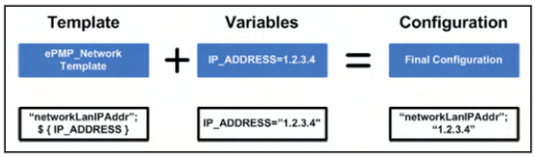
“networkLanIPAddr”: ${IP ADDRESS="10.1.1.254"},

The default value is "10.1.1.254". In this case, if the variable is not set for a device, the default value is used.

Variable Usage

The Templates and Variables are merged to create the final configuration that is pushed to the device. The figure below explains the usage of variables for configuration:

Figure 303 *Variable Usage*



Macros

Macros can be used in templates similar to variables except that they automatically embed values provided by the device itself.

- %{ESN} will be replaced with the MAC address of the device
- %{MSN} will be replaced with the Serial Number of the device

Variable Caching

Variables set for a particular device will be cached, so they can be reused later. This means the next time a template is applied that leverages a variable with the same name as used previously that value will be pre-populated with the previous value. It is therefore beneficial to define a uniform variable naming and usage scheme for variables across different templates.

Device Type-Specific Configurations

The format and values of a configuration template are unique to the different device types. Templates that work with device type do not work with others, and all templates need to be mapped to a specific device type upon creation.

Device Mode restrictions

Some devices, such as ePMP execute in AP and SM modes. The ePMP templates can be configured to only apply to devices that support a selected mode.

Variable validation

All variables for a selected template must be mapped to a value in order to create a configuration job. If any variables are not mapped, an error will be generated. Variables with default settings do not cause an error if they are unset.

Sample Templates

A number of sample templates are provided for each device type. These are not meant to be applied directly, but rather serve as an example of the configuration data format accepted by the device. Refer to the device documentation for complete information.

Template file creation

The typical process for creating your own configuration templates is below:

1. On a test device configure the parameters to the devices. This can be done directly on the device UI .
2. Export the device configuration using cnMaestro.

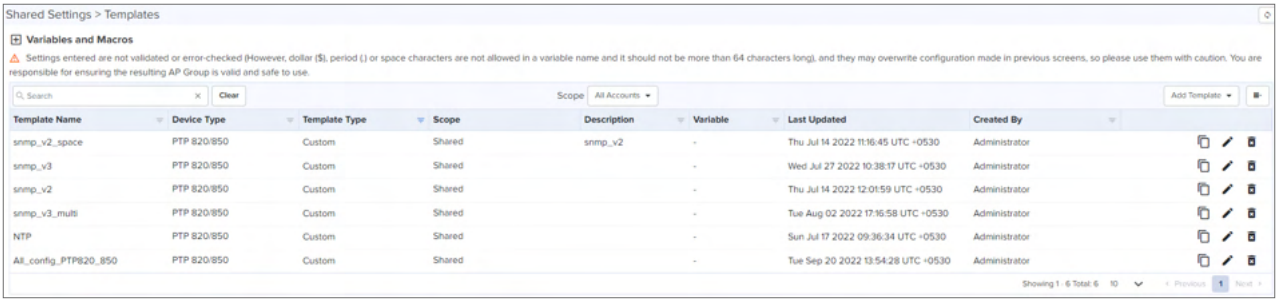
- Navigate to **Configuration > Templates**, select the device in the left-hand tree and click the **View Device Configuration** link. This can also be done via the device GUI, typically in the Administration or Operations section where there will be an **Export** for configuration.

3. View the configuration file in a text editor like Notepad++ and search for the values entered in step 1. You can also search for the parameter name to find the correct lines.
4. Copy and paste the relevant lines into a new file.
5. Optionally replace values with replacement variable text. This will allow you to set the value per device.
6. Once you have this partial template, it can be copied into the template creation text field and saved.

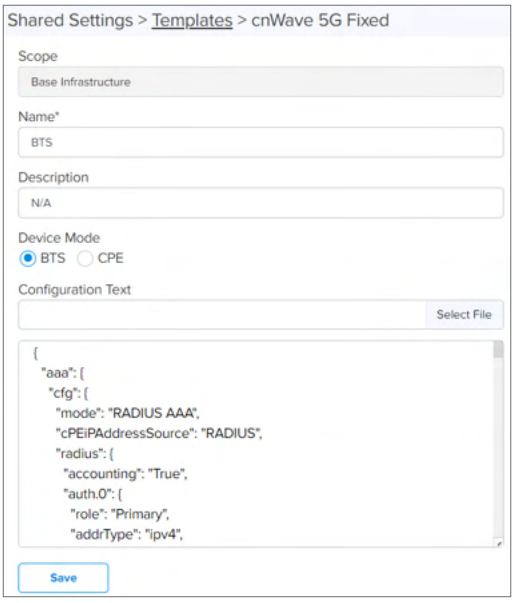
Template

To create a configuration template:

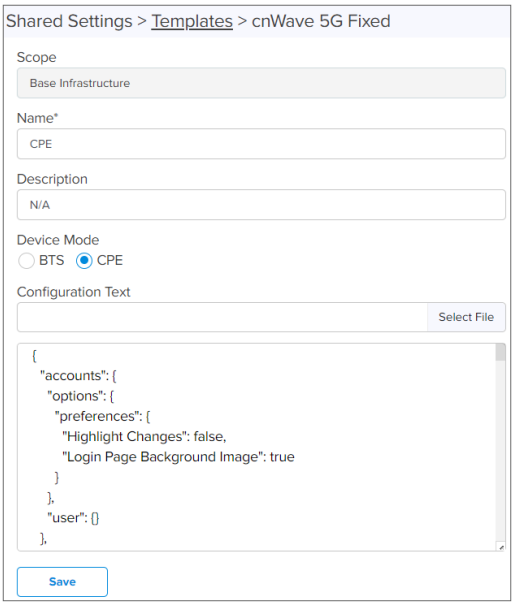
1. Navigate to **Configuration > Templates** in the main menu.



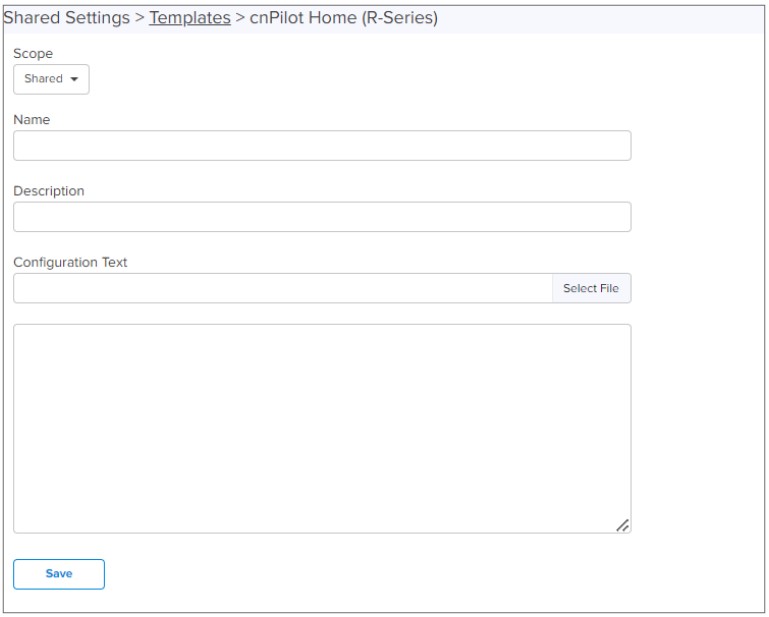
The following template is for BTS:



The following template is for CPE:



2. Click **Add Template** button.



3. Choose a **Device Type**, **Name**, and **Description** for the template. For ePMP, PMP, cnWave 5G Fixed, cnReach, and cnMatrix templates, you should select a **Device Type** as well.
4. Either upload your template into the UI or paste the template text into the text area.

Note

No default templates available for R-series. User needs to create a new template.

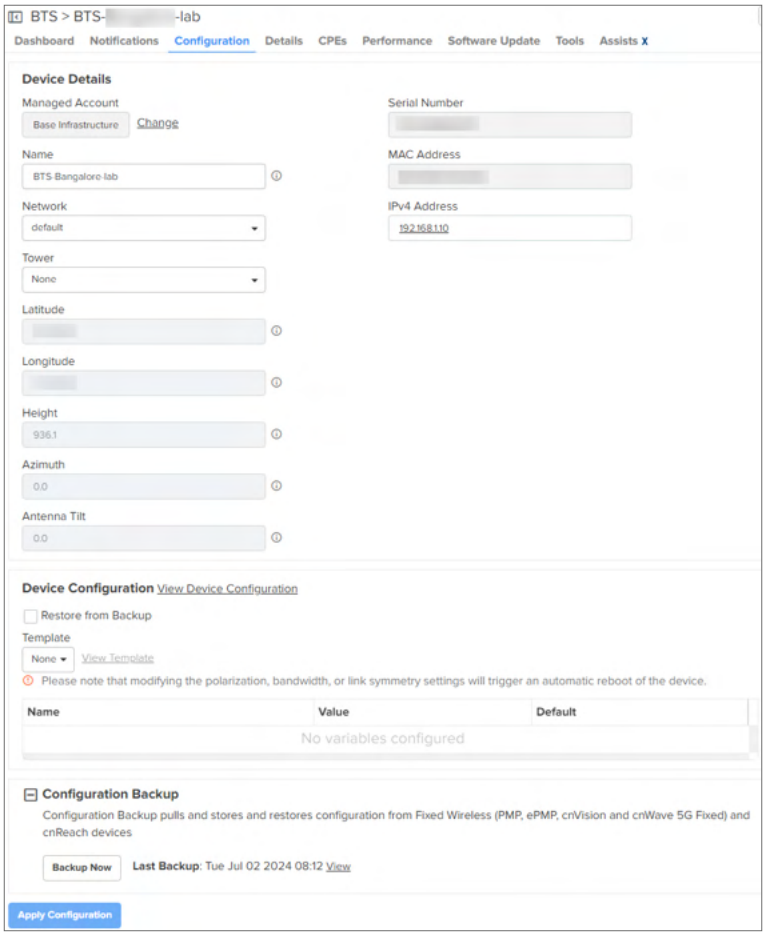
5. After clicking **Save**, the template will be available in the selection menu on the configuration and onboarding pages, as long as the device type and model match the device selected.
6. By selecting the Custom option under the Template type filter All Default templates will be hidden.

Note

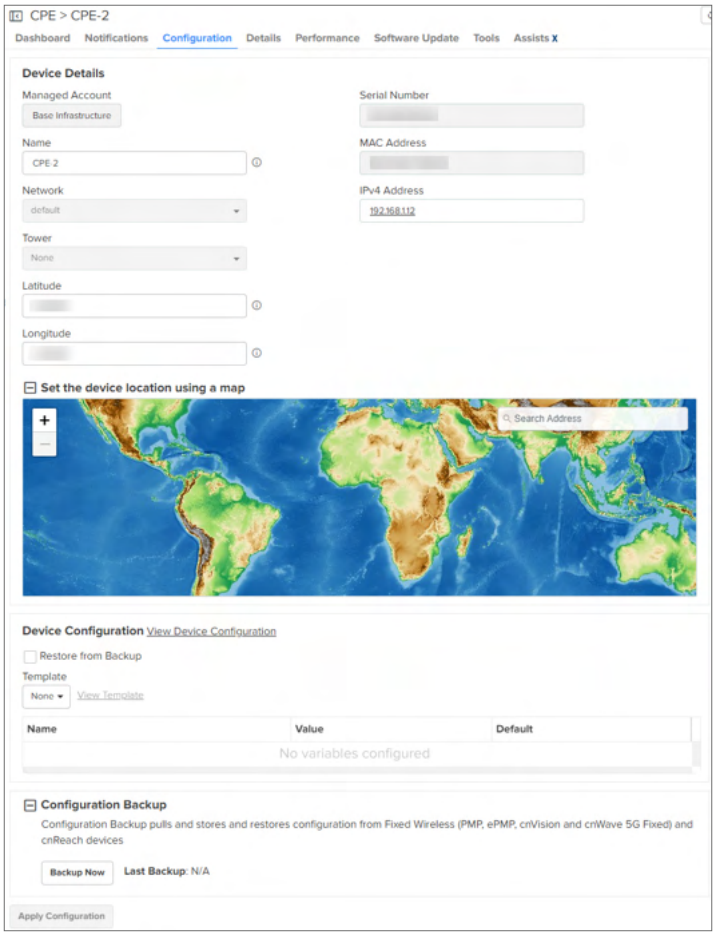
When you navigate to the Template page default template type filter will be custom. User needs to select **All** or **Default** to view other templates.

BTS and CPE Configuration

To configure BTS, navigate to **Monitor and Manage** > **BTS** > **Configuration**.



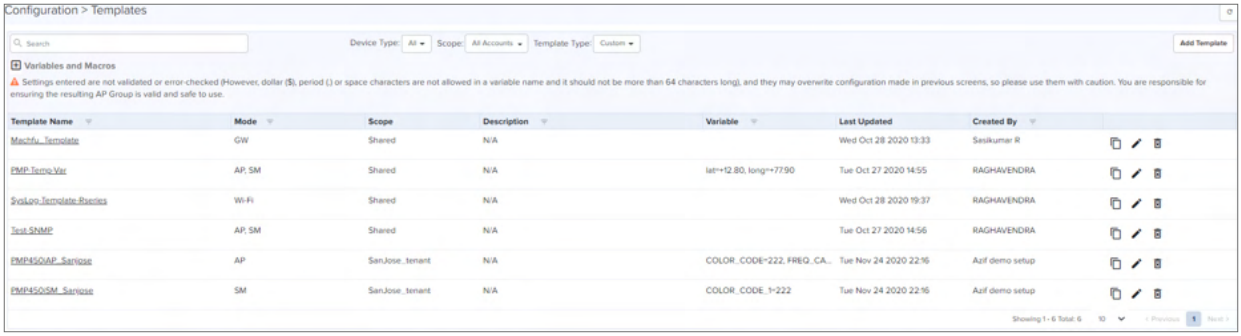
To configure CPE, navigate to **Monitor and Manage** > **BTS** > **CPE** > **Configuration**.



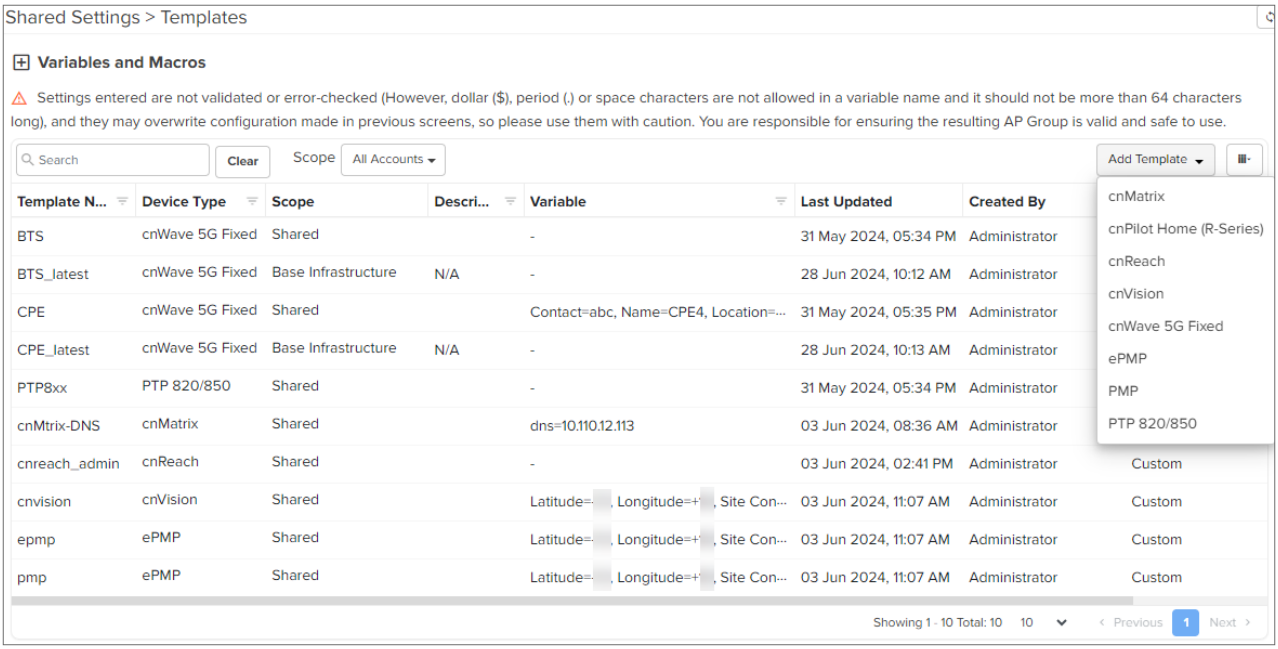
Configuration Template for PTP 820/850

To create a configuration template of PTP 820/850 device, perform the following steps:

1. Navigate to **Configuration** > **Templates** in the main menu.



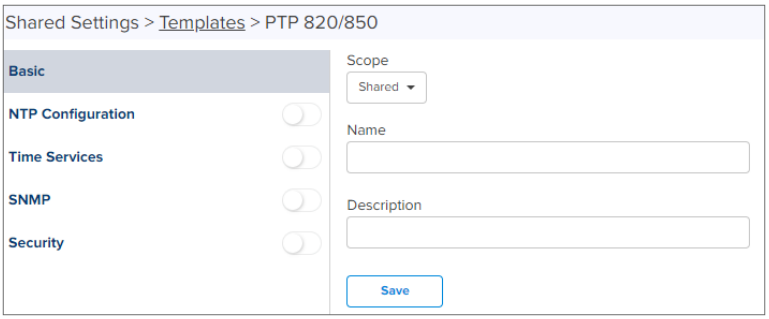
2. In the **Add Template** drop-down, select PTP 820/850.



The **Basic** template page appears.

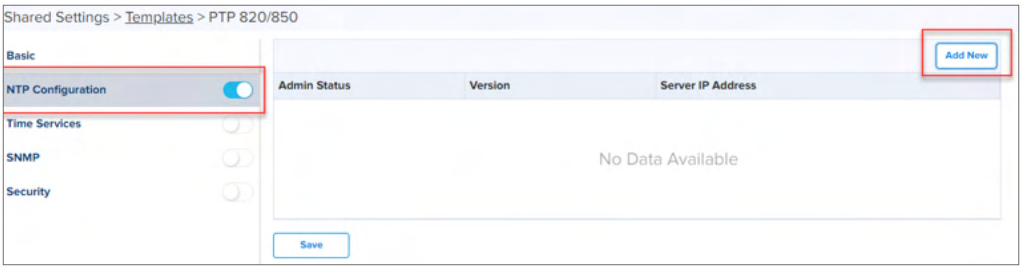
3. In the **Basic** page, enter **Name** and **Description** and click **Save**.

   By default, **NTP Configuration, Time Services**, **SNMP,** and **Security** pages are disabled. Click slider icon next to the fields to enable the pages and configure the template.



NTP Configuration

1. In the **NTP Configuration,** click **Add New**.



Create window appears.



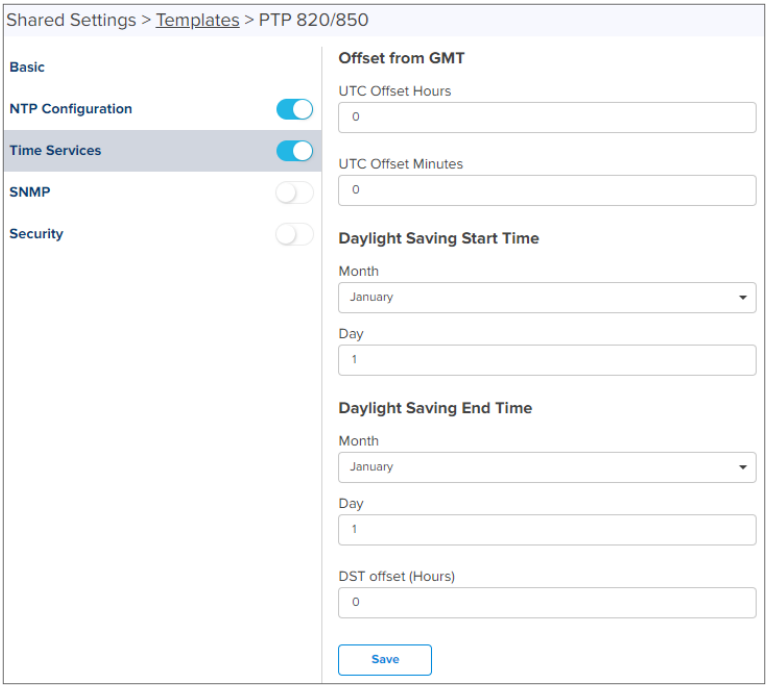
2. Select **Admin Status** from drop-down.
3. Select **Version** from drop-down.
4. Enter **Server IP Address**.
5. Click **Save.**

NTP configuration is added to the table. You can perform the following actions for configurations added in the table.

1. Click edit icon to edit the configuration
2. Click delete icon to delete the configuration.

Time Services

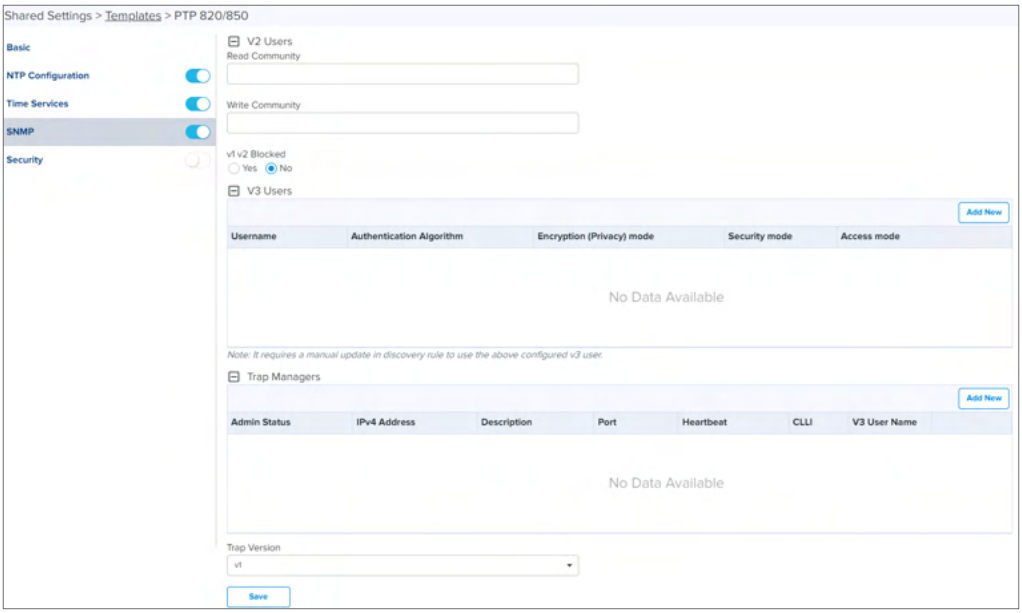
1. Enter the values for the following fields:
   - Offset from GMT
   - Daylight Saving Start Time
   - Daylight Saving End Time



2. Click **Save**.

SNMP

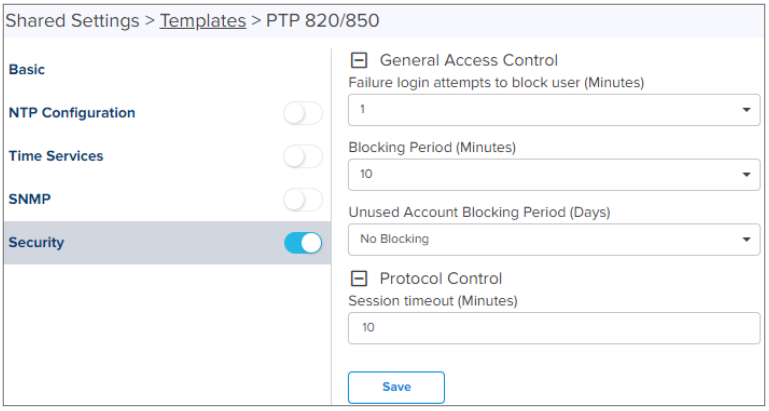
1. Enter the details for **V2 Users**, add **V3 Users** and **Trap Managers**, and select **Trap Version**.



2. Click **Save**.

Security

1. Select the values for **General Access Control**.
2. Select **Protocol Control**.



3. Click **Save**.

Configuration Update

Device Selection

Navigate to the **Configuration Update** tab, and then navigate the Device Tree to the appropriate level for device selection. For example, selecting a Fixed Wireless AP will enable selection of the AP and all its SMs.

Device Type

Configuration jobs are created for a single device type. The type includes the specific hardware (ePMP, PMP) as well as the mode of the device (cnVision, PMP or PTP mode for ePMP for example).

Device Table

Select the devices to upgrade in the Devices Table. The following parameters are visible in the table:

Table 64 *Device Table parameters*

Parameter	Description
Devices	The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree.
Network/Tower	The network and the tower on which the device is located.
Status	The status of a particular device in a system. Devices that are “Down” can not have images pushed to them.

Note

- You can only push configuration to a device when its status is **Up**.
- The user should validate the configuration before pushing it to the device from cnMaestro.

Options

Stop all Configuration on a Critical Error

If one of the configuration updates fails, then do not start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off.

Parallel Upgrades

Define how many configuration updates to perform in parallel.

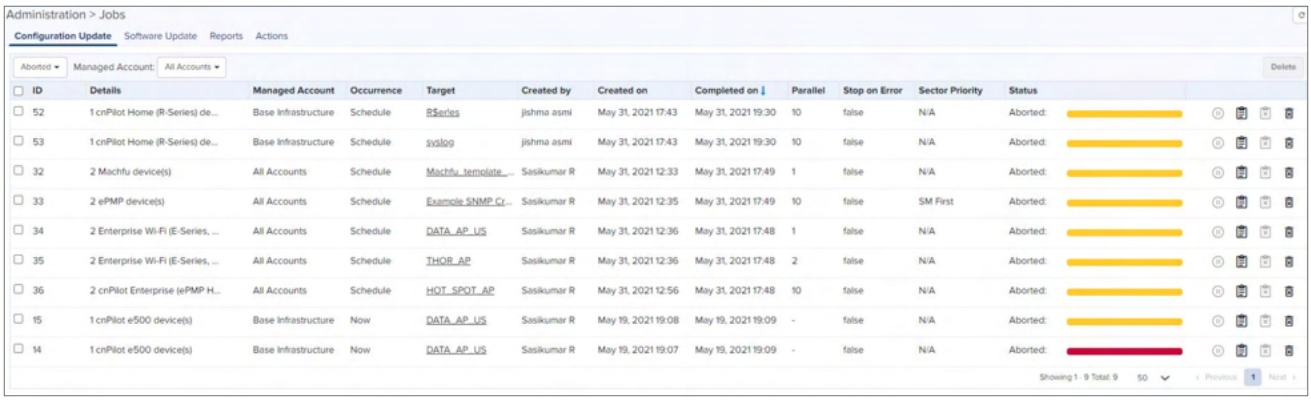
Update Ordering

Allows you to specify update ordering within a Fixed Wireless sector. Options are SMs first and then AP or AP first and then SMs.

Abort Configuration

Abort operation will skip devices that are waiting for update to begin. Devices already being updated may continue but cnMaestro will stop tracking their progress. Aborting a Configuration Job puts the device into a complete state that cannot be manually restarted by the user. The pending devices will not begin their updates.

Figure 304 *Abort Configuration*



Note

1. Devices which are already updated display as **Completed** with a message Update Complete along with the status as **Completed**.
2. Devices which are ongoing display as **Aborted** with a message Manually Aborted with the status as **Aborted**.
3. Devices which have not yet started display as **Skipped** with a message Job was Aborted with the status as **Skipped**.

Configuration Update Steps

To update the configuration of an ePMP (Sectors) device, perform the following steps:

1. Navigate to **Manage** > **Configuration** > **Device Details** in the Main Menu.
2. Navigate to **System** > **Network** in the Device Tree. From the list of available networks, select a network in which the device belongs.
3. Select ePMP (Sectors) from the **Device Type** drop-down.
4. Select the configuration template to upgrade from the **Template** drop-down.
5. Select the device(s) to upgrade.
6. Click the gear icon to view or edit variables that are required for selected devices.
7. Click **Apply Configuration**.

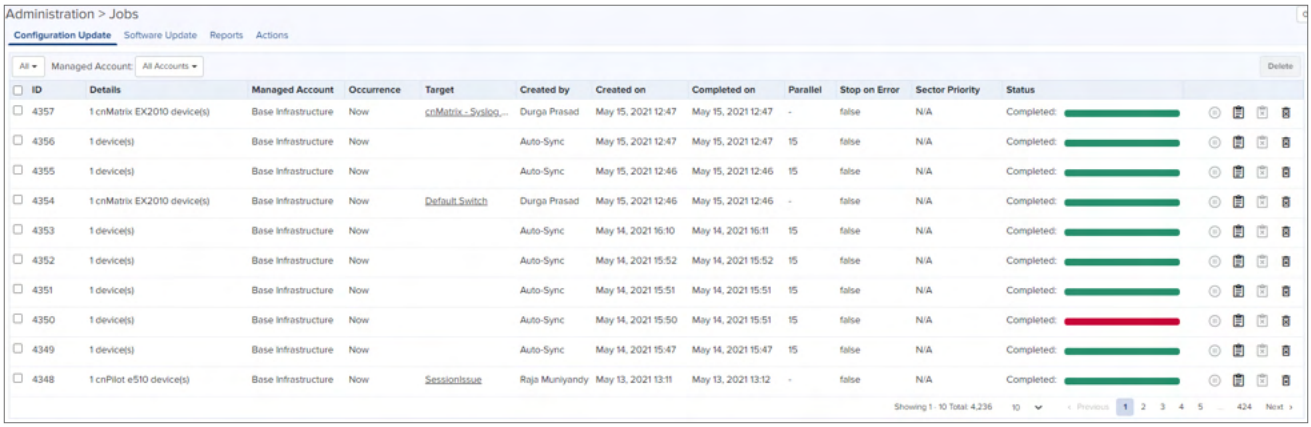
Note

- The Configuration Upgrade cannot proceed until all required variables (those without default parameters) are entered. If you attempt to create a configuration job without setting required variables, the gear icon will turn red for any devices not meeting this requirement.
- To save and download the existing Device Configuration as Template, click **View Device Configuration** link.

Configuration Jobs

Navigate to **Administration** > **Jobs** > **Configuration Update** tab.

Jobs are presented with various Status values: Running, Queued, Skipped, and Completed. They can be triggered to execute immediately or run later. The list of parameters in the Jobs tab is shown below:



Note

cnMaestro X account user can run any number of **Jobs** in parallel.

The following table displays the list of parameters in the **Jobs** tab:

Table 65 *Configuration Update parameters*

Parameter	Description
Action	Use the **Start** or **Delete** button to manage the upgrade process. After the upgrade has started, the **Pause** button will stop new upgrades from the beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the **Resume** button.
Created By	The user who has created this job.
Created On	Date and time on which the job is created.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Parallel	Number of devices to start in parallel.
Sector Priority	For ePMP/PMP, cnRanger, cnVision Hub/Client, the priority of AP/BBU/SM to start.
Status	Status of update.
Stop on Error	Stop the job, if any device in middle finds any error.
Target	Target software version to upgrade.
By selecting the **Show More** icon, you can view the following parameters:	
Device	Device for which the upgrade is initiated.
Message	The message displayed after the update.
Result	The upgrade status of the device.
Status	Status of the device.
Mode	SM or AP mode selected.
Network	Type of Network.
Tower	Name of the Tower.

Configuration Update at Onboarding

Administrators can apply the configuration to devices during the onboarding process: Prior to approving the device in the Onboarding Queue, the configuration template and variables can be specified. These will then be pushed to the device during onboarding. For more details on onboarding, see Device Onboarding.

Wi-Fi Configuration

Wi-Fi configuration is handled through AP Groups or Templates, which Fixed Wireless devices, such as ePMP and PMP, exclusively use Templates. This section will focus exclusively on AP Groups.

This chapter provides details on the following sections:

- Enterprise Wi-Fi AP
- Factory Reset
- Association ACL

- Access Control Policies
- Custom Applications

Enterprise Wi-Fi AP

There are four types of Wi-Fi hardware:

- Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
- cnPilot Enterprise APs
- cnPilot Home (cnPilot R-series devices)
- Enterprise Wi-Fi (Xirrus-Series)

These four hardware types map to the following AP group types:

- Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
- Enterprise Wi-Fi (Xirrus-Series)
- cnPilot Home (R-Series)
- RV22 Home Mesh

Multiple AP Group types are needed, because the features available across the groups are different.



Note

Wi-Fi devices can alternately be configured using a template mechanism, in which a subset of configuration is pushed to the device manually through a user-defined template of parameters. See the section on Templates for more information. Template configuration and AP Group configuration cannot be used simultaneously.

Configuring Enterprise Wi-Fi APs using Wi-Fi Profiles

Wi-Fi devices are configured by creating an AP Group, mapping it to shared WLANs, and assigning it to devices through the Configuration tab. Once assigned, the configuration is pushed manually or automatically (if **Auto Sync** is enabled).



Note

Xirrus devices embed WLAN configuration directly into the AP Group Full Configuration tab and do not support separate WLAN profiles.

Auto Synchronization

AP Groups can automatically synchronize device configuration whenever the AP Group or associated WLANs are updated. This is done by enabling **Auto Sync** in the AP Group **Configuration** page.

Manual Synchronization

When a device is mapped to an AP Group without **Auto Sync** turned on, the device is placed in an **Unsynchronized** state until it is manually synchronized. Manual synchronization can be done as follows:

- Navigate to device **Configuration** page > **Sync Now** or
- Navigate to **Administration > Sync Configuration > Sync Configuration.** page.

Create an AP Group



Note

- This example demonstrates how to create an Enterprise Wi-Fi (E-Series, XE/XV/X7-Series) AP Group. A similar process can be followed for the cnPilot Home (R-Series) AP Group.
- The Enterprise Wi-Fi (Xirrus-Series) AP Group is different than the others. It embeds a full configuration template of CLI commands that needs to be updated manually. The Xirrus AP Group will support Auto Synchronization when the embedded template is changed, which makes it different than applying the configuration through the standalone Template mechanism.

To create an AP Group, perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** > **AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.



Note

- Certain special characters can be used when creating the AP Group and WLAN passwords, such as a-zA-Z_-*&%#@!<>.() []^~`$1234567890.
- By default, the password is not configured. User must configure the password for AP Groups.

  You can also rename the password after creating one.

Basic

In the **Basic** page, configure the following details such as:

1. Select **Type** from one of the following:
   - cnPilot Home (R-Series)
   - Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
   - Enterprise Wi-Fi (Xirrus-Series)
2. Enter the mandatory fields based on device type.
   - Name
   - Country
   - Description
   - WLAN
3. Click **Add WLAN** and select **WLAN** from the list.
4. Click **Save**.

Figure 305 *Basic: cnPilot Home (R-Series)*

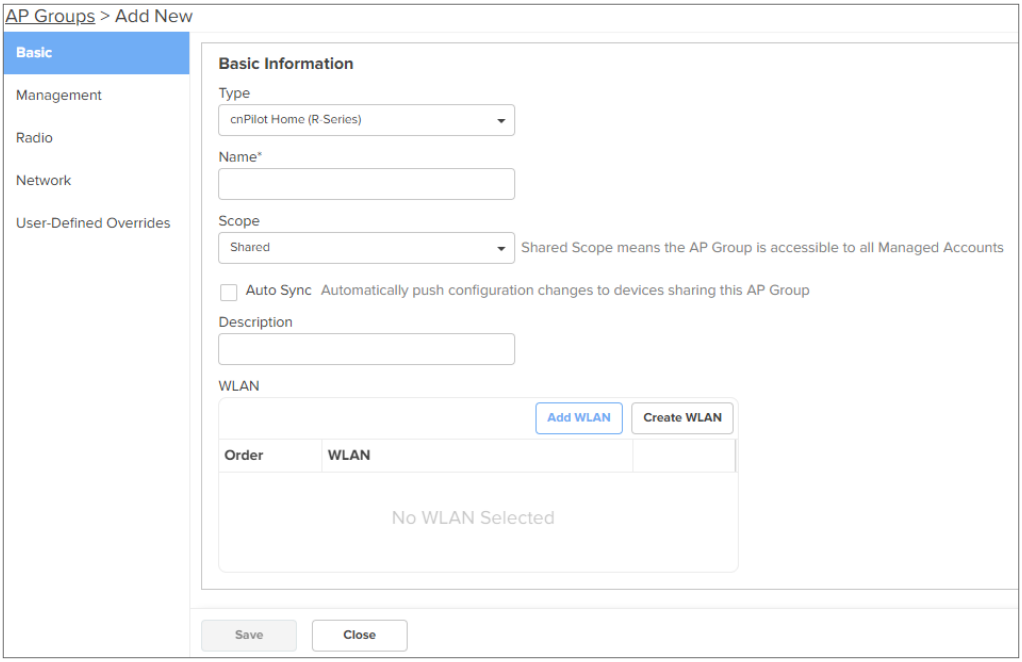


Figure 306 *Basic: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*

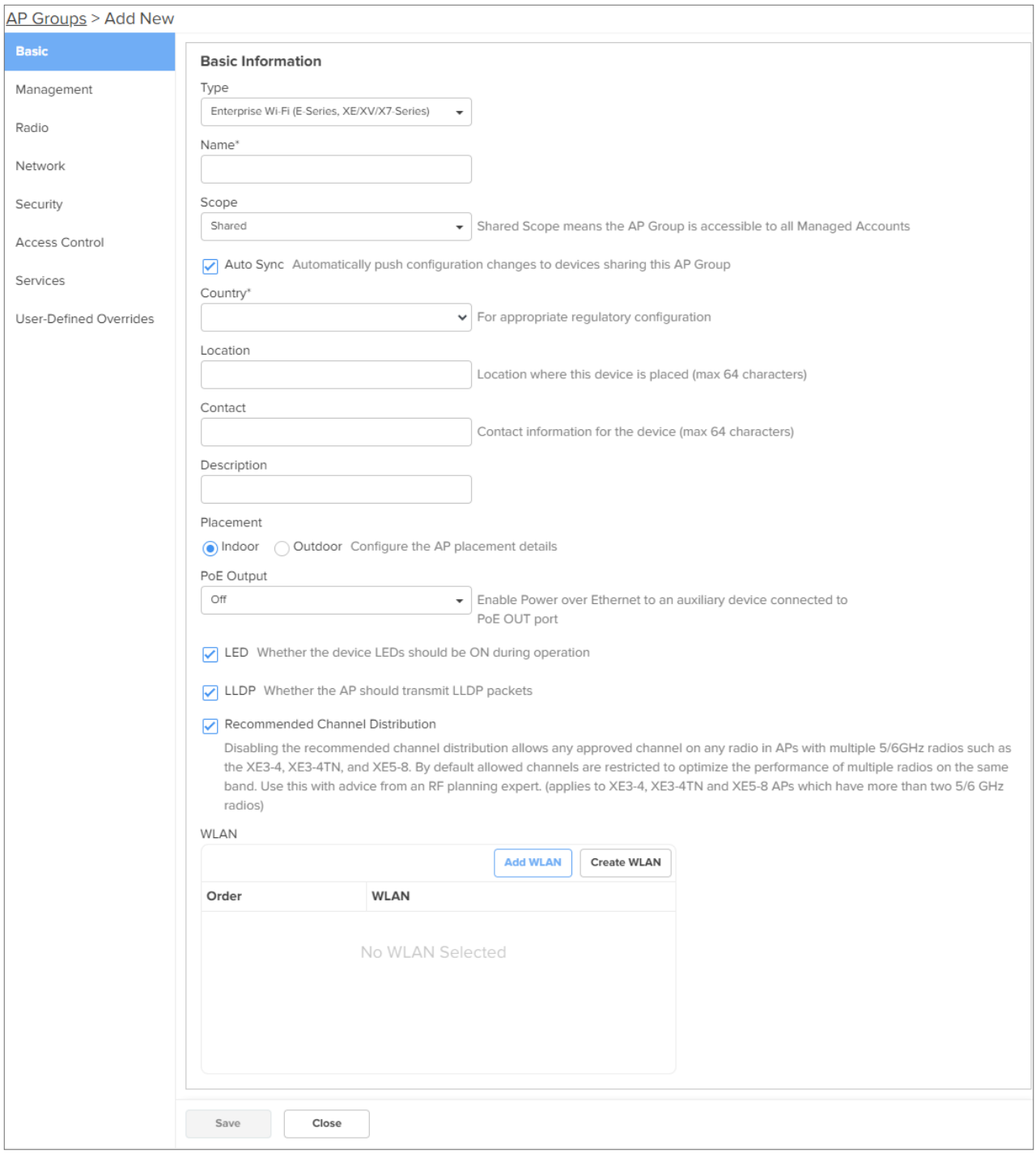
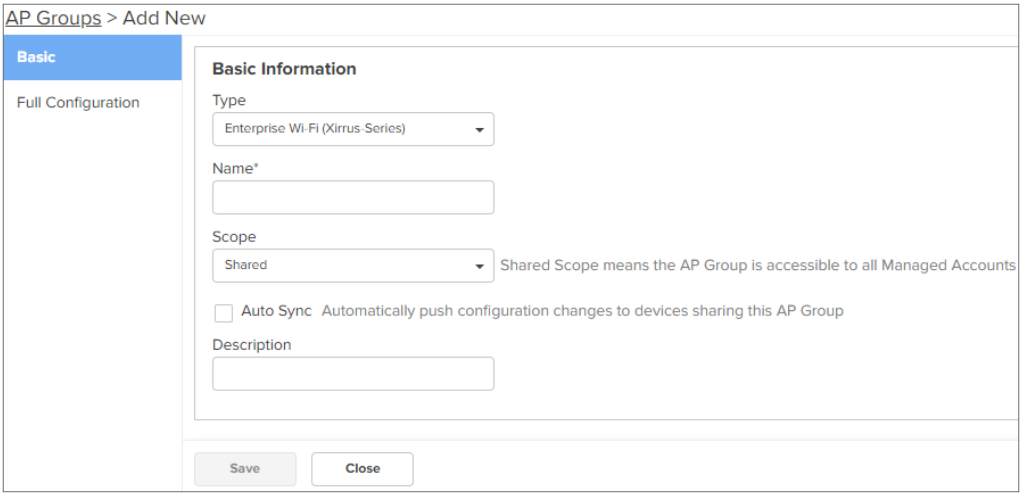
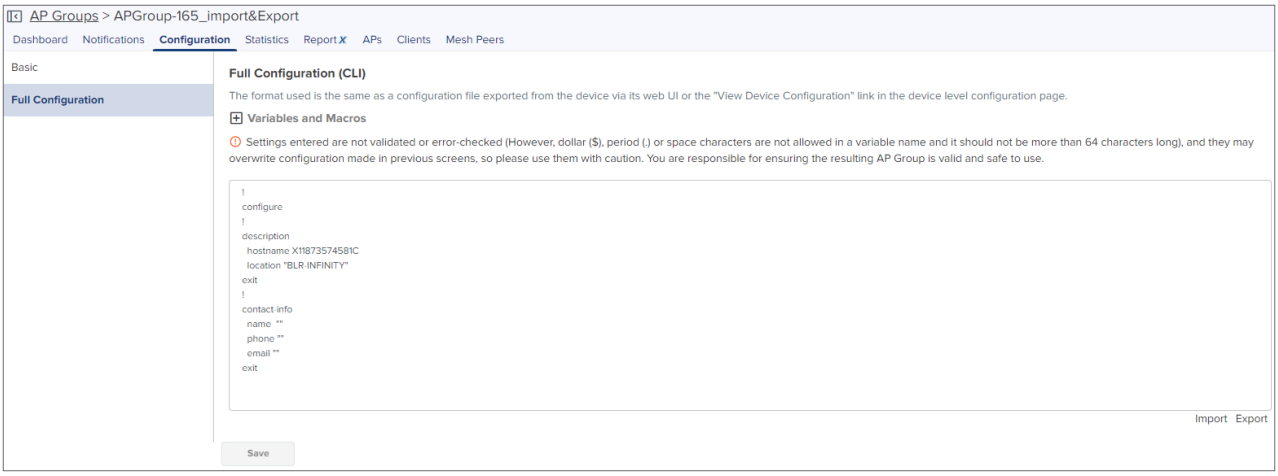


Figure 307 *Basic: Enterprise Wi-Fi (Xirrus-Series)*



The Xirrus AP Group embeds a Full Configuration of CLI commands.

Figure 308 *Full Configuration: Enterprise Wi-Fi (Xirrus-Series)*



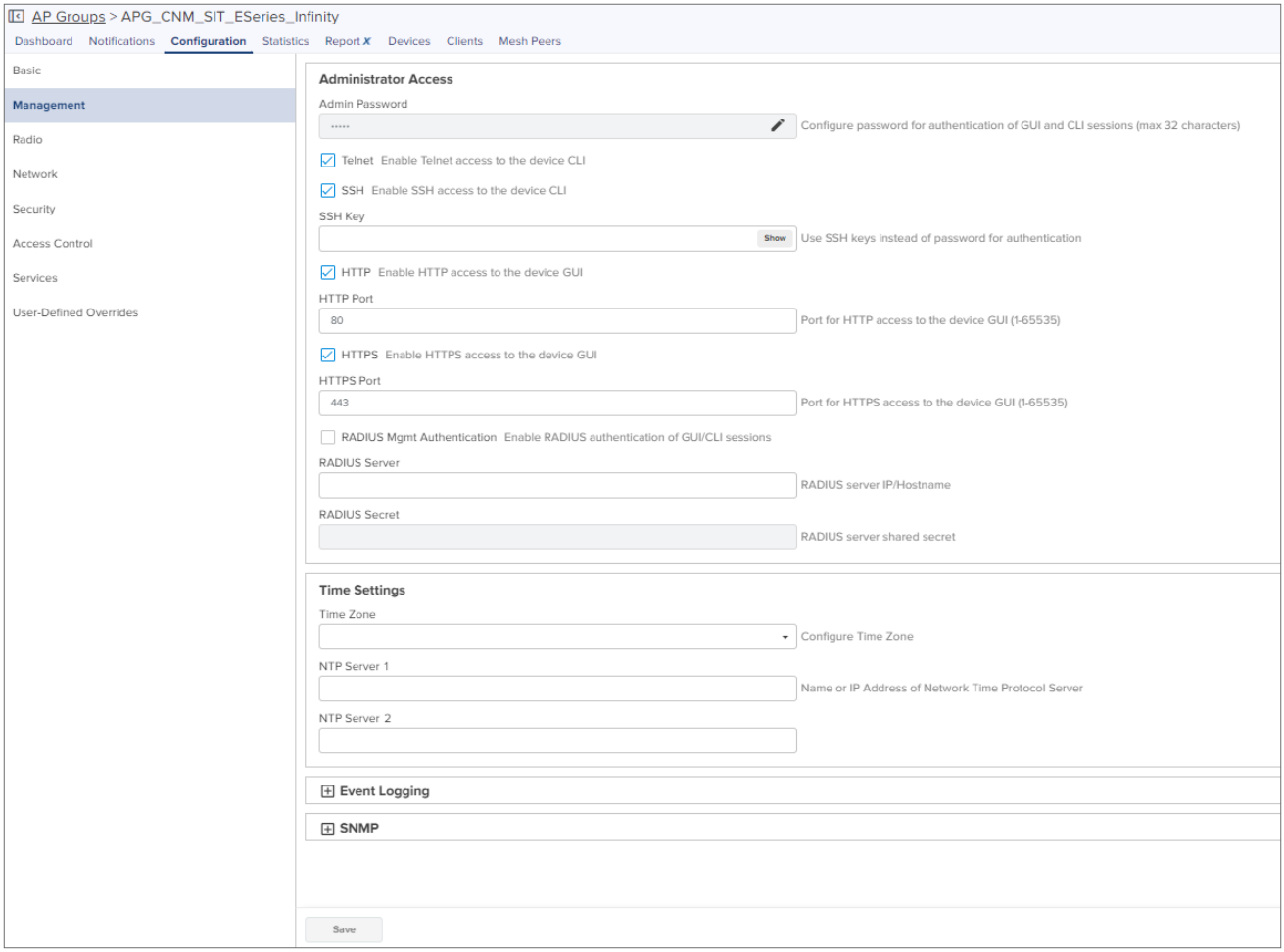
Management

The **Management** page allows to configure the **Administrator Access, Time Settings, Event Logging** and **SNMP.**

Note

The AP uses the AES algorithm for encryption and SNMPv3 password configuration parameter is used for encryption and authentication.

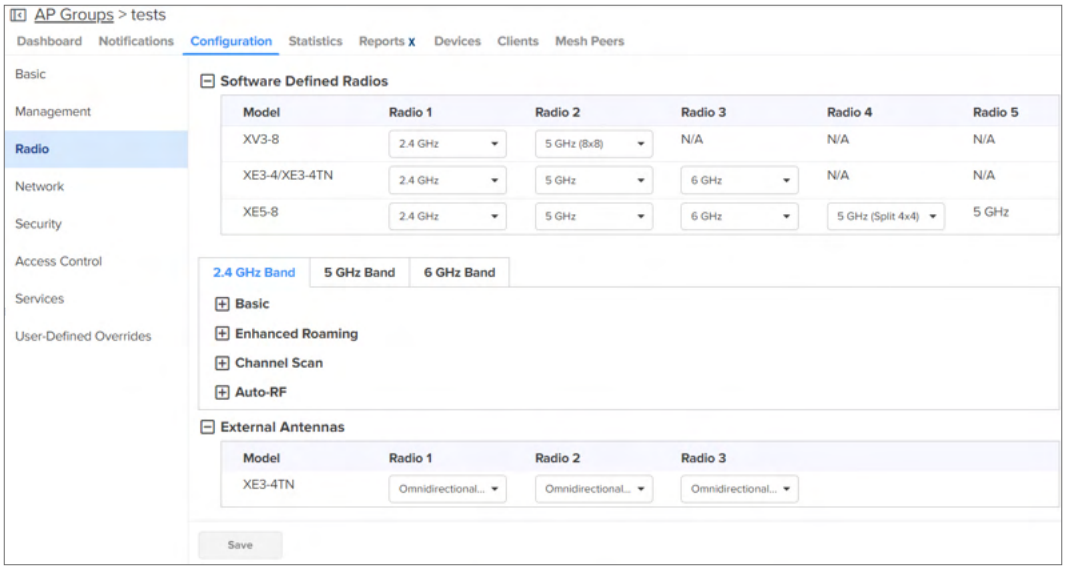
Figure 309 *Management: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*



Radio

The **Radio** page allows the user to enable or disable the Software Defined Radio operations. It allows to configure **Software Defined Radios, Basic**, **Enhanced Roaming**, **Off Channel Scan**, **Auto-RF, and External Antennas**.

Figure 310 *Radio: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*



Note

The software defined radio creation and channel listing are populated based on the country-specific restrictions, device type, and release version.

Software Defined Radios

The Software Defined Radios (SDR) allows you to configure radio parameters for XV3-8, XE3-4, and XE5-8 device models. By default these device models are configured for radio bands as shown in Figure 310. The other radio bands for which the devices can be configured are as shown in Table 66.

Table 66 *Supported Radio bands for Enterprise Wi-Fi Series (E-Series, XV-Series and XE-Series)*

Models	Radios	Supported Radio Bands	Channel Specification		
			Channel width	Default Channel width	Supported channel list
XV3-8	Radio 1	2.4 GHz	20/40	20	1 to 13
	Radio 2	5 GHz (8x8 - single radio) or 5 GHz (Split 4x4 dual radio)	20 / 40 / 80	40	• 100 to 165 in Split 4x4 dual radio • 36 to 165 in 8x8 - single radio
	Radio 3		20 / 40 / 80	40	36 to 64 in Split 4x4 dual radio
XE3-4	Radio 1	2.4 GHz	20/40	20	1 to 13
	Radio 2	5 GHz	20 / 40 / 80	40	36 to 64
	Radio 3	5 GHz	20 / 40 / 80 / 160	40	100 to 165
		6 GHz		160	Any 6 GHz channel
XE3-4TN	Radio 1	2.4 GHz	20/40	20	1 to 13
	Radio 2	5 GHz	20 / 40 / 80	40	36 to 64
	Radio 3	5 GHz	20 / 40 / 80 / 160	40	100 to 165
		6 GHz		160	Any 6 GHz channel
XE5-8	Radio 1	2.4 GHz	20/40	20	1 to 13
	Radio 2	5 GHz or 6 GHz	20 / 40 / 80 / 160	20*/80**	Refer to Table 67 for Supported Channel list in 5 GHz and 6 GHz
	Radio 3	5 GHz or 6 GHz	20 / 40 / 80 / 160	20*/80**	
	Radio 4	5 GHz (8x8 - single radio) or 5 GHz (Split 4x4 dual radio)	20 / 40 / 80	20	
	Radio 5		20 / 40 / 80		
* 5 GHz **6 GHz					

Note

- Split 4x4 is applicable only for 8x8 spatial streams supported devices. (Supported device models are XV3-8 and XE5-8).
- Dual 5 GHz Radio (Supported only on XV3-8 and XE5-8 APs) splits 8x8 5 GHz radio into two 4x4 5 GHz radios.
- In XV3-8, radio 3 is available only in the SBS mode.
- In XE5-8, radio 5 is available only in the SBS mode.

Table 67 *Supported Channel list 5 GHz or 6 GHz in XE5-8*

Radio Index				Radio 1	Radio 2	Radio 3	Radio 4	Radio 5
8x8 mode of operation: Radio 4 & 5 as single radio with 8x8								
Radio 2	**Radio 3**	**Radio 4 & 5**						
5 GHz	5 GHz	5 GHz		NA	100 to 128	149 to 165	36 to 64	
6 GHz	5 GHz	5 GHz		NA	Any 6 GHz channel	100 to 165	36 to 64	
5 GHz	6 GHz	5 GHz		NA	100 to 165	Any 6 GHz channel	36 to 64	
6 GHz	6 GHz	5 GHz		NA	* 1 to 93	** 97 to 233 / 65 to 93	36 to 165	
Split 4x4 mode of operation: Radio 4 and 5 as individual radio with 4x4								
Radio 2	**Radio 3**	**Radio 4**	**Radio 5**					
5 GHz	5 GHz	5 GHz	5 GHz	NA	60 to 64	100 to 128	149 to 165	36 to 40
6 GHz	5 GHz	5 GHz	5 GHz	NA	Any 6 GHz channel	100 to 128	149 to 165	36 to 64
5 GHz	6 GHz	5 GHz	5 GHz	NA	100 to 128	Any 6 GHz channel	149 to 165	36 to 64
6 GHz	6 GHz	5 GHz	5 GHz	NA	* 1 to 93	** 97 to 233	100 to 165	36 to 64
Note: *FCC SKU 6GHz UNII-5 or 6 (1 - 93) EU SKU UNII-5 low (1 - 61) **FCC SKU 6GHz UNII-7 or 8 (97 - 233) EU SKU UNII-5 High (65 - 93)								

Note

You can use `no channels-distribution` global configuration CLI command for all multi-radio platforms, such as XE3-4, XE3-4TN, and XE5-8 APs. When configured on the device, the predefined default channel list can be overridden.

To configure `no channels-distribution` using the AP groups in cnMaestro UI, complete the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** > **AP Groups** page.
2. Select the AP group that you want to update with the `no channels-distribution` CLI.
3. Click **User-Defined Overrides** tab.
4. Enter the following command in the box:

```
!
no channels-distribution
!
```

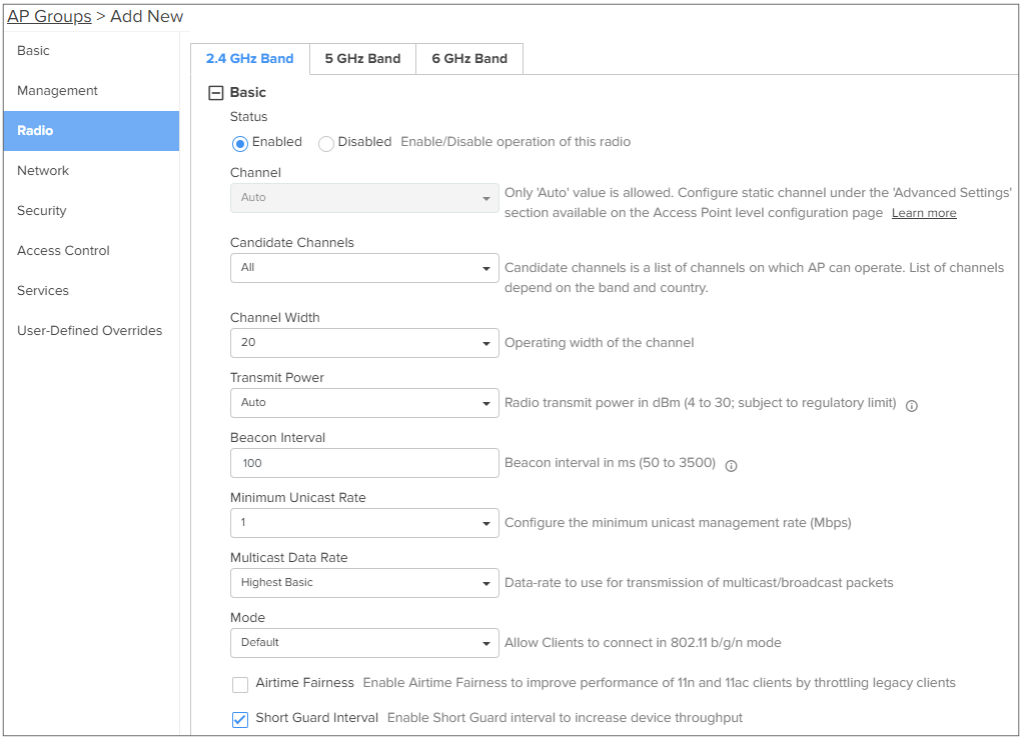
5. Click **Save**.

1. In the **Radio** tab, you can configure **Software Defined Radios** for the required **Model** as shown in Table 66.

   Enterprise Wi-Fi (E-Series, XE/XV/X7-Series) devices can be configured with radio features for 2.4 GHz, 5 GHz, and 6 GHz radio bands.

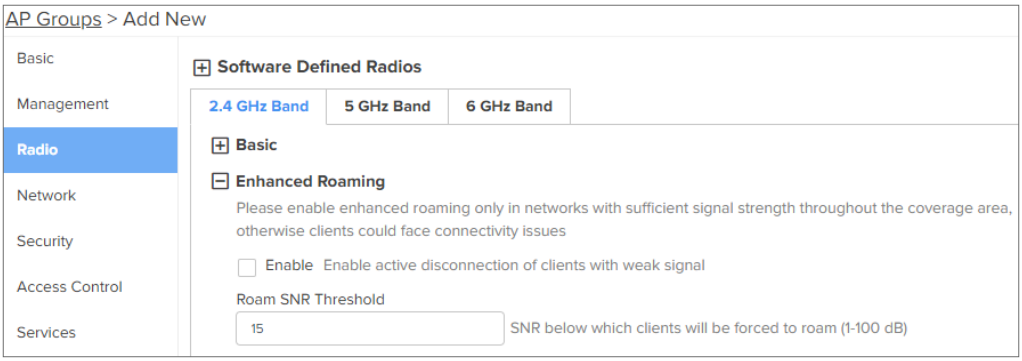
2. Expand the **Basic** section, select either **Enable** or **Disable** option to enable or disable the radio.
3. Select **Auto** in the **Channel** drop-down.
4. In the **Candidates Channel** select **All.**
5. Select the parameter values from the drop-down for the following fields:.
   - Channel Width
   - Transmit Power
   - Beacon Interval
   - Minimum Unicast Rate
   - Multicast Data Rate
   - Mode

Figure 311 *Radio page - Basic section*



6. Expand the **Enhanced Roaming** section and select the **Enable** check box to enable enhanced roaming.

   Configure the threshold value (in dB) in the **Roam SNR Threshold** field.

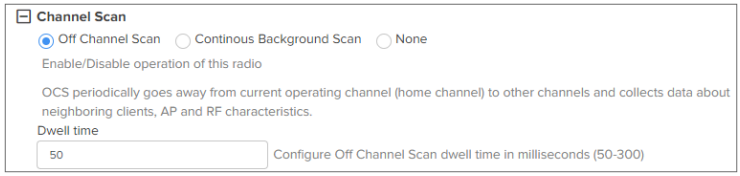


Note

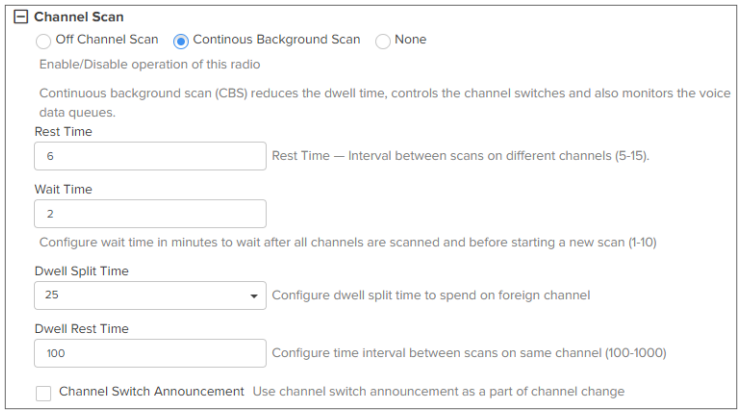
Enable **Enhanced Roaming** only in networks with sufficient signal strength throughout the coverage area, otherwise clients could face connectivity issues.

7. Expand the **Channel Scan** section and select one of the following options to enable the feature and configure corresponding parameters:

   - Off Channel Scan (OCS)



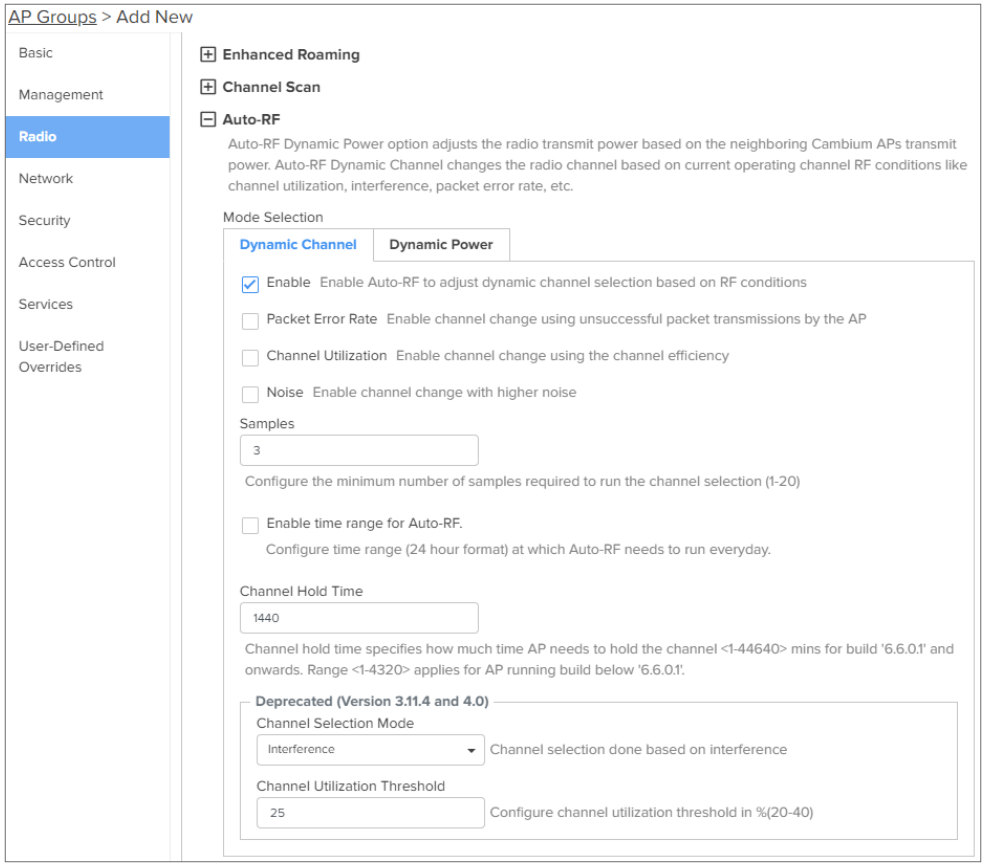
   - Continuous Background Scan (CBS)



   - None—Select this option if no channel scan is needed.

8. Expand the **Auto-RF** section and configure any of the following modes:

- **Dynamic Channel**



Note

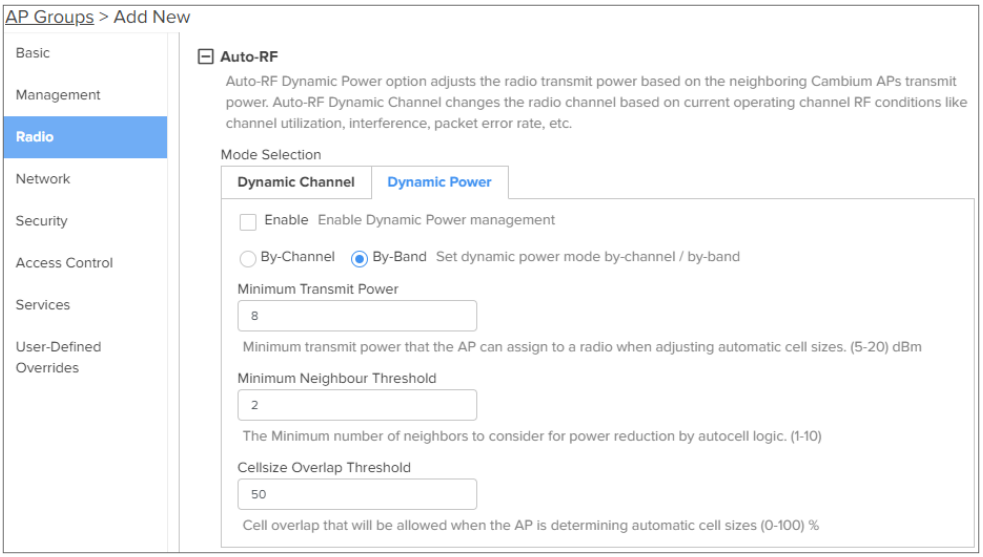
The **Channel Hold Time** parameter specifies the time (in minutes) for which the AP will hold the channel.

The supported values vary as per the AP firmware version installed:

- 1-44640 minutes for APs running version 6.6.0.1 and later.
- 1-4320 minutes for APs running versions earlier than 6.6.0.1.

Default value: 1440 minutes

- **Dynamic Power**



9. Click **Save**.

External Antennas

This feature allows users to customize the antenna models for each of the three radios in the XE3-4TN AP as shown in Figure 312. This customization helps in achieving optimal wireless network performance customized for specific deployment scenarios.

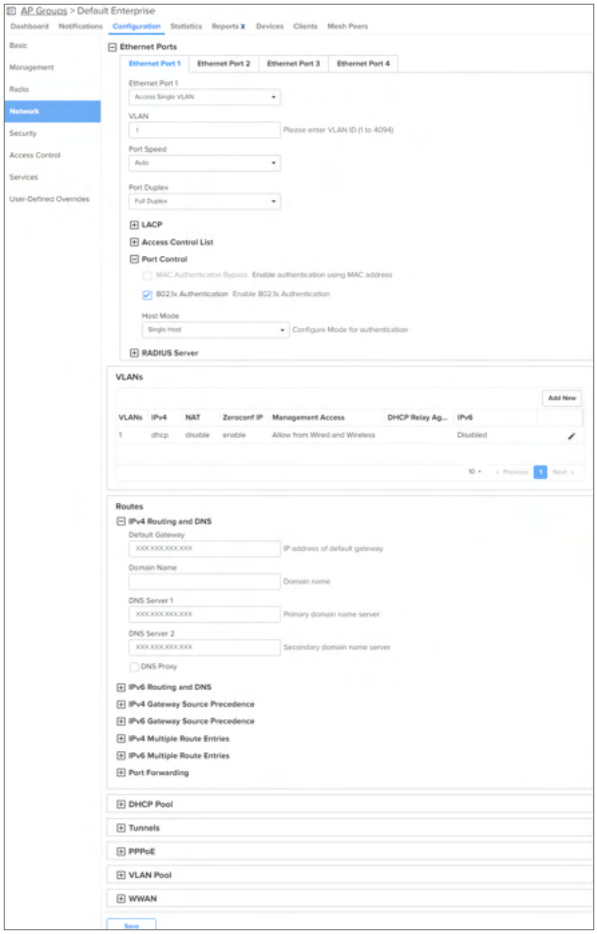
Figure 312 *External Antennas for XE3-4TN APs*



Network

The **Network** page allows to configure **Ethernet Ports**, **VLANs**, **Routes** for IPv4 and IPv6, **DHCP Pool, Tunnels, PPPoE , VLAN Pool,** and **WWAN**.

Figure 313 *Network: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*



Configuring 802.1X port-based authentication

802.1X authentication on Ethernet ports enhance the network security of the AP.

The AP supports 802.1X port-based authentication with the following authentication modes:

- Single-host authentication—Only one client is allowed to access the network after successful 802.1X port-based authentication. After successful authentication, the port VLAN is assigned based on RADIUS assigned VLAN.
- Multi-host authentication—Authentication is enforced on all clients connecting to the wired port. After the first client authenticates, the port VLAN is assigned based on RADIUS assigned VLAN. Any further client connections to the port will be part of the initial Radius VLAN that was assigned.

Note

- By default, the 802.1X port-based authentication feature is enabled in the single-host authentication mode.
- 802.1X port-based authentication does not support CoA messages.

802.1X port-based authentication also requires a RADIUS AAA server for authentication and accounting.

To configure 802.1X, complete the following steps:

1. Navigate to **Configuration** > **Network** > **Ethernet Ports**.
2. Expand the **Port Control** section and select the **802.1x Authentication** check box.

The **Host Mode** field is enabled.

3. Select from the following authentication modes in the **Host Mode** drop-down list.
   - Single Host
   - Multi Host
4. Expand the **RADIUS Server** section and configure the RADIUS server parameters for 802.1X authentication.

   Table 68 *RADIUS Server parameters*

Parameters	Description	Range	Default
Authentication Server	Specifies the authentication server details, such as: • **Host**—IPv4 or IPv6 address or hostname of the server • **Secret**—Text string that is used to encrypt data in RADIUS packets shared between the AP and the sever. Format—Text string • **Port**—Port number of the authentication server. Default—1812 A maximum of three RADIUS authentication servers can be configured.	-	Disabled
Accounting Server	Specifies the accounting server details, such as: • **Host**—IPv4 or IPv6 address or hostname of the server • **Secret**—Text string that is used to encrypt data in RADIUS packets shared between the AP and the sever. Format—Text string • **Port**—Port number of the accounting server. Default—1813 A maximum of three RADIUS accounting servers can be configured.	-	Disabled
Timeout	Time (in seconds) to wait for a response from the RADIUS server.	1–30	3
Attempts	Number of retry attempts for contacting the RADIUS server.	1–3	1
Accounting Mode	Specifies the accounting mode to be used. The following modes are supported: • **Start-Stop**—Accounting packets are transmitted by APs to the AAA server when a wireless client is connected and when the client disconnects. • **Start-Interim-Stop**—Accounting packets are transmitted by APs to the AAA server when a wireless client connects, then at regular intervals (configured in the **Interim Update Interval** field) and also when the client disconnects. • **None**—Disables the accounting mode. This is the default mode.	-	**None** (Disabled)
Server Pool Mode	Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode.	-	Failover

Parameters	Description	Range	Default
	• **Load Balance**—AP equally distributes the requests between the configured RADIUS servers, • **Failover**—AP selects the RADIUS server that is functional based on the order of configuration.		
Interim update interval	Time (in seconds) to wait for sending RADIUS interim accounting update packets. **Note**: This interval is applicable only when you select the **Start-Interim-Stop** option in the **Accounting Mode** parameter.	10-65535	1800
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Enabled

IPv6 Support

IPv6 enables the next generation of large-scale IP networks by supporting addresses that are 128 bits long.

Note

- In the current release, IPv6 functionality is supported only for cnPilot Enterprise devices.
- IPv6 functionality is supported on cnPilot from System Release 4.0.

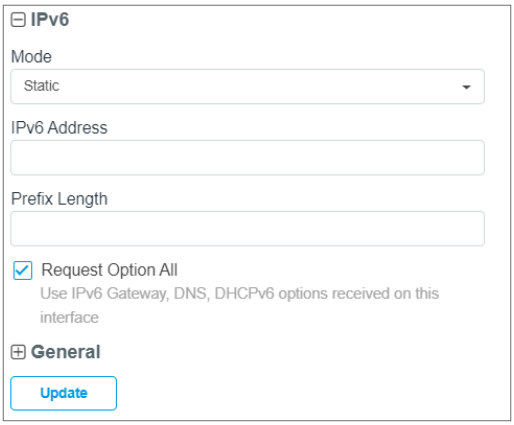
Configuring IPv6

To configure IPv6, perform the following:

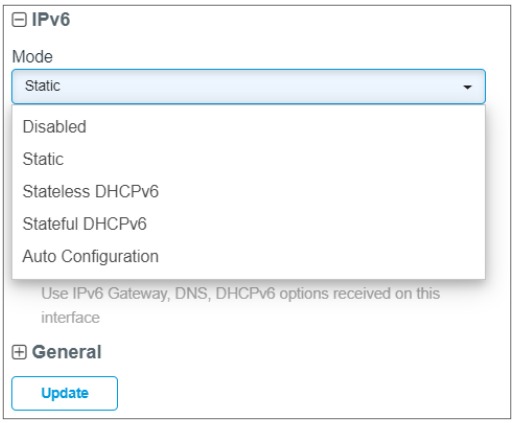
1. Navigate to **Configuration Wi-Fi Profiles** > **AP Groups** tab.
2. Select **Network** tab and click **Edit VLAN**.



3. Click the (+) plus sign next to **IPv6** option.



4. Select **Mode** from drop-down list. By default, the IPv6 Mode is **Disabled**. The different IPv6 modes are **Static**, **Stateless DHCPv6**, **Stateful DHCPv6**, and **Auto Configuration**.



If **Static** is selected, provide the following details:

- **IPv6 Address**: Enter IPv6 address.
- **Prefix Length**: Enter IPv6 prefix. For example: 2001:1111:2222:3333::/64.

5. Enable **Request Option All** to use the IPv6 Gateway, DNS, DHCPv6 options received on this interface.

   By default the priority of **IPv6 Gateway Source Precedence** is **Static** and then **Auto-config/DHCPv6**.

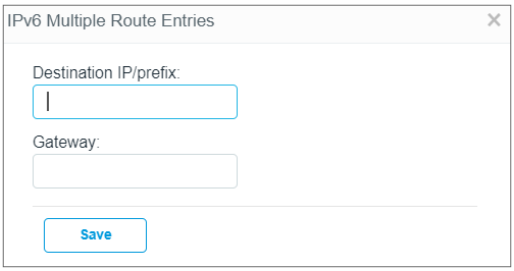


To create a new static Route,

1. Navigate to **IPv6 Multiple Route Entries** section.
2. Click **Add New.**



3. Enter **Destination IP/Prefix** and **Gateway**.



4. Click **Save**.

To set the preference of IPv4 and IPv6:

1. Navigate to **Routes** tab.
2. Select the **IPv6 Preference** checkbox.



Security

The **Security** page allows to configure **DoS Protection** and **Rogue AP**.

Map WLANs to AP Groups

WLANs are added in the AP Group configuration. Ensure the WLANs are ordered correctly if Mesh mode is used. When a WLAN uses Mesh Client mode it must always be the first WLAN in the AP Group, and only one Mesh Client WLAN is allowed per AP Group.

The ordering when using Mesh mode is as follows:

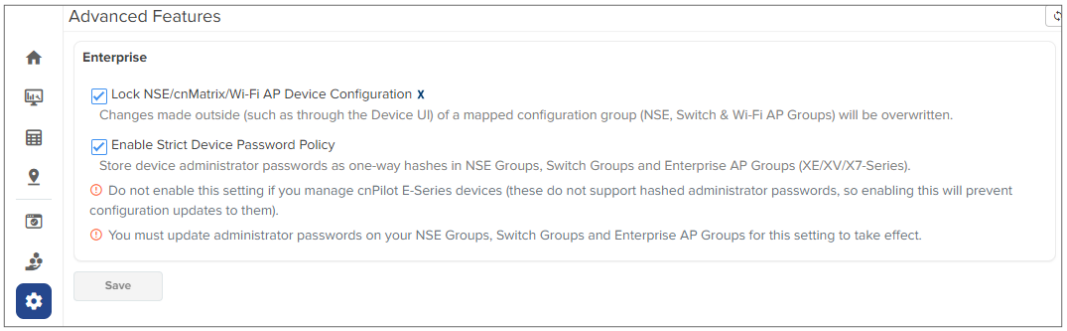
1. Client (maximum of one Mesh Client is selected)
2. Base (maximum of two Mesh Base is selected)
3. Recovery (maximum of one Mesh Recovery is selected)
4. WLANs with Mesh Mode Off (total WLAN limit including Mesh WLANs)

Note

Maximum of 16 WLAN policies are supported for E-Series and XV-Series devices. Only one WLAN is available for cnPilot Home devices.

Lock device Configuration

Locking automatically restores the configuration of devices if it is changed outside of cnMaestro. When this feature is enabled, external configuration changes are automatically reverted by reapplying the AP Group configuration. The configuration is pushed only if the device is in Sync status.

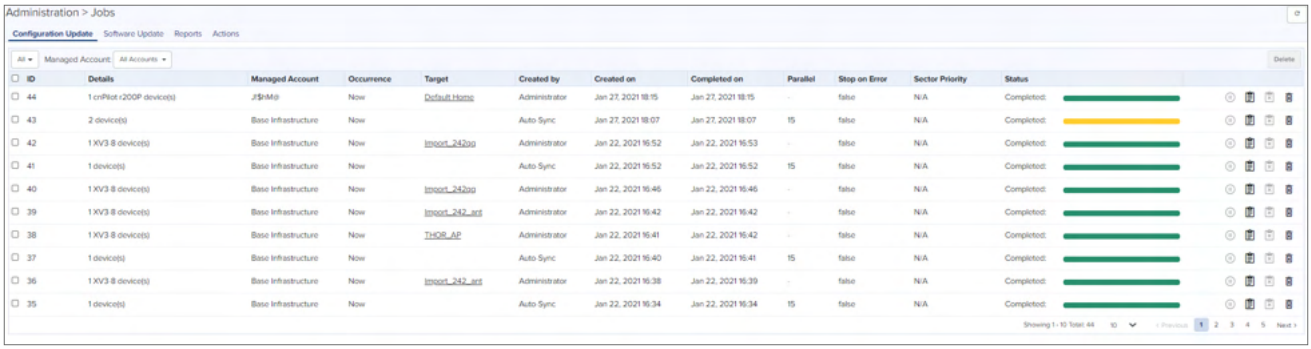


To enable this feature, perform the following steps:

1. Navigate to **Configuration** > **Advanced Features** page.
2. Select the **Lock cnPilot/cnMatrix device Configuration** checkbox.
3. Click **Save**.

When a configuration change is made on the device using UI or CLI, cnMaestro detects the change and the device is marked **Not In Sync**. In this scenario, an **Auto-Sync** job is triggered to automatically revert the changes.

The **Auto-Sync** job can be viewed in **Administration** > **Jobs** > **Configuration Update** page.

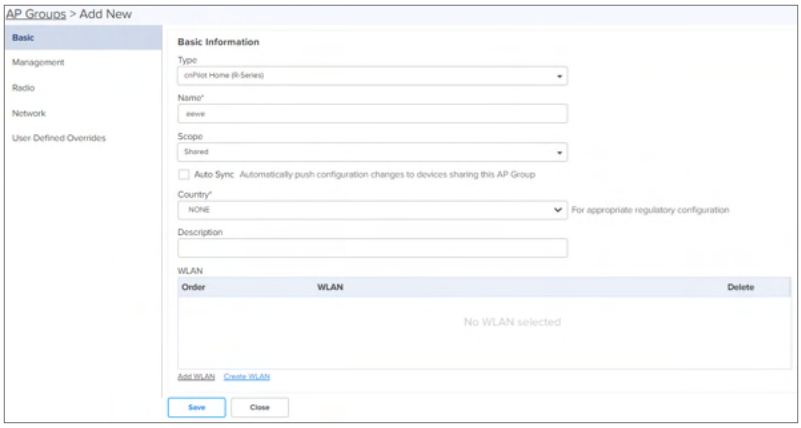


Retry Configure

When the user applies an AP Group to the device, and the Job is skipped because the device is Offline, the reason for the skip will be displayed as **Device was offline** in the **Jobs** page. When device comes up and connects to cnMaestro, an **Auto-Sync** job pushes the AP Group to the device. (It will not apply the AP Group if **Auto-Sync** is disabled in the AP Group).

Note

The Config Update (**Auto-Sync**) will happen only when the **Auto-Sync** option is enabled in the AP Groups page. If the device was Skipped/Failed for any reason other than the **Device was offline**, the device will not be updated.



The default password **admin** of cnPilot R-Series should be changed before upgrading to the build 4.6-RX.



After upgrading to 4.6-RX, the default password **admin** is invalid and needs to be reset through the WAN.

Note

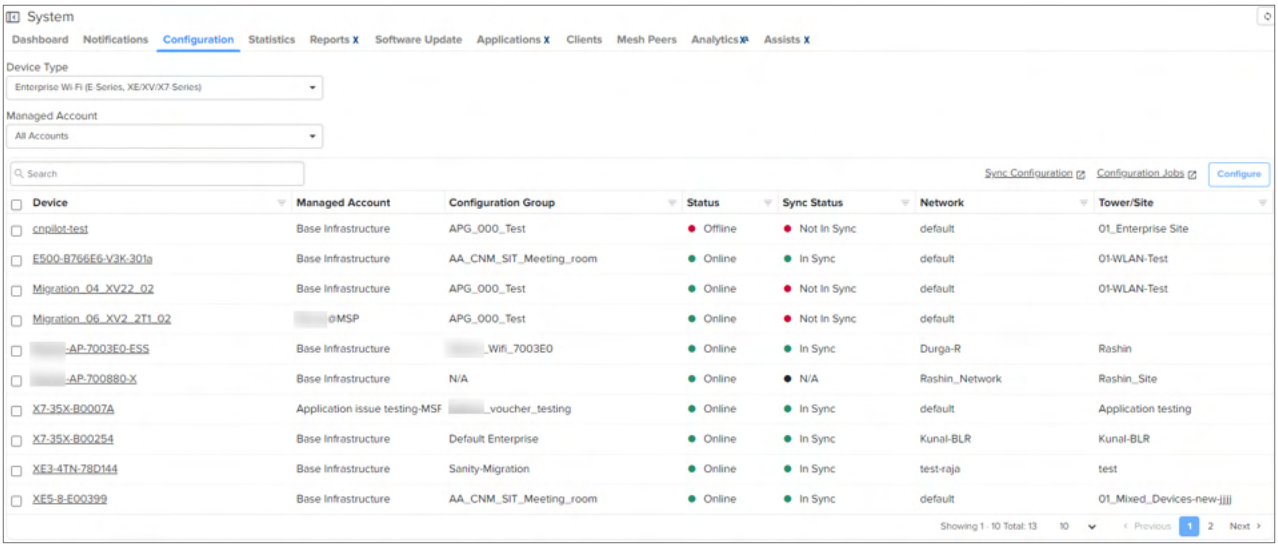
Default User Name: **admin** can be used after the upgrade.

Apply AP Group to Device

A Configuration Job can be created as follows:

1. Navigate to **Monitor and Manage** > **System** > **Configuration**.

   Figure 314 *System Configuration (Enterprise Wi-Fi E-Series, XE,/XV/X7-Series)*



2. Select from one of the following options in the **Device Type** drop-down list:
   - cnPilot Home (R-Series)
   - cnPilot Enterprise (ePMP Hotspot)

- Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
- Enterprise Wi-Fi (Xirrus-Series)
- The list of enterprise Wi-Fi devices are listed.

3. Select the devices to which you want to apply the AP group.
4. Click **Configure**.

   The **System** > **Configuration** page is displayed.

   Figure 315 *Configuration page: Enterprise Wi-Fi (E-Series, XE,/XV/X7-Series)*



   Figure 316 *Configuration page: cnPilot Home (R-Series)*

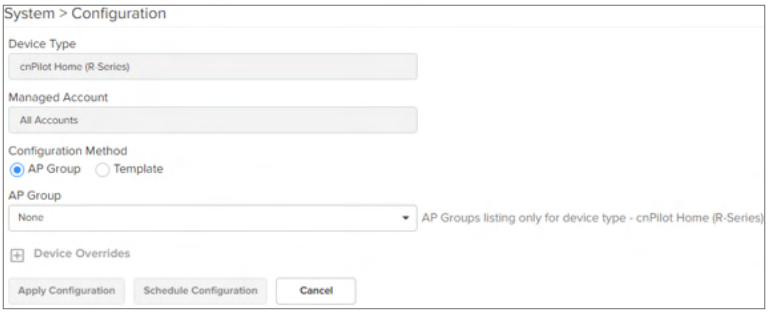
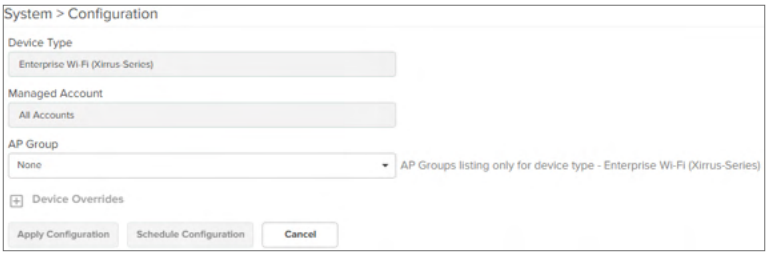


   Figure 317 *Configuration page: Enterprise Wi-Fi (Xirrus-Series)*



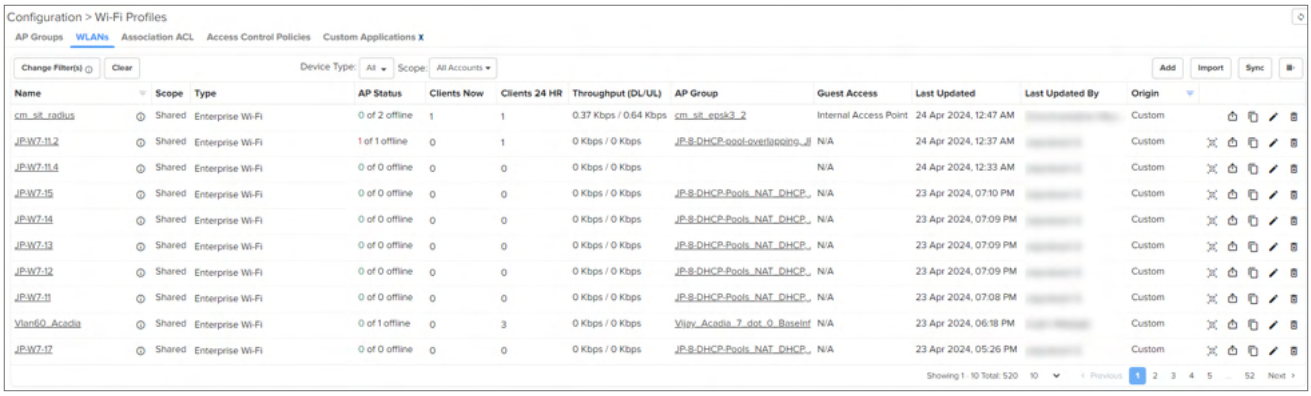
5. Select the AP group from the **AP Group** drop-down list.
6. Click **Apply Configuration.**

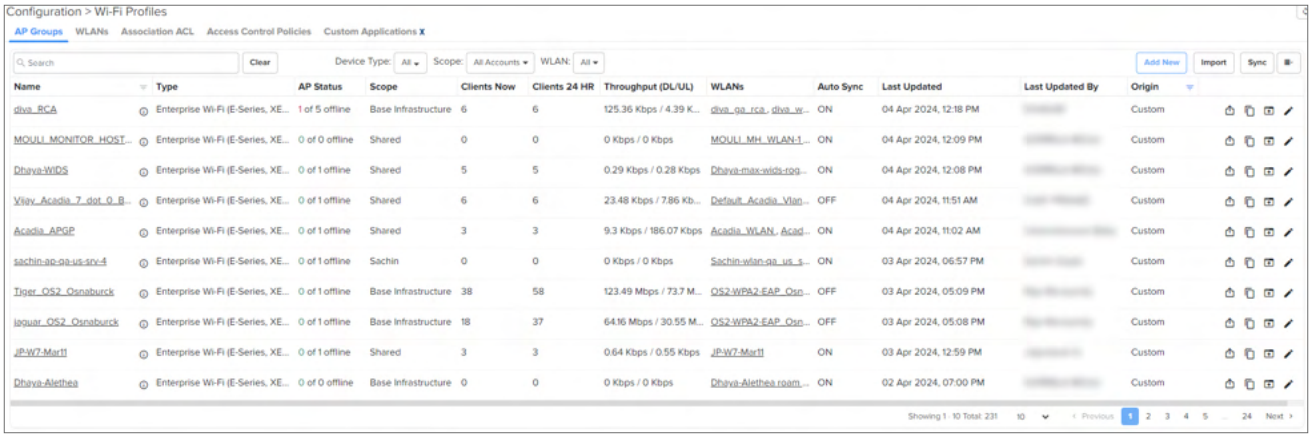
AP Group and WLAN Import/Export

The AP groups and WLANs are created for cnPilot Home and Enterprise Wi-Fi devices. The configurations that are created for each WLAN and AP group in a server can be exported and imported to a different server.

Note

From release 5.1.0, **Built-In** profiles will not be created for MSP accounts and you can create your own profile.





Export AP Groups and WLANs

To export AP Group or WLANs, perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** page.
2. Select **AP Group** or **WLAN** tab.
3. Click **Export** icon in the row of the AP Group or WLANs to export**.**

Note

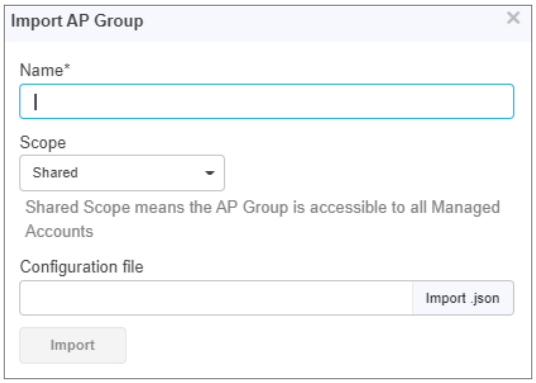
- The AP Groups and WLANs should be exported separately as the associated WLANs are not included while exporting an AP Group.
- The AP Groups and WLANs will be exported with proper name and timestamp.

Import AP Groups and WLANs

To import AP Group and WLANs, perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** page.
2. Select **AP Group** or **WLAN** tab.
3. Click **Import.**

Import AP Group window appears.



1. Enter the **Name.**
2. Select the **Scope** from drop-down.
3. Select the **Configuration file** in JSON format.
4. Click **Import**.

Note

- To import an AP Group, ensure all associated WLANs in the AP Group are already imported. If the WLAN associated with the AP Group is unavailable, an error message will be displayed during import.
- If the name is not provided for WLAN or AP Group while importing, it will take the name of the imported file.
- If the name provided for the AP Group/WLAN is already in use, an error message **The specified policy name already exists** will be displayed.

Creating a WLAN

To create a WLAN, perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** > **WLAN** tab,or WLAN page in the Wireless LAN View.
2. In **WLAN** tab select **New**.

As with AP Groups, WLANs are separated into cnPilot Home and Enterprise Wi-Fi. You can configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters with Enterprise Wi-Fi WLANs. With the cnPilot Home WLANs, you can configure SSID, Scheduled Access, and Access parameters.

Note

The special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z_-*&%#@!<>.() []^~`$1234567890). The user can also rename them if required.

To create a WLAN, perform the following steps:

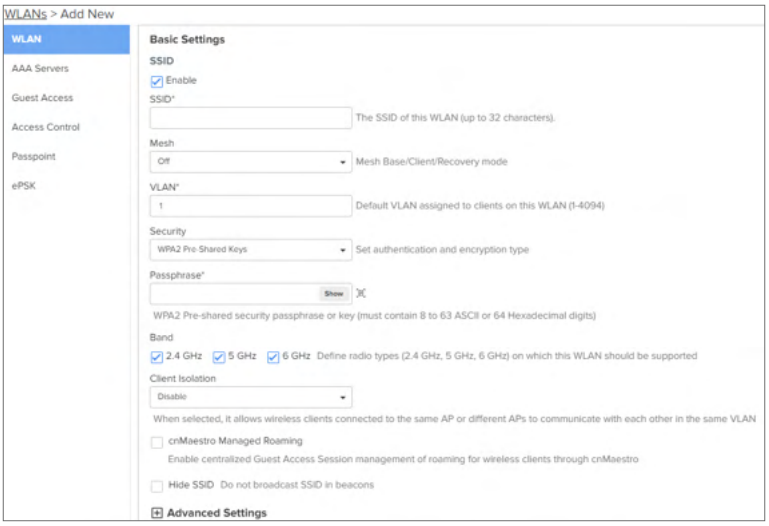
1. Navigate to **Configuration** > **Wi-Fi Profiles**.
2. Select **WLANs** tab and then click **Add**.
3. Enter **Type, Name**, and WLAN parameters.
4. Ensure **WPA2 PSK** is enabled in **Security** drop-down.

Note

To support ePSK with WPA3, you must select either the **WPA2/WPA3 Pre-shared Keys** or **WPA3**

Pre-shared Keys option in the **Security** drop-down list, and configure ePSK passphrase.

For information on client (WPA2 and WPA3-compliant) registration with ePSK passphrase, see ePSK registration for WPA3 clients.



5. Click **Save**.

Note

In 6 GHz Band, **Open** option is not supported in **Security**.

ePSK registration for WPA3 clients

For the ePSK feature, when you configure WPA3-WPA2 (mixed mode)-PSK or WPA3-PSK as the WLAN security, the clients connection in the WPA3 mode must go through an additional registration phase. This is different from the flow when you configure WPA2-PSK as the WLAN security, where users can authenticate by using only a passphrase.

When clients use WPA3-PSK security, Simultaneous Authentication of Equals (SAE) is the authentication mechanism. Here an extra authentication is added, which is more secure than WPA2. For WPA2-PSK clients, the passphrase is matched against a database to identify the user. However, this is not possible for WPA3-PSK clients because of the extra authentication in WPA3-SAE. When WPA2-PSK security is used, the Pairwise Master Key (PMK) is the same for every connection made by the client. This is due to the underlying weaknesses in WPA2-PSK, which make it easier to validate the passphrase. In contrast, when WPA3-PSK security is used, a new PMK is generated each time a client joins the network. Therefore, registration will help us to know the passphrase upfront when a client tries to connect. This mandates the users to register themselves with the ePSK passphrase to bind the client MAC with the passphrase to successfully connect to the Wi-Fi network.

For WPA3 clients to connect to the network using ePSK flow:

1. First connect to the WLAN with the WLAN passphrase.

   A simple password is recommended to be configured, for example, `signmeup`, or any other appropriate passphrase.

2. Register themselves with the WPA3-ePSK unique passphrase.

   After the MAC binding is complete, users can use the WPA3-ePSK unique passphrase for subsequent WLAN connections.

This section describes the following topics:

- ePSK with WPA3 feature recommendations
- Scenarios while registering clients
- Configuring ePSK registration for WPA3 clients
- Registration flow screenshots
- Recommended best practices

ePSK with WPA3 feature recommendations

The following are the recommendations for this feature:

- This feature is supported only on cnMaestro Cloud 5.1.0 onwards.
- Supported AP firmware version is 6.6.1 or 7.0 and above.
- Security mode must be configured to either **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys**.
- APs must be managed from cnMaestro Cloud for client registration.
- The WLAN VLAN must be able to provide DHCP to clients and must have internet connectivity.
- This feature is not supported on Enterprise Wi-Fi 5 APs and Xirrus APs.

Scenarios while registering clients

When a client connects to the WLAN, the following scenarios are possible:

- When a client connects for the first time using WPA2 security and ePSK passphrase (either on 2.4 GHz or 5 GHz radios), the AP performs an ePSK lookup. The following are the outcome:
  - If a match is found, the MAC binding is created with the respective ePSK key.

    AP shares this MAC binding information with the other APs in the network.
  - If a match is not found, the connection fails.
- If the WPA2 client is connected using the WLAN passphrase, client registration steps are performed to bind the passphrase to the client.
- When a client connects for the first time using WPA3 security, the following two possibilities may occur:
  1. If MAC binding is not available for the client on the AP, the following procedure must be completed for successful registration of clients:
     a. User must authenticate using the configured WLAN passphrase, for example, `signmeup`.

        If the user tries to sign in with some other password other than the configured WLAN password (`signmeup`), the connection fails.

     b. If the connection with the configured password (`signmeup`) is successful, the AP redirects the client to the registration page.

        This is the only traffic allowed for the client with this WLAN passphrase.

     c. User must now enter the configured ePSK passphrase and register.

        The AP redirects the client to the registration page with instructions.

     d. Users must select the checkbox after reading the instructions (provided for different clients, such as Android, Windows, and iOS), and then disconnect from the network.

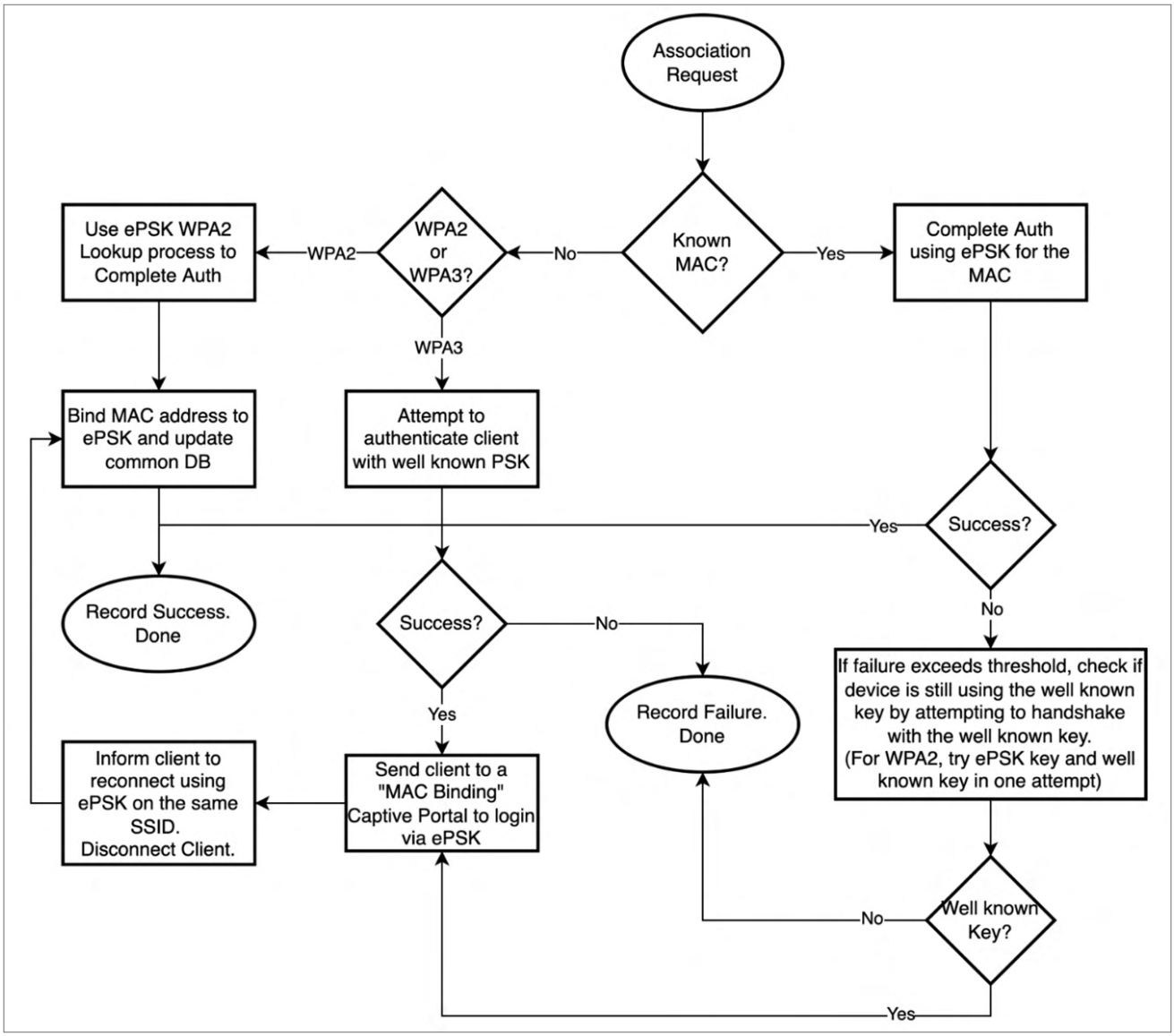
e. User must forget the WLAN/SSID and reconfigure using the ePSK passphrase.

User then reconnects with ePSK passphrase and gets authenticated.

For a more detailed information, see Registration flow screenshots.

2. When MAC binding is available for the client on the AP, users can authenticate the client with the passphrase present in the MAC binding, that is the ePSK passphrase.

Figure 318 *Client registration flow for WPA3 clients*



Configuring ePSK registration for WPA3 clients

To enable WPA3-ePSK registration, you must create a WLAN profile and add ePSK entries in the ePSK grid.

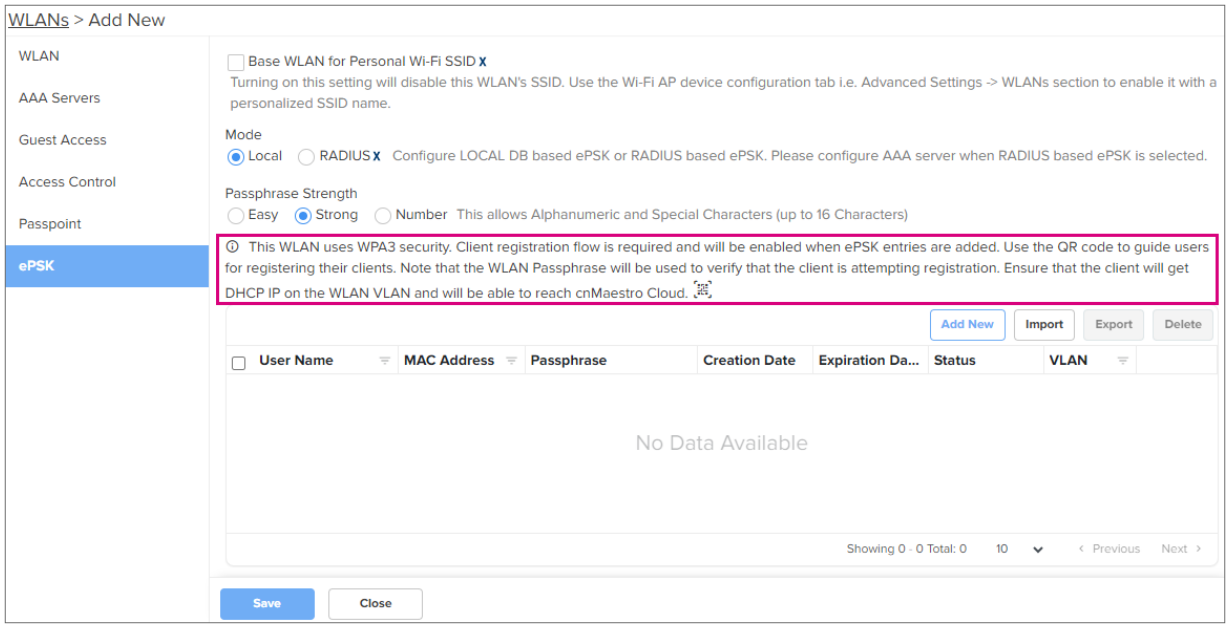
To create WLAN profile and add ePSK entries, complete the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** page.
2. Select **WLANs** tab and click **Add**.
3. Select **Enterprise Wi-Fi** from the **Type** drop-down list and configure the WLAN parameters.

4. In the **Basic Settings** section, ensure either the **WPA2/WPA3 Pre-shared Keys**or **WPA3 Pre-shared Keys** option is selected in the **Security** drop-down list.
5. Enter the WLAN passphrase.
6. Click **Save**.

- When ePSK passphrase is not configured in the **WLANs** > **ePSK** page, the following message is displayed explaining the registration flow.

Figure 319 *Message on the ePSK page when no ePSK entries are added*



- For existing WLANs where ePSK entries are present and when **WPA2/WPA3 Pre-shared Keys**or **WPA3 Pre-shared Keys** option is selected in the **Security** drop-down list, the following messages appear respectively

Figure 320 *When **WPA3 Pre-shared Keys** option is selected*

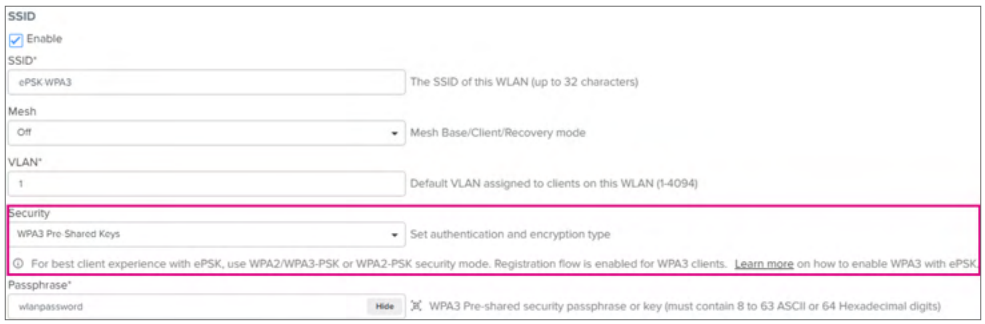
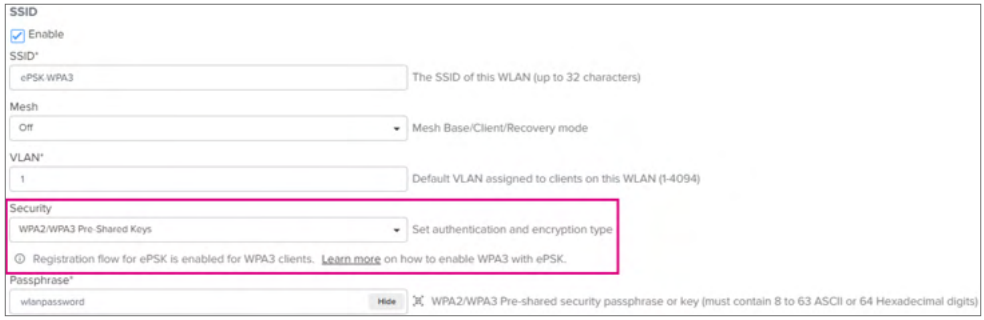


Figure 321 *When **WPA2/WPA3 Pre-shared Keys** option is selected*



7. Click the **ePSK** tab and add the passphrase.

   After the ePSK passphrase is added, the following message is displayed explaining the registration flow.

   Figure 322 *Message on the ePSK page when ePSK entries are added*

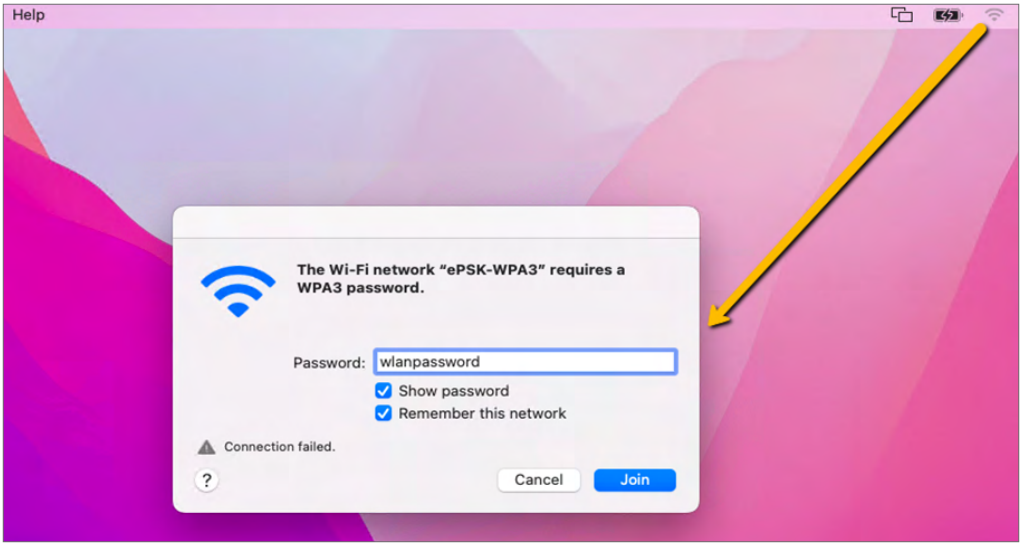


Registration flow screenshots

To register the clients to the network using the ePSK passphrase, users must complete the following steps:

1. Connect the client to the network using the WLAN passphrase.

   Figure 323 *Using WLAN passphrase for connecting to network*

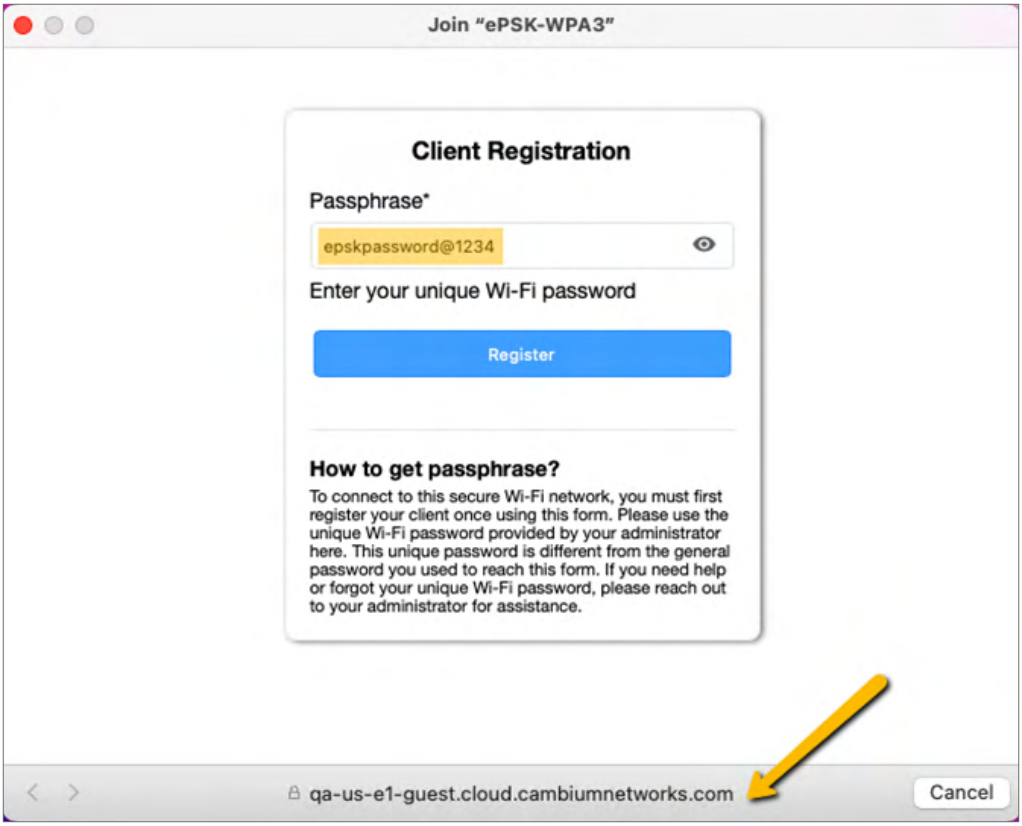


2. Click **Join**.

   Clients are redirected to the **Client Registration** page for providing the ePSK passphrase.

3. Enter the ePSK passphrase in the **Passphrase** field and click **Register**.

Figure 324 *Using ePSK passphrase for connecting*



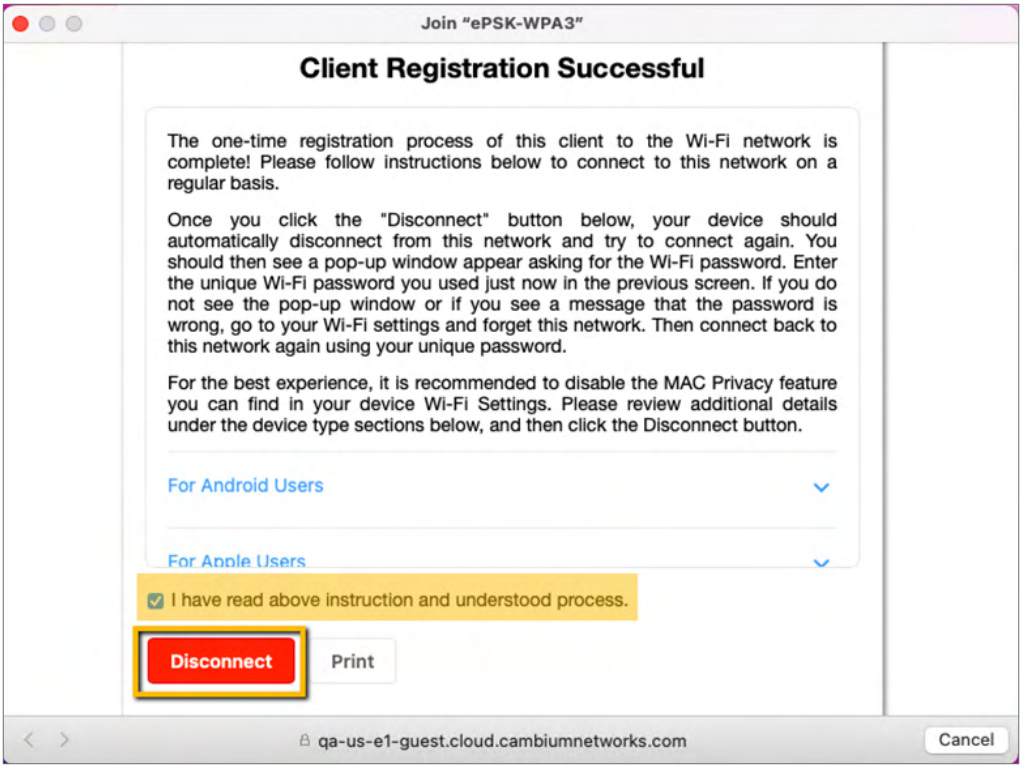
The registration success page is displayed along with a set of instructions.

4. Read the instructions (provided for different devices, such as Android, Windows, and iOS) and select the checkbox for confirmation.

   The instructions provide details of the next steps for different devices.

   The **Disconnect** button is enabled.

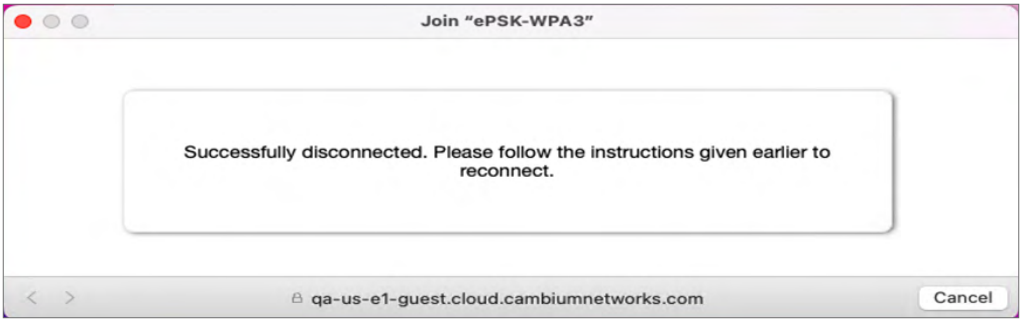
Figure 325 *Registration success page with instructions*



5. Click **Disconnect**.

   The client is disconnected and a disconnect success message is displayed.

   Figure 326 *Disconnect success page*



6. Reconnect to the network using the ePSK passphrase that you provided in the **Client Registration** page earlier.

   The client connects to the network with the mapped VLAN.

Figure 327 *Using ePSK passphrase for connecting to network*



Recommended best practices

Following are some of the best practices you can follow while configuring ePSK registration for WPA3 clients:

- WPA3 PSK is not recommended for unmanaged (BYOD) clients (For example, multi-dwelling unit (MDU), hospitality, and educational institutions).

  In MDUs, with IoT clients, making WPA3 mandatory with a single SSID may not be a successful deployment.
- WPA2/WPA3 PSK is recommended for unmanaged clients and to transition from the current (WPA2-PSK).
- Most of the WPA3-capable clients favor WPA3 PSK when available. This behavior is different among other clients, where some fallback to WPA2 and some which do not.
- When the SSID is mapped to 2.4 GHz and 5 GHz radios, WPA2 PSK or WPA2/WPA3 PSK security is recommended.
- When the SSID is mapped to 2.4 GHz, 5 GHz, and 6 GHz radios, or only the 6 GHz radio, then WPA3 PSK security is recommended.

Creating an ePSK WLAN

To create an ePSK WLAN, perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** or WLAN page in the Wireless LAN View.
2. Select **WLANs** tab and click **Add**.

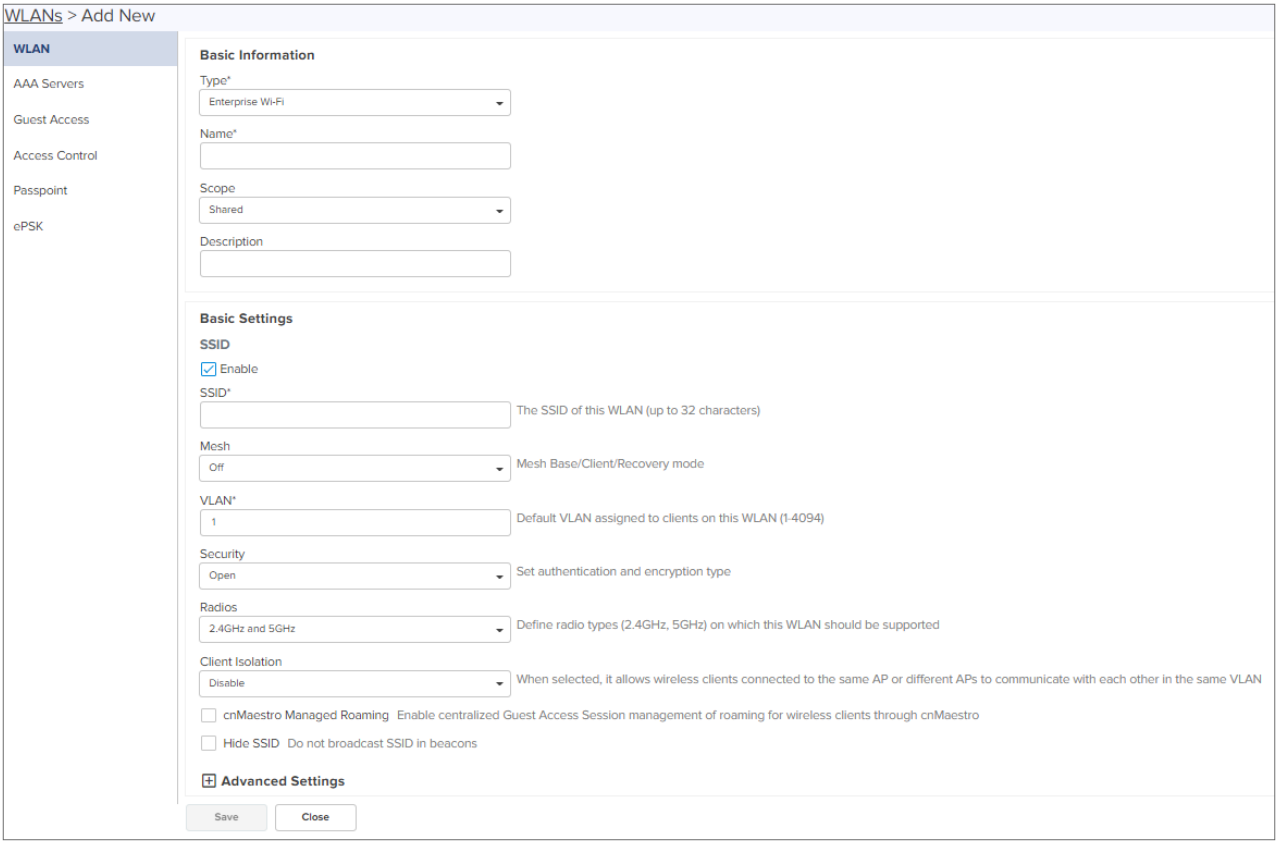
As with AP Groups, WLANs are separated into cnPilot Home and Enterprise Wi-Fi types. You can configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters with Enterprise Wi-Fi WLANs. With the cnPilot Home WLANs, you can configure SSID, Scheduled Access, and Access parameters.

Note

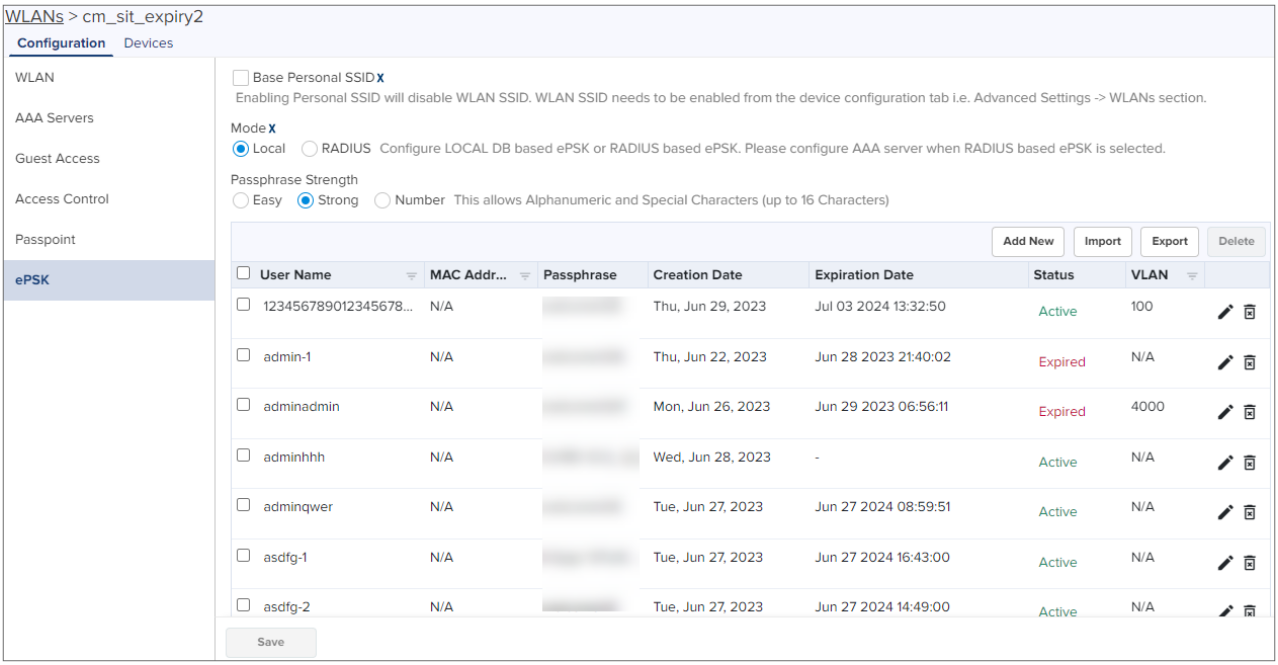
- The special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z_-*&%#@!<>.() []^~`$1234567890). The user can also rename them if required.
- By default, password will not be configured. User has to configure the password for WLAN.

To create WLAN policy, perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles**.
2. Select **WLAN** tab and click **Add**.
3. Select **Enterprise Wi-Fi** from the **Type** drop-down list and enter details in the **Basic Information** section.
4. In the **Basic Settings** section, ensure the **WPA2 Pre-Shared Keys** option is selected in the **Security** drop-down list.



5. Click **Save**.
6. In the **ePSK** page select the type of passphrase strength in the **Passphrase Strength** field (Available options: **Easy**, **Strong**, or **Number**).

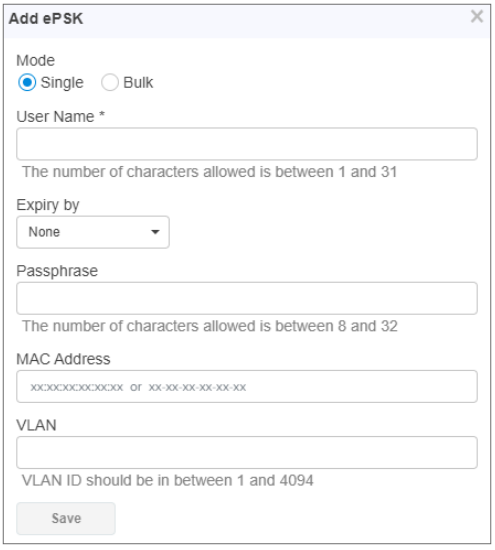


7. Click **Add New**.

   The **Add ePSK** window is displayed.

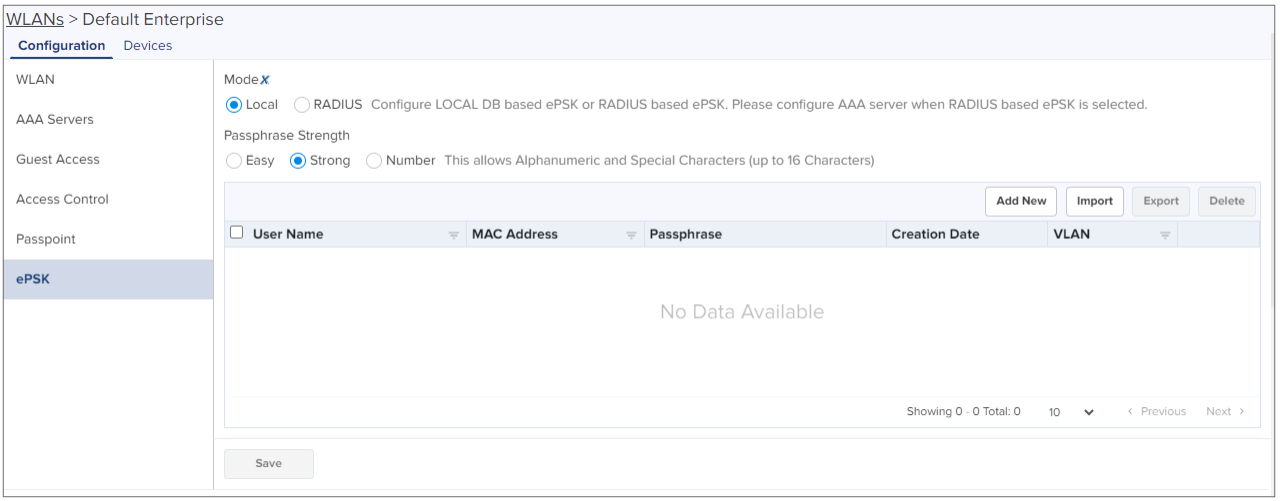
8. Select **Mode** type as one of the following:

   - **Single**: In the Single mode, only the **User Name** is mandatory and rest of the entries are optional. There is only one entry in this mode.

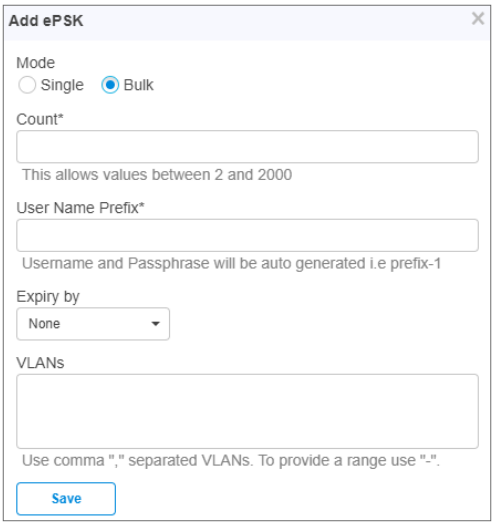


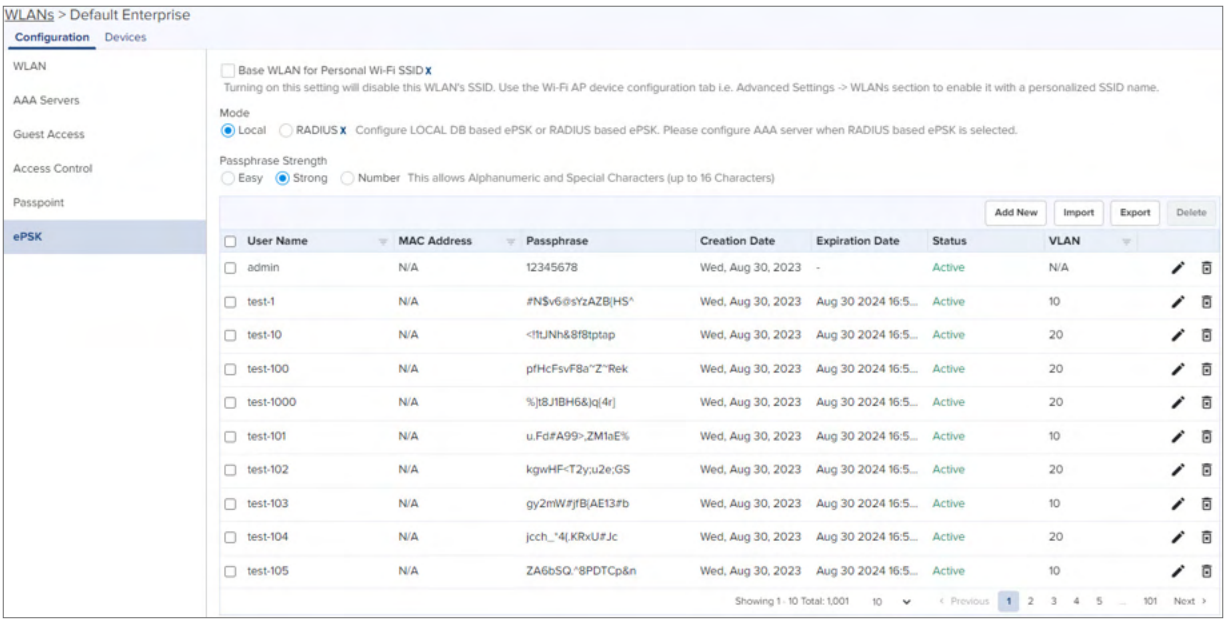
Note

Passphrase is optional and unless manually configured, it will be automatically generated based on the selected **Passphrase Strength**.



- In the **Bulk** mode, the **Count** and **User Name Prefix** are mandatory. There are multiple entries in this mode.





9. To automatically expire ePSK details after a specific duration. The following options are available:

- **None**—ePSK details never expire. Select **None** to never expire the ePSK credentials.
- **Date and Time**— ePSK expires after the specified date and time (in dd/mm/yyyy hh:mm AM/PM format)

  Supported minimum time is 12 A.M. on the next day and the maximum is five years.
- **Duration**— ePSK expires after the specified (in hours, days, months, or years) in the **Expiry by** drop-down.

  Supported minimum duration is one hour and the maximum is five years. No decimal values are supported, for example, 1.5 hours.



Note

- The configured expiry time appears in the **Expiration Date** column on the **WLANs** > <WLAN name> page.
- The **Status** column on the **WLANs** > <WLAN name> page displays the status of the ePSK details—**Active**, **Expired**, or **None**. **None** is displayed only when older ePSK keys are imported to cnMaestro.
- Expired ePSK details are deleted from the AP only when the next configuration sync functionality is initiated or when there is a configuration change in the AP.

Creating a Personal Wi-Fi ePSK X

In Multiple Dwelling Units (MDU), personal Wi-Fi allows a user to connect all the personal devices to a unique SSID associated with a VLAN. For example, a user can connect multiple devices to a single personal Wi-Fi.

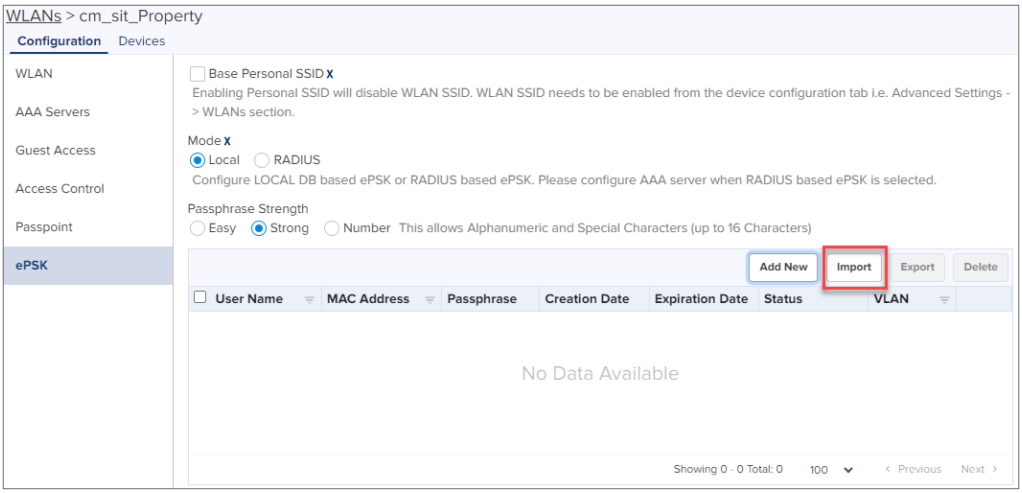
To configure personal Wi-Fi on the AP, complete the following steps:

1. Add and enable the SSID details (to be used as personal Wi-Fi) in the **WLANs** tab, under **Manage and Operation > Networks >** <network name> **> Configuration > Device Configuration > Advanced Settings** section.
   a. Select the **Enable SSID** checkbox.
   b. In the **Passphrase** field, configure the passphrase.
   c. Configure the VLAN with which the SSID must be associated.
2. Enable personal Wi-Fi on the ePSK page for the WLAN profile by selecting the **Base Personal SSID** checkbox.

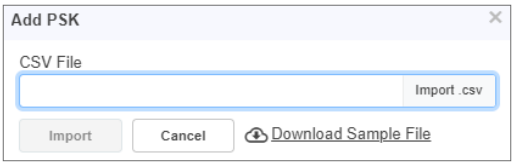
   By default, this feature is disabled. Once enabled, the **Enable** checkbox (under **WLANs > WLAN > Basic Settings > SSID**) is cleared. Also, the local and RADIUS ePSKs are disabled.

Import ePSK

1. Click **Import**.



2. Select **Import.csv** file.



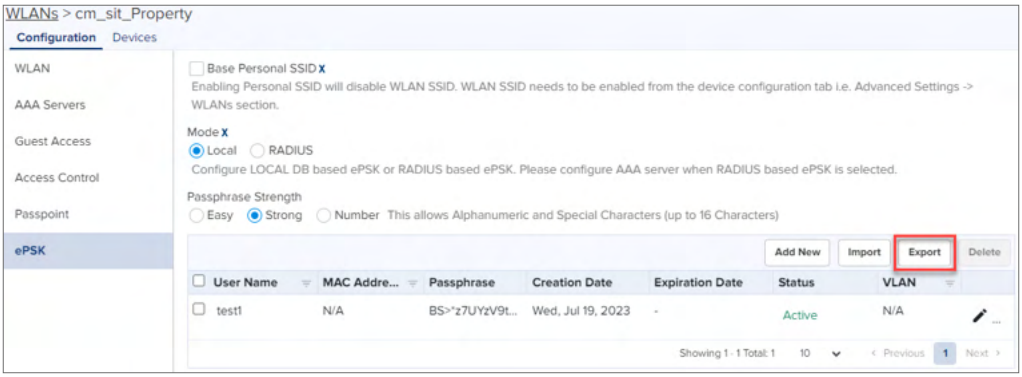
Alternatively, one can import a CSV file containing a list of ePSK entries. A sample file format is available from the Import dialog.

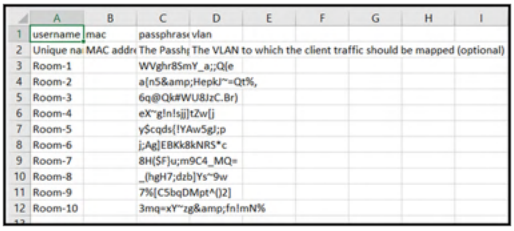
3. Click **Download Sample File**, to view sample ePSK Excel sheet.

	A	B	C	D	E
1	username	mac	passphrase	vlan	expiration_time
2	Unique name of this entry	MAC address of the client,if any (optional)	The Passhprase (Pre Shared Key) to be used in the WPA2 handshake	The VLAN to which the client traffic should be mapped (optional)	Expiration time should be either none or Jun 22 2024 09:07:28 format only
3	Lounge-1	11:11:11:11:11:11	646)hj6ab;^B((;	9	Jun 22 2024 08:34:28
4	Lounge-2	22:22:22:22:22:22	9jdf};q)*38GU53%	10	Aug 22 2024 05:07:28
5	Lounge-3		*({;nQgUdeM2ErR	1	Jul 27 2024 19:07:28
6	Lounge-4		]jJzam4F1)x]Zgg%	2	May 22 2024 12:07:28

Export ePSK

1. Click **Export**.
2. Select **export.csv** file.





	A	B	C	D	E	F	G	H	I
1	username	mac	passphras	vlan					
2	Unique na	MAC addr	The Passhr	The VLAN to which the client traffic should be mapped (optional)					
3	Room-1		WVghr8SmY_a;;Q{e						
4	Room-2		a{n5&HepkJ~=Qt%,						
5	Room-3		6q@Qk#WU8JzC.Br)						
6	Room-4		eX~g!n!sjj]tZw[j						
7	Room-5		y$cqds{!YAw5g];p						
8	Room-6		j;Ag]EBKk8kNRS*c						
9	Room-7		8H($F]u;m9C4_MQ=						
10	Room-8		_{hgH7;dzb]Ys~9w						
11	Room-9		7%[C5bqDMpt^()2]						
12	Room-10		3mq=xY~zg&fn!mN%						

Editing ePSK

To edit an ePSK, select the required ePSK and click the edit ( ) icon in the row.

You can edit only the passphrase and the expiry duration information.

Deleting ePSK

To delete an ePSK, select the required ePSK and click **Delete**. You can also click the delete ( ) icon in the row.

To delete multiple ePSK entries, select the checkboxes corresponding to the ePSK entries and click **Delete**.

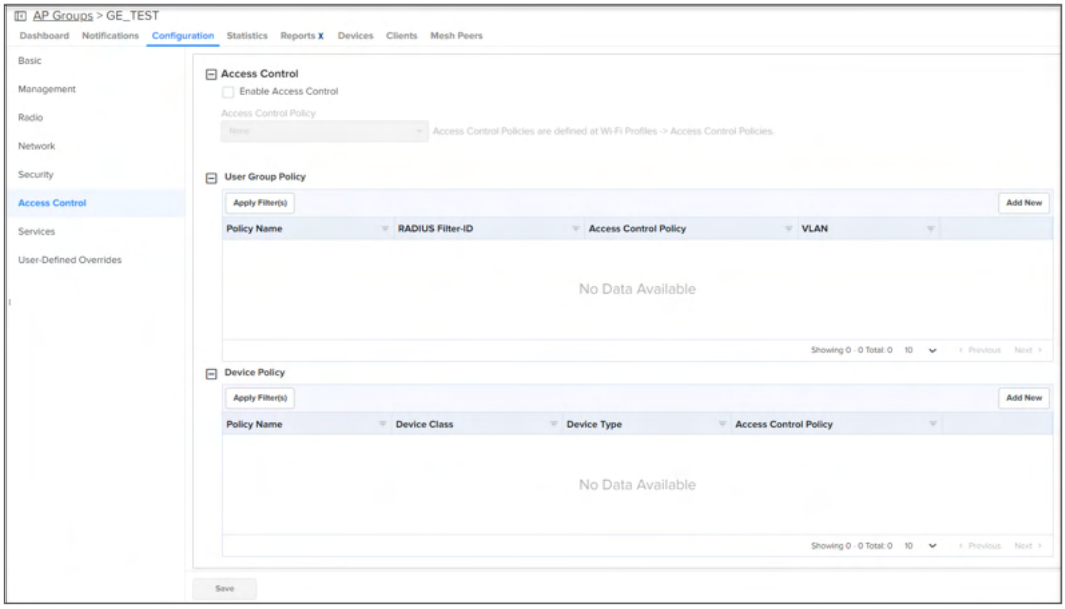
Note

ePSK feature is supported on cnPilot from Release version 3.11.1.

Access Control

The Access Control page allows user to enable or assign access control policies and configure **User Group Policy** and **Device Policy**. It offers visibility into the configured rules, ensuring efficient and secure network management.

Figure 328 *Access Control page*



Note

If an Access Control Policy is assigned at the AP group level, it does not appear under User Group or Device Group policies.

Enable Access Control Policy

Users have the provision to enable or disable access control policies under **Access Control** tab as shown in Figure 329.

Figure 329 *Enabling Access Control Policy*



Note

User can select the available access control policies listed in Wi-Fi profiles in **Access Control Policy** drop-down list. User can review the configured rules associated with these policies by clicking **View Rule** icon as shown in Figure 329. This provides a comprehensive view of the policies and rules within the network.

User Group Policy

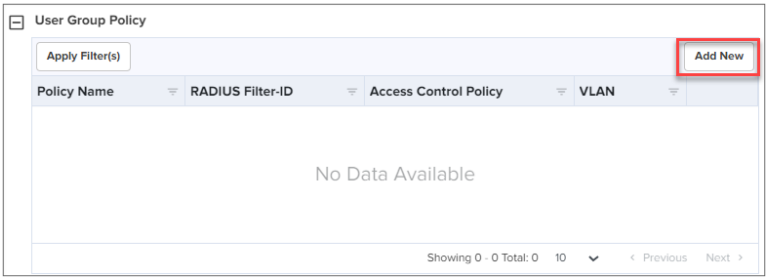
User Group Policy enables users to categorize into specific roles with customized access permissions and restrictions, facilitating fine-tuned control over network access.

Adding a new User Group Policy

To add a new User Group Policy, perform the following steps:

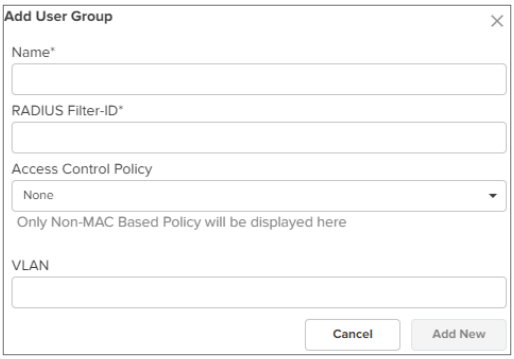
1. Navigate to **Configuration** > **Access Control** page.
2. Click **Add New** in the top right corner of the User Group Policy as shown in Figure 330.

Figure 330 *User Group Policy*



3. Complete the details in the **Add User Group** pop-up window as shown in Figure 331.

Figure 331 *Add User Group*



Note

- The user needs to assign an Access Control Policy or VLAN to create a User Group.
- Users can add a maximum of 64 User Groups and Device Policies each.
- Users can only select Access Control Policies (ACPs) with NON-MAC filters from the **Access Control Policy** drop-down menu.
- Mapping an Access Control Policy (ACP) to a User Group Policy (UGP) enables its use for the AP group, and vice versa. However, the same ACP cannot be shared between UGP and AP group; you can apply it to only either UGP or AP group.

Device Policy

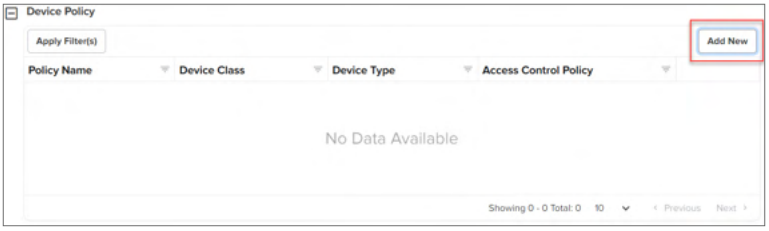
Device Policy allows users to apply specific rules and access control policies based on the type and characteristics of devices, offering customized control over device behavior within the network.

Adding a new Device Policy

To add a new Device Policy, perform the following steps:

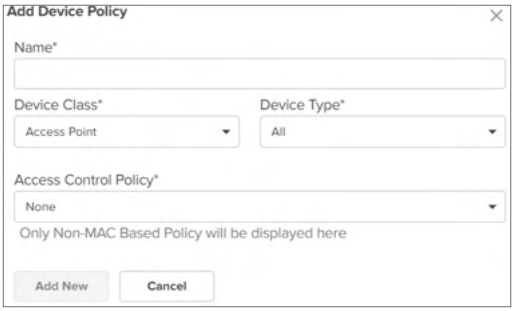
1. Navigate to **Configuration** > **Access Control** page.
2. Click **Add New** in the top right corner of the Device Policy as shown in Figure 332.

Figure 332 *Device Policy*



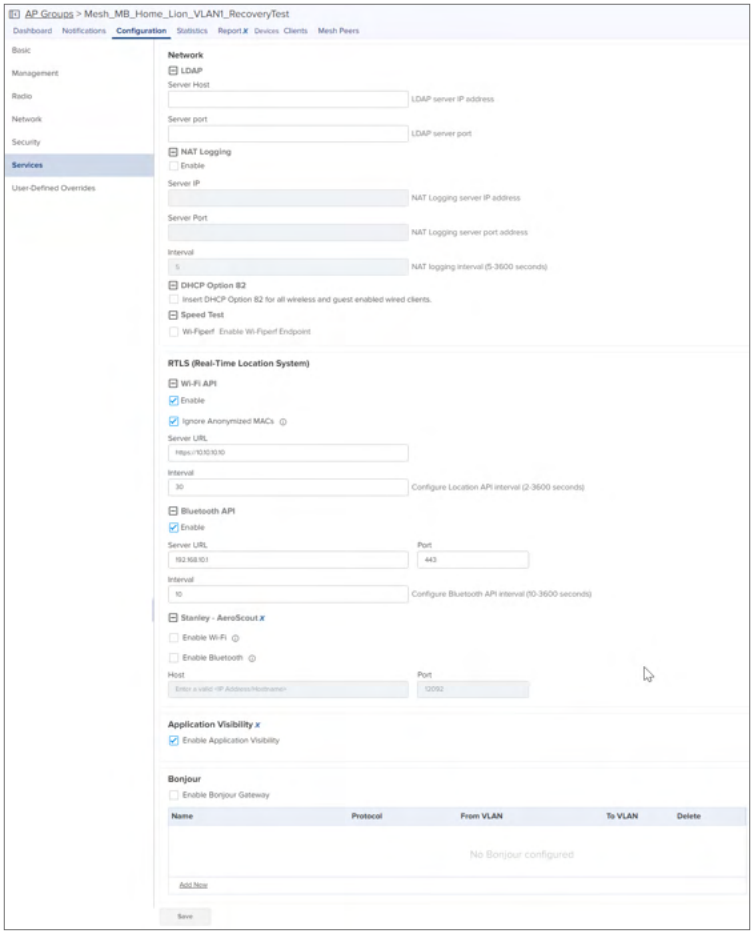
3. Complete the details in the **Add Device Policy** pop-up window as shown in Figure 333.

Figure 333 *Add Device Policy*



Services

The **Services** tab allows to configure the **LDAP, NAT Logging, DHCP Option 82, Speed Test, RTLS (Real-Time Location System)** such as **Wi-Fi API, Bluetooth API, Stanley-AeroScout,** and **Bonjour**.

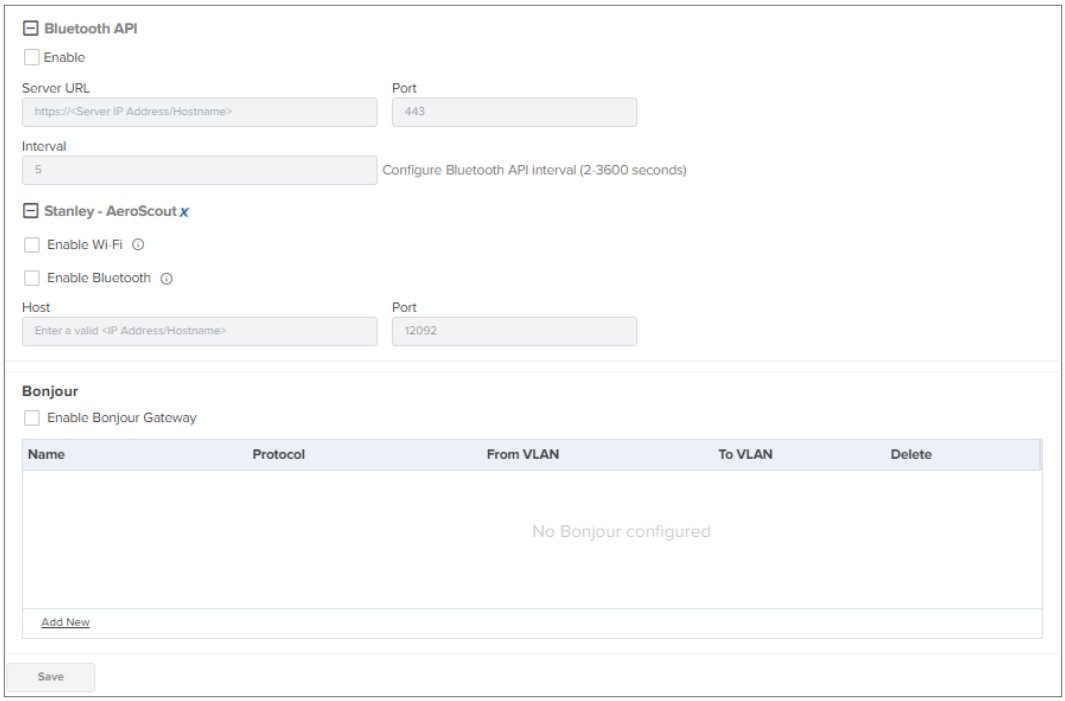


Note

Stanley-AeroScout is supported only for cnMaestro X features.

Stanley-AeroScout

Stanley-AeroScout delivers an accurate and reliable location data for assets and customers with the STANLEY Healthcare Wi-Fi tags. It is an integral component of STANLEY Healthcare's Stanley-AeroScout RTLS solutions. The Stanley-AeroScout determines a location using signal strength measurements (RSSI) which are collected by the Cambium Wi-Fi Access Points. These Wi-Fi Access Points can simultaneously serve location sensors and provides network access. Stanley-AeroScout utilizes a location engine to determine the position of Wi-Fi tags.



Pre-Defined Overrides

Some device configuration is specific to an individual device and not easily shared through an AP Group. This includes IP Address, Radio Channel settings, and WLAN details such as Enabling/Disabling SSID and Passphrase. These items can be configured in the Device Configuration page, which can be selected by choosing **Manage** > **Configuration** in the menu, and then selecting the device in the tree to update.

You can then choose/change different values from AP Group to be overridden. The icon to the left of a field must be selected first to override that parameter. After specifying override parameters, select **Apply Configuration** on the bottom right to save your changes to the server and create a job to push the new values to the device. This option is also applicable for Onboarding process queue.

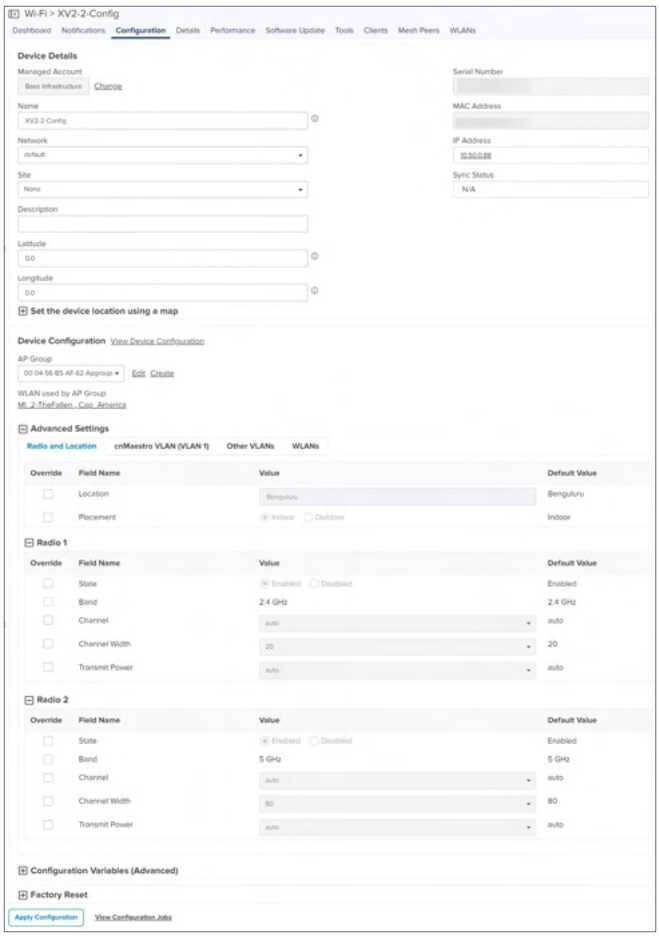
Advanced Settings

By default, Enterprise Wi-Fi devices have **Auto-set from device** enabled. This option reads several network related configuration fields from the device and uses those as override values to prevent overwriting values that would disconnect the device.

Modify the **Advanced Settings** section on the Access Point level configuration page as below:

- Add option to override Dual 5 GHz Radio setting for XV3-8 APs below the Placement field.
- If the Dual 5 GHz Radio feature is **Enabled**, then show the settings to override/configure the 3rd 5 GHz radio.

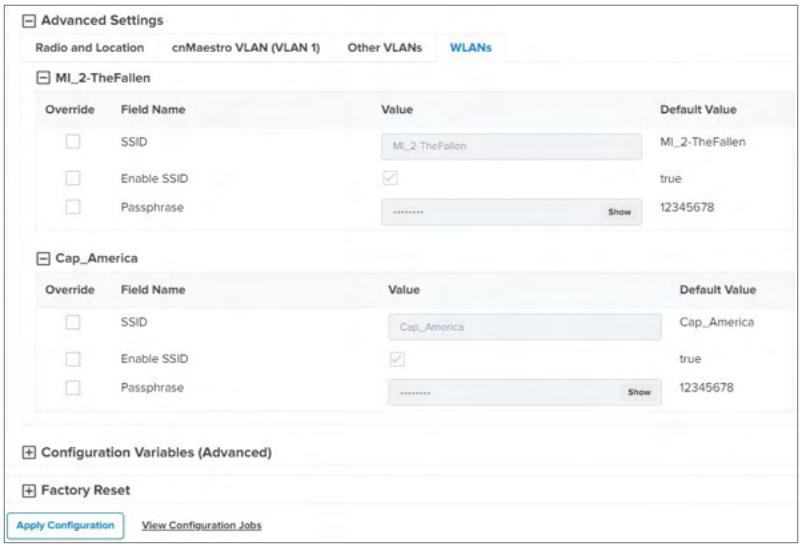
- If the Dual 5 GHz Radio option is enabled, then allow channel range > = 100 for Radio 2 and 36 – 64 for Radio 3.





Note

XE3-4TN features a radio antenna override option.



User-Defined Overrides

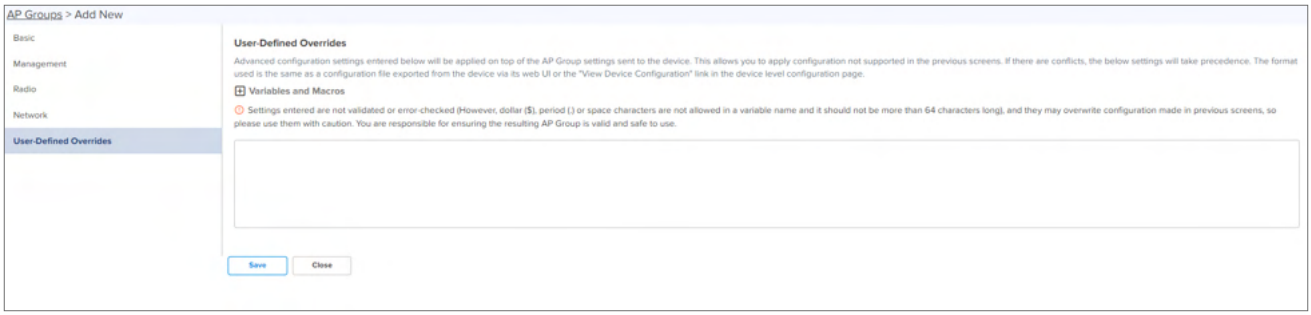
User-Defined Overrides can be entered into the end of an AP Group configuration. They will be appended to the AP Groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI; this is an advanced operation that should rarely be used. The format of the commands is same as with the device CLI.

For example, if a new version of the software had a feature unsupported in cnMaestro, it could can be pushed to the device using CLI commands through the User-Defined Override mechanism.

This can be explained with the following example, in which country-code and hostname are appended to the end of the configuration and will override any settings in the UI.

```
country-code IN

hostname Wi-Fi_Device
```



User-Defined Variables

Override configuration also supports a programmatic concept called User-Defined Variables (which are also used with templates). User-Defined Variables can be embedded into the User-Defined Override text area. They require a value to be set for each device mapped to the AP Group before the configuration can be applied. This is either through a default value, or an explicit setting in the device configuration.

The syntax for User-Defined Variables is shown in the following example: the VariableName maps to an identifier set by each Device. If the value is not set, the optional DefaultValue will be used.

```
Parametername ${VariableName=DefaultValue}
```

Note

You can also configure User-Defined Variables in the Onboarding process queue page. They are mapped individually to each device.

Other Examples

Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP hotspot)

```
country-code ${countryname=US} // country name with US as default value

hostname ${hostname=ePMP_1000_Hostpot}
```

cnPilot Home R-Series

```
Parametername ${variableName=someDefaultValue}
```

Example

```
CountryCode=${countryName=IE}

RTDEV_CountryCode=${5GHz_CountryName=IE}

wan_ipaddr=${wan_ip=10.110.68.10}
```

Macros can be used in advanced configuration similar to User-Defined Overrides, except that they automatically obtain values provided by the device itself.

The following macros are supported:

- `%{ESN}` will be replaced with the MAC address of device.
- `%{esn}` will be replaced with the MAC address of the device in lowercase.
- `%{ESN-}` will be replaced with the MAC address of the device separated by a hypen (-).
- `%{esn-}` will be replaced with the MAC address of the device in lowercase separated by a hypen (-).
- `%{ESN6}` will be replaced with the last six non-separator characters of the device MAC address.
- `%{esn6}` will be replaced with the last six non-separator characters of the device MAC address in lowercase.
- `%{MSN}` will be replaced with the serial number of the device.

Bulk Overrides

Bulk Overrides allow the user to edit the multiple configurations shared through an AP Group for one or more devices.

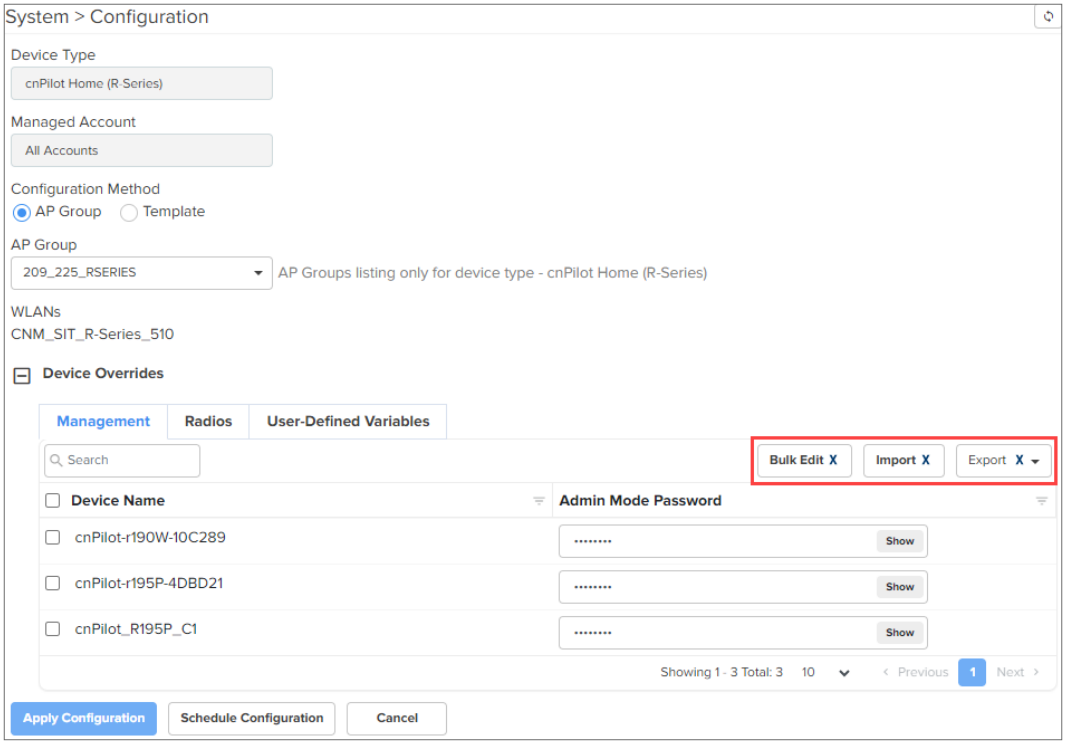
Note

Bulk Edit option under **Configuration** > **Devices Overrides** is supported only for cnMaestro X.

The user can override for the following configurations in cnPilot (R-Series):

- Management
- Radios
- Wi-Fi Configuration

Figure 334 *Bulk Override: cnPilot (R-Series)*



The user can override for the following configurations in Enterprise Wi-Fi (E-Series, XV-Series):

- Location
- Management VLAN
- Radios
- WLANs
- User-Defined Variables

Figure 335 *Bulk Override: Enterprise Wi-Fi (E-Series, XE-Series, XV-Series)*

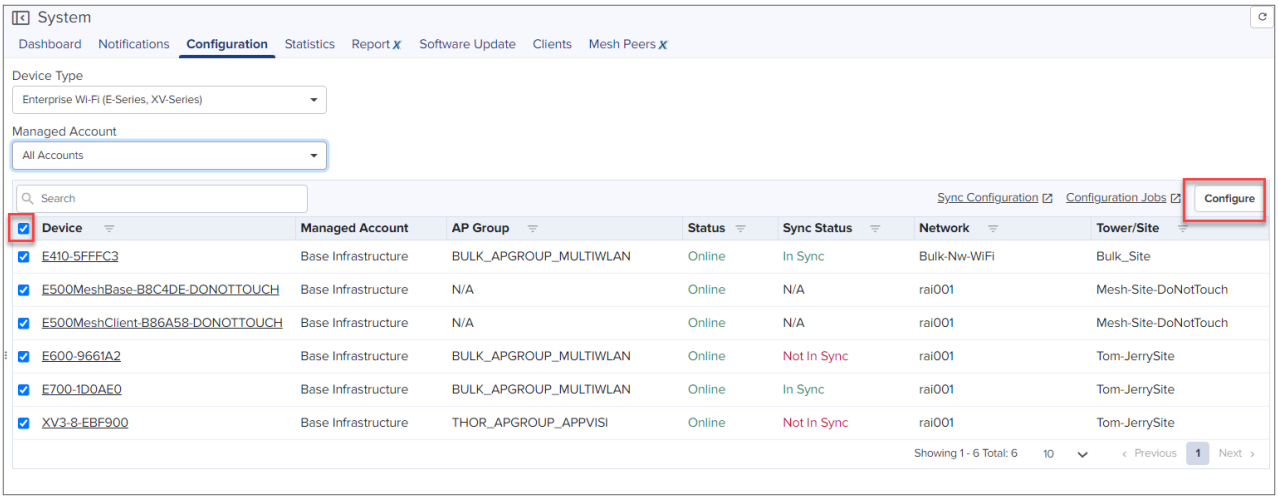


Note

Configuration tab will be available from other container levels like Network/Site and also from AP group level.

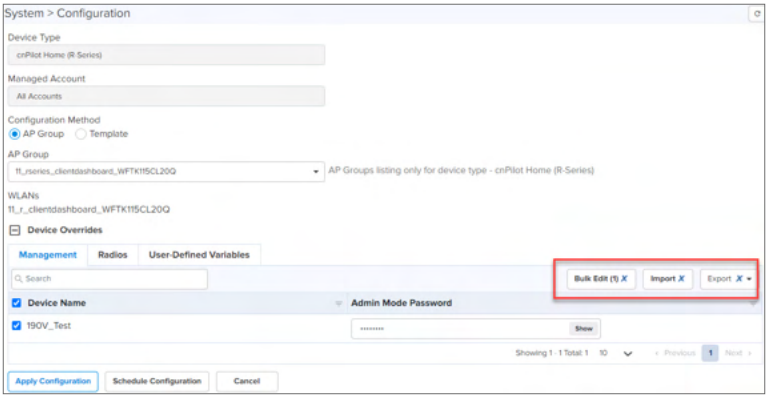
To configure Bulk Overrides for the devices, perform the following steps:

1. Navigate to **Manage > System > Configuration.**
2. Select the **Device Type** from the drop-down.
3. Select **Device** from the list and click **Configure**.



4. Click the plus (+) next to **Device Override(s)**, to override the list of devices.
5. In the Device Override table, reconfigure tabs and perform the following actions:
   - Bulk Edit
   - Export

- Import



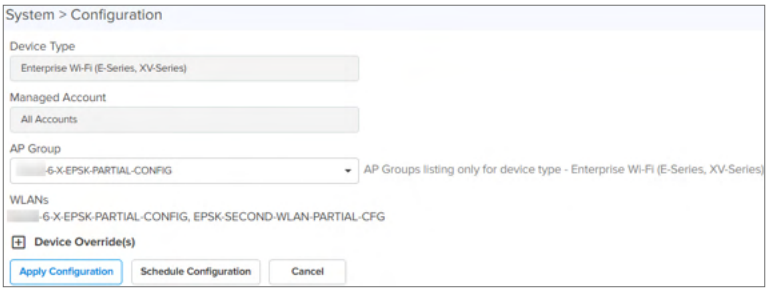
6. Select the device(s) from the Device Override table to configure.
7. Click **Bulk Edit.**

   A pop-up window appears for the fields to reconfigure.
8. Click **Save**.

   You can export, as described:

   - Export page as CSV
   - Export all as CSV

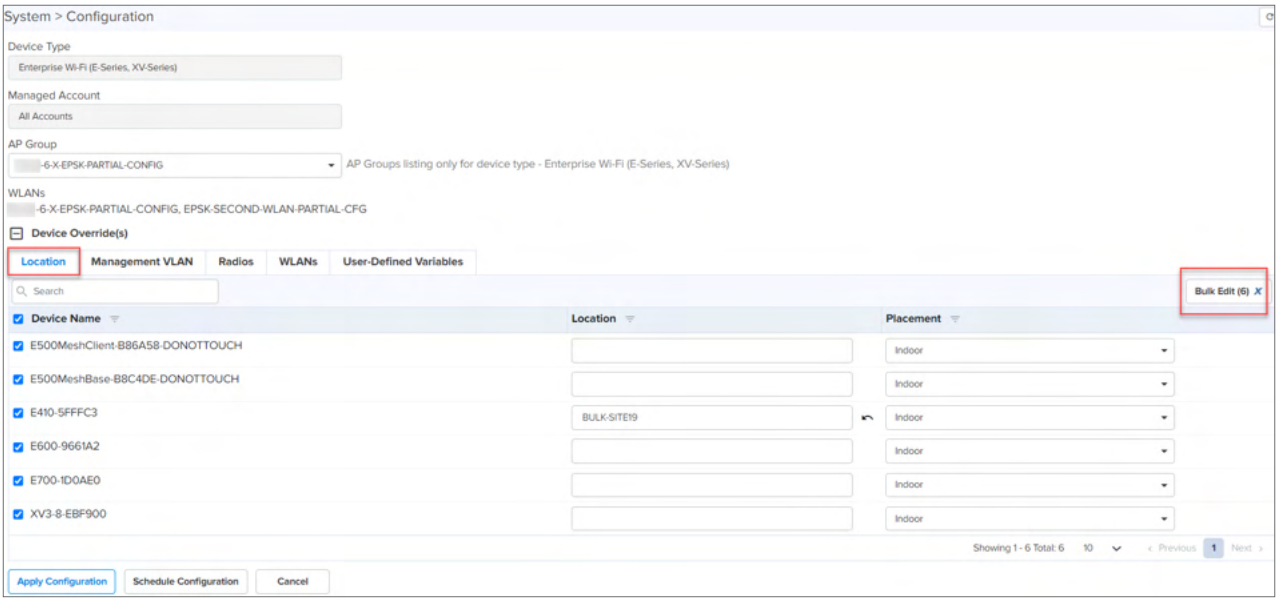
   After modifying the field values, the CSV file can be imported.



9. Click **Import**, to import the file.
10. Select the file to import in CSV file format.
11. Click **Apply**.

Location

1. In the **Location** tab, select the devices from the list.
2. Click **Bulk Edit.**

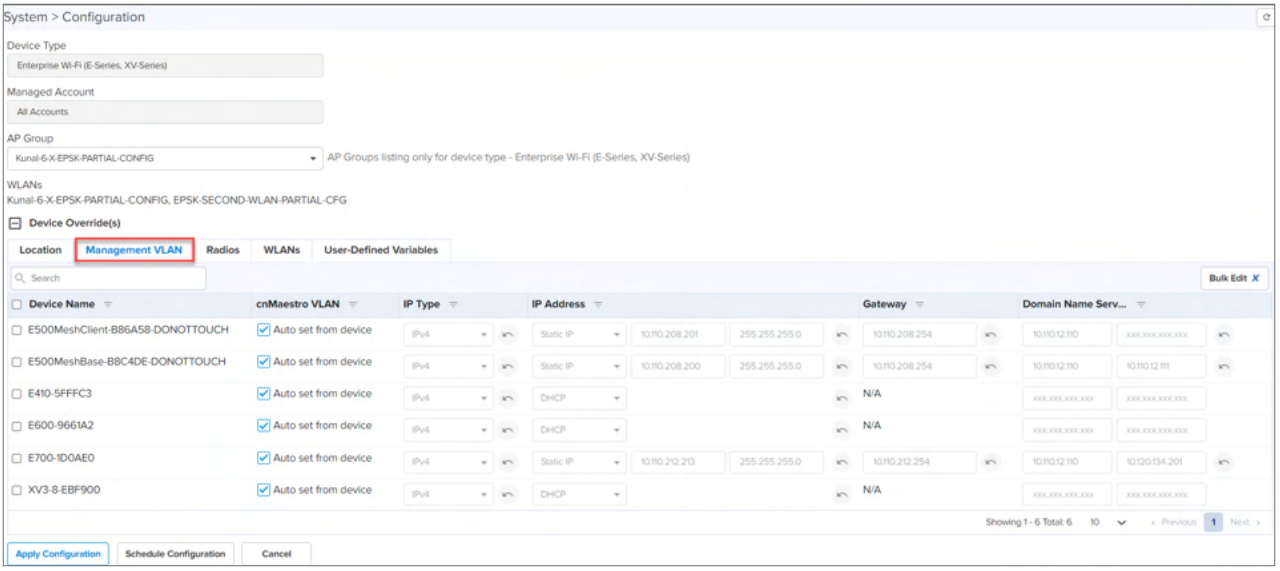


3. **Override Location** window appears, edit the configuration details and click **Save**.

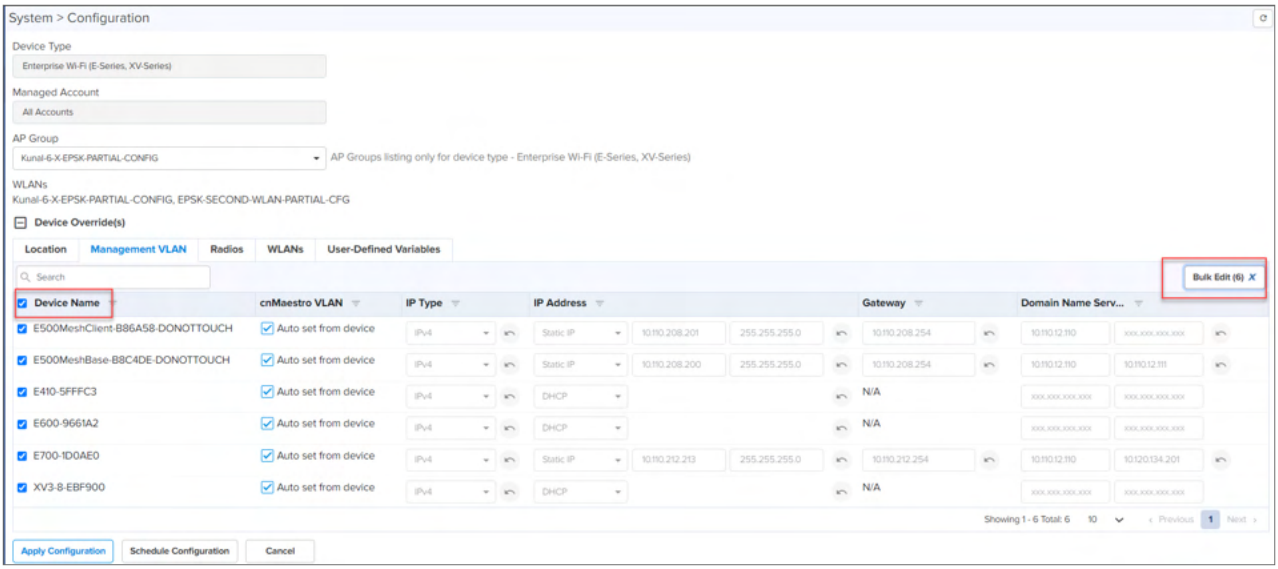


Management VLAN

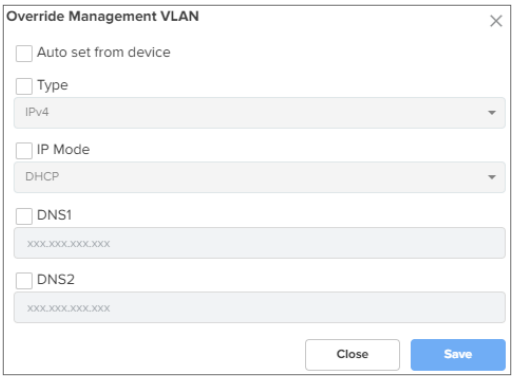
4. In the **Management VLAN** tab, select the **VLAN** of the device from the list.



5. Click **Bulk Edit**.

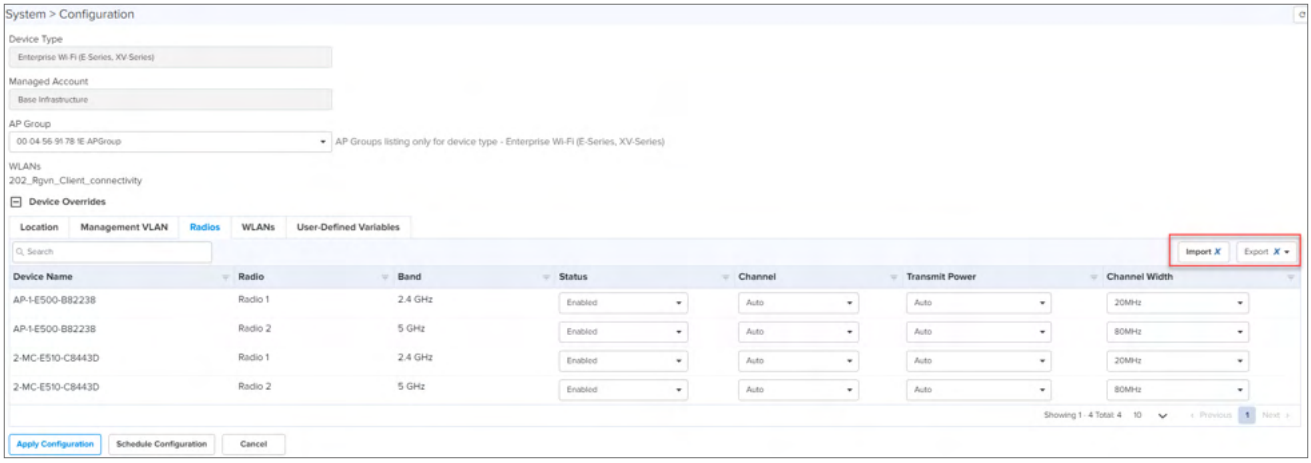


6. **Override Management VLAN** window appears, edit the changes and click **Save**.



Radios

In the **Radio** tab, select the radios from the device list, to perform **Import** and **Export** actions.



Note

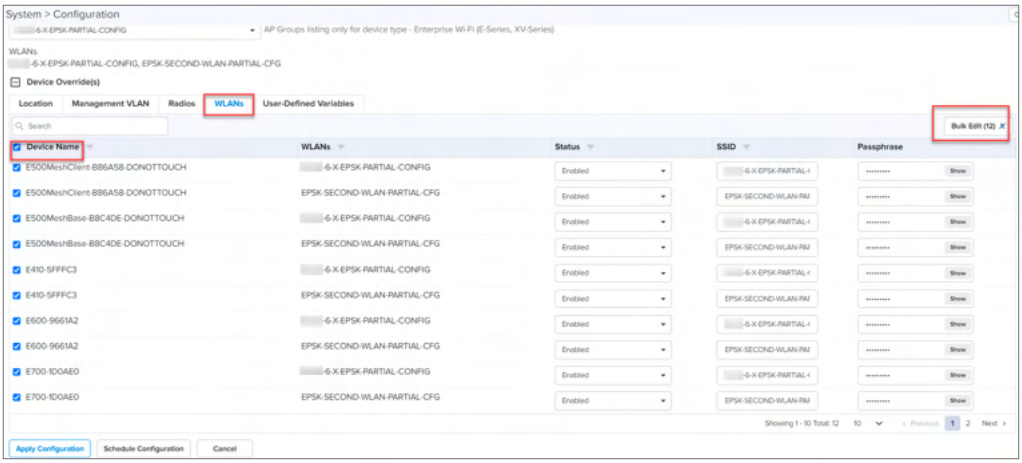
Bulk Edit tab is removed from Radio configuration from 3.1.1 release.

7. Export the report to edit the radio parameters. You can export the radio parameter details as described:
    - Export page as CSV
    - Export all as CSV

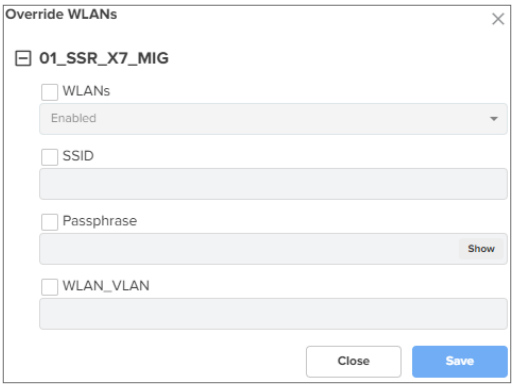
    After modifying the field values, the CSV file is imported.
8. Click **Import**, to import the file.
9. Select the file to import in CSV file format.
10. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

WLANs

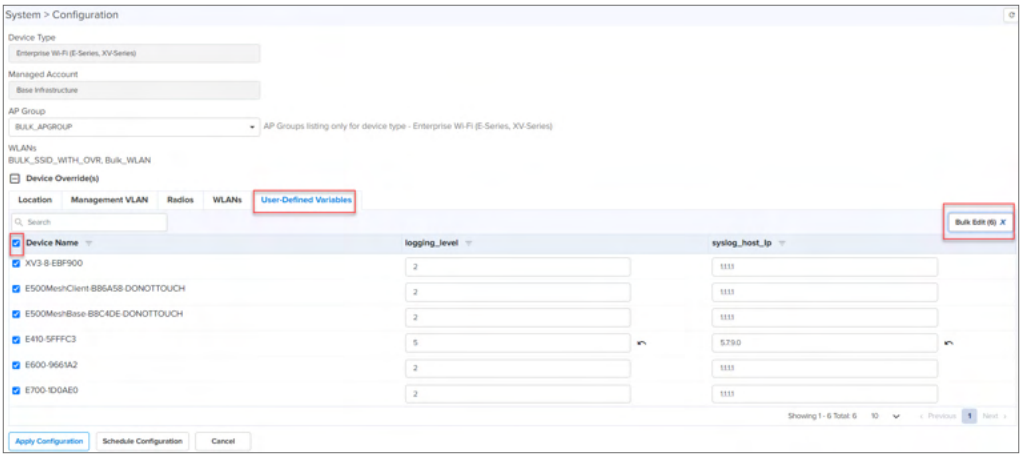
11. In the **WLANs** tab, select the WLAN of the devices from the list.



12. Click **Bulk Edit**.
13. **Override WLANs** window appears, edit the configuration details and click **Save**.



14. In the **User-Defined Variables** tab, select the devices from the list.



15. Click **Bulk Edit**.

    The **Override User-Defined Variables** window appears.



16. Edit the configuration details and click **Save**.

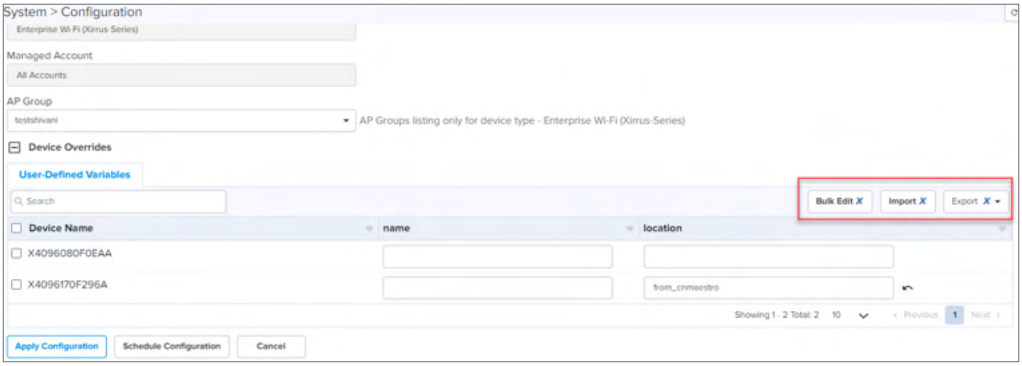
> **Note**
>
> For Bulk overrides to be enabled in **User-Defined Overrides** tab, you must define the overrides in the **User-Defined Overrides** section of AP groups. For more details, see User-Defined Overrides

17. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

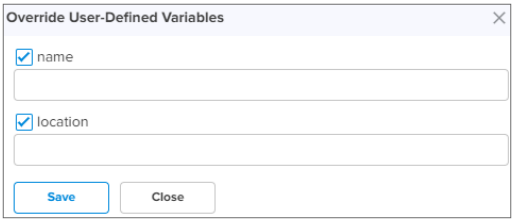
The user can override for the following configurations in Enterprises Wi-Fi (Xirrus-Series):

- User-Defined Variables

Figure 336 *Bulk Override: Enterprises Wi-Fi (Xirrus-Series)*



18. In the **User-Defined Variables** tab, select the devices from the list.



19. Click **Bulk Edit**. The **Override User-Defined Variables** window appears , edit the configuration details and click **Save**.
20. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

Synchronize (Sync) Configuration

AP Groups can be configured to synchronize automatically or manually when they are updated. The setting is available in the AP Group configuration page.

1. **Enterprise Wi-Fi AP Groups** by default synchronize automatically (so any change of AP Group or WLAN, followed by a **Save**, will immediately push configuration to the devices without manual intervention).
2. **cnPilot Home AP Groups** by default synchronize manually. Updates to them (or the WLANs to which they map) need manual synchronization to push configuration to the devices.

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately.

Navigate to **Administration** > **Sync Configuration**.

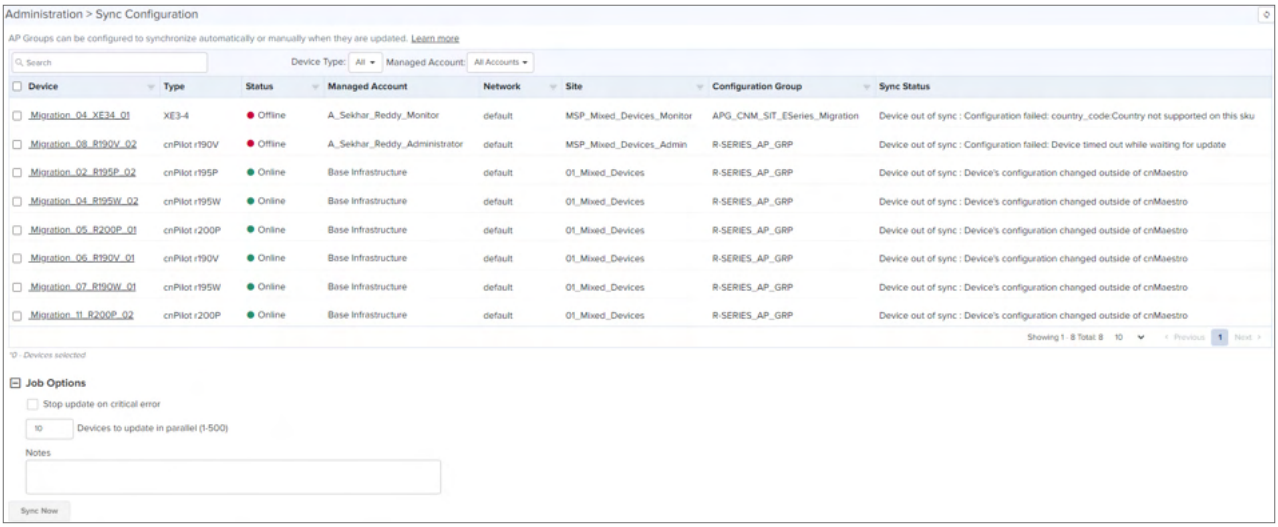
Sync Configuration only displays devices currently **Out-of-Sync** with a mapped AP Group.

Sync Configuration has the following fields:

- AP Group (AP Group to which device is mapped)
- Device (Hostname)
- Device Type
- Network (Network in which device is present)
- Status (Up/Down)
- Site (Site under which device is present)
- Sync Status (Sync status will tell whether job is completed or failed)

Steps to Sync Configuration:

1. Click the **Sync Configuration** inthe top right of the **Configuration** > **WLAN and AP Groups** or **Manage** > **Configuration** > **Device Details** or **Jobs** tab.
2. Select devices to synchronize.



3. Click **Sync Now**.

Note

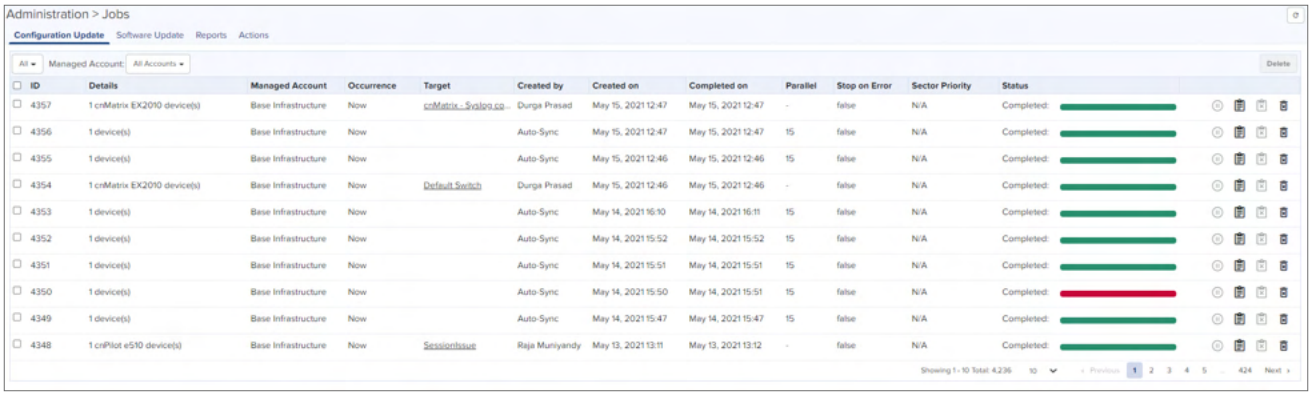
- Sync Configuration can only be used if an AP Group is already mapped to the device.
- Software Update Jobs can be scheduled in parallel irrespective of other running Jobs in cnMaestro X. Configuration and Software Update jobs execute sequentially if mapped to the same device.

Configuration Job Status

After applying the configuration, the Configuration Job status is viewed at:

- Navigate to **Monitor and Manage** > **Configuration** > **View Update Jobs** (for Access and Backhaul devices) or
- **Administration** > **Jobs** (for Wireless LAN devices).

When the configuration is pushed from the Sync Configuration page, a Configuration job will be created in the background.



Note

- Configuration jobs skip offline devices. With manual synchronization, they need to be synchronized by the administrator.
- For more information on Wi-Fi AP configuration, refer to the following URLs:
  - Unique per-Device values in Profiles Using User-Defined Overrides
  - AP Groups and Overrides for Wi-Fi Devices.

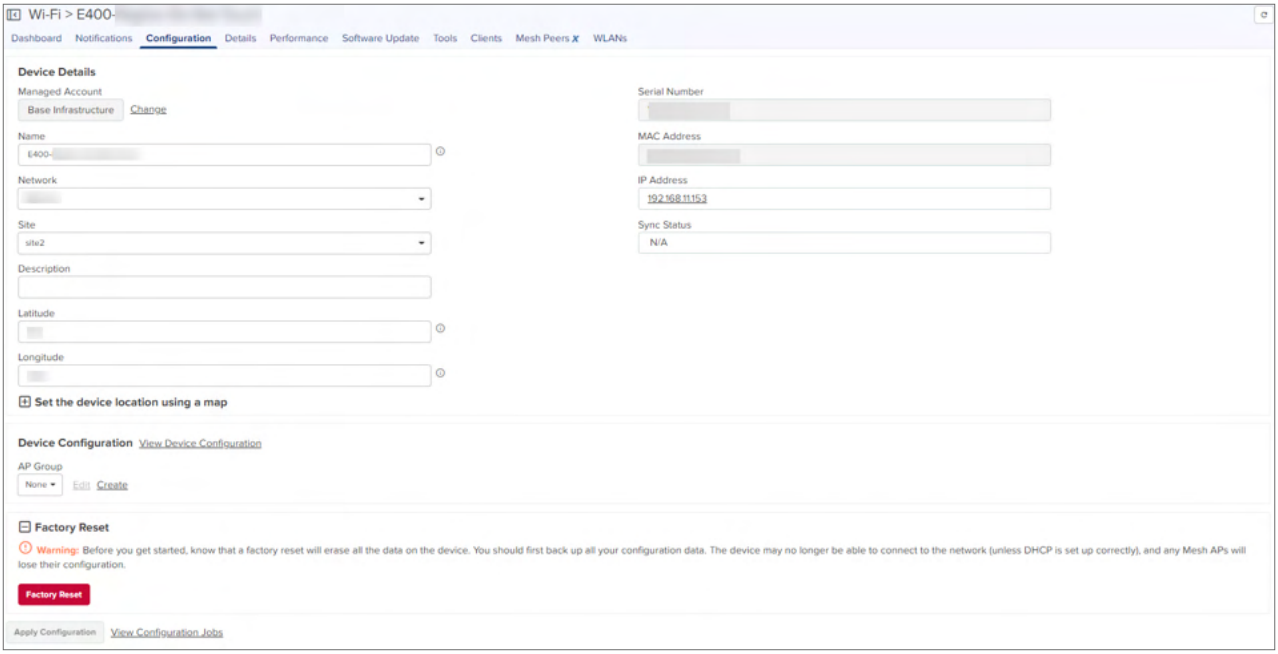
- Migrating from Templates to Profiles
- cnMaestro X can run any number of Jobs in parallel.

Factory Reset

A factory reset erases all the data on the device. Factory reset is supported for two device models: Enterprise Wi-Fi higher than 3.10-R6 version and cnMatrix higher than 4.0 version.

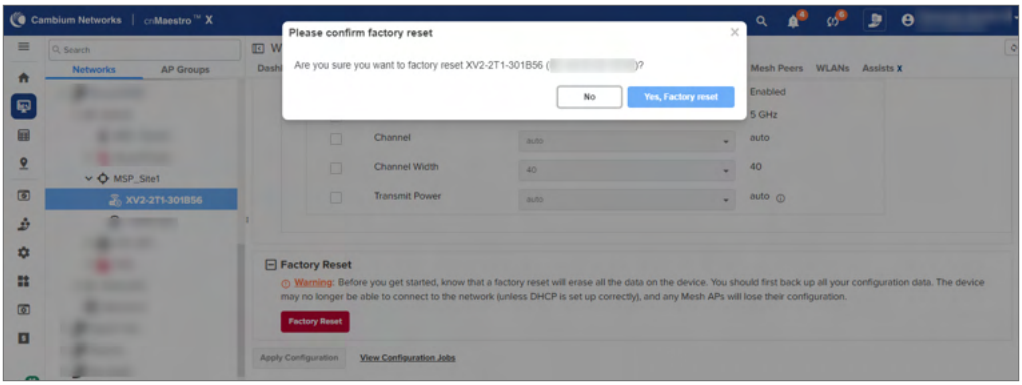
To factory reset the device perform as follows:

1. Navigate to the **Configuration** page of the device.
2. Select **Factory Reset.**

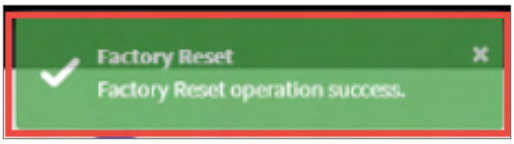


3. Click **Factory Reset**.

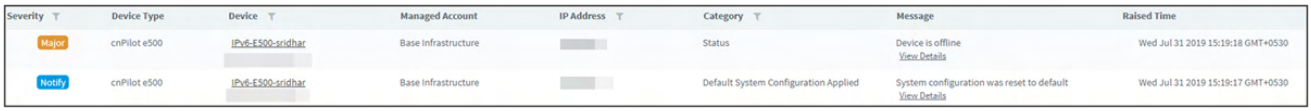
   It displays **Please confirm factory reset** message as shown below:



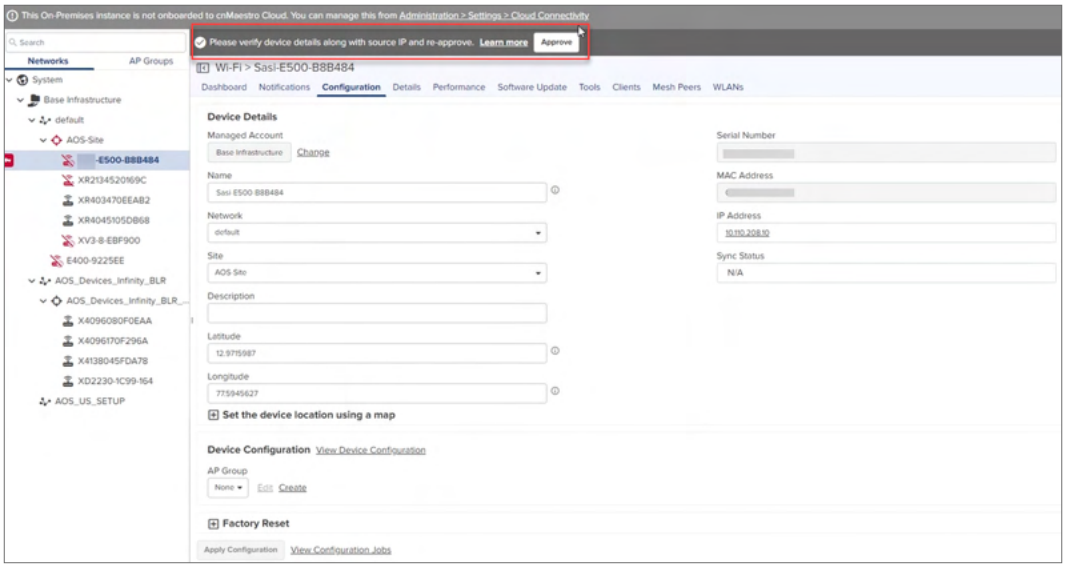
4. Click **Yes, Factory reset** option.



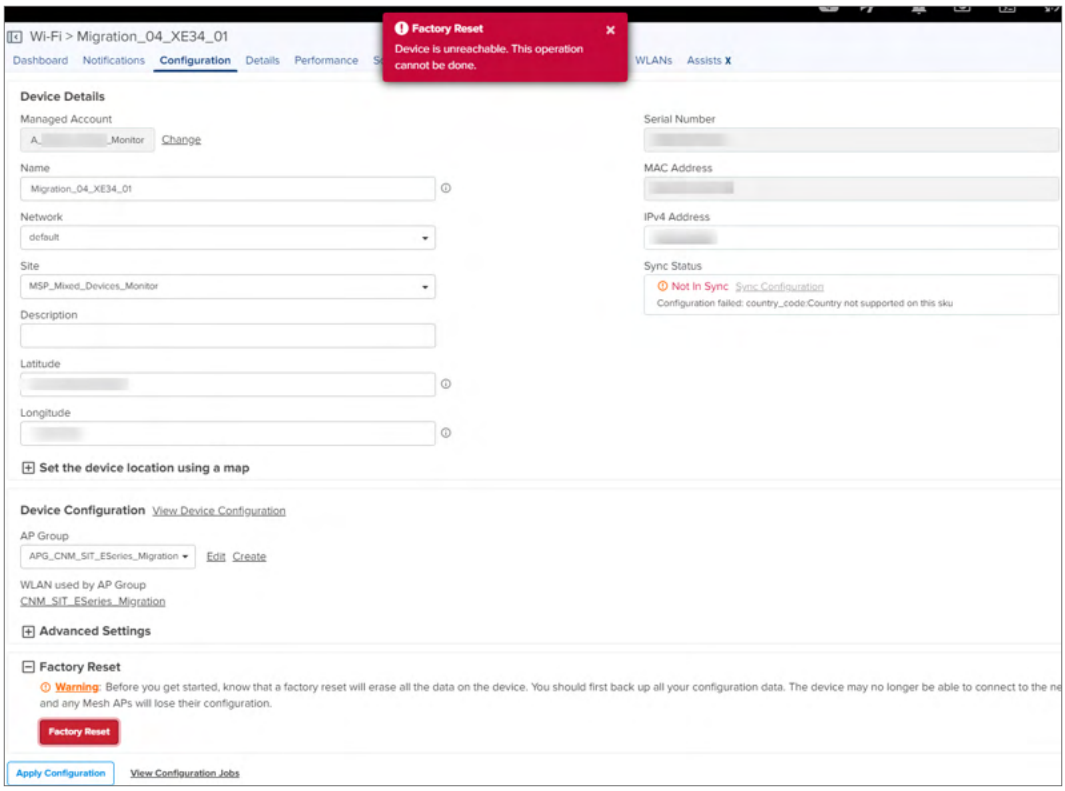
If the Factory Reset is successful, the following message is displayed on the **Notifications** tab.



When Factory Reset is performed, cnMaestro deletes the existing device cookie and displays message to **Approve** in the homepage. When the device connects back you have to re-approve the device as shown below:



When Factory Reset is applied to an offline device, it displays an error as shown below:



Association ACL

This section describes how cnMaestro replies to AP's request to allow or disallow client associations. This feature allows you to configure a MAC Association list that is used to allow/deny client associations.

Overview

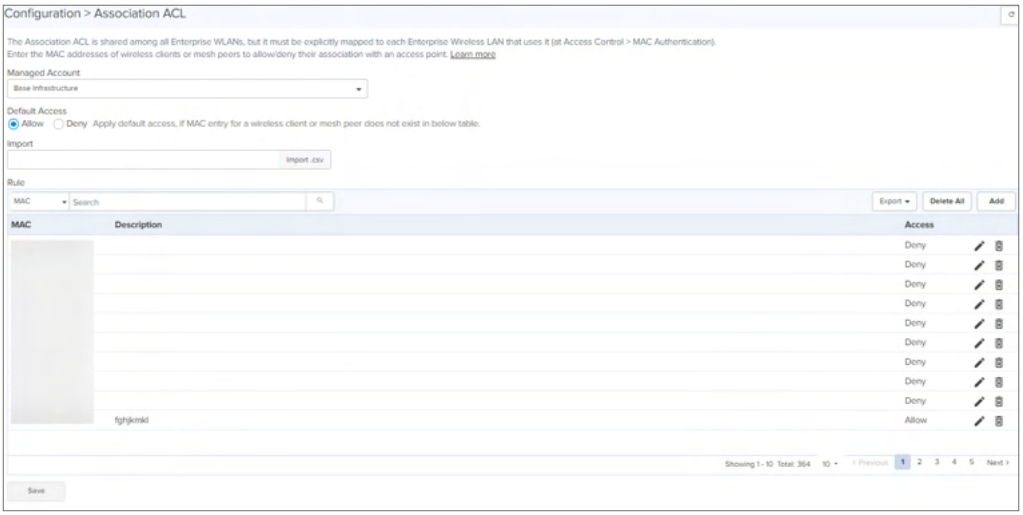
When a client tries to connect to an AP, the following occurs:

1. The AP sends MAC authentication request along with the MAC Address of client and the Customer ID (CID) to the Controller. This is optional and occurs only if MAC ACL is configured for the WLAN on the AP and the policy for the MAC ACL is cnMaestro.
2. Controller checks and responds with an action to Allow or Deny the request.
3. AP allows or denies the client's request based on the response of the Controller.

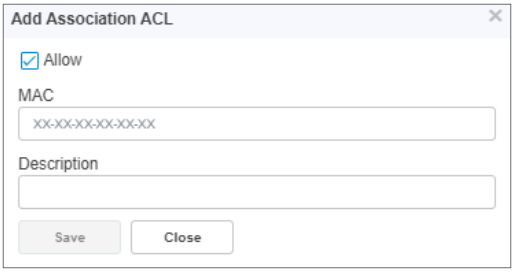
Configuring Association ACL

To configure the Access Control List (ACL) in cnMaestro:

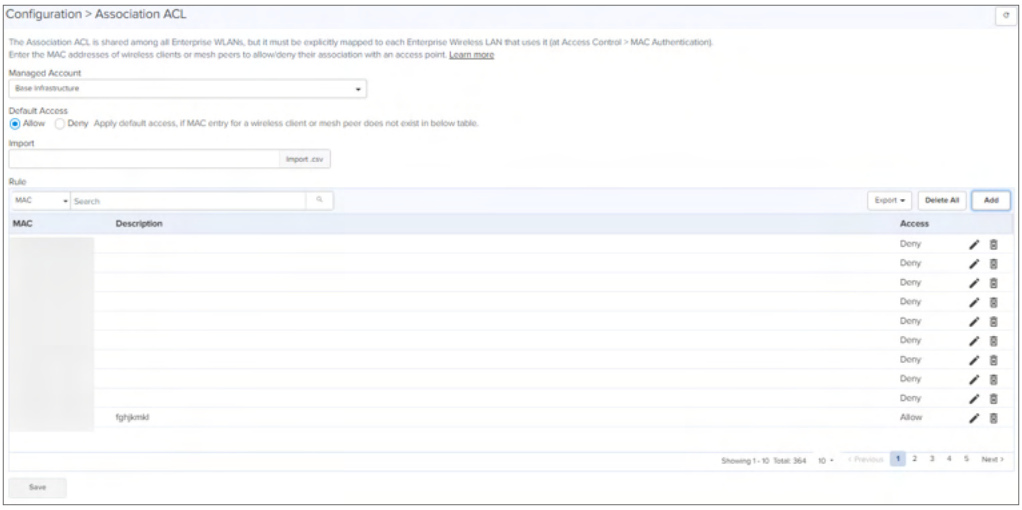
1. Navigate to **Configuration** > **Wi-Fi Profiles** > **Association ACL** tab**.**
2. Click **Add.**



3. Select **Allow.**
4. Enter the **MAC** and **Description**.
5. Click **Save**.



It displays the **Success** message.



6. To configure MAC authentication as cnMaestro:

   The Association ACL is shared among all Enterprise WLANs, but it must be explicitly mapped to each Enterprise Wireless LAN that uses it (at **Access Control > MAC Authentication**).



Note

- If MAC is not configured under the policy (to Allow or Deny), the default action will be applied.
- You can perform the following actions by selecting the respective icons in the table:
  - Edit
  - Delete
  - Export
  - Import Association ACL, by selecting **Import.csv** file.

Access Control Policies

This feature allows you to configure policies that define who can connect to the network, and how or when they are allowed to connect and access a specific device. The policies are a set of conditions, constraints, and settings.

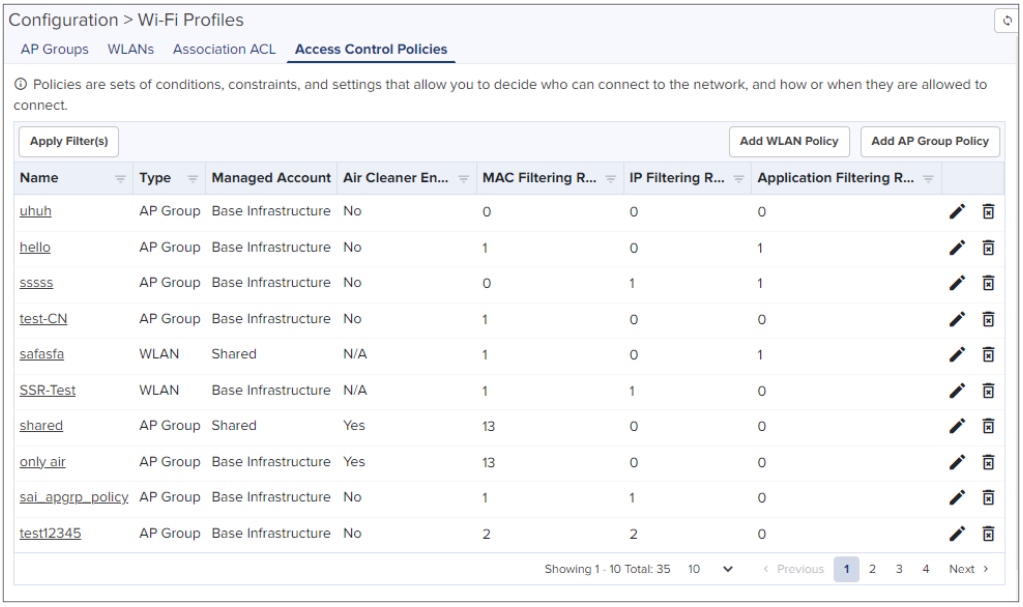
The policies can be configured on both AP Group level and WLAN level, AP Group policies have more priority than WLAN Access Control policies.

On both AP group policy and WLAN policy, we can have L2, L3 and L3 Rules. The configuration rules are processed in following priority: MAC Filters followed by IP and Application Filters.

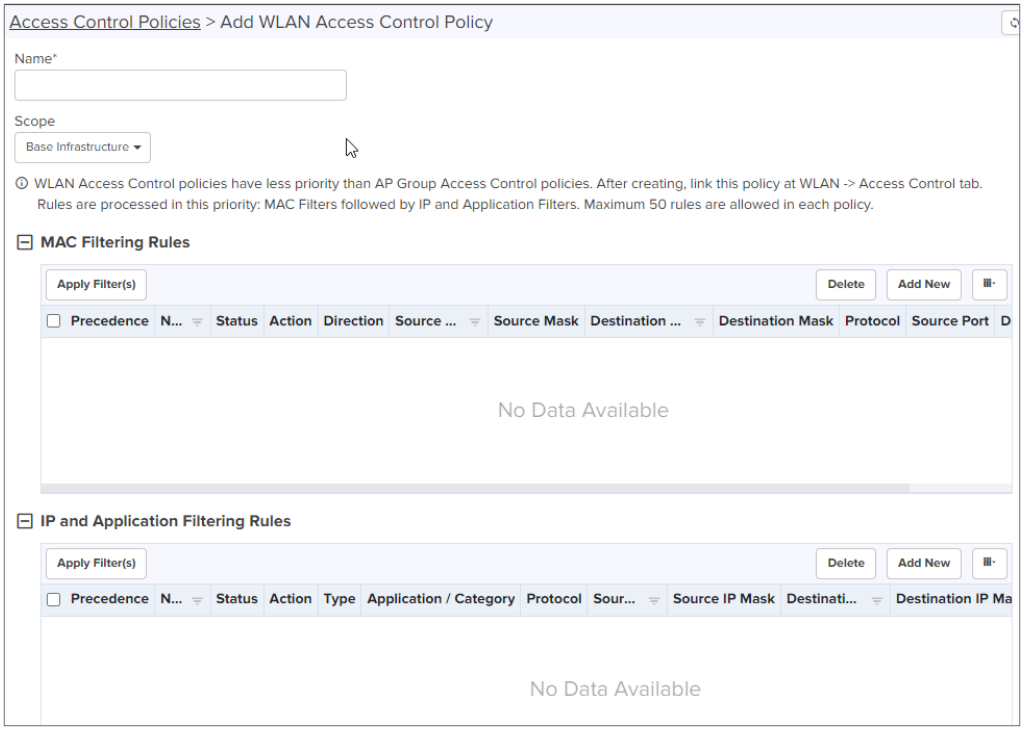
Configuring Access Control Policies for AP Groups and WLANs

To configure the Access Control Policies:

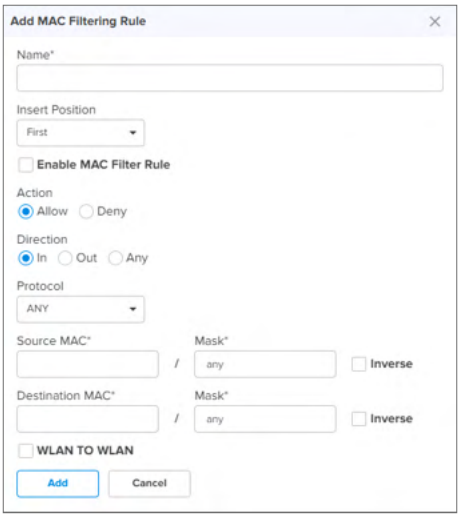
1. Navigate to **Configuration > Wi-Fi Profiles > Access Control Policies** tab.



2. Click **Add WLAN Policy** or **Add AP Group Policy**.



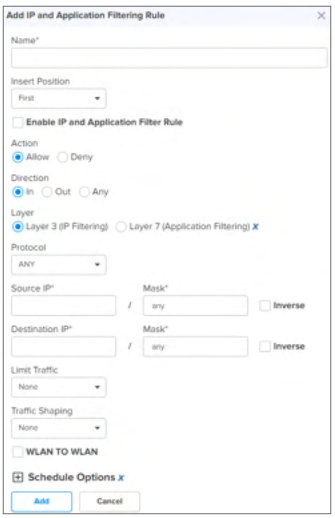
3. Enter a **Name** for the policy.
4. Select the **Scope** from the drop-down list.
5. For AP Groups, **Enable Air Cleaner**.
6. Click **Add New** in the top right corner of the **MAC Filtering Rules** list and complete the details in the **Add MAC Filtering Rule** pop-up window.



7. Click **Add New** in the top right corner of the **IP and Applications Filtering Rules** list and complete the details in the **Add IP and Application Filtering Rule** pop-up window.

Note

Application Filtering Rule is an X Feature.



8. After adding all the required rules, Click **Add** in the bottom left corner of the window.
9. Navigate to **WLAN** > **Access Control** or **AP Group** > **Access Control** tab and link this policy.

Note

- AP Group Access Control Policies are applied at the device level.
- WLAN Access Control policies have less priority than AP Group Access Control policies.

Custom Applications X

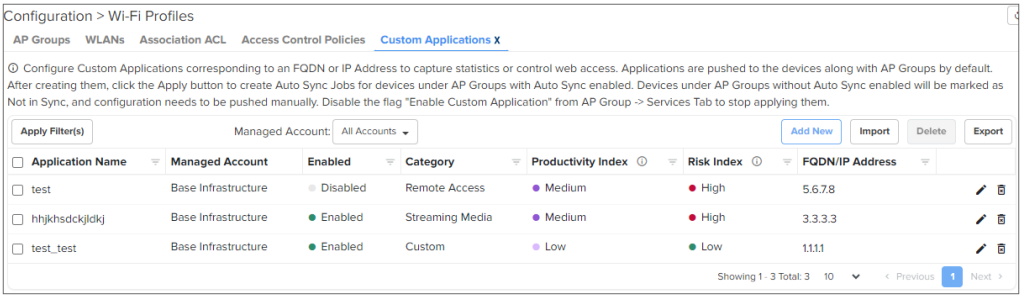
Custom applications allow you to configure applications with a specific IP address or a domain name, and apply filter rules, such as enable or disable traffic from these applications. By default, these applications are applied on the devices along with the AP group configuration.

After creating the custom application, when you click **Apply**, cnMaestro creates a job for devices in the AP group that has auto sync enabled. Devices in AP groups that do not have auto sync enabled, are marked as **Not in Sync**, and users must manually apply the configuration on to the devices.

To disable cnMaestro from applying the custom application configuration on the devices, clear the **Enable Custom Application** check box from the **AP Groups** > **Services** tab > **Application Visibility** X section.

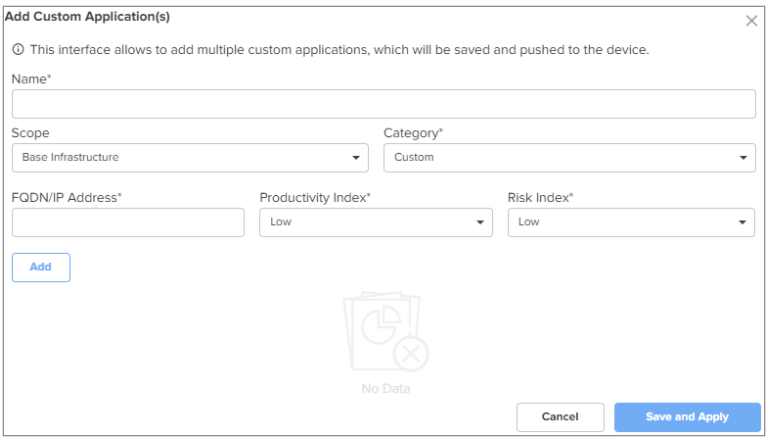
To add a new custom application, complete the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** > **Custom Applications** X.



2. Click **Add New** on the **Custom Applications** X page.

   The **Add Custom Application(s)** window is displayed.



   Configure the following parameters:

Table 69 *Custom Application Parameters*

Parameter	Description
Name	Specifies the name for the custom application. Supports a maximum of 20 characters.
Scope	Specifies the availability of the custom application across managed accounts. The following values are supported: • Base Infrastructure—Custom application is available only for the global account. It is not shared with other managed accounts. • Shared—Custom application is shared across all managed accounts. It can be mapped to devices in the managed account, but it cannot be modified. To modify the configuration, it must be copied into the managed account and then updated. • Managed Account—Custom application is available only for that specific managed

Table 69 *Custom Application Parameters*

Parameter	Description
	account. **Note**: Once the scope has been configured on a custom application, it cannot be modified.
Category	Specifies the category to which the application must belong. Select the appropriate category from the drop-down list.
FQDN/IP Address	Specifies the IPv4 address or the domain name of the custom application.
Productivity Index	Indicates how appropriate an application is useful for business purposes. The higher the rating number, the more business-oriented an application is.
Risk Index	Indicates how likely an application is to pose a threat to the security of your network. The higher the rating number, the riskier of an application is.
Enable	Select the check box to enable this custom application.

3. Click **Add**.
4. To apply this configuration on the AP, click **Save and Apply**.

cnMatrix Switches

cnMatrix switches simplifies the network deployment and operation. cnMaestro provides management, configuration and control, and security services for cnMatrix with deployment options such as Policy-Based Automation (PBA) to simplify core operations and improve network security. Central to cnMaestro's orchestration of cnMatrix devices is the concept of Switch Groups.

This chapter contains the following topics:

- Switch Group Configuration
- Synchronize (Sync) Configuration
- Policy Based Automation (PBA)
- Switches
- Switch Ports
- Device Details

Switch Group Configuration

A Switch Group represents a virtual stack of switches, independent of their locations or networks. The Switch Group functionality enables users to manage multiple switches with the same configuration.

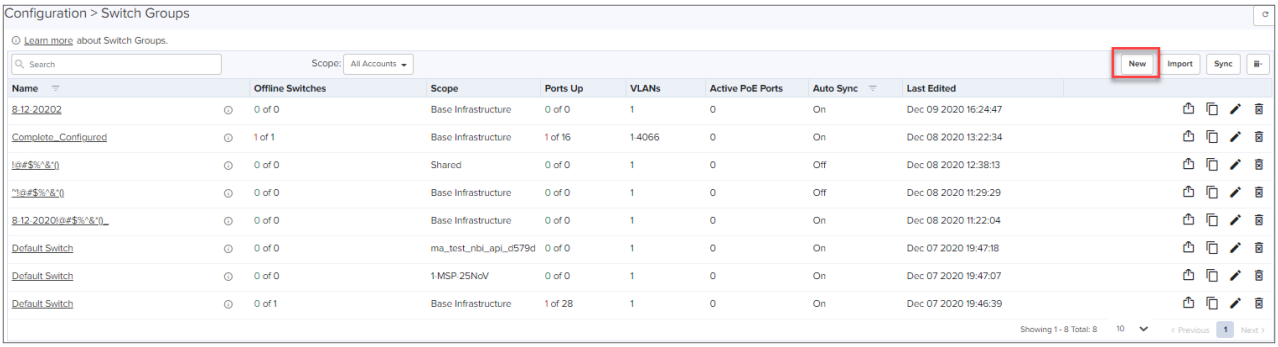
Configuration is common to all switches belonging to a Switch Group:

- Configuration changes are synchronized and applied for all the switches in a Switch Group.
- A subset of configuration attributes can be overruled for an individual switch.
- Switch Ports across all physical switches are associated with a Switch Group and can be simultaneously bulk edited.

From the **Switch Groups** tab, the administrator can navigate to the Switches and the Switch Ports tabs for configuration. The Dashboard tab is used to monitor the health condition of the virtual stack.

The process for creating a new switch group configuration is as follows:

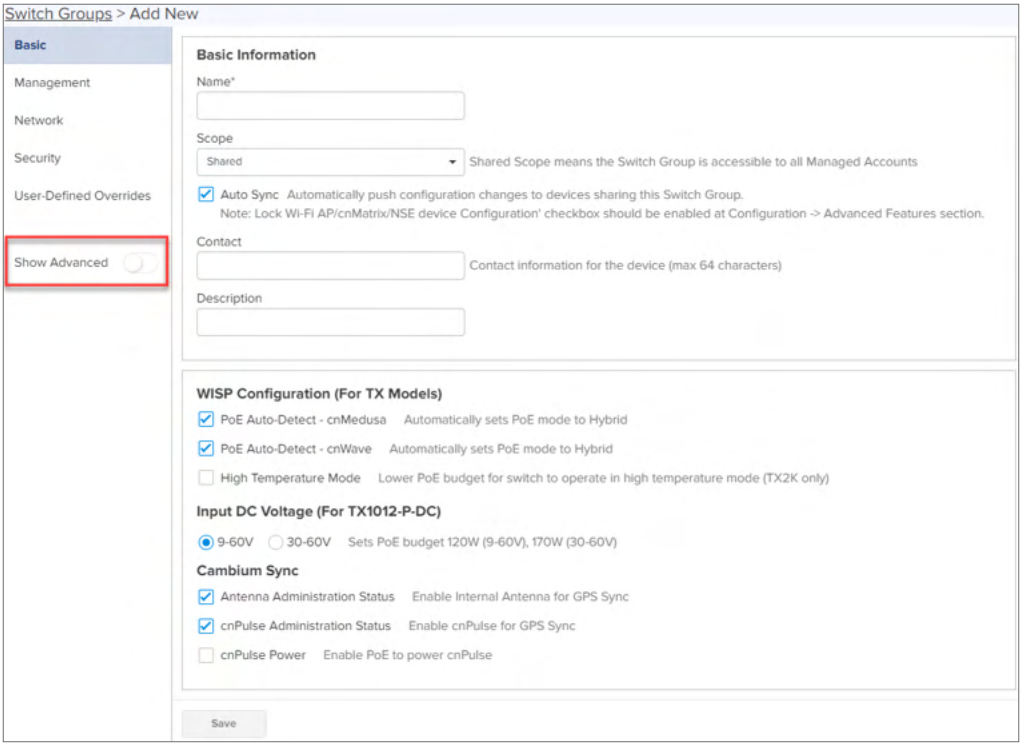
1. Navigate to **Configuration > Switch Groups.**
2. Click **New Switch Group**.



Note

To edit the Configuration of an existing switch group, click the edit ( ) icon, navigates to Switch Group Configuration page.

3. Configure the following tab parameters to create a Switch groups:
4.
   - Basic
   - Management
   - Network
   - Security
   - User-Defined Overrides



Note

- Toggle the **Show Advanced** button to view the advanced options of the Switch Groups.
- Click **Save** on individual tab parameters or click once after configuring parameters across all the tabs.

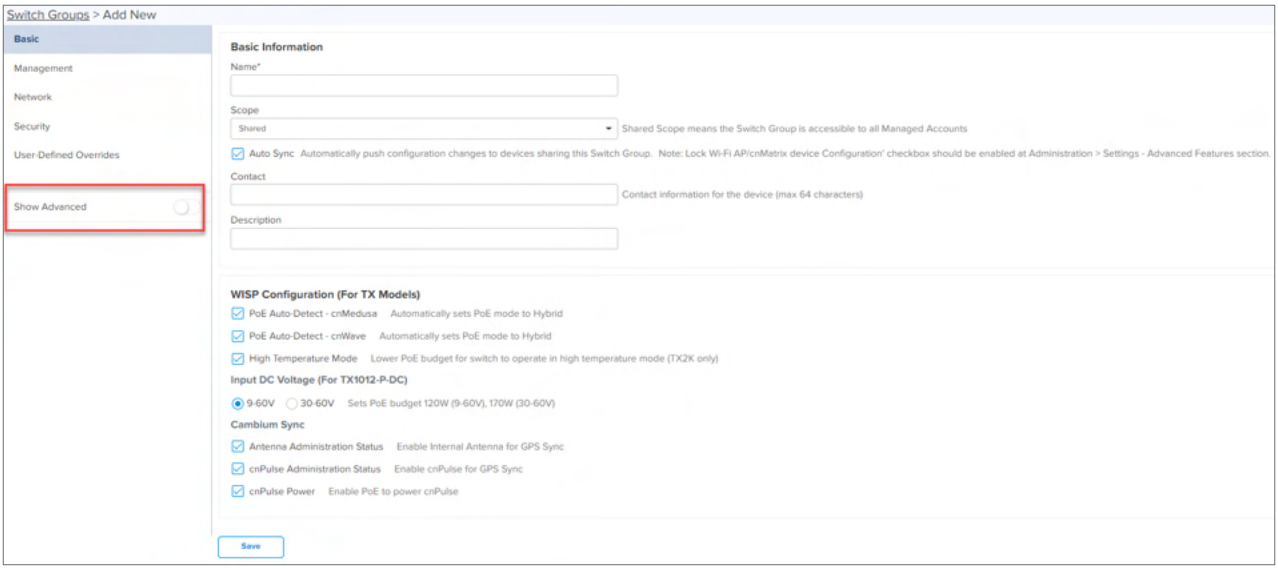
Basic

The Basic tab provides options to the user to configure the device name as well as other standard values used to identify a switch.

1. Navigate to **Configuration** > **Switch Groups** > **Basic.**
2. On the Basic page enter device identification data such as:
    - Name
    - Contact
    - Description
    - Scope
    - WISP Configuration
    - Input DC Voltage
    - Cambium Sync

Note

- The special characters should be used to create Switch Groups names (Eg: a-zA-Z_-*&%#@!<>.() []^~`$1234567890). The user can also rename them if required.
- By default, the password is not configured. User has to configure the password for Switch Group.
- By default, the **Auto Sync** option for automatically applying the configuration is enabled.



3. Click **Save**.

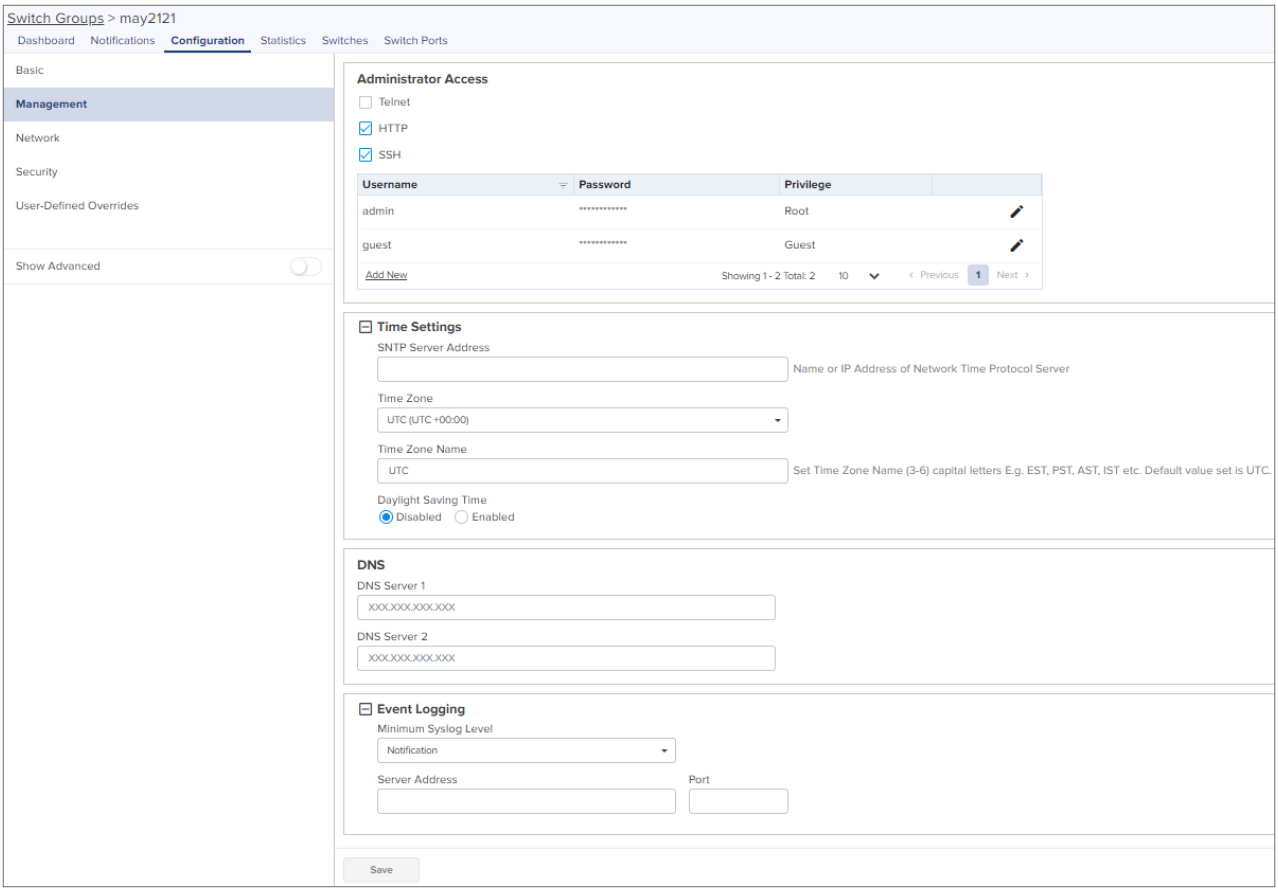
Management

The **Management** page allows you to configure Administrator Access, Time Settings, DNS, and Event Logging.

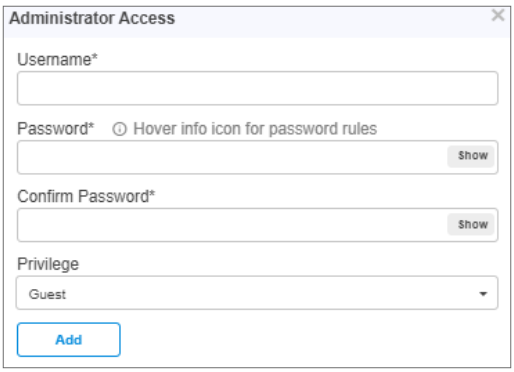
1. Navigate to **Switch Groups** > **Management** page**.**
2. Enable the **Daylight Saving Time** and enter the details.

Note

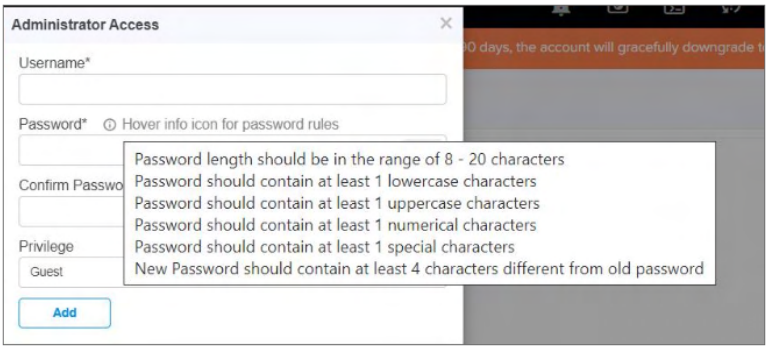
cnMatrix Switches supports SNMP configuration from release 3.0.4.



3. Click **Add New** to add **Administrator Access**, enter the details and click **Add.**



4. Password should match the special characters as shown below:



5. **Time Settings**: Enable the **Daylight Saving Time** and enter the corresponding details.
6. **DNS**: Enter DNS server details.
7. **SNMP**: Enter SNMP details.
8. **Event Logging**: Select **Minimum Syslog Level** from drop-down and enter server details.
9. Click **Save.**

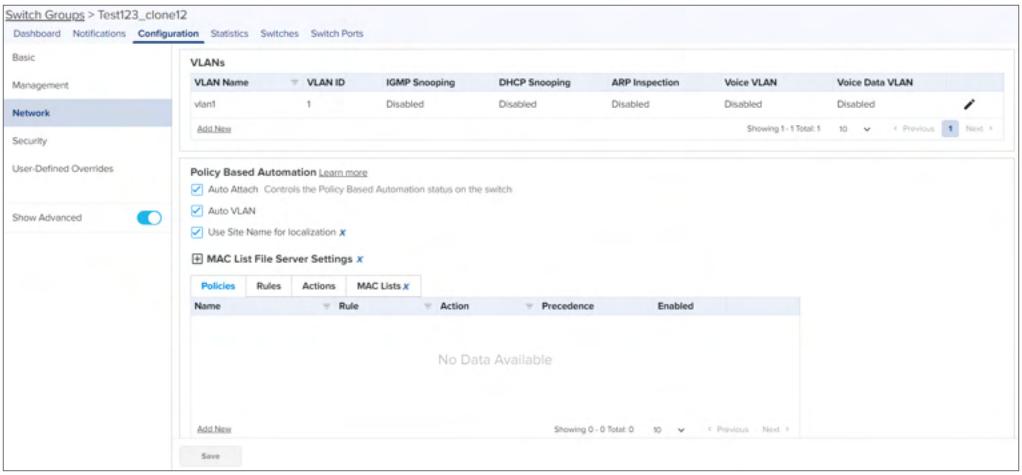
Network

The Network page allows the user to configure VLANs, PBA, IP Route, and Spanning Tree details.

Note

From release 3.0.4 cnMatrix Switches supports MSTP Mode and Path Cost Method in Spanning Tree.

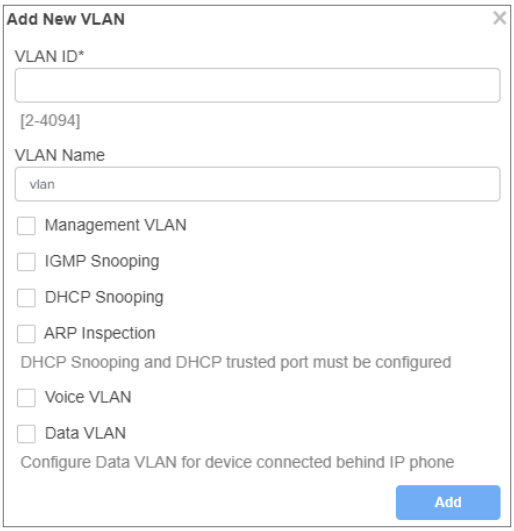
1. Navigate to **Switch Groups > Network,** enter the details of **VLANs**, **Policy Based Automation**, **MAC List File Server Settings**, **IP route**, and **Spanning Tree**.



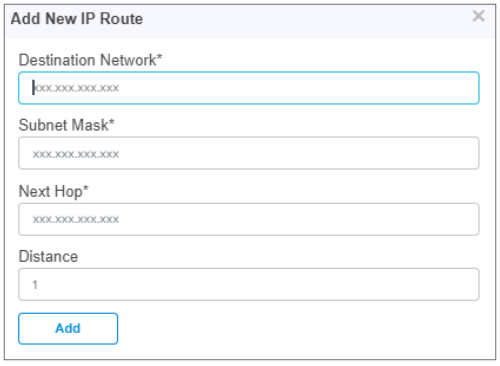
Note

Use Site Name for localization, **MAC List File Server Settings**, and **MAC Lists** are cnMaestro X features.

2. To Add a new VLANs click **Add New.**
3. Enter the **VLAN ID**.
4. Enter the **VLAN Name**.



5. Enable or disable the following options:
   - Management VLAN
   - IGMP Snooping
   - DHCP Snooping
   - ARP Inspection
   - Voice VLAN
   - Data VLAN
6. Click **Add.**
7. To Add a new IP Route click **Add New.**
   a. Enter the **Destination Network**.
   b. Enter the **Subnet Mask**.



   c. Enable the **Next Hop.**
   d. Enable the **Distance.**
   e. Click **Add.**
8. Enable **Spanning Tree**.

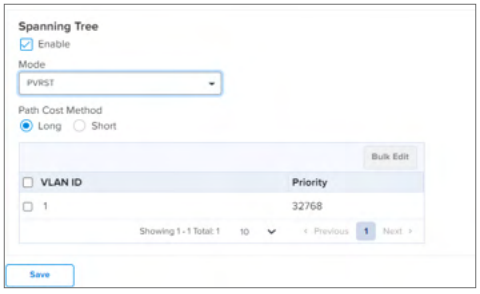
a. Select the Mode **RSTP** from the drop-down.

- Select Path Cost Method **Long** or **Short.**
- Select **Priority**.



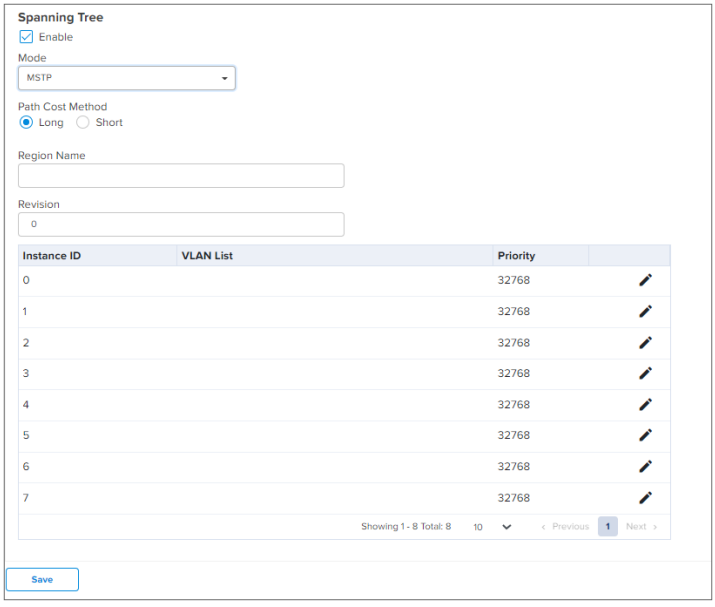
b. Select the Mode **PVRST** from the drop-down.

- Select Path Cost Method **Long** or **Short.**
- Select **Priority**.



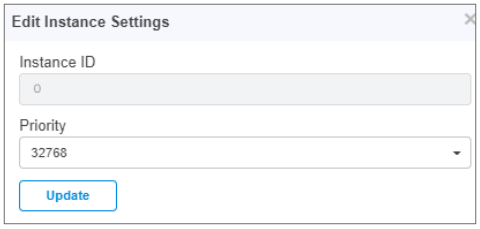
c. Select the Mode **MSTP** from the drop-down.

- Select Path Cost Method **Long** or **Short.**
- Enter the **Region Name** and **Revision.**



- User can edit **Priority** by clicking the edit (✎) icon.

- Select the Priority and click **Update.**



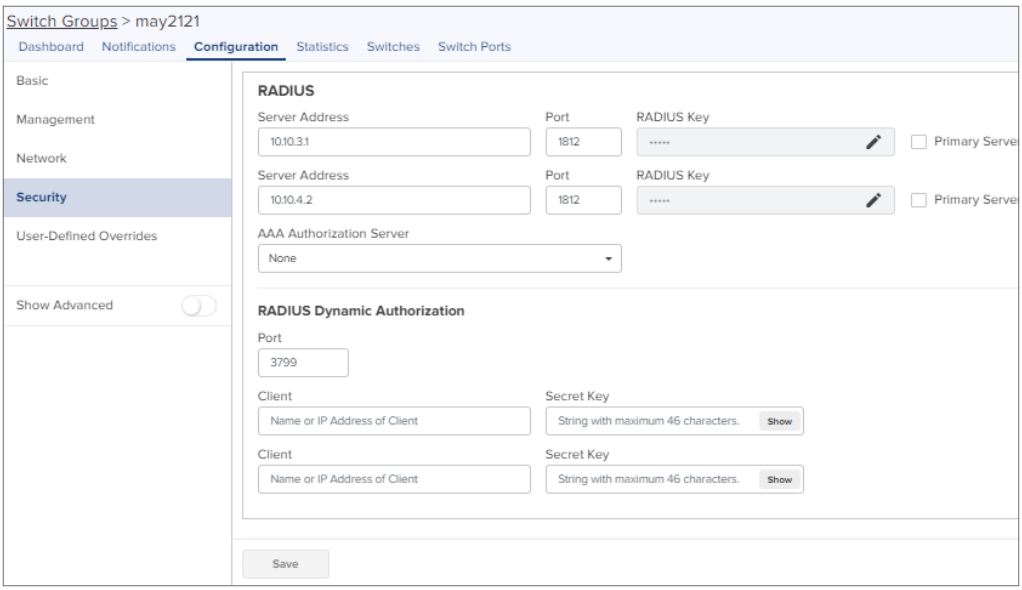
9. Click **Save.**

Security

In **Security** page user can configure **RADIUS** and **Access Control List (ACL)** details.

To configure Security:

1. Navigate to **Switch Groups** > **Configuration** > **Security** tab
2. Enter **Server Address**.
3. Enter **RADIUS Key**.
4. In **AAA Authorization Server** select **None** or **RADIUS** from the drop-down.
5. Enter **RADIUS Dynamic Authorization**.



6. In **IP ACL**, click **Add New**.



- Enter **ACL Name**.
- Select the appropriate **Protocol** from the drop-down.
- Enter **Source IP/Mask**.
- Enter **Destination IP/Mask**.
- Click **Add**.

7. Click **Save**.

User-Defined Overrides

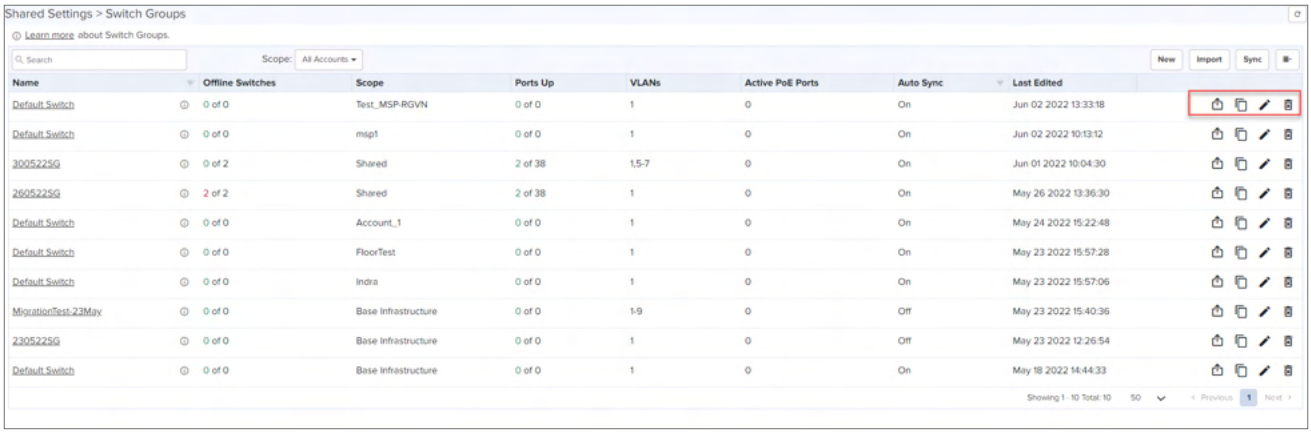
> **Note**
>
> The minimum device software version supported for this feature is 4.0.

User-Defined Overrides allows you to apply configuration in cnMatrix switches. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.



Switch Group Operations

Switch Groups can be Exported, Imported, Cloned, and Deleted.

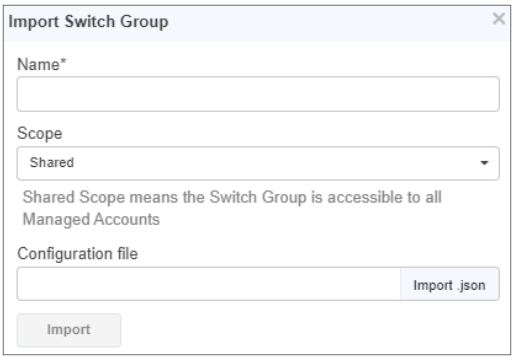


Export Switch Group

Click on the **Export** ( ) icon in the Switch Group Table to download the configuration as a JSON file.

Import Switch Group

1. Click **Import Switch Group**. A dialogue box appears.
2. Select the **Scope** from drop-down.
3. Select **import.json** and import the file.



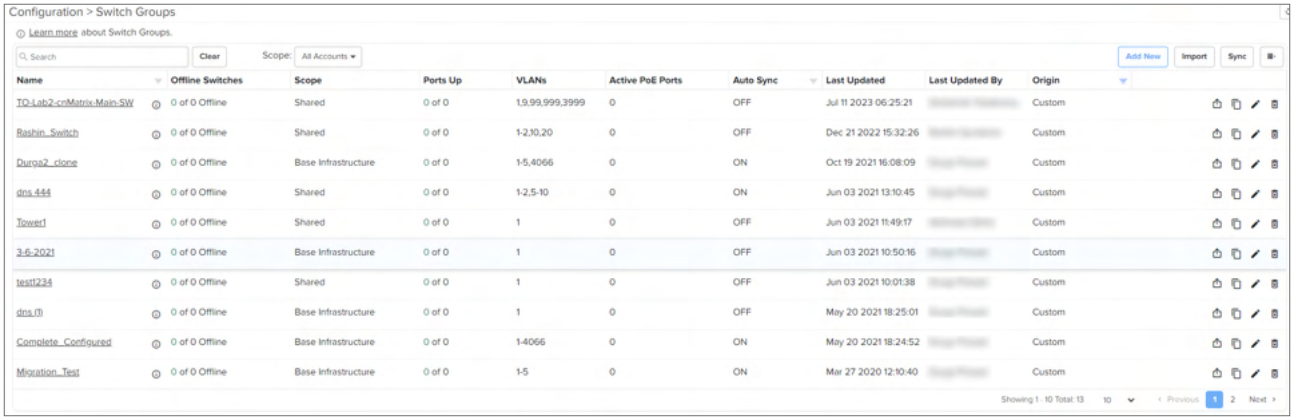
4. Click **Import.**

Clone Switch Group

Click on the **Clone** ( ) icon in the Switch Group Table to make a copy of the Switch Group.

Delete Switch Group

To delete Switch Group from the list click **Delete** icon of the specific device row.



Retry Configure

When the user tries to apply any Switch Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as " Device was offline", in the Jobs page. In this case, when device comes Up and connects to cnMaestro, then cnMaestro will create an Auto-sync job for that device and pushes the Switch Group. (It will not apply to the switch group if the "Auto-Sync" was disabled in the switch group).

Note

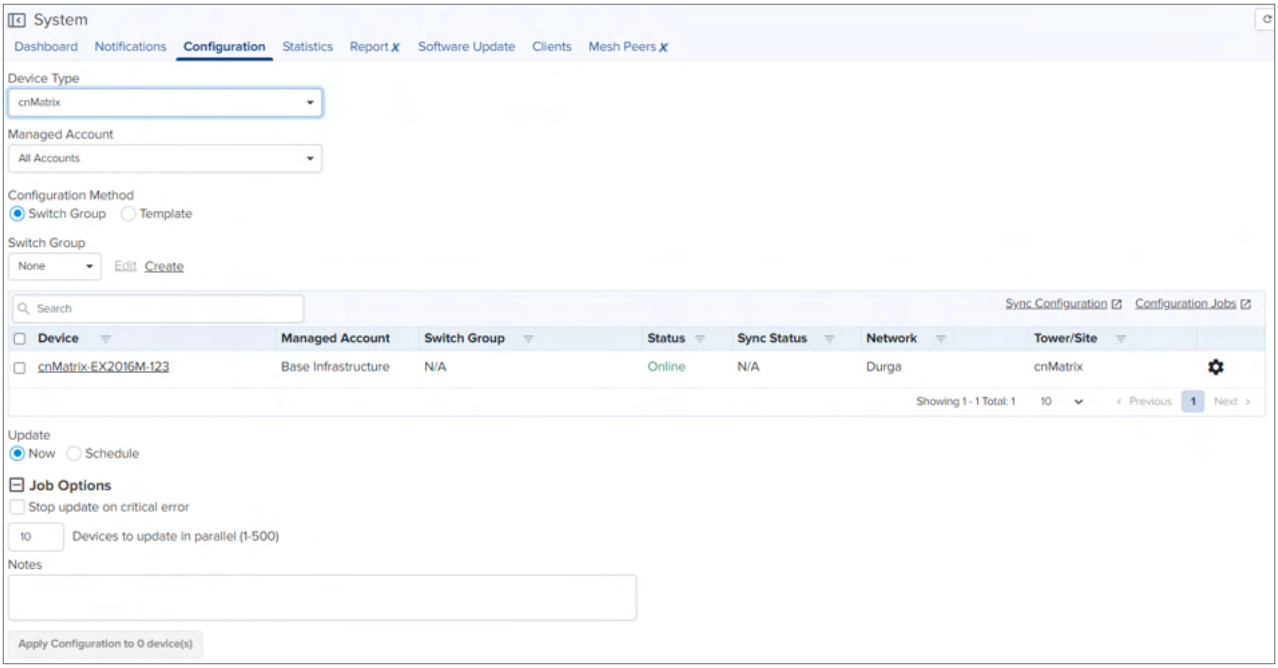
The config update (auto-sync) will happen only when the **Auto-Sync** option was enabled in the Switch Groups page. If the device was skipped/failed because of any other reason other than the "Device was offline", then the device will not be updated.

Create a Configuration Job

Configuration job can be created from **System/Network/Tower/Site/Device Configuration** page. Select a device type and a set of devices along with switch groups to which they will be mapped. This can be done in three steps:

1. Select the Switch Group that needs to be pushed from drop-down.
2. Select the list of Switch Group **Device**.

3. Click **Apply Configuration**



Synchronize (Sync) Configuration

Switch Groups can be configured to synchronize automatically or manually when they are updated. The setting is found in the Switch Group configuration.

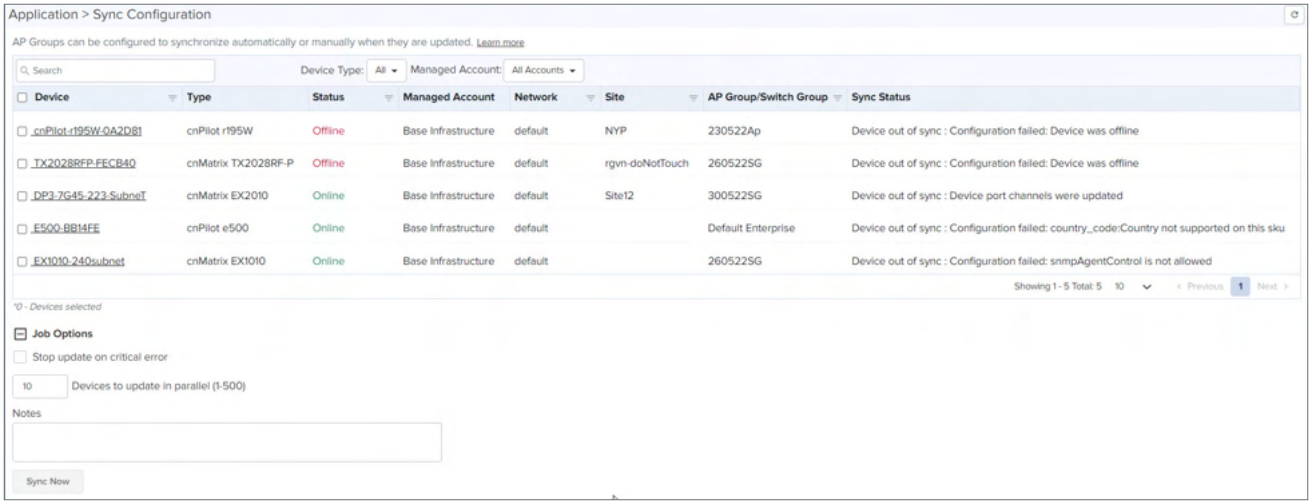
Switches by default synchronize automatically (so any change of switch group, followed by a Save, will immediately push configuration to the devices without manual intervention).

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately. The page is located at **Administration > Sync Configuration**.

To sync the device manually, navigate to **Administration** > **Sync Configuration**. This location can also be accessed by clicking the **Sync** button on the **Switch Groups** page.

Figure 337 *Sync Configuration page*



Sync Configuration has the following fields:

- Device (Hostname)
- Type
- Status (Online/Offline)
- Network (Network in which device is present)
- Site (Site under which device is present)
- Configuration Group (AP Group/Switch Group to which device is mapped)
- Sync Status (Sync status will tell whether job is completed or failed)

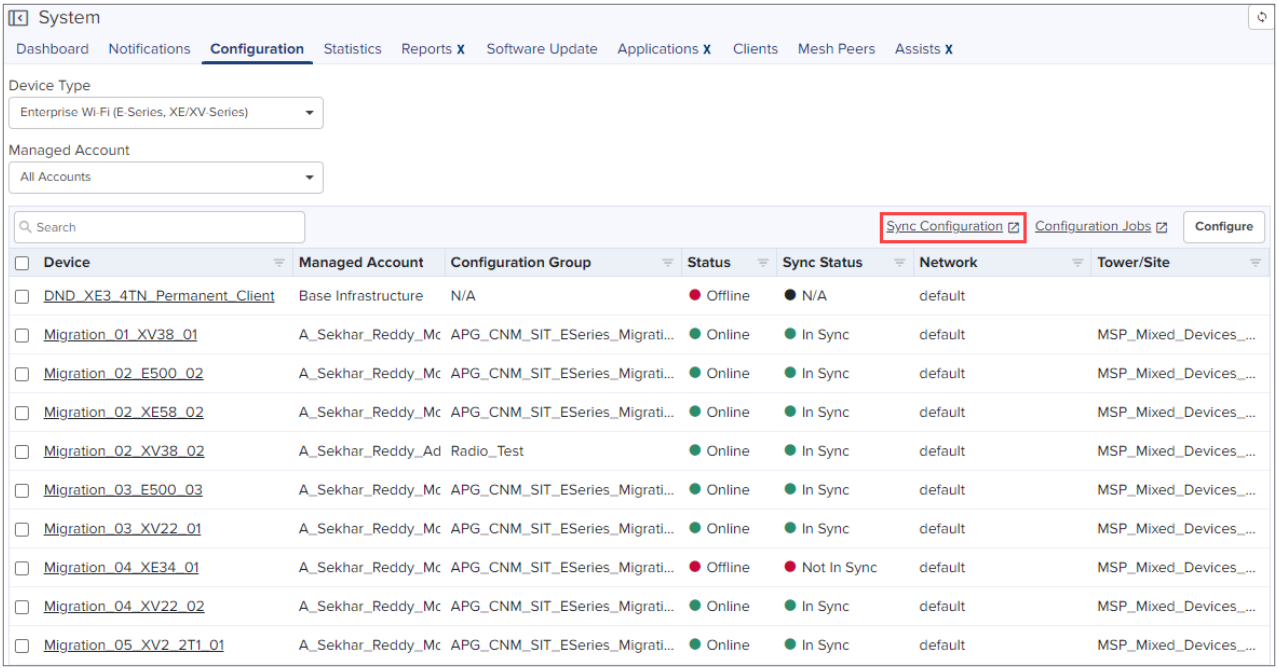
Table 70 *Sync Configuration parameters*

Parameter	Description
Configuration Group	AP Group or Switch Group to which the device is mapped.
Device	Name of the device or hostname.
Network	Network in which device is present.
Site	Site under which device is present.
Status	Status of device online or offline.
Sync Status	Sync status specifies whether job is completed or failed.
Type	Name of the device platform.

Steps to Sync Configuration:

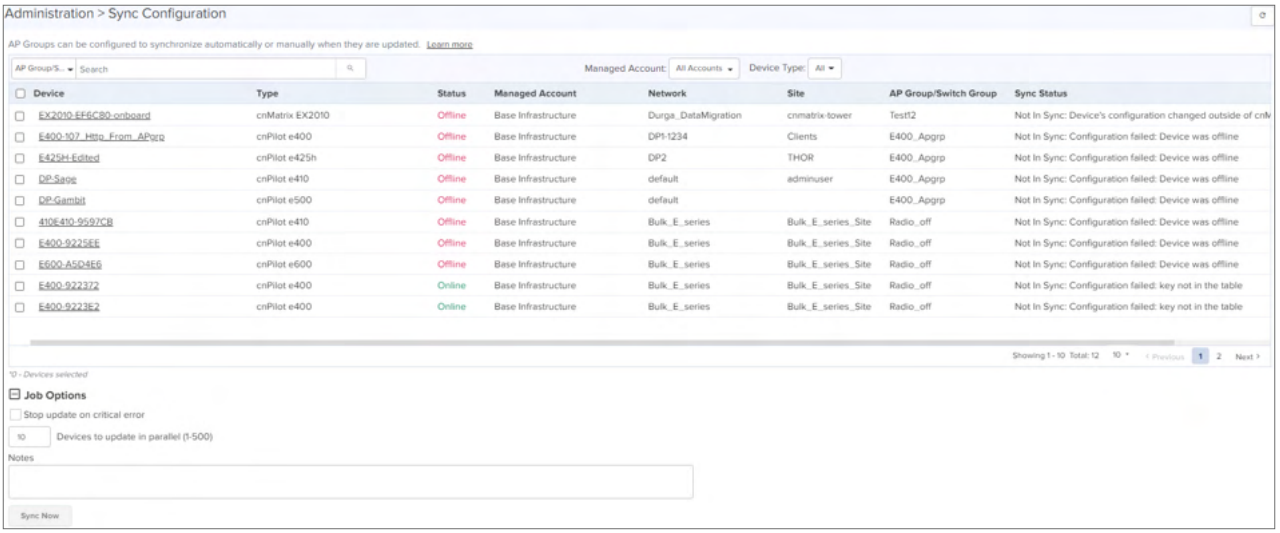
Navigate to **Monitor and Manage** > **Network** > **Configuration** or the **Jobs** tab.

1. Navigate to **System** > **Configuration** > **Sync Configuration.**
2. Select the devices to synchronize and click **Sync Configuration.**

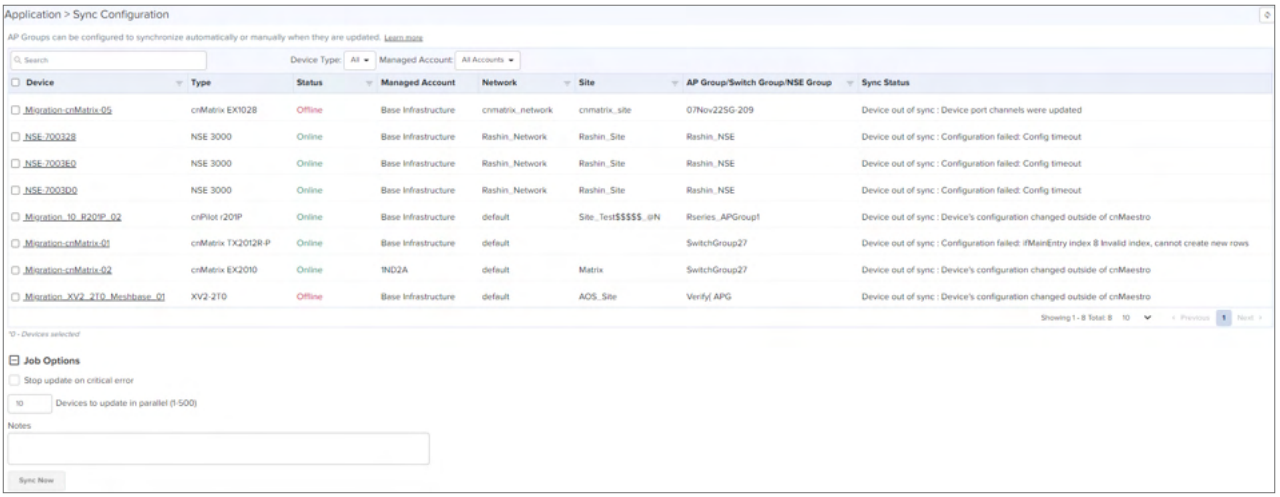


3. The **Administration** > **Sync Configuration** page is displayed.

   Select the devices to synchronize.



4. Click **Sync Now**.



User can also synchronize devices from **Application** > **Sync Configuration**.

Note

Sync configuration can only be used if a Switch Group is already mapped to the device.

Policy Based Automation (PBA)

Cambium Networks PBA feature fully automates commonly performed operations, improving network security while eliminating potential configuration errors. It allows the user to automatically configure switch port settings based on the device connected to the port. These dynamic PBA settings remain in-use for the duration of the device connection and are automatically cleared when the device disconnects from the switch.

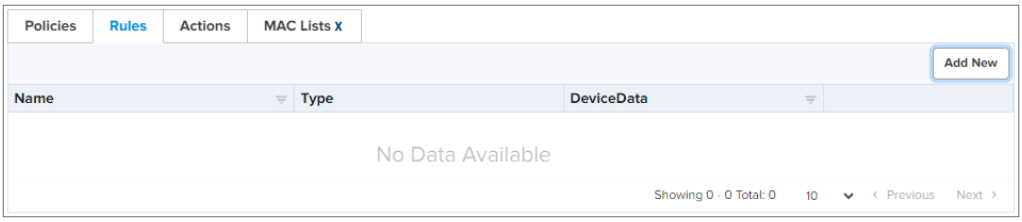
PBA configuration is common to all switches within a Switch Group.

Note

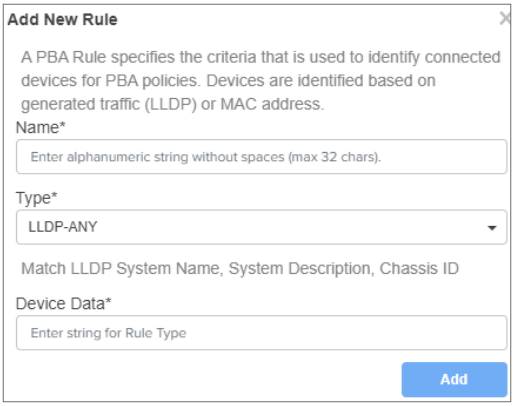
Dynamic PBA updates are indicated by asterisk * on the Switch Dashboard and on the Switch Ports pages.

Configure the PBA as follows:

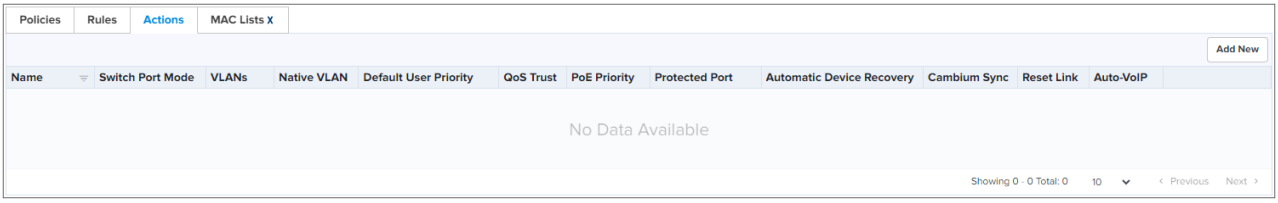
1. Navigate to **Configuration > Switch Groups > Network > Policy Based Automation.**
2. Navigate to **Rules** tab**.**



3. Click **Add New** to set the rules.



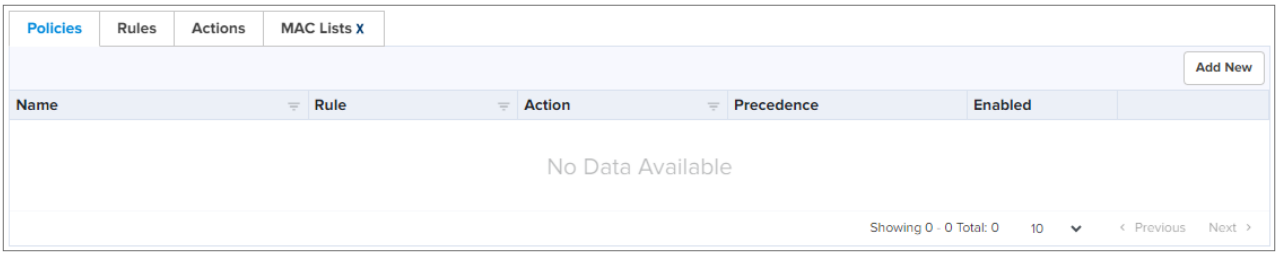
4. Click **Add**.
5. Navigate to **Actions** tab.



6. Click **Add New** to set the actions.

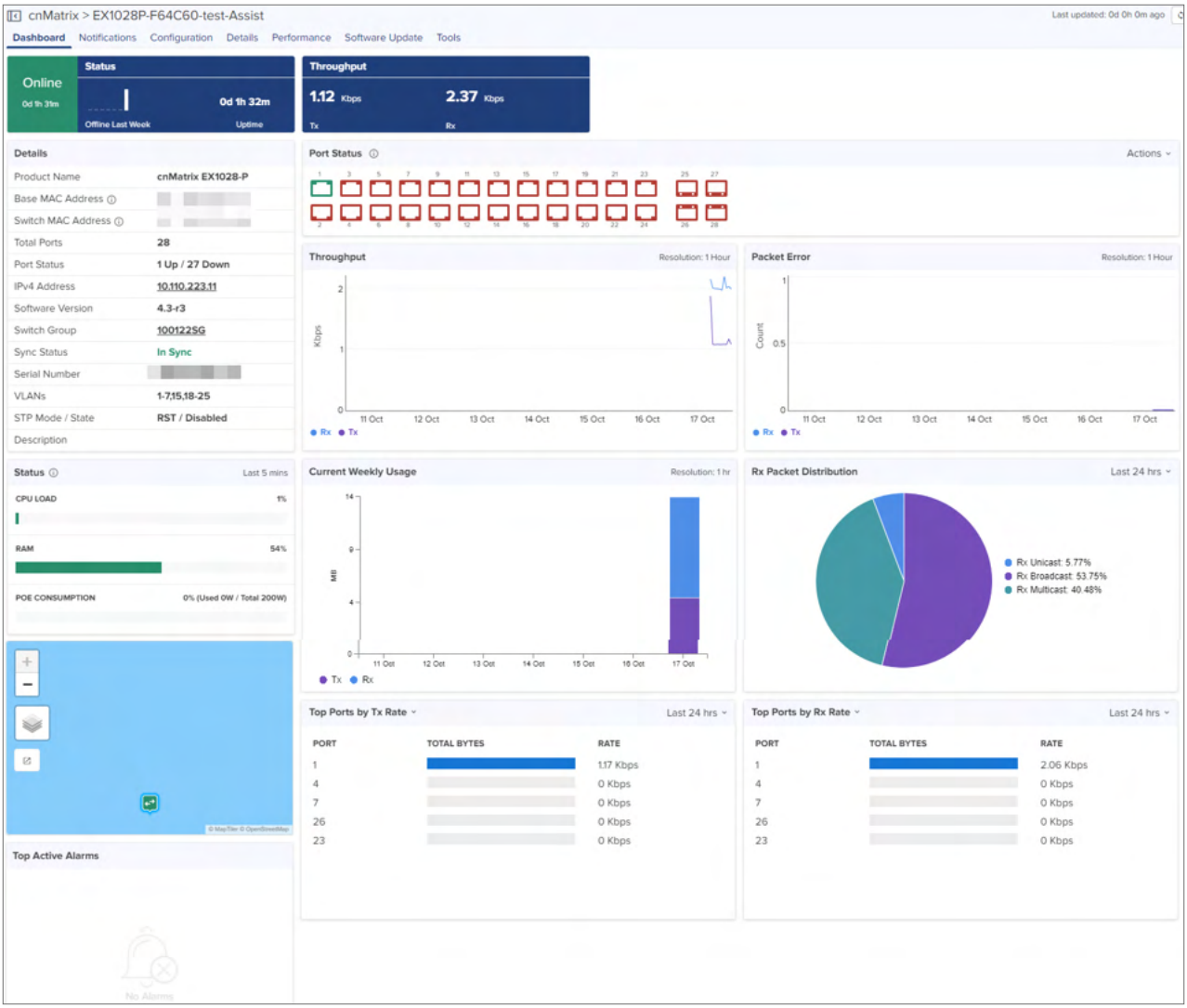


7. Click **Add**.
8. Navigate to **Policies.**



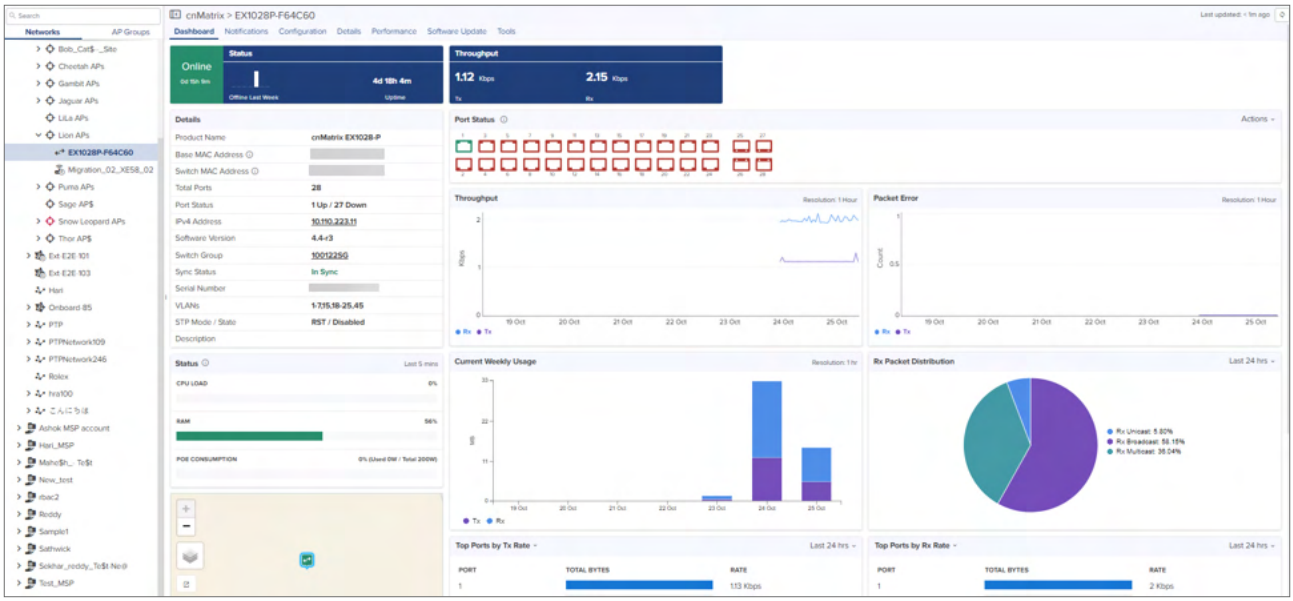
9. Click **Add New** to set the policies.



10. 

In the cnMatrix dashboard, user can navigate to the following pages using the **Action** drop-down menu in Port Status.

- Port Configuration
- Port Statistics
- Topology
- Remote CLI
- Port Operations



Switches

This section contains the following topics:

- Export Switches
- cnMatrix Switches
- Action
- Switch Configuration

The Switches page is accessed by selecting the **Switch Groups > Switches** tab lists all of the physical switches assigned to the Switch Group. The Switch Dashboard and switch override configurations settings are accessible through this page.

Switch overrides allows certain attributes for each switch to be configured individually.

Note

For configuration, a switch must belong to a Switch Group.

Configure the Switch Group as follows:

- Navigate to **Switch Groups >** select the switch from the list and click **Switches** page to view and edit the onboarded switches.

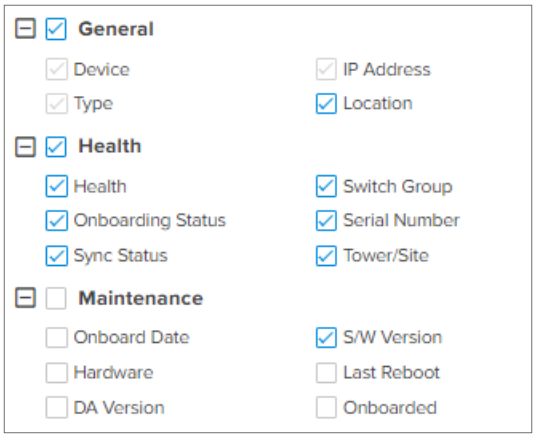


The Switches details view displays following fields by default:

- Device, Health, Onboarding Status, Serial Number, IP Address, Switch Group, Type, Site, and Action tab.

Action column can be used to edit or delete any device of the Switches.

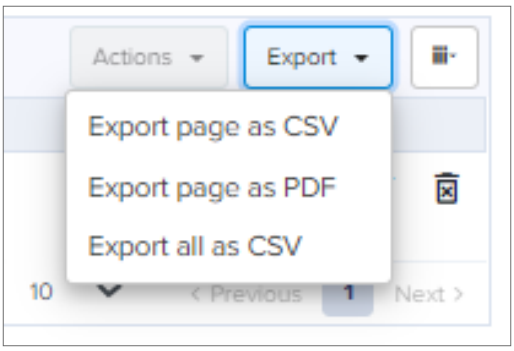
User can click on top bar to include additional fields in Switches Detail view.



Export Switches

Perform the following steps to export the Switch table:

1. Click **Export**. A dialogue box appears.

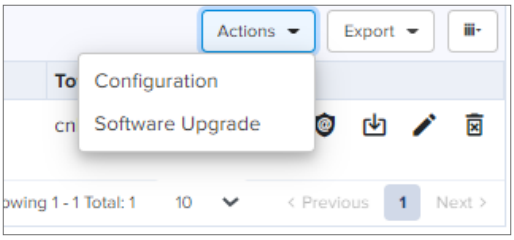


2. Select **Export page as CSV/PDF/all as CSV** and export the file.

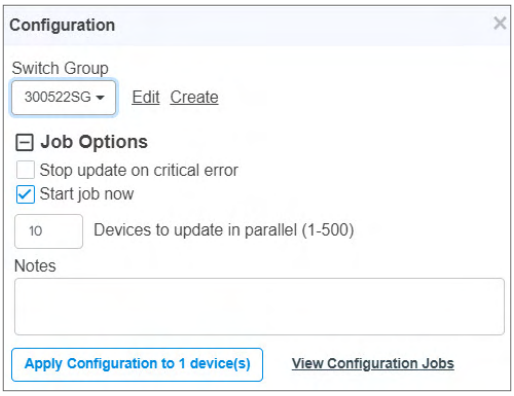
Action

Action column can be used to edit or delete any device of the Switches.

1. Click **Action**. A dialogue box appears.



2. Select Configuration to edit the device details or click the edit (✎) icon.



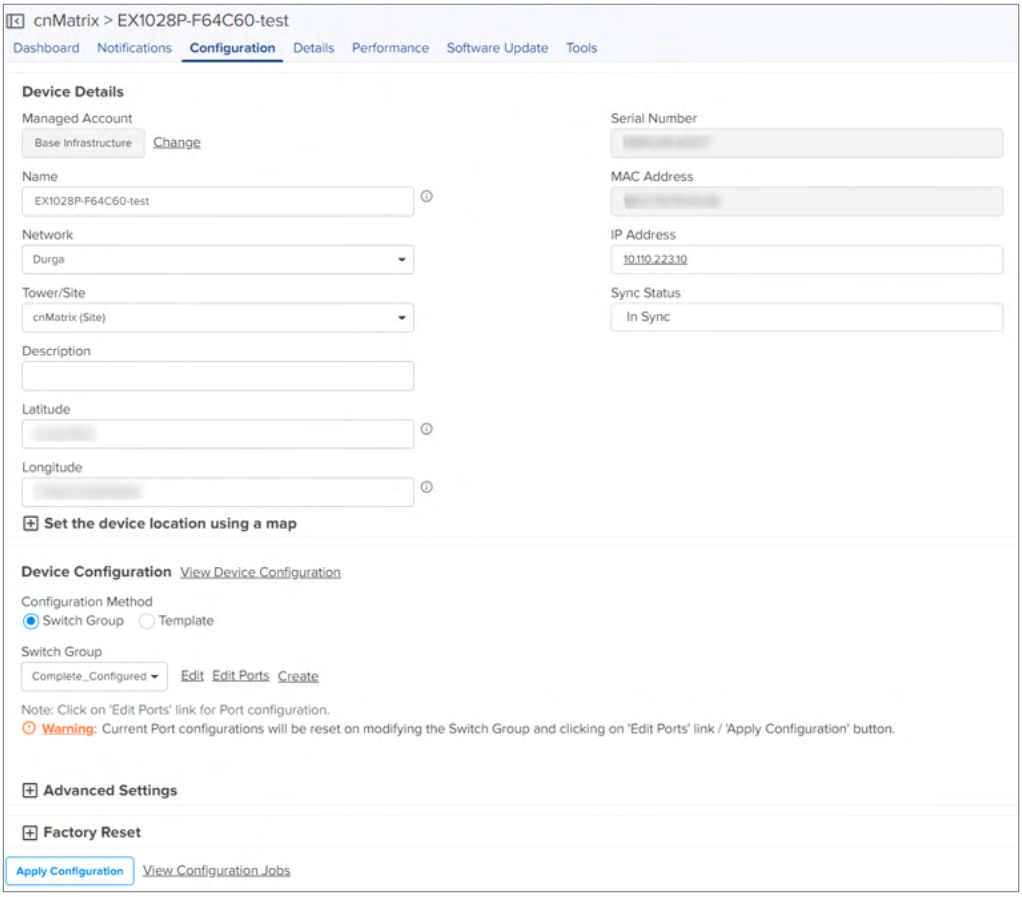
3. Select Software Upgrade to update the device software or click the (⬇) icon.
4. Click the delete (🗑) icon to delete the selected device from the list.

Switch Configuration

To edit or configure the switches, click the **Edit** or **Configuration** from the **Action** drop-down.

Navigates to the Device **Configuration** page.

1. Enter the **Device Details, Set the service location** and **Device Configuration.**



2. Click **Apply Configuration**.

In the Configuration page, you can override the group configuration with device-specific configuration:

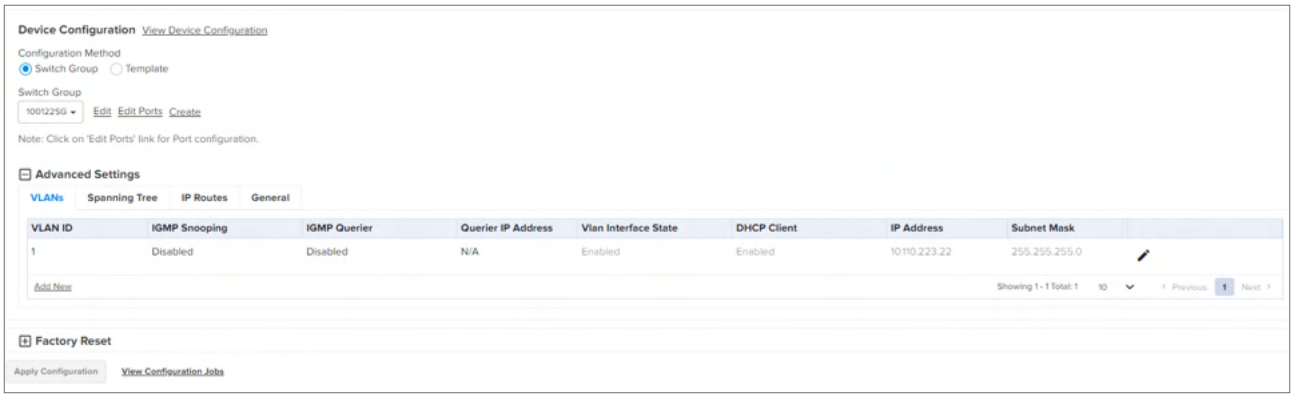
- Device Configuration
- Advanced Settings
- Factory Reset

Device Configuration

Device Configuration allows you to configure the Configuration Method as Switch Group/Template.

Switch Group Configuration Method

Enable the Switch Group and select a device from the Switch Group drop-down.



To Edit or Create a Switch Group. Refer to the Switch Groups Configuration.

Advanced Settings

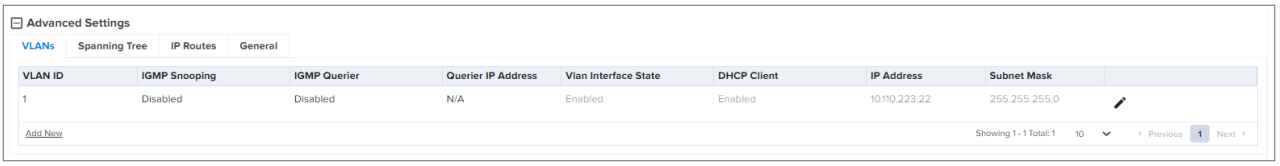
Navigate to the Advanced Settings and configure the following parameters:

- VLANs
- Spanning Tree
- IP Routes
- General

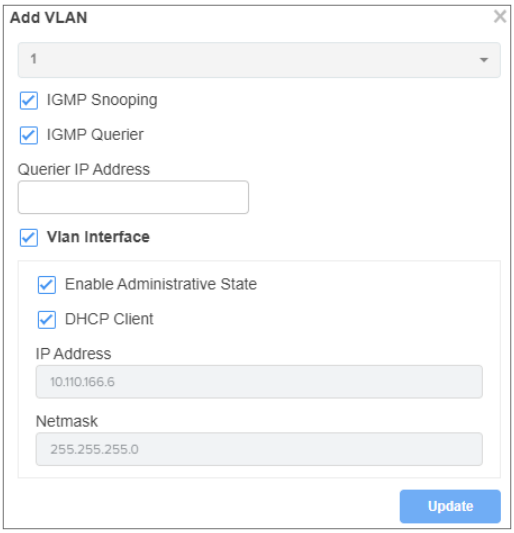
VLANs

VLANs interface allows the user to edit/Add the VLAN details such as **VLAN ID, DHCP Client, IP Address**, and **Subnet Mask.**

- Click **Advanced Settings** in **Configuration** page and navigate to **VLAN Interface** tab.



- Click the edit (✎) icon or **Add New**.
- Enter the required details and click **Add**



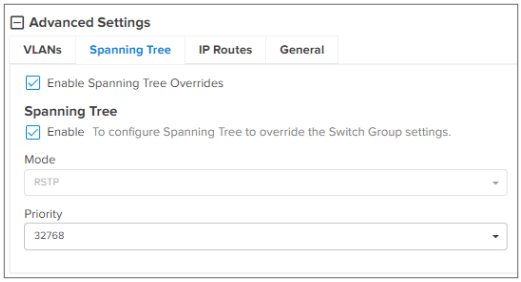
Spanning Tree

Certain configuration parameters are different for each Switch, and these are highlighted within cnMaestro as Overrides.

Configure the spanning tree to override as follows:

- Click **Advanced Settings** in **Configuration** page and navigate to **General** tab.
- ● Click **Enable Spanning Tree Overrides.**

- Select the **Spanning Tree** parameters.



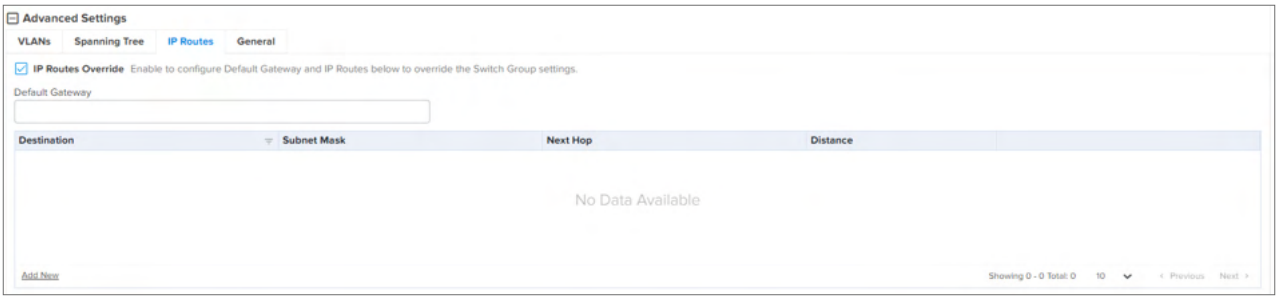
Note

If Spanning Tree is disabled the overrides feature will be disabled on the Switch configuration.

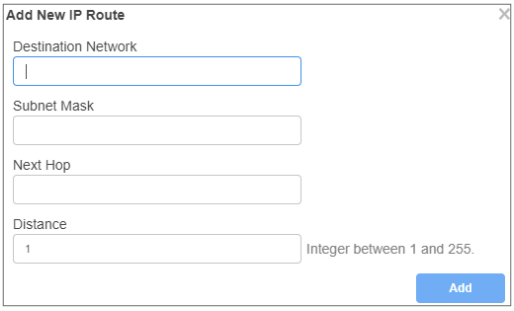
IP Routes

IP Routes allows the user to configure the Default Gateway and IP Routes to override the Switch Group.

- Configure the IP Route as follows:
- Enable the **IP Routes Override** and enter the **Default Gateway.**



- Click **Add New**.
- Enter the parameters such as Destination Network, Subnet Mask, Next Hop, and Distance.
- Click **Add.**



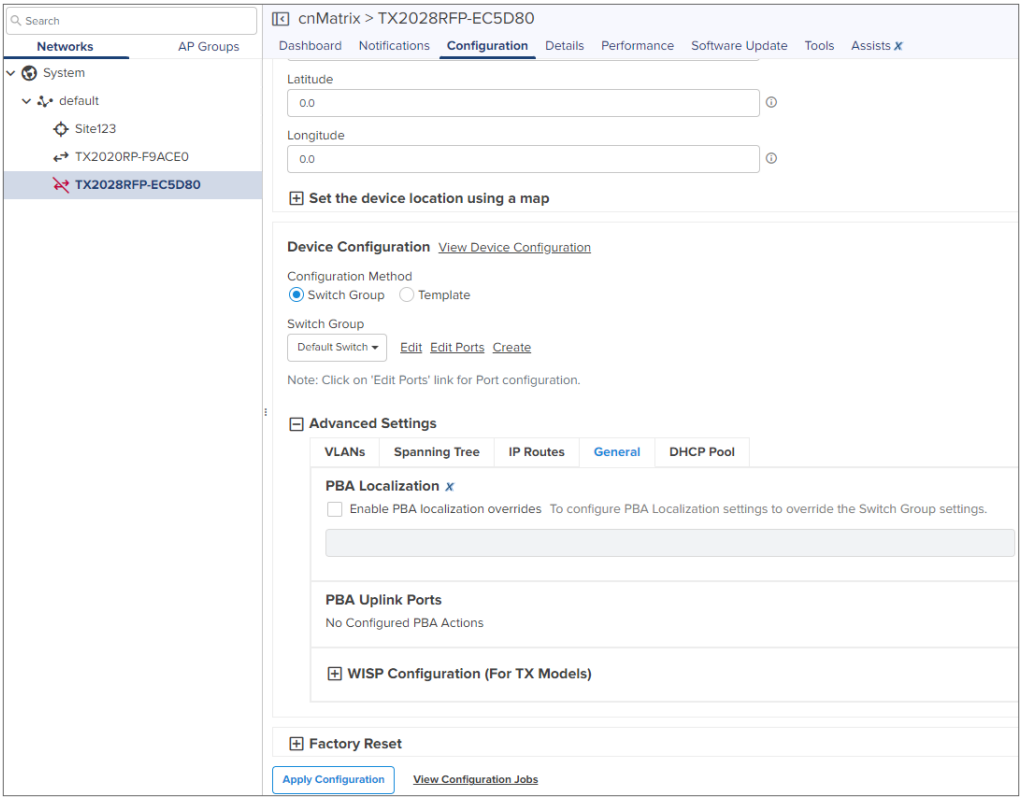
Default gateway IP will override the all IPs of the Switch Groups.

General

General tabs allows to configure PBA Localization settings to override the Switch Group settings.

To configure the PBA localization, perform as follows:

- Click **Advanced Settings** in **Configuration** page and navigate to **General** tab.

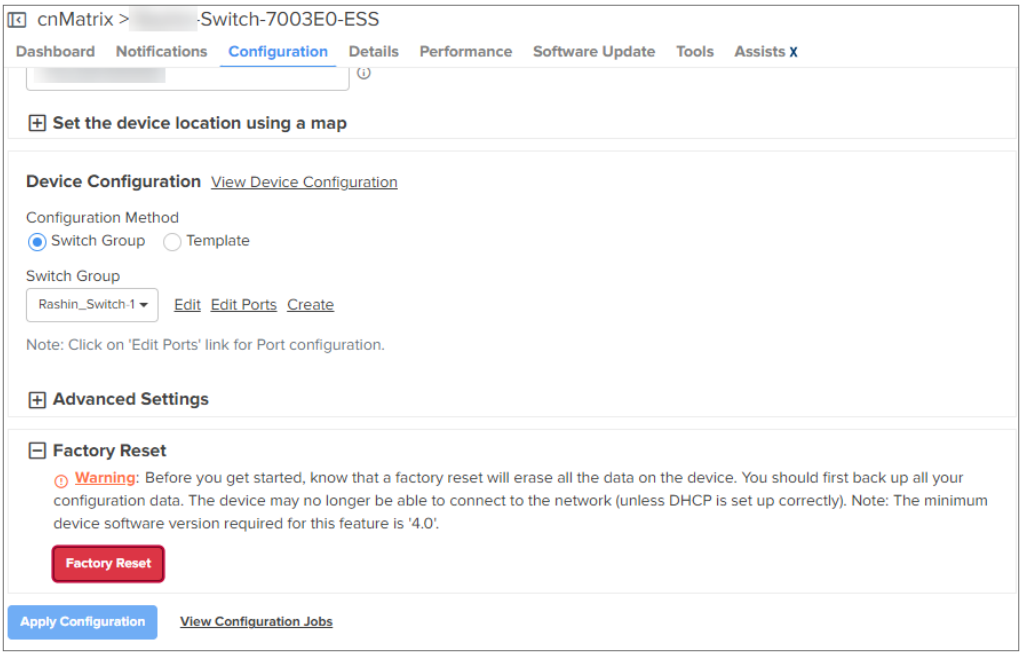


- Enable **PBA localization** overrides.
- Select **Use Site Name** or **Custom**.
- Enter **PBA Uplink Ports**.

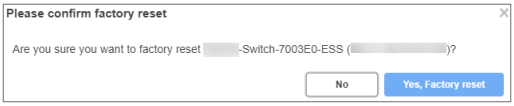
Factory Reset

To erase all the configuration on the device and bring the device back to the default factory configuration, complete the following steps:

1. Navigate to the cnMatrix device **Configuration** page.
2. Expand the **Factory Reset** section. and click **Factory Reset**.



3. In the pop-up window that appears, Click **Yes, Factory reset**.



Switch Ports

The **Switch Ports** table displays the list of Ports and the Port Channel assigned to the specific switch. The **Switch Ports** table allows administrators to configure the port settings by port ID for all ports within the **Switch Group**. By default, a port ID identifies the switch (by switch name) and port number.

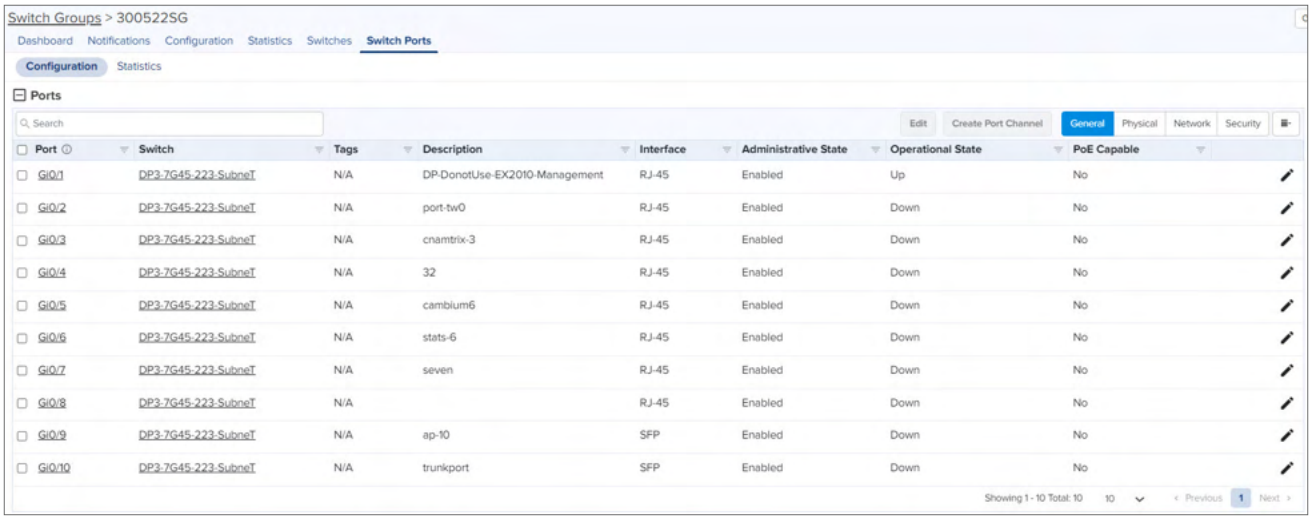
For example: Gi0/1

It supports bulk editing of Switch Port settings across all physical switches.

To view the **Switch Ports**, navigate to **Configuration** > **Switch Groups** > **Switch Ports**.

Ports

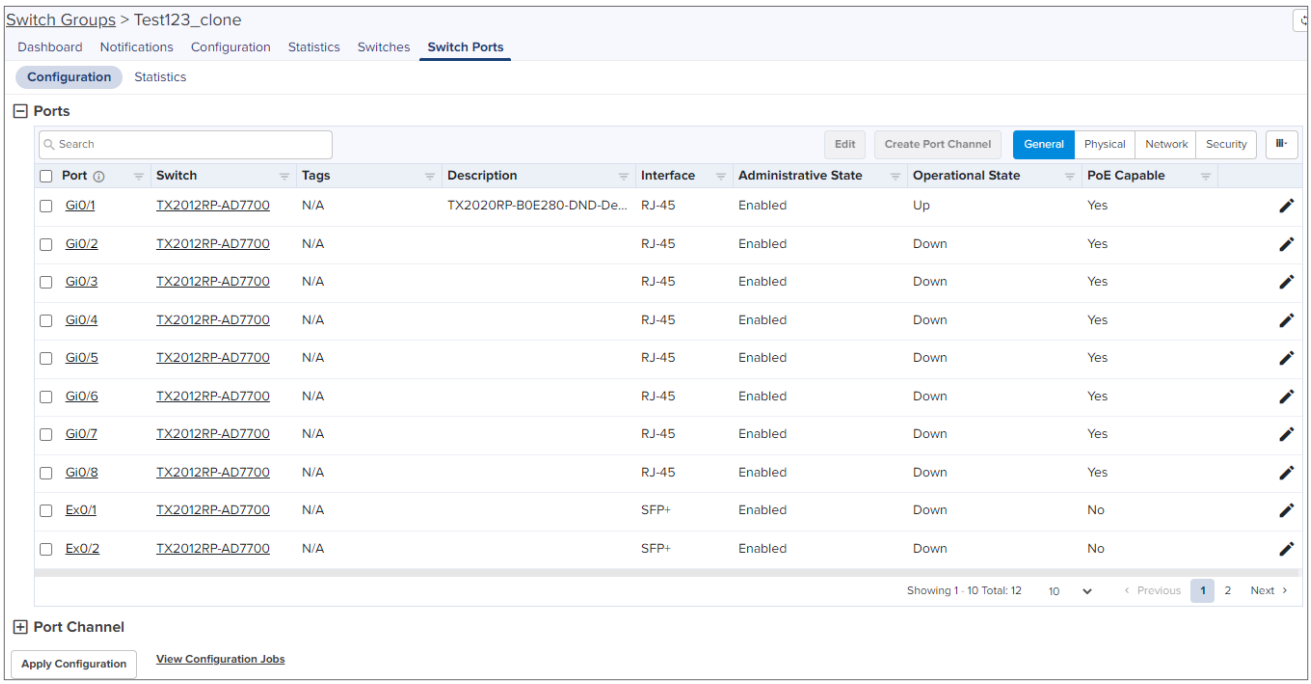
The **Ports** table supports creating port channels, editing port configuration and configuring port parameters.



Navigate to **Switch Ports** > **Configuration** tab, configure the following parameters:

- General
- Physical
- Network
- Security

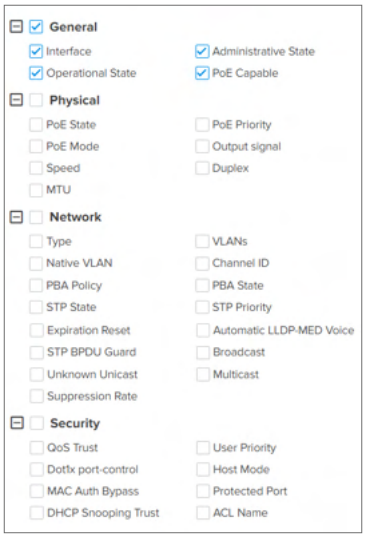
General Tab



The **Ports** General details view displays following fields by default:

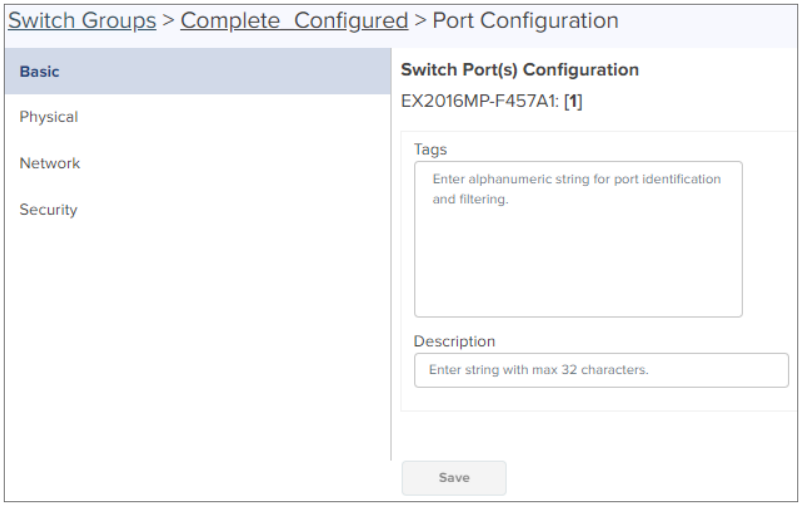
- Port, Tags, Description, Interface, Administrative State, Operational State, PoE Capable, and Edit.
- Click on **Apply Configuration** whenever you are sure to apply the modified configuration, preferably after all the port details are updated.

User can click on top bar to include additional fields in **Ports** General Detail view.



Click the edit ( ) icon or Port device in the list to edit the Ports Configuration General tab details.

Navigate to **Switch Groups > Switches > Port Configuration.**



Enter the **Tags** and **Description** details and Click **Save**.

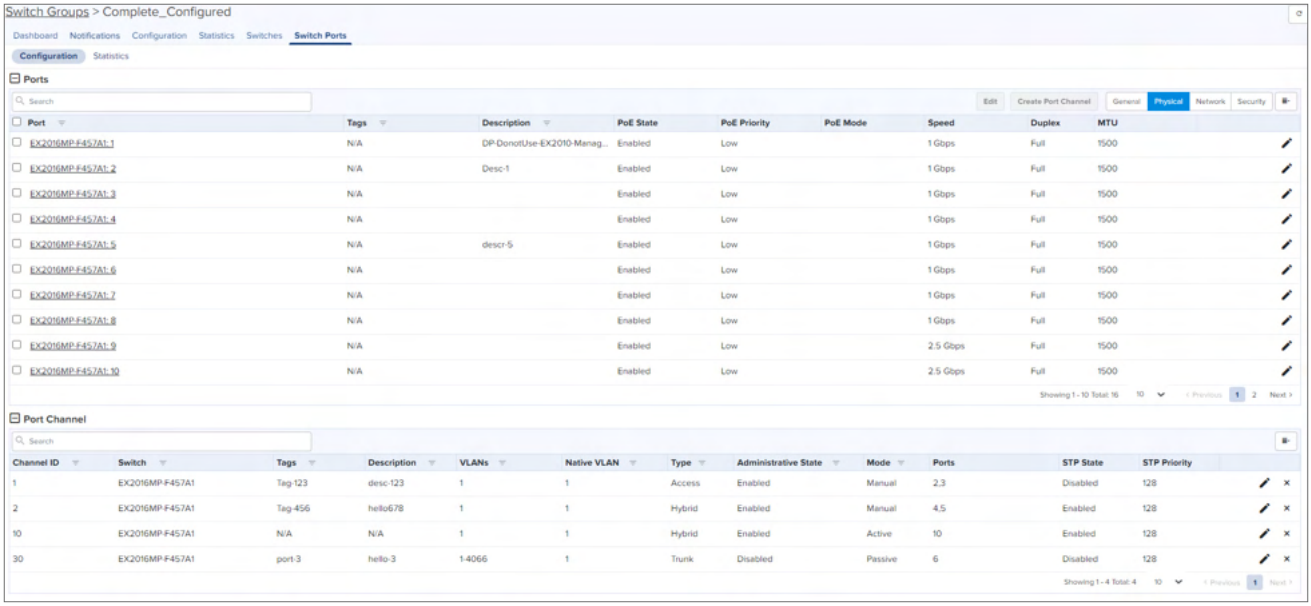
Note

After modifying the port or channel details, you can apply the configuration to the device by clicking the **Apply Configuration** button at the bottom of the **Switch Ports** page.

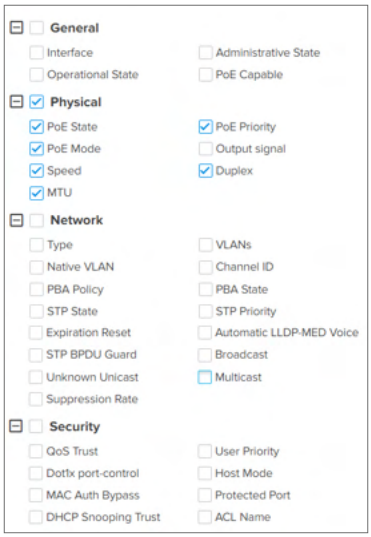
Physical Tab

The **Ports Physical** details view displays following fields by default:

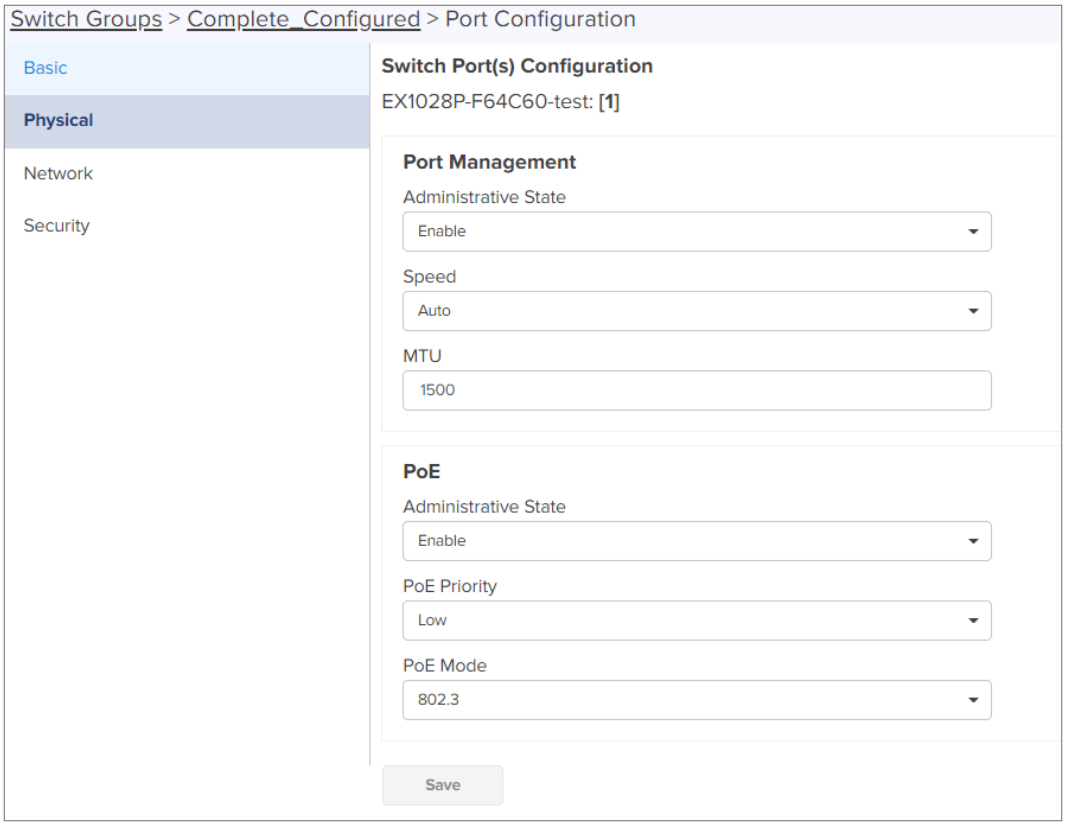
- Port, Tags, Operational State, PoE State, PoE Priority, Speed, Duplex, MTU, and Edit.



You can click on top bar to include additional fields in **Ports** Physical Detail view.



Click the edit (✎) icon or Port device in the list to edit the Ports Configuration **Physical** tab details.

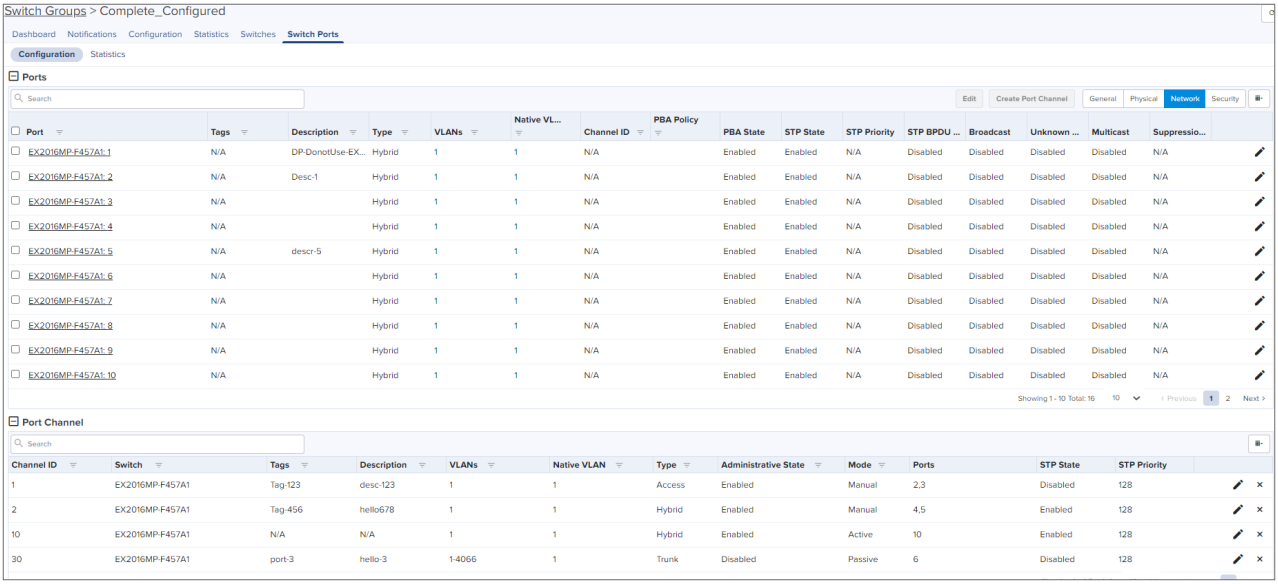


Enter the **Port Management** and **PoE details** and click **Save**.

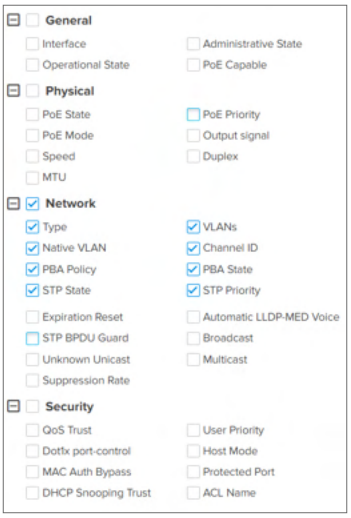
Network Tab

The **Ports Network** details view displays following fields by default:

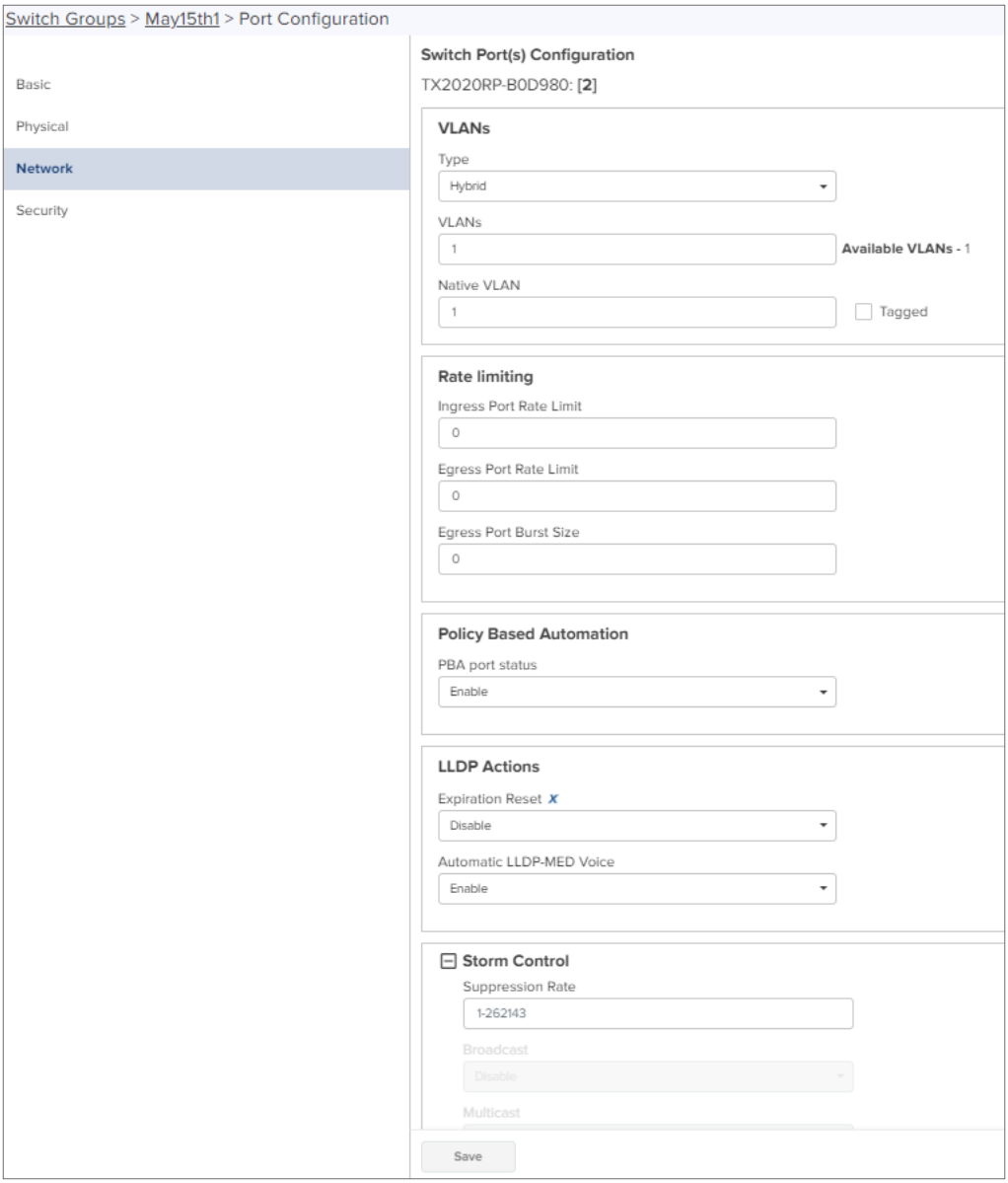
- Port, Tags, Type, VLANs, Native VLAN, Channel ID, PBA Policy, PBA State, STP State STP Priority, and Edit.



- User can click on top bar to include additional fields in **Ports** Network Detail view.



- Click the edit (✎) icon or Port device in the list to edit the Ports Configuration Network tab details.



Note

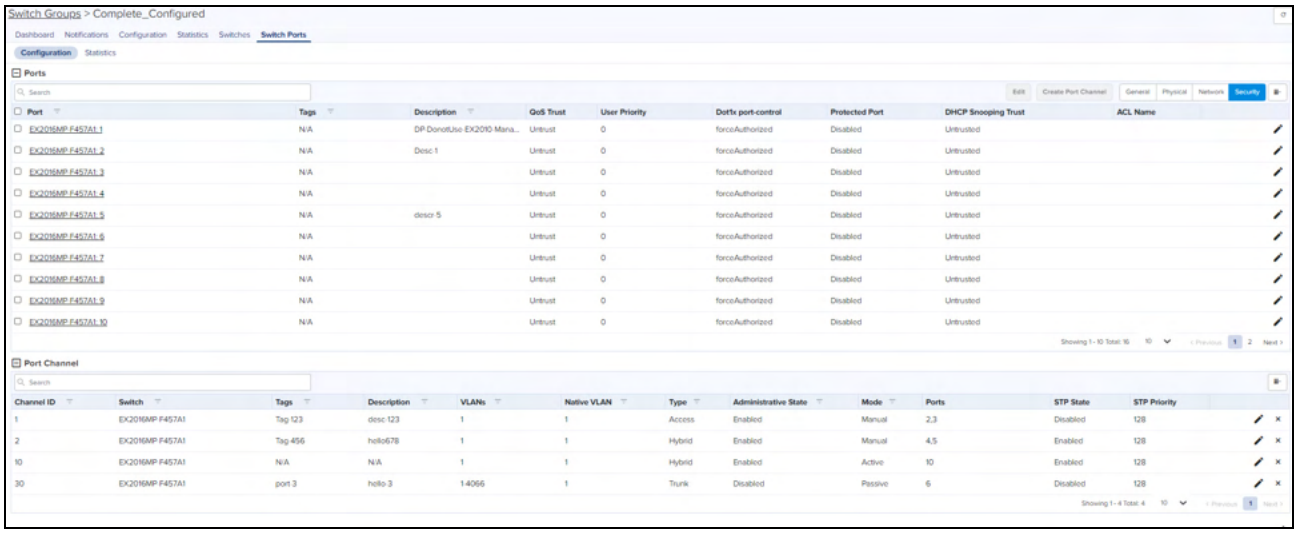
LLDP Actions > Expiration Rest option is a Pro feature.

Enter **VLANs, STP, Policy Based Automation,** and **Storm Control** details and click **Save.**

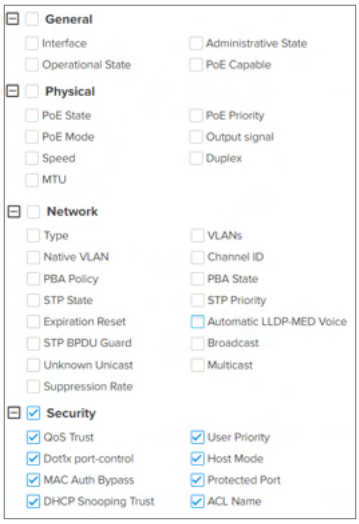
Security Tab

The **Ports Security** details view displays following fields by default:

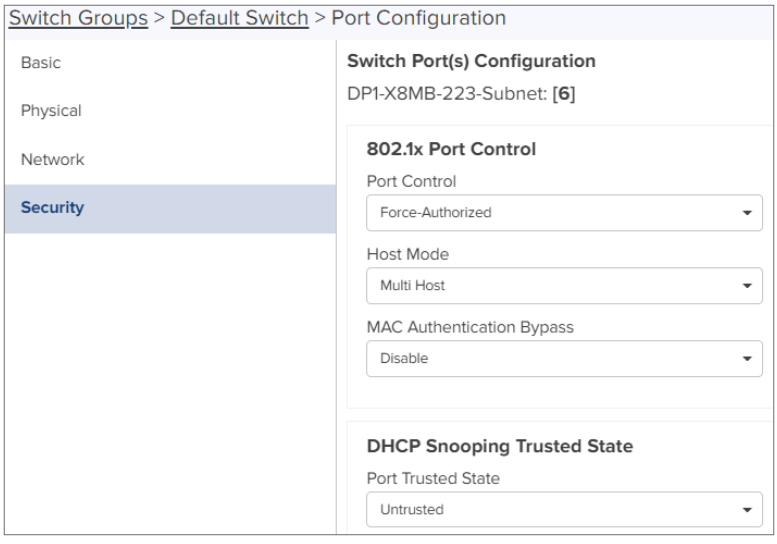
- Port, Tags, QoS Trust, User Priority, Dot1x port-control, Protected Port, DHCP Snooping Trust, ACL Name, and Edit.



User can click on top bar to include additional fields in **Ports** Security Detail view.



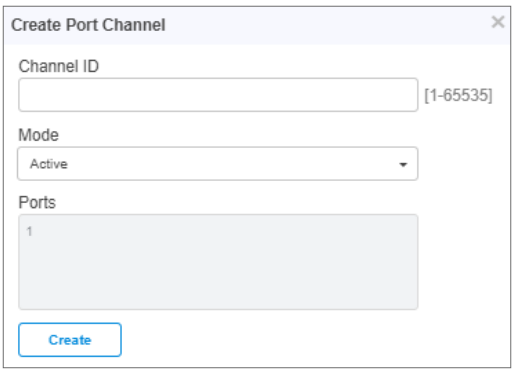
Click the edit ( ) icon or Port device in the list to edit the Ports Configuration Security tab details.



Enter **802.1xPort Control, DHCP Snooping Trusted State, QoS, Protected Port, Access Control List** details and click **Save.**

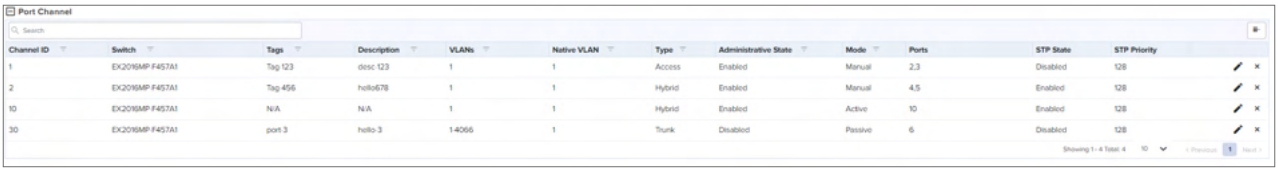
Port Channel

- To create a Port Channel, select a **Port** from the list under the specific parameters and click **Create Port Channel**.
- **Create Port Channel** window Pops-up, enter details.
- Click **Create**.

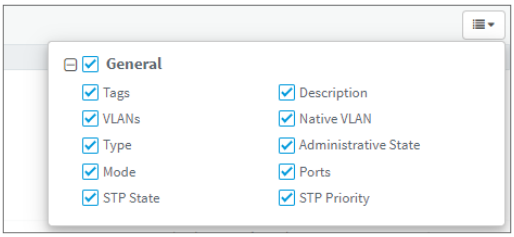


The **Port Channel** details view displays following fields by default:

- Channel ID, Switch, Tags, Description, VLANs, Native VLAN, Type, Administrative State, Mode, Ports, STP State, and STP Priority.



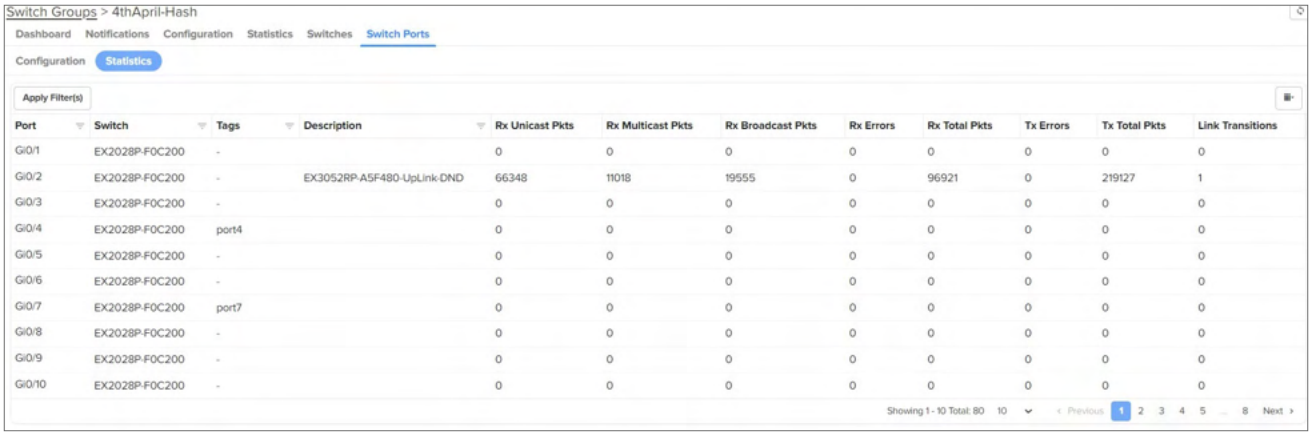
User can click on top bar to include additional fields in **Port Channel** Detail view.



Statistics

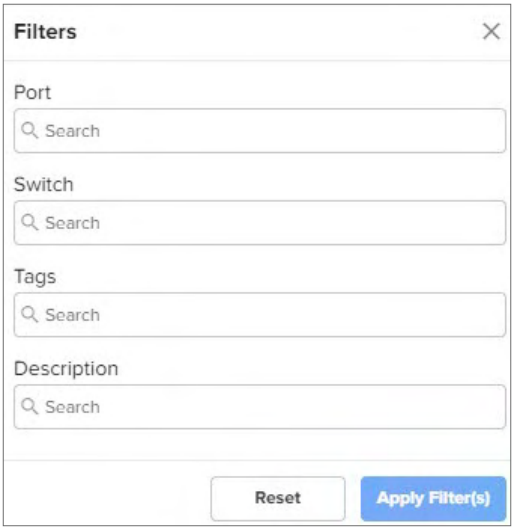
The **Statistics** page displays the latest data and statistics of each Port. Port statistics match the Client statistics and generate the Client View.

To view the Switch Ports Statics navigate to **Configuration** > **Switch Groups** > **Switch Ports** > **Statistics**.



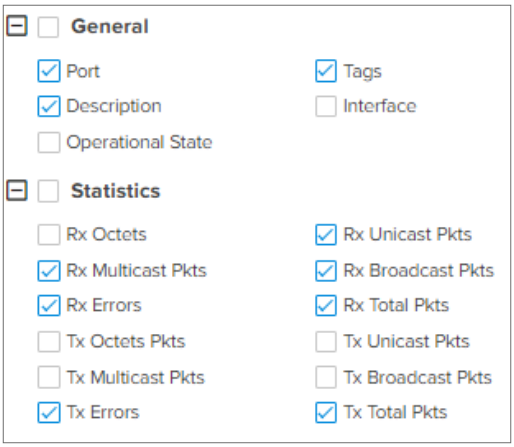
To apply filters, follow the below steps:

1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.



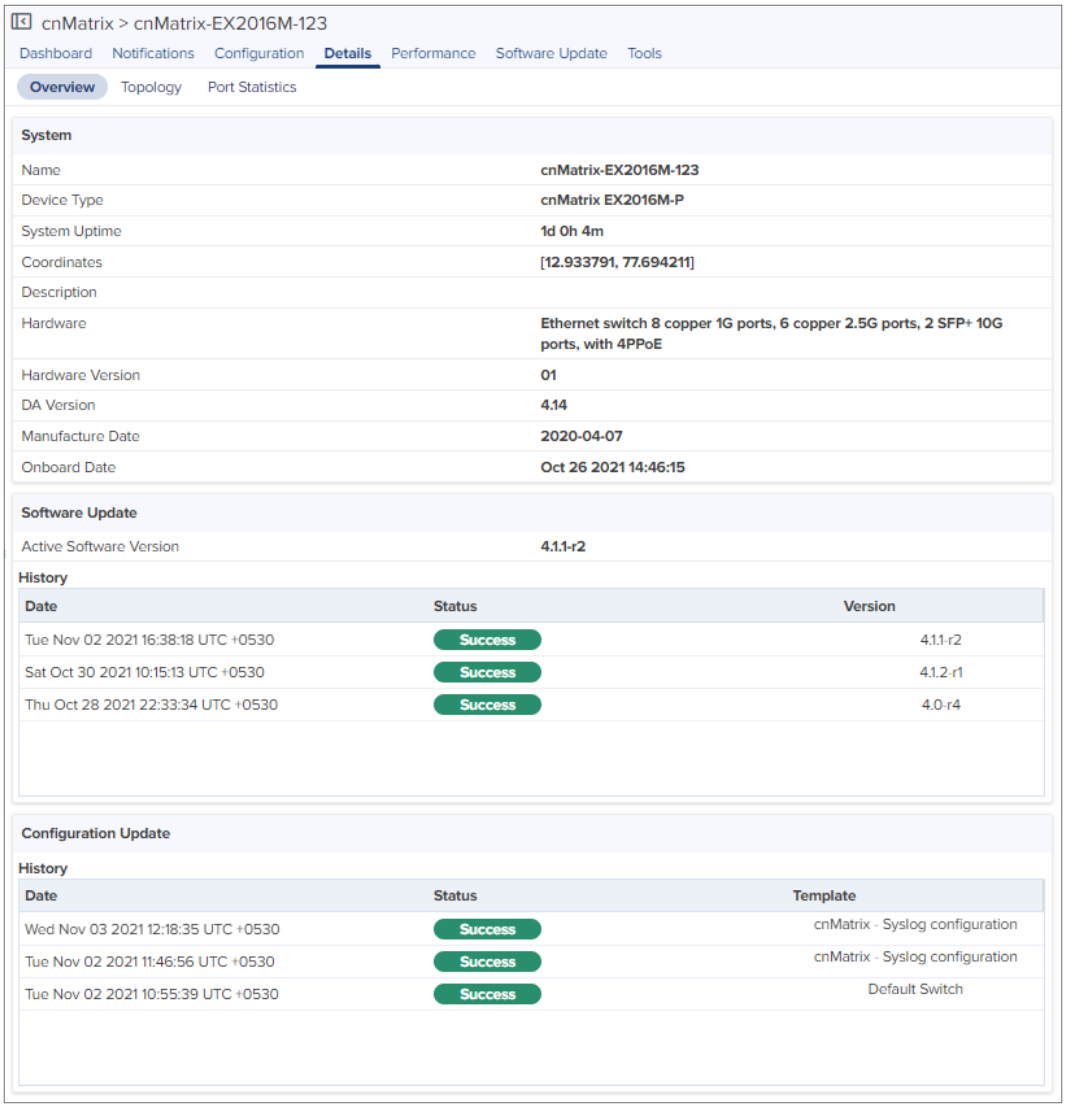
3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

   User can click on top bar to include additional fields in **Statistics** Detail view.



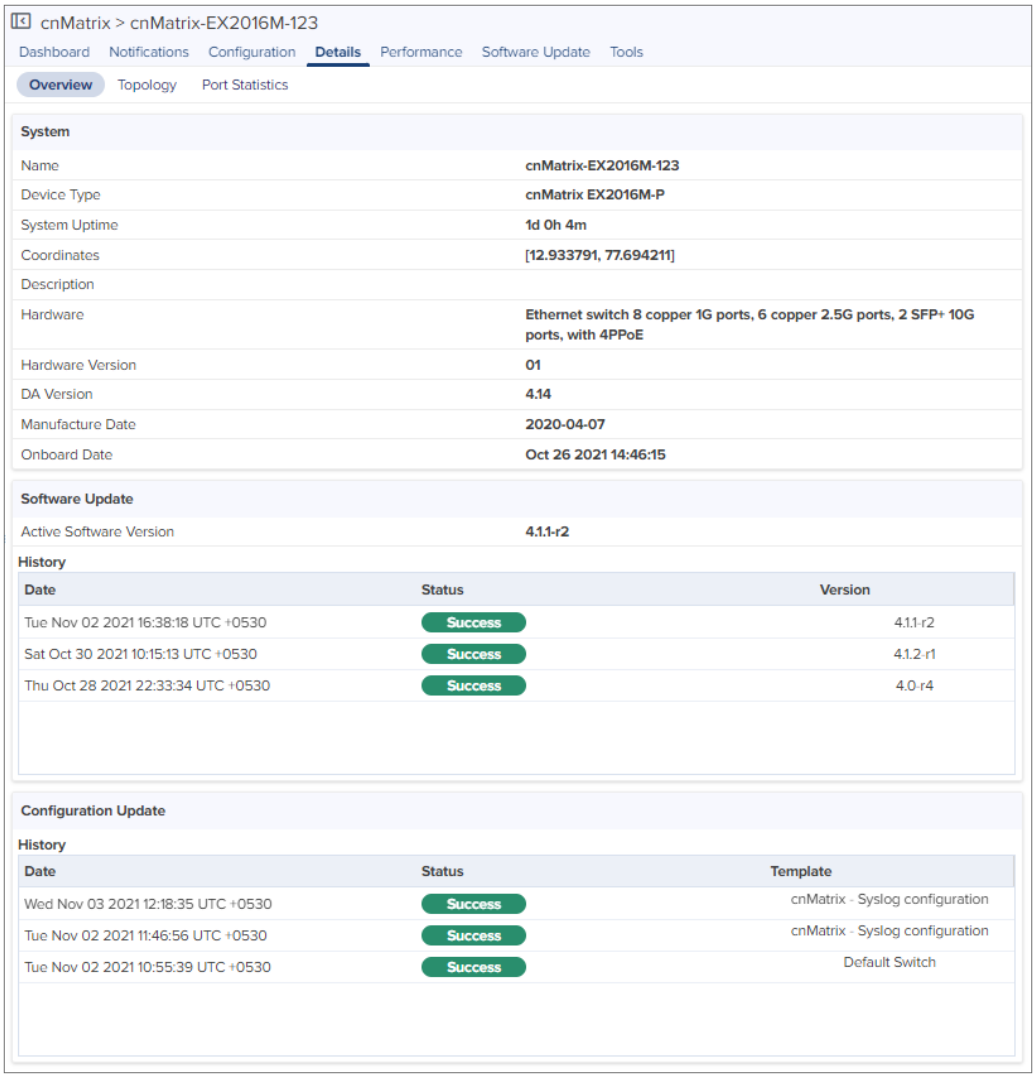
Device Details

Details page provide the information about the switches **Overview**, **Topology**, and **Port Statistics**.



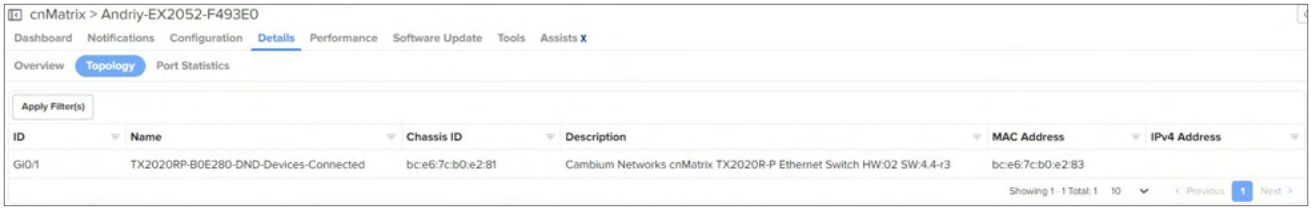
Details Overview

To view the details of the overview page, navigate to the **Details > Overview** tab.



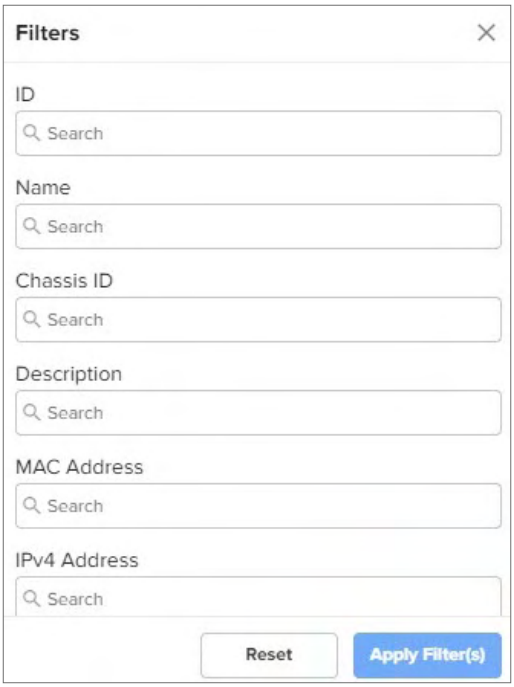
Topology

To view the details of the Topology page, navigate to the **Details** > **Topology** tab.



To apply filters, follow the below steps:

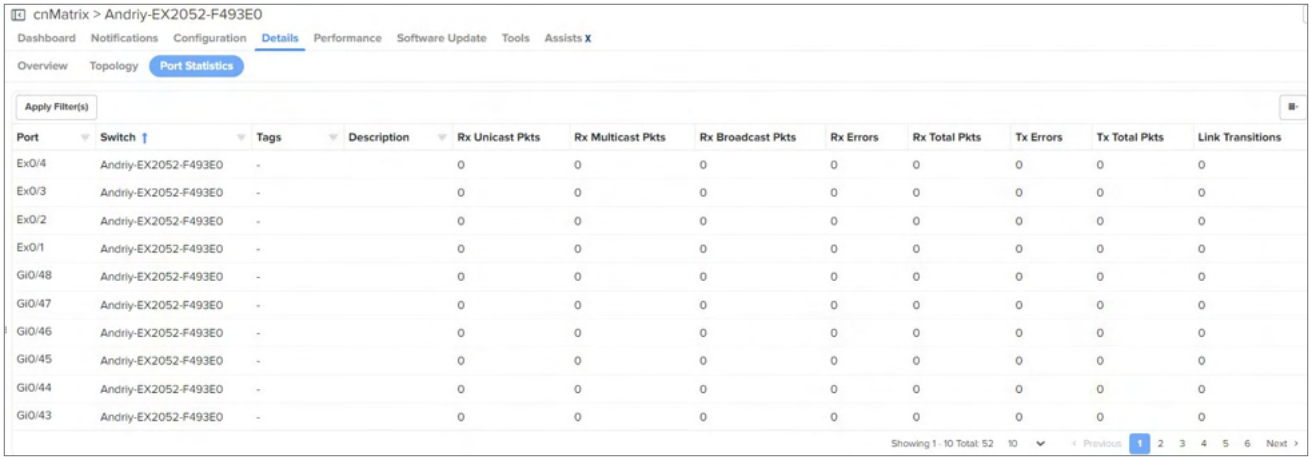
1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.



3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

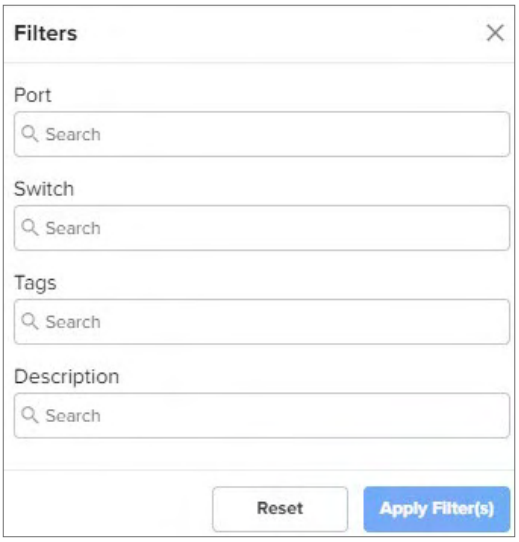
Port Statistics

To view the details of the Port Statistics page, navigate to the **Details > Port Statistics** tab.



To apply filters, follow the below steps:

1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.



3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

60 GHz cnWave Network Configuration

cnWave 60 GHz operates with Cambium Networks cnMaestro management system. cnMaestro simplifies device management by offering full network visibility and zero-touch provisioning. Using cnMaestro, user can view network status and perform a full suite of wireless network management functions in real time including optimizing system availability, maximizing throughput, and meeting the emerging needs of business and residential customers.

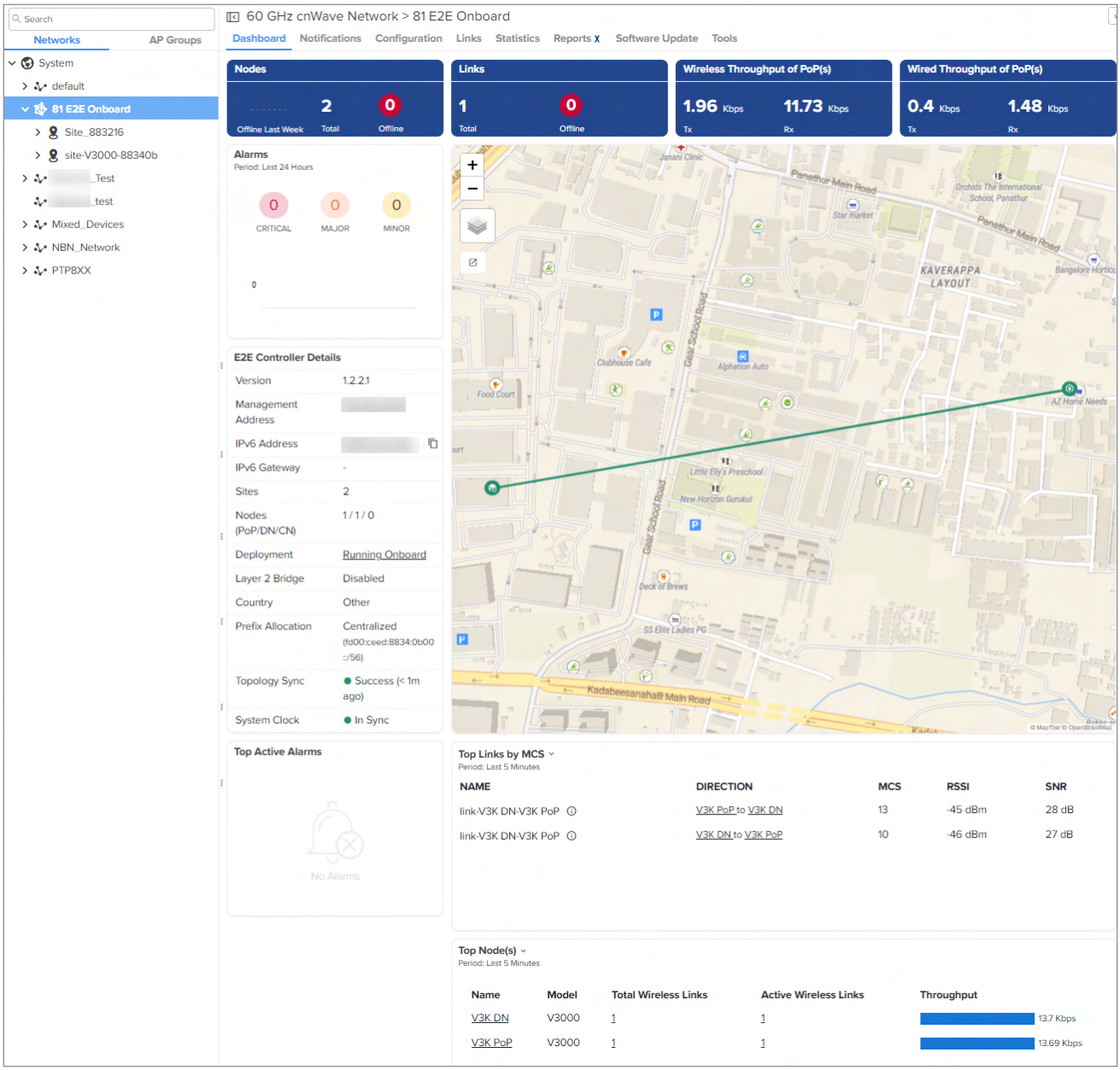
Managing E2E Network

The Monitor and Manage tab displays the monitoring panel of 60 GHz cnWave for cnMaestro. This section includes the following:

- Dashboard
- Notifications
- Configuration
- Links
- Statistics
- Software Update
- Report
- Tools

Dashboard

Dashboard pages are customized for each device type and aggregation level (such as E2E Network, Node, and Site). The dashboard section displays the **Nodes, Links, Wireless Throughput of PoP(s), Wired Throughput of PoP(s), Alarms, E2E Controller Details, Top Active Alarms, Map, Top Links by MCS, Top Links by RSSI, Top Links by SNR, Top Node(s) Top PoP(s), Top DN(s),** and **Top CN(s).**



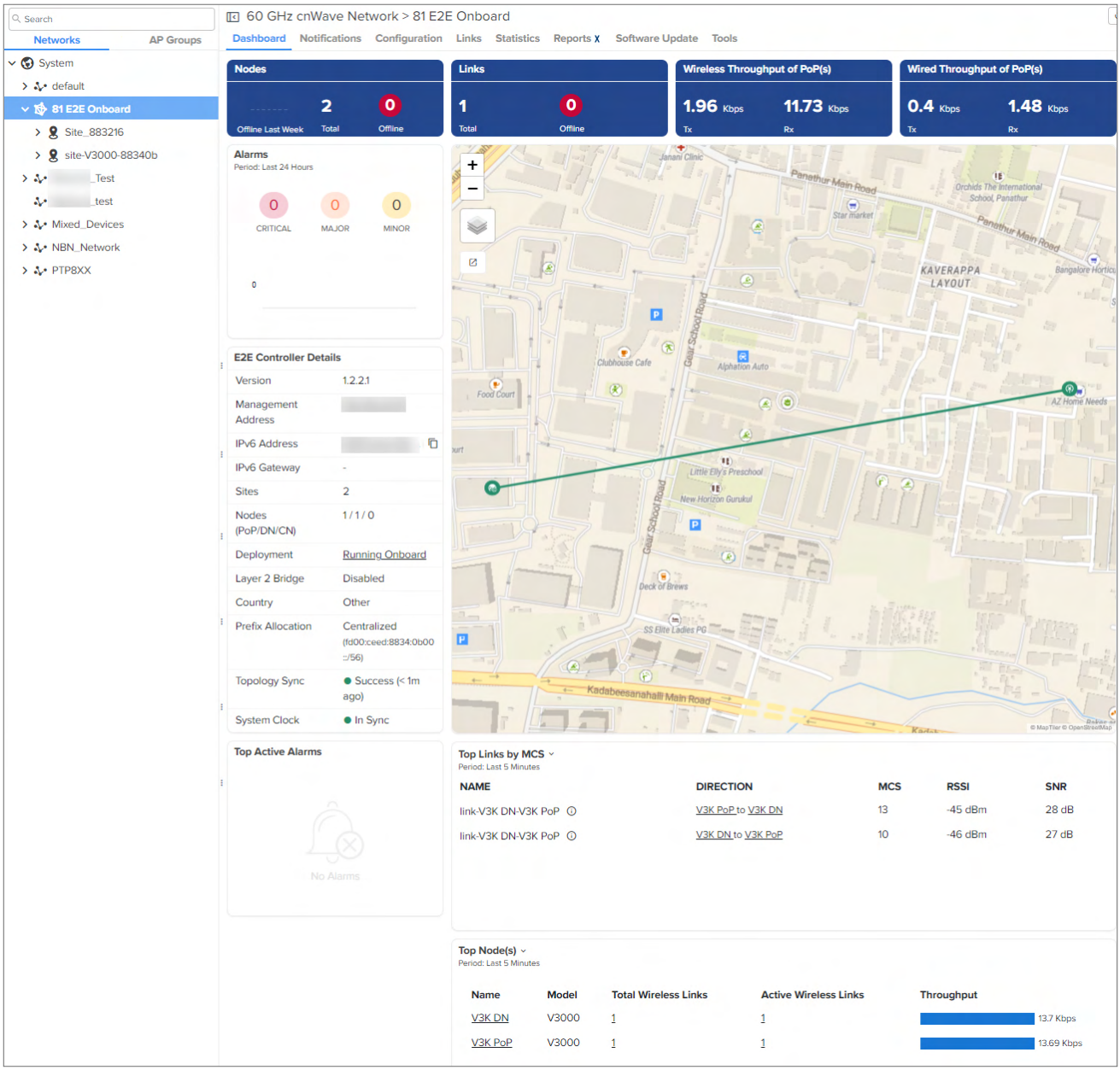
Note

Backup CN links are not shown as Offline links in links widget.

Auto Manage IPv6 Routes (E2E Controller↔ Node)

The **External E2E Network**. dashboard page displays the **Auto Manage IPv6 Routes (E2E Controller ↔ Node)** tab, if you enable **Auto Manage Routes** in the **Tools > Settings** page of **External E2E Network**.

This feature automates IPv6 routes for DNs and CNs based on status of the topology and PoP nodes. It is applicable only if PoP nodes and E2E Controller are in the same Network or containing the same prefix length.



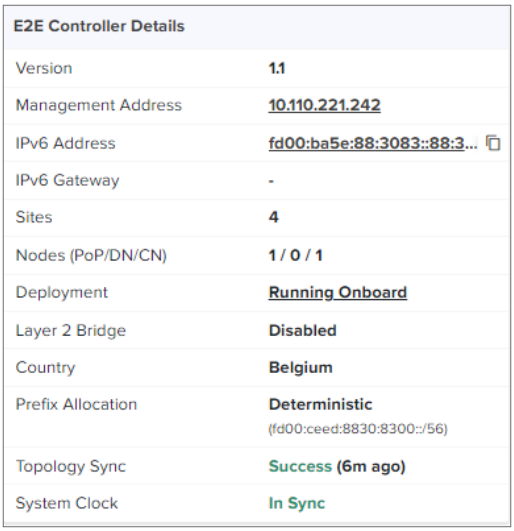
Note

Auto Manage IPv6 Routes is not applicable for Onboard E2E Controller.

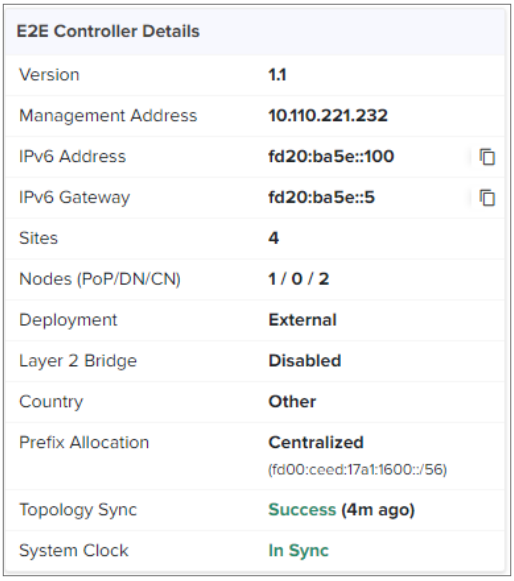
E2E Controller Details

E2E Controller Details displays the details such as **Version**, **Management Address, IPv6 Address, IPv6 Gateway, Sites, Nodes, (PoP/DN/CN), Deployment, Layer 2 Bridge, Country, Prefix Allocation, Topology Sync,** and **System Clock**

- If Onboard E2E controller is enabled in device and managed by cnMaestro, it displays deployment as **Running Onboard.**

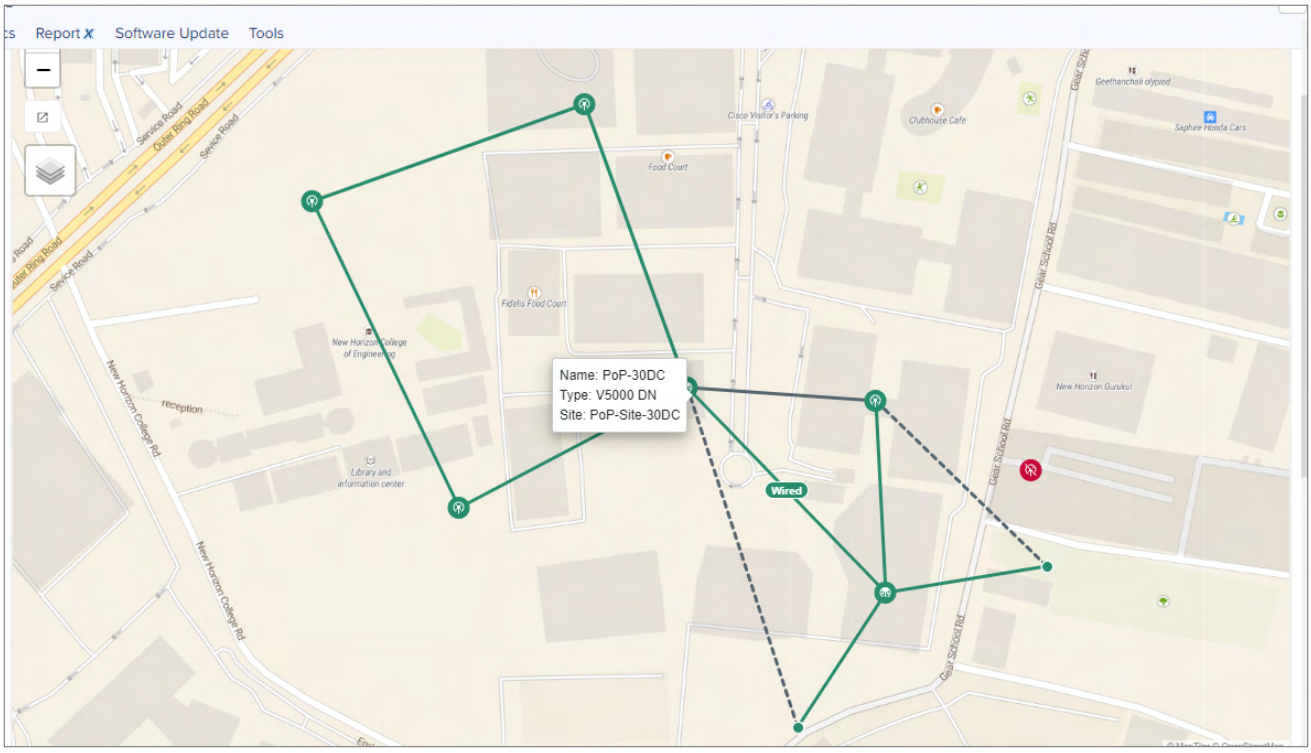


- If External E2E controller is managed by cnMaestro, it displays deployment as **External.**

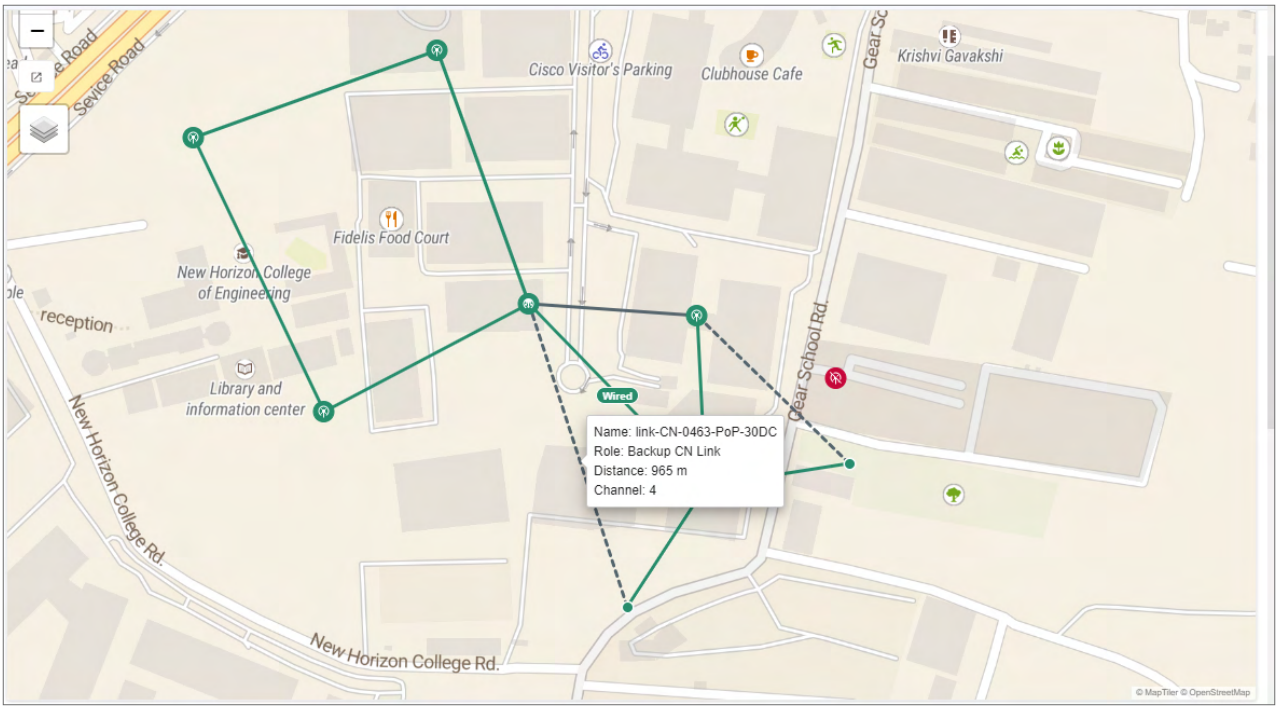


Dashboard Maps

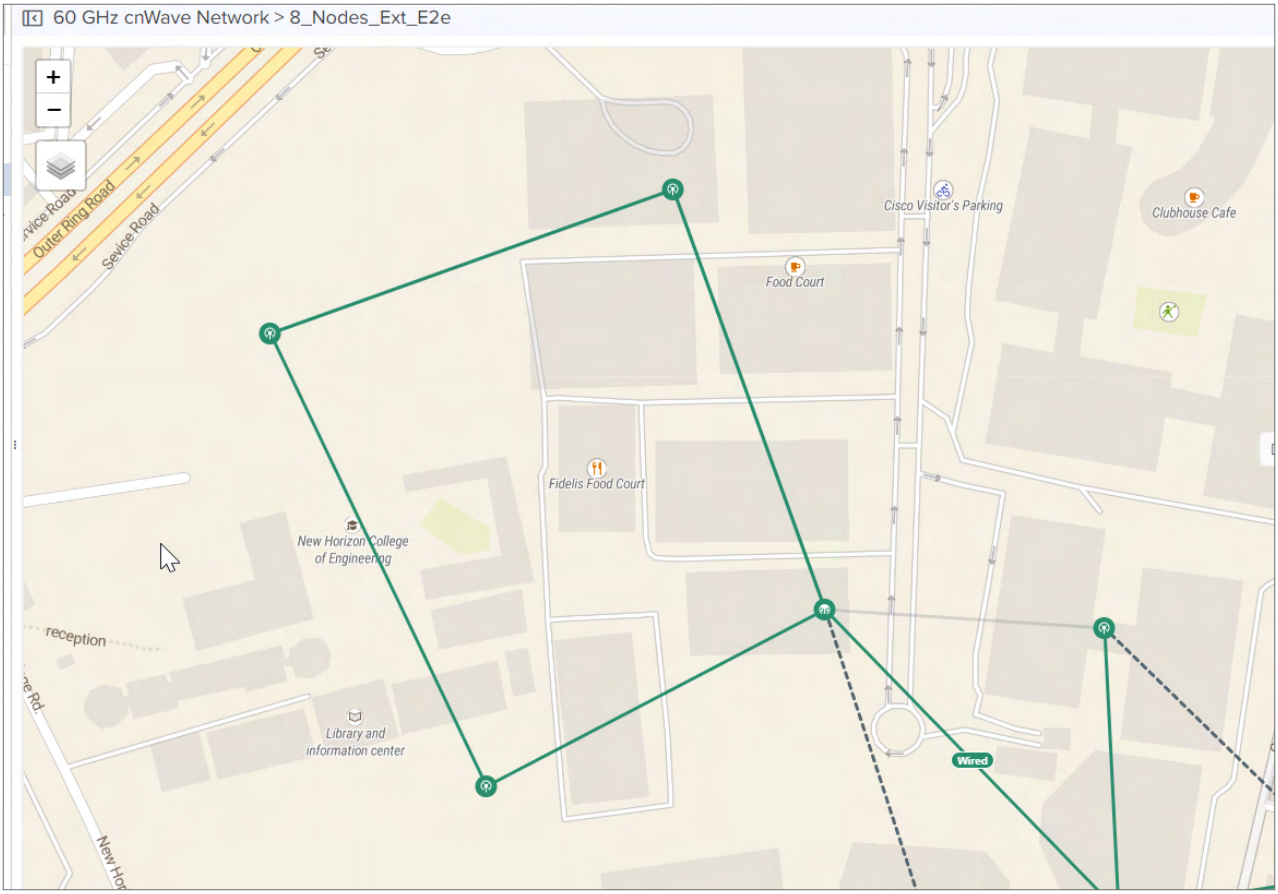
In the dashboard map, when user hovers on particular **PoP, DN** or **CN** it pops-up the device details. When user hovers on particular link it pops up the link details.



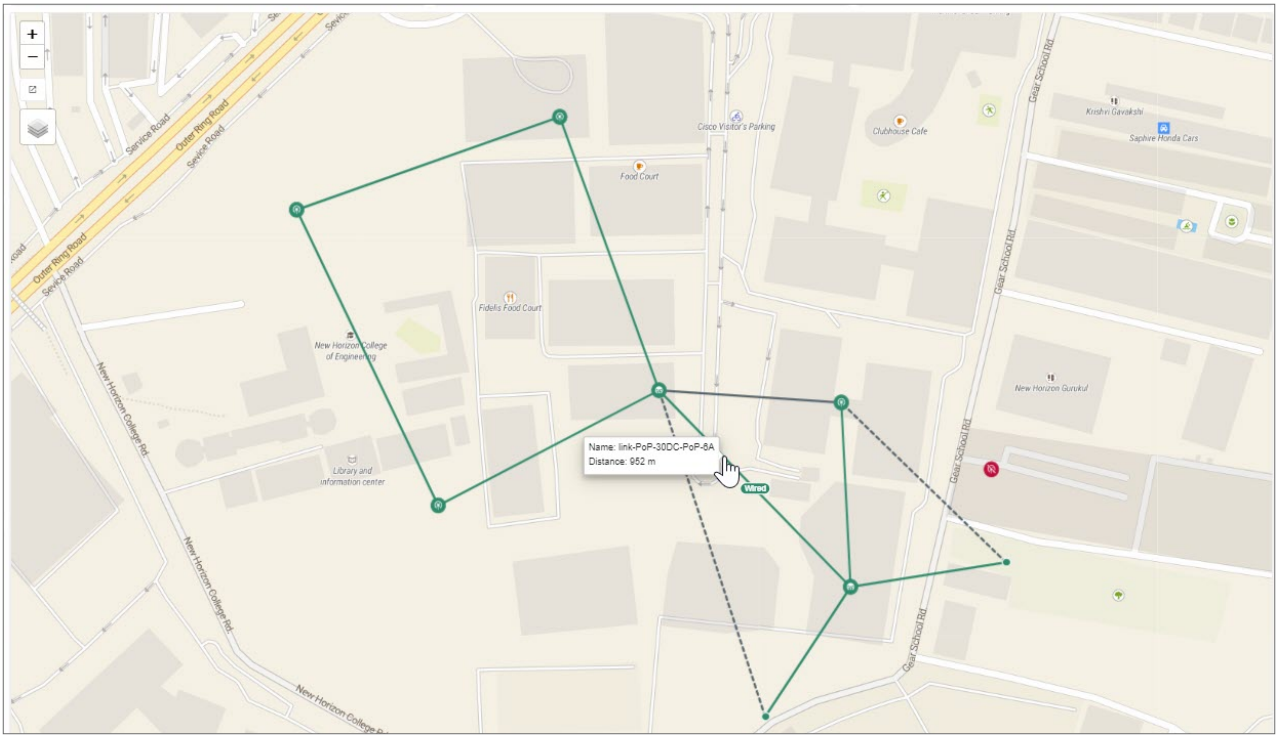
- Dotted line displays the Backup CN link between the DN and CN..



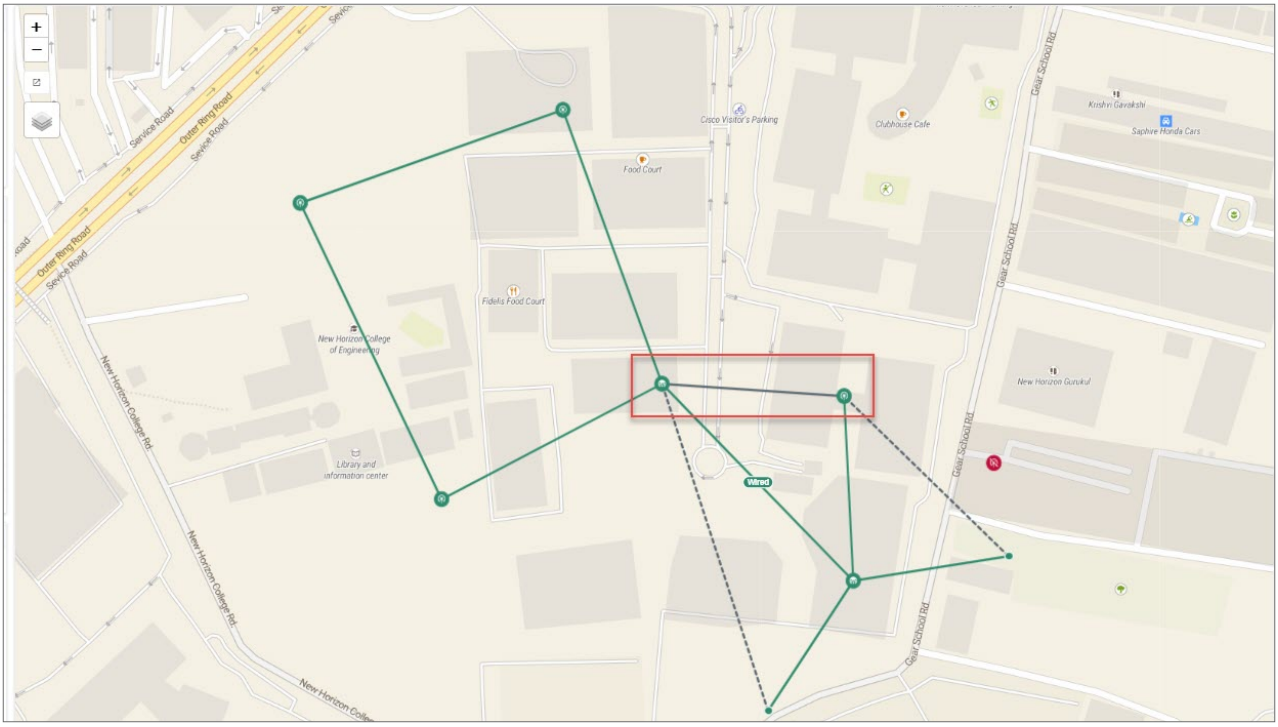
- Continuous line display the wireless link between PoP, DN, or CN..



- Continuous line with **Wired** tag displays the wired link between PoP, DN, or CN.



- Continuous line with gray color displays the **Disabled Ignition** link.



Notifications

Notifications are same as shown above for other devices, refer to Notification for more details.

Configuration

Configure the following after onboarding the External or Onboard E2E Controller:

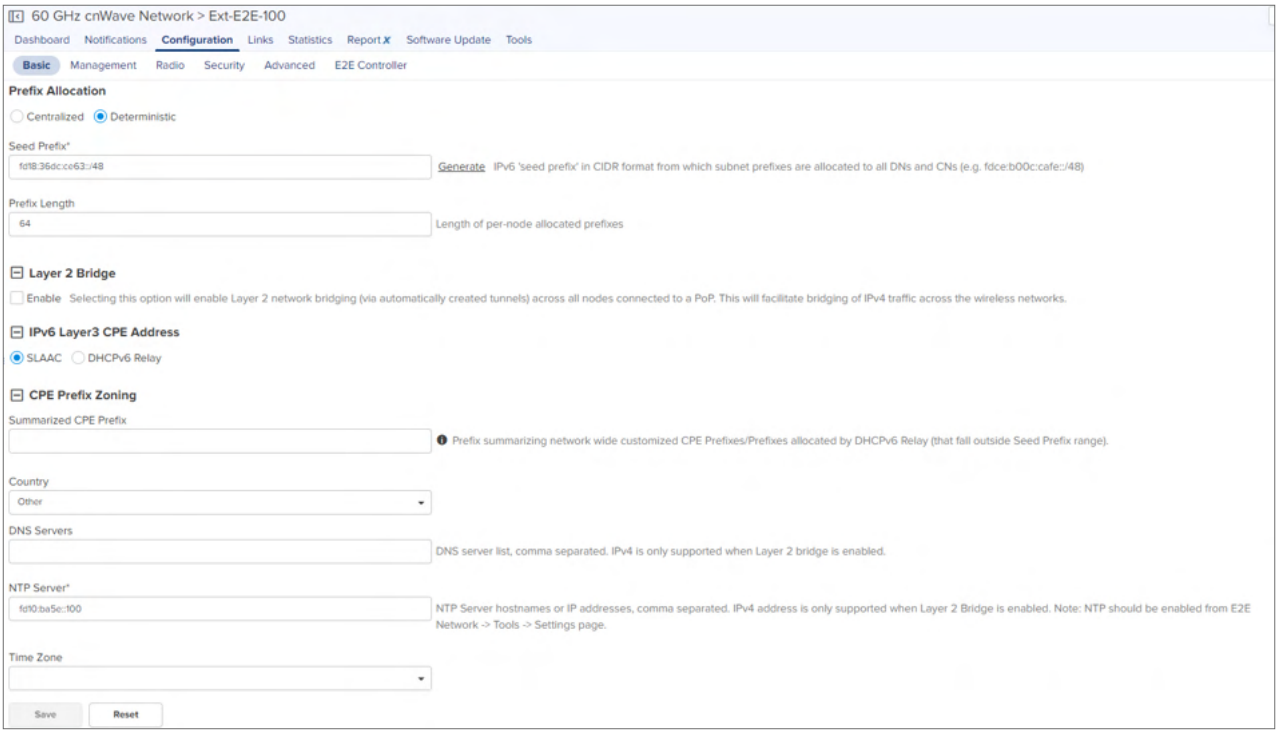
- Basic
- Management
- Radio
- Security
- Advanced
- E2E Controller
- High Availability X

Note

Once user selects the **Auto-assign** IPv6 Addresses while configuring E2E Controller and PoP node. Use the same IPv6 during the prefix allocation.

Basic Configuration

1. Navigate to **Configuration** > **Basic** to configure basic settings of E2E Controller.



Note

- **Prefix allocation** automatically gets updated, when E2E Controller is managed by cnMaestro.
- Prefix Length of 48 is supported in Seed Prefix configuration.

6 GHz radio does not work in Italy country. 6 GHz radio does not work in Italy.

2. In the **Prefix Allocation**, select **Centralized** or **Deterministic** to allocate the loopback IPv6 address for the devices.
3. Enter the **Seed Prefix** and **Prefix Length**.
4. Enabling **Layer 2 Bridge** is optional.

   Enabling this option will enable Layer 2 network bridging (via automatically created tunnels) connected across all nodes and facilitates bridging of IPv4 traffic across the wireless networks. It also enables the configuration of VLAN Management and Ports on all PoP, DN, and CN Nodes.

   In **Layer 2 Bridge**, select the check box to enable Layer2 Network Bridging, choose **Tunnel Concentrator** as **Best PoP** or **Static.**If user selects Tunnel Concentrator as Static, enter an external switch/router IPv6 address.

Note

IPv6 Layer3 CPE Address can be enabled when E2E Controller is running 1.1 verison and Layer 2 Bridge is disabled.

1. Select the **IPv6 Layer3 CPE Address** as **SLAAC** or **DHCPv6 Relay.**

   If user selects **IPv6 Layer3 CPE Address** as **DHCPv6 Relay**, user can configure the DHCPv6 server address. The CPE device sends a DHCP request.The CN device uses the Address and Prefix from the corresponding DHCP pool and DHCPv6 server assigns address to the CPE device.

Note

- By default **Country** is **Other**, user can configure it.
- Enter the **Hostnames** or **IP address** of NTP server.

2. Select the **Country** from the drop-down.
3. Enter the **DNS Server.**
4. Enter **NTP Server.**
5. Select the **Time Zone** from the drop-down.

Note

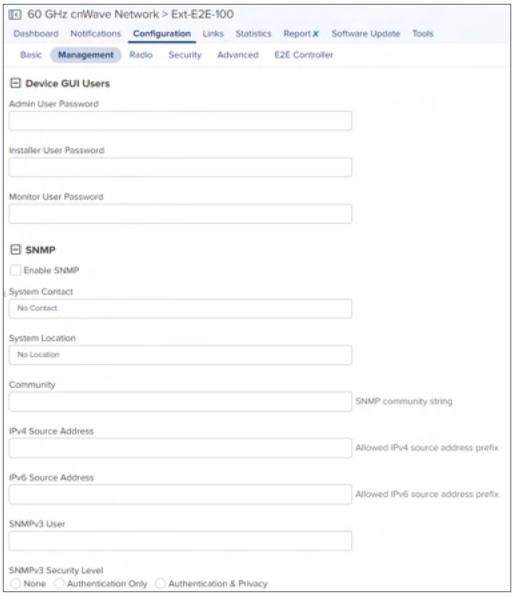
By default **Wireless Scans** will be disabled.

6. Click **Save.**

Management

Management configuration allows user to configure and manage the credentials of the administrator and it allows enable **SNMP**.

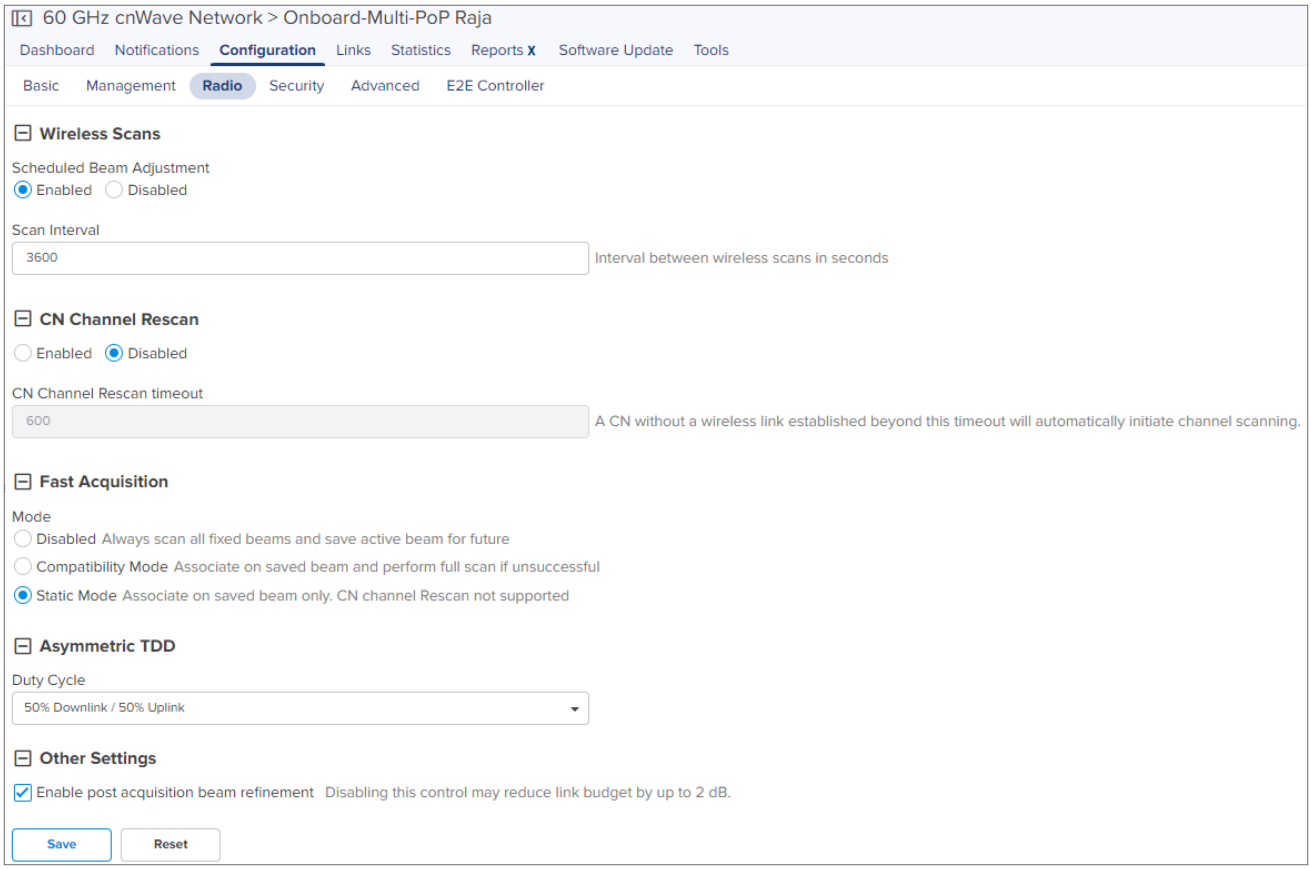
1. Navigate to **Configuration** > **Management** to set the **Device GUI Passwords** and to enable the **SNMP**.



2. Click **Save.**

Radio

The Radio page manages the Radio related settings.



- **Wireless Scans**
  - **Enabled/Disabled**—Enable or disable scheduled beam adjustment.
  - **Scan Interval**—Specify an interval between wireless scans, in seconds.
- **CN Channel Rescan**
  - **Enabled/Disabled—**Enable or disable CN channel rescan.

> **Note**
>
> You can enable CN channel rescan only when Fast Acquisition is set to either **Disabled** or **Compatibility Mode**.

  - **CN Channel Rescan timeout**—Specify a timeout interval for a CN that does not have a wireless link to reinitiate channel scanning, in seconds.
- **Fast Acquisition**

> **Note**
>
> Fast acquisition is supported only on 60 GHz cnWave devices running System Release version 1.3 or later.

  - **Mode**
    - **Disabled**—On link acquisition, performs IBF scan on 61 fixed beams. This is the default option.
    - **Compatibility Mode**—On link acquisition, tries the last known (if present) beam index. If unsuccessful, tries normal IBF scan.

- **Static Mode**—On link acquisition, tries the last known (if present) beam index. If unsuccessful, the association fails.

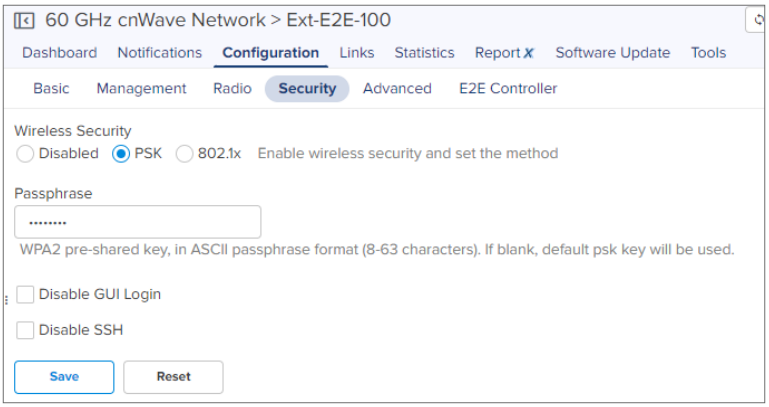
- **Asymmetric TDD**
  - **Duty Cycle**—Select a duty cycle from the drop-down list. For example:
    - **60% Downlink / 40% Uplink**—Set 60% of physical bandwidth for downloading and 40% of the physical bandwidth for uploading.
- **Other Settings**
  - **Enable post acquisition beam refinement**—Select to enable.

Security

Security page allows the user to enable the wireless security **PSK** or **802.1x.** The disabled option connects as unsecure devices.

To Enable PSK, complete the following steps:

1. Navigate to **Configuration** > **Security** tab**.**
2. Select **PSK** in **Wireless Security**.



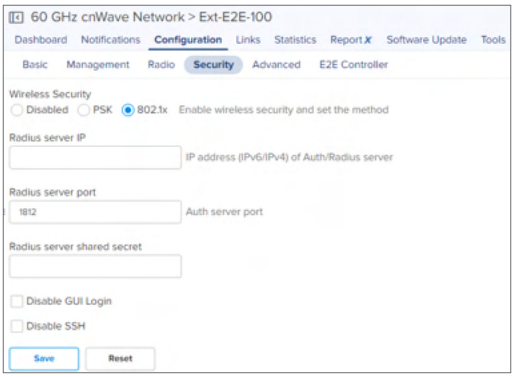
3. Enter the **Passphrase**.

> **Note**
>
> If **Passphrase** field is blank, default psk key is used.

4. Click **Save.**

To **Enable 802.1x**, complete the following steps:

1. Navigate to **Configuration** > **Security.**
2. Select **802.1x** in **Wireless Security**.



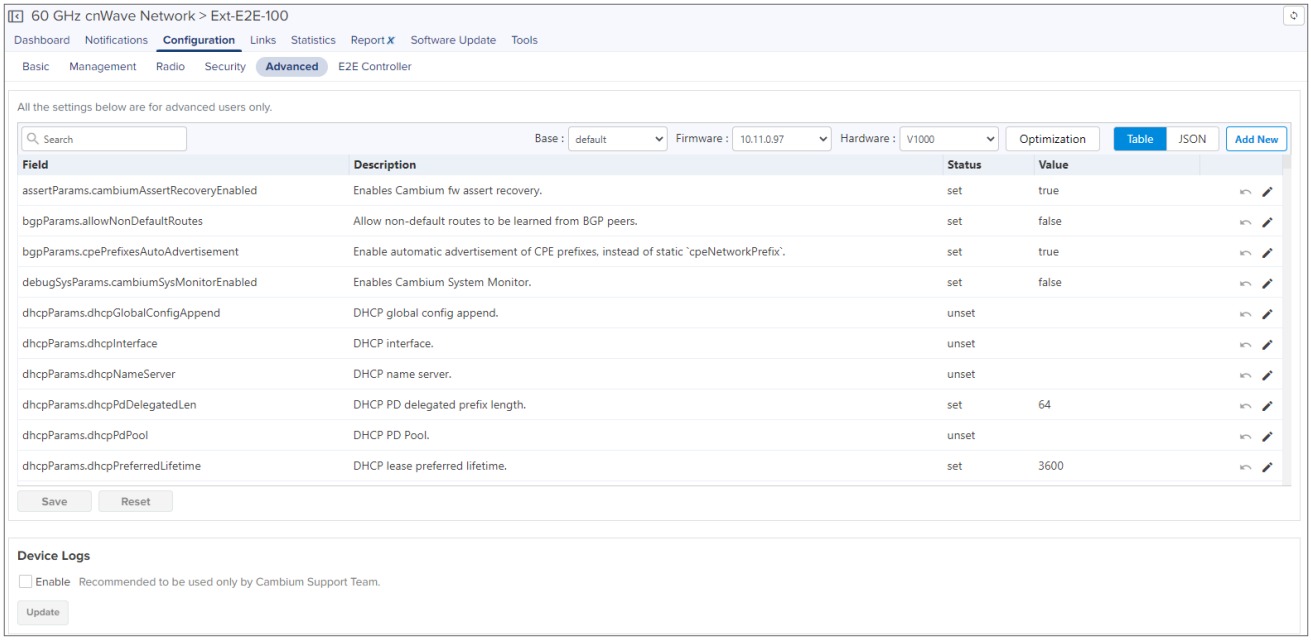
3. Enter the **Radius server IP.**
4. Enter the **Radius Server port.**
5. Enter the **Radius Server Shared Secret.**
6. Click **Save**.

Advanced

Advanced tab allows the advanced user to edit the settings of the Table and JSON format of the E2E Controller.

It also allows to optimize the network using the following options:

- Optimize Control Superframe Allocation
- Optimize DPA Zone Allocation
- Clear Node Auto Configuration

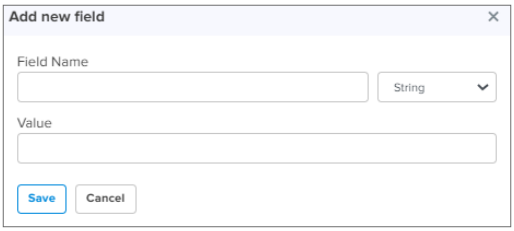


Table

In the **Table** advanced user can view and edit **Field Name** and **Value**. The field names are sorted in alphabetical order.

To add a field:

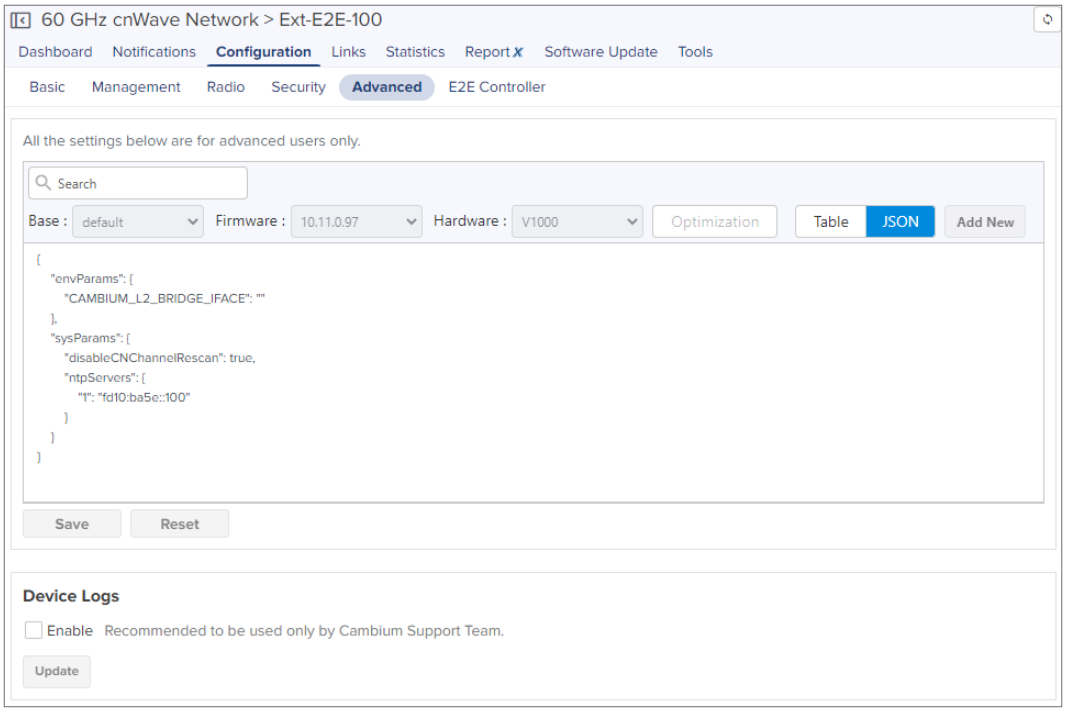
1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

JSON

JSON allows Advanced user to download or view and edit in json format.



To view or edit the JSON file:

1. Navigate to **Configuration** > **Advanced** > **JSON.**

Note

Enabling the Device Logs is supported only for External E2E Controller devices and it allows the Support team to view the logs.

2. Enable **Device Logs** and click **Update.**

E2E Controller

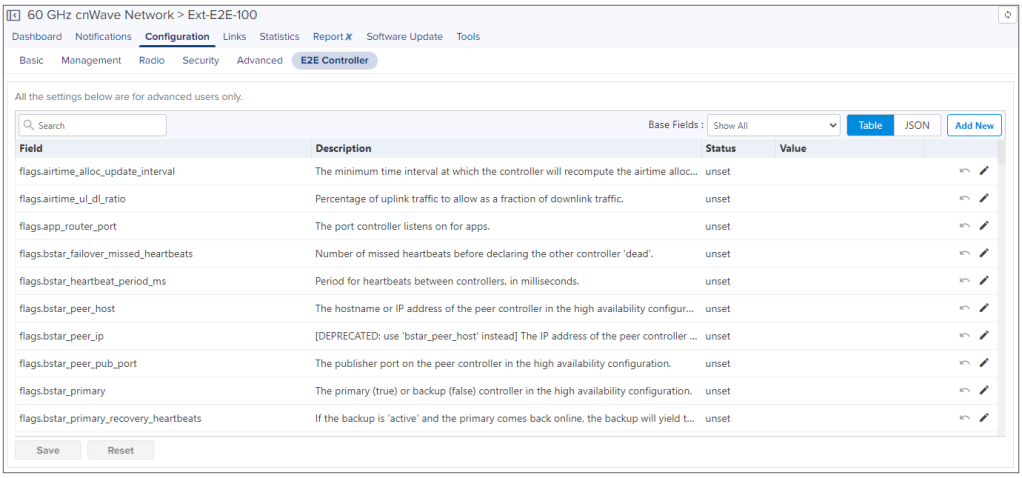
E2E Controller allows the advanced user to set the **Table** and download the **JSON** file.

Table

In **E2E Controller Table** user can edit or add **Field Name** and **Value.**

To Add Field:

1. Navigate to **Configuration** > **E2E Controller.**
2. Click **Add New.**



3. Enter the **Field Name** and **Value.**



4. 1. Click **Save.**

JSON

JSON allows Advanced user to download or view and edit in JSON format. To view or edit the JSON file, navigate to **Configuration** > **E2E Controller** > **JSON.**

High Availability X

Using cnMaestro, you can enable and configure high availability (HA) support in a Multi-PoP Onboard E2E Controller that is running 60 GHz cnWave devices in a mesh network. This HA support configuration allows you to configure a primary (active mode) and a backup or secondary (passive mode) E2E Controller from cnMaestro.

If the active primary E2E Controller, with HA enabled and functioning, goes down, then the backup E2E Controller is active and manages the 60 GHz cnWave devices. All the devices report to the backup E2E Controller until the primary E2E Controller comes back.

This topic covers the following sections:

- Theory of operation
- Configuring HA support
- Caveats of HA configuration

Theory of operation

E2E Controllers use the high-availability protocol (primary-backup) and support the HA configuration. In such a primary-backup setup, two controllers (peers) run on separate PoP nodes and are designated as either primary or backup. If the primary controller catastrophically fails (for example, power outage, network failure, hardware failure), the backup controller assumes control of the cnWave 60 GHz network.

The HA configuration supports the following operational mechanisms for Onboard E2E Controller:

1. **Role designation**: At setup, one controller is statically designated as primary, and the other as backup. This designation determines their initial operational roles during network management.
2. **Initial state**: The primary controller starts in an active state, overseeing network configuration and collecting network statistics. The backup controller remains in a passive state, prepared to assume control if needed.
3. **Health monitoring**: Both primary and backup controllers monitor each other's status through regular heartbeat messages, sent every five seconds. These messages are crucial for detecting any disruptions or failures in the primary (active) controller.
4. **Data synchronization**: Both primary and backup controllers periodically synchronize topology and configuration data. This synchronization is key to enabling a fast and seamless transition from passive to active state, ensuring the backup controller can immediately manage the network with up-to-date settings and configurations.
5. **Failover process**: If the primary (active) controller fails, detected by a loss of heartbeat messages for 20 seconds, the backup controller automatically transitions from passive to active. This change ensures continuous network management without manual intervention.
6. **Recovery and Reversion**: After the failed primary controller is repaired and comes back online, it starts in a passive state. It remains in this passive state until it has successfully exchanged heartbeat messages for 150 seconds, ensuring stability. Following this period, a role reversal occurs where the primary controller transitions back to active and the backup controller reverts to passive.

Configuring HA support

Note

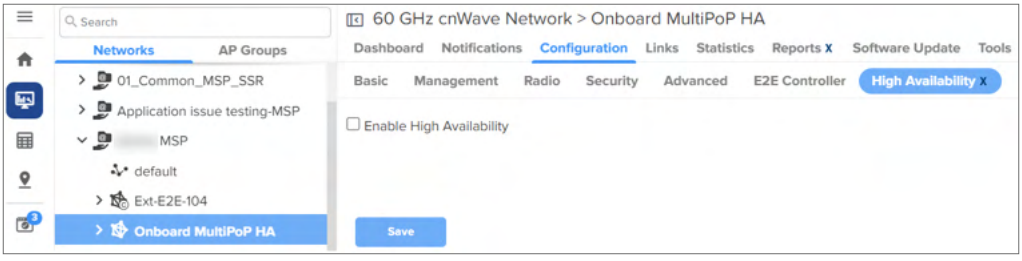
The HA support is applicable only to cnMaestro X accounts. Consider the following key points:

- The Onboard E2E Controller must be managed using cnMaestro.
- The Onboard network must have at least two PoP nodes to enable HA.
- The two PoP nodes are selected to host Primary. The backup controllers should be able to communicate over wire/ethernet.
- For HA, all the DN/CN nodes in network are expected to have a route to report to both the HA peers.
- The HA feature is supported in a network when devices are running 1.4 or above software version.

To enable the HA support for E2E Controller, complete the following steps:

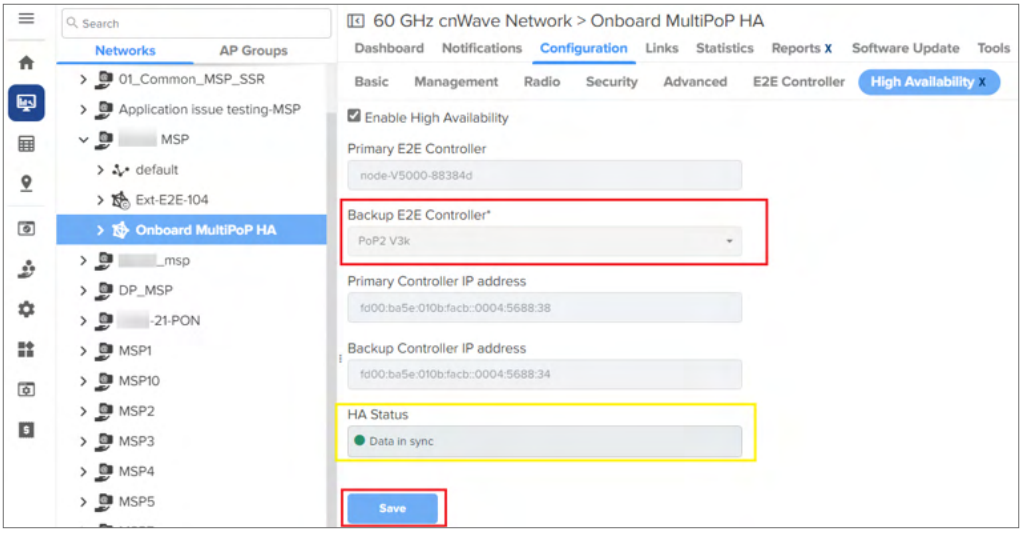
1. From the Home page of cnMaestro, navigate to **Monitor and Manage** > **E2E Network** > **Configuration** > **High Availability X**.

   The **Enable High Availability** check box appears.



2. To enable the HA support for E2E Controller, select the **Enable High Availability** check box.

The **High Availability X** page displays options to configure the backup Controller. By default, the current Onboard Controller is selected as the primary controller.



3. From the **Backup E2E Controller** drop-down list, select the required node that is connected to the complete network.

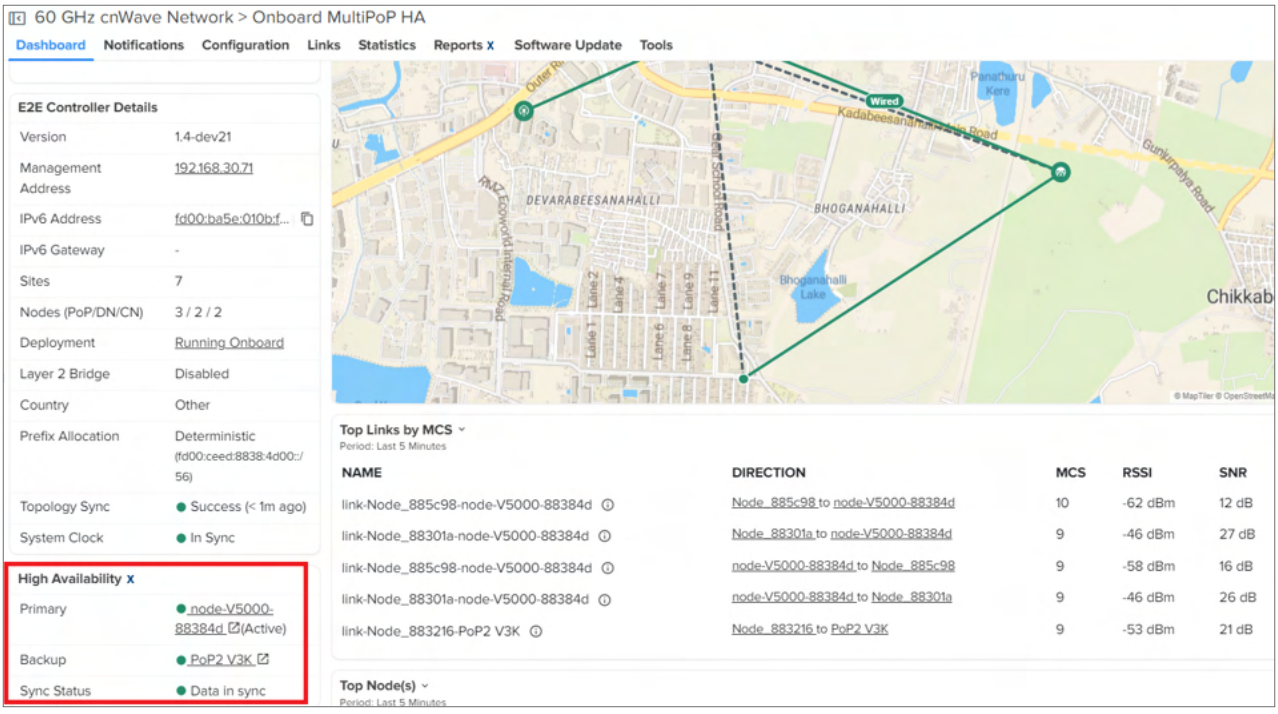
   You can check the IP addresses (read only) of primary and backup controllers.

4. Click **Save** to apply the changes.

5. When you configure the HA support, ensure to check the **HA Status** parameter.`

   The **HA Status** parameter must display the green button, indicating that the HA support is functioning and data is in sync. If **HA Status** displays the red button, then it indicates that the HA support is not functioning.

   You can also view the HA status in the **High Availability X** section on the **Dashboard** page.



The **Primary** field displays the primary node name. The **Backup** field displays the backup node name. Green bullets in **Primary** and **Backup** fields show the online/offline status of nodes. The keyword **Active** toggles between

Primary and **Backup** fields, indicating that the respective node is currently functioning as the active controller, managing the network and is connected to cnMaestro.

Caveats of HA configuration

Consider the following caveats of the HA configuration for cnWave 60 GHz devices:

Table 71 *Caveats of HA configuration*

Configuration	Caveats
Configuration backup and restoration	• The configuration backups are supported when the HA is enabled. • The backup collected from a non-HA network can only be restored in a non-HA network. • The backup collected from a HA enabled network is restored only in a HA enabled network. • When HA is enabled, the restoration is allowed only when the primary node is active, managing the network and connected to cnMaestro.
Software update flow	• When HA is enabled, it is recommended to update the nodes when primary is functioning as the active controller. • It is always recommended to run the HA Pairs in same version to avoid HA functionality issues. • Avoid downgrading the device version to less than 1.4 when HA is enabled in the network. • Avoid updating the device software from a device UI when HA is enabled. You must update the software from cnMaestro.
Device UI	• It is always recommended to make changes in the network only from cnMaestro. • Making changes through device UIs may have issues in HA functionality.
cnMaestro X to Essentials downgrade	• The HA functionality will be disabled leaving the current active controller that is connected to cnMaestro as the only controller in the network. • The HA functionality can be enabled back when the subscription is enabled.
Connecting a HA enabled E2E Controller network to an Essential cnMaestro account	• The HA functionality will be disabled leaving the current active controller that is connected to cnMaestro as the only controller in the network. • The HA functionality can be enabled back when the network is connected to cnMaestro X account.

Links

Links provide the details about the link established between the nodes and also provides the option to create a new Wireless, Wired and Backup CN link.

- List
- Statistics

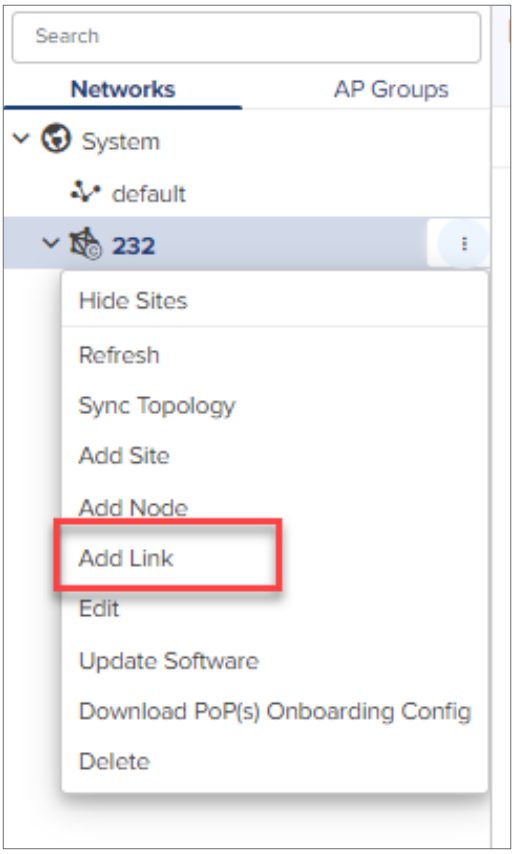
- Events

List

The **List** page provides details of **General**: Name, A-Node, Z-Node, A-Node MAC, Z-Node MAC, Alive, Link Time, Type, Ignition Attempts, Distance, Azimuth, Backup CN Link, and Ignition Status for each link of all the devices in the E2E Network in a page format.

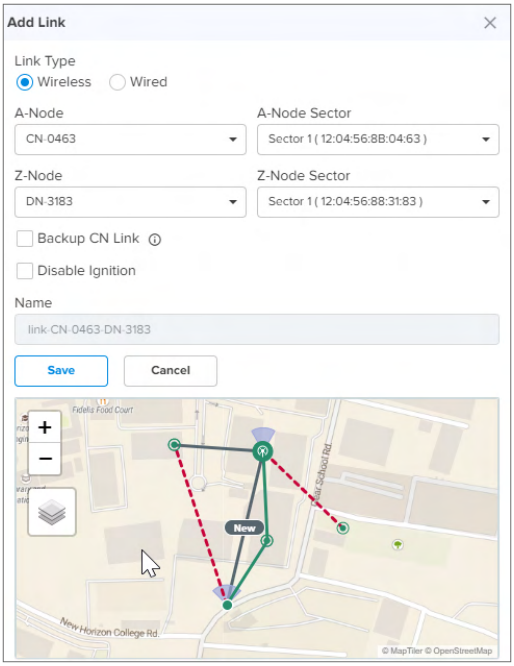
To add a link, perform the following steps:

1. Navigate to the E2E Network tree menu click (⋮) icon and click **Add Link** from the drop-down or navigate to **Network** > **Links** > **List** > **Add New**.



2. **Add Link** window pops-up.
3. Select **Link Type** Wireless or Wired.

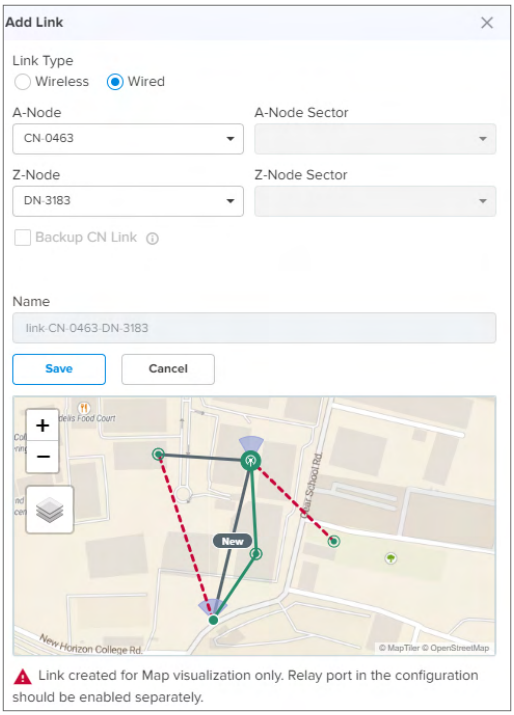
Figure 338 *Wireless link*



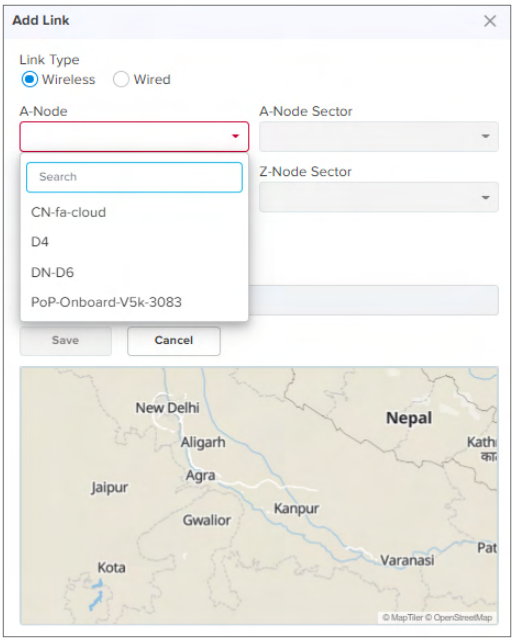
Note

In Wired Link Type, add Sector is disabled.

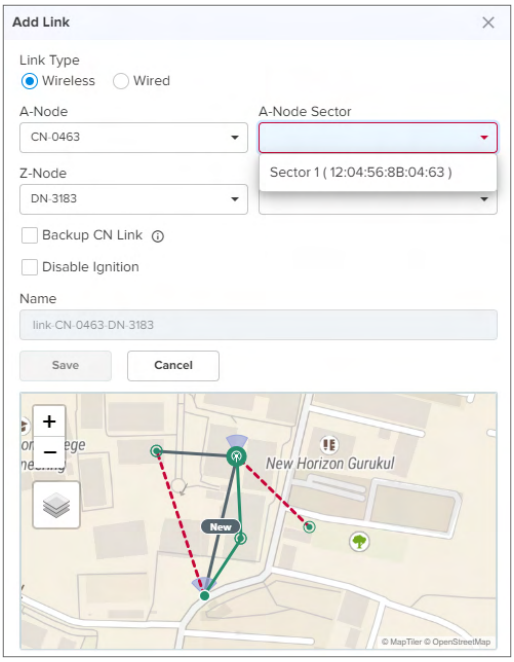
Figure 339 *Wired link*



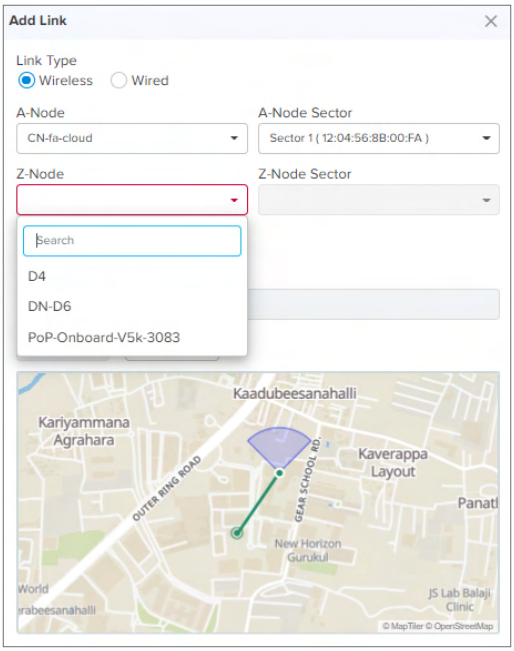
4. Select the **Node** from the drop-down in **A-Node.**



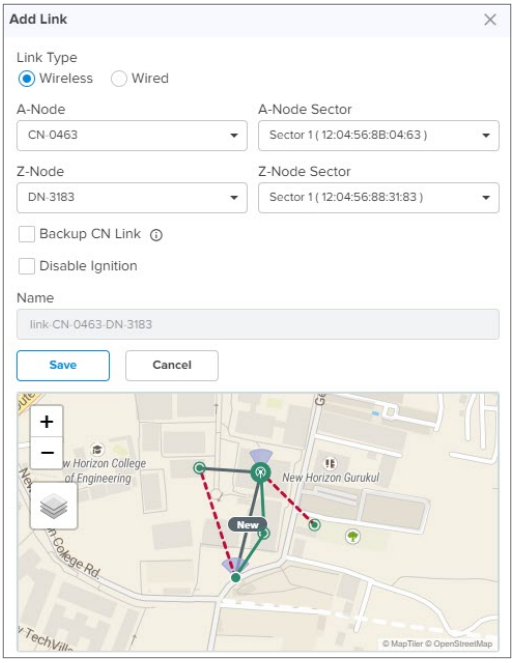
5. Select the **Sector** of the node from the drop-down in **A-Node Sector.**



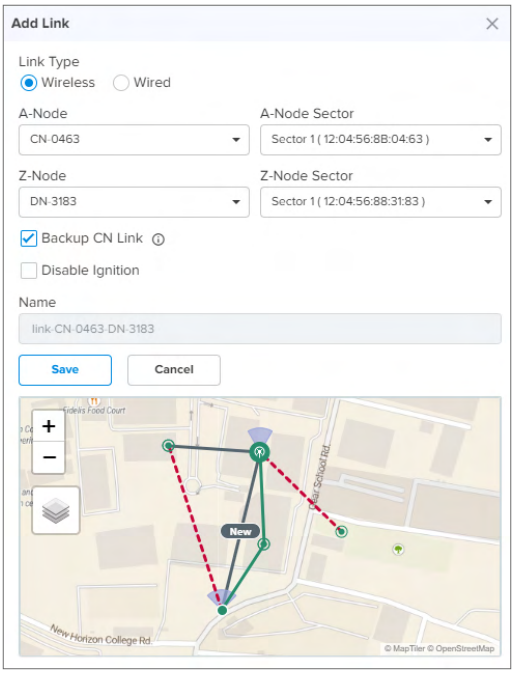
6. Select the **Node** from the drop-down in **Z-Node.**



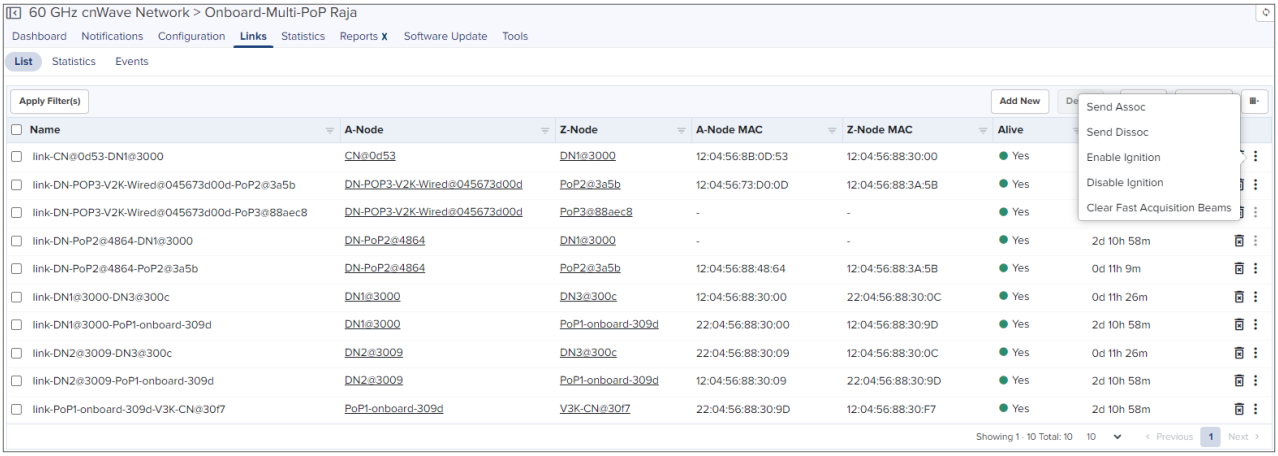
7. Select the **Sector** of the node from the drop-down in **Z-Node Sector.**



8. Enable the **Backup CN Link**.
    - If the link between PoP or DN and CN gets disconnected. This Backup CN link provides the backup connectivity from DN or PoP to particular CN.



9. If user selects **Disable Ignition** option, wireless link creates with disable ignition. User need to manual select **Enable Ignition** from link options.
10. Click **Save**.
11. Once the link is successful it displays the **Alive** status as **Yes**.



Available link options are:

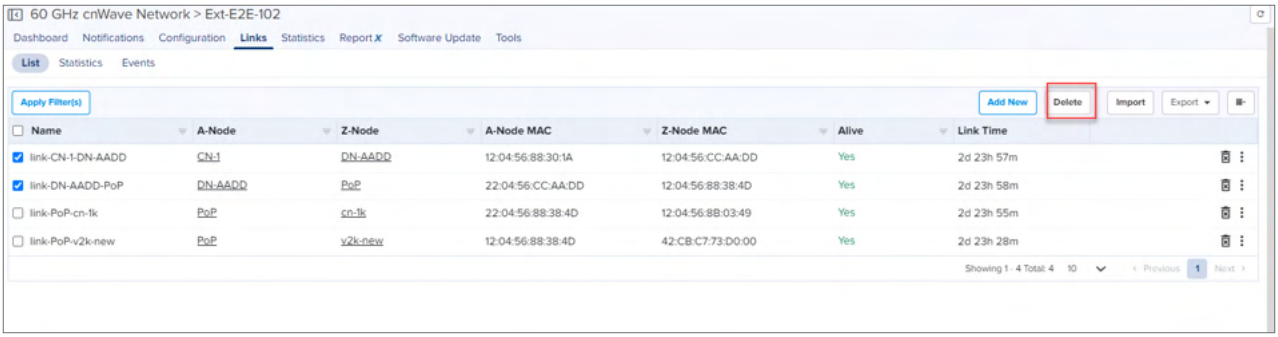
- Send Assoc
- Send Dissoc
- Enable Ignition
- Disable Ignition
- Clear Fast Acquisition Beams

Delete Links

In the **Links** tab you can delete the E2E Controller Network Links.

To delete the links:

1. Navigate to **Links** > **List.**
2. In the **List** table select one or more links to delete. User can also delete individual link, by selecting delete (🗑) icon in the table.



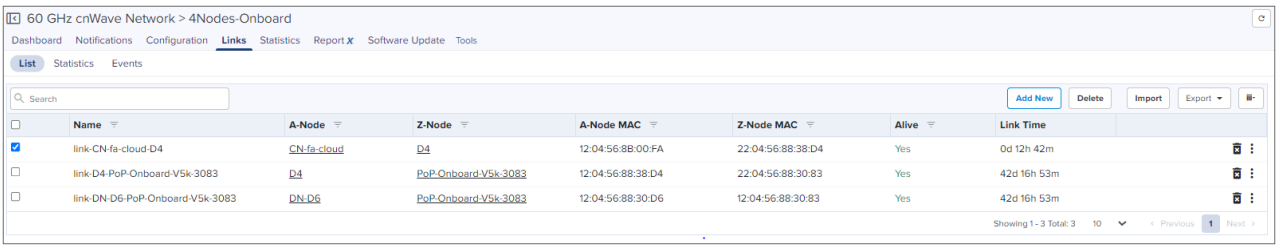
1. Click **Delete**.

Import List

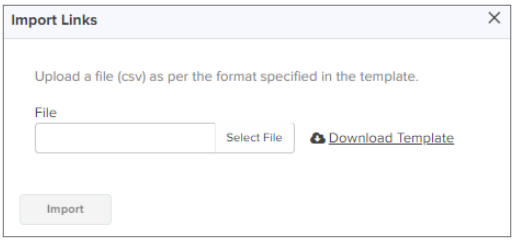
In **Links** tab you can import the E2E Controller Network Links.

To import the links:

1. Navigate to **Links > List.**
2. Select **Import.**



3. **Import Links** pops-up.



4. Click **Download Template** to download the sample template in .CSV format.

	A	B	C	D	E
1	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of the device	Sector 1/2 MAC Address	Z node name of the device	Sector 1/2 MAC Address	Wireless or Wired
3	POP	[illegible]	DN1	[illegible]	wireless
4	DN1	[illegible]	CN1	[illegible]	wireless
5	DN1		CN2		wired
6					
7					

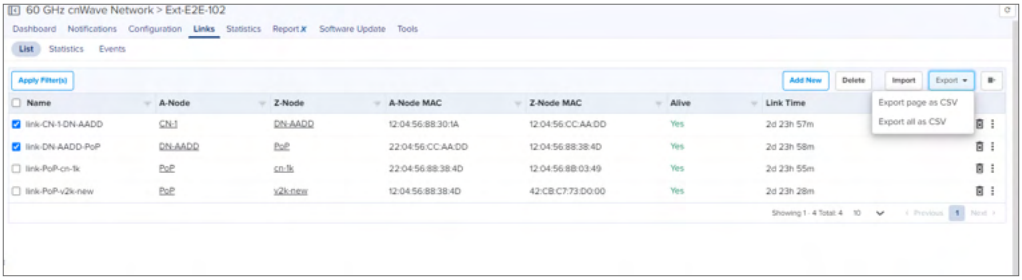
5. Select the file and click **Import**.

Export List

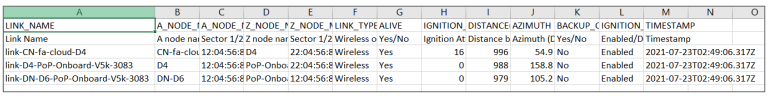
In **Links** tab you can export the E2E Controller Network Links.

To export the links:

1. Navigate to **Links** > **List** > select **Export.**



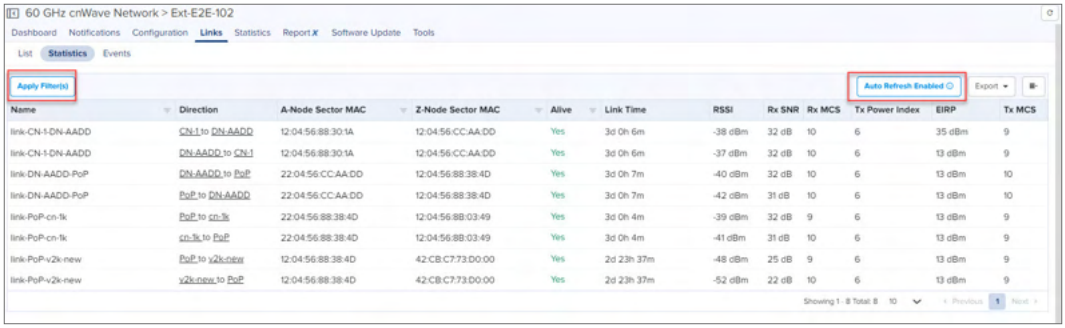
2. It exports .csv file format as shown below.



LINK_NAME	A_NODE_I	A_NODE_I	Z_NODE_P	Z_NODE_I	LINK_TYPE	ALIVE	IGNITION_	DISTANCE	AZIMUTH	BACKUP_C	IGNITION_	TIMESTAMP
Link Name	A node nai	Sector 1/2	Z node nar	Sector 1/2	Wireless o	Yes/No	Ignition At	Distance b	Azimuth (C	Yes/No	Enabled/D	Timestamp
link-CN-fa-cloud-D4	CN-fa-clou	12:04:56:8	D4	22:04:56:8	Wireless	Yes	16	996	54.9	No	Enabled	2021-07-23T02:49:06.317Z
link-D4-PoP-Onboard-V5k-3083	D4	12:04:56:8	PoP-Onbo	22:04:56:8	Wireless	Yes	0	988	158.8	No	Enabled	2021-07-23T02:49:06.317Z
link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	12:04:56:8	PoP-Onbo	12:04:56:8	Wireless	Yes	0	979	105.2	No	Enabled	2021-07-23T02:49:06.317Z

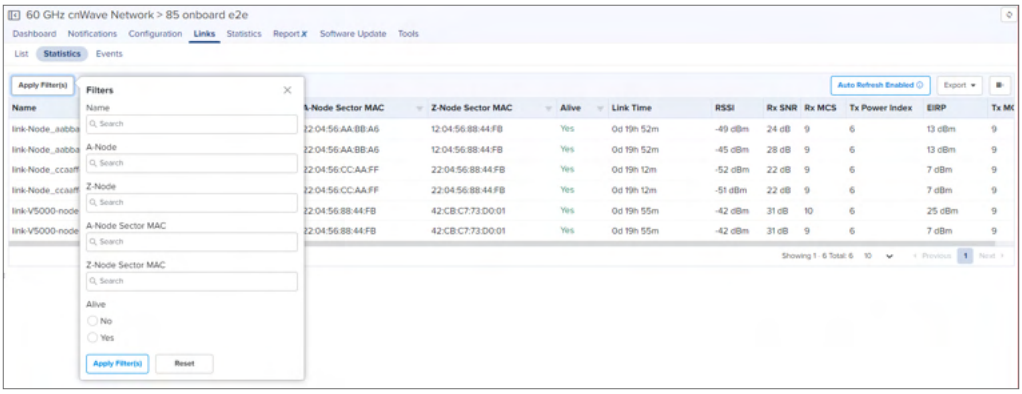
Statistics

Statistics pages provides details of **Basic**: Name, Direction, A-Node, Z-Node, Alive, Link Time, Type, Distance, Azimuth, Rx Golay, Tx Golay **Detailed Statistics**: A-Node Sector MAC, Z-Node Sector MAC, RSSI, Rx Airtime%, Rx Beam Azimuth Angle, Rx Beam Elevation Angle, Rx SNR, Rx MCS, Rx PER, Rx Scan Beams, Rx Throughput, Tx Airtime%, Tx Beam Azimuth Angle, Tx Beam Elevation Angle, Tx Power Index, EIRP, Tx MCS, Tx PER, Tx Scan Beams, Rx Errors, Rx Frames, Tx Errors, Tx Frames, Tx Throughput, Rx Time, Tx Time and Link Fade Margin each link of all the devices in the E2E Network in a page format.

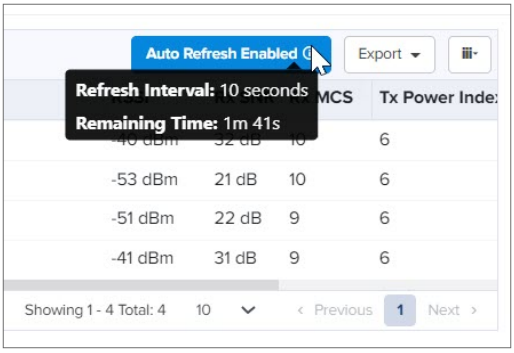


You can **Apply Filter(s)** for Name, A-Node, Z-Node, A-Node Sector MAC, Z-Node Sector MAC, and Alive. The **Auto Refresh** option allows to refresh data automatically as per Refresh Interval, which is configured for five minutes. By default, Refresh Interval is 10 seconds. This option gets disabled after five minutes. Then you must click **Enable Auto Refresh** and specify the refresh intervals to enable this option. To **Enable Auto Refresh**, perform the following steps:

1. Click **Enable Auto Refresh**.
2. Select **Refresh Interval** from the drop-down.
    - 10 seconds
    - 30 seconds
    - 60 seconds
3. Click **Start** to start **Auto Refresh.**



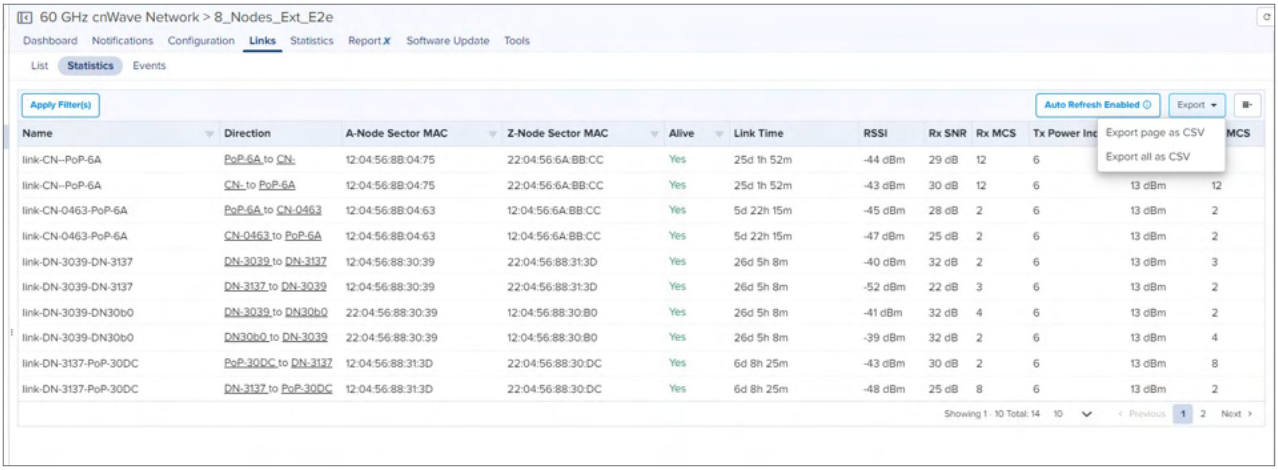
4. Click the info icon to view **Refresh Interval** and **Remaining Time**.



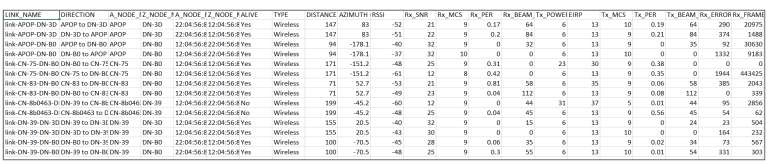
Export Statistics

To export the Statistics:

1. Navigate to **Links > Statistics >** select **Export.**



2. It exports .csv file format as shown below.



Events

Events provide the details of link availability, hourly link availability in percentage, link availability in different time lines, and distance of the link.

Figure 340 *Links > Events*

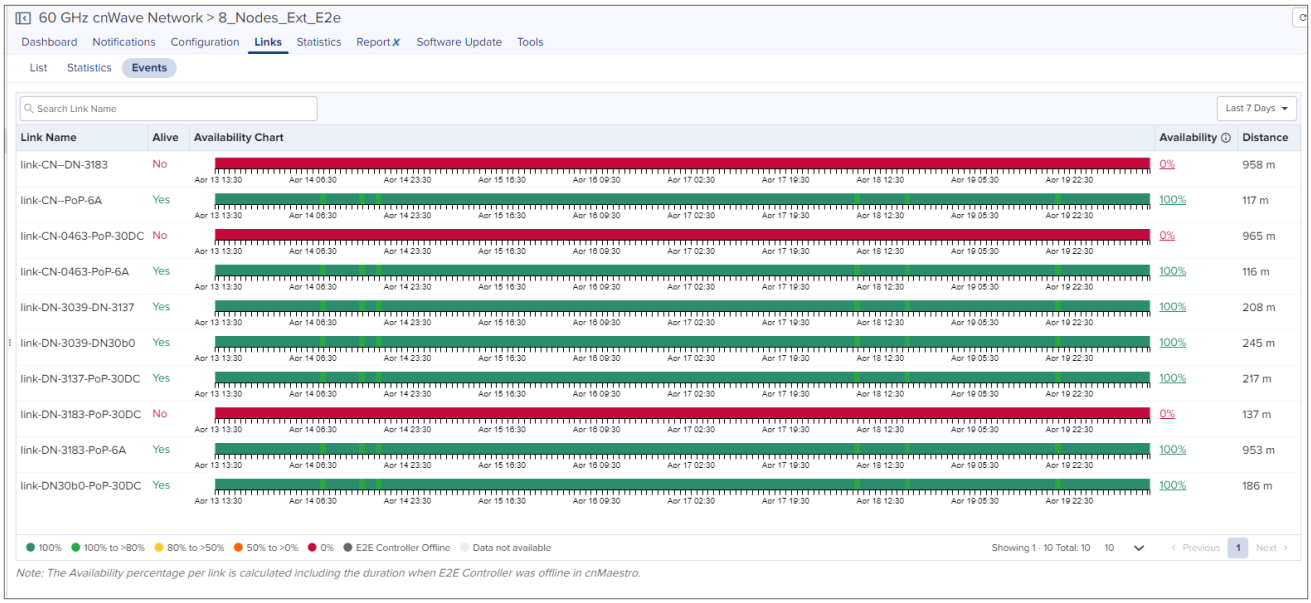
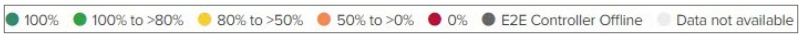
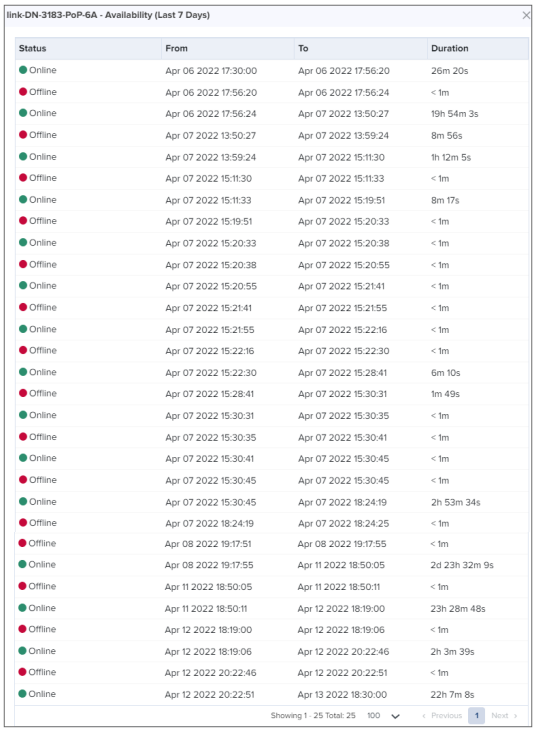


Table 72 *Events fields*

Field	Description
Link Name	Name of the link.
Alive	Status of the link (Yes or No).
Availability Chart	Displays the link availability based on time range selected from the drop-down.When you hover the mouse on the Availability Chart, the link availability is shown as described: • If you select time range as **Last 1 Hour**, then link availability for every 5 minutes is displayed. • If you select time range other than **Last 1 Hour**, then link availability for every 1 hour is displayed. Hover on the link to see the hourly availability as shown in Figure 342. Clicking on percentage link availability displays pop-up window as shown in Figure 343 Link availability is presented in different colors in the chart as shown in Figure 341
Availability Percentage	Availability of link is shown in percentage in the Availability column as shown in Figure 342.
Distance	Distance of the link in meters.

Figure 341 *Link Availability in Percentage*





Availability percentage per link is calculated including the duration when E2E Controller was Offline in cnMaestro.

Figure 342 *Link Availability*

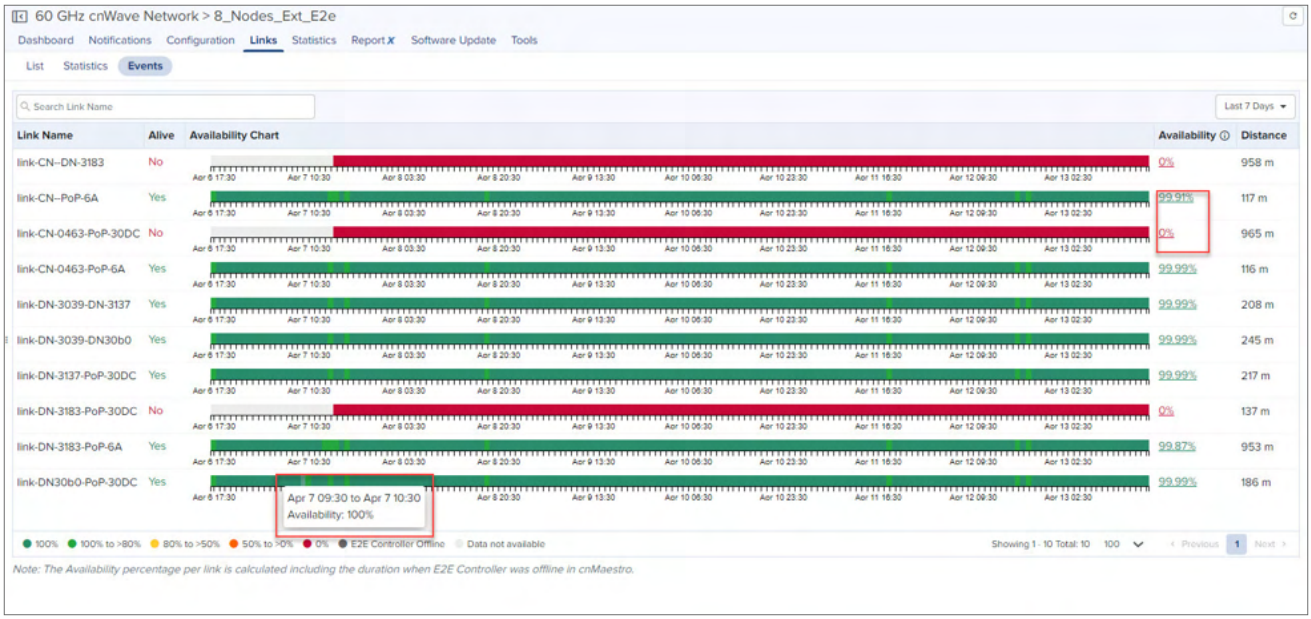
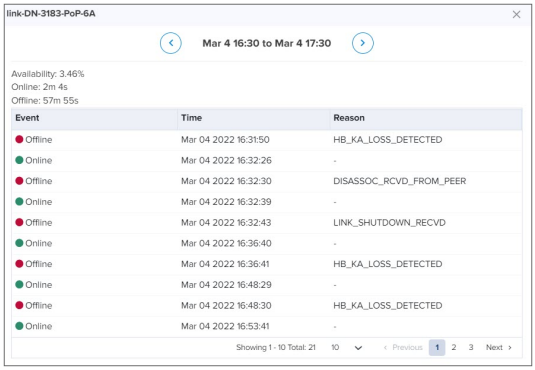


Figure 343 *Link Status*



Events details are available for Last 1 hour, Last 6 hours, Last 12 hours, Last 24 Hours, Last 2 days, Last 4 days, and Last 7 days.

Note

Event details for **Custom Range** and **Last 30 days** is available only for cnMaestro X users.

Statistics

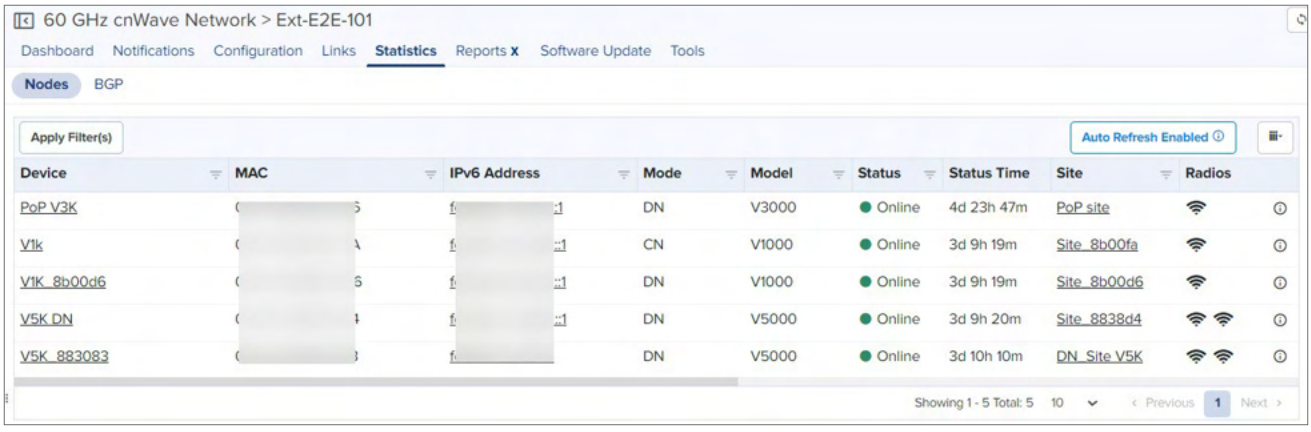
The E2E Network provides the following statistics:

- Nodes
- BGP

Statistics

Nodes provide a tabular aggregation of data, including General information on the nodes monitored, as well as Wireless, Network, and Traffic metrics. Node Statistics pages provide details of **General**: Device, Serial Number, IPv6 Address, MAC, Mode, Model, Status, Status Time, Site, Zone, PoP Node, Software Version. **GPS**: Sync Mode, Fix Type, Satellites Tracked, Latitude, Longitude, Height. **Network**: Radio Channel, Main Aux SFP, Sector Throughput (Tx), Sector Throughput (Rx),Ethernet Throughput (Tx), and Ethernet Throughput (Rx) each device in E2E Network, generally in a page format**.**

Figure 344 *Nodes Statistics*



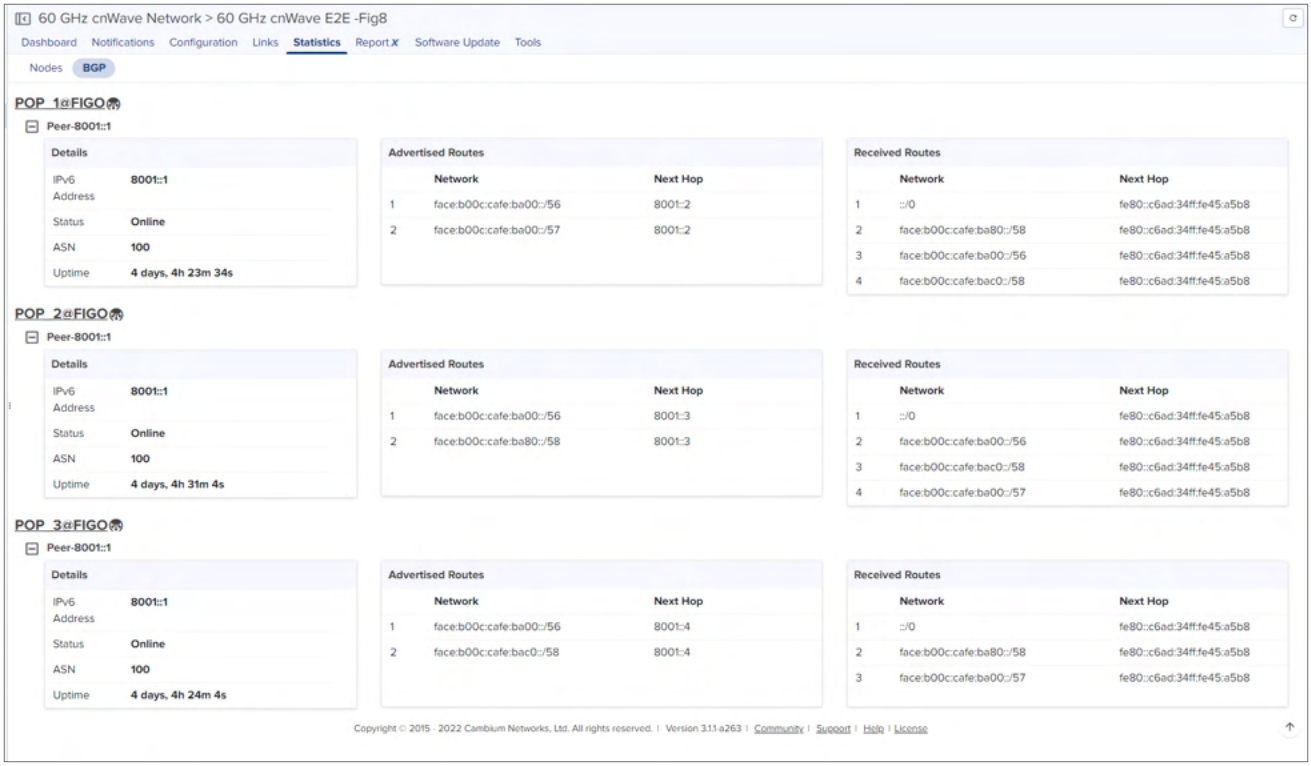
BGP

Note

BGP statistics displays only if BGP option is enabled in Routing in PoP configuration.

BGP provides the details of **Advertised Routes, Received Routes,** and **Peer** details.

Figure 345 *BGP Statistics*

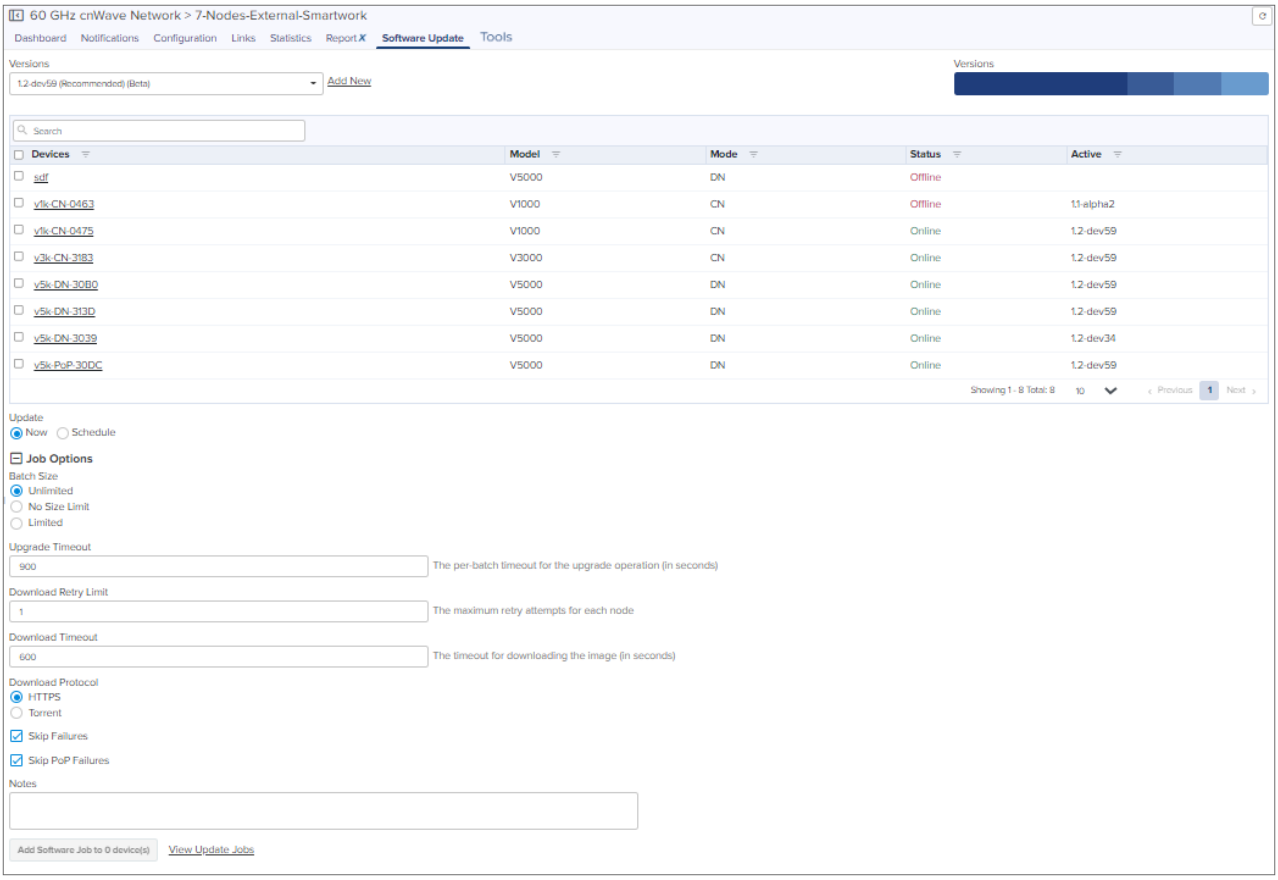


Software Update

The **Software Update** tab allows to update with the latest device software.

To update the software:

1. Select the **Network** and navigate to the **Software Update** tab.
2. In **Software Update** tab select the desired Versions from drop-down in **Versions** tab.
3. Select the **Device**.
4. In **Job Options**, do the following:
    - Select **Batch Size**
    - Enter **Upgrade Timeout.**
    - Enter **Download Retry Limit.**
    - Enter **Download Timeout.**
    - Select the Download Protocol as **HTTPS** or **Torrent.**
    - Enable the **Skip Failures** or **Skip PoP Failures**.
5. Click **Add Software Job to device.**



Note

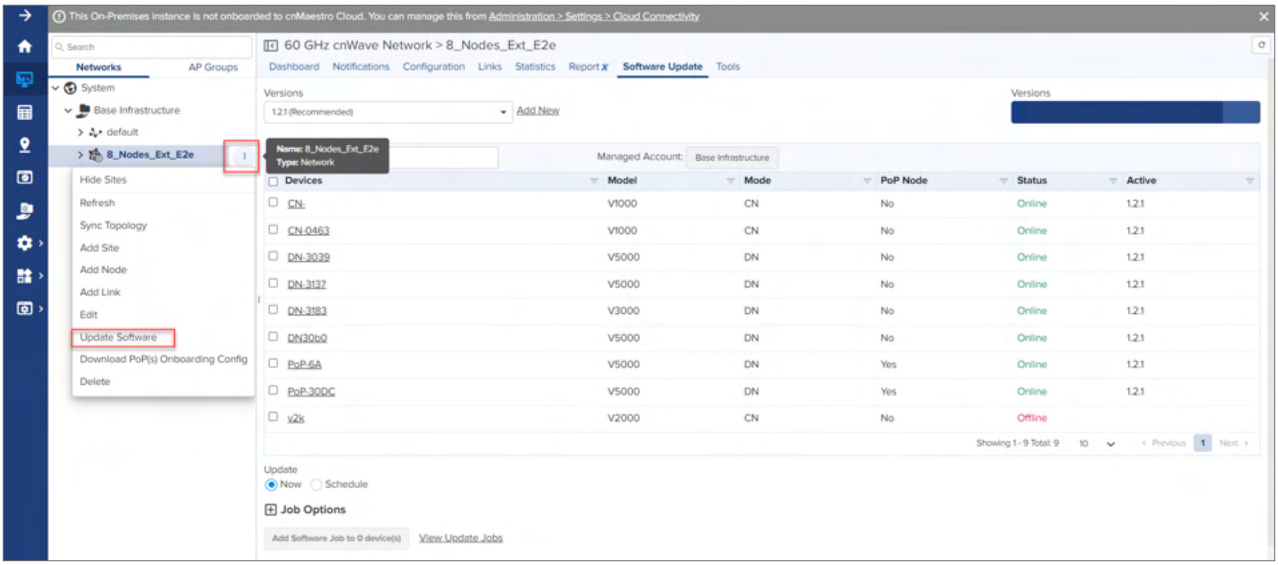
Onboard E2E controller will support only one synced image. If user needs to sync another image, select the image from **Versions** drop down and click **Sync Selected Image.**

The Software Update is performed on the devices managed by External E2E Controller and Onboard E2E Controller as follows:

External E2E Controller

1. In the **Networks**, select External E2E Controller and check the Software Version.
2. From External E2E Controller menu options, select **Update Software**.

   Software Update page appears.



3. In **Versions** drop-down select the version and the devices in the network for software upgrade.

   Device software update version check for External E2E Controller is described in Table 73.

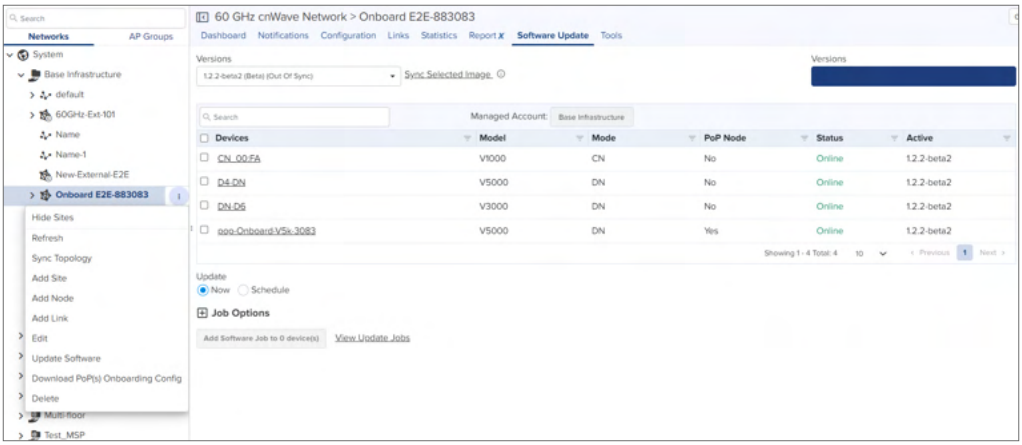
   Table 73 *Device Software Update: External E2E Controller*

Version	Example
If Software Version of the device is less than the Software Version of the External E2E Controller then Software Upgrade is successful.	External E2E Controller software version: 1.2.1 When Device Software Version is selected as 1.2.1 or lower then Device Software is upgraded successfully.
If Software Version of the Device is selected higher than the External E2E Controller version then Software Upgrade fails.	E2E External Controller Software Version :1.2.1 When Device Software Version is selected as 1.2.2 or higher then Device Software upgrade fails. Error message: **Device version should not be higher than External E2E Controller version 1.2.1**

Onboard E2E Controller

1. In the **Networks**, select Onboard E2E Network and check the software version.
2. From Onboard E2E Network menu options, select **Update Software.**

   Software Update page appears.



Device software update version check for Onboard E2E Controller is described in Table 74.

Table 74 *Device Software Upgrade: Onboard E2E Controller*

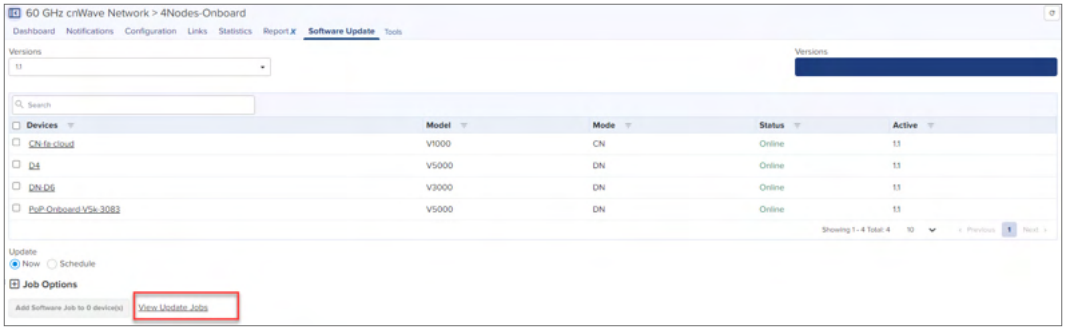
Software Upgrade	Example
If software version of Onboard PoP device is lower and upgraded to higher version then Software Upgrade is successful.	If the Onboard PoP device is running with 1.2, and selected software version is 1.2.1 or higher then Onboard PoP device is upgraded successfully.
If software version of all devices including Onboard PoP are lower and upgraded to higher version then Software Upgrade is successful.	If all the devices including the Onboard PoP are running with 1.2, and selected software version is 1.2.1 or higher then all the devices including PoP device are upgraded successfully.
If software version of all devices are higher and downgraded to lower version except Onboard PoP then Software Upgrade are successful.	If all the devices are running with 1.2.2, and selected software version is 1.2 then all the devices expect PoP device are upgraded successfully.
If software version of all devices including PoP are higher and downgraded to lower version then Software Upgrade are successful.	If all the devices including PoP are running with 1.2.2, and selected software version is 1.2 then all the devices are upgraded successfully.
If software version of all devices including Onboard PoP are higher and downgraded to lower version then Software Upgrade should fail if one or more nodes running with higher version in list.	If all the devices including the Onboard PoP are running with 1.2.2, and selected software version is 1.2.1 then Software Upgrade should fail.
If software version of Onboard PoP device is higher and upgraded to lower version then Software Upgrade for PoP fails, only when other devices software version are higher.	If the Onboard PoP device is running with 1.2.2, and selected software version is 1.2.1 or lower then Software Upgrade of Onboard PoP device fails, only when the other devices software version is 1.2.2.
If software version of all devices are lower and upgraded to higher version except Onboard PoP then Software Upgrade should fail.	If all the devices including Onboard PoP are running with 1.2.2, and selected software version is 2.0 excluding PoP node, then Software Upgrade for all the devices should fail except PoP node.
If software version of all devices including PoP is running with same version, and when you select all nodes to upgrade, then PoP fails to upgrade. You need to manually upgrade the PoP node.	If all the devices including PoP are running with software version 1.1 and selected software version is 1.2. If PoP failed to upgrade, then you need to manually upgrade the PoP.

3. From the **Versions** drop-down, select the version and the devices in the network for software upgrade.

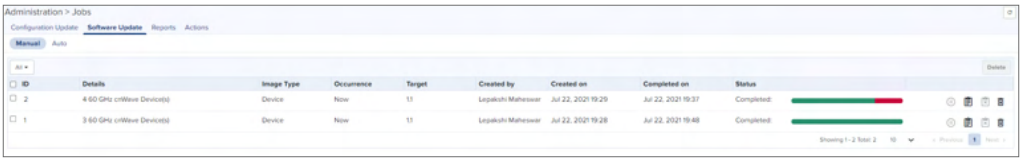
The Software Upgrade scenario for Onboard E2E Controller is explained in Table 74.

View Update Jobs

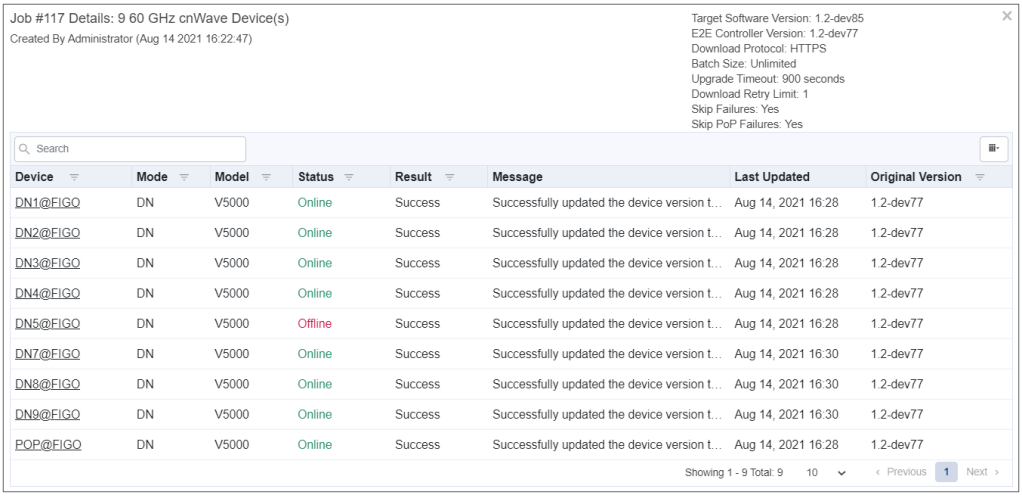
After adding the new Software Images, click **View Update Jobs.**



1. Navigate to the **Administration > Jobs > Software Update**.



2. Click **Show More** to view the Job Details.



Reports

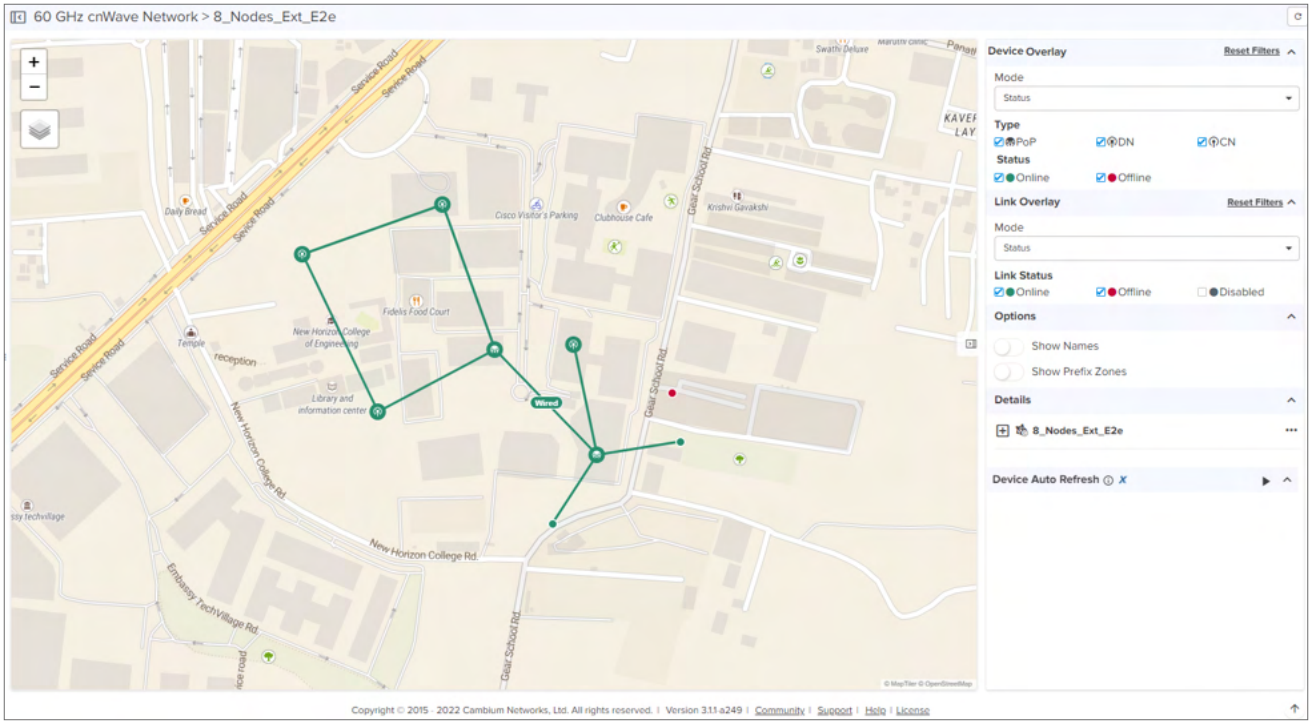
Reports page provides details on how to schedule and generate different types of data reports such as Devices, Active Alarms, Alarm History, and Events. For further details refer to Reports.

Map

Map shows how devices are connected in a E2E network, the state of the devices, and links in the E2E network. To view the map, perform the following:

- Navigate to **E2E Network** > select **Map** icon in the left pane of the homepage to view E2E Network and 60 GHz cnWave devices and links as shown in Figure 346.

Figure 346 *Viewing E2E Network*



Note

Gray color lines are un-managed links and gray color nodes are un-managed nodes.

The following fields provides visual representation of the nodes and links:

- Device Overlay
- Link Overlay
- Options
- Details
- Device Auto Refresh

Table 75 *Map fields in E2E Network*

Field	Description
Device Overlay	1. Select the **Mode** type as **Status** to view the following: • Status: The device status is Online or Offline. • Type: The device types are PoP, CN, or DN in the E2E Network.

Table 75 *Map fields in E2E Network*

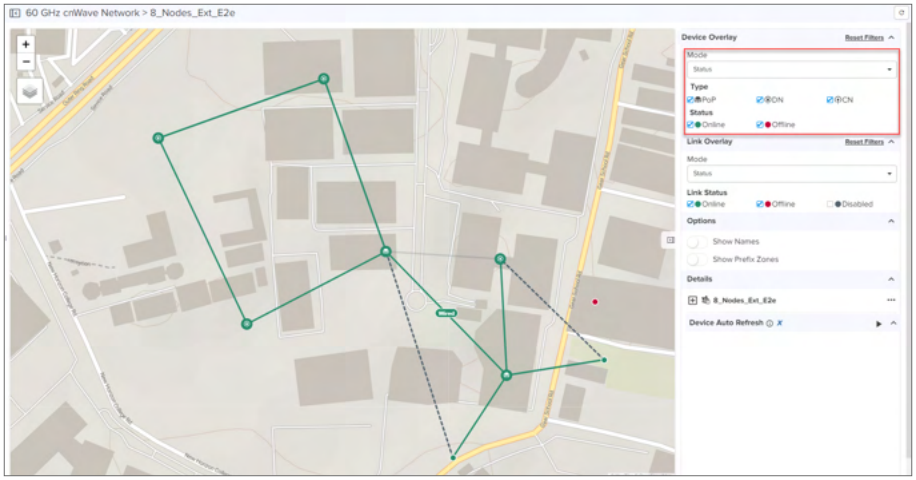
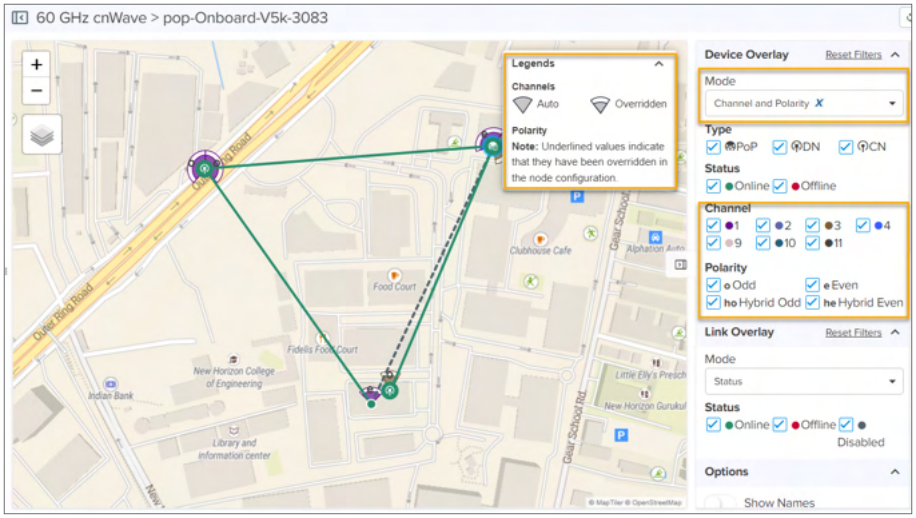
Field	Description
	 2. Select the **Mode** type as **Channel and Polarity** to view the following: • Channel: The seven channels are represented in different color codes. Auto channel is indicated as and Overridden channel is indicated as . • Polarity: The polarity is represented as odd, even, hybrid odd, and hybrid even. Underlined values indicate they have been Overridden in the node configuration.  3. Select the **Mode** type as **Sector** to view the following: Sector: The two sectors are represented in two different color codes.

Table 75 *Map fields in E2E Network*

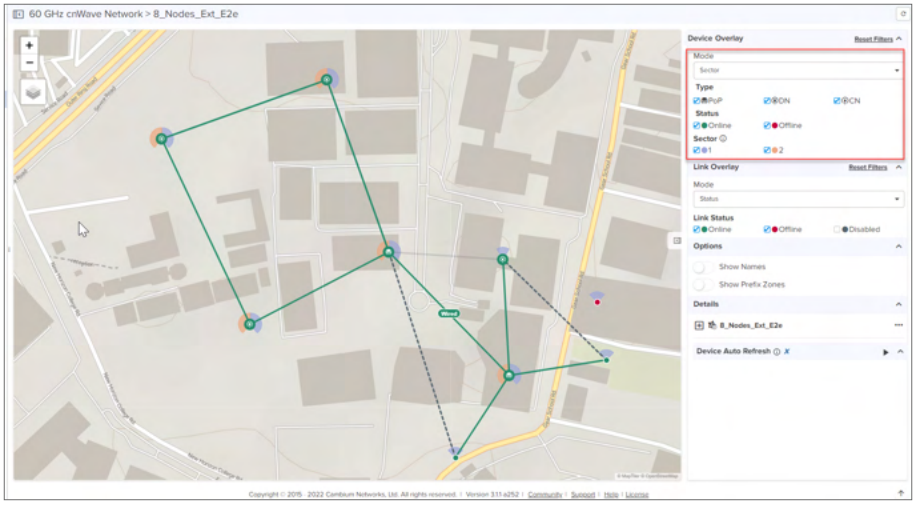
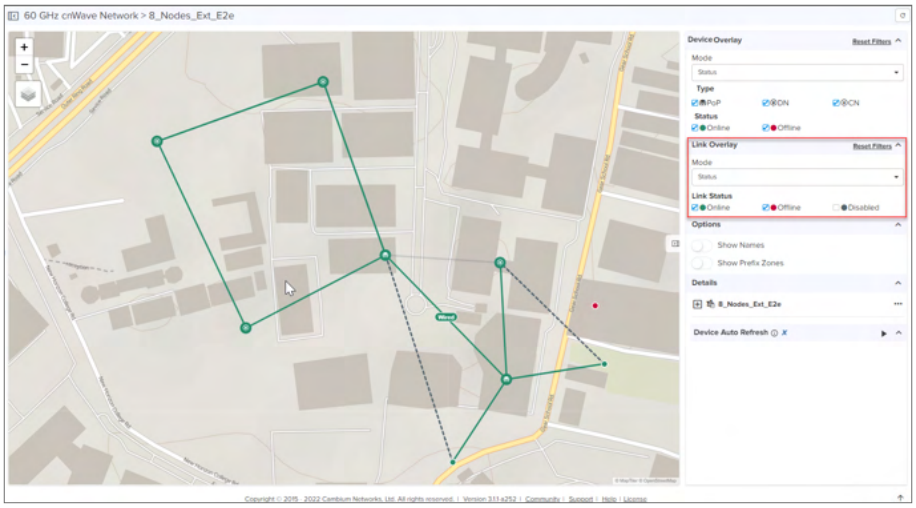
Field	Description
	 V5000 Sectors is shown below: 
Link Overlay	1. Select the **Mode** type as **Status** to view the following: Status: The link status is Online or Offline.  By default **Ignition Disabled** is checked, which appears in light gray.

Table 75 *Map fields in E2E Network*

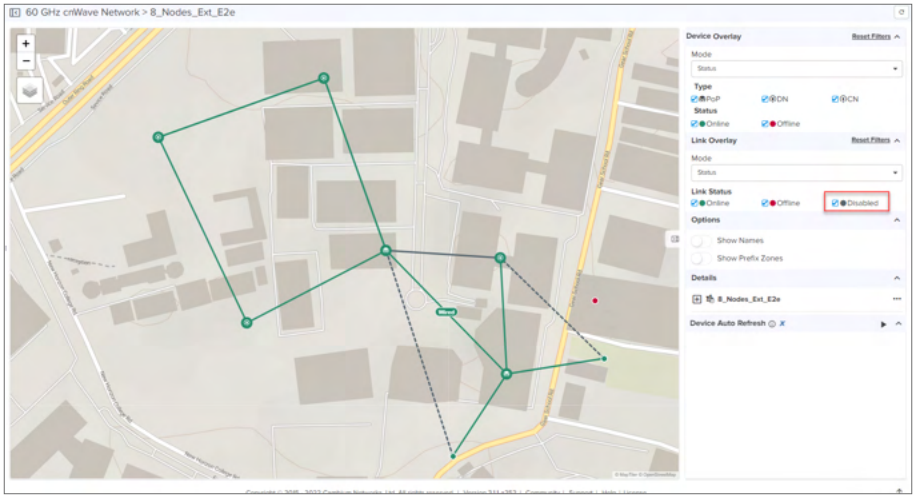
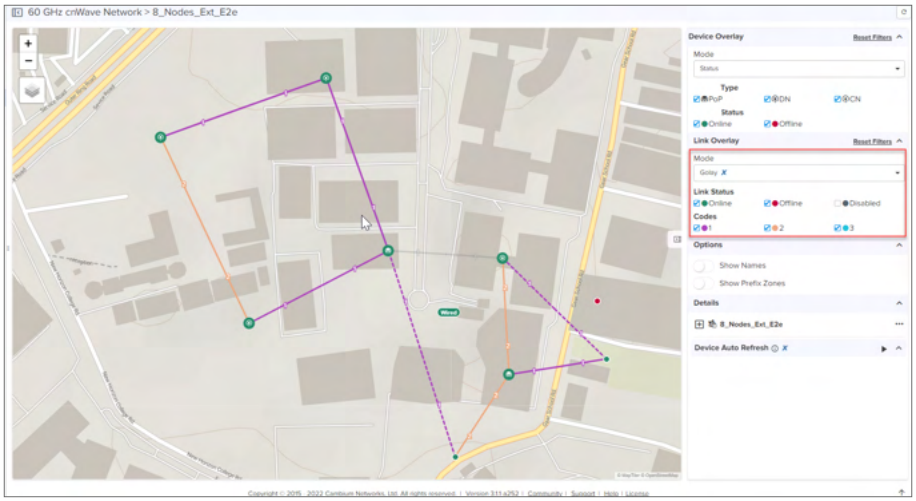
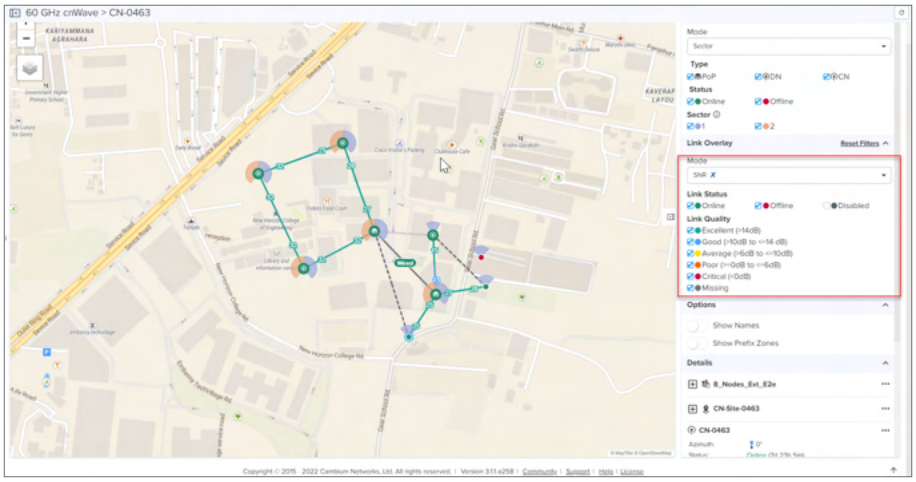
Field	Description
	 2. Select the **Mode** type as **Golay** to view codes. Golay: Golay is represented in color codes, as shown below:  3. Select the **Mode** type as **SNR** to view link qualities. • SNR: SNR shows various SNR link qualities and is represented in different colors. 

Table 75 *Map fields in E2E Network*

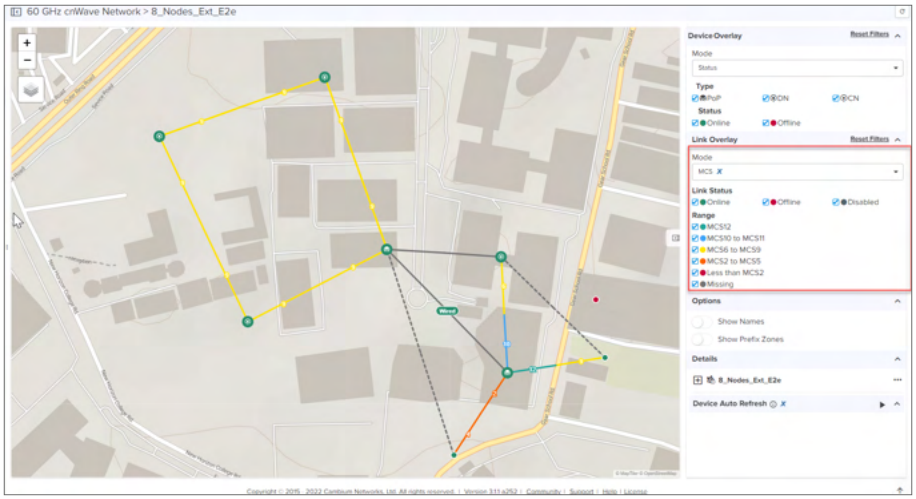
Field	Description
	4. Select the **Mode** type as **MCS** to view link range. MCS: MCS shows the link status, and various link ranges represented in different colors.  5. Select the **Mode** type as **RSSI** to view link qualities. RSSI: RSSI shows various RSSI link qualities represented in different colors.  6. Select the **Mode** type as **Link Fade Margin** to view link fade margins. Link Fade Margin: calculates link fade margins between two devices. For details on overview and calculation, refer to the example described in Figure 347.

Table 75 *Map fields in E2E Network*

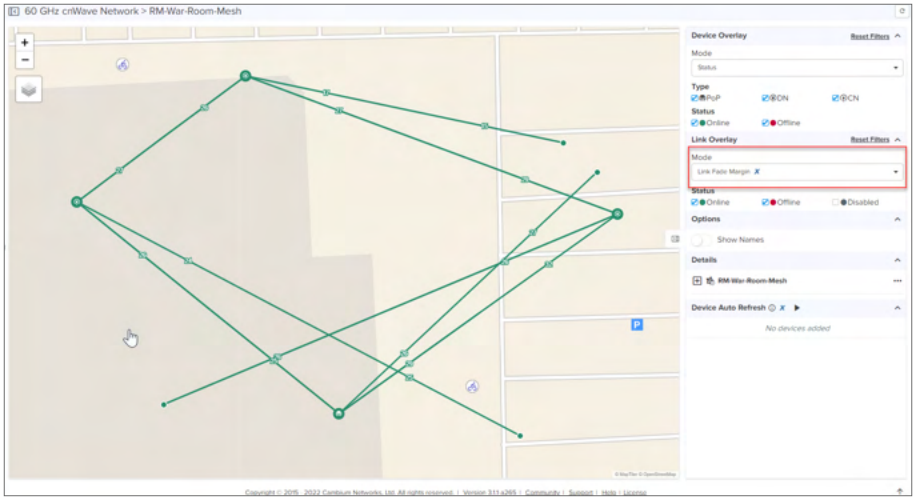
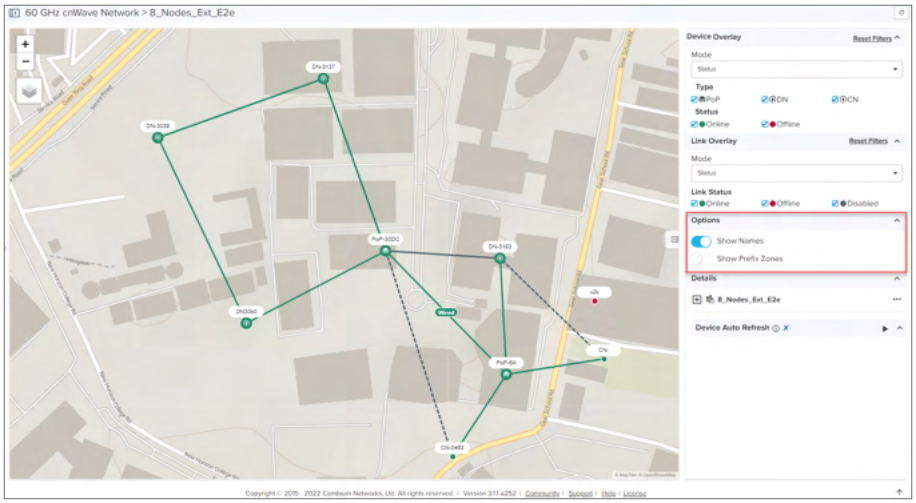
Field	Description
	 **Note**: Link Fade Margin is applicable only when E2E Controller and Device version are 1.2.2. • Airtime% • Throughput (Mbps)
Options	Toggle to view **Show Names** and **Show Prefix Zones,** as described**:** • **Show Name**: shows the name of the nodes available in the E2E Network.  • **Show Prefix Zones**: shows the prefix zone of each PoP that is communicating with each other.

Table 75 *Map fields in E2E Network*

Field	Description
	
Details	Details: displays the basic details of E2E Network when E2E Network is selected from the tree.  1. Click ellipsis (...) icon in the **Details** section to view E2E Network Dashboard. 

Table 75 *Map fields in E2E Network*

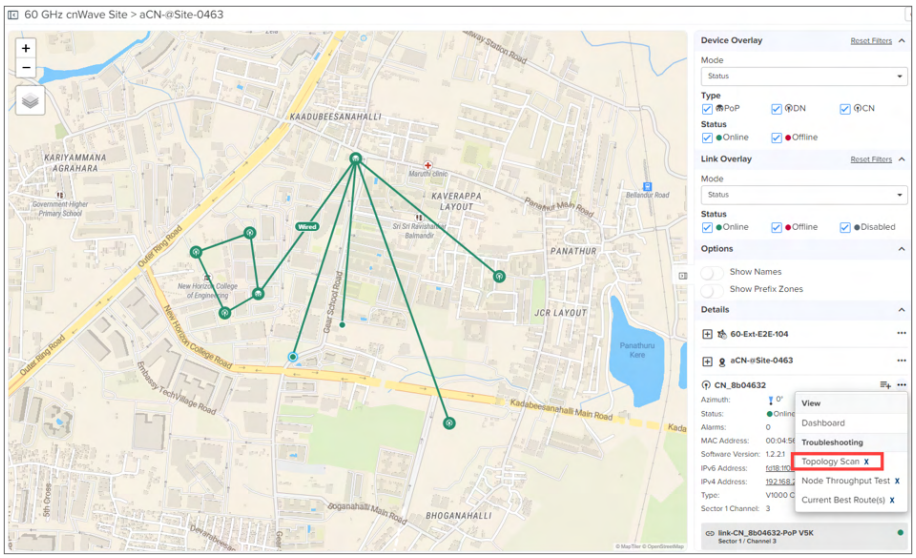
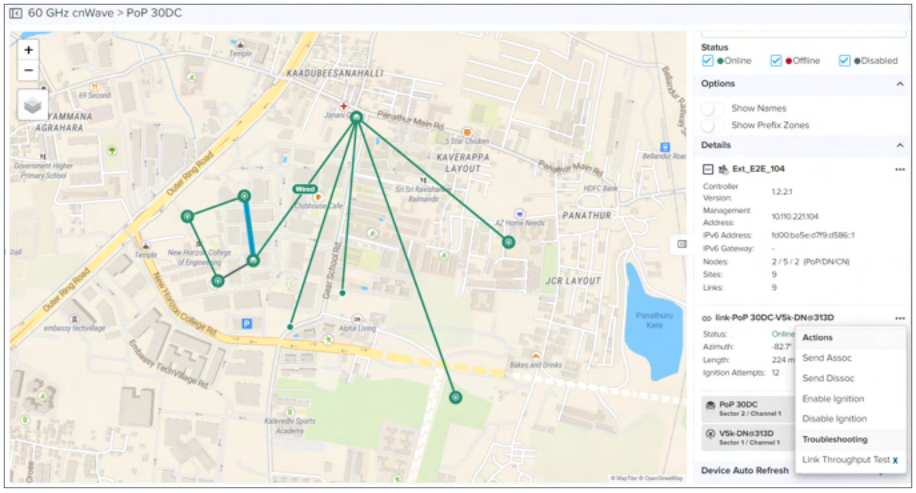
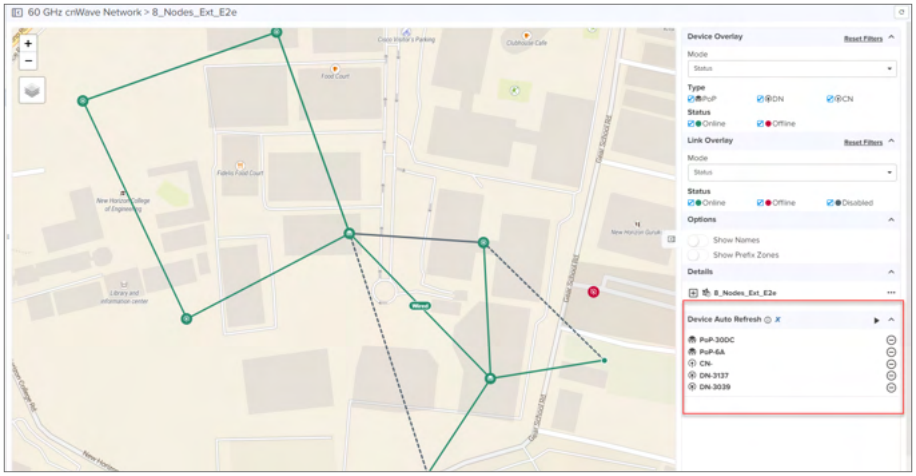
Field	Description
	2. When a device is selected from the map, the device details are displayed. Click ellipsis (...) icon next to the device to view the device **Dashboard** and **Topology Scan.** For more details on how to troubleshoot a node using Topology Scan refer Topology Scan.  • Node Throughput Test and Current Best Routes are added in the Troubleshooting section. 3. When a link is selected from the map, link details are displayed. Click ellipsis (...) icon next to link to view the **Actions** details for the links.  • Link Throughput Test is added in the Troubleshooting section. **Device Auto Refresh:** allows to refresh data automatically in the E2E Network. 1. Select the devices in the map and add it to the watch list for **Device Auto Refresh**. 2. Click the (▶) play icon to start **Auto Refresh**.

Table 75 *Map fields in E2E Network*

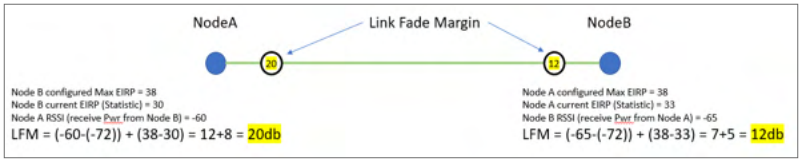
Field	Description
	 **Note**: A maximum of 10 devices can be added to **Device Auto Refresh**. 3. Click (⊖) to remove devices from **Auto Refresh**.

Note

- Channel and Polarity mode type are available for cnMaestro X users only.
- Airtime%, Golay, SNR, RSSI, MCS, Link Fade Margin, and Throughput (Mbps) are cnMaestro X features.

A new Link Fade Margin (LFM) statistics has been added to the displayed **Link Statistics** tab in 60 GHz cnWave 1.2.2 software version release. This statistic is shown in units of dB, and it is meant to provide operators with a quick way to assess any additional **system gain** a RF link has available in order to help ride out potential RF link fades due to weather (most typical) or other temporary RF link impairments. The rough calculation for LFM is comprised of the RSSI received from a remote transmitter and assessing how much more TX power is available (from the remote transmitter) and how far away the RSSI value is from an established receiver sensitively floor of -72 dBm. The LFM allows operators quicky assess if/where you may have some marginal RF links that need to be addressed in some way. Typical options would be changing an existing node out for a V3K (to get more margin) or possibly dropping in an intermediate DN node such that their RF paths are shorter, typically resulting in a much larger LFM.

Figure 347 *Link Fade Margin*



Troubleshooting

- Topology Scan
- Node Throughput Test
- Current Best Routes X
- Link Throughput Test

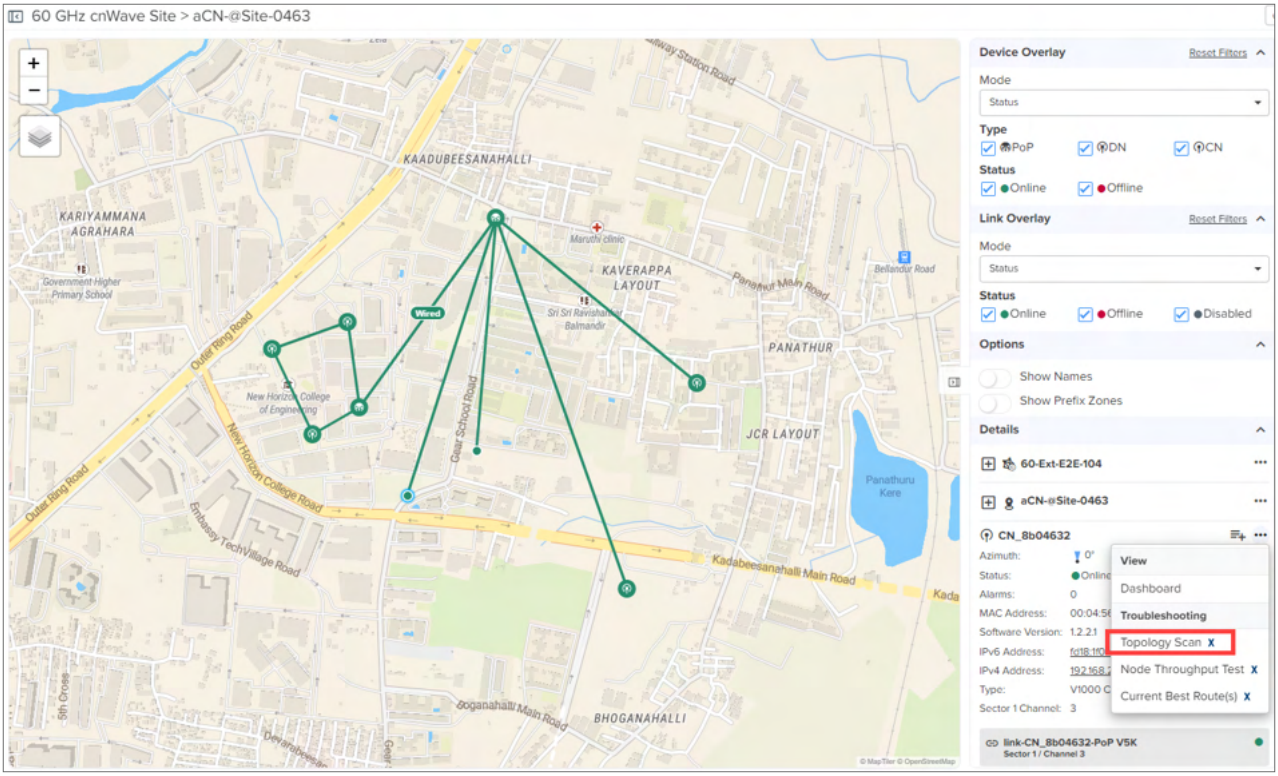
Topology Scan

Topology Scan X allows you to discover your entire network and create comprehensive, detailed network topology maps. This tool will only detect nodes operating in responder mode. It will not detect CNs with a wireless link already established. Offline nodes with a configured channel override will not be detected on a different channel.

Note

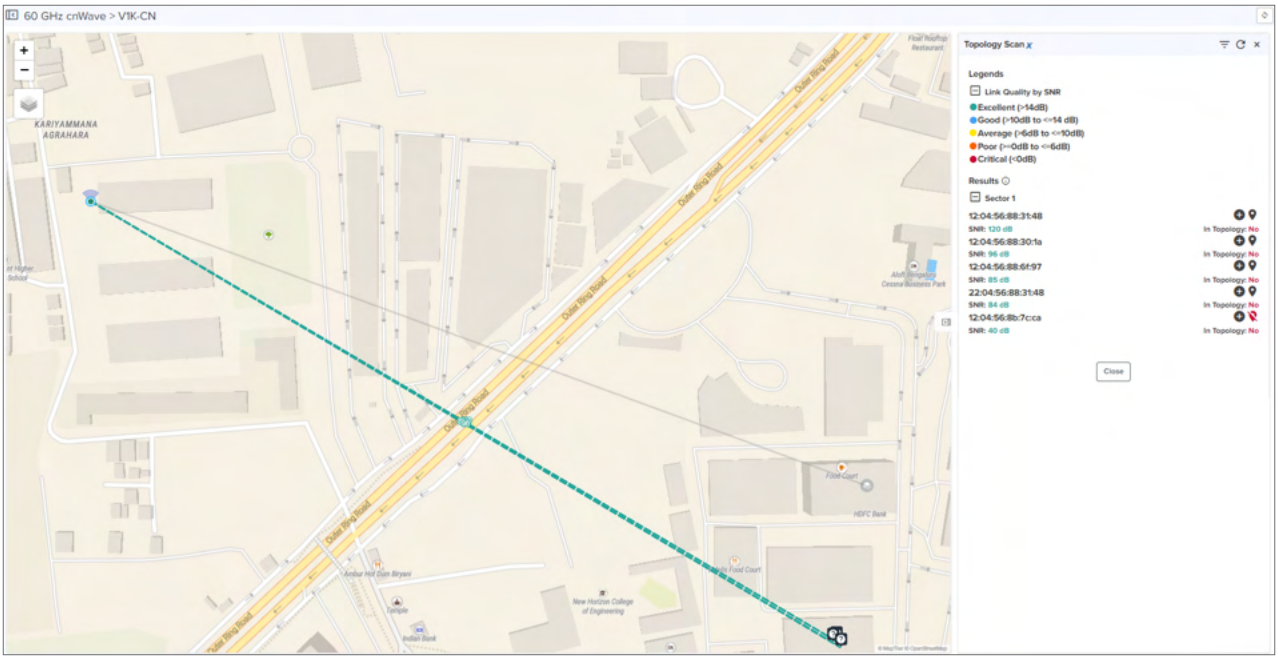
Topology Scan will cause a momentary throughput reduction in nearby links.

1. Select a node from the Map.
2. Click ellipsis (•••) icon next to the device to select the **Troubleshooting** > **Topology Scan.**



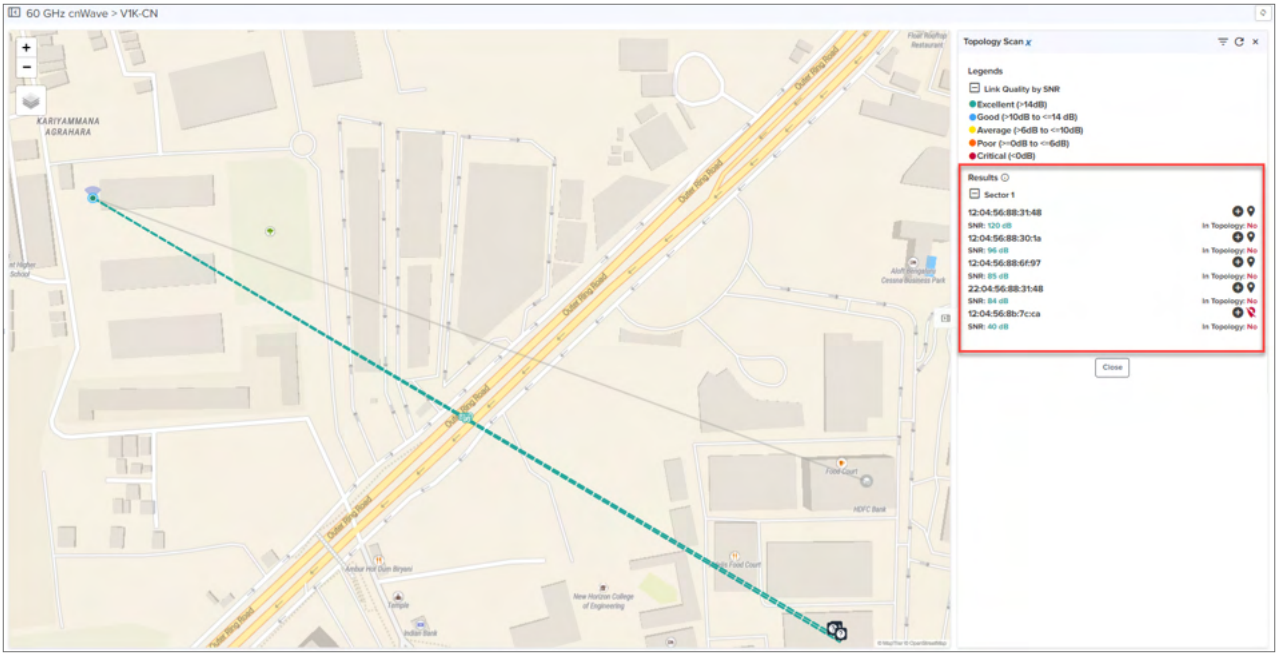
Topology Scan preview window is displayed towards the left pane.

3. Click **Start Topology Scan**. Topology Scan begins as shown in the following figure.



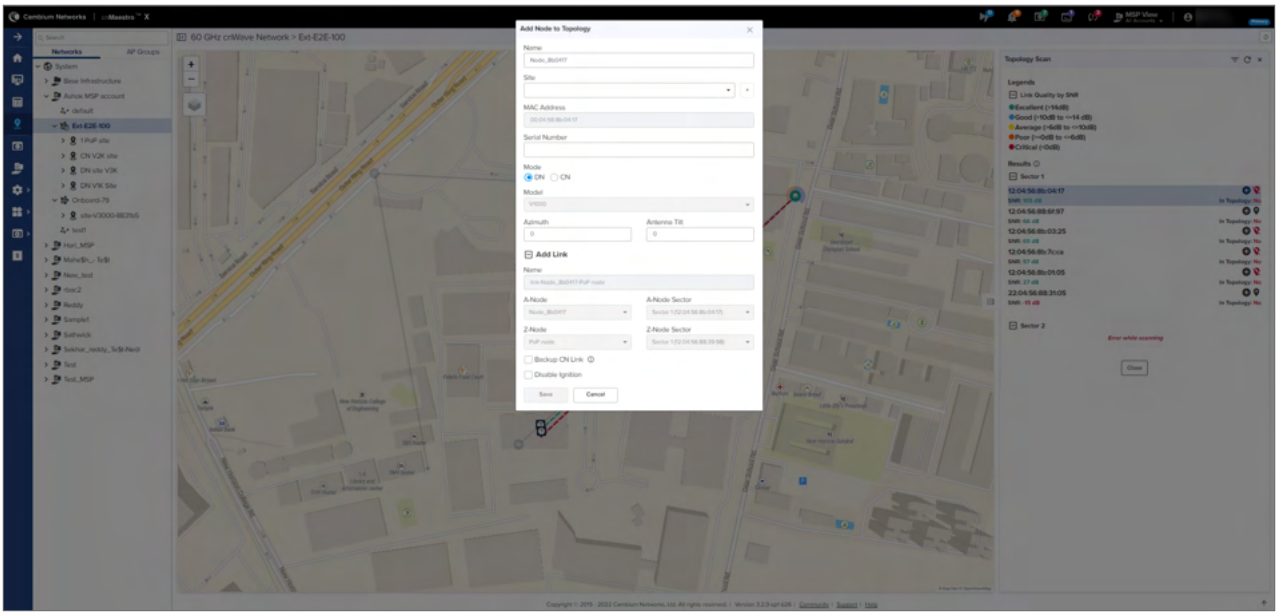
4. Click **Configure SNR Limit** ( ) next to **Topology Scan** header to add new value or reset the existing value. By default SNR value is 5 dB.
5. Click ( ) refresh icon to scan again.

   The results are based on **Link Quality by SNR** and the results are shown in the left pane. MAC Address of the links and the Link Quality is displayed.



   After topology scan, map displays available nodes and links in the network by Link Quality color codes. Only links available with GPS coordinates are shown in the map. You can add site, node, and link to the topology by clicking the plus sign **In Topology.**

6. **Add Node to Topology** window pops up.



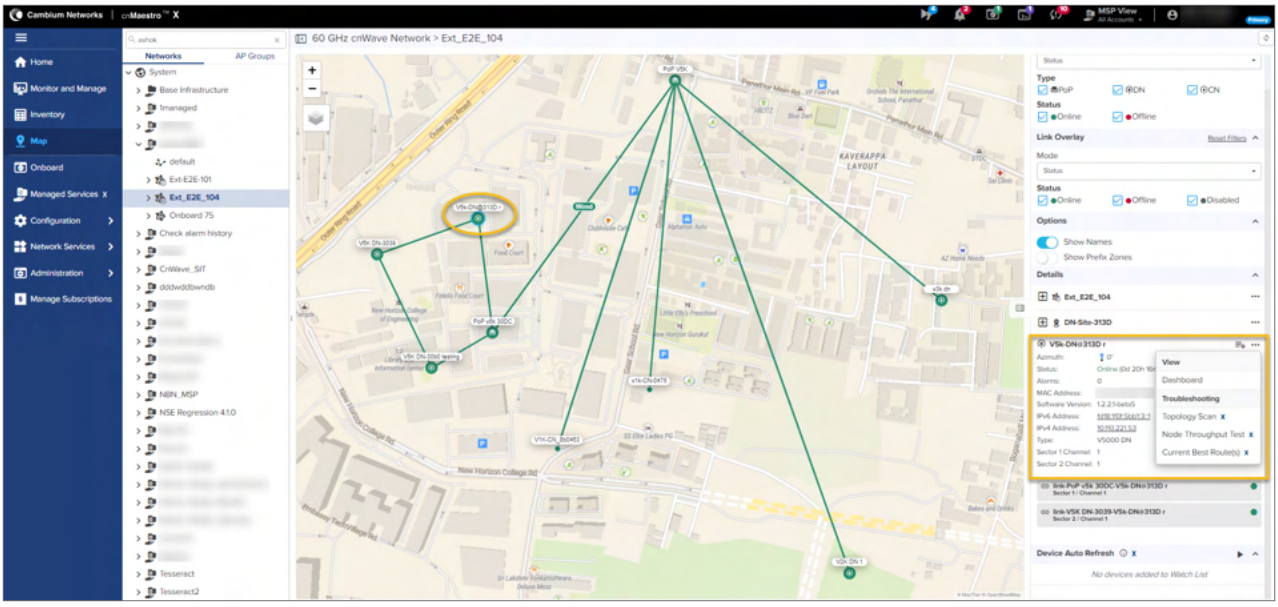
7. Enter the node and link details and click **Save**.

Node Throughput Test X

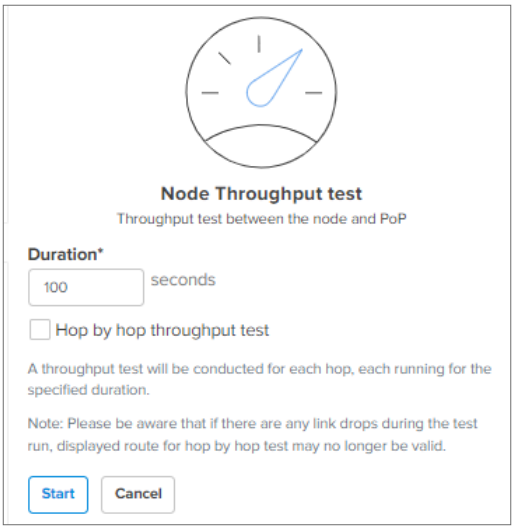
The **Node Throughput Test X** option allows you to test the throughput between a node and PoP. Using this option, you can conduct a throughput test for each hop seamlessly.

To run a node throughput test, complete the following steps:

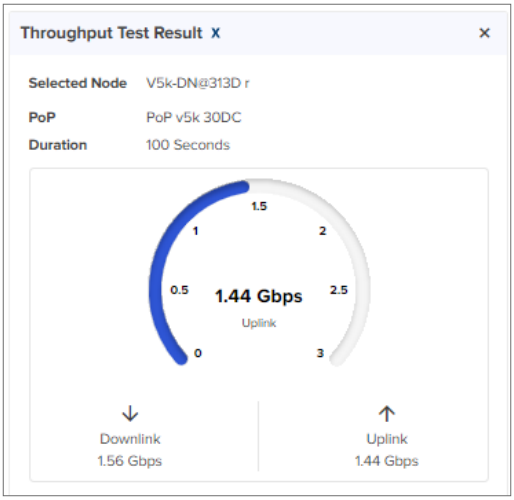
1. Select a device except the POP Node from the Map.

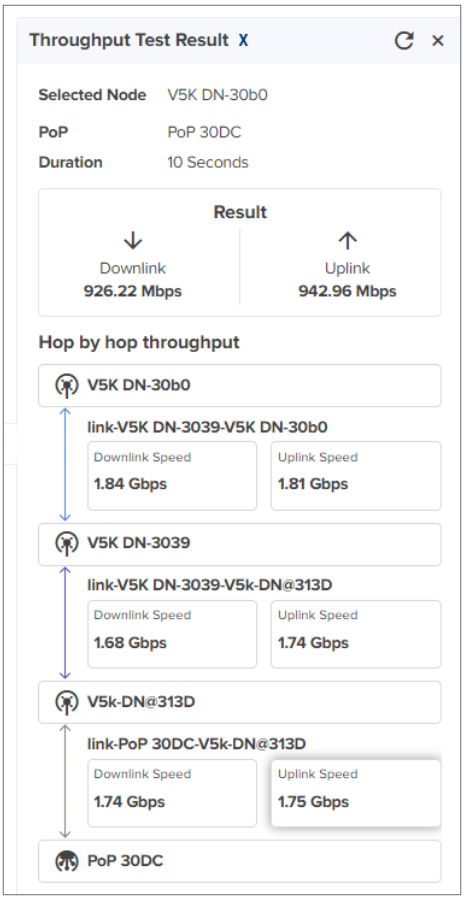


2. Click ellipsis (•••) icon next to the device name in the right pane, and select **Troubleshooting** >**Node Throughput Test X**



3. Enter the **Duration** between 5 to 300 seconds.
4. Select the **Hop by hop throughput test** check box to view the throughput for each hop separately.
5. Click **Start**.





Current Best Route(s) X

The Current Best Route(s) X feature is used to view the best route from a CN/DN to PoP. The **Current Best Route (s) X** map view displays statistics of the following parameters for uplink and downlink of wireless link of a node:

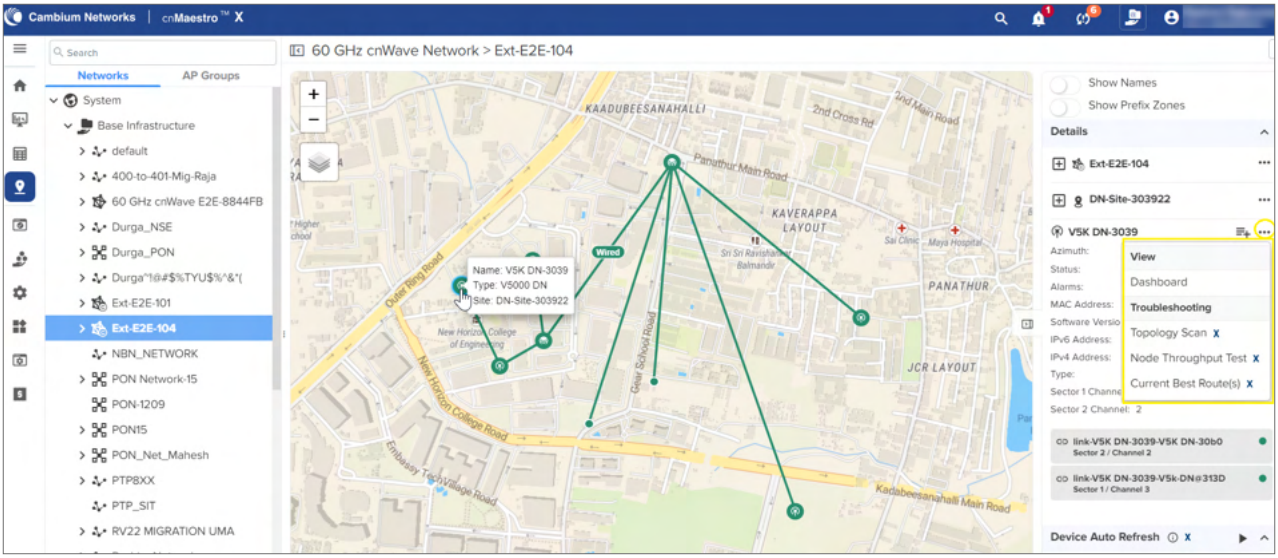
- Golay
- SNR
- MCS
- RSSI
- Throughput (Mbps)
- Airtime (%)
- Link Fade Margin (LFM)

Note

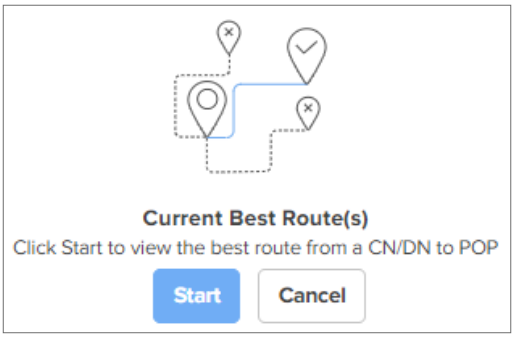
The **Current Best Route(s) X** feature is applicable only to X accounts. In addition, this feature is supported only on the E2E Controller (Onboard or external) running with software version 1.2.2.1 or later.

To view the current best routes, complete the following steps:

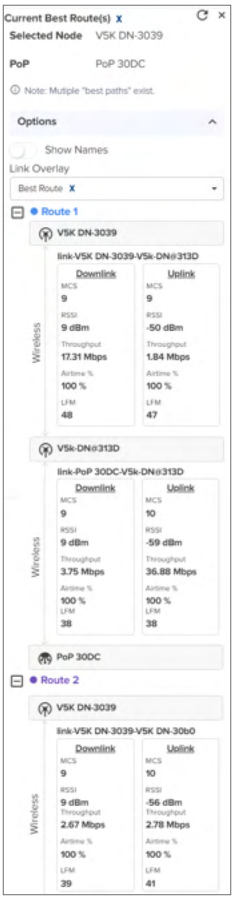
1. On the **Map** page, select a device node. The node details are displayed on the right side of the map.



2. Click the ••• icon next to the node name, and select **Troubleshooting** > **Current Best Route(s) X**. The **Current Best Route(s)** screen appears on the right side of the map.



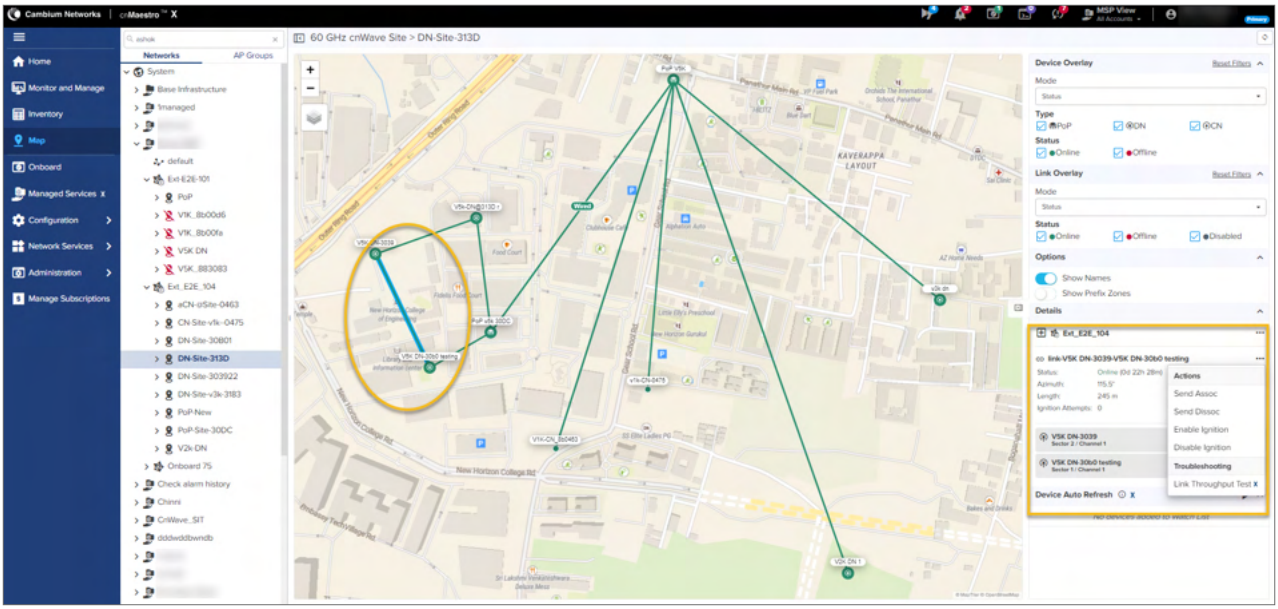
3. Click **Start**. The **Current Best Routes(s) X** section displays route details for the selected node.



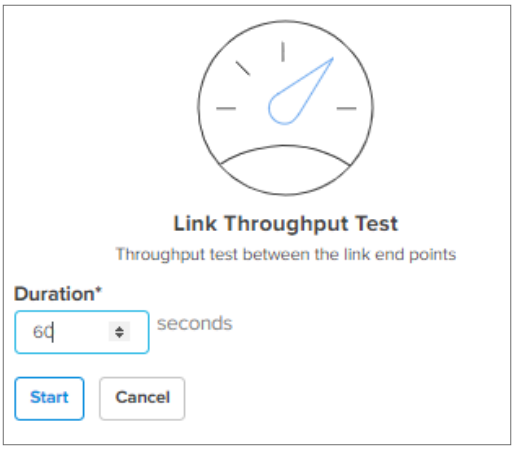
Link Throughput Test X

The **Link Throughput Test X** option allows you to test the throughput between the link end points. To run a link throughput test, complete the following steps:

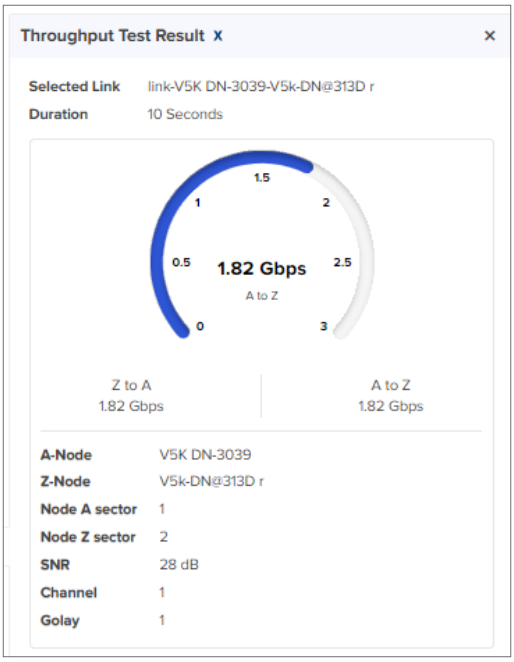
1. Select a Link from the Map.



2. Click ellipsis (•••) icon next to the link, and select the **Troubleshooting** >**Link Throughput Test X**



3. Enter the **Duration** between 5 to 300 seconds.
4. Click **Start**.



Note

Show Prefix Zones is enabled only if **Prefix Allocation** is set to **Deterministic**.

Tools

The Tools page allows the user to perform the following actions:

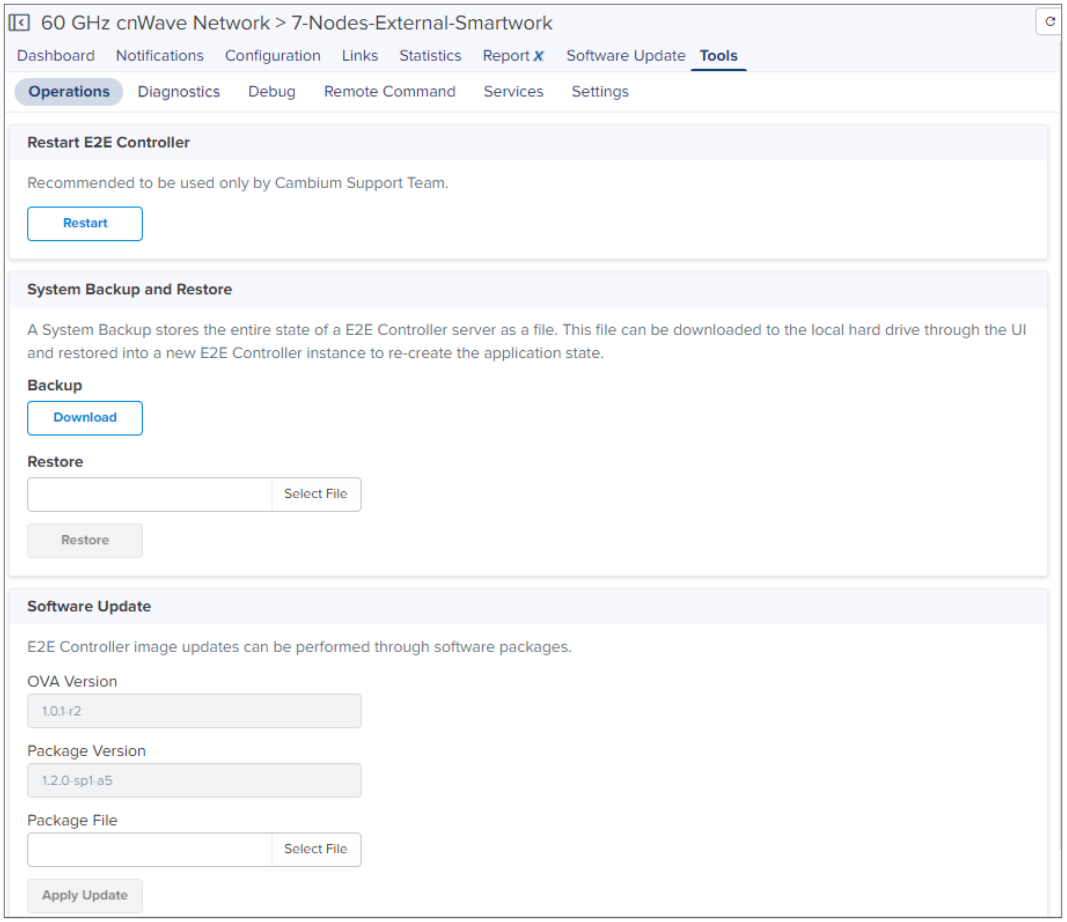
- Operations
- Diagnostics
- Debug
- Remote Command
- Services
- Settings

Operations

External E2E Controller deployment

If the device is deployed through **External E2E Controller** it displays the operations page as follows:

- **Restart E2E Controller** performs the **Restart.**
- A **System Backup and Restore** the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create.
- The **Software Upgrade** is to upgrade E2E controller and can be done through E2E controller package.

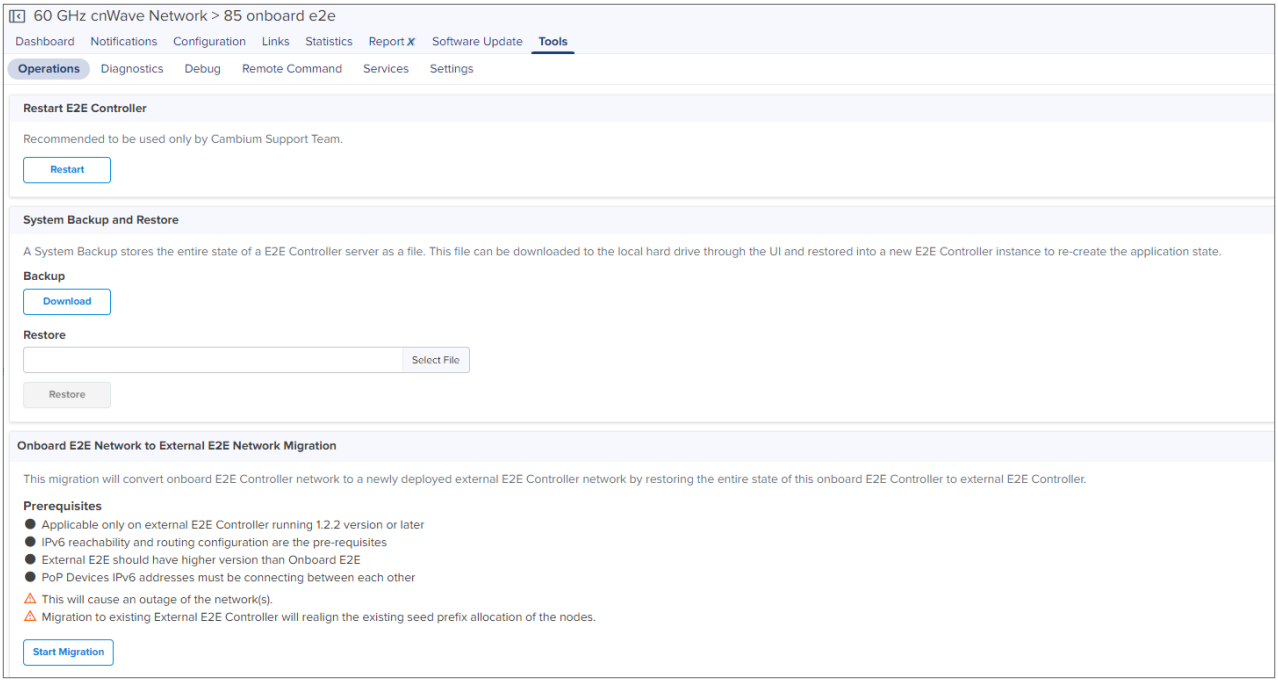


Onboard E2E Controller deployment

If the device is running **Onboard E2E Controller** it displays the operations page as follows:

- **Operations** page allows the user to **Restart E2E Controller** and perform the **System Backup**. It also stores the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller

instance to re-create the application state.



Onboard E2E to External E2E Migration

When you onboard an E2E Controller to External E2E Controller with or without sites, consider the following prerequisites:

- Applicable only on external E2E Controller running with 1.2.2 version or later.
- IPv6 reachability and routing configuration are pre-requisites.
- External E2E Controller should have higher version than Onboard E2E.
- PoP Devices IPv6 addresses must be connecting between each other.

When you onboard an E2E Controller to External E2E Controller with sites, consider the following prerequisites:

- Multiple Multi-PoP Networks must not be connected to same wired switch.
- Selected Onboard Network and External E2E Controller networks for migration should not have same site and device names.

Post Migration Steps:

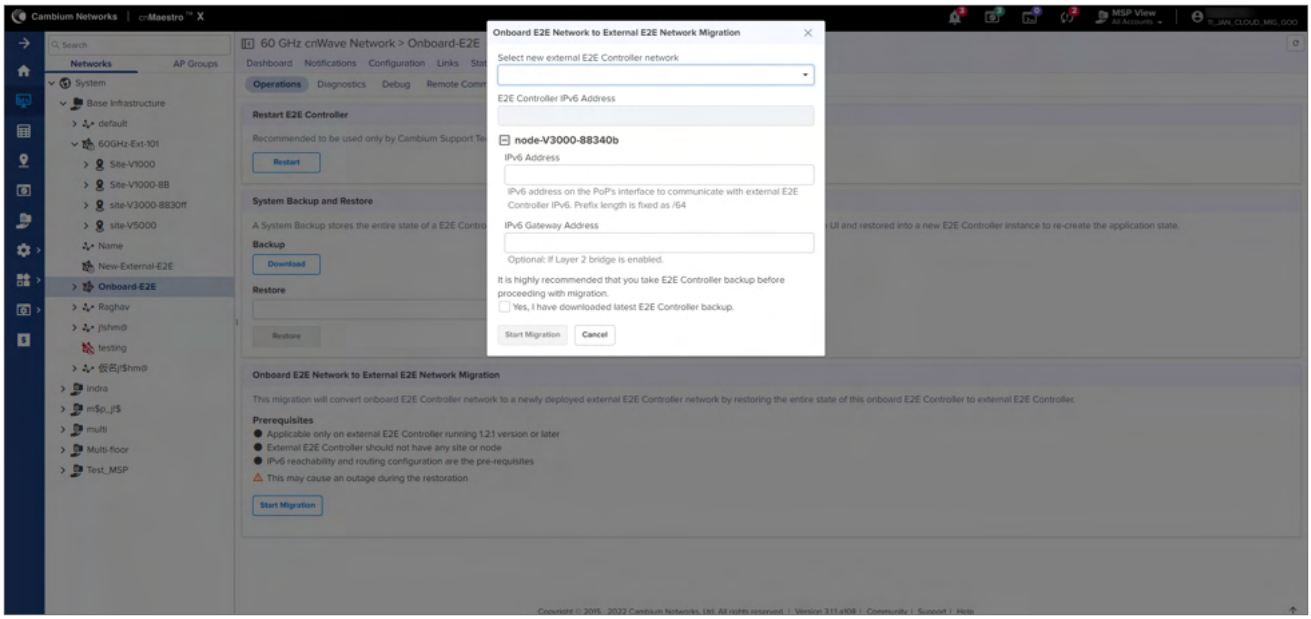
- Multi-PoP / Relay Port should be updated with the interface as in PoP interface configuration if not already done, to allow the connection between PoPs.
- If the existing E2E Network if configured with BGP, migrated PoP BGP Configuration must be updated in cnMaestro and then in POP GUI
- If the PoPs are not on the same L2 network:
  - Controller configuration about broadcast should be set to true.
  - If External E2E Controller and PoP devices are not connected/routed through a network router

- It is recommended to set Deterministic prefix algorithm
- Routes to each PoP with respective Seed Prefix should be added manually in E2E Controller.

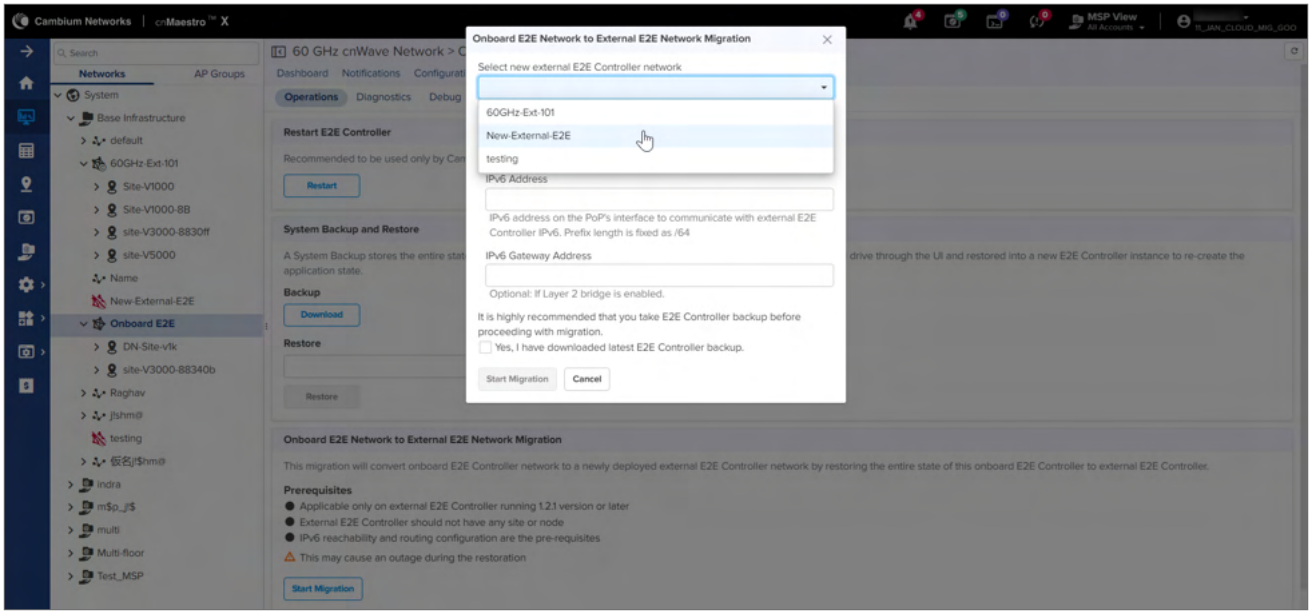
Perform the following steps to migrate Onboard E2E Controller to External E2E Controller:

1. 1. Select Onboard E2E Network > **Tools** > **Operations.**
2. 2. Click **Start Migration**.

The **Onboard E2E Controller to External E2E Migration** window appears.

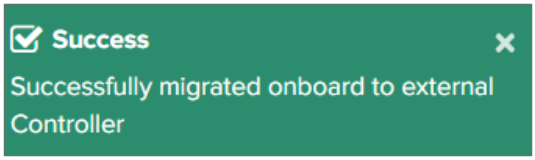


1. 3. Select a new external E2E Controller network from the drop-down.

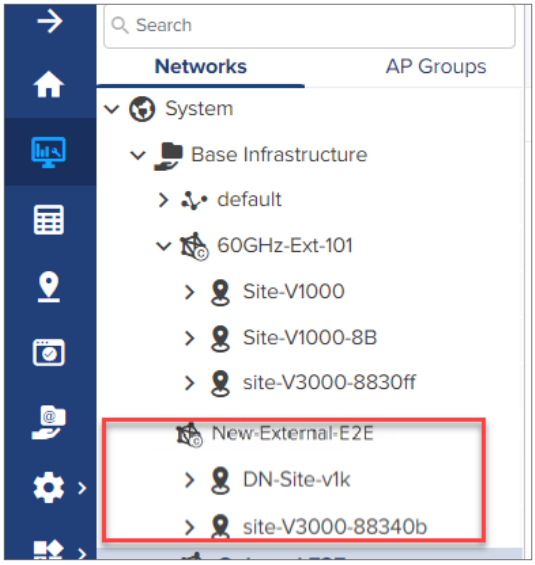


1. 4. Enter **IPv6 Address**.
2. 5. Enter **IPv6 Gateway Address** of PoP node, which is optional.
3. 6. Select the checkbox next to **Yes, I have downloaded latest E2E Controller backup**.
4. 7. Click **Start Migration**.

A successful message on migration process is displayed.



The Onboard E2E Controller network is migrated with all the sites and nodes into External E2E Controller, as shown below:



Fallback to Onboard E2E Network

The fallback process is applicable only for External E2E networks where Onboard to External E2E Network migrated. Perform the following steps to fallback to Onboard E2E Network after the migration from Onboard to External E2E Network.

1. 1. Change the Controller IPv6 in the PoP from cnMaestro in External E2E Controller.
2. 2. Go to PoP GUI and when the status displays as not connected, Enable Onboard E2E Controller.
3. 3. Disconnect the External E2E controller from cnMaestro.
4. 4. Delete the devices and sites in cnMaestro when the External Controller is offline, as they will conflict with Onboard E2E network devices when connected to cnMaestro.
5. 5. In cnMaestro, approve the Onboard E2E network and restore the backup taken before the Migration.
6. 6. Verify the Network and devices status in PoP device GUI and cnMaestro.

Scheduling configuration backup of E2E Controller

You can configure FTP or sFTP and schedule to backup the configuration of E2E Controller (onboard or external) using cnMaestro. The backup scheduling option allows you to schedule and save the automated configuration backup in a FTP or sFTP path (which you provided as an input during FTP or sFTP configuration). This scheduling option helps in availing the latest configuration backup and recovering the 60GHz cnWave network to the latest available configuration when E2E Controller crashes or rebuilt.

Note

- The scheduling option requires the sFTP or FTP configuration as the backups are uploaded to the sFTP or FTP remote path only.

- This backup scheduling option is supported for both Onboard and External E2E Controller deployments.
- FTP or sFTP Ports must be allowed in network firewall from a VM or device running E2E Controller service to the respective FTP or sFTP server.
- The backup scheduling option is supported in 5.1.0 Cloud and On-Premise cnMaestro release and 1.4 E2E Controller release.

To configure the FTP or sFTP settings and schedule the backup, complete the following steps:

1. From the **Home** page of cnMaestro, navigate to Monitor and Manage > E2E Network > Tools > Operations.

   The **Operations** page displays options to configure settings for E2E Controller.

2. In the **FTP Server Settings** section, configure a remote file server (FTP or sFTP) to upload the backups generated through the scheduled jobs.

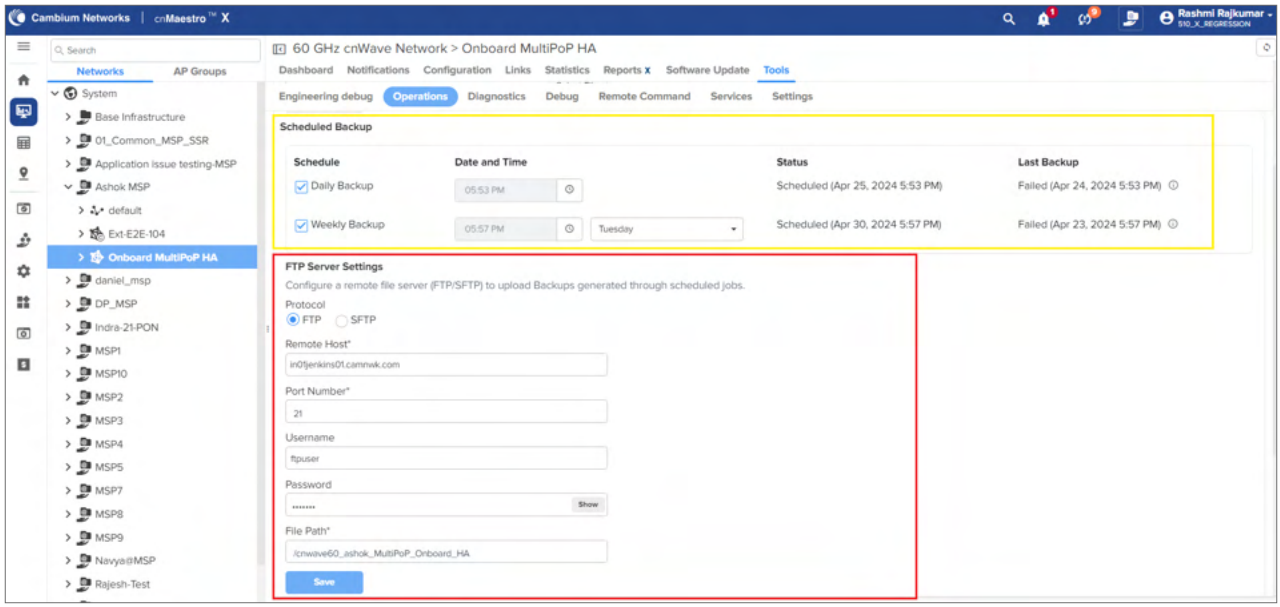


Table 76 lists the parameters required for configuring the remote FTP or sFTP server.

Table 76 *Parameters for FTP/sFTP server settings*

Parameter	Description
Protocol	File protocol (FTP or sFTP) required for uploading the backup of E2E Controller over the network. Select the required protocol.
Remote Host	The remote host name of the FTP or sFTP file server. Provide IP or DNS resolvable host name in the text box. This is a mandatory parameter.
Port Number	The port number used to allow in network firewall from a VM or device running E2E Controller service to the respective FTP or sFTP server. This is a mandatory parameter.
Username	Username to log in to the remote FTP or sFTP server.

Table 76 *Parameters for FTP/sFTP server settings*

Parameter	Description
Password	Password that is required to authenticate the remote FTP or sFTP server.
File Path	The remote file path of FTP or sFTP server where the backups are uploaded automatically on scheduling.

3. Click **Save**.

   The remote FTP or sFTP configuration is successfully updated.

4. To schedule the backup job, use the following options (either one or both) in the **Scheduled Backup** section:

   - **Daily Backup**: For the daily backup, set the time (in 24-hours format) using the **Date and Time** parameter.
   - **Weekly Backup**: For the weekly backup, set the time (in 24-hours format) and day.

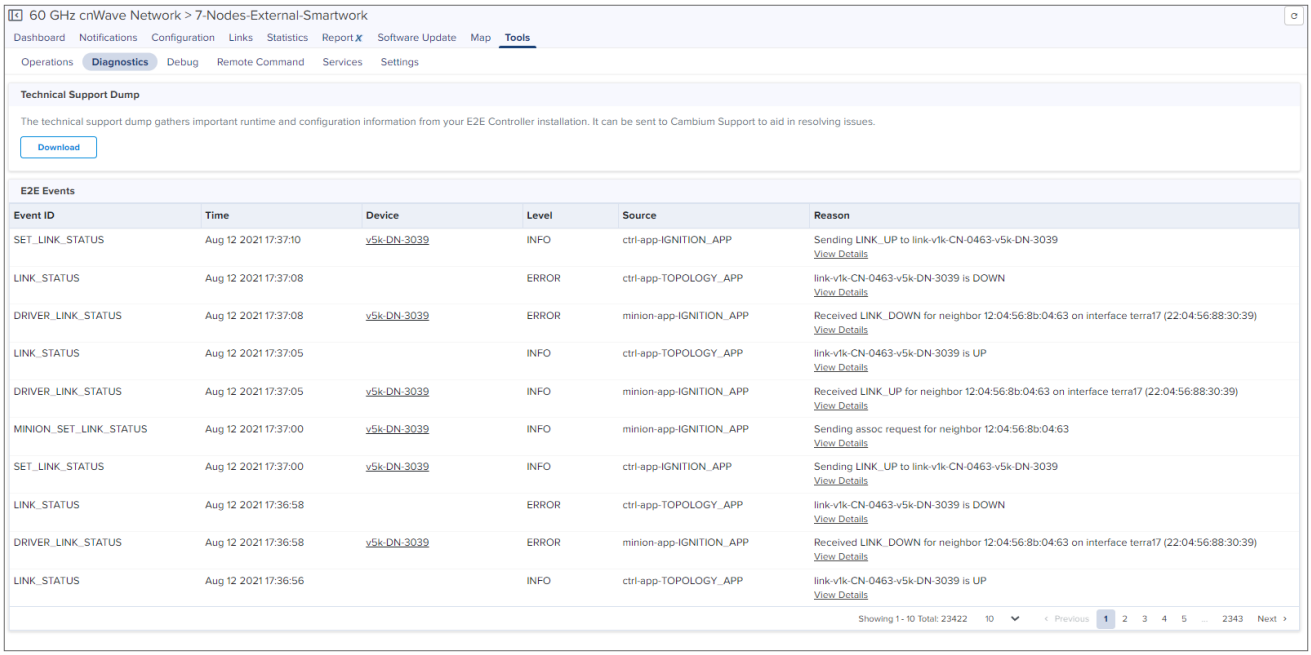
     The **Status** field in the **Scheduled Backup** section displays date and time of the scheduled job. Similarly, the **Last Backup** field displays date and time of the last failed job.

Diagnostics

Diagnostics page allows the user to gather Technical Support Dump and can be downloaded and sent to cambium support team.

All the events information of E2E controller can be viewed under E2E Events. In **E2E Events** tab user can view the **Event ID, Time, Device, Level, Source** and **Reason** of the E2E Network**.**

Figure 348 *Diagnostics*



Debug

In **Debug** tab, you can view and download the Node logs by executing the following log:

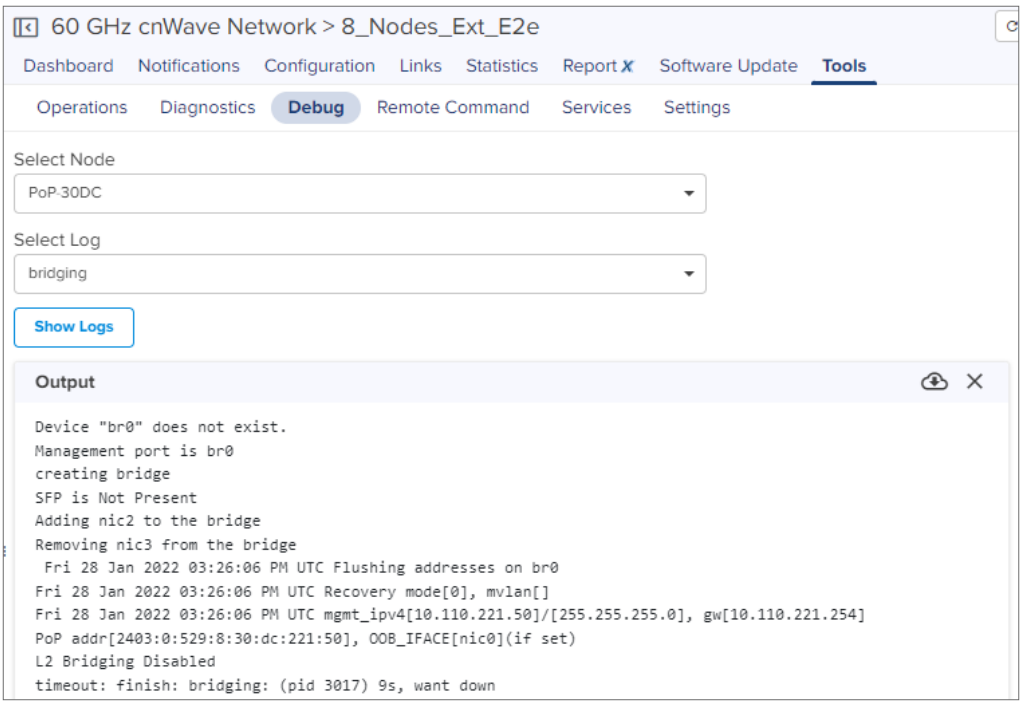
- bridging
- e2e_minion
- openr
- pop_config (available for PoP device)

- exabgp (available for PoP device)
- cnAgent (available for Onboard PoP device)
- e2e_controller (available for Onboard PoP device)

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select a node name from the **Select Node** drop-down.
3. Select the required log name from the **Select Log** drop-down.
4. Click **Show Logs.**

   The output for the selected criteria appears as shown:



   - Click download ( ) icon to download the generated output.
   - Click clear (×) icon to clear the output.

Remote Command

In **Remote Command** tab, user can view or download command logs by executing the following command:

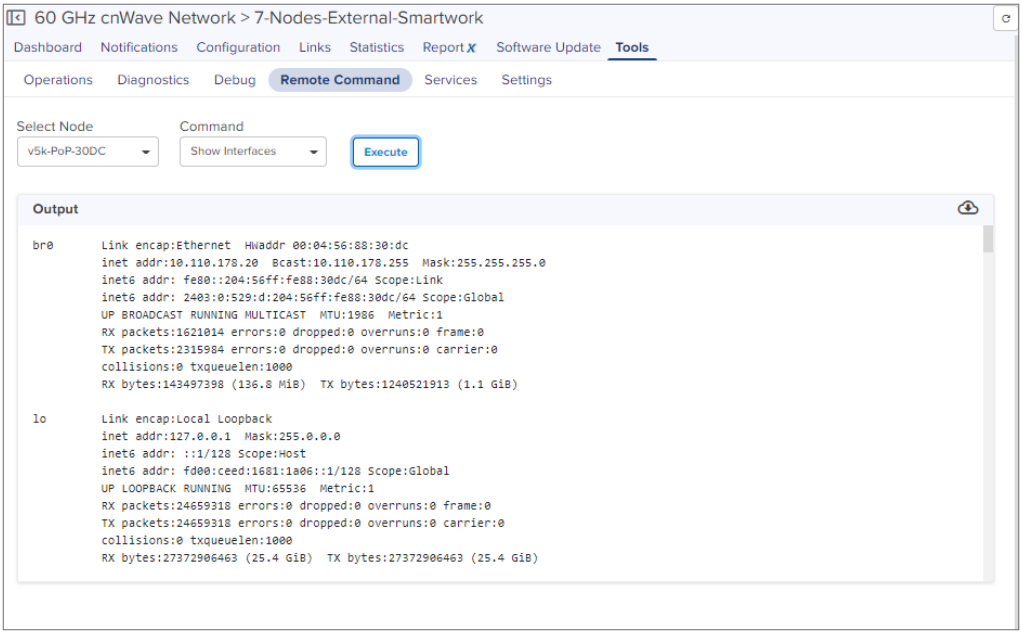
- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 and V3000)
- Show IPv4 Neighbors
- Show IPv6 Neighbors
- Show Wired Interface State Changes

- show DHCP client lease
- Ping

To execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select a node name from the **Select Node** drop-down.
3. Select the required command from the **Command** drop-down.
4. Click **Execute.**

   The output for the selected criteria appears as shown:



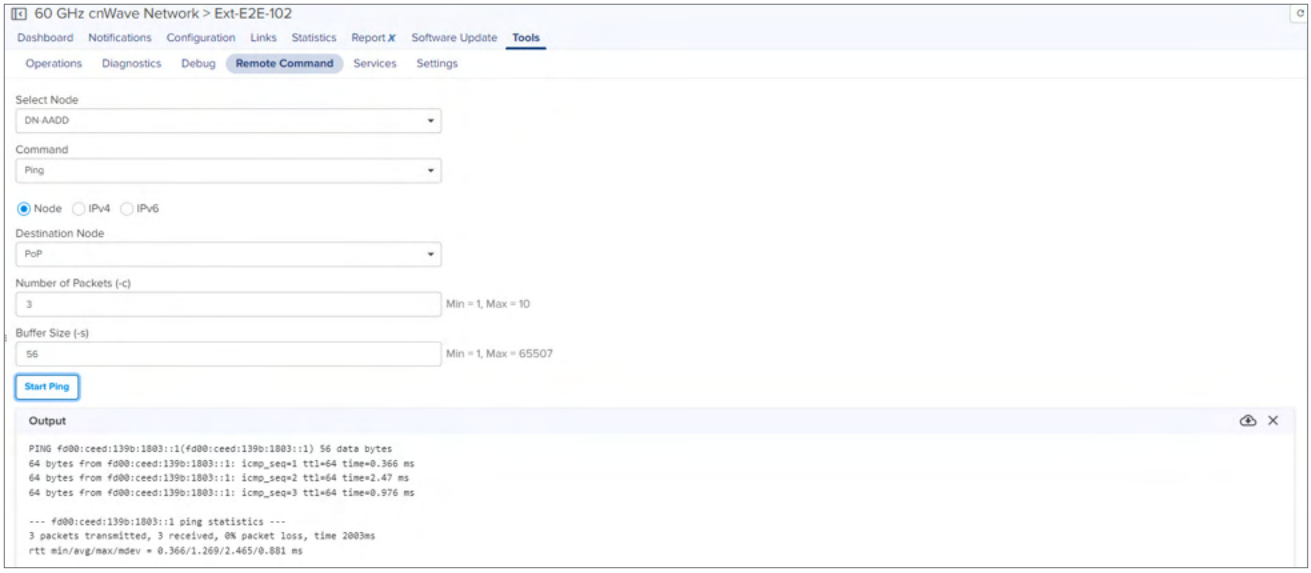
5. Click the download ( ) icon to download the generated output.
6. Click the clear (✕) icon to clear the generated output.

To execute Ping command, perform the following steps:

1. Select the **Ping** command from drop-down.
2. Select **Node** or type of **IP address** (IPv4 or IPv6).
3. Select the following options:
   - Destination Node
   - Number of packets minimum 1 to maximum 10 (-c)
   - Buffer Size minimum 1 to maximum 65507 (-s)
4. Click **Start Ping**.

Output is displayed, as shown in Figure 349.

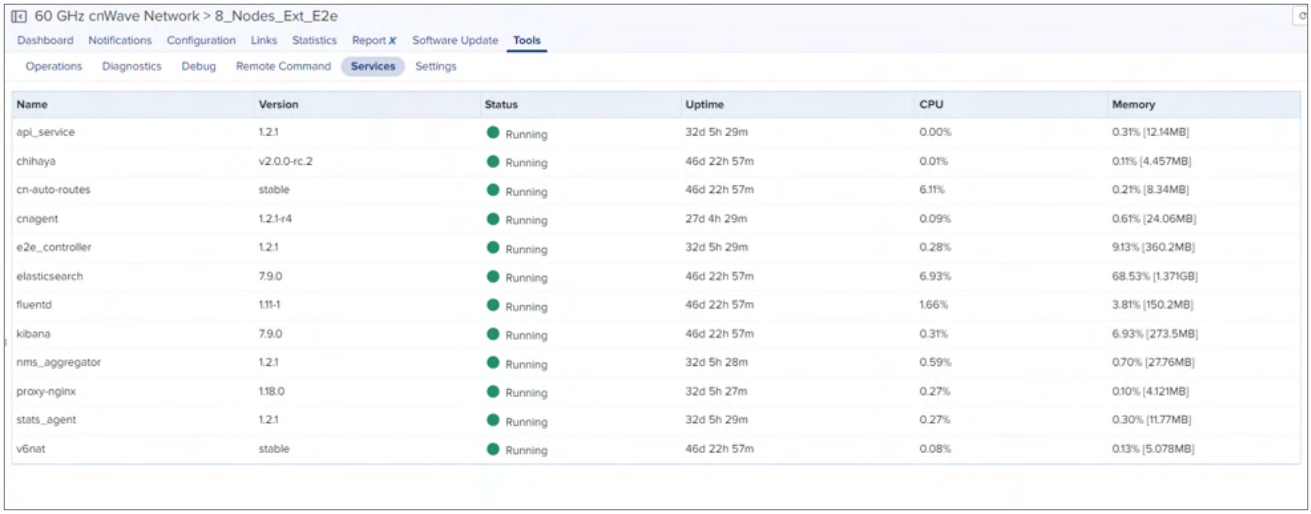
Figure 349 *Remote Command: Ping*



Services

In **Services** page user can view the services running in E2E Controller.

Figure 350 *Services*



Settings



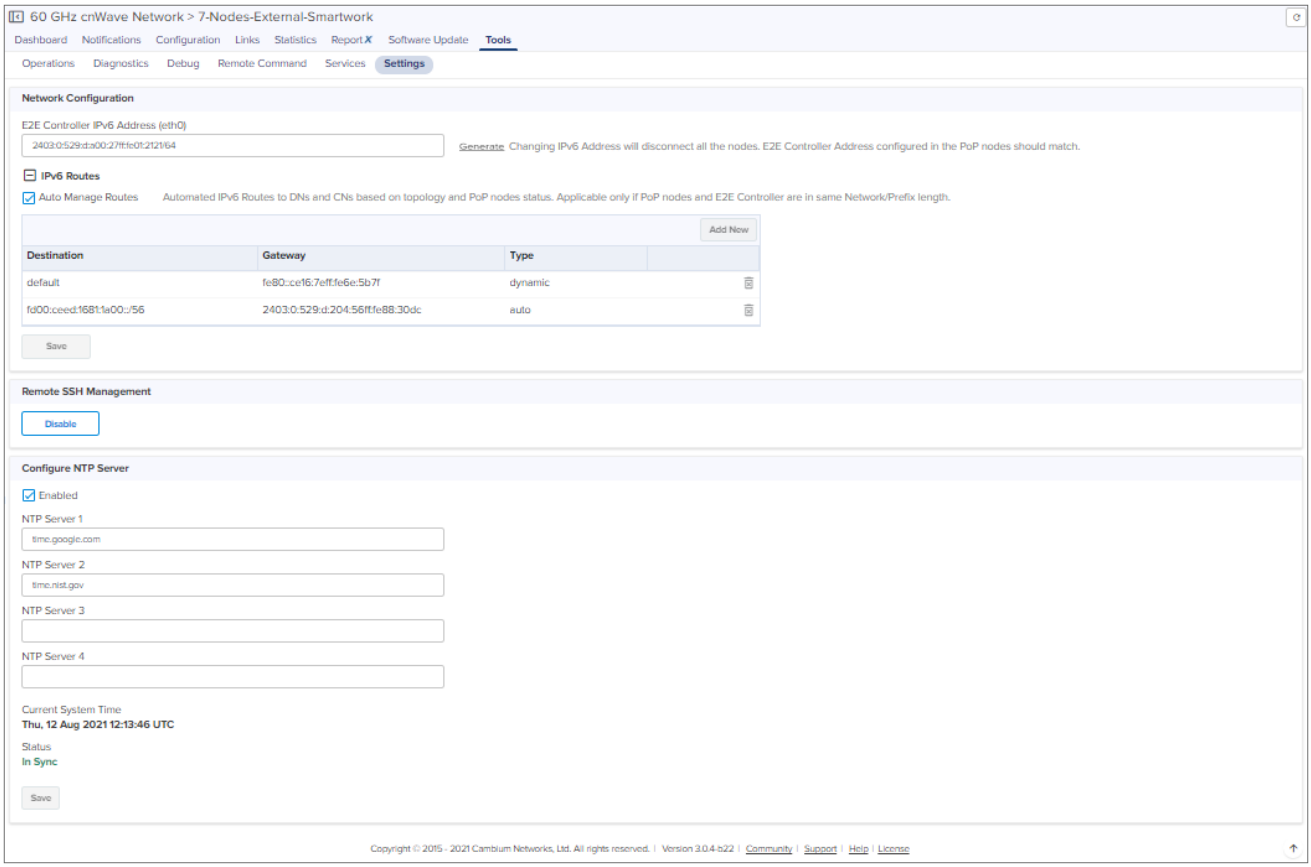
Note

E2E Settings are not applicable for Onboard E2E Controller deployment.

External E2E Controller deployment

External E2E Network displays the **Settings** page as follows:

Remote SSH Management allows the user to enable and disable **Remote SSH Management**.



In **Network Configuration** user can configure the **E2E Controller IPv6 Address** and **IPv6 Routes**.

To change **E2E Controller IPv6 Address**, perform the following:

1. Navigate to **Tools** > **Settings** > **Network Configuration** tab.
2. Click **Generate** to automatically generate IPv6 address or manually change the IPv6 Address of E2E Controller.
3. Click **Save**.

To configure **IPv6 Routes**, perform the following:

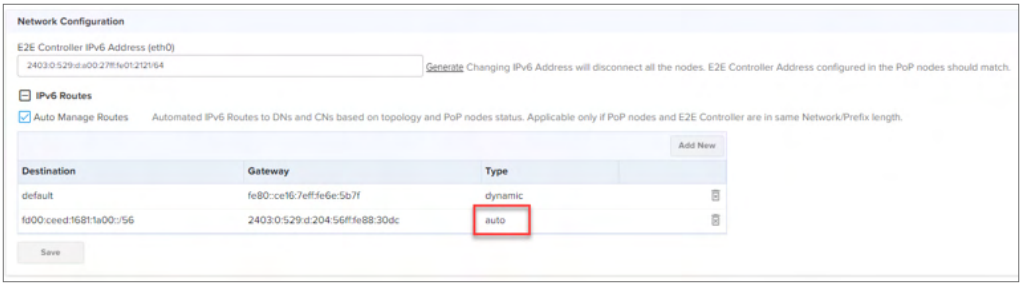
You can also enable the **Auto Manage Routes**. This automates IPv6 Routes to DNs and CNs based on the topology and PoP nodes status. It is applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

If IPv6 routes is enabled as **Auto Manage Routes**, **Type** field displays as **Auto**.

To Enable Auto Managed Routes:

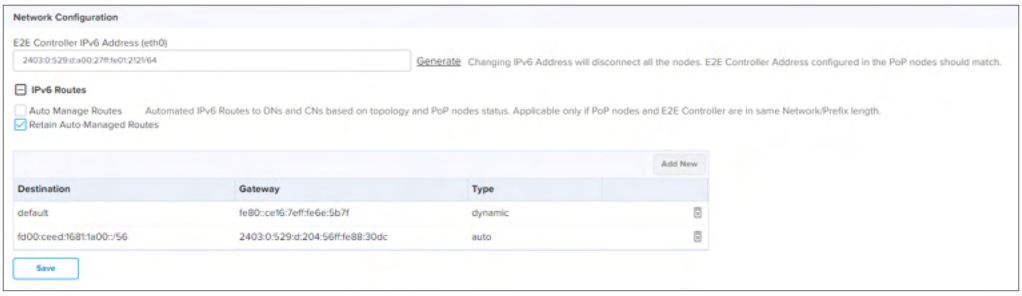
1. Navigate to **Tools** > **Settings** > **Network Configuration** tab.
2. Enable **Auto Manage Routes**.

3. Click **Save**.

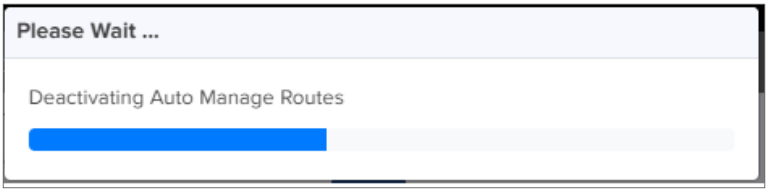


To retain auto-managed routes, even after auto-managed routes is disabled, complete the following steps:

1. Navigate to **Tools > Settings > Network Configuration** tab.

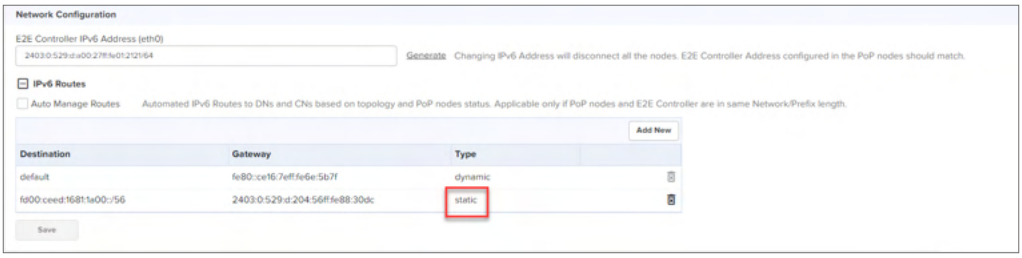


2. Enable **Retain Auto-Managed Routes.**
3. Click **Save.**



4. Please wait pops-up.

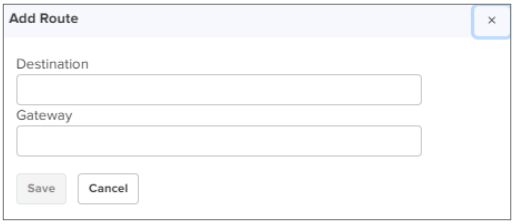
   Once the Auto Manage Routes is disabled, IPv6 routes can be managed through static routes and in type it displays as **Static**.



5. Click **Save**.

To add new static **IPv6 Routes**:

1. Click **Add New**.

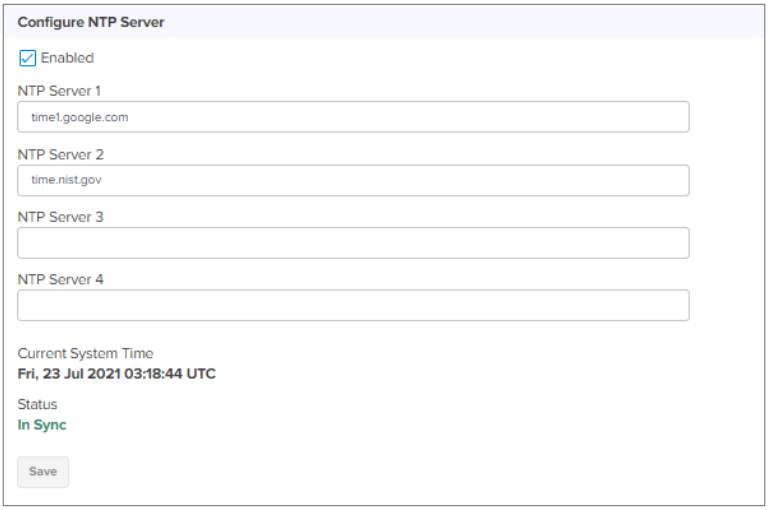


2. Enter **Destination** and **Gateway**.
3. Click **Save.**

The user can configure the **NTP Settings** to configure the time configuration of the server with hostname or IP address.

To configure the NTP server:

1. Navigate to **Tools** > **Settings** > **NTP Settings** tab.
2. Enable the **NTP Settings**.
3. Enter **Host Name** or **IP Address**. It displays **Current System Time** and **Status** of the server.

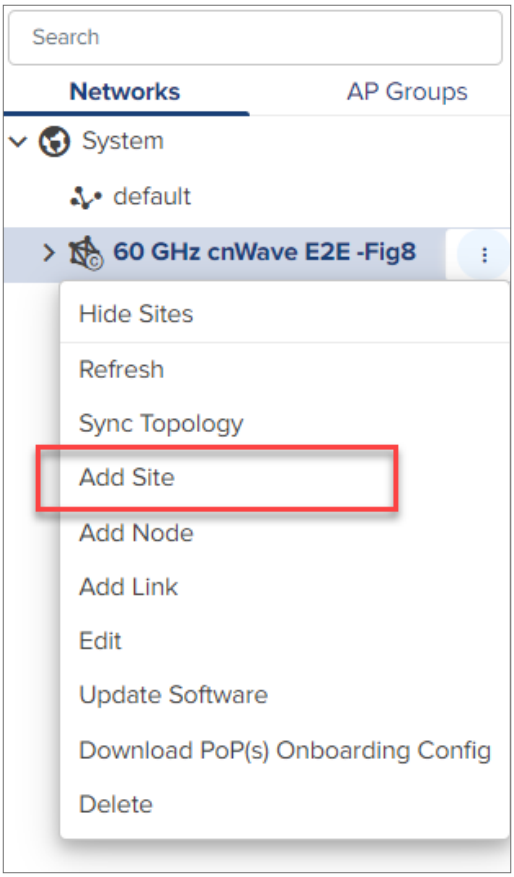


Site Configuration

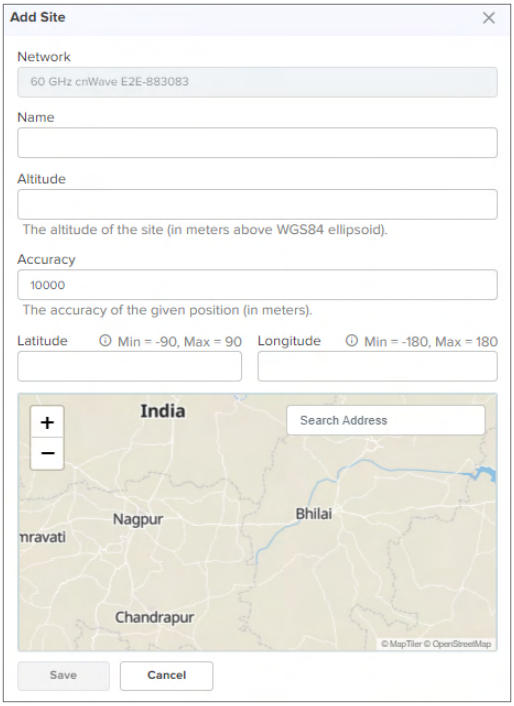
Sites are located within the networks and wireless access points attached to it.

To Add a Site

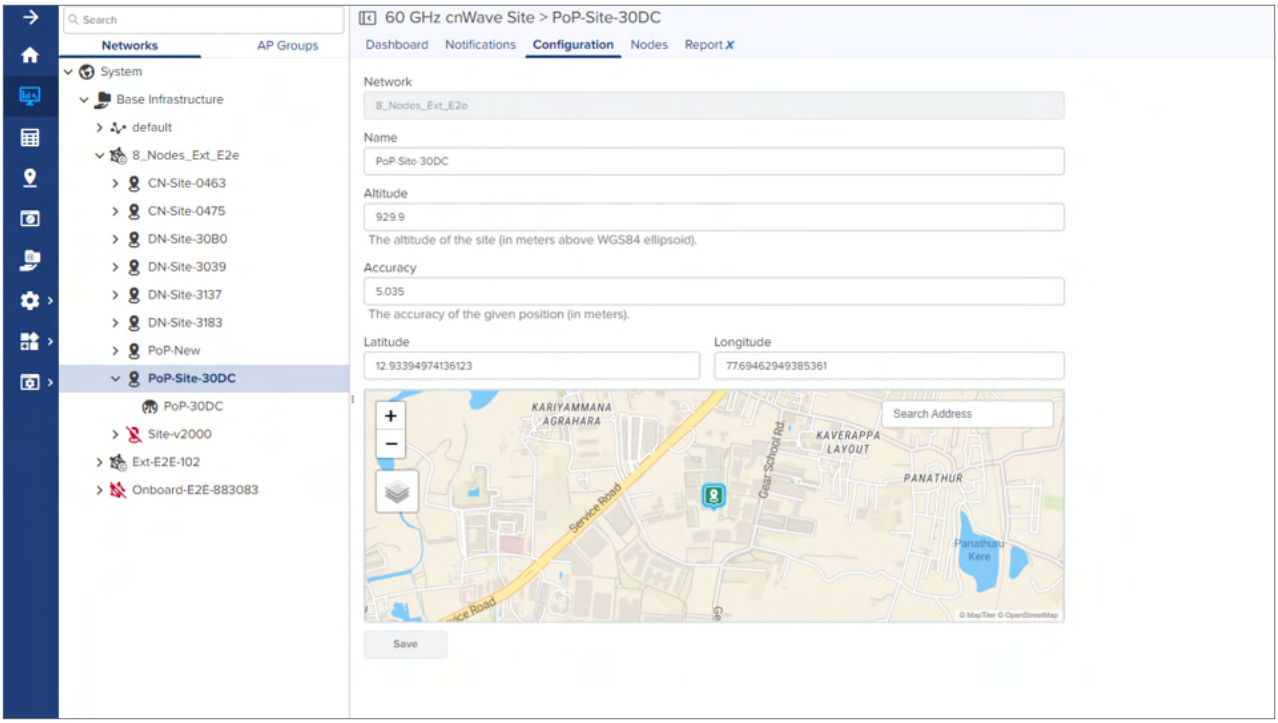
1. Navigate to **Network** and click ⋮ icon.
2. Select **Add Site** from the drop-down.



3. Enter the **Name**, **Altitude**, and **Accuracy.**
4. Once the address is entered in the Map, Latitude and Longitude gets fetched automatically. You can also enter the details Manually.

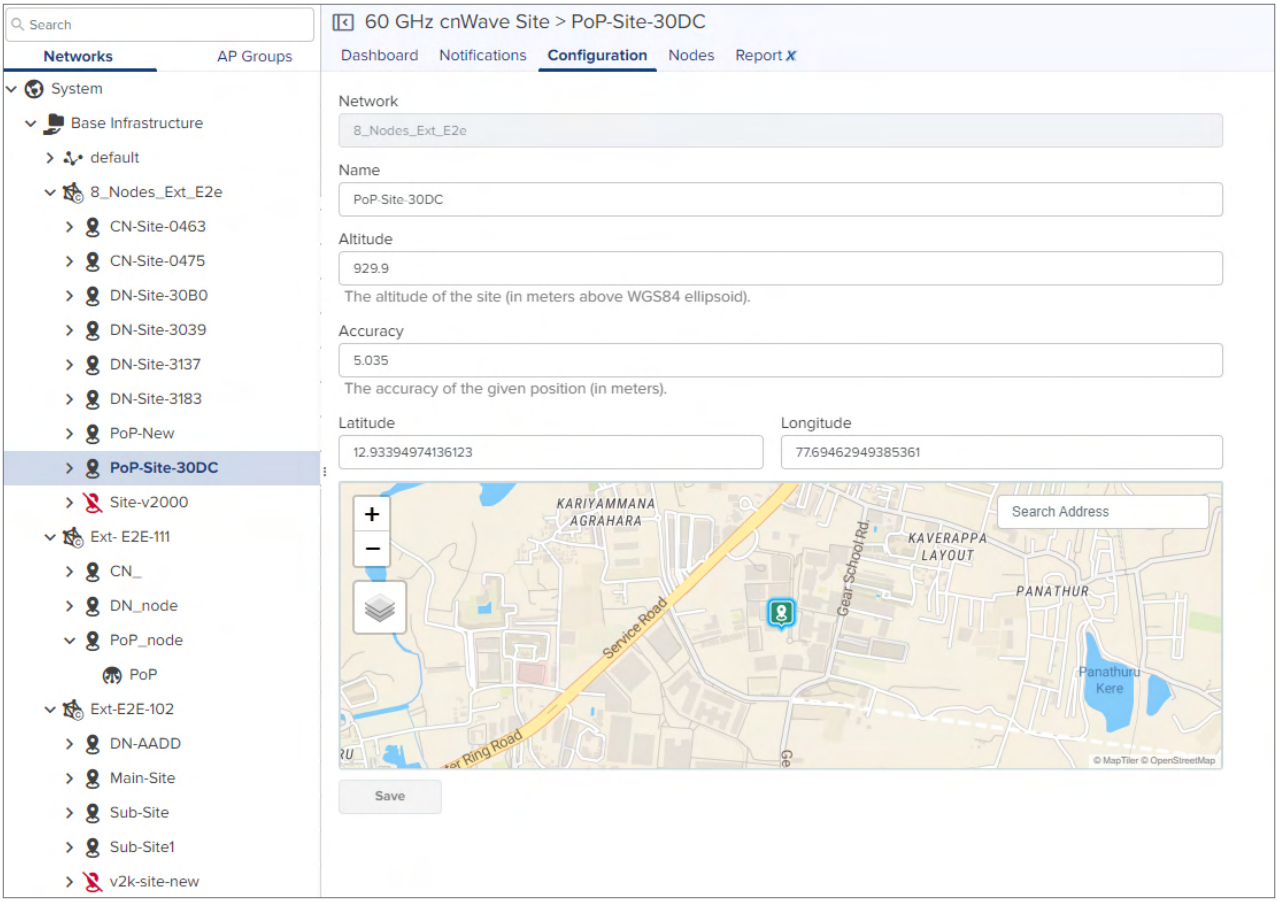


5. Click **Save**. When the Site is configured it gets added under the E2E Network.



To edit the **Site** perform the following:

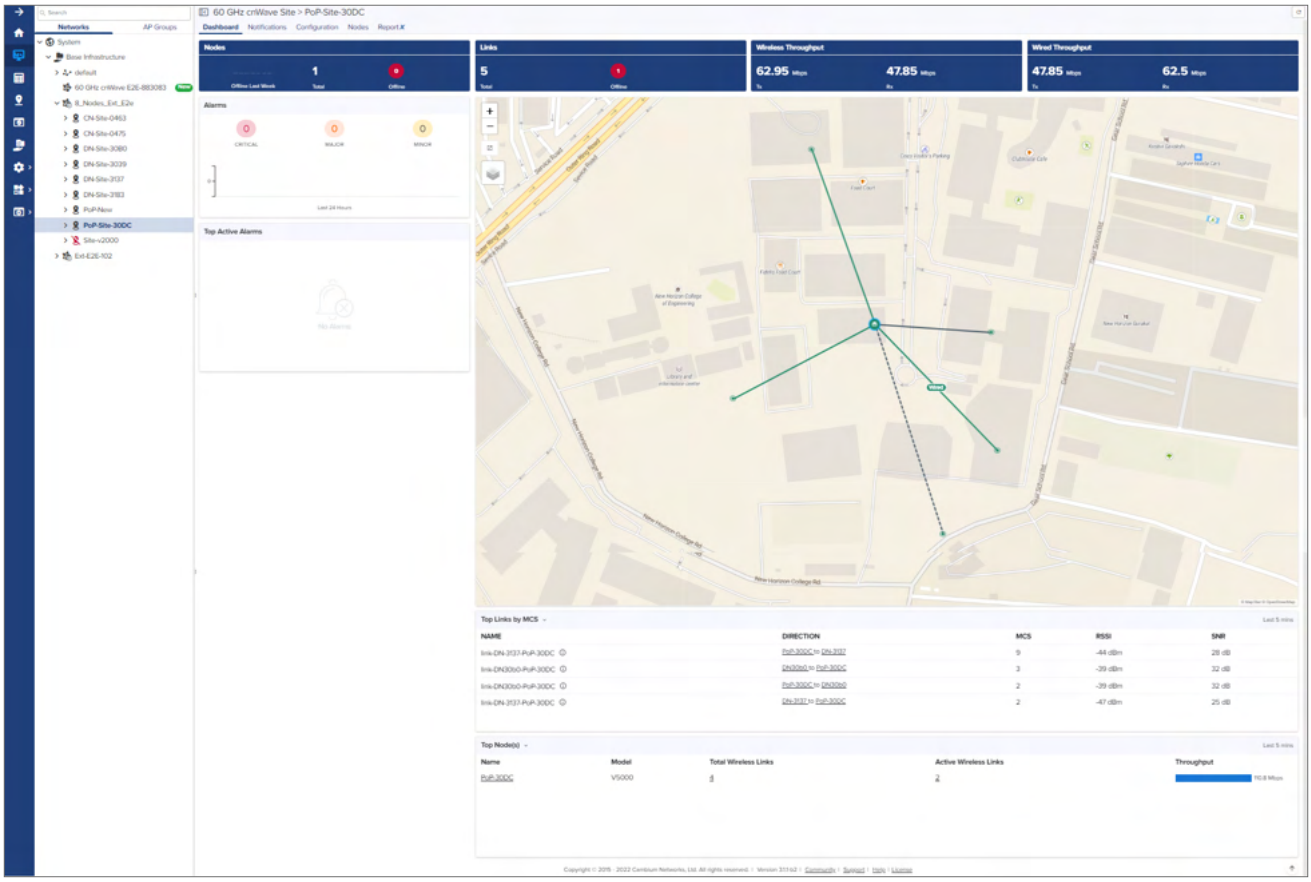
1. Navigate to **Network** > **Site** > **Configuration**.
2. Edit the details and click **Save.**



Site Dashboard

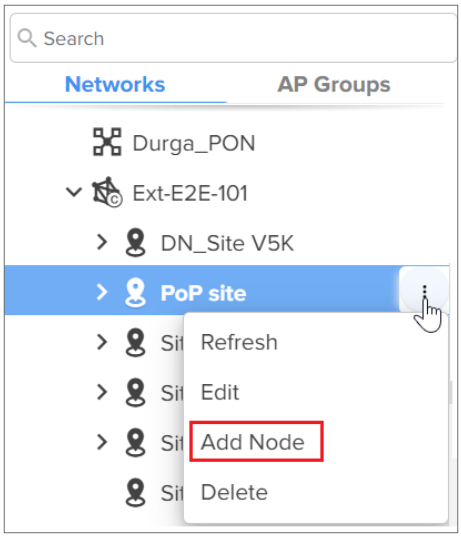
Dashboard pages are customized for each device type and aggregation level. The Site dashboard section displays the **Nodes, Links, Wireless Throughput, Wired Throughput, Alarms, Top Active Alarms, Top Links by MCS, Top Links by RSSI, Top Links by SNR, Top Node(s), Top PoP(s), Top DN(s), and Top CN(s).**

Figure 351 *Site Dashboard*



Node Configuration

Node can be configured through the **Site Menu** option by clicking the ⋮ icon in **Network** or **Site** tree menu or through **Network** > **Site** > **Nodes** and click **Add Node**.

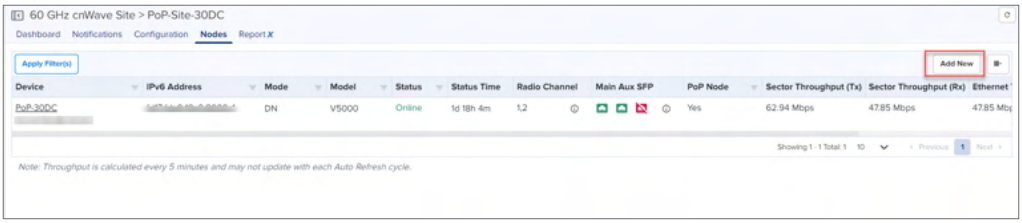


Note

From 3.1.1 release V2000 device (beta version) is supported.

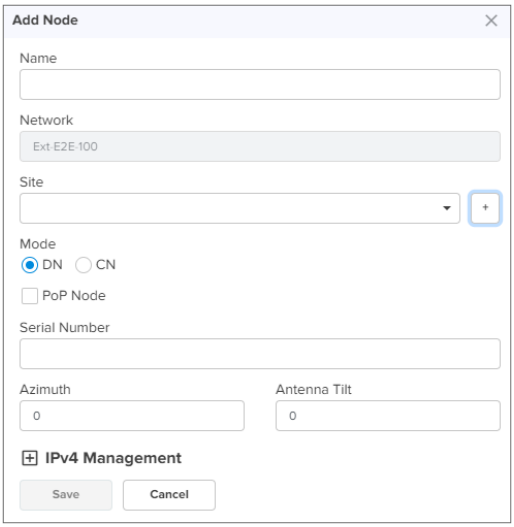
To Add a Node:

1. Navigate to the **Network** > **Site** > **Nodes.**



Add Node window pops-up.

2. Click **Add new.**



3. Click to add site.

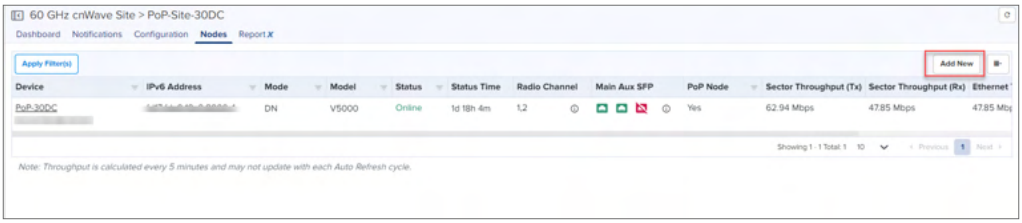
Adding the Node allows the user to create the different Nodes as shown below:

- PoP Node
- DN
- CN

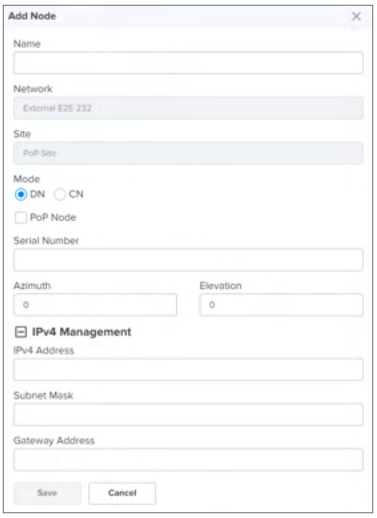
PoP Node configuration

To add a PoP Node:

1. Navigate to the **Network** > **Site** > **Nodes.**
2. Click **Add New.**



3. **Add Node** window pops-up.



4. Enter the **PoP Name**, select the Mode **DN.**
5. Enable **PoP Node**.

> **Note**
>
> Once the PoP Node is enabled user needs to select the **Routing** and **Interface** details**.**

6. Enter the **Serial Number** .
7. Enter the **Azimuth** and **Elevation**.
8. In the **PoP Configuration** select **BGP** or **Static Routing**.
9. In **Interface** select **Aux** or **Main** or **SFP** or **Disabled**.



10. Enter the **IPv6** and **Gateway Addresses.**

Note

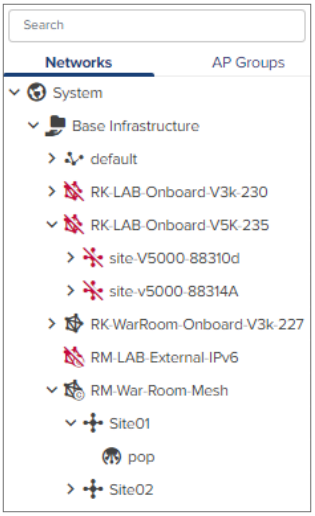
Generate IPv6 provides **Seed Prefix** in CIDR format from which subnet prefixes are allocated to all DNs and CNs (e.g. fdce:b00c:cafe:ba00::/56)

11. In IPv4 Management, enter the **IPv4 Address, Subnet Mask** and **Gateway Address**.
12. Click **Save.**

Note

Once the PoP Node is configured, **PoP(s) Onboarding Config.json** file gets downloaded automatically, which can be used to import and configure in the PoP Node UI.

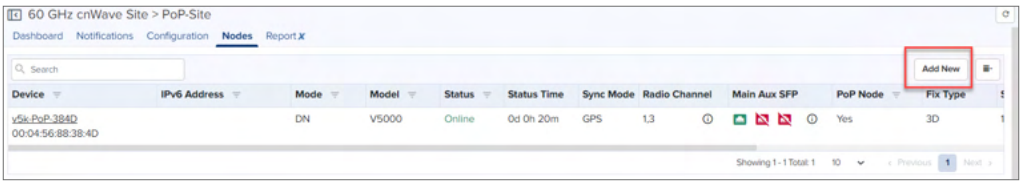
Once the **PoP** node is configured it gets listed under the **Site.**



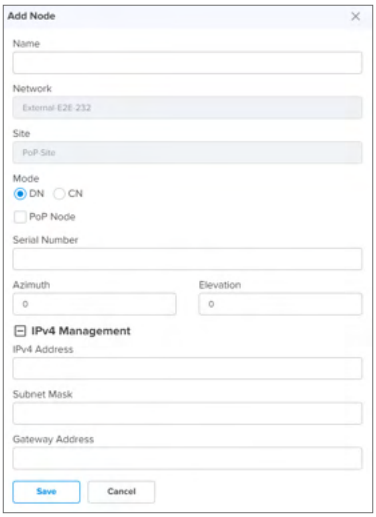
DN/CN Node configuration

To add DN/CN node:

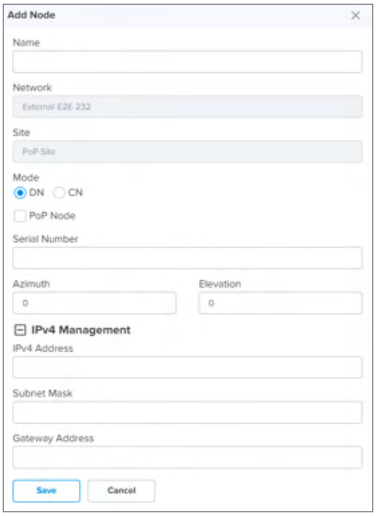
1. Navigate to the **Network** > **Site** > **Nodes.**
2. Click **Add New.**



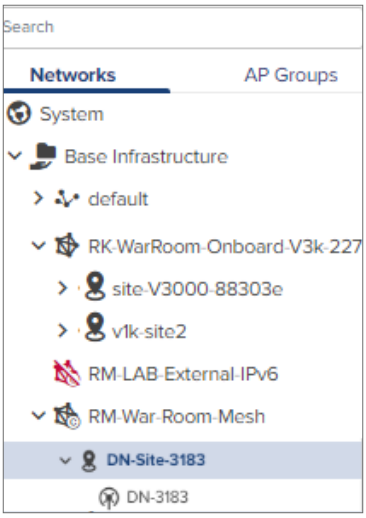
3. **Add Node** window pops-up.



4. Enter the **Node Name**, select the Mode **DN** or **CN.**
5. Enter the **Serial Number**.
6. Enter the **Azimuth** and **Elevation**.



7. In IPv4 Management enter the **IPv4 Address, Subnet Mask** and **Gateway Address**.
8. Click **Save.**
9. Once the **DN/CN** node is configured, it gets listed under the Site**.**



Replace Node

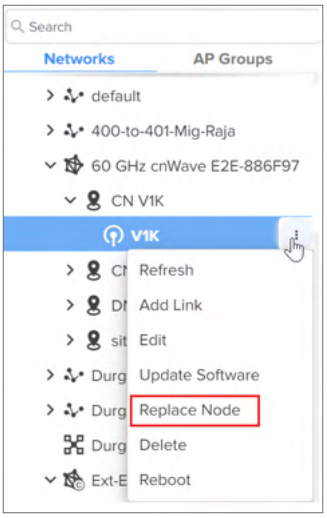
Replace Node allows to replace the existing faulty nodes with new nodes along with the configuration and links of existing faulty nodes.

Note

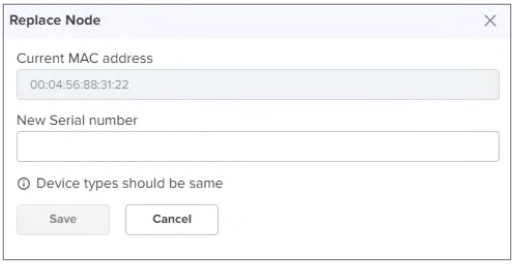
New node should be replaced with same model as existing node.

To replace Node:

1. Navigate to **Node** tree menu and select the node.



2. Click icon and Select **Replace Node** from the drop-down.
3. **Replace Node** window pops-up.



4. Enter the **New Serial number.**
5. Click **Save**.

PoP Node

Once the PoP node is configured it displays the monitoring panel of the PoP node.

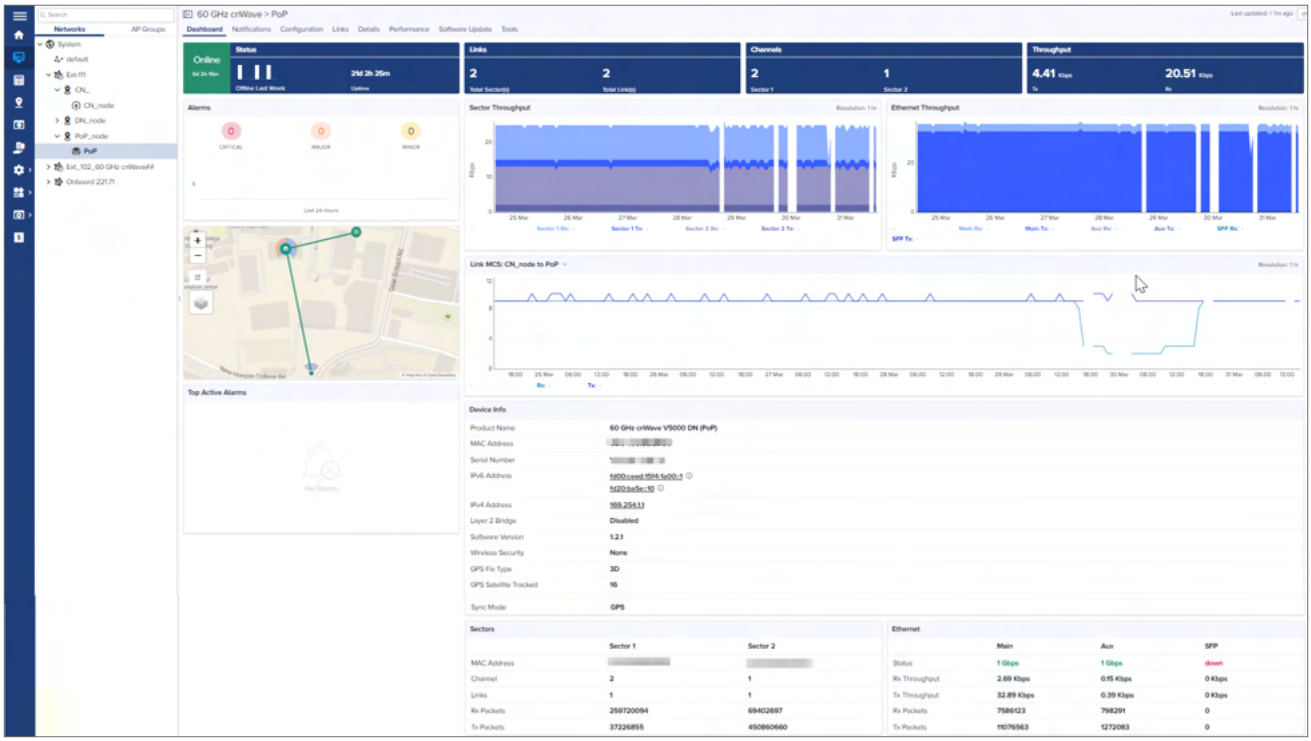
Dashboard

Dashboard pages can be customized for each device type and aggregation level. The PoP node dashboard section displays the **Status, Links, Channels, Throughput, Sector Throughput (Sector 1 and Sector 2), Ethernet Throughput (Main, Aux, SFP**), **Alarms, Top Active Alarms, Link MCS, Device Info, Sectors, and Ethernet**.

Note

- Sector Throughput (sector1) for V3000, V2000 and V1000.
- Sector Throughput (sector1 and sector2) for V5000.
- Ethernet Throughput graph with Main for V1000.
- Ethernet Throughput graph with Main, Aux, SFP for V5000 and V3000.
- Ethernet Throughput graph with Main and Aux for V2000.

Figure 352 *PoP Node Dashboard*

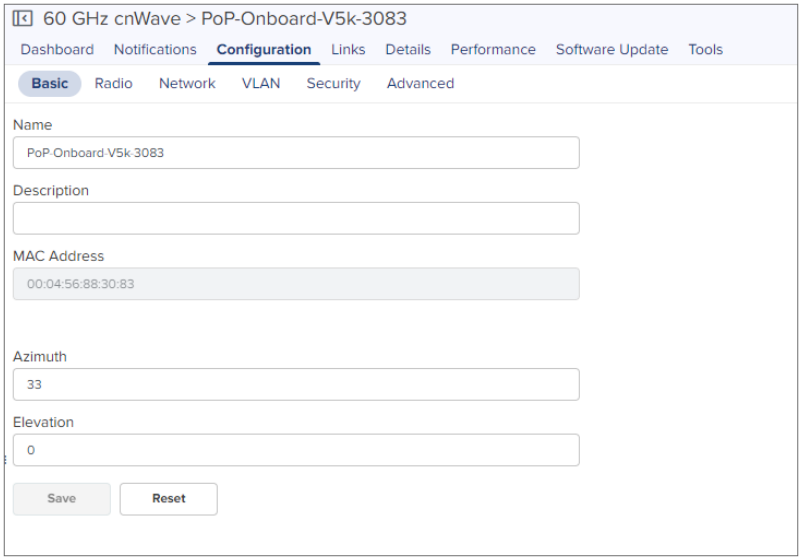


Configuration

Basic

It displays the basic details of PoP node such as **Name, Description, MAC Address, Azimuth,** and **Elevation**. It also allows to edit the name of the node.

Figure 353 *Basic*



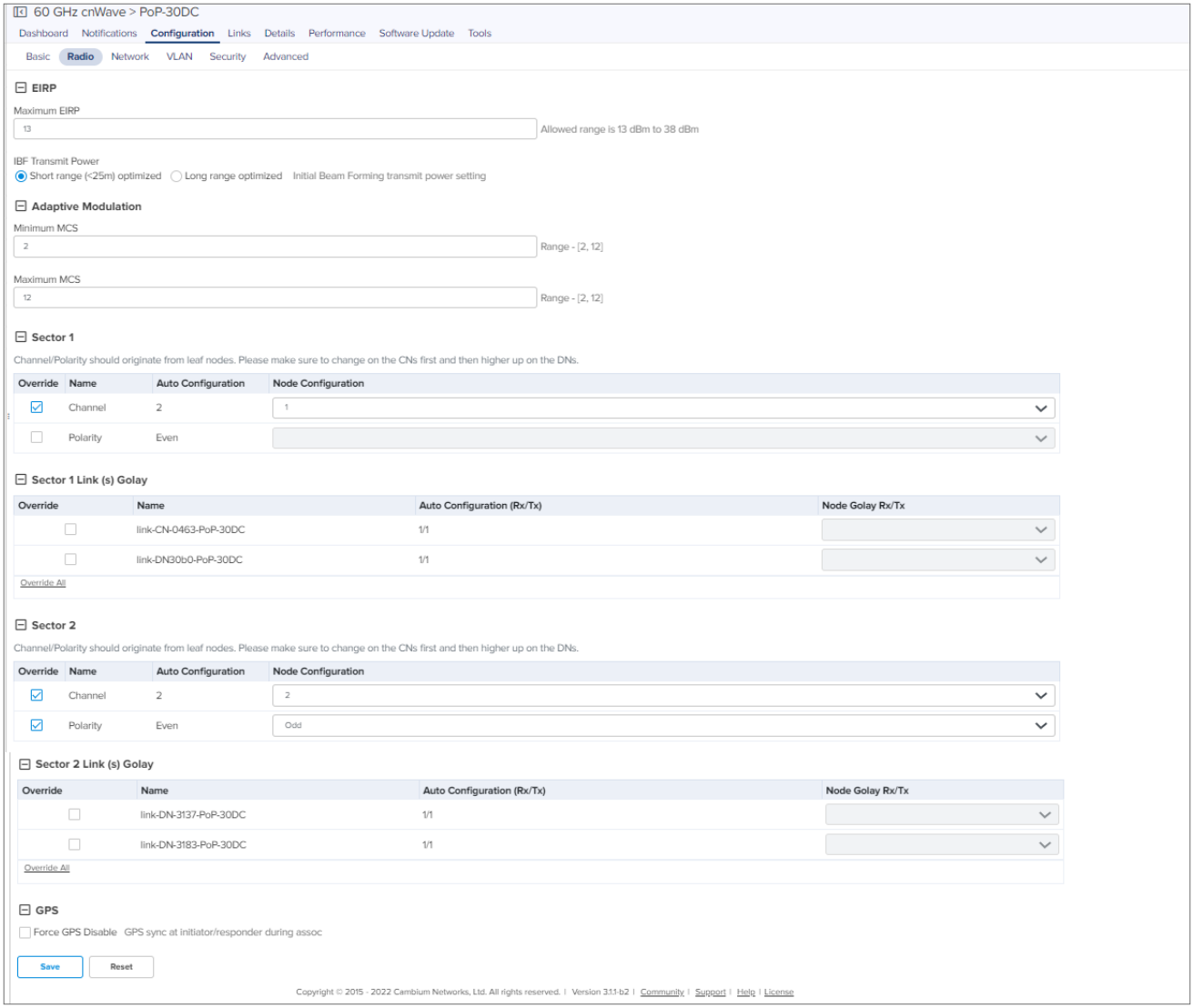
Radio

It allows the user to configure the **EIRP**, **Adaptive Modulation**, **Sectors (channels, Polarity and Link(s) Golay)**, and **GPS**.

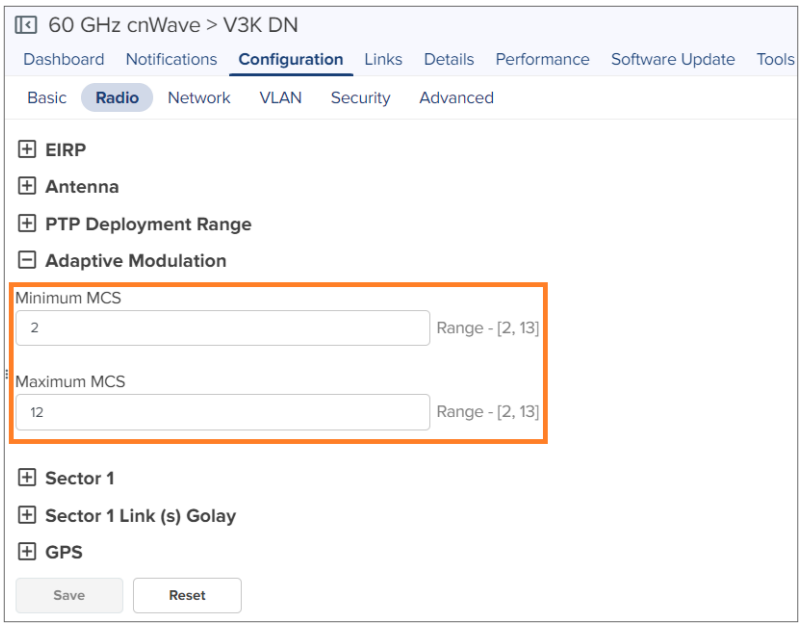
Note

Antenna and PTP deployment Range options is available only for v3000.

Figure 354 *Radio*



For V3000, MCS 13 is supported as seen the following UI:



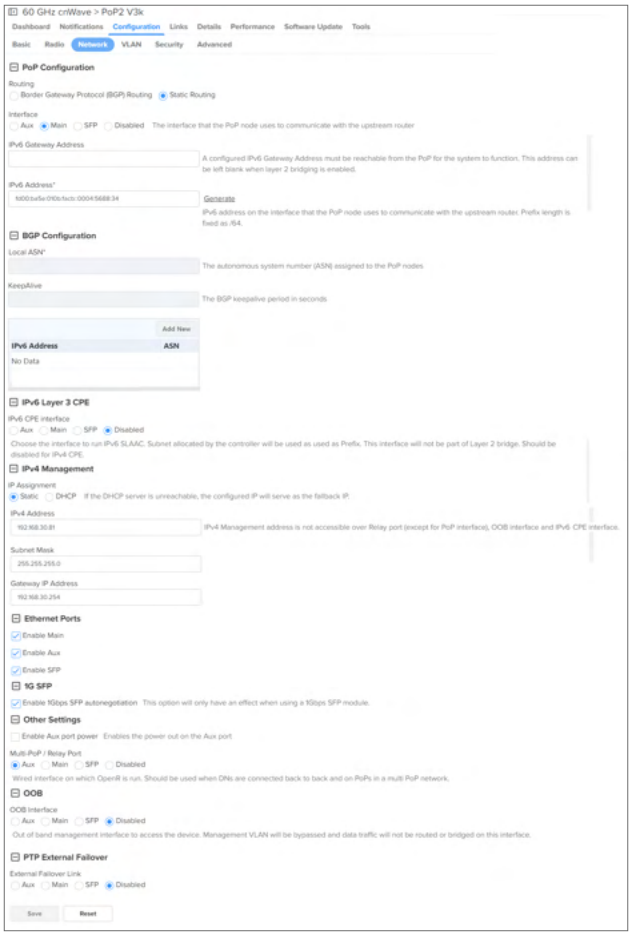
Network

Network tab allows the user for the **PoP configuration**, **E2E Controller Configuration**, **BGP Configuration**, **IPv6 Layer 3 CPE**, **IPv4 Management, OOB**, **Other Settings (Multi-PoP or Relay Port, Enable Aux port power), PTP External Failover**, **Ethernet Ports,** and **1G SFP.**

Note

When Layer 2 Bridge is enabled in E2E Controller, Layer 2 Bridge option will be available in PoP Network Configuration

Figure 355 *Network*

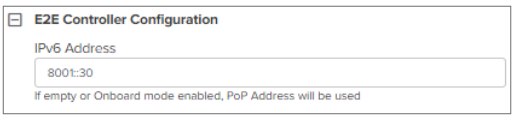


Configure the Network as shown below:

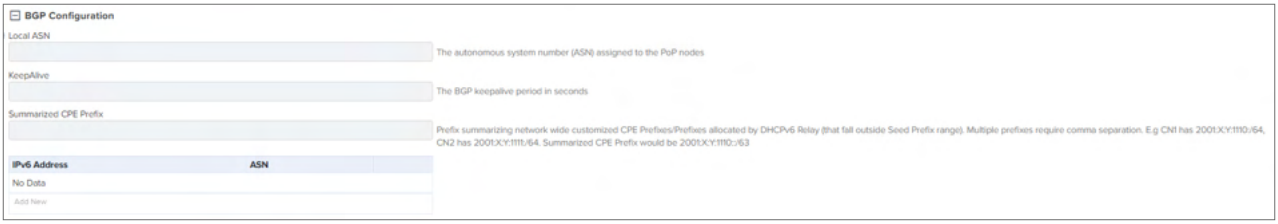
1. Navigate to the **Configuration** > **Network.**
2. In **PoP Configuration:**
    - Select the appropriate option in **Routing** and **Interface**.
    - Enter the **IPv6 Address.**
    - Enter **IPv6 Gateway Address** its optional.



3. In **E2E Controller Configuration**, enter the **IPv6 Address.**

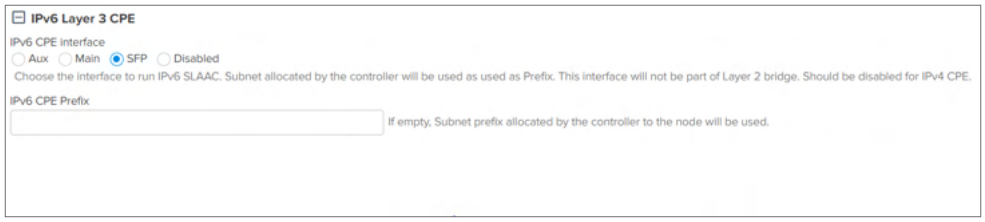


4. In BGP Configuration add IPv6 Address.



5. In **IPv6 Layer 3 CPE**

   - Select **IPv6 CPE interface** as Aux, Main, or SFP.
   - Enter **IPv6 CPE Prefix.**



6. In the **IPv4 Management** section, the following options are supported:

   - **Static**: If you select Static, enter the IPv4 address, Subnet mask, and Gateway IP address manually.
   - **DHCP**: If you select DHCP, there is no need to set the IP address, Subnet mask, and Gateway IP address manually. These properties (IPv4 address, Subnet mask, and Gateway IP address) are automatically obtained from the DHCP server. Note that the DHCP configuration is available only for the PoP nodes. It is not available for CN and DN nodes.



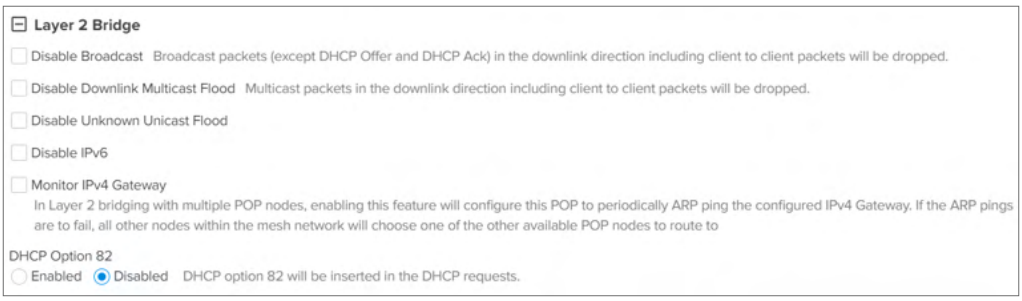
7. In **Ethernet Ports** enable the appropriate option **Main** or **Aux** or **SFP.**
8. In **Layer 2 bridge** enable the appropriate options such as:

- Disable Broadcast Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be dropped.
- Disable Downlink Multicast Flood - Multicast packets in the downlink direction including client to client packets will be dropped
- Disable Unknown Unicast Flood
- Disable IPv6
- Monitor PoP Interface Layer 2 tunnels will failover to next best PoP when the backhaul interface of this PoP is down.

Note

The configuration is applicable only when static routing is used and IPv4 gateway is configured..

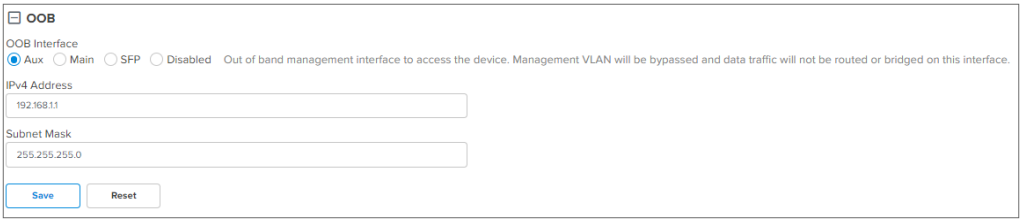
- Insert DHCP Option 82



9. In **Other Settings** enable **Enable Aux port power** and **Multi-PoP / Relay Port**.



10. In **OOB Interface** enable the appropriate option **Main** or **Aux** or **SFP.**
    - Enter **IPv4 Address.**
    - Enter **Subnet Mask**.



11. Click **Save.**

Note

Once the configuration is updated successfully in cnMaestro, the same parameters needs to be entered in the UI of the **PoP Node GUI**.

VLAN

Note

From Software Update Version 1.1 of all nodes, supports configuration of the VLAN Management and Ports.

Virtual Local Area Networks (VLANs) is a broadcast domain in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set and traffic will be tagged when transporting over wireless.

Note

Only PoP node Management VLAN can be configured, if Layer 2 Bridge is not enabled in **E2E Network > Configuration > Basic** page.

Node running version 1.0.1:

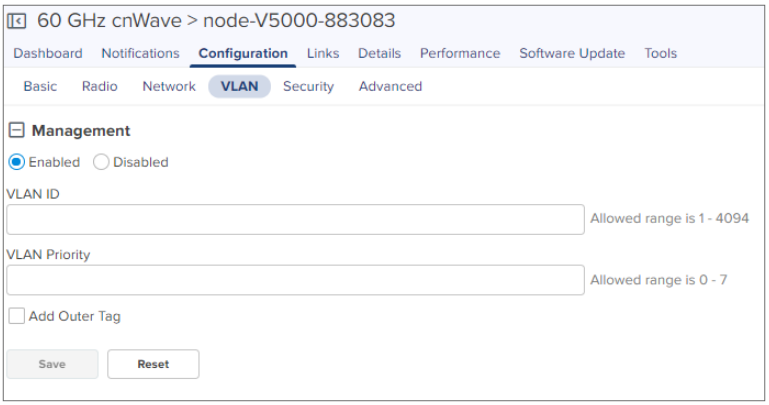
- When Layer2 bridge is disabled, Only PoP node Management VLAN ID can be configured.
- When Layer2 bridge is enabled, all nodes Management VLAN ID can be configured.

Node running version 1.1:

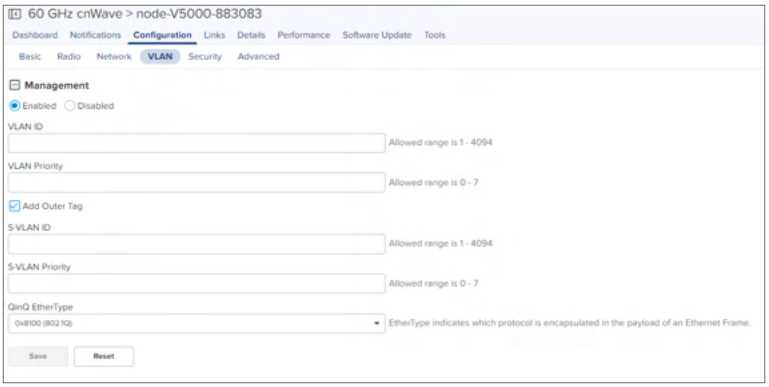
- When Layer2 bridge is disabled, Only PoP node Management VLAN ID, Priority with Outer Tag can be configured.
- When Layer2 bridge is enabled, all node management VLAN and ports can be configured.

To add a Management VLAN:

1. Navigate to **Configuration > VLAN.**
2. Click Enabled.



3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.



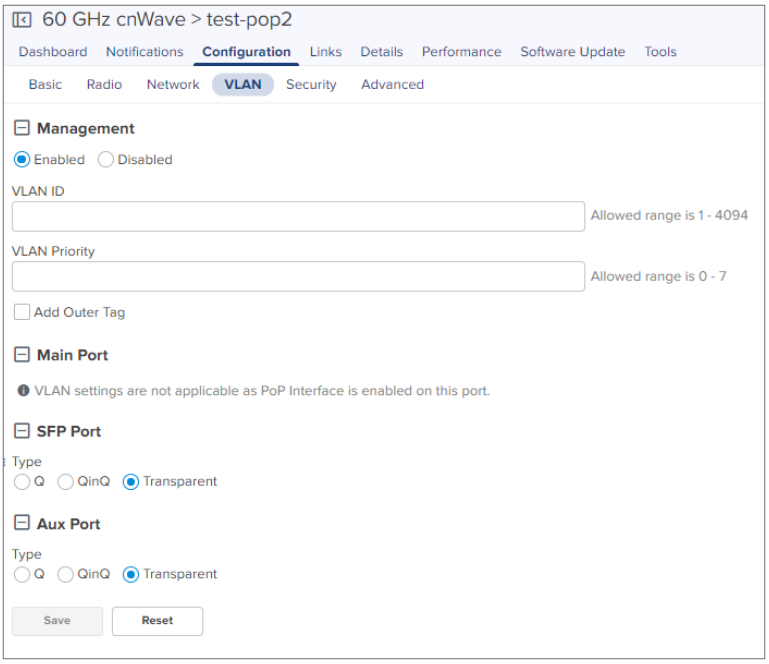
5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**

7. Enter **QinQ EtherType.**
8. Click **Save.**

If Layer 2 Bridge is enabled in **60 GHz cnWave Network > Configuration > Basic** page. User can configure Management VLAN and Ports of PoP node, DN and CN.

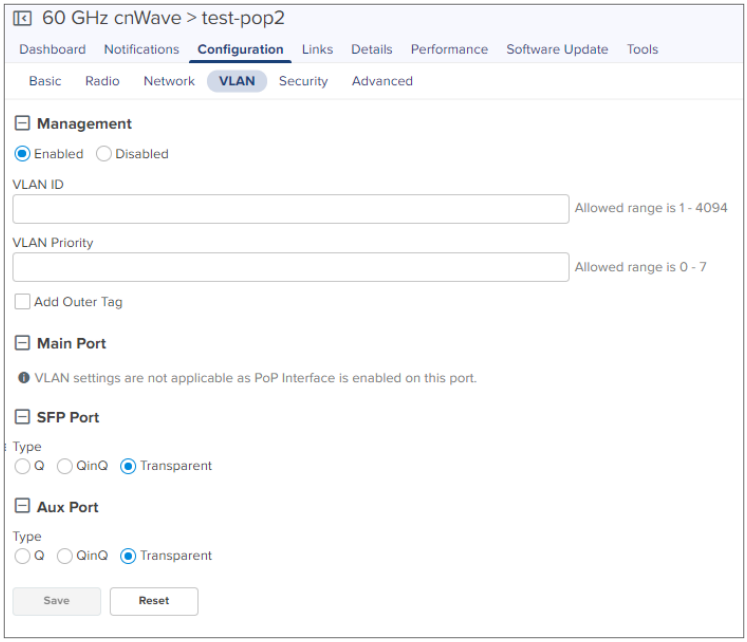
Note

VLAN settings are not applicable if Relay Port, SFP Port, or Aux Port is enabled on Network page.



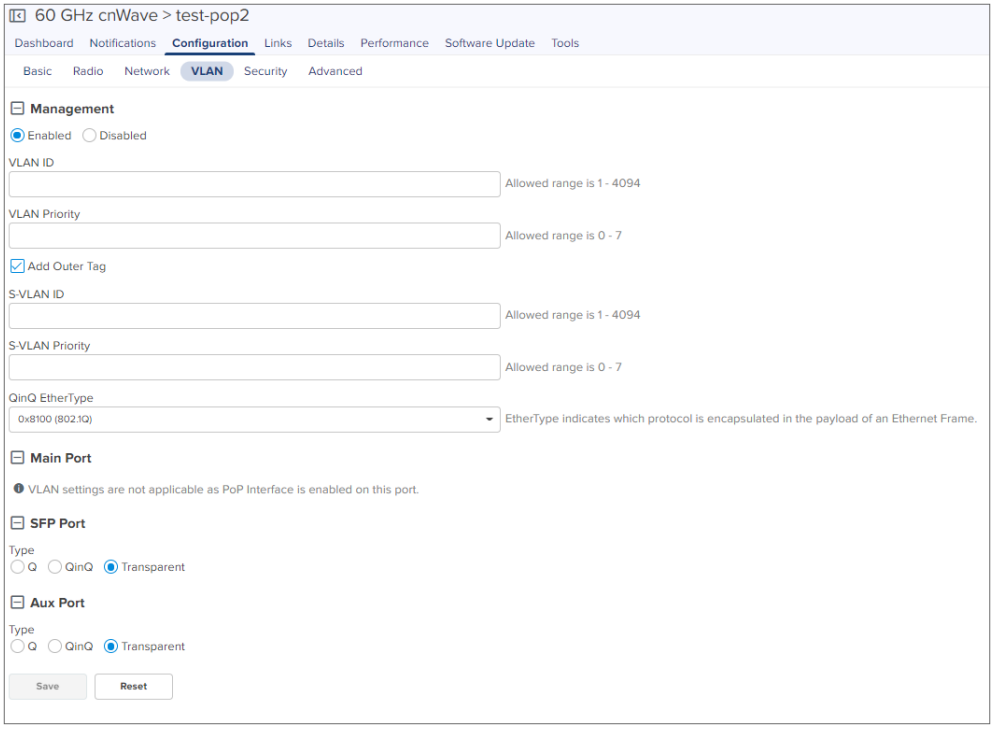
To add a VLAN:

1. 1. Navigate to **Configuration > VLAN.**
2. 2. Click Enabled.



3. 3. Enter the **VLAN ID** and **VLAN Priority**.

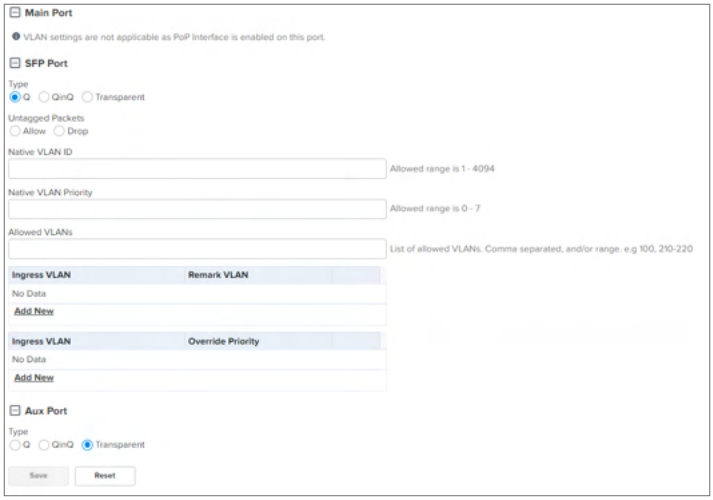
4. 4. Enable **Add Outer Tag**.



5. 5. Enter **S-VLAN ID**.
6. 6. Enter **S-VLAN Priority.**
7. 7. Enter **QinQ EtherType.**

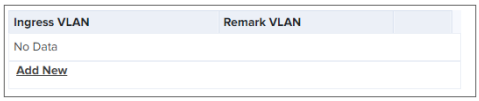
> **Note**
>
> VLAN settings configuration of Main Port, SFP Port, or Aux Port is similar.

8. Select Port **Q** or **QinQ** types.
   a. If user selects **Q type** perform as follows:

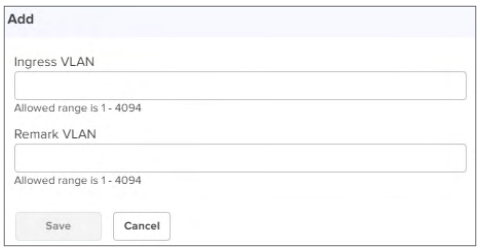


   - Select **Untagged Packets** Allow or Drop.
   - Enter **Native VLAN ID.**

- Enter **Native VLAN Priority**.
- Enter **Allowed VLANs**.
- To add new **VLAN Remarking.**



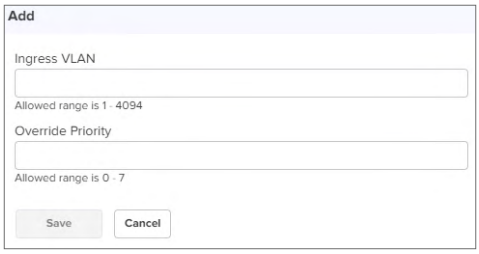
- Click Add New



  - Enter **Ingress VLAN** and **Remark VLAN**.
  - Click **Save**.
- To add new **VLAN Priority Override**.

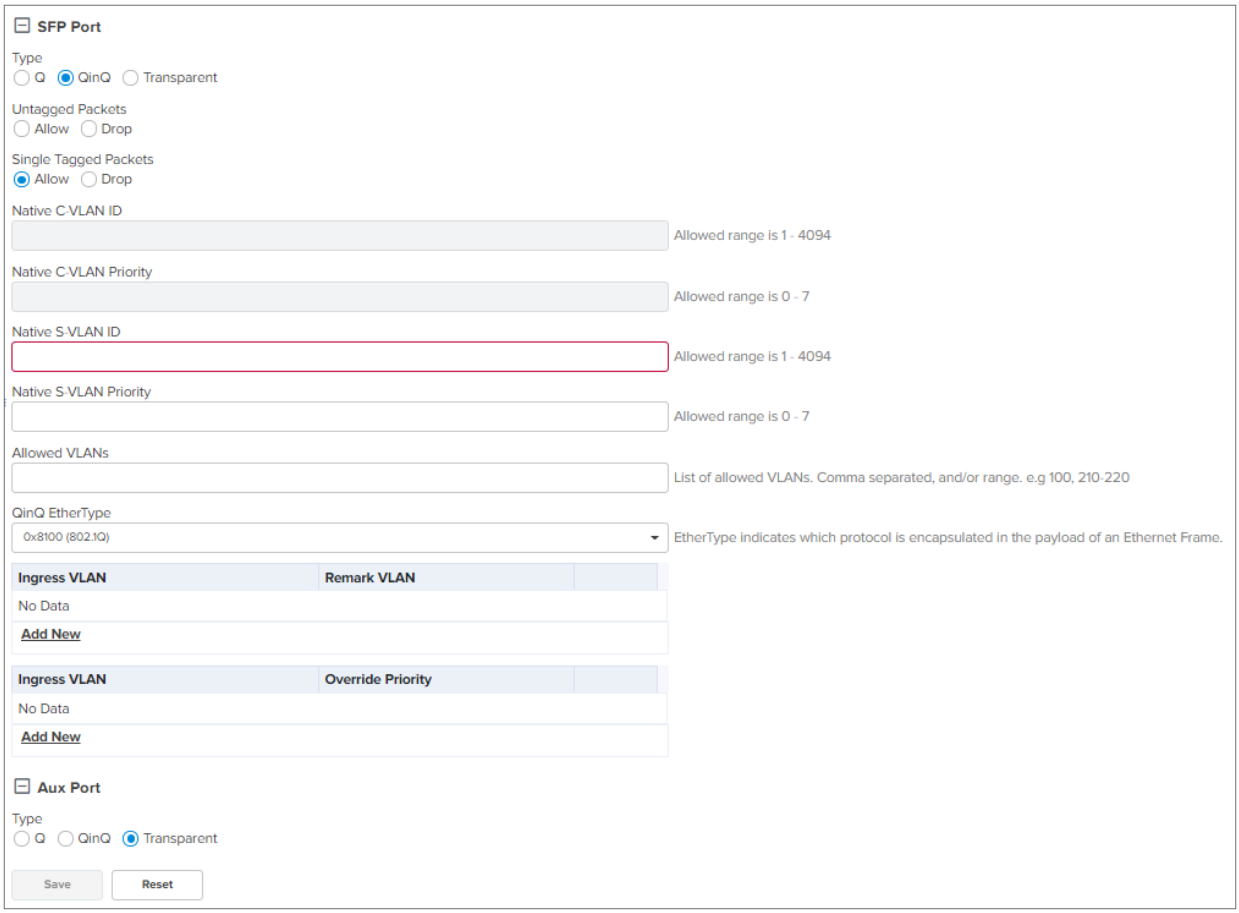


- Click **Add New**.



  - Enter **Ingress VLAN** and **Remark VLAN**.
  - Click **Save**.
- Click **Save**.

b. If user selects **QinQ** type perform as follows:



- In **Untagged Packets** select **Allow** or **Drop.**
- In **Single Tagged Packets** select **Allow** or **Drop.**
- Enter **Native C-VLAN ID.**
- Enter **Native C-VLAN Priority**.
- Enter **Native S-VLAN ID**.
- Enter **Native S-VLAN Priority**.
- Enter **Allowed VLANs**.
- Enter **QinQ EtherType**.
- To add new **VLAN Remarking.**



- Click **Add New**.



- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- To add new **VLAN Priority Override**.



- Click **Add New**.



- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- Click **Save**.

Security

Security tab allows to reset the identity and password of the Radius user.

Figure 356 *Security*



Advanced

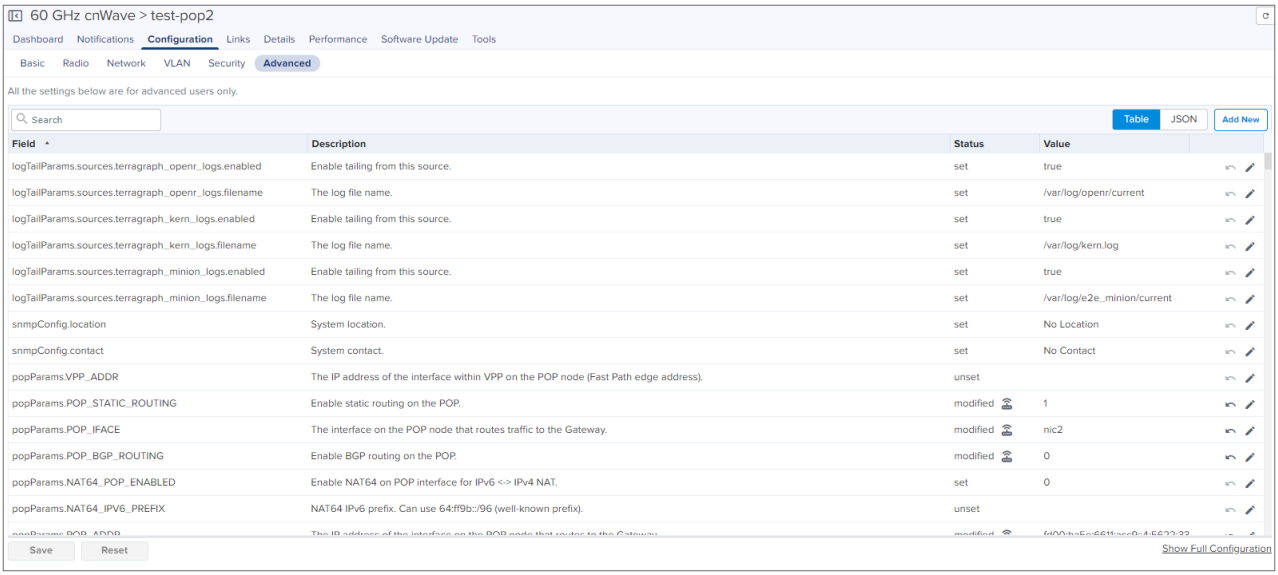
Advanced tab allows the advanced user to edit the settings of the Table and JSON format of the PoP Nodes.

Table

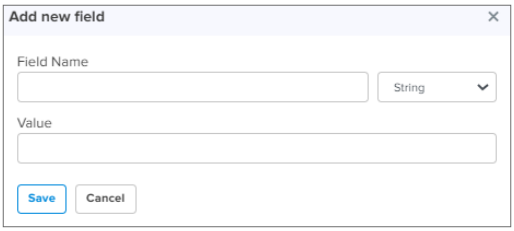
In the **Table** user can view and edit **Field Name** and **Value**. You can sort field name in alphabetical order.

To add a field:

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



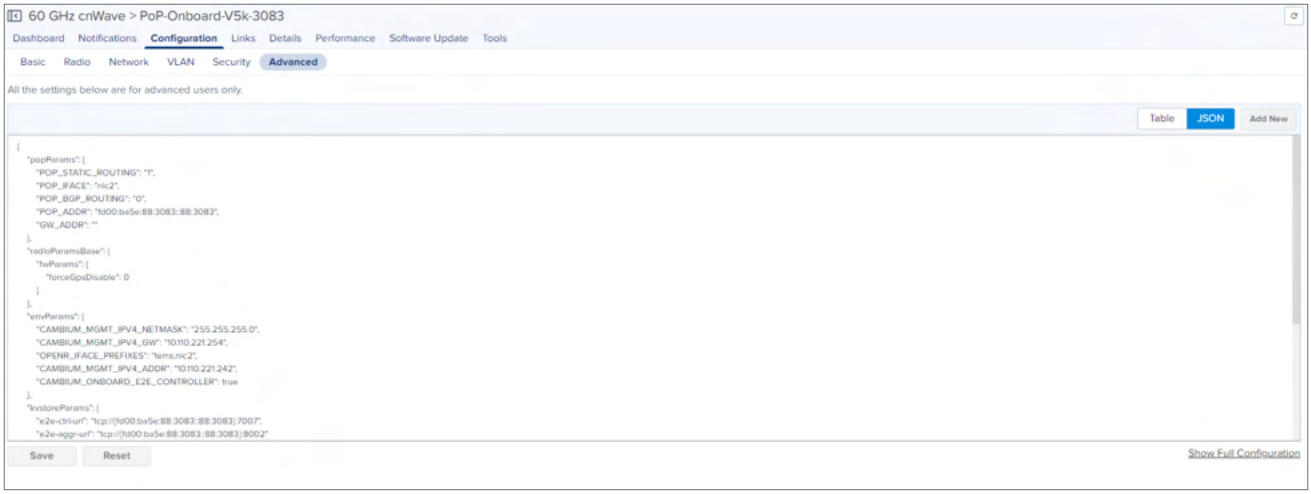
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

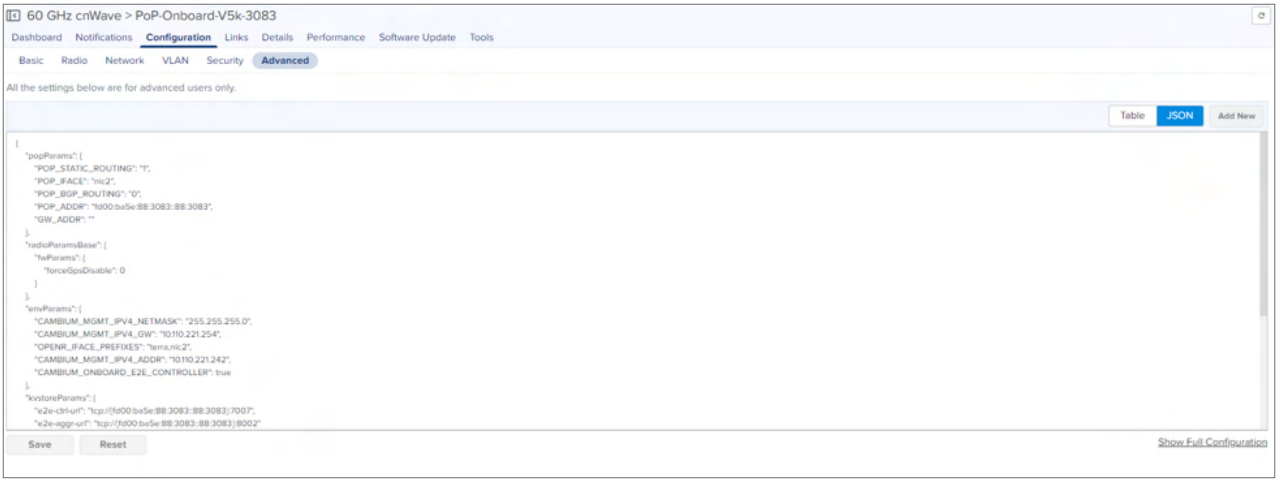
JSON

JSON allows advanced user to download or view the JSON format.



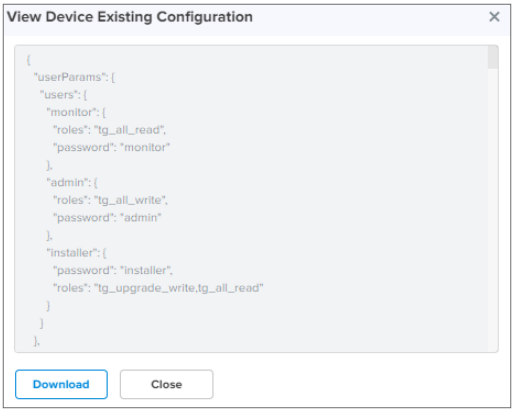
To download the file:

1. Navigate to **Configuration** > **Advanced** > **JSON.**



2. Click **Show Full Configuration.**

   View Device Existing Configuration window pops up.



3. Click **Download**.

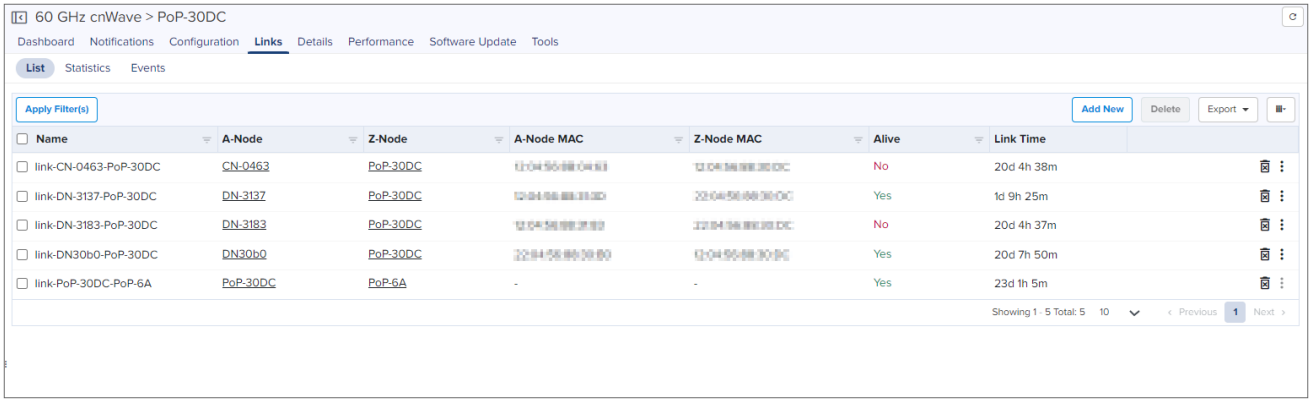
Links

Links provide the details about the links between nodes, statistics and events of the links in the E2E Network.

List

List provide the details about the links of the nodes and also provides the option to create a new link. User can delete the links in bulk by selecting the particular links. It also allows to export or import link details.

Figure 357 *List*



For more details about adding a link and deleting a link in the network, refer the List section.

Note

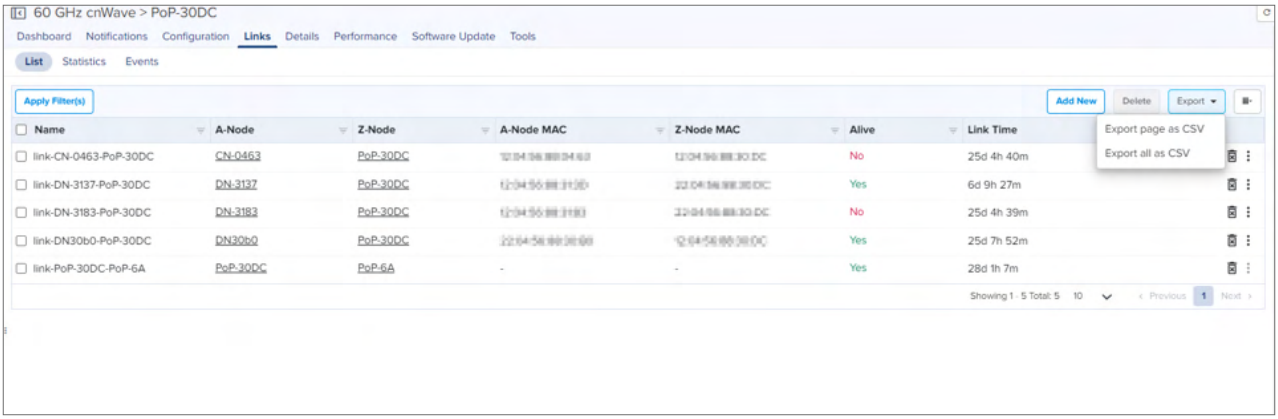
By default A Node is selected as node, when adding new link in the network.

Export List

Export list allow the user to export the PoP links list.

To export the links :

1. Navigate to **Links** > **List** > select **Export.**



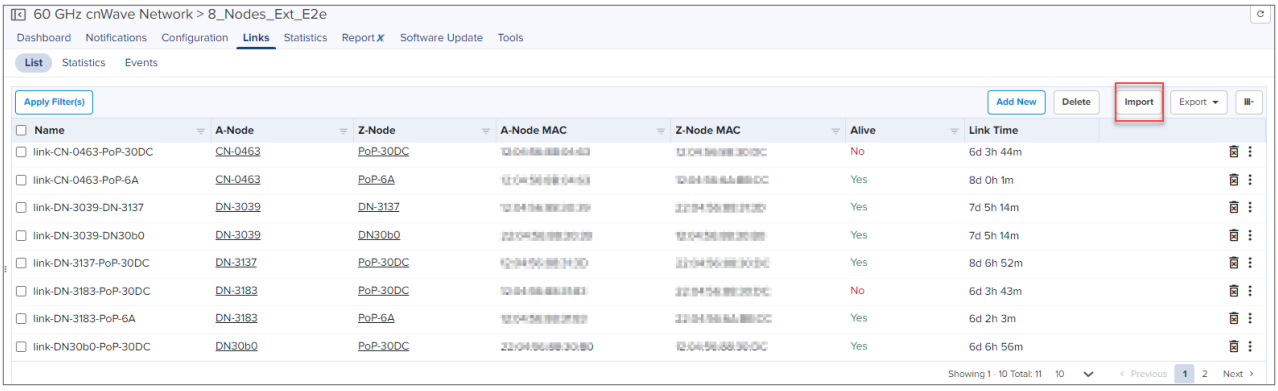
2. It exports .csv file format as shown below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	LINK_NAME	A_NODE_I	A_NODE_I	Z_NODE_I	Z_NODE_I	LINK_TYPE	ALIVE	IGNITION_	DISTANCE	AZIMUTH	BACKUP_C	IGNITION_	TIMESTAMP		
2	Link Name	A node nai	Sector 1/2	Z node nar	Sector 1/2	Wireless o	Yes/No	Ignition At	Distance b	Azimuth (D	Yes/No	Enabled/D	Timestamp		
3	link-CN-fa-cloud-D4	CN-fa-clou	12:04:56:8	D4	22:04:56:8	Wireless	Yes	16	996	54.9	No	Enabled	2021-07-23T02:49:06.317Z		
4	link-D4-PoP-Onboard-V5k-3083	D4	12:04:56:8	PoP-Onbo	22:04:56:8	Wireless	Yes	0	988	158.8	No	Enabled	2021-07-23T02:49:06.317Z		
5	link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	12:04:56:8	PoP-Onbo	12:04:56:8	Wireless	Yes	0	979	105.2	No	Enabled	2021-07-23T02:49:06.317Z		

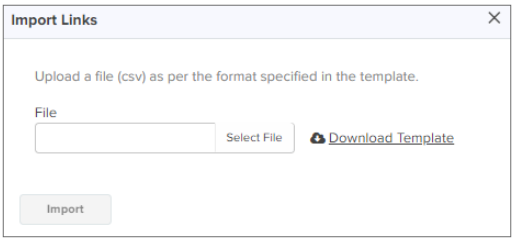
Import List

Import list allow the user to import the PoP links list.

1. Navigate to **Links**> **List** > select **Import.**



Import Links window appears.



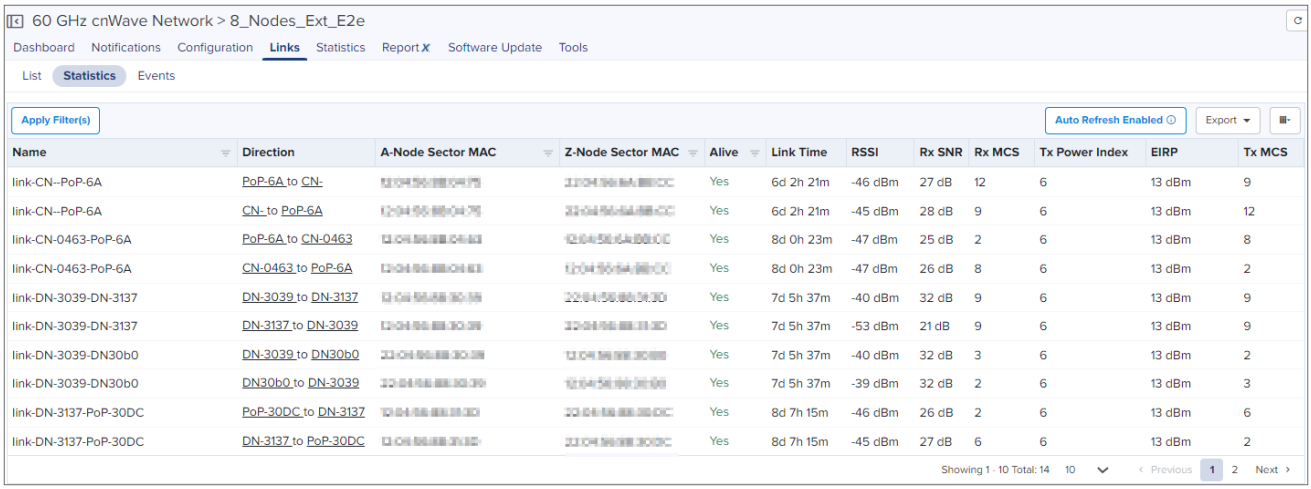
2. Click **Download Template** to download the .CSV format file.

	A	B	C	D	E
1	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of the device	Sector 1/2 MAC Address	Z node name of the device	Sector 1/2 MAC Address	Wireless or Wired
3	POP	[redacted]	DN1	[redacted]	wireless
4	DN1	[redacted]	CN1	[redacted]	wireless
5	DN1		CN2		wired
6					
7					

3. Select the file and click **Import**.

Statistics

Links Statistics pages provides details of **Basic:** Name, Direction, A-Node, Z-Node Alive Link Time Type Distance Azimuth, Rx Golay, Tx Golay **Detailed Statistics**: A-Node Sector MAC, Z-Node Sector MAC, RSSI, Rx Airtime%, Rx Beam Azimuth Angle, Rx Beam Elevation Angle, Rx SNR, Rx MCS, Rx PER, Rx Scan Beams, Rx Throughput, Tx Airtime%, Tx Beam Azimuth Angle, Tx Beam Elevation Angle, Tx Power Index, EIRP, Tx MCS, Tx PER, Tx Scan Beams, Rx Errors, Rx Frames, Tx Errors, Tx Frames, Tx Throughput, Rx Time, Tx Time, and Link Fade Margin links created with PoP node, generally in a page format.

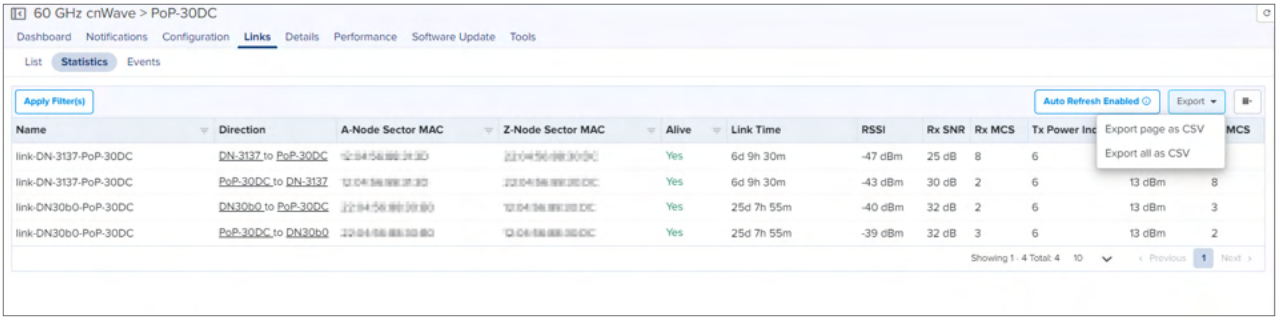


Export Statistics

Export list allow the user to export the PoP links Statistics.

To export the Statistics :

1. Navigate to **Links** > **Statistics** > select **Export.**



2. It exports .csv file format as shown below.

LINK_NAME	DIRECTION	A_NODE_I	Z_NODE_I	A_NODE_I	Z_NODE_I	ALIVE	TYPE	DISTANCE	AZIMUTH	RSSI	Rx_SNR	Rx_MCS	Rx_PER	Rx_BEAM_	Tx_POWEI	EIRP	Tx_MCS	Tx_PER	Tx_BEAM_	Rx_ERROR	Rx_FRAME
link-APOP-DN-3D	APOP to DN-3D	APOP	DN-3D	22:04:56:8	12:04:56:8	Yes	Wireless	147	83	-52	21	9	0.17	64	6	13	10	0.19	64	290	20975
link-APOP-DN-3D	DN-3D to APOP	APOP	DN-3D	22:04:56:8	12:04:56:8	Yes	Wireless	147	83	-51	22	9	0.2	84	6	13	9	0.21	84	374	1488
link-APOP-DN-B0	APOP to DN-B0	APOP	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	94	-178.1	-40	32	9	0	32	6	13	9	0	35	92	30630
link-APOP-DN-B0	DN-B0 to APOP	APOP	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	94	-178.1	-37	32	10	0	0	6	13	10	0	0	1332	9183
link-CN-75-DN-B0	DN-B0 to CN-75	CN-75	DN-B0	12:04:56:8	12:04:56:8	Yes	Wireless	171	-151.2	-48	25	9	0.31	0	23	30	9	0.38	0	0	0
link-CN-75-DN-B0	CN-75 to DN-B0	CN-75	DN-B0	12:04:56:8	12:04:56:8	Yes	Wireless	171	-151.2	-61	12	8	0.42	0	6	13	9	0.35	0	1944	443425
link-CN-83-DN-B0	CN-83 to DN-B0	CN-83	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	71	52.7	-53	21	9	0.81	58	6	35	9	0.06	58	385	2043
link-CN-83-DN-B0	DN-B0 to CN-83	CN-83	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	71	52.7	-49	23	9	0.04	112	6	13	9	0.08	112	0	339
link-CN-8b0463-D	DN-39 to CN-8b	CN-8b046	DN-39	12:04:56:8	22:04:56:8	No	Wireless	199	-45.2	-60	12	9	0	44	31	37	5	0.01	44	95	2856
link-CN-8b0463-D	CN-8b0463 to D	CN-8b046	DN-39	12:04:56:8	22:04:56:8	No	Wireless	199	-45.2	-48	25	9	0.04	45	6	13	9	0.56	45	54	62
link-DN-39-DN-3D	DN-39 to DN-3(	DN-39	DN-3D	12:04:56:8	22:04:56:8	Yes	Wireless	155	20.5	-40	32	9	0	15	6	13	9	0	24	23	504
link-DN-39-DN-3D	DN-3D to DN-3(	DN-39	DN-3D	12:04:56:8	22:04:56:8	Yes	Wireless	155	20.5	-43	30	9	0	0	6	13	10	0	0	164	232
link-DN-39-DN-B0	DN-B0 to DN-3(	DN-39	DN-B0	22:04:56:8	12:04:56:8	Yes	Wireless	100	-70.5	-45	28	9	0.06	35	6	13	9	0.02	34	73	567
link-DN-39-DN-B0	DN-39 to DN-B(	DN-39	DN-B0	22:04:56:8	12:04:56:8	Yes	Wireless	100	-70.5	-48	25	9	0.3	55	6	13	10	0.01	54	331	303

Events

Events provide the details of link availability, hourly link availability in percentage, link availability in different time lines, and distance of the link.

Figure 358 *Link Events*

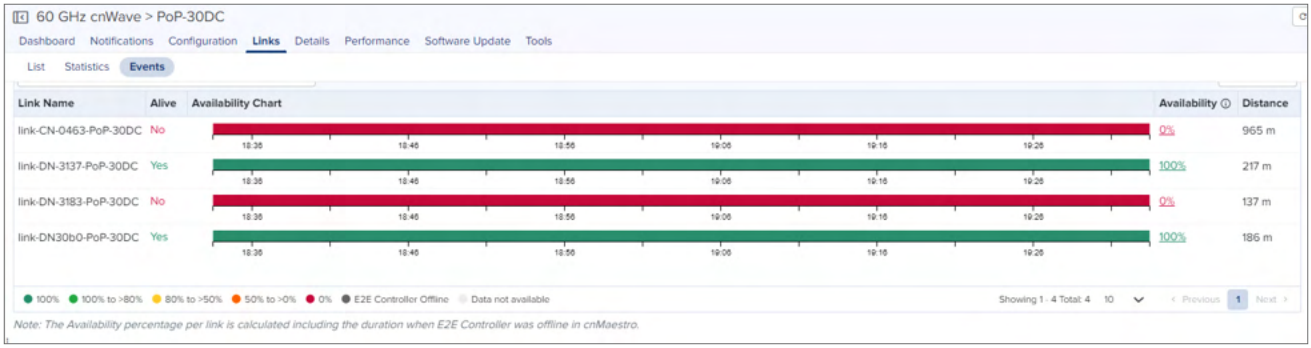


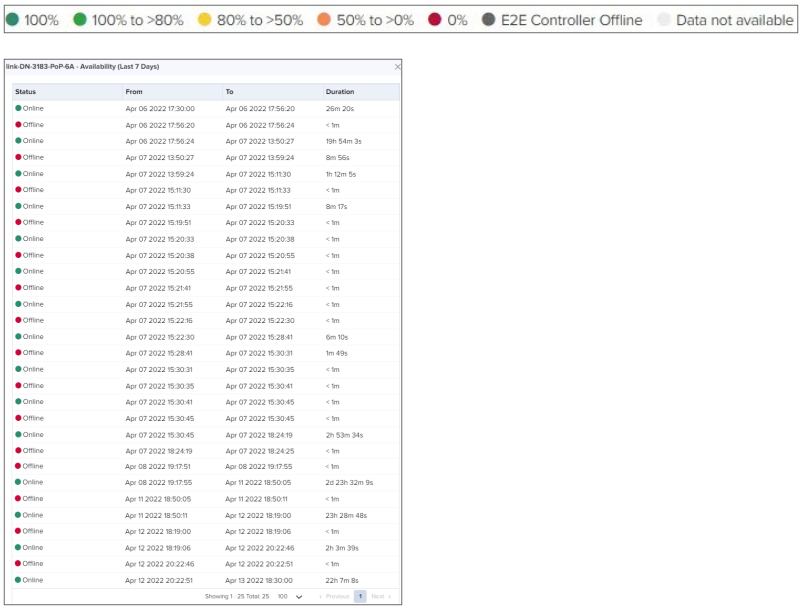
Table 77 *Link > Events fields*

Field	Description
Link Name	Name of the link.
Alive	Status of the link (Yes or No).
Availability Chart	Displays the link availability based on time range selected from the drop-down.When you hover the mouse on the Availability Chart, the link availability is shown as described: 1. If you select time range as **Last 1 Hour**, then link availability for every 5 minutes is displayed. 2. If you select time range other than **Last 1 Hour**, then link availability for every 1 hour is displayed. • Hover on the link to see the hourly availability as shown in Figure 342. • Clicking on percentage link availability displays pop-up window as shown in Figure 343 • Link availability is presented in different colors in the chart as shown in Figure 341

Table 77 *Link > Events fields*

Field	Description
Availability Percentage	Availability of link is shown in percentage in the Availability column, as shown in Figure 342.
Distance	Distance of the link in meters.

Figure 359 *Link Availability in Percentage*

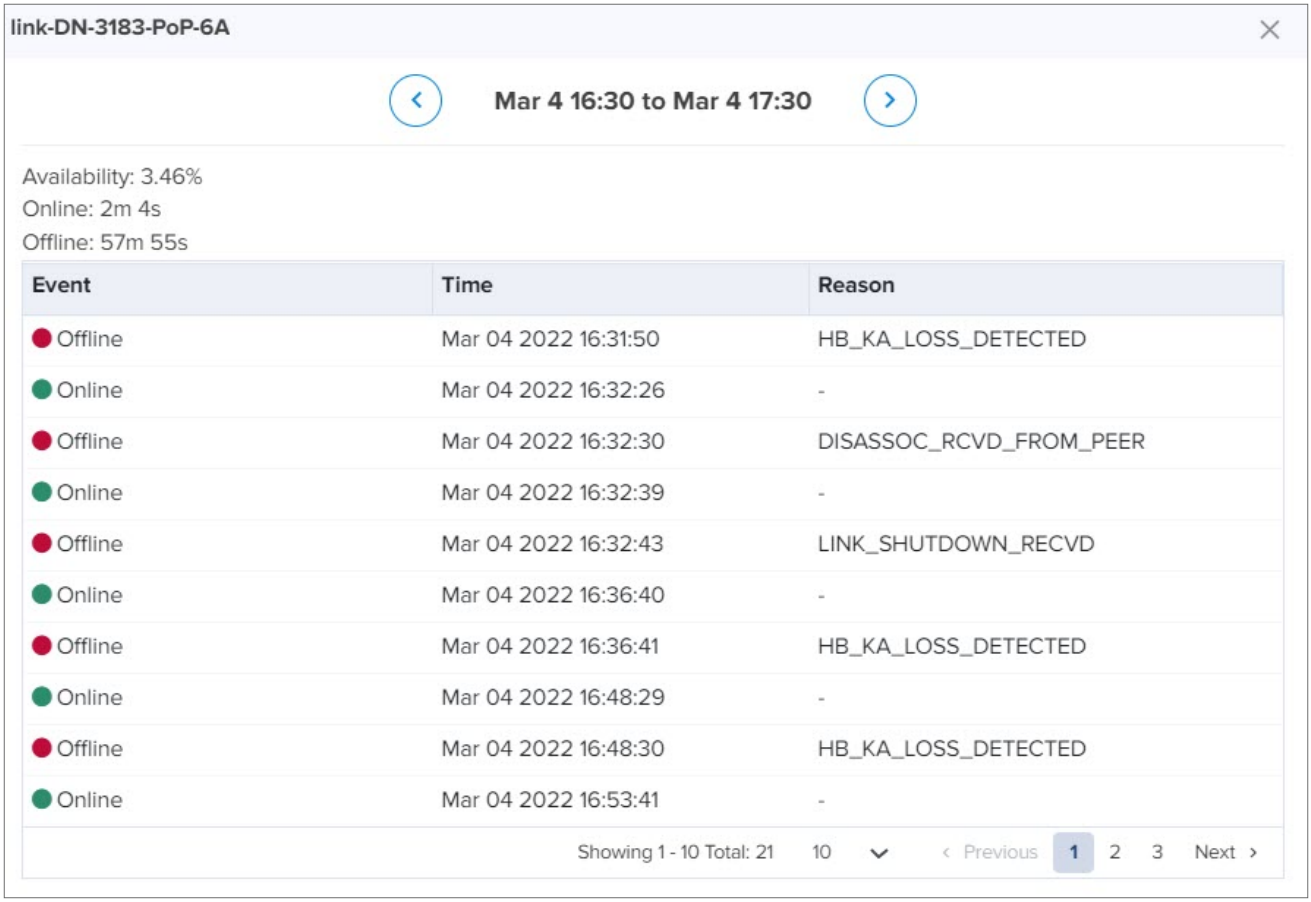


Availability percentage per link is calculated, including the duration, when E2E Controller goes Offline in cnMaestro.

Figure 360 *Link Availability*



Figure 361 *Link Status*



Events details are available for Last 1 hour, Last 6 hours, Last 12 hours, Last 24 Hours, Last 2 days, Last 4 days, and Last 7 days.

Note

Event details for **Custom Range** and **Last 30 days** are available only for cnMaestro X users.

Details

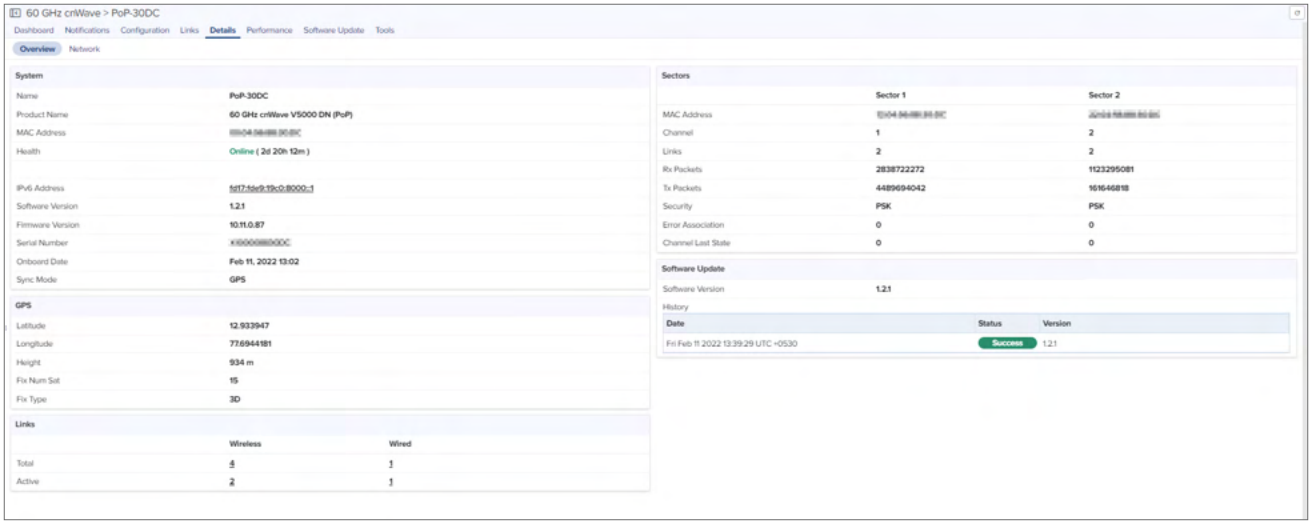
Details page provides the following device information:

- Overview
- Network

Overview

Overview page provides the device details and it also details of the last 3 software update history.

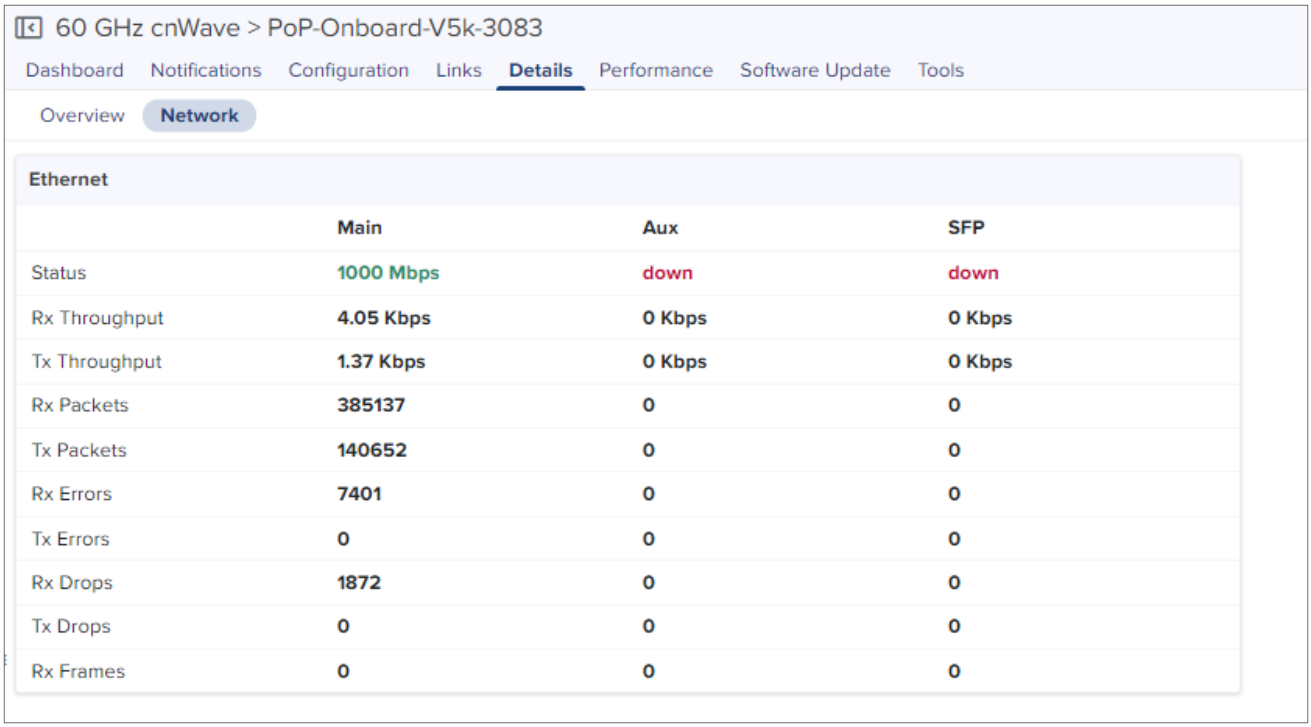
Figure 362 *Details Overview Page*



Network

Network page provides the **Ethernet** details of **Main, Aux**, and **SFP**.

Figure 363 *Details Network Page*



Tools

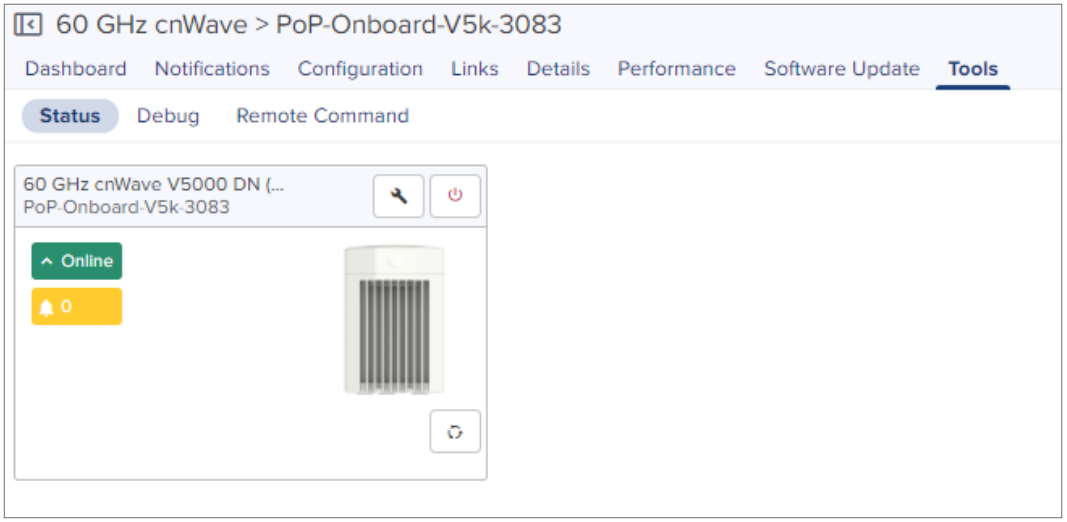
In Tools page, you can view the **Status**, **Debug,** details and **Remote Command** results of the device.

Status

In **Status** tab you can view the status of the device:

- Critical alarms
- Download Tech Support File

- Online or Offline
- Restart minion
- Reboot the device.



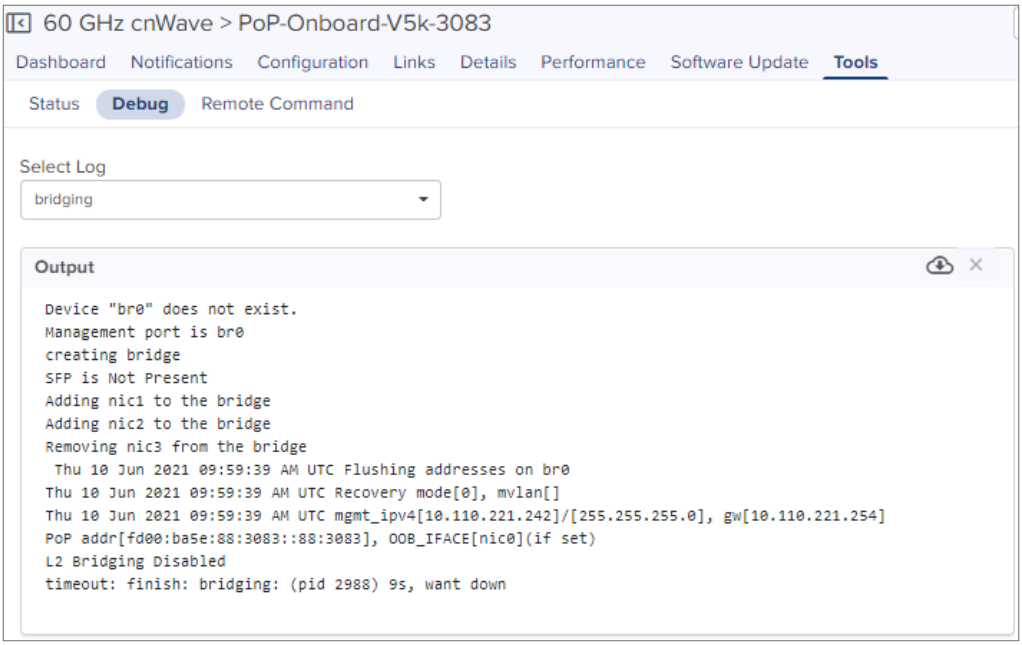
Debug

In **Debug** tab user view or download the PoP logs by executing the following log commands:

- Bridging
- pop-config
- e2e_minion
- openr
- exabgp
- cnAgent (available for Onboard PoP device)

To view the logs:

1. Navigate to **Tools** > **Debug**.
2. Select the required log name from the **Select Log** drop-down list box.



- Click the download icon to download the generated output.
- Click the clear × icon to clear the generated output.

Remote Command

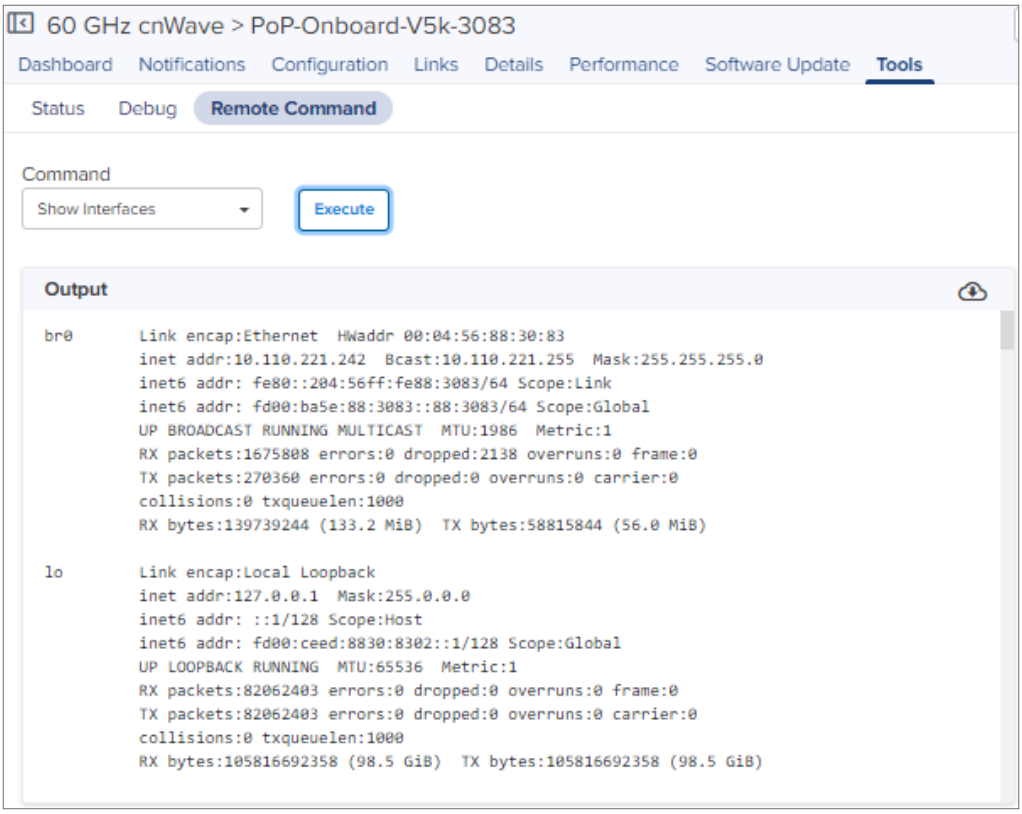
In **Remote command** tab user view or download Command logs by executing the following commands:

- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 and V3000)
- Show IPv4 neighbors
- Show IPv6 neighbors
- Show Wired Device State Changes
- Ping

To Execute the command:

1. Navigate to **Tools** > **Remote Command**.
2. Select the required command from the **Command** drop-down list box.
3. Click **Execute.**

   The output for the selected critera appears as shown:



- Click the download icon to download the generated output.
- Click the clear × icon to clear the generated output.

DN/CN Node

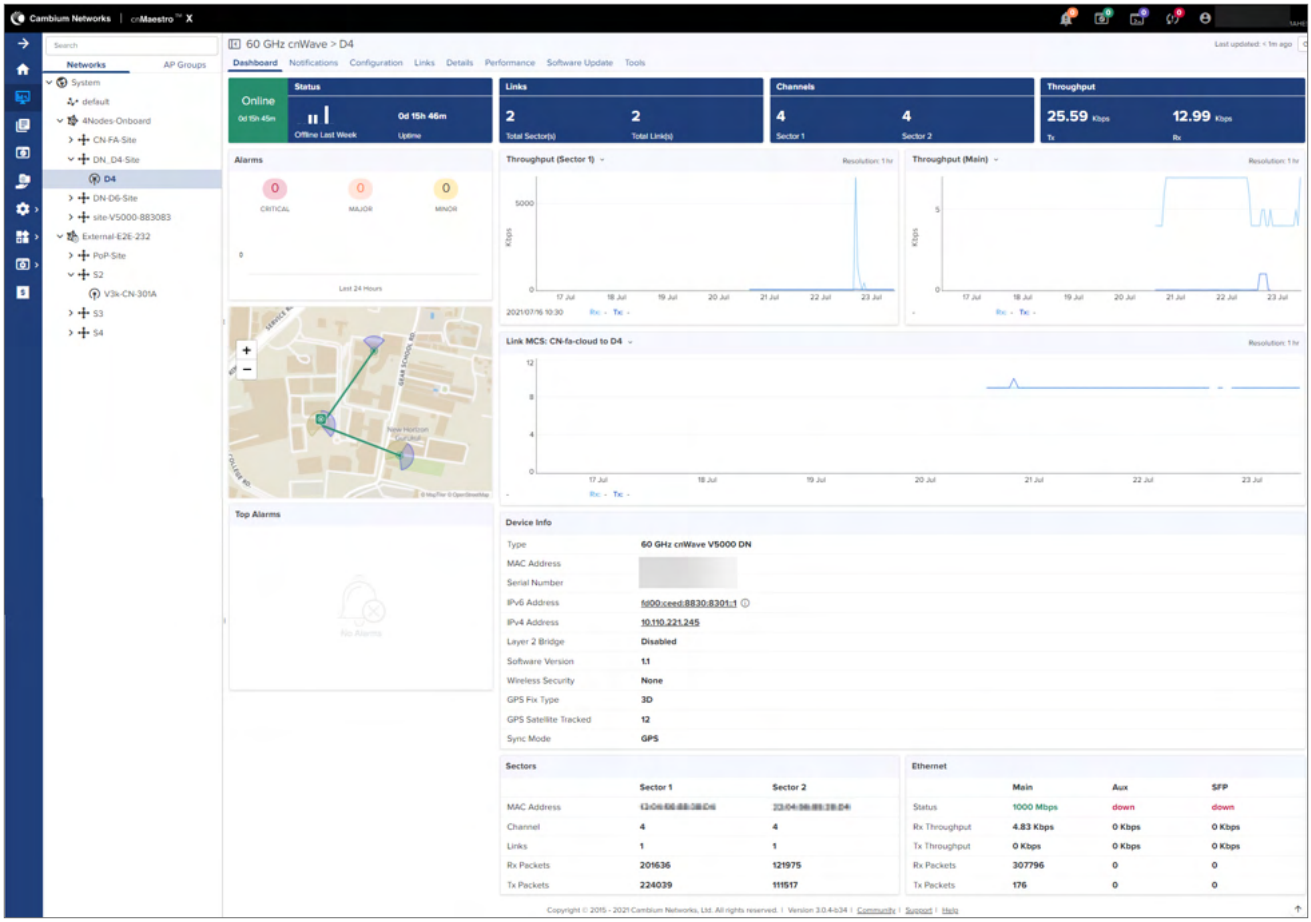
To create a new site, refer to Site.

To create a node, refer to DN/CN.

Dashboard

Dashboard pages are customized for each device type and aggregation level. The DN/CN node dashboard section displays the **Status, Links, Channels, Throughput, Sector Throughput (Sector 1 and Sector 2), Ethernet Throughput (Main, Aux, SFP**), **Alarms, Top Active Alarms, Link MCS, Device Info, Sectors, and Ethernet**.

Figure 364 *DN/CN Node Dashboard*



Configuration

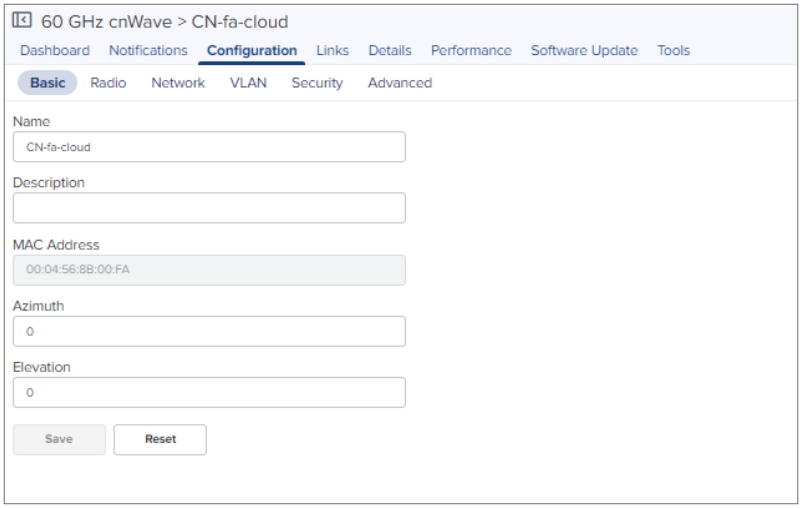
Configuration page allows the user to configure the following details of CN/DN:

- Basic
- Radio
- Network
- VLAN
- Security
- Advanced

Basic

It allows to configure and reset the basic details of DN/CN node such as Name, Description, MAC Address, Azimuth, and Elevation. It also allows to edit the name of the node.

Figure 365 *Basic*



Radio

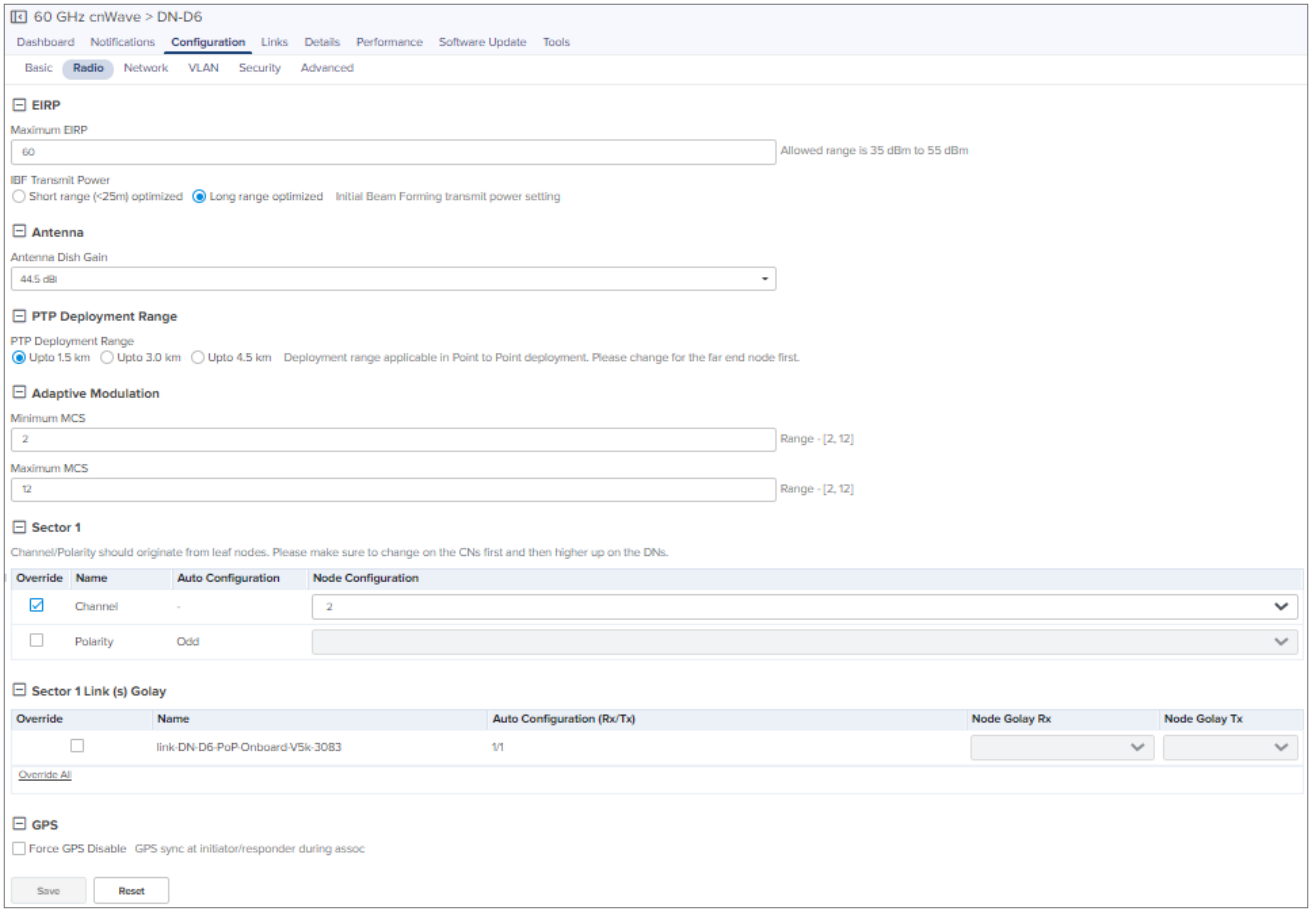


Note

GPS option is not enabled for v1000.

It allows the you to configure the **EIRP**, **Adaptive Modulation**, **Sectors (channels, Polarity and Link(s) Golay),** and **GPS**.

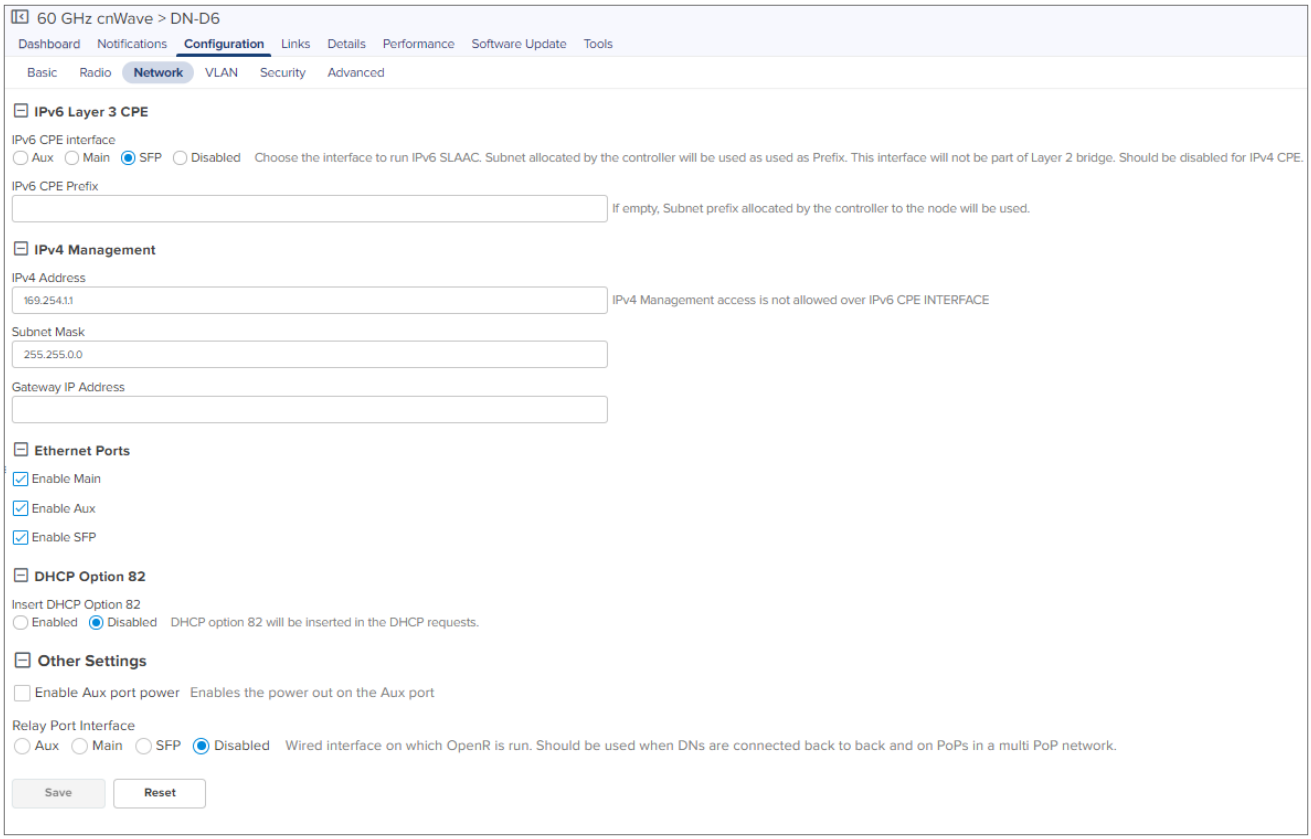
Figure 366 *Radio*



Network

Network tab allows the user to edit the **Layer 3 CPE, IPv4 Management**, **Ethernet Ports, PTP External Failover**, and **Other Settings.**

Figure 367 *Network*



VLAN

VLAN configuration of CN/DN is same as PoP Node VLAN as shown above.

Note

Enable Layer 2 Bridge in **60 GHz cnWave > Configuration > Basic** page to configure the CN/DN VLAN.

Security

Security tab allows to reset the identity and password of the Radius user.

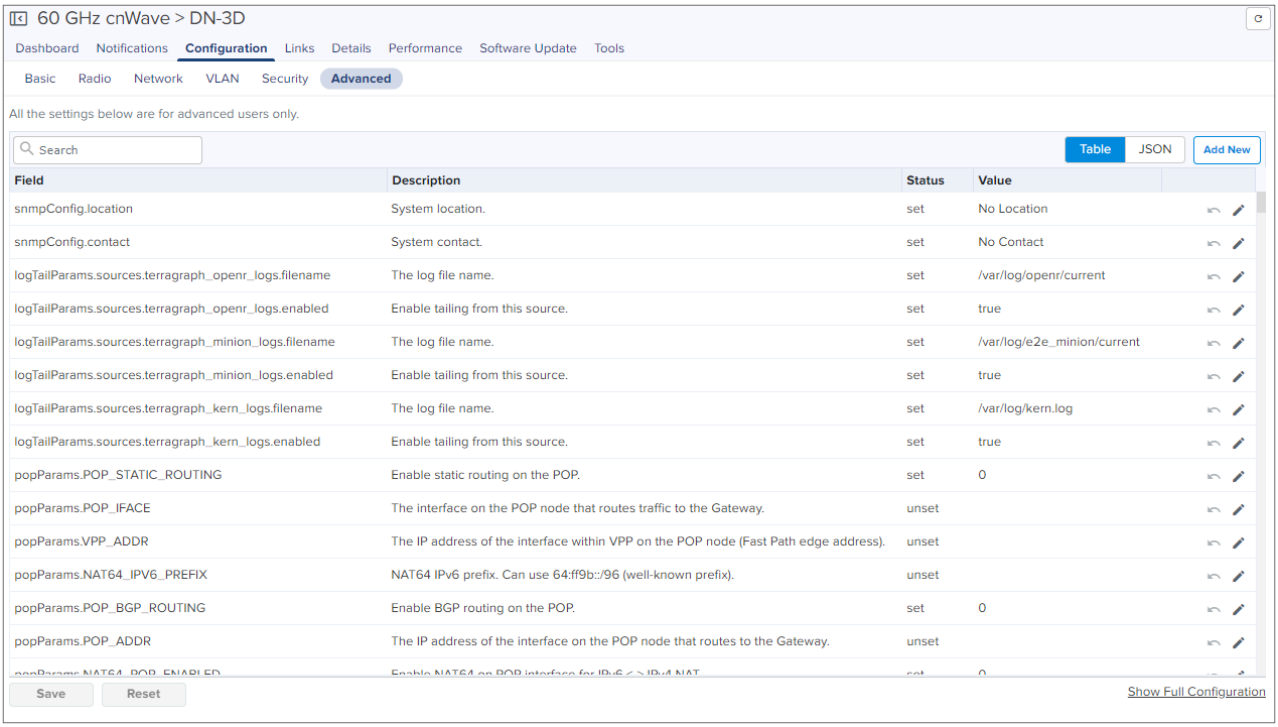
Figure 368 *Security*



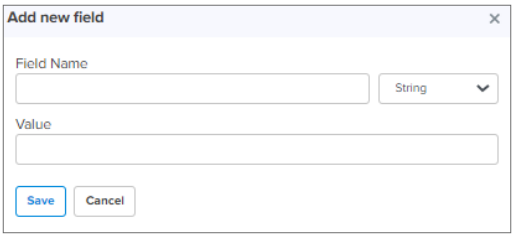
Advanced

Advanced tab allows the advanced user to set Field Name and Value.

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



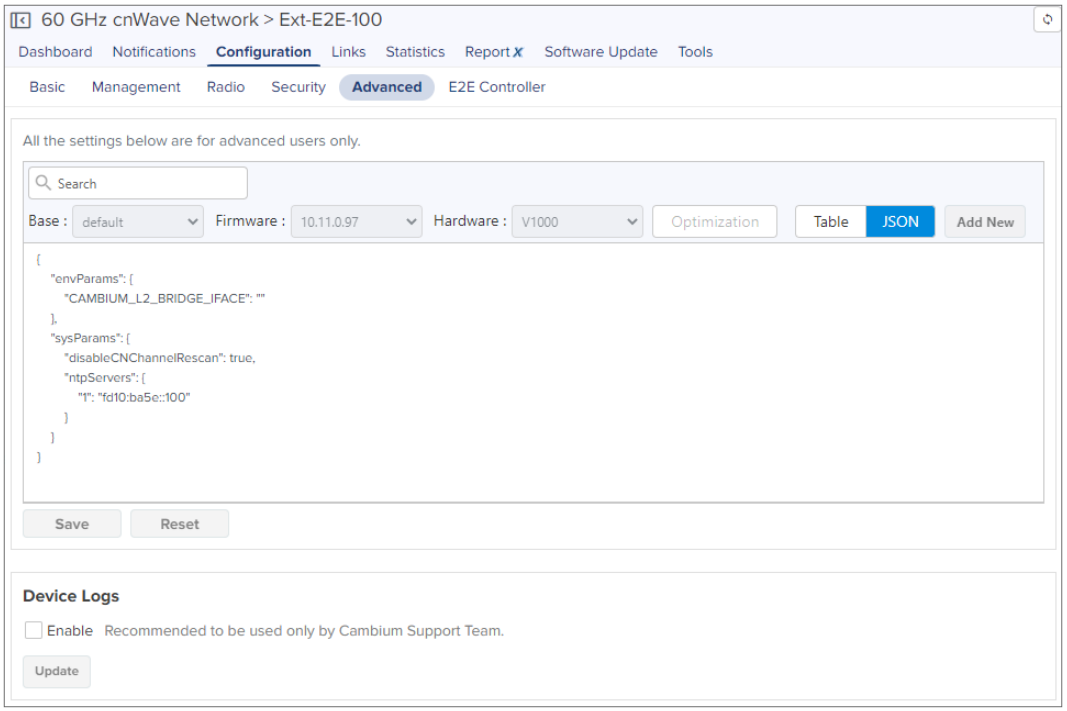
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

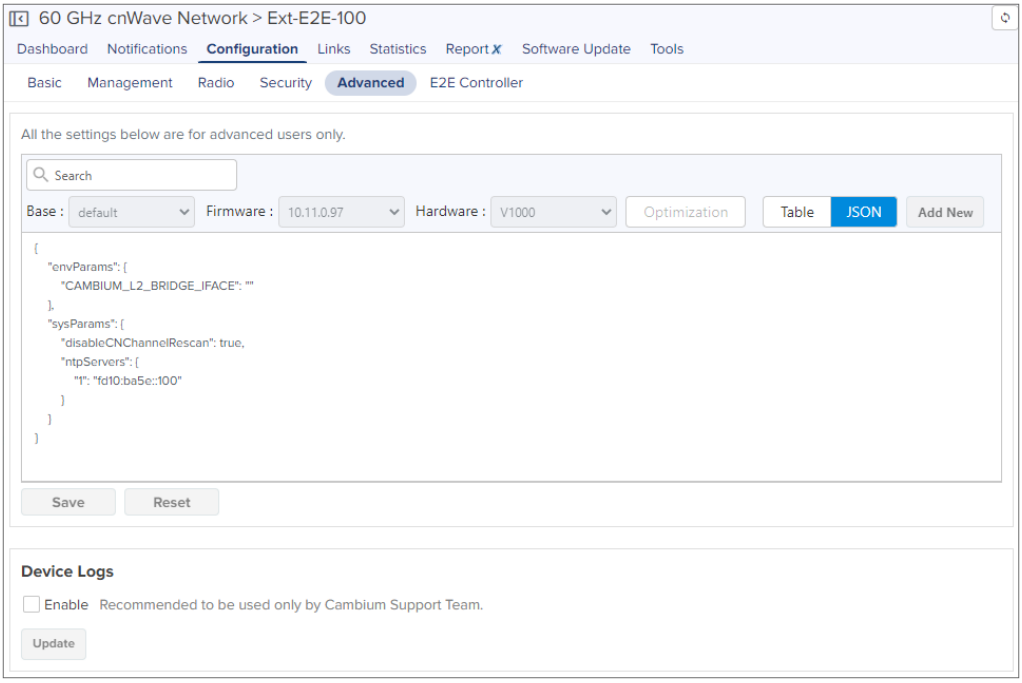
JSON

JSON allows Advanced users to view the JSON format.

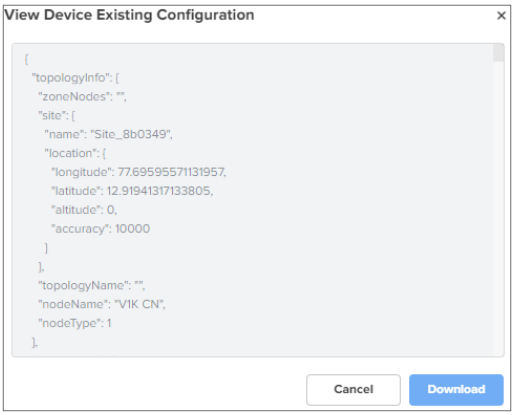


To download the file, perform the following steps:

1. Navigate to **Configuration** > **Advanced** > **JSON.**



2. Click **Show Full Configuration.**
3. **View Device Existing Configuration** pops up.



4. Click **Download**.

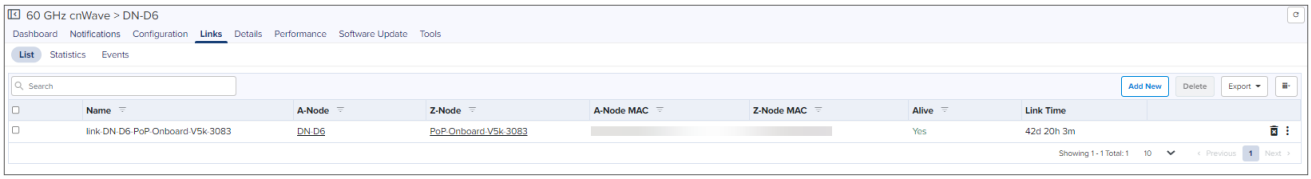
Links

Links provide the details about links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular devices.

List

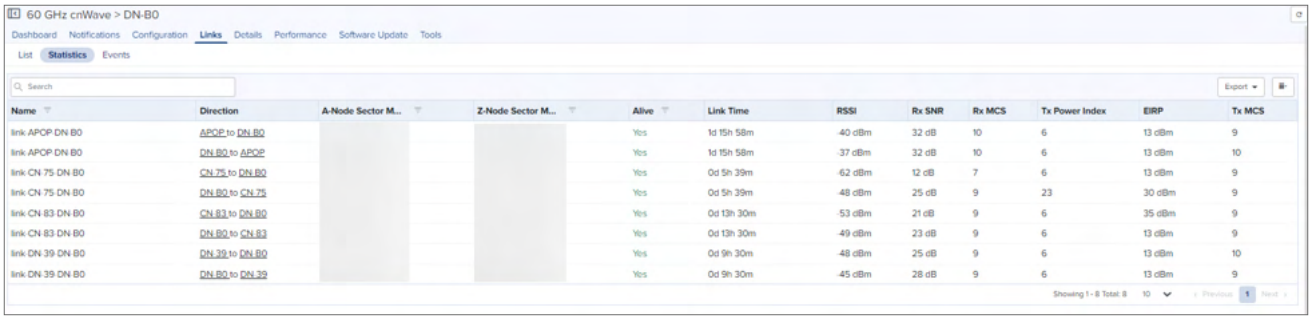
List provide the details about the links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular link.

Figure 369 *List*



Statistics

Links Statistics pages provides details of **Basic:** Name, Direction, A-Node, Z-Node Alive Link Time Type Distance Azimuth, Rx Golay, Tx Golay **Detailed Statistics**: A-Node Sector MAC, Z-Node Sector MAC, RSSI, Rx Airtime%, Rx Beam Azimuth Angle, Rx Beam Elevation Angle, Rx SNR, Rx MCS, Rx PER, Rx Scan Beams, Rx Throughput, Tx Beam Azimuth Angle, Tx Power Index, EIRP, Tx MCS, Tx PER, Tx Scan Beams, Rx Errors, Rx Frames, Tx Errors, Tx Frames, Rx Time, Tx Airtime%, Tx Beam Azimuth Angle, Tx Beam Elevation Angle, Tx Throughput, Tx Time, and Link Fade Margin links created with DN/CN node, in a page format.



Events

Events provide the details of link availability, hourly link availability in percentage, link availability in different time lines, and distance of the link.

Figure 370 *Events*

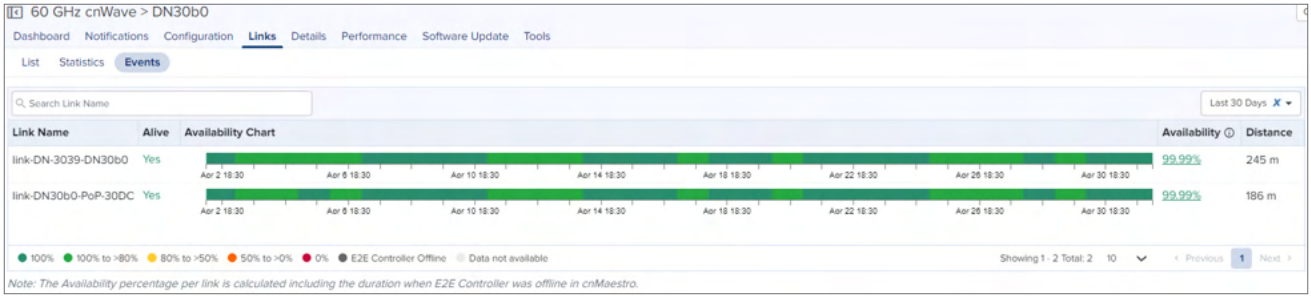


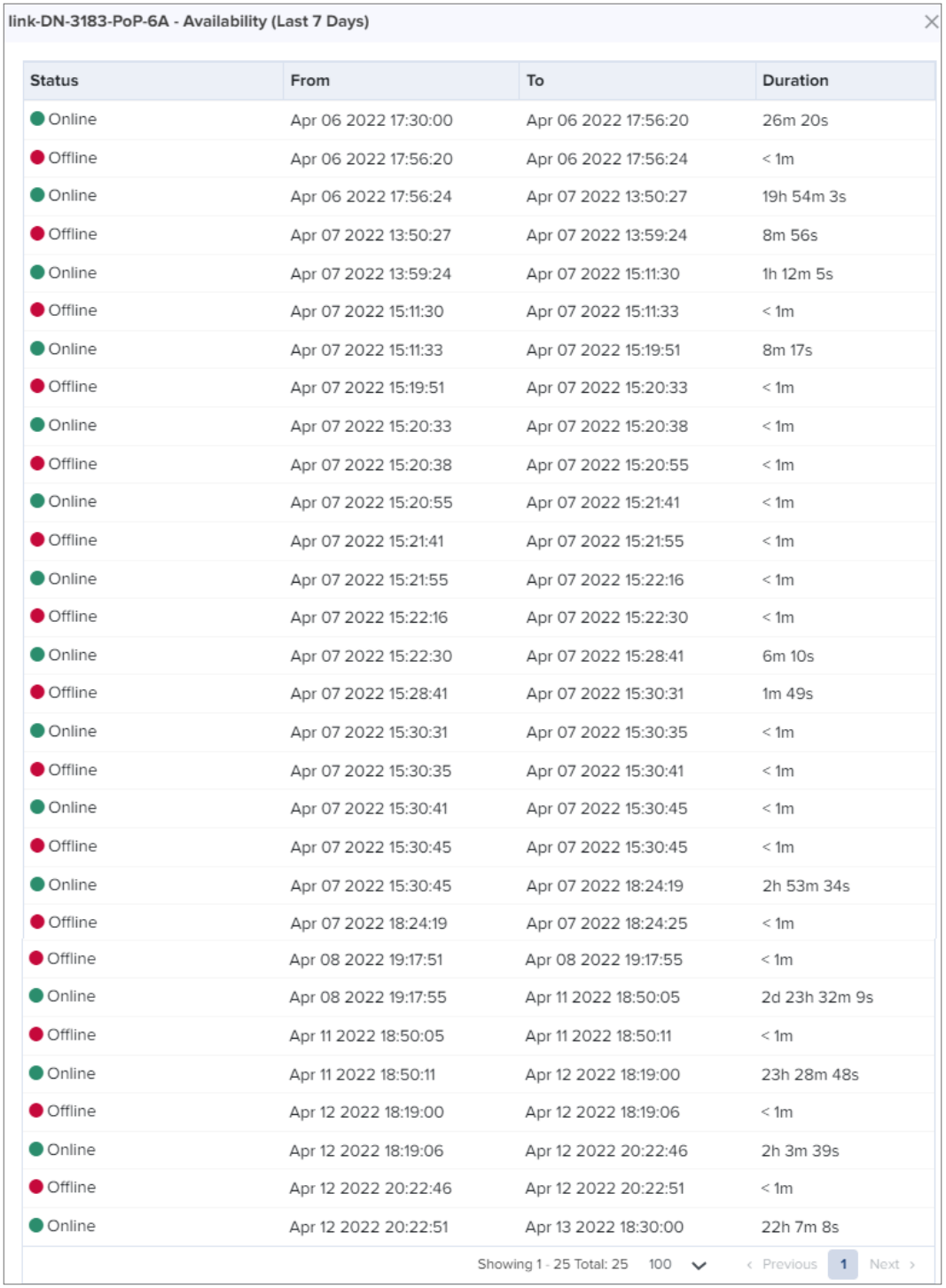
Table 78 *Events fields*

Field	Description
Link Name	Name of the link.
Alive	Status of the link (Yes or No).
Availability Chart	Displays the link availability based on time range selected from the drop-down.When you hover the mouse on the Availability Chart, the link availability is shown as described: 1. If you select time range as **Last 1 Hour**, then link availability for every 5 minutes is displayed. 2. If you select time range other than **Last 1 Hour**, then link availability for every 1 hour is displayed. • Hover on the link to see the hourly availability as shown in Figure 342. • Clicking on percentage link availability displays pop-up window as shown in Figure 343 • Link availability is presented in different colors in the chart as shown in Figure 341
Availability Percentage	• Clicking on percentage for the complete timeline link availability displays pop-up window as shown in Figure 372. • Availability of link is shown in percentage in the Availability column as shown in Figure 342.
Distance	Distance of the link in meters.

Figure 371 *Link Availability in Percentage*



Figure 372 *Link Availability details*



link-DN-3183-PoP-6A - Availability (Last 7 Days)

Status	From	To	Duration
Online	Apr 06 2022 17:30:00	Apr 06 2022 17:56:20	26m 20s
Offline	Apr 06 2022 17:56:20	Apr 06 2022 17:56:24	< 1m
Online	Apr 06 2022 17:56:24	Apr 07 2022 13:50:27	19h 54m 3s
Offline	Apr 07 2022 13:50:27	Apr 07 2022 13:59:24	8m 56s
Online	Apr 07 2022 13:59:24	Apr 07 2022 15:11:30	1h 12m 5s
Offline	Apr 07 2022 15:11:30	Apr 07 2022 15:11:33	< 1m
Online	Apr 07 2022 15:11:33	Apr 07 2022 15:19:51	8m 17s
Offline	Apr 07 2022 15:19:51	Apr 07 2022 15:20:33	< 1m
Online	Apr 07 2022 15:20:33	Apr 07 2022 15:20:38	< 1m
Offline	Apr 07 2022 15:20:38	Apr 07 2022 15:20:55	< 1m
Online	Apr 07 2022 15:20:55	Apr 07 2022 15:21:41	< 1m
Offline	Apr 07 2022 15:21:41	Apr 07 2022 15:21:55	< 1m
Online	Apr 07 2022 15:21:55	Apr 07 2022 15:22:16	< 1m
Offline	Apr 07 2022 15:22:16	Apr 07 2022 15:22:30	< 1m
Online	Apr 07 2022 15:22:30	Apr 07 2022 15:28:41	6m 10s
Offline	Apr 07 2022 15:28:41	Apr 07 2022 15:30:31	1m 49s
Online	Apr 07 2022 15:30:31	Apr 07 2022 15:30:35	< 1m
Offline	Apr 07 2022 15:30:35	Apr 07 2022 15:30:41	< 1m
Online	Apr 07 2022 15:30:41	Apr 07 2022 15:30:45	< 1m
Offline	Apr 07 2022 15:30:45	Apr 07 2022 15:30:45	< 1m
Online	Apr 07 2022 15:30:45	Apr 07 2022 18:24:19	2h 53m 34s
Offline	Apr 07 2022 18:24:19	Apr 07 2022 18:24:25	< 1m
Offline	Apr 08 2022 19:17:51	Apr 08 2022 19:17:55	< 1m
Online	Apr 08 2022 19:17:55	Apr 11 2022 18:50:05	2d 23h 32m 9s
Offline	Apr 11 2022 18:50:05	Apr 11 2022 18:50:11	< 1m
Online	Apr 11 2022 18:50:11	Apr 12 2022 18:19:00	23h 28m 48s
Offline	Apr 12 2022 18:19:00	Apr 12 2022 18:19:06	< 1m
Online	Apr 12 2022 18:19:06	Apr 12 2022 20:22:46	2h 3m 39s
Offline	Apr 12 2022 20:22:46	Apr 12 2022 20:22:51	< 1m
Online	Apr 12 2022 20:22:51	Apr 13 2022 18:30:00	22h 7m 8s

Showing 1 - 25 Total: 25 100 ‹ Previous 1 Next ›

Availability percentage per link is calculated including the duration when E2E Controller was Offline in cnMaestro.

Figure 373 *Link Availability*

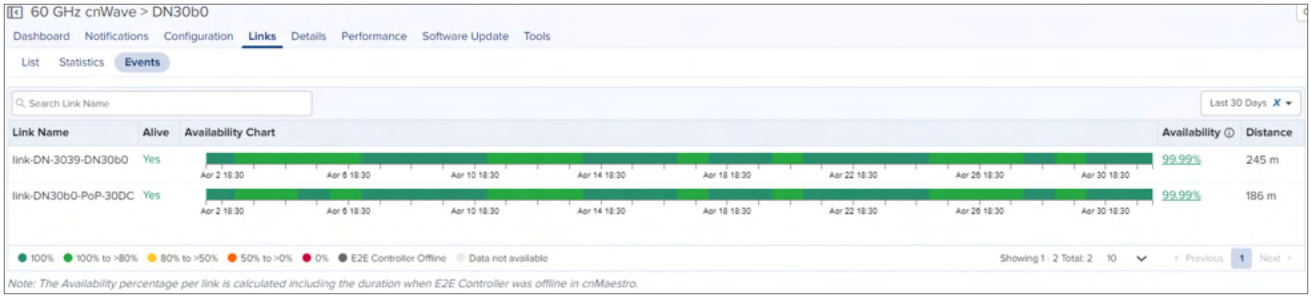
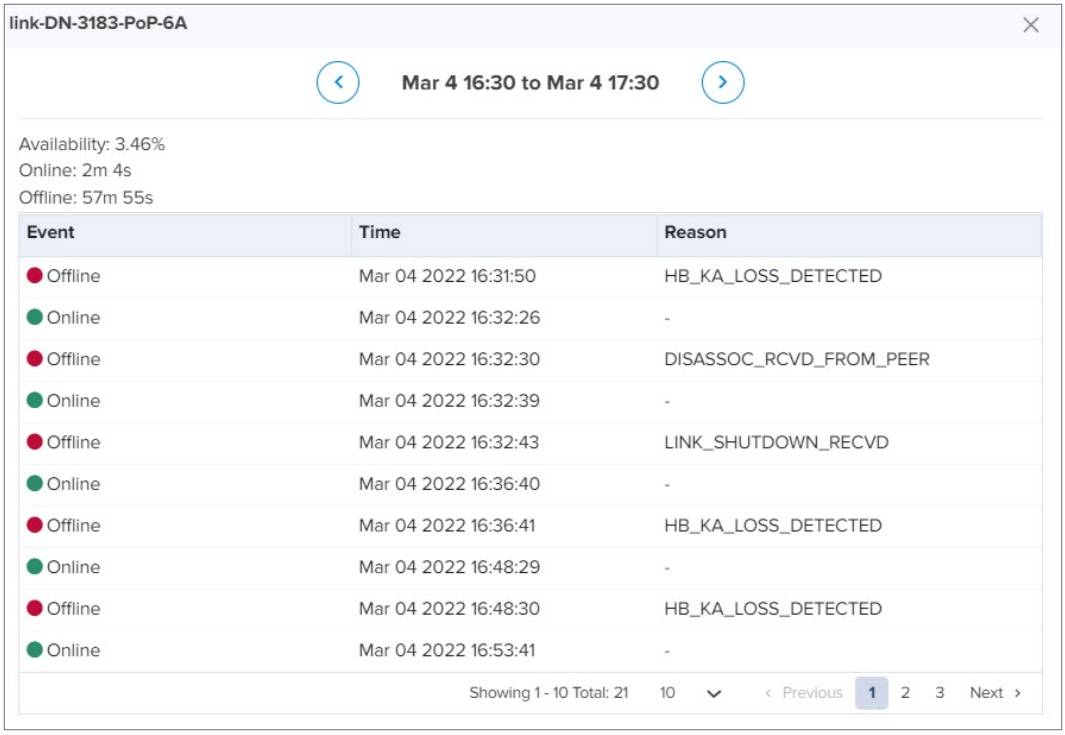


Figure 374 *Link Status*



Events details are available for Last 1 hour, Last 6 hours, Last 12 hours, Last 24 Hours, Last 2 days, Last 4 days, and Last 7 days.

Note

Event details for **Custom Range** and **Last 30 days** is available only for cnMaestro X users.

Tools

In Tools page you can view the **Status** and **Debug** details of the device.

Status

In **Status** tab you can view the status of the device:

- Critical alarms
- Download Tech Support File
- Online or Offline
- Reboot the device.

- Restart Minion
- Factory reset



Debug

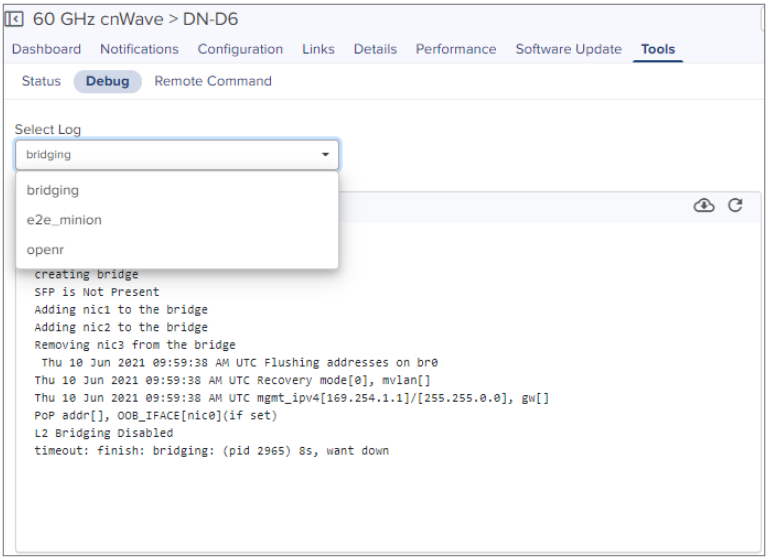
In **Debug** tab, you can view or download the DN or CN logs by executing the following log commands:

- Bridging
- e2e_minion
- openr

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select the required log name from the **Select Log** drop-down list box.

   The output for the selected critera appears as shown:



   - Click the download icon to download the generated output.
   - Click the clear ✕ icon to clear the generated output.

Remote Command

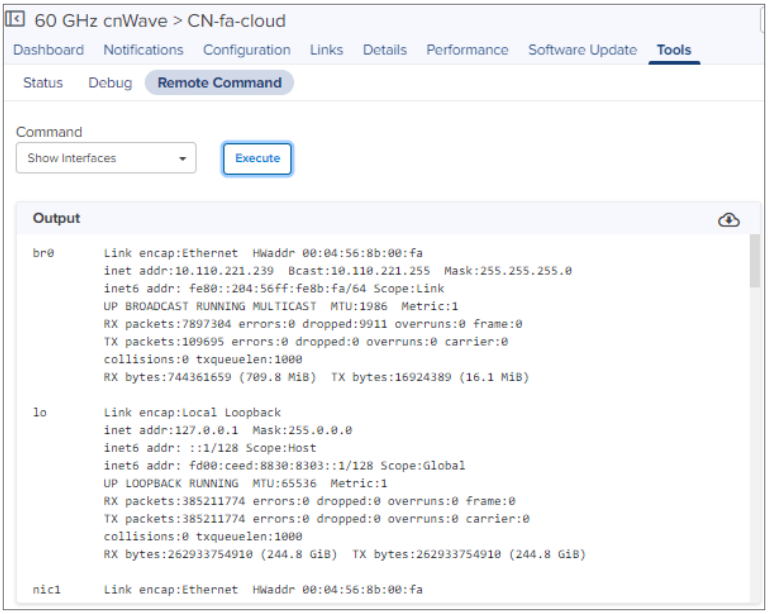
In **Remote command** tab, you can view and download Command logs by executing the following commands:

- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 an V3000)
- Show IPv4 neighbors
- Show IPv6 neighbors
- Show Wired Device State Changes
- Ping

To Execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select the required command from the **Command** drop-down.
3. Click **Execute.**

   The output for the selected critera appears as shown:



   - Click the download icon to download the generated output.
   - Click the clear ✕ icon to clear the generated output.

Managing NSE 3000 using cnMaestro

NSE 3000 is managed using the cloud-hosted cnMaestro (a management solution from Cambium Networks).

This section covers the following topics:

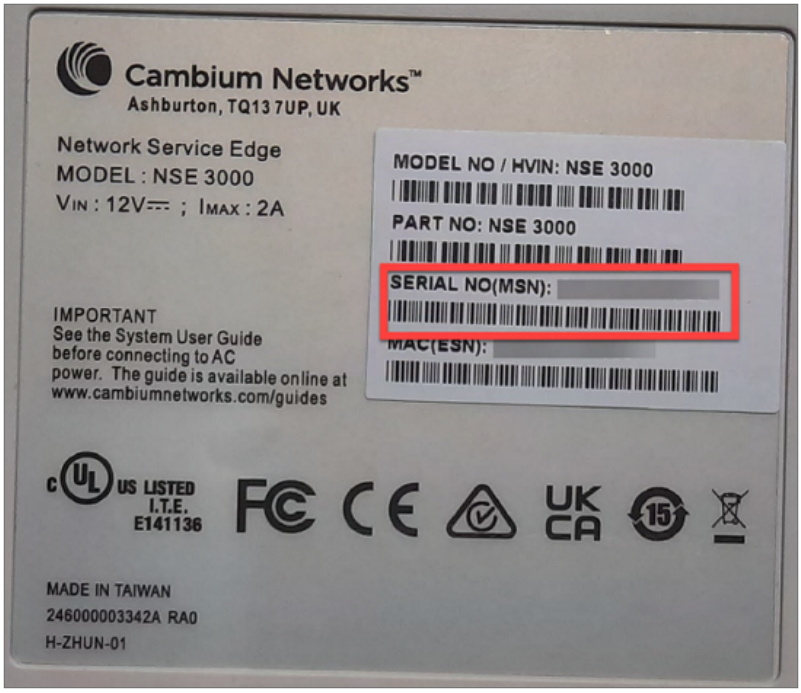
- Claiming an NSE 3000 device associated with a site
- High availability support for NSE 3000

- Configuring NSE 3000
- Configuring WAN in the device UI

Claiming an NSE 3000 device associated with a site

A device manufacturer serial number (MSN) is required to claim an NSE 3000 device. You can find the device MSN at the bottom of the device as shown in Figure 375.

Figure 375 *MSN of the NSE 3000 device*

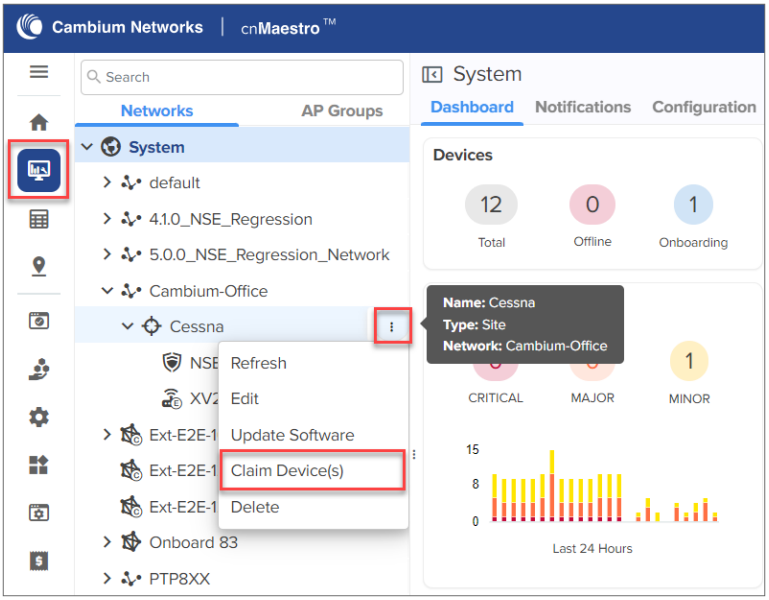


To claim an NSE 3000 device that is associated with a site, complete the following steps:

1. From the home page, navigate to **Monitor and Manage**.

   The **System** page appears, as shown in Figure 376.

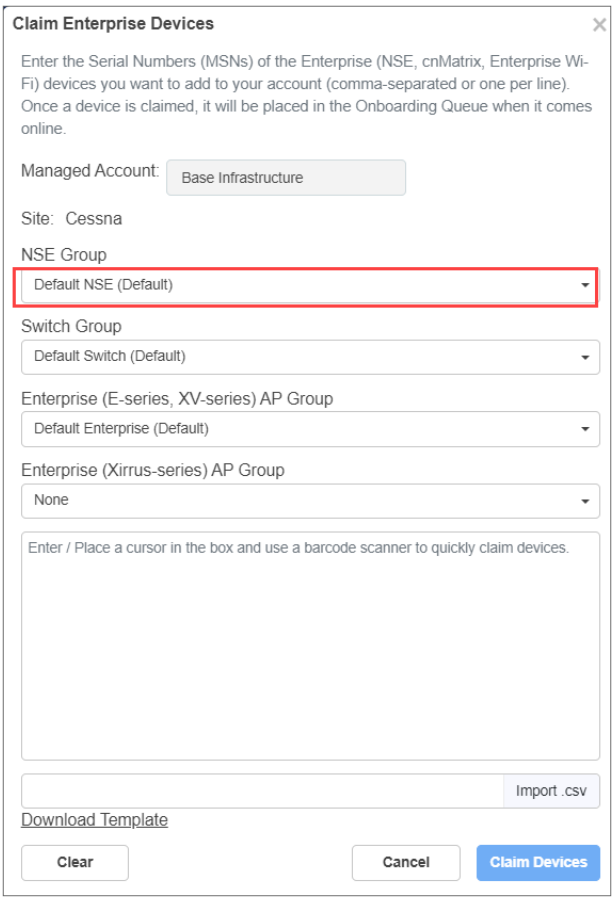
Figure 376 *The System page*



2. On the left panel, in the **Networks** section, expand the site panel.
3. Click the actions (⋮) icon and select **Claim Device(s)**.

   The **Claim Enterprise Devices** window appears, as shown in Figure 377.

Figure 377 *The Claim Enterprise Devices window*



4. From the **NSE Group** drop-down list, select the required group.



Note

The selected NSE group is automatically pushed to the device while onboarding.

5. In the **Enter** field, enter the MSN of the NSE 3000 device.
6. Click **Claim Devices**.

   The NSE 3000 device that is associated with a site is claimed successfully.

High availability support for NSE 3000

The high availability (HA) support allows two NSE 3000 devices to share health information when connected through a LAN port (Port-6). When the devices are connected as an HA pair, one is configured as **Primary** and the other as **Spare**. The **Spare** device serves as a backup in case of hardware failures.

If the **Primary** device goes down, the **Spare** device becomes active. When the **Primary** device is restored, it regains its active state and the **Spare** device reverts to a backup state.



Note

The HA support is available from NSE release version 1.7 and higher.

Licensing

An NSE 3000 device requires a Tier-30 license to onboard to cnMaestro.

An HA pair (Primary - Spare) requires only one Tier-30 license. The **Spare** device does not require an additional license as it inherits the license from the **Primary** device.

On the expiry of the license, the device management is deactivated using cnMaestro. However, the devices are not deleted from the device list in cnMaestro.

Constraints on NSE 3000 devices

The following are the constraints on NSE 3000 devices in cnMaestro:

- A site can have either a single NSE 3000 device or a single NSE 3000 HA pair.
- An HA pair can only be created under a site. NSE group is mandatory for all NSE 3000 devices to onboard to the cnMaestro cloud 5.1.1 version.
- An NSE 3000 device must exist (with an NSE group attached) under the site to form an HA pair.
- If a device is in the **Onboarding** state under a site, you cannot claim another device under the same site.

Creating an HA pair in cnMaestro

You can create an HA pair using either of the following options:

- **Onboard as HA spare** (from the Onboarding queue)
- **Claim Device(s)** (at the site level)

The HA pair configuration involves the following tasks:

- Onboarding an NSE 3000 device as an HA spare
- Claiming an NSE 3000 device as an HA spare
- Moving the HA pair (in the tree)

- Deleting an NSE 3000 device from the HA pair
- Deprecation of device overrides
- Upgrading the firmware
- Viewing aggregated data of HA pair
- Creating Wireguard clients for NSE HA pair

Onboarding an NSE 3000 device as an HA spare

The primary device onboards as a standalone device to cnMaestro. An additional NSE 3000 device can be brought into the onboarding queue (without Tier-30 license) either by bulk claim (on the Onboard page) or using cambium-id and password. An HA pair is formed using the **Onboard as HA spare** option from the **Approve Device** window.

Note

- The primary device must have the firmware that supports HA functionality.
- The spare device must have the same firmware as the primary device. Otherwise, the system automatically upgrades the firmware of the spare device to match with the primary device.
- The spare device must have the same model as the primary device. NSE 3000 device can be paired only with an NSE 3000 device model. It cannot be paired with an NSE 5000 device model.

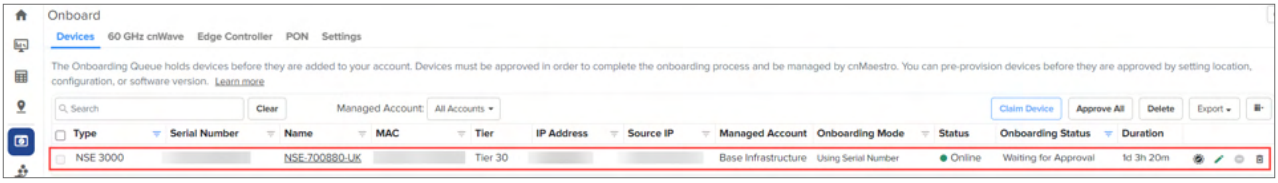
When onboarding an NSE 3000 device as a spare, the device automatically inherits the NSE group of the primary device. This holds good even if the devices are claimed at the site level. Additionally, any change in the NSE group of the primary device is automatically reflected in the spare device.

To onboard an NSE 3000 device as a spare device, complete the following steps:

1. From the home page, click the Onboard ( ) icon.

   The Onboard page appears.

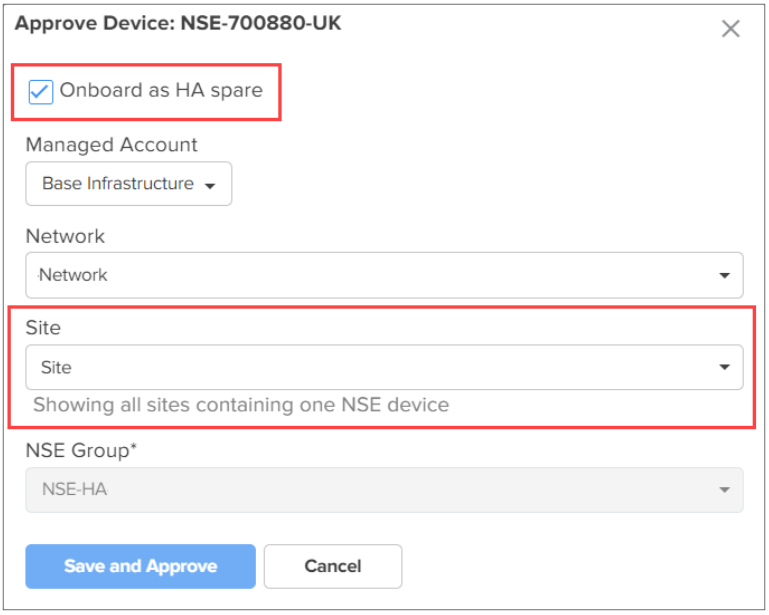
   Figure 378 *The Onboard page*



2. Click the approve device ( ) icon of the NSE 3000 device.

   The **Approve Device** window appears with the **Onboard as HA spare** option and shows all sites that have only one NSE device (as shown in Figure 379).

Figure 379 *The Approve Device window*



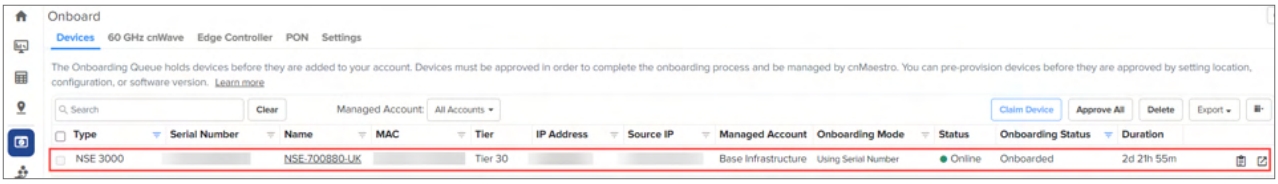
Note

The spare device has the same NSE group as that of the primary device.

3. Click **Save and Approve** from the **Approve Device** window (as shown in Figure 379).

   The spare device is onboarded (as shown in Figure 380) without an additional Tier-30 license.

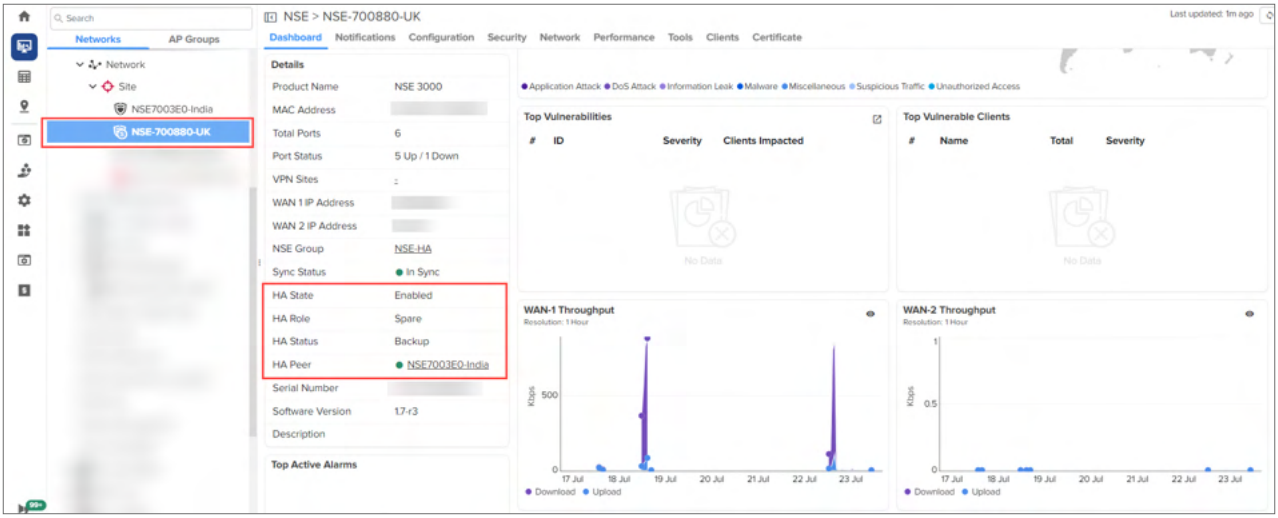
   Figure 380 *Spare device onboarded*



4. Click on the spare device name.

   You can see the spare device under a site (as shown in Figure 381). You can view the HA details in the **Details** section of the dashboard (as shown in Figure 381).

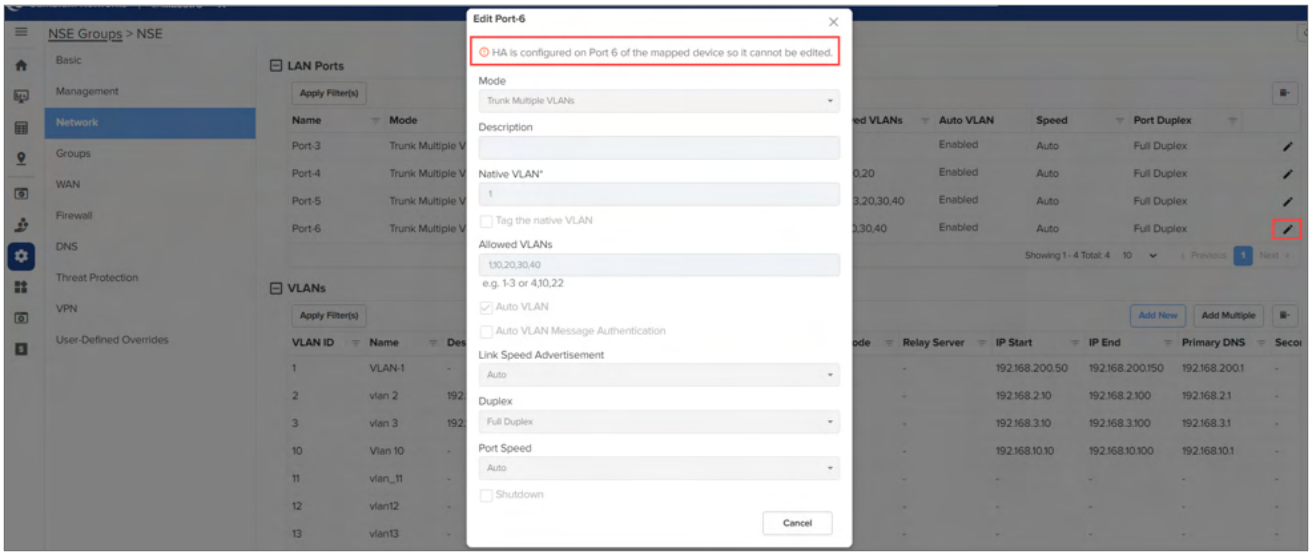
Figure 381 *Details about HA for the Spare device*



Note

When HA is configured on Port-6 of the mapped device, you cannot edit the Port-6 configuration. A message is displayed on the **Edit Port-6** window (as shown in Figure 382).

Figure 382 *The Edit Port-6 window*



Note

The fields in the **Approve Device** window (as shown in Figure 379) can also be configured using the Edit Device ( ) icon from the **Onboard** page.

Claiming an NSE 3000 device as an HA spare

An NSE 3000 HA pair can be additionally formed using the **Claim Device(s)** option at the site level. When a second NSE 3000 device is claimed (assuming the primary already exists under the site), you have the option to claim it as a spare. However, claiming a second NSE 3000 device under the same site as a regular device is restricted.

To claim an NSE 3000 device as an HA spare, complete the following steps:

1. From the home page, click the Monitor and Manage ( ) icon.

   The **System** page appears.

2. On the left panel, in the **Networks** section, expand the site panel.

3. Click the actions ( ) icon and select **Claim Device(s)**.

   The **Claim Enterprise Devices** window appears.

4. In the **Enter** field, enter the MSN of the NSE 3000 device.

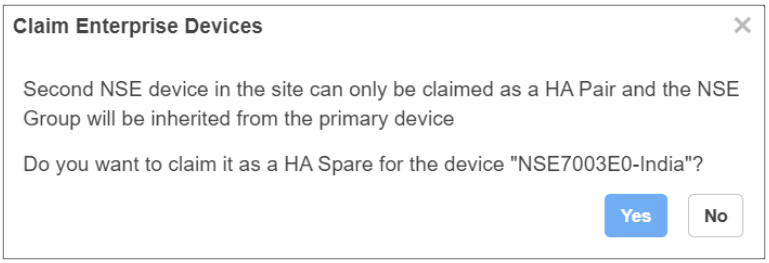
   Note

   You can find the device MSN at the bottom of the NSE 3000 device.

5. Click **Claim Devices**.

   The **Claim Enterprise Devices** window appears.

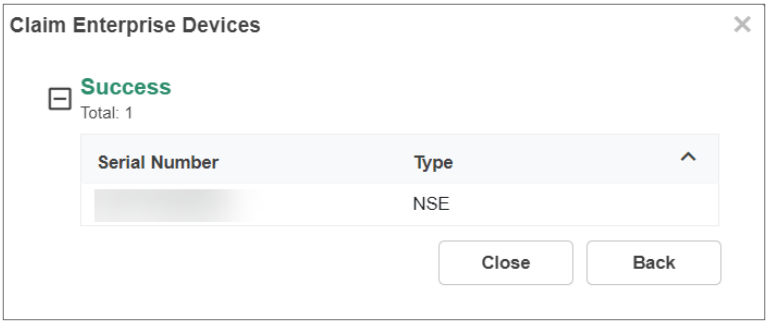
   Figure 383 *The Claim Enterprise Devices window*



6. Click **Yes**.

   The **Claim Enterprise Devices** window appears.

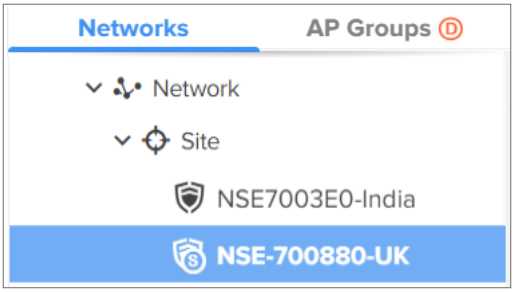
   Figure 384 *The Claim Enterprise Devices window*



7. Click **Close**.

   The device is claimed as an HA spare.

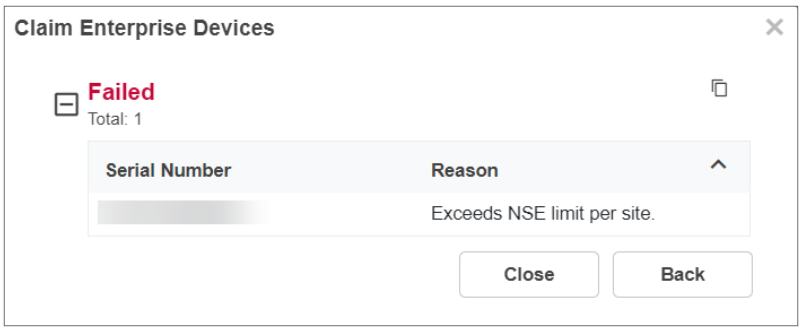
Figure 385 *Device claimed as an HA spare*



The ( ) icon indicates the primary NSE 3000 device. The ( ) icon indicates the spare NSE 3000 device.

When you click **No** in the **Claim Enterprise Devices** window (as shown in Figure 383), the **Claim Enterprise Devices** window appears (as shown in Figure 386). You cannot claim the device as an HA spare.

Figure 386 *The Claim Enterprise Devices window*



Moving the HA pair (in the tree)

The NSE 3000 HA pair can be moved as a single unit only. This can be done by changing the Network and Site for the primary device. The devices in the pair cannot be moved individually. Moreover, the NSE 3000 device or HA pair can only be moved to a site that has no NSE 3000 devices. Moving to a network is not allowed.

Note

An HA pair of NSE 3000 devices shares the same NSE group. Consequently, the NSE group selection for the spare device is disabled.

Deleting an NSE 3000 device from the HA pair

If one of the NSE 3000 devices in a pair is deleted, the other NSE 3000 device becomes standalone.

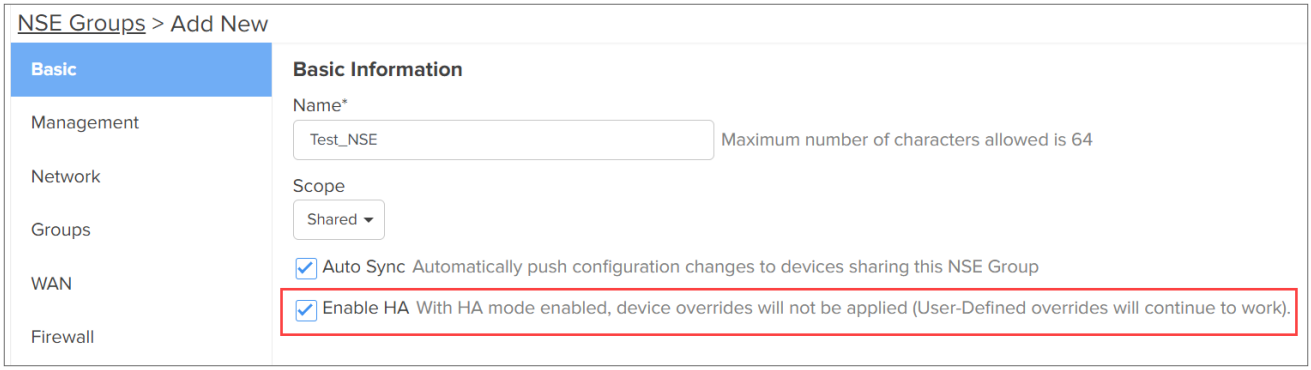
- When the primary device is deleted from the pair, the spare device becomes a standalone device and the pair's Tier-30 license is mapped to the spare device (instead of the primary device). Also, a configuration job for this standalone device with HA mode **Disable** is triggered.
- When the spare device is deleted from the pair, the primary device becomes a standalone device.
- When both primary and spare devices are deleted, a slot is released.

Deprecation of device overrides

The device overrides are removed from the Onboard page. The bulk overrides cannot be done for NSE 3000 devices.

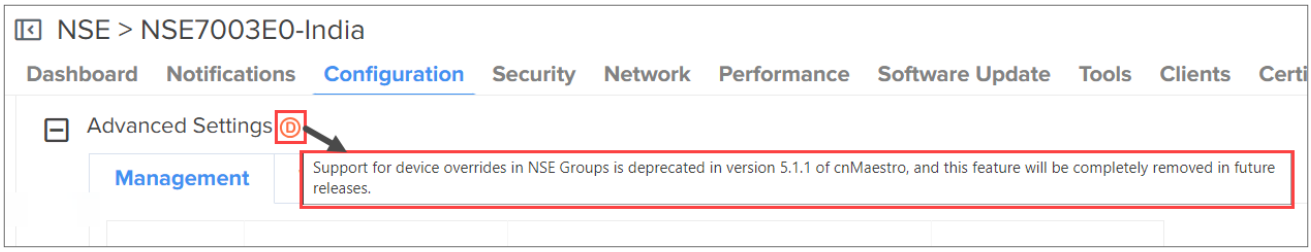
When HA is enabled in the NSE group, the device overrides in the device context are hidden.

Figure 387 *Device overrides are not applied when HA is enabled*



When HA is disabled in the NSE group, the deprecated icon (Ⓓ) is shown. Device overrides are being deprecated for NSE devices in the 5.1.1 version. When you hover the cursor over the deprecated (Ⓓ) icon, a message about the deprecation is displayed (as shown in Figure 388).

Figure 388 *A deprecation message*



Upgrading the firmware

When you upgrade the firmware on the primary device, the firmware on the spare device is automatically upgraded. This ensures that both primary and spare devices run the same version.

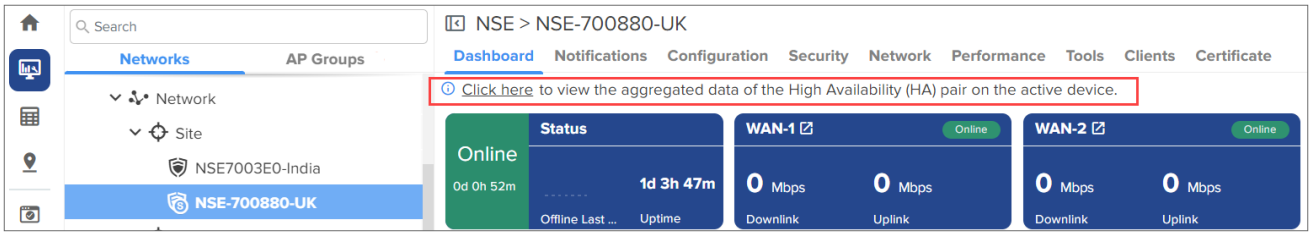
Note

The **Software Update** tab is available only for the primary device.

Viewing aggregated data of HA pair

In an HA pair, the active NSE 3000 device shows the aggregated data for the pair. In the spare NSE 3000 device, a banner provides a link to the active device's page (as shown in Figure 389) to view the aggregated data. The same banner is displayed under the **Security > Threats**, **Security > Vulnerabilities**, and **Clients** > **Local** tabs.

Figure 389 *Banner*



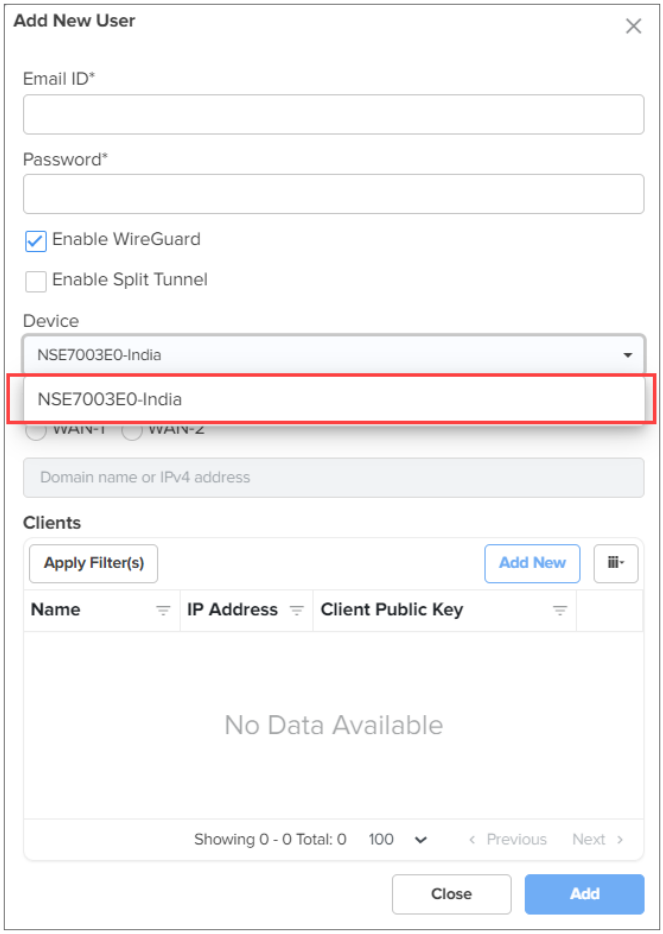
Note

- If the active device is offline, the aggregated data is not shown.

Creating Wireguard clients for NSE HA pair

When adding Wireguard clients from the **VPN** page, only the primary device is listed in the **Device** drop-down list (as shown in Figure 390).

Figure 390 *The Add New User window -Wireguard*

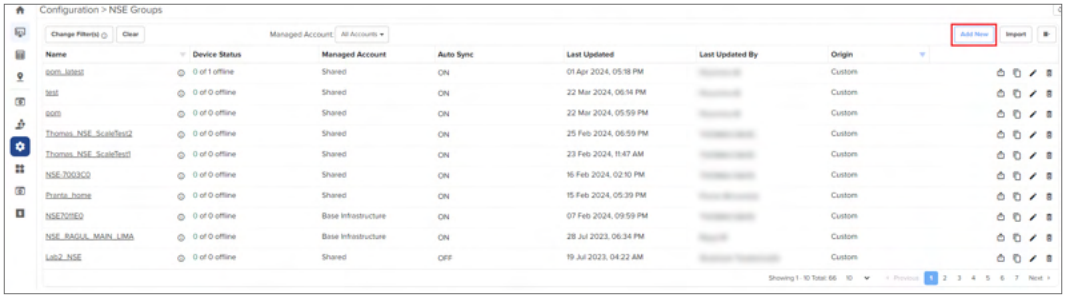


Configuring NSE 3000

To configure NSE 3000 devices, create configuration profiles called NSE Groups.

To create and configure a new NSE 3000 group, navigate to **Configuration** > **NSE Groups** and click **Add New**.

Figure 391 *Creating NSE groups*



For a new NSE group, you must configure parameters using the following tabs:

- Basic
- Management
- Network
- Groups
- WAN
- Firewall
- DNS
- Threat Protection
- VPN
- User-Defined Overrides

Basic

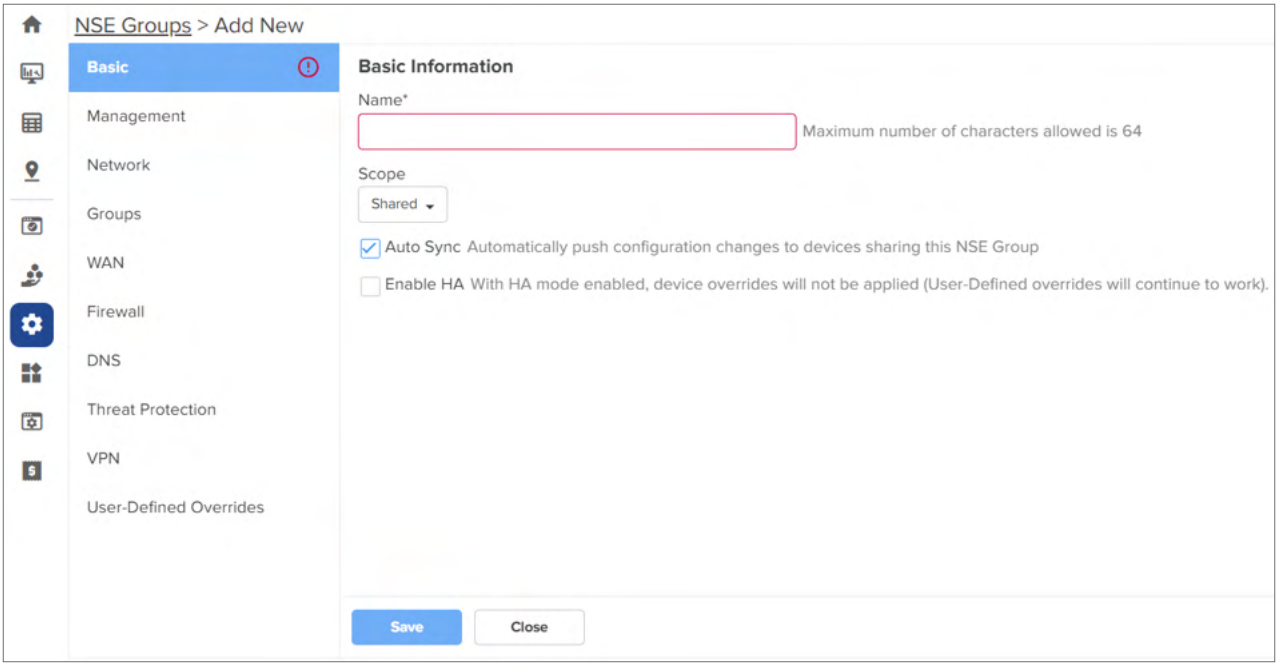
Using the **Basic** tab, you can configure basic group information, such as group name and group scope. You have the option to enable automatic synchronization of the configuration changes for devices associated with the NSE group.

To configure parameters on the **Basic Information** page, complete the following steps:

1. Navigate to **Configuration** > **NSE Groups** and click **Add.**

   The **Basic Information** page appears, as shown in Figure 392.

   Figure 392 *The Basic Information page*



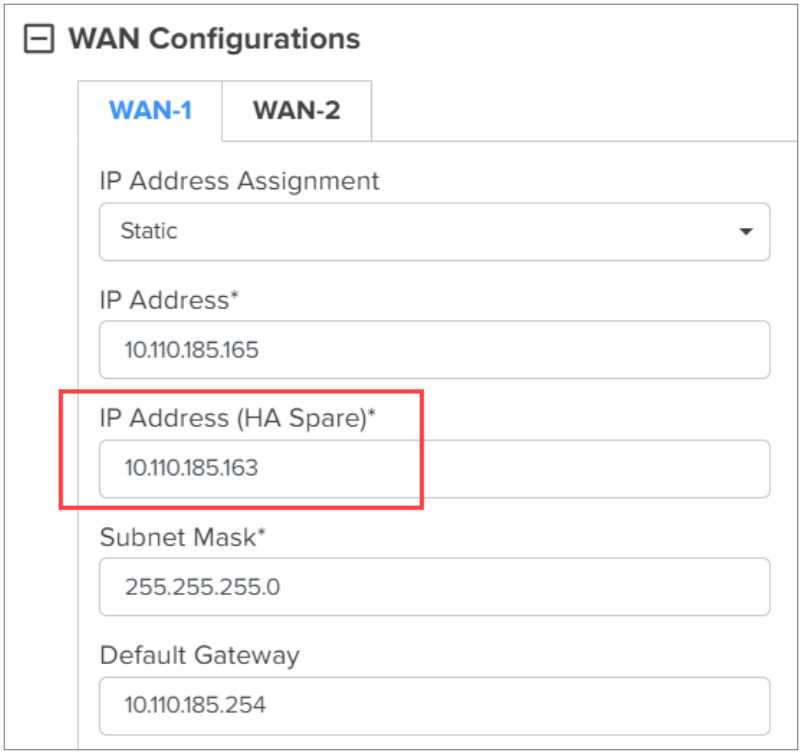
2. Configure the parameters, as described in Table 79.

   Table 79 *Parameters on the Basic Information page*

Parameter	Description
Name	Name for the NSE group.

Parameter	Description
	This parameter allows a maximum of 64 characters. This is a mandatory parameter.
Scope	Scope determines the availability of the NSE group across different tenant accounts. By default, the following options are supported: • **Shared -** Configured NSE group will be available to other tenant accounts. • **Basic Infrastructure -** Configured NSE group will be available only to the Basic Infrastructure user. Other tenant accounts will not have access to the NSE group.
Auto Sync	Specifies whether the configuration changes made to the NSE group are automatically applied to all devices associated with the group. By default, auto sync is enabled.
Enable HA	Enables or disables the HA. By default, this parameter is disabled. **Note**: When this parameter is enabled, you must configure the **IP Address (HA Spare)** parameter by selecting the **Static** option from the **IP Address Assignment** drop-down list in the **WAN Configurations** section of the **WAN** screen (as shown in Figure 393).

Figure 393 *The WAN Configurations section*



3. Click **Save**.

Management

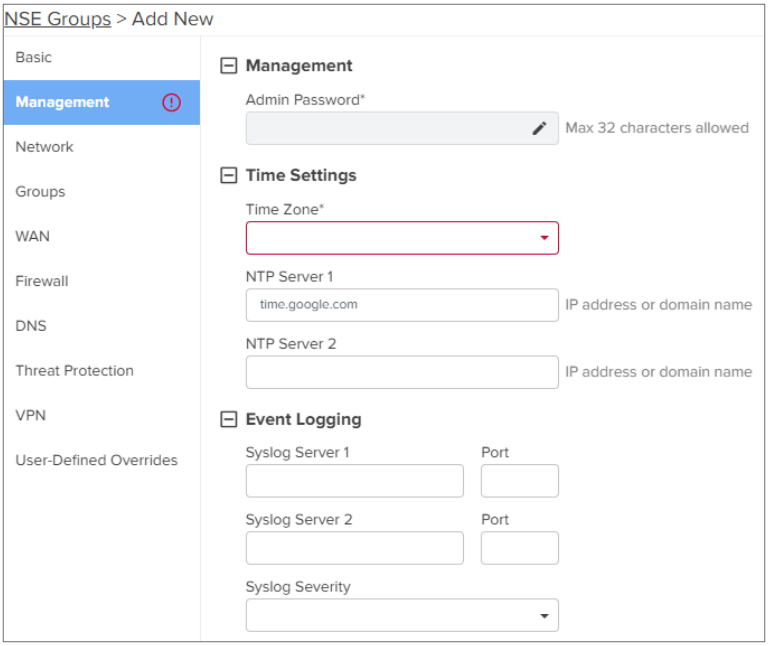
Using the **Management** tab, you can configure the profile-related parameters such as time settings and event logging.

To configure parameters on the **Management** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Management** tab.

   The **Management** page appears, as shown in Figure 394.

   Figure 394 *The Management page*



2. Configure the parameters, as described in Table 80.

   Table 80 *Parameters on the Management page*

Parameter	Description
On the Management page, there are **Management**, **Time Settings**, and **Event Logging** sections.	
Management	
Admin Password	The password used to authenticate the NSE 3000 users who access through SSH or web. This parameter allows a maximum of 32 characters. This is a mandatory parameter. **Note**: Click the edit icon to reset the password.
Time Settings	
Time Zone	The time zone based on the installation location of the device. Select an appropriate time zone from the drop-down list to ensure that the device clock is synchronized with the wall clock time.
NTP Server 1	The IPv4 address or domain name of the primary Network Time Protocol (NTP) server.
NTP Server 2	The IPv4 address or domain name of the secondary or a backup NTP server.
Event Logging	
Syslog Server 1	The IPv4 address or the domain name of the syslog server 1.
Port	The port number of the syslog server 1 to which the syslog messages are sent. Supported value: 1 to 65535.

Parameter	Description
Syslog Server 2	The IPv4 address or the domain name of the syslog server 2.
Port	The port number of the syslog server 2 to which the syslog messages are sent. Supported value: 1 to 65535.
Syslog Severity	The logs with the selected severity level that must be forwarded to the server. The following options are supported: • **Emergency (Level 0)** • **Alert (Level 1)** • **Critical (Level 2)** • **Error (Level 3)** • **Warning (Level 4)** • **Notice (Level 5)** • **Info (Level 6)** • **Debug (Level 7)**

3. Click **Save**.

Network

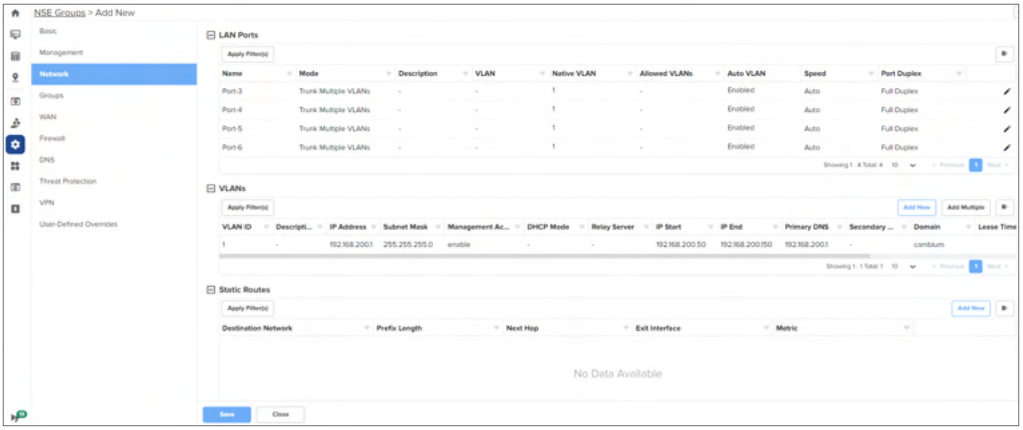
Using the **Network** tab, you can configure LAN ports, VLANs, and static routes.

To configure parameters on the **Network** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Network** tab.

   The **Network** page appears, as shown in Figure 395.

   Figure 395 *The Network page*



2. Configure the parameters, as described in Table 81.

   Table 81 *Parameters on the Network page*

Parameter	Description
On the Network page, there are **LAN Ports**, **VLANs**, and **Static Routes** sections.	
LAN Ports	

Parameter	Description
Click the edit icon to modify the configuration of the corresponding LAN port as shown in Figure 396, and click **Update** to apply the changes.	
Name	Name of the LAN port. This parameter cannot be modified.
Mode	The VLAN mode of the port. The following options are supported: • **Access Single VLAN**: An access port which places all traffic on its configured VLAN and only passes untagged traffic. • **Trunk Multiple VLANs**: A trunk port which allows the selected port to accept or pass 802.1Q tagged traffic.
Description	A brief description of the LAN port.
VLAN	This parameter is applicable only when the **Mode** parameter is set to **Access Single VLAN**. By default, VLAN value is 1. VLAN value can be in the range: 1 to 4094 This is a mandatory parameter.
Native VLAN	Indicates that the traffic on the native VLAN is untagged. This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**. The Native VLAN value can be in the range: 1 to 4094 This is a mandatory parameter.
Tag the native VLAN	This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**. When the**Tag the native VLAN** parameter is enabled, the native VLAN traffic is tagged with 802.1Q.
Allowed VLANs	This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**. This parameter supports a range or comma-separated list of VLANs. Example: 1-3 or 4, 10, 22
Auto VLAN	This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**. This parameter facilitates automatic assignment of VLANs in cnMatrix switches and access points (APs). When this parameter is enabled, the cnMatrix switches and APs use the Link Layer Discovery Protocol (LLDP) packets to obtain a list of VLANs for automatic assignment. **Note**: Auto VLAN works only with cnMatrix switches and access points (APs). It does not work with any third-party switches and APs. Auto VLAN allows cnMatrix switch to dynamically learn VLANs from an AP. The AP advertises the configured VLANs to the cnMatrix switch. The cnMatrix switch then advertises those VLANs to the uplink NSE 3000 device. This process ensures that VLANs are properly bridged. This parameter is enabled by default.
Auto VLAN Message	This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple**

Parameter	Description
Authentication	**VLANs**. This parameter enables authentication for the LLDP messages where the VLANs are advertised. This parameter is enabled by default.
Link Speed Advertisement	Indicates the port speed that must be configured for advertisement. Default: Auto The following options are supported: • **Auto** • **10 Mbps** • **100 Mbps** • **1000 Mbps**
Port Duplex	Specifies the mode of port communication. The following options are supported: • **Full Duplex** • **Half Duplex**
Port Speed	Specifies the port speed. Default: Auto The following options are supported: • **Auto** • **10 Mbps** • **100 Mbps** • **1000 Mbps**
Shutdown	Enables or disables the port. By default, this parameter is disabled.
VLANs **Note**: You can configure up to 128 VLANs. To add a new VLAN, click **Add New**. The **Add New VLAN** window appears, as shown in Figure 397. To edit an existing VLAN configuration, click the edit icon and modify the parameters in the **Edit VLAN** window. Finally, click **Update** to apply the changes.	
VLAN ID	Indicates the VLAN ID. The VLAN ID value can be in the range: 1 to 4094 This is a mandatory parameter.
Description	Displays the user-configured description for the VLAN.
IP Address	IPv4 address that is assigned to the VLAN. This is a mandatory parameter.
Subnet Mask	Subnet mask that is assigned to the VLAN. This is a mandatory parameter.

Parameter	Description
Management Access	Indicates whether the management access is enabled or disabled. By default, this parameter is enabled.
Enable Rate Limit	Indicates whether the rate limit is enabled or disabled. By default, this parameter is disabled. When you select the **Enable Rate Limit** check box, the **Rate Limit** parameter appears**.**
Rate Limit	Specifies the rate of requests sent or received. This parameter appears only when you enable the **Enable Rate Limit** parameter. This parameter supports only integer values. This is a mandatory parameter.
DHCP mode	Specifies the DHCP mode. The following options are supported: • **None** • **DHCP Server -** When you select this option, the DHCP server-related parameters appear. • **DHCP Relay -** When you select this option, the **Relay Server IP address** parameter appears.
DHCP Server In addition to the below parameters, you must also configure the parameters in the **DHCP Options** and **MAC Binding List** sections, as shown in Figure 398.	
Start IP address	Starting IPv4 address in the range. This is a mandatory parameter.
End IP address	Ending IPv4 address in the range. This is a mandatory parameter.
Primary DNS	The primary DNS server for clients on the network. If the DNS server option is enabled on the NSE, the IPv4 address configured for the VLAN can be provided as the DNS server for the network.
Secondary DNS	The secondary DNS server for clients on the network.
Domain	The DNS search domain for the network.
Lease Time	The DHCP lease expiry time for the DHCP pool (in days, hours, and minutes). This is a mandatory parameter.
DHCP Options NSE allows configuration of standard and custom DHCP options. To add a new DHCP option, click **Add New**. The **Add New DHCP Option** window appears, as shown in Figure 399. To edit an existing DHCP option, click the edit icon and modify the parameters in the **Edit DHCP Option** window. Finally, click **Update** to apply the changes.	
Option	The following DHCP options are supported:

Parameter	Description
	• **Log server(7)** • **Domain name(15)** • **NTP server(42)** • **Vendor specific information(43)** • **Vendor class identifier(60)** • **TFTP server name(66)** • **Boot file name(67)** • **Proxy auto config(252)** • **Custom** This is a mandatory parameter.
Code	A value for the code. This parameter allows a maximum value of 254. This is a mandatory parameter.
Type	The following options are supported: • **Text** • **IP Address** • **Integer** This is a mandatory parameter.
Value	A value in ASCII. This is a mandatory parameter.
MAC Binding List For every DHCP pool configured, the user can bind the client MAC address with an IPv4 address from the network. This enables the client to obtain the same IPv4 address whenever they connect to the NSE 3000 device. Following parameters are required to create the binding list: • MAC address of the client • IPv4 address from the configured pool When you set **MAC** and **IP address** fields and click **Add**, the binding of MAC and IP address is added. **Note**: Upto 200 MAC to IP address bindings are supported per DHCP pool. **Note**: When you bind, the binding IP address should be outside the DHCP pool range. To add a new MAC binding, click **Add New**. The **Add New MAC Binding** window appears, as shown in Figure 400. To edit an existing MAC binding, click the edit icon and modify the parameters in the **Edit MAC Binding** window. Finally, click **Update** to apply the changes.	
MAC	The MAC address of the client. This is a mandatory parameter.

Parameter	Description
IP Address	The IPv4 address that must be assigned to the client. This is a mandatory parameter.
Description	Displays the user-configured description.
Import	Imports the MAC bindings. **Note**: The CSV file that you import must be in the three-column format, for example, MAC, IP address, and Description. To import MAC bindings, click **Import**. The **Import MAC Bindings** window appears, as shown in Figure 401.
Replace existing list	Indicates whether the imported bindings will overwrite the existing list or append to the list. • If enabled, the imported bindings will overwrite the existing list • If disabled, the imported bindings will append to the existing list. By default, this parameter is enabled.
Export	Exports the configured bindings list. The following options are supported: • **Export all as CSV** • **Export page as CSV** To export MAC bindings, click **Export**. The export options appear, as shown in Figure 402.
DHCP Relay	Indicates whether the DHCP relay unicasts the DHCP request to an external DHCP server. This is a mandatory parameter.
Relay Server IP address	IPv4 address of the external DHCP server. This is a mandatory parameter.
Static Routes To add a new route, click **Add New**. The **Add New Route** window appears, as shown in Figure 403. To edit an existing route, click the edit icon and modify the parameters in the **Edit Route** window. Finally, click **Update** to apply the changes.	
Destination Network	The IPv4 address of the destination network. This is a mandatory parameter.
Prefix Length	The prefix length for the network address. This parameter supports integer values and a maximum value of 32. This is a mandatory parameter.
Next Hop	The next hop IPv4 address for the route. This is a mandatory parameter.
Exit Interface	The exit interface through which the next hop is reachable. This is a mandatory parameter.

Parameter	Description
Metric	The metric for the route.
To add multiple VLANs, click the **Add Multiple** button. The **Add Multiple VLANs** window appears, as shown in Figure 404. To edit an existing VLAN configuration, click the edit icon and modify the parameters in the **Edit VLAN** window. Finally, click **Update** to apply the changes.	
Description	Displays the user-configured description for the VLAN.
First VLAN ID	Indicates the first VLAN ID. The supported VLAN ID value range is between 1 and 4094. This is a mandatory parameter.
Number of VLANs	Indicates the number of VLANs that you want to add. **Note**: You can configure up to 128 VLANs. This is a mandatory parameter.
Subnet The following options are supported: • **IP Address and Netmask** - When you select this option, the **IP address** and **Netmask** options appear. • **Hosts per subnet** - When you select this option, the **First IP Address** and **Hosts per subnet** options appear.	
IP address	The IPv4 address of the first VLAN. This is a mandatory parameter.
Netmask	The netmask of the subnet. This is a mandatory parameter.
First IP Address	The first IPv4 address of the subnet. This is a mandatory parameter.
Hosts per subnet	The number of hosts that you want for the subnet. This is a mandatory parameter.
DHCP mode	Specifies the DHCP mode. The following options are supported: • **None** • **DHCP Server -** When you select this option, the DHCP server-related parameters appear. • **DHCP Relay -** When you select this option, the **Relay Server IP address** parameter appears.
Lease Time	The DHCP lease expiry time for the DHCP pool (in days, hours, and minutes). This is a mandatory parameter.
DHCP Options NSE allows configuration of standard and custom DHCP options. To add a new DHCP option, click **Add New**. The **Add New DHCP Option** window appears, as shown in	

Parameter	Description
Figure 399. To edit an existing DHCP option, click the edit icon and modify the parameters in the **Edit DHCP Option** window. Finally, click **Update** to apply the changes.	
Option	The following DHCP options are supported: • **Log server(7)** • **Domain name(15)** • **NTP server(42)** • **Vendor specific information(43)** • **Vendor class identifier(60)** • **TFTP server name(66)** • **Boot file name(67)** • **Proxy auto config(252)** • **Custom** This is a mandatory parameter.
Code	A value for the code. This parameter allows a maximum value of 254. This is a mandatory parameter.
Type	The following options are supported: • **Text** • **IP Address** • **Integer** This is a mandatory parameter.
Value	A value in ASCII. This is a mandatory parameter.
DHCP Relay	Indicates whether the DHCP relay unicasts the DHCP request to an external DHCP server. This is a mandatory parameter.
Relay Server IP address	IPv4 address of the external DHCP server. This is a mandatory parameter.

Figure 396 *The Edit Port window*

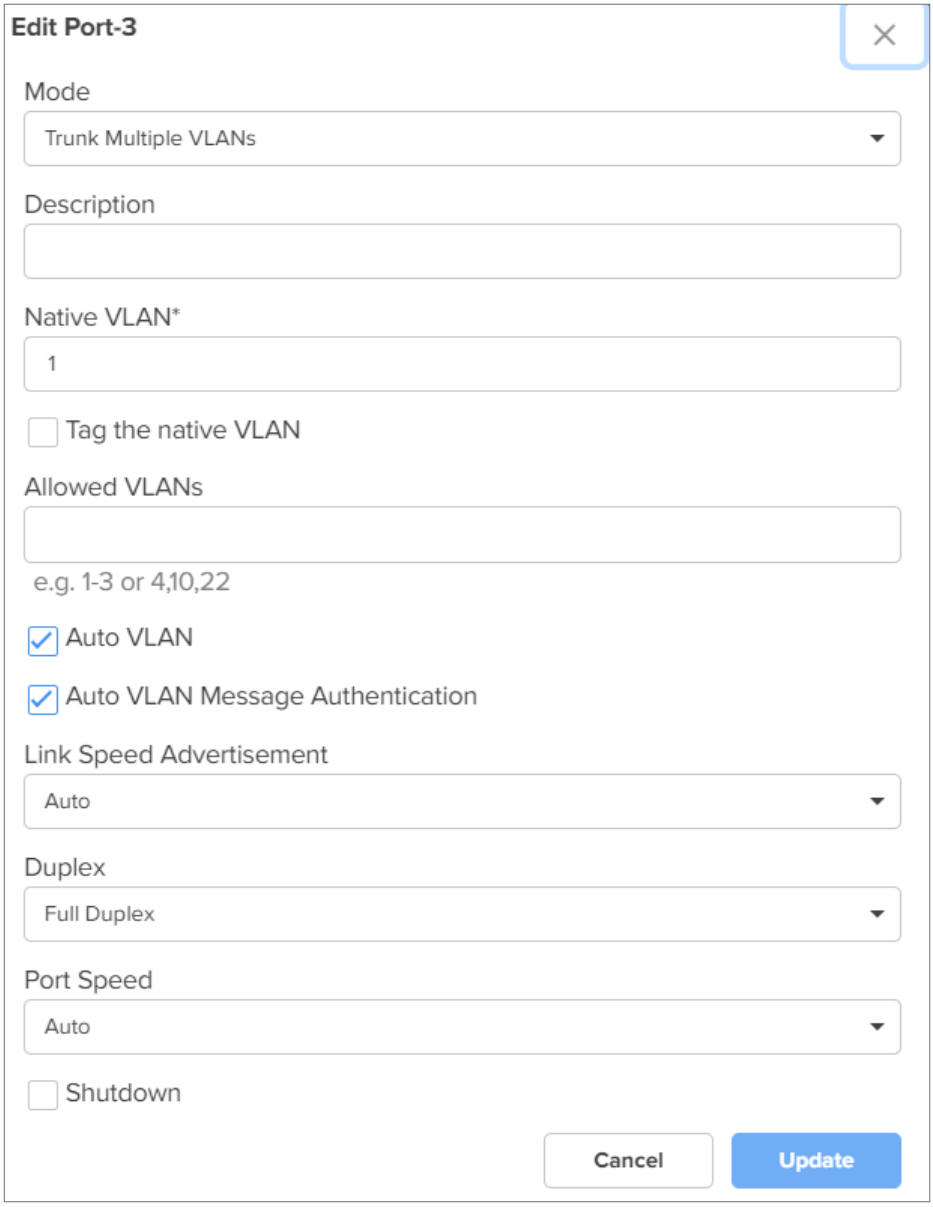


Figure 397 *The Add New VLAN window*

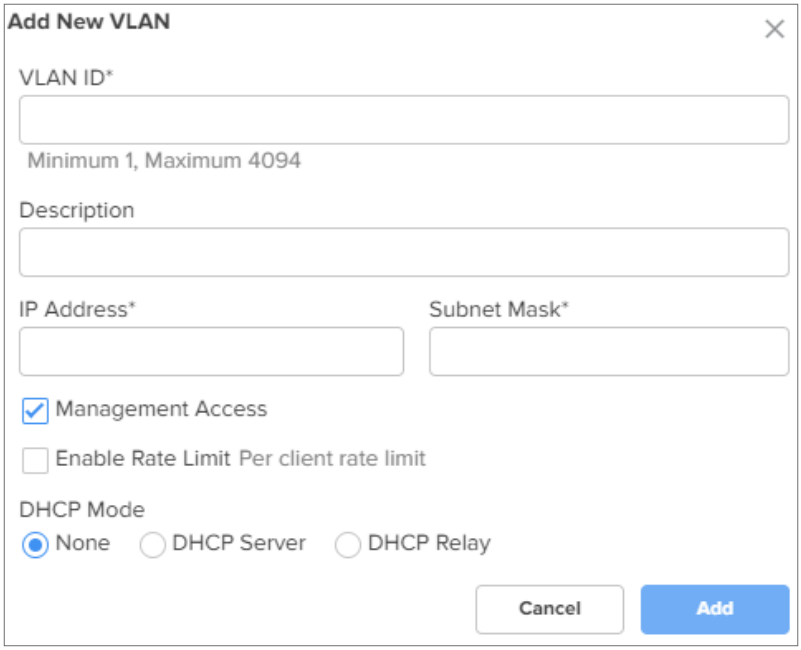


Figure 398 *DHCP Options and MAC Binding List*

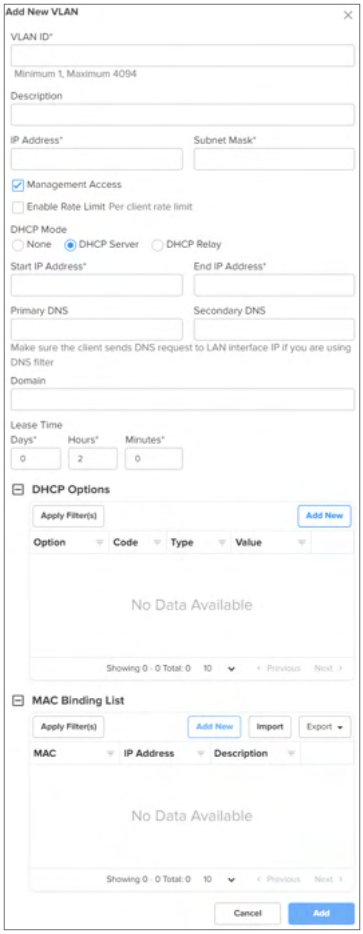


Figure 399 *The Add New DHCP Option window*

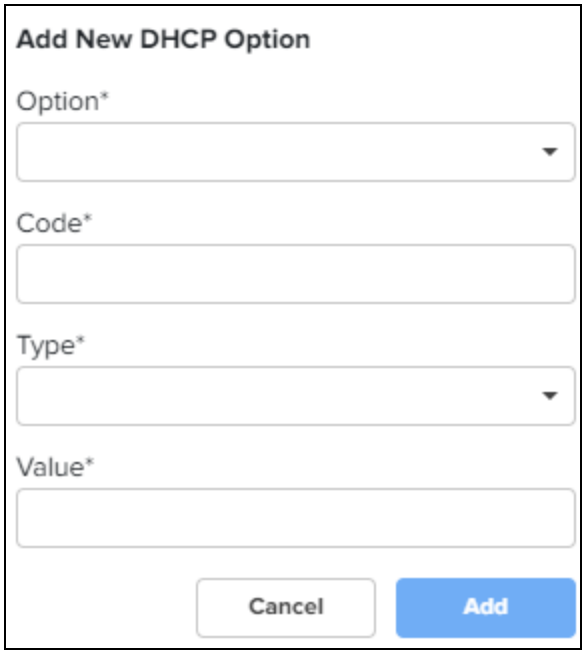


Figure 400 *The Add New MAC Binding window*

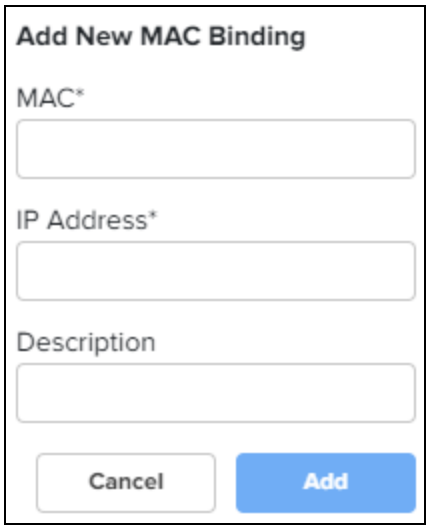


Figure 401 *The Import option in MAC Binding List*

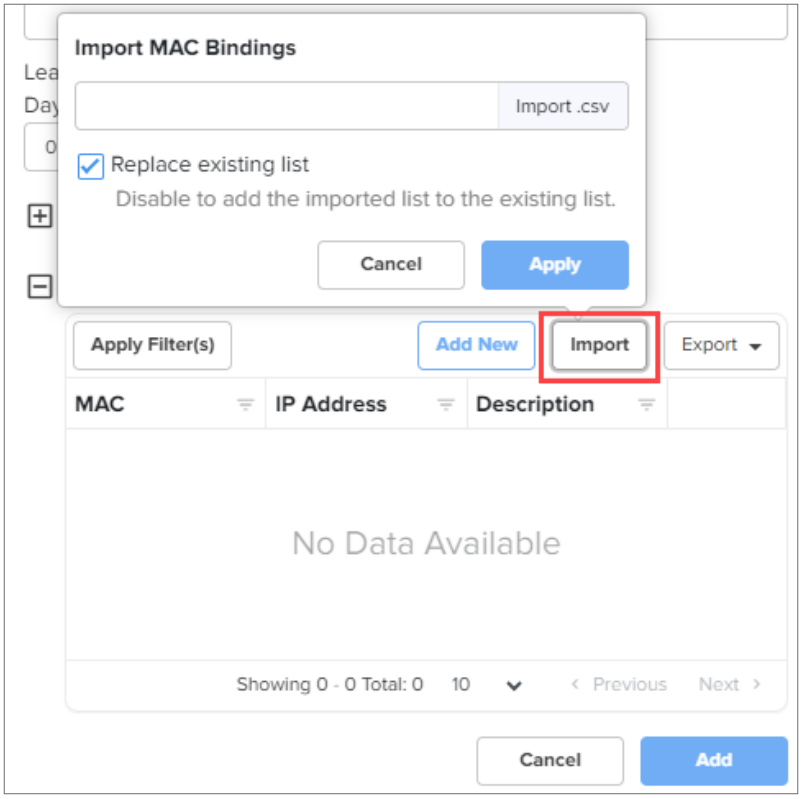


Figure 402 *The Export option in MAC Binding List*

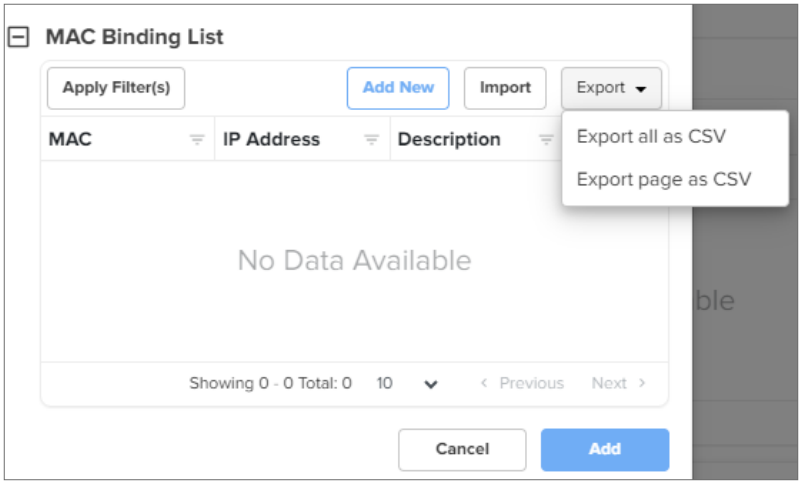


Figure 403 *The Add New Route window*

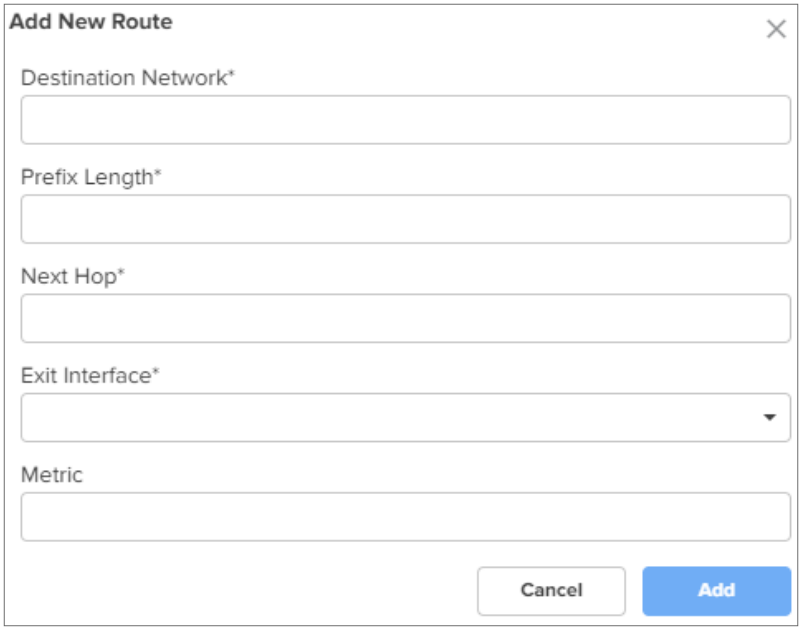
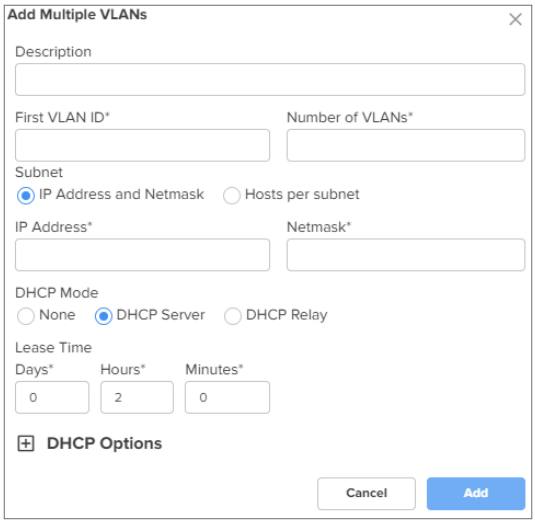


Figure 404 *The Add Multiple VLANs window*



3. Click **Save**.

Groups

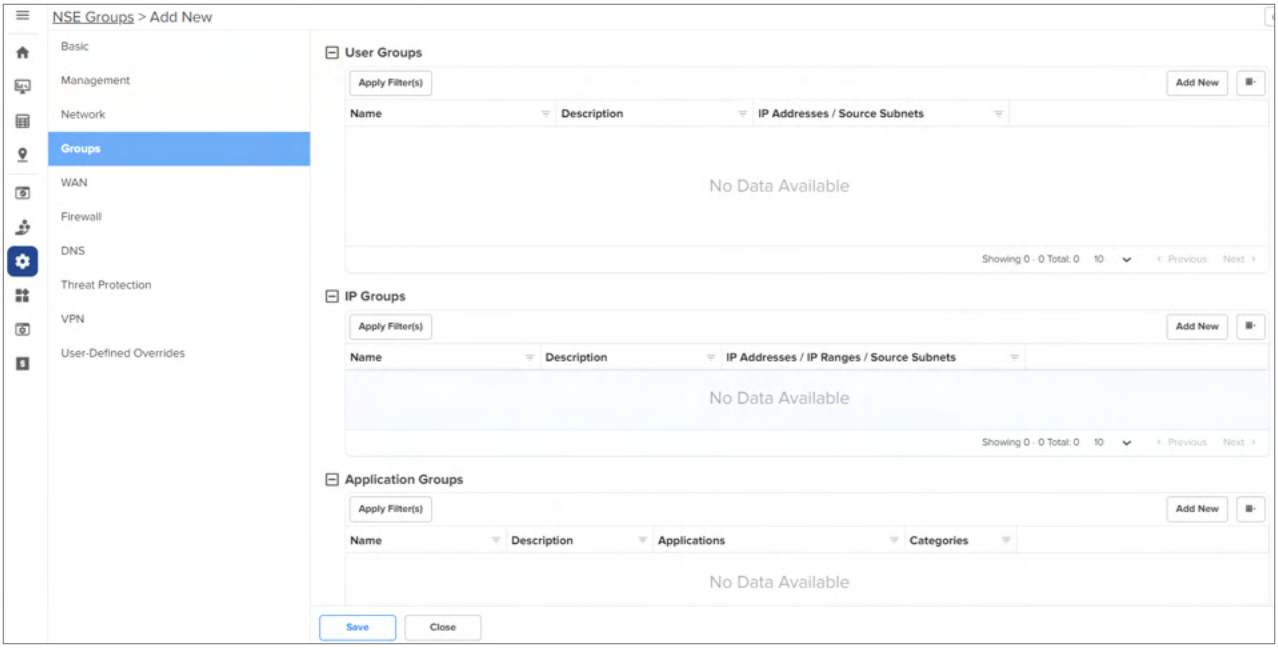
Using the **Groups** tab, you can configure user groups, IP groups, and application groups.

To view the **Groups** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Groups** tab.

   The **Groups** page appears, as shown in Figure 405.

Figure 405 *The Groups page*



2. Configure the parameters, as described in Table 82.

Table 82 *Parameters on the Groups page*

Parameter	Description
On the Groups page, there are **User Groups**, **IP Groups**, and **ApplicationGroups** sections.	
User Groups User groups are used to group locally configured networks and these groups can be used to associate with policies, especially application rules or DNS rules. To add a new user group, click **Add New**. The **Add User Group** window appears, as shown in Figure 406. To edit a user group, click the edit icon and modify the parameters in the **Edit User Group** window. Finally, click **Update** to apply the changes.	
Name	Name for the user group. This is a mandatory parameter.
Description	Description for the user group.
IP Addresses/Source Subnets	IPv4 addresses or source subnets for the user group. This is a mandatory parameter.
IP Groups IP groups are used to group networks originating from the WAN, and can be used to attach port forwarding rules. To add a new IP group, click **Add New**. The **Add IP Group** window appears, as shown in Figure 407. To edit an IP group, click the edit icon and modify the parameters in the **Edit IP Group** window. Finally, click **Update** to apply the changes.	

Parameter	Description
Name	Name for the IP group.
Description	Description for the IP group.
IP Addresses/IP Ranges/Source Subnets	IPv4 addresses, IP ranges, or source subnets for the IP group. This is a mandatory parameter.
Application Groups Application groups are used to group applications by using application names or categories, which can then be attached to a policy for permitting or denying access. To add a new application group, click **Add New**. The **Add New Application Group** window appears, as shown in Figure 408. To edit an application group, click the edit icon and modify the parameters in the **Edit Application Group** window. Finally, click **Update** to apply the changes.	
Name	Name for the application group.
Description	Description for the application group.
Applications To add applications to the application group, select the required application(s) from the drop-down list and click **Add New**. The selected applications are added in the **Name** list.	
Application Name	Applications for the new application group.
Categories To include categories for the new application group, select the required categories.	
Categories	Categories for the new application group.

Figure 406 *The Add User Group window*

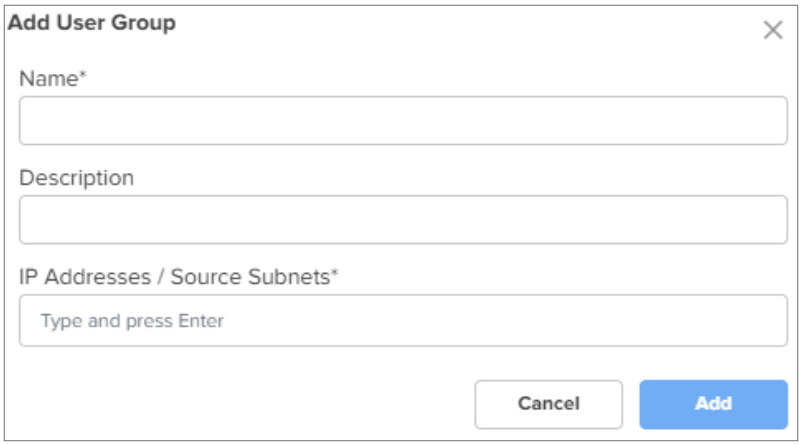


Figure 407 *The Add IP Group window*

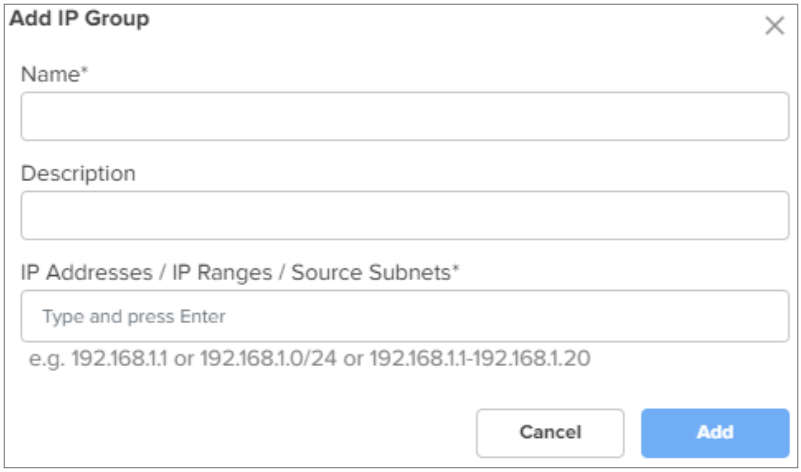
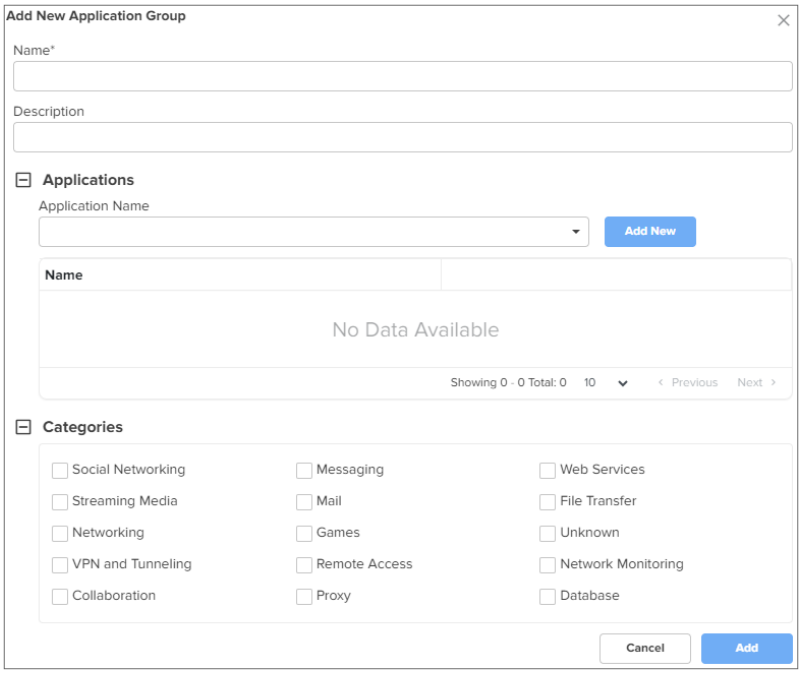


Figure 408 *The Add New Application Group window*



3. Click **Save**.

WAN

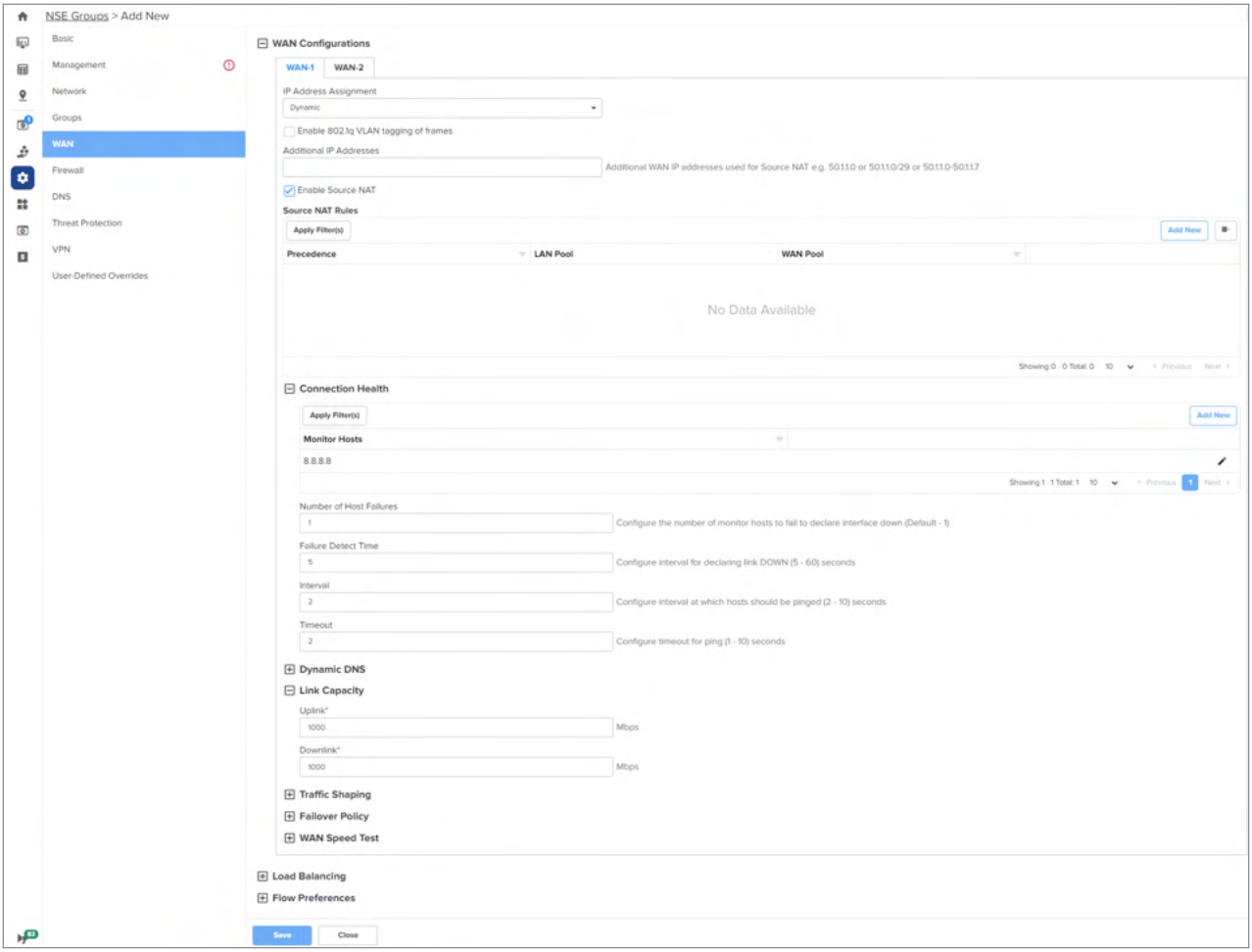
Using the **WAN** tab, you can configure the settings related to the WAN interface.

To configure parameters on the WAN page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **WAN** tab.

   The **WAN** page appears.

Figure 409 *The WAN page*



2. Configure the parameters, as described in Table 83.

Table 83 *Parameters on the WAN page*

Parameter	Description
On the WAN page, there are **WAN Configurations**, **LoadBalancing**, and **Flow Preferences** sections.	
WAN Configurations In this section, you can configure the parameters in **Connection Health**, **Dynamic DNS**, **Link Capacity**, **Traffic Shaping**, **Failover Policy**, and **WAN Speed Test** subsections. The same parameters appear in both **WAN-1** and **WAN-2** tabs.	
IP Address Assignment	Determines the mode of IP address assignment for the WAN interface. The following options are supported: • **Dynamic**: Dynamically learn the IP address and DNS from the DHCP server. • **Static**: Manually configure the IP address, gateway, and DNS server IP provided by the service provider. • **PPPoE**: When you configure PPPoE, you must provide the username and password of the service provider. While the account name and service name are not mandatory configurations, they may be required if the service provider enforces it. By default,

Parameter	Description
	the MTU is set to 1492 and the TCP MSS clamping is enabled. If required, you can also tag the packet on the WAN link to send.
Enable 802.1q VLAN tagging of frames	When this parameter is enabled, 802.1Q tag is inserted with configured VLAN ID for all the packets going out of the WAN interface. By default, this parameter is disabled.
VLAN ID	This parameter is applicable only when **Enable 802.1q VLAN tagging of frames** check box is selected. VLAN ID range: 1 and 4094. This is a mandatory parameter. When the 802.1Q header is configured, all transmitted frames are expected to include the 802.1Q header with the same VLAN ID.
Following parameters appear when you select **Static** from the **IP Address Assignment** drop-down list.	
IP Address	The IPv4 address of the WAN interface. This is a mandatory parameter.
IP Address (HA Spare)	This parameter appears only when **Enable HA** check box is selected from the **Basic** screen. The IPv4 address of the HA spare. This is a mandatory parameter.
Subnet Mask	The subnet mask for the IPv4 address of the WAN interface. This is a mandatory parameter.
Default Gateway	The IPv4 address of the default gateway for the WAN interface.
Primary DNS	The IPv4 address of primary upstream DNS server on this interface. This is a mandatory parameter.
Secondary DNS	The IPv4 address of secondary upstream DNS server on this interface.
Following parameters appear when you select **PPPoE** from the **IP Address Assignment** drop-down list.	
Account Controller Name	Name of the account controller. This parameter allows a maximum of 32 characters. This parameter is optional.
Service Name	Indicates the service name of the Account Controller. This parameter allows a maximum of 32 characters. The service name configuration is optional.
User	User name for PPPoE authentication. This is a mandatory parameter.
Password	Password for PPPoE authentication. This parameter is optional.
MTU	MTU for PPPoE interface. MTU ranges from 500 to 1492 bytes.

Parameter	Description
	Default: 1492 bytes.
TCP MSS Clamping	Indicates whether TCP MSS Clamping is enabled or disabled. By default, this parameter is enabled.
Additional IP Addresses	WAN IP addresses that are available for source NAT. **Note**:The WAN interface supports up to 16 IP addresses.
Enable Source NAT	Indicates whether the source NAT is enabled or disabled. When enabled, NSE 3000 device will replace the source IP address of the traffic routed from LAN to WAN with the WAN interface IP address. By default, this parameter is enabled.
Source NAT Rules Allows user to configure source NAT rules. User can choose the WAN IP addresses from the Additional IP Address for source NAT. User can configure WAN IP address(es) of their choice for source NAT. By default, all the LAN users' traffic will be source NATed to the configured WAN IP address(es). When LAN pool is configured, the traffic from the specified LAN networks will be source NATed to the configured WAN IP address(es). **Note**: Source NAT Rules supports up to 16 rules per WAN. To add a new source NAT, click **Add New**. The **Add New Source NAT Rule** window appears, as shown in Figure 410.	
Precedence	The precedence value for the source NAT rule. The precedence value can be between 1 and 150. This is a mandatory parameter.
LAN Pool	The following options are supported: • **All** • **IP Group** • **IP Address / Source Subnet**
WAN Pool	The following options are supported: • **Single IP Address** • **Multiple IP Addresses**
IP Address	IPv4 address for the WAN pool. Applicable only when **Single IP Address** option is selected.
Start IP	Starting IP address in the range. This parameter is applicable only when **Multiple IP Addresses** option is selected. This is a mandatory parameter.
End IP	Ending IP address in the range. This parameter is applicable only when **Multiple IP Addresses** option is selected. This is a mandatory parameter.
IP Group	Select the IP group for the source NAT. IP groups are the ones that you configure in the **Groups** > **IP Groups** section.

Parameter	Description
	This parameter is applicable only when **IP Group** option is selected. This is a mandatory parameter.
IP Address / Source Subnet	This parameter is applicable only when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.
Connection Health This section is configured to monitor the WAN connection health. Click the edit icon to modify the **Monitor Host** configuration, as shown in Figure 411. Finally, click **Update** to apply the changes. To add a new monitor host, click **Add New**. The **Add New Monitor Host** window appears, as shown in Figure 412.	
Monitor Host	The hosts used to monitor and collect network traffic data. Default: 8.8.8.8 This is a mandatory parameter.
Number of Host Failures	The number of monitor hosts that fail to declare the link down. Default value: 1 The maximum number of monitor hosts that can be configured to fail is 5.
Failure Detect Time	The time period (in seconds) during which the device waits for the response from the monitored host before declaring the link down. Default: 5. Range: 5 to 60
Interval	The time interval (in seconds) used by the device to check and reach the monitor hosts. Default: 2. Range: 2 to 10
Timeout	The time period (in seconds) the device waits for a response from the monitor host after which the connection is timed out. Default: 2. Range: 1 to 10
Dynamic DNS	
Enable Dynamic DNS	Indicates whether the dynamic DNS for the interface is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when **Enable Dynamic DNS** check box is selected**.**	
DNS Provider	The following options are supported: • **Cloudflare:** Requires secret/access token and zone configuration. In the Cloudflare account, navigate to **Profile** > **API Tokens** to create a token. Following is the recommended setting: ◦ Permissions: Zone, DNS, Edit ◦ ZoneResource: Include, Specific Zone, <zone name> • **Godaddy:** Requires API key, secret/access token, and zone configuration. In the Godaddy account, create an API key at https://developer.godaddy.com/keys

Parameter	Description
	• **Hetzner:** Requires secret/access token and zone configuration. In the Hetzner account, navigate to **Profile** > **API Tokens** and create an access token. • **Namecheap:** Requires password and zone configuration**.** 1. In the Namecheap account, navigate to **Domains** > **Free DNS** to manage external domains. 2. Before you update/create a record, a new record of type **A** must exist. To create a record, navigate to the dashboard, and then navigate to **Products** > **Advanced DNS**. Add a new record of type **A**. On the same page, enable Dynamic DNS and note the password. • **Noip:** Requires server name, username, and password configuration**.** • **Route53:** Requires API key, secret/access token, and zone configuration**.** 1. In the Route 53 account, navigate to **route53** > **Hosted Zones** > **Create Hosted Zone** to create a zone. Use type Public hosted zone. Note the name servers in hosted zone details and the hosted zone ID. 2. Navigate to **IAM** > **Users** > **Create user**. Select attach policies directly. Create a policy. The following is an example of a policy: { "Version": "2012-10-17", "Statement": [{ "Sid": "", "Effect": "Allow", "Action": ["route53:ListResourceRecordSets", "route53:GetChange", "route53:ChangeResourceRecordSets"], "Resource": ["arn:aws:route53:::hostedzone/<ZONE_ID>", "arn:aws:route53:::change/*"] }, { "Sid": "", "Effect": "Allow",

Parameter	Description
	"Action": ["route53:ListHostedZonesByName", "route53:ListHostedZones"], "Resource": "*" }] } 3. Replace ZONE_ID in the policy with the previously noted zone id. Select the new policy for the previously created user. 4. To create access key, navigate to users, select the user, **Security Credentials** > **Create Access Key**. • **Porkbun:** Requires API key, secret/access token, and zone configuration**.** In the Porkbun account, navigate to **Account** > **API Access** to create a token. Additionally, the domain configuration much be changed to enable API access. • **Dyn:** Oracle Dyn requires server name, username, and password configuration**.** • **DynDNS2 compliant:** Requires server name, username, and password configuration**.** By default, **Noip** option is selected.
DNS Hostname	Indicates the DNS host name.
Link Capacity	
Uplink	The WAN uplink capacity in Mbps. Default:1000. Range: 1 to 1000 This is a mandatory parameter.
Downlink	The WAN downlink capacity in Mbps. Default:1000. Range: 1 to 1000 This is a mandatory parameter.
Traffic Shaping **Note**: Traffic Shaping supports up to 16 rules per WAN. To add a new traffic shaping rule, click **Add New**, the **Add New Traffic Shaping Rule** window appears, as shown in Figure 413.	
Enable Traffic Shaping	Indicates whether traffic shaping is enabled or disabled. By default, this parameter is disabled.
Precedence	The precedence value for the traffic shaping rule. The precedence value can be between 1 and 150. This is a mandatory parameter.
Description	Displays a user-configured description for the traffic shaping rule.

Parameter	Description
Uplink Bandwidth	Indicates the uplink bandwidth in Mbps. Range: 1 to 1000 This is a mandatory parameter.
Downlink Bandwidth	Indicates the downlink bandwidth in Mbps Range: 1 to 1000 This is a mandatory parameter.
DSCP	Differentiated Services Code Point (DSCP) can range from 0 to 63, with 0 being the lowest priority and 63 being the highest priority.
Type	Indicates the type of filter rule. The following options are supported: • **IP Based** – Allows you to configure **Protocol** parameter as **TCP**, **UDP**, or **any**. • **Application Based** – Allows you to configure **Deep Packet Inspection (DPI) Type** parameter as **Application** or **Category**.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **Application** – Specific type of application within a category. • **Category** – All applications belonging to a category (For example, Social Messaging). This is a mandatory parameter.
DPI Application	This parameter is applicable only when **Deep Packet Inspection (DPI) Type** parameter is set to **Application**. This is a mandatory parameter.
DPI Category	This parameter is applicable only when **Deep Packet Inspection (DPI) Type** parameter is set to **Category**. This is a mandatory parameter.
Protocol	This parameter is applicable only when **Type** parameter is **IP Based**. The following options are supported: • **TCP** – Match TCP traffic. • **UDP** – Match UDP traffic. • **any** – Match any of the above protocol traffic.
Source IP Address	The source IPv4 address for the shaping rule. This is a mandatory parameter.
Mask	The subnet mask for the shaping rule. This is a mandatory parameter.
Port	Displays the source port from which IPv4 address messaging is sent. This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the shaping rule. This is a mandatory parameter.

Parameter	Description
Mask	The subnet mask for the shaping rule. This is a mandatory parameter.
Port	Displays the destination port to which IPv4 address messaging is sent. This is a mandatory parameter.
Failover Policy **Note**: Failover Policy supports up to 32 rules per WAN. To add a new failover policy, click **Add New**. The **Add New Failover Policy** window appears, as shown in Figure 414.	
Enable Failover Policy	Indicates whether failover policy is enabled or disabled. By default, this parameter is disabled.
Precedence	The precedence value for the failover policy. The precedence value can be between 1 and 150. This is a mandatory parameter.
Description	A description for the policy.
Action	By default, this parameter is disabled.
Type	The type of failover rule. The following options are supported: • **IP Based** – Allows you to configure the **Protocol** parameter as **TCP**, **UDP**, or **any**. • **Application Based** – Allows you to configure **Deep Packet Inspection (DPI)Type** parameter as **Application**, **Category**, or **Application Group**.
Protocol	This parameter is applicable only when **Type** parameter is **IP Based**. The following options are supported: • **TCP** – Match TCP traffic. • **UDP** – Match UDP traffic. • **any** – Match any of the above protocol traffic.
Source IP Address	The source IPv4 address for the failover rule. This is a mandatory parameter.
Mask	The subnet mask for the failover rule. This is a mandatory parameter.
Port	The source port for the failover rule. This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the failover rule. This is a mandatory parameter.
Mask	The subnet mask for the failover rule. This is a mandatory parameter.
Port	Displays the destination port for the failover rule.

Parameter	Description
	This is a mandatory parameter.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **Application** – Specific type of application within a category. • **Category** – All applications belonging to a category (For example, Social Messaging). • **Application Group -** All applications belonging to a group. This is a mandatory parameter.
Apply to	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **All** • **User Group** • **IP Address / Source Subnet**
User Group	This parameter is applicable when **User Group** option is selected. This is a mandatory parameter.
IP Address / Source Subnet	This parameter is applicable when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.
WAN Speed Test	
Enable WAN Speed Test	Enable or disable the WAN speed test. By default, this parameter is disabled.

Figure 410 *The Add New Source NAT Rule window*

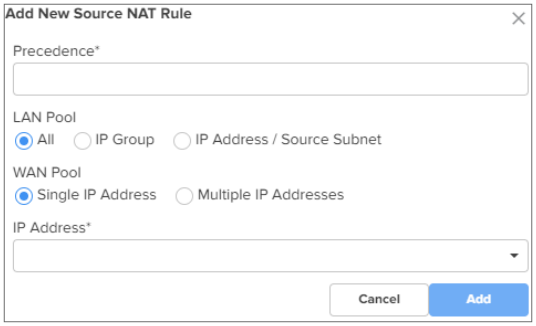


Figure 411 *The Edit Monitor Host window*

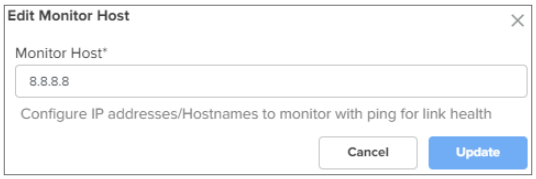


Figure 412 *The Add New Monitor Host window*

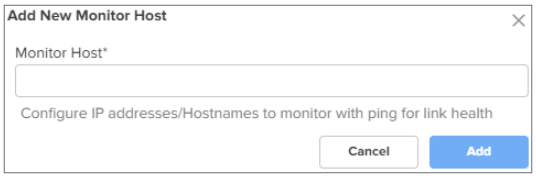


Figure 413 *The Add New Traffic Shaping Rule window*

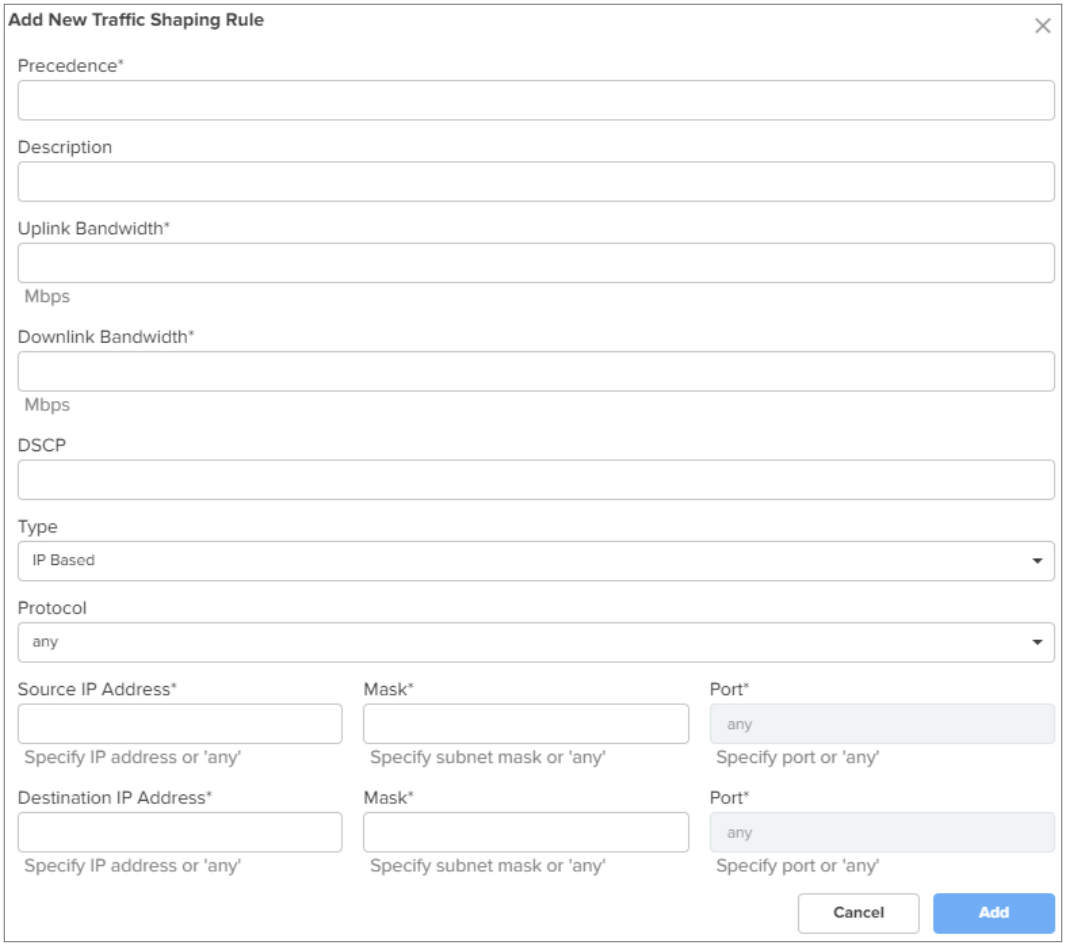
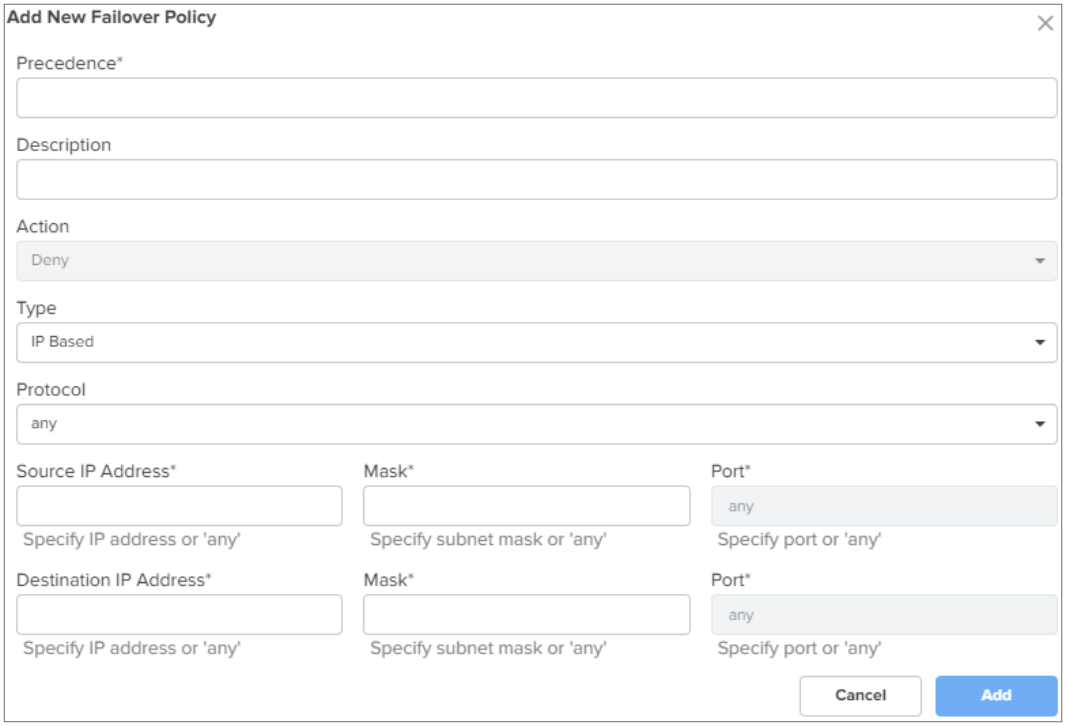


Figure 414 *The Add New Failover Policy window*



3. Expand the **Load Balancing** section and configure the parameters, as described in Table 84.

Table 84 *Parameters on the Load Balancing section*

Parameter	Description
Load Balancing	
WAN-1 Mode	Determines the load balancing mode of device. By default, the **WAN-1 Mode** parameter is set to **Shared**. The following options are supported: • **Shared** – Enables the WAN link to actively forward a percentage of user traffic. The percentage of user traffic on this link is set via the **Traffic Share Percentage** parameter. • **Backup** – The WAN link forwards user traffic only when all of the Shared WAN interfaces are down. • **Disabled** – Disables the WAN link from participating in WAN link load sharing, and failover procedures.
Traffic Share Percentage	For the **Shared** mode, the traffic share percentage must be between 5 and 100. This is a mandatory parameter.
WAN-2 Mode	Determines the load balancing adjust mode of device. By default, the **WAN-2 Mode** parameter is set to **Backup**. The following options are supported: • **Shared** – Enables the WAN link to actively forward a percentage of user traffic. The percentage of user traffic on this link is set via the **Traffic Share Percentage** parameter. • **Backup** – The WAN link forwards user traffic only when all of the Shared WAN interfaces are down. • **Disabled** – Disables the WAN link from participating in WAN link load sharing, and failover procedures.
Traffic Share Percentage	For the **Shared** mode, the traffic share percentage between 5 and 100. This is a mandatory parameter.

4. Expand the **Flow Preferences** section and configure the parameters, as described in Table 85.

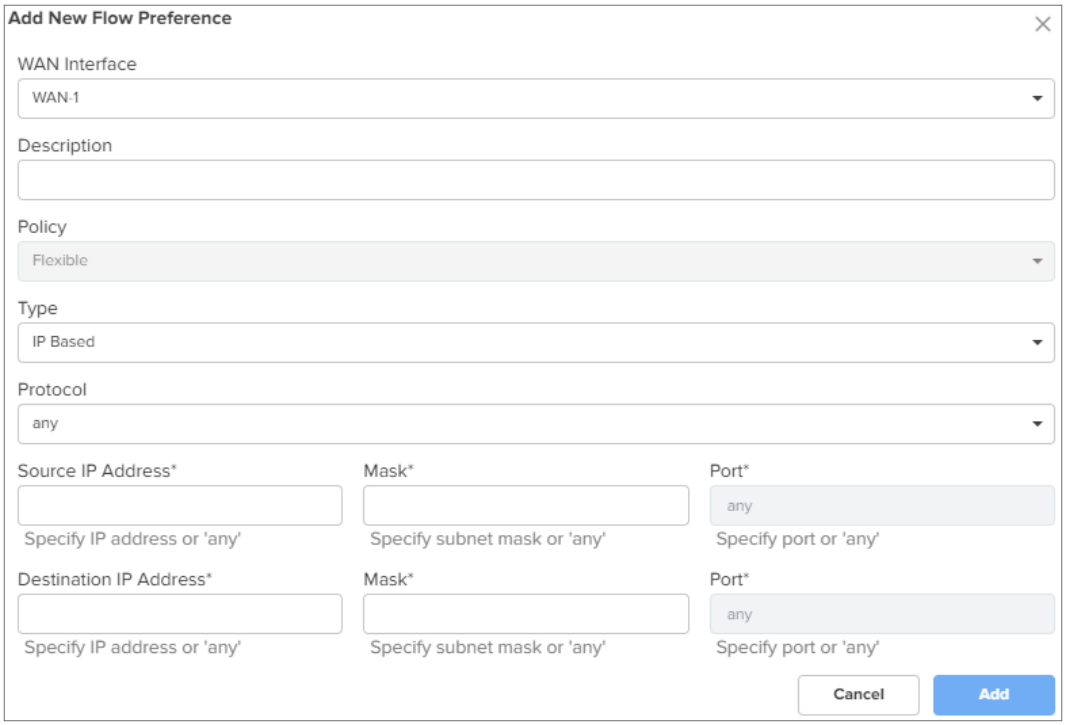
Table 85 *Parameters on the Flow Preferences section*

Parameter	Description
Flow Preferences Flow preferences support up to 30 rules for both WANs combined. To add a new flow preference, click **Add New**. The **Add New Flow Preference** window appears, as shown in Figure 415.	
WAN Interface	The following options are supported: • **WAN-1** • **WAN-2**
Description	Provide a description for the flow preference.

Parameter	Description
Policy	The flow preference policy. The following options are supported: • **Flexible** – Allow traffic to failover if the preferred WAN link goes down. • **Strict** – Traffic is dropped in strict mode, if the preferred WAN link goes down.
Type	The flow preference type. The following options are supported: • **IP Based** – Allows you to configure **Protocol** parameter as **TCP**, **UDP**, or **any**. • **Application Based** – Allows you to configure **Deep Packet Inspection (DPI) Type** parameter as **Application** or **Category**.
Protocol	This parameter is applicable only when **Type** parameter is **IP Based**. The following options are supported: • **TCP** – Match TCP preference. • **UDP** – Match UDP preference. • **Any** – Match any of the above preferences.
Source IP Address	The source IPv4 address for the flow preference. This is a mandatory parameter.
Mask	The subnet mask for the flow preference. This is a mandatory parameter.
Port	The source port for the flow preference. This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the flow preference. This is a mandatory parameter.
Mask	The subnet mask for the flow preference. This is a mandatory parameter.
Port	The destination port for the flow preference. This is a mandatory parameter.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **Application** – Specific type of application within a category. • **Category** – All applications belonging to a category (For example, Social Messaging). This is a mandatory parameter.
DPI Application	This parameter is applicable only when **Deep Packet Inspection (DPI) Type** parameter is set to **Application**. This is a mandatory parameter.
DPI Category	This parameter is applicable only when **Deep Packet Inspection (DPI) Type** parameter is set to **Category**.

Parameter	Description
	This is a mandatory parameter.

Figure 415 *The Add New Flow Preference window*



5. Click **Save**.

Firewall

NSE 3000 firewall allows the user to configure the IP-based and application-based outbound rules, GEO IP filters, port forward rules, one-to-one NAT mappings, and one-to-many NAT mappings. All inbound connections are denied by default. You can configure port forwarding or NAT rules to allow inbound traffic. Outbound traffic is allowed by default. Using application-based outbound rules, users can create rules to block websites without specifying IP addresses or port ranges. Application-based rules allow the user to block a specific type of application within a category or all applications belonging to a category (For example, social messaging).

Note

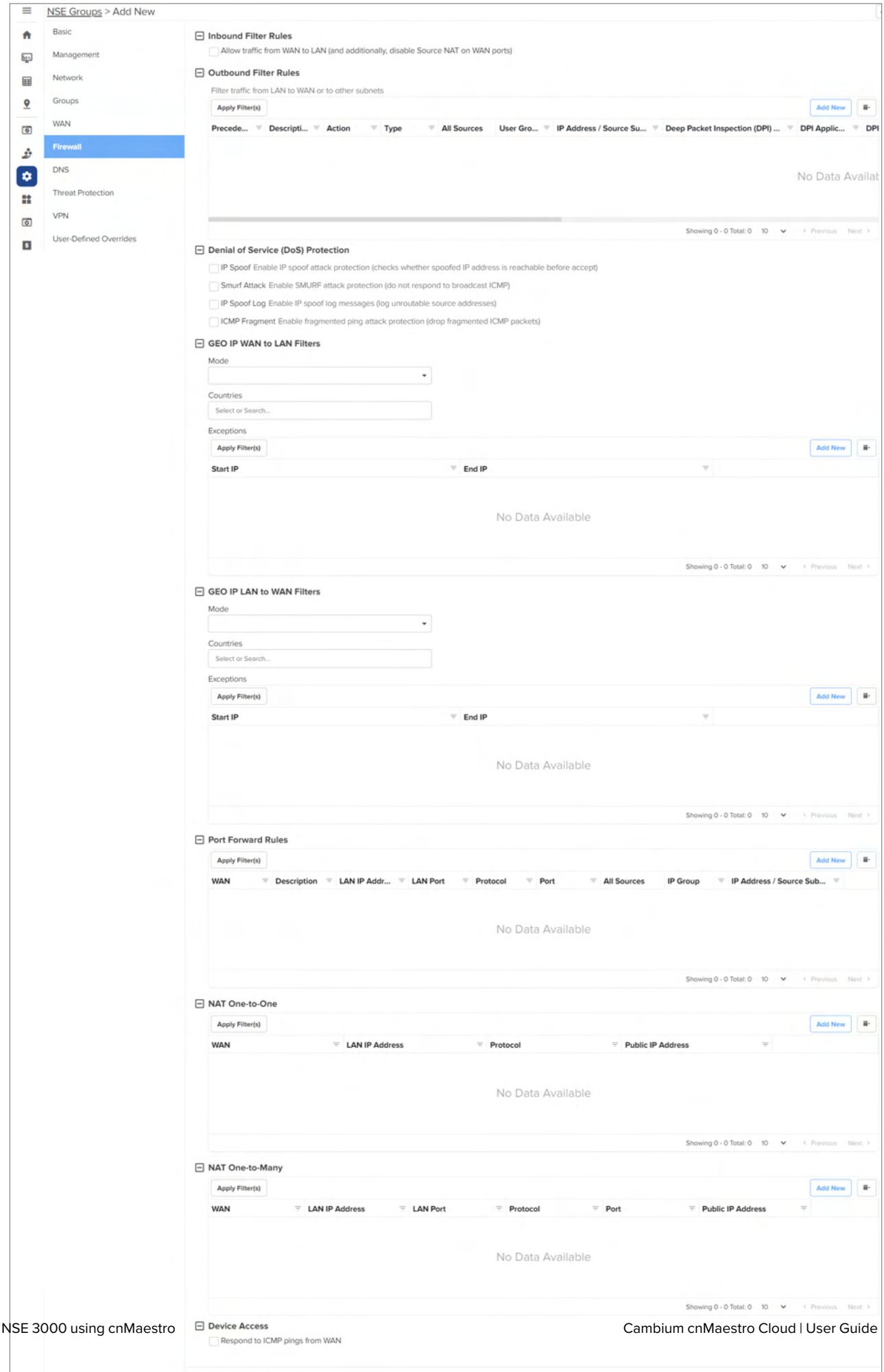
Up to 150 outbound firewall rules are supported for an NSE Group including combinations of IP-based and application-based rules.

To configure parameters on the **Firewall** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Firewall** tab.

   The **Firewall** page appears, as shown in Figure 416.

Figure 416 *The Firewall page*


NSE Groups > Add New
Basic
Management
Network
Groups
WAN
Firewall
DNS
Threat Protection
VPN
User-Defined Overrides
Inbound Filter Rules
Allow traffic from WAN to LAN (and additionally, disable Source NAT on WAN ports)
Outbound Filter Rules
Filter traffic from LAN to WAN or to other subnets
Apply Filter(s)
Add New
Precede... Descripti... Action Type All Sources User Gro... IP Address / Source Su... Deep Packet Inspection (DPI) ... DPI Applic... DPI
No Data Availat
Showing 0 - 0 Total: 0 10 Previous Next
Denial of Service (DoS) Protection
IP Spoof Enable IP spoof attack protection (checks whether spoofed IP address is reachable before accept)
Smurf Attack Enable SMURF attack protection (do not respond to broadcast ICMP)
IP Spoof Log Enable IP spoof log messages (log unroutable source addresses)
ICMP Fragment Enable fragmented ping attack protection (drop fragmented ICMP packets)
GEO IP WAN to LAN Filters
Mode
Countries
Select or Search...
Exceptions
Apply Filter(s)
Add New
Start IP End IP
No Data Available
Showing 0 - 0 Total: 0 10 Previous Next
GEO IP LAN to WAN Filters
Mode
Countries
Select or Search...
Exceptions
Apply Filter(s)
Add New
Start IP End IP
No Data Available
Showing 0 - 0 Total: 0 10 Previous Next
Port Forward Rules
Apply Filter(s)
Add New
WAN Description LAN IP Addr... LAN Port Protocol Port All Sources IP Group IP Address / Source Sub...
No Data Available
Showing 0 - 0 Total: 0 10 Previous Next
NAT One-to-One
Apply Filter(s)
Add New
WAN LAN IP Address Protocol Public IP Address
No Data Available
Showing 0 - 0 Total: 0 10 Previous Next
NAT One-to-Many
Apply Filter(s)
Add New
WAN LAN IP Address LAN Port Protocol Port Public IP Address
No Data Available
Showing 0 - 0 Total: 0 10 Previous Next
Device Access
Respond to ICMP pings from WAN

2. Configure the parameters, as described in Table 86.

Table 86 *Parameters on the Firewall page*

Parameter	Description
On the Firewall page, there are **Inbound Filter Rules**, **Outbound Filter Rules**, **Denial of Service (DoS) Protection**, **GEO IP WAN to LAN Filters**, **GEO IP LAN to WAN Filters**, **Port Forward Rules**, **NAT One-to-One**, **NAT One-to-Many**, and **Device Access** sections.	
Inbound Filter Rules By default, NSE firewall routers are configured to function as stateful firewalls by dropping packets that are not related to an established connection.	
Allow traffic from WAN to LAN	An option to enable or disable the stateful firewall behavior. By default, this parameter is disabled. In special deployment cases, when NSE is positioned behind an MPLS uplink router, you can enable this behavior. To enable this behavior, select the **Allow traffic from WAN to LAN** checkbox. Additionally, you must disable source NAT on the WAN UI page to allow routing of traffic without NAT, originated on the LAN directed towards the WAN.
Outbound Filter Rules To add a new outbound filter rule, click **Add New**. The **Add New Filter Rule** window appears, as shown in Figure 417.	
Precedence	The precedence value for the filter rule. The precedence value can be between 1 and 150. This is a mandatory parameter.
Description	Displays a user-configured description for the filter rule.
Action	Determines the action of filter. The following options are supported: • **Permit** - Allow traffic matching this filter rule. • **Deny** - Drop traffic matching this filter rule.
Type	The type of filter rule. The following options are supported: • **IP Based** – Configure **Protocol** parameter as **TCP**, **UDP**, **ICMP** or **any**. • **Application Based** – Configure **Deep Packet Inspection (DPI) Type** parameter as Application, Category, or Application Group
Protocol	This parameter is applicable only when **Type** parameter is **IP Based**. The following options are supported: • **TCP**: Match TCP traffic. • **UDP**: Match UDP traffic. • **ICMP**: Match ICMP traffic. • **any**: Match any of the above protocol traffic.
Source IP Address	The source IPv4 address for the filter rule.

Parameter	Description
	This is a mandatory parameter.
Mask	The source subnet mask for the filter rule. This is a mandatory parameter.
Port	This parameter is applicable only when **Protocol** parameter is **TCP** or **UDP**. Supported values: 1 to 65535 or any This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the filter rule. This is a mandatory parameter.
Mask	The destination subnet mask for the filter rule. This is a mandatory parameter.
Port	This parameter is applicable only when **Protocol** parameter is **TCP** or **UDP**. Supported values: 1 to 65535 or any This is a mandatory parameter.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **Application** – Specific type of application within a category. • **Category** – All applications belonging to a category (For example, Social Messaging). This is a mandatory parameter.
DPI Application	This parameter is applicable only when **DPI Type** parameter is set to **Application**. This is a mandatory parameter.
DPI Category	This parameter is applicable only when **DPI Type** parameter is set to **Category**. This is a mandatory parameter.
Apply to	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **All** • **User Group** • **IP Address / Source Subnet**
User Group	This parameter is applicable when **User Group** option is selected. This is a mandatory parameter.
IP Address / Source Subnet	This parameter is applicable when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.

Parameter	Description
Denial of Service (DoS) Protection	
IP Spoof	Enable or disable the IP spoof attack protection. By default, this parameter is disabled.
Smurf Attack	Enable or disable the smurf attack protection. By default, this parameter is disabled.
IP Spoof Log	Enable or disable IP spoof log messages. By default, this parameter is disabled.
ICMP Fragment	Enable or disable the fragmented ping attack. By default, this parameter is disabled.
GEO IP WAN to LAN Filters GEO IP WAN to LAN filters allows users to configure rules to permit/deny traffic based on the source country of inbound traffic.	
Mode	Specifies the mode for GEO IP WAN to LAN filters. The following options are supported: • **Allow Only (Deny by default)** – Allow traffic coming from the countries that are configured. The traffic coming from the countries which are not part of the configured countries will be dropped. • **Deny Only (Allow by default)** – Block traffic coming from the countries that are configured. The traffic coming from countries that are not part of the configured countries will be allowed. • **None** – Disables the feature. Traffic is allowed from all the countries.
Countries	The source countries from which the traffic originates.
Exceptions Exceptions allow users to configure source IP address ranges that are allowed in the inbound traffic. To add a new exception, click **Add New**. The **Add New Exception** window appears, as shown in Figure 418.	
Start IP	Starting IPv4 address in the range. This is a mandatory parameter.
End IP	Ending IPv4 address in the range. This is a mandatory parameter.
GEO IP LAN to WAN Filters GEO IP LAN to WAN Filters allows users to configure rules to permit/deny traffic based on the destination country of outbound traffic.	
Mode	Specifies the mode for GEO IP LAN to WAN filters. The following options are supported: • **Allow Only (Deny by default)**: Allow traffic destined to the countries matching the configured countries. The traffic destined for the countries which are not part of the configured countries will be dropped. • **Deny Only (Allow by default)**: Block traffic destined to the countries

Parameter	Description
	matching the configured countries. The traffic destined for the countries which are not part of the configured countries will be allowed • **None**: Disables the feature. Traffic is allowed in all countries.
Countries	The destination countries to which the traffic is destined.
Exceptions Exceptions allow users to configure destination IPv4 address ranges that are allowed in the outbound traffic. To add a new exception, click **Add New**. The **Add New Exception** window appears, as shown in Figure 418.	
Start IP	Starting IPv4 address in the range. This is a mandatory parameter.
End IP	Ending IPv4 address in the range. This is a mandatory parameter.
Port Forward Rules Port Forward Rules allow users to forward traffic destined to the WAN Interface IP address of NSE 3000 on a specific TCP or UDP port to any of the LAN IP address. Port Forward Rules provides remote access to internal resources. To add a new port forward rule, click **Add New**. The **Add New Port Forward Rule** window appears, as shown in Figure 419.	
WAN	The interface to forward inbound traffic to the internal host. The following options are supported: • **WAN-1** • **WAN-2**
Description	Displays the user-configured description for the port forward rule.
LAN IP Address	The IPv4 address to which traffic will be forwarded. This is a mandatory parameter.
LAN Port	The LAN port to which the traffic will be forwarded. Supported values: 1 to 65535. This is a mandatory parameter.
Protocol	The protocol of forwarded traffic. The following options are supported: • **TCP** • **UDP**
Port	The destination port of the incoming traffic on the WAN interface. Supported values: 1 to 65535. This is a mandatory parameter.
Apply To	The following options are supported: • **All** • **IP Group**

Parameter	Description
	• **IP Address / Source Subnet**
IP Group	This parameter is applicable only when **IP Group** option is selected.
IP Address / Source Subnet	This parameter is applicable only when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.
NAT One-to-One NAT One-to-One allows users to map an IP address on the WAN side to a LAN IP address. The IP address on the WAN side should be different from any of the WAN interface (WAN-1/WAN-2) IP addresses. NAT One-to-One rules provide remote access to any of the LAN resources. To add a new NAT one-to-one, click **Add New**. The **Add New NAT One-to-One** window appears, as shown in Figure 420.	
WAN	The following options are supported: • **WAN-1** • **WAN-2**
Public IP Address	The public IPv4 address on the WAN side that is used to access the LAN resource. The public IPv4 address is different from the IPv4 address of the WAN (WAN-1/WAN-2) interfaces. This is a mandatory parameter.
LAN IP Address	The LAN IPv4 address of the server which is hosting the resource. This is a mandatory parameter.
Protocol	The protocol of the incoming traffic. The following options are supported: • **TCP** • **UDP**
NAT One-to-Many NAT One-to-Many provides remote access to internal resources. It maps a public IP address to multiple LAN IPs and ports. To add a new NAT one-to-many, click **Add New**, the **Add New NAT One-to-Many** window appears, as shown in Figure 421.	
WAN	The following options are supported: • **WAN-1** • **WAN-2**
Public IP Address	The public IPv4 address on the WAN side that is used to access the LAN resource. The public IPv4 address is different from the IPv4 address of the WAN (WAN-1/WAN-2) interfaces. This is a mandatory parameter.

Parameter	Description
LAN IP Address	The LAN IPv4 address of the server which is hosting the resource. This is a mandatory parameter.
LAN Port	The LAN Port which is hosting the resource. This is a mandatory parameter.
Protocol	The protocol of the incoming traffic. The following options are supported: • **TCP** • **UDP**
Port	The destination port of the incoming traffic on the WAN interface. This is a mandatory parameter.
Device Access	
Respond to ICMP pings from WAN	This parameter is disabled by default. When enabled, this service is enabled for all the sources, unless specific IP addresses or IP groups are configured in the **IP Group** and **IP Address / Source Subnet** parameters.
IP Group	Specifies the IP group for this service.
IP Address / Source Subnet	Specifies the IPv4 address or source subnet for this service.

Figure 417 *The Add New Filter Rule window*

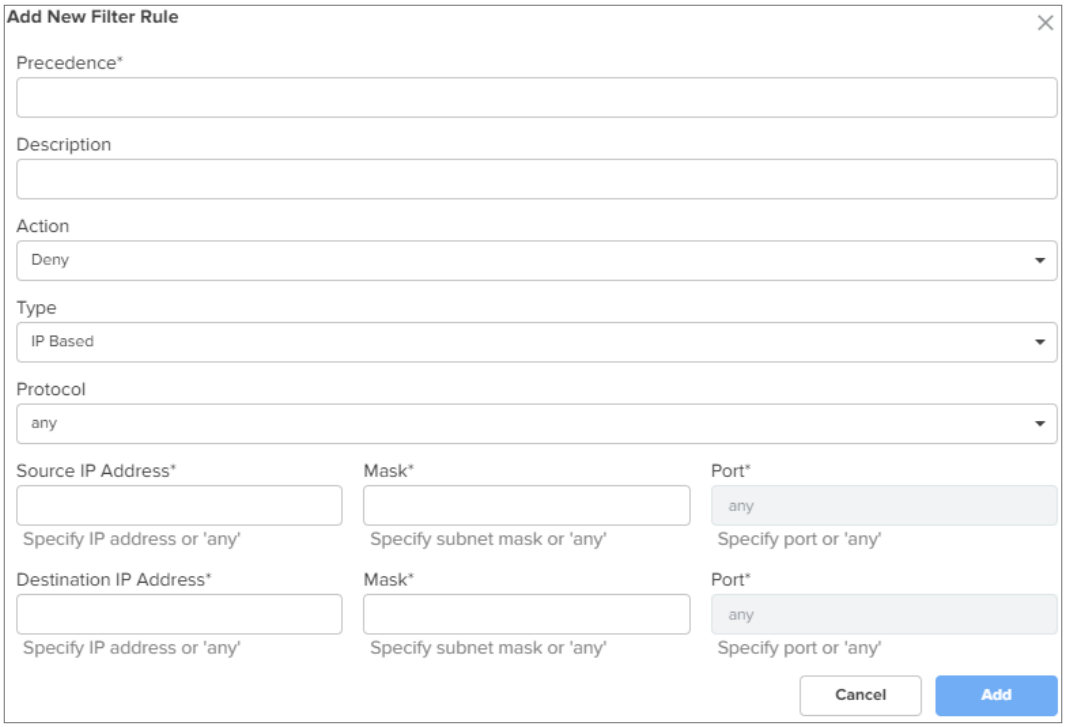


Figure 418 *The Add New Exception window*



Figure 419 *The Add New Port Forward Rule window*

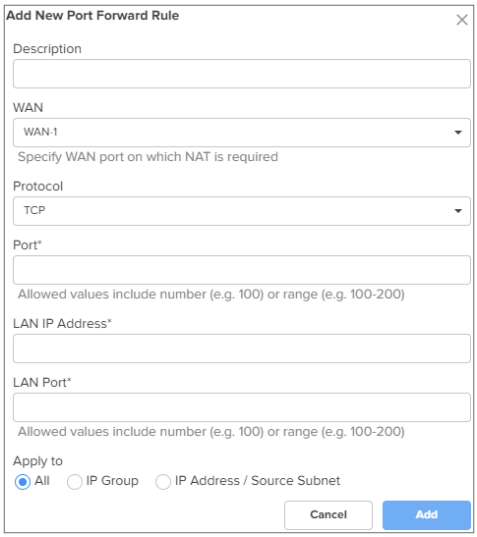


Figure 420 *The Add New NAT One-to-One window*

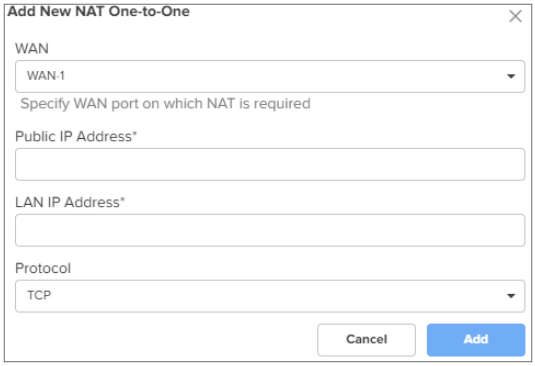
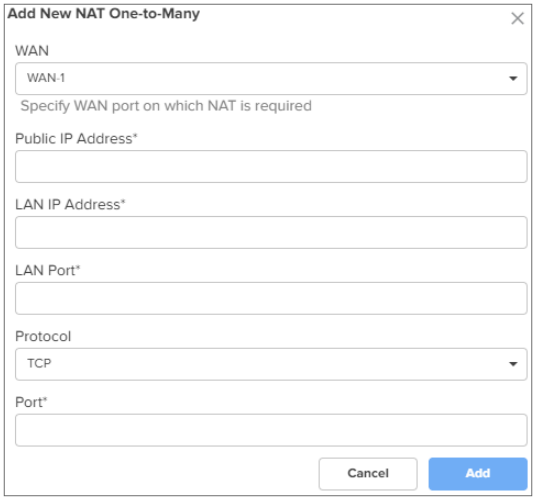


Figure 421 *The Add New NAT One-to-Many window*



3. Click **Save**.

DNS

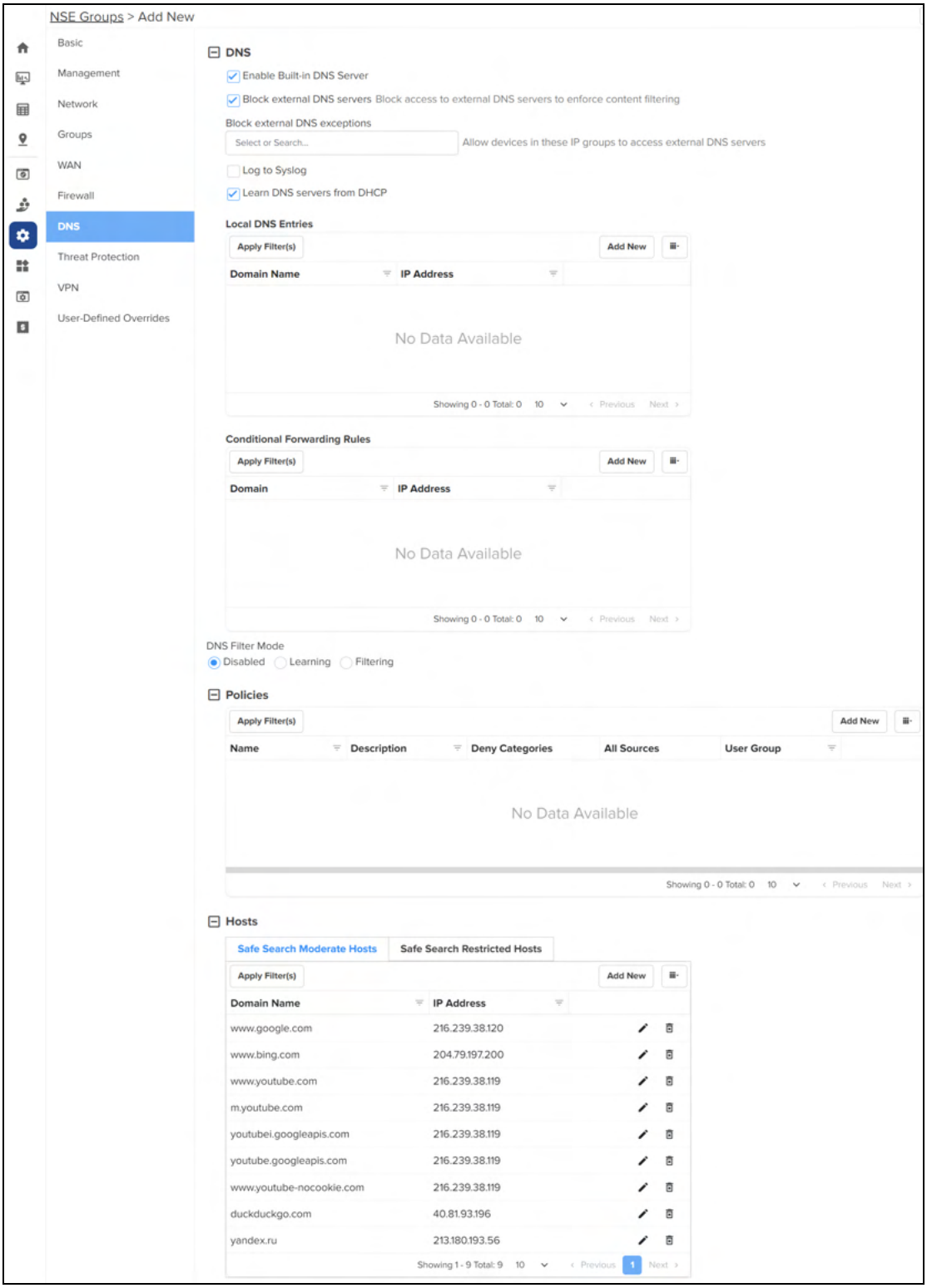
NSE 3000 supports DNS-based filters. DNS-based filters allow users to block certain category of websites. From the blocked list, users can still allow certain websites by adding them to the exception list. For example, if user blocks social-media category then all the social websites will be blocked including linkedin.com since linkedin.com belongs to social-media category. Adding linkedin.com to the Exception to filters list will allow access to linkedin.com while blocking other social-media websites.

To configure parameters on the **DNS** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **DNS** tab.

   The **DNS** page appears, as shown in Figure 422.

Figure 422 *The DNS page*



2. Configure the parameters, as described in Table 87.

Table 87 *Parameters on the DNS page*

Parameter	Description
On the DNS page, there are **DNS**, **Policies**, and **Hosts** sections.	
DNS	
Enable Built-in DNS Server	Indicates whether the on-board DNS server is enabled or disabled. By default, this parameter is enabled.
Block external DNS servers	Blocks the client to reach to any external DNS servers. By default, this parameter is enabled.
Block external DNS exceptions	Allows the clients added in the exceptions list to reach to any external DNS servers.
Log to Syslog	Specifies whether the DNS queries received from the client is logged to an external syslog server.
Learn DNS servers from DHCP	Dynamically learns the DNS server IP on WAN. By default, this parameter is enabled. When you disable this parameter, the **Primary DNS** and **Secondary DNS** parameters are displayed.
Primary DNS	The IPv4 address of the primary upstream DNS server.
Secondary DNS	The IPv4 address of the secondary upstream DNS server.
Local DNS Entries To add a new local host, click **Add New**. The **Add New Local Host** window appears, as shown in Figure 423.	
Domain	A domain name for the local host. This is a mandatory parameter.
IP address	The IPv4 address of the local host. This is a mandatory parameter.
Conditional Forwarding Rules To add a new forwarding rule, click **Add New**. The **Add New Forwarding Rule** window appears, as shown in Figure 424.	
Domain	A domain name for the forwarding rule. This is a mandatory parameter.
IP address	The IPv4 address of the server to which the DNS query is forwarded.
DNS Filter Mode	Specifies the mode for DNS filtering. The following options are supported: • **Disabled**: Disables DNS filter. By default, this option is selected. • **Learning**: Builds local cache for domain categories but does not filter requests. • **Filtering**: Filters requests based on configuration.

Parameter	Description
Policies To add a new policy, click **Add New**. The **Add New Policy** window appears, as shown in Figure 425.	
Name	Name for the policy. This is a mandatory parameter.
Description	Description about the policy.
Deny categories	Categories to deny in the following sections: • **Productivity** • **Privacy** • **Sensitive** • **Misc** • **IT Resources** • **Security** Expand the sections and select individual categories. To select all categories in a section, select the check box provided for the section.
Safe Search Mode	The following options are supported: • **Disabled:** Disables safe search mode. By default, this option is enabled. • **Moderate:** Enable moderate safe search mode. • **Restricted:** Enable restricted safe search mode.
Allow Exceptions (List of Domain Names)	Enter the exempted domain names separated by a comma (,).
Apply to	The following options are supported: • **All**: Apply to all user groups. By default, this option is selected. • **User Group**: Apply to selected user groups.
User Group	This parameter is applicable only when **User Group** option is selected for **Apply to** parameter. This is a mandatory parameter.
Hosts Hosts section contains two tabs - **Safe Search Moderate Hosts** and **Safe Search Restricted Hosts** The following parameters appear in both the tabs and can be configured as required. A list of hosts are already added by default. You can modify these hosts by clicking the edit icon or you can add new hosts by clicking **Add New** in the respective tabs as shown in Figure 426 and Figure 427.	
Domain Name	The domain name for the safe search host This is a mandatory parameter.
IP address	The IPv4 address of the safe search host. This is a mandatory parameter.

Figure 423 *The Add New Local Host window*



Figure 424 *The Add New Forwarding Rule window*



Figure 425 *The Add New Policy window*

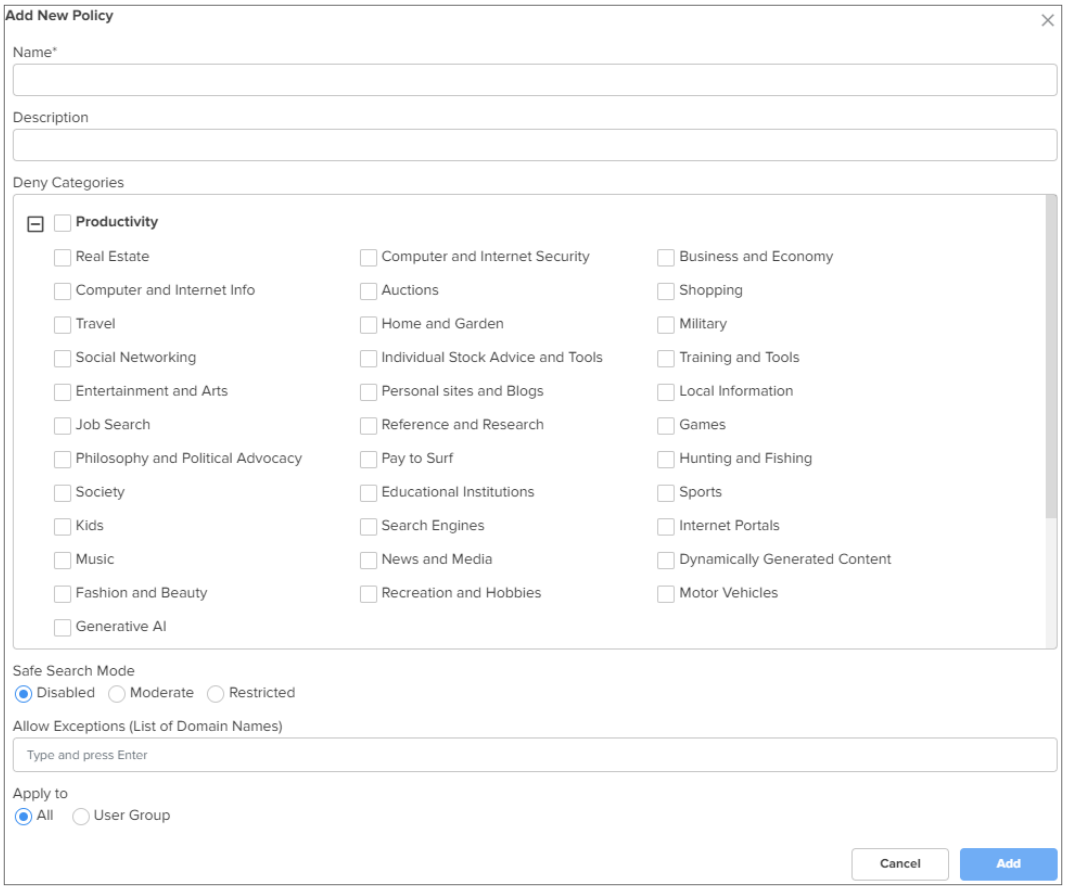


Figure 426 *The Add New Safe Search Moderate Host*

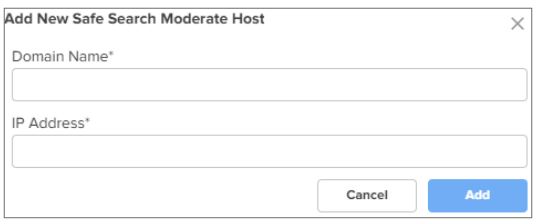


Figure 427 *The Add New Safe Search Restricted Host*



3. Click **Save.**

Threat Protection

Using the **Threat Protection** tab, you can configure the Intrusion Detection and Prevention system (IDS/IPS) parameters.

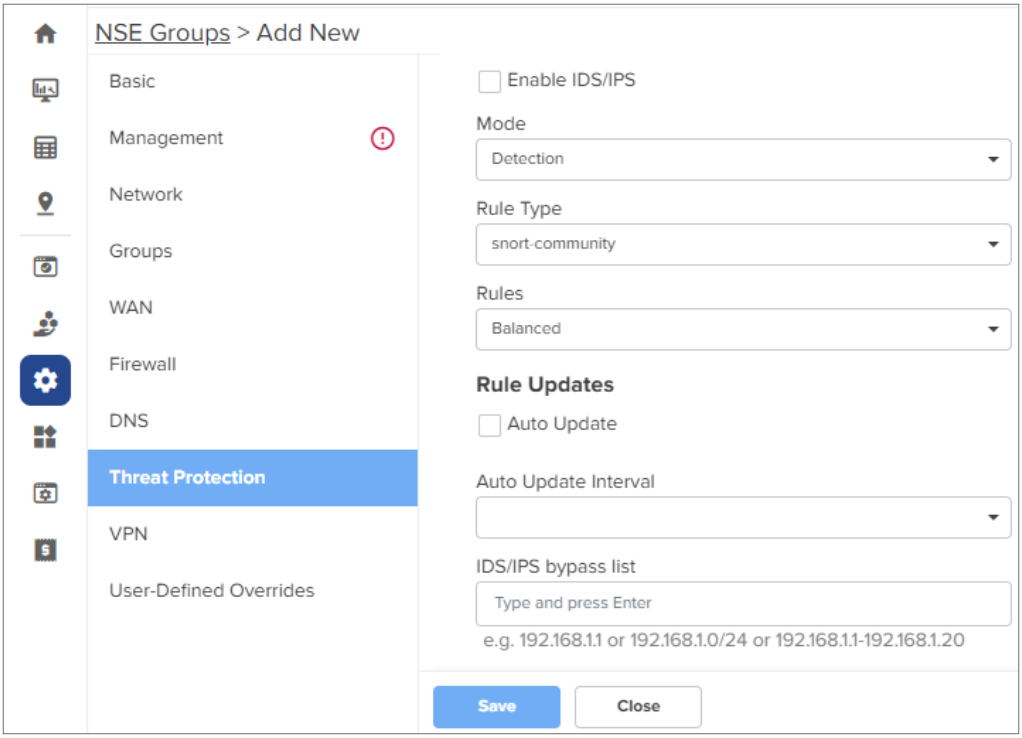
NSE 3000 supports IDS/IPS engine. IPS engine uses a series of rules that help define a malicious network activity. IPS engine supports rules from snort and emerging threats. The solution supports both community and licensed rules. The IPS engine uses these rules to find packets that match against them and generates alerts for users.

To configure parameters on the **Threat Protection** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Threat Protection** tab.

   The **Threat Protection** page appears, as shown in Figure 428.

   Figure 428 *The Threat Protection page*



2. Configure the parameters, as described in Table 88.

Table 88 *Parameters on the Threat Protection page*

Parameter	Description
IDS/IPS	
Enable IDS/IPS	Indicates whether IDS/IPS is enabled or disabled. By default, this parameter is disabled.
Mode	Specifies the IDS/IPS mode. The following options are supported: • **Detection** – Detects malicious activity and generates alerts for users. • **Prevention** – Detects malicious activity, generates alerts for users, and takes action to prevent attacks.
Rule Type	Specifies the IDS/IPS rule type. The following options are supported: • **snort-community** – The community rule set is a GPLv2 Talos certified rule set that is distributed free of charge and without any license restrictions. The rules are updated every Tuesday and Thursday. • **snort-vrt** – The Snort Subscriber rule set is developed by Talos research team and is governed by license agreement. The rule set is updated on Tuesday and Thursday. The snort-vrt rule set requires an oinkcode to download and activate rules. • **emerging-threats open** – Consists of signatures contributed from the community. The emerging-threats open rule sets are distributed free of charge. • **emerging-threats pro** – Consists of signatures created as a result of Proofpoint research. The rule sets are governed by license agreement. The emerging-threats pro rule set requires an oinkcode to download and activate the rules.
Rules	Specifies the IDS/IPS rule policy. This parameter is applicable when **Rule Type** is **snort-vrt** or **snort-community**. The following options are supported: • **Connectivity** – Policy designed to favor device performance over the security controls in the policy. • **Balanced** – This policy is the default policy that is recommended for initial deployments. The policy attempts to balance security needs and performance characteristics. • **Security** – This policy is designed for customer base that is extremely concerned about organizational security. This policy is deployed in networks that have higher security requirements.
Oink Code	This parameter is applicable when **Rule Type** is **snort-vrt** or **emergency- threats pro**.
Category	Categories to select from the **Category** section. This parameter is applicable when **Rule Type** is **snort-vrt** or **emergency- threats pro**.
Rule Updates	
Auto Update	Indicates whether the IDS/IPS rules must be automatically updated or not. By default, this parameter is disabled. When **Auto Update** is enabled, NSE 3000 will periodically download and activate the IDS/IPS

Parameter	Description
	rules.
Auto Update Interval	Time interval for the periodic updates of IDS/IPS rules. The following options are supported: • **12 Hrs** – Auto updates the rules every 12 hours. • **24 Hrs** – Auto updates the rules every 24 hours.
IDS/IPS bypass list	List of allowed IPv4 addresses or range of allowed IPv4 addresses. IDS/IPS operating in prevention mode blocks traffic from a host on detecting malicious traffic from the host. When an IPv4 address is part of allowed IP addresses, IDS/IPS will not block traffic from the host even when malicious traffic is detected.

3. Click **Save**.

VPN

NSE 3000 provides an on-board VPN server that allows remote users to establish a connection using the native VPN client supported in most of the operating systems. The VPN server uses the L2TP/IPsec protocol with the IPsec encryption and hashing algorithms. The VPN server maintains a pool of IP addresses and leases the IP addresses from this pool for remote users.

NSE 3000 also provides an on-board RADIUS server that allows authentication and accounting of enterprise and remote users. The RADIUS server maintains user profiles in a central database.

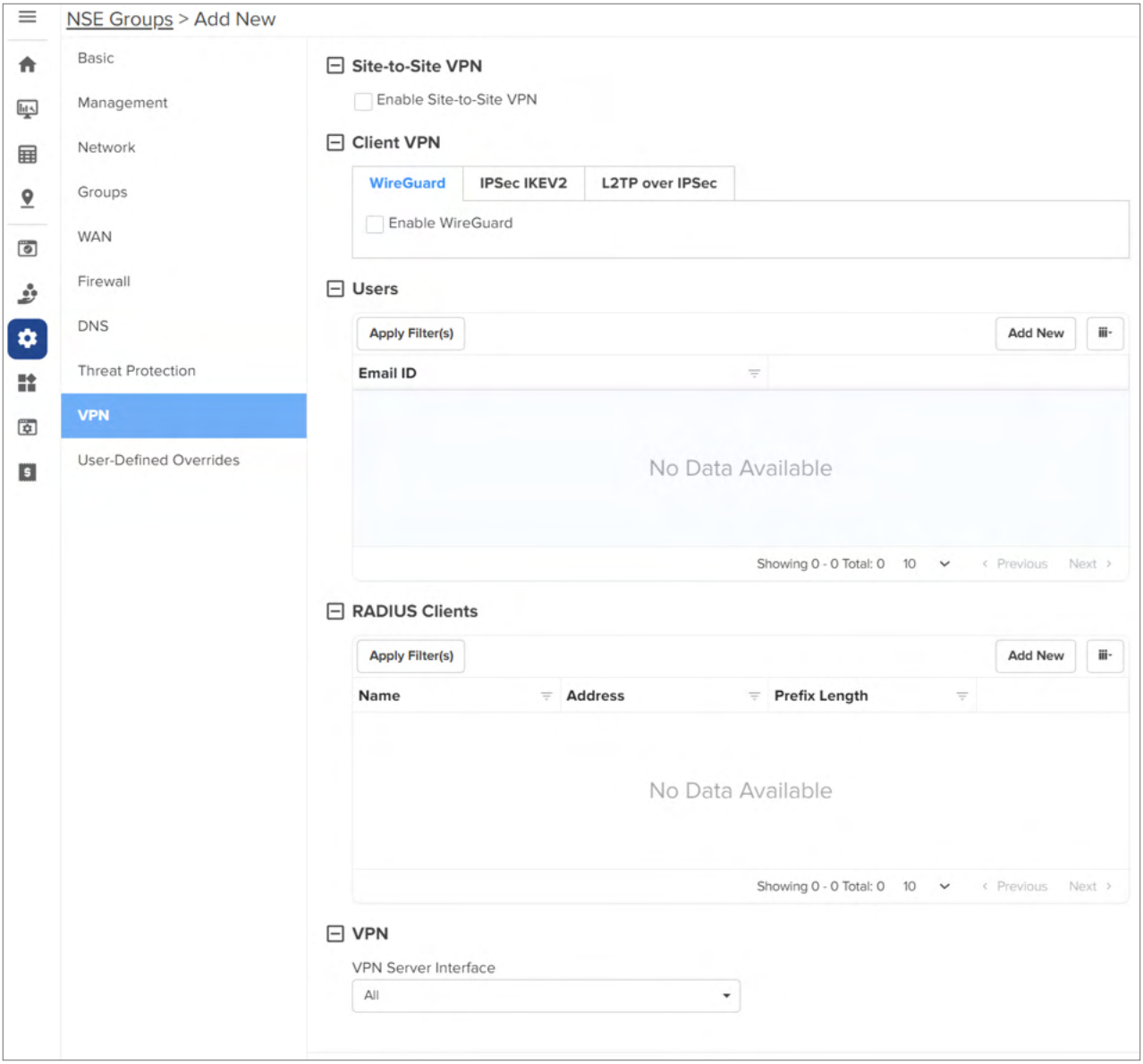
Using the **VPN** tab, you can configure DNS server, VPN server, and RADIUS server parameters.

To configure parameters on the **VPN** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **VPN** tab.

   The **VPN** page appears, as shown in Figure 429.

Figure 429 *The VPN page*



2. Configure the parameters, as described in Table 89.

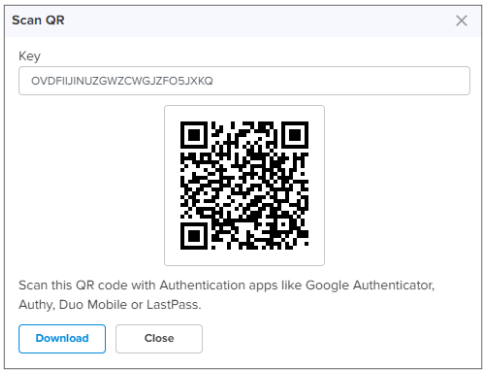
Table 89 *Parameters on the VPN page*

Parameter	Description
On the VPN page, there are **Site-to-Site VPN**, **Client VPN**, **Users**, **RADIUSClients**, and **VPN** sections.	
Site-to-Site VPN IPsec tunnel is a VPN technology that provides a secure, encrypted connection between two devices or networks over the internet or another public network. It uses IPsec protocols to encrypt the traffic between two endpoints, making it difficult for anyone to intercept the communication. IPsec site-to-site tunnel is used to connect two remote sites for secure communications. NSE allows setting up tunnels both in responder mode and initiator mode. Both, IKEv1 and IKEv2 are supported in the configuration. The default version is IKEv2.	

Parameter	Description
Note: You can configure up to 100 IPsec tunnels. Pre-shared key is the authentication method supported by the device. Each site can have its own pre-shared key. The site is identified by an identifier (string or the IP address of the site). Each site has to be configured with a local and remote site for the tunnel to establish. To view the IPsec tunnel stats, navigate to the **NSE Group > Network > VPN Sites** tab, as shown in Figure 431. To add a new site-to-site VPN, click **Add New**. The **Add New Site-to-Site VPN** window appears, as shown in Figure 430.	
Enable Site-to-Site VPN	Indicates whether site-to-site VPN is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select **Enable Site-to-Site VPN** check box.	
Name	A name for the new site-to-site VPN. This is a mandatory parameter.
IKE version	The Internet Key Exchange (IKE) version for the site-to-site VPN. The following options are supported: • **IKE v1** • **IKE v2**
Role	Specifies the role for the tunnels. The following options are supported: • **Initiator** • **Responder** Default role: Responder
Dead peer detection interval	The interval (in seconds) for detecting dead peers. Range: 30 - 600 seconds. Default: 120 seconds This is a mandatory parameter.
Remote ID	The remote ID. The value of 192.168.50.10 is pre-configured and is not modifiable. This is a mandatory parameter.
Local ID	The local ID. This is a mandatory parameter.
Local Subnets	The comma-separated list of local subnets. This is a mandatory parameter.
Remote Subnets	The comma-separated list of remote subnets. This is a mandatory parameter.
Remote PSK	The remote PSK. This is a mandatory parameter.
Local PSK	The local PSK.

Parameter	Description
	This is a mandatory parameter.
The following parameters are common for both **IKE Phase 1** and **IKE Phase 2**.	
Encryption	The following options are supported: • **aes128** • **aes192** • **aes256** • **aes128-gcm16** • **aes192-gcm16** • **aes256-gcm16** • **3des**
Integrity	The following options are supported: • **md5** • **sha1** • **sha256**
DH Group	The following options are supported: • **1** • **2** • **5** • **14** • **15**
Key Lifetime	The duration (in hours) for the pre-shared key. Range: 1 to 24
Client VPN: This section contains the following tabs: • **WireGuard: A VPN protocol that is highly secure.It is simpler and more efficient than traditional IPSec.** • **IPSec IKEV2** • **L2TP over IPSec**	
WireGuard: A VPN protocol that is highly secure.It is simpler and more efficient than traditional IPSec.	
Enable WireGuard	Indicates whether WireGuard is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select **Enable WireGuard** check box.	
Port	Indicates the WireGuard listen port number. Default: 51820 This is a mandatory parameter.
Client Pool	Indicates the WireGuard interface IP for the device and the client IPs to be assigned for the WireGuard clients.

Parameter	Description
	This is a mandatory parameter.
Keep Alive	Periodic keep alive packets sent for the configured duration. Default: 5 seconds This is a mandatory parameter.
Enable Split Tunnel	Indicates whether the split tunnel is enabled or disabled. By default, this parameter is disabled. **Note**: When you enable split tunnel, only the traffic destined to tunnelled subnets is allowed. You can override the **Enable Split Tunnel** parameter at the user level.
Tunnelled Subnets	Specifies the list of local subnets in NSE that should be allowed access from the WireGuard clients. **Note**: The same **Tunnelled Subnets** field is auto-populated in the **Add New User** window. You can edit this field at the user level.
IPSec IKEV2	
Enable IPSec IKEV2	Indicates whether IPSec IKEV2 is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select **Enable IPSec IKEV2** check box.	
Client IP Pool Range Start	Starting IPv4 address in the range. This is a mandatory parameter.
Client IP Pool Range End	Ending IPv4 address in the range. This is a mandatory parameter.
L2TP over IPSec	
Enable L2TP over IPSec	Indicates whether L2TP over IPSec is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select **Enable L2TP over IPSec** check box.	
Client IP Pool Range Start	Starting IPv4 address in the range. This is a mandatory parameter.
Client IP Pool Range End	Ending IPv4 address in the range. This is a mandatory parameter.
IPsec Shared Secret	Enter a pre-shared key string for the IPsec protocol. The shared secret is used between the VPN Client and Server for device authentication. This is a mandatory parameter.
Enable 2FA	Indicates whether two-factor authentication (2FA) is enabled or disabled. By default, this parameter is disabled.
VPN Two-Factor Authentication 1. When you enable two-factor authentication (2FA), scan the QR code to add a 16-digit key to a particular	

Parameter	Description
user's Google Authenticator app.  2. An email is also sent to the configured email address with the QR code and the 16-digit key. 3. The two-factor authentication gets enabled for the user when the user tries to connect to the NSE 3000 device using the remote VPN client from the WAN side. Users on the LAN side do not require two-factor authentication.	
Users: This section is common for all the three protocols - WireGuard, IPSec IKEV2, and L2TP over IPSec. To add a new user, click **Add New**. The **Add New User** window appears, as shown in Figure 432.	
Email ID	Email ID of the user. User is either an enterprise user or a remote user. This is a mandatory parameter.
Password	Password for the user. This is a mandatory parameter.
Enable WireGuard	Indicates whether WireGuard is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when **Enable WireGuard** check box is selected in the **Add New User** window.	
Enable Split Tunnel	Indicates whether split tunnel is enabled or disabled. By default, this parameter is enabled.
Tunnelled Subnets	Specifies the list of local subnets in NSE that should be allowed access from the WireGuard clients.
Device	Indicates the NSE 3000 device. When you select an NSE 3000 device, the device's public key is populated in the[Peer]section of the WireGuard client configuration file. This is a mandatory parameter.
WAN Interface	WAN Interface of the NSE 3000 device. When you select a WAN interface, the NSE 3000 device's WAN IP is populated as the endpoint IP in the [Peer] section of the WireGuard client configuration file. The following WAN Interface options are supported: • WAN-1

Parameter	Description
	• WAN-2
Clients: In this section, you have an option to add a new WireGuard client. To add a new WireGuard client, click **Add New**. The **Add New WireGuard Client** window appears, as shown in Figure 433.	
Name	Name for the new WireGuard client. This is a mandatory parameter.
Auto generate key pair	Generates a public and private key pair for the client. By default, this parameter is enabled. When this option is enabled, the **Client Public Key** field is auto-populated with the public key generated for that client. When this option is disabled, you need to provide the WireGuard client public key generated on the WireGuard client device.
Client Public Key	Public key of the client. This is a mandatory parameter.
IP Address	Auto-generated IP address of the WireGuard client.
Note: You have options to download QR code and configuration file in the **Add New WireGuard Client** window, as shown in Figure 433.	
RADIUS Clients To add a new RADIUS client, click **Add New**. The **Add New RADIUS Client** window appears, as shown in Figure 434.	
Name	Name of the RADIUS client. This is a mandatory parameter.
Secret	The shared secret of the RADIUS client. This is the shared secret (password) that the NAS needs to communicate with the RADIUS server. This is a mandatory parameter.
Address	The IPv4 address or network address of the RADIUS client. This is a mandatory parameter.
Prefix Length	The client network prefix length. This is a mandatory parameter.
VPN	
VPN Server Interface	The following options are supported: • **WAN-1 -** The first WAN interface on your server. • **WAN-2 -** The second WAN interface on your server. • **All -** Applies to all WAN interfaces.

Figure 430 *The Add New Site-to-Site VPN window*



Figure 431 *The VPN Sites page*

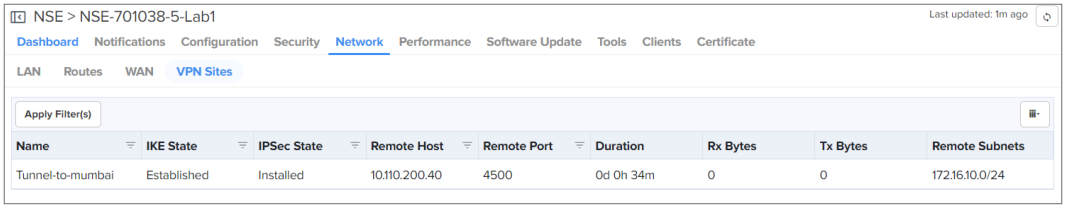


Figure 432 *The Add New User window*

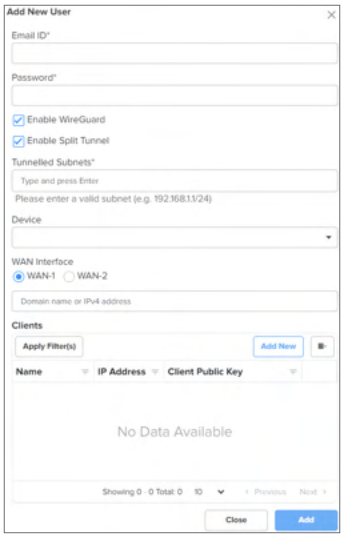


Figure 433 *The Add New WireGuard client window*

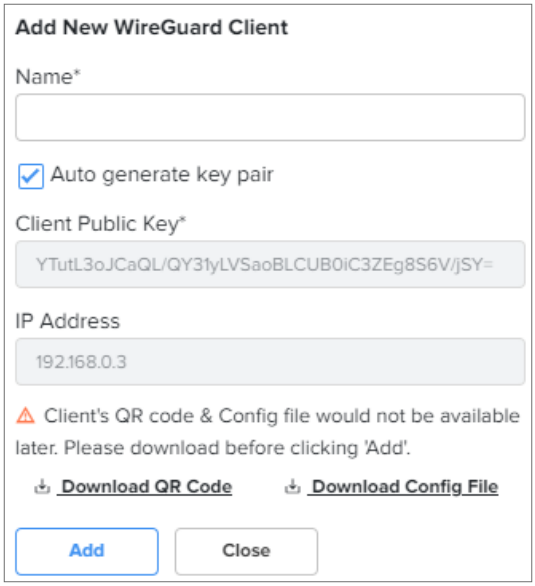
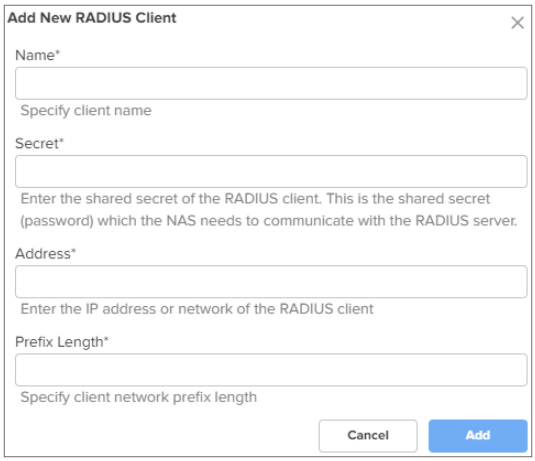


Figure 434 *The Add New RADIUS Client window*



3. Click **Save**.

User-Defined Overrides

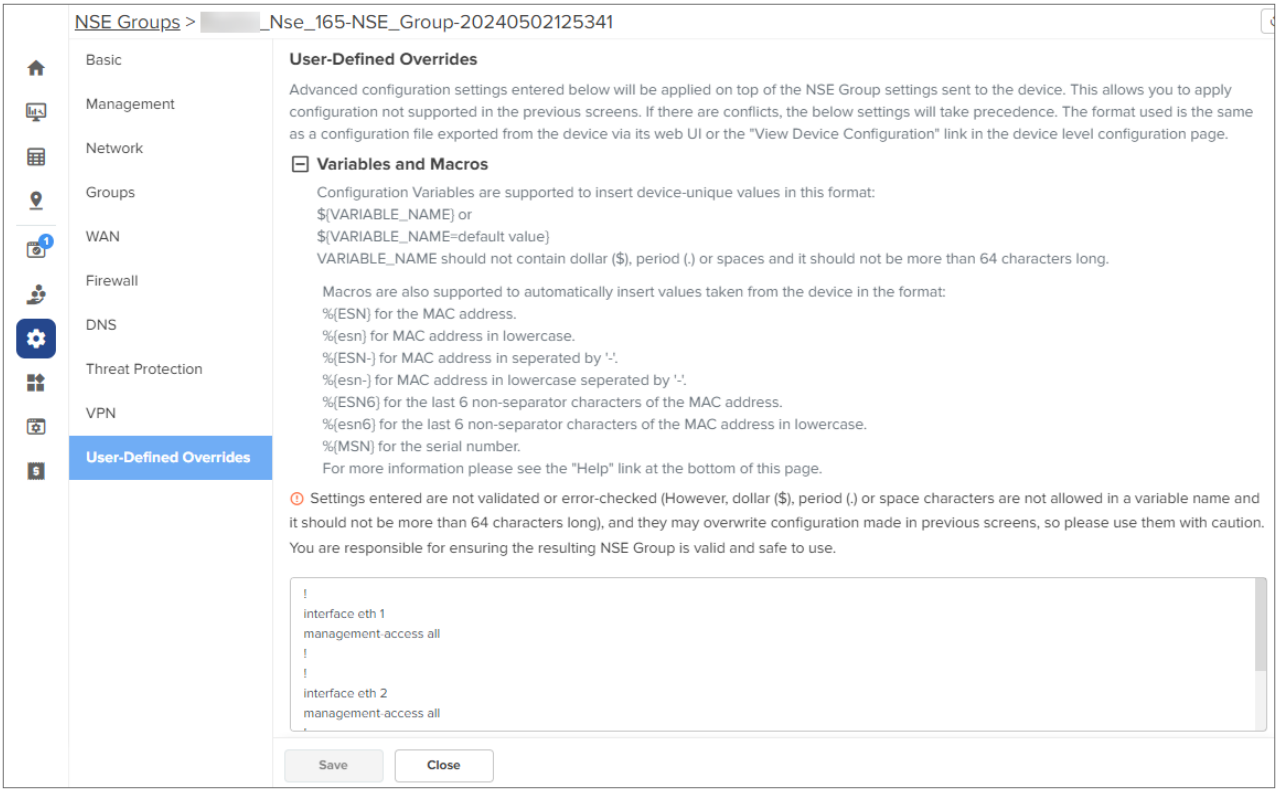
Using the **User-Defined Overrides** tab, you can configure the user-defined overrides.

To configure parameters on the **User-Defined Overrides** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **User-Defined Overrides** tab.

   The **User-Defined Overrides** page appears, as shown in Figure 435.

Figure 435 *The User-Defined Overrides page*



2. In the text box, enter the configuration that you want to apply to the device.
3. Click **Save**.

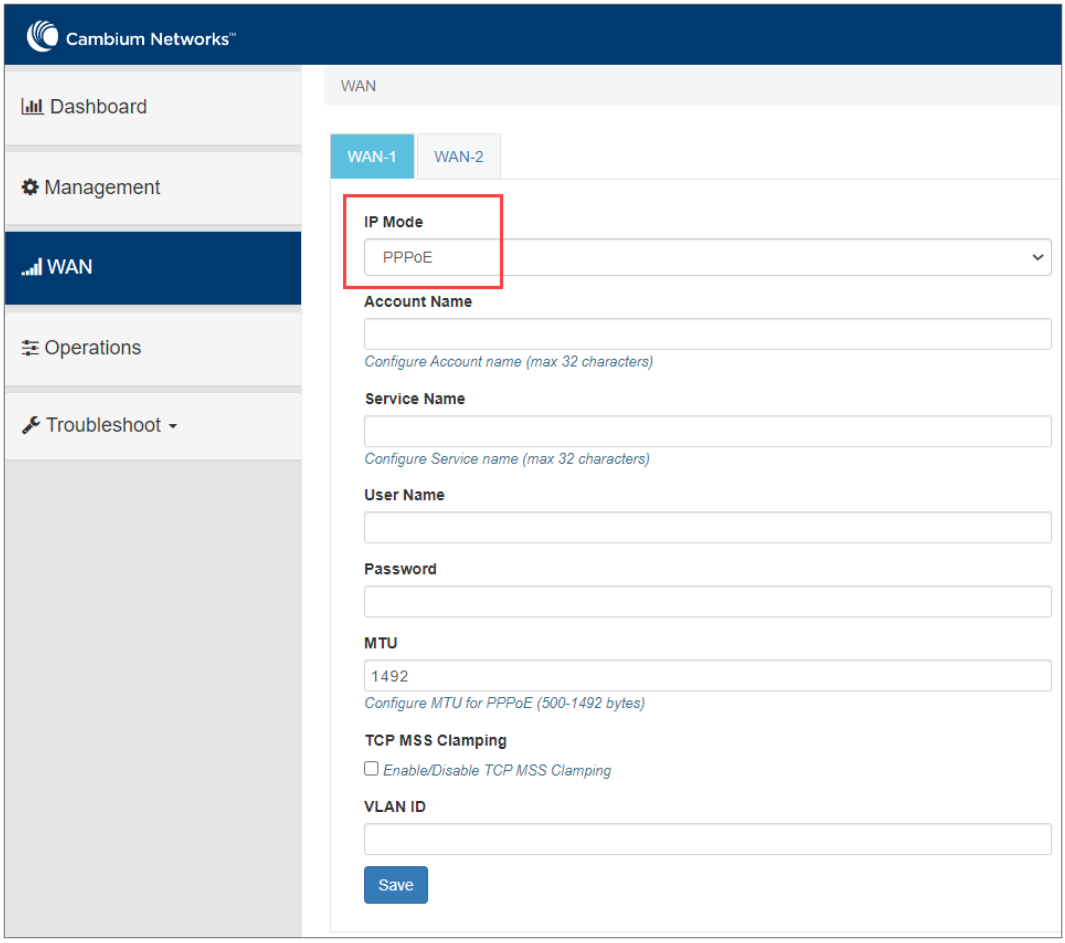
Configuring WAN in the device UI

In the **WAN** page, you can configure the device's IPv4 address based on the IP mode.

Note

If **PPPoE** is used as the WAN connection mode as shown in Figure 436, make sure to configure the PPPoE username and password. Once you have configured the PPPoE user name and password, you can proceed to configure the NSE group by providing the same username and password and then attaching the default NSE group to the device.

Figure 436 *PPPoE as WAN connection mode*



To view and configure the WAN settings, complete the following steps in the device UI:

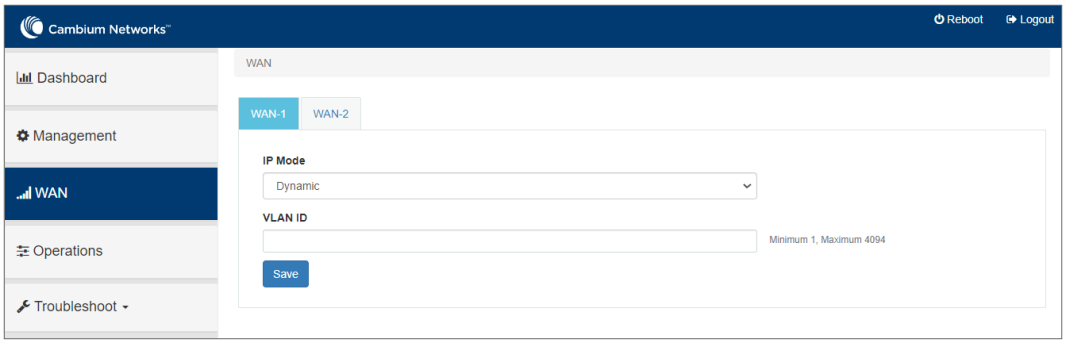
1. From the main NSE 3000 dashboard page, click **WAN** tab from the left panel.

   The **WAN** page appears, as shown in Figure 437.

Note

By default, WAN-1 page appears. You can configure WAN on WAN-1 or WAN-2.

Figure 437 *The WAN page*



2. Configure the parameters, as described in Table 90.

Table 90 *Parameters on the WAN page*

Parameter	Description
IP Mode	Determines the network that must be configured to use IPv4 addresses. The following options are supported: • **Dynamic** • **Static** • **PPPoE** By default, the **Dynamic** mode is selected.
VLAN ID	The VLAN ID can range from 1 to 4094. The VLAN configuration is optional. When the 802.1Q header is configured, all transmitted frames are expected to include the 802.1Q header with the same VLAN ID.
Following parameters appear only when you select the mode as **Static** from the **IP Mode** drop-down list, as shown in Figure 438.	
IP Address	The 32-bit binary number that identifies a network element by both network and host.
Subnet Mask	The subnet mask for the destination IP/network for the route.
Gateway	The gateway for the destination IP/network for the route.
DNS	
Primary DNS	The IPv4 address of primary upstream DNS server.
Secondary DNS	The IPv4 address of secondary upstream DNS server.
Following parameters appear only when you select the mode parameter as **PPPoE** from the **IP Mode** drop-down list, as shown in Figure 439.	
Account Name	The name of Access Controller. This parameter allows a maximum of 32 characters. This parameter is optional.
Service Name	Service name of Access Controller. This parameter allows a maximum of 32 characters. This parameter is optional.
User Name	A user name for PPPoE authentication. This parameter is mandatory.
Password	A password for PPPoE authentication. This parameter is optional.
MTU	MTU for PPPoE interface in bytes. Default: 1492. Range: 500 to 1492
TCP MSS Clamping	Indicates whether TCP MSS Clamping is enabled or disabled. By default, this parameter is disabled.

Figure 438 *Static mode*

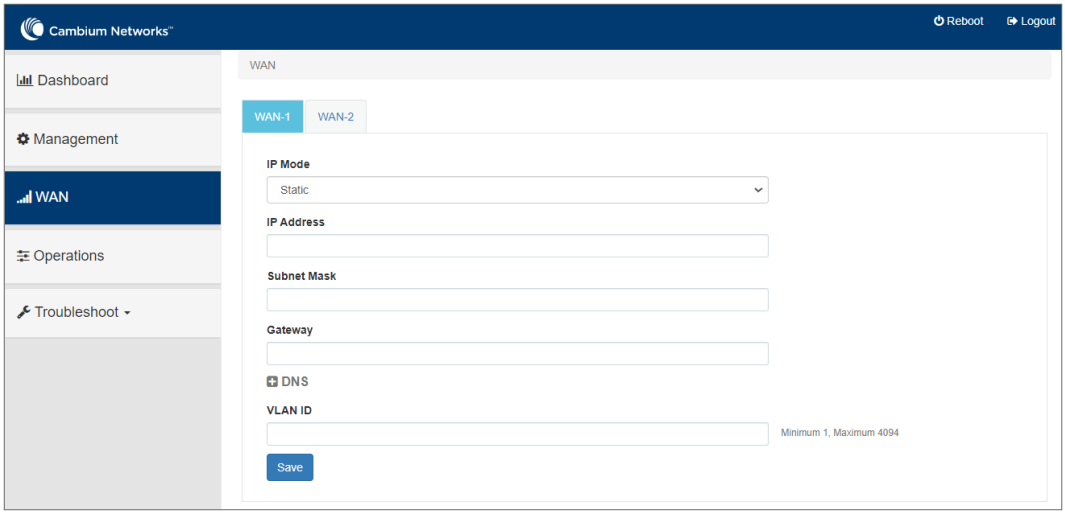
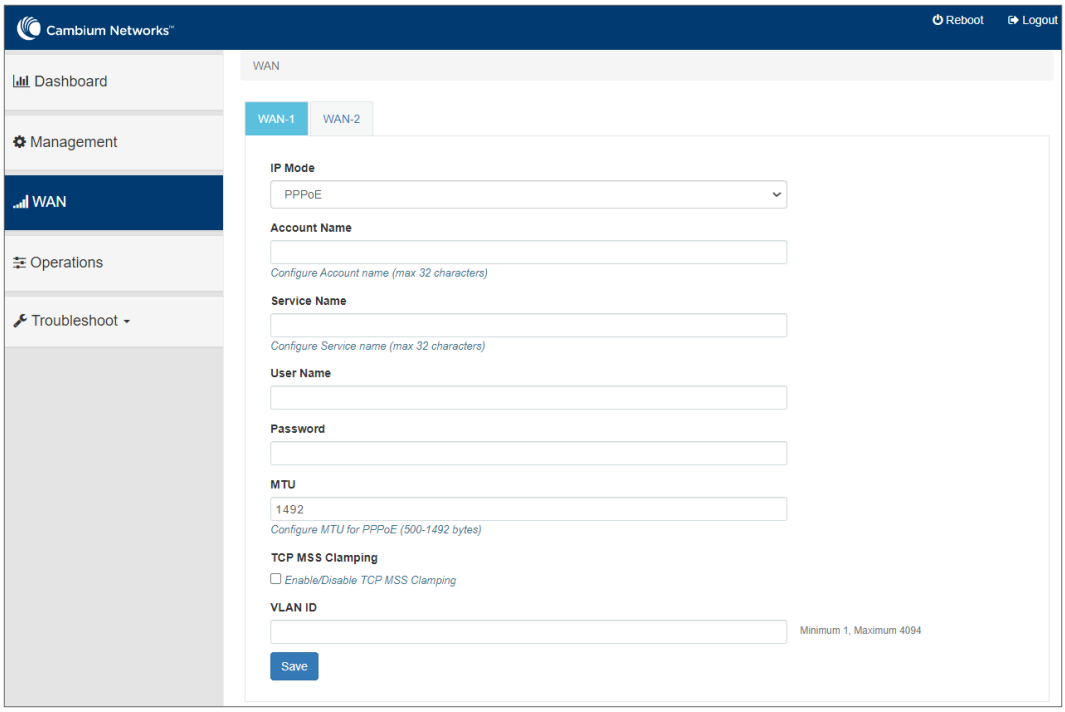


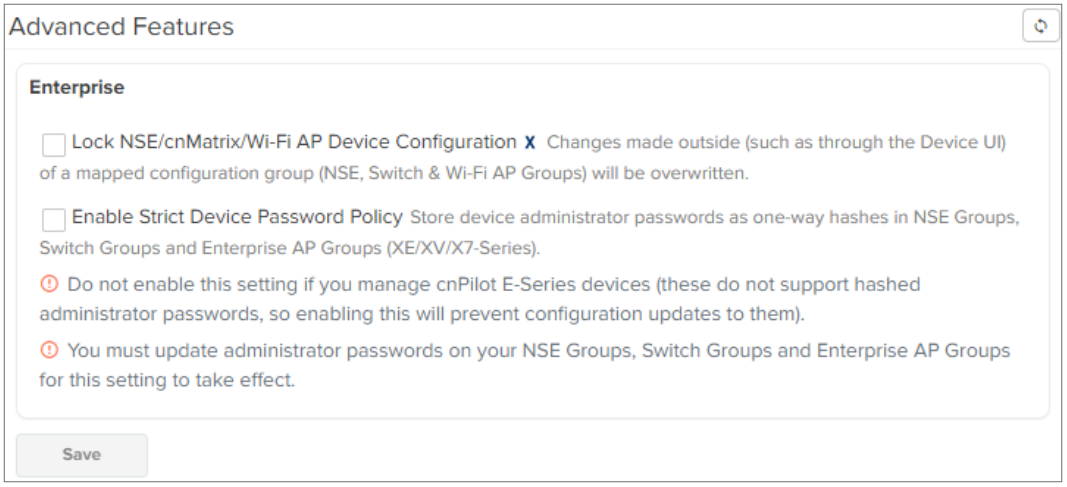
Figure 439 *PPPoE mode*



3. Click **Save**.

Configuring Advanced Features

To configure advanced features, navigate to **Configuration > Advanced Features** page.



Lock Device Configuration

To lock NSE, cnMatrix, and Wi-Fi device configuration, select the check box. Once you enable this check box, you cannot update the device-level configuration using the device UI or any other method. Only the configuration pushed from cnMaestro for NSE, switch, and Wi-Fi AP groups will be retained on the device.

Strict Device Password Policy

To enable strict password policy for Switch Groups or Enterprise AP Groups, select the **Enable Strict Device Password Policy** check box.

If you enable this option:

- The device administrator passwords are stored as one-way hashes for all NSE Groups, Switch Groups, and Enterprise AP Groups (XE/XV/X7-series).
- The administrator password has to be updated for all NSE Groups, Switch Groups, and Enterprise AP Groups under **Configuration > NSE Group > Management** page, **Configuration > Switch Group > Management** page, and **Configuration > Wi-Fi Profiles > AP Group > Management** page respectively for this setting to take effect.
- The configuration cannot be pushed to cnPilot E-series device.
- Device software versions must be at or above 1.3 for NSE, 4.6.1 for cnMatrix, and 6.5.3 for Enterprise Wi-Fi XE/XV/X7-Series to support the strict password policy. cnMaestro will not push any configuration to devices not meeting these requirements, including all cnPilot E-Series devices when the strict policy is enabled.

If you disable this option:

- The password must be updated for all NSE Groups, Switch Groups, and Enterprise AP Groups under the respective **Management** pages for this setting to take effect.

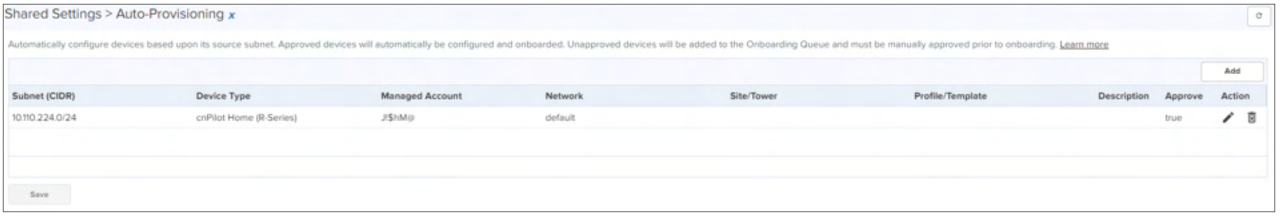
Auto-Provisioning

cnMaestro supports Auto-Provisioning for cnVision, Wireless LAN devices (Enterprise Wi-Fi, cnPilot R-Series, and Xirrus) and fixed devices (PMP and ePMP). It is enabled at **Configuration > Auto-Provisioning**, and it allows one to automatically configure and approve devices based upon IP address.

Creating Auto-Provisioning Rule

To create a rule for Auto-Provisioning, perform the following steps:

1. Navigate to **Shared Settings > Auto-Provisioning** page.



2. Click **Add** and following window appears.

Figure 440 *Auto-Provisioning - cnPilot Home (R-Series) devices*

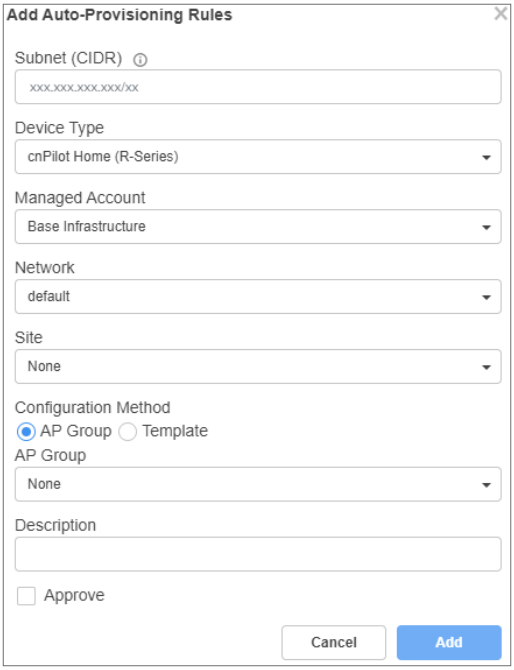
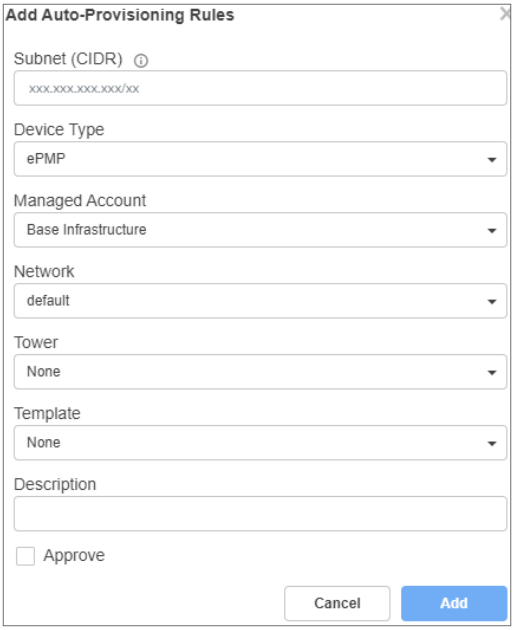


Figure 441 *Auto-Provisioning - All Other Devices*



3. Enter the following details:
    - **Subnet:** The subnet with CIDR of the devices to which the rule has to be applied.
    - **Device Type:** Select the rule to be created for Enterprise Wi-Fi, Enterprise Wi-Fi (Xirrus-Series), cnVision, cnPilot Home (R-Series), ePMP, and PMP devices.
    - **Managed Account:** Select the Managed Account from the list.
    - **Network:** To which network the device should be onboarded, once device contacts the server.
    - **Site:** Site under which the device must be onboarded, once device contacts the server. Applicable for Enterprise (E) or Home (R).
    - **Tower:** Site under which the device must be onboarded, once device contacts the server. Applicable for ePMP AP, PMP AP, and cnVision.
    - **Template:** Template to be applied on the device when onboarding, once device contacts the server. Applicable for ePMP AP, PMP AP, cnVision, and cnPilot Home (R-Series).
    - **AP Group:** AP Group to be applied on the device when onboarding, once device contacts the server. Applicable for Enterprise (E-, XE-, XV-, and X7-Series), Xirrus, and cnPilot Home (R-Series).
    - **Description:** Brief information about the device.
    - **Approve:** Indicates whether the device is auto-approved or must be manual approved when onboarding.
4. Click **ADD**.

Managing Home Mesh Router

The Home Mesh Router is engineered to provide superior Wi-Fi performance and mesh networking capabilities. It incorporates the advanced 802.11ax technology, ensuring it is fully compatible with a wide range of consumer devices while offering low latency and high throughput. These routers are specifically designed for comprehensive home coverage, supporting simultaneous operation on both 2.4 GHz and 5 GHz bands. This enables extended range, enhanced efficiency, and reduced interference compared to previous generations of Wi-Fi technology.

Additionally, the routers are configured to work in tandem, creating a seamless mesh network that covers the entire home, effectively eliminating areas with weak or no Wi-Fi signal.

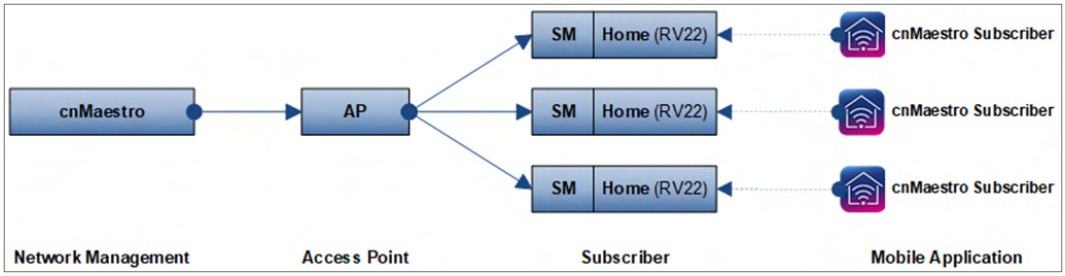
The Home Mesh Routers can be configured using cnMaestro Cloud and the cnMaestro Subscriber application.

For information on supported platforms and hardware overview, see *Home Mesh Router User Guide*.

Warning

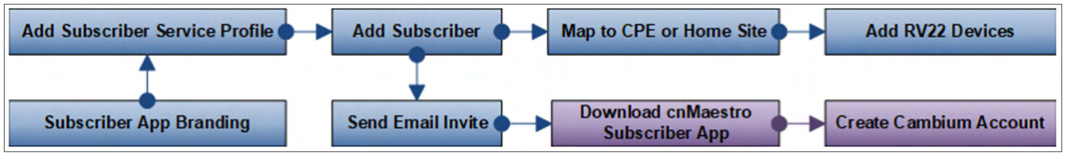
The WAN port of the Home Mesh Router may be damaged if a 48 VDC passive power (passive POE) is connected to the WAN port.

The basic architecture of the Home Mesh Router is as shown below.



The cnMaestro Subscriber application allows home customers to manage RV22 devices using their mobile phones. In the graphic above, the Subscriber is demarcated by the SM CPE. Alternatively, it could be mapped to a PON ONU, or to no explicit backhaul at all. In the latter case, the Subscriber would be attached to a new cnMaestro Home Site.

The workflow for creating and onboarding Subscribers, so customers can use the mobile application, has a cnMaestro (blue) and a customer (purple) component, as shown below.



A Subscriber is configured in cnMaestro Cloud, and an invite is sent to the customer's email address, which will enable home Wi-Fi management using the mobile application. The customer must download the cnMaestro Subscriber application from the Apple App store or Google Play Store. The "Site" in the application, which maps to the Subscriber, can be customized and branded.

Feature	Details
Onboarding	Supported using Cambium ID or Serial Number (MSN).
Dashboard	Dashboards tailored for Home Site and RV22 Home Mesh.
Configuration	Available through RV22 Home Mesh AP Groups.
Details	Overview and network information display.
Notifications	Alarms, AP Events, and Wi-Fi Events aggregated at System, Managed Account, Network, Site, and Device levels.
Performance	WAN Throughput, Wireless Throughput (downlink/uplink), Clients by Band, Noise Floor, Interference, and Airtime (2.4/5 GHz) performance graphs.
Statistics	System, Managed Service, and Network statistics available.
Software Update	Software update provided at System, Managed Account, Network, Site, and Device levels.

Feature	Details
Maps	Location of Home Sites and Devices.
Clients	Both Wired and Wireless Clients supported at Site and Device levels.
Tools	Status, Debug, Network Connectivity, Wi-Fi Analyzer, Speed Test, and Packet Capture tools available.
Reports	Data Reports downloaded from the System, Managed Service, Network, and Site levels.

This topic contains the following sections:

- Configuring Home Mesh Router
- Viewing router system information and network traffic status
- Viewing, editing, and blocking connected clients
- Monitoring and troubleshooting the Home Mesh Router

Configuring Home Mesh Router

Before shipping the Home Mesh Routers to the subscribers, they must be configured with AP groups, Wi-Fi profiles, and associated with the corresponding subscriber.

Configuring the routers involves the following steps:

1. Configuring WLAN profiles (SSIDs)
2. Configuring AP Groups
3. Onboarding the Home Mesh Router to cnMaestro
   a. cnMaestro Subscriber application branding
   b. Adding a Subscriber Service Profile
   c. Adding a subscriber
   d. Claiming the Home Mesh Router

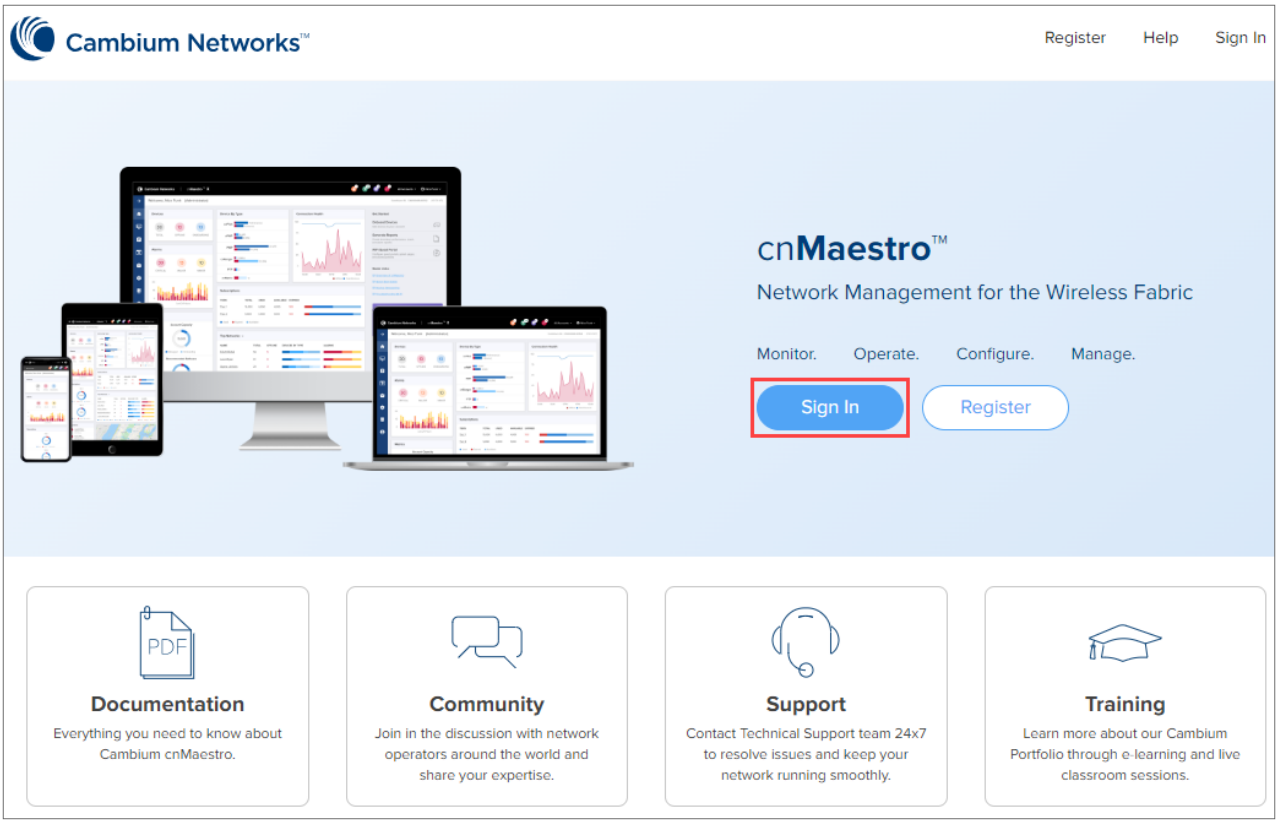
Configuring WLAN Profiles (SSIDs)

WLANs allow you to configure home and guest access SSIDs for the Home Mesh Router. This WLAN profile is associated with an AP group that contains configuration applied on the Home Mesh Routers. These SSIDs act as default SSIDs on all routers associated with the AP group.

To configure a WLAN profile, complete the following steps:

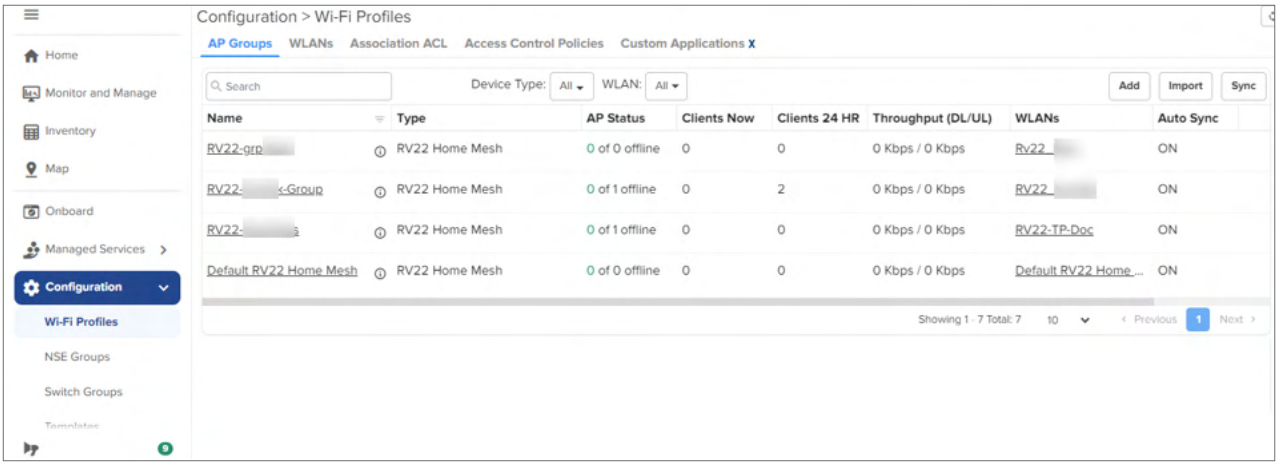
1. Sign in to cnMaestro.

   The home page appears.



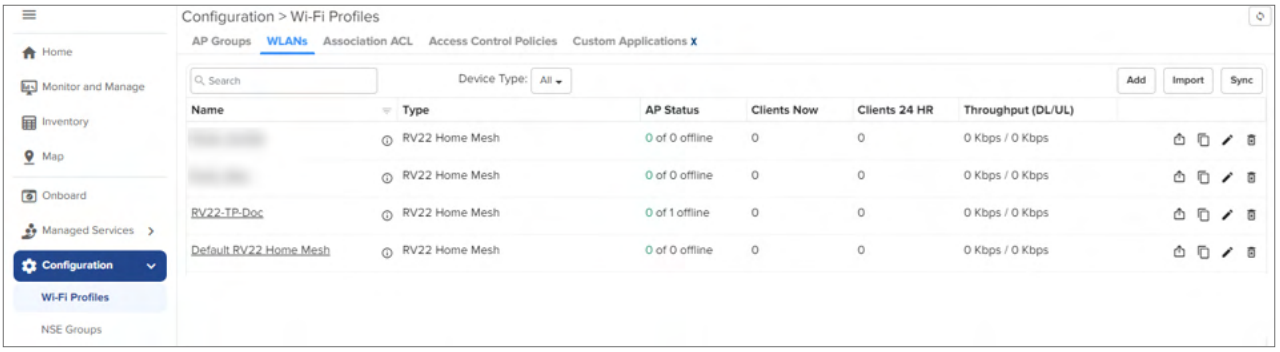
2. Navigate to **Configuration** > **Wi-Fi Profiles**.

   The **AP Groups** page under **Wi-Fi Profiles** appears, by default.



3. Click the **WLANs** tab.

   The **WLANs** page appears.



4. Click **Add**.

   The **WLANs** > **Add New** window appears.

   In the **WLANs** > **Add New** window, configure the WLAN parameters as described in Table 91.

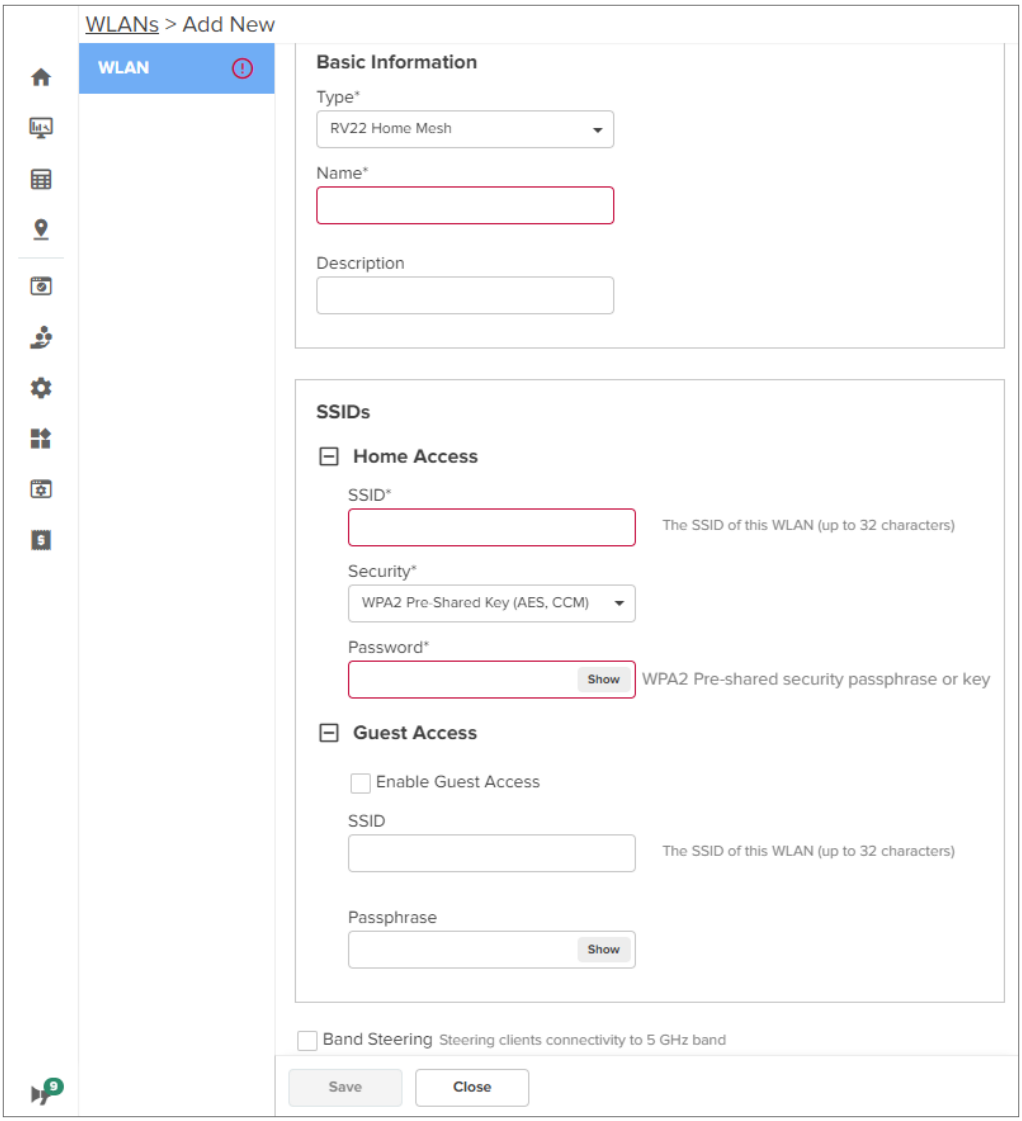


Table 91 *WLAN parameters*

Parameter	Description
Basic Information	
Type	Type of device for which the WLAN profile is configured. Select **RV22 Home Mesh** from the drop-down list.
Name	Name of the WLAN profile.
Description	Brief description for the WLAN profile.
SSIDs—Home Access Configure the default SSID for connecting devices wirelessly. Only one home SSID can be configured.	
SSID	Unique name of the SSID for this WLAN. Supports a maximum of 32 characters. You must either configure the default SSID or enter a customized SSID. The default SSID: `RV22_<last 6 digits of device MAC>`. For example, `RV22_123456`.
Security	Security method used for encryption. The following security methods are supported: • **Open** • **WPA Pre-Shared Key (AES, CCM)** • **WPA2 Pre-Shared Keys (AES, CCM)** • **WPA2 Pre-Shared Keys (TKIP, AES)** • **WPA Pre-Shared Key (TKIP, AES)**
Password	Security passphrase or key used to connect to this SSID. You must either configure the default password or enter a customized password. Default password: `password`
SSIDs—Guest Access Configure the guest SSID to allow any guest devices to access the wireless network.	
Enable Guest Access	Determines whether the guest access is enabled. Select the check box to enable guesst access.
SSID	Unique name of the guest SSID for this WLAN. Supports a maximum of 32 characters.
Password	Security passphrase or key used to connect to this guest SSID.
Band Steering	Determines whether the band steering is enabled for the wireless clients. When enabled, APs steer wireless clients to connect to the 5 GHz band.

5. Click **Save**.

Configuring AP Groups

AP groups apply the same configuration to multiple Home Mesh Routers. AP groups contain configuration, such as administrator password, event logging, radio settings, WAN mappings, and DNS mode.

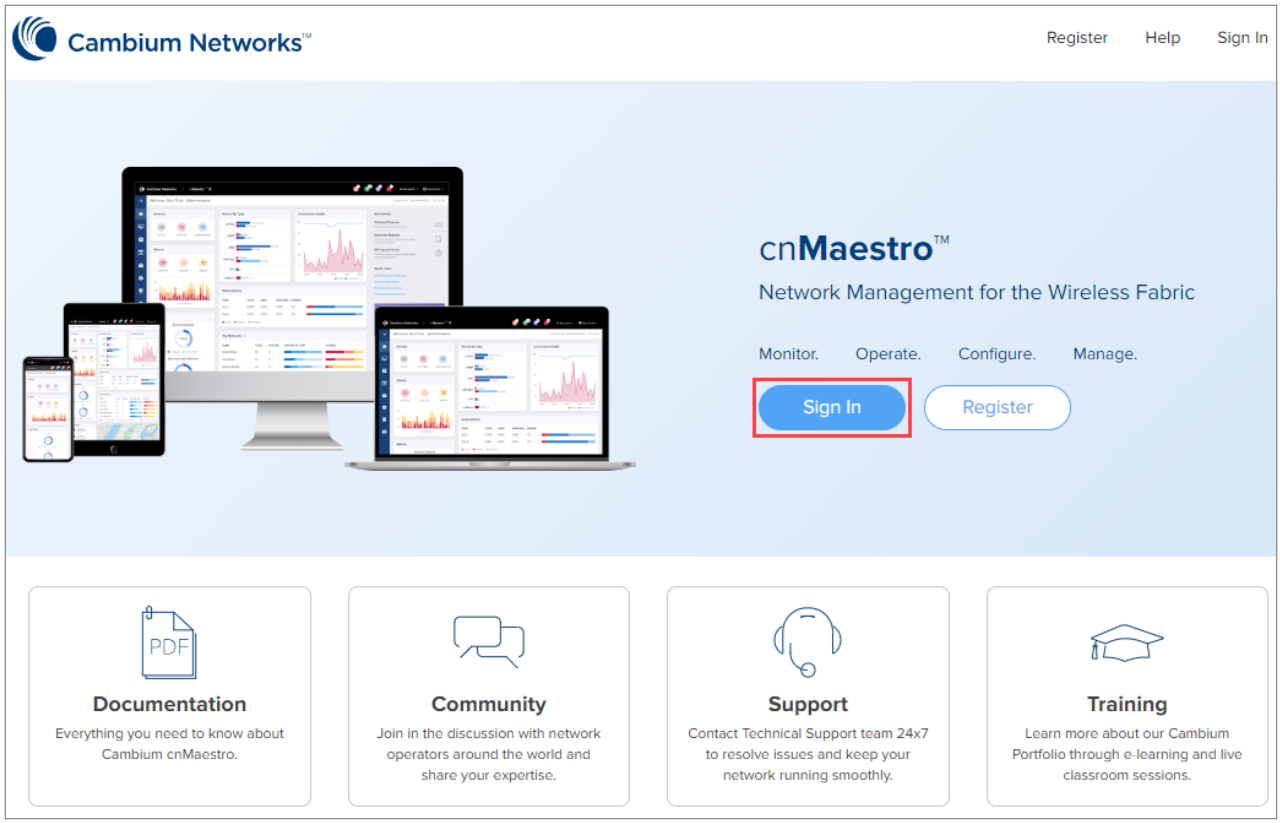
The following are part of the AP group:

- **Basic**
- **Management**
  - Administrator Access
  - Time Settings
  - Event Logging
  - SNMP
- **Radio**
- **Network**
  - WAN Configuration
  - LAN Configuration
- **Security**
  - DoS Protection
  - Access Control List (ACL)

To configure an AP group, complete the following steps:

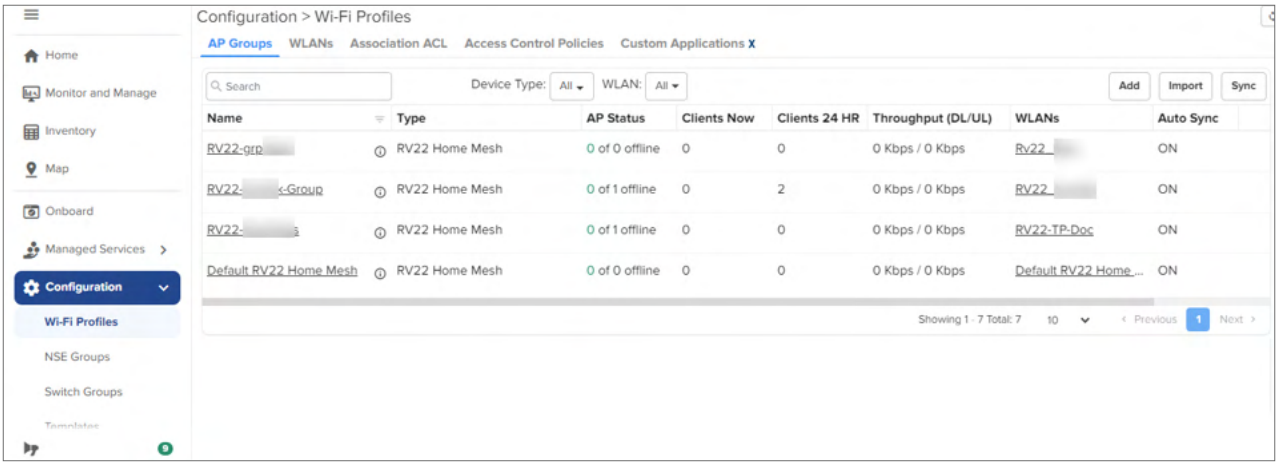
1. Sign in to cnMaestro.

   The home page appears.



2. Navigate to **Configuration** > **Wi-Fi Profiles**.

   The **AP Groups** page under **Wi-Fi Profiles** appears, by default.



3. Click **Add**.

   The **Add New** window appears with multiple tabs. By default, the **Basic** tab is selected.

4. In the **Add New** window > **Basic** tab, select **RV22 Home Mesh** in the **Type** drop-down list and configure the parameters described in Table 92.

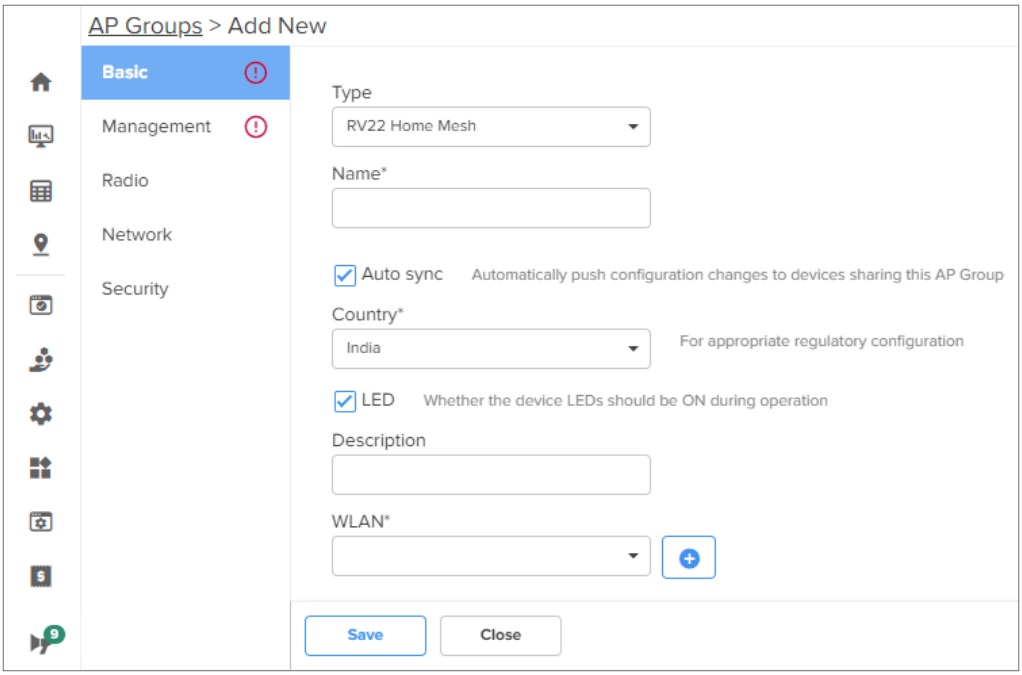


Table 92 *Basic parameters*

Parameter	Description
Type	Type of device for which the AP group is configured. Select **RV22 Home Mesh** from the drop-down list.
Name	Hostname of the device. Supports a maximum of 64 characters.
Auto sync	Specifies whether configuration is applied to the router automatically after saving. Select the check box to enable auto sync of configuration.

Parameter	Description
Country	Country from where the device is operated. To be set by the administrator only. The allowed operating channels and the respective transmit power levels depend on the country of operation. The list of countries supported depends on the SKU of the device (FCC and ROW). **Note**: Radios remain disabled unless this parameter is configured.
LED	When enabled, turns on the device LEDs during operation.
Description	Brief description for the AP group.
WLAN	WLAN profile to be associated with this AP group. WLAN profile contains SSID details of the wireless network. Select the WLAN from the drop-down list. If no WLAN is configured, create one by clicking the add ( ) icon. For more information, See Configuring WLAN profiles (SSIDs).

5. Click the **Management** tab on the left pane and configure the parameters described in Table 93.

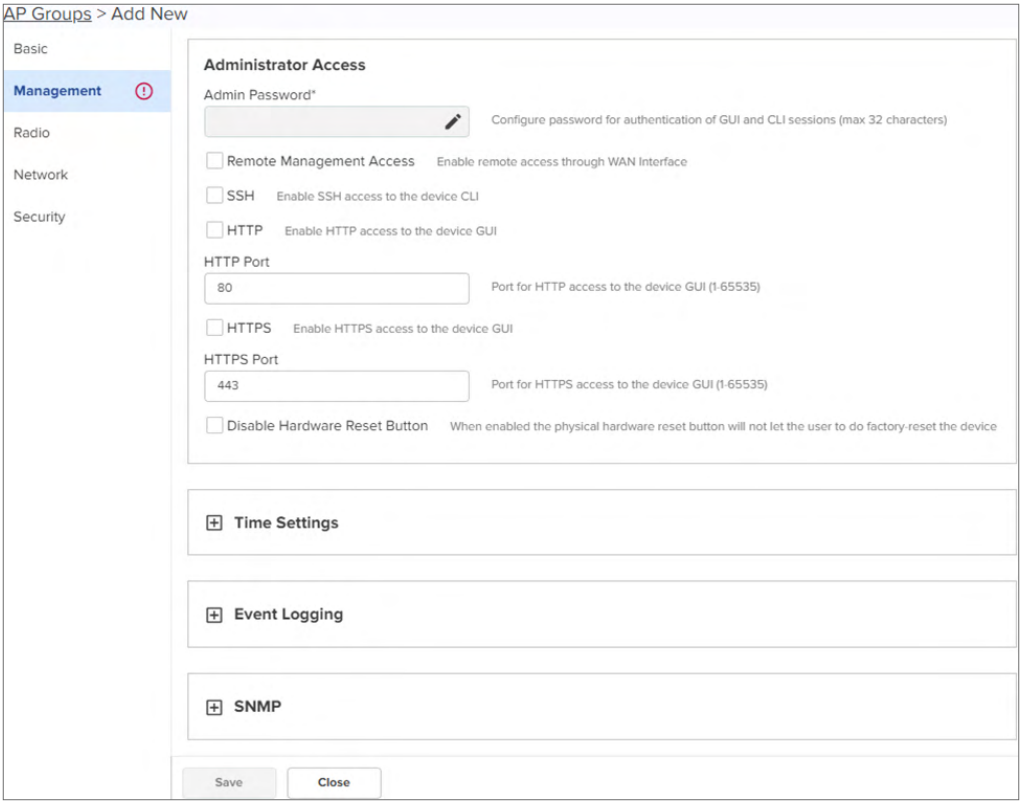


Table 93 *Management parameters*

Parameter	Description
Administrator Access	
Admin Password	Password required for authentication of the router.
Disable Hardware	Determines whether the reset button on the router is required to prevent a factory

Parameter	Description
Reset Button	reset operation of the router. Select the check box to prevent the user from performing the factory reset operation.
Time Settings	
Time Zone	Time zone of the location where the router is installed. Select an appropriate time zone from the drop-down list.
NTP Server 1	Hostname or IPv4 address of the Network Time Protocol (NTP) server.
NTP Server 2	Hostname or IPv4 address of a second NTP server.
Event Logging	
Syslog Server	Hostname, IPv4, or IPv6 address of the Syslog server and the respective port number. Default port number: 514
Syslog Severity	The severity level of event that must be forwarded to the server. The supported severity levels (0-7) are based on RFC standards.
SNMP	
Enable	Determines whether SNMPv2c or SNMPv3 support on the router is enabled. Select the check box to enable SNMP support.
Trap Receiver IP	IPv4 address of the SNMP server to receive the SNMP traps. This parameter is appicable to both SNMP v2c and v3 versions.
Version	Specifies the SNMP version configured for the router. The following options are available: • v2c • v3
SNMPv2c	
SNMPv2c RO community	The SNMP v2c read-only community string used as a password when obtaining information from the router.
SNMPv2c RW community	The SNMP v2c read-write community string as a password when writing information to the router.
SNMPv3	
SNMPv3 Username	Username for the SNMPv3 server. Supports a maximum of 32 characters.
Enable Authentication	Indicates whether authentication is enabled for SNMP communication. Select the check box to enable authentication.
Authentication Protocol	Specifies the authentication protocol. The following options are available: • MD5 • SHA Cambium uses SHA-1 authentication protocol. By default, the **SHA** option is selected.

Parameter	Description
Authentication Password	Password used for authentication. Supports 8 to 32 characters.
Enable Encryption	Indicates whether encryption is enabled for SNMP communication. Select the check box to enable encryption.
Encryption Type	Specifies the encryption type. The following options are available: • AES • DES By default, the **AES** option is selected.
Encryption Password	Password used for encryption. Supports 8 to 32 characters.

6. Click the **Radio** tab on the left pane and configure the preferred radios (2.4 GHz or 5 GHz or both).

   By default, both the radios are enabled. You can disable only the 2.4 GHz radio.

   Configure the parameters (described in Table 94), which are similar across 2.4 and 5 GHz radios.

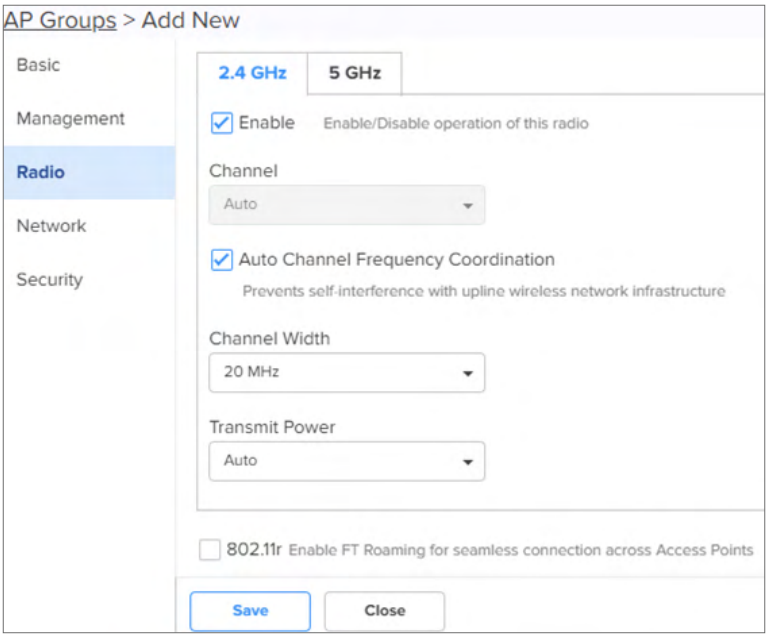
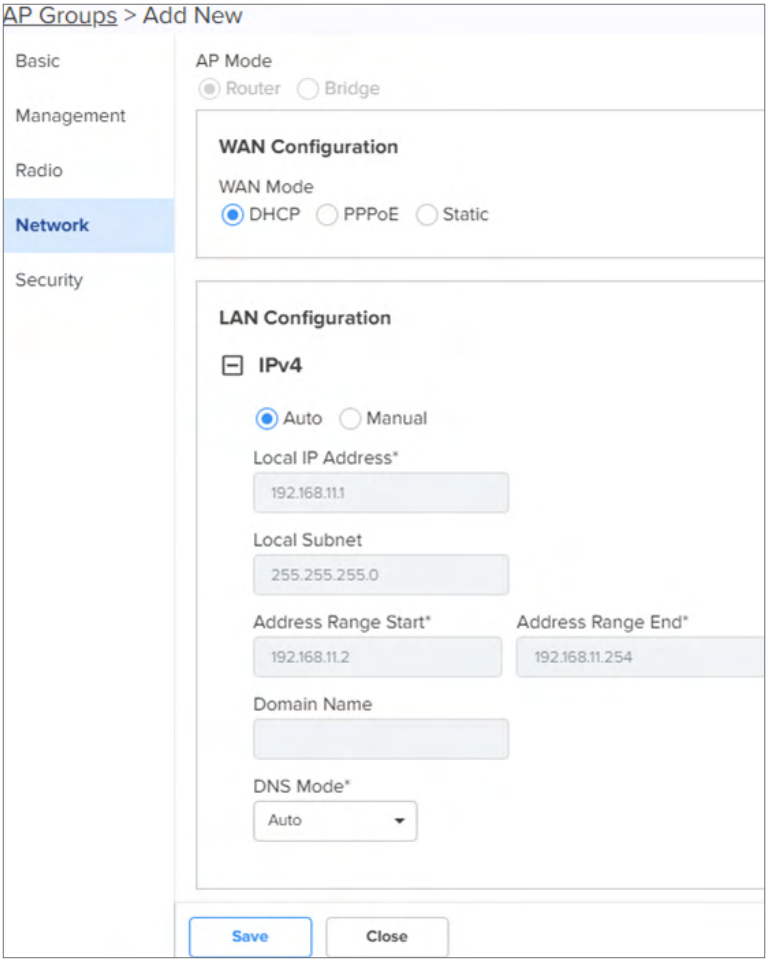


Table 94 *Radio parameters*

Parameter	Description
Enable	Enables the operation of radio.
Channel	This parameter cannot be modified. Default: Auto
Auto Channel Frequency Coordination	Enable to prevent router from self-interference with upline wireless network infrastructure.

Parameter	Description
Channel Width	Select the following channel widths for the operation: • For 2.4 GHz—20 MHz and 40 MHz channel widths are supported. Default: 20 MHz • For 5 GHz—20 MHz, 40 MHz, 80 MHz, and 160 MHz channel widths are supported. Default: 80 MHz
Transmit Power	Transmit power of the router in percentage (%). The following options are available: • Auto • 20 • 40 • 60 • 80 • 100

7. Click the **Network** tab on the left pane and configure the WAN mode and IP address assignment parameters.



a. The **AP Mode** is pre-configured as **Router** and cannot be modified.

b. In the **WAN Configuration** section, select the required WAN mode and configure the corresponding parameters.

This mode selects the mode of IP address assignment for the WAN interface. The following WAN modes are supported:

- **DHCP**—This mode is selected by default.

  No additional parameter configuration is required.

- **PPPoE**—Configure the PPPoE parameters as described in Table 95.

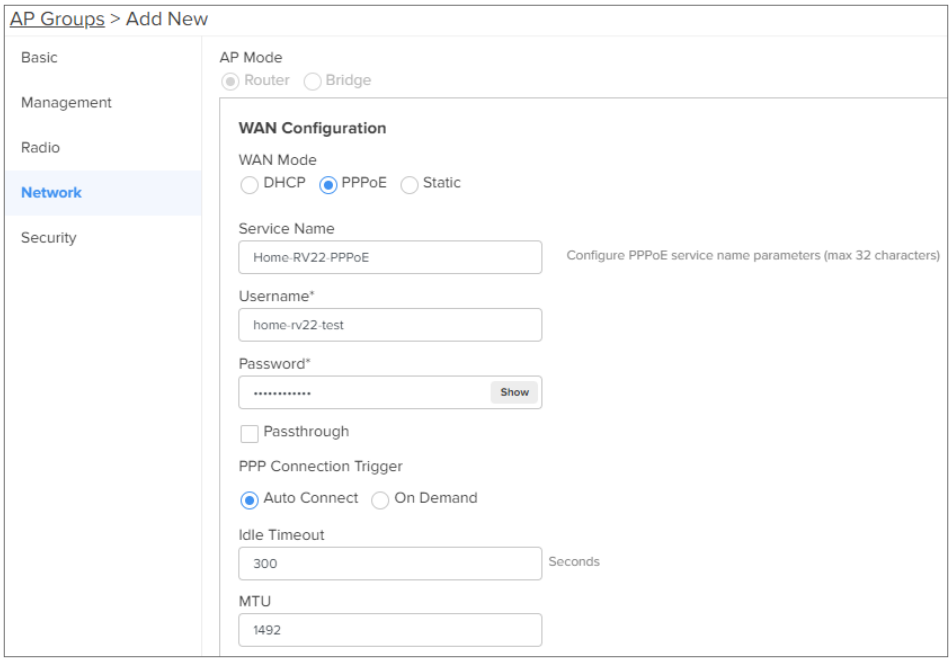


Table 95 *WAN Mode: PPPoE parameters*

Parameter	Description
PPPoE-related parameters	
Service Name	Name of the PPPoE service name. Supports a maximum of 32 characters.
Username	Username of the PPPoE service required for authentication.
Password	Password of the PPPoE service required for authentication.
Passthrough	Indicates whether the clients must directly establish connection with the service provider. Select the check box to enable passthrough.
PPP Connection Trigger	Indicates the connection method for the router for keeping the connection intact. The following options are supported: • Auto Connect

Table 95 *WAN Mode: PPPoE parameters*

Parameter	Description
	• On Demand
Idle Timeout	This parameter is mandatory when you select **On Demand** type of **PPP Connection Trigger**. Specifies the duration (in seconds) after which PPPoE keep-alive packets must be sent to keep the connection intact. Default: 300
MTU	Maximum size (in bytes) of each packet sent in a single transmission between connected devices. Default: 1492

- **Static**—Configure the Static parameters as described in Table 96.

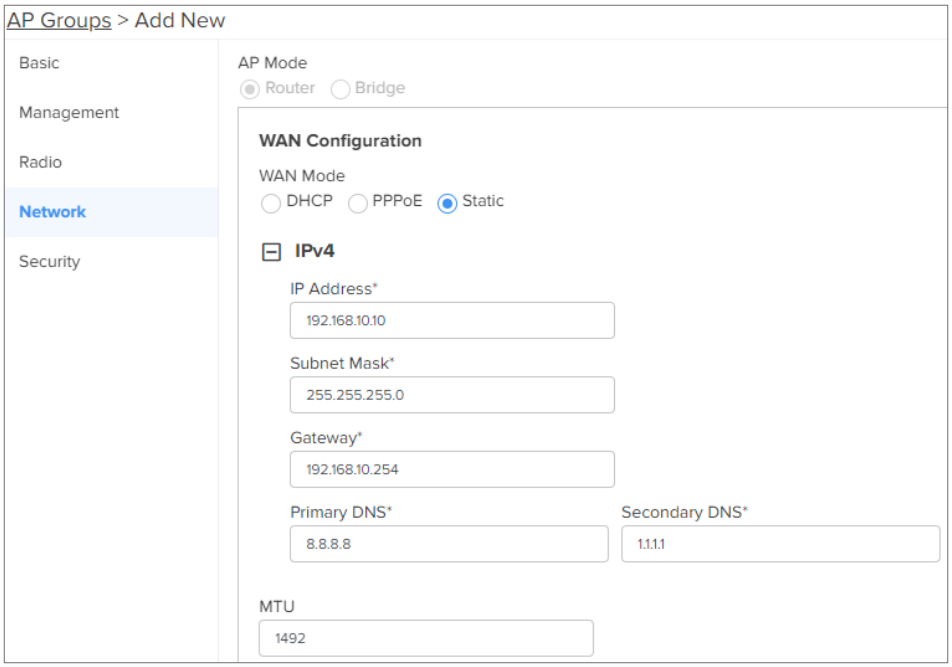


Table 96 *WAN Mode: Static parameters*

Parameter	Description
Static-related parameters	
IP Address	IPv4 address assigned to the router.
Subnet Mask	Subnet mask assigned to the router's IPv4 address.
Gateway	IPv4 address of the gateway used for communication.
Primary DNS	IPv4 address of the primary DNS server.
Secondary DNS	IPv4 address of the secondary DNS server.
MTU	Maximum size (in bytes) of each packet sent in a single transmission between connected devices. Default: 1492

Note

If you select **PPPoE** or **Static** mode, you must preconfigure the settings in the router before shipping the routers to customers. Complete the following steps before shipping the Home Mesh Router to the customers:

1. Onboard the Home Mesh Router using the standard WAN mode as **DHCP**.
2. After the Home Mesh Router is onboarded, set the WAN mode to **PPPoE** or **Static**.
3. Configure the username and password credentials.

   The configuration and the credentials are applied on the Home Mesh Router.
4. Disconnect the Home Mesh Router and ship it to the customer.

   When the customer connects the router to the PPPoE authenticated network, the Home Mesh Router uses the PPPoE credentials to authenticate.

c. In the **LAN Configuration** section, configure the mode of IP address assignment for connecting devices to **Auto** or **Manual**.

   If you select Manual mode of assignment, configure the following parameters:

Table 97 *LAN Configuration parameters for Manual mode*

Parameter	Description
IPv4-related parameters	
Local IP Address	Local IPv4 address assigned to the router.
Local Subnet	Subnet mask assigned to the router's IPv4 address.
Address Range Start	Starting IPv4 address in the address pool.
Address Range End	Ending IPv4 address in the address pool.
Domain Name	The domain name.
DNS Mode	DNS mode used for IP address resolution. Following are the supported options: • Auto • Manual • Proxy

8. Click the **Security** tab on the left pane and configure protection against different types of attacks, such as Smurf attack and ICMP fragment.

   Select the check box corresponding to the DoS protection options.

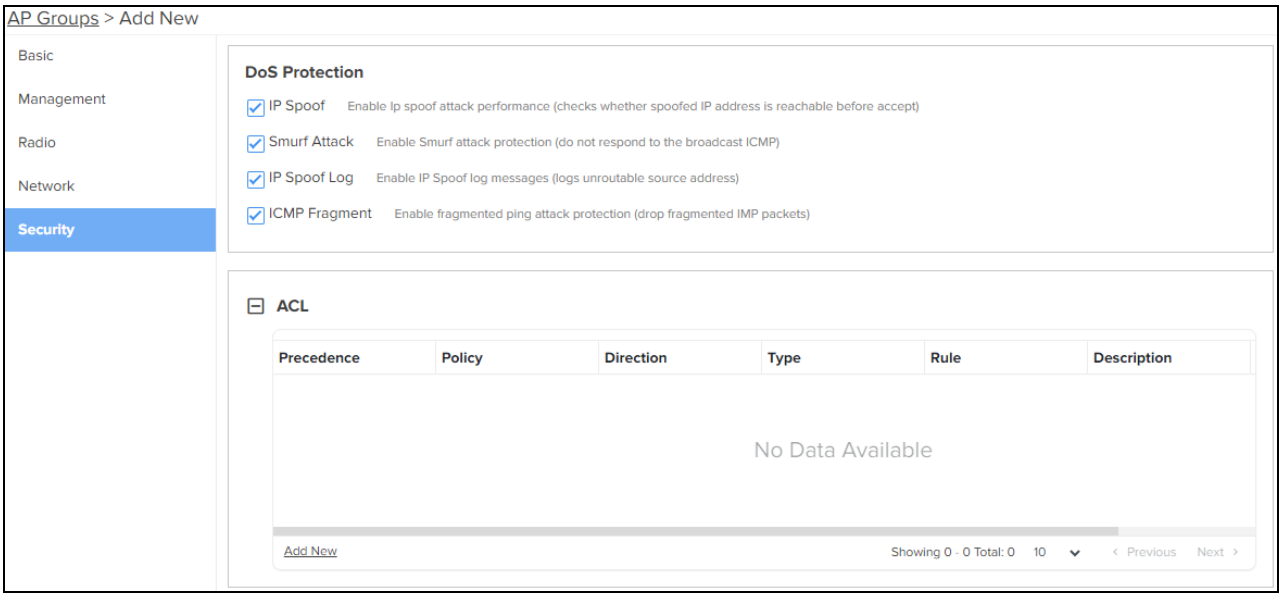


Table 98 *Security parameters: DoS Protection*

Parameter	Description
IP Spoof	Enable protection agains IP spoof attacks. When enabled, the router checks whether the spoofed IP address is reachable before accepting.
Smurf Attack	Enable protection agains Smurf attacks. When enabled, the router does not respond to the broadcast ICMP.
IP Spoof Log	Enable logging of IP spoof addresses. When enabled, the router logs the unroutable source IP address.
ICMP Fragment	Enable protection against ICMP fragmented ping attack. When enabled, the router drops the fragmented ICMP packets.

9. Click **Add New** in the **ACL** section and configure the parameters as described in Table 98.

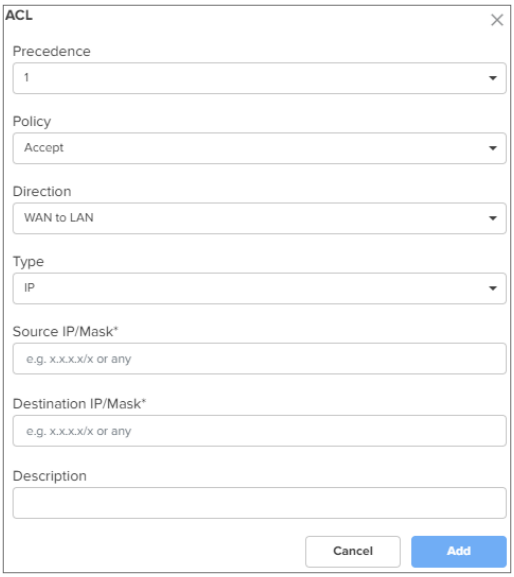


Table 99 *Security parameters: Access Control List (ACL)*

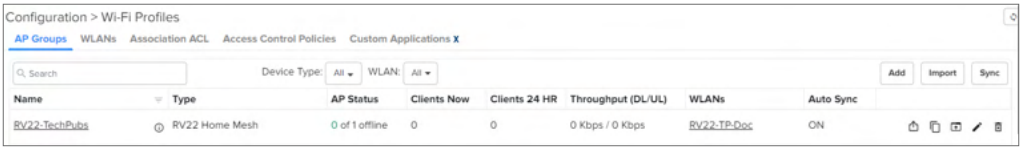
Parameter	Description
Precedence	Specifies the priority of the rule configured. Select the precedence from the drop-down list.
Policy	Indicates the action to be taken for the policy. The following are the supported actions: • Accept • Drop • Reject
Direction	Direction to which the policy must be applied. The following are the supported options: • WAN to LAN • LAN to WAN • WAN to Router • Router to WAN
Type	Type of traffic to which the policy must be applied. The following are the supported options: • IP • IPv6 • MAC • Protocol • Protocolv6 Additional parameters are enabled when you selct the type.
Source IP/Mask Destination IP/Mask	This field is applicable when you select the **Type** as **IP**, **IPv6**, **Protocol**, or **Protocolv6**. Specifies the source IPv4 or IPv6 address and the destination IPv4 or IPv6 address for the policy. You can configure **Any** if there is no specific IP address to apply the policy to any source IP address.
Source MAC/Mask Destination MAC/Mask	This field is applicable when you select the **Type** as **MAC**. Specifies the source MAC address and the destination MAC address for the policy. You can configure **Any** if there is no specific MAC address to apply the policy to any source IP address.
Protocol	Type of protocol for which the policy must be applied. The following are the supported options: • TCP • UDP • ICMP

Table 99 *Security parameters: Access Control List (ACL)*

Parameter	Description
	• Any Additional parameters are enabled when you selct the protocol.
Source Port	This field is applicable when you select the **Protocol** as **TCP**, **UDP**, or **Any**. Specifies the source port number for the policy.
Destination Port	This field is applicable when you select the **Protocol** as **TCP**, **UDP**, or **Any**. Specifies the source port number for the policy.
Description	Description for the rule.

10. Click **Save**.

    The AP group is successfully created with the configured parameters.



Onboarding the Home Mesh Router to cnMaestro

After creating a WLAN profile and an AP group, you must now create a subscriber profile and associate it with the subscriber. Finally, you must onboard the router(s) to the corresponding subscriber.

Adding a subscriber and onboarding the router involves the following steps:

1. cnMaestro Subscriber application branding
2. Adding a Home Site
3. Adding a Subscriber Service Profile
4. Adding a subscriber
5. Claiming the Home Mesh Router

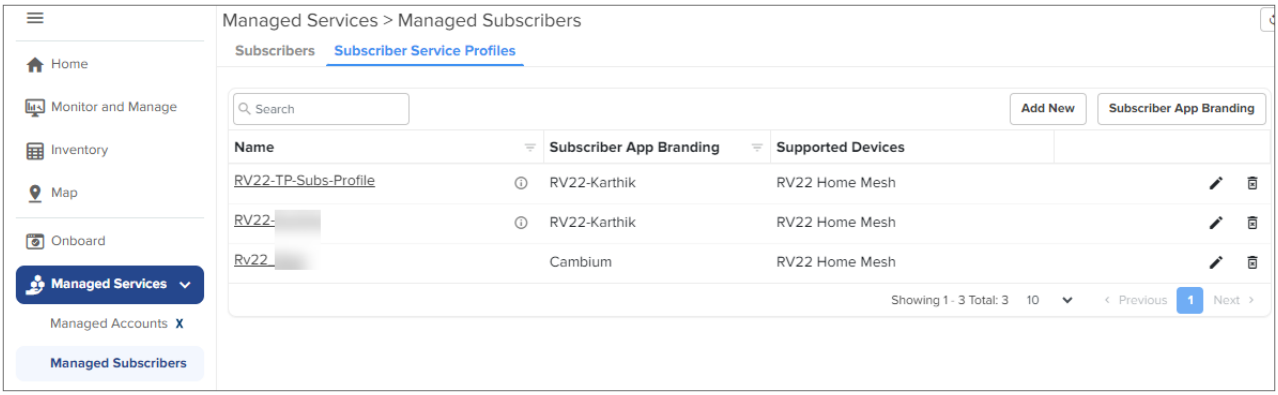
cnMaestro Subscriber application branding

Customize the cnMaestro Subscriber mobile application with your company name, brand logo, and other details, such as support contact information and hours. This branding can be associated with individual subscriber service profiles.

To add brand details to the cnMaestro Subscriber application, complete the following steps:

1. Navigate to the **Manage Service Providers** > **Managed Subscribers** > **Subscriber Service Profiles** tab.

   The **Subscriber Service Profiles** page appears.



2. Click **Subscriber App Branding**.

3. Click the add (+) icon.

   The **Subscriber App Branding** window appears. Configure the following parameters as described in Table 100.

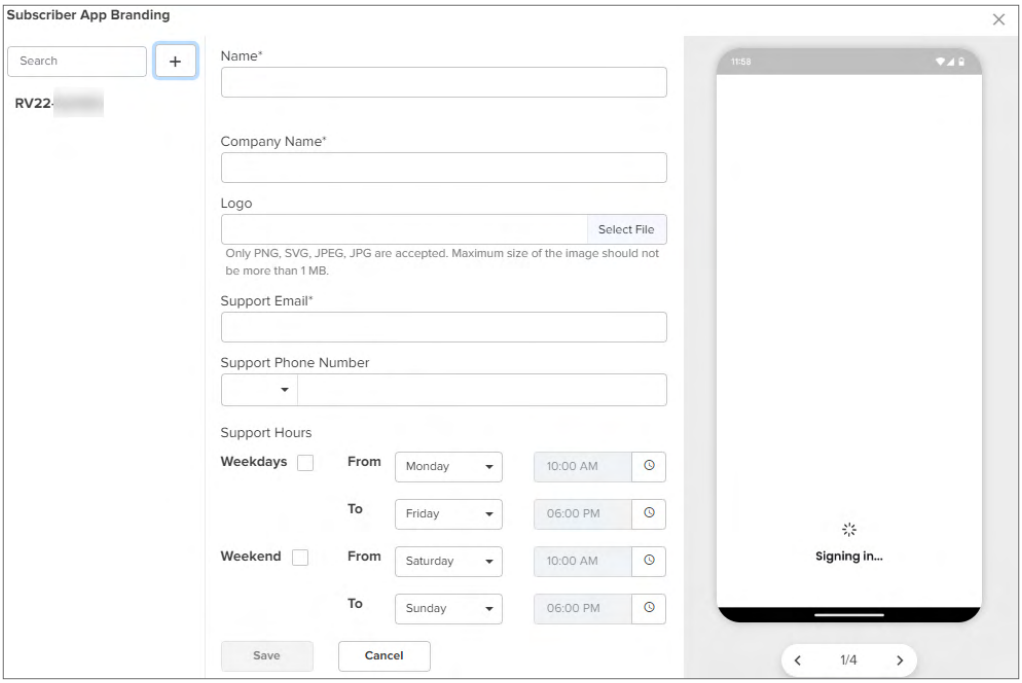


Table 100 *Subscriber App Branding parameters*

Parameter	Description
Name	Name of the application branding.
Logo	Brand logo displayed in the cnMaestro Subscriber application. Maximum size of the image supported is 1 MB. Only JPEG, JPG, PNG, and SVG file formats are supported.
Support Email	Email address for customer support team displayed in the application.
Support Phone	Phone number for customer support team displayed in the application.

Parameter	Description
Number	
Support Hours	Contact hours for the customer support team. • Select the **Weekdays** check box and configure the week days on when the customer support team is available. You can also configure the time using the time picker tool. • Select the **Weekends** check box and configure the weekend days on when the customer support team is available. You can also configure the time using the time picker tool.

You can preview your branding updates by scrolling through the images in the preview window on the right.

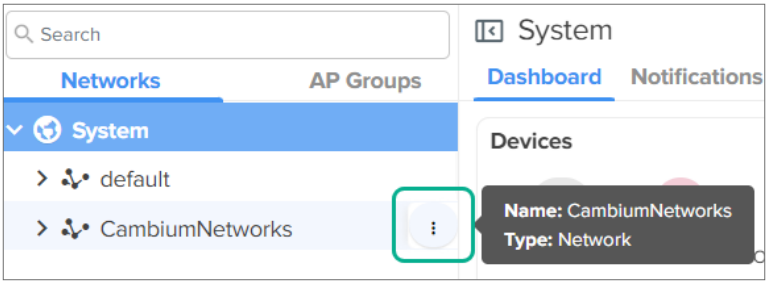
4. Click **Save**.

Adding a Home Site

A home site is required to associate the subscriber's device with the device configuration.

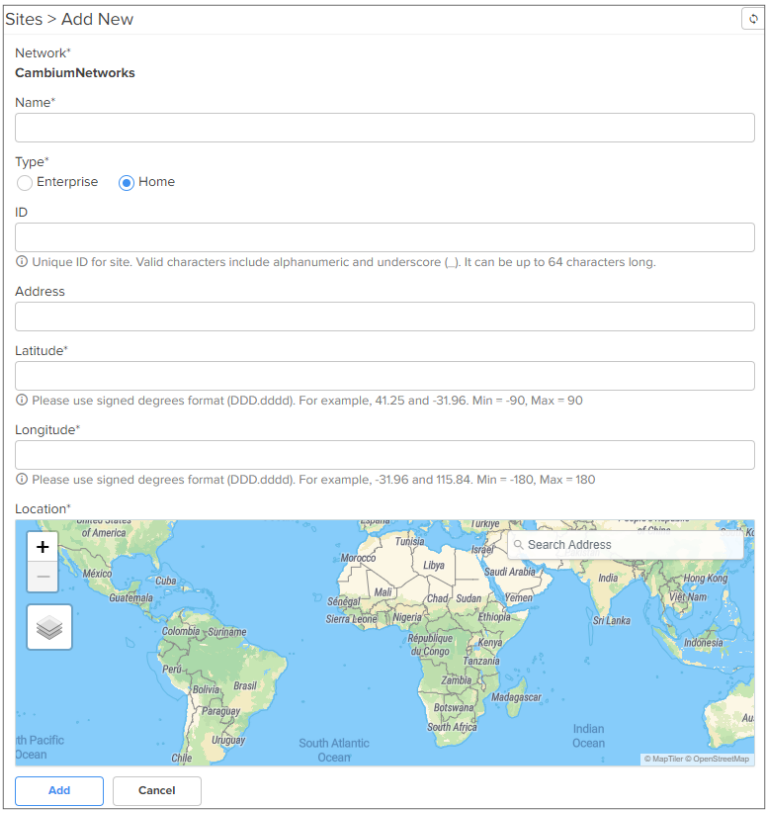
To create a home site, complete the following steps:

1. Click **Monitor and Manage** ( ).
2. In the **Networks** tab, search for the network and hover over the network name.



3. Click the actions ( ) icon and select **Add Site**.

   The **Sites** > **Add New** page appears.



4. Select the **Home** option in the **Type** field.
5. Enter the location details in the **Longitude** and **Latitude** fields.

   You can also search for the location in the map to fill in the details.
6. Click **Add**.

Managing subscribers (end-customer)

To enable a subscriber to manage the router using the Android or iOS application, you must add a subscriber profile in cnMaestro and send an invitation to the subscriber.

This pocess involves the following actions:

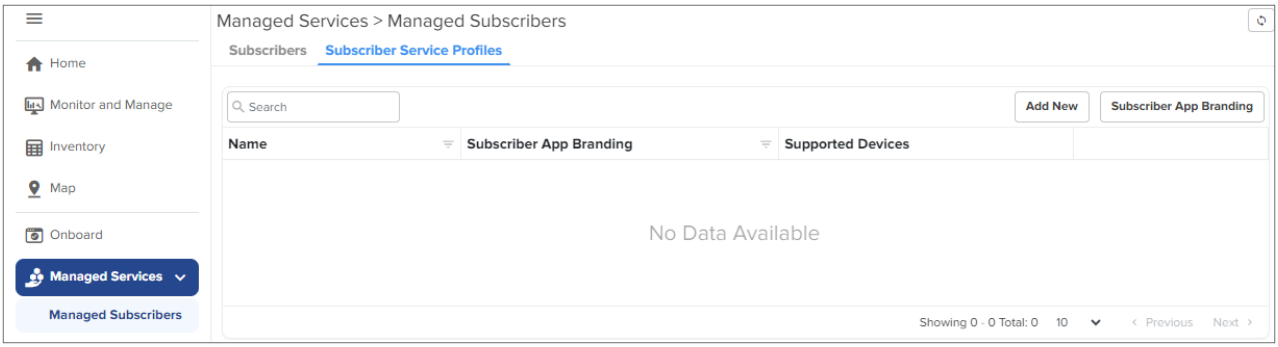
1. Adding a Subscriber Service Profile
2. Adding a subscriber
   a. Modifying the owner details for the Subscriber App
3. Claiming the Home Mesh Router

Adding a Subscriber Service Profile

To add a subscriber service profile, complete the following steps:

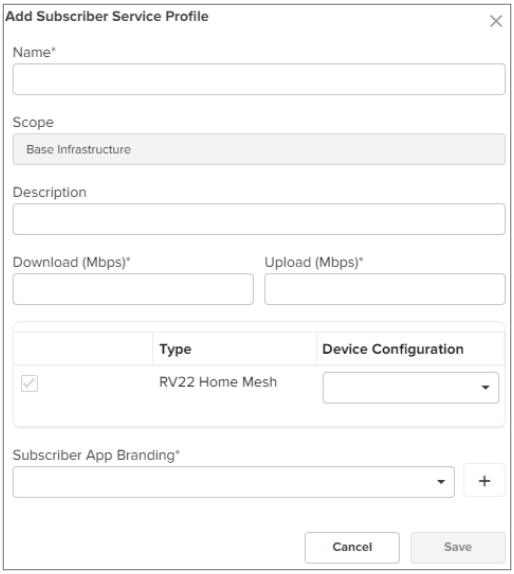
1. Navigate to the **Manage Services** > **Managed Subscribers** > **Subscriber Service Profiles** tab.

   The **Subscriber Service Profiles** page appears.



2. Click **Add New**.

   The **Add Subscriber Service Profile** window appears.



3. Select the Home Mesh Router configuration to which you want to associate with the subscriber service profile and configure the parameters as described in Table 101.

   Table 101 *Subscriber Service Profile parameters*

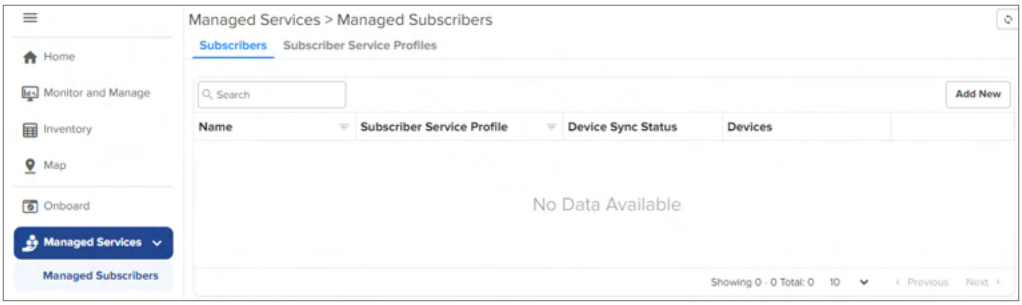
Parameter	Description
Name	Name of the subscriber service profile.
Description	Brief description for the subscriber service profile.
Download (Mbps)	Download speed (in Mbps) configured for the profile.
Upload (Mbps)	Upload speed (in Mbps) configured for the profile.
Type	Displays the device type as **RV22 Home Mesh**. This field cannot be modified.
Device Configuration	Specifies the Wi-Fi AP group (created for the Home Mesh Router device type) that must be associated with the service profile. Select the group from the drop-down list.
Subscriber App Branding	Specifies the cnMaestro Subscriber application branding that must be used in this profile.

Parameter	Description
	All routers sent to subscribers in this service profile contain the selected branding logo and information. Select the required branding from the drop-down list. If no branding is present, create one by clicking the add (+) icon. See cnMaestro Subscriber application branding for more information.

4. Click **Save**.

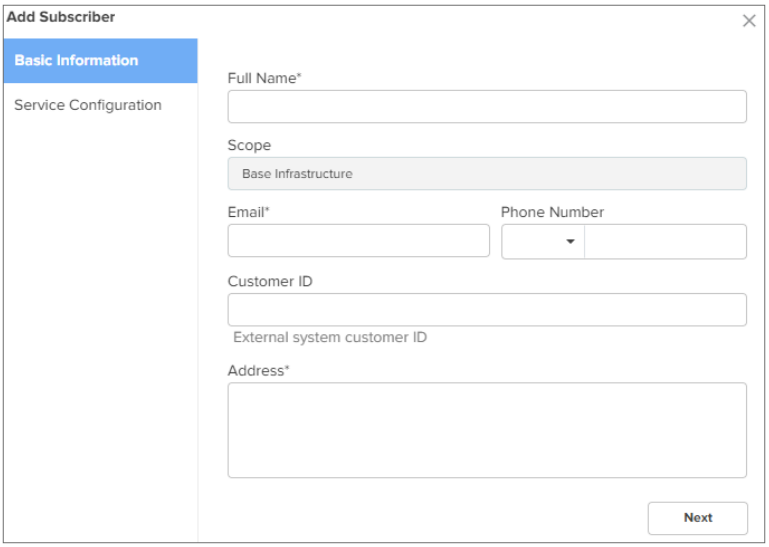
Adding a subscriber

5. Click the **Subscribers** tab on the **Managed Subscribers** page.



6. Click **Add New**.

   The **Add Subscriber** window appears.



7. In the **Add Subscriber** window, configure the details of the subscriber in the **Basic Information** section, as described in Table 102.

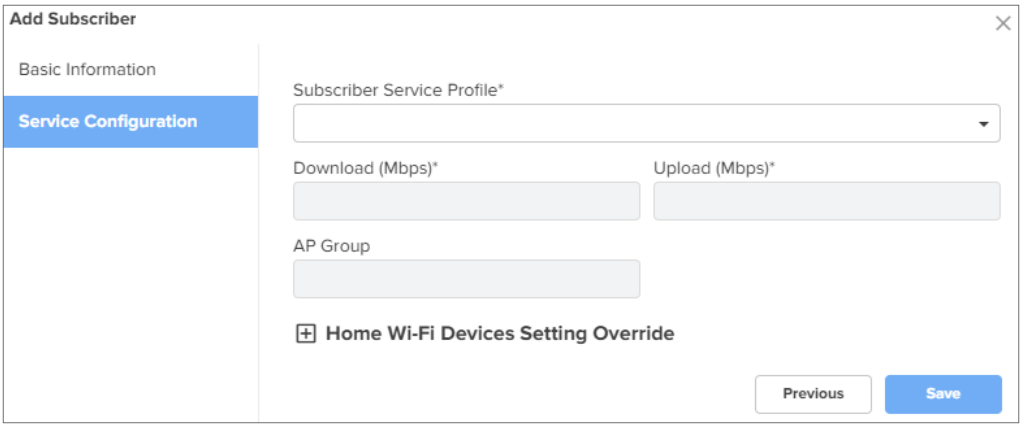
   Table 102 *Subscriber > Basic tab parameters*

Parameter	Description
Full Name	Name of the subscriber.
Email ID	Email address of the subscriber.

Parameter	Description
	This email address receives the invitation to join the Home Mesh Router (RV22) site. Through this email address the user will be able to access and manage the router as a primary user and invite other users (secondary users), through the mobile application, to manage the routers. **Note** You can edit this email address at anytime. However, editing this email address will remove all existing users, both primary and secondary. For information about how to modify the email ID, refer to Modifying the owner details for the Subscriber App.
Phone Number	Phone number of the subscriber.
Customer ID	Unique ID for the subscriber.
Address	Address of the subscriber where the routers will be installed.

8. Click **Next**.

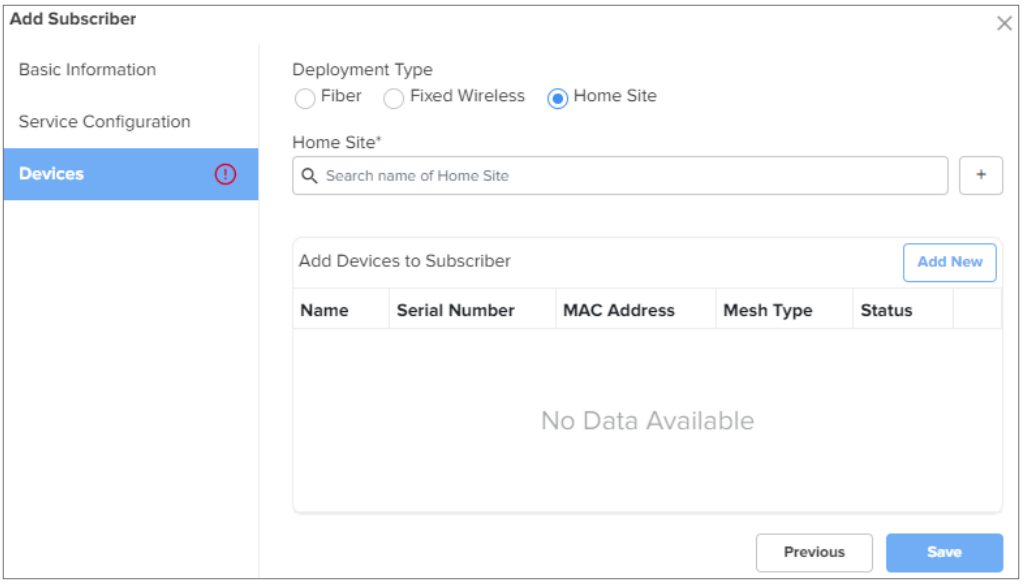
   The **Service Configuration** tab is displayed.



9. Select the subscriber service profile to be associated with this subscriber from the **Service Profile** drop-down list.
10. Click **Save**.

    A new tab, **Devices** appears, where you can link (or claim) the Home Mesh Router to the subscriber. See Claiming the Home Mesh Router.

    The cnMaestro Subscriber application invitation email is sent to the subscriber with the link to join the account.
11. Click **Devices**.



12. Select one of the following options in the **Deployment Type** field to filter the available deployment types:
    - **Fiber**—Select the Optical Network Unit (ONU) device that you want to associate with the subscriber's router by searching in the **ONU** search box.
    - **Fixed Wireless**—Select the Subscriber Module (SM) device that you want to associate with the subscriber's router by searching in the **SM** search box.
    - **Home Site**—Select the home site you want to associate with the subscriber's router by searching in the **Home Site** search box. To add a home site, see Adding a Home Site.
13. Before linking the Home Mesh Router to the subscriber, click **Save**.

Modifying the owner details for the Subscriber App

You can modify the owner details for the Subscriber App by modifying the email ID.

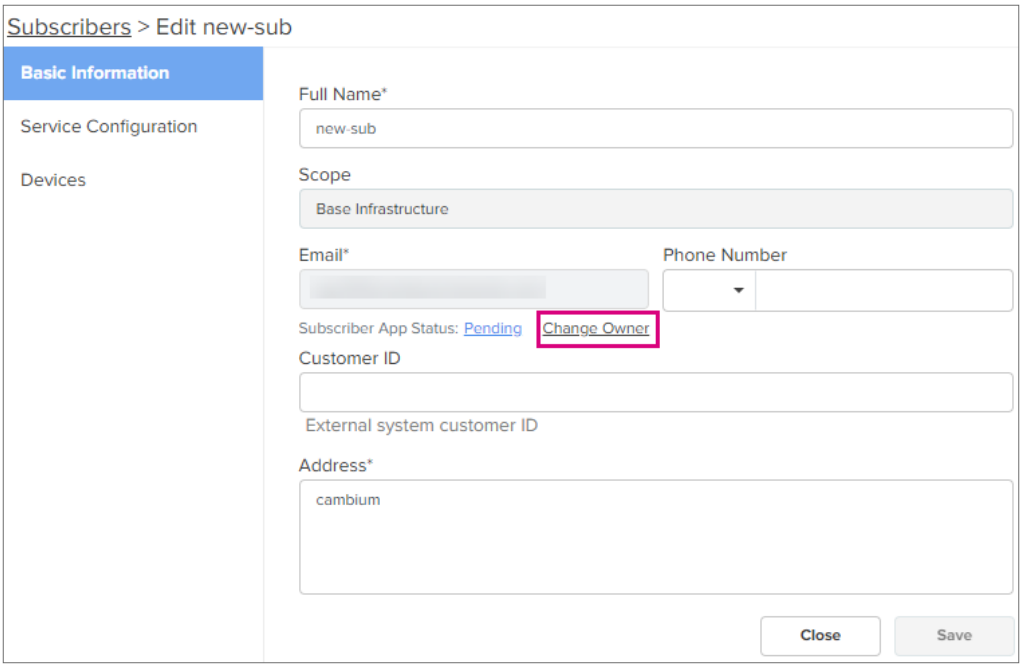
Warning

Modifying the email address will remove all existing users, both primary and secondary.

To modify the email address, complete the following steps:

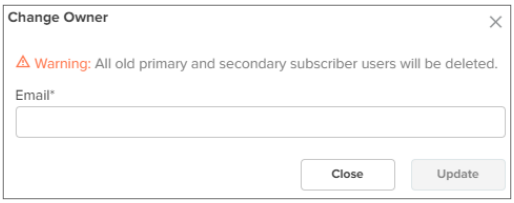
1. Navigate to the **Manage Services** > **Managed Subscribers** > **Subscribers** tab.
2. In the list of subscribers, click the subscriber name for which you want to modify the email ID.

   The corresponding subscriber details are displayed.



3. Under the **Email** parameter, click **Change Owner**.

   The Change Owner window is displayed.



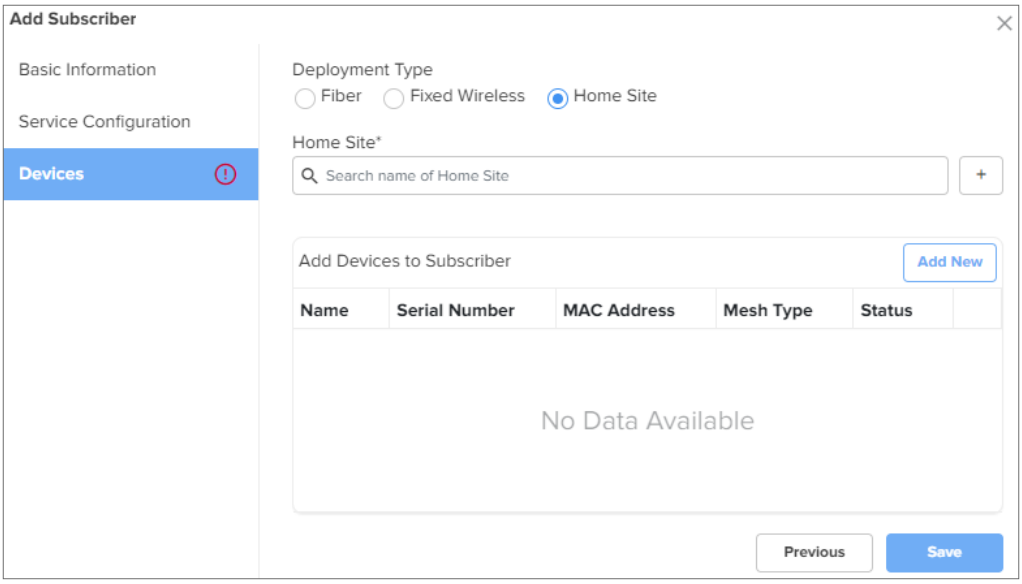
4. Enter the new email ID for the subscriber.
5. Click **Update**.

Claiming the Home Mesh Router

After adding a subscriber profile and a subscriber, you must now associate the Home Mesh Router to the subscriber by claiming the router in cnMaestro.

To claim the router, complete the following steps:

1. Navigate to the **Manage Services** > **Managed Subscribers** > **Subscribers** tab.
2. In the list of subscribers, select the subscriber name for which you want to associate the Home Mesh Router.
3. Click the **Devices** tab.
4. In the **Add Devices to Subscriber** section, click **Add New**.

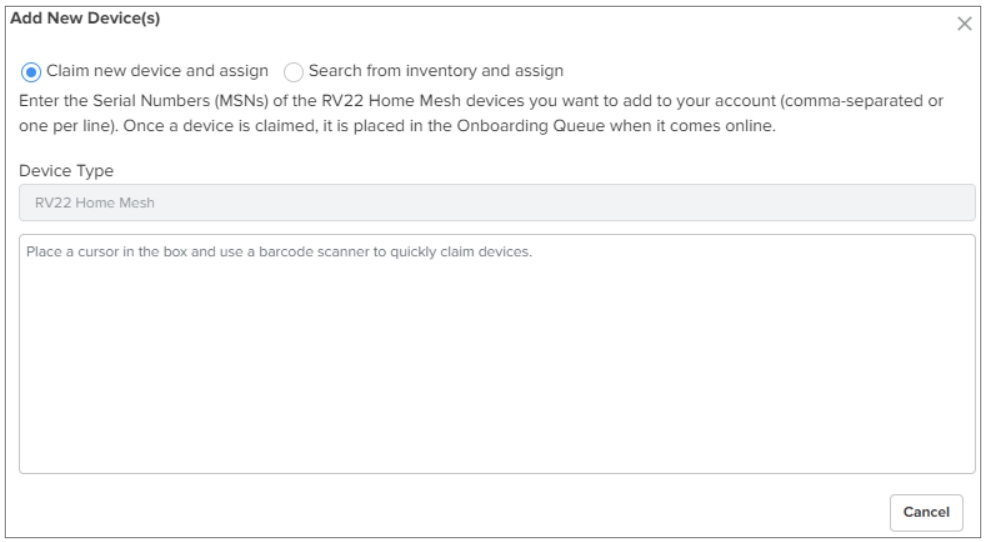


The **Link Subscriber** window appears.

5. In the **Link Subscriber** window, link the Home Mesh Router to the subscriber by using any of the following methods:

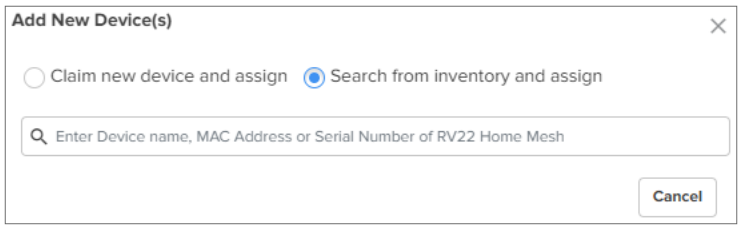
   - To claim a new router that is not onboarded to cnMaestro, select the **Claim new and assign** option and enter the serial number of the device to be claimed.

     You can claim multiple routers by adding multiple serial numbers separated by commas.



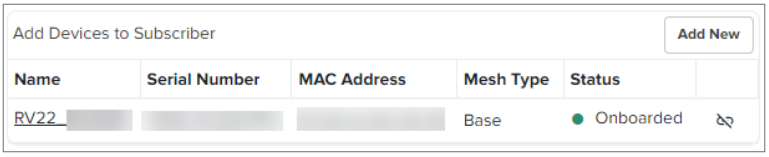
   - To claim a router that is already onboarded to cnMaestro, select the **Search for inventory and assign** option.

Enter the details of the router you want to claim.



6. Click **Assign**.

   The assigned router appears in the **Add Devices to Subscriber** section.



Note

Click the unlink ( ) icon to unlink the router from the subscriber.

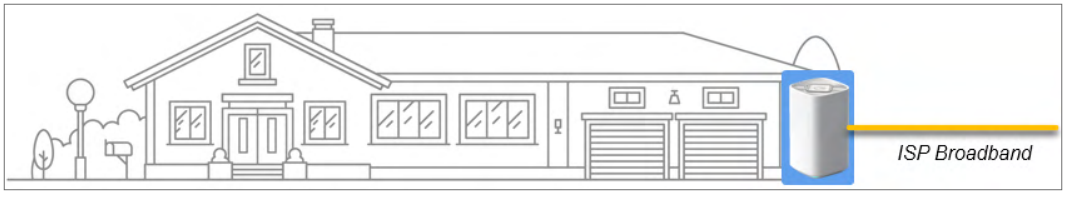
Setting up the Home Mesh Router

Home Mesh Routers can be deployed in one of the following modes:

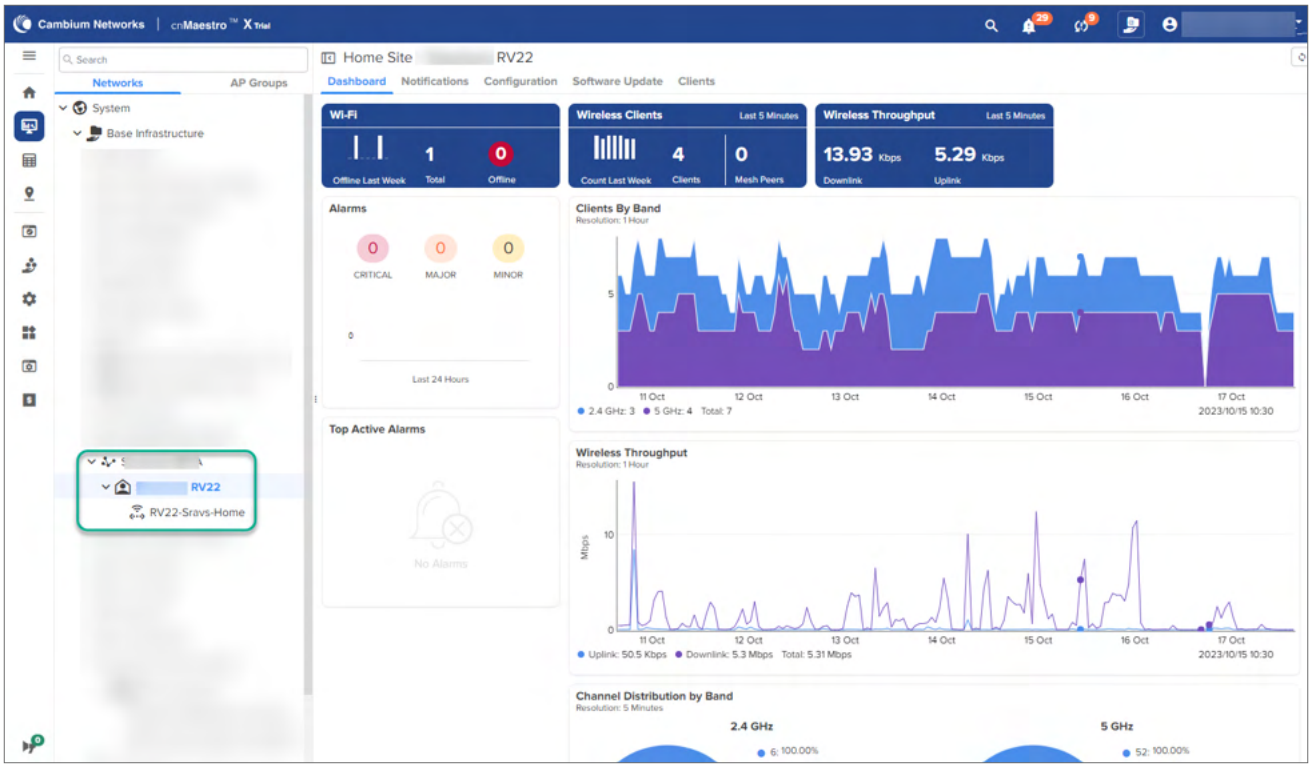
- Setting up the Home Mesh Router—Standalone mode
- Setting up the Home Mesh Router—Wireless Mesh Mode
- Setting up the Home Mesh Router—Wired Mesh Mode

Setting up the Home Mesh Router—Standalone mode

In standalone mode of deployment, there is only one Home Mesh Router deployed. A sample scenario is shown in the following figure:



A sample cnMaestro dashboard for the standalone mode of deployment is shown in the following figure:



Setting up the Home Mesh Router—Wireless Mesh Mode

To configure a wireless mesh, onboard the routers to a site—Claim all the routers, which you want to be part of the mesh, on cnMaestro in the subscriber workflow. See Claiming the Home Mesh Router. Connect the mesh base router to the internet and wirelessly connect the node routers. The AP group mapped to the subscriber is applied to all the routers to sync the configuration.

Following are some of the wireless mesh configuration scenarios and the corresponding dashboards and hierarchy in cnMaestro:

- Wireless mesh: 1-1 deployment
- Wireless mesh: 1-1-1 deployment
- Wireless mesh: 1-2 deployment
- Wireless and wired mixed mesh 1-2 deployment

Wireless mesh: 1-1 deployment

In this deployment, the base router is connected to one node router, thereby creating a wireless 1-1 mesh deployment.

Figure 442 *Wireless mesh: 1-1 deployment*

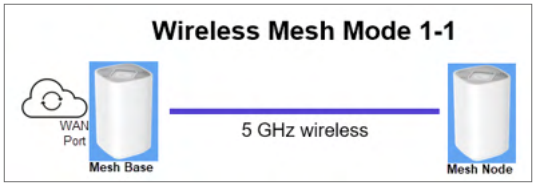


Figure 443 displays a sample cnMaestro dashboard for the wireless mesh 1-1 deployment.

Figure 443 *Sample dashboard for wireless mesh: 1-1 deployment*

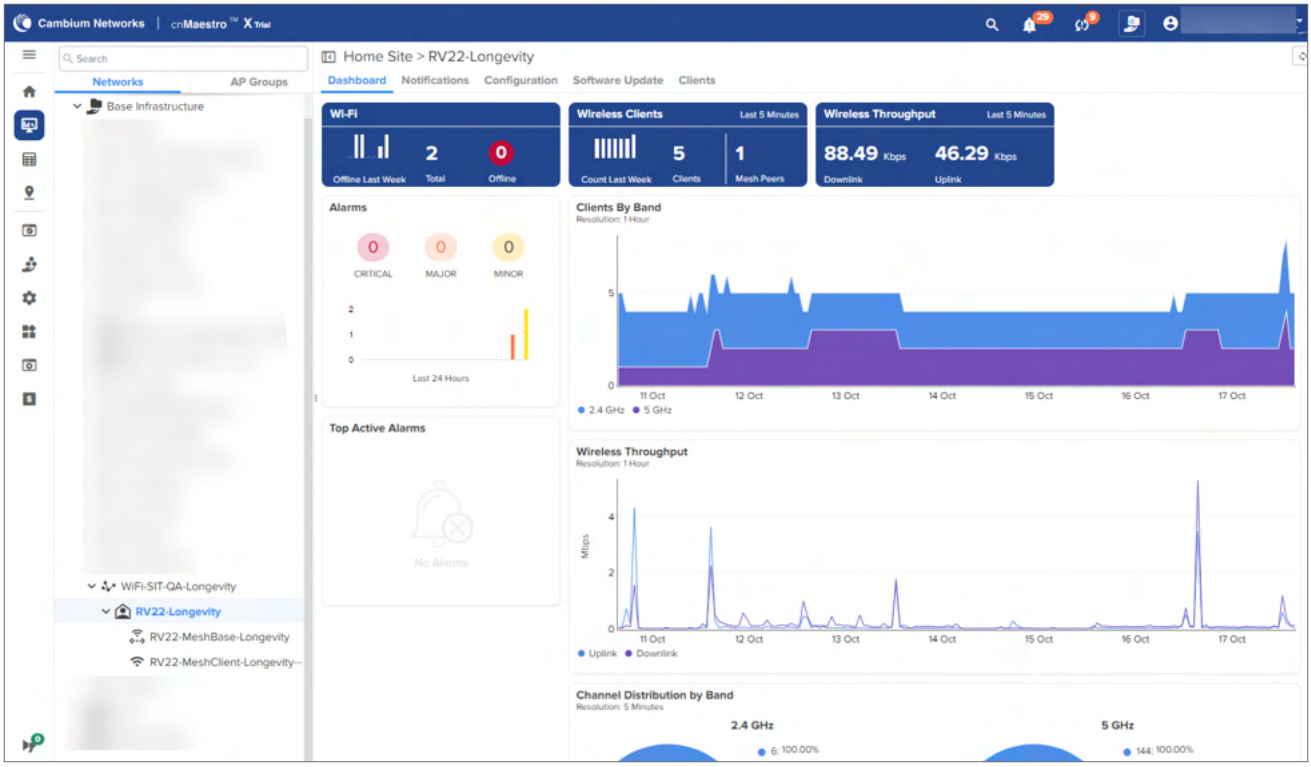
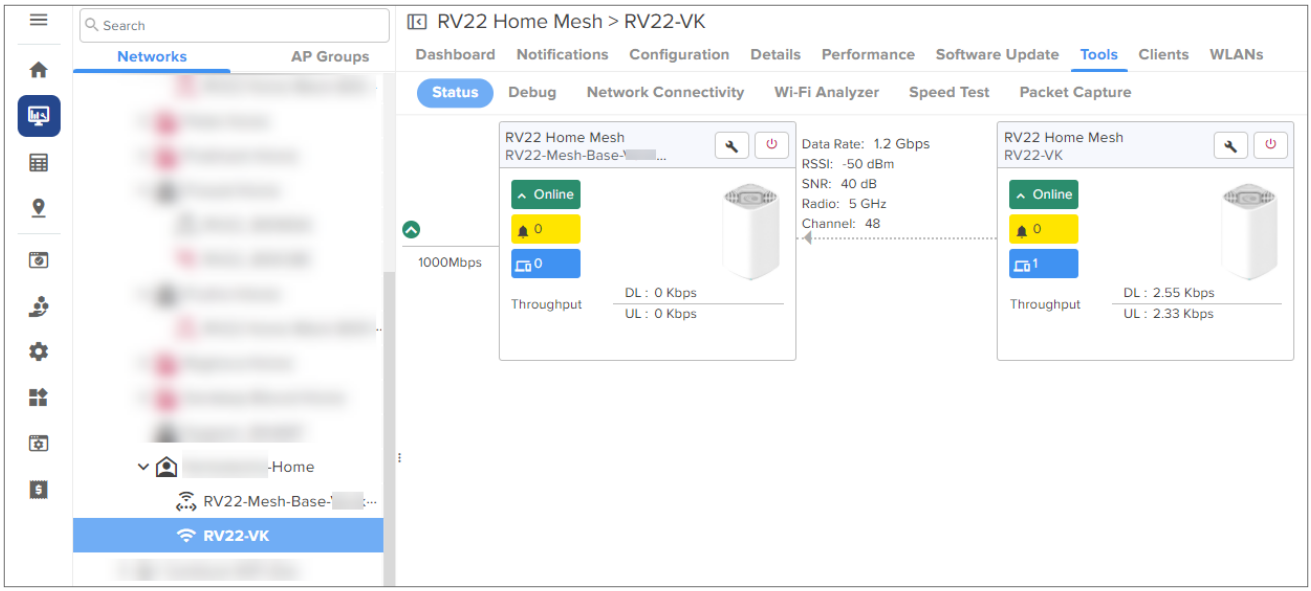


Figure 444 displays a sample cnMaestro status page for the wireless mesh 1-1 deployment.

Figure 444 *Sample status page for wireless mesh: 1-1 deployment*



Wireless mesh: 1-1-1 deployment

In this deployment, the base router is connected wirelessly to only one of the node routers, which is in turn connected to another node router, thereby creating a wireless 1-1-1 mesh deployment.

Figure 445 *Wireless mesh: 1-1-1 deployment*

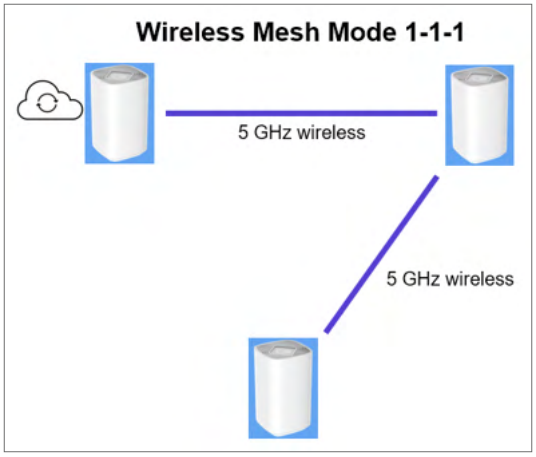


Figure 446 displays a sample cnMaestro dashboard for the wireless mesh 1-1-1 deployment.

Figure 446 *Sample dashboard for wireless mesh: 1-1-1 deployment*

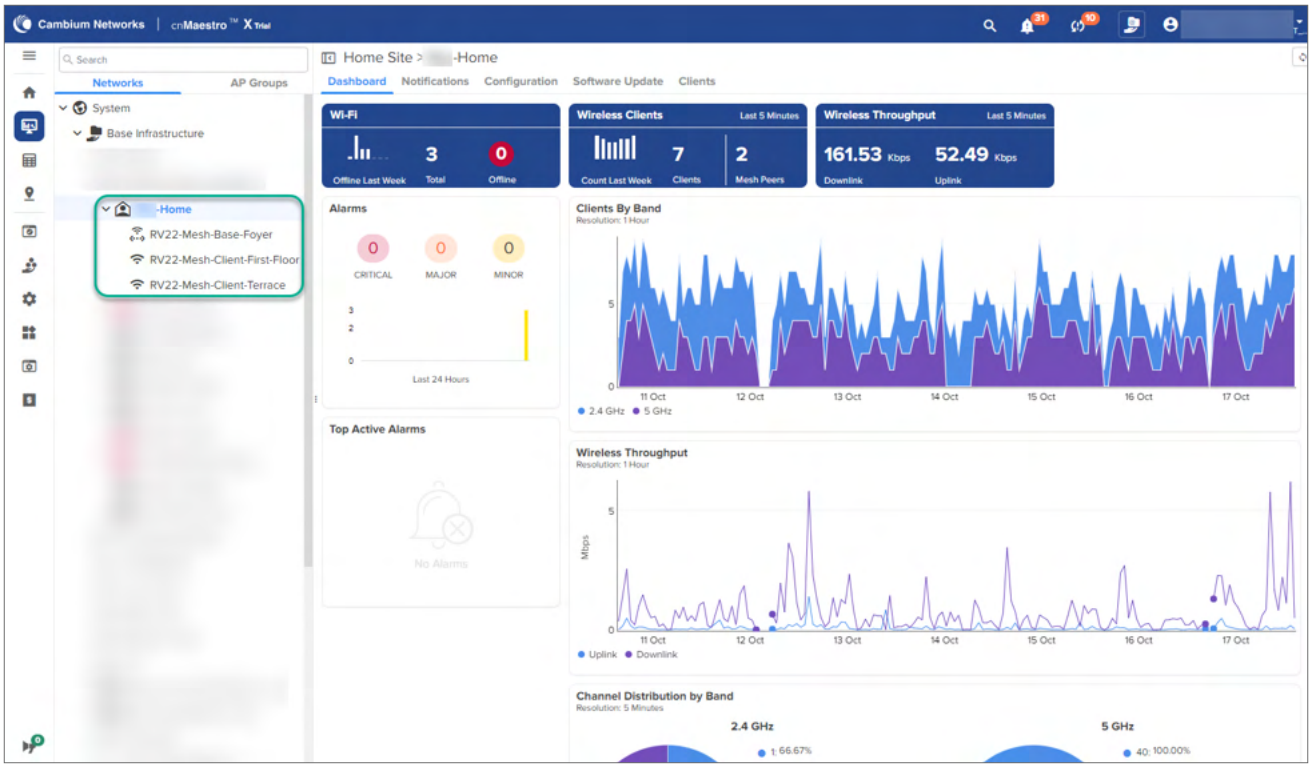
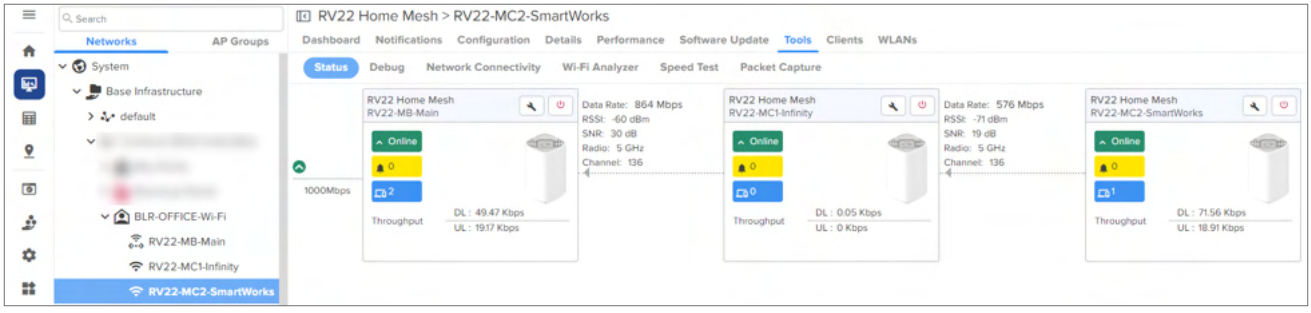


Figure 447 displays a sample cnMaestro status page for the wireless mesh 1-1-1 deployment.

Figure 447 *Sample status page for wireless mesh: 1-1-1 deployment*



Wireless mesh: 1-2 deployment

In this deployment, the base router is connected to two node routers simultaneously, thereby creating a wireless 1-2 mesh deployment.

Figure 448 *Wireless mesh: 1-2 deployment*

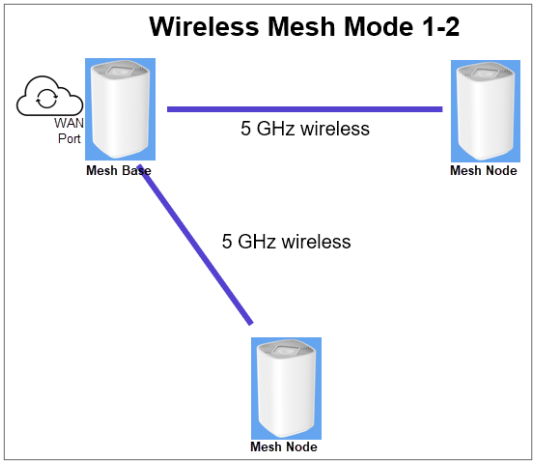


Figure 449 displays a sample cnMaestro dashboard for the wireless mesh 1-2 deployment.

Figure 449 *Sample dashboard for wireless mesh: 1-2 deployment*

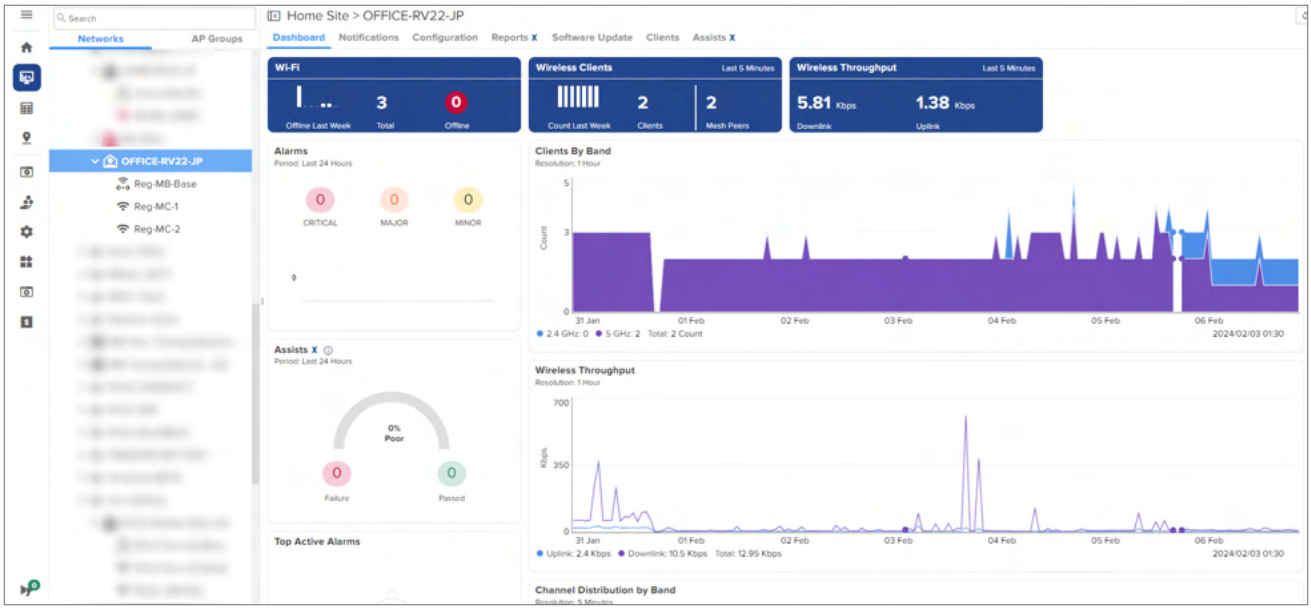
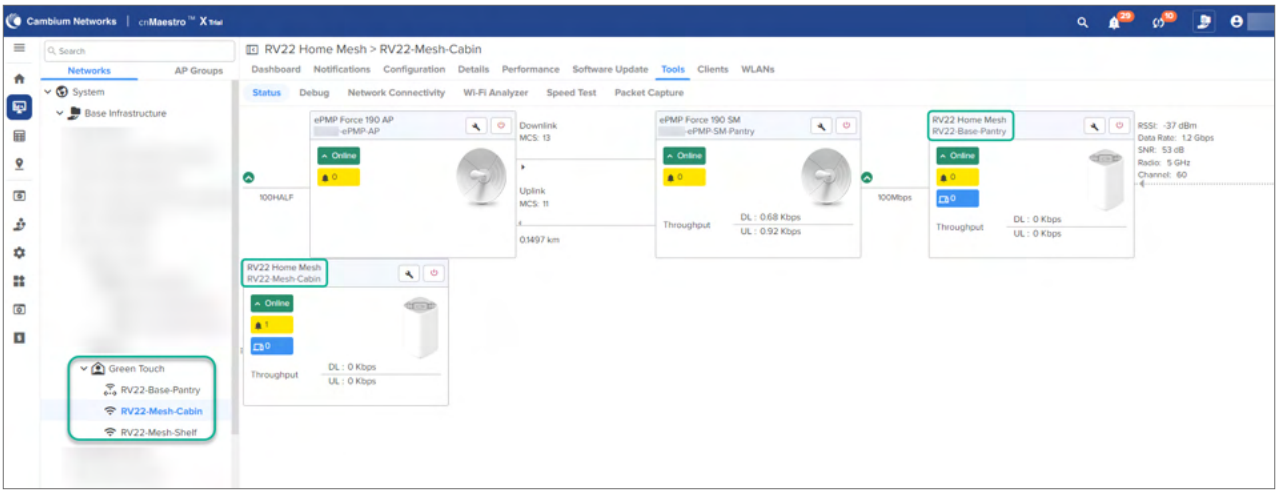


Figure 450 and Figure 451 display sample status pages for the node routers in a wireless mesh 1-2 deployment.

In the following status samples, the **RV22-Base-Pantry** router is connected to both **RV22-Mesh-Shelf** and **RV22-Mesh-Cabin** routers, forming a 1-2 multi-mesh topology.

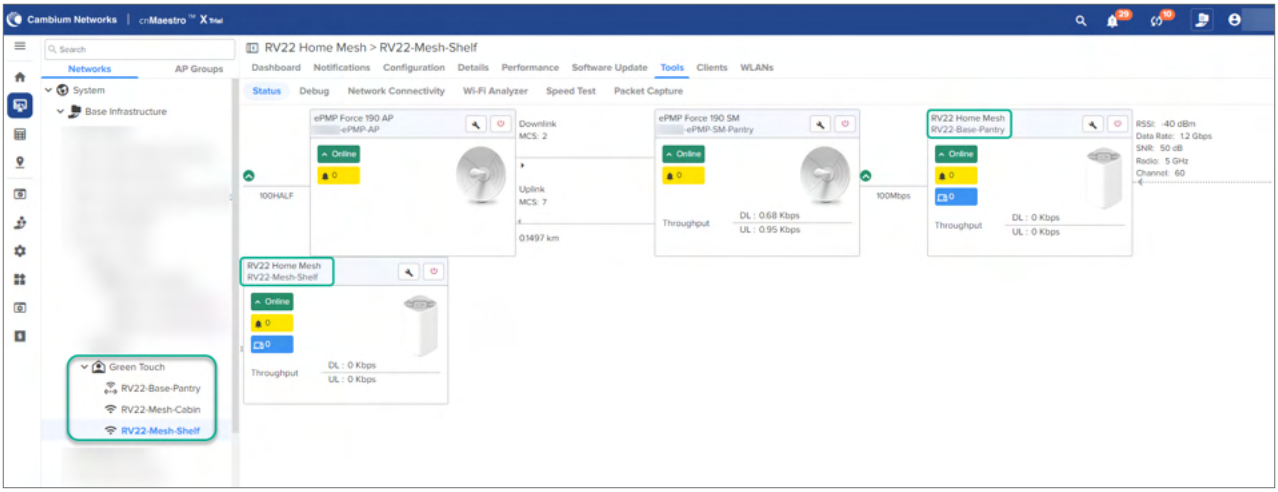
- Network toplogy for the **RV22-Mesh-Cabin** router

Figure 450 *Sample status page for RV22-Mesh-Cabin node router in a wireless mesh: 1-2 deployment*



- Network toplogy for the **RV22-Mesh-Shelf** router

Figure 451 *Sample status page for RV22-Mesh-Shelf node router in a wireless mesh: 1-2 deployment*



Wireless and wired mixed mesh 1-2 deployment

In this deployment, the base router is connected to one node router wirelessly and simultaneously to another by a wired connection, thereby creating a mixed 1-2 mesh deployment.

Figure 452 *Wireless and wired mixed mesh: 1-2 deployment*

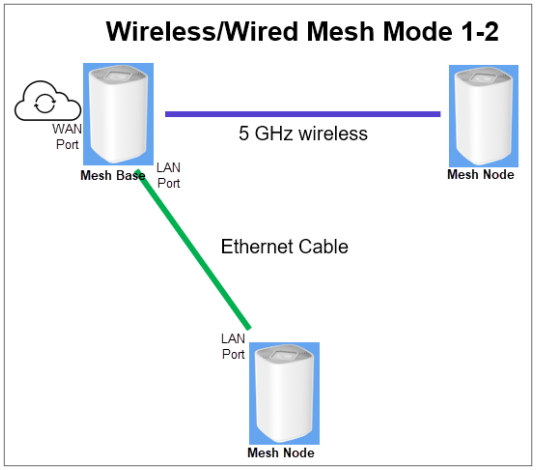
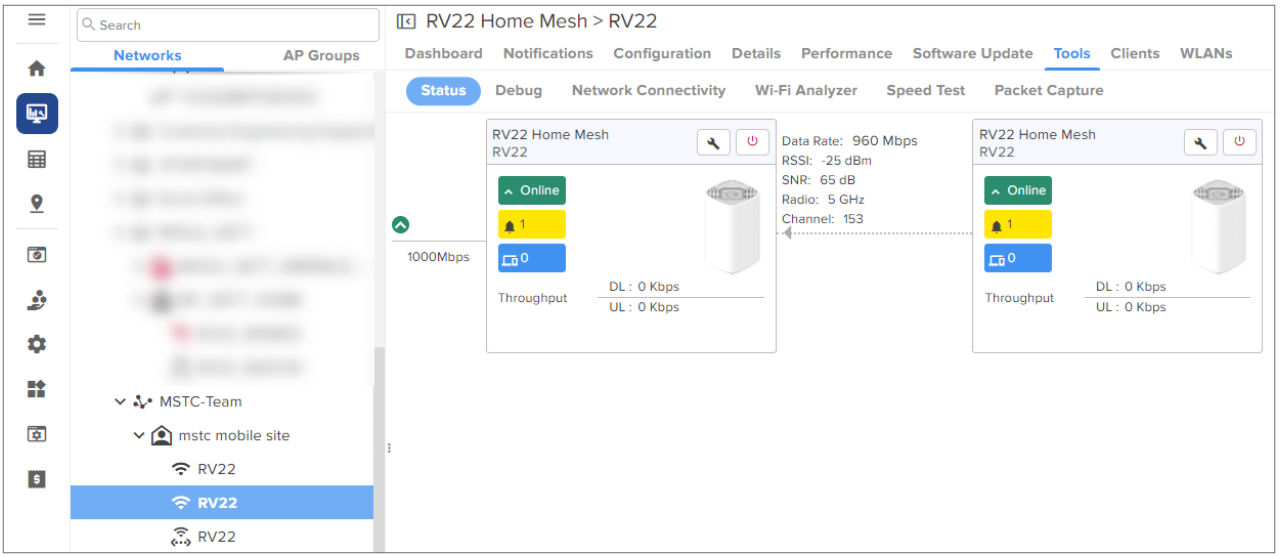


Figure 450 and Figure 451 display sample status pages for the node routers in a mixed mesh 1-2 deployment.

In the following status samples, one RV22 base router is connected to one RV22 node router wirelessly and simultaneously to another RV22 node router by a wired connection.

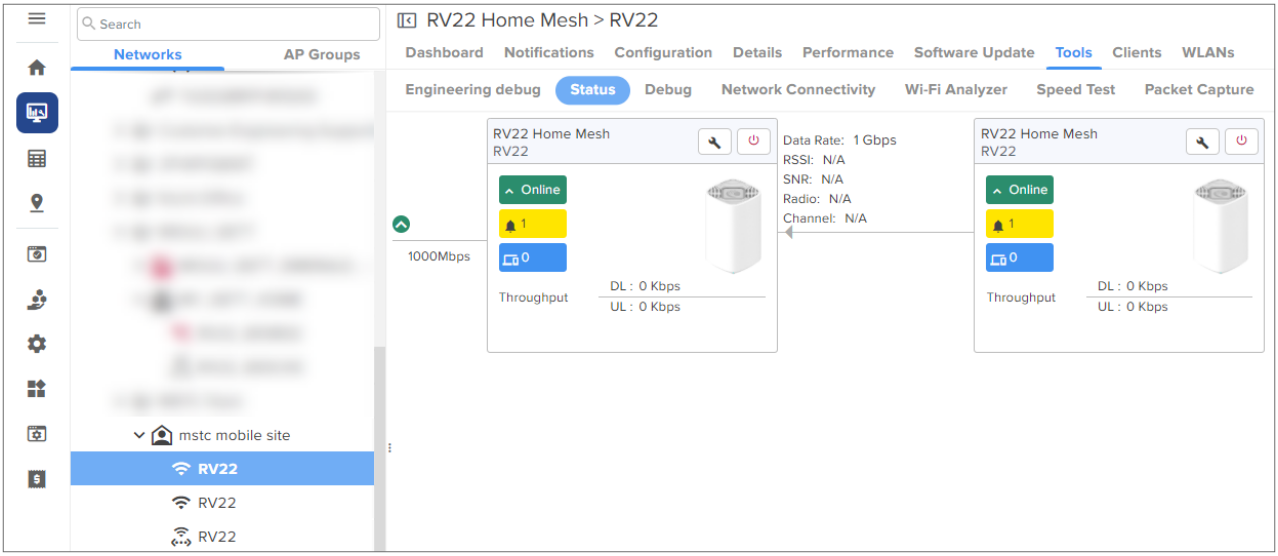
- Network toplogy for the wireless RV22 node router

  Figure 453 *Sample status page for the wireless RV22 node router in a mixed mesh: 1-2 deployment*



- Network toplogy for the wired RV22 node router

Figure 454 *Sample status page for the wired RV22 node router in a mixed mesh: 1-2 deployment*



Setting up the Home Mesh Router—Wired Mesh Mode

To configure a wired mesh, onboard the routers to a site—Claim the routers, which you want to be part of the mesh, on cnMaestro in the subscriber workflow. See Claiming the Home Mesh Router. Connect the mesh base router to the internet and connect the node routers to the base router using Ethernet cables. The AP group mapped to the subscriber is applied to all the routers to sync the configuration.

No configuration changes are required for RV22 routers to work in both wired and wireless mesh modes. Use any LAN port on the mesh base and any LAN port on the mesh node routers to establish a wired mesh connection. When a mesh node router detects an RV22 neighbor on its LAN port, it automatically establishes a wired mesh link using the LAN ports.

Note

You must not use the WAN port on the mesh node router to establish a wired mesh.

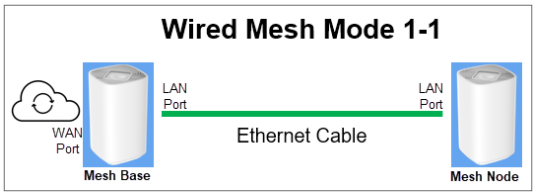
Following are some of the wired mesh configurations supported:

- Wired mesh: 1-1 deployment
- Wired mesh: 1-1-1 deployment
- Wired mesh: 1-2 deployment

Wired mesh: 1-1 deployment

In this deployment, the base router is connected to one node router using an Ethernet cable (between any LAN ports on both routers), thereby creating a wired 1-1 mesh deployment.

Figure 455 *Wired mesh: 1-1 deployment*



Wired mesh: 1-1-1 deployment

In this deployment, the base router is connected to only one of the node routers, which is in turn connected to another node router, by a wired connection (between any LAN ports on the routers), thereby creating a wired 1-1-1 mesh deployment.

Figure 456 *Wired mesh: 1-1-1 deployment*

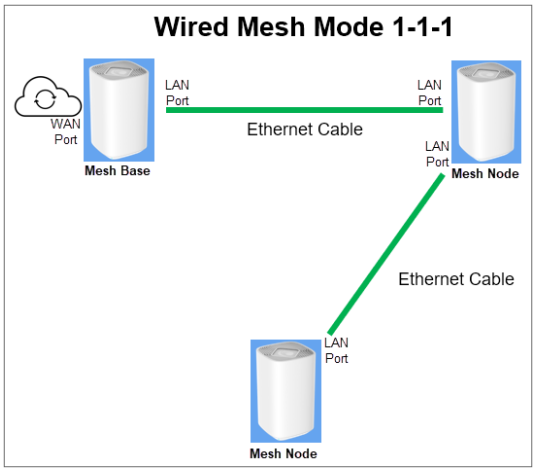


Figure 457 displays a sample cnMaestro status page for the wired mesh 1-1-1 deployment.

Figure 457 *Sample status page for wired mesh: 1-1-1 deployment*



Wired mesh: 1-2 deployment

In this deployment, the base router is connected to two node routers simultaneously by a wired connection, thereby creating a wired 1-2 mesh deployment.

Figure 458 *Wired mesh: 1-2 deployment*

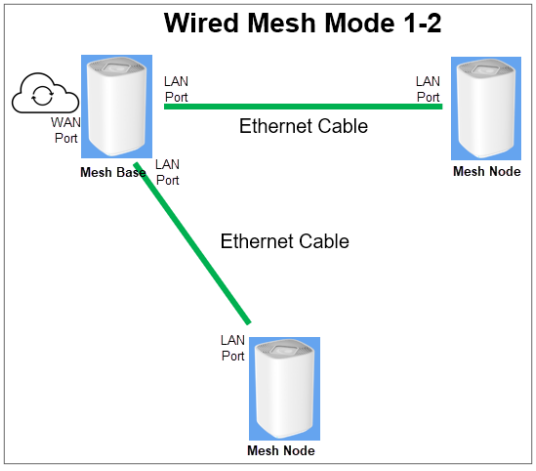
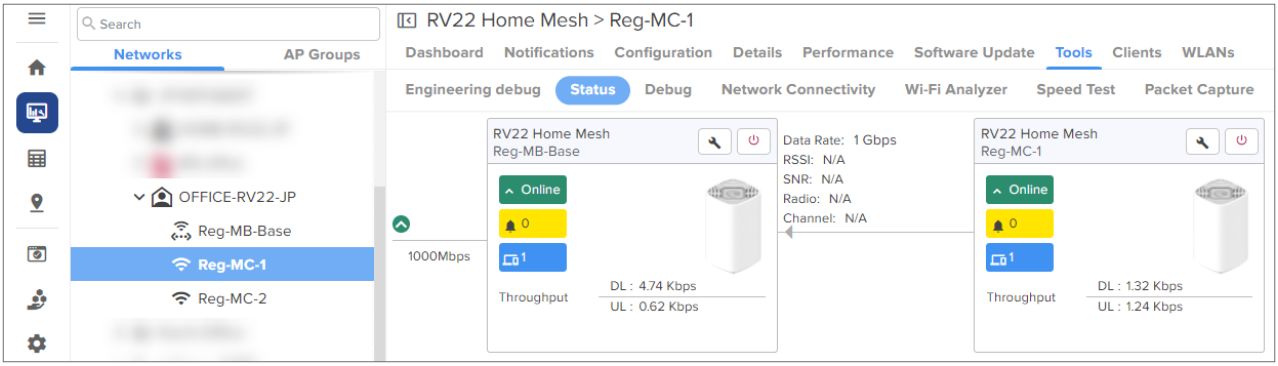


Figure 459 and Figure 460 display sample status pages for the node routers in a wired mesh 1-2 deployment.

In the following status samples, the **Reg-MB-Base** router is connected to both **Reg-MC-1** and **Reg-MC-2** routers using Ethernet cables, forming a wired 1-2 multi-mesh topology.

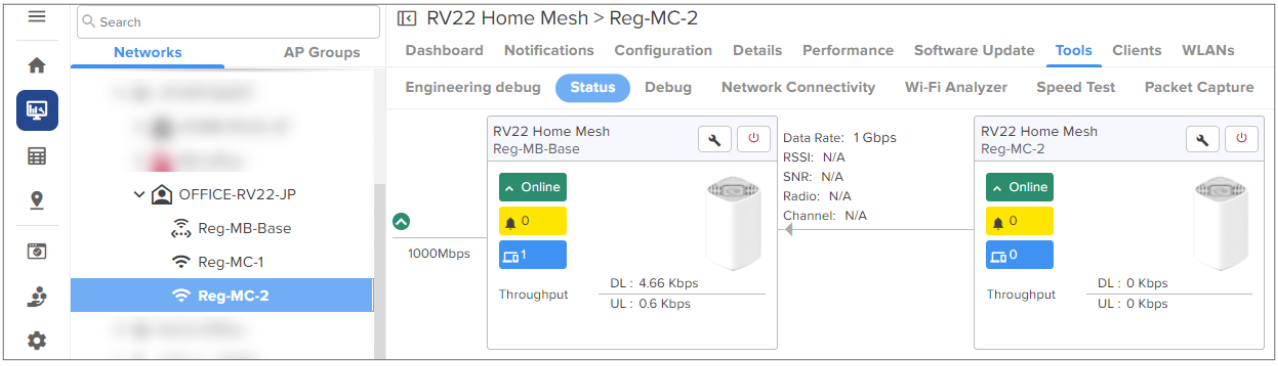
- Network toplogy for the **Reg-MC-1** router

  Figure 459 *Sample status page for Reg-MC-1 node router in a wired mesh: 1-2 deployment*



- Network toplogy for the **Reg-MC-2** router

  Figure 460 *Sample status page for Reg-MC-2 node router in a wired mesh: 1-2 deployment*



Viewing router system information and network traffic status

When the customer configures the Home Mesh Router and connects to the internet, you can check the connection of the router in cnMaestro. You can also check the details of the clients that are connected.

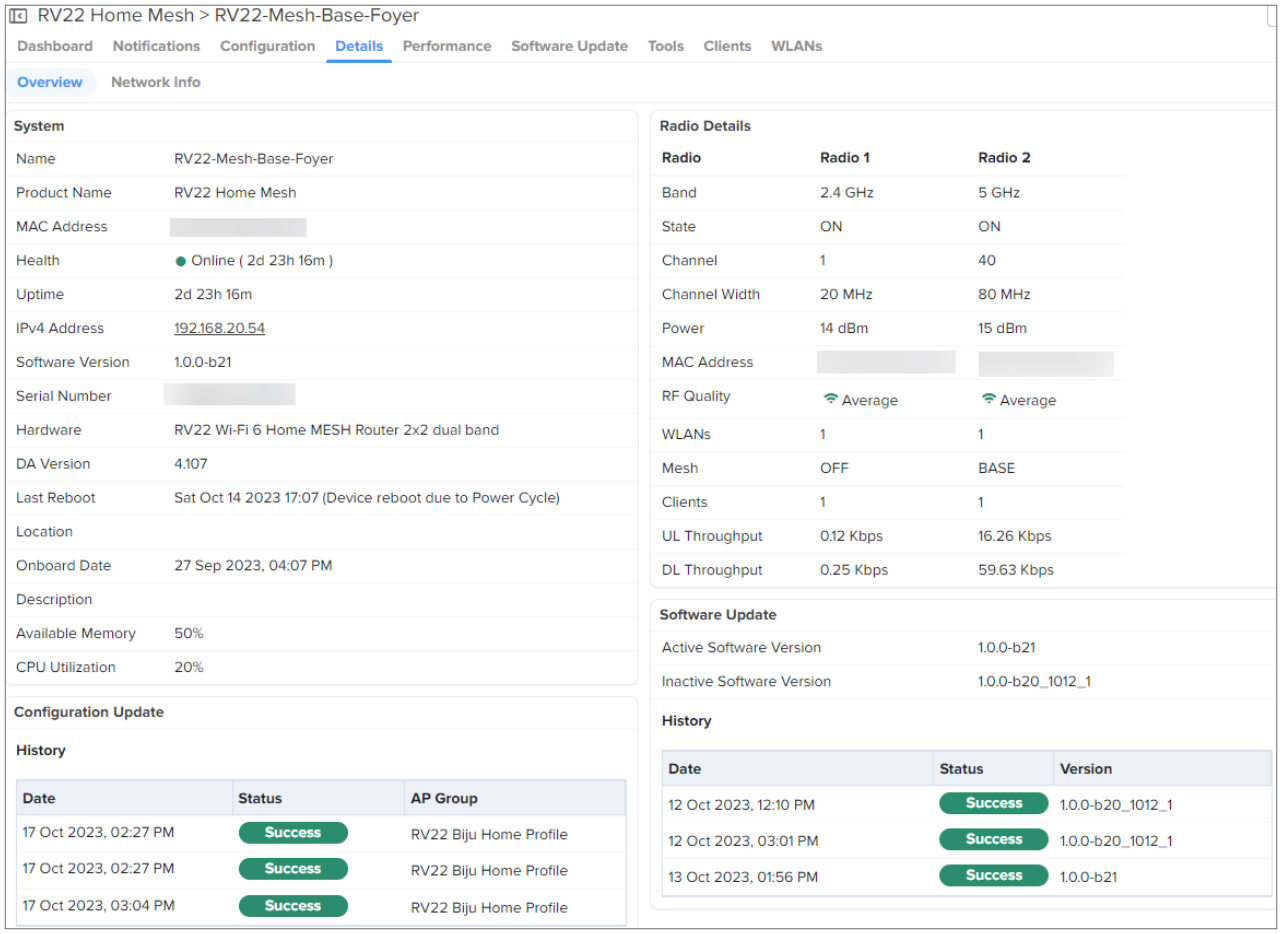
To view router system information and the connection status, navigate to **Monitor and Manage** > *<Home-Mesh-Router-name>* > **Details** tab.

The **Details** page displays information in the following tabs:

- **Overview**

  This page displays information in the following sections:

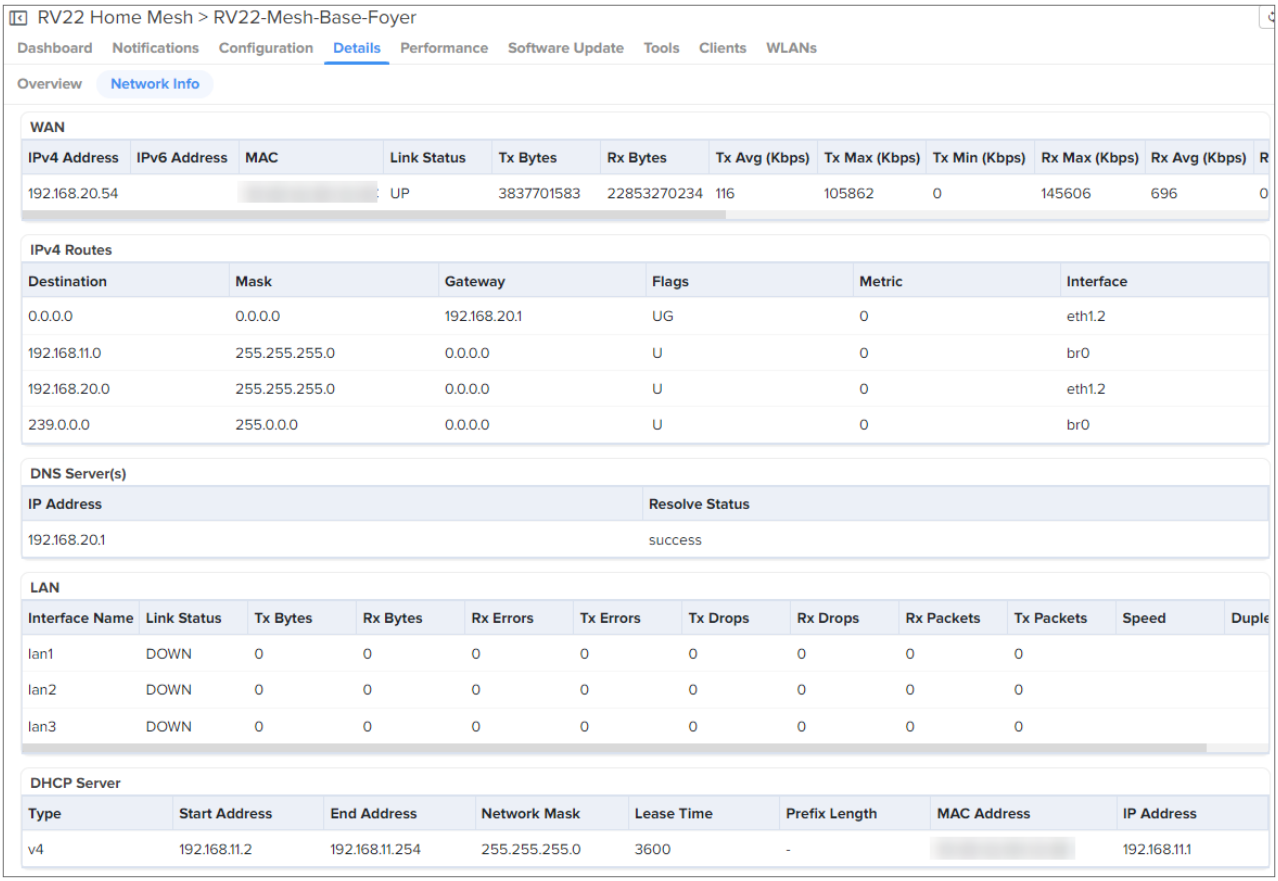
  - **System**—Displays information, such as router name, MAC address, health of the router (online, offline), software version, and location.
  - **Radio**—Displays radio details, such as the running bands, RF quality, count of clients connected to each radio, and the average throughput.
  - **Configuration Update**—Displays the history of configuration updates to the router.
  - **Software Update**—Displays the currently running software version and a history of software updates that were performed and the status.



- **Network Info**

  This page displays information in the following sections:

  - **WAN**—Displays collective statistics about total number of transmitted and received data packets, data bytes, packets dropped, maximum and average speeds
  - **IPv4 Routes**—Displays the IPv4 routes configured for the router.
  - **DNS Server(s)**—Displays the details of the DNS servers.
  - **LAN**—Displays details of the LAN interfaces, their status, total number of transmitted and received data packets and size (in bytes), packet errors and drops.
  - **DHCP Server**—Displays details of the DHCP servers, start and end IP address in the range used for allocation, and the lease time.



Viewing, editing, and blocking connected clients

cnMaestro allows you to view details of clients (both wired and wireless) connected to the router and edit the name of clients. You can also block certain clients that you do not want to be connected to your wireless networks.

This topic contains the following sections:

- Viewing connected clients
- Editing client host name
- Blocking clients

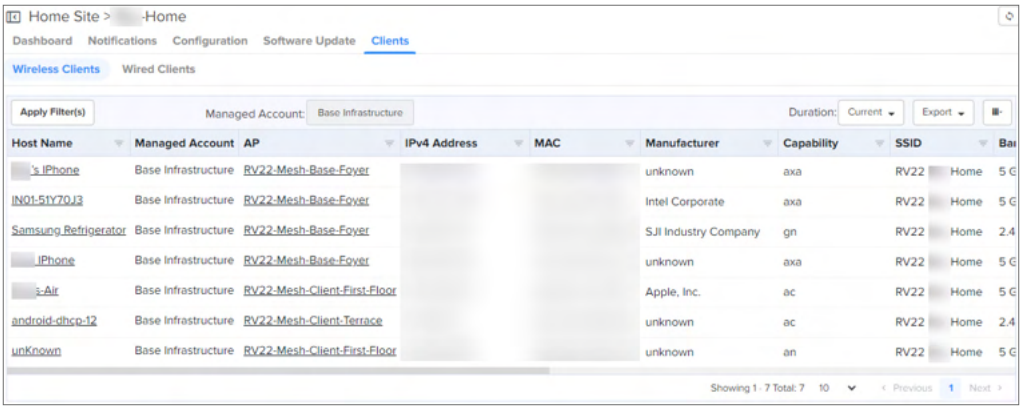
Viewing connected clients

To view the list of connected clients, both wired and wireless, navigate to **Monitor and Manage** > *<Home-Mesh-Router-name>* > **Clients** tab.

The **Details** page displays information in the following tabs:

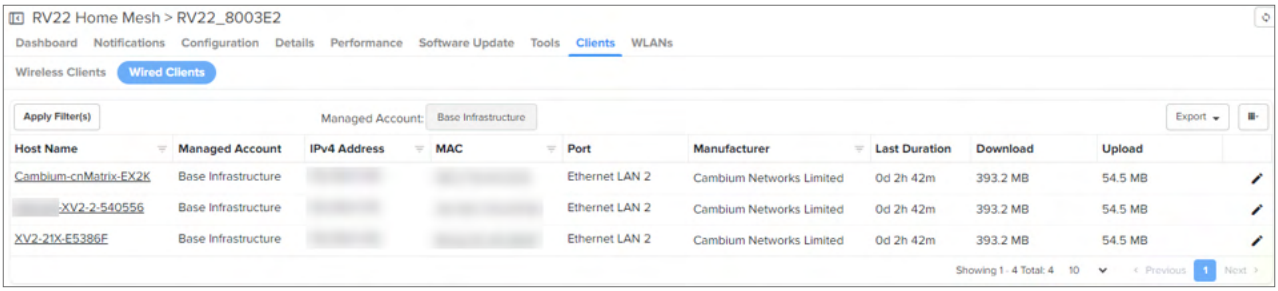
- **Wireless Clients**

  This page displays information about the wireless clients connected to the router, such as the host name, MAC address, IPv4 addess assigned, the router it is connected to, and the status of connection with the router (online, offline).



- **Wired Clients**

  This page displays information about the wired clients connected to the router, such as the host name, MAC address, IPv4 addess assigned, port number to which it is connected, the manufacturer of device connected, last connected duration, and the download and upload data size (in MB).



Editing a client's host name

To edit the host name of a connected client, click the edit client name ( ) icon corresponding to the client.

Enter the name in the **Host Name** field and click **Save**.



Blocking clients

To block a connected client, click the block ( ) icon corresponding to the client.

Monitoring and troubleshooting the Home Mesh Router

You can monitor and perform troubleshooting tasks on the Home Mesh Router using cnMaestro. This topic covers the following sections

- Monitoring the Home Mesh Router
- Troubleshooting the Home Mesh Router
- Upgrading the Home Mesh Router firmware

Monitoring the Home Mesh Router

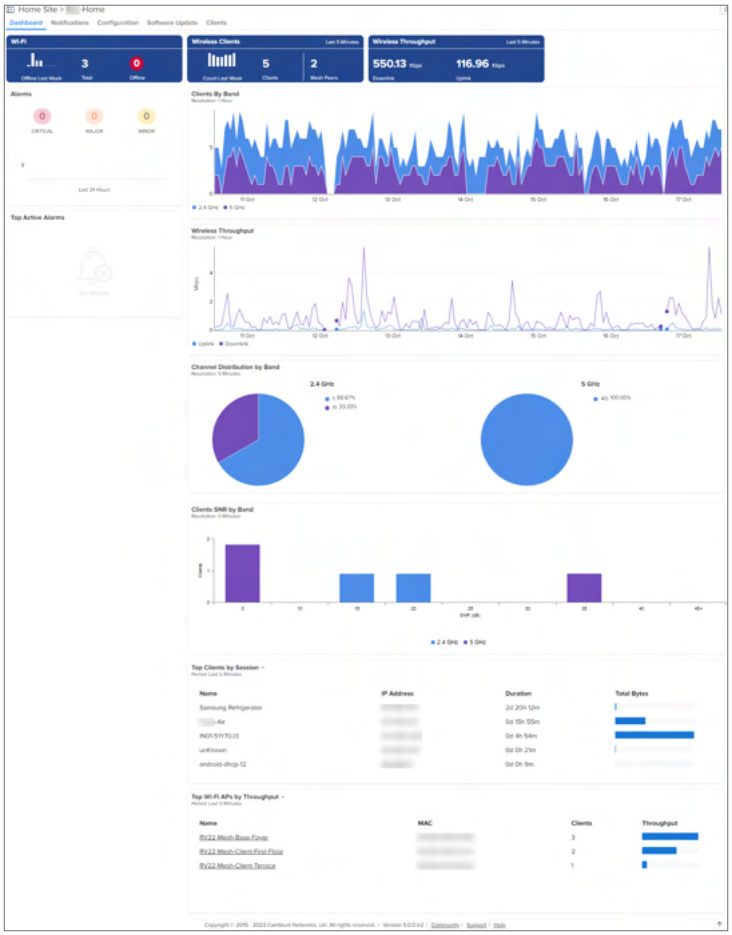
When the device is onboarded to cnMaestro, based on the deploymnet type, the router is displayed under the site that it is configured.

Using the following pages in cnMaestro, monitor and view details of the router and the deployment.

- Home Site Dashboard
- Notifications
- Software Update
- Performance

Home Site Dashboard

To view the site dashboard, access the **Dashboard** page under **Monitor and Manage >** <Home-site-name> **> Dashboard.**



Notifications

The Notifications page displays current alarms, previous alarms, Wi-Fi-related events, and other device-related events.

cnMaestro displays the following types of notifications:

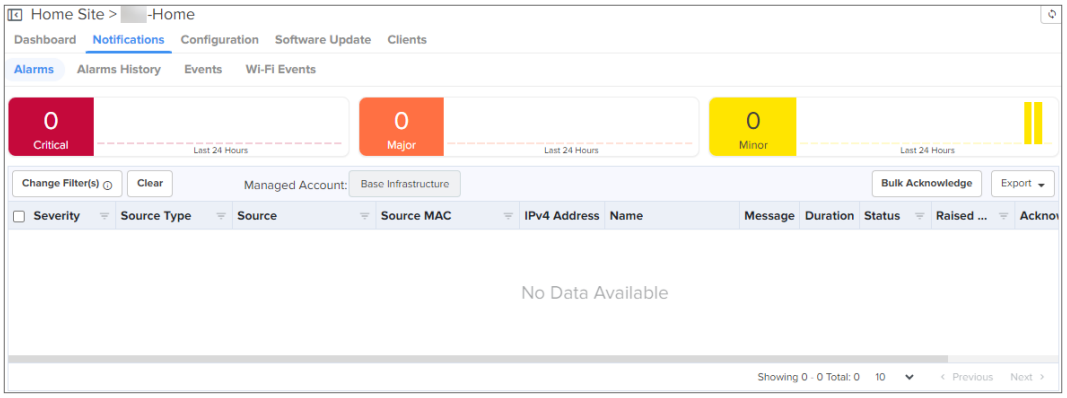
- Alarms
- Alarms History

- Events
- Wi-Fi Events

Alarms

The Alarms page displays the number of critical, major, and minor events observed for the Home Mesh Router.You can also view the details of the events, such as severity level, name of the event, time and action taken.

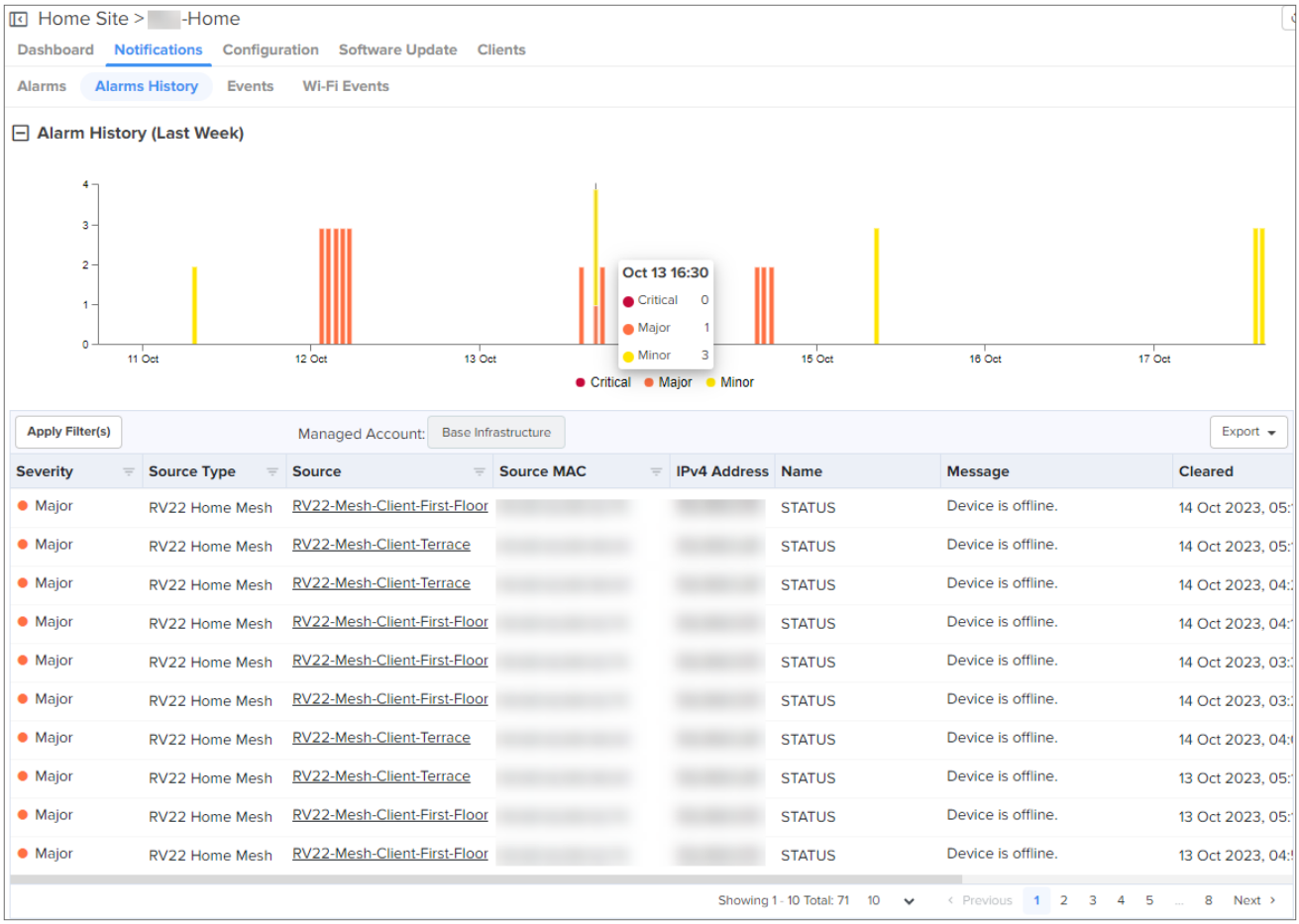
To view the alarms raised, access the **Alarms** page under **Monitor and Manage >** <Home-site-name> **> Notifications > Alarms.**



Alarms History

The Alarms History page displays the number of critical, major, and minor events observed in the previous week.

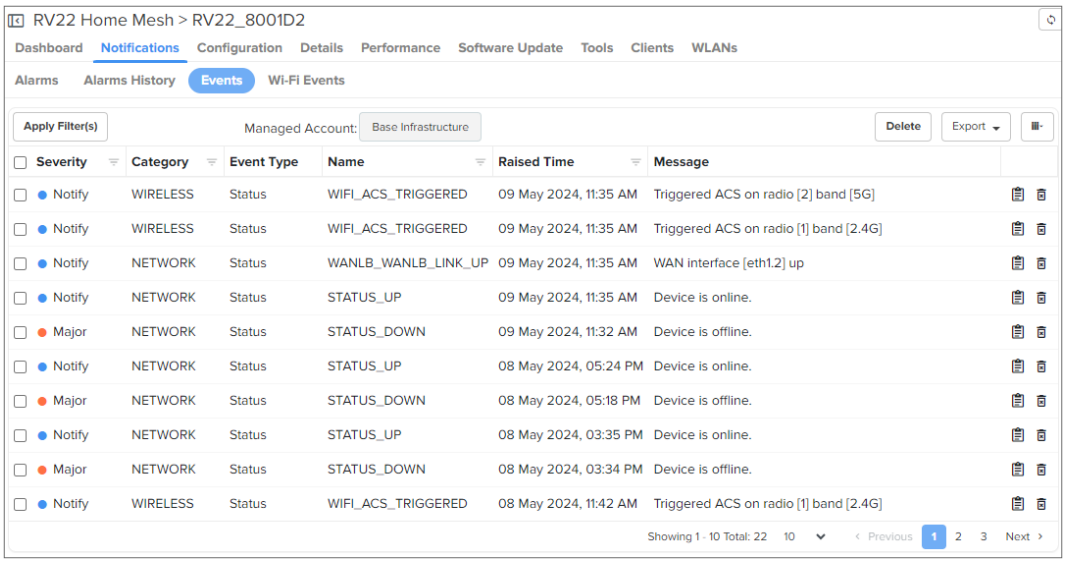
To view the alarms history displayed as a graphical representation, access the **Alarms History** page under **Monitor and Manage >** <Home-site-name> **> Notifications > Alarms History**.



Events

The Events page displays Home Mesh Router-related events, such as its status, if there were any changes in bandwidth, and when the DHCP server IP was assigned to the connected clients.

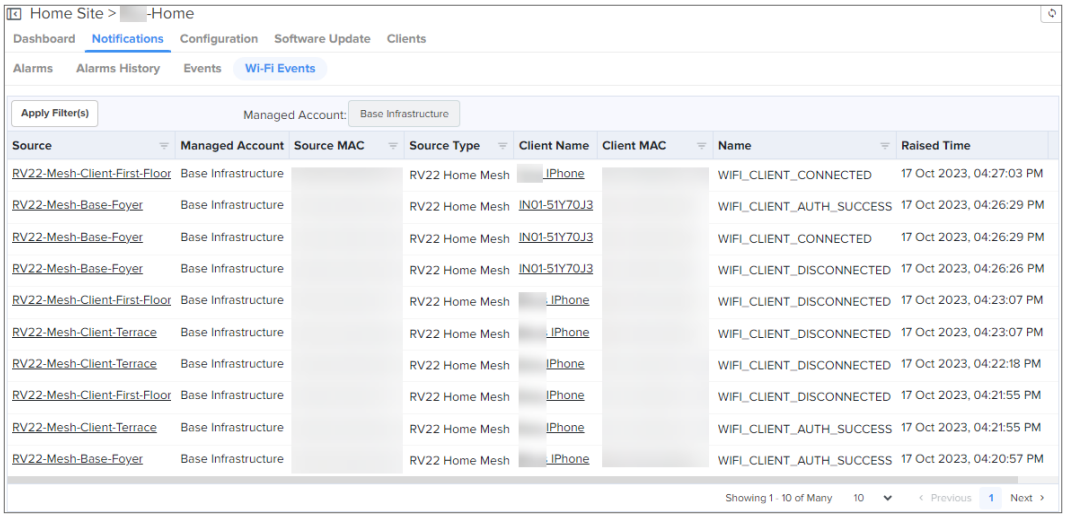
To view the events, access the **Events** page under **Monitor and Manage** > <Home-site-name> > **Notifications** > **Events**.



Wi-Fi Events

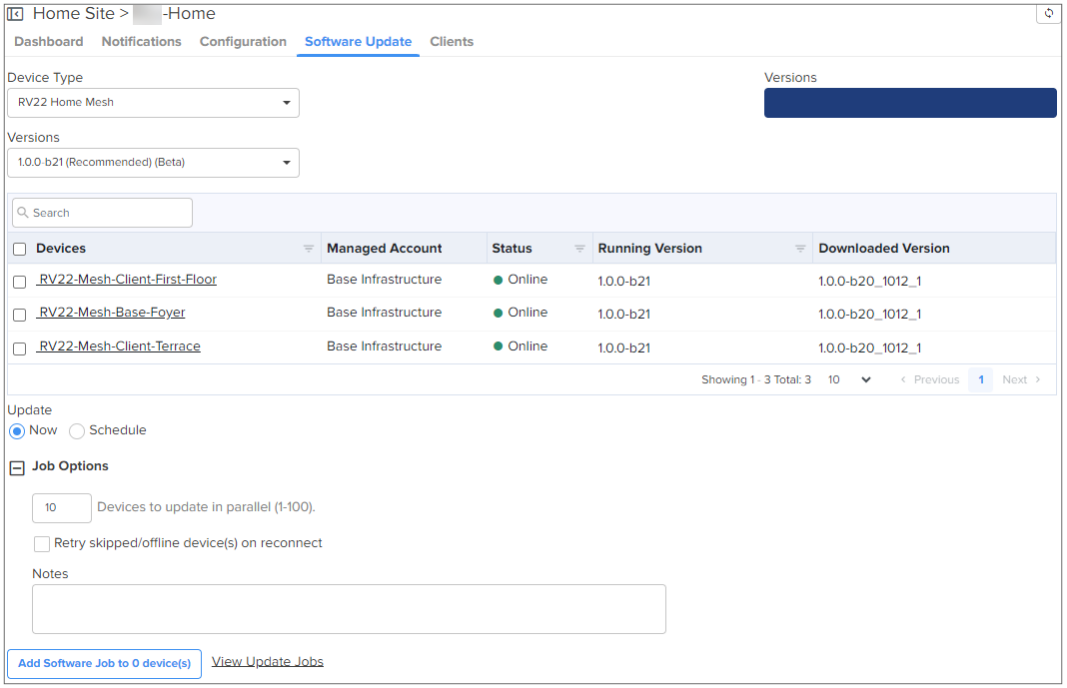
The Wi-Fi Events page displays client-related events, such as when the client connected to the network, when it was disconnected, and authentication events.

To view the Wi-Fi events, access the **Wi-Fi Events** page under **Monitor and Manage >** <Home-site-name> **> Notifications > Wi-Fi Events**.



Software Update

To upgrade the router firmware, go to the **Software Update** page. See Upgrading the Home Mesh Router firmware for more information.



Performance

To view the performace of the router, access the **Wi-Fi Events** page under **Monitor and Manage >** <Home-Mesh-Router-name> **> Performance**.

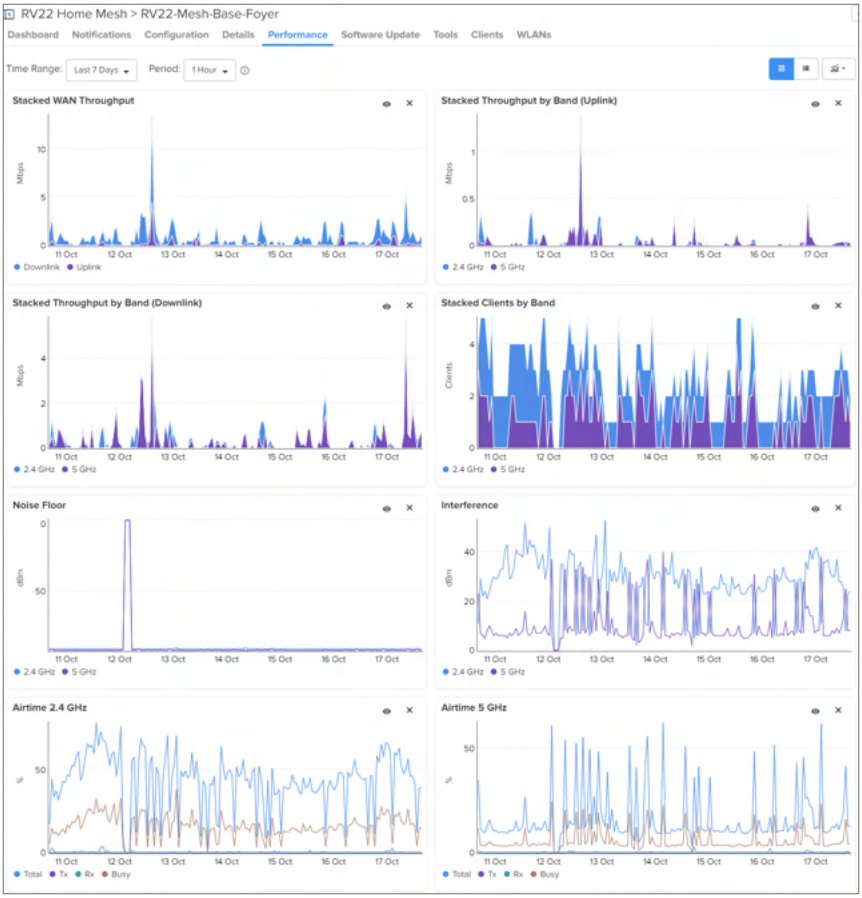
The page displays the following graphical information:

Table 103 *Performance page graphs—Base and Node routers*

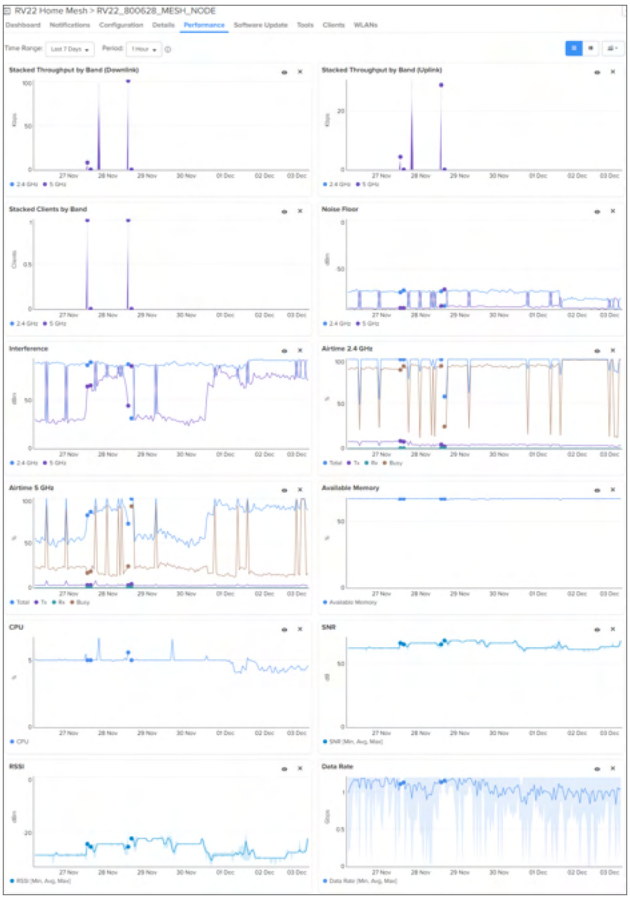
Parameter	Description	Router (Base / Node / Both)
Stacked WAN Throughput	Hourly throughput for both downlink and uplink in the WAN interface for each band of the mesh base router.	Base only
Stacked Throughput by Band (Downlink)	Downlink speed in each band.	Both
Stacked Throughput by Band (Uplink)	Uplink speed in each band.	Both
Stacked Clients by Band	Count of number of clients connected in each band.	Both
Noise Floor	Amount of background noise (in dBm) or interference created by devices in the same frequency.	Both
Interference	Interefence (in dBm) caused by other wireless signals and devices interrupting the router's Wi-Fi signal.	Both
Airtime 2.4 GHz	Capacity utilization (in %) of the 2.4 GHz band for effective transmission.	Both
Airtime 5 GHz	Capacity utilization (in %) of the 5 GHz band for effective transmission.	Both
Available Memory	Amount of router memory (in %) available for use.	Both
CPU	Router CPU utilization in percentage (%).	Both
SNR	Minimum, average, and maximum SNR values (in dB) for the mesh node router.	Node only
RSSI	Received Signal Strength Indicator (RSSI) value (in dBm) for the mesh node router.	Node only
Data Rate	Minimum, average, and maximum data rates (in Mbps or Gbps) provided by the mesh node router to the client devices.	Node only

Following are sample performance graphs for base and node routers:

- Performance of the base router in a mesh deployment



- Performance of the node router in a mesh deployment



Troubleshooting the Home Mesh Router

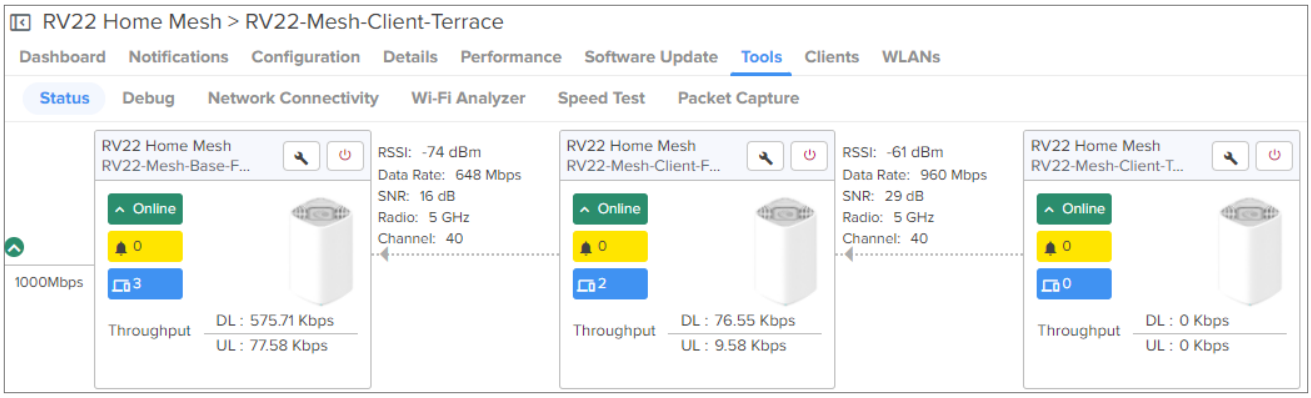
cnMaestro provides the following troubleshooting options for the router:

- Status
  - Downloading tech support file
- Debug
- Network Connectivity
- Wi-Fi Analyzer
- Speed Test
- Packet Capture

Status

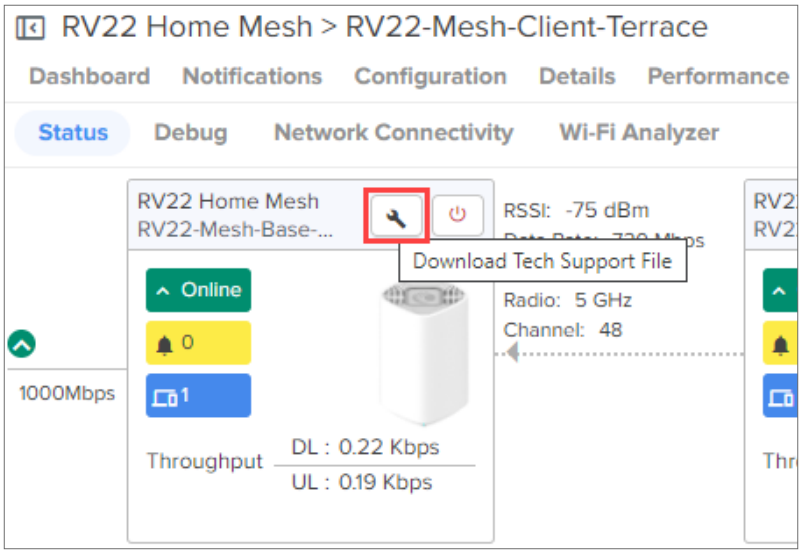
The Status page displays the status of link between the Home Mesh Router base and client devices.

To view the status of the link between the Home Mesh base and client devices, access the **Status** page under **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools.**



Downloading tech support file

To download the tech support file, click the Download Tech Support File ( ) icon on the **Status** page.

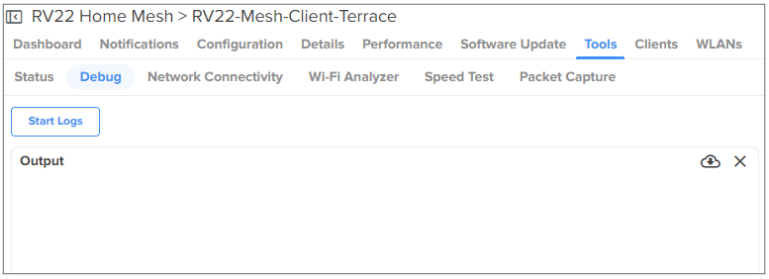


Debug

The Debug page displays log information of the Home Mesh Router. To view the debug information, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Debug** tab.
2. Click **Start Logs**.

   The log information is displayed in the **Output** window.



Network Connectivity

The Network Connectivity page provides network connectivity information of the Home Mesh Routers.

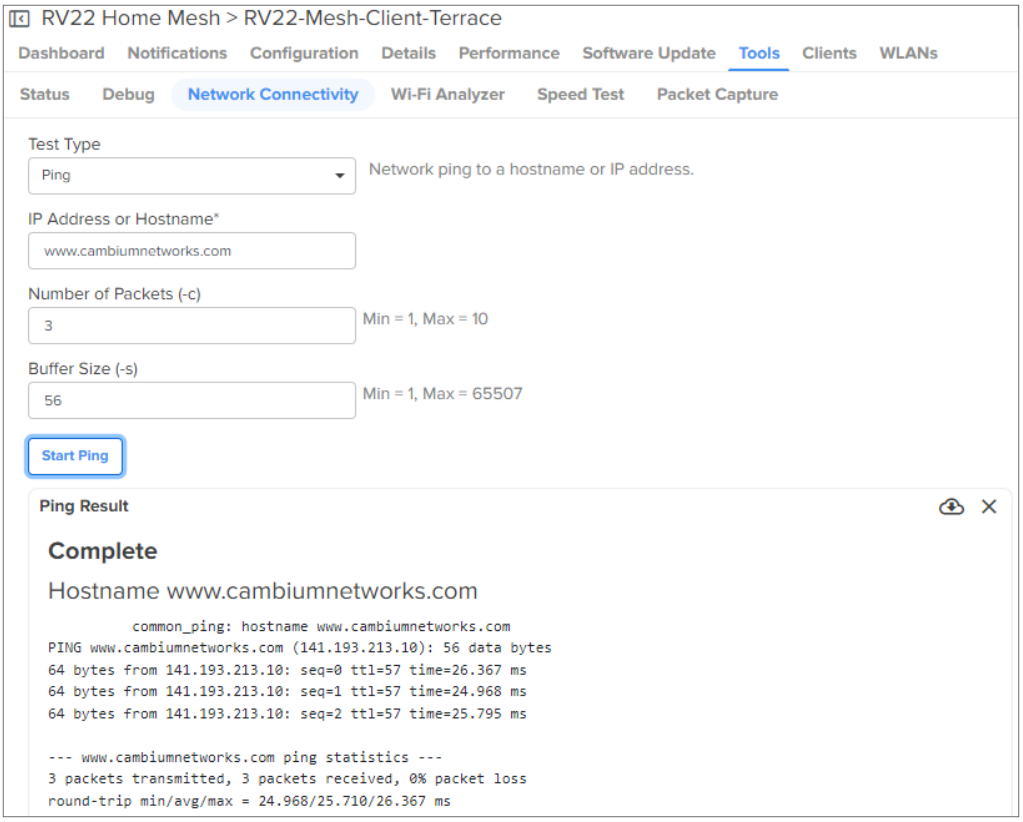
cnMaestro supports the following tests to provide connectivity information for the Home Mesh Routers:

- Ping
- DNS Lookup
- Traceroute

To test network connectivity of the router, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Network Connectivity** tab.
2. Select the required test type from the **Test Type** drop-down list and configure the corresponding parameters required for the test.
3. Click **Start Test**.

   cnMaestro initiates the test and displays the result in the **<Test Type> Result** window.



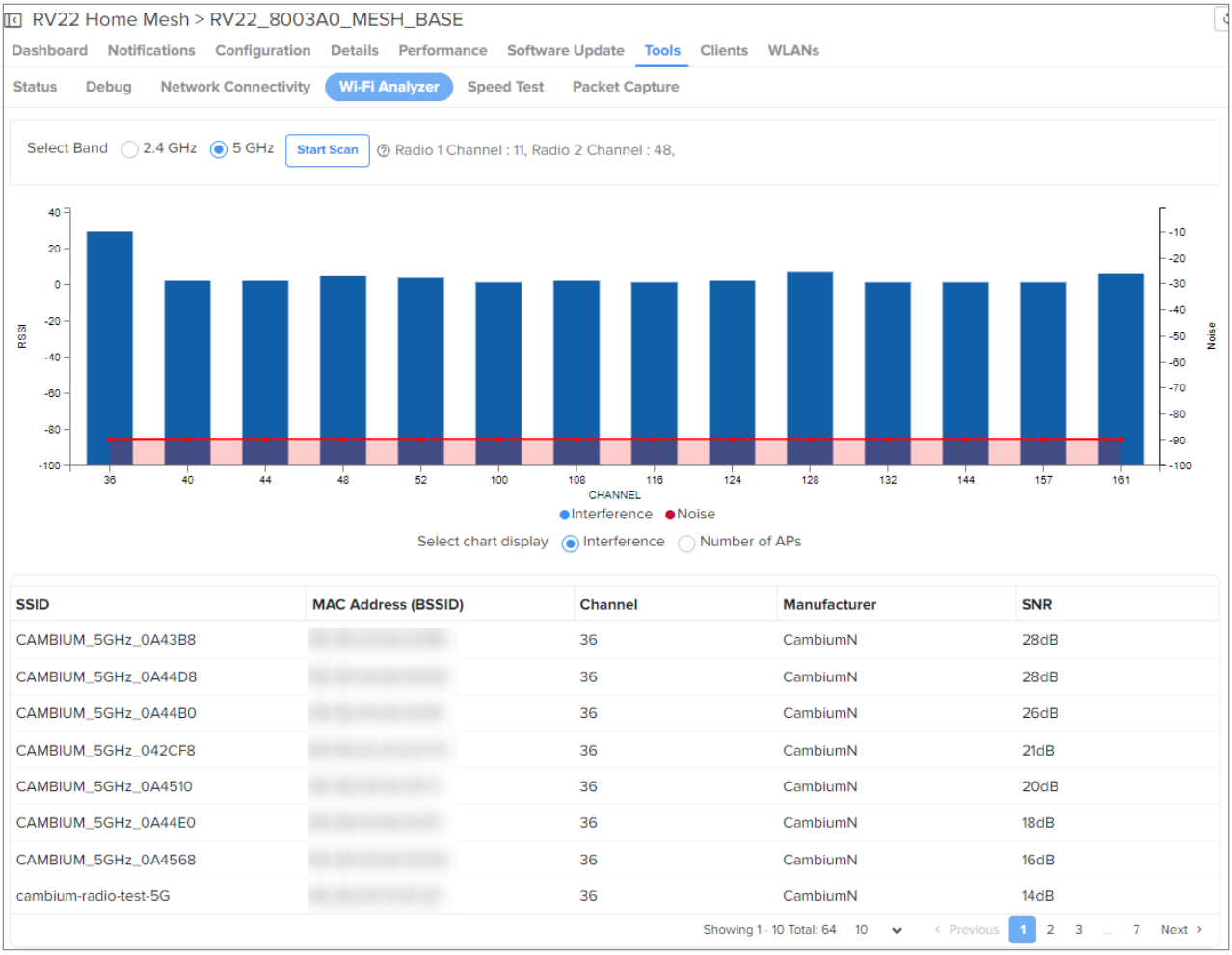
Wi-Fi Analyzer

The Wi-Fi Analyzer page displays radio traffic and signal information for the selected band. It displays the interference and noise measured for the selected band.

To view the Wi-Fi Analyzer details, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Wi-Fi Analyzer** tab.
2. Select the required band (2.4 or 5 GHz).
3. Click **Start Scan**.

cnMaestro analyzes the band and displays the result in a table.



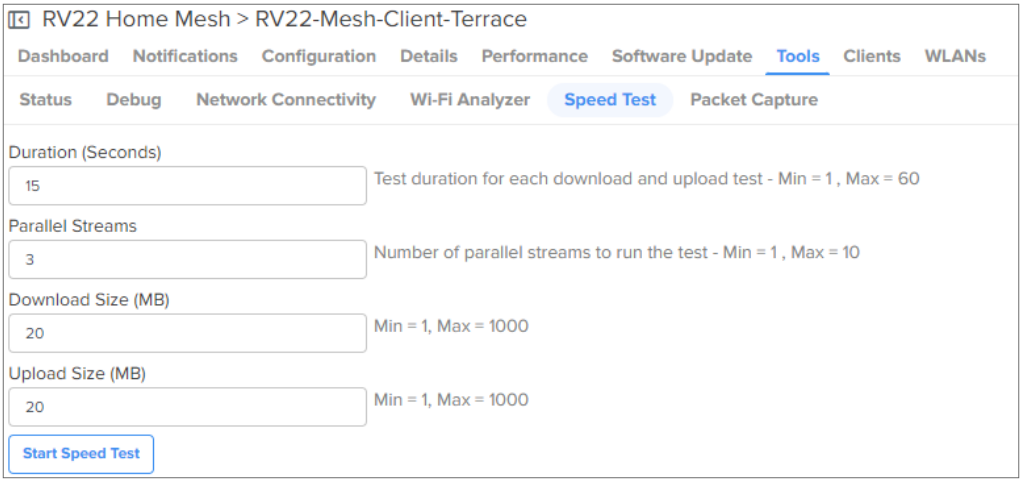
Speed Test

The Speed Test page displays the internet speed provided by the Home Mesh Router.

To know the speed of the router, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Speed Test** tab.
2. Configure the required values for testing the speed.
3. Click **Start Speed Test**.

cnMaestro checks the speed and displays both download and upload speeds in megabits per second (Mbps).

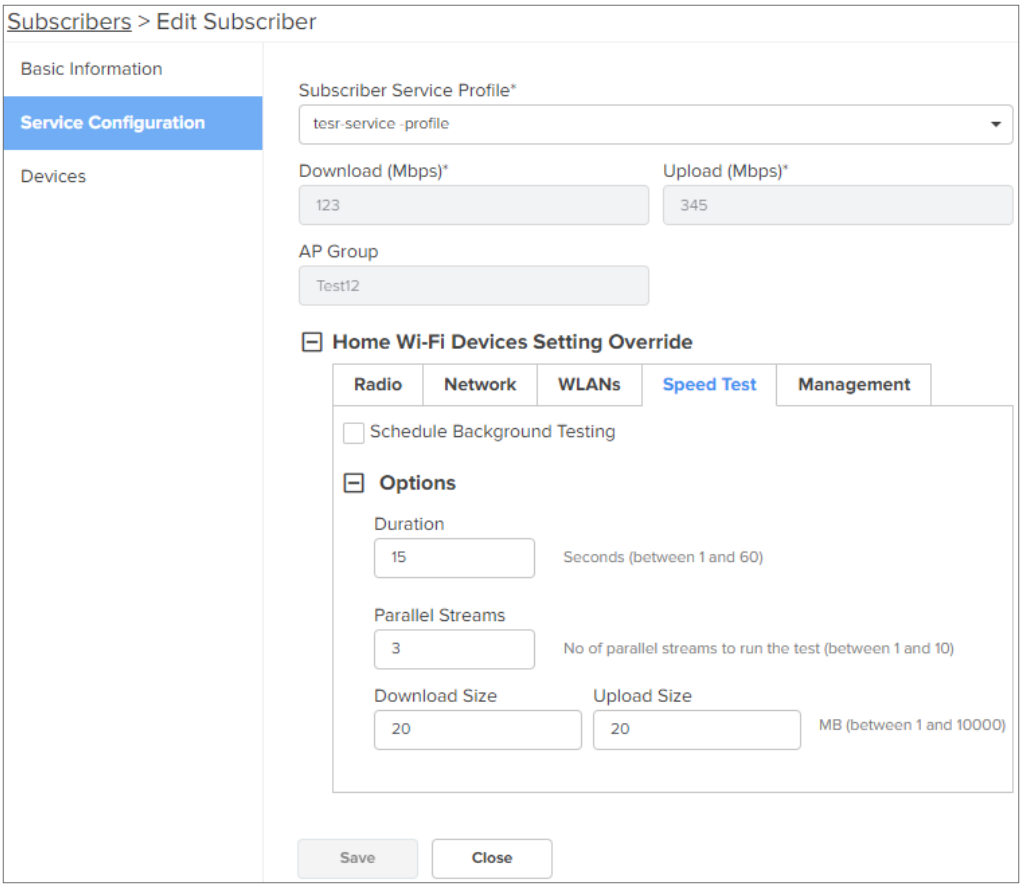


The speed test option is also available on the **Subscriber** page in the **Home Wi-Fi Devices Setting Override** section.

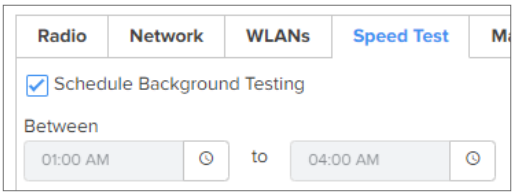
To avail this speed test option, complete the following steps:

1. Navigate to the **Manage Service Providers** > **Managed Subscribers** > **Subscribers** tab.
2. From the list of subscribers, click the subscriber name for which you want to configure the speed test.

   The **Edit <Susbcriber-name>** window is displayed.
3. Click the **Service Configuration** tab.
4. In the **Home Wi-Fi Devices Setting Override** section, click the **Speed Test** tab.



5. To schedule the speed test at a particular duration, select the **Schedule Background Testing** check box.
6. Select the start and end time for performing the speed test on the router.



Packet Capture

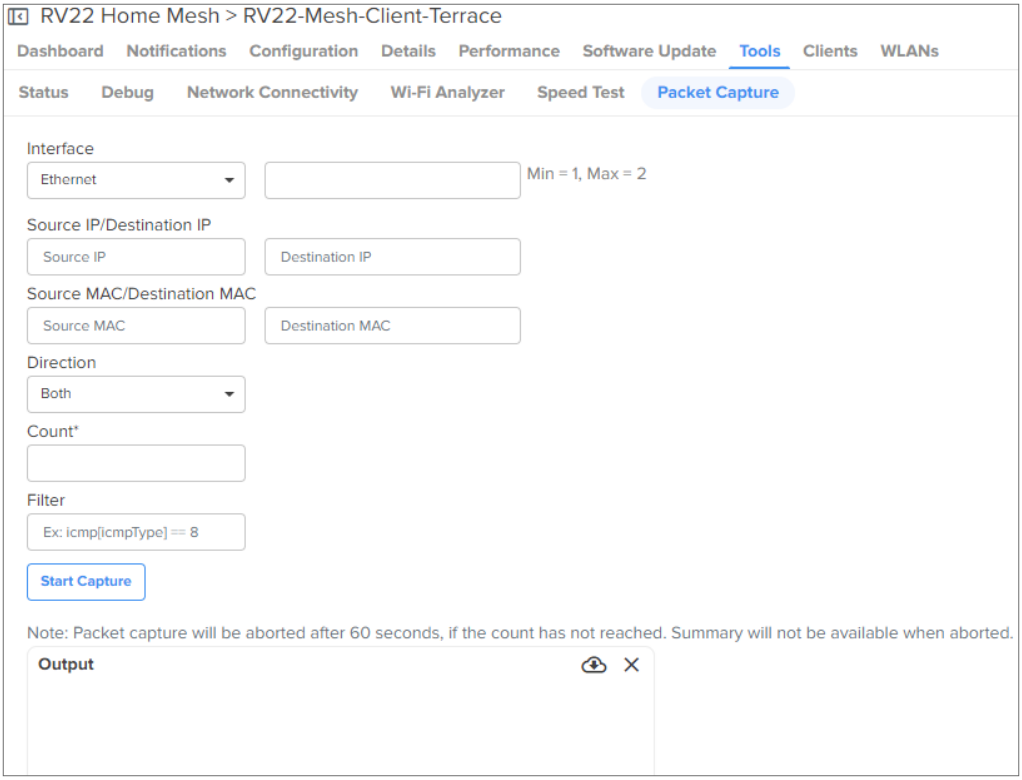
The Packet Capture page allows the user to capture all packets on a specified interface.

To capture packet data, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Packet Capture** tab.
2. Select the required interface, and provide the source and destination IP address or MAC address.
3. Provide the number of packets that must be captured.
4. Click **Start Capture**.

   cnMaestro displays the information in the **Ouput** window.

5. To download the PCAP file, click the download ( ) icon.



Upgrading the Home Mesh Router firmware

To upgrade the firmware of Home Mesh routers present in a home site, complete the following steps:

1. Navigate to **Monitor and Manage** > <Home-site-name> > **Software Update**.

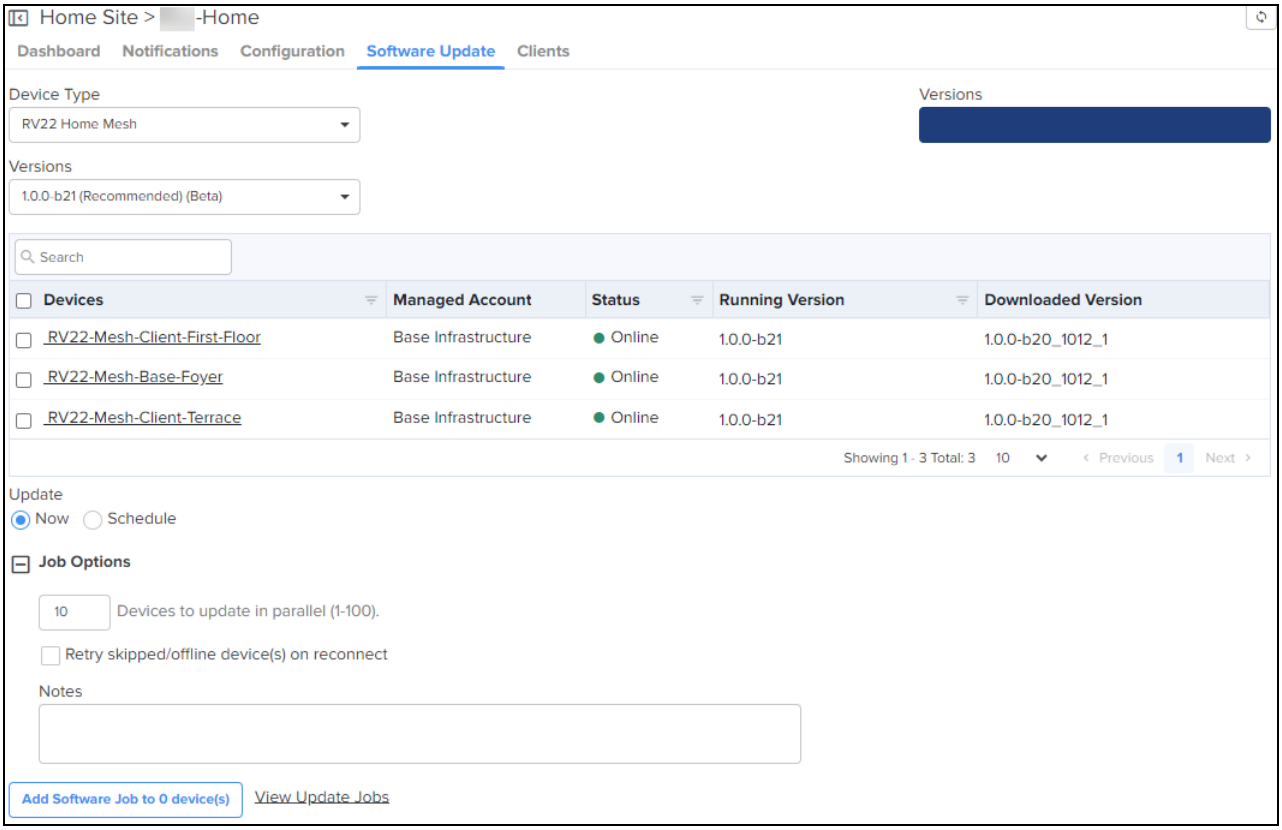
   The Software Update page appears.
2. Select **RV22 Home Mesh** from the **Device Type** drop-down list.
3. Select the software version from the **Versions** drop-down list.
4. In the list of devices table, select the check boxes corresponding to the devices for which you want to upgrade the firmware.

   You can also select one router to upgrade the firmware of only that router.
5. Select the **Now** option in the **Update** field to upgrade the firmware immediately.

   To schedule the upgrade job, select the **Schedule** option and configure the required date and time.
6. Click **Add Software Job to** <number of devices> **device(s)**.

   The upgrade is scheduled to run at the specified date and time.

To view the status of the update jobs, click **View Update Jobs**.



Analytics

This chapter covers the following topics:

- Site Analytics
- Client Analytics

Analyzing Connection Failures of Wi-Fi Clients and Poor Performance of Wi-Fi Networks

The Wi-Fi Analytics feature provides deep visibility into the health of Wi-Fi client connections, including root cause analysis of failures and possible remediations. It also provides analytics on aggregated data that can help to improve client connectivity in the Wi-Fi network.



Note

This feature is currently available as a free trial to all cnMaestro X customers, but will require a separate paid subscription in the future.

This section covers the following topics:

- Overview
- Use cases
  - Resolve connectivity issues
  - Address poor performance of applications
  - Identify OS, SSID, and AP-specific issues
- Accessing the Analytics XA page
- Accessing Site-level consolidated details at the System- and MSP-levels
- Setting filters to view the connection data
- Viewing the connection events
  - Dashboard page
  - Analytics XA page
    - Connection tab
    - Disconnection tab
    - Viewing a client or host-specific connection or disconnection event
    - Viewing an event-based connection or disconnection event
    - Viewing an AP-specific information

Overview

The Analytics X^A feature analyzes the Wi-Fi client connection events and helps to troubleshoot common network connectivity and performance issues such as the following:

- **Connectivity**—Association, authentication, and network connectivity failures.
- **Poor Performance**—Low RSSI, low data rate, high retry rate, and high latency in AAA, DHCP, DNS, and applications.

You can use this feature to detect and analyze common network problems that occur in your wireless networks.

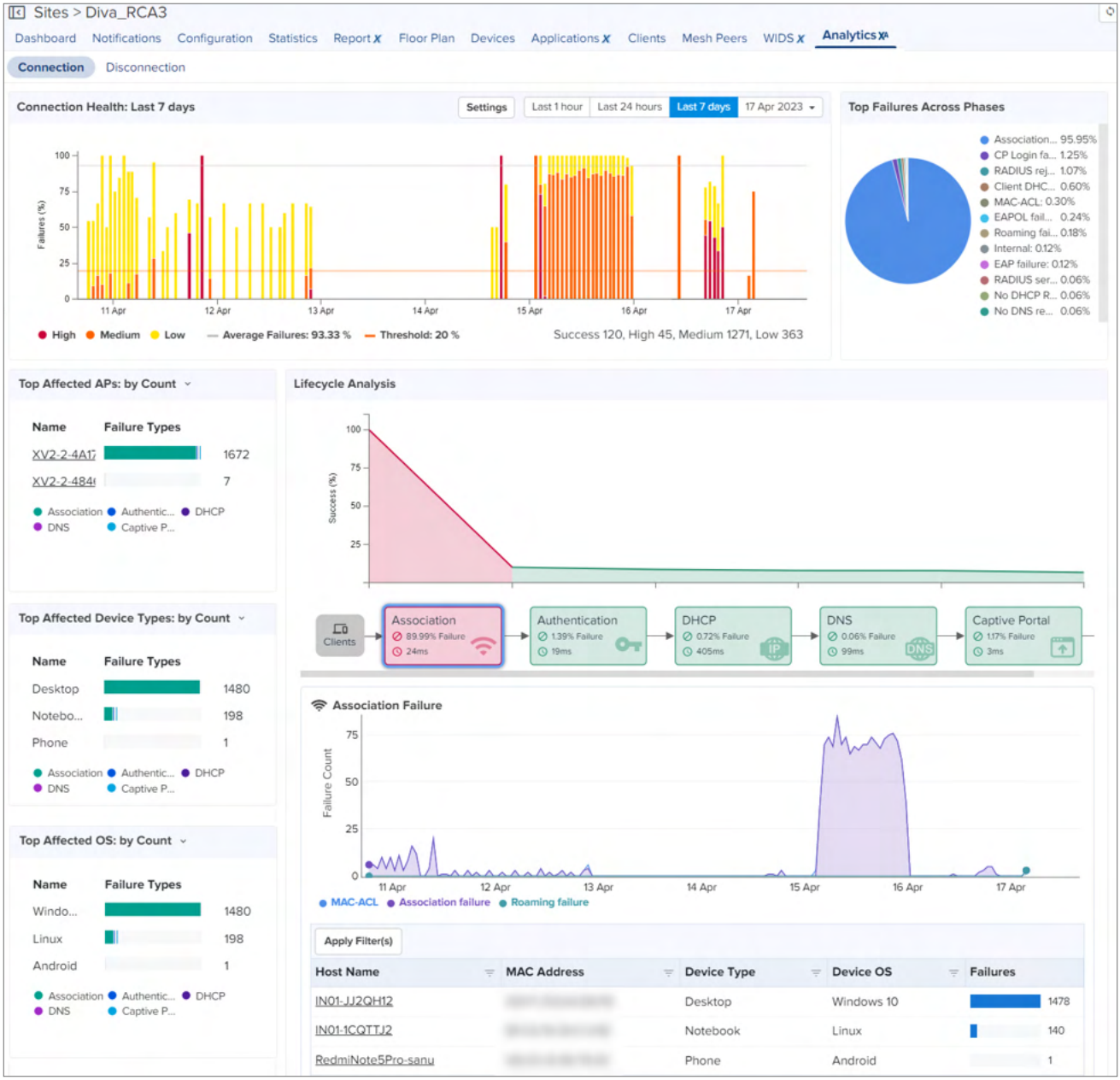
Note

Analytics X^{A} is supported only for XV and XE devices.

The **Analytics X^{A}** page reports the following data for the Wi-Fi clients:

- Statistics of successful connections per connection type such as new, reconnection, and roaming.
- Statistics of failed connections and disconnections, such as reason codes for association, EAP/EAPOL handshake, DHCP, DNS, and Captive Portal failures.

Figure 461 *The Analytics X^{A} page*



Use cases

Following are some of the **use cases**, to identify the connectivity issue and analyze the root cause:

Resolve connectivity issues

The **Analytics X[A]** page provides visual analytics of client connection failures in each phase such as baseline performance and key metrics in the form of graphs and tables with multiple data filters. You can easily identify the root cause based upon the phase of the Wi-Fi connection lifecycle.

- **Association**—Accessing the AP may fail if the client has low RSSI; if the request for capabilities is not supported by the AP; or if the AP is already handling the maximum number of clients.
- In such cases, you can use the **Lifecycle Analysis** widget on the **Analytics X[A]** page. This widget displays the statistics of 802.11 authentication/association failures in percentage. In addition, you can use the **Events** page to analyze the reason, cause, impact, and the recommended action.
- **Authentication**—Authentication may fail when 802.1X/EAP key is incorrect; the RADIUS server cannot be reached; or the WPA2-PSK or WPA3-SAE key derivation is invalid.
- In such cases, the **Lifecycle Analysis** widget displays the RADIUS authentication failure count in percentage.
- **Network connection**—When a client is successfully authenticated, it must be assigned an IP address by the DHCP server and provided networking information such as for DNS and Gateway. When the DHCP server fails, connectivity to the network cannot be established.
- In such cases, the **Lifecycle Analysis** widget can help identify that the DHCP server failure, and the **Events** page can analyze the reason and cause.
- **Aggressive roaming**—Time sensitive applications such as voice and video require uninterrupted connectivity. To ensure this, Wi-Fi clients monitor the RSSI from local APs and probe better APs when the connection degrades. The RSSI threshold at which a client moves from the current AP to another AP may be different for each client and is vendor specific. Some clients may have aggressive roaming where they move frequently across APs. This can result in increased contention in the network and longer delay for other clients connecting or transmitting data. The client drill down presents the association, authentication, and network connectivity events generated due to aggressive roaming.
- You can use the **Lifecycle** page to analyze the RSSI ranges, roam quality, and lifecycle eventsts.
- **DHCP, AAA, or DNS latency**—Each of the association, authentication, and network connectivity stages might add latency to the total connection time.
- The **Lifecycle Analysis** widget and the **Events** page display statistics for the DHCP, AAA, and DNS latencies.

Address poor performance of applications

Wi-Fi clients may use a wide range of advanced video coding (AVC) applications such as Google Meet, Microsoft Teams, Zoom, Skype, YouTube, and multiple e-commerce applications such as Flipkart and Amazon. In such scenarios, clients may experience poor network performance or network disconnection due to low RSSI or bad roam quality.

You can view the **Session Timeline** section in the **Lifecycle** page to analyze the RSSI ranges, and events such as success, failed, connected, disconnected, and roam quality. This analysis helps you to understand the cause and take recommended actions.

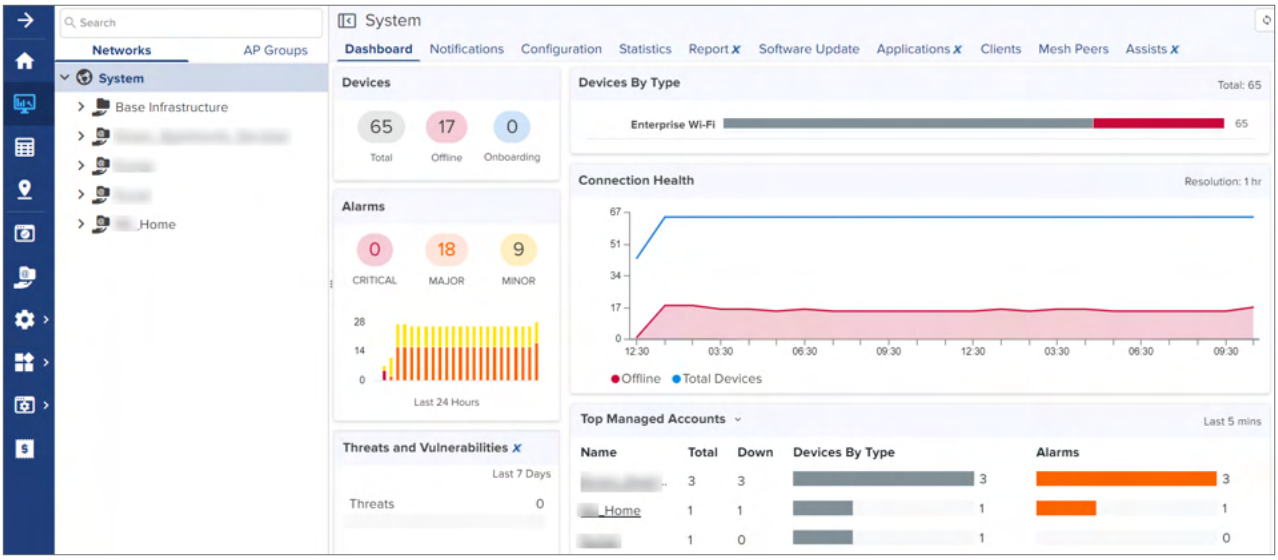
Identify OS, SSID, and AP-specific issues

Apart from run-time metrics, the **Connection Health** widget provides filters to identify performance issues with a specific vendor, operating system, and associated AP and SSID.

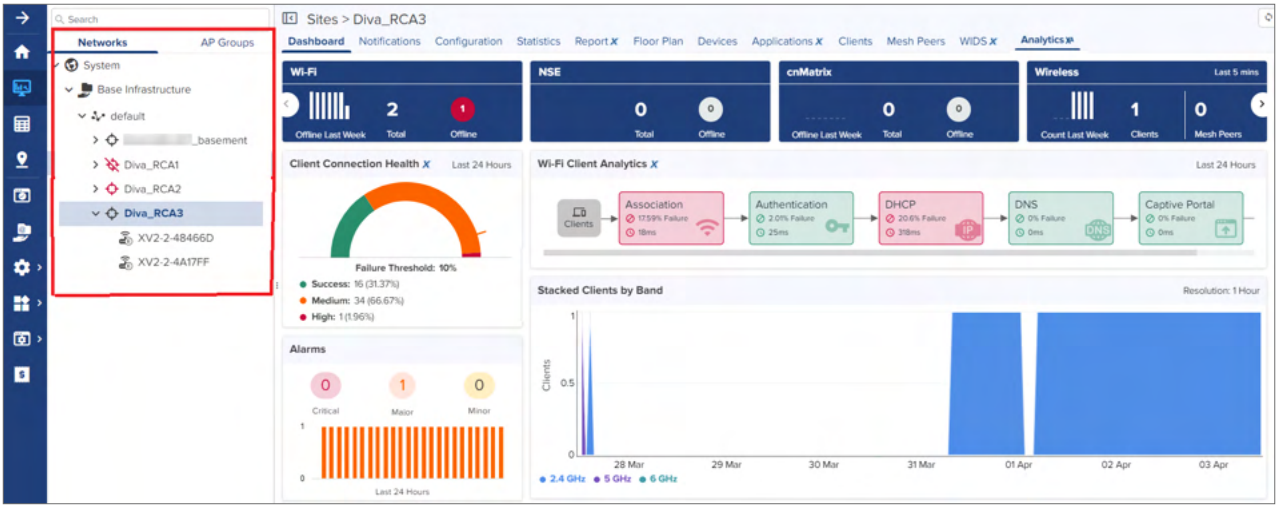
Accessing the Analytics X[A] page

To access the Analytics X[A] page:

1. On the left navigation pane, select the **Monitor and Manage** ( ) icon.



2. Select either a **System, MSP,** or **Network,** and then a **Site** node in the tree.





Note

The **Analytics X[A]** page is available only at site and client levels.

The **Dashboard** tab displays the default Wi-Fi connection statistics.

3. Select the **Analytics X[A]** tab.

Accessing Site-level consolidated details at the System- and MSP-levels

cnMaestro allows you to access consolidated information from all sites located in an account- or at the MSP-level. The information is displayed in a tabular format including details, such as the Managed Account name, the network

to which the site belongs, failure threshold and what percentage of events have crossed this threshold, and the high, medium, and low impact events.

Note

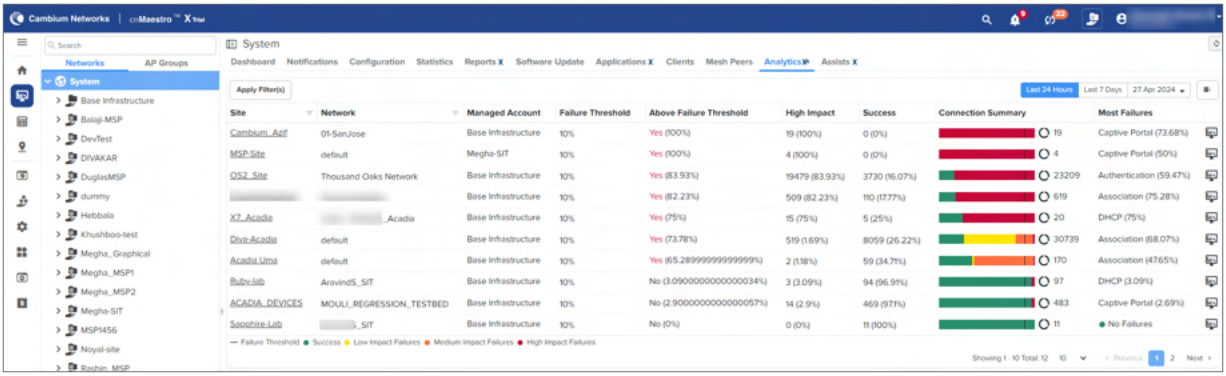
Site-level consolidated details at the System- and MSP-levels are available only for those sites where devices are onboarded and clients are connected.

To view consolidated site-level information, complete the following steps:

1. Navigate to **Monitor and Manage**.
2. In the **Networks** tab, select one of the following options:
   - To view account-level information, click **System** > **Analytics X^{A}**.

     The **Analytics X^{A}** page is displayed with consolidated information from all the sites in that account. At the system-level, data is aggregated from all sites including under any MSP accounts. However, at the MSP-level, data is aggregated from only those sites under the MSP account.

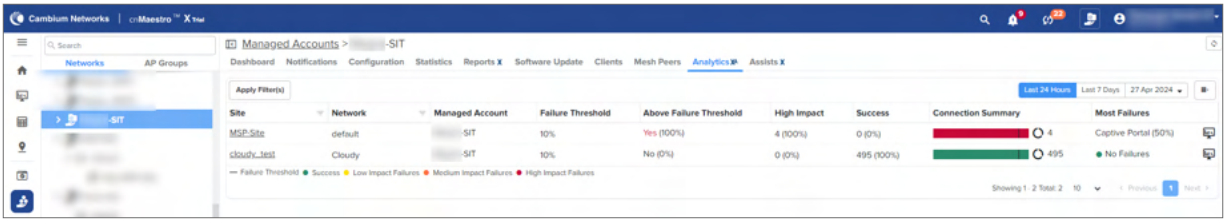
     Figure 462 *Site-level information for the complete System*

   - To view MSP-level information, click ***<MSP-Name>*** > **Analytics X^{A}**.

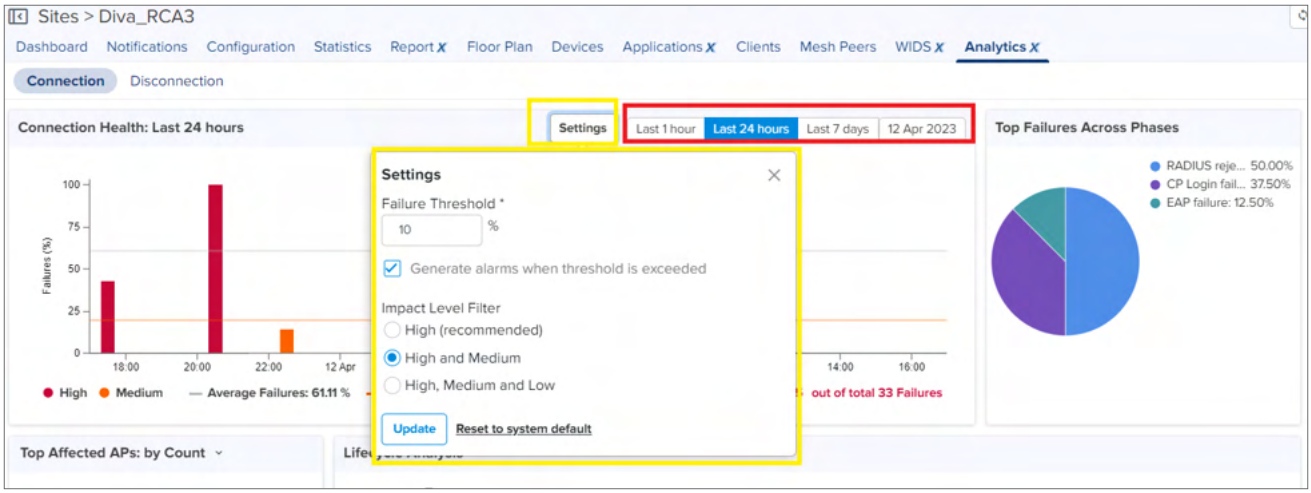
     The **Analytics X^{A}** page is displayed with consolidated information about from all the sites in that account.

     Figure 463 *Site-level information for an MSP*

Setting filters to view the connection data

After accessing the **Analytics X^{A}** page, you may change the default threshold for failed connections and set the period to view the connection events such as 1 hour or 24 hours, or 7 days.



To set failure threshold and period:

1. Navigate to the **Connection** tab
2. Click **Settings** located inside the **Connection Health** widget.
3. Enter the **Failure Threshold**.

   The default value is 10% and higher. To reset the threshold, click **Reset to system default**.
4. Select the **Generate alarms when threshold is exceeded** check box to generate a System Alarm whenever the threshold is surpassed.
5. Select the **Impact Level Filter** as:
   - High (recommended) or
   - High and Medium or
   - High, Medium, and Low
6. To apply the configuration changes, click **Update**.
7. To view the connection or disconnection events for a specific period, select the **Settings** filter as
   - Last 1 Hour or
   - Last 24 hours (Resolution 1 hour) or
   - Last 7 days (Resolution 1 hour) or
   - **Date**: To view the connection or disconnection data for a specific date. The **Date** filter supports today's date and dates of the last seven days.

   Based on the failure threshold, failure Impact filter, and the period, the **Dashboard** and **Analytics X^{A}** pages display the Wi-Fi client's connection data. Whenever the failure percentage exceeds the configured failure threshold, the Analytics X^{A} page automatically generates alerts.

Note

Consider the following key points specific to impact level failures:

- **High impact failure**—Occurs when a client is unable to establish a connection with an access point or transmit data over a connection. These failures are typically permanent until the underlying problem is resolved. High impact failures include incorrect pre-shared key (PSK); the VLAN not being configured or present on the switch; and AP software issues.
- **Medium impact failure**—Occurs when a client is intermittently unable to connect to a network,and the time to connect is relatively short (sub-seconds). These failures may not be

noticed by end users. They are caused by transient issues such as the moving client or when an access point locks the necessary information during the initial connection attempt. Medium impact failure events include fast transition (FT); authentication failure; missed packets during the four-way handshake; DHCP request process; or momentary interference from other wireless devices.

- **Low impact failure**—Occurs when a client is unable to connect to a network, without causing any noticeable impact for end users. These failures may arise due to specific wireless LAN features or configurations, such as band steering. These failures are expected, based upon the Wireless LAN protocols, and do not impact the user experience. In some cases, adjusting WLAN configuration can resolve such failure issues.

Viewing the connection events

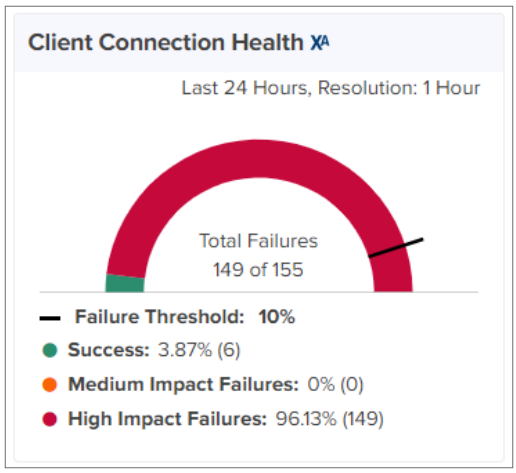
You can view and analyze the Wi-Fi connection events using the following UI pages:

- Dashboard page
- Analytics X^A page

Dashboard page

The site **Dashboard** page displays the following widgets:

- **Client Connection Health**—Displays overall statistics for connection events through a gauge/dial chart. Based on the impact level filter set on the **Analytics X^A > Settings** page, this widget displays the statistics for failed connections.



The default Impact filter for a Site is High. The resolution of this chart is 1 hour, which means every 1 hour this chart is updated. This chart displays the data based on the threshold and the impact level filter you set.

- Number and percentage of successful connections.
- Number and percentage of impact level failures for failed connections.

Note

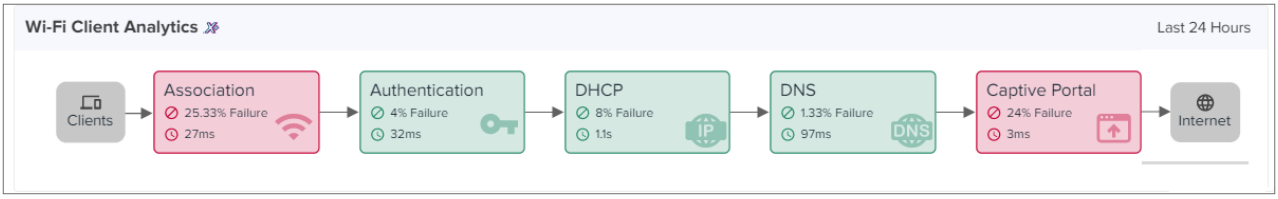
The **Client Connection Health** widget score is calculated, as follows.

Score = (Failures * 100)/(Failures+Success) %

Depending on the selection of the impact level filter on the **Analytics X^A > Settings** page, the failure count is calculated as follows:

- **High Impact**—Includes high impact failures only.
- **High and Medium Impact**—Includes medium and high impact failures.
- **High, Medium, and Low Impact**—Includes all failures: high, medium, and low impact.

- **Wi-Fi Client Analytics**—Indicates the percentage of failed connections at each step in the client lifecycle.



The phase-wise chart displays the current status by highlighting the phase in:

- **Red**—If the failure percentage exceeds the configured failure threshold configured in **Analytics X^A> Settings** page,
- **Orange**—If the failure percentage falls within the range of 80-100% of the configured failure threshold,
- **Green** —If the failure percentage is below 80% of the configured failure threshold.

The **Wi-Fi Client Analytics** widget displays the connection state of clients to the Internet in the following phases:

- Duration in each phase indicates the average time taken by the clients in the respective phase.
- **Association**—Indicates the percentage of failed connections during the association phase.
- **Authentication**—Indicates the percentage of failed client authentications such as EAP, RADIUS, and authentication key derivation (EAPOL) failures.
- **DHCP**—Indicates the percentage of failed DHCP request/responses from/to the client.
- **DNS**—Indicates the percentage of failed DNS request/responses from/to the client.
- **Captive Portal**—Indicates the percentage of failed captive portal accesses.

Note

A captive portal is a web page launched in a browser that enables access to a public network. For example, business centers, airports, hotel lobbies, coffee shops, and other public venues use captive portals to offer free Wi-Fi hotspots for internet users.

Analytics XA page

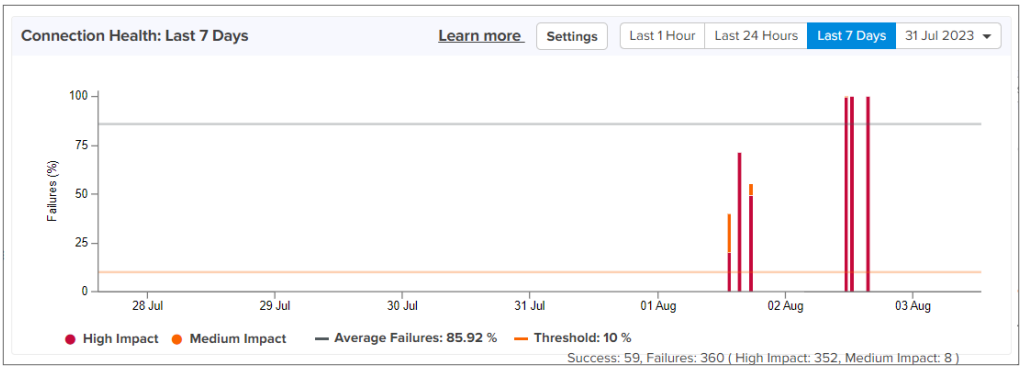
After accessing the **Analytics X** page and setting the failure threshold percentage, failure impact filter, and duration, you can analyze the connection events using the following tabs:

- Connection—Provides statistics for the connection events.
- Disconnection—Provides statistics for the disconnection events.

Connection tab

Following widgets on the **Connection** tab show connection failure events for the configured duration:

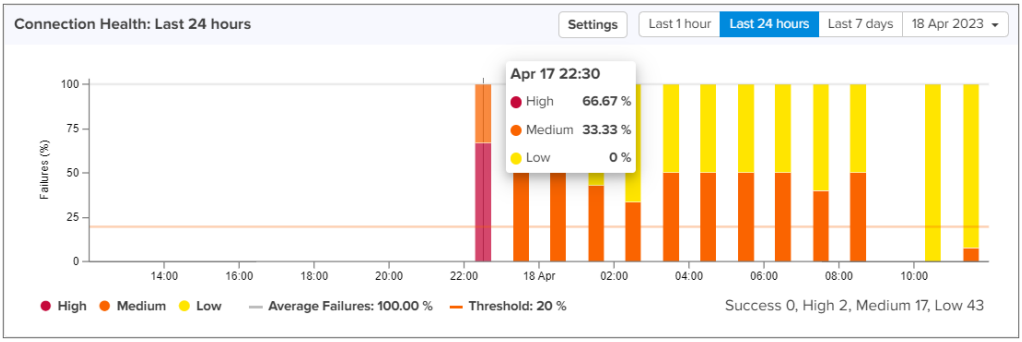
- **Connection Health**—Displays statistics of the failed connections in a bar chart, based on the threshold you set and the impact level failures in percentage.



The **Connection Health** bar chart represents the following data:

- Percentage of failed connections in a specific period for each Failure impact.
- Percentage of average failures highlighted by a grey line.
- Percentage of high, medium, and low impacted connections in different colors.
- Orange line indicates the Failure threshold percentage configured.

When you click on a bar in the chart, the chart displays the connection statistics for the selected date and time.



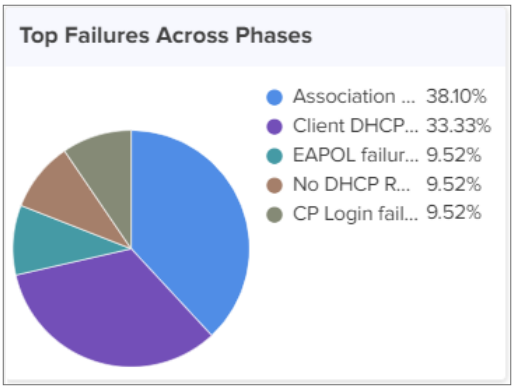
When you select a bar on the **Connection Health** chart, the following widgets display data for the selected failed connection event for the selected duration:

- Top Failures Across Phases
- Lifecycle Analysis
- Top Affected APs
- Top Affected Devices
- Top Affected OSes

Note

Click the icon, located on the top right corner of the **Analytics X^A** page, to refresh the page.

- **Top Failures Across Phases**—Displays statistics of top failed connections in a pie chart, indicating failure reasons across phases in percentage.



When you select any top failure slice on the pie chart, the following widgets display data for the selected top failure:

- Lifecycle Analysis
- Top Affected APs
- Top Affected Devices
- Top Affected OSes

- **Lifecycle Analysis**—Displays statistics for failed connections that help you analyze the life cycle of an event. By default, the phase with highest failure percentage is selected and highlighted.

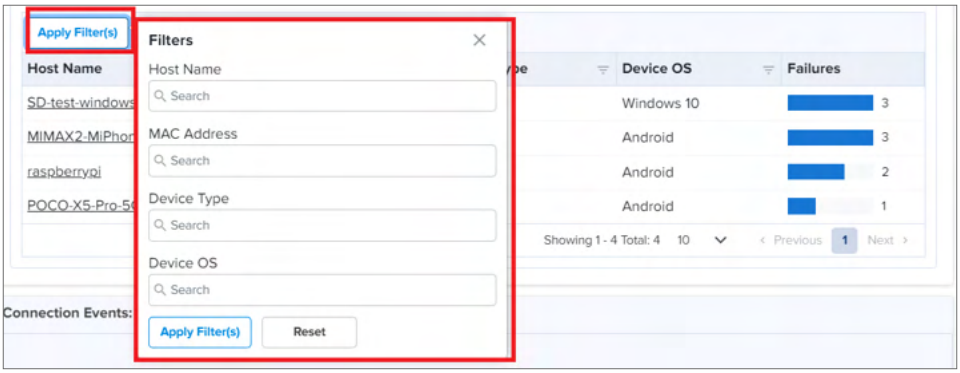


This **Lifecycle Analysis** widget displays data through the following formats:

- **Phase-wise chart**—Displays the phase-wise chart that indicates the percentage of failed Wi-Fi client connections. When you click on a phase, the line graph below the phase-wise chart displays the corresponding data.
- **Line graph**—Displays the count of failed connections based on the date and time.
- **Filters to view the required failed connection in detail**—Displays a detailed table to view failed connection events.

  To use filters and view the details of a failed connection, perform the following steps:

  1. Inside the **Lifecycle Analysis** widget, click **Apply Filter(s)** located below the line graph section.

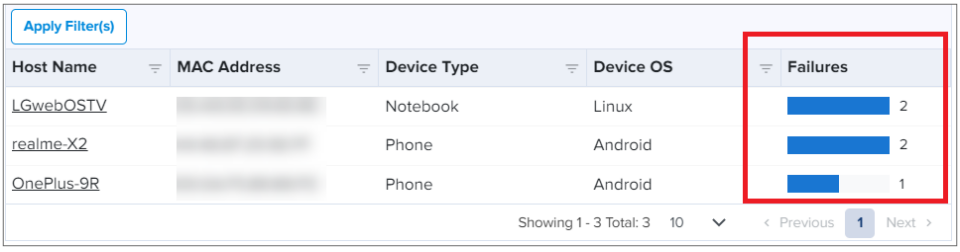


  2. To search for and view data of the required client's connection event, enter one or more of the following values:

Filter name	Description
Host Name	The name of the host for which you want to view the failed connection details.
MAC Address	The MAC address of the device for which you want to view the failed connection details.
Device Type	Type of device used for the connection.
Device OS	The operating system (OS) running on the device.

  3. Click **Apply Filter(s)** to apply the changes.

     A table below the line graph displays the count of failures for the searched criteria, as shown in the following figure:

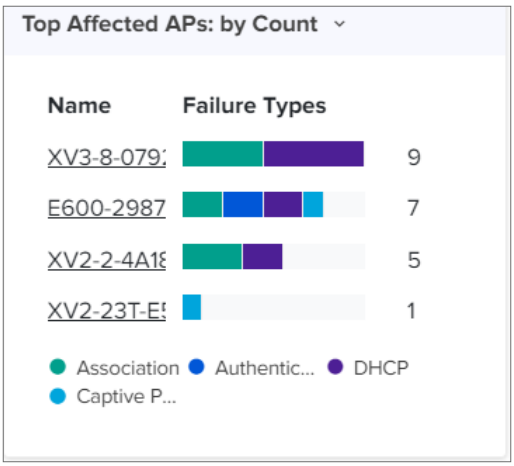


Note

You can also click the icon in the table to quickly search for Mac address, device type, device OS, and failure count.

When you click on a host name, the site-specific **Clients** page appears, displaying the connection data for the selected host.

- **Top Affected APs**—Displays the name of top affected APs and the statistics for the failed connection. To view the statistics of top affected APs in percentage or count, click the ⌄ icon next to the **Top Affected APs** widget title.



Placing the cursor on any colored bar, displays the failure type and count specific to the failed connection. If you click on any AP name, the site-specific **Wi-Fi** dashboard appears with the AP or device information.

- **Top Affected Device Types**—Displays the name of top affected device types and the statistics for the failed connection in count or percentage.
- **Top Affected OS**: Displays the name of top affected OS and the statistics for the failed connection in count or percentage.
- **Connection Events : Last 1 Hour**—A table with filters displays the details of successful or failed connection events that occurred in the last one hour.

Note

Failure events per AP, Device type, and OS are displayed only when an hourly bar is selected.

To use filters and view the connection details for the last one hour, perform the following steps:

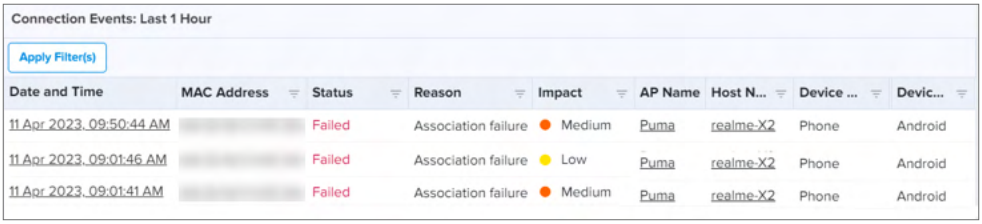
1. Inside the **Connection Events : Last 1 Hour** widget, click **Apply Filters**.
2. To search and view data for the last one hour, enter one or more of the following details:

Filter name	Description
MAC Address	The MAC address of the device with connection events.
Success	Select whether you want to view successful or failed connection events. • Success • Failed
Reason	Select the required reason type from the drop-down list such as MAC-ACL, MAC-AUTH, QoS failure, Passpoint failure, Capability mismatch, L2 Auth failure, Association failure, Roaming failure, SAE failure, Cipher failure, or TDLS failure.

Filter name	Description
Impact	Select the required impact type from the list: • Low • Medium • High
Host Name	The name of the host for which you want to view the connection state.
Device Type	The type of device used for the connection.
Device OS	The operating system (OS) running on the device.

3. Click **Apply Filter(s)** to apply the changes.

   The table displays the connection event details with date, time, and AP names for the searched criteria.



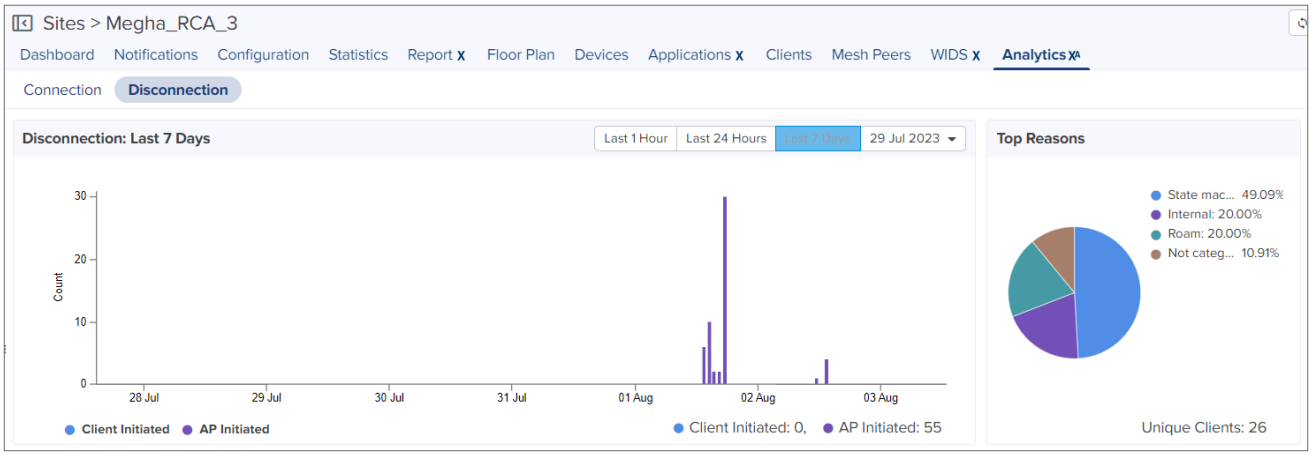
Note

You can also click the icon in the table to quickly search for status, reason, impact level, AP name, host name, device type, and device OS.

- When you click on any date and time, the **Events** page displays connection state data for the selected date and time.
- When you click on any AP name, the site-specific **Wi-Fi** dashboard displays the AP or device information.
- When you click on a host name, the site-specific **Clients** page displays the connection data for the selected host.

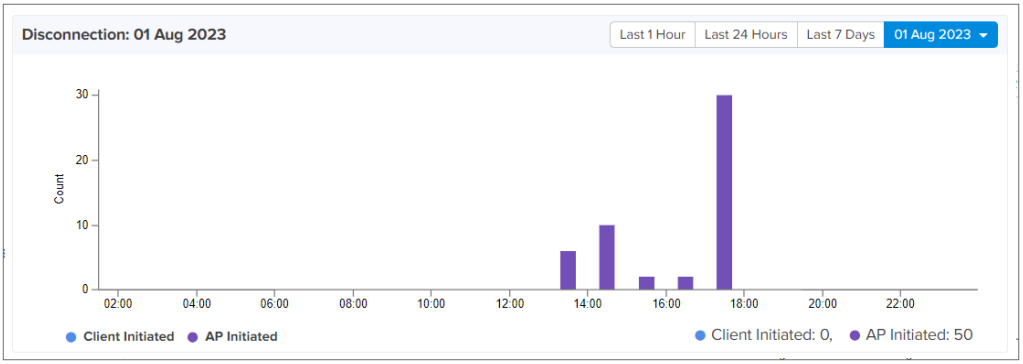
Disconnection tab

On accessing the **Analytics X^A** page, click on the **Disconnection** tab and set the time filter by choosing the required time period as last 1 hour, last 24 hours, last 7 days, or a custom date. The **Disconnection** tab displays the data for the selected time period.



The following widgets on the **Disconnection** page support root cause analysis:

- **Disconnection**—Displays the count of clients and APs initiated during the time period.



  When you click on a bar in the chart, the chart displays the count of Clients and APs initiated at the specific date and time.

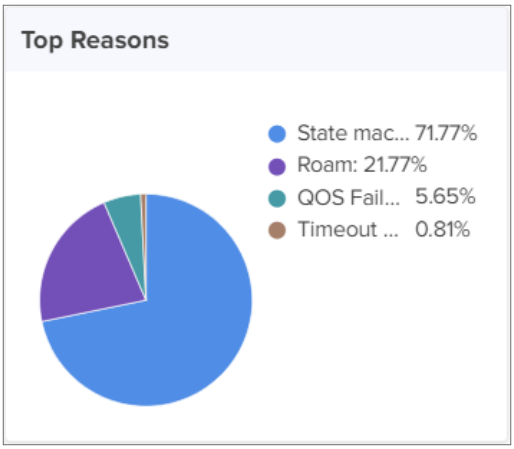
  When you select any bar on the **Disconnection** chart, the following widgets display data for the selected disconnection event:

  - Top Reasons
  - Top Reporting APs
  - Analytics
  - Top Reporting Device Models
  - Top Reporting Device Types
  - Top Reporting OSes

  Note

  Click the icon, located on the top right corner of the **Analytics X[A]** page, to refresh the page.

- **Top Reasons**—Displays statistics of top failure reasons such as state machine issues, roam, QoS failures, and timeout failures.



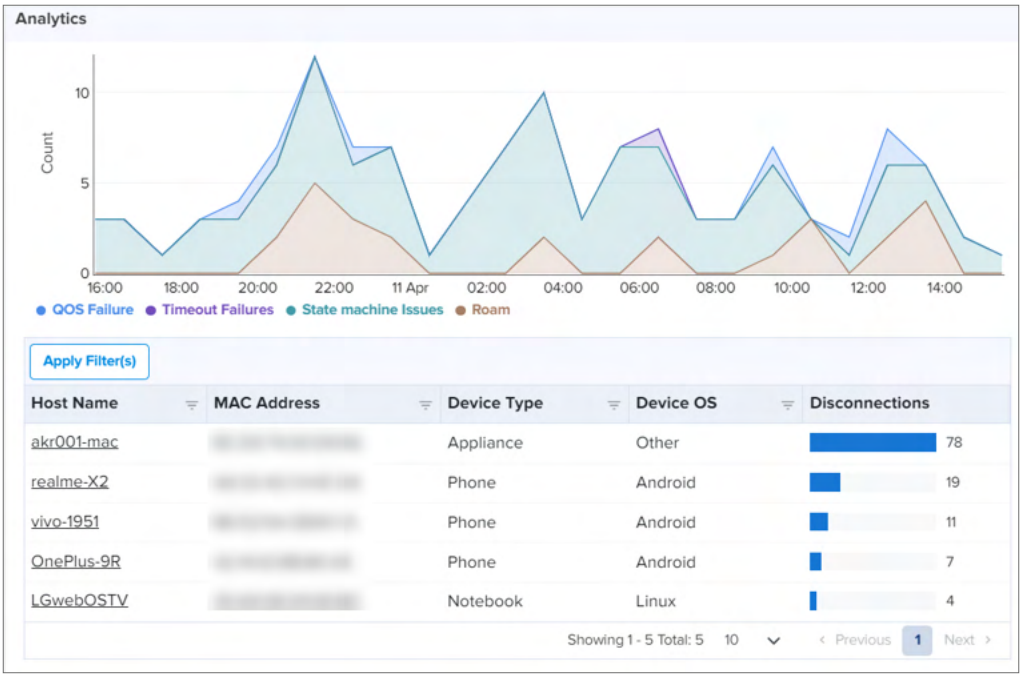
When you select any top failure slice on the pie chart, the following widgets display data for the selected top failure:

- Top Reporting APs
- Analytics
- Top Reporting Device Models
- Top Reporting Device Types
- Top Reporting OSes

Note

Click the icon, located on the top right corner of the **Analytics X^A** page, to refresh the page.

- **Analytics**—Displays statistics for disconnections to help analyze failure events in detail.



This **Lifecycle Analysis** widget displays data in the following formats:

- **Line graph**: Displays the count of disconnections, including the date, time, and failure reasons in different colors.
- **Filters to view the required disconnection in detail**: A table with filters displays detailed information of a disconnection event.

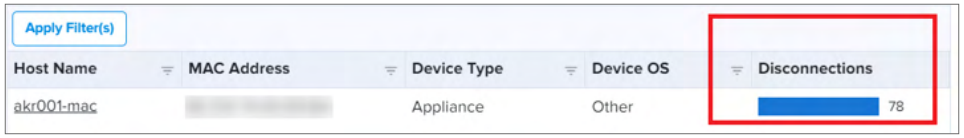
  To use filters and view the details of a disconnection event, perform the following steps:

  1. Inside the **Analysis** widget, click **Apply Filters** located below the line graph section.
  2. To search for and view data of the required client's disconnection state, enter one or more of the following:

Filter name	Description
Host Name	The name of the host for which you want to view the disconnection details.
MAC Address	The MAC address of the device for which you want to view the disconnection details.
Device Type	Type of device used for the connection.
Device OS	The operating system (OS) running on the device.

  3. Click **Apply Filter(s)** to apply the changes.

     A table below the line graph section displays the count of disconnections for the searched criteria, as shown in the following figure:

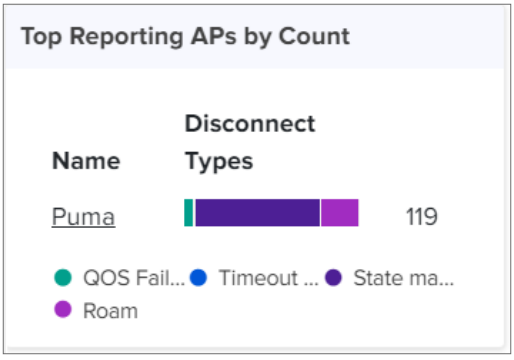


Note

You can also click the icon in the table to quickly search for MAC address, device type, device OS, and disconnection count.

When you click on a host name, the site-specific **Clients** page displays the disconnection state data for the selected host.

- **Top Reporting APs**—Displays the names of top APs and the count of disconnections in different colors based on the disconnection types.



When you place your cursor on any color, you can view the reason type and count specific to the disconnection type.

- **Top Reporting Device Types**—Displays the names of the top devices and the count of disconnections in different colors based on the disconnection reasons. When you place your cursor on any color, you can view

the reason type and count specific to the disconnection events.

- **Top Reporting OS**—Displays the names of top OS and the count of disconnections. Different colors are used to highlight the disconnection reasons. When you place your cursor on any color, you can view the reason type and count specific to disconnection.
- **Disconnect Events: Last 1 Hour**—A table with filters displays the data of disconnection events that occurred in the last one hour.

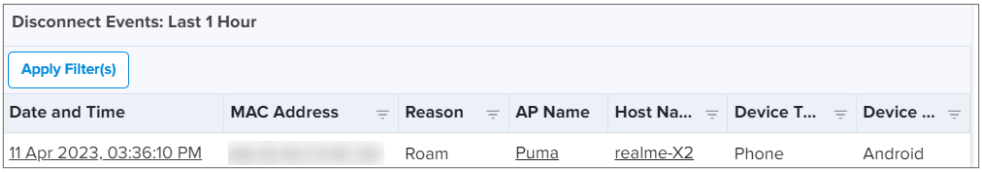
  To use filters and view the disconnection state details for the last one hour, perform the following steps:

  1. Inside the **Disconnection Events : Last 1 Hour** widget, click **Apply Filters**.
  2. To search for and view data of the disconnection events, enter one or more of the following:

Filter name	Description
MAC Address	The MAC address of the device for which you want to view the disconnection events.
Reason	Select the type of reason from drop-down list such as Unknown-disc-O, QoS failure, Radius failures, TDLS failures, timeout failures, state machine issues, AP Resource failures, AP assisted roaming, and roam.
Host Name	The name of the host for which you want to view the disconnection state.
Device Type	Type of device used for the connection.
Device OS	The operating system (OS) running on the device

  3. Click **Apply Filter(s)** to apply the changes.

     The table displays the disconnection state with date, time, and AP names for the searched criteria.



Note

You can also click the icon in the table to quickly search for MAC address, reason, AP name device type, device OS, and disconnection count.

- When you click on any date and time, the **Events** page displays the disconnection state data for the selected date and time.
- When you click on any AP name, the site-specific **Wi-Fi** dashboard displays the AP or device information.
- When you click on a host name, the site-specific **Clients** page displays the disconnection state data for the selected host.

Viewing a client or host-specific connection or disconnection event

You can analyze client or host-specific connection or disconnection events in detail and take appropriate actions.

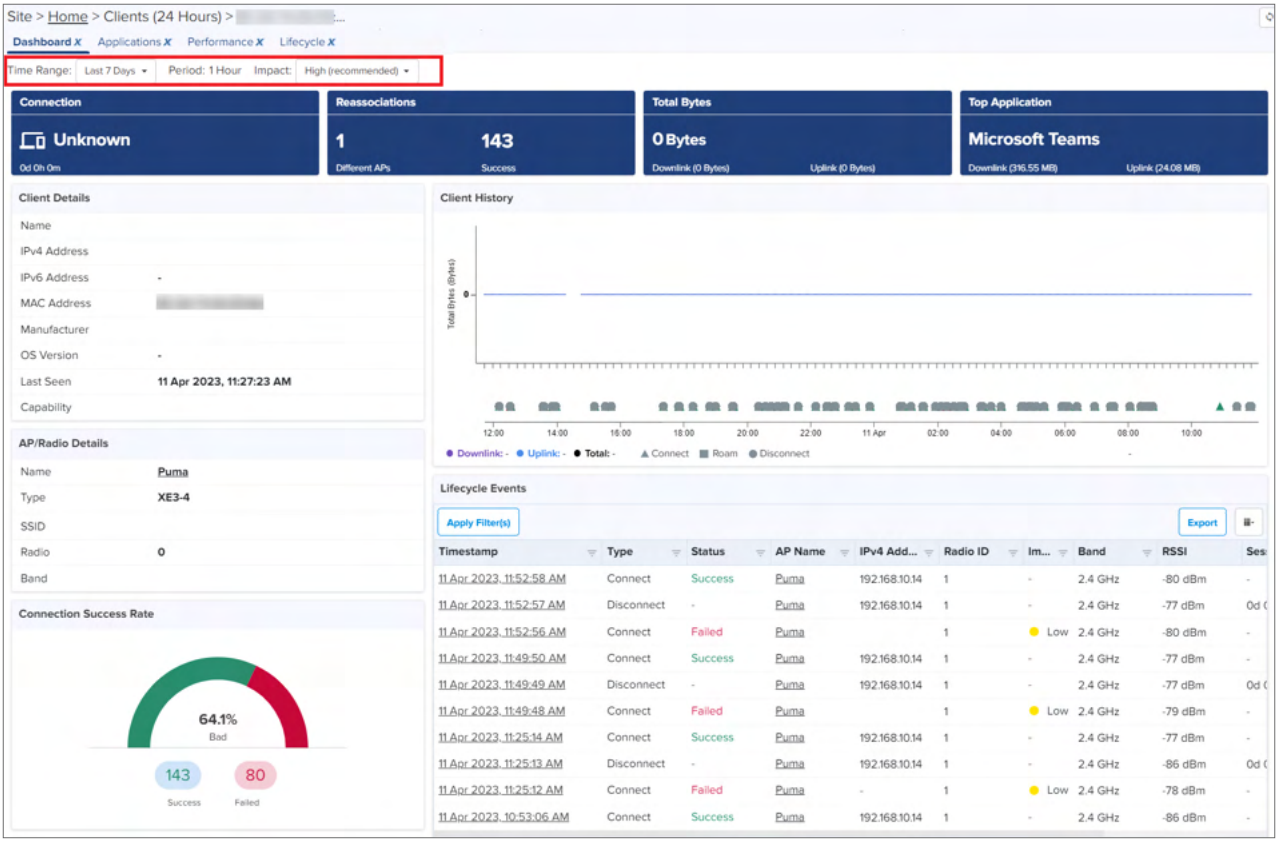
To view client or host-specific information, perform the following steps:

1. Click on a host name to view the connection or disconnection state in detail.

   You can locate the host names in the following widgets:

   - **Lifecycle Analytics** on the Connection page—host names are available in a table below the line graph section.
   - **Connection Events: Last 1 Hour** on the Connection page.
   - **Analytics** on the Disconnection page.
   - **Disconnect Events: Last 1 Hour** on the Disconnection page.

   When you click the required host name, the site-specific **Clients** page displays detailed information for the selected host. The following figure is an example of the site-specific **Clients** page:



   This site-specific **Clients** page contains the following tabs:

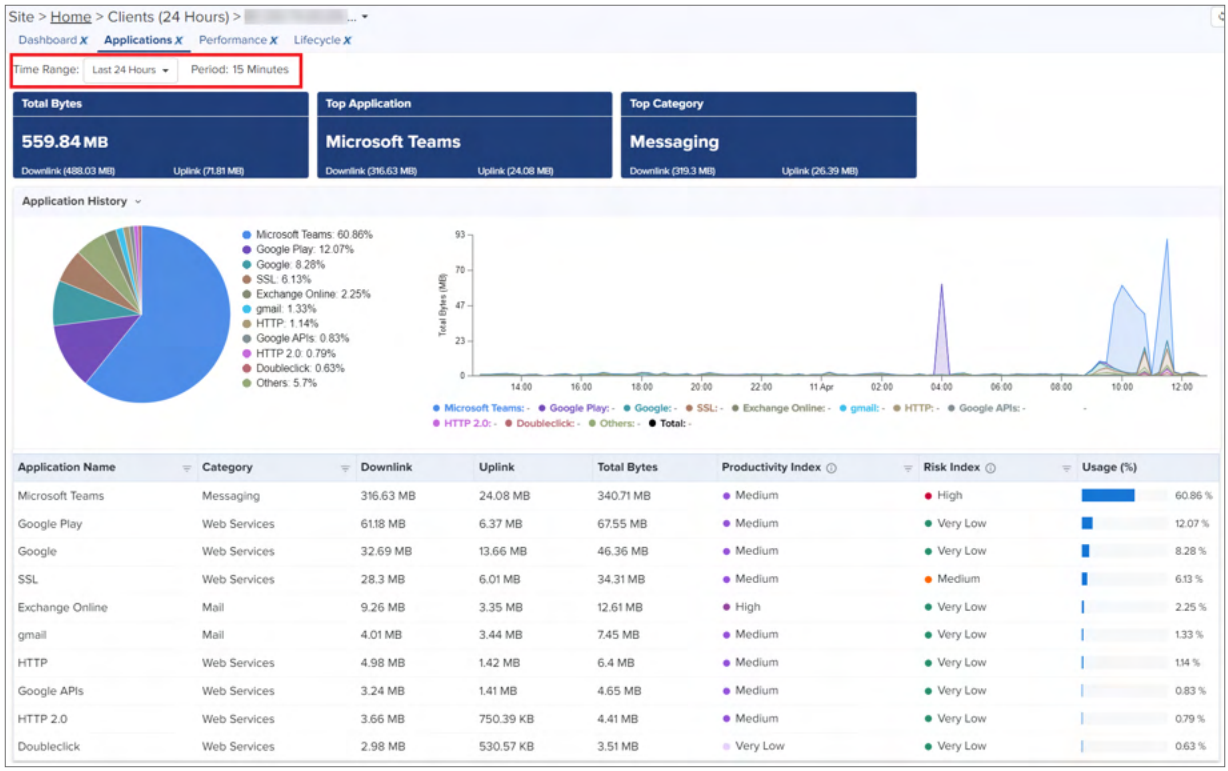
   - **Dashboard**—Provides a summary of the client connection or disconnection events such as Client history or lifecycle events.

     By default, the **Dashboard** tab is visible when the site-specific **Clients** page appears. Based on the period options such as Last 24 Hours or Last 7 Days from the **Time Range** filter on the **Dashboard** page, the site-specific **Dashboard** page displays the Wi-Fi client information in the following widgets:

     - Connection
     - Reassociations
     - Total Bytes
     - Top Application
     - Client Details

- Client History
- AP/Radio Details
- Lifecycle Events
- Connection Success Rate
- Top Failures Across Phases
- RSSI
- SNR
- Top Applications
- Data Rate
- Top Categories

- **Applications**—Provides detailed information of top applications used for the connection.

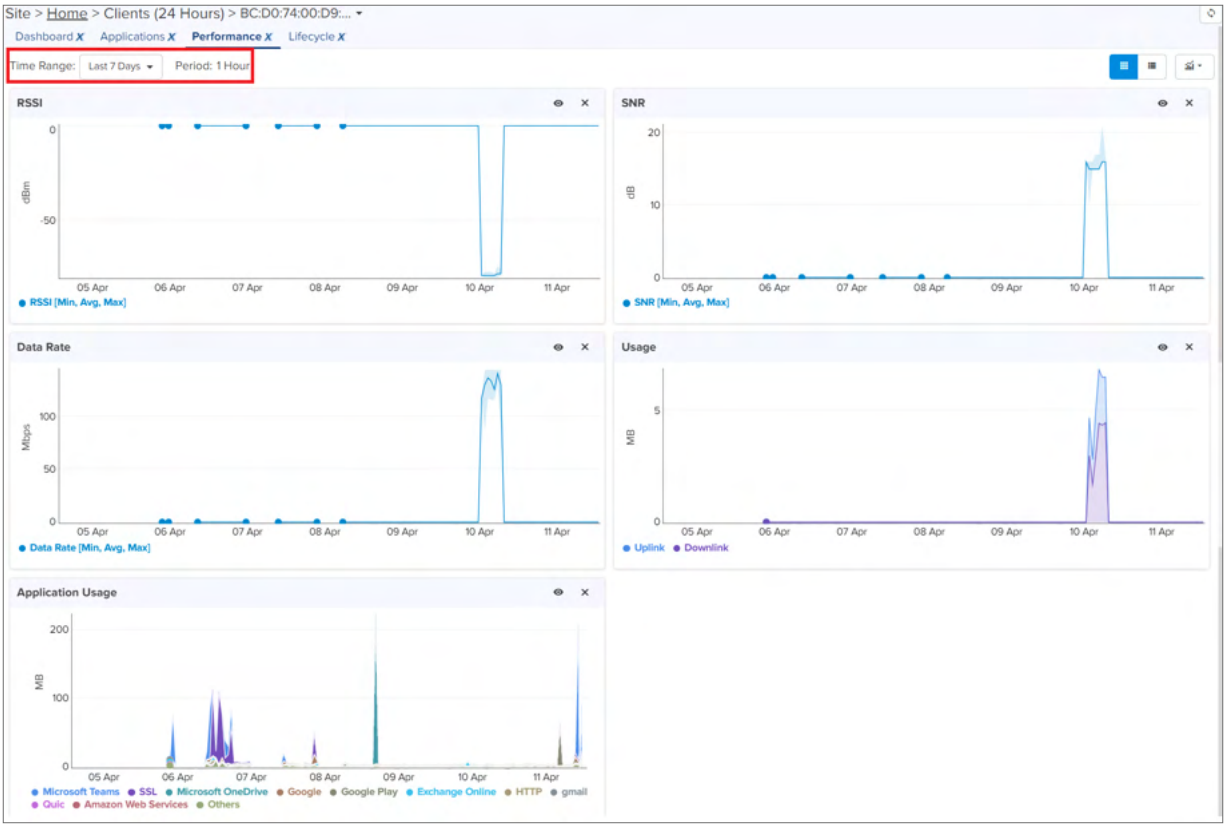


Based on the time period you select from the **Time Range** filter on the **Applications** page, the **Applications** page displays the application information for the Wi-Fi client in the following widgets:

- Total Bytes
- Top Application
- Top Category
- Application / Category History

  Click the ⌄ icon (for example, next to **Application History**) to view the history of category details.

- **Performance**—Provides detailed information of RSSI, SNR, date rate, usage in uplink and downlink, and the application usage.

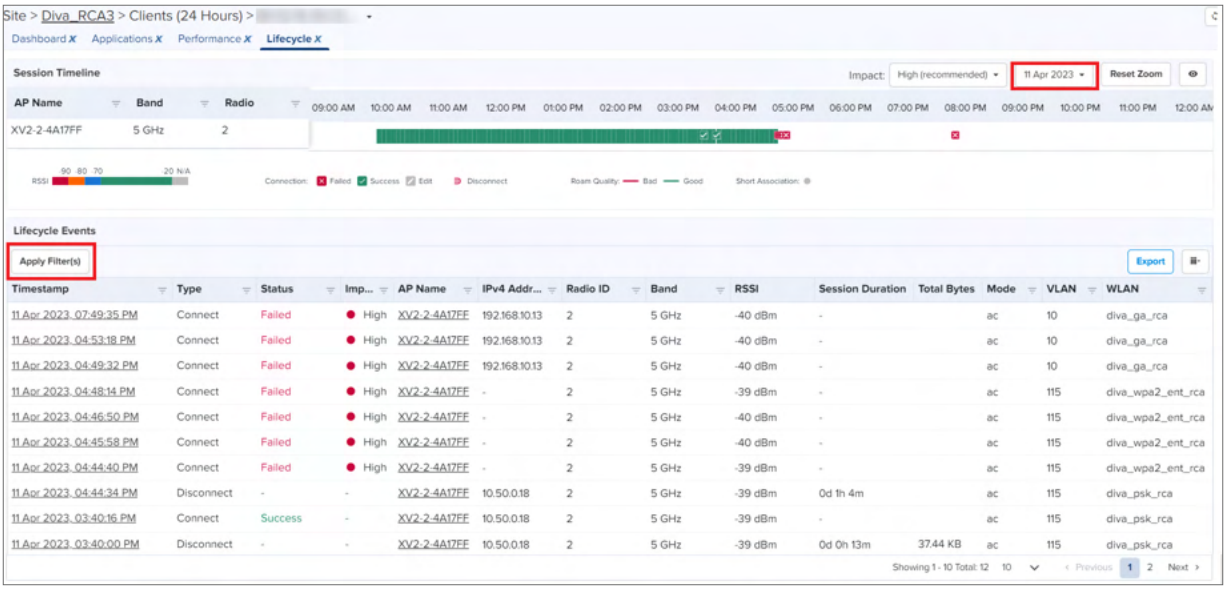


Based on the time period you select from the **Time Range** filter on the **Performance** page, the **Performance** page displays the network performance for the Wi-Fi client in the following widgets:

- RSSI
- SNR
- Data Rate
- Usage
- Application Usage

You can click the icon (Data point selector) to filter and view the required options specific to performance in the widgets.

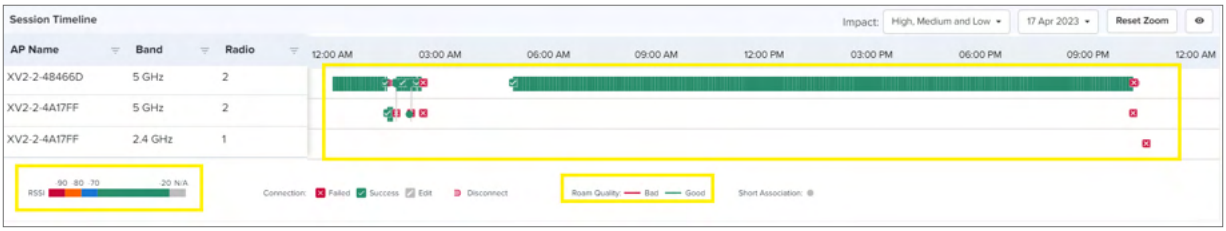
- **Lifecycle**—Provides detailed information of the client's connection or disconnection events.



Based on the date and impact levels you select from the date and **Impact** filters, the **Lifecycle** page displays the session timeline and the lifecycle events of the Wi-Fi client for the selected date.

In the **Session Timeline** section, you can find the AP names, band used, and the radio index. In addition, different indicators mark RSSI, the connection event as failed or success, the disconnection event, roam quality as bad or good, and short association.

For example, in the following UI page, the RSSI ranges and bad and good roam quality are highlighted using different colors.



- Placing the cursor on the ✓ icon, displays date and time of the succeeded event.
- Placing the cursor on the ✗ icon, displays reason and cause for the failed event.
- Clicking ✓ or ✗ icon in the **Session Timeline** section, displays the **Events** page with detailed information for the selected event.
- Clicking the disconnect ( ) icon, displays details about the event and disconnection reason.
- The short association ( ) icon denotes that the client connected and disconnected within a minute.
- The edit ( ) icon denotes that the client connection failed in DHCP, DNS or Captive portal phase in the first connection attempt but succeeded later.

Note

A client connection is considered failed in DHCP, DNS, or CP, if the client fails to complete the phase within 45-60 secs.

The **Lifecycle Events** section provides detailed information of the client's connection and disconnection events such as timestamp, connection type, connection status, AP name, IPv4 address, radio ID, impact of

the event, band used, RSSI, session duration, total bytes, wireless mode used, VLAN used, and WLAN details.

You can also use the filters to view and analyze the required event information. To view the required lifecycle event using filters, perform the following steps:

a. In the **Lifecycle Events** section, click **Apply Filter(s)**.

b. Enter one or more of the following details:

Filter name	Description
Timestamp	Time period for which you want to view the data: • Between • After • Before
Type	Type of event for which you want to view the data: • Roam • Connect • Disconnect
Status	State of the event: • Success • Failed
AP Name	Name of the AP that is used in the event.
IPv4 Address	The IPv4 address used for the connection.
Radio ID	ID of the radio used in the event.
Impact	Impact level of the event. • Low • Medium • High
Band	The bandwidth used for the connection.
Mode	The standard wireless mode used for the connection. For example: 802.1ac
VLAN	The VLAN ID used for the connection.
WLAN	The WLAN ID used for the connection.



Note

You can also click the icon in the **Lifecycle Events** table to quickly search for type, status, AP name, IPv4 address, radio ID, impact, band, RSSI, VLAN, and WLAN.

c. Click **Apply Filter(s)**.

The table in the **Lifecycle Events** section is updated with the required information for the client or host.

You can also drill-down an event to view what went wrong during the connection or the reason for the disconnection event.

2. Analyze the data for the required client or host and take actions.

Viewing an event-based connection or disconnection event

After viewing the lifecycle events for a specific client or host, you can drill-down an event to analyze what caused a failed connection or a disconnection.

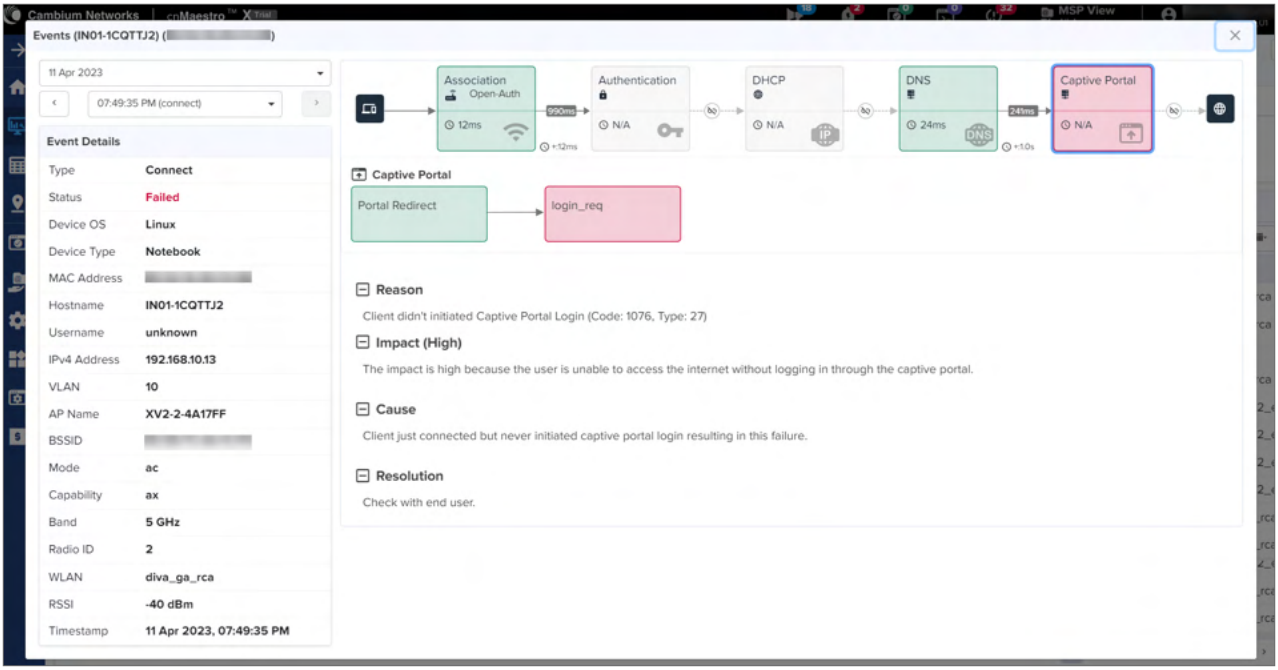
To view an event-based connection or disconnection state, perform the following steps:

1. Click **Date and Time** or **Timestamp** to view the connection or disconnection event in detail.

   You can locate a date or timestamp in the following widgets:

   - **Timestamp** in the **Lifecycle Events** widget available on both the **Connection** page and the **Disconnection** page)
   - **Date and Time** in the Connection Events: Last 1 hour widget on the **Connection** page
   - **Date and Time** in the Disconnect Events: Last 1 hour widget on the **Disconnection** page

   When you click on **Timestamp** or **Date and Time**, the **Events** screen displays the detailed event information.



   The **Events** page provides phase-wise information with complete event details such as reason, impact, cause, and resolution. These event-based details help with troubleshooting.

2. To view an event for a specific date, you can select the required date from the date drop-down list.



Similarly, you can use < or > to view time-based events for a client. You can also select the time-based events from the drop-down list.

3. Click the ✕ icon to close the **Events** page.

Viewing an AP-specific information

You can view an AP-specific information for the required client or event and analyze the connection or disconnection data. This analysis helps identify device details used for the connection.

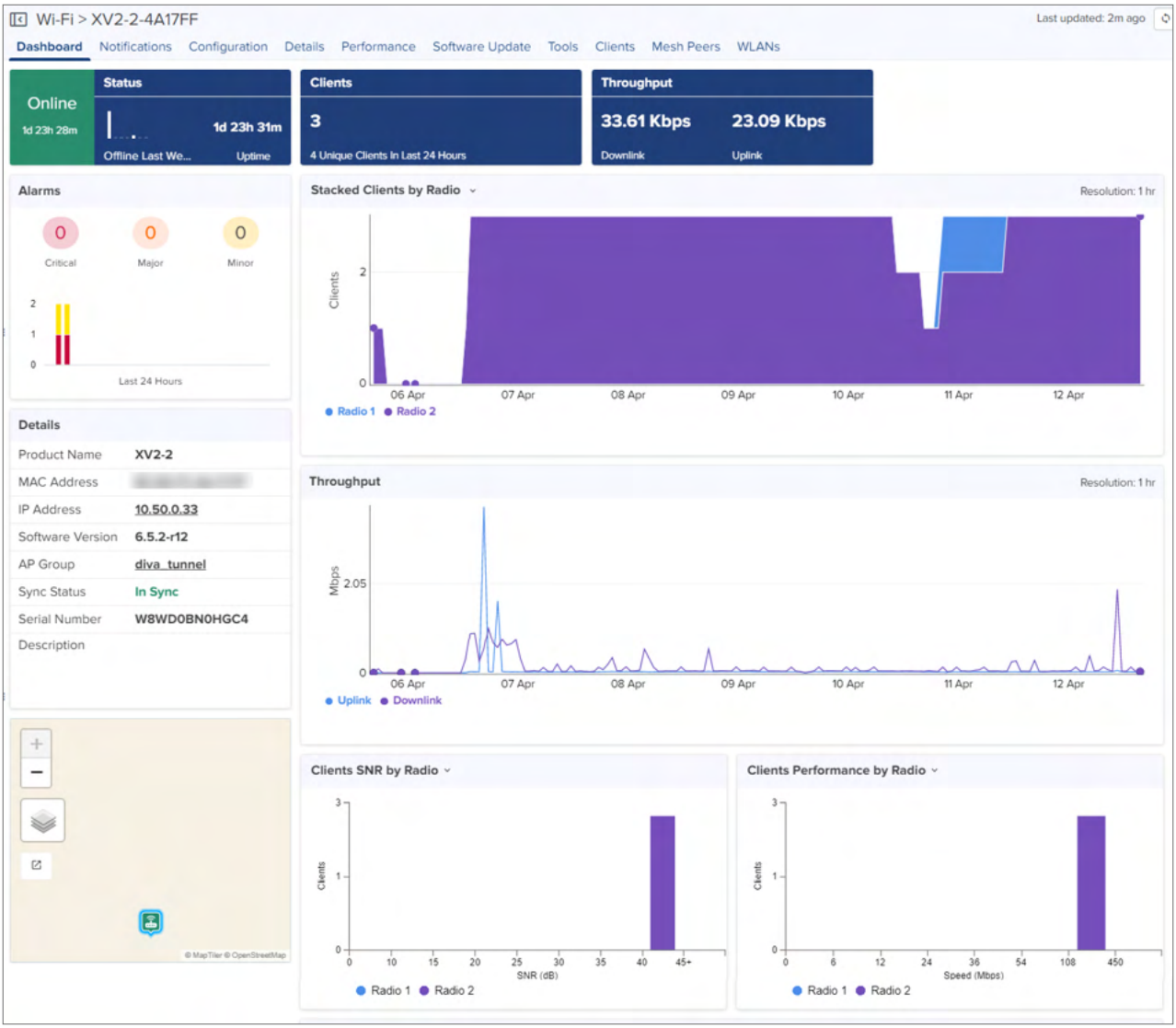
To view AP-specific information, perform the following steps:

1. Click the **AP Name** to view the data.

   You can locate an AP name in the following widgets:

   - Top Affected APs on the **Connection** page
   - Connection Events—Last 1 Hour on the **Connection** page
   - Top Reporting APs on the **Disconnection** page
   - Disconnect Events—Last 1 Hour on the **Disconnection** page
   - Lifecycle Events on both the **Connection** and **Disconnection** pages

   When you click on the required AP name, the site-specific **Wi-Fi** dashboard dispalys the AP or device information.



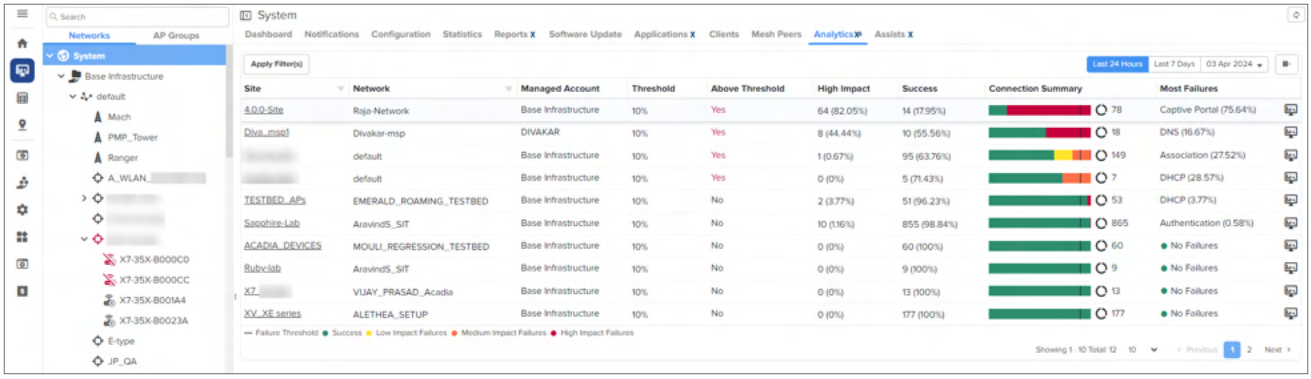
For more information on the AP (or device) specific dashboard, refer to the Wireless LAN Dashboards section of cnMaestro Cloud User Guide.

2. Analyze the AP data and take appropriate actions.

System Analytics

The System Analytics page provides the consolidated data of all the Site Analytics. For more information, refer to the Analytics X[A] page section.

Figure 464 *System Analytics*



Managed Services

This section includes the following topics:

- Managed Accounts
- Managing subscribers (end-customer)

Managed Accounts

This section includes the following topics:

- Overview
  - Managed Accounts
  - Accounts
  - Managed Account Service
  - Account Service Users (Administrators)
- Configuring Managed Account Services
  - Enable Managed Accounts
  - Creating Managed Account Services
  - Creating Account
  - Validating Account Users
- Managed Account Administration
  - Overview
  - System Dashboard
  - Account Administration
  - Device Management
  - Swap 60 GHz cnWave Accounts
  - Disabling the Managed Accounts feature

Overview

Managed Accounts allow the cnMaestro owner to partition their installation into independent accounts with their own administrators and configuration. This feature is for MSPs who want to provision a full cnMaestro account for their customers, while still maintaining control over the global deployment.

Managed Accounts

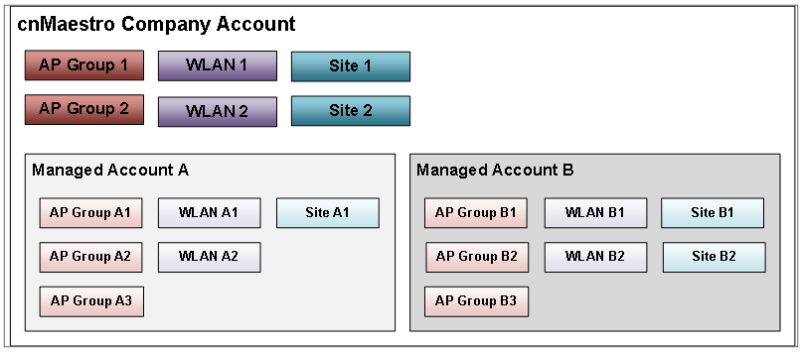
The Managed Accounts feature combines Accounts with Account Services.



Accounts

Managed Accounts group cnMaestro devices and configuration objects (such as AP Groups, WLANs, and Sites) into administration domains within a single cnMaestro deployment . Accounts are independent, and the devices added to them are configured using the objects in the Account.

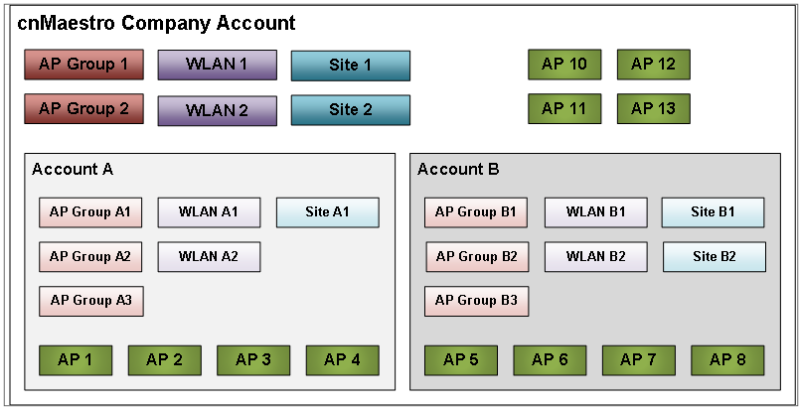
Figure 465 *Accounts*



Access Points

Access Points exist in the global Company Account, or they can be added to a single Managed Account. Access Points in a Managed Account are configured using the Wi-Fi Profiles in that Managed Account.

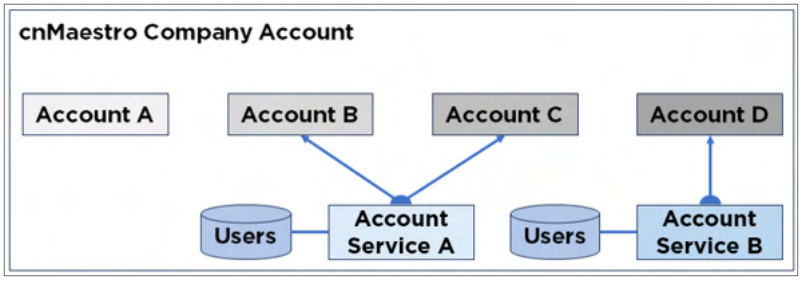
Figure 466 *Access Points*



Managed Account Service

A Managed Account Service creates a branded version of the cnMaestro UI. Each Account Service can be mapped to multiple Accounts.

Figure 467 *Account Service*



Each Managed Account Service adds the following support to an Account:

Support	Details
Administrator Database	Each Account Service has its own independent database of users who can be shared across multiple Accounts.
Custom Login URL	The path of the login URL used by the Account Service Administration can be tailored to the Account Service. The path must be unique across all cnMaestro.
Branded UI	The Account UI is customized for the Account Service through graphics, colors, and text.
Account Service Users	List of all the users mapped to the Managed Account Service. They may be mapped to zero or more associated Accounts.

Account UI

The Account UI can be customized to represent the service brand. A sample Account UI is shown below:

Figure 468 *Account UI - Sample 1*

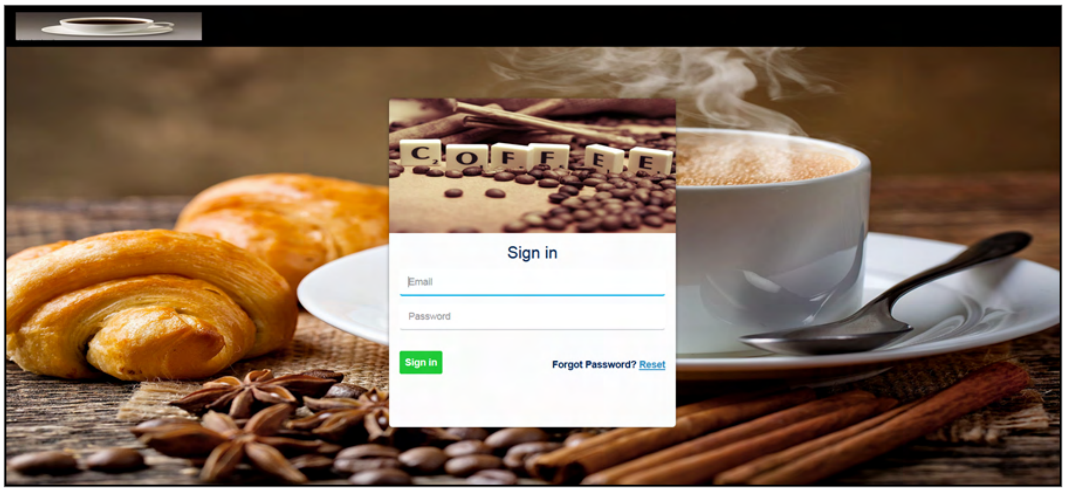
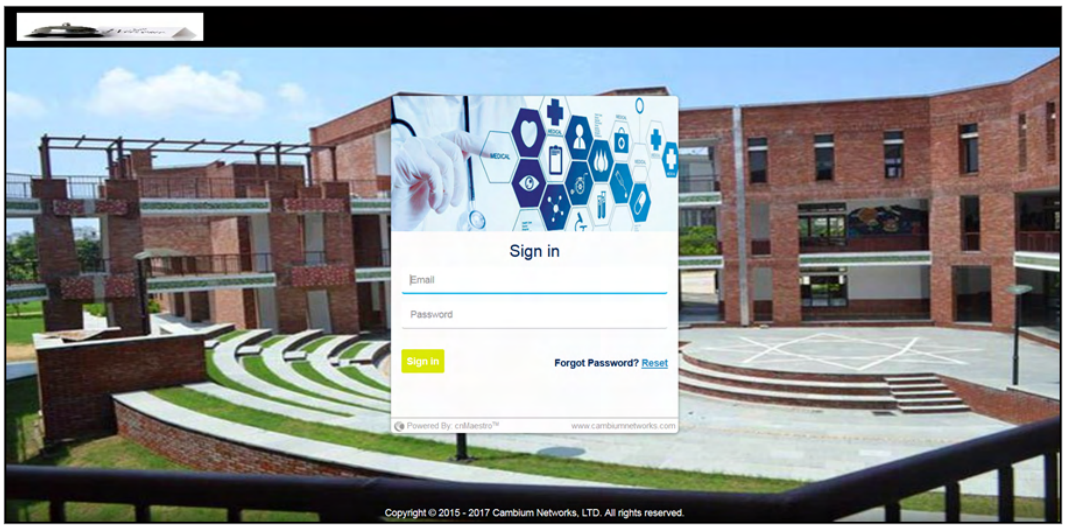


Figure 469 *Account UI - Sample 2*



Account Service Users (Administrators)

Account Service Users are assigned to Accounts. They access similar features as the Global cnMaestro Administrators, except they are only allowed to manage the subset of devices and objects (AP Groups, WLAN, Sites, etc.).

Account Service Users (Administrators) Roles

Account Service Users can be assigned one of three roles as shown below for each account:

- Administrator
- Monitor
- Operator

The authorizations for each Role are listed in the table below:

Table 104 *Tenant Administrator Roles*

Feature	Description	Administrator	Operator	Monitor
AAA Services (Global cnMaestro administrator only)	Add AAA services	None	None	None
Administration Settings (Global cnMaestro administrator only)	Change global application configuration, Onboarding settings like password change	None	None	None
API Management (Global cnMaestro administrator only)	Create API clients	None	None	None
Application Operations 1	Create Networks, Towers, and Sites	All	View	View
Application Operations 2	Tech Dump, import/export server data, change Account Type (Enterprise or Access and Backhaul)	None	None	None
Association ACL	Configure MAC list on the controller	All	View	None
Auto-provisioning (Global cnMaestro administrator only)	Support for global auto-provisioning rules	None	None	None
Audit logs	Logs user action of different features	All	All	All
Device Operations	Reboot device, link test, connectivity test	All	All	None
Device Override	Per-device configuration changes	All	All	View
Global Configuration	Apply Configuration through Templates and AP Group	All	View	View
Guest Access	Guest Access	All	View	View

Table 104 *Tenant Administrator Roles*

Feature	Description	Administrator	Operator	Monitor
Portal				(Sessions)
Monitoring	Access Device Statistics Data	All	All	View
Notifications	View Alarms and Events	All	All	View
Onboarding	Approve Device Onboards	All	All	View
Reporting	Generate reports	All	All	All
Software Images (Global cnMaestro administrator only)	Download device software images	All	None	None
Software Upgrade	Upgrade device	All	All	View
System Operations	Reboot VM, change log level, system upgrade, system monitoring	None (Except System Monitoring)	None (Except System Monitoring)	None (Except System Monitoring)
User Management	Manage users, roles, and sessions	All	None	None

Configuring Managed Account Services

This section provides the following details on configuration of Account Services in cnMaestro:

- Enable Managed Accounts
- Creating Managed Account Services
- Creating Account
- Validating Account Users

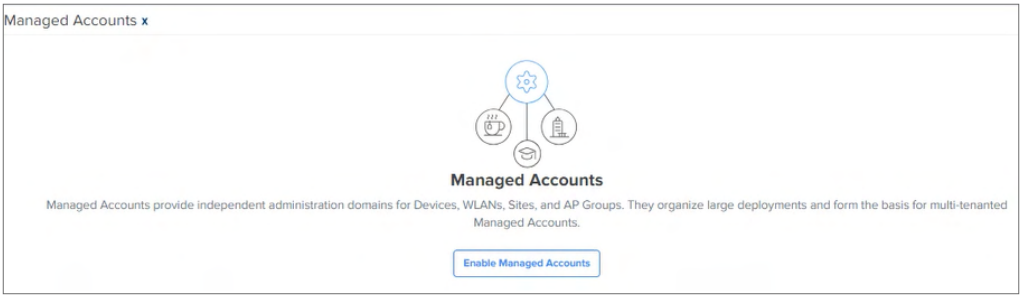
Enable Managed Accounts

By default, Account Services is disabled in the cnMaestro UI.

To enable Account Services:

1. Navigate to **Managed Services** > **Managed Accounts**.
2. Click the **Enable Managed Accounts.**

Figure 470 *Enabling Managed Accounts*



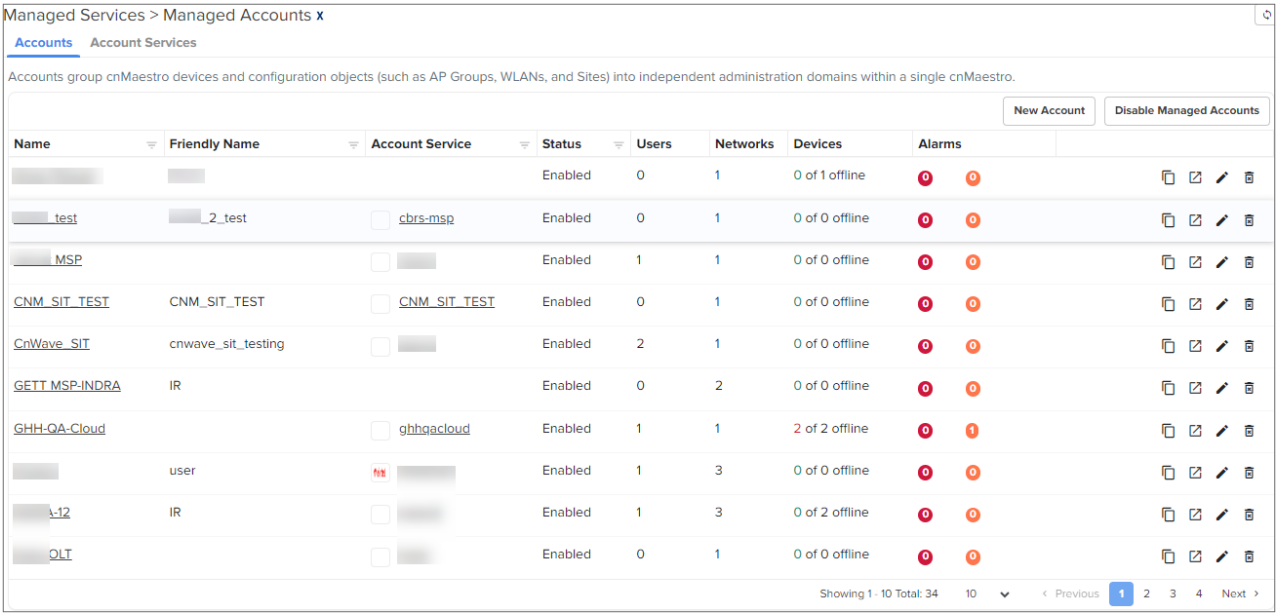
Note

Account Services provide independent administration domains for Devices, WLANs, Sites, and AP Groups. They organize large deployments and form the basis for multi-tenanted Account Services.

Additions in the cnMaestro UI when Managed Accounts is Enabled

- Once Managed Accounts is enabled, **Accounts** and **Account Services** tabs appear in the cnMaestro UI.

  Figure 471 *Accounts and Account Services tabs*



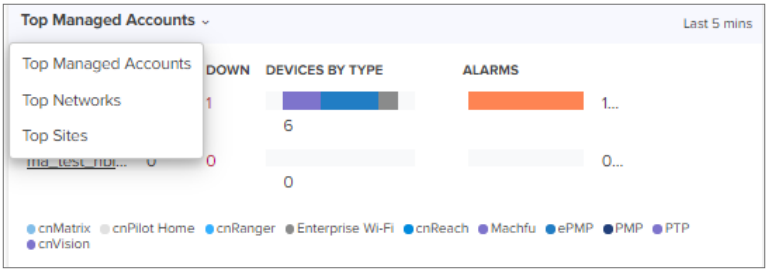
- The Header adds a select box that allows the Global Administrator to enter the context of Account selected.

  Figure 472 *Managed Accounts Component in Header*



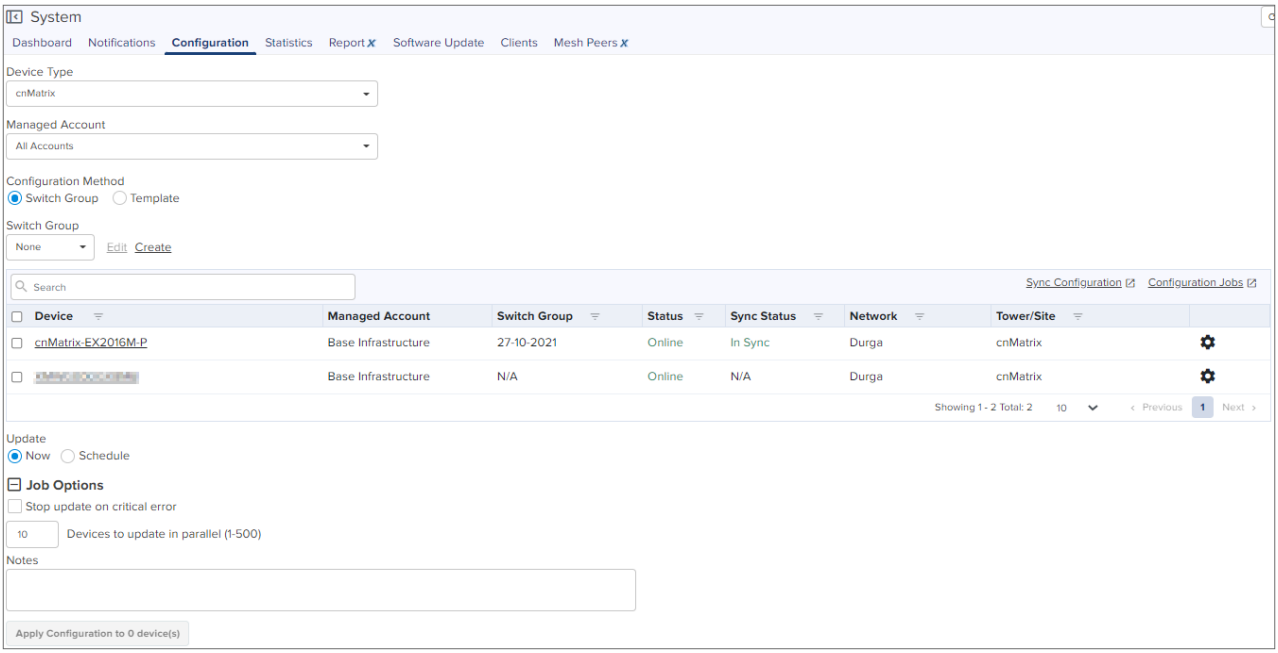
- The System Dashboard adds a Health component for Top Managed Accounts.

Figure 473 *Dashboard > Top Managed Accounts*



- Global tabs in the UI are updated with a Managed Account column.

Figure 474 *Managed Account Column*



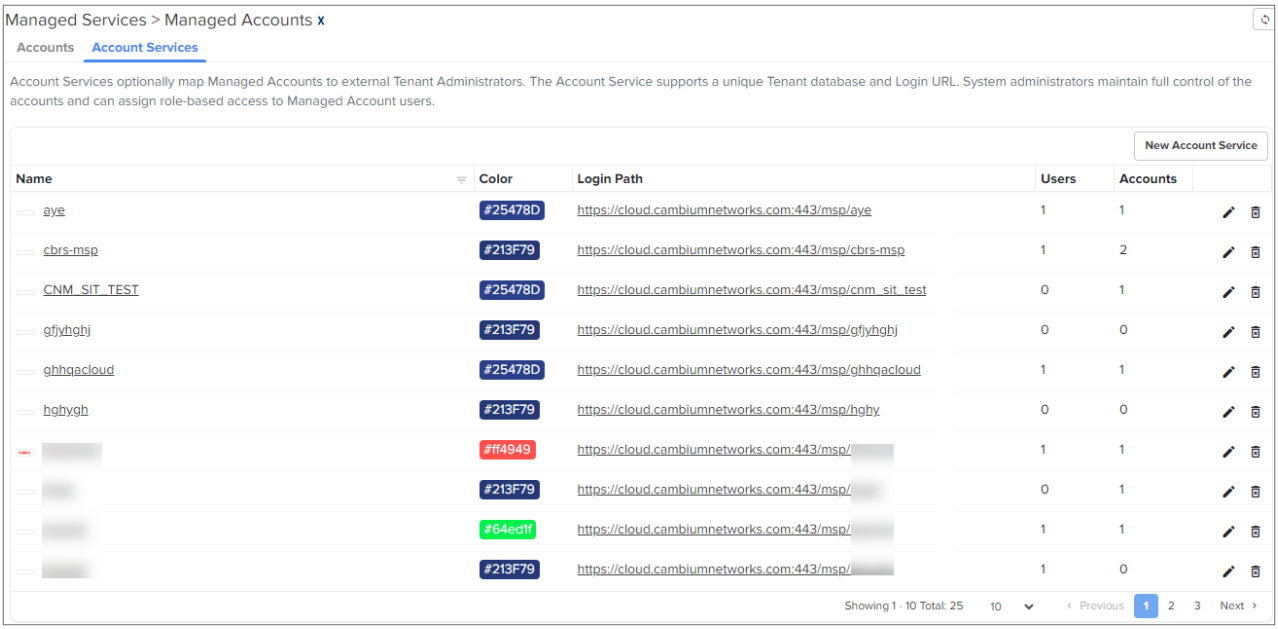
Creating Managed Account Services

The user can create an Account Service and map it to an Account. The Account Service supports an independent user database and a customized user interface. There is a default Account Service, so creating a new one is optional.

To create an Account Service:

1. Navigate to **Managed Services** > **Managed Accounts** > **Account Services** tab.

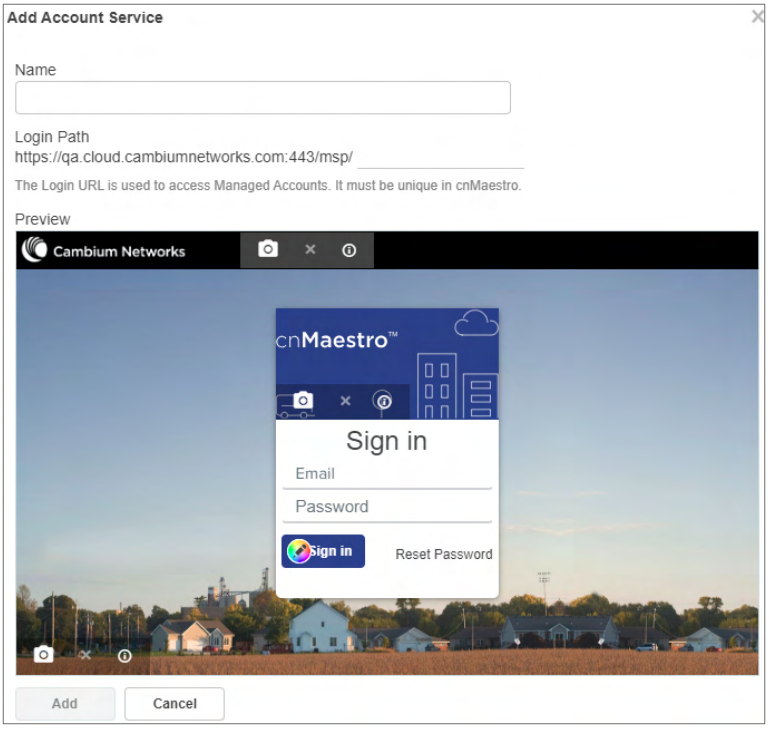
   Account Services Tab



2. Click **New Account Service.**

   The **Add Account Service** window is displayed.

   Add Account Service Window



3. Enter the following details:

Table 105 *Parameters in the Add Account Service Window*

Parameter	Description
Name	Name of the service. This name is visible to Account Administrators.

Table 105 *Parameters in the Add Account Service Window*

Parameter	Description
	A maximum of 64 characters are supported for the name.
Login Path	Account Administrators log into cnMaestro using a standard URL with an additional Path that defines the Account Service. For example, https://<cnmaestro cloud URL>/msp/<branded_service_path> **Note** • The Path name must be unique across all Account Service accounts hosted of Cambium Cloud. • A maximum of 16 characters are supported for the path name.

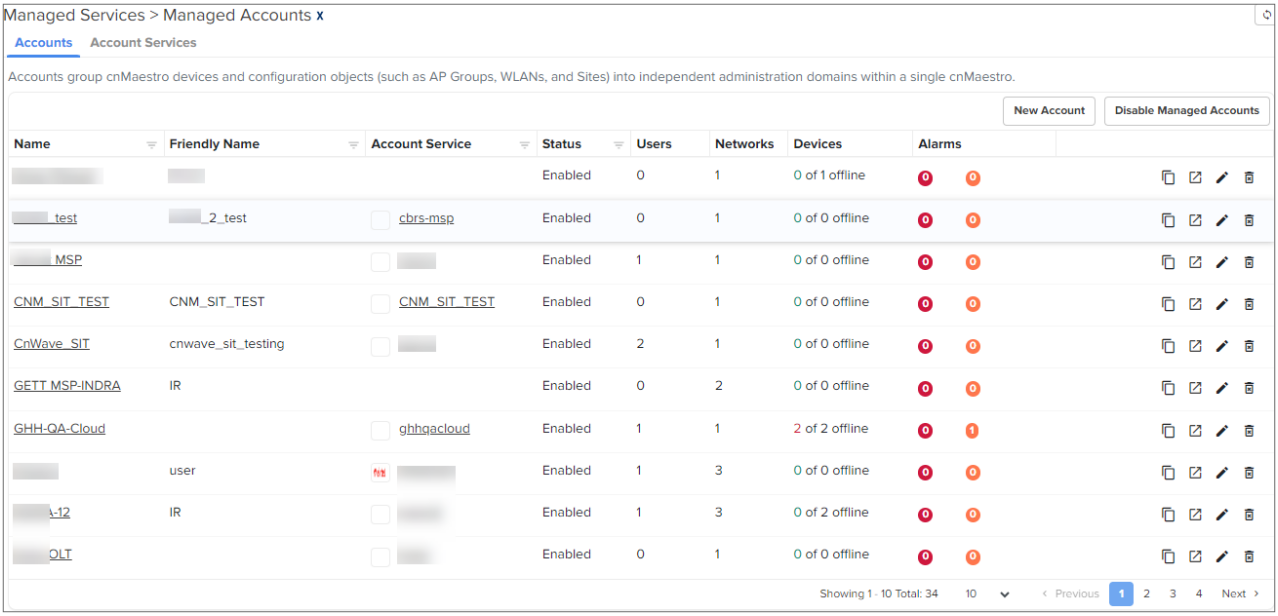
4. Click **Add**.

Creating Account

To create an Account:

1. Navigate to **Managed Accounts** > **Accounts** tab.

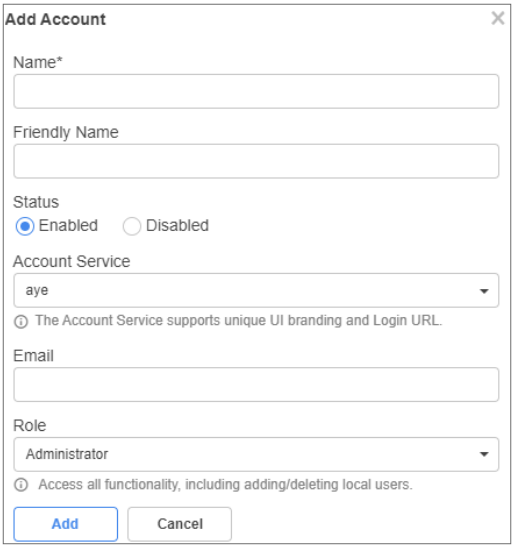
   Figure 475 *Accounts Tab*



2. Click **New Account**.

   The **Add Account** window is displayed.

Figure 476 *Add Account window*



3. Enter the following details:

Table 106 *Parameters in the Add Account Window*

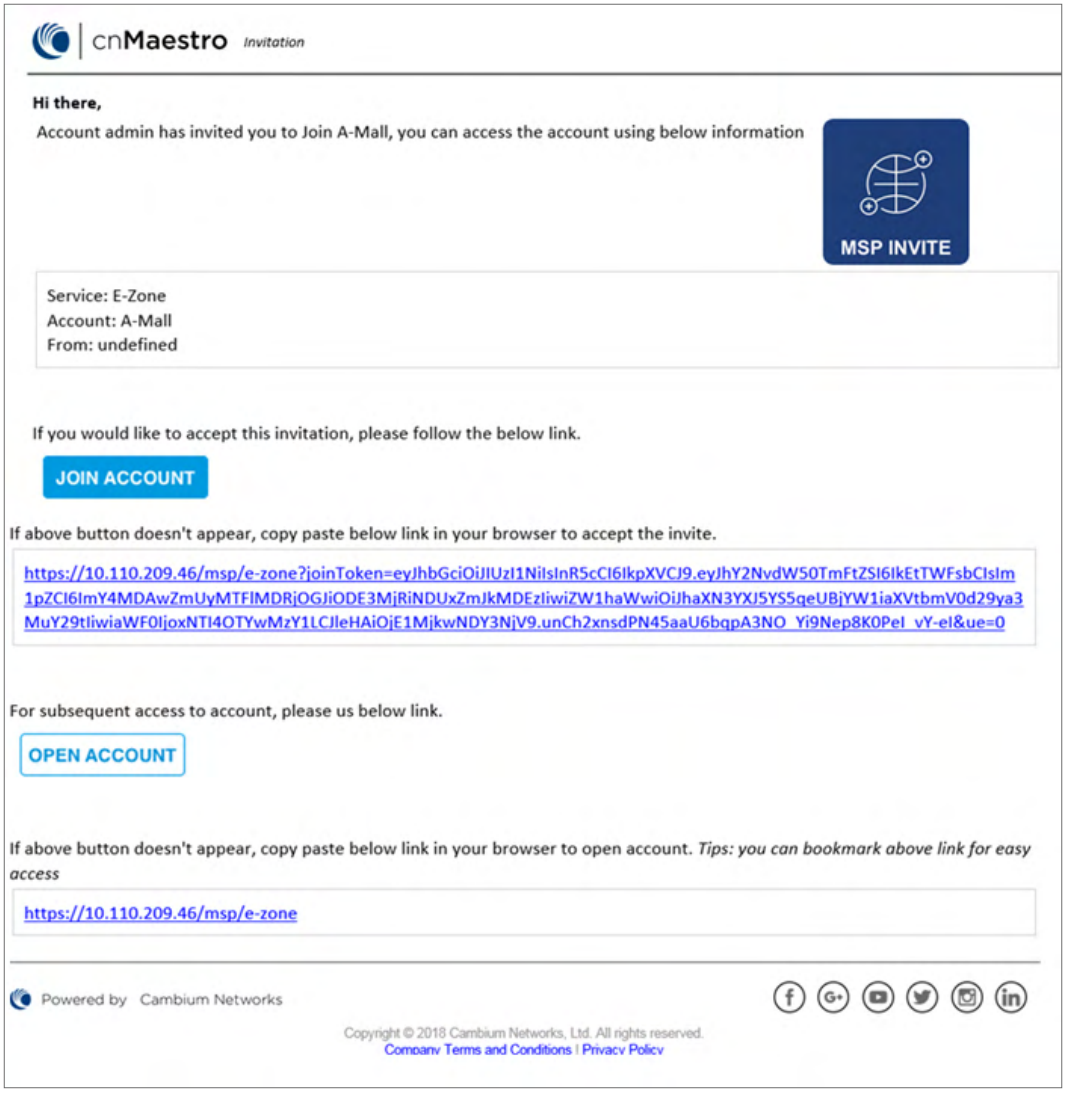
Parameter	Description
Name	Name of the Account. This is sent in the invitation email when users are invited to the account.
Friendly Name	The Friendly Name will be sent in the invitation email.
Status	Determines whether the account is enabled or disabled. When an account is disabled, all Account Users (users) are logged out.
Account Service	The Account Service used for branding and authentication.
Email	The email address of the first Account User. You can add more users after the account has been created.

4. Click **Add**.

Validating Account Users

Once an Account is created, the Account User is sent an email invitation. The email provides directions on how to access the Account UI and set their password.

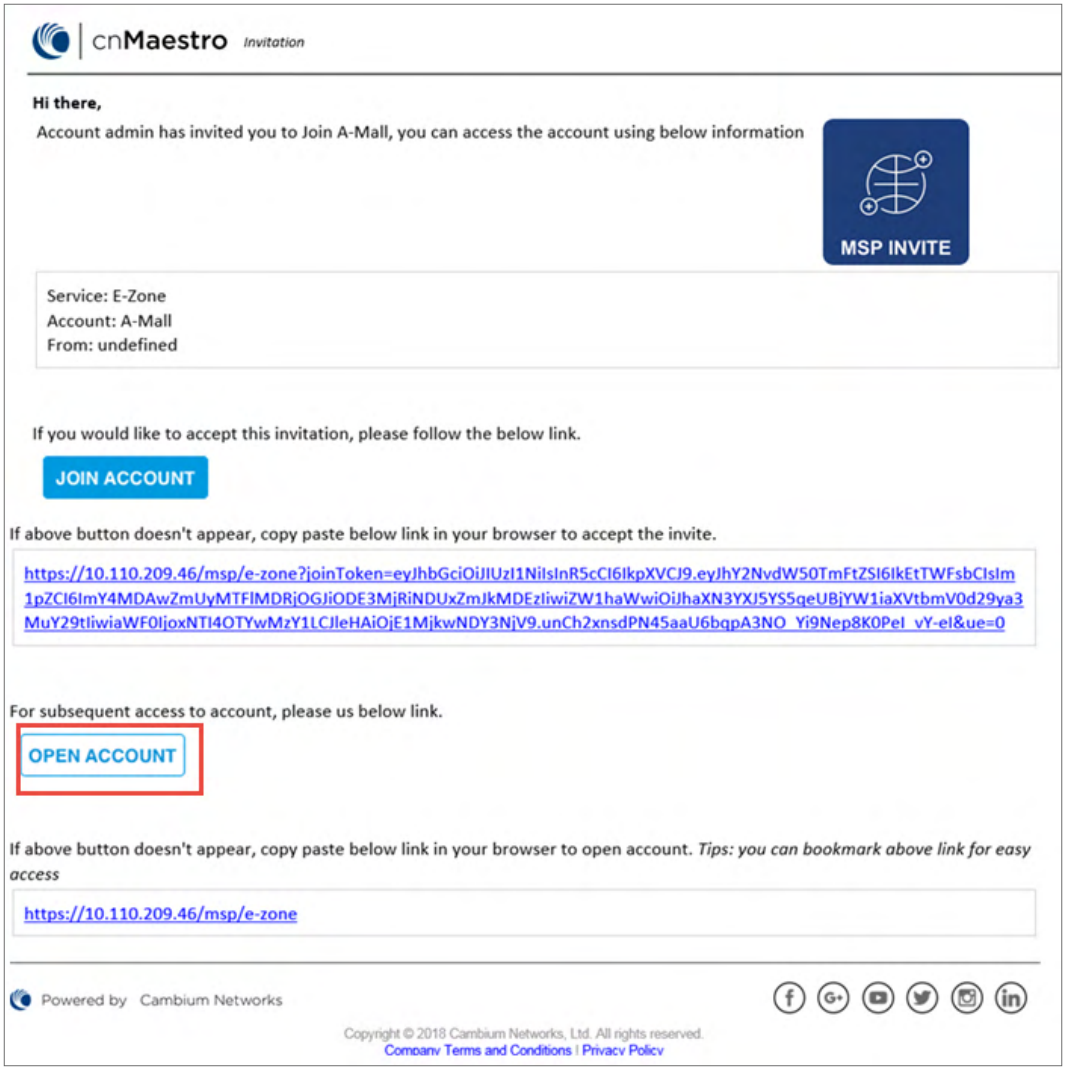
Figure 477 *Sample Email Invitation*



Check Email for Invite

An email is sent inviting the Account User to view their new Managed Account. It has a link that must be clicked to enable access.

Figure 478 *Checking Account Administrator User Email*



Create Account in Account Service

Clicking the link prompts the user to create a new Account or use an existing Account.

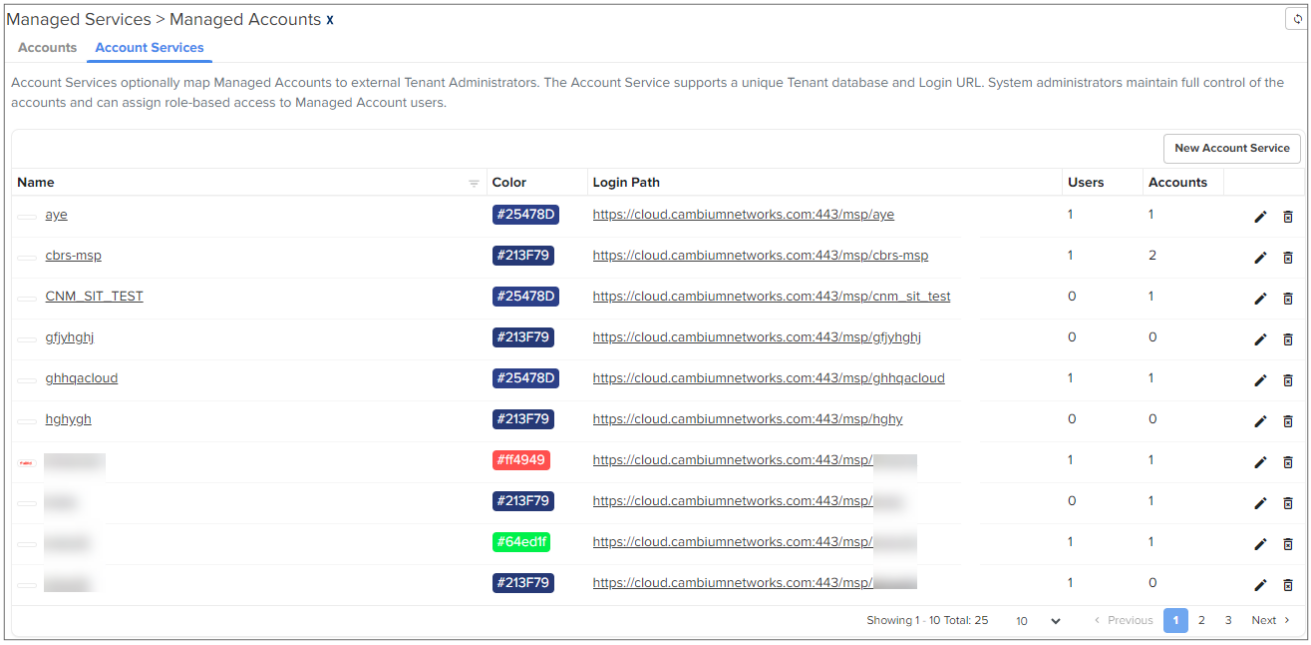
Note

If a user already has an Account in the Account Service, they can use their existing email login to accept the invite for the new Account. In the global cnMaestro UI, switching between accounts is accomplished using the choice box in the UI header (upper right).

Login to the Accounts UI

Once the Account Administrator (User) is created, use the URL listed in the **Login Path** column to login.

Figure 479 *A Sample Login URL*



Managed Account Administration

Overview

Once Managed Accounts are enabled, there are three ways to administrator the Accounts.

- System View
- Account View
- Account Administrator (User) View

Important Points to Remember

Please note the following points for Account Services administration:

Note

- When a device is moved from one Account to other, it goes offline for one minute before appearing online. Only active alarms are moved to the new account and other data is retained in the old account.
- The Managed Accounts feature can be disabled only if all devices in Accounts are deleted or moved to Base Infrastructure account.
- Administrators of Accounts do not have access to the settings page of the server to change the account type.
- When Global Super Administrators trigger Configure/Software/Reports Jobs, the Account users cannot view them.
- When Account Users trigger Configure/Software/Reports Jobs, they are reflected under the Global Super Administrator view along with respective Job IDs enrolled in the respective Accounts.
- The devices that have not started Software/Configure Jobs cannot be moved across Accounts.
- The Global Super Administrator and the Account Administrator cannot trigger a Software or

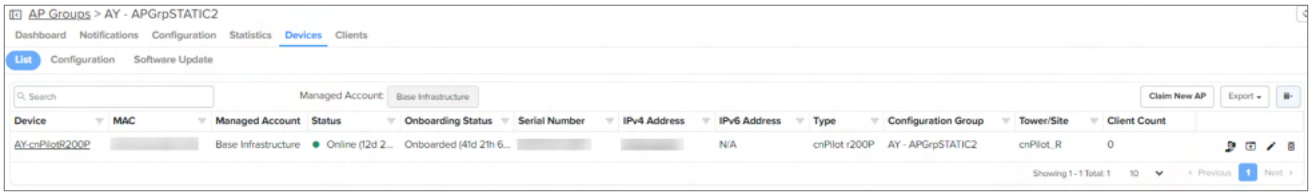
Configure Job simultaneously on the same device.

- The Lock AP configuration can be enabled only by the Global Super Administrator. But whenever a device configuration is changed outside of cnMaestro by either a Global Super Administrator or an Accounts Administrator, the Auto Synchronization Job starts automatically with the configuration job ID as in Accounts and reflects in both the Global Super Administrator and Accounts Administrator accounts.

System View

At the System level, one can view APs, AP Groups, or Sites across all Managed Accounts in a single, unified table. This allows one to review the status of all accounts in context to each another. The following figure displays the AP table, and specifies which APs are mapped to Accounts.

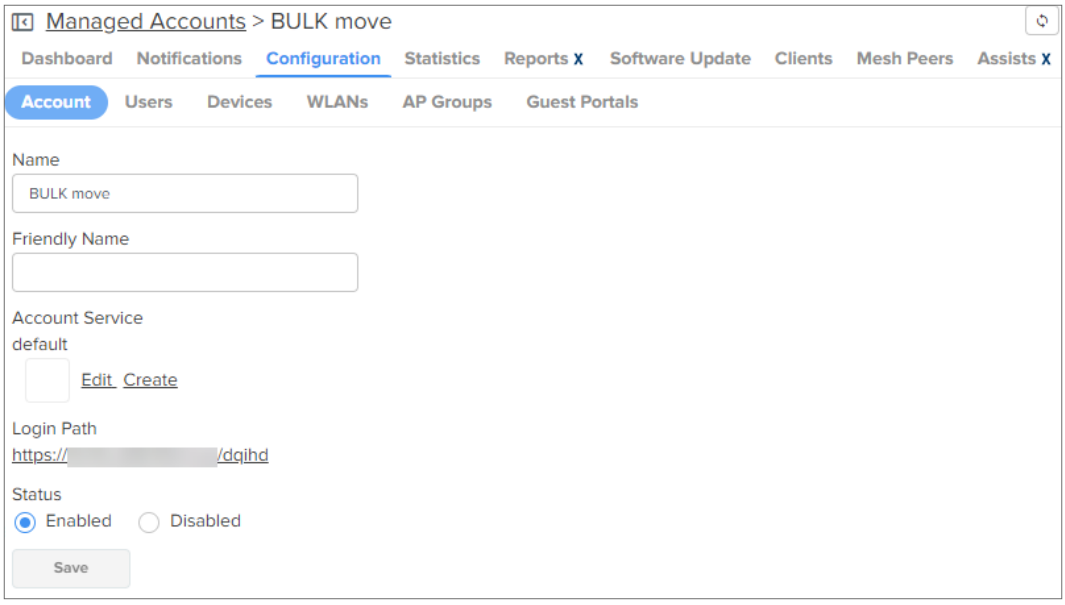
Figure 480 *System View*



Account View

The **Managed Accounts** > **Accounts** page allows you to select individual Accounts, which launches the Account View. This provides full status and configuration for all components of the Account, including Dashboard, Notifications, Configuration, Software Update, Reports, Clients, etc.

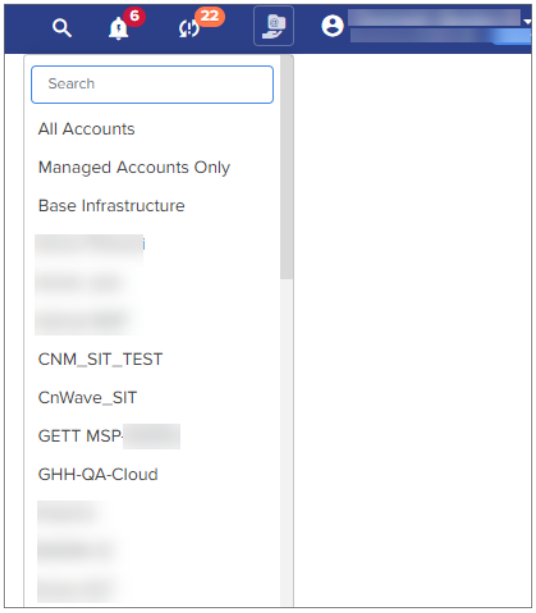
Figure 481 *Account View*



Account Administrator (User) View

The Account Administrator View presents the branded Account UI, without having to explicitly log into it. It is accessed through the Account drop-down in the UI header. Selecting a specific Account (rather than **All**) updates the UI to the Account Administrator's view. From here, the Global Administrator can update the configuration and monitor issues.

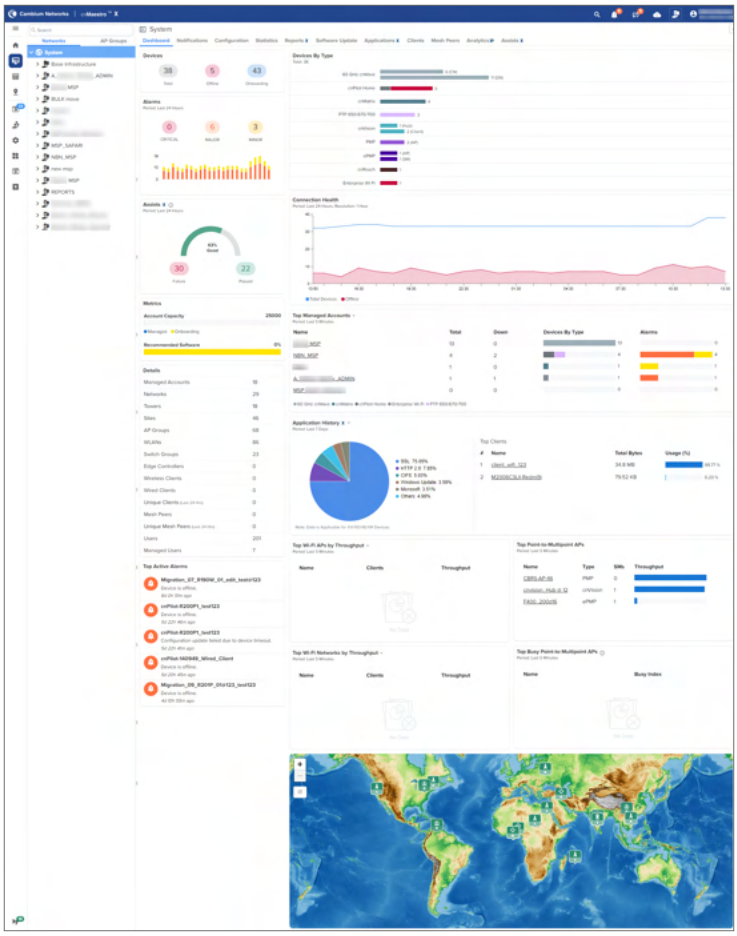
Figure 482 *Managed Account Administrator (User) View*



System Dashboard

The System Dashboard integrates Accounts into the global health component. It ranks the top Accounts based upon device count.

Figure 483 *System Dashboard*



Account Administration

AP Groups, WLANs, and Switch Groups have three types of accessibility scope as shown below:

Table 107 *Types of Scope*

State	Description
Base Infrastructure	The object is only available for the global account.
Managed Account	The object belongs to a Managed Account.
Shared	The object is shared among all Managed Accounts. It can be mapped to devices in the Account, but it cannot be modified. To change the configuration, it needs to be copied into the Account and then updated.

Note

Once the scope has been configured on an object, it cannot be changed.

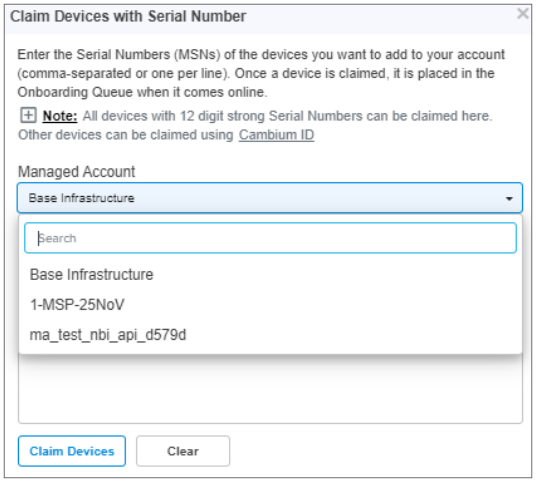
Device Management

Devices are added at the global System level or within Managed Accounts. Devices added at the System level can be moved into Accounts at a later time.

System Onboarding

Onboarding at the global System level supports both MSN and Cambium ID. In the example below, a Management Account can be selected for all devices onboarded in the MSN batch.

Figure 484 *System Onboarding*



Device Onboarding

Onboarding devices through the Managed Account UI automatically places the devices in the Account.

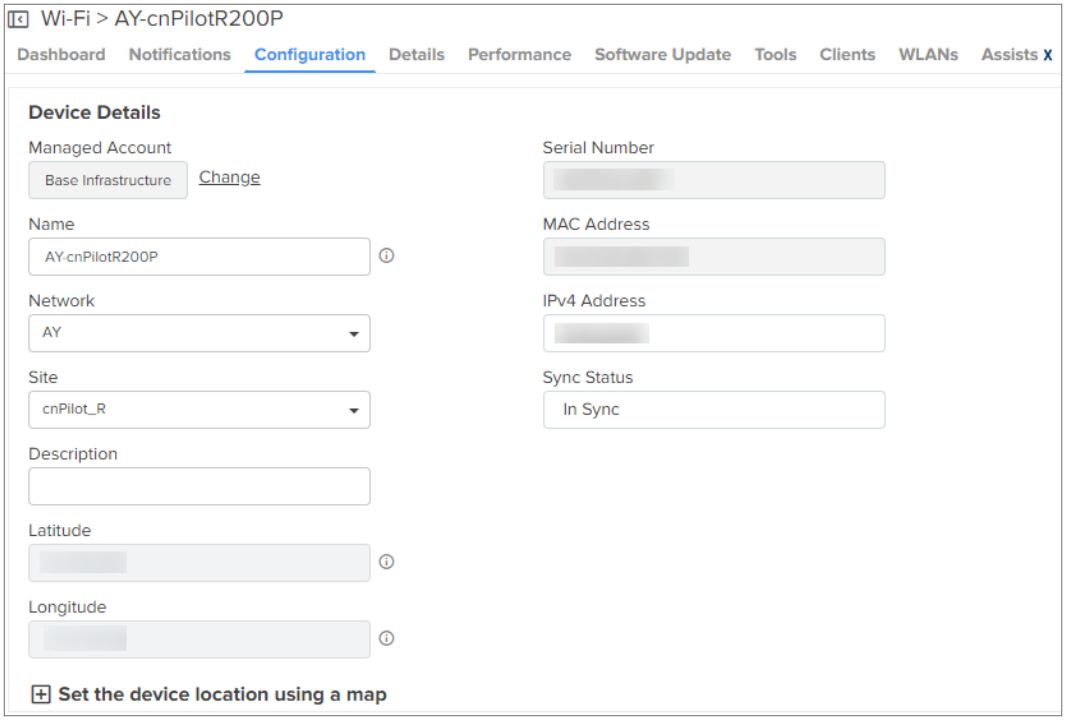
Note

cnMaestro supports onboarding through either MSN or Cambium ID. Within Accounts, only MSN onboarding is supported.

Moving a Device Between Accounts

You can move a device from one Managed Account to another by using the **Change** option in the device configuration page.

Figure 485 *Moving a Device Between Accounts*



In Enterprise view, the device can be moved between Accounts using the **Managed Account** ( ) icon in the **AP Groups** > *<AP-group-name>* > **Devices** > **List** tab.

Figure 486 *Moving a device between Accounts in Enterprise View*



Account Deletion

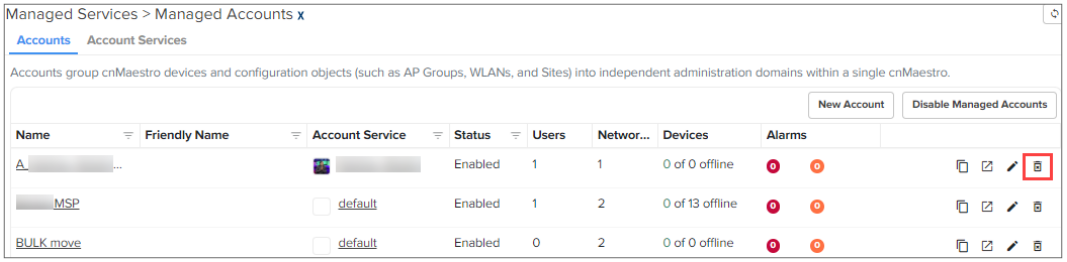


Note

All devices must be removed from the Account before deleting the account.

To delete a Managed Account, navigate to the **Account Services** page and click the delete icon.

Figure 487 *Account Deletion*



Disabling the Managed Accounts feature

The Managed Accounts feature can be disabled within the system only after all the devices are deleted or moved to the Global context. By disabling Account Services, the Account field will be disabled across all the tables, such as Clients, Notifications, Inventory.

Managing subscribers (end-customer)

To enable a subscriber to manage the router using the Android or iOS application, you must add a subscriber profile in cnMaestro and send an invitation to the subscriber.

This pocess involves the following actions:

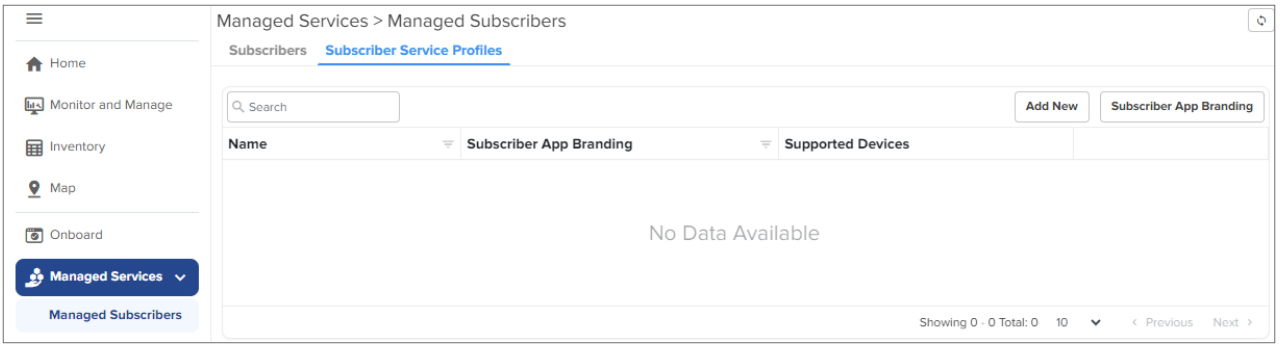
1. Adding a Subscriber Service Profile
2. Adding a subscriber
   a. Modifying the owner details for the Subscriber App
3. Claiming the Home Mesh Router

Adding a Subscriber Service Profile

To add a subscriber service profile, complete the following steps:

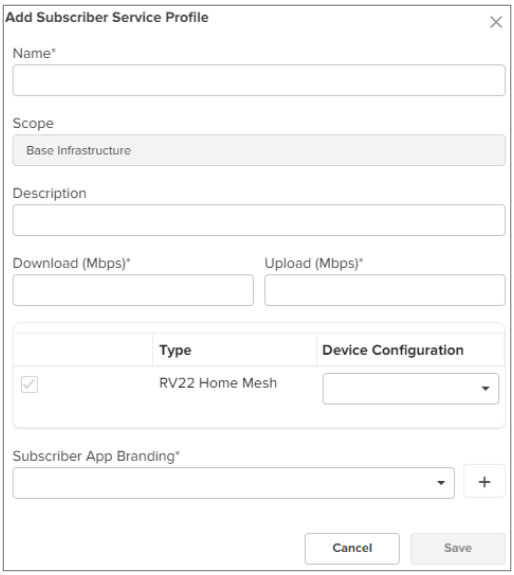
1. Navigate to the **Manage Services** > **Managed Subscribers** > **Subscriber Service Profiles** tab.

   The **Subscriber Service Profiles** page appears.



2. Click **Add New**.

   The **Add Subscriber Service Profile** window appears.



3. Select the Home Mesh Router configuration to which you want to associate with the subscriber service profile and configure the parameters as described in Table 108.

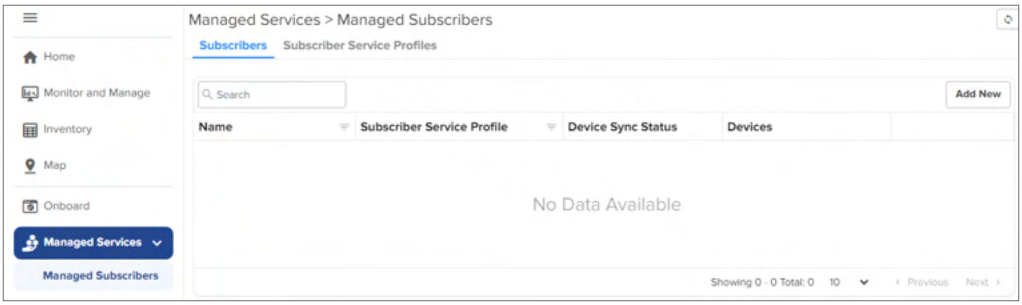
Table 108 *Subscriber Service Profile parameters*

Parameter	Description
Name	Name of the subscriber service profile.
Description	Brief description for the subscriber service profile.
Download (Mbps)	Download speed (in Mbps) configured for the profile.
Upload (Mbps)	Upload speed (in Mbps) configured for the profile.
Type	Displays the device type as **RV22 Home Mesh**. This field cannot be modified.
Device Configuration	Specifies the Wi-Fi AP group (created for the Home Mesh Router device type) that must be associated with the service profile. Select the group from the drop-down list.
Subscriber App Branding	Specifies the cnMaestro Subscriber application branding that must be used in this profile. All routers sent to subscribers in this service profile contain the selected branding logo and information. Select the required branding from the drop-down list. If no branding is present, create one by clicking the add (+) icon. See cnMaestro Subscriber application branding for more information.

4. Click **Save**.

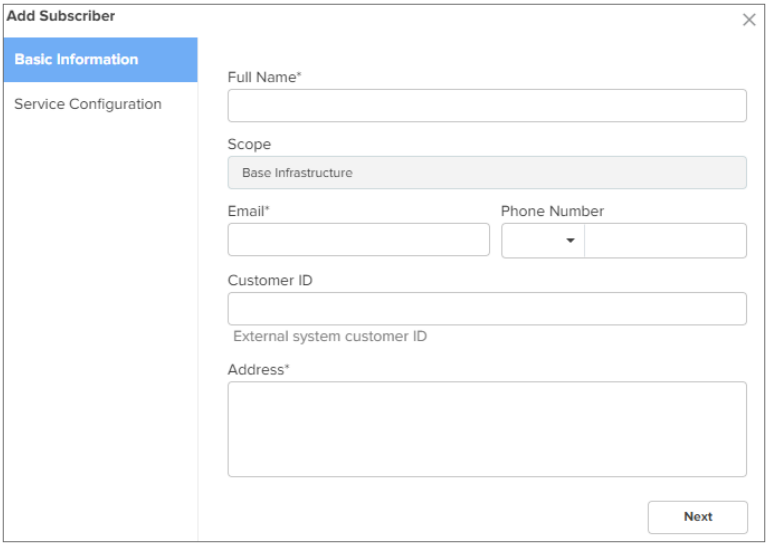
Adding a subscriber

5. Click the **Subscribers** tab on the **Managed Subscribers** page.



6. Click **Add New**.

   The **Add Subscriber** window appears.



7. In the **Add Subscriber** window, configure the details of the subscriber in the **Basic Information** section, as described in Table 109.

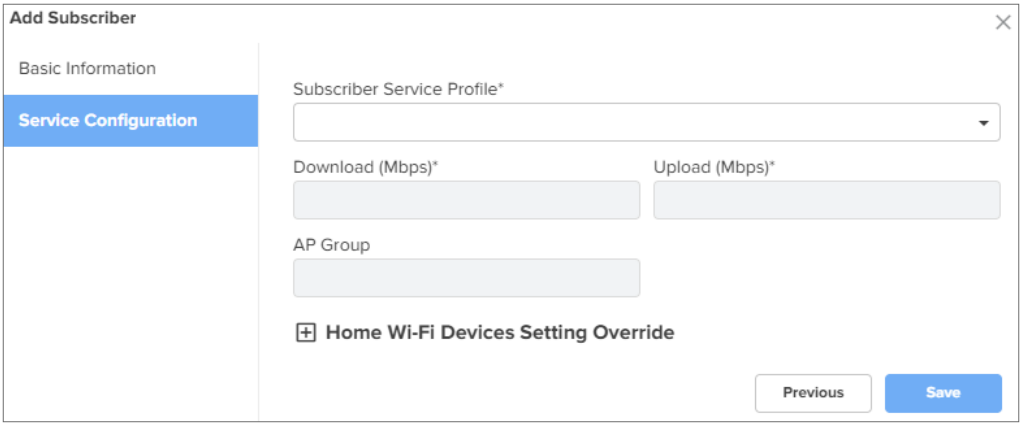
   Table 109 *Subscriber > Basic tab parameters*

Parameter	Description
Full Name	Name of the subscriber.
Email ID	Email address of the subscriber. This email address receives the invitation to join the Home Mesh Router (RV22) site. Through this email address the user will be able to access and manage the router as a primary user and invite other users (secondary users), through the mobile application, to manage the routers. **Note** You can edit this email address at anytime. However, editing this email address will remove all existing users, both primary and secondary. For information about how to modify the email ID, refer to Modifying the owner details for the Subscriber App.

Parameter	Description
Phone Number	Phone number of the subscriber.
Customer ID	Unique ID for the subscriber.
Address	Address of the subscriber where the routers will be installed.

8. Click **Next**.

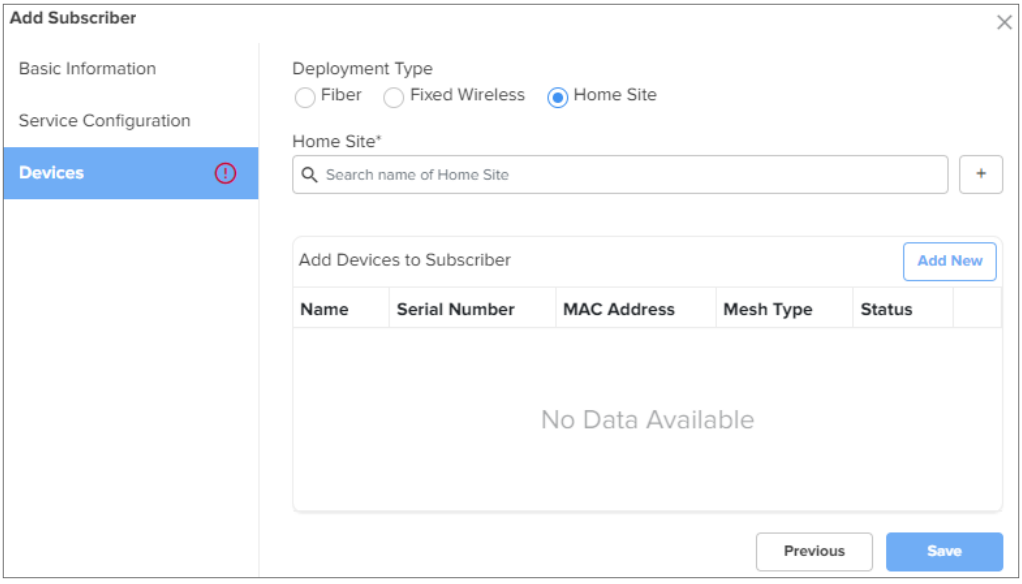
   The **Service Configuration** tab is displayed.



9. Select the subscriber service profile to be associated with this subscriber from the **Service Profile** drop-down list.
10. Click **Save**.

    A new tab, **Devices** appears, where you can link (or claim) the Home Mesh Router to the subscriber. See Claiming the Home Mesh Router.

    The cnMaestro Subscriber application invitation email is sent to the subscriber with the link to join the account.
11. Click **Devices**.



12. Select one of the following options in the **Deployment Type** field to filter the available deployment types:

- **Fiber**—Select the Optical Network Unit (ONU) device that you want to associate with the subscriber's router by searching in the **ONU** search box.
- **Fixed Wireless**—Select the Subscriber Module (SM) device that you want to associate with the subscriber's router by searching in the **SM** search box.
- **Home Site**—Select the home site you want to associate with the subscriber's router by searching in the **Home Site** search box. To add a home site, see Adding a Home Site.

13. Before linking the Home Mesh Router to the subscriber, click **Save**.

Modifying the owner details for the Subscriber App

You can modify the owner details for the Subscriber App by modifying the email ID.

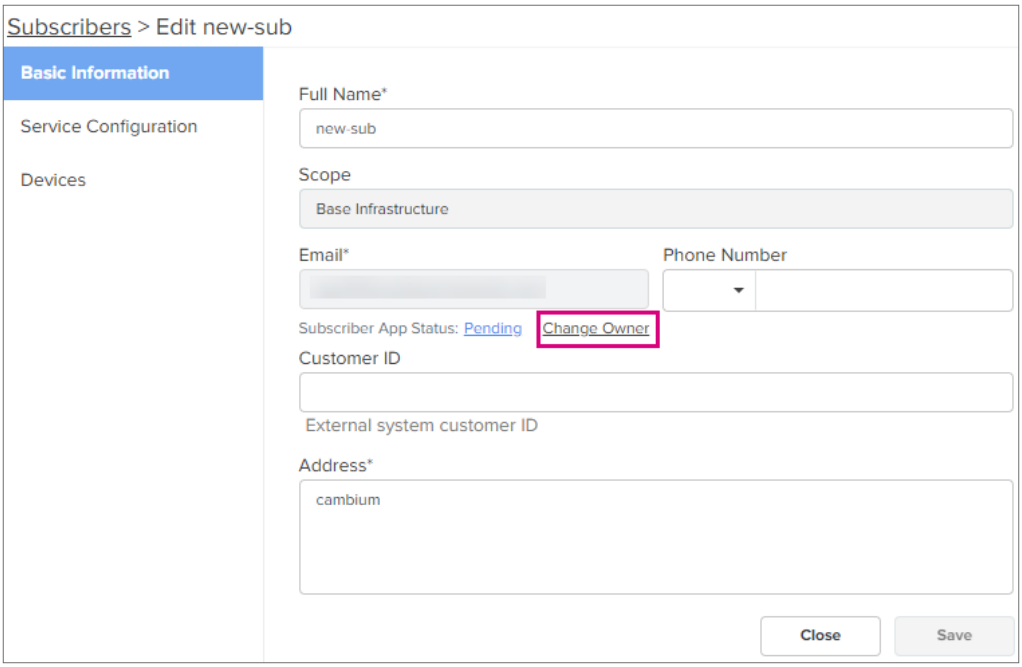
Warning

Modifying the email address will remove all existing users, both primary and secondary.

To modify the email address, complete the following steps:

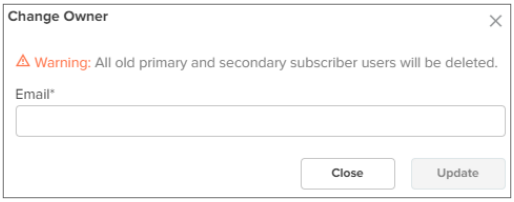
1. Navigate to the **Manage Services** > **Managed Subscribers** > **Subscribers** tab.
2. In the list of subscribers, click the subscriber name for which you want to modify the email ID.

   The corresponding subscriber details are displayed.



3. Under the **Email** parameter, click **Change Owner**.

   The Change Owner window is displayed.



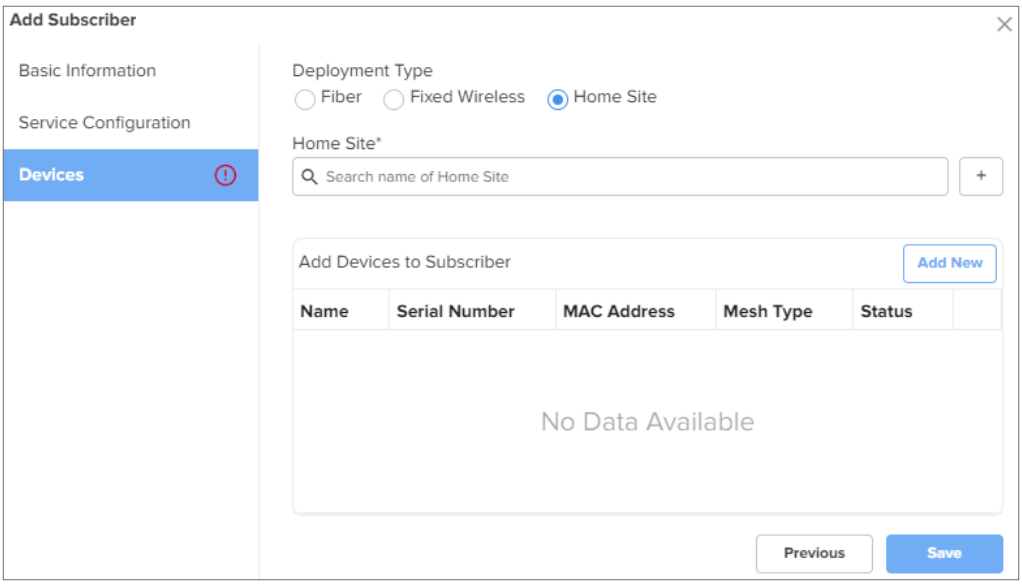
4. Enter the new email ID for the subscriber.
5. Click **Update**.

Claiming the Home Mesh Router

After adding a subscriber profile and a subscriber, you must now associate the Home Mesh Router to the subscriber by claiming the router in cnMaestro.

To claim the router, complete the following steps:

1. Navigate to the **Manage Services** > **Managed Subscribers** > **Subscribers** tab.
2. In the list of subscribers, select the subscriber name for which you want to associate the Home Mesh Router.
3. Click the **Devices** tab.
4. In the **Add Devices to Subscriber** section, click **Add New**.

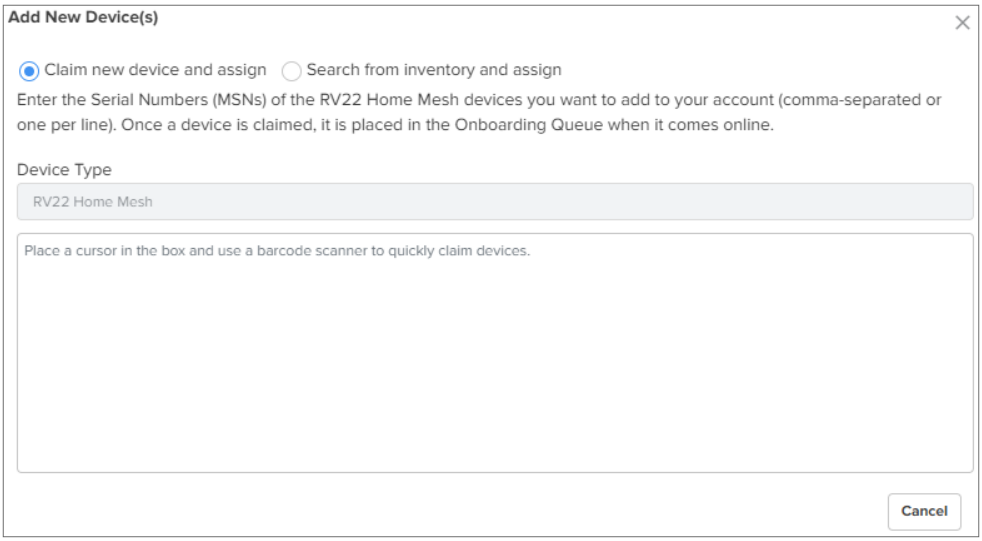


The **Link Subscriber** window appears.

5. In the **Link Subscriber** window, link the Home Mesh Router to the subscriber by using any of the following methods:

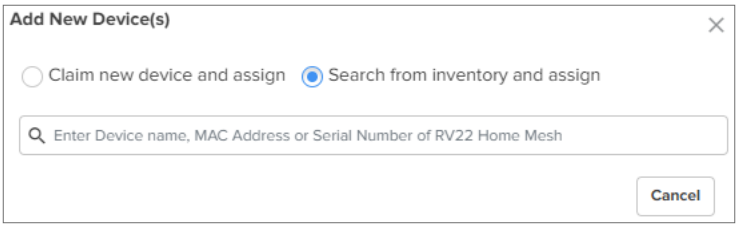
   - To claim a new router that is not onboarded to cnMaestro, select the **Claim new and assign** option and enter the serial number of the device to be claimed.

     You can claim multiple routers by adding multiple serial numbers separated by commas.



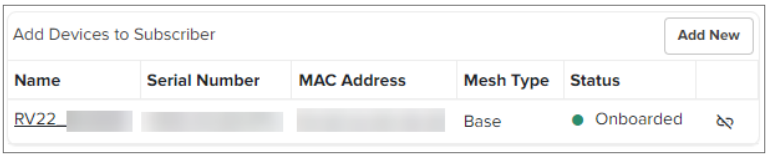
- To claim a router that is already onboarded to cnMaestro, select the **Search for inventory and assign** option.

  Enter the details of the router you want to claim.



6. Click **Assign**.

   The assigned router appears in the **Add Devices to Subscriber** section.



Note

Click the unlink ( ) icon to unlink the router from the subscriber.

Network Services

This section includes the following topics:

- API Client
- RESTful API
- Guest Access
- EasyPass
- RADIUS Proxy
- CBRS
- Organization
- LTE
- Managing Edge Controller
- cnArcher Summary
- Spectrum Analyzer

API Client

Overview

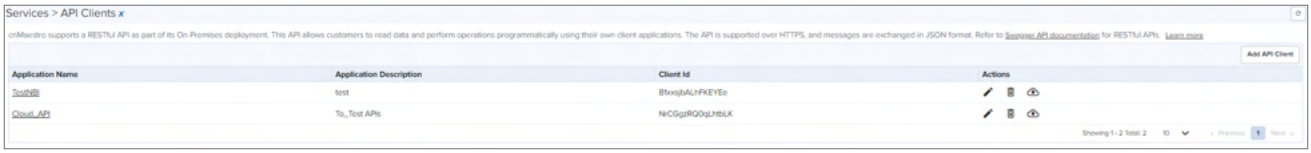
The cnMaestro RESTful API allows customers to manage their deployment programmatically using their own client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Modern programming languages have rich support for RESTful interfaces.

Note

cnMaestro currently provides monitoring data over the API (such as inventory, statistics, events, and alarms).

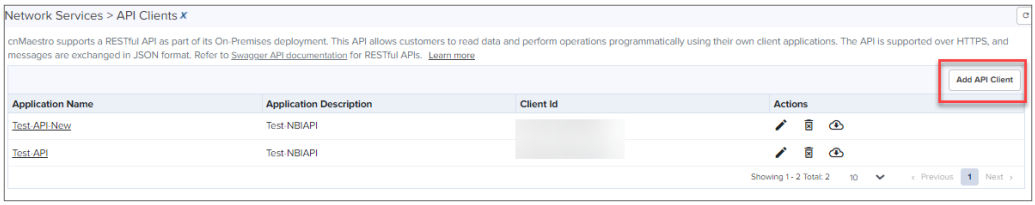
API Clients

API Clients are external applications that access the RESTful API over HTTPS using OAuth 2.0 Authentication. They require a Client ID and Client Secret for access, both of which are detailed later in this chapter. For more information, refer to RESTful API Specification.

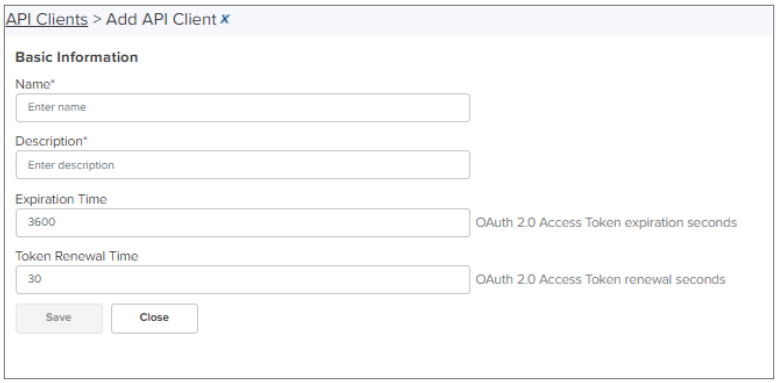


To add **API Client**:

1. Navigate to **Network Services > API Clients**.

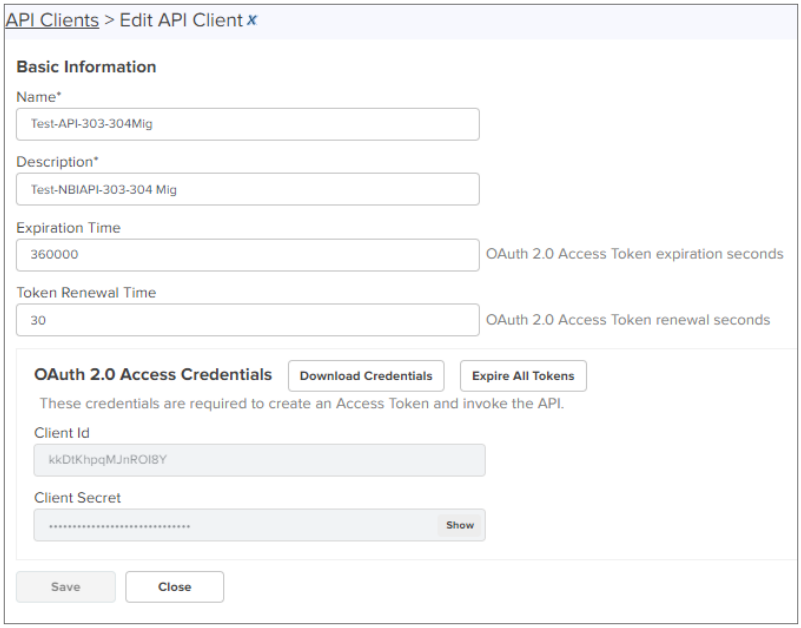


2. Click **Add API Client**.



3. Enter **Name**.
4. Enter **Description**.
5. Enter **Expiration Time**.
6. Enter **Token Renewal Time**.
7. Click **Save**.

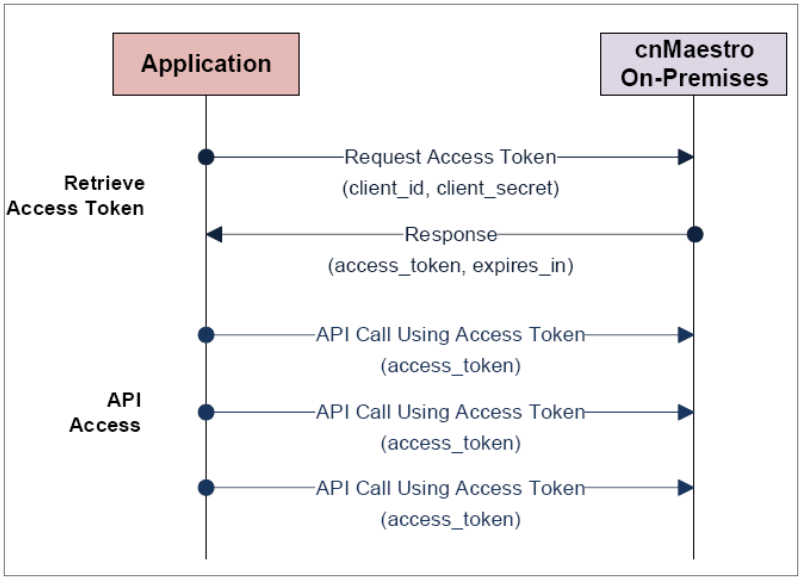
Once the API Clients is added you can able to view or download credentials shown in the **OAuth 2.0 Access Credentials.**



RESTful API Specification

Authentication

API Authentication uses OAuth2. The client retrieves an Access Token to start the session. It then sends API requests until the Access Token times out, at which point the token can be regenerated.



Establish a Session

A session is created by sending the Client ID and Client Secret to the cnMaestro server. These are generated in the cnMaestro UI and stored within the application. The Client ID defines the cnMaestro account and application, and the Client Secret is a private string mapped to the specific application. The Client Secret should be stored securely.

If the session is established successfully, an Access Token is returned along with an expiration string. The Access Token is used to authenticate the session. The expiration is the interval, in seconds, in which the Access Token remains valid. If the Access Token expires, a new session needs to be created.

API Access

The application sends the Access Token, in every API call. The token is sent in an Authentication header. Details are provided later in this document.

Session Expiration

If a token expires, an expiration error message is returned to the client. The client can then generate a new token using the Client ID and Client Secret. The token expires immediately if the Client API account is deleted. The default expiration time for a token is 3600 seconds (1 hour). The session expiration is configurable in the UI.

Rate Limiter

The Rate Limiter API request helps in improving the availability of API based services by avoiding resource starvation.

This API calculates the rate limit per customer based on various factors such as system configuration, number of devices onboarded, Network, Towers, Sites, etc.

The API limits the number of NBI API calls to a single cnMaestro account per minute. Once the limit is reached, the API receives a standard HTTP Response Status code such as 429 or 503.

HTTP Response Status Code	Response Headers	Explanation	Action to be taken
429	RateLimit-Limit: 10	Number of API calls allowed for the cnMaestro account per minute	If the **RateLimit-Remaining** value is 0, then the client application waits for the number of seconds to **Reset-RateLimit** before sending the next subsequent API requests
	RateLimit-Remaining: 0	Number of remaining API calls for the current minute is zero	
	RateLimit-Reset: 35	Number of seconds remaining to reset the rate limit	
503	Retry-After	Number of seconds during which users wait before retrying	If the value of **Retry-After** is greater than 0, then the client application waits for the number of seconds to **Retry-After** before sending the next subsequent API requests

The following table below displays the approximate limit calculated by the system on a 4 vCPU, 8 GB RAM Cloud instance.

Devices	GET	POST/Others
101	10	3
501	24	3
1001	47	5
2001	92	10
4001	163	17

Example of a Python client:

```
import sys
import requests
import json
import base64
import time

HOST = # host here
CLIENT_ID = # client id here
CLIENT_SECRET = # client secret here
TOKEN_URL = # token url here

# Retrieve access parameters (url, access_token, and expires_in).
def get_access_parameters(token_url, client_id, client_secret):
    """
    Authenticates to API.
    Parameters:
        `token_url` - Endpoint to authenticate to\n
        `client_id` - Auth client id\n
        `client_secret` - Auth client secret\n
    Returns:
        `(access_token, expiry)`
    """
    data = "%s:%s" % (client_id, client_secret)
    encoded_credentials = base64.b64encode(data.encode('ascii')).decode('ascii')
    headers = {
      "Authorization":"Basic %s" % encoded_credentials,
      "Content-Type":"application/x-www-form-urlencoded"
    }
    body = "grant_type=client_credentials"
    r = requests.post(token_url, body, headers=headers, verify=False)
    print ("Status Code: %s" % r.status_code)
    return r.json()['access_token'], r.json()['expires_in']

def call_api(method, host, path, access_token):
    """
```

```
    Makes HTTP call to an API with given method.
    Parameters:
        `method` -
 method for the new Request object: GET, OPTIONS, HEAD, POST, PUT, PATCH, or DELE
TE\n
        `host` - host for the url\n
        `path` - path for the url\n
        `access_token` - a valid access token for header
    Returns:
        `(response_status_code, headers, body)`
    """
    api_url = "https://%s%s" % (host, path)
    headers = {
      "Authorization":"Bearer %s" % access_token,
    }
    response = requests.request(method=method, url=api_
url, headers=headers, verify=False)
    headers = response.headers
    body = response.json()
    response_status_code = int(response.status_code)
    return response_status_code, headers, body


def main():


    try:
        # Getting the access token using client id and client secret
        access_token, expires_in = get_access_parameters(TOKEN_URL, CLIENT_
ID, CLIENT_SECRET)


        # For the purpose of the example, let's send 100 requests back to back
        for i in range(100):
            # Calling the endpoint with GET method
            status_code, header, body = call_api
('GET', HOST, '/api/v2/devices/statistics', access_token)
            # identifying any client or server side error codes
            client_errors = (status_code - status_code%100) == 400
            server_errors = (status_code - status_code%100) == 500
```

```
            # handling error status code
            if client_errors or server_
errors: # check for all 400 and 500 responses
                print("Failure: [%s]-[%s]" %(status_code, (json.dumps
(body, indent=2))))
                # For 429, wait until `RateLimit-Reset` seconds
                if (status_code == 429):
                    sleep_time = 10 # default wait time
                    # try block prevents any dict value exception
                    try:
                        # Reading the header
                        sleep_time = int(header["RateLimit-Reset"])
                    except: pass
                    # if sleep_
time is not greater than 0, defaulting to 10 seconds
                    sleep_time = sleep_time if sleep_time > 0 else 10
                    print("Sleeping for %d seconds" % sleep_time)
                    # sleeping the main thread
                    time.sleep(sleep_time)
                if (status_code == 503):
                    sleep_time = 10 # default wait time
                    # try block prevents any dict value exception
                    try:
                        # Reading the header
                        sleep_time = int(header["Retry-After"])
                    except: pass
                    # if sleep_
time is not greater than 0, defaulting to 10 seconds
                    sleep_time = sleep_time if sleep_time > 0 else 10
                    print("Sleeping for %d seconds" % sleep_time)
                    # sleeping the main thread
                    time.sleep(sleep_time)
            else:
                # process response
                print("Success: [%s]" %(json.dumps(body, indent=2)))

    except Exception as E:
```

```
        print("Failure: [%s]"%E)
        sys.exit()


if __name__ == "__main__":
    main()
```

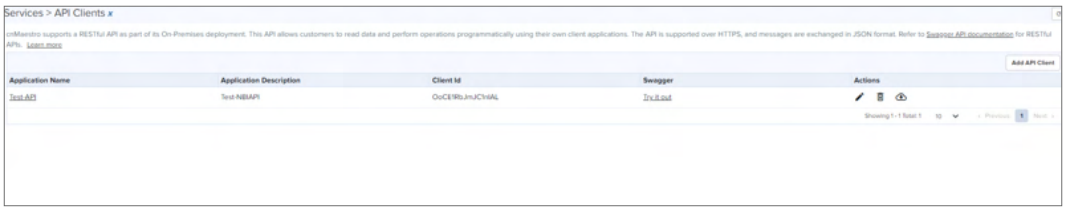
Swagger API

Introduction

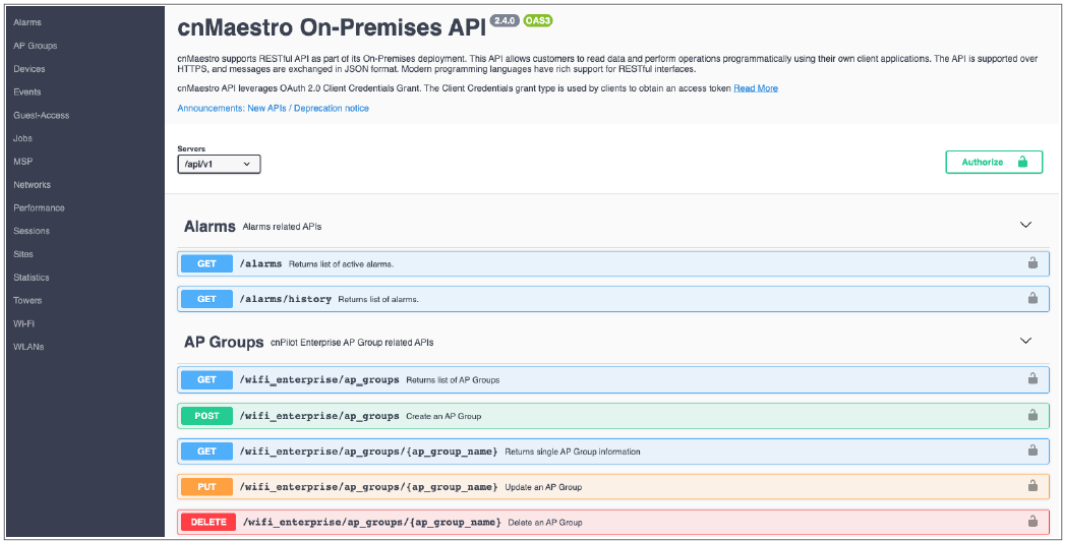
The RESTful API documentation is supported through Swagger, which allows visualization and interaction with the API resources.

To access Swagger, perform the following steps:

1. Navigate to **Services > API Client** grid.
2. Click **Swagger API documentation**.



Sample Swagger UI



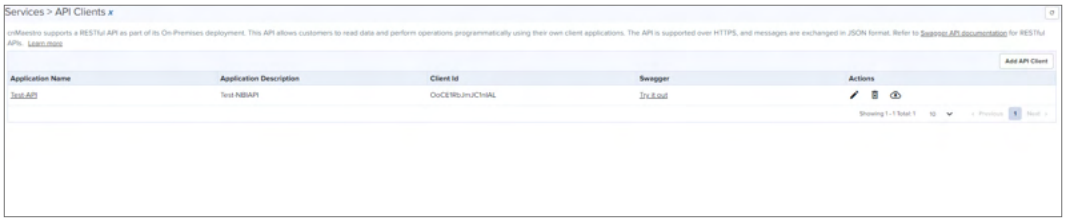
Generating Client ID and Client Secret

cnMaestro User Interface

To create the Client Id and Client Secret in the cnMaestro UI, perform the following steps:

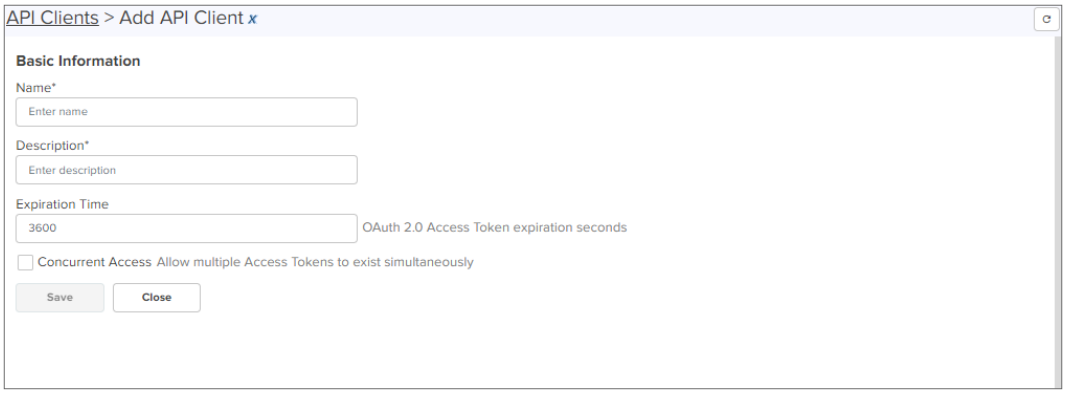
1. Navigate to **Services > API Client**.

   Each client application should be added as an API Client.



2. Click **Add APIClient** to add a client.

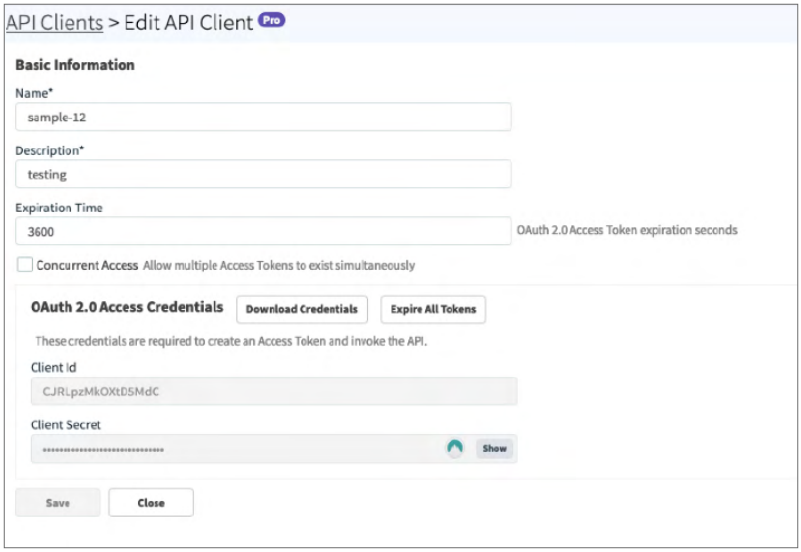
   Add API Client window pops up.



3. Enter **Name** and **Description**.
4. Click **Save**.

Download the Client ID and Client Secret

You can download and store the Client ID and Client Secret by clicking **Download Credentials**. The Client Id is required to create an API session.



API Session

Introduction

The cnMaestro API leverages the Client Credentials section of the OAuth 2.0 Authorization Framework (RFC 6749). An API session can be created using any modern programming language. The examples below highlight how messages are encoded and responses returned.

Retrieve Access Token

Access Token Request (RFC 6749, section 4.4.2)

To generate a session, the client should retrieve an Access Token from cnMaestro. This is done by base64 encoding the **Client_ID** and **Client_Secret** downloaded from the cnMaestro UI and sending them to the cnMaestro server. The **Authorization** header is created by base64 encoding these fields as defined below.



Note

The fields are separated by a colon (:).

```
Authorization: Basic BASE64(<client_id>:<client_password>)
```

In the body of the **POST** the parameter **grant_type** must be set to **client_credentials.**

```
POST /api/v2/access/token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials
```

Alternatively, the credentials can be passed within the body of the **POST** without using the **Authorization** header.

```
POST /api/v2/access/token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&client_id=s6BhdRkqt3&client_secret=7Fjfp0ZBr1KtDRbnfVdmIw
```

Access Token Response (RFC 6749, section 4.4.3)

The response returned from cnMaestro includes the Access_Token that should be used in subsequent requests. The **expires_in field** defines how many seconds the token is valid.

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token":"2YotnFZFEjr1zCsicMWpAA",
  "token_type":"bearer",
  "expires_in":3600
}
```

Sample 200 response body.

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token": "290eeaba71d3f4885405eac2fd18a4f3c300448d",
  "expires_in": 3600,
  "token_type": "bearer",
  "redirect_uri": https://10.110.241.252
}
```

Note

The returned **redirect_uri** should be used to generate the session.

Error Response (RFC 6749, section 5.2)

If there is an error, an HTTP 400 (Bad Request) error code is returned along with one of the following error messages as shown below:

Table 110 *Error Responce*

Message	Details
`invalid_request`	Required parameter is missing from the request.
`invalid_client`	Client authentication failed.
`unauthorized_client`	The client is not authorized to use the grant type sent.
`unsupported_grant_type`	The grant type is not supported.

An example error response is below:

```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
   "error": "invalid_request"
}
```

Access Resources

When the **Access_Token** is retrieved, API requests are sent to cnMaestro server using the format below. The **Access_Token** is sent within the HTTP **Authorization** header.

```
GET /api/v2/devices
Accept: application/json
Authorization: Bearer ACCESS_TOKEN
```

API Details

HTTP Protocol

HTTP Response codes

Table 111 lists the response codes that are supported in cnMaestro and may be returned through the HTTP protocol.

Table 111 *HTTP Response codes returned*

Code	Description	Use in cnMaestro
200	OK	Standard response for successful HTTP requests.
400	Bad Request	Status field in request validation related errors.
401	Unauthorized	User tried to access a resource without authentication.
403	Forbidden	An authenticated user tries to access a non-permitted resource.

Code	Description	Use in cnMaestro
404	Not Found	Server could not locate the requested resource.
405	Method Not Allowed	A method (GET, PUT, POST) is not supported for the resource.
413	Payload Too Large	The request is larger than the server is willing to handle
422	Unprocessable Entity	The server understands the request but cannot process it.
429	Too Many Requests	The client has sent too many requests in a given interval.
431	Request Header Fields Too Large	The header fields are too large to be processed.
500	Internal Server Error	A server-side error happened during processing the request.
501	Not Implemented	The request method is not recognized.
502	Bad Gateway	Internal server error that may require a reboot.
503	Service Unavailable	Internal server error that may require a reboot.

HTTP Response codes

Table 112 lists the HTTP request codes supported in cnMaestro.

Table 112 *Request Headers*

Header	Details
Accept	Set to application/json
Authorization	Used in every API request to send the Access Token. Example: Authorization: Bearer <Access-Token>
Content-Type	Set to application/json

REST Protocol

Resource URLs

The format for cnMaestro path and parameters are the following:

Access a collection of resources:

```
/api/{version}/{resource}?{parameter}={value}&{parameter}={value}
```

Access a single resource:

```
/api/{version}/{resource}/{resource_id}?{parameter}={value}&{parameter}={value}
```

Access a sub-resource on a collection (this is also possible on single resources):

```
/api/{version}/{resource}/{sub-resource}?{parameter}={value}&{parameter}={value}
```

For example – read the statistics for MAC, Type, and IP on all devices:

```
/api/v2/devices/statistics?fields=mac,type,ip_wan
```

Version

The version is equal to v2 in this release.

Resource

Resources are the basic objects in the system. Examples include:

Table 113 *Resource*

Context	Details
alarms	Current active alarms.
alarms/history	Historical alarms, including active alarms.
devices	Devices, including ePMP, PMP, and WiFi.
events	Historical events.
msp	MSP managed services.
networks	Configured networks.
sites	Configured WiFi sites.
towers	Configured Fixed Wireless towers.

Sub-Resources

Sub-Resources apply to top-level resources. They provide a different view of the resource data, or a filtered collection based upon the resource. Examples include:

Table 114 *Sub-Resources*

Context	Details
alarms	Alarms mapped to the top-level resource.
alarms/history	Historical alarms mapped to the top-level resource.
clients	Wireless LAN clients mapped to the top-level resource.
devices	Devices mapped to the top-level resource.
events	Events mapped to the top-level resource.
mesh/peers	Wireless LAN mesh peers mapped to the top-level resource.
operations	Operations available to the top-level resource
performance	Performance data for the top-level resource.
statistics	Statistics for the top-level resource.

Responses

Successful Response

In a successful HTTP 200 response, data is returned using the following structure. The payload is presented in JSON format.

The request URL is:

```
/api/v2/devices?fields=mac,type&limit=5
```

Response:

```
{
 "paging": {
   "offset": 0,
   "limit": 5,
   "total": 540
 },
 "data": [
   {
     "mac": "C1:00:0C:00:00:21",
     "type": "wifi-home"
```

```
    },
    {
      "mac": "C1:00:0C:00:00:18",
      "type": "wifi-home"
    },
    {
      "mac": "C1:00:0C:00:00:12",
      "type": "wifi-home"
    },
    {
      "mac": "C1:00:0C:00:00:15",
      "type": "wifi-home"
    },
    {
      "mac": "C1:00:0C:00:00:06",
      "type": "wifi-home"
    }
  ]
}
```

Error Response

Error Responses return a message and an error cause.

```
{
  "error": {
    "message": "Missing required property: stop_time \n Missing required property:
start_time",
    "cause": "InvalidInputError"
  }
}
```

Parameters

Most APIs can filter the data and limit the number of entries returned. The parameter options are listed below. The specific fields and the appropriate values vary for each API.

Field selection

Field selection is supported through the optional **Fields** parameter, which can specify the data to return from the server. If this parameter is missing, all available fields will be returned.

Table 115 *Fields*

Parameter	Details
fields	Define exactly what fields should be returned in a request. The names are provided as a comma-separated list.

Fields can limit which JSON parameters are returned as shown below:

Example: To retrieve name, type and location information for all devices.

Request:

`/api/v2/devices?fields=mac,type`

Response:

```
{
```

```
  "paging": {
    "total": 3,
    "limit": 100,
    "offset": 0
  },
  "data": [
    {
      "mac": "00:44:E6:34:89:48",
      "type": "wifi-enterprise"
    },
    {
      "mac": "00:44:16:E5:33:E4",
      "type": "wifi-enterprise"
    },
    {
      "mac": "00:44:26:46:32:22",
      "type": "wifi-enterprise"
    }
  ]
}
```


Filtering

A subset of fields support filtering. These are defined as query parameters for a particular resource, and they are listed along with the API specification.

Table 116 describes the standard filtering parameters as shown below:

Table 116 *Filtering*

Field	Details
network	(Devices) Configured Network name.
severity	(Alarms, Events) Alarm or Event severity (critical, major, minor, notice).
site	(Devices) Configured Site name.
state	(Alarms) Alarm state (active, cleared).
status	(Devices) Device status (online, offline, onboarding).
tower	(Devices) Configured Tower name.
type	(Devices) Device type (60ghz-cnwave, cnreach, cnmatrix, epmp, pmp, wifi-enterprise, wifi-home, wifi, ptp) (wifi includes wifi-home and wifi-enterprise).

Filters can be used simultaneously for **Resources** and **Sub-Resources**.

Example: Retrieve all WiFi devices that are online.

Request:

```
/api/v2/devices?type=wifi&status=online
```

Response:


```
{
  "paging": {
    "total": 1,
    "limit": 100,
    "offset": 0
   },
   "data": [
```

```
      {
        "ip": "233.187.212.38",
        "location": {
          "type": "Point",
          "coordinates": [
            77.55310127974755,
            12.952351523837196
          ]
        },
        "mac": "C1:00:0C:00:00:24",
        "msn": "SN-C1:00:0C:00:00:24",
        "name": "Hattie",
        "network": "Bangalore",
        "product": "cnPilot R201",
        "registration_date": "2017-05-23T21:28:37+05:30",
        "status": "online",
        "site": "Bangalore_Industrial",
        "type": "wifi-home",
        "hardware_version": "V1.1",
        "software_version": "2.4.4",
        "status_time": 1495560086
      }
    ]
}
```


Time Filtering

Events, Alarms, and Performance data can be filtered by date and time using ISO 8601 format.

Example: January 12, 2015 UTC would be encoded as **2015-01-12.**

Example: January 12, 2015 1:00 PM UTC would be encoded as **2015-01-12T13:00:00Z.**

If the parameters that are described in the Table 117 are not specified, then the start or stop times will be open-ended.

Table 117 *Time Filtering*

Parameter	Details
start_time	Inclusive start time of interval.
stop_time	Inclusive stop time of interval.

Sorting

Sorting is supported on a subset of fields within certain requests. Sort is used to specify sorting columns. The sort order is ascending unless the path name is prefixed with a '-', in which case it would be descending.

Table 118 *Sort*

Parameter	Details
sort	Used to get the records in the order of the given attribute.

Example: To retrieve devices in sorted (ascending) order by name.

Request:

```
/api/v2/devices?sort=name
```

Example: To retrieve devices in sorted (descending) order by mac.

Request:

```
/api/v2/devices?sort=-mac
```

Pagination

The limit and offset query parameters are used to paginate responses.

Table 119 *Pagination*

Parameter	Details
limit	Maximum number of records to be returned from the server.
offset	Starting index to retrieve the data.

Example: To retrieve the first 10 ePMP devices

Request:

```
/api/v2/devices?offset=3&limit=1
```

Response:


```
{
  "paging": {
    "total": 6,
    "limit": 1,
    "offset": 3
  },
  "data": [
    {
      "status": "online",
      "product": "cnPilot E400",
      "network": "Mumbai",
      "software_version": "3.3-b14",
      "registration_date": "2017-04-28T08:57:33+00:00",
      "site": "Central",
      "hardware_version": "Force 200",
      "status_time": "3498",
      "msn": "Z834275ABCDH",
      "mac": "00:04:36:46:34:AA",
      "location": {
        "type": "Point",
        "coordinates": [
          0,
          0
        ]
      },
      "type": "wifi-enterprise",
      "name": "E400-4634AA"
    }
  ]
}
```


Internal Response limits

When clients try to access a resource type without pagination, the server will return the first 100 entries that match the filter criteria. The response will always carry metadata to convey total count and current offset and limit. Maximum number of results at any point is 100 even when the provided is more than 100.

Example: To retrieve all devices.

Request:

```
/api/v2/devices
```

Response:

```
{
  data: {devices: [ {name: 'ePMP_5566', type:'ePMP', location:'blr'} , {….}… ] },
  paging:{
    "limit":25,
    "offset":50,
    "total":100
  }
}
```

The response returns the following values in the paging section:

Table 120 *Internal Response limits*

Parameter	Details
limit	Current setting for the limit.
offset	Starting index for the records returned in the response (begins at 0).
total	Total number of records that can be retrieved.

Access API

Token (basic request)

POST
`/api/v2/access/token`

The access API generates token using the **Client ID** and **Client Password** created in the cnMaestro UI. The token can be leveraged by API calls through the expiration time. Only one token is supported for each Client ID at any given time.

Request

Table 121 describes about the header and its values as shown below:

Table 121 ***Headers***

Header	Value
Accept (optional)	application/json.
Authorization	Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW.
Content-Type	application/x-www-form-urlencoded.

The **client_id** and **client_secret** are encoded and sent in the Authorization header. The encoding is:

```
BASE64(client_id:client_secret)
```

Body

The body needs to have the **grant_type**.

```
grant_type=client_credentials
```

Response

The response returns credentials for API access.

Body

Name	Details
access_token	Access token to return with each API request.
expires_in	Time in seconds that the API session will remain active.
token_type	This will always be bearer.

```
{
   "access_token":"2YotnFZFEjr1zCsicMWpAA",
   "token_type":"bearer",
   "expires_in":3600
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/token \

```
 -X POST -k \
 -u 8YKCxq72qpjnYmXQ:pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF \
 -d grant_type=client_credentials
```

Response

```
{"access_token":"d587538f445d30eb2d48e1b7f7a6c9657d32068e","token_type":"
 bearer","expires_in":86400}
```

Token (alternate request)

POST

```
/api/v2/access/token
```

An alternative form is supported in which the **client_ID** and **client_secret** are sent in the body, rather than the Authorization header.

Request

Headers

Header	Value
Accept (optional)	application/json
Content-Type	application/x-www-form-urlencoded

Body

```
grant_type=client_credentials&client_id=s6BhdRkqt3&client_secret=7Fjfp0ZBr1KtDRbnfVdmIw
```

Response

The response to both forms is the same.

Body

Name	Details
access_token	Access token to return with each API request.
expires_in	Time in seconds that the API session will remain active.
token_type	This will always be bearer.

Name	Details

<pre>{
"access_token":"2YotnFZFEjr1zCsicMWpAA",
"token_type":"bearer",
"expires_in":3600
}</pre>	

Example

Request

curl https://10.110.134.12/api/v2/access/token \
<pre>-X POST -k \
-d grant_type=client_credentials \
-d client_id=8YKCxq72qpjnYmXQ \
-d client_secret=pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF</pre>

Response

<pre>{"access_token":"ee4e077cf457196eb4d27cf6f02686dc07763059","token_type":"
bearer","expires_in":86400}</pre>

Validate Token

GET
/api/v2/access/validate_token

Verify if an Access Token is valid and return the time remaining before it expires.

Request

HTTP Headers

Header	Value
Accept (optional)	application/json
Authorization	Bearer <ACCESS_TOKEN>

Response

Body

Name	Details
expires_in	Time in seconds that the API session will remain active.

<pre>{
'expires_in': 86399
}</pre>	

Example

Request

curl https://10.110.134.12/api/v2/access/validate_token \
<pre>-X GET -k \
-H "Authorization: Beareree4e077cf457196eb4d27cf6f02686dc07763059"</pre>

Response
<pre>{"expires_in":85643}</pre>

Selected APIs

Overview

cnMaestro APIs are defined within the Swagger specification, accessed here https://docs.cloud.cambiumnetworks.com/api/5.1.1/index.html. This section only presents additional details for the Device, Statistics and Performance APIs, which have unique responses based upon Device Type, and are difficult to present within Swagger.

cnMaestro v2 API

Beginning with cnMaestro 3.0.0, the API version changes from **v1** to **v2**. The **v1** version will be supported through 3.1.0, but Cambium recommends updating existing API code to use **v2**. For most commands, swapping v1 in the URL with v2 should be sufficient. However, the following APIs may need to be rewritten while moving to the **v2** version.

- AP Groups
- Devices
- Statistics
- Performance
- Mesh Peers
- Operations

There are unique API responses such as:

- Devices API Response (v2 Format)
- Statistics API Response (v2 Format)
- Performance API Response (v2 Format)

Devices API Response (v2 Format)

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed	NSE
profile_attached	Profile attached to the device			✓								✓
ap_group	AP Group			✓								✓
cbrs_state	CBRS state		✓									
cbrs_status	CBRS status		✓									
config.sync_reason	Configuration synchronization reason	✓	✓	✓	✓	✓	✓	✓	✓			✓
config.sync_status	Configuration synchronization status	✓	✓	✓	✓	✓	✓	✓	✓			✓
config.variabl	Device is	✓	✓	✓	✓	✓	✓	✓	✓			✓

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed	NSE
es	mapped to configuration variables											
config.version	Current configuration version	✓	✓	✓	✓	✓	✓	✓	✓			✓
country	Country	✓	✓	✓		✓						
country_code	Regulatory band						✓					
description	Description	✓	✓	✓	✓	✓	✓		✓	✓		✓
hardware_version	Hardware version	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
inactive_software_version	Inactive software version	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
ip	IP address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ipv6	IPv6	✓		✓		✓				✓	✓	
last sync	Last Synchronized							✓				
last_reboot_reason	Reason for the last reboot (see 24.1)	✓	✓	✓	✓	✓	✓		✓		✓	✓
link_symmetry	Link symmetry						✓					
location	Location	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
mac	MAC address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
managed_account	Managed account name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
maximum_range	Maximum range (KM)	✓	✓			✓	✓					
mode	Mode type							✓			✓	✓
msn	Manufacturer serial number	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
name	Device name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
network	Network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
onboarding.error_code	Error code of the device if it fails to onboard	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed	NSE
onboarding.state	Onboarding state of the device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
online	Offline or online	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
product	Product name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
registration_date	Registration date	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
role							✓					
site	Site			✓					✓	✓		✓
site_id	Site unique identifier			✓					✓	✓		
software_version	Active Software version	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
status	Status (online, offline, onboarding).	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
status_time	Uptime/downtime time interval (sec)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
temperature	Temperature							✓				
tower	Tower	✓	✓		✓	✓	✓	✓	✓		✓	
type	Device type (epmp, pmp, wifi-home, wifi-enterprise, cnreach, ptp, cnmatrix, 60ghz-cnwave, nse)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Devices onboarding error codes

Error Codes	Details
ERR_UNSUPPORTED_DEVICE	Claiming {{type}} devices is not currently supported.
ERR_NON_ENTERPRISE_WIFI_TYPE	Only cnPilot Enterprise (ePMP Hotspot), Enterprise Wi-Fi (E-Series and XE/XV-Series) and cnMatrix devices are allowed into Enterprise account.
ERR_NON_WIFI_TYPE	Cannot claim non Wi-Fi device under a Site.
ERR_UNSUPPORTED_	Unsupported device type in current account view - {{view}}.

Error Codes	Details
TYPE	
ERR_UNKNOWN_DEVICE	Unknown Device.
ALREADY_CLAIMED	Device already claimed.
LTE_CLAIMED	cnRanger devices are not supported in production accounts.
ERR_INVALID_MSN	Invalid Serial Number.
ERR_OWNER_DIFFERENT	Device is claimed into another account.
ERR_INTERNAL	System encountered an internal error; please try again later. If the problem persists, contact support.
ERR_INVALID_MAC	Invalid MAC.
ERR_DUPLICATE_KEY	The device is already claimed.
UNPROCESSABLE	Device state does not allow to cloud sync.
CBRS_ERROR_DEVICES	MAC is already claimed. It cannot be claimed on CBRS.
SUBSCRIPTION_FAIL	Device could not acquire slot.
SUBSCRIPTION_FAIL_ FEATURE_MISMATCH	Device is mapped to another onprem instance.
SUBSCRIPTION_FAIL_ TOO_MANY_ASSOCS	Device is mapped to another onprem instance.

Statistics API Response (v2 Format)

Statistics API Response v2 format are shown for the following devices:

- 60 GHz cnWave
- cnMatrix
- cnReach
- Fixed Wireless
- PTP
- PTP 820/850
- Wi-Fi
- cnWave 5G Fixed

60 GHz cnWave

General

Name	Details	Mode
cpu	CPU utilization	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
IP	IP address	All
managed_account	Managed account name	All
memory	Available memory	All
mode	Device mode	All

Name	Details	Mode
name	Device name	All
network	Network	All
site	Site name	All
site_id	Site ID	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
sync_mode	Radio Sync mode [RF, GPS, None]	All
type	Device type	All

Networks

Name	Details	Mode
ipv6	IPv6 address	All

Radios (Array format)

Name	Details	Mode
radios[].channel	Channel	All
radios[].id	Radio Id	All
radios[].mac	Radio MAC	All
radios[].rx_bps	Receive bits per second	All
radios[].sync_mode	Radio Sync mode [RF, GPS, None]	All
radios[].tx_bps	Transmit bits per second	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx_pkts	Received packets	All
ethports[].rx_errors	Received packets errors	All
ethports[].rx_pkts_drop	Dropped received packets	All
ethports[].speed	Port speed and duplex	All
ethports[].tx_pkts	Transmitted packets	All
ethports[].tx_errors	Transmitted packets errors	All
ethports[].tx_pkts_drop	Dropped transmitted packets	All

cnMatrix

General

Name	Details
cpu	CPU utilization
config_version	Configuration version
last_sync	Last synchronization (UTC Unix time milliseconds)

Name	Details
mac	MAC address
managed_account	Managed account name
memory	Available memory
mode	Device mode
name	Device name
network	Network
site	Site name
site_id	Site unique identifier
status	Status [online, offline, claimed, waiting, onboarding]
status_time	Uptime/downtime interval (seconds)
tower	Tower name
type	Device type

Networks

Name	Details
ip	IP address

cnReach

General

Name	Details	Mode
config_version	Configuration version	All
connected_sms	Connected SM count	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
tower	Tower name	All
type	Device type	All

Networks

Name	Details	Mode
ip	IP address	All

Radios (Array format)

Name	Details	Mode
radios[].device_id	Device ID	Radios
radios[].id	Radio Id	Radios
radios[].linked_with	Linked with	Radios
radios[].mac	Radio MAC	Radios
radios[].margin	Margin	Radios
radios[].mode	Radio mode [ap, ep, rep]	Radios
radios[].neighbors	Radio neighbors	Radios
radios[].network_address	Network address	Radios
radios[].noise	Average noise (dB)	Radios
radios[].power	Transmit power	Radios
radios[].rssi	RSSI value (dB)	Radios
radios[].rx_bytes	Receive bytes	Radios
radios[].software_version	Current software version.	Radios
radios[].temperature	Radio temperature	Radios
radios[].type	Radio type [ptp, ptmp]	Radios
radios[].tx_bytes	Transmit bytes	Radios

Fixed Wireless (cnVision, ePMP and PMP)

General

Name	Details	cnVision	ePMP	PMP
ap_mac	AP MAC	SM	SM	SM
config_version	Configuration version	AP/SM	AP/SM	AP/SM
connected_sms	Connected SM count	AP	AP	AP
cpu	CPU utilization			AP/SM
distance	SM distance (KM)	SM	SM	SM
gain	Antenna gain (dBi)	AP/SM	AP/SM	AP/SM
gps_sync_state	GPS synchronization state	AP/SM	AP/SM	
last_sync	Last synchronization (UTC Unix time milliseconds)	AP/SM	AP/SM	AP/SM
mac	MAC address	AP/SM	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM	AP/SM
network	Network	AP/SM	AP/SM	AP/SM
reboots	Reboot count	AP/SM	AP/SM	
status	Status [online, offline, claimed, waiting, onboarding]	AP/SM	AP/SM	AP/SM
status_time	Uptime/downtime interval (seconds)	AP/SM	AP/SM	AP/SM
temperature	Temperature			AP/SM

Name	Details	cnVision	ePMP	PMP
tower	Tower name	AP	AP	AP
type	Type	AP/SM	AP/SM	AP/SM
vlan	VLAN			AP/SM

Networks

Name	Details	cnVision	ePMP	PMP
default_gateway	Default gateway	AP/SM	AP/SM	AP/SM
ip	IP address	AP/SM	AP/SM	AP/SM
ipv6	IPv6 address	AP/SM	AP/SM	
ip_dns	DNS	AP/SM	AP/SM	AP/SM
ip_dns_secondary	Secondary DNS			AP/SM
ip_wan	WAN IP	AP/SM	AP/SM	
lan_mode_status	LAN mode status [no-data, half, full]	AP/SM	AP/SM	
lan_mtu	MTU size	SM	SM	
lan_speed_status	LAN speed status	AP/SM	AP/SM	
lan_status	LAN status [down, up]	AP/SM	AP/SM	AP/SM
netmask	Network mask	AP/SM	AP/SM	AP/SM

Radios

Name	Details	cnVision	ePMP	PMP
radio.auth_mode	Authentication mode	SM	SM	
radio.auth_type	Authentication type ePMP [open, wpa1, eap-ttls] PMP [disabled, enabled]	AP/SM	AP/SM	AP/SM
radio.channel_width	Channel width ePMP [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP [...]	AP/SM	AP/SM	AP/SM
radio.color_code	Color code			AP/SM
radio.dfs_status	DFS status ePMP: [not-applicable, channel- availability-check, in-service, radar- signal-detected, alternate-channel- monitoring, not-in- service] PMP: [Status String]	AP/SM	AP/SM	AP/SM
radio.dl_err_drop_pkts	Downlink error drop packets	SM	SM	
radio.dl_err_drop_pkts_ percentage	Downlink error drop packets percentage	SM	SM	
radio.frequency	RF frequency	AP/SM	AP/SM	AP/SM
radio.frame_period	Frame period			AP
radio.dl_frame_utilization	Downlink frame utilization			AP
radio.dl_lqi	Downlink Link Quality Indicator			SM

Name	Details	cnVision	ePMP	PMP
radio.dl_mcs	Downlink MCS	SM	SM	
radio.dl_modulation	Downlink Modulation			SM
radio.dl_pkts	Downlink packet count	AP/SM	AP/SM	AP/SM
radio.dl_pkts_loss	Downlink packet loss			AP/SM
radio.dl_retransmits	Downlink Retransmission	AP/SM	AP/SM	
radio.dl_retransmits_pct	Downlink Retransmission percentage	AP/SM	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance			AP
radio.dl_snr	Downlink SNR (dB)	SM	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal			SM
radio.dl_snr_v	Downlink SNR (dB) vertical			SM
radio.dl_throughput	Downlink throughput	AP/SM	AP/SM	AP/SM
radio.mac	Wireless MAC	AP/SM	AP/SM	
radio.mode	Radio mode [eptp-master, eptp- slave, tdd, tdd-ptp, ap/sm]	AP/SM	AP/SM	
radio.sessions_dropped	Session drops	AP	AP	AP/SM
radio.software_key_throughput	Software key – max throughput			SM
radio.ssid	SSID	AP/SM	AP/SM	
radio.sync_source	Synchronization source			AP
radio.sync_state	Synchronization state			AP
radio.tdd_ratio	TDD ratio ePMP [75/25, 50/50, 30/70, flexible] PMP [...]	AP	AP	AP
radio.tx_capacity	SM transmit capacity	SM	SM	
radio.tx_power	Radio transmit power	AP/SM	AP/SM	AP/SM
radio.tx_quality	SM transmit quality	SM	SM	
radio.ul_err_drop_pkts	Uplink error drop packets	SM	SM	
radio.ul_err_drop_pkts_ percentage	Uplink error drop packets percentage	SM	SM	
radio.ul_frame_utilization	Uplink frame utilization			AP
radio.ul_mcs	Uplink MCS	AP/SM	AP/SM	
radio.ul_modulation	Uplink Modulation example [2X MIMO-B)]			SM
radio.ul_lqi	Uplink Link Quality Indicator			SM
radio.ul_pkts	Uplink packet count	AP/SM	AP/SM	AP/SM
radio.ul_pkts_loss	Uplink packet loss			AP/SM
radio.ul_retransmits	Uplink Retransmission	SM	SM	
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM	SM
radio.ul_snr	Uplink SNR (dB)	SM	SM	

Name	Details	cnVision	ePMP	PMP
radio.ul_snr_h	Uplink SNR (dB) horizontal			SM
radio.ul_snr_v	Uplink SNR (dB) vertical			SM
radio.ul_throughput	Uplink throughput	AP/SM	AP/SM	AP/SM
radio.wlan_status	WLAN status [down, up]	AP/SM	AP/SM	

PTP 650/670/700

General

Name	Details	Mode
config_version	Configuration version	All
connected_sms	Connected SM count	Master
gain	Antenna gain (dBi)	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
temperature	Temperature	All
tower	Tower name	All
type	Device type	All
vlan	VLAN	All

Networks

Name	Details	Mode
default_gateway	Default gateway	All
ip	IP address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
lan_status	LAN status [down, up]	All
netmask	Network mask	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx_frames	Ports receive frames oversize	All
ethports[].rx_util	Ports receive bandwidth utiliization	All
ethports[].speed	Ports speed and duplex	All
ethports[].tx_util	Ports transmit bandwidth utiliization	All

Radios

Name	Details	Mode
radio.byte_error_ratio	Byte Error Ratio	All
radio.channel_width	Channel width ePMP: [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP: [...]	All
radio.color_code	Color code	All
radio.rx_frequency	Receive frequency	All
radio.tx_frequency	Transmit frequency	All
radio.tx_power	Radio transmit power	All

PTP 820/850

General

Name	Details	Mode
ip	IP address	All
last_sync	Last synchronized	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
temperature	Temperature	All
tower	Uptime/downtime interval (seconds)	All
type	Device type	All

Radio

Name	Details	Mode
radios[].defective_blocks	Radio defective blocks	All
radios[].id	Radio Id	All
radios[].radio_location	Radio location	All
radios[].rx_bps	Receive bits/second	All
radios[].rx_level	Receive level	All
radios[].rx_frequency	Receive frequency	All
radios[].tx_bps	Transmit bits/second	All
radios[].tx_level	Transmit level	All
radios[].tx_frequency	Transmit frequency	All
radios[].tx_mute_status	Transmit mute status	All
radios[].modem_mse	Modem Mean Square Error (MSE) in dB	All
radios[].modem_xpi	Modem Cross-Polar Isolation (XPI) in dB	All

Interfaces

Name	Details	Mode
interfaces[].admin_state	Admin state	All
interfaces[].auto_negotiation	Auto Negotiation	All
interfaces[].interaface_location	Interface location	All
interfaces[].mac	MAC address	All
interfaces[].media_type	Media type	All
interfaces[].operational_status	Operational Status	All
interfaces[].port_duplex	Interface duplex type	All
interfaces[].speed	Interface speed	All

Wi-Fi



Note

Mode is Enterprise, Home, or All.

General

Name	Details	Mode
config_version	Configuration version	All
cpu	CPU utilization	All
mac	MAC address	All
managed_account	Managed account name	All
memory	Available memory	All
mode	Device mode	All
name	Device name	All
network	Network	All
parent_mac	Parent MAC	All
site	Site name	All
site_id	Site unique identifier	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
type	Device type	All

Networks

Name	Details	Mode
ip	IP address	All
ipv6	IPv6 address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
ip_wan	WAN IP	All
lan_mode_status	LAN mode status [no-data, half, full]	Enterprise
lan_speed_status	LAN speed status	All

Name	Details	Mode
lan_status	LAN status [down, up]	Home
netmask	Network mask	All

Radios (Array format)

Name	Details	Mode
radios[].airtime	Airtime	All
radios[].band	Radio band	All
radios[].bssid	Radio mac	Enterprise
radios[].channel	Channel	All
radios[].id	Radio Id	All
radios[].multicast_rate	Multicast rate	Enterprise
radios[].noise_floor	Noise floor	Enterprise
radios[].num_clients	Number of clients	All
radios[].num_wlans	Number of WLANs	Enterprise
radios[].power	Transmit power	All
radios[].quality	RF Quality description	Enterprise
radios[].radio_state	Radio state	Enterprise
radios[].rx_bps	Receive bits/second	All
radios[].rx_bytes	Receive bytes	All
radios[].tx_bps	Transmit bits/second	All
radios[].tx_bytes	Transmit bytes	All
radios[].unicast_rates	Unicast rates	Enterprise
radios[].utilization	Radio utilization	Enterprise

cnWave 5G Fixed

General

Name	Details	Mode
cpu	CPU utilization	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
ip	IP Address	All
mode	Device mode	All
name	Device name	All
network	Network	All
tower	Tower name	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
config_version	Current config version	All
type	Device type	All

Name	Details	Mode
connected_cpe	Number of CPEs connected to the BTS	BTS
registered_cpe	Number of CPEs registered with the BTS	BTS
cpe_registration_state	CPEs Registration State	CPE
cpe_registration_count	CPEs Registration Count	CPE
cpe_imsi	CPE Device Identity	CPE

Boot

Name	Details	Mode
startup_count	Startup Count for the device	BTS
startup_reason	Startup Reason for the device	BTS

Shutdown (Array format)

Name	Details	Mode
shutdown[].date	Shutdown Date	BTS
shutdown[].detail	Shutdown Detail	BTS
shutdown[].index	Shutdown Index	BTS
shutdown[].reason	Shutdown Reason	BTS

Interface Config

Name	Details	Mode
sfp1_speed	SFP1 Speed	BTS
sfp2_speed	SFP2 Speed	BTS

Interfaces (Array format)

Name	Details	Mode
interfaces[].port_name	Port name	BTS
interfaces[].in_octets	Received octets	BTS
interfaces[].out_octets	Transmitted octets	BTS
interfaces[].in_ucast_pkts	Received unicast packets	BTS
interfaces[].out_ucast_pkts	Transmitted unicast packets	BTS
interfaces[].in_mcast_pkts	Received multicast packets	BTS
interfaces[].out_mcast_pkts	Transmitted multicast packets	BTS
interfaces[].in_bcast_pkts	Received broadcast packets	BTS
interfaces[].out_bcast_pkts	Transmitted broadcast packets	BTS
interfaces[].in_discards	Received discarded packets	BTS
interfaces[].out_discards	Transmitted discarded packets	BTS
interfaces[].in_errors	Received errored packets	BTS
interfaces[].out_errors	Transmitted errored packets	BTS

Radio

Name	Details	Mode
dl_throughput	Received Throughput	BTS
ul_throughput	Transmitted Throughput	BTS
frequency	Frequency	BTS
max_eirp	Maximum EIRP	BTS
polarization	Polarization	All
link_symmetry	Link Symmetry	BTS
bandwidth	Bandwidth	BTS
ul_target_rxPower	Transmitted Target Power	BTS
ul_tx_power_init	Transmitted Initial Power	BTS
ul_tx_power_cont	Transmitted Control Power	BTS
ul_frame_util	Transmitted Frame Utilization	BTS
dl_frame_util	Received Frame Utilization	BTS
dl_mcs	Downlink MCS	CPE
ul_mcs	Uplink MCS	CPE
alignment_active	Alignment Active Status	CPE
cpe_range	Range of CPE	CPE
current_eirp	Current Effective radiated power	CPE
ul_backoff	Uplink Backoff	CPE
dl_backoff	Downlink Backoff	CPE
ul_sounding_state	Uplink Sounding State	CPE
dl_sounding_state	Downlink Sounding State	CPE
ul_channel_distortion	Uplink Channel Distortion	CPE
dl_channel_distortion	Downlink Channel Distortion	CPE
ul_evm	Uplink EVM	CPE
dl_evm	Downlink EVM	CPE
ul_rx_power	Uplink Received Power	CPE
dl_rx_power	Downlink Received Power	CPE
ul_spatial_freq	Uplink Spatial Frequency	CPE
dl_spatial_freq	Downlink Spatial Frequency	CPE

Wireless and Ethernet interfaces

Name	Details	Mode
in_octets	Received octets	CPE
out_octets	Transmitted octets	CPE
in_ucast_pkts	Received unicast packets	CPE
out_ucast_pkts	Transmitted unicast packets	CPE
in_mcast_pkts	Received multicast packets	CPE
out_mcast_pkts	Transmitted multicast packets	CPE

Name	Details	Mode
in_bcast_pkts	Received broadcast packets	CPE
out_bcast_pkts	Transmitted broadcast packets	CPE
in_discards	Received discarded packets	CPE
out_discards	Transmitted discarded packets	CPE
in_errors	Received errored packets	CPE
out_errors	Transmitted errored packets	CPE

Performance API Response (v2 Format)

Performance API Response v2 Format are shown for following devices:

- 60 GHz cnWave
- cnMatrix
- cnReach
- Fixed Wireless
- PTP 650/670/700
- PTP 820/850
- Wi-Fi
- cnWave 5G Fixed

60 GHz cnWave

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
site	Site	All
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].id	Radio ID	All
radios[].rx_bps	Receive bits per second	All
radios[].tx_bps	Transmit bits per second	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].max_rx	Ports maximum receive bytes	All
ethports[].max_tx	Ports maximum transmit bytes	All
ethports[].min_rx	Ports minimum receive bytes	All
ethports[].min_tx	Ports minimum transmit bytes	All
ethports[].port	Port name	All
ethports[].rx	Ports receive bytes	All
ethports[].tx	Ports transmit bytes	All
ethports[].rx_bps	Ports receive bits per second	All
ethports[].tx_bps	Ports receive bits per second	All
ethports[].min_rx_bps	Ports minimum receive bits per second	All
ethports[].min_tx_bps	Ports minimum transmit bits per second	All
ethports[].max_rx_bps	Ports maximum receive bits per second	All
ethports[].max_tx_bps	Ports maximum transmit bits per second	All

cnMatrix

General

Name	Details
mac	MAC address
managed_account	Managed account name
mode	Device mode
name	Device name
network	Network
site	Site
timestamp	Timestamp
tower	Tower
type	Device type

Switch

Name	Details
switch.rx.broadcast_pkts	Receive broadcast packets
switch.dl_kbits	Downlink usage (in kbits on hour or minute basis)
switch.dl_throughput	Downlink throughput (Kbps)
switch.ul_kbits	Uplink (in Kbits on hour or minute basis)
switch.rx.multicast_pkts	Receive multicast packets
switch.ul_throughput	Uplink throughput (Kbps)
switch.rx.pkts_err	Receive Packet error
switch.rx.unicast_pkts	Receive unicast packets
switch.tx.broadcast_pkts	Transmit broadcast packets

Name	Details
switch.tx.multicast_pkts	Transmit multicast packets
switch.tx.pkts_err	Transmit packet error
switch.tx.unicast_pkts	Transmit unicast packets

cnReach

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
sm_count	Connected SM count	All
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].id	Radio ID	Radios
radios[].neighbors	Radio neighbors	Radios
radios[].noise	Average noise	Radios
radios[].power	Transmit power	Radios
radios[].rssi	RSSI value	Radios
radios[].rx_bytes	Receive bytes	Radios
radios[].throughput	Total throughput	Radios
radios[].tx_bytes	Transmit bytes	Radios

Fixed Wireless (cnVision, ePMP and PMP)

General

Name	Details	cnVision	ePMP	PMP
mac	MAC address	AP/SM	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM	AP/SM
network	Network	AP/SM	AP/SM	AP/SM

Name	Details	cnVision	ePMP	PMP
online_duration	Duration of device connection with server (seconds)	AP/SM	AP/SM	AP/SM
sm_count	Connected SM count	AP	AP	AP
sm_drops	Session drops	AP/SM	AP/SM	AP
timestamp	Timestamp	AP/SM	AP/SM	AP/SM
tower	Tower	AP/SM	AP/SM	AP/SM
type	Device type	AP/SM	AP/SM	AP/SM
uptime	Device online time (seconds)	AP/SM	AP/SM	AP/SM

Radios

Name	Details	cnVision	ePMP	PMP
radio.dl_frame_utilization	Downlink frame utilization			AP
radio.dl_kbits	Downlink usage (in Kbits on hour or minute basis)	AP/SM	AP/SM	
radio.dl_mcs	Downlink MCS	SM	SM	
radio.dl_modulation	Downlink modulation			SM
radio.dl_pkts	Downlink packet count	AP/SM	AP/SM	
radio.dl_pkts_loss	Downlink packet loss			AP/SM
radio.dl_retransmits_pct	Downlink retransmission percentage	AP/SM	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance			SM
radio.dl_snr	Downlink SNR	SM	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal			SM
radio.dl_snr_v	Downlink SNR (dB) vertical			SM
radio.dl_throughput	Downlink Throughput (Kbps)	AP/SM	AP/SM	AP/SM
radio.ul_frame_utilization	Uplink frame utilization			AP
radio.ul.kbits	Uplink usage (in Kbits on hour or minute basis)	AP/SM	AP/SM	
radio.ul_mcs	Uplink MCS	SM	SM	
radio.ul_modulation	Uplink modulation			SM

Name	Details	cnVision	ePMP	PMP
radio.ul_pkts	Uplink packet count	AP/SM	AP/SM	
radio.ul_pkts_loss	Uplink packet loss			AP/SM
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM	SM
radio.ul_snr	Uplink SNR	SM	SM	
radio.ul_snr_h	Uplink SNR (dB) horizontal			SM
radio.ul_snr_v	Uplink SNR (dB) vertical			SM
radio.ul_throughput	Uplink Throughput (Kbps)	AP/SM	AP/SM	AP/SM

PTP 650/670/700

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
sm_count	Connected SM count	Master
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].max_rx	Ports maximum receive bytes	All
ethports[].max_tx	Ports maximum transmit bytes	All
ethports[].min_rx	Ports minimum receive bytes	All
ethports[].min_tx	Ports minimum transmit bytes	All
ethports[].pkt_error	Ports packet error	All
ethports[].port	Port name	All
ethports[].rx	Ports receive bytes	All
ethports[].tx	Ports transmit bytes	All
ethports[].rx_bps	Ports receive bits per second	All
ethports[].tx_bps	Ports receive bits per second	All
ethports[].min_rx_bps	Ports minimum receive bits per second	All
ethports[].min_tx_bps	Ports minimum transmit bits per second	All

Name	Details	Mode
ethports[].max_rx_bps	Ports maximum receive bits per second	All
ethports[].max_tx_bps	Ports maximum transmit bits per second	All

Ethernet

Name	Details	Mode
ethernet.link_loss	Link loss	All
ethernet.pcb_temperature	PCB temperature	All
ethernet.rx_channel_util	Receive channel utilization	All
ethernet.rx_capacity	Receive capacity	All
ethernet.ssr	Signal strength ratio	All
ethernet.rx_power	Receive power	All
ethernet.sfp_interface.tx	SFP transmit bytes	All
ethernet.rx_throughput	Receive throughput	All
ethernet.tx_channel_util	Transmit channel utilization	All
ethernet.tx_capacity	Transmit capacity	All
ethernet.tx_power	Transmit power	All
ethernet.tx_throughput	Transmit throughput	All
ethernet.vector_error	Vector error	All

PTP 820/850

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device Mode	All
name	Device name	All
network	Network	All
online_duration	Duration online	All
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All
uptime	Device online time (seconds)	All

Radio

Name	Details	Mode
radios[].id	Radio ID	All
radios[].max_rsl	Radio Maximum Receiver Signal Level	All
radios[].max_tsl	Radio Maximum Transmission Signal Level	All
radios[].min_rsl	Radio Minimum Receiver Signal Level	All

Name	Details	Mode
radios[].min_tsl	Radio Minimum Transmission Signal Level	All
radios[].peak_throughput	Radio Peak Throughput	All
radios[].radio_location	Radio Location	All
radios[].throughput	Radio Throughput	All
radios[].modem_max_mse	Modem maximum MSE in dB	All
radios[].modem_min_mse	Modem minimum MSE in dB	All
radios[].modem_max_xpi	Modem maximum XPI in dB	All
radios[].modem_min_xpi	Modem minimum XPI in dB	All
radios[].modem_max_mrmc_profile	Modem maximum MMRC	All
radios[].modem_max_mrmc_profile	Modem minimum MMRC	All

Radio Groups

Name	Details	Mode
radios_groups[].id	Radio Group ID	All
radios_groups[].peak_throughput	Radio Group peak throughput	All
radios_groups[].radio_location	Radio Group location	All
radios_groups[].throughput	Radio Group throughput	All

Wi-Fi

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
site	Site	All
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].clients	Number of clients	All
radios[].id	Radio ID	All
radios[].rx_bps	Receive bits/second	All
radios[].throughput	Total throughput	All
radios[].tx_bps	Transmit bits/second	All
radios[].band	Radio band (2.4 GHz/5 GHz)	All

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All
cpe_registered	Registered CPEs count	BTS
cpe_connected	Connected CPEs count	BTS
cpe_registrationCnt	Number of times the CPE registered with the BTS	CPE

Radio

Name	Details	Mode
ul_throughput	Uplink Throughput	BTS
dl_throughput	Downlink Throughput	BTS
cpe_ul_throughput	Uplink Throughput	CPE
cpe_dl_throughput	Downlink Throughput	CPE
cpe_ul_evm	Uplink EVM	CPE
cpe_dl_evm	Downlink EVM	CPE
cpe_ul_mcs	Uplink MCS	CPE
cpe_dl_mcs	Downlink MCS	CPE
cpe_ul_rxPower	Uplink Rx Power	CPE
cpe_dl_rxPower	Downlink Rx Power	CPE

Client API Response (v2 Format)

Client details API Response v2 format are shown below:

Name	Details	Wi-Fi
ap_mac	AP MAC	
client_type	Client type(Client | Guest Client)	
download_quota	Download quota (Note: only applicable for Guest Client)	
download_quota_balance	Download quota balance (Note: only applicable for Guest Client)	
ip	IP address of client	
mac	Client MAC	

Name	Details	Wi-Fi
managed_account	Managed account name	
manufacturer	Manufacturer name	
name	Client name	
radio.band	Band(2.4 GHz/5 GHz)	
radio.rssi	RSSI	
radio.rx_bytes	Received bytes	
radio.snr	SNR	
radio.ssid	SSID	

External Guest Access Login API

Integrates an external captive portal with the Cambium Networks AP while posting directly to cnMaestro. This API provides the support for the external captive portal to make login requests.

POST `/api/v2/ext-portals/login`

Request:

curl -X

```
/api/v2/ext-portals/login" -H "accept: */*" -H "Authorization: Bearer
e88916f5b663c1ea966af835c8a0a19c20d17686" -H "Content-Type: application/json"-d
```

Body

```
"{\"ga_ap_mac\":\"11-22-33-44-55-66\",\"ga_cmac\":\"11-22-33-44-55-65\",\"ga_
Qv\":\"eUROBR86HBgAGDEEVgQAGw4UWRUCACYVMgFPMV5ZWVFfUVdGX1ZFJXxZR1dLBhMUMww\",\"ga_
user\":\"test-user\",\"ga_pass\":\"test-pass\"}"
```

Response:

```
{
"data": {
         "mType": 3,
         "msgId":28,
         "status":<integer values>,
         "prefixQs":<true/false>,
         "expiry":<integer values>,
         "action":<integer values>,
         "cmac":<client mac>,
         "msg":<Radius Returned Message>,
         "extURL":<external url string>
         }
}
```

The status value description is provided in the table below.

Status	Description
0	Login is successful.
1	Invalid login request, the client is not currently associated to the AP which is being requested for login here.
2	RADIUS reject due to invalid username/password.
3	RADIUS timeout, AP didn't received the RADIUS response.
4	Missing RADIUS server config on the WLAN config of the AP.

Status	Description
5	If LDAP configured on the AP for authentication then LDAP server responded back with reject.
6	LDAP timeout happened on the AP for the request.
7	Missing LDAP configuration on the WLAN configuration of the AP.
8	Logout is successful.
9	Logout failed due to missing session on the AP. Most likely client session is already deleted from this AP.

The response parameter name and details is shown below.

Name	Details
action	0: On success action redirects the user to AP onboard logout page. 1: On success redirects user to an external URL. 2: On success redirects user to its original URL.
cmac	MAC address of the client.
expiry	Displays the session time for the given guest session.
msg	Message is based on RADIUS attribute reply message (18) in the RADIUS Access Accept or Reject message.
prefixQs	True: Add query strings to landing URL on success. False: Remove query strings from landing URL on success. `prefixQs` and `action` values are driven based on WLAN configuration.

60 GHz cnWave RESTful API

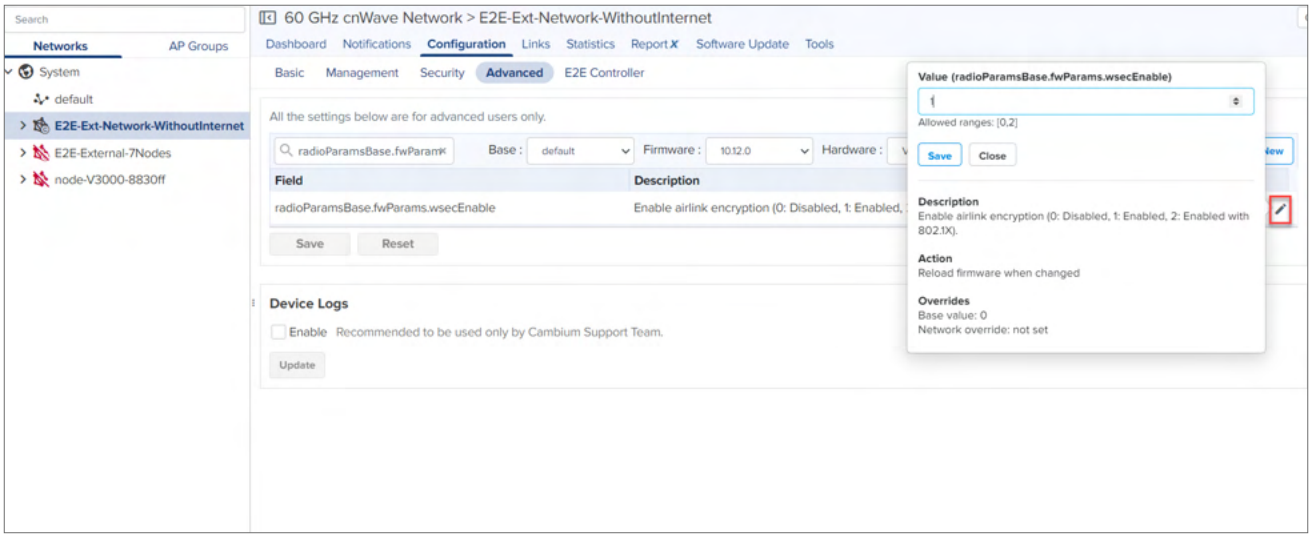
cnMaestro supports configuration overrides for 60 GHz cnWave E2E Network, E2E Controller, and Node(s) using the RESTful API.

E2E Network

To determine the configuration parameters available in an E2E Network, navigate to **E2E Network** > **Configuration** > **Advanced**. Search for the desired **Field**, and review its **Description**, allowed **Values**, and **Override status**. Use the RESTful API to override single or multiple fields.

GET `/api/v2/cnwave60/networks/{network_id}/configuration`

PUT `/api/v2/cnwave60/networks/{network_id}/configuration`



Field names are separated by dots. Each substring between the dots will be converted to objects and the last substring will be the key and value.

Example

In case of field name `radioParamsBase.fwParams.wsecEnable`, payload will be:

```
{
  "radioParamsBase": {
    "fwParams": {
       "wsecEnable": 1
     }
   }
}
```

Warning

Partial update is not allowed. Always send full configuration that needs to be pushed to E2E Network.

Optimization

To determine the optimization parameters available in an E2E Network, navigate to **E2E Network** > **Configuration** > **Advanced**.

GET `/api/v2/cnwave60/networks/{network_id}/optimization/{optimization_type}`

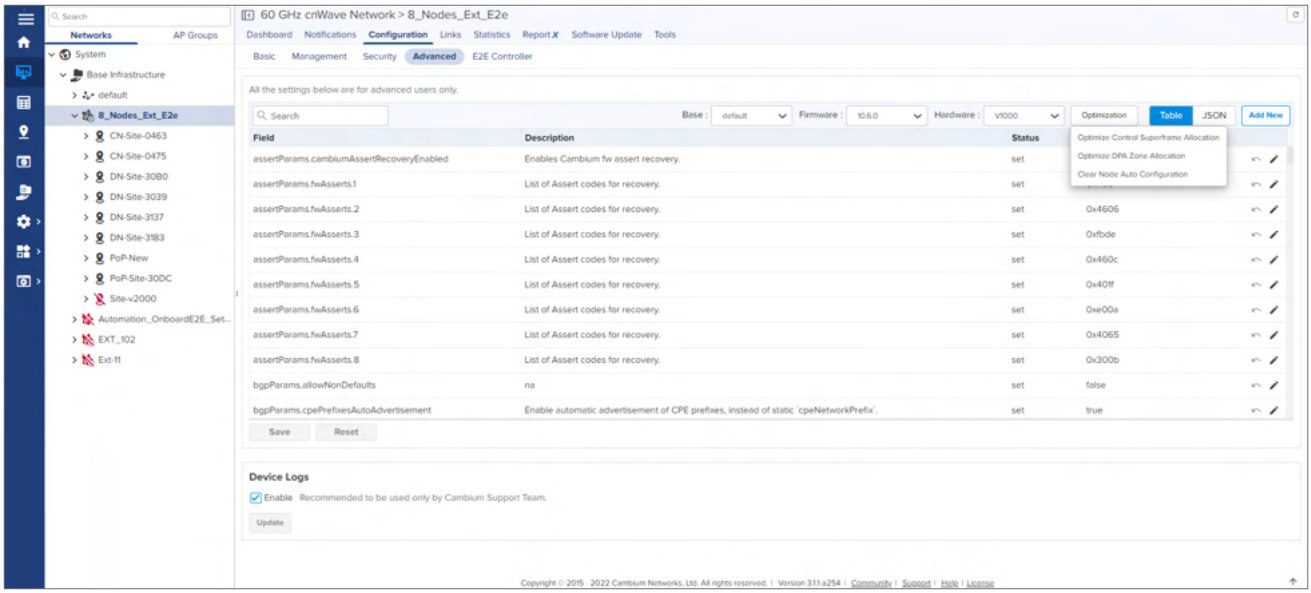
PUT `/api/v2/cnwave60/networks/{network_id}/optimization/{optimization_type}`

Available values :

`controlSuperframeAllocation`,

`dpaZoneAllocation`

`clearNodeAutoConfig`



Example

```
{
  "clearUserConfig": true,
  "nodes": [
    "string"
  ],
  "configPaths": "string"
}
```

Device (Node) Configuration

To update Device configuration, navigate to **Node** > **Configuration** > **Advanced**. Search for the **Field**, and review its **Description**, allowed **Values**, **and Overrides status**. Use the RESTful API to override those fields.

GET `/api/v2/cnwave60/networks/{mac}/configuration`

PUT `/api/v2/cnwave60/networks/{mac}/configuration`

Field names are separated by dots. Each substring between the dots will be converted to objects and the last substring will be the key and value.

Example

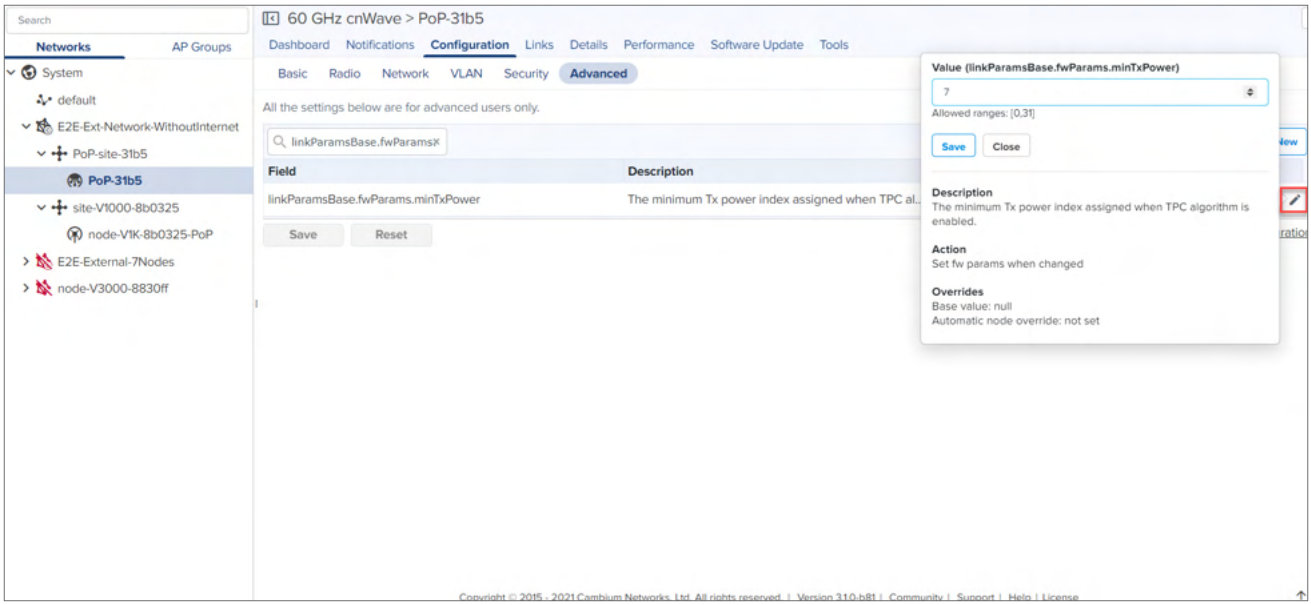
In case of field name `linkParamsBase.fwParams.minTxPower`, object to send in the API payload will be:

```
{
    "linkParamsBase": {
        "fwParams": {
            "minTxPower": 6
            "maxTxPower": 8
         }
      }
}
```

The below two APIs are introduced in Release 3.1.0 to update multiple device configurations overrides.

GET `/api/v2/cnwave60/networks/{network_id}/devices/overrides`

PUT `/api/v2/cnwave60/networks/{network_id}/devices/overrides`



Warning

Partial update is not allowed. Always send full configuration that needs to be pushed to 60 GHz cnWave Devices.

The example payload for PUT request is seen from cnMaestro UI.

Example

```
{
  "device1_name": {
    "radioParamsBase": {
     "fwParams": {
       "txPower": 6
     }
    }
   },
   "device2_name": {
     "popParams": {
      "POP_IFACE": "nic2"
     }
    }
  }
```

Note

You can download the full config of the node by clicking on the **Show Full Configuration** as well and then get the JSON key and pass in RESTful API.

E2E Controller

To update E2E Controller configuration, navigate to **E2E Network** > **Configuration** > **E2E Controller**. Search for the desired **Field**, and review its **Description**, allowed **Values**, and **Override status**. Use the RESTful API to override those fields.

GET `/api/v2/cnwave60/networks/{network_id}/controller/configuration`

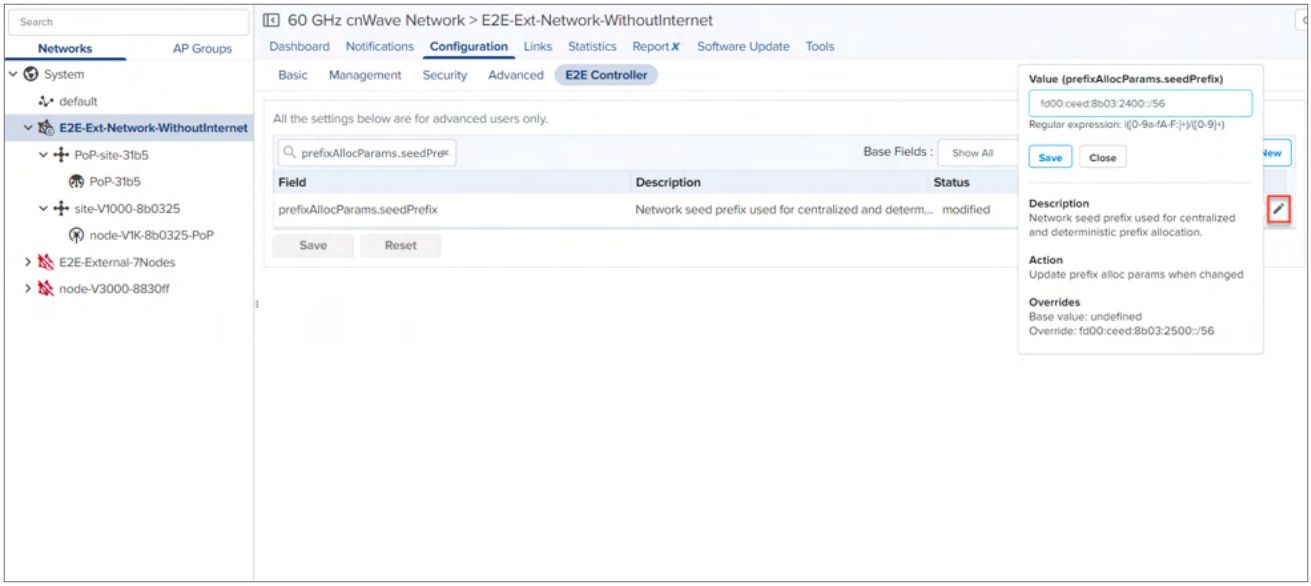
PUT `/api/v2/cnwave60/networks/{network_id}/controller/configuration`

Field names are separated by dots. Each substring between the dots will be converted to objects and the last substring will be the key and value.

Example

In case of field name `prefixAllocParams.seedPrefix`, payload will be:

```
{
   "prefixAllocParams": {
    "seedPrefix": "fd00:ceed:1992:1400::/56"
   }
}
```



Warning

Partial update is not allowed. Always send full configuration that needs to be pushed to the E2E Controller.

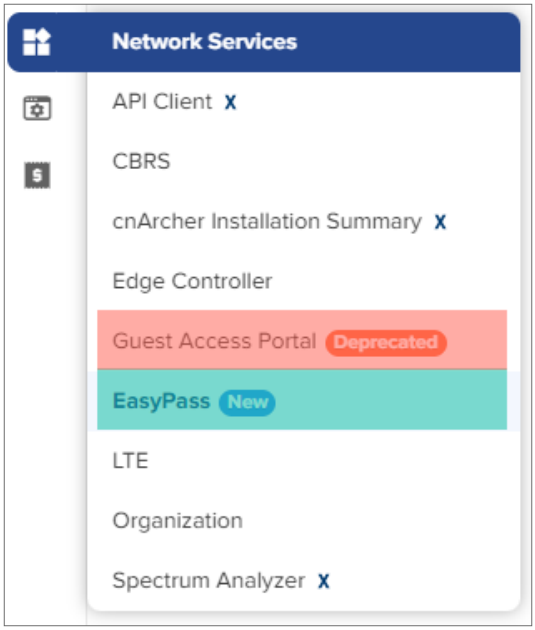
Guest Access

This section describes how to configure Guest Access using cnMaestro. This feature allows the clients to connect to the internet through Free Tier, Vouchers, or Paid Access types.

Note

From cnMaestro 5.1.0 release onwards, the **Guest Access Portal** configuration wizard is deprecated, and a new wizard called **EasyPass** is introduced, as shown in Figure 488.

Figure 488 *Network Services*



Note

For information on EasyPass, see EasyPass.

The Guest Access feature creates a separate network for guests by providing Internet access to guest wireless devices such as mobiles, tabs, and laptops.

Note

The Guest Access feature is supported only on Enterprise Wi-Fi devices.

Configuration

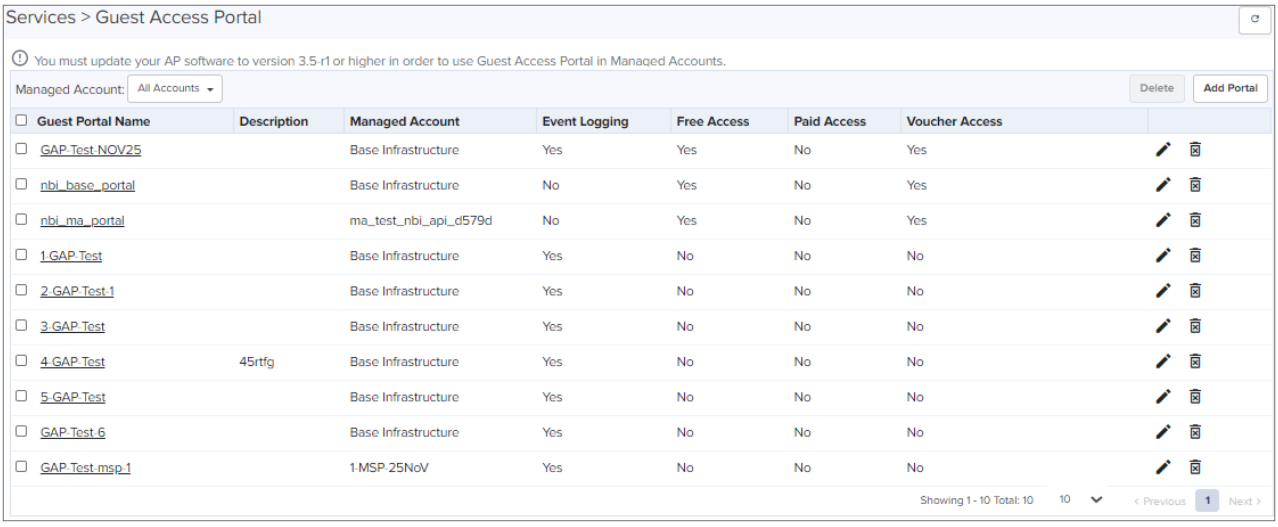
- Create the Guest Access Portal in cnMaestro
- Map the device to cnMaestro

Creating the Guest Access Portal in cnMaestro

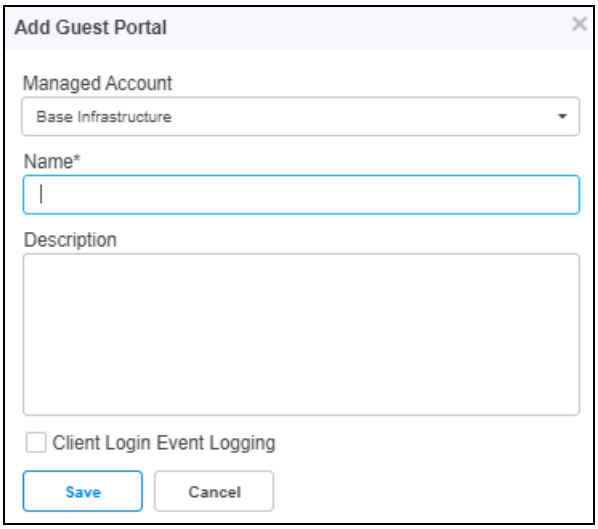
1. Basic Details
2. Access Portal
3. Design Page
4. Sessions
5. Guests

Procedure for Creating Guest Access

1. Navigate to **Network Services** > **Guest Access Portal**.



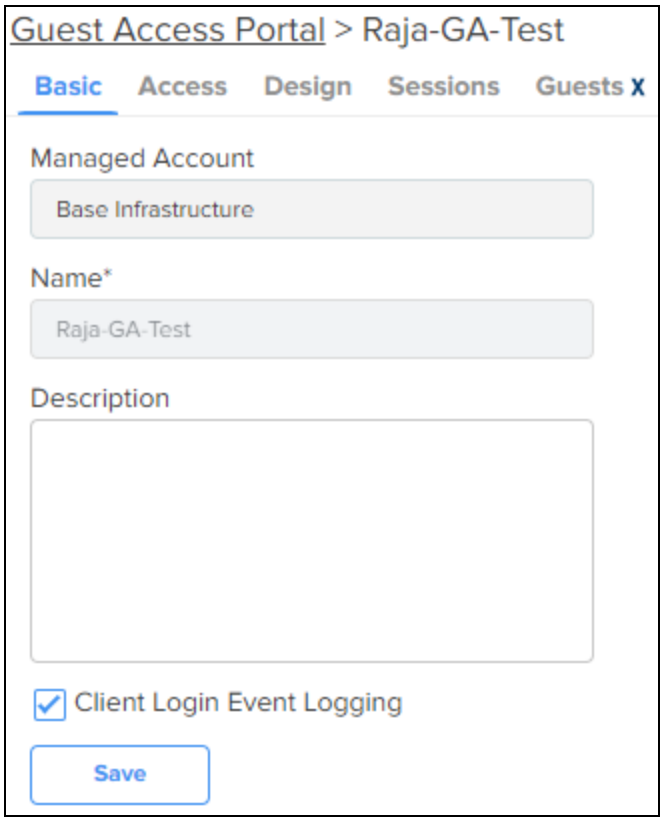
2. Click **Add Portal**. A maximum of four portals can be created per account.
3. Enter a name and brief description for the portal.



4. Click **Save**.

Basic Details

The **Basic** details page contains the **Managed Account** Type, **Name**, and **Description**.



Note

A name once created for the Portal cannot be changed.

Access Portal

The Access Portal tab has four different access types:

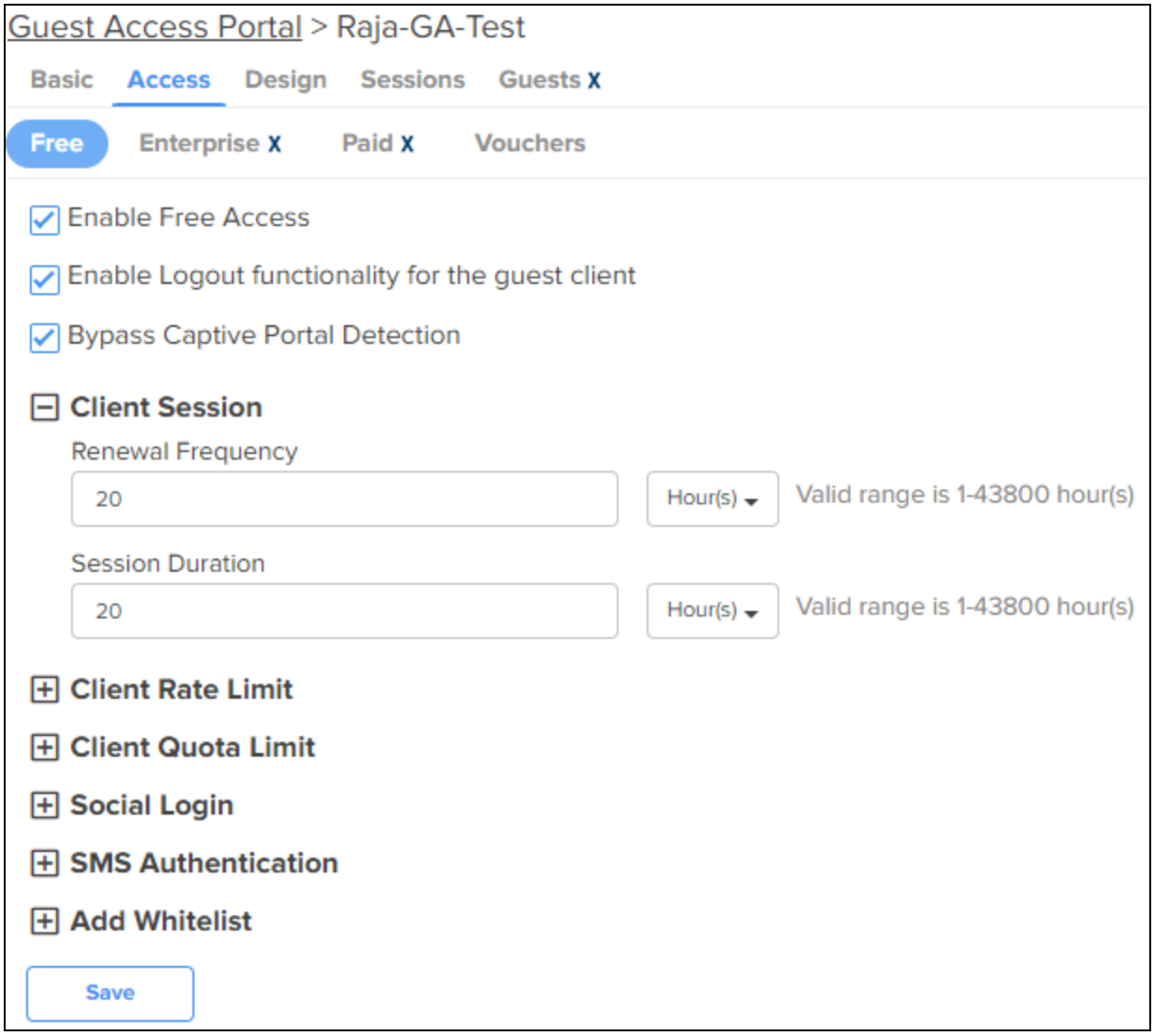
- Free
- **Enterprise** X access through one of the following options:
  - Microsoft Azure
  - Sponsored Guest
  - Self Registration
  - Google
- **Paid** X
- Vouchers

The parameters under each access method can be configured only after the corresponding access method is enabled.

Note

Microsoft Azure and Google-based access are not supported on devices running release version 4.x.

Free Access Type Configuration



Free Access type contains configurable parameters such as:

- Session validity
- Renewable frequency
- Client rate limits
- Social login

You can select authentication using Google, Facebook, Twitter and Office 365, or all. You will need to enter the App ID of your social login App. If you enable Facebook login you will also need to enter your Facebook App secret.

Table 122 *Free Access Type Parameters*

Parameter	Description
Add Whitelist	Options for configuring the IP address or the domain name.
Client Rate Limit	Options for configuring downlink and uplink parameters in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied.

Table 122 *Free Access Type Parameters*

Parameter	Description

Client Quota Limit	The data quota limit feature has been added for RADIUS-based as well as controller-based guest portals. For controller-based, it is either directional or total data quota limit. Once the client logs in as a guest, the data quota limit is enforced and the values are sent to the AP to which the client is connected. The access point keeps track of the data limits and sends client statistics to the controller every 30 minutes. In case of multiple devices allowed for a given policy, the data quota limits enforcement has some limitations and works with the latency of 30 minutes during which the cumulative data quota limits of the devices can be exceeded beyond the configured data quota limits.
	
	The similar behavior is supported through RADIUS attributes for RADIUS-based onboard guest access clients.
	
	`RADIUS_VENDOR_ID_CAMBIUM 9 (17713)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP (151)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN (152)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP_GIGWORDS (153)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN_GIGWORDS (154)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL (155)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL_GIGWORDS (156)`
	
	The `gigwords` attributes are used for supporting data quota limits above 4 GB when required.

Renewable Frequency	Once the session duration for the client expires, the client needs to wait for the period specified by renewal frequency before logging in again.
Session Duration	The duration for which the client is provided access.
SMS Authentication	SMS OTP supports Twilio, SMS Country, and SMS Gupshup SMS gateway providers. Any one of the gateway providers can be used to support the SMS OTP to be delivered to the cell phone of the end user. Once OTP is received the client can enter the OTP to get Internet access.
Social Login	Consists of the following options: • Domain URL: The redirected URL used by the client when trying to access the Internet. • Google: Consists of ID and Secret options to configure, which admin can create from https://console.cloud.google.com/. • Facebook: Consists of ID and Secret options to configure, which admin can create from https://developers.facebook.com/apps/. • Twitter: Consists of consumer key, consumer secret key, and callback URL. • Office 365: Consists of ID and Replyback URL.



Note

- Renewal frequency should be greater than session expiration.
- Client will get Social login options only when enabled in Access Control page in Portal.
- If Social login is enabled, it is mandatory in free access method for client to login through Google/Facebook/Twitter/Office 365.

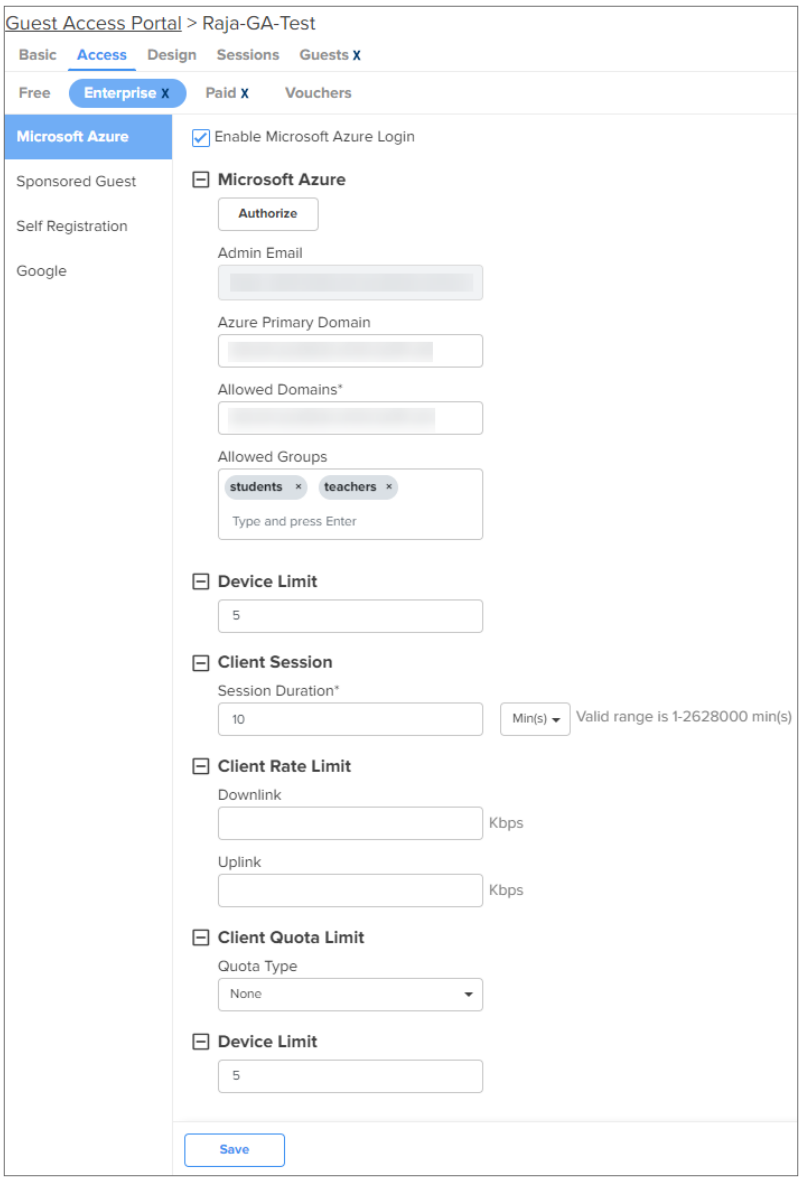
Enterprise Wi-Fi Access X using Microsoft Azure Login, Sponsored Guest, Self Registration, or Google

Note

- Microsoft Azure and Google-based access are supported only on Enterprise Wi-Fi 6 APs running firmware version 6.5.1 and later.
- Microsoft Azure is supported on cnMaestro 4.1.0 and later versions.
- Google-based access is supported on cnMaestro 5.0.0 and later versions.

Microsoft Azure

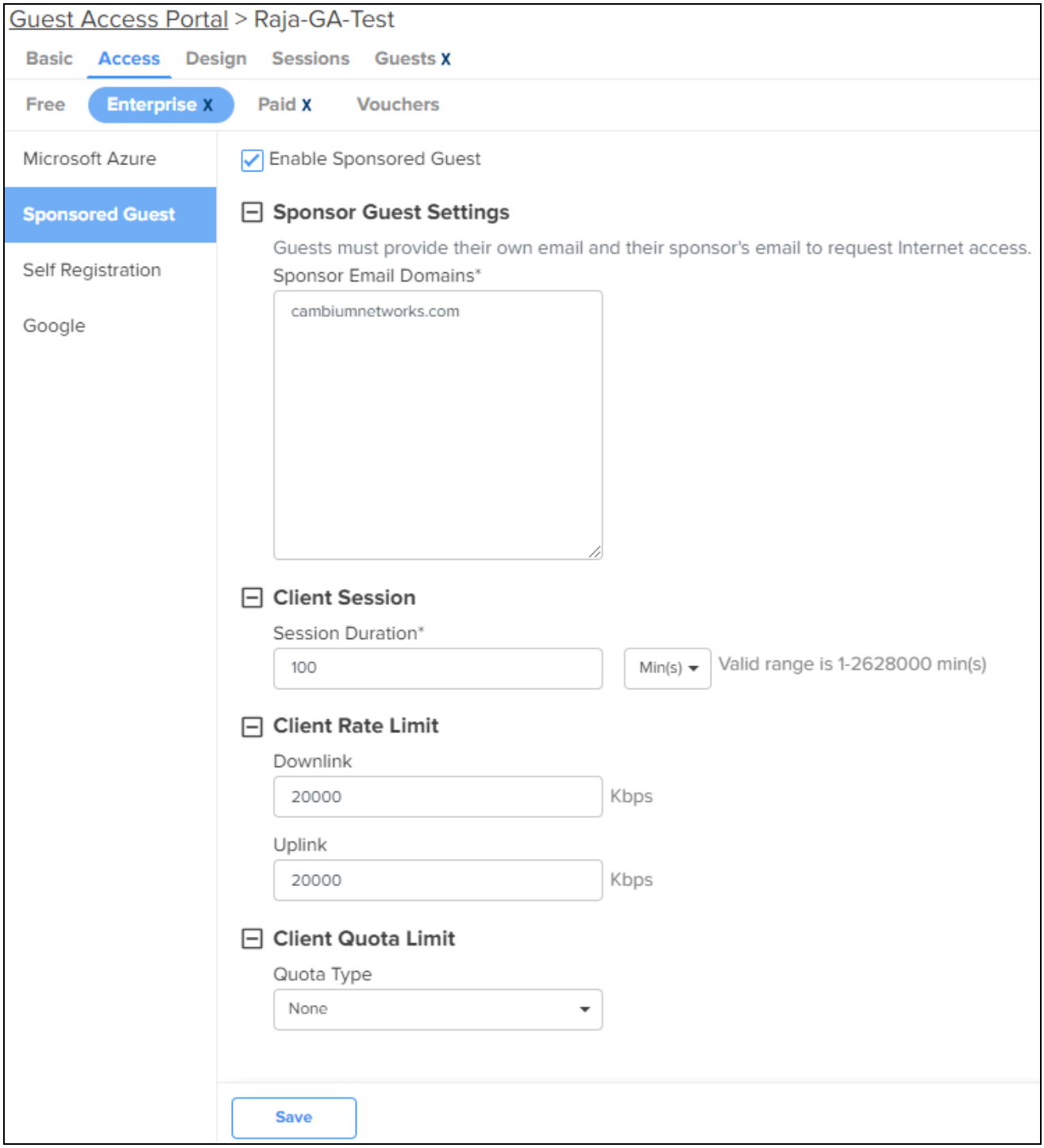
Enterprise Microsoft Azure access page enables Microsoft Azure users to log in to access the Enterprise Wi-Fi. To set up users to authenticate from Microsoft Azure, navigate to **Network Services** > **Guest Access Portal** > **Access** > **Enterprise X** > **Microsoft Azure**, complete the following parameters and click **Save**:



Sponsored Guest

In this type of access, guests must provide their own email address and their sponsor's email address to request Internet access.

To allow sponsored guests to access the Wi-Fi, navigate to **Network Services** > **Guest Access Portal** > **Access** > **Enterprise X** > **Sponsored Guest** complete the following parameters, and click **Save**:



Self Registration

Self registration enables guests to register themselves when connecting to the Wi-Fi network for the first time. The Wi-Fi administrator can configure the self registration process to require a sponsor approval or not. The sponsor approval can also be configured to be manual or automatic confirmation.

To configure self registration, navigate to **Network Services** > **Guest Access Portal** > **Access** > **Enterprise X** > **Self Registration** and configure the following parameters.

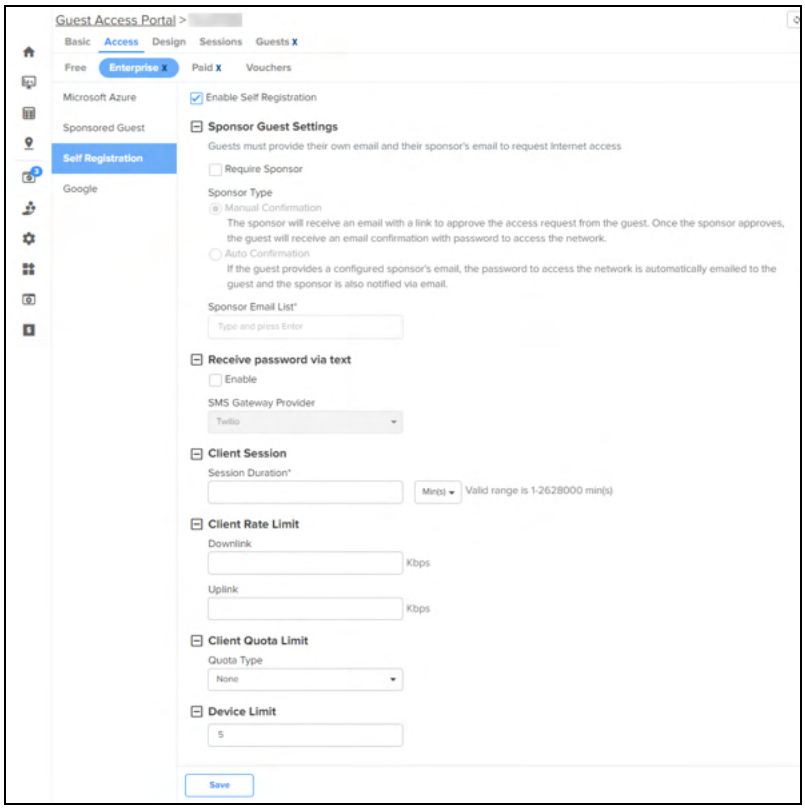


Table 123 *Self Registration Parameters*

Parameter	Description
Enable Self Registration	Select the check box to enable self registration feature and configure the following parameters.
Sponsor Guest Settings The guests must enter a sponsor email address when registering to connect to the wireless network. The administrator can choose to configure whether the sponsor must manually approve each request or the approval is automatic.	
Require Sponsor	Select the check box if you want the self registration to be approved by a sponsor. The guests must enter the sponsor email address when registering for access to the SSID.
Sponsor Type	Specifies whether the sponsor approval for guest internet access must be automatic or manual. The following options are available: • **Manual Confirmation**—The sponsor receives an email for approving the guest's access request. After approval, the guest receives an email confirmation along with the password to connect to the wireless network. • **Automatic Confirmation**—If the guest provides a configured sponsor's email address, the password to access the network is automatically emailed to the guest and the sponsor is also notified via email.
Sponsor Email List	Configure the list of sponsor email addresses for approving access requests.

Table 123 *Self Registration Parameters*

Parameter	Description
Receive password via text By default, the guests receive the password to their email address. However, if you want the guests to receive the password to their mobile devices as well, configure the following parameters.	
Enable	Select the check box to send the password to the guest's mobile device.
SMS Gateway Provider	Select the SMS gateway to be used to send the OTP to the guest's mobile device. The following gateways are supported (each of the gateways have their own respective parameters that must be configured): • Fast SMS • Generic SMS API • SMS Country • SMS Gupshup • SMSAPI • Twilio • Victory Link SMS Each of the above gateways must be configured with their respective parameters.
Client-related parameters	
Client Session—**Session Duration**	Specifies the maximum duration (in minutes) that the guest can browse the internet in a single session. Supported range: 1-2628000 minutes
Client Rate Limit	Specifies the download and upload speed limit (in Kbps) for the guests. Configure the speed limit in the **Downlink** and **Uplink** fields.
Client Quota Limit	
Quota Type	Specifies the type of quota for configuring the data usage limit. The following options are supported: • None—No limit is configured for data usage. Guests can access unlimited data in the configured session duration. • Directional—Configure limits separately for downlink and uplink directions. The **Downlink** and **Uplink** fields are enabled. • Total—Configure the limit for both directions totally. The **Total** field is enabled.
Downlink	Specifies the downlink data usage limit (in either MB or GB, selected from the drop-down list). This field is available only when you select **Directional** in the **Quota Type** field.
Uplink	Specifies the uplink data usage limit (in either MB or GB, selected from

Table 123 *Self Registration Parameters*

Parameter	Description
	the drop-down list). This field is available only when you select **Directional** in the **Quota Type** field.
Total	Specifies total data usage limit for both the directions (in either MB or GB, selected from the drop-down list). This field is available only when you select **Total** in the **Quota Type** field.
Device Limit	Specifies the number of devices that the guest can connect to the wireless network. Default: 5.

Google-based access

Google-based access enables users with a Google account to connect to the wireless network by synchronizing the active directory. When enabled, if a guest who is part of the supported group tries to connect to the Wi-Fi network, the AP provides access to the guest.

Note

To configure Google-based access, you must have a Google Workspace account.

To configure Google-based access, navigate to **Network Services** > **Guest Access Portal** > **Access** > **Enterprise** X > **Google** and configure the following parameters.

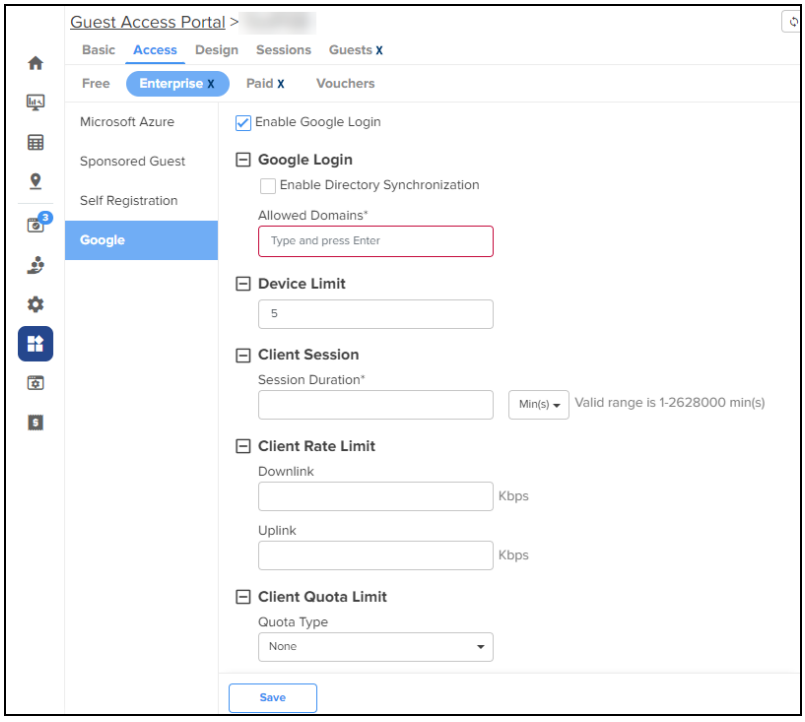


Table 124 *Google Parameters*

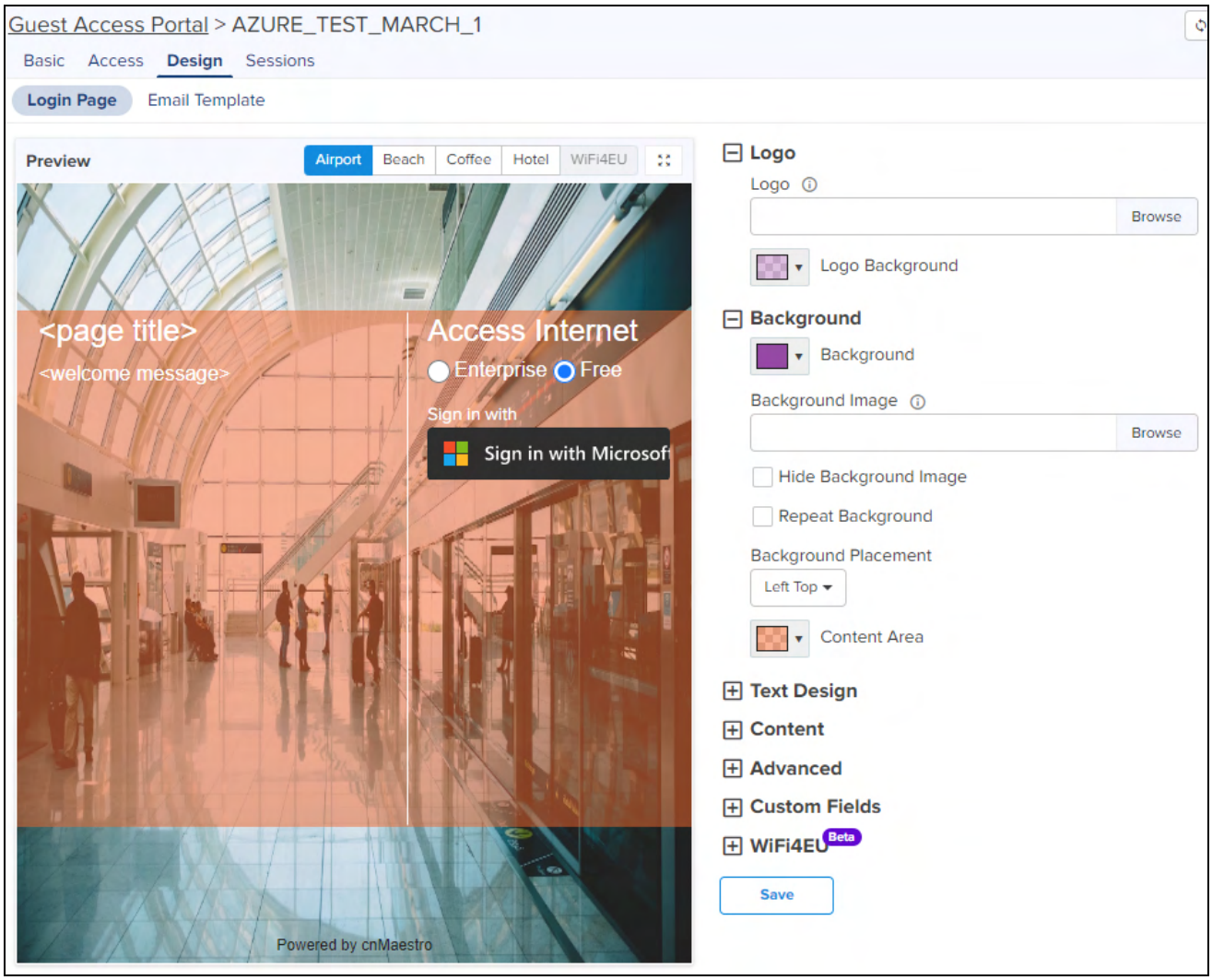
Parameter	Description
Enable Google Login	Select the check box to enable Google-based Wi-Fi access and configure the following parameters.
Device Limit	Specifies the number of devices that the guest can connect to the wireless network.

Table 124 *Google Parameters*

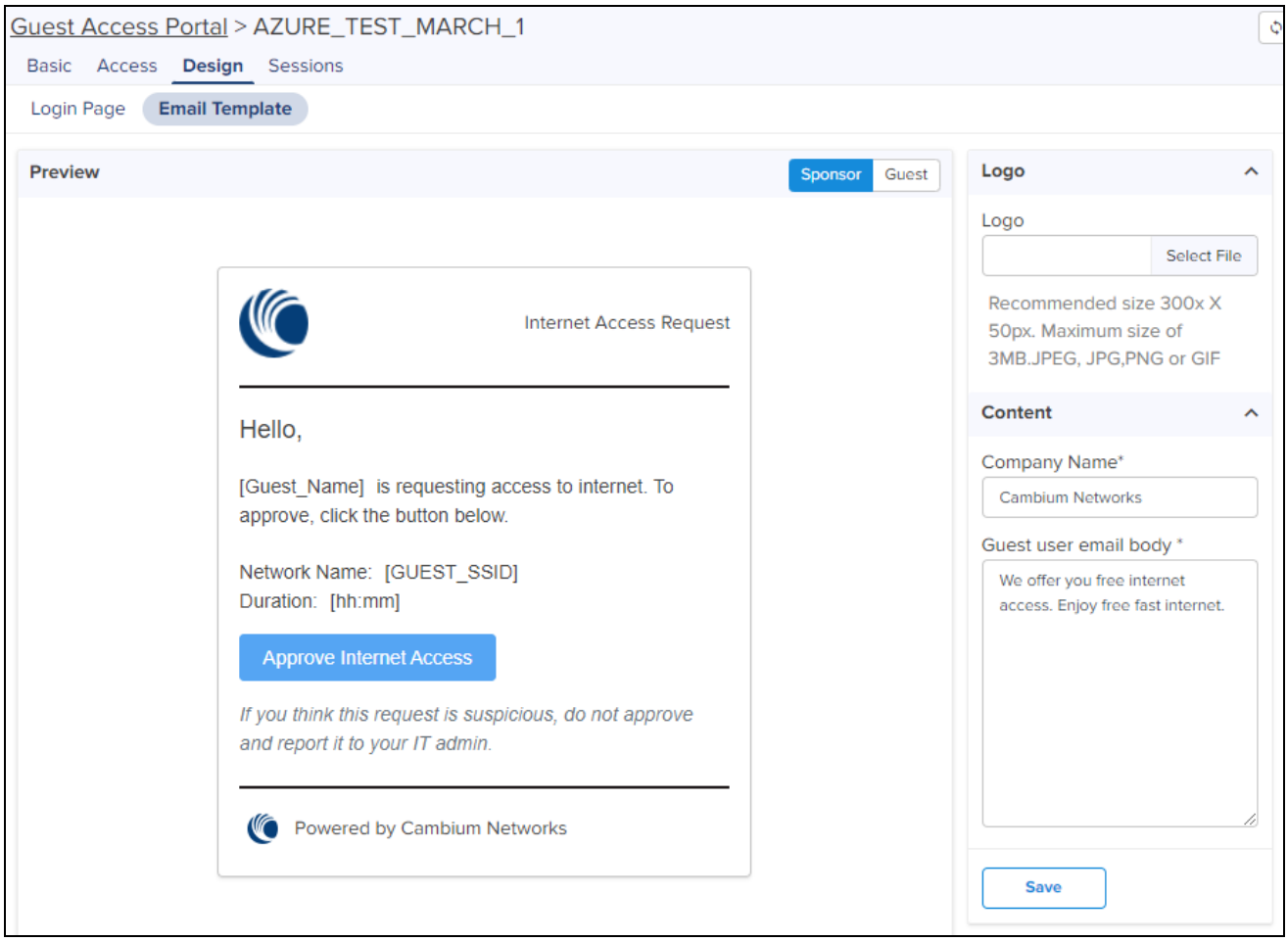
Parameter	Description
	Default: 5.
Google Login	
Enable Directory Synchronization	Select the check box to enable synchronization of Google Apps Domain Directory. This functions requires authorization. Click **Follow these steps** for information on configuring your Google Apps Domain Directory.
Allowed Domains	List of domains to be allowed for Google-based access. Enter the domain name in the text box.
Client-related parameters	
Client Session—Session Duration	Specifies the maximum duration (in minutes) that the guest can access internet in a single session. Supported range: 1-2628000 minutes
Client Rate Limit	Specifies the download and upload speed limit (in Kbps) for the guests. Configure the speed limit in the **Downlink** and **Uplink** fields.
Client Quota Limit	
Quota Type	Specifies the type of quota for configuring the data usage limit. The following options are supported: • None—No limit is configured for data usage. Guests can access unlimited data in the configured session duration. • Directional—Configure limits separately for downlink and uplink directions. The **Downlink** and **Uplink** fields are enabled. • Total—Configure the limit for both directions totally. The **Total** field is enabled.
Downlink	Specifies the downlink data usage limit (in either MB or GB, selected from the drop-down list). This field is available only when you select **Directional** in the **Quota Type** field.
Uplink	Specifies the uplink data usage limit (in either MB or GB, selected from the drop-down list). This field is available only when you select **Directional** in the **Quota Type** field.
Total	Specifies total data usage limit for both the directions (in either MB or GB, selected from the drop-down list). This field is available only when you select **Total** in the **Quota Type** field.

Designing the Guest Access Login Page and Email Templates

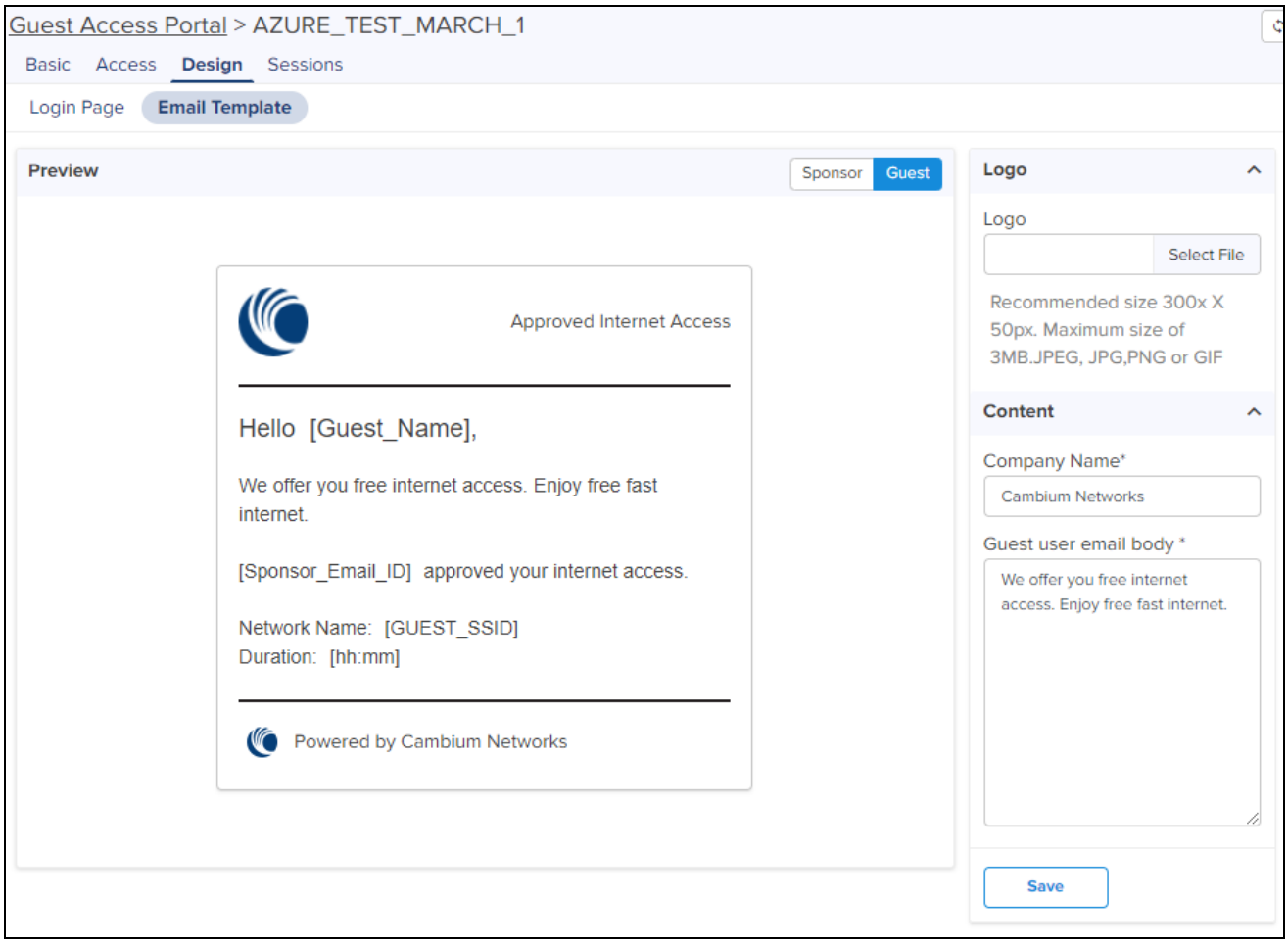
To design the guest login page for users to see when requesting access, navigate to **Network Services > Guest Access Portal > Design > Login Page**, complete the following parameters, and click **Save:**



To design the email template that should be used to send approval request to the sponsor (in Sponsored Guest and Self Registration access types), navigate to **Network Services > Guest Access Portal > Design > Email Template > Sponsor**, complete the following parameters, and click **Save:**



To design the email template that should be used to send approved access details to the guest, navigate to **Network Services > Guest Access Portal > Design > Email Template > Guest**, complete the following parameters, and click **Save:**



Paid Access[X]

Paypal has been added as a payment gateway service where end users can purchase Internet connectivity using a credit card or their existing PayPal accounts. For purchasing Internet plans, clients are directed to PayPal portal where they purchase the plan and then they are automatically redirected to guest access portal where the purchased voucher is displayed. The user should ensure to save this Voucher information if s/he plans to use it on multiple devices.

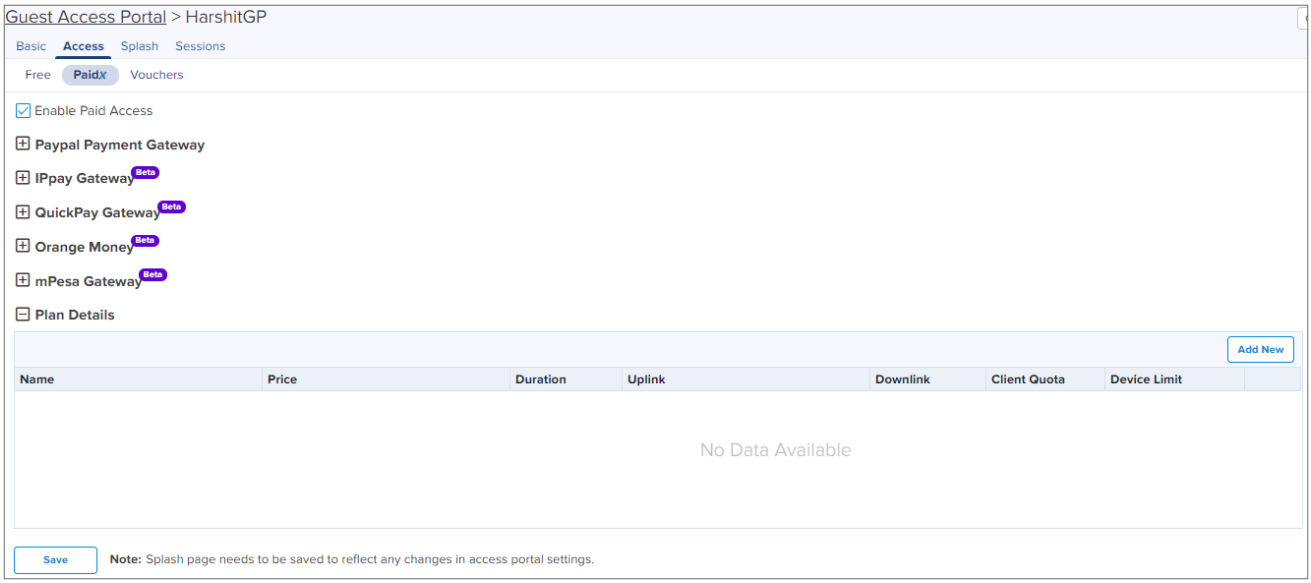
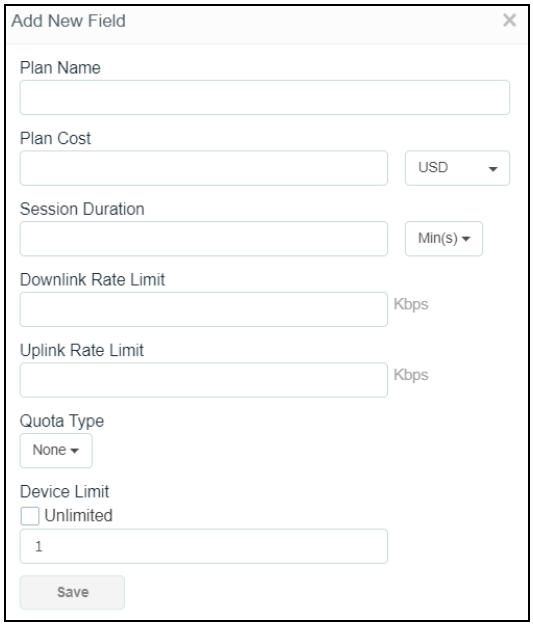


Table 125 *Paid Access Type Parameters*

Parameter	Description
General	**Plan Name:** The name of the plan.
	Session Duration: The duration for which the client is allowed to access the network.
	Client Rate Limit: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limit s are applied.
	Device Limit: The device limit allow that number of devices to be connected or select the unlimited to connect any number of devices.



Voucher Access Type Configuration

Important Points to Remember

- Vouchers can only be generated after enabling Vouchers and creating at least one Voucher plan.
- A maximum of 50,000 Vouchers per portal can be created on cnMaestro.

> **Note**
>
> User is allowed to add only 1000 vouchers at a time. In order to create 50,000 vouchers user needs to add 50 times.

- A maximum of 1,000 Vouchers per portal can be created on cnMaestro Cloud (https://cloud.cambiumnetworks.com/).
- Total number of generated Vouchers = Vouchers Unclaimed + Vouchers Claimed + Vouchers Expired.
- The admin can export all/valid/current page Voucher codes as PDF/CSV document.

Voucher contains options to add new plans and Vouchers. Based on user requirements, the plans can be created with different validity and rate limits.

1. **Create a plan**

   - Navigate to **Network Services > Access Control Portal** page and select **Access Control** tab.
   - Enable **Vouchers.**
   - Click **Add New Plan** button. The window with general and design parameters for the plan is displayed.

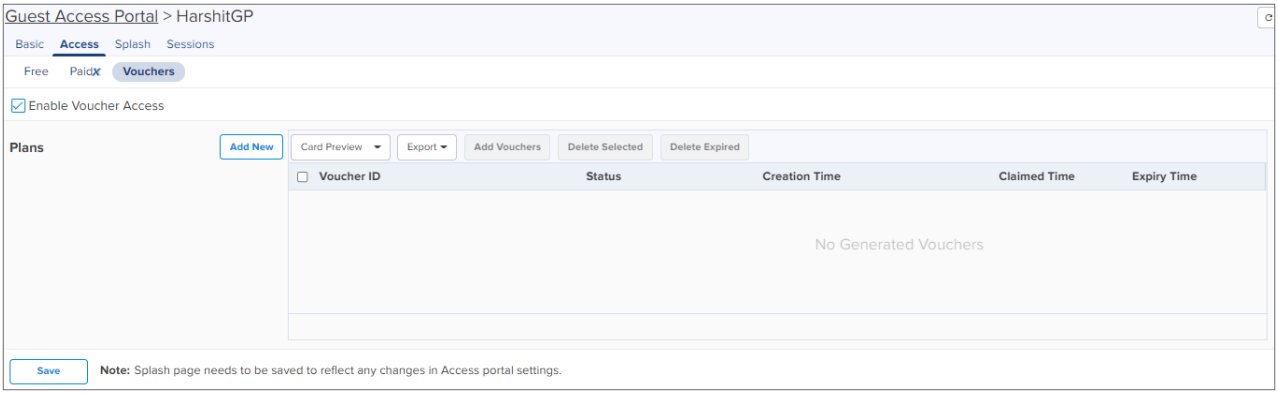


Table 126 *Voucher Access Type Parameters*

Parameter	Description
Design	• **Color:** There are options to modify colors for the title, message, code, and background. • **Background Image:** You can browse and select a background image for this page. • **Title:** The title of the voucher plan. • **Message:** Detailed information about the plan. • **Access Code Message**: 8 digit access code will be provided to use the voucher. With all the above parameters, administrators can create their own design for the card with text, color, and message to be displayed on card.
General	• **Name**: The name of the plan. • **Session Duration:** The duration for which the client is allowed network access. • **Voucher Expiry**: The expiry time for the generated Vouchers. Once this time lapses, the Vouchers cannot be used. • **Client Rate Limit**: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied. • **Voucher Device Limit**: Limit the devices to use the voucher.



2. Once a plan is configured, Vouchers can be generated for it. Each Voucher is a unique, randomized alphanumeric code.

Figure 489 *Select a plan*

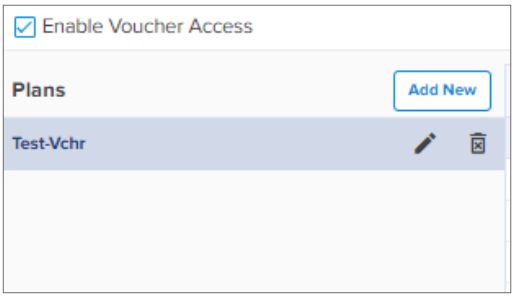
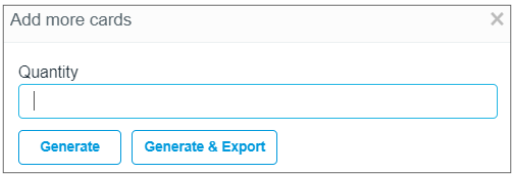


Figure 490 *Add Vouchers*



3. Once the plan is created and the Vouchers are generated, the following page is displayed.

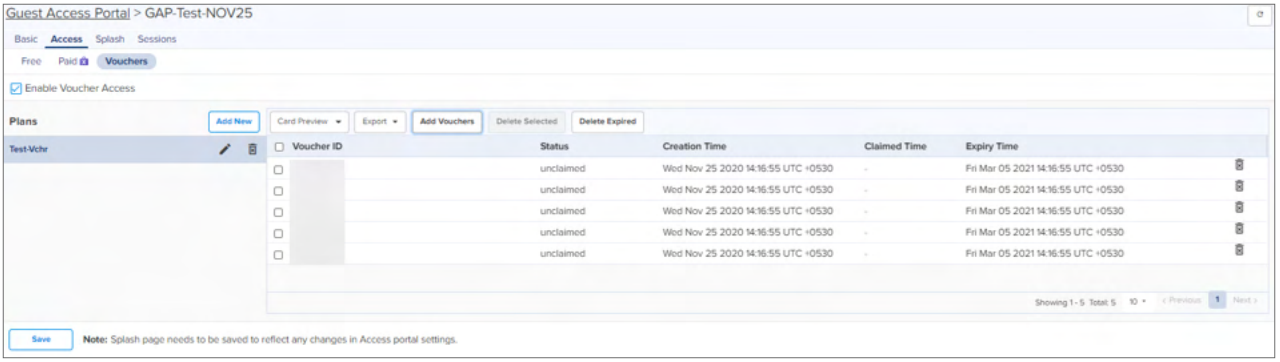


Figure 491 *Sample Voucher Code*



Note

The modified values in the Access Portal page is reflected on the design page only when the design page is saved after making the changes.

Design Page

The Design page refers to the page to which a wireless client is redirected when it connects to the guest portal. Administrators can create their own Design page by modifying the default logo, background, and text to be displayed in the Design page with different colors and fonts.

- If **Free** is selected in **Access Portal**, the client only sees free access related parameters.
- If **Voucher** is selected in **Access Portal**, the client only sees Voucher related parameters with a text box to enter the **Voucher code**.
- If both **Free** and **Voucher** are selected, then the client sees both Free and Voucher related parameters.

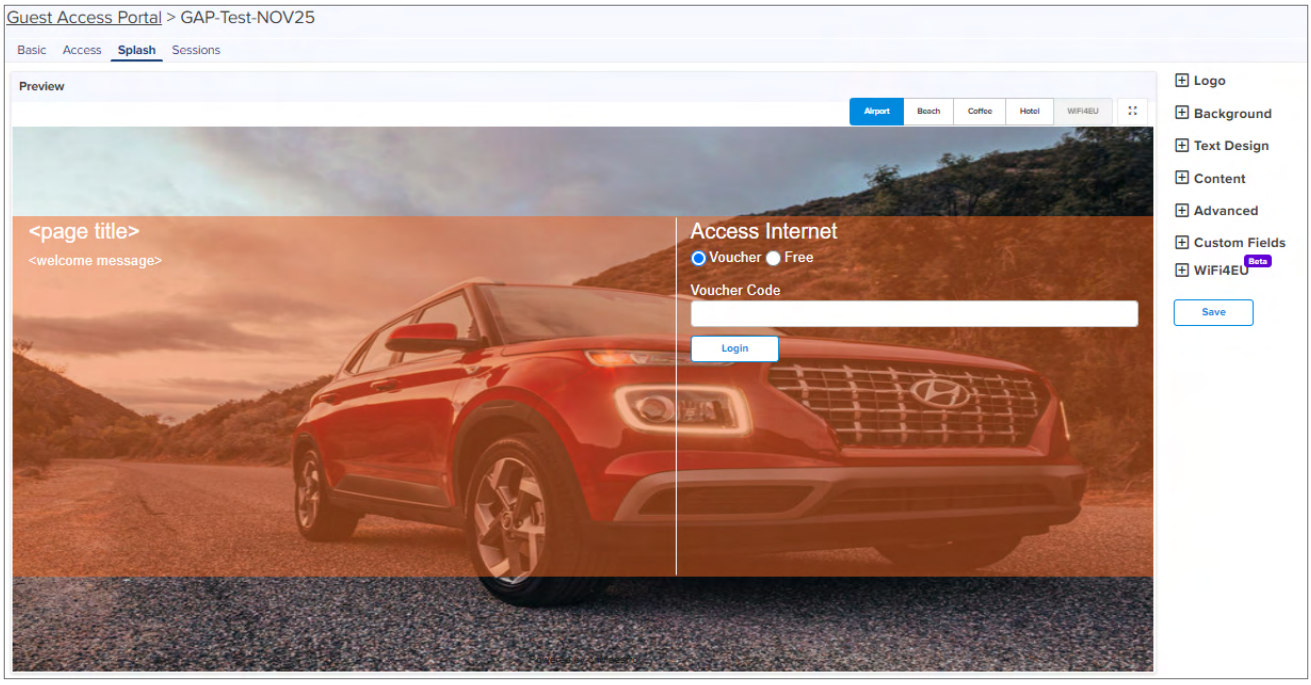


Table 127 *Design Page Parameters*

Parameter	Description
Accept Terms Message	Text to appear as the accept terms message.
Advanced	Expand **Advanced** option. Browse and select the advanced fields.
Background	Browse and select the image that needs to be displayed as the background. • Recommended image resolution—1024 pixels × 800 pixels

Table 127 *Design Page Parameters*

Parameter	Description
	• Maximum supported image file size—5 MB • Supported file formats—JPEG, JPG, PNG, and GIF
Background Placement	Choose the option from the drop-down for placing the background image in the **Design** page.
Custom Fields	Expand **Custom Field** option. The user can customize the fields in the **Design** page by choosing the **Custom Field** option in the **Guest Access Portal** page and clicking **Add New** button.
Enter Voucher Code Message	Enter the text to appear in **Voucher Code Message**.
Free Label	Enter the text that should appear on the **Free Label**.
Login Button	Enter the text that should appear on the window to submit.
Login Failure Message	Message to appear when any error occurs during login.
Login Success Message	Message to appear after successful login.
Login Title	Title of the login section.
Logo	Browse and select the logo that needs to be displayed on the **Design** page. • Recommended image resolution—300 pixels × 50 pixels • Maximum supported image file size—3 MB • Supported file formats—JPEG, JPG, PNG, and GIF
Message	Text to appear as the welcome text. You can choose the font style and size for the welcome text.
On Success Redirect to URL	Enter the URL to be redirected to a page, such as Google, Twitter, and Facebook.
Opacity	The transparency of background image.
Page Title	Text to appear as the title of the page. You can choose the font style and size for the title.
Please wait Message	Text to appear in the waiting screen.
Repeat Background	Enable the check box if you want the background image to be repeated.
Select Plans Label	Enter the text to appear in the label to select plan.
Server Error Message	Text to appear if there is an error while contacting server.
Terms and Conditions Title	Text to appear as the title for the terms and the conditions.
Terms and Conditions	Text to appear as the terms and conditions.
Terms Agree	Text to appear in the terms agree button.

Table 127 *Design Page Parameters*

Parameter	Description
Button	
Terms Cancel Button	Text to appear in the terms cancel button.
Text Design	Choose the appropriate colors for the background, logo in the background, content area, and for the text.
Voucher Code	Enter the text to appear in Voucher Code, Voucher Label, Enter Voucher Code Message, and Voucher Code Error Message.
Voucher Code Error Message	Enter the text to appear in Voucher Code Error Message.
Voucher Label	Enter the text to appear in Voucher Label.
Failure	Enter the text to appear in Google Authentication Failure Message, Twitter Authentication Failure Message, and Facebook Authentication Failure Message.
WIFI4EU	WiFi4EU provides free, high-quality Internet access only across the European Union.

WIFI4EU

WiFi4EU provides free, high-quality Internet access across the European Union. Administrators can enable the WiFi4EU checkbox to provide access to the free internet.

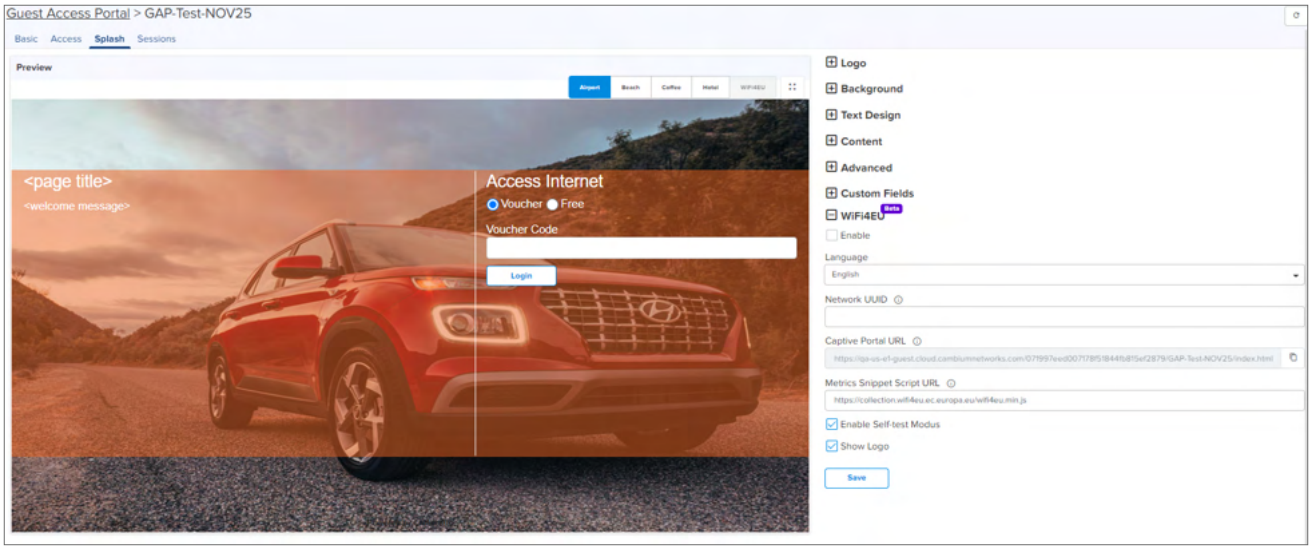


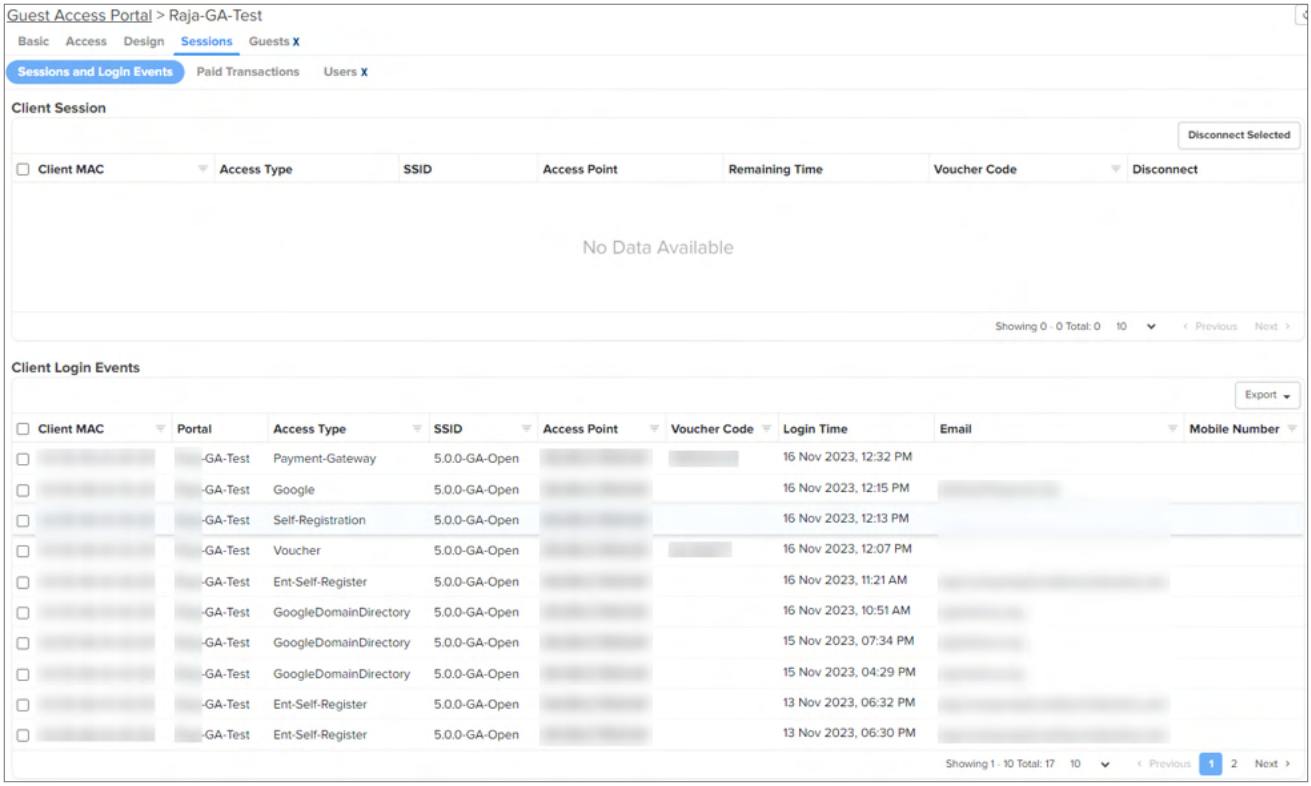
Table 128 *WiFi4EU Parameters*

Parameter	Description
General	• **Network UUID**: Universally Unique Identifier (UUID) that the EC attribute is generated when the network installation is created in the Installation. • **Language:** Allows to select the preferred language. • **Enable Self Test Mode**: Allows the browsers background script verification. • **Show Logo:** Displays the WiFi4EU logo provided by the European union.

Sessions

Sessions tab contains Client MAC address, Access Point MAC address, Access Type as Free (Google or Facebook) or Voucher, WLAN-SSID of client connected AP, Remaining time and Disconnect option.

Administrator can check how many clients are connected, Access Type (Free/Voucher) of the client, and can disconnect the clients.



Client Login Events table creates events of client login sessions. It maintains the login events for 7 days. This table has Client MAC address, Portal Name, SSID, Access point MAC, Voucher code (if client connected with Voucher), Access type (Google/Facebook/Voucher).

Admin can export the client login events as PDF / CSV.

Table 129 *Sessions Parameters*

Parameter	Description
Access Point	MAC address of the Access Point.
Access Type	Access type as Free or Voucher.
Client MAC	MAC address of the client.
Disconnect	Displays if the client is disconnected from the network.
Remaining Time	The time left for the client to access the Internet. It depends upon the session duration configured in the Access Portal.
Voucher	Displays the valid applied voucher.
WLAN	SSID of the network.

Note

For **Free** access method, the client MAC address is displayed even after the free session duration expires. Delete the MAC address of the client after the Renewable Frequency completes.

Users table displays details of users accessing the network using Enterprise Google-based access.

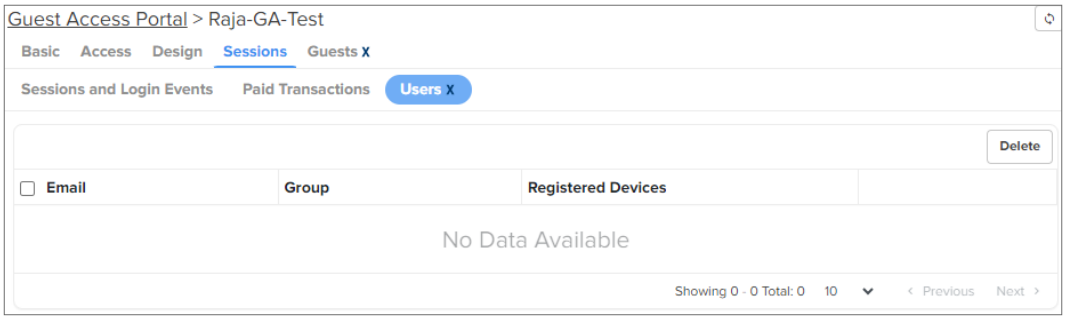


Table 130 *Users Table Parameters*

Parameter	Description
Email	Email address of the registered user.
Group	Name of the group to which the user belongs.
Registered Devices	MAC address of the registered devices.

Guests X

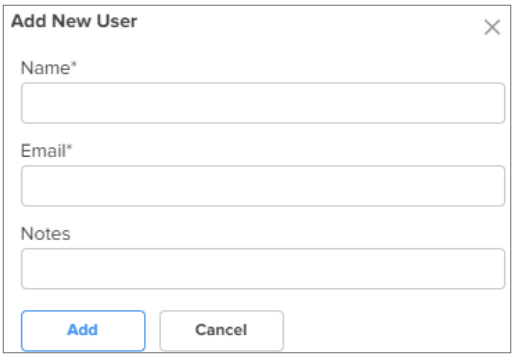
The Guests page allows you to view details of self registered guests connecting to the wireless network. However, to view this page, you must first enable and configure self registration under **Network Services > Guest Access Portal > Access Type > Enterprise X > Self Registration**.

You can also add new guest details on this page. These users can directly access the wireless network after entering the required details in the access portal.

To add a new user, complete the following steps:

1. Click **Add New** on the **Guests** page.

   The **Add New User** window is displayed.



2. Configure the name and email address of the guest in the **Name** and **Email** fields.

   Add a description, if required, in the **Notes** field.

3. Click **Add**.

   The details of the Enterprise self registered guests that are connected to the Wi-Fi network are displayed in

the table

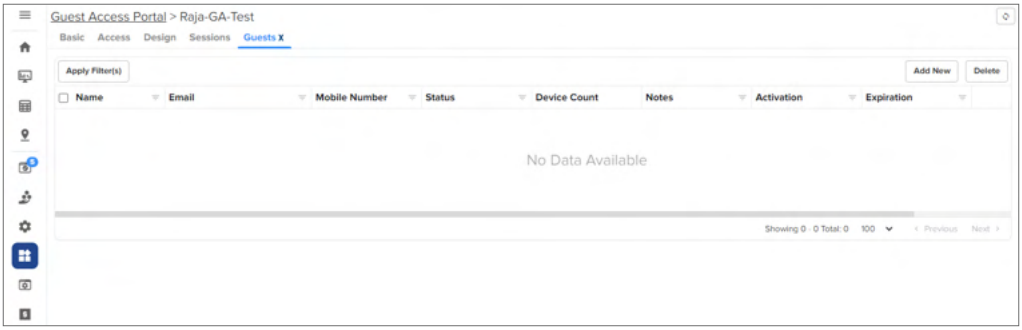


Table 131 *Guests Table Details*

Parameter	Description
Name	Name of the guest that was entered at registration.
Email	Email address of the guest.
Status	Displays the whether the guest is connected or offline.
Device Count	Displays the number of devices that the guest has connected to the network.
Notes	Displays the comments or description provided when adding the guest.
Activation	Displays the date and time when the guest first connected to the network.
Expiration	Displays the date and time when the guest disconnected from the network. For currently connected guests, this field displays the date and time of session expiration.

Mapping the device to Guest Access Portal in cnMaestro

The administrator needs to configure the name of the Guest Access Portal in the device which redirects the device to cnMaestro for client connectivity.

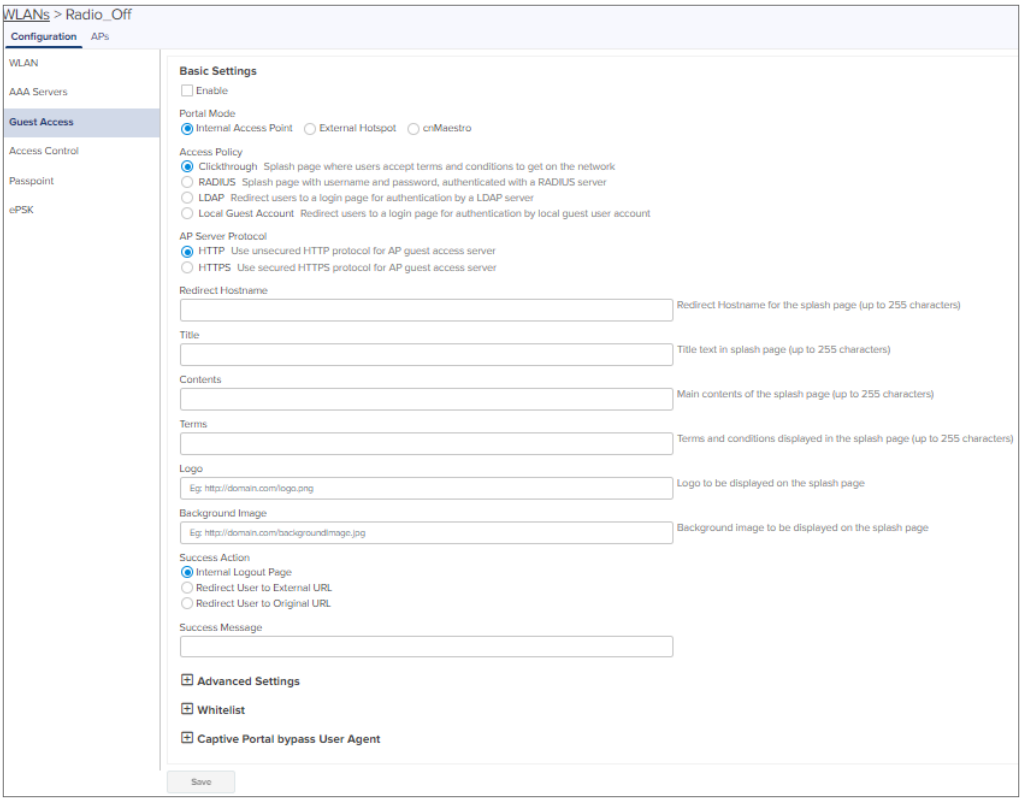
Note

The client gets the fully configured **Design** page for login only if the Access Point is onboarded to the server.

Configuration at device level

To configure the Guest Access at device level, perform the following:

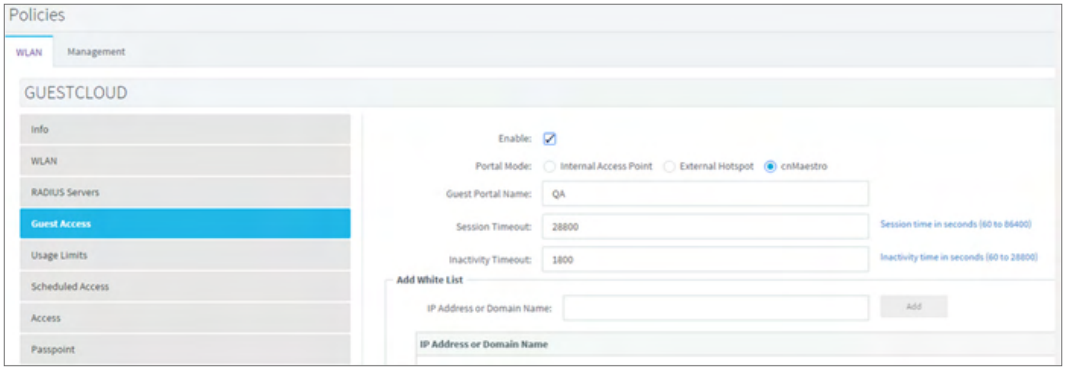
1. Login to the device.
2. Navigate to **Configuration** > **WLAN** > **Guest Access**.

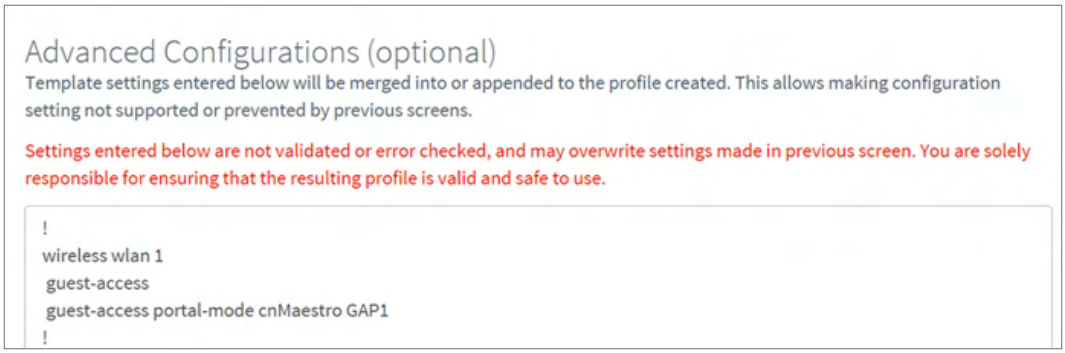


3. Enable the **Guest Access** check box.
4. Choose the **Portal Mode** radio as **cnMaestro**.
5. In the **Guest Portal Name** text box, select the name of the portal that was created in cnMaestro and enter the respective parameters.

Configuration at cnMaestro side

The administrator can push the configuration from cnMaestro through policy or advanced configuration.

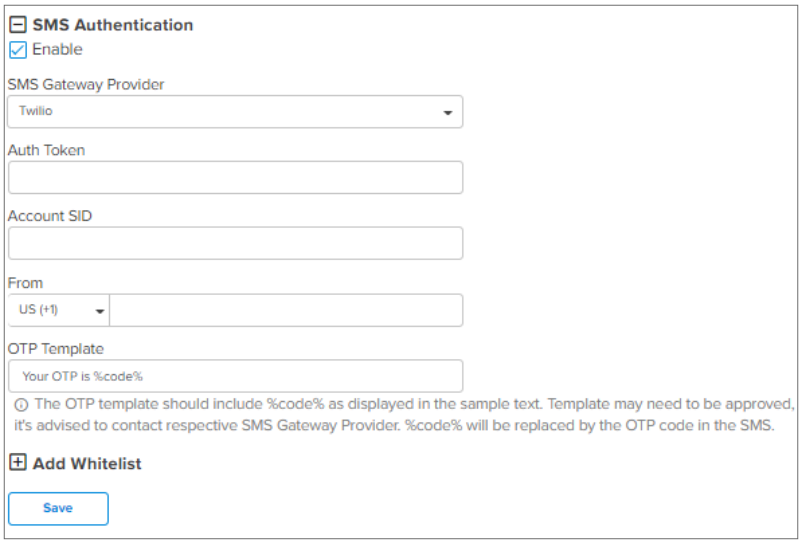




Access Types

The following table describes the parameters described in configuring SMS authentication parameters:

Parameter	Description	SMS Gateway Provider				
		Fast SMS	SMS Country	SMS Gupshup	Twilio	Victory Link SMS
Enable	It indicates to enable the SMS Authentication feature.	✓	✓	✓	✓	✓
Username	Indicates the username of the vendor.	✓	✓	✓	X	✓
Sender ID	It is the name or number which flashes on the recipients mobile phone when they receive SMS. This is Optional not mandatory.	✓	✓	✓	X	✓
API Key	It's a token which is provided by vendors.	✓	X	X	X	X
Account Type	It shows type of accounts such as International, OTP, Promotional and Transaction.	✓	X	X	X	X
OTP Template	The template with which SMS has to be sent.	✓	✓	✓	✓	✓
Password	It indicates the password.	X	✓	✓	X	✓
Country Code	It enables to select country code based on deployments.	X	✓	✓	X	X
Auth Token	It acts as a password.	X	X	X	✓	X
Account SID	It acts as a username.	X	X	X	✓	X
From	It enables to select the country code.	X	X	X	✓	X
Language	It indicates the Language.	X	X	X	X	✓



To configure SMS Authentication on cnMaestro, perform the following:

1. Enable SMS Authentication feature.
2. In SMS Gateway provider, select your required gateway from the drop-down.
3. Enter the **User Name**.
4. Enter the **Sender ID**. This field is optional. This allows user to send SMS through the ID which he chooses.
5. Enter **API Key**.
6. Select your **Account Type** from the drop-down.

7. Enter the **OTP Template**. The OTP template should include “%code%. %code% replaces the OTP code in the SMS.

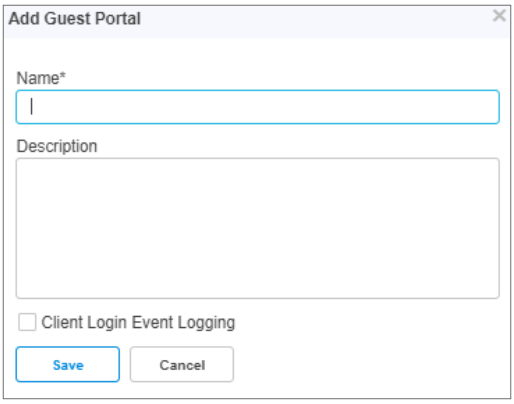
Guest Access using Social Login

Configuration

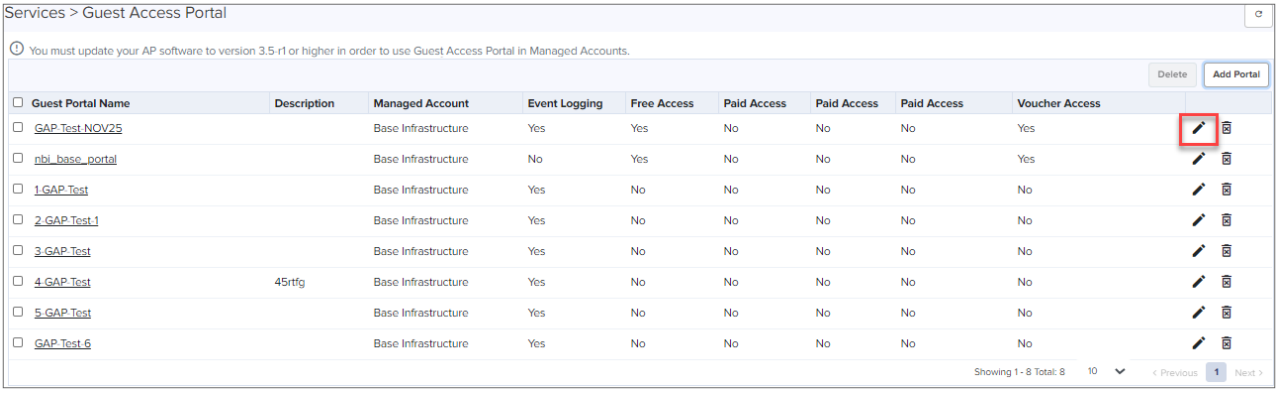
To achieve cnMaestro Guest Access using Social Logins like Google, Twitter, Facebook, and Office 365, perform the following steps:

To create Guest Access profile on cnMaestro, do the following:

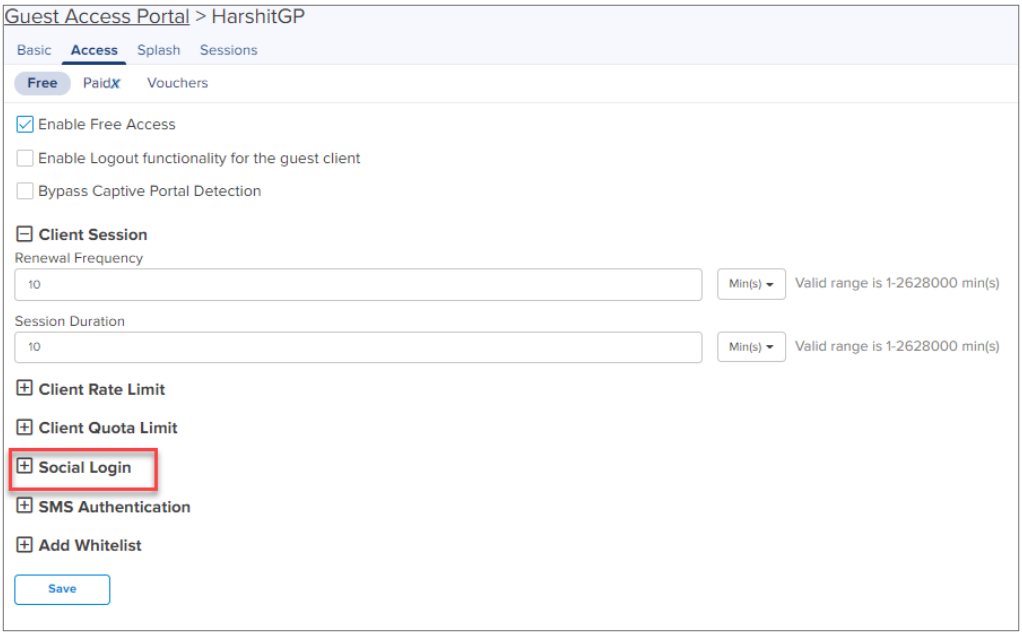
1. Login to cnMaestro and navigate to **Network Services > Guest Access Portal** > **Add Portal.**
2. Enter Portal Name, Description, enable logging for client login events.
3. Click **Save.**



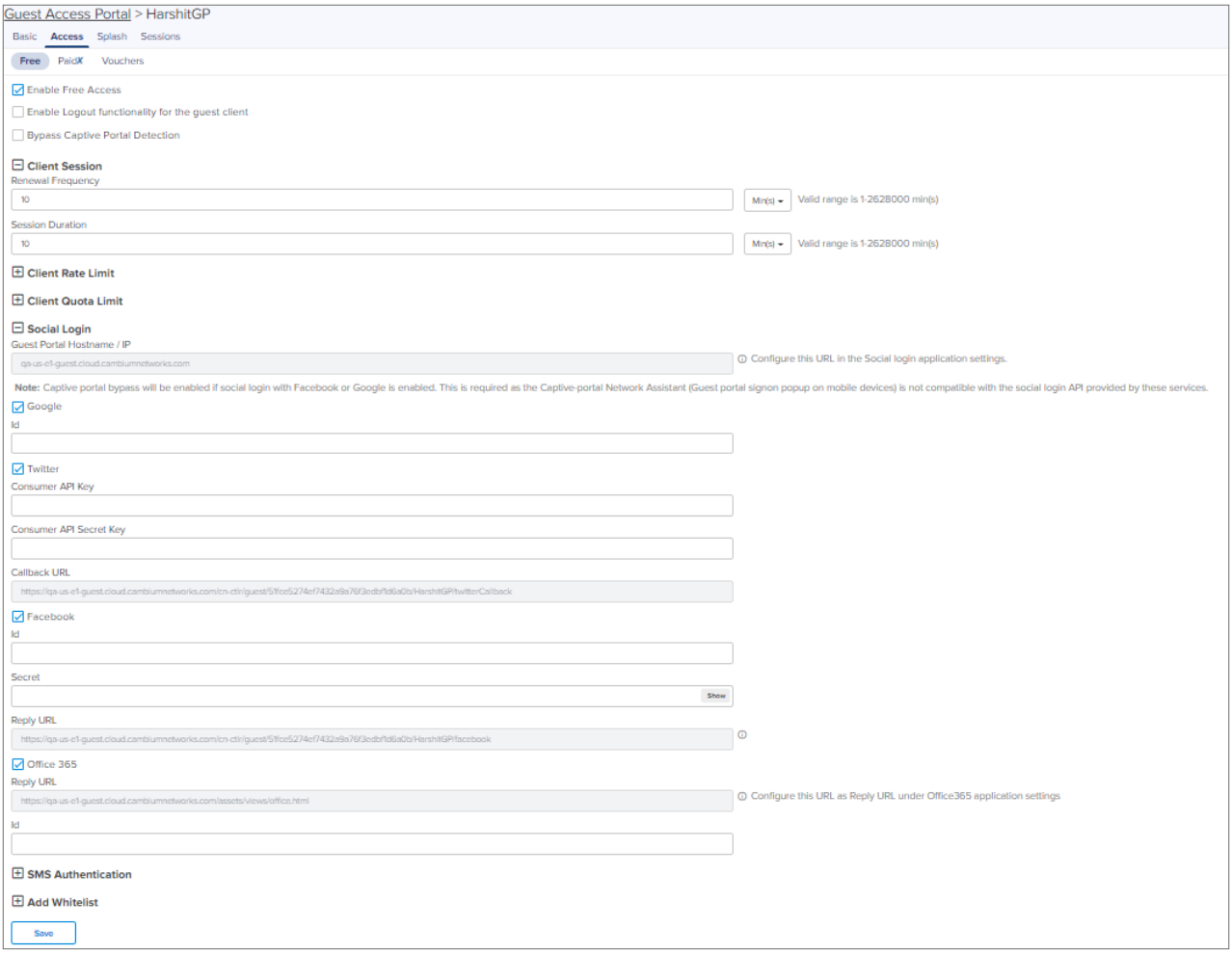
4. Click **Edit Guest Portal Details.**



5. Navigate to **Access** tab and expand **Social Login**.



6. Select Google, Twitter, Facebook, Office 365 based on your requirement.



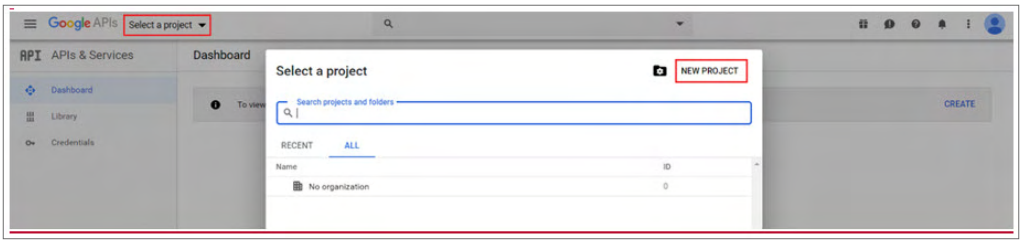
API Key Generation

Perform the following steps to create APIs for cnMaestro to integrate with Google, Twitter, Facebook, and Office 365:

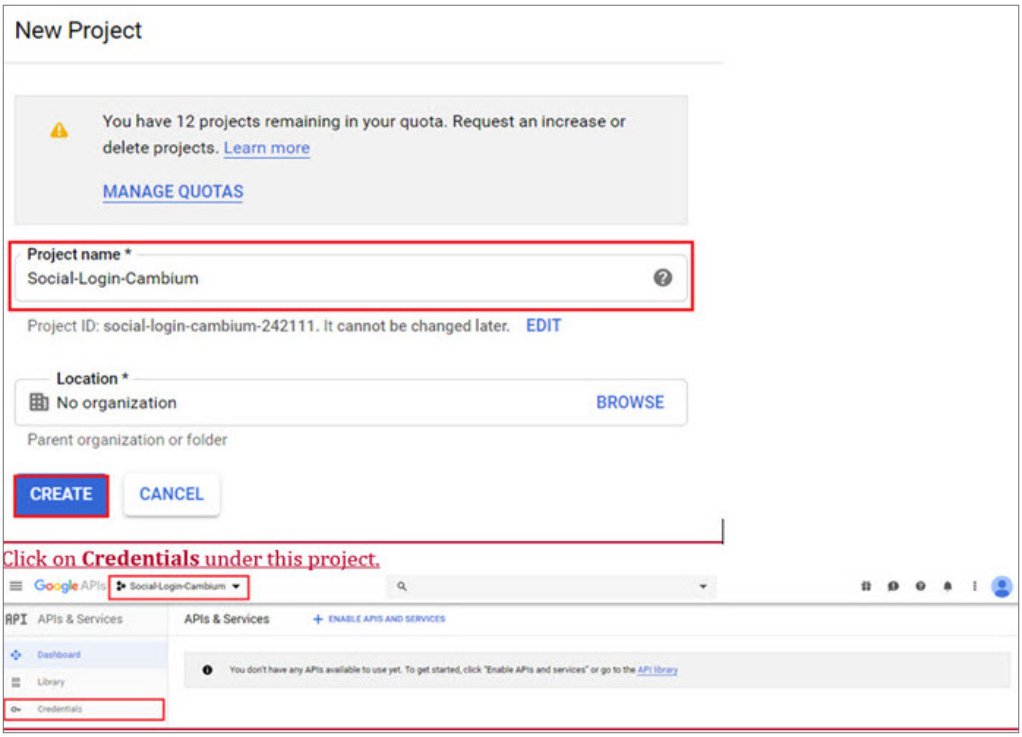
- Google
- Twitter
- Facebook
- Office 365

Google

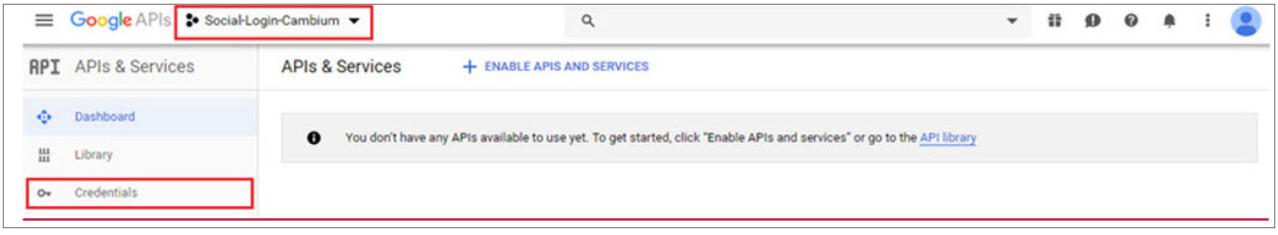
1. Login to Google Account and navigate to https://console.cloud.google.com/.
2. Click **Select a Project** and create a **New Project.**



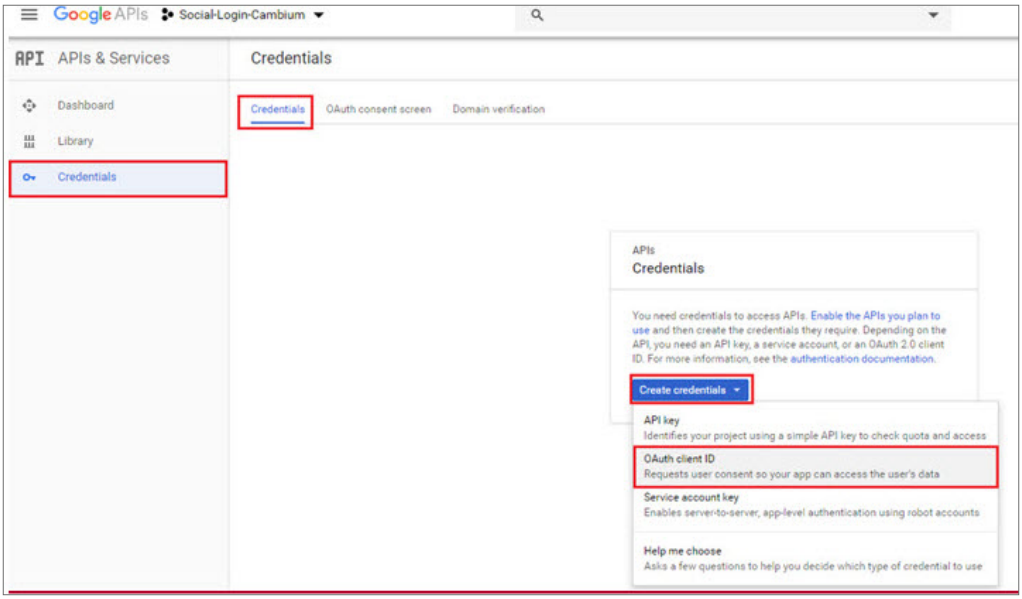
3. Give a name to the Project and click **CREATE**..



4. Click **Credentials** under this project.



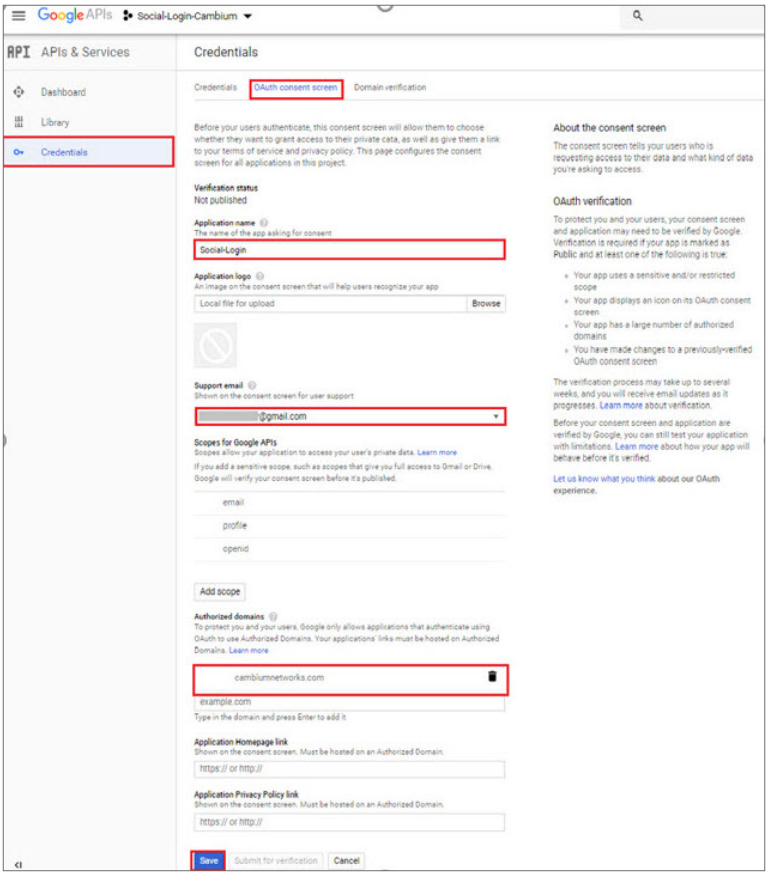
5. Under **Credentials** tab, create OAuth Client ID.



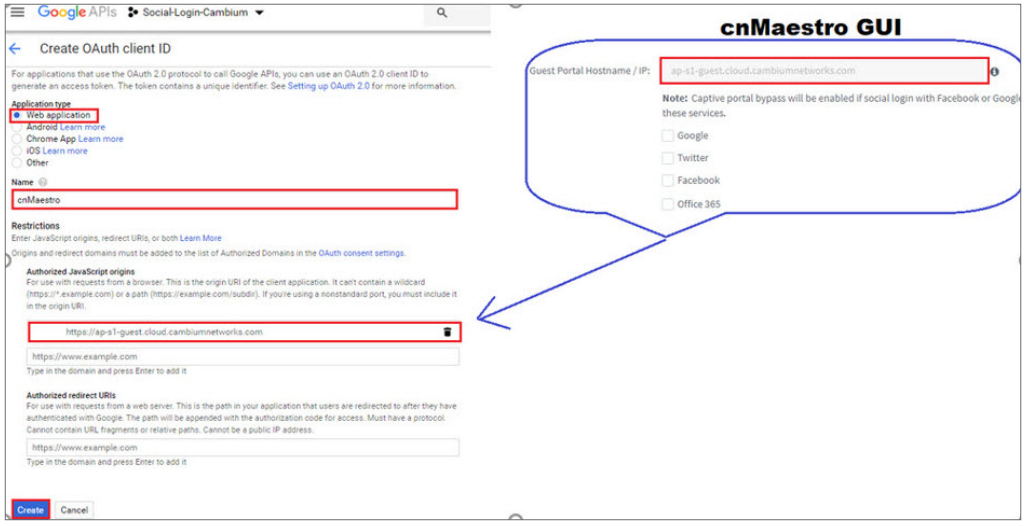
6. Click **Configure Consent Screen**



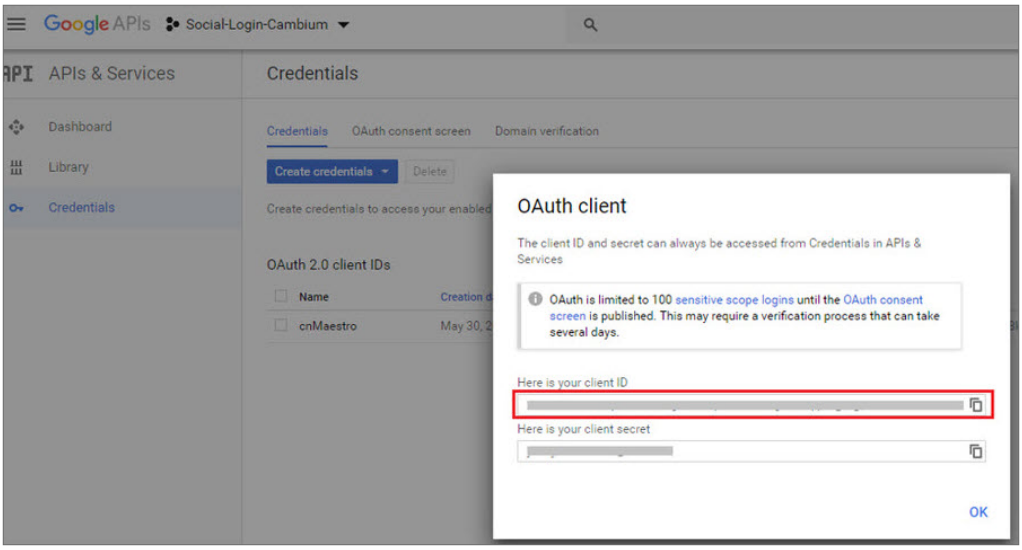
7. Assign a name to the application, map to an email address, add cambiumbnetworks.com to the authorized domain and click **Save**.



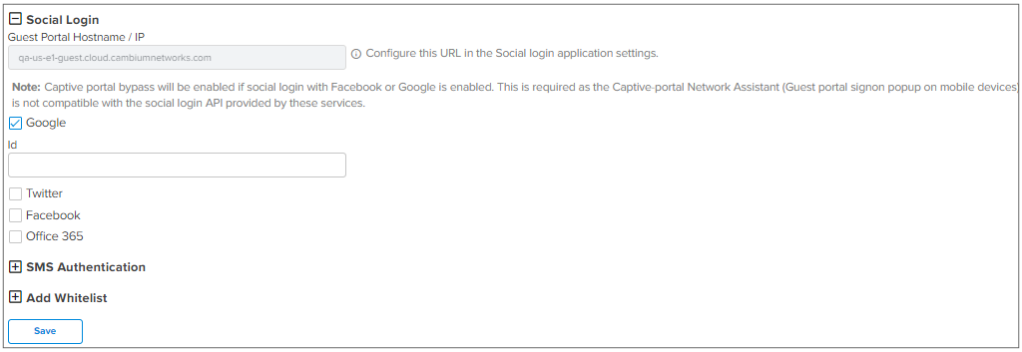
8. Once clicked **Save** for above page it redirects to creation of OAuth Client ID.
9. Select **Application type** as **Web Application**, give a Name, add Guest Portal Hostname URL/IP which you will get from cnMaestro UI and click **Create**.



10. Clicking Create on above page it redirects to the screen showing Client ID and Client Secret.

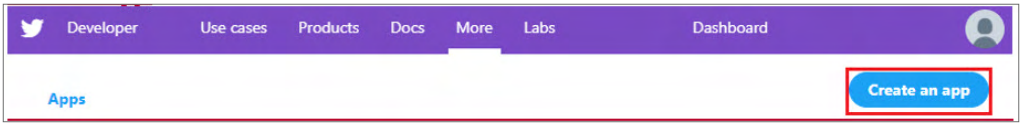


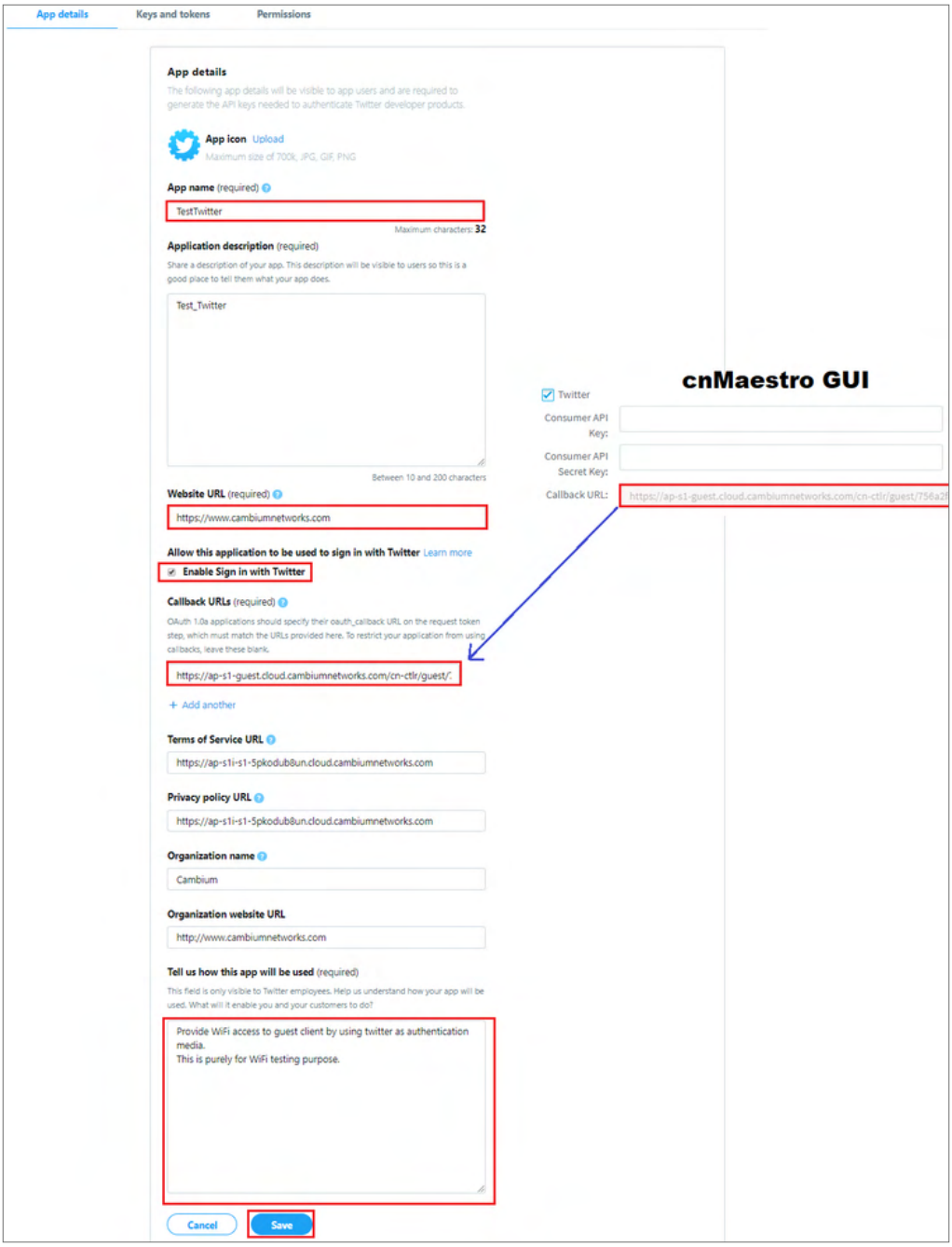
11. Copy the Client ID and paste it to the cnMaestro enabling Google under Social Logins and click **Save**.



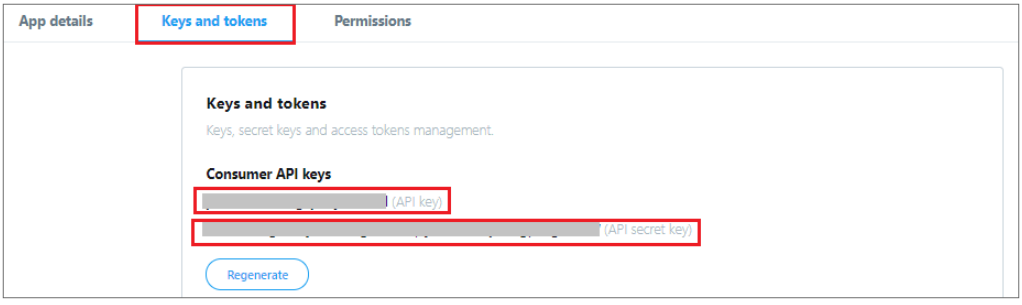
Twitter

1. Login to Twitter Account and access **https://developer.twitter.com/en/apps** and click **Create an app**.

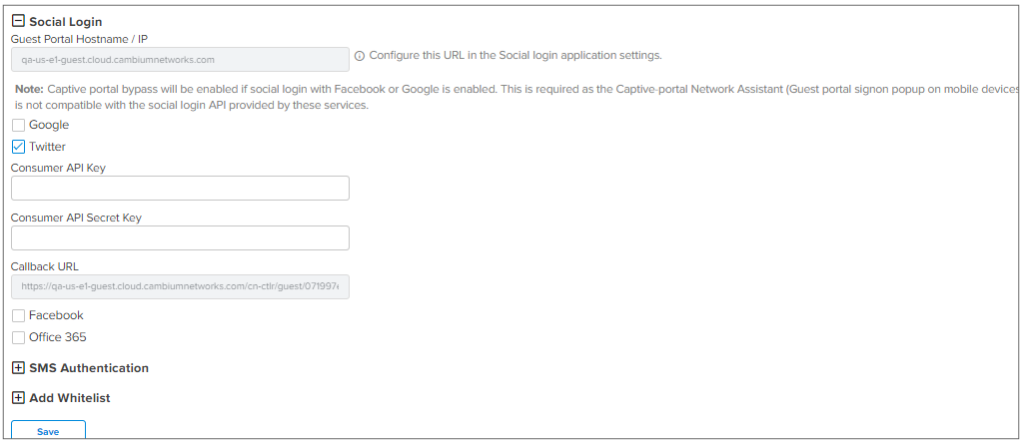




2. Click **Keys** and **Tokens** and copy **Consumer API Key** and **Consumer API Secret Key**..

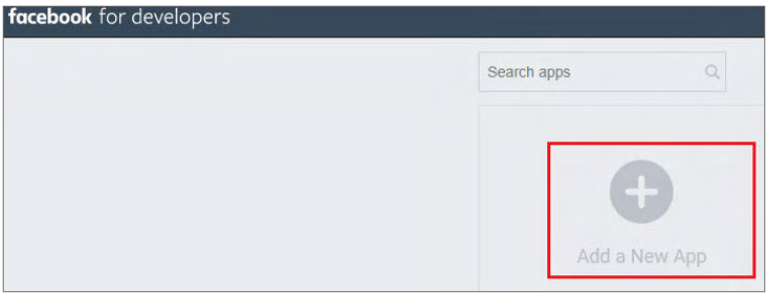


3. Paste them to cnMaestro GUI for Twitter social login.

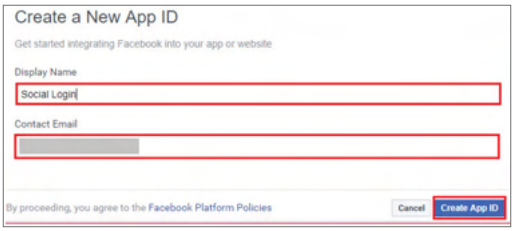


Facebook

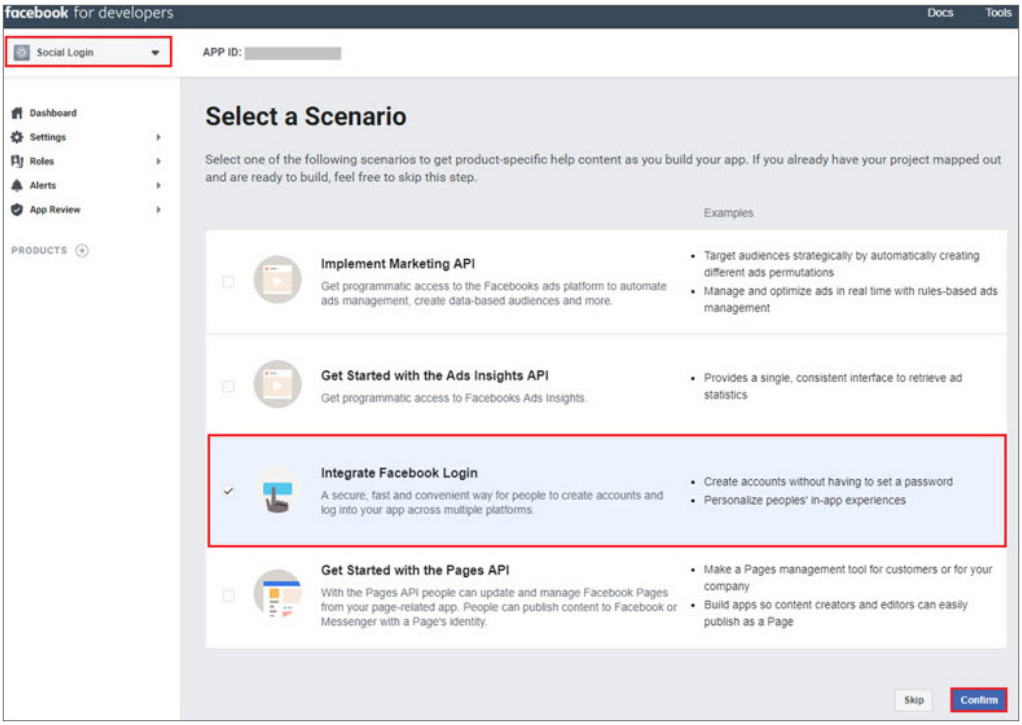
1. Login to Facebook Account and access **https://developers.facebook.com/apps/** and click **Add a New app**.



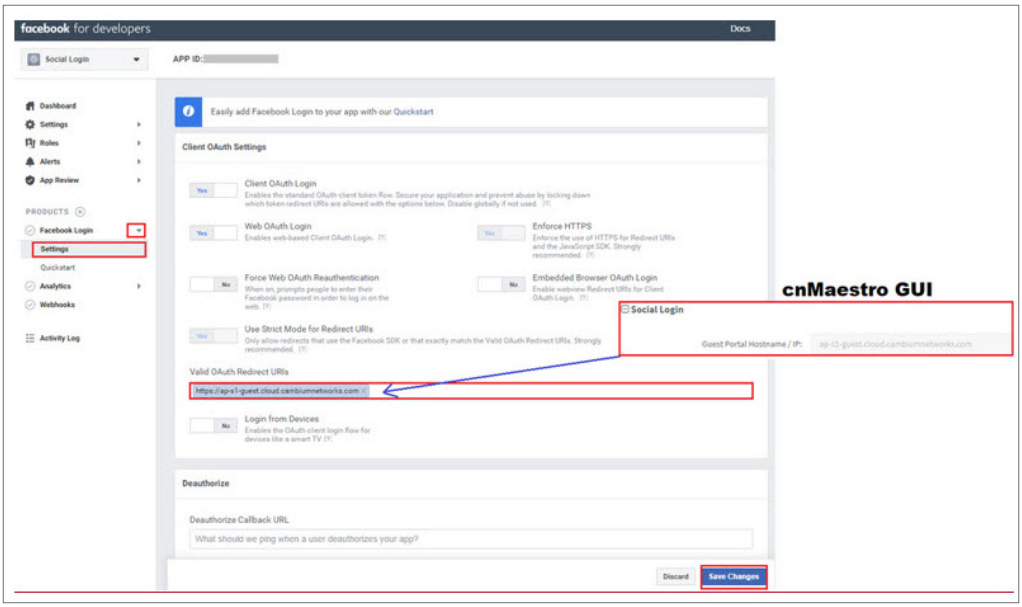
2. Enter App **Display Name**, **Contact Email**, and click on **Create App ID**.



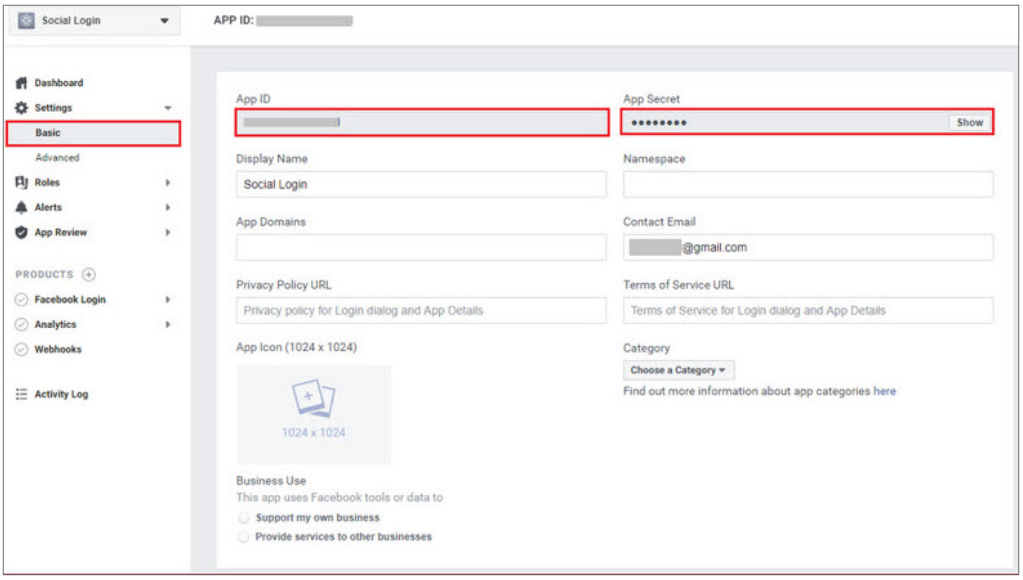
3. Select a Scenario as Integrate Facebook Login and click **Confirm.**

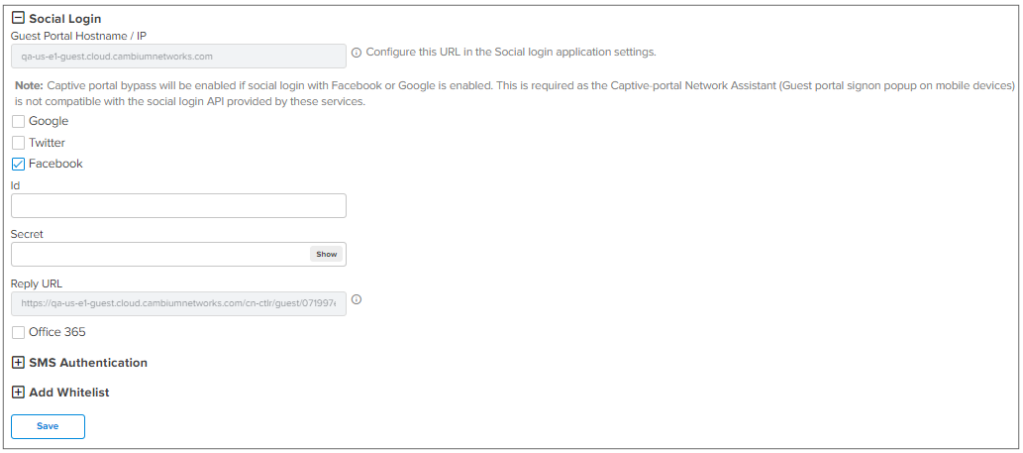


4. Navigate to **Settings** tab under Facebook Login and add Guest Portal Hostname from cnMaestro to Valid OAuth Redirect URLs section and click **Save Changes**.



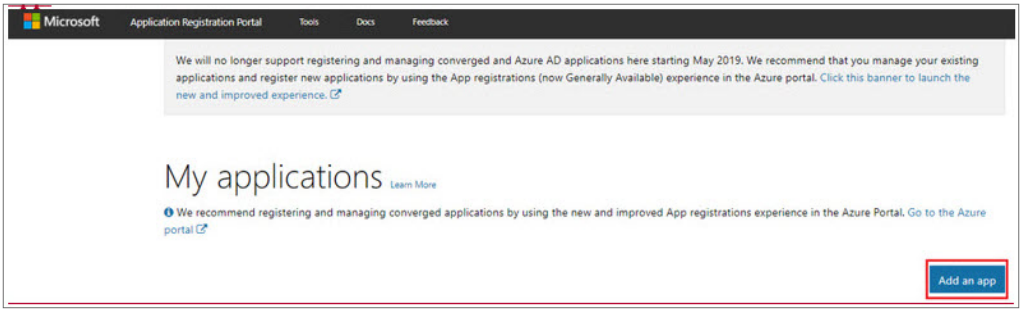
5. Navigate to **Settings** > **Basic** and copy **App ID** and **App Secret**.

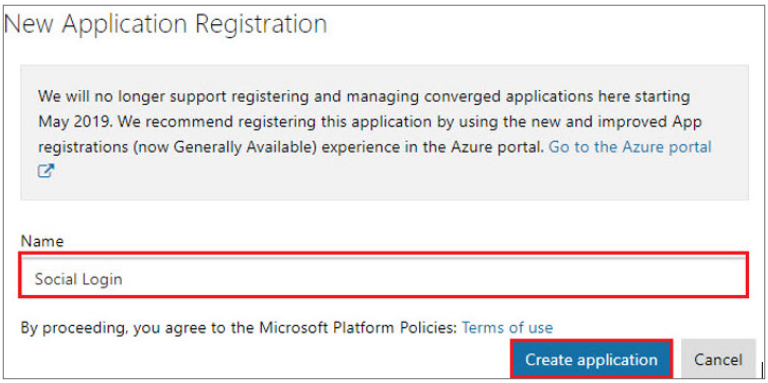




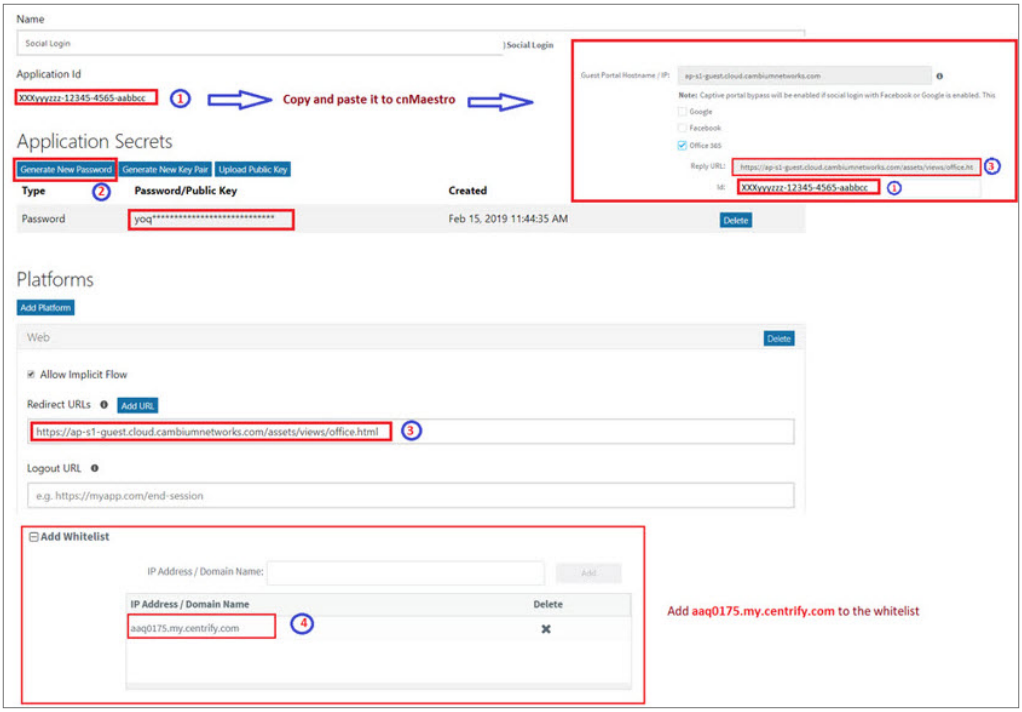
Office 365

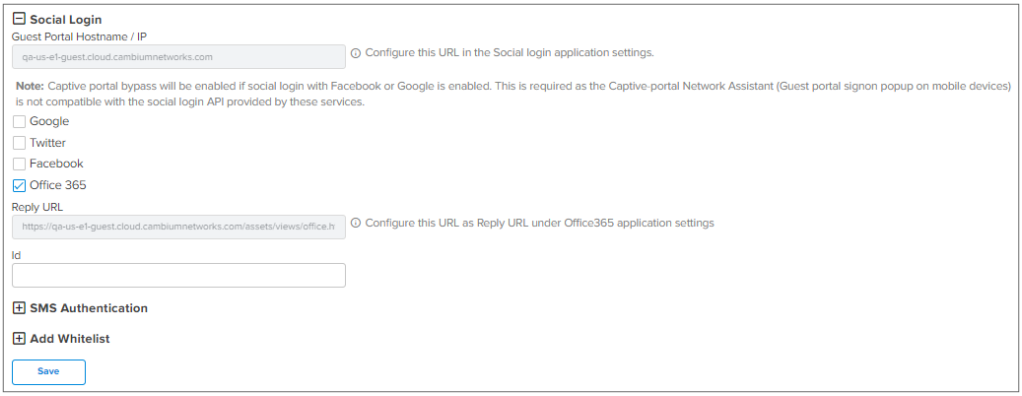
1. Login to Office 365 Account and access https://apps.dev.microsoft.com/ and click **Add an app**.





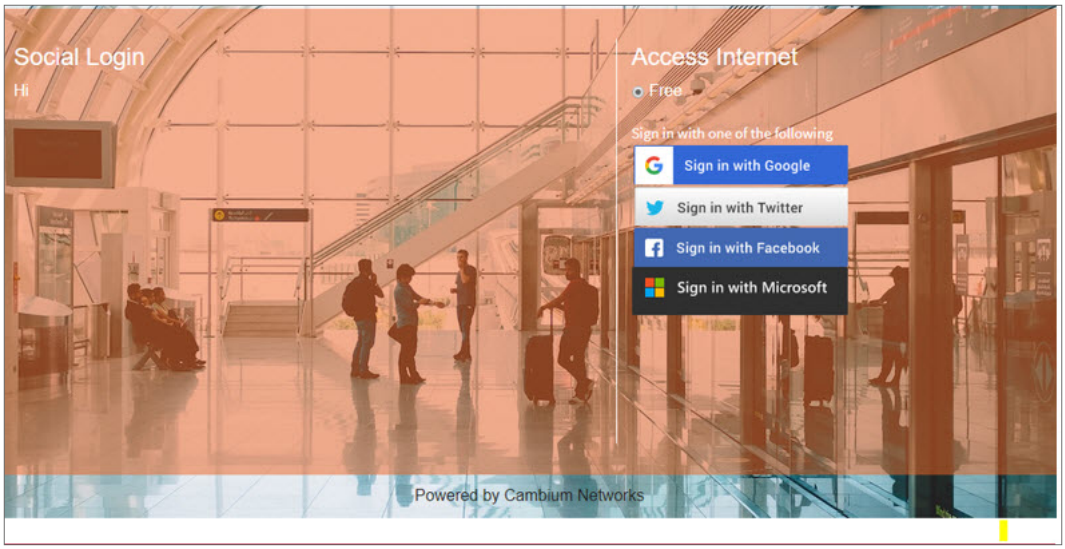
2. Upon Adding your App name and clicking Create application, it redirectes to App page.
3. Copy Application ID and paste it to cnMaestro Guest Access page under Office 365.
4. Click **Generate New Password**.
5. Copy Reply URL from cnMaestro and paste it under Redirect URLs.
6. Add my.centrify.com to the Whitelist on the cnMaestro.





Sample Template

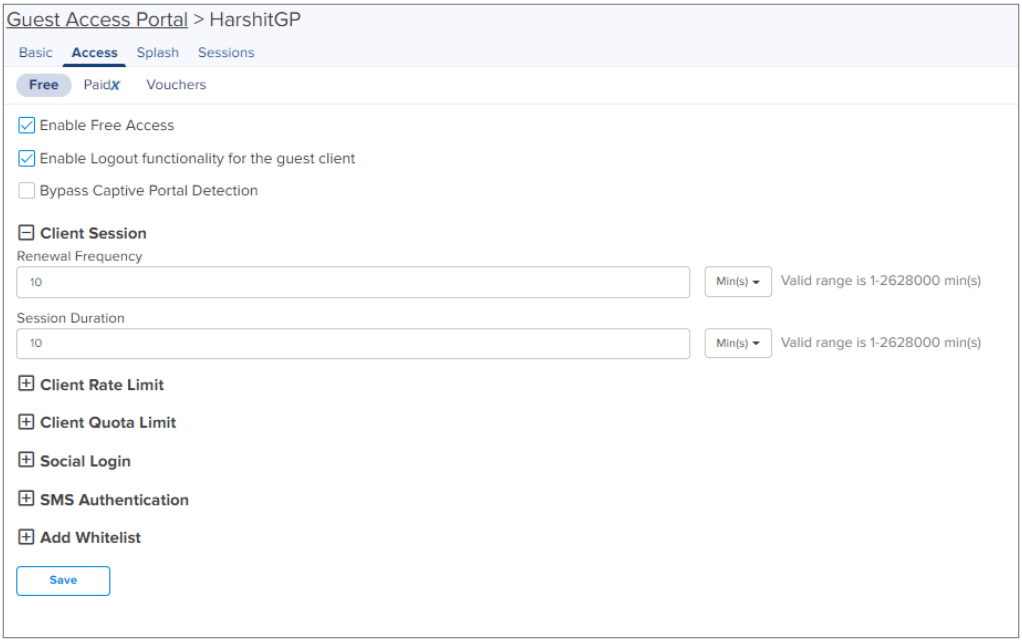
Sample of client login page is displayed below:



Guest Access Portal Logout

To logout from cnMaestro Guest Access Portal perform as follows:

1. Navigate to **Services > Guest Access Portal** page and select the respective **Guest Portal Name**.
2. Select **Access** tab.
3. Select **Enable Logout functionality for the guest client** check box.
4. Click **Save**.



The users can access and use the Guest Access Portal at any time within the specified **Renewal Frequency** and **Session Duration** provided.

SMS Authentication

The gateway provider sends a text SMS containing the OTP to the end user's phone number. Once OTP is received the client can enter the OTP and get Internet access.

Twilio, SMS Country, and SMS Gupshup are the SMS gateway providers that support the SMS OTP. Also there is a generic SMS gateway option, which provides flexibility to configure any preferred SMS gateway by cnMaestro users. Configuring SMS Gateway through this generic SMS gateway does require a little more involvement to review the integration specifications of the given SMS gateway. Please follow the guidelines as mentioned on the Generic SMS Gateway configuration section.

Generic SMS Gateway configuration

SMS Service providers expose a SMS API which typically works over HTTP GET or HTTP POST requests. Most of the SMS Gateways use username and password in the API requests to validate a given SMS send a request and some use special authorization token in the HTTP Headers.

Apart from that many API have specific tokens that need to be passed into the request along with the authentication part. To start off one has to first go through the SMS API document of the given SMS provider and understand all components do that need to be provided in the HTTP request and then build the corresponding cnMaestro configuration.

In general, all SMS API documents show example curl commands which can be used to create an SMS request with the server. Curl examples demonstrate the required components in the request and help to find the right configuration for the cnMaestro Guest Portal Generic SMS API.

The cnMaestro Generic SMS API configuration is split into multiple components which makes it easy to configure the static and the dynamic parts of the SMS API request. It also provides a way to handle the SMS API response and validate the API success or failure case. To handle the reply type, refer the **Advanced** options.

SMS Gateway provider name

Provide the SMS Gateway name which is used for reference purposes. This is not part of API request so please provide a meaningful name to identify this SMS Gateway service provider.

HTTP Request type

Based on the SMS gateway provider and the API document information, identify the SMS API. The SMS API uses HTTP GET or HTTP POST requests for communication with the SMS gateway server.

Example HTTP GET API request

https://smsapiserver.com/service/sms/send?user=xxx&password=yyyyy&message="Your OTP is ABCD"&mobileNumber=123456789&dnd=yes&sid=SenderID&v=1.1&messagType=N

Curl command to do HTTP GET request

```
Curl -v https://smsapiserver.com/service/sms/send?user=xxx&password=yyyyy&message='Your OTP is ABCD'&mobileNumber=123456789&dnd=yes&sid=SenderID&v=1.1&messagType=N
```

Example HTTP POST request

HTTP POST URL

https://smsapiserver.com/service/sms/send

HTTP POST Form Content

user=xxx&password=yyyyy&message="Your OTP for Internet Access is QW123"&mobileNumber=123456789&dnd=yes&sid=SenderID&v=1.1&messagType=N

Curl command to do HTTP POST request

```
curl -v “https://smsapiserver.com/service/sms/send” -H "Content-Type: application/x-
www-form-urlencoded" -X POST \
--data-urlencode 'user=xxx' \
--data-urlencode 'passwd=yyyyy' \
--data-urlencode 'mobilenumber=1234567789' \
--data-urlencode 'message=Your OTP for Internet access is QW123' \
--data-urlencode 'sid=Sid' \
--data-urlencode 'v=1.1' \
--data-urlencode 'mtype=N' \
--data-urlencode 'dnd=yes' \
--data-urlencode 'DR=Y'
```

If the SMS Gateway is using an authorization token, then below example curl request shows how the **Authorization** field is added into a HTTP header.

```
curl -v -H "Authorization: Bearer nZYIoU7QoUxfD03ct1CC2YvInqI7DmUAH6RYz01K1" \
"https://smsapiserver.com/service/sms/send?\
from=Test&\
to=123456789&\
message=’Your OTP for Internet access is QW123’&\
format=json"
```

All the SMS API have components as follows:

- Static components which are part of the request.
- Two dynamic components which are part of the mobile number, to which the SMS needs to be sent and the message which contains the OTP.

Static components

API URL

Based on the above curl request example the URL configures as https://smsapiserver.com/service/sms/send where the request needs to be sent.

API URL information

From the example curl request please find the static components of the URL. Based on our above example this configures as user=xxx&password=yyyyy&dnd=yes&sid=SenderID&v=1.1&messagType=N.

Remove the message and mobile number query strings from that URL and configure the rest. This is what a static component is for a given SMS API so identify what all options are required for the SMS API request and add it in the format: key1=value1&key2=value2....

HTTP request header key

Based on the above example, If the SMS Gateway Provider API uses some HTTP header field like authorization token, etc. The corresponding HTTP header field name will be configured as **Authorization**.

HTTP request header key value

Based on the above example, the SMS gateway API configuration settings expose some authorization token or auth token, and the provided HTTP header key value will be configured as Bearer nZYIoU7QoUxfD03ct1CC2YvInqI7DmUAH6RYz01K1 in this configuration.

Dynamic components

Message parameter name

From the example curl request or the SMS gateway provider the parameter name used for the message key component where the OTP is added. It could be something like message|text|msg or whatever custom parameter name is used for sending the message component.

For example curl request, we have used “message” and this is what configures based on the example curl request.

Mobile number parameter name

From the example curl request or the SMS gateway provider the parameter name used for the mobile number key component where the OTP has to be sent. It could be something like To|mobile|mobile number or whatever custom parameter name is used for sending the mobile number component.

In our example curl request, we have used mobile number and this is what configures based on the example curl request.

Advanced options

If you care for adding functionality for parsing the SMS API response on the cnMaestro and find if the request was successful or if the server returned an error. Then one can use this advanced configuration to let cnMaestro parse the SMS API reply.

The usual HTTP response code is anyway handled by default and this advanced config parses the reply content is configured. This should be configured by advanced users only and in case if there is any failure seen in SMS functionality then disable this and report the issue to Cambium Networks support.

Reply type

The SMS gateway API sends back a response to let the client know about the request results, this result could be in text format or in json/xml format. So based on the SMS API document select the reply type here as **TEXT**.

Success

Configure the text to match the success case as follows:

- Typically, servers may respond with a text message in reply like success or sent, then configure the exact message which should be matched in the response.
- If a server response is like success, sent message to xxxxx, then configure just success which matches in the reply.

Error

Configure the text which matches the failure case as follows:

- Typically, servers may respond with a text message in reply like **Error** or **Failure**, then configure the exact message which should be matched in the response.
- If a server response is like **ERROR**, failed to send SMS to xxxxx, out of credit, then configure just **ERROR** which matches in the reply to mark it as an error.

Reply Type JSON

JSON reply success key name

Please look for the SMS gateway provider API document in detail and find the JSON examples for the reply and identify the key which contains the successful response status value.

cnMaestro guest portal generic SMS supports nested JSON too and one has to configure the complete path for the given result key which contains the SMS message sent status. Example JSON replies are given below to be configured for this configuration:

Example 1

```
{
  "messages": {
  "to": "123456789",
  "status": {
  "id": 0,
  "groupId": 0,
  "groupName": "ACCEPTED",
  "result": [
 {
  "status": "MESSAGE_ACCEPTED"
 }
],
  "description": "Message accepted"
 },
  "smsCount": 1,
  "messageId": "2250be2d4219-3af1-78856-aabe-1362af1edfd2"
 }
}
```

Success key name to be configured based on the above example messages.status.result[0].status.

Example 2

```
{
  "count": 1,
  "list": [
 {
  "id": "1460978572913968440",
  "points": 0.16,
  "number": "48500500500",
  "date_sent": 1460978579,
  "submitted_number": "48500500500",
  "status": "QUEUE"
  }
 ]
}
```

Success key name to be configured based on the above example list [0]. Status.

Example 3

```
{
 "status": "Sent"
}
```

Success key name to be configured based on the above example is status.

JSON reply success key value

The success status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message successfully sent or successfully queued, which is also a success case that the queued message sents out shortly.

Based on our examples the status or the result field can be mapped to multiple values like as follows:

- Sent
- Queued
- Success
- Message Accepted

So in this configuration one can add multiple such values that should be matched for the success case for the value as received for the JSON reply success key name field.

JSON reply failure key name

Look for the SMS Gateway Provider API document in detail and find the JSON examples for the reply and identify the key which contains the Error/Failure response status value.

cnMaestro guest portal generic SMS supports nested JSON too and one has to configure the complete path for the given result key which contains the SMS message sent failure field. Example JSON replies are given below to be configured for this configuration:

Example

```
{
  "invalid_numbers": [
{
  "number": "456456456",
  "submitted_number": "456456456",
  "message": "Invalid phone number"
  }
],
  "error": 13,
  "message": "No correct phone numbers"
}
```

JSON reply failure key name to be configured based on the above example is error.

JSON reply key value

The error/failure status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message sent error or multiple error codes for the corresponding error.

Based on our examples the error can be mapped to multiple values like 13|12|-1 etc. So in this configuration, one can add multiple such values which should be matched for the failure case for the value as received for the JSON reply failure key name field. reply type **XML**.

Reply type XML

XML reply success element

Look for the SMS gateway provider API document in detail and find the XML examples for the reply and identify the elements which contain the successful response status value.

cnMaestro guest portal generic SMS supports nested XML too and one has to configure the complete path for the given result element which contains the SMS message sent status. Example XML replies are given below to be configured for this configuration:

Example 1

```
<items>
<item id="0001" type="result">
<status>Success</status>
</item>
```

```
</items>
```

Success Element Name to be configured based on the above example is items/item/status.

Example 2

```
<?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://tempuri.org/">-11</int>
```

Success Element Name to be configured based on the above example.

XML reply success element value

The success status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message successfully sent or successfully queued, which is also a success case that the queued message sents out shortly.

Based on our examples the status or the result field can be mapped to multiple values like as follows:

- Sent
- Queued
- Success
- Message Accepted

So in this configuration one can add multiple such values that should be matched for the success case for the value as received for the XML Reply Success Element field.

SMS message sent failure field. Example XML replies are given below to be configured for this configuration:

Example 1

```
<items>
<item id="0001" type="result">
<error>-12</status>
</item>
</items>
```

XML Reply Failure Key Name to be configured based on the above example is items/item/error.

Example 2

```
<items>
<item id="0001" type="result">
<status>Error</status>
</item>
</items>
```

XML Reply Failure Key Name to be configured based on the above example is items/item/status.

Example 3

```
<?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://tempuri.org/">-11</int>
```

XML Reply Failure Key Name to be configured based on the above example is int.

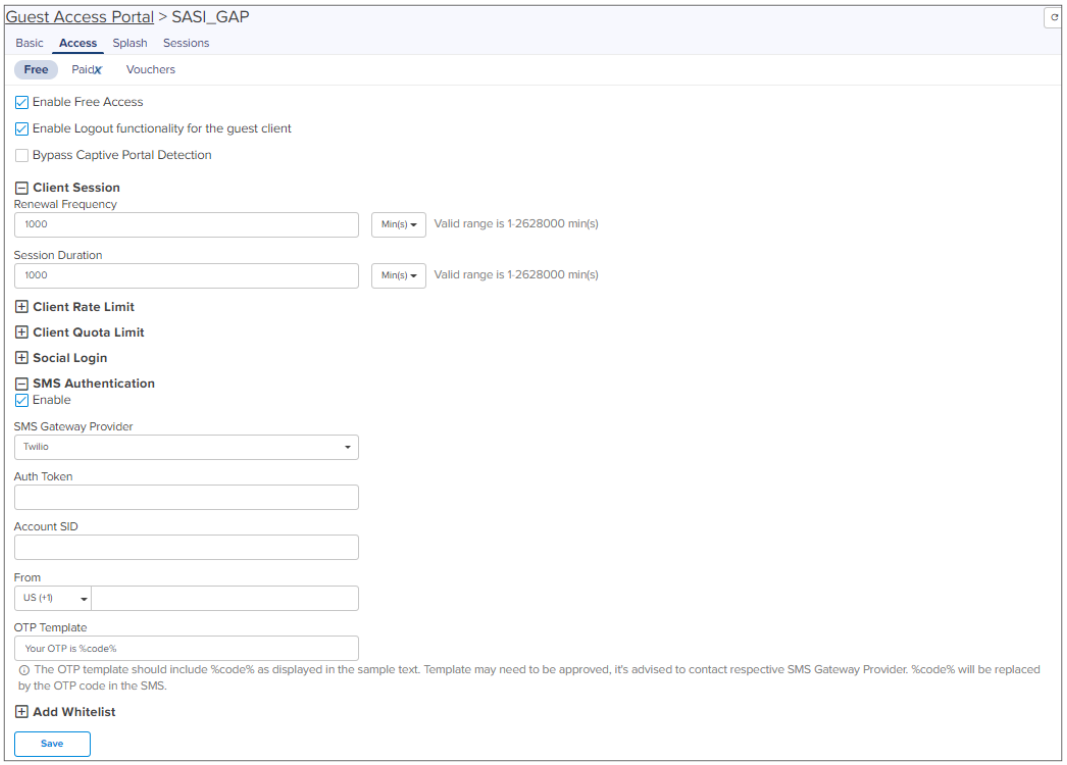
XML reply failure element value

The error/failure status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message sent error or multiple error codes for the corresponding error.

Based on our examples the error can be mapped to multiple values like 13|12|-1 etc so in this configuration, one can add multiple such values which should be matched for the failure case for the value as received for the XML reply failure element field.

Sample configuration in the cnMaestro

Figure 492 *: Guest Access Portal*



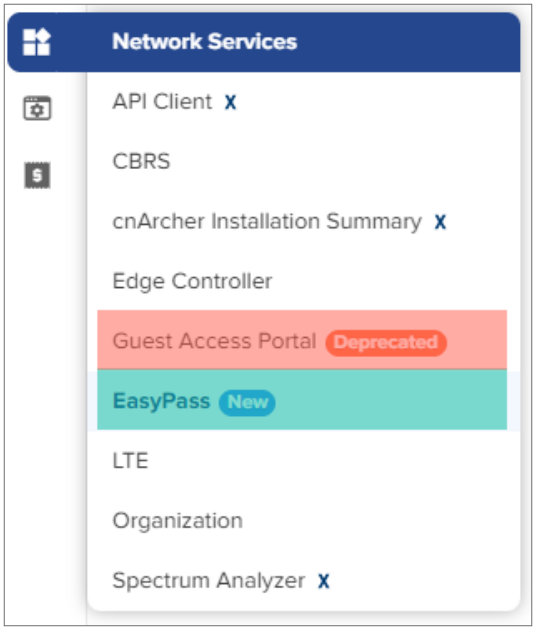
EasyPass

cnMaestro supports a guest access solution which provides an intuitive interface for various guest access methods used in the customer deployments. It allows the clients to connect to the internet through free tiers, vouchers, or paid access types. It also creates a separate network for guests by providing internet access to wireless devices such as mobile phones, tablets, and laptops.

Note

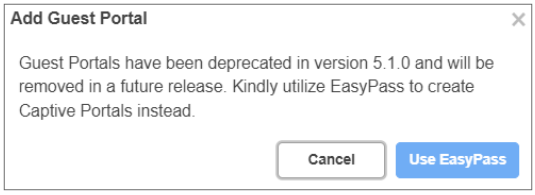
From cnMaestro 5.1.0 release onwards, the **Guest Access Portal** configuration wizard is deprecated and a new wizard, **EasyPass**, is introduced (as shown in Figure 493).

Figure 493 *Network Services > EasyPass*



When you create a new portal in the **Guest Access Portal** page, a window appears notifying that guest portals are discontinued and **EasyPass** must be used (as shown in Figure 494).

Figure 494 *The Add Guest Portal window*



The EasyPass access services provide secure and controlled access to users and visitors on your Wi-Fi network.

Table 132 lists the supported devices and their compatibility with EasyPass.

Table 132 *List of supported devices - EasyPass*

Device	EasyPass support
Wi-Fi 5	Yes **Note**: Azure and GSuite are not supported.
Wi-Fi 6	Yes
Wi-Fi 7	Yes
Xirrus APs	No

EasyPass portal types are grouped into the following categories:

- Guest/Public Access
- Employee/Student Access
- Combined

Each category serves a different purpose and provides distinct features to accommodate various user requirements and access levels.

Guest/Public Access

This category includes the following portal types:

- One Click— All guests have access after agreeing to terms of use without needing to create an account. The **Social Login** options are integrated with One Click.
- Self Registration X— Guests must register themselves when connecting to the Wi-Fi network for the first time. The administrator can configure the self-registration process to determine whether sponsor approval is required. The sponsor approval can also be configured as manual or automatic confirmation. Additionally, the **SMS Gateway Provider** option is available as a self-registration method.
- Sponsored Guest X— Guests must provide their email address and their sponsor's email address to request internet access.
- Voucher— Users can access the network using a pre-assigned voucher. A voucher allows network administrators to create unique guest keys in bulk for retailers, hotels, conventions, and enterprises providing temporary visitor Wi-Fi access. These keys can be exported into a CSV file and integrated with other systems as point-of-sale (POS), property management, ticketing, or registration systems. Voucher also allows administrators to set a device limit for guests. If a guest tries to connect with more devices than allowed, the system alerts the guest with a warning message. Guests can manage their devices by deleting some of the device accounts without IT assistance.
- Paid X— IP Pay and Quickpay payment methods allow users to purchase internet services using a credit card. For purchasing internet plans, users are directed to a portal where they purchase the plan and then they are automatically redirected to the guest access portal where the purchased voucher is displayed. The users must save the voucher information if they use it on multiple devices.
- WiFi4EU— Provides free internet access only across the European Union (EU) to citizens and visitors through free-of-charge Wi-Fi hotspots in public spaces such as parks, squares, administrations, libraries, and health centers.



Note

X indicates that the feature is available only in cnMaestro **X**.

Employee/Student Access

This category includes the following portal types:

- Microsoft Azure X—A single sign-on process allows seamless access to Microsoft Azure X by integrating Wi-Fi and authentication.
- Google Login X—A single sign-on process allows seamless access to Google Login X by integrating Wi-Fi and authentication.



Note

Azure and Google Workspace are available on 6.x and later versions supporting firmware AP.

Combined

This category includes the following portal types:

- One Click + Voucher—Combines the benefits of both One Click access and voucher-based promotions, providing users with an easy and cost-effective way to access services.
- One Click + Paid X—Combines the benefits of One Click access with paid access to services.
- Voucher + Paid X—Combines the benefits of voucher-based promotions and paid access to services.

Note

- Using **Essentials**, you can create a maximum of four EasyPass portals.
- Using **cnMaestro-X**, you can create a maximum of 500 EasyPass portals.

Implementation of EasyPass portals for various types of users

Table 133 lists the various types of users for whom the EasyPass portals can be implemented or best suited:

Table 133 *Implementation of EasyPass portals for various types of users*

EasyPass portal type	BYOD Employee or Student	Co-working Space User	Business Visitor	MDU Resident	Residence Hall Student	Hotel Guest	Retail Customer	Convention/Fair Attendee	Sports Event Fan	Public Wi-Fi user
Self Registration X		✔				✔	✔	✔	✔	✔
Sponsored Guest X			✔							
Voucher			✔			✔	✔	✔		
One Click							✔	✔	✔	✔
Paid X		✔				✔		✔		✔
WiFi4EU										✔
Microsoft Azure X	✔				✔					
Google Login X	✔				✔	✔				

EasyPass configuration

You can configure EasyPass using the cnMaestro UI. The EasyPass configuration process involves the following tasks:

- Creating a portal
  - Creating One Click portal
  - Creating Self Registration X portal
  - Creating Sponsored Guest X portal
  - Creating Voucher portal
  - Creating Paid X portal
  - Creating WiFi4EU portal

- Creating Microsoft Azure X portal
- Creating Google Login X portal
- Creating One Click + Voucher portal
- Creating One Click + Paid X portal
- Creating Voucher + Paid X portal

- Configuring common parameters
  - The Basic screen parameters
  - The Limits screen parameters
  - The Design screen parameters
  - The Voucher screen parameters
  - The Plans screen parameters

- Accessing the common tabs
  - Sessions
  - Guests
    - Adding a new guest user
  - Vouchers
  - Paid Transactions X
  - Users X

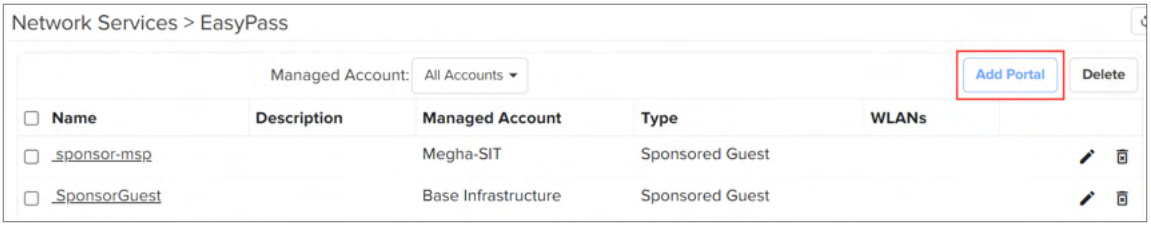
Creating a portal

Complete the following steps to create a portal:

1. From the home page of cnMaestro UI, navigate to **Network Services** > **EasyPass**.

   The **Network Services** > **EasyPass** screen appears.

   Figure 495 *The EasyPass screen*



2. Click the **Add Portal** button.

   The **Select Portal Type** window appears.

   Note

   The options in the **Select Portal Type** window are different for **cnMaestro Essentials** and **cnMaestro X**.

   Figure 496 displays the options available for cnMaestro Essentials.

Figure 496 *The Select Portal Type window—cnMaestro Essentials*

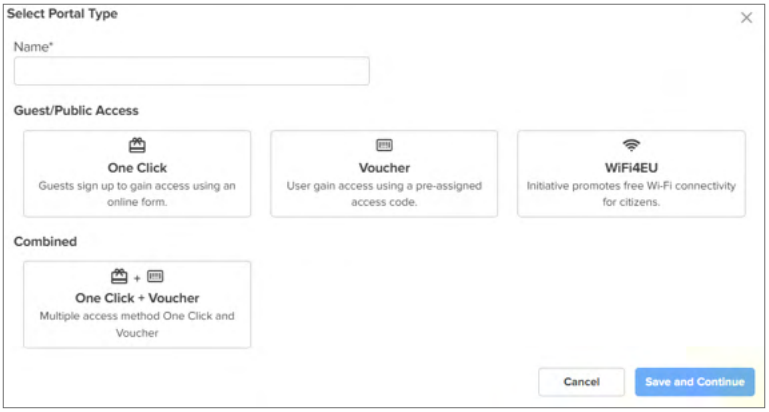
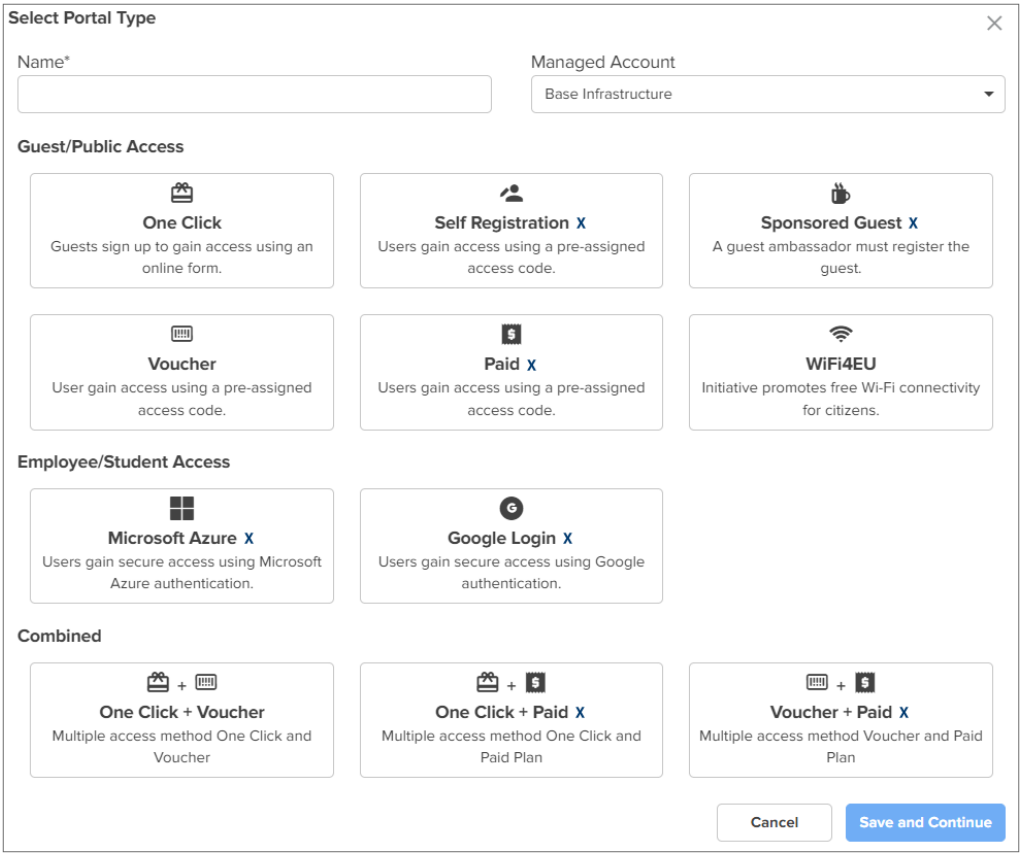


Figure 497 displays the options available for cnMaestro X.

Figure 497 *The Select Portal Type window—cnMaestro X*



Note

The **WiFi4EU** option is applicable only to users in the EU region. Users from Asia-Pacific (APAC), Americas, and other non-EU regions do not have access to this option.

3. In the **Name** field, enter a name for the portal. For example, **test1**.

   A name once created for the portal cannot be changed.

   The **Name** field supports:

- A minimum of five and maximum of 64 characters.
- Only alphanumeric, underscore (_), and dashes (-).

4. Select the required option from the **Managed Account** drop-down list. For example, **Base Infrastructure**.



Note

- When creating the EasyPass service, select the required managed account to which the service must be mapped.

5. Select the required option from the **Select Portal Type** window.
6. Click the **Save and Continue** button.

   The portal is created and the **Basic** screen appears.

   For information on parameters of the **Basic** screen, see The Basic screen parameters.
7. Click the next tab.

   Depending on the option you select, you will either see a **Limits** screen or portal-specific screen.

   - For a **Self Registration X** portal type, follow the additional steps described in Creating Self Registration X portal.
   - For the **Sponsored Guest X** portal type, follow the additional steps described in Creating Sponsored Guest X portal.
   - For the **Voucher** portal type, follow the additional steps described in Creating Voucher portal.
   - For the **WiFi4EU** portal type, follow the additional steps described in Creating WiFi4EU portal.
   - For the **Microsoft Azure X** portal type, follow the additional steps described in Creating Microsoft Azure X portal.
   - For the **Google Login X** portal type, follow the additional steps described in Creating Google Login X portal.
8. Configure the parameters of the **Limits** screen.

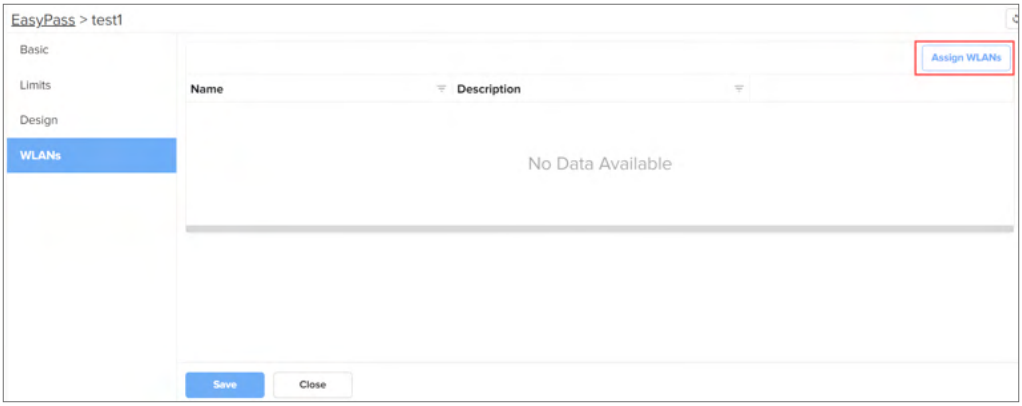
   For information on parameters of the **Limits** screen, see The Limits screen parameters.
9. Click the **Design** tab.

   The **Design** screen appears.
10. Configure the parameters of the **Design** screen.

    For information on parameters of the **Design** screen, see The Design screen parameters.
11. Click the **WLANs** tab.

    The **WLANs** screen appears.

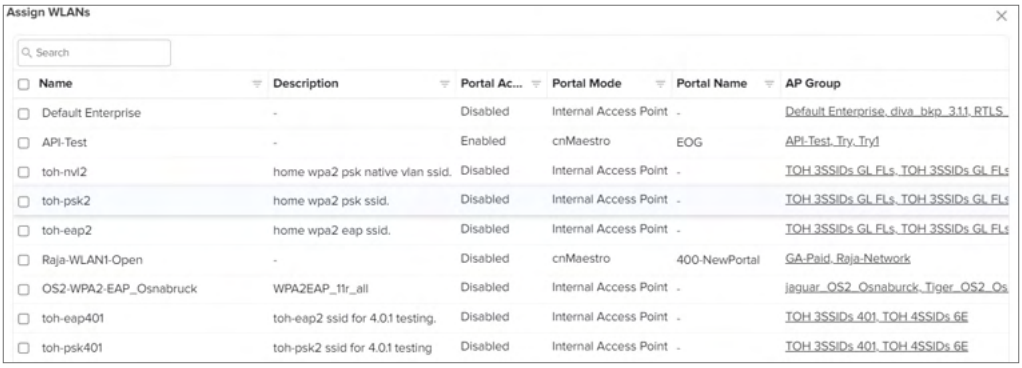
Figure 498 *The WLANs screen*



12. Click the **Assign WLANs** button.

    The **Assign WLANs** window appears.

Figure 499 *The Assign WLANs window*



13. Select the required WLAN(s) and click **Assign**. For example, **testWLAN**.

    The selected WLAN is added to the WLANs page.

Figure 500 *Assigned WLAN*



- Use the unlink (⊖) icon to unlink a WLAN.
- Use the **Save** button to apply the changes.
- Use the **Close** button to exit from the portal.

These buttons are available across all portal types.

Note

- The **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types have some common parameters that you must configure on their respective **Voucher** screens. For information on parameters of the **Voucher** screen, see The Voucher screen parameters.

- The **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types have some common parameters that you must configure on their respective **Plans** screens. For information on parameters of the **Plans** screen, see The Plans screen parameters.

14. Click **Save**.

Configuring common parameters

The following are the common parameters required for creating various portal types in EasyPass:

- The Basic screen parameters
- The Limits screen parameters
- The Design screen parameters
- The Voucher screen parameters
- The Plans screen parameters

The Basic screen parameters

Figure 501 displays the **Basic** screen parameters.

Figure 501 *The Basic screen*

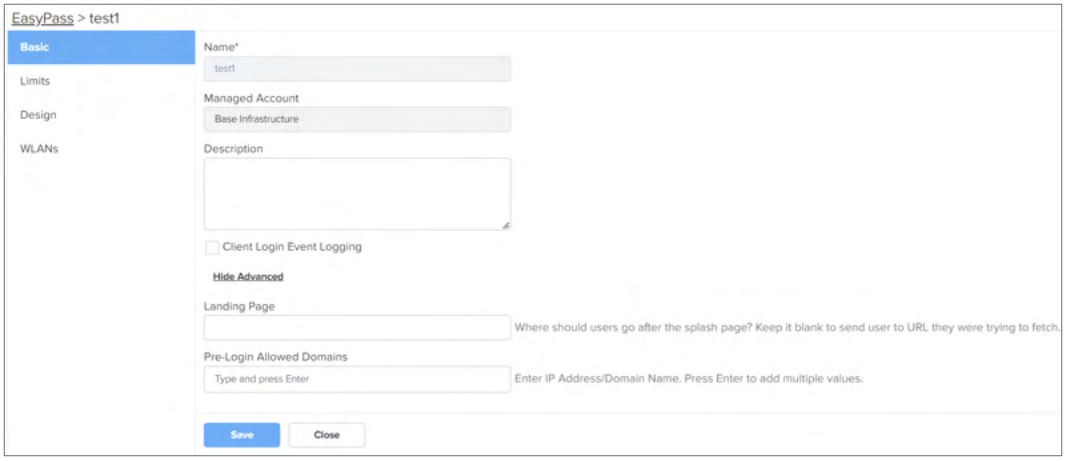


Table 134 describes the **Basic** screen parameters that appear across all portal types on their respective **Basic** screens.

Table 134 *The Basic screen parameters*

Parameter	Description
Description	A brief description of the portal.
Client Login Event Logging	Indicates whether the **Client Login Event Logging** parameter is enabled or disabled. By default, this parameter is disabled.
Show Advanced This section consists of settings related to the landing page and pre-login allowed domains.	
Landing Page	Determines where the users are directed to after they have viewed or interacted with a splash page or login screen. Enter the complete URL with the protocol. For example, **https://www.google.com** **Note**: If the landing page field is kept blank, the users are automatically redirected to

Table 134 *The Basic screen parameters*

Parameter	Description
	the URL they were trying to access.
Pre-Login Allowed Domains	Allows the administrators to specify domains that are allowed for access before the user logs in. Enter the IP address or domain name. **Note**: You can add multiple IP addresses or domain names.

Note

After configuring the **Basic Screen** parameters, proceed to step 7 described in the Creating a portal process.

The Limits screen parameters

Figure 502 displays the **Limits** screen parameters.

Figure 502 *The Limits screen*

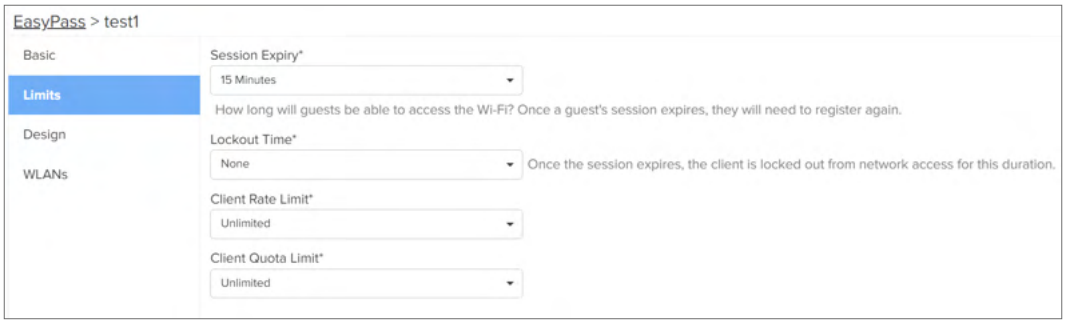


Table 135 describes the **Limits** screen parameters that appear across all portal types on their respective **Limits** screens.

Table 135 *The Limits screen parameters*

Parameter	Description
Session Expiry	The specified duration after which a user's session automatically expires, disconnecting the user from the Wi-Fi network. The following options are supported: • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom By default, **15 Minutes** is selected. Select the required option from the drop-down list.
Lockout Time	The lockout time restricts the ability to create a new session for the specified duration when a session expires.

Table 135 *The Limits screen parameters*

Parameter	Description
	The following options are supported: • None • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom By default, **None** is selected. Select the required option from the drop-down list. **Note**: The **Lockout Time** parameter is not available for Self Registration X, Sponsored Guest X, Voucher, Paid X, Microsoft Azure X, and Google Login X portal types.
Client Rate Limit	Indicates the client rate limit. The following options are supported: • Limited—When the **Limited** option is selected, the **Downlink** and **Uplink** parameters appear. • Unlimited By default, **Unlimited** is selected.
Downlink	This parameter is applicable only when **Client Rate Limit** is set to **Limited**. Downlink of client rate limit in Kbps. Maximum value: 1000000
Uplink	This parameter is applicable only when **Client Rate Limit** is set to **Limited**. Uplink of client rate limit in Kbps. Maximum value: 1000000
Client Quota Limit	Indicates the client quota limit. The following options are supported: • Limited—When the **Limited** option is selected, the **Total** parameter appears. • Unlimited By default, **Unlimited** is selected.
Total	The total client quota in MB or GB. You can either select **MB** or **GB** option from the drop-down list. By default, **MB** option is selected. **Note**: This parameter supports: • A minimum of 1 MB and a maximum of 8000000 MB.

Table 135 *The Limits screen parameters*

Parameter	Description
	• A minimum of 1 GB and a maximum of 8000 GB.
Note: An additional parameter, **Device Limit**, must be configured for the following portal types in the **Limits** screen: • Self Registration X • Microsoft Azure X • Google Login X The **Device Limit** parameter must also be configured for the following portal types: • Voucher— Use the **Vouchers** tab to configure the **Device Limit** parameter. • Paid X— Use the the **Add New Plan** window of the **Plans** screen to configure the **Device Limit** parameter.	
Device Limit	Specifies the number of devices that the guest can connect to the wireless network. Default value: 1 Maximum value supported: 10

Note

After configuring the **Limits screen** parameters, proceed to step 9 described in the Creating a portal process.

The Design screen parameters

Figure 503 displays the **Design** screen parameters.

Figure 503 *The Design screen*

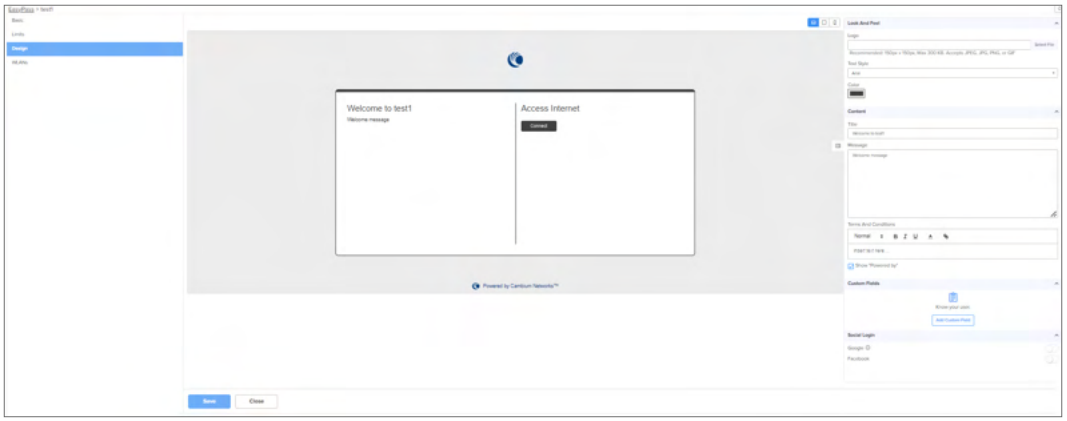


Table 136 describes the common **Design** screen parameters that appear across all portal types on their respective **Design** screens.

Table 136 *The Design screen parameters*

Parameter	Description
Logo	Logo for the design page.
Text Style	Text style for the design page. The following options are supported: • Arial

Table 136 *The Design screen parameters*

Parameter	Description
	• Times New Roman • Verdana • Tahoma
Color	Color for the design page.
Title	Title for the design page.
Message	Welcome message for the design page.
Terms and Conditions	Terms and Conditions for the design page.
Show Powered By	Indicates that a service is provided by an organization. You can disable this parameter. By default, this parameter is enabled.
Custom fields	Select the required field(s) to include in the design page by clicking the **Add Custom Field** button. The following options are supported: • Date • Email • Name • Number • Phone • Text
Connect	An option to provide access for users to the internet. Click the **Connect** button to access the internet. This is the default option available on the design page.
Social Login	You can enable the required social login option(s). The following options are supported: • Google • Facebook When social login option(s) are enabled, the design page contains **Sign in with Facebook** and **Sign in with Google** options.  **Note**: When **Sign in with Facebook** and **Sign in with**

Table 136 *The Design screen parameters*

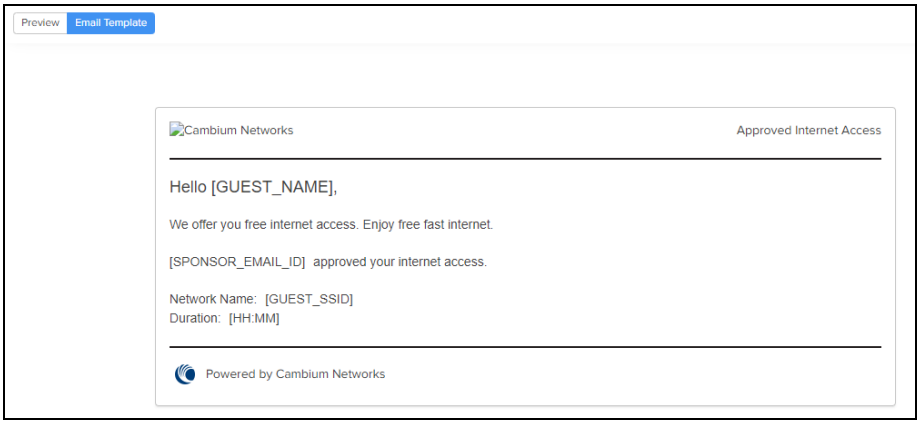
Parameter	Description
	Google options are enabled, they replace the default **Connect** option.
Device-specific view options of the design page 	The view options on the design page are tailored for various devices. The following options are supported: • Desktop View • Tablet/iPad View • Mobile View By default, Desktop View is selected. **Note:** The device-specific view options are available across all portal types on their respective **Design** screens.
Note: For the **Self RegistrationX** portal type, you must also configure additional parameters using the **Preview** tab and the **Email Template** tab.	
Preview tab The **Preview** tab is selected, by default. The following fields appear on the design page.	
Email	Enter the email ID. This field is mandatory.
Password	Enter the password. This field is mandatory.
Email Template tab When you click the **Email Template** tab, the following email template appears: 	
Note: For the **Sponsored Guest X** portal type, configuration of additional parameters is required to identify users, create personalized accounts, verify email ownership, and send targeted notifications to guests. Additionally, these fields are necessary to notify users of important updates, promotions, or account-related changes. Configure the following additional parameters:	
Guest Name	Enter the guest name.
Guest Email	Enter the guest email ID.
Sponsor Email	Enter the sponsor email ID.
Note: For the **Voucher** portal type, configure the following additional parameter:	
Voucher Code	Indicates a voucher code.

Table 136 *The Design screen parameters*

Parameter	Description
	Enter a voucher code. This is a mandatory field.
Note: For the **Paid X** portal type, configure either of the following options:	
Select a Plan	Select the required plan from the drop-down list.
Payment Code	The payment code of the plan. Enter the payment code.
Note: For the **Microsoft Azure X** portal type, the following option is available:	
Sign in with Microsoft	Use this option to sign in with Microsoft.
Note: For the **Google Login X** portal type, the following option is available:	
Sign in with Google	Use this option to sign in with Google.
Note: For the **One click + Voucher** portal type, configure either of the following options:	
Free	You can select this option to provide free access to the internet.
Voucher	You must enter a voucher code when you select this option.
Note: For the **One click + Paid X** portal type, configure either of the following options:	
Free	You can select this option to provide free access to the internet.
Paid	When you select this option, you can either use **Select a Plan** or **Payment Code** option.
Note: For the **Voucher + Paid X** portal type, configure either of the following options:	
Voucher	When you select this option, you must enter a voucher code.
Paid	When you select this option, you can either use **Select a Plan** or **Payment Code** option.

Note

After configuring the **Design screen** parameters, proceed to step 11 described in the Creating a portal process.

The Voucher screen parameters

Table 137 displays the **Voucher** screen parameters that appear across **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types on their respective **Voucher** screens.

Table 137 *The Voucher screen parameters*

Parameter	Description
Voucher Plan Name	Name of the voucher plan. **Note**: This parameter supports: • A minimum of one and maximum of 64 characters. • Only alphanumeric, underscore (_), and dashes (-). This parameter is mandatory.

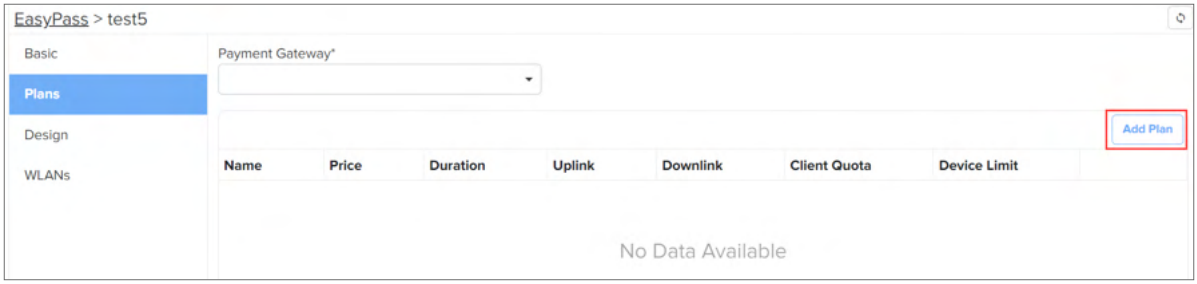
Table 137 *The Voucher screen parameters*

Parameter	Description
Quantity	Quantity (in integers) of the voucher. Minimum value: 1 Maximum value: 2000
Voucher Message	Message for the voucher. This parameter supports a minimum of one and maximum of 128 characters.
Session Expiry	For information on this parameter, see Table 135.
Voucher Expiry	The expiry time of the voucher. The following options are supported: • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom By default, **1 Day** is selected. This parameter is mandatory.
Client Rate Limit	For information on these parameters, see Table 135.
Downlink	
Uplink	
Client Quota Limit	
Total	
Device Limit	
Bind Voucher to Device	Allows you to associate a voucher with a specific device. By default, this parameter is disabled.
Unlimited	Enable or disable the parameter. By default, this parameter is disabled. If you enable the check box, you can connect unlimited number of devices.

The Plans screen parameters

Figure 504 displays the **Plans** screen parameters that appear across **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types on their respective **Plans** screens.

Figure 504 *The Plans screen*



Note

Before selecting a payment gateway, you must add a plan.

To add and manage a plan, complete the following steps:

1. Click the **Add Plan** button (as shown in Figure 504).

   The **Add New Plan** window appears.

   Figure 505 *The Add New Plan window*

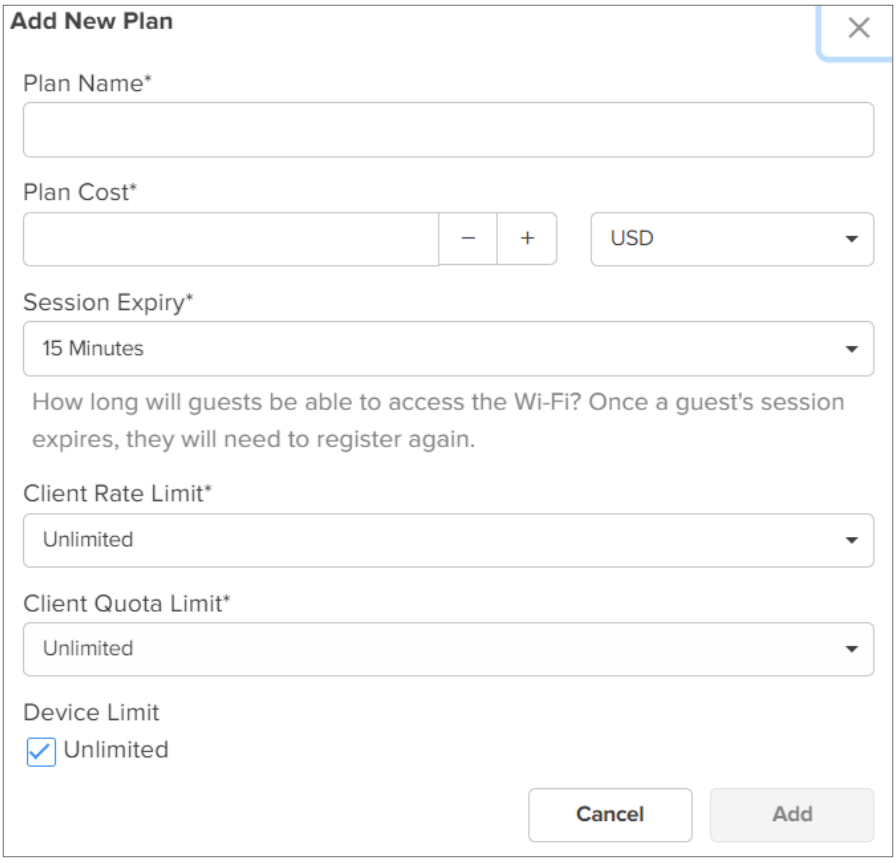


   Table 138 describes the common **Plans** screen parameters that appear across **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types on their respective **Plans** screens.

Table 138 *The Add New Plan window parameters*

Parameter	Description
Plan Name	Name for the plan. This parameter supports a minimum of one and maximum of 32 characters. **Note**: Alphanumeric and special characters are supported. This parameter is mandatory.
Plan Cost	Cost for the plan. This parameter is mandatory.
Currency	Currency for the plan. By default, **USD** is selected.
Session Expiry	For information on these parameters, see Table 135.
Client Rate Limit	
Downlink	
Uplink	
Client Quota Limit	
Total	
Device Limit	
Unlimited	Enable or disable the parameter. If you disable the check box, you must specify the device limit. If you enable the check box, you can connect unlimited number of devices.

2. Click the **Add** button (as shown in Figure 505).

   The plan is added.

Figure 506 *Plan added*

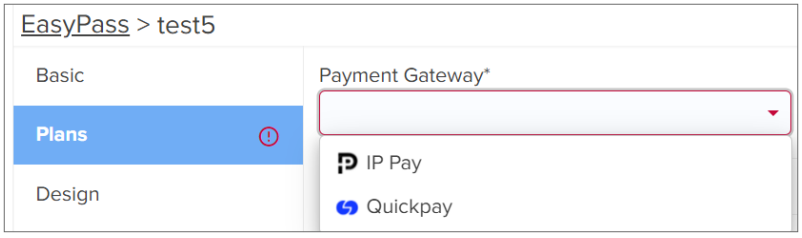


Note

Use the edit ( ) icon to modify a plan.

3. Select the required payment gateway option from the **Payment Gateway** drop-down list (as shown in Figure 507).

Figure 507 *Payment gateway options*



The following options are supported:

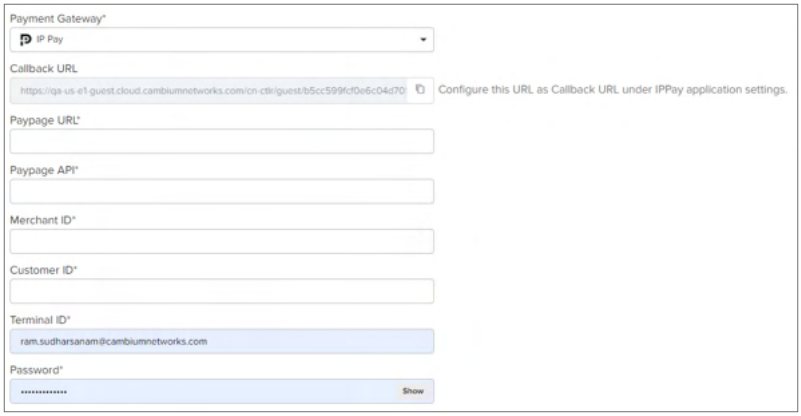
- IP Pay
- Quickpay

Note

Set the mandatory fields for the selected payment gateway option(s).

Figure 508 displays the parameters available for the **IP Pay** payment gateway.

Figure 508 *The IP Pay option*



When you select the **IP Pay** option, you must configure the parameters described in Table 139.

Table 139 *Parameters specific to the IP Pay option*

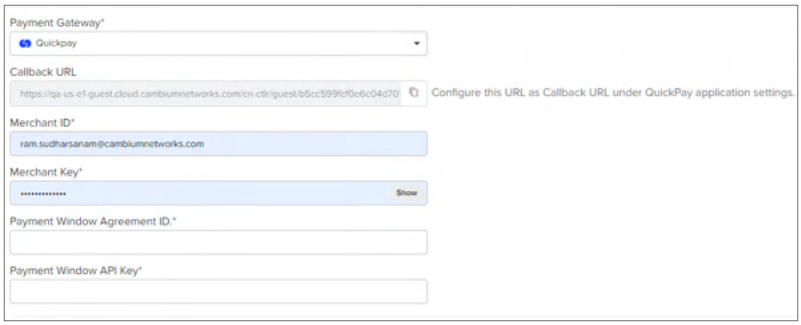
Parameter	Description
Callback URL	A URL that is called back by the payment gateway after a transaction is processed. Configure the Callback URL in the IPPay application settings.
Paypage URL	A URL that users are redirected to when they are asked to pay for a transaction. This URL typically points to a payment page where the user can enter the payment information. Enter the paypage URL. This parameter is mandatory.
Paypage API	A paypage API to create and manage payments, and retrieve payment information. Enter the Paypage API. This parameter is mandatory.
Merchant ID	A merchant ID to identify the merchant. Enter the merchant ID. This parameter is mandatory.
Customer ID	A customer ID to identify the customer. Enter the customer ID. This parameter is mandatory.
Note: **Terminal ID** and **Password** fields are populated, by default.	
Terminal ID	A terminal ID to identify the terminal and authenticate transactions processed through it.

Table 139 *Parameters specific to the IP Pay option*

Parameter	Description
Password	A password to authenticate the user.
Note: The parameters of the **IP Pay** option are also applicable to **One Click + Paid X** and **Voucher + Paid X** portal types.	

Figure 509 displays the parameters available for the **Quickpay** payment gateway.

Figure 509 *The Quickpay option*



When you select the **Quickpay** option, you must configure the parameters described in Table 140.

Table 140 *Parameters specific to the Quickpay option*

Parameter	Description
Callback URL	A URL that is called back by the payment gateway after a transaction is processed. Configure the Callback URL in the QuickPay application settings.
Note: **Merchant ID** and **Merchant key** fields are populated, by default.	
Merchant ID	A merchant ID to identify the merchant.
Merchant key	A merchant key to authenticate the merchant's identity.
Payment Window Agreement ID	Payment window agreement ID. Enter the payment window agreement ID. This parameter is mandatory.
Payment Window API Key	Payment window API key. Enter the payment window API key. This parameter is mandatory.
Note: The parameters of the **Quickpay** option are also applicable to **One Click + Paid X** and **Voucher + Paid X** portal types.	

Accessing the common tabs

The following common tabs are available for various portal types in EasyPass:

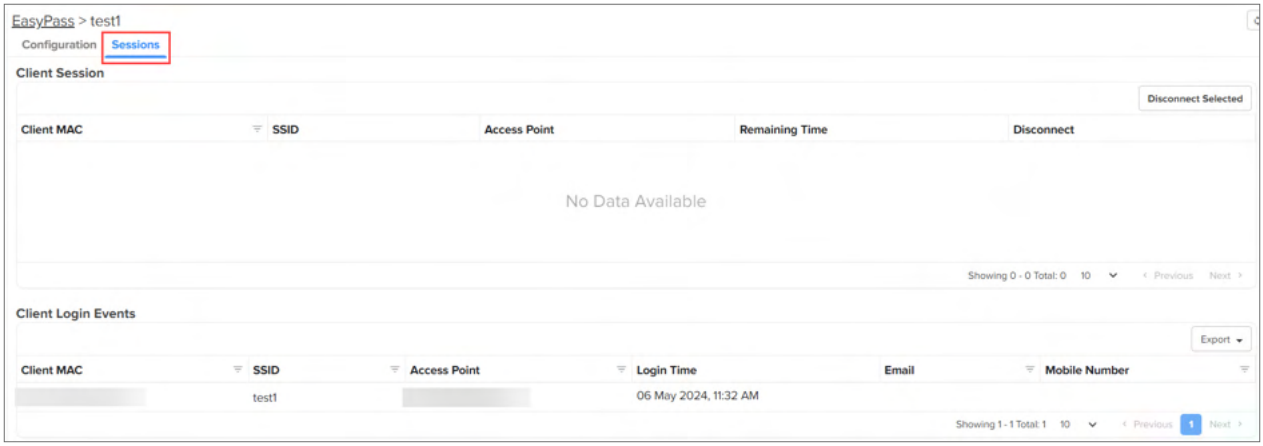
- Sessions
- Guests
  - Adding a new guest user
- Vouchers
  - EasyPass

- Paid Transactions X
- Users X

Sessions

You can access the **Sessions** page using the **Sessions** tab from, as shown in Figure 510, from any of the portals.

Figure 510 *The Sessions page*



The **Sessions** tab includes two sections:

- Client Session—Administrators can view the details of all client sessions.
- Client Login Events—Administrators can view the details of all the sessions of client login events.

Note

- The **Client Login Events** section displays the client login events only if the **Client Login Event Logging** check box is selected on the **Basic** screen. This checkbox is available across all portal types.
- The **Client Login Events** section displays the login events for 7 days.

Administrators can export the client login events using the following options:

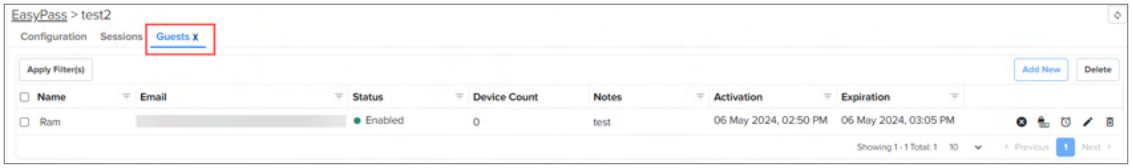
- Export page as CSV
- Export page as PDF
- Export all as CSV

Guests

The **Guests** page allows you to view details of self-registered guests connecting to the wireless network.

You can access the **Guests** page using the **Guests** tab (as shown in Figure 511).

Figure 511 *The Guests page*



Note

The **Guests** tab appears only for the **Self Registration X** portal type.

Adding a new guest user

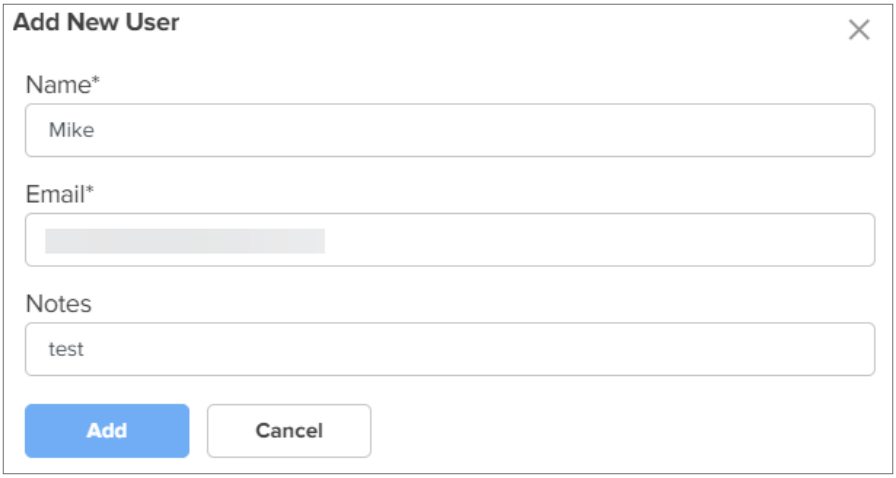
You can also add a new guest user from the **Guests** page.

Complete the following steps to add a new user:

1. On the **Guests** page, click **Add New**.

   The **Add New User** window appears.

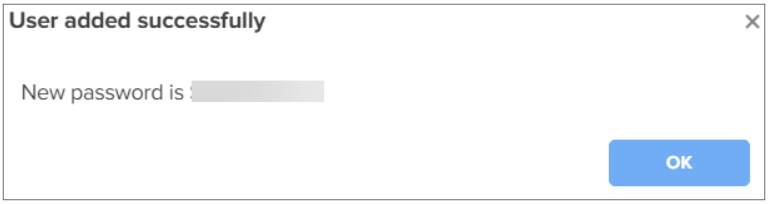
   Figure 512 *The Add New User window*



2. In the **Name** field, enter the name of a user. This field is mandatory.
3. In the **Email** field, enter an email ID of the user. This field is mandatory.
4. In the **Notes** field, enter the description for creating a new user. This field is optional.
5. Click the **Add** button.

   The **User added successfully** window appears with a message showing a new password (as shown in Figure 513).

   Figure 513 *The User added successfully window*



6. Click **OK**.

   A new guest user is added (as shown in Figure 514).

   Figure 514 *The new guest user details*



   You can view the details of the self registered guest connected to the Wi-Fi network (as shown in Figure 514).

Note

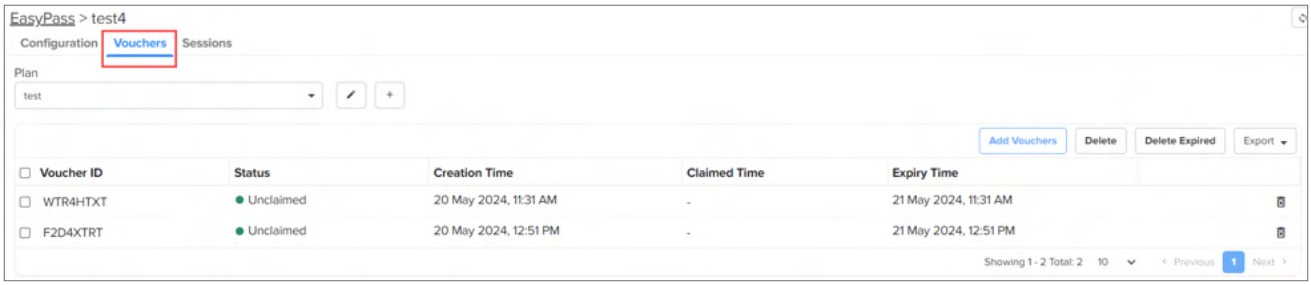
- Use the disable access ( ) icon to disable access.
- Use the reset password ( ) icon to reset a password.
- Use the extend session ( ) icon to extend a session.
- Use the edit ( ) icon to edit the user details.
- Use the delete ( ) icon to delete a user.

Vouchers

You can access the **Vouchers** page using the **Vouchers** tab (as shown in Figure 515).

You can view a list of created vouchers, edit an existing voucher plan, and add a new voucher plan using the **Vouchers** tab. You also have options to add vouchers and delete all expired voucher(s).

Figure 515 *The Vouchers tab*



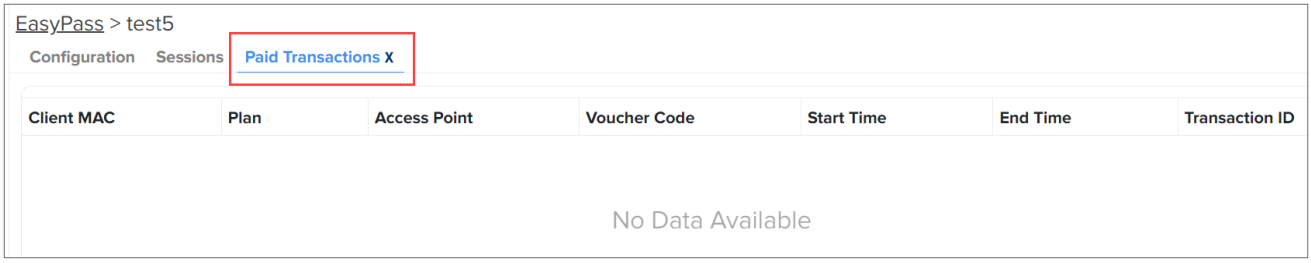
Note

The **Vouchers** tab appears only for the **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types.

Paid Transactions X

You can access the **Paid Transactions X** page using the **Paid Transactions X** tab (as shown in Figure 516).

Figure 516 *The Paid Transactions X tab*



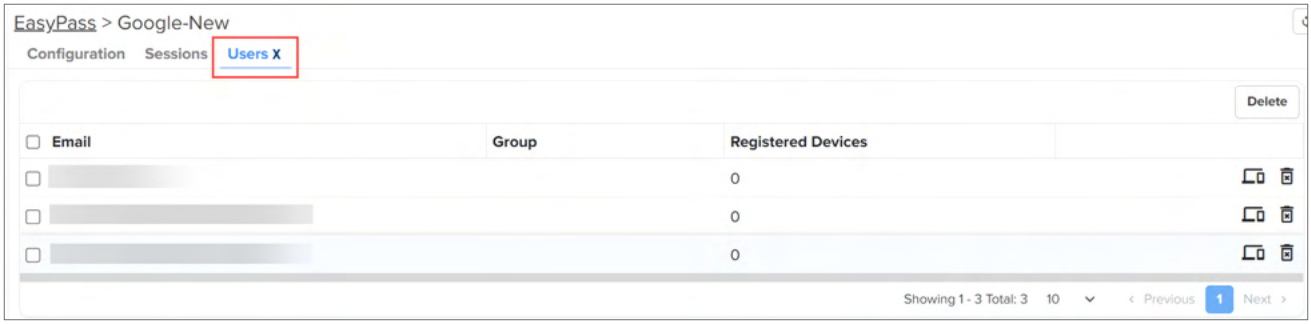
Note

The **Paid Transactions X** tab appears only for the **Paid X, One Click + Paid,** and **Voucher + Paid X** portal types.

Users X

You can access the **Users X** page using the **Users X** tab (as shown in Figure 517).

Figure 517 *The Users X tab*



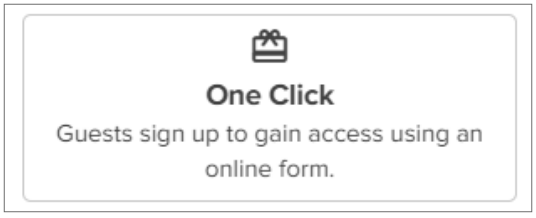
Note

The **Users X** tab appears only for the **Microsoft Azure X** and **Google Login X** portal types.

Creating One Click portal

You can create a One Click portal to provide guests with quick Wi-Fi access, adherence to policies, customized brand experiences, and secure Wi-Fi management with timing controls.

Figure 518 *The One Click option*



Note

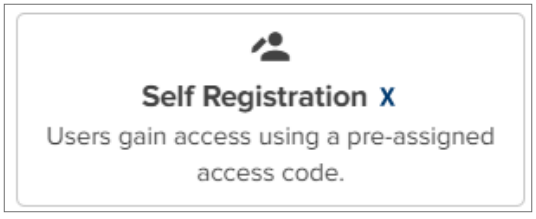
To create a One Click portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Creating Self Registration X portal

You can create a self-registration portal to provide guests with easy account management, minimize IT involvement, offer SMS integration, email password delivery, sponsor workflow approvals, and enhance security and access control.

This section includes only the additional parameters that you must configure for the Self Registration X portal.

Figure 519 *The Self Registration X option*



Note

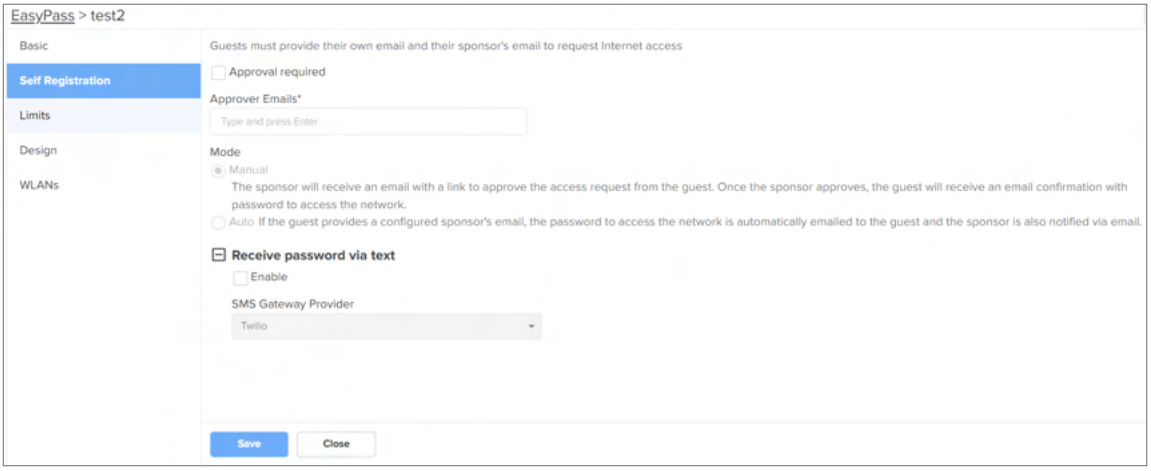
To create a Self Registration X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Self Registration** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Self Registration X portal:

1. From the **Basic** screen, click the **Self Registration** tab.

   The **Self Registration** screen appears.

   Figure 520 *The Self Registration screen*



2. Configure the parameters described in Table 141.

   Table 141 *The Self Registration screen parameters*

Parameter	Description
Approval required	Enable or disable this option. By default, this option is disabled. When this parameter is enabled, you must provide the approver email ID(s) in the **Approver Emails** field. When this parameter is enabled, you have an option to select the required mode.
Approver Emails	This parameter is applicable when the **Approval required** check box is selected. Indicates the approver email ID(s) that must be provided. This parameter is mandatory.
Mode	This parameter is applicable when the **Approval required** check box is selected. The following options are supported: • Manual—The sponsor receives an email with a link to approve the access request from the guest. Once the sponsor approves, the guest receives an email confirmation with password to access the network. • Auto—If the guest provides a configured sponsor's email, the password to access the network is automatically emailed to the guest and the sponsor is also notified through email.
Receive password via text By default, the guests receive the password through email address and text message.	
Enable	Select the **Enable** check box. This parameter is disabled by default. When you select the **Enable** check box, the **SMS Gateway Provider** option is enabled.
SMS Gateway Provider	Select the required SMS gateway option to be used to send the OTP to the guest's mobile device.

Table 141 *The Self Registration screen parameters*

Parameter	Description
	By default, the **Twilio** option is selected. The following gateway options are supported: • Fast SMS • Generic SMS API • SMS Country • SMS Gupshup • SMSAPI • Twilio • Victory Link SMS Each of these gateway options can be configured with their respective parameters. For more information on the gateway options, see **SMS Gateway Providers** section.

SMS Gateway Providers

This section describes the different types of SMS gateway providers.

Figure 521 displays the parameters available for the **Twilio** option.

Figure 521 *Twilio option*



When you select the **Twilio** option, you must configure the parameters described in Table 142.

Table 142 *Parameters of Twilio*

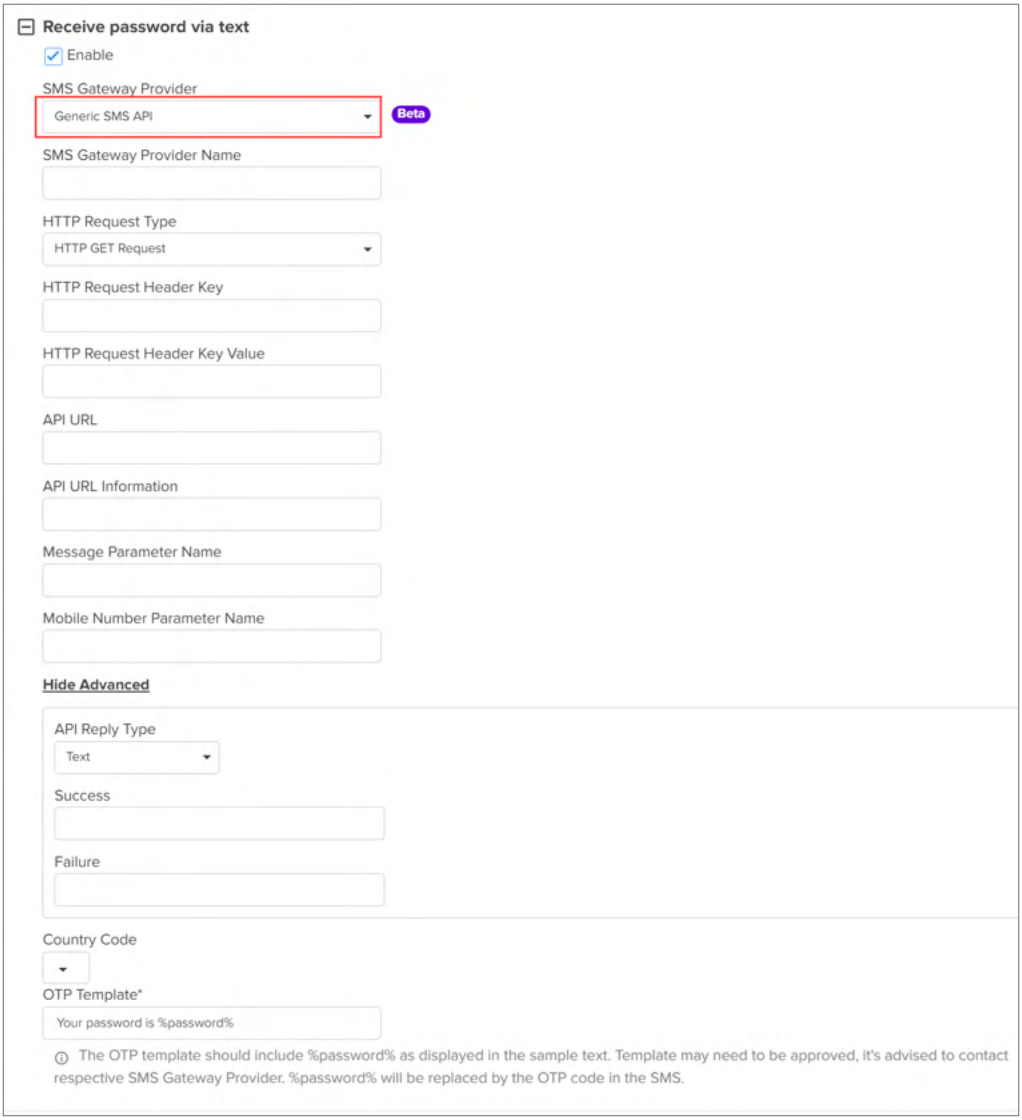
Parameter	Description
Note: The **Username** and **Password** fields are populated, by default.	
Auth Token	Auth token. Enter the auth token.
Account SID	Account SID. Enter the account SID.
From	Select the required country code from the drop-down list and enter the mobile number.
OTP Template	OTP template.

Table 142 *Parameters of Twilio*

Parameter	Description
	Enter the password in the **OTP Template** field. This parameter is mandatory.

Figure 522 displays the parameters available for the **Generic SMS API** option.

Figure 522 *Generic SMS API option*



When you select the **Generic SMS API** option, you must configure the parameters described in Table 143.

Table 143 *Parameters of Generic SMS API*

Parameter	Description
SMS Gateway Provider Name	SMS gateway provider name. Enter a name for the SMS gateway provider. Enter the user name.

Table 143 *Parameters of Generic SMS API*

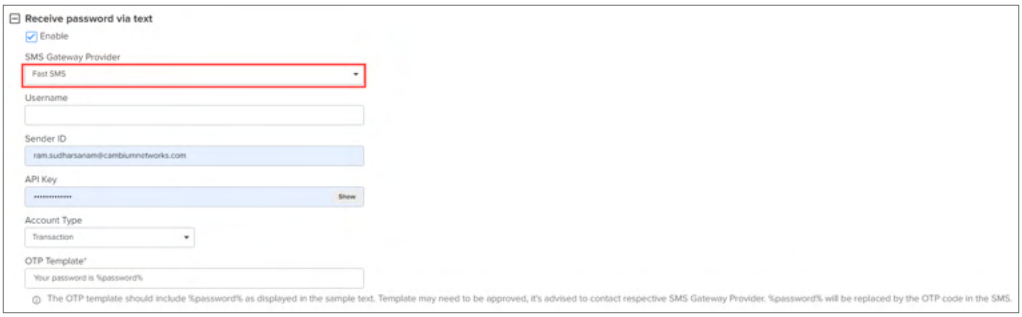
Parameter	Description
HTTP Request Type	HTTP request type. The following options are supported: • HTTP GET Request • HTTP POST Request
HTTP Request Header Key	HTTP request header key
HTTP Request Header Key Value	HTTP request header key value
API URL	API URL Enter the API URL.
API URL Information	API URL information. Enter the API URL information.
Message Parameter Name	Message parameter name. Enter the message parameter name.
Mobile Number Parameter Name	Mobile number parameter name. Enter the mobile number parameter name.
Show Advanced This section consists of advanced settings related to API reply type.	
API Reply Type	API reply type. Select the required option from the drop-down list. The following options are supported: • Text • JSON • XML
Text	
Success	Success message. Enter the success message.
Failure	Failure message. Enter the failure message.
JSON	
JSON Reply Success Key Name	JSON reply success key name. Enter the JSON reply success key name.
JSON Reply Success Key Value	JSON reply success key value. Enter the JSON reply success key value.
JSON Reply Failure Key Name	JSON reply failure key name. Enter the JSON reply failure key name.

Table 143 *Parameters of Generic SMS API*

Parameter	Description
JSON reply Failure Key Value	JSON reply failure key value. Enter the JSON reply failure key value.
XML	
XML Reply Success Element	XML reply success element. Enter the XML reply success element.
XML Reply Success Element Value	XML reply success element value. Enter the reply success element value.
XML Reply Failure Element	XML reply failure element. Enter the XML reply failure element.
XMl Reply Failure Element Value	XML reply failure element value. Enter the XML reply failure element value.
Country Code	Country code. Select the required country code from the drop-down list. For example, **United States (+1)**
OTP Template	OTP template. Enter the password in the **OTP Template** field. This parameter is mandatory.

Figure 523 displays the parameters available for the **Fast SMS** option.

Figure 523 *Fast SMS option*



When you select the **Fast SMS** option, you must configure the parameters described in Table 144.

Table 144 *Parameters of Fast SMS*

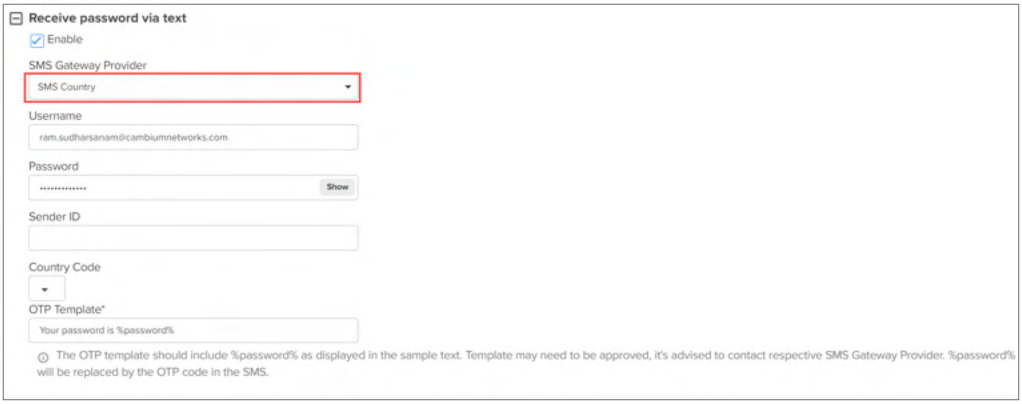
Parameter	Description
Username	User name. Enter the user name. This field is optional.
Note: The **Sender ID** and **API key** fields are populated, by default.	
Account Type	Account type. Select the required option from the drop-down list.

Table 144 *Parameters of Fast SMS*

Parameter	Description
	The following options are supported: • Transaction • Promotional • International • OTP • Other
OTP Template	OTP template. Enter the password in the **OTP Template** field. This parameter is mandatory.

Figure 524 displays the parameters available for the **SMS Country** option.

Figure 524 *SMS Country option*



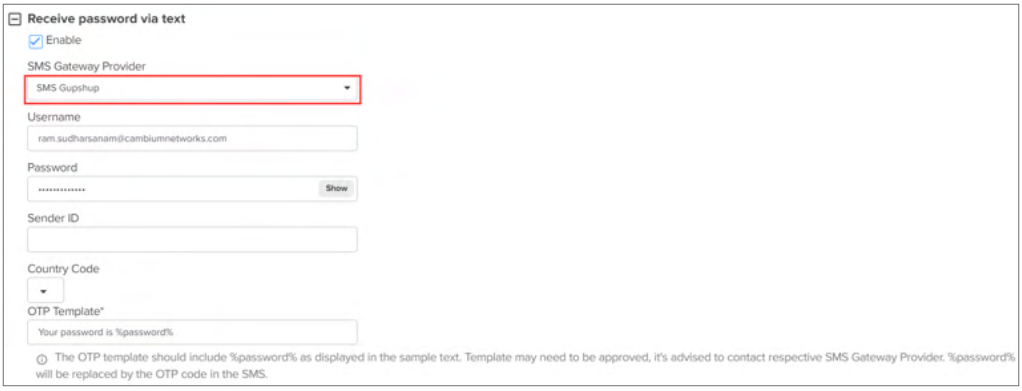
When you select the **SMS Country** option, you must configure the parameters described in Table 145.

Table 145 *Parameters of SMS Country*

Parameter	Description
Note: The **Username** and **Password** fields are populated, by default.	
Sender ID	Sender ID. Enter the sender ID.
Country Code	Country code. Select the required country code from the drop-down list. For example, **United States (+1)**
OTP Template	OTP template. Enter the password in the **OTP Template** field. This parameter is mandatory.

Figure 525 displays the parameters available for the **SMS Gupshup** option.

Figure 525 *SMS Gupshup option*



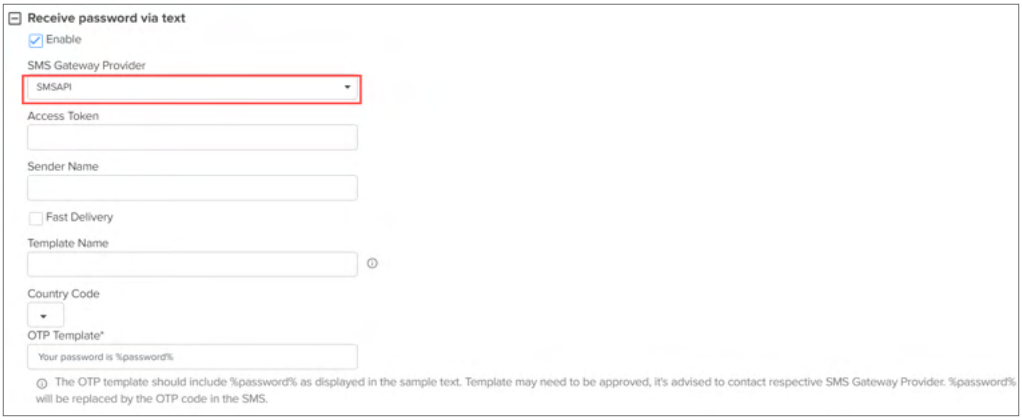
When you select the **SMS Gupshup** option, you must configure the parameters described in Table 146.

Table 146 *Parameters of SMS Gupshup*

Parameter	Description
Note: The **Username** and **Password** fields are populated, by default.	
Sender ID	Sender ID. Enter the sender ID.
Country Code	Country code. Select the required country code from the drop-down list. For example, **United States (+1)**
OTP Template	OTP template. Enter the password in the **OTP Template** field. This parameter is mandatory.

Figure 526 displays the parameters available for the **SMS API** option.

Figure 526 *SMS API option*



When you select the **SMS API** option, you must configure the parameters described in Table 147.

Table 147 *Parameters of SMS API*

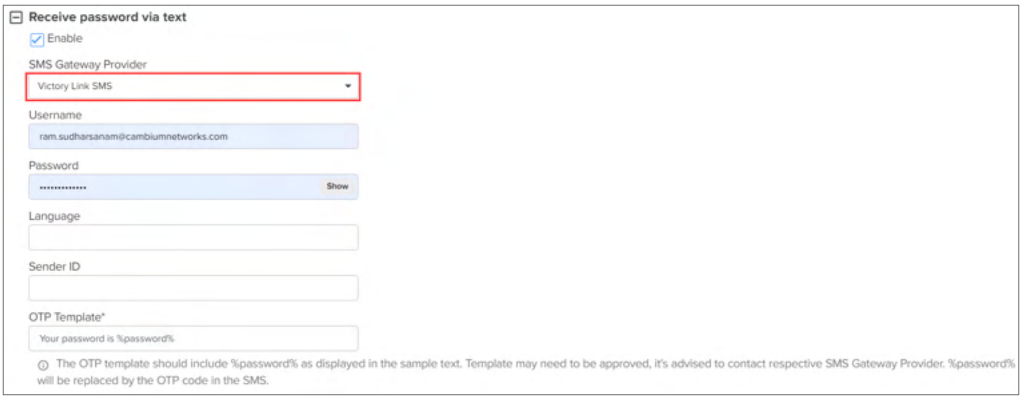
Parameter	Description
Note: The **Username** and **Password** fields are populated, by default.	

Table 147 *Parameters of SMS API*

Parameter	Description
Access Token	Access token. Enter the access token.
Sender Name	Sender name. Enter the sender name.
Fast Delivery	Enable the check box. By default, the check box is disabled.
Template Name	Template name. Enter the template name.
Country Code	Country code. Select the required country code from the drop-down list. For example, **United States (+1)**
OTP Template	OTP template. Enter the password in the **OTP Template** field. This parameter is mandatory.

Figure 527 displays the parameters available for the **Victory Link SMS** option.

Figure 527 *Victory Link SMS option*



When you select the **Victory Link SMS** option, you must configure the parameters described in Table 148.

Table 148 *Parameters of Victory Link SMS*

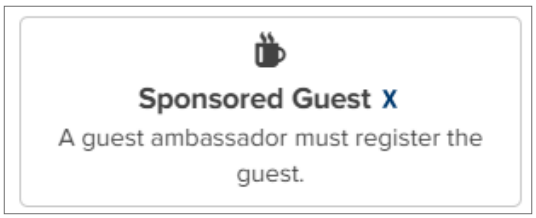
Parameter	Description
Note: The **Username** and **Password** fields are populated, by default.	
Language	Language. Enter the language.
Sender ID	Sender ID. Enter the sender ID.
OTP Template	OTP template. Enter the password in the **OTP Template** field. This parameter is mandatory.

Creating Sponsored Guest X portal

You can create a sponsored guest portal to enable non-IT staff to create, delete, or extend the validity of guest accounts.

This section includes only the additional parameters that you must configure for the Sponsored Guest X portal.

Figure 528 *The Sponsored Guest X option*



Note

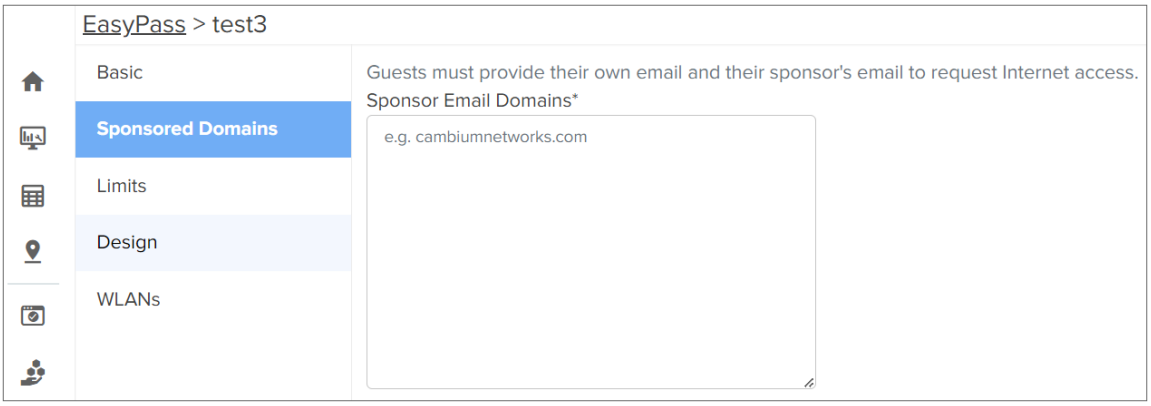
To create a Sponsored Guest X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Sponsored Domains** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Sponsored Guest X portal:

1. From the **Basic** screen, click the **Sponsored Domains** tab.

   The **Sponsored Domains** screen appears.

   Figure 529 *The Sponsored Domains screen*



2. Configure the parameters described in Table 149.

   Table 149 *The Sponsored Domains screen parameters*

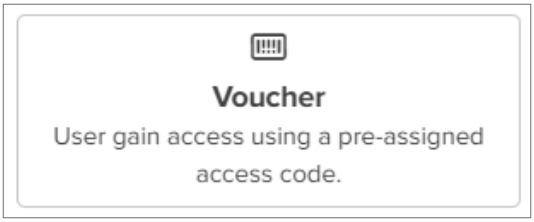
Parameter	Description
Sponsor Email Domains	Sponsor's domain(s). This parameter is mandatory.

Creating Voucher portal

You can create a voucher portal to create unique guest keys in bulk for retailers, hotels, conventions, and enterprises providing temporary visitor or guest Wi-Fi access.

This section includes only the additional parameters that you must configure for the Voucher portal.

Figure 530 *The Voucher option*



Note

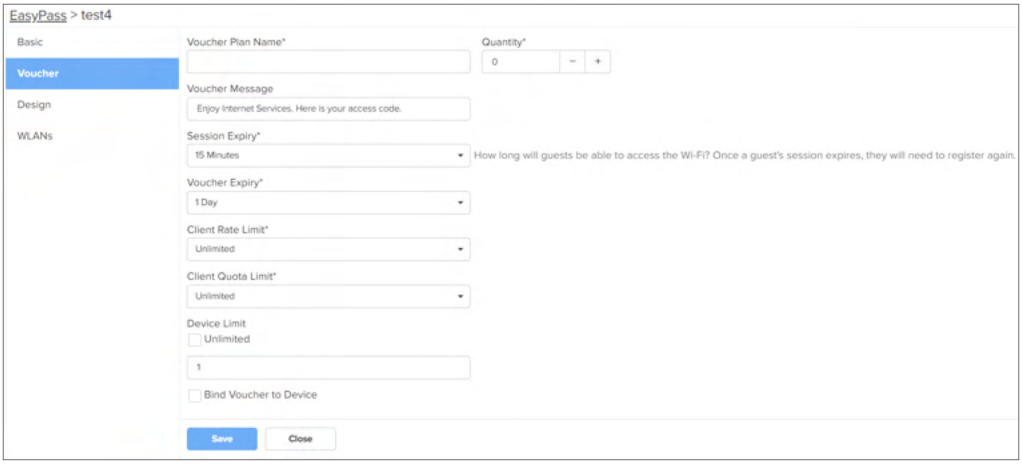
To create a Voucher portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Voucher portal:

1. From the **Basic** screen, click the **Voucher** tab.

   The **Voucher** screen appears.

   Figure 531 *The Voucher screen*

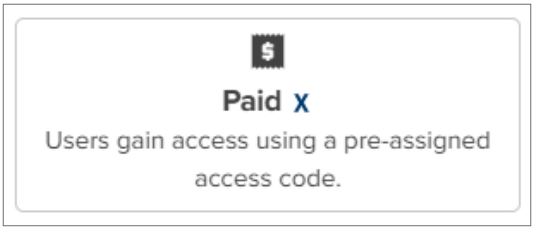


2. Configure the parameters described in Table 137.

Creating Paid X portal

You can create a Paid X portal with IP Pay or Quickpay gateway for smooth internet connectivity purchase, and improving user experience.

Figure 532 *The Paid X option*



Note

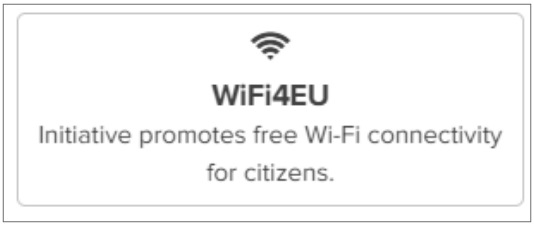
To create a Paid X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Plans** screen, **Design** screen, and **WLANs** screen.

Creating WiFi4EU portal

You can create a WiFi4EU portal to provide free Wi-Fi access across the European Union (EU) to citizens and vistors in public spaces such as parks, squares, administrations, libraries, and health centers.

This section includes only the additional parameters that you must configure for the WiFi4EU portal.

Figure 533 *The WiFi4EU option*



Note

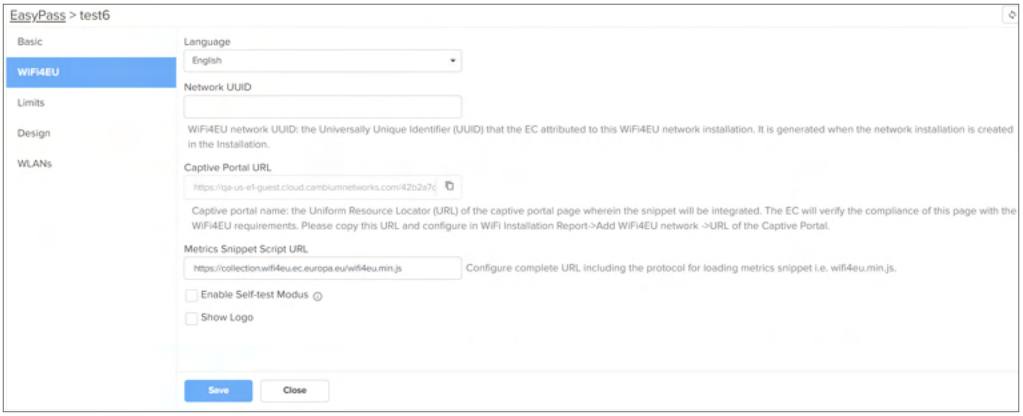
To create a WiFi4EU portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **WiFi4EU** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a WiFi4EU portal:

1. From the **Basic** screen, click the **WiFi4EU** tab.

   The **WiFi4EU** screen appears.

   Figure 534 *General parameters*



2. Configure the parameters described in Table 150.

Table 150 *General parameters - WiFi4EU*

Parameter	Description
Language	Select the preferred language from the drop-down list.
Network UUID	Universally Unique Identifier (UUID) that the EC attributed to the WiFi4EU network installation.
Enable Self-test Modus	Allows the browsers background script verification.
Show Logo	Displays the WiFi4EU logo provided by the European union.

Creating Microsoft Azure X portal

Creating a **Microsoft Azure X** portal allows you to combine Wi-Fi access with authentication using Microsoft Office 365 credentials, making it easier for users to connect to the Wi-Fi network and access domain resources.

This section includes only the additional parameters that you must configure for the Microsoft Azure X portal.

Figure 535 *The Microsoft Azure X option*



Note

To create a Microsoft Azure X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Azure** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Microsoft Azure X portal:

1. From the **Basic** screen, click the **Azure** tab.

   The **Azure** screen appears.

   Figure 536 *The Azure screen*



Note

Only Microsoft Azure administrator role users can perform the **Authorize** step.

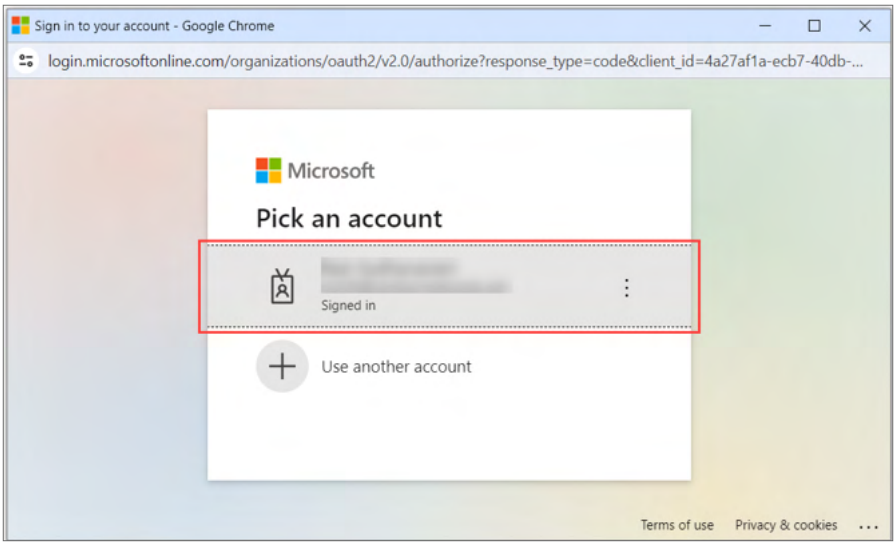
The **Authorize** step allows the Easypass Azure application to:

- Make API calls to Microsoft Azure customer
- Sign in users
- Periodically sync the customer Azure directory
- Ensure only active user sessions are maintained or enforce relogin if user group information changes

2. Click the **Authorize** button.

The following screen appears, as shown Figure 537.

Figure 537 *Sign in to your account page*



NOTE:

For information on how to integrate Active Directory with Azure, see Azure AD Integration.

Creating Google Login X portal

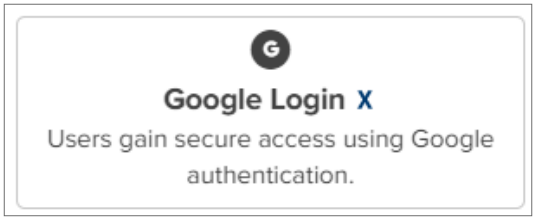
Creating a **Google Login X** portal enables users with a Google account to connect to the wireless network by synchronizing the active directory. When enabled, if a guest who is part of the supported group tries to connect to the Wi-Fi network, the AP provides access to the guest.

NOTE:

You must have a Google Workspace account before creating a Google Login X portal.

This section includes only the additional parameters that you must configure for the Google Login X portal.

Figure 538 *The Google Login X option*



Note

To create a Google Login X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Google** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Google Login X portal:

1. From the **Basic** screen, click the **Google** tab.

   The **Google** screen appears.

Figure 539 *The Google screen*



2. Configure the parameters described in Table 151.

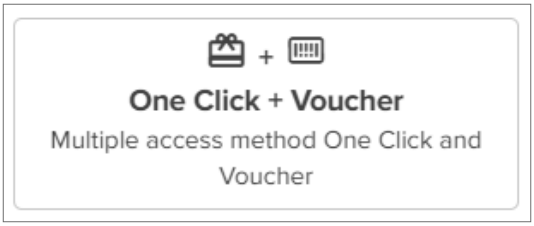
Table 151 *The Google screen parameters*

Parameter	Description
Enable Directory Synchronization	Select the check box to enable the directory synchronization. When you select the **Enable Directory Synchronization** check box, the following screen appears:  When you click the **Follow these steps** link, the following window appears describing how to configure the Google Apps domain category. Follow the steps to configure your Google Apps domain directory.  **Note**: For information on how to integrate Active Directory with Google Workspace, see Google Workspace AD Integration. When you clear the **Enable Directory Synchronization** checkbox, you must configure the **Allowed Domains** parameter.
Allowed Domains	Enter the required domain(s). This is a mandatory parameter.

Creating One Click + Voucher portal

Creating a One Click + Voucher portal combines the benefits of both One Click access and voucher-based promotions, providing users with an easy and cost-effective way to access services.

Figure 540 *The One Click + Voucher option*



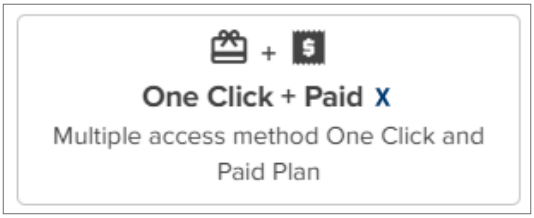
Note

To create a One Click + Voucher portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **One Click** screen, **Design** screen, and **WLANs** screen.

Creating One Click + Paid X portal

Creating a One Click + Paid X portal combines the benefits of One Click access with paid access to services.

Figure 541 *The One Click + Paid X option*



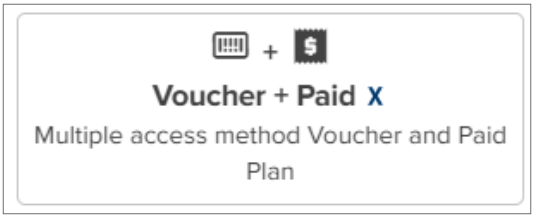
Note

To create a One Click + Paid X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Plans** screen, **One Click** screen, **Design** screen, and **WLANs** screen.

Creating Voucher + Paid X portal

Creating a Voucher + Paid X portal combines the benefits of voucher-based promotions and paid access to services.

Figure 542 *The Voucher + Paid X option*



Note

To create a Voucher + Paid X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **Plans** screen, **Design** screen, and **WLANs** screen.

MarketApps X

This section includes the following topics:

- Overview
- Adding a new MarketApp
- Managed Wi-Fi App
  - Basic tab
  - Settings tab
  - Design tab
- Self-Service Personal Wi-Fi App
  - Basic tab
  - Personal Wi-Fi configuration
- How to configure units by property managers

Overview

MarketApps is an advanced service within cnMaestro that is designed to enhance network management through tailored applications. It offers specialized tools that empower Managed Service Providers (MSPs) to deliver greater value to their customers and end users by addressing their specific needs and challenges.

MarketApps introduces two new apps for the Multi-Dwelling Unit (MDU) market within MarketApps—**Managed Wi-Fi** and **Self-Service Personal Wi-Fi**. These applications simplify management of Wi-Fi services for property managers, residents, and service providers, by featuring an intuitive and streamlined workflow.

Target audience

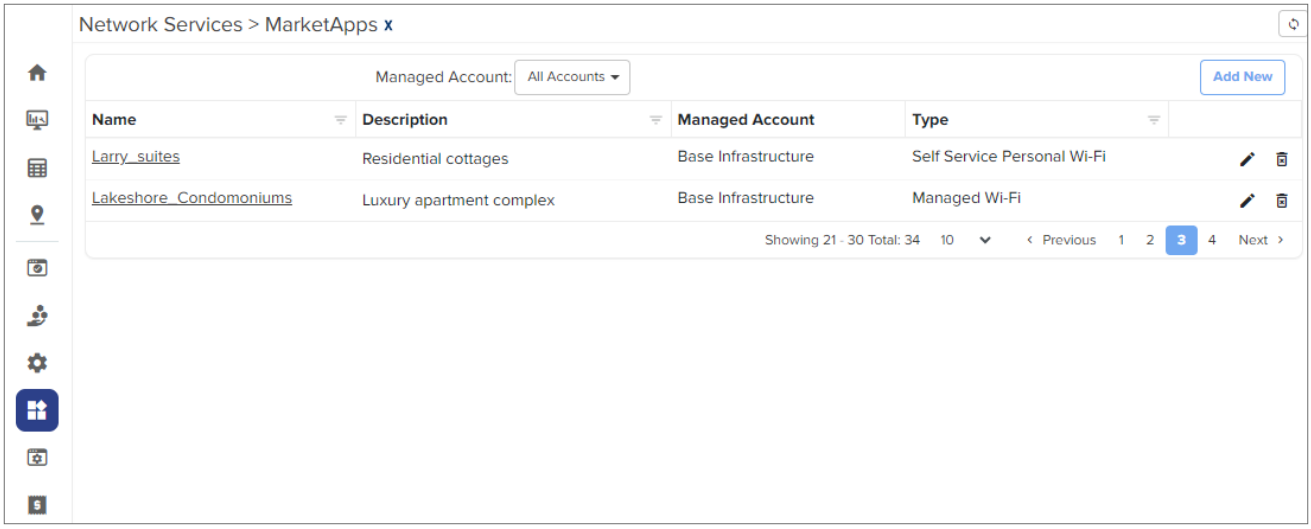
- **Property managers**—MarketApps empowers property managers to centrally administer Wi-Fi access across their properties. They can set up community-wide Wi-Fi networks and manage personal Wi-Fi networks for local residents.
- **Residents**—Residents can set up and manage their own Wi-Fi networks within the community, ensuring personalized and secure internet access.
- **Solution providers**—MarketApps helps the solution providers to offer tailored Wi-Fi solutions, enhancing network performance and user satisfaction in multi-dwelling units and apartment complexes.

Benefits

- **Centralized management**—Property managers can oversee and control Wi-Fi access across multiple units or buildings from cnMaestro.
- **Customization**—Residents can set up personal Wi-Fi networks with customized SSIDs and passwords, enhancing their user experience.

To access MarketApps, navigate to **Network Services** > **MarketApps** in cnMaestro.

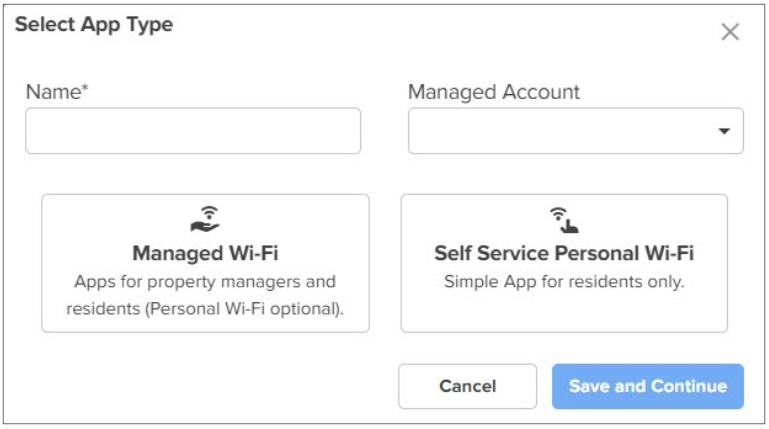
Figure 543 *MarketApps*



Adding a new MarketApp

To add a new MarketApp, complete the following steps:

1. Navigate to **Network Services** > **MarketApps** in cnMaestro.
2. Click the **Add New** button on the top right corner.
3. A new window **Select App Type** appears.



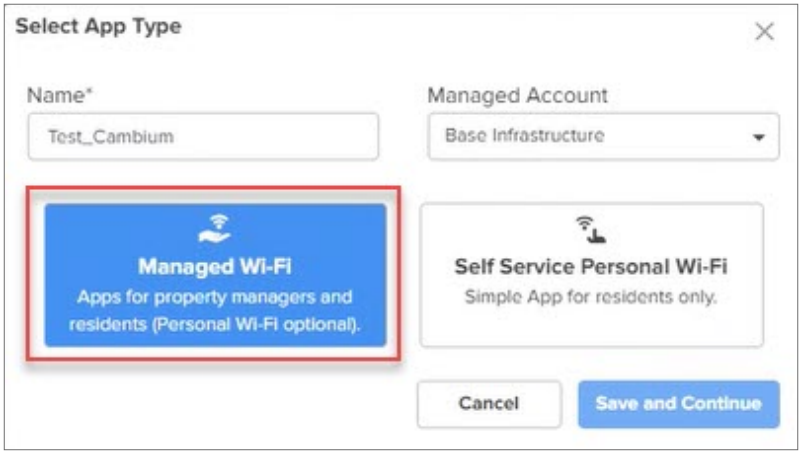
4. Enter a name for the new Market App in the **Name** field.
5. Choose the type of managed account for the app from the **Managed Account** drop-down box.
6. Select the required app.
7. Click **Save and Continue**.

   The respective app screens appears as discussed in the sections below.

Managed Wi-Fi App

The Managed Wi-Fi App in MarketApps enables property managers to centrally administer and manage Wi-Fi networks within their properties. This feature provisions both community-wide Wi-Fi networks and personal Wi-Fi networks for residents, allowing control and customization.

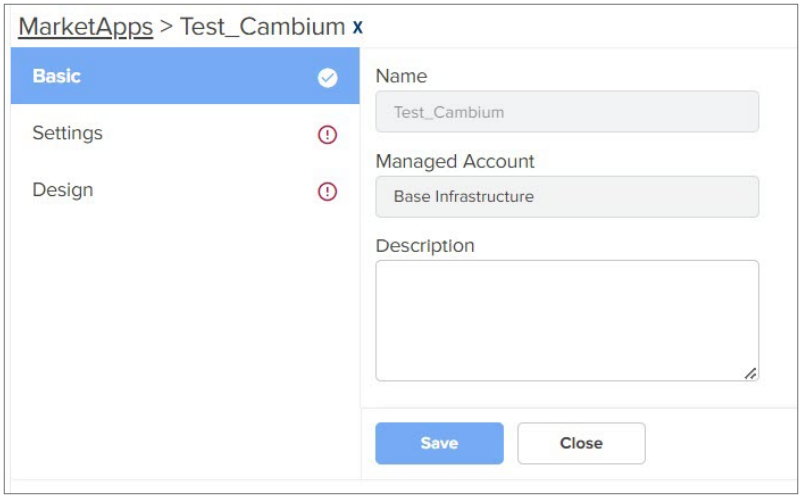
Figure 544 *Managed Wi-Fi App type*



Basic tab

The Basic tab in MarketApps allows you to provide a description for your Wi-Fi network. The network name and managed account details are automatically populated and cannot be modified. Enter a brief description to clarify the network's purpose.

Figure 545 *Basic tab parameters*



To configure the Basic tab, complete the following steps:

1. **Name**—Displays the chosen name for the Wi-Fi network.
2. **Managed Account**—This field is pre-populated based on previous selections.
3. **Description**—Enter a brief description that clearly explains the intended purpose or specific details of this Wi-Fi configuration.
4. Click **Save**.

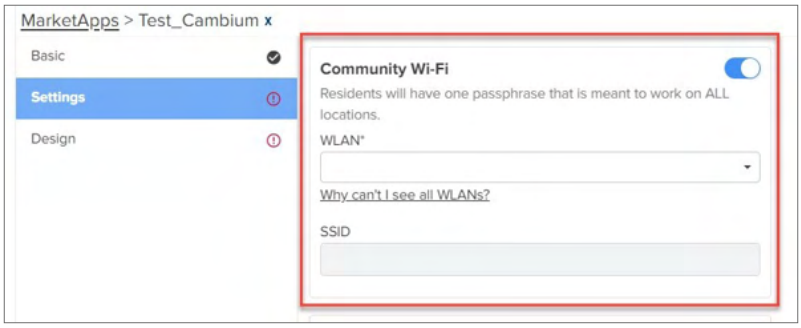
Settings tab

The Settings tab in MarketApps enables you to configure advanced settings for your Wi-Fi network. You can set up Community Wi-Fi, Personal Wi-Fi, or other options based on your specific requirements.

Community Wi-Fi

Community Wi-Fi in MarketApps allows property managers to set up and manage a single SSID for all residents within a property. This configuration is designed to provide centralized control over Wi-Fi access while ensuring uniform connectivity for all users.

Figure 546 *Community Wi-Fi settings*



To configure Community Wi-Fi under the Settings tab in Managed Wi-Fi, complete the following steps:

1. Select the **WLAN** for the community-wide Wi-Fi network.

Note

Valid WLANs must satisfy the following conditions:

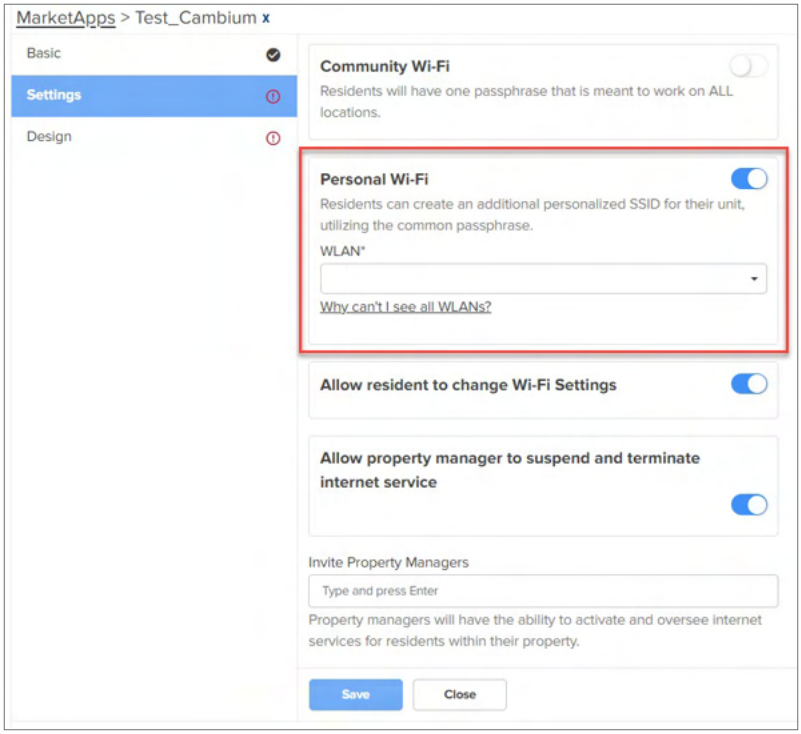
- WLAN's Personal SSID must be disabled.
- Local ePSK table must not have any existing entries.
- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys**, **WPA3 Pre-Shared Keys**, or **WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

2. Select the SSID for the community Wi-Fi from the **SSID** drop-down list.
3. Click **Save**.

Personal Wi-Fi

The Personal Wi-Fi option in MarketApps allows residents to set up and manage their own personalized Wi-Fi networks within the community. This feature provides flexibility and customization for individual units, enhancing the user experience by allowing residents to manage their SSIDs and passwords.

Figure 547 *Personal Wi-Fi settings*



To configure Personal Wi-Fi under the Settings tab in Managed Wi-Fi, complete the following steps:

1. Select the WLAN for the personal Wi-Fi network from the **WLAN** drop-down list.

Note

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be enabled.
- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys**, **WPA3 Pre-Shared Keys**, or **WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

2. **Allow Resident to Change Wi-Fi Settings**—Solution providers can enable or disable the option for residents to configure their own personalized settings.
3. **Allow Property Manager to Suspend and Terminate Internet Service**—Solution providers can enable or disable the option for property managers to suspend or terminate internet service.
4. Enter the property manager's email address in the **Invite Property Managers** text box to send an invitation. Property managers can activate and oversee internet services for residents within their property.
5. Click **Save**.

Note

Solution providers can select Community Wi-Fi, Personal Wi-Fi, or both options, depending on their requirements.

Design tab

The Design tab in MarketApps allows you to customize the branding and appearance of the property manager and resident portals, ensuring a cohesive and professional user experience.

Figure 548 *Design tab parameters*

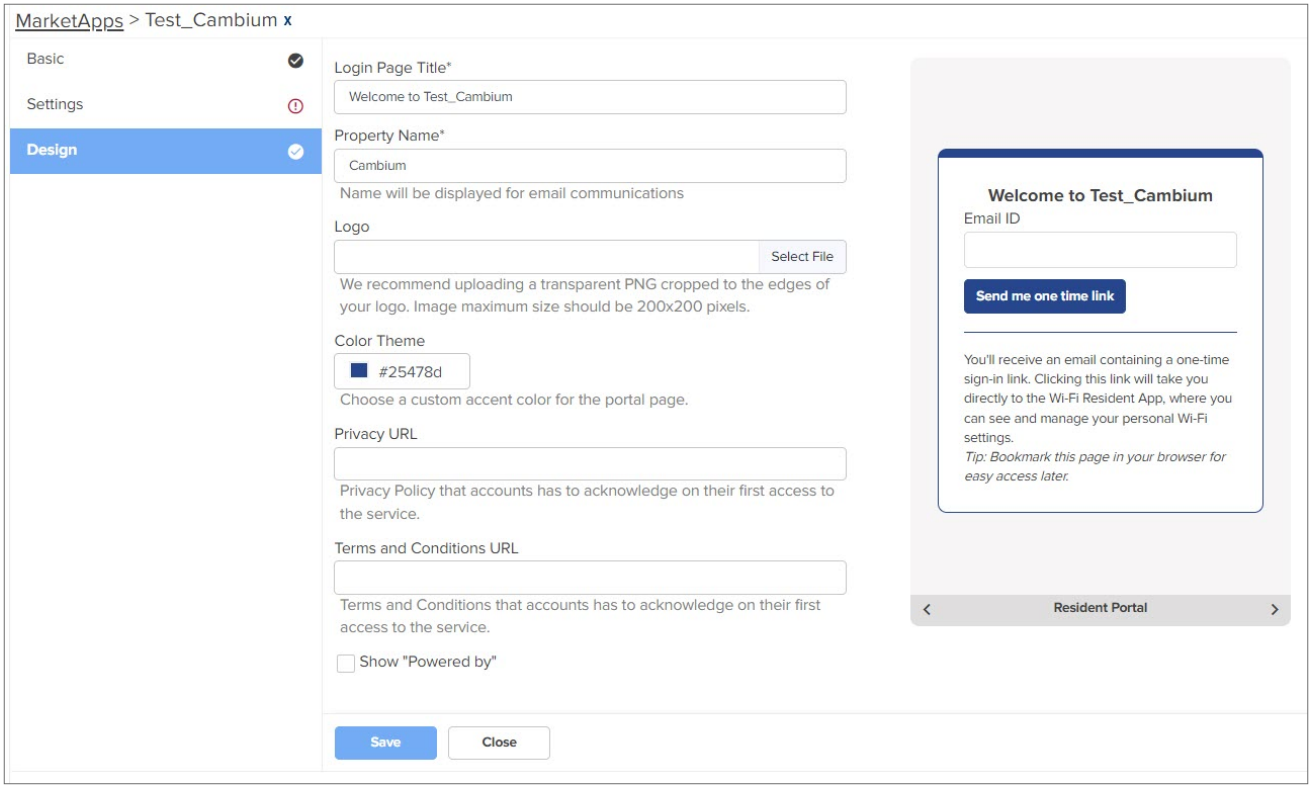


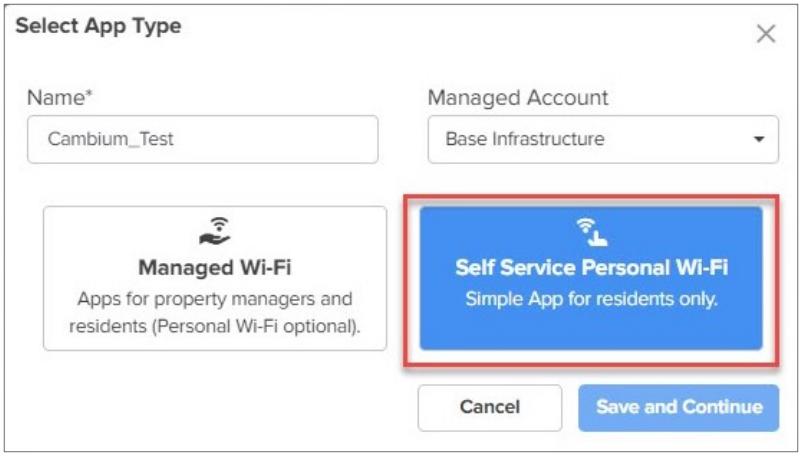
Table 152 *Design tab parameters*

Parameter	Description
Login Page Title	Customize a welcome message displayed on the login page
Property Name	Specify the property name used for internal identification and email communications.
Logo	Upload a logo file (PNG recommended) cropped to the edges and sized up to 200x200 pixels.
Color Theme	Customize the portal's color scheme with a chosen accent color.
Privacy URL	Provide the URL to your Privacy Policy that users must acknowledge on first access.
Terms and Conditions URL	Provide the URL to your Terms and Conditions that users must acknowledge.
Show "Powered by"	Enable this option to display the Powered by message.
Sample screen	The sample screen section includes three views: 1. **Property Manager**—Displays the Property Manager interface where users can enter their email and request a one-time link for access. 2. **Resident Portal**—Shows the Resident Portal interface where users can input their email to receive a one-time link for accessing their personal Wi-Fi settings. 3. **Email**—Provides a view of the email format that users receive, which contains a link to access the Wi-Fi Manager App.

Self-Service Personal Wi-Fi App

The Self-Service Personal Wi-Fi App in MarketApps allows residents to independently manage and customize their Wi-Fi networks within residential properties. This feature provides residents with the capability to create and personalize SSIDs for their units, enhancing their control over network settings.

Figure 549 *Self-Service Personal Wi-Fi App*



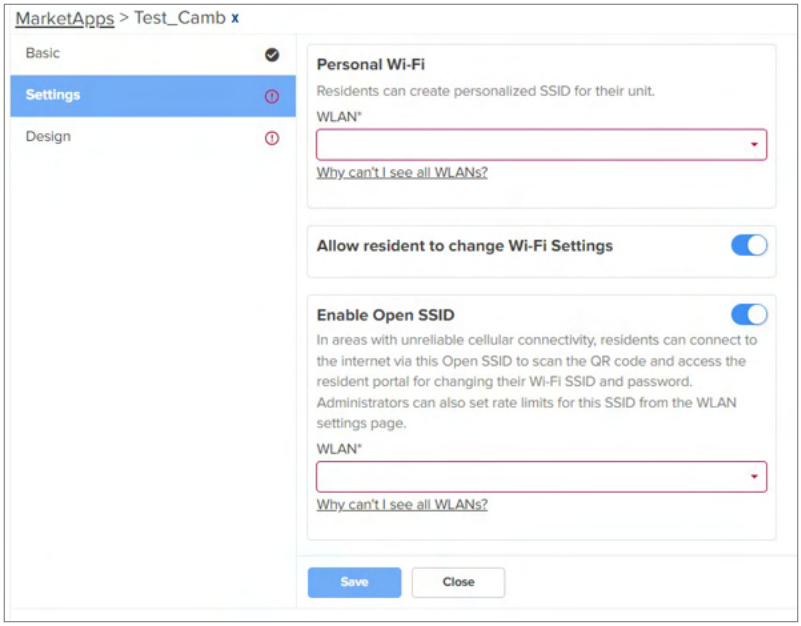
Basic tab

The configuration steps for the Basic tab are the same as those detailed earlier in the documentation. For information on setting the network name, managed account, and description, refer to the Basic tab configuration steps.

Personal Wi-Fi configuration

Residents can create personalized SSIDs for their units, allowing them to customize their network identification.

Figure 550 *Personal Wi-Fi settings*



To configure Personal Wi-Fi, complete the following steps:

1. Select the WLAN for the personal Wi-Fi network from the **WLAN** drop-down list.



Note

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be disabled.
- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys**, **WPA3 Pre-Shared Keys**, or **WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

2. **Allow Resident to Change Wi-Fi Settings**—Solution owners can enable or disable the option for residents to configure their own personalized configuration.
3. **Enable Open SSID** option allows residents to connect to the internet, scan the QR code, and access the resident portal to change their Wi-Fi SSID and password. Administrators can set rate limits for this SSID from the WLAN settings page.
4. Select the WLAN for the Open SSID network from the **WLAN** drop-down list.



Note

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be disabled.
- WLAN Security settings must be configured as Open or OWE.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

5. Click **Save.**

How to configure units by property managers

This sections contains the following topics:

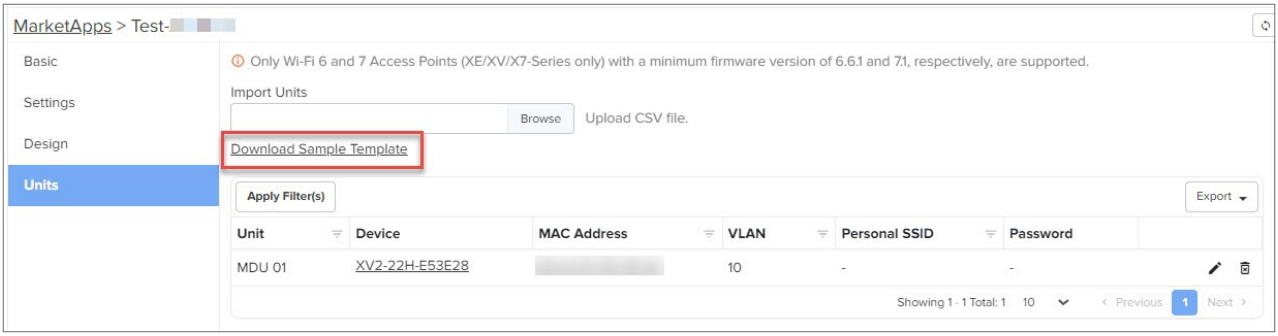
- Units managed in the Managed Wi-Fi App
  - Assign Unit
  - Send Portal Link
  - Suspend
  - Extend
  - Terminate
  - View options in the Property Manager App
- Units managed in Self-Service Personal Wi-Fi App

Units managed in the Managed Wi-Fi App

Managed Wi-Fi enables property managers to configure and oversee network settings for units using cnMaestro.

To set up and manage your Wi-Fi networks, complete the following steps:

1. Navigate to the **Unit** tab and click on the **Download Sample Template** option to get the sample file.

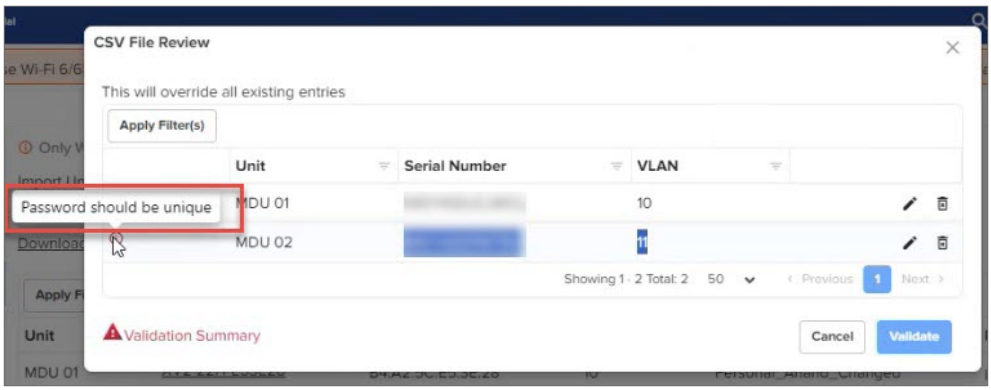


2. An example of the sample template and parameters is shown below:

Unit	Serial Number	MAC Address	VLAN	Personal SSID	Password
Unit name	Serial number of device	MAC Address of device	VLAN ID	SSID for the personal Wi-Fi	Password for Wi-Fi
MDU 01	B1000D000000	B1:00:0D:00:00:00	10	SSID 01	Pa$$Word123
MDU 02	B1000D000001	B1:00:0D:00:00:01	13	SSID 02	Pa$$Word123

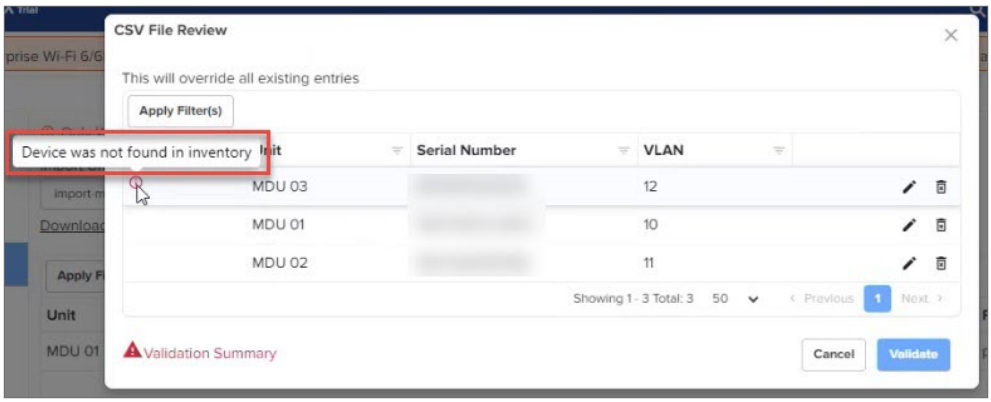
Parameter	Description
Unit	Enter the name or number of the unit (for example, MDU01 and MDU 02 are apartment numbers).
Serial Number	Enter the serial number of the device.
VLAN	Enter the VLAN ID assigned to the unit.
Personal SSID	Enter the SSID for the personal WiFi network.
Password	Enter the password for the Wi-Fi network.

3. After entering the details, save the Excel file with a new name to ensure you have a copy of the filled template and import it to cnMaestro. Note this step is crucial to avoid overwriting the original template.
4. During the import, you might encounter validation error messages. Here are some common error messages and their solutions:
   a. **Password should be unique**—Ensure each unit has a unique password. Modify the password in the template so no two units share the same password.



   b. **Device not found in inventory**—Ensure the serial number and MAC address entered correspond to devices that are already registered in the cnMaestro inventory. Make sure to import the details only after

onboarding the device.



c. **Validates the unit**—Ensure the unit is less than 32 characters and contains only alphanumeric characters, underscores (_), hyphens (-), and spaces.

d. **Checks for duplicate units**—Ensure each unit is unique.

e. **Validates the password**—Ensure the password is between 8 and 64 characters long and does not include ", ', , /, ?, =, -, +, or spaces.

f. **Validates the SSID**—Ensure the SSID is less than 32 characters and contains only alphanumeric characters, underscores (_), hyphens (-), and spaces.

g. **Validates the VLAN**—Ensure the VLAN is an integer between 1 and 4094.

h. **Check if the device is already linked to another EasyApp**—Ensure devices are not linked to another application.

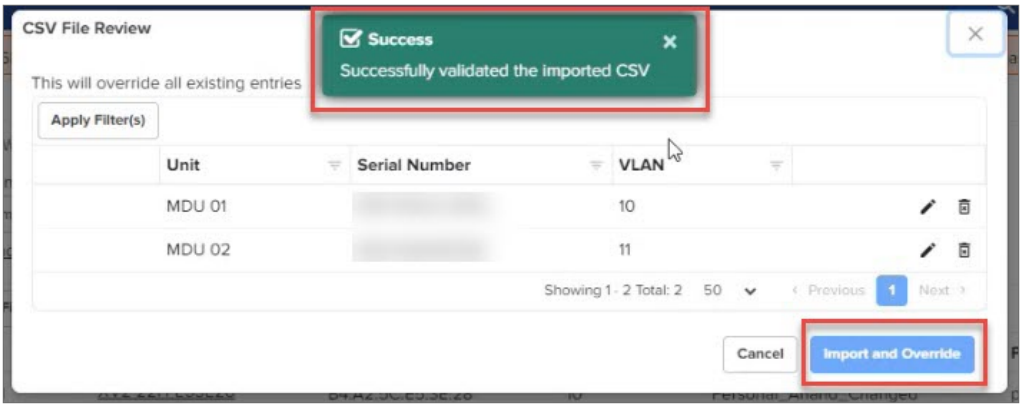
i. **Checks for duplicate devices**—Ensure each device is unique.

j. **Ensures that there is a device present**—Verify a device is specified as it is required.

k. **Validates that the AP group is linked to the personal WLAN**—Ensure the device has an AP group linked with the personal WLAN.

l. **Ensures the SSID is not duplicated**—Ensure each SSID is unique.

5. Once the file imports correctly, you can see the Successfully validated the imported CSV message as shown in the below figure.



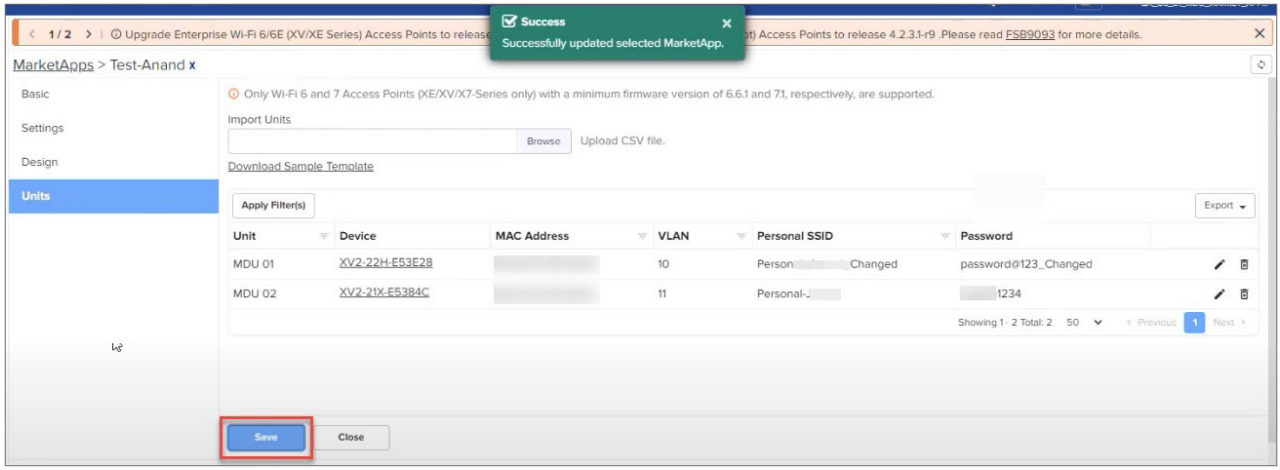
6. Click **Import and Override** to finalize the import process.

Note

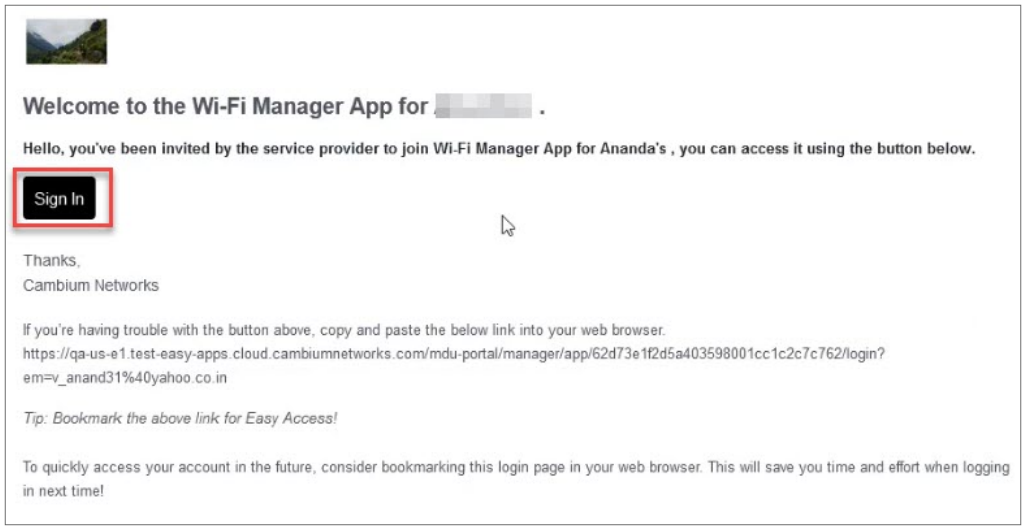
After importing, note the following points:

- Ensure the SSID name and password in the Excel sheet remain unchanged unless updated by the customer.
- Residents can modify their SSID and password through the resident portal later on.
- If **Allow residents to change Wi-Fi settings** (Figure 547) is enabled, tenants can change their SSID and password settings, and these changes do not get overwritten later.

7. Once the devices are successfully added, click **Save**.



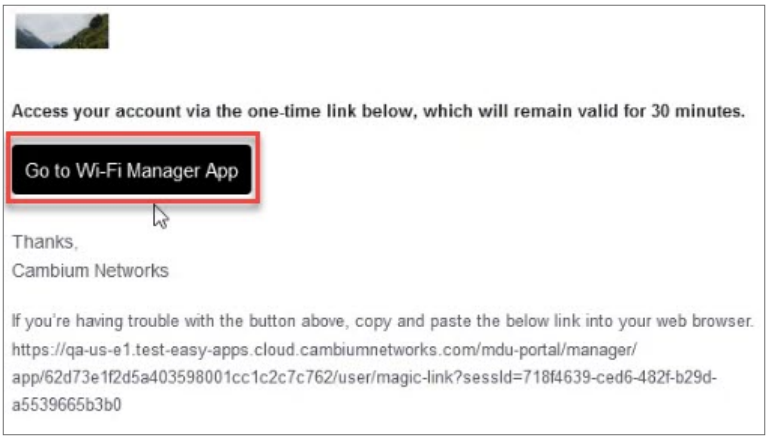
8. The property manager receives an email titled **Welcome to the Wi-Fi Manager APP** and can **Sign In**.



9. The property manager enters the same email ID provided in the Managed Wi-Fi settings.



10. clicks **Send me a one-time link**.
11. The property manager receives an email containing a one-time link for logging into the property manager app.



12. Click **Go to Wi-Fi Manager App.**
13. The Property Manager app interface is shown below.

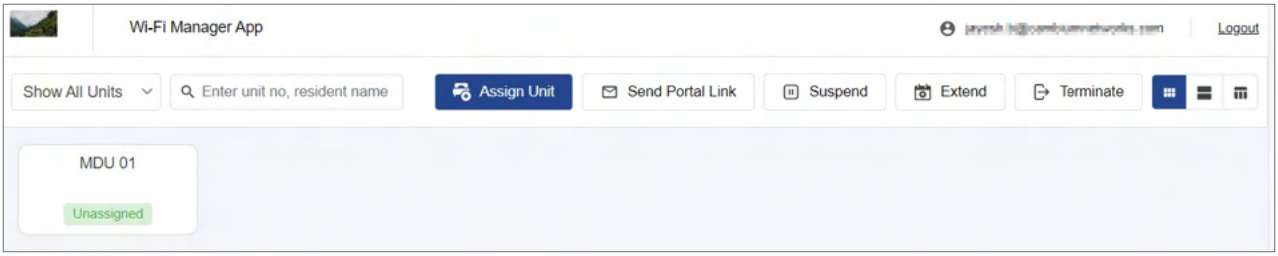


Table 153 *Wi-Fi Manager App Interface*

Options	Description
Show All Units	Provides a drop-down menu with the following options: • **Show Assigned**—Filters the list to display only the assigned units. • **Show Unassigned**—Filters the list to display only the unassigned units. • **Show Suspended**—Filters the list to display only the suspended units.
Search	Allows searching for units or residents by entering the unit number or resident name.

Options	Description
Assign Unit	Assigns a unit to a resident.
Send Portal Link	Sends a link to the resident for accessing the portal.
Suspend	Suspends a unit, making it temporarily inactive.
Extend	Extends the duration of a unit's assignment.
Terminate	Terminates a unit's assignment, making it available for reassignment.

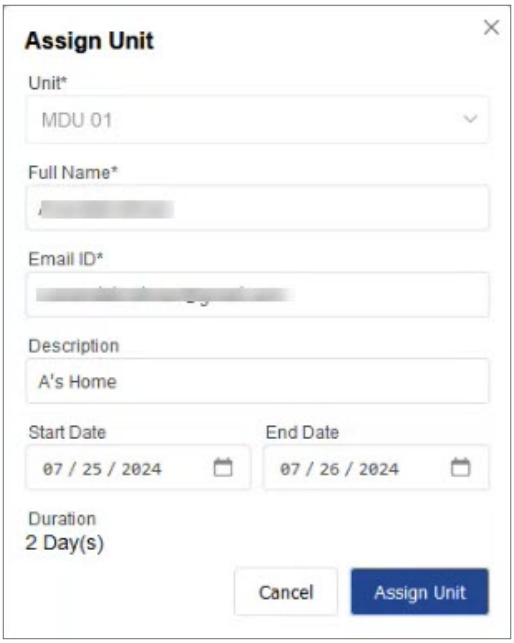
Assign Unit

The Assign Unit option allows property managers to allocate specific units to residents. This feature simplifies tenant management and facilitates communication between managers and residents.

To assign a unit, follow these steps:

a. Click on **Assign Unit** in the Property Manager app.

b. A new window titled **Assign Unit** appears.



c. Select the unit from the **Unit** drop-down menu.

d. Enter the resident's **Full Name**.

e. Enter the resident's **Email ID**.

f. Provide a **Description**.

g. Set the **Start Date** for the assignment.

h. Set the **End Date** for the assignment.

Note: Minimum duration is one day.

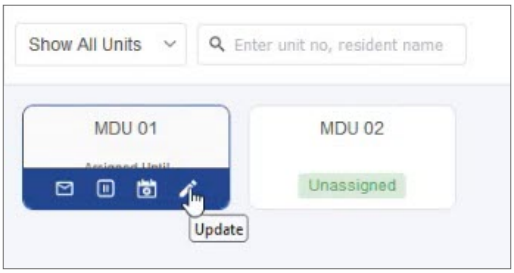
i. Review the **Duration** displayed in days.

j. Click **Assign Unit** to finalize the assignment.

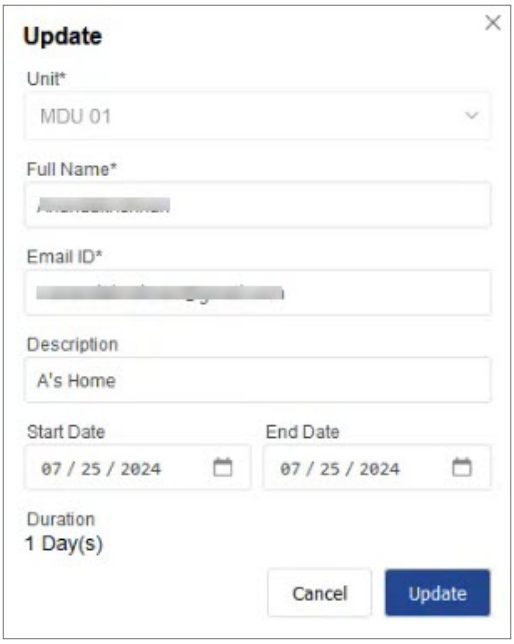
k. A message confirms **Assign Unit action completed successfully**.



l. After updating, if the property manager wants to change any of these parameters, they can do so by clicking the cursor below the unit as shown.



m. A new window titled **Update** appears.



n. The property manager can update any details and then click **Update**.

Send Portal Link

This feature allows you to send the portal link associated with a specific unit to residents or other designated recipients.

To send a portal link, complete the following steps:

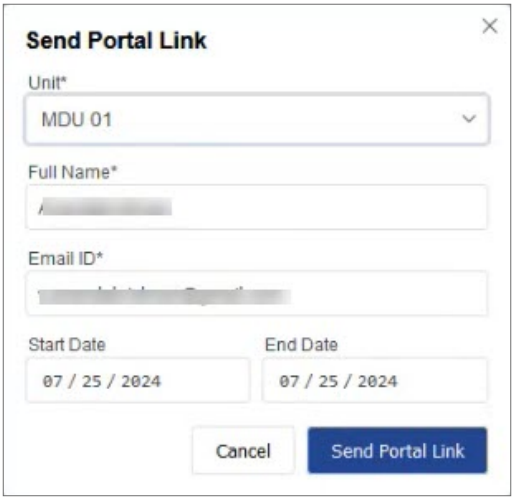
a. Click on the **Send Portal Link** in the Property Manager app.

b. A new window titled **Send Portal Link** appears.



c. Select the unit number or name from the **Unit** drop-down.

d. A new window titled **Send Portal Link** appears.



e. Click **Send Portal Link** to send the portal link.

f. A message confirms **Send Portal Link action completed successfully**.



g. An email is sent to the resident to log in to the resident portal.

Suspend

The Suspend option allows you to temporarily suspend a unit in the Property Manager app.

To suspend a unit, complete the following steps:

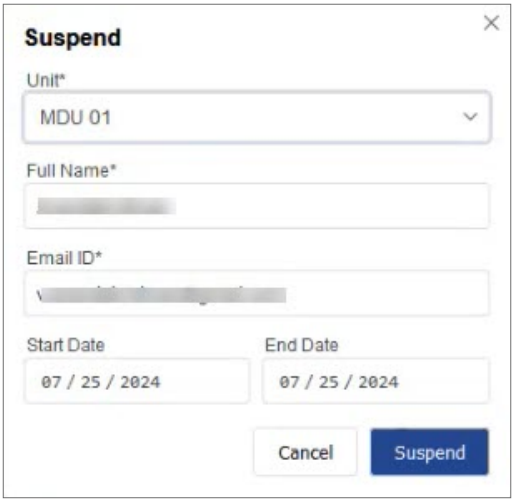
a. Click on **Suspend** in the Property Manager app.

b. A new window titled **Suspend** appears.



c. Select the unit number or name from the **Unit** drop-down.

d. A new window titled **Suspend** appears.

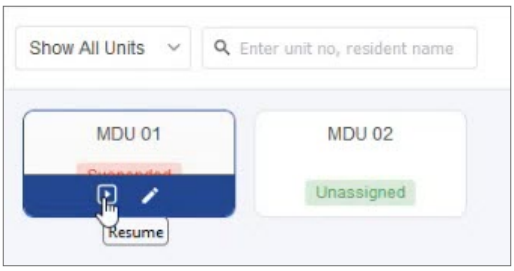


e. Click **Suspend** to confirm.

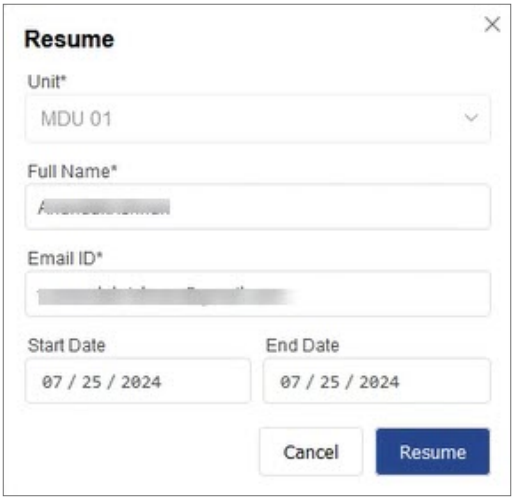
f. A message confirms **Suspend action completed successfully**.



g. After a unit is suspended, the property owner can resume the unit by clicking the cursor below the unit as shown below.



h. A new window titled **Resume** appears.



i. Click **Resume** to confirm.

j. A message confirms **Resume action completed successfully**.



Extend

Extend allows you to prolong the duration of a unit's assignment period within the Property Manager app.

To extend a unit, complete the following steps:

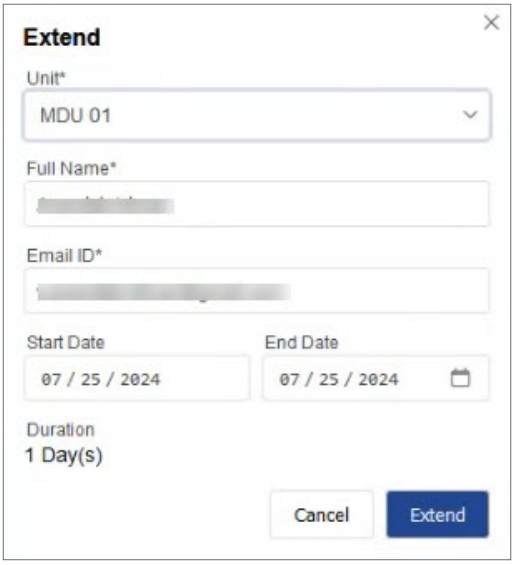
a. Click on **Extend** in the Property Manager app.

b. A new window titled **Extend** appears.



c. Select the unit number or name from the **Unit** drop-down.

d. A new window titled **Extend** appears.



e. Set the **End Date** for the assignment.

f. Review the **Duration** displayed in days.

g. Click **Extend** to confirm.

h. A message confirms **Extend action completed successfully**.



Terminate

Terminate allows you to end the assignment of a unit within the Property Manager app.

To terminate a unit, complete the following steps:

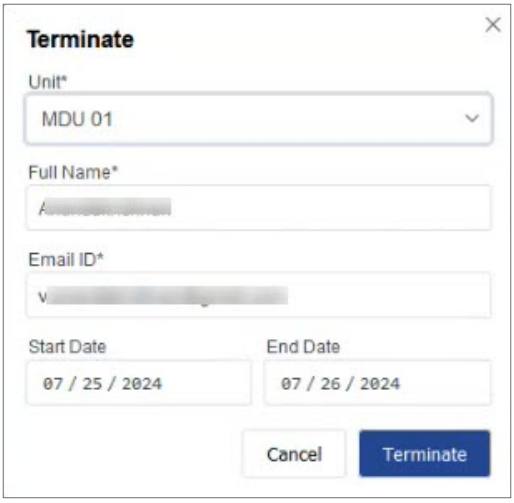
a. Click on **Terminate** in the Property Manager app.

b. A new window titled **Terminate** appears.



c. Select the unit number or name from the **Unit** drop-down.

d. A new window titled **Terminate** appears.



e. Click **Terminate** to confirm.

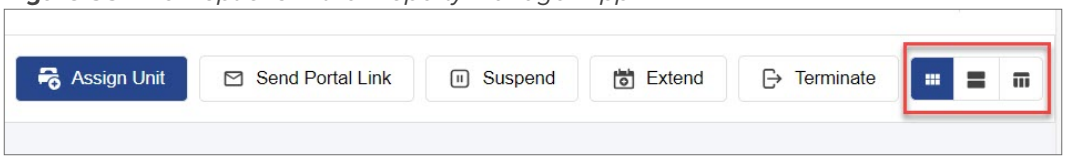
f. A message confirms **Terminate action completed successfully**.



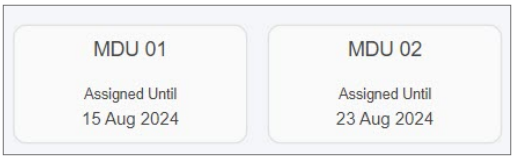
View options in the Property Manager App

In the Property Manager app, there are three different view options to manage units efficiently. These view options can be accessed using icons located at the top right corner of the Property Manager app interface as shown in Figure 551.

Figure 551 *View options in the Property Manager App*

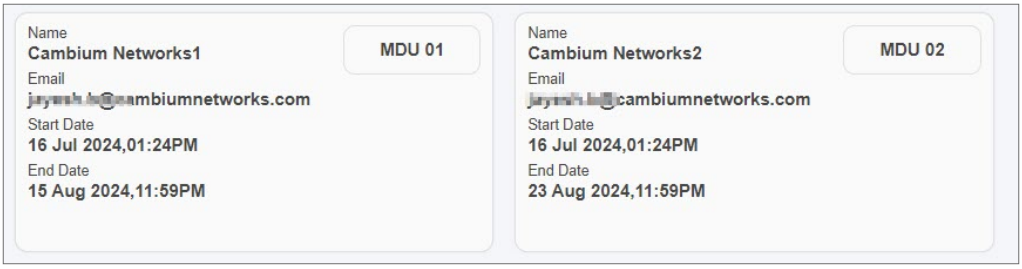


1. **Thumbnail View**—This view displays units as thumbnails or small images, providing a visual representation of each unit.



   Beneath each thumbnail, you can access options such as Send Portal Link, Suspend, Extend, and Update by hovering your cursor over the unit.

2. **Title View**—Units are listed with their names or titles, showing unit name, email ID, start date, and end date for quick reference.



3. **Table View**—Table View presents units in a structured table format with columns for Unit, Status, Name, Email, Start Date, and End Date, allowing for detailed management and organization of unit information.



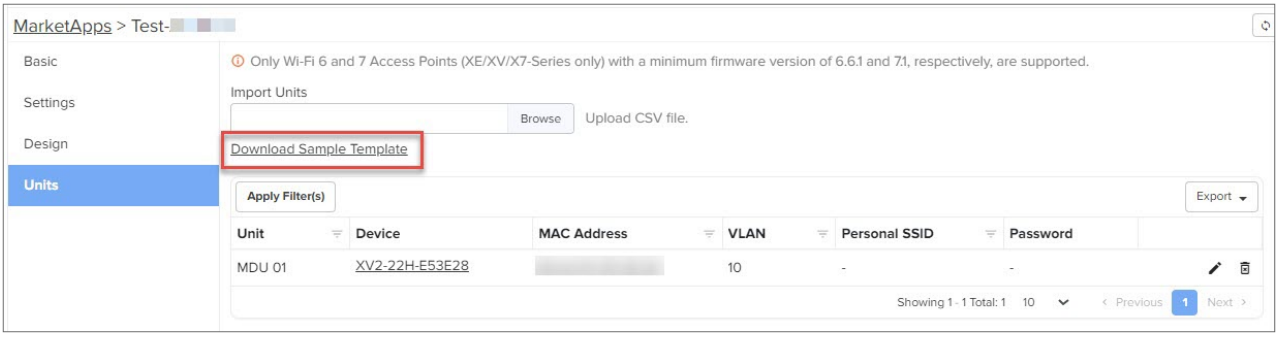
Unit	Status	Name	Email	Start Date	End Date
MDU 01	Assigned	Cambium Networks1	@cambiumnetworks.com	16 Jul 2024,01:24PM	15 Aug 2024,11:59PM
MDU 02	Assigned	Cambium Networks2	@cambiumnetworks.com	16 Jul 2024,01:24PM	23 Aug 2024,11:59PM

Units managed in Self-Service Personal Wi-Fi App

Self-Service Personal Wi-Fi App allows users to configure their personal Wi-Fi networks using cnMaestro.

To set up and manage your personal Wi-Fi network settings, complete the following steps:

1. Navigate to the **Unit** tab and click on the **Download Sample Template** option to get the sample file.

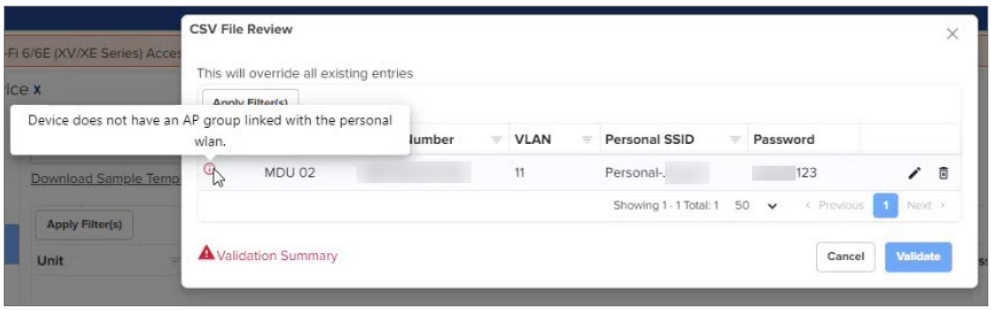


2. An example of the sample template and parameters is shown below:

Unit	Serial Number	MAC Address	VLAN	Personal SSID	Password
Unit name	Serial number of device	MAC Address of device	VLAN ID	SSID for the personal Wi-Fi	Password for Wi-Fi
MDU 01	B1000D000000	B1:00:0D:00:00:00	10	SSID 01	Pa$$Word123
MDU 02	B1000D000001	B1:00:0D:00:00:01	13	SSID 02	Pa$$Word123

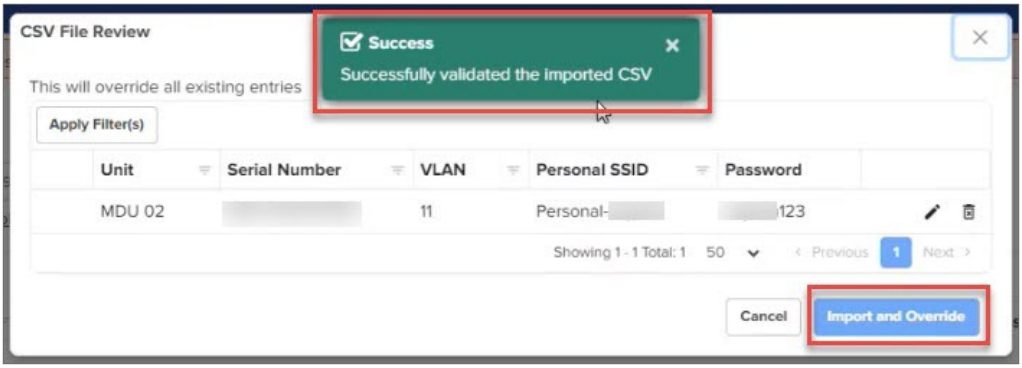
Parameter	Description
Unit	Enter the name or number of the unit (For example, MDU01 and MDU 02 are apartment numbers).
Serial Number	Enter the serial number of the device.
VLAN	Enter the VLAN ID assigned to the unit.
Personal SSID	Enter the SSID for the personal WiFi network.
Password	Enter the password for the Wi-Fi network.

3. After entering the details, save the Excel file with a new name to ensure you have a copy of the filled template and import it to cnMaestro. Note this step is crucial to avoid overwriting the original template.
4. During the import, you might encounter validation error messages. Here are some common error messages and their solutions:
   a. **Device does not have an AP group linked with the personal wlan**—Ensure each device is only linked to one application at a time. Verify the device has an AP group associated with the personal WLAN before proceeding with the configuration.



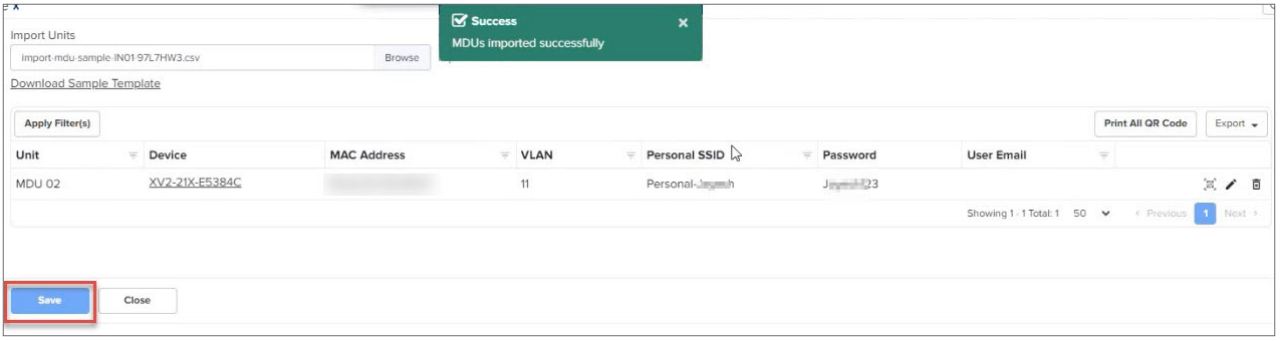
   All the error messages are similar to those described in the Units managed in Managed Wi-Fi sections.

5. Once the file imports correctly, you can see the **Successfully validated the imported CSV** message as shown in the below figure.

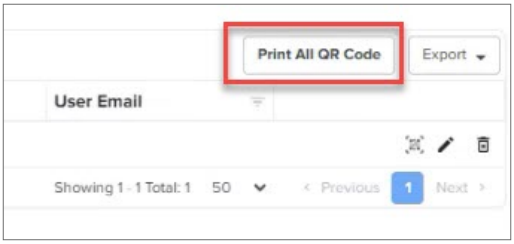


6. Click **Import and Override** to finalize the import process.

7. Once the devices are successfully added, click **Save**.



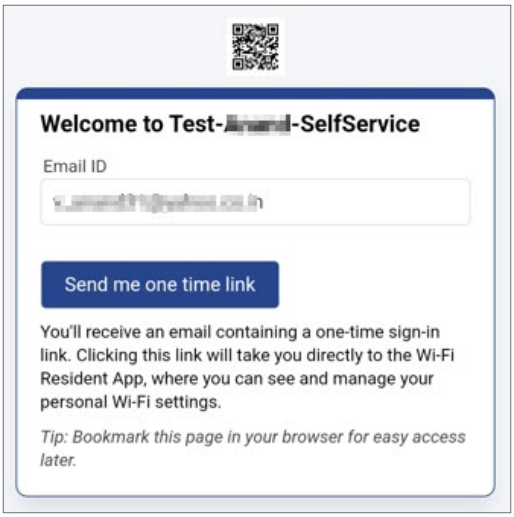
8. Click the **Print All QR Code** option on the right side to open a QR scan page.

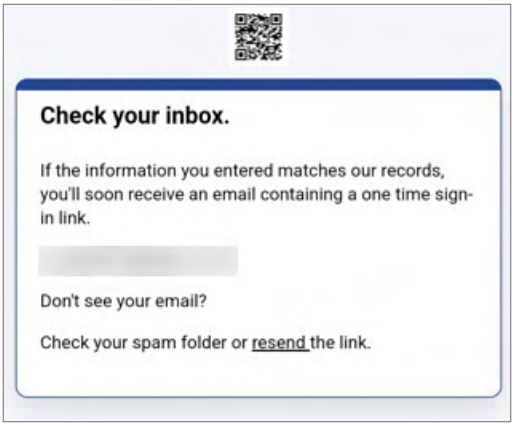


9. Scan the QR code using your mobile device to get a link.

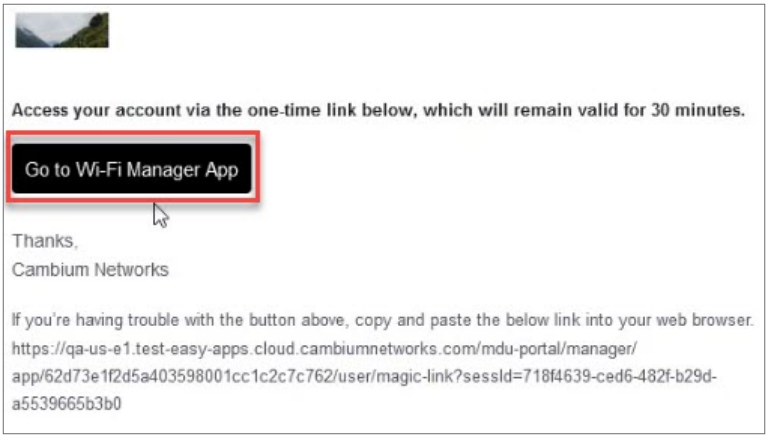


10. Enter your email ID and click **Send me a one time link**.





11. Open the email and click **Go to the Wi-Fi Manager App**.



12. You see a page titled **Welcome to APP** and click on **Change**.



13. A new window titled **Change Wi-Fi Settings** appears. Change your Personal Wi-Fi Network Name and Wi-Fi password in the respective fields.



14. Click **Update**.
15. You receive a message says **Wi-Fi settings updated successfully**.



16. Scan the QR code to verify that your Personal Wi-Fi Network Name and Wi-Fi password have been updated.

RADIUS Proxy X

Note

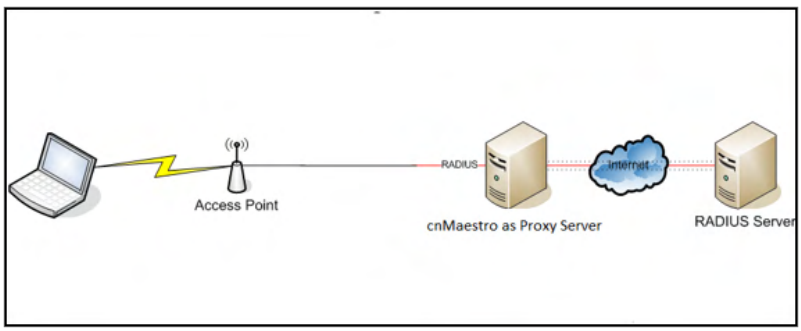
- **RADIUS Proxy** is not supported in cnMaestro Cloud.
- It is available only as a cnMaestro X feature.

Overview

cnMaestro can act as a proxy server to authenticate **RADIUS** requests for cnPilot Wi-Fi devices. In this scenario, cnMaestro acts as a Network Access Server (NAS) for the RADIUS server.

The Access Point sends RADIUS packets to cnMaestro , and cnMaestro sends them to the RADIUS server. cnMaestro can act as a proxy for either authentication or accounting messages, as show in Figure 552.

Figure 552 *RADIUS Proxy on cnMaestro On-Premises*



Minimum version requirements are as follows:

- Minimum cnPilot AP release version required: 3.3.

RADIUS Proxy Configuration

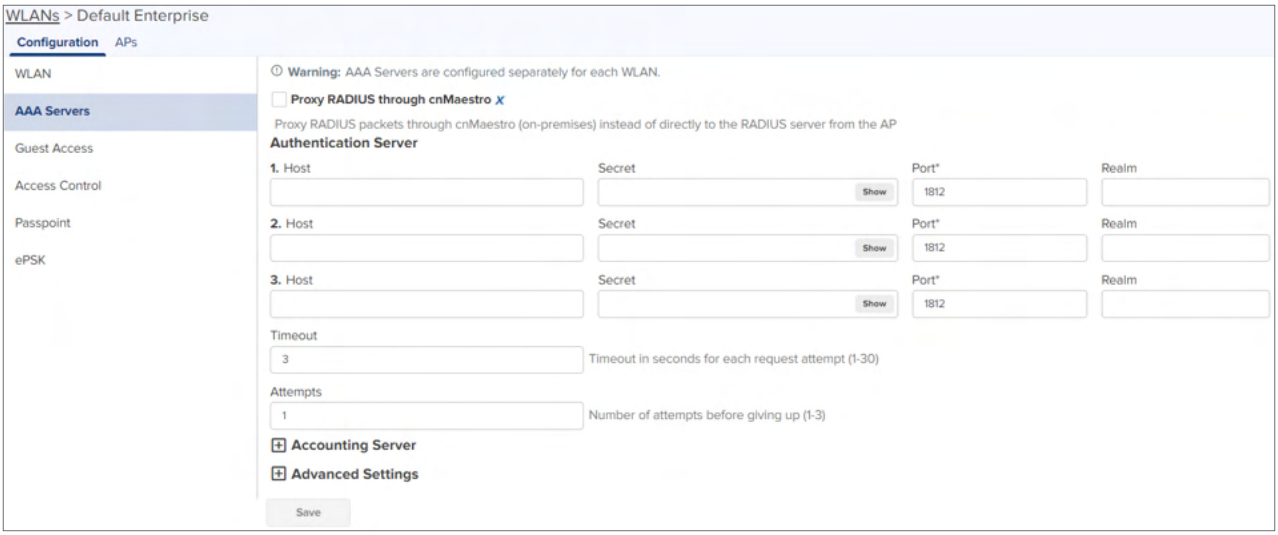
To configure RADIUS Proxy on cnMaestro , perform the following:

1. Navigate to **Shared Settings** > **AP Groups and WLANs** page.
2. Select **Enterprise WLAN** to edit, and then select **AAA Servers.**
3. Under AAA servers, select **Proxy RADIUS through cnMaestro** check box.
4. Configure **Authentication Server** details.
5. Configure **Accounting Server** details.
6. Configure **NAS-Identifier**.

> **Note**
>
> Include **NAS-Identifier** attribute to use the RADIUS request packets and default the system name.

7. Push the configuration from cnMaestro to AP.

Figure 553 *RADIUS Proxy Configuration*



Citizens Broadband Radio Service (CBRS)

This chapter details cnMaestro support for the Citizens Broadband Radio Service (CBRS) subscription which is required to manage CBRS-compliant devices in the 3.6 GHz band (3550 MHz to 3700 MHz).

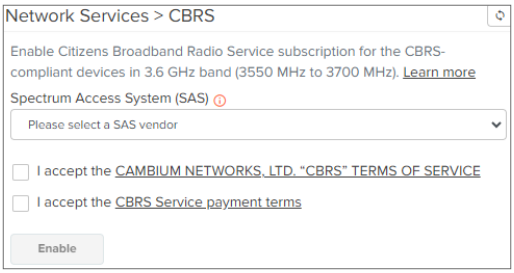
This topic describes the following sections:

- Enabling CBRS in Cloud
- Management Tool
- Domain Proxy View
- Actions for Existing CBRS On-Premises Users

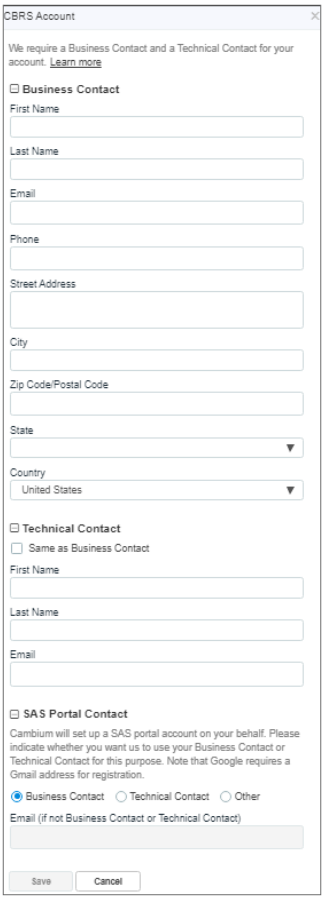
Enabling CBRS in Cloud

1. Login to a cnMaestro Cloud NMS account or Cloud Anchor account (if hosting on an On-Premises instance).
2. Navigate to **Network Services > CBRS** page.
3. Select the preferred SAS vendor from the **Spectrum Access System (SAS)** drop-down list.

   Figure 554 *Network Services > CBRS > Account tab*



4. Read both the terms and conditions, and accept them by selecting the checkboxes.
5. Click **Enable.**
6. In the **Billing Information** window configure the following details:



- **Business Contact**
  - First Name
  - Last Name
  - Email

- Phone
- Street Address
- Zip Code
- Country
- State

- **Technical Contact**

  Enable **Same as Business Contact** or enter a separate Technical Contact.

  - First Name
  - Last Name
  - Email

- **SAS Portal Contact**

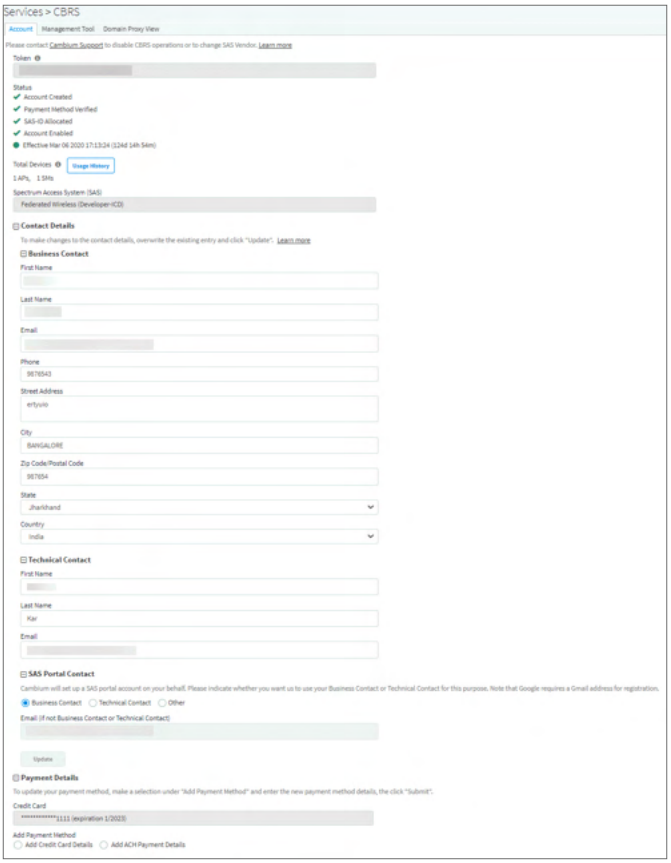
  Cambium Networks creates the SAS portal account on behalf of the operator.

7. Click **Save.**

   The CBRS account is enabled.

After you save the CBRS account, you must complete the following steps:

1. The **Account** page displays the following information and configurable parameters:
   - Token
   - Status
   - Total Devices
   - SAS
   - Contact Details
   - Payment Details



a. **Token:**

Token used for authenticated communication with SAS through Cambium Domain Proxy. It gets generated automatically once CBRS is enabled for the Cloud account.

b. **Status:**

Displays the account status.

Pending Status	Success Status
Status ✔ Account Created ✖ Payment Method Verification Pending ✖ SAS-ID Allocation Pending ● Effective Jul 07 2020 16:54:10 (< 1m) Total Devices ⓘ Usage History 0 APs, 0 SMs	Status ✔ Account Created ✔ Payment Method Verified ✔ SAS-ID Allocated ✔ Account Enabled ● Effective Mar 19 2020 15:02:02 (110d 2h 0m) Total Devices ⓘ Usage History 3 APs, 68 SMs

i. **Account Creation**: Displays as **Account Created** once the account is enabled. Refer to **Step f** for entering contact information and enabling account.

ii. **Payment Method**: Displays as **Verified** once the Payment Details are approved. Refer to **Step g**Payment Details.

iii. **SAS ID**: Once the payment details are verified, the SAS ID is allocated automatically.

Note

When the SAS ID allocation is pending or unavailable in the server,

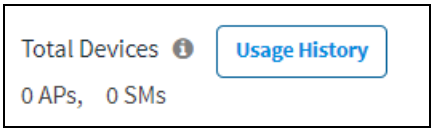
even after the payment details are configured and verified,

It may take up to one day for the SAS ID to be allocated.

iv. **Effective:**

- **Grey**: indicates the **Pending Status**.
- **Green**: indicates **Success Status**.
- **Red**: indicates the account has been **Deactivated**.

c. **Total Devices:** Displays the count of **Total Devices** registered with the SAS using the **Token ID**. **Usage History** provides the list of devices registered with **Month** and **Year**.



Note

Initially the device counts will be 0 APs and 0 SMs.

d. **SAS:** Displays the SAS vendor preferred by the operator.

Note

Contact Cambium support to disable CBRS operation or to change SAS Vendor.

e. **SAS:** An operator needs to select which SAS vendor they prefer.

f. **Contact Details**:

For new CBRS account migrations, this information would have already been entered in Citizens Broadband Radio Service (CBRS). Review and update if necessary, else refer to Payment Details.

Cambium Networks selectively communicates with both the **Business Contact** and the **Technical Contact** with changes of interest: such as SAS administrator updates, CBRS initiative changes from the CBRS Alliance and WInnForum, and announcements of new Cambium Network CBRS features and options.

Business Contact

Cambium Networks communicates with the **Business Contact** for all commercial aspects of the CBRS Service such as invoicing, payment, change in terms, change in pricing, and other details. This page requires:

- **First Name**
- **Last Name**
- **Email**
- **Phone**
- **Street Address**
- **City**
- **Zip code/Postal Code**
- **State**
- **Country**

Technical Contact

Cambium Networks communicate with the **Technical Contact**: such as software updates, release notes, learning guides, technical issues, etc.

- **First Name**
- **Last Name**
- **Email**

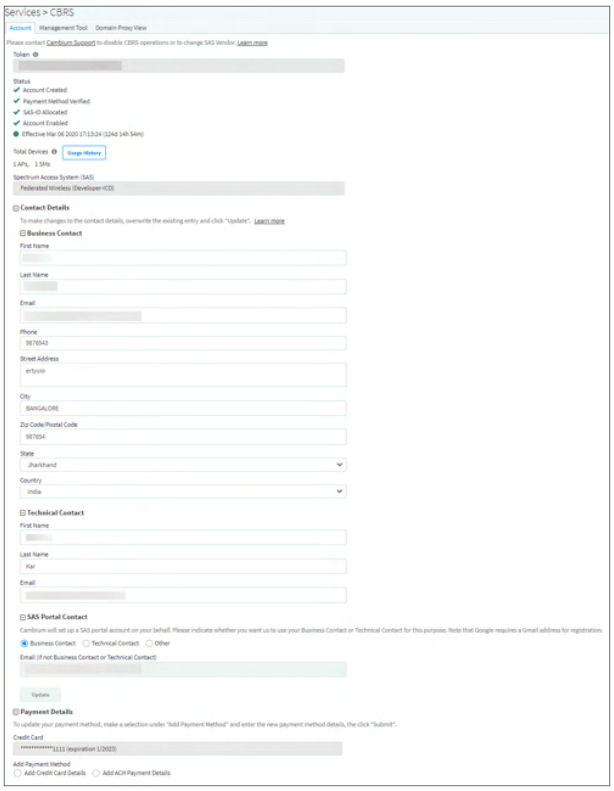
SAS Portal Contact

Cambium Networks sets up the SAS portal account on behalf of the operator. Please select whether to use the **Business Contact, Technical Contact,** or **Other.**

Note

Google requires a Gmail address for registration.

- Click **Update.**



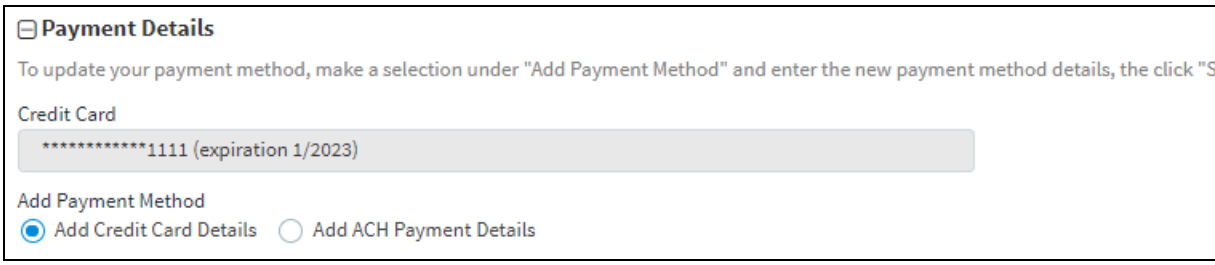
Note

Clicking **Update** on the **Account Page** overwrites the current entries.

g. **Payment Details**

Select one of the payment methods below:

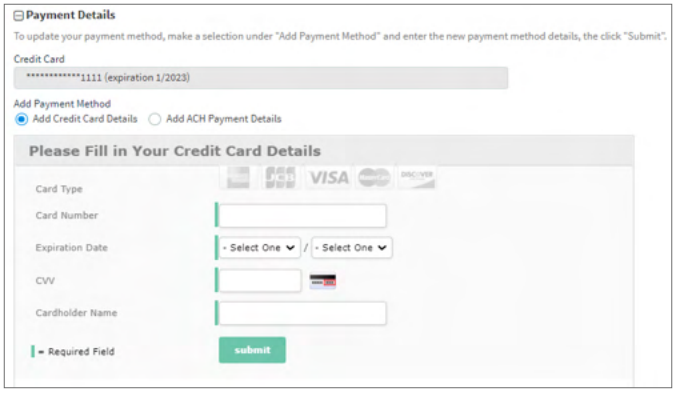
- Add Credit Card Details
- Add ACH Payment Method



Add Credit Card Details

Enter the following and click **Submit**:

- 16 digit Credit **Card Number**.
- **Expiration Date** and **Year** on the card.
- **CVV** and **Cardholder Name**.

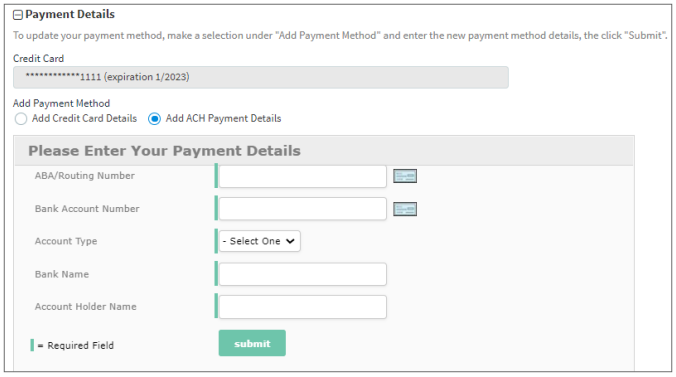


Add ACH Payment Method

Enter the following details and click **Submit**:

- **ABA/Routing Number**.
- **Bank Account Number**.
  - Select one of the following for **Account Type:**
    - Checking
    - Saving
    - Business Checking

- **Bank Name** and **Account Holder Name**.



Management Tool

The Management Tool allows one to register CBRS devices to the SAS provider before physically connecting CBRS-complaint devices to the network. The following Cambium CBRS-compliant devices operate in 3.6 GHz band frequency, ranging from 3550 to 3700 MHz:

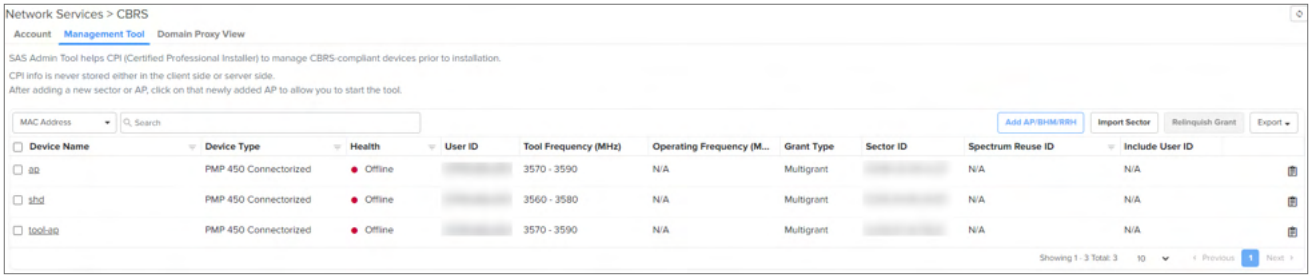
Note

The CBRS Multi-Grant feature was first supported in cnMaestro 3.0.2 and PMP 20.2.

- PMP 450b 3 GHz
- PMP 450m AP 3 GHz
- PMP 450i AP and SM 3 GHz
- PMP 450 AP and SM 3.6 GHz
- PTP 450i BHM and BSHS 3 GHz
- PTP 450 BHM and BHS 3.6 GHz
- LTE 3 GHz cnRanger 201 SM
- LTE 3 GHz cnRanger 210 RRH

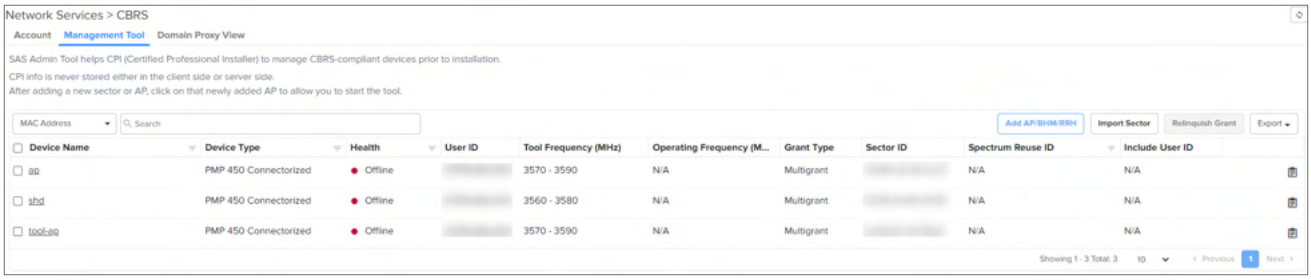
The CBRS procedure can be performed by an authorized CPI (Certified Professional Installer). CPIs are required to enter necessary credentials to update the CBRS parameters.

A CBRS sector view is shown below:



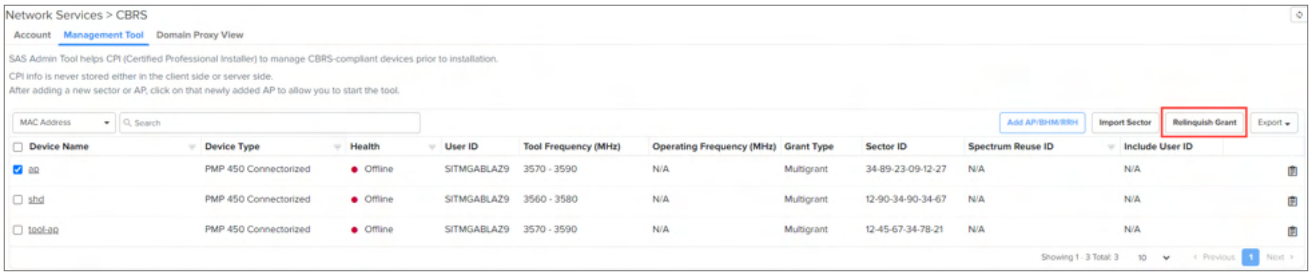
Export

The **Export** button allows one to export multiple device reports in the **CSV** format.



Relinquish Grant

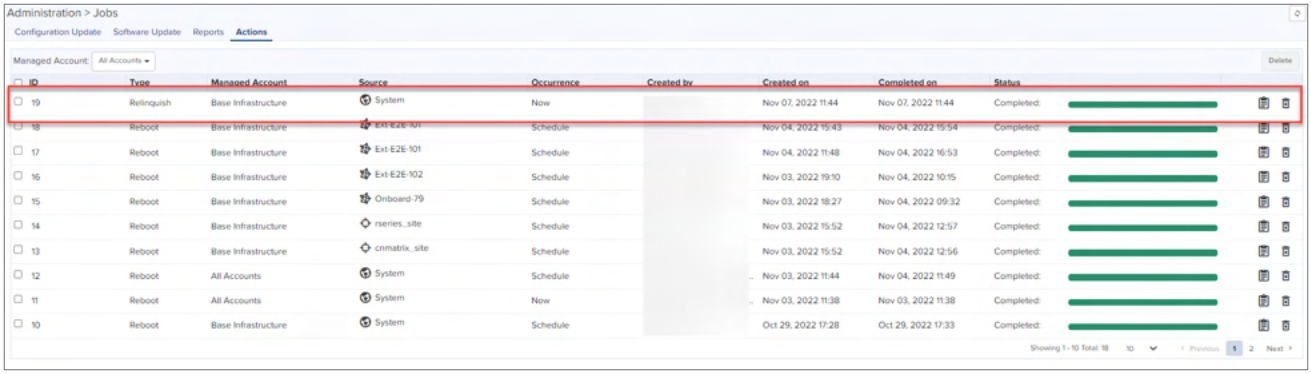
The Relinquish Grant button relinquishes all grants of selected sector and places devices in the Registered state. The device will start the Multi-Grant procedure if the Multi-Grant feature is enabled on the device.



Note

- Relinquish Grant can be performed only for the Config_Synced devices running in Single Grant.
- PMP devices must be upgraded to release 20.2, which supports the Multi-Grant feature.

Relinquish grant creates a job in **Action** page, when relinquish of sector is initiated from **Management Tool** page.



Creating a Management Tool Sector

A sector can be created by two ways:

- Add AP/BHM/RRH: Add all parameters manually of an AP/BHM/RRH.
- Import Sector: Upload a file with details from all sector devices.

Add AP/BHM

1. Navigate to **Services** > **CBRS** > **Management Tools** and click **Add AP/BHM/RRH**.
2. Enter all parameters under the following categories when the user selects the **Mode** as **AP/BHM**:

- **Common parameters**: Device Name, Mode, Device Type, MAC Address, and MSN.
- **Location related parameters:** Latitude, Longitude, Height, and Height Type, Horizontal Accuracy, and Vertical Accuracy.
- **Antenna related Parameters**: External Antenna Gain, Beamwidth, Azimuth, and Down Tilt.
- **Co-Existence related parameters:** Sector ID, Spectrum Reuse ID, and Include User ID.

Note

Include User ID parameter is applicable only for PMP devices, when SAS is **Federated Wireless.**

Select **Yes** or **No** to Include the user ID.

- **Add CPI Certificate**: Certificate File, File Password, CPIR Name.

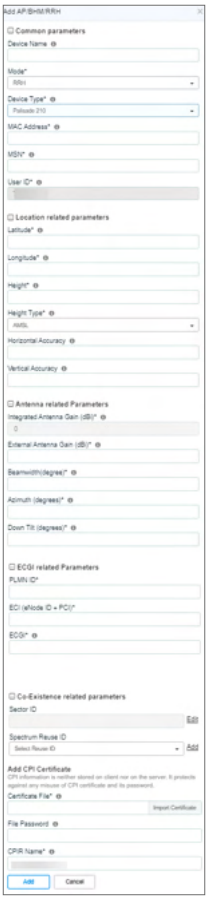


3. Click **Add** to add a sector.

Add RRH

1. Navigate to **Services > CBRS > Management Tools** and click **Add AP/BHM/RRH.**
2. Enter all parameters under the following categories when the user selects the **Mode** as **RRH**:
   - **Common Parameters**: Device Name, Mode, Device Type, MAC Address, and MSN.
   - **Location Related Parameters:** Latitude, Longitude, Height and Height Type, Horizontal Accuracy, and Vertical Accuracy.
   - **Antenna Related Parameters**: External Antenna Gain, Beamwidth, Azimuth, and Down Tilt.
   - **ECGI Related Parameters**: PLMN ID, ECI (eNode ID + PCI), and ECGI.

- **Co-Existence Related Parameters:** Sector ID and Spectrum Reuse ID.
- **Add CPI Certificate**: Certificate File, File Password, CPIR Name.



3. Click **Add** to add a sector.

> **Note**
>
> Refer to CBRS Device Parameters for additional details.

Import Management Tool Sector

To import a sector:

1. Navigate to **Services** > **CBRS** > **Management Tool** and click **Import Sector** button.



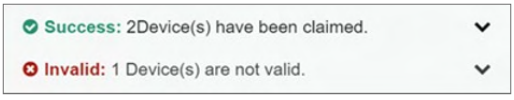
1. Click **Download Template** if user does not have an Import Sector template. Users can download two different template formats:
   a. PMP: Excel or ODS
   b. LTE: Excel or ODS
2. Click **Import Excel** to select **Import Sector** template file. File must be Microsoft Excel format (.xlsx) or OpenDocument Spreadsheet (ods) format.
3. Enter CPI credentials:
   a. Upload CPI Certificate File by clicking **Import Certificate**.
   b. Enter CPI File Password.
   c. Enter CPI Registered Name.
4. Enter the **Sector ID.**
5. Select **Spectrum Reuse ID** from the drop-down.
6. Select **Include User ID**.

   Selecting **Yes** in the **Include User ID** parameter prefixes the **User ID** to the **Sector ID** and **Spectrum Reuse ID** in the registration message of the SAS.

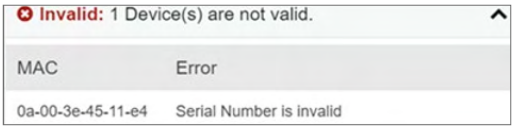
> **Note**
>
> - **Include User ID** is applicable only for PMP devices, when SAS is selected as **Federated Wireless**.
> - See the CBRS Consolidated Procedures Guide and the Cambium PMP Release 20.3 training slides for more details on when to select **Yes** or **No.**

7. Click **Import.**

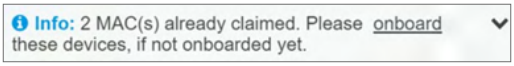
   Import status is displayed as **Success, Info**, and **Invalid**.



8. Details of **Success**, **Info,** and **Invalid** section can be seen by clicking expand ( ) arrow.



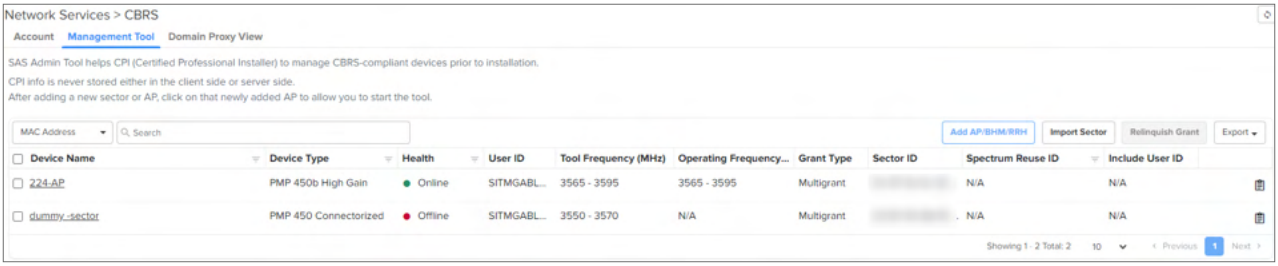
9. If the device is already claimed, it can be onboarded by clicking the onboard link.



Management Tool Sector Statistics

To view Sector Statistics:

1. Navigate to **Services > CBRS > Management Tool.**
2. Click **View Sector Statistics** under **Status**.



3. **Sector Statistics** window pops up.



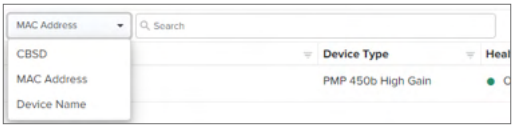
Note

Refer to the CBRS State Diagram for additional details.

Search Management Tool Sector

To search for a sector:

1. Navigate to **Services > CBRS > Management Tool.**
2. Select **CBSD** or **MAC.**
   - For **CBSD**: Search by CBSD ID.
   - For **MAC**: Search by MAC Address.
3. Enter text in search box to display filtered records.

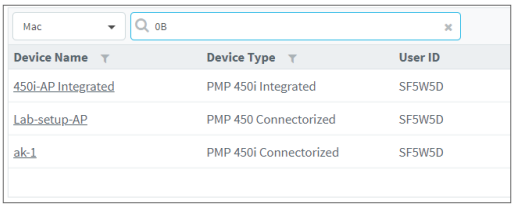


Note

- If an AP device is entered into Search, it displays both AP devices and the related SM

devices.

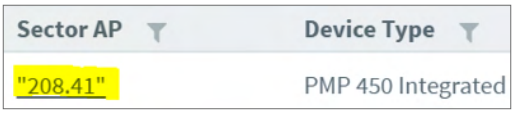
- If an SM devices is entered into Search, it displays only SM devices.



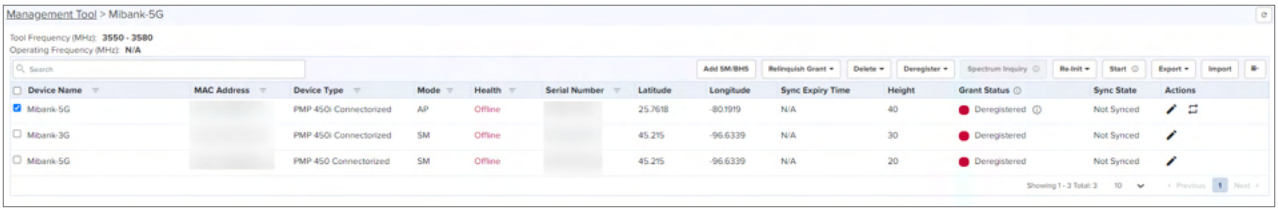
1. Filter AP or sectors can be cleared by clicking or **Clear** button.

Sector View

1. Click a sector from the Sector AP column to get the list of devices.

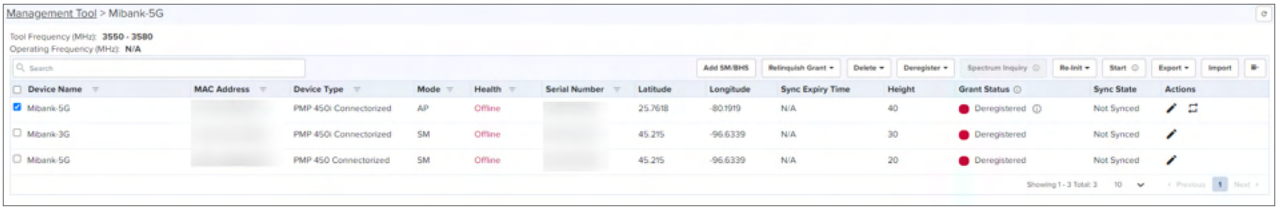


2. All devices of the sector are displayed.



Sector Details View

- The Sector Details view displays the following fields by default:
  - Device Name, Device Type, Mode, Health, MSN, Latitude, Longitude, Sync Expiry Time, Height, Registered, Sync State, Actions.

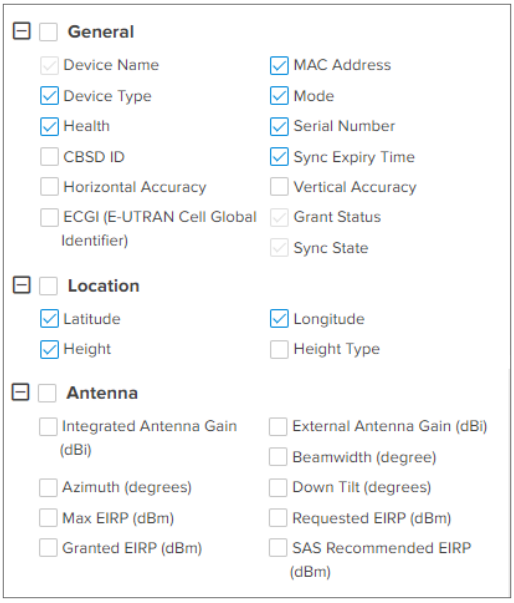


Note

If the device is **Config_Synced**, the CBSD state of the device will be updated from the device in real-time.

- SM can be added in the sector by manually entering all parameters using **Add SM** button or uploading a file containing all SM details using **Import SMs** button.
- Action column can edit or delete any device in the sector. **Edit** and **Delete** buttons are available depending upon the device state. Refer to Edit device and Delete device for more details.
- To include additional fields to be displayed in the **Sector Details** view, select required fields in the column

selector( ).



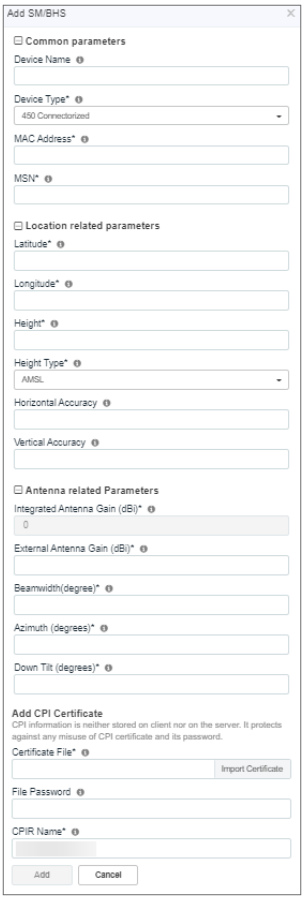
- User can use following button to control the CBRS procedure:



  - **Start** and **Stop**: manage to start and stop CBRS procedure of a sector.
  - **Reinitialize**: restarts the CBRS procedure and reinitializes the devices.
  - **Deregister:** deregisters the device (single or multiple).
  - **Spectrum Inquiry**: checks the availability of frequencies.
  - **Delete**: deletes the device (single or multiple).
  - **Unblock**: clears the de-registered state on an LTE, allowing a registration or reregistration request.
  - **Export**: exports the sector data in .xlsx format.
  - **Import:** imports the SM in the sector.
  - **Relinquish Grant:** relinquishes grants generated in Wide-Grant mode.
- Once the sector is authorized (AUTHORIZED state), button transfers grant details from the Management Tool to real devices.

Add SM or BHS

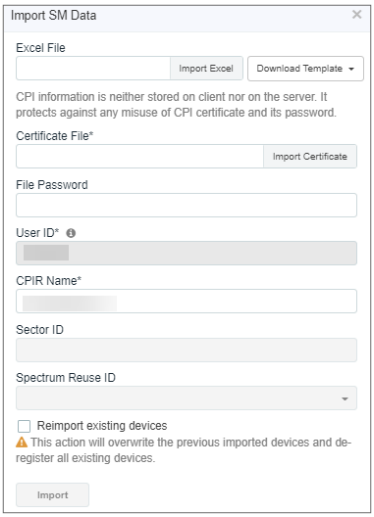
1. Navigate to **Services** > **CBRS** > **Management Tool** > select a sector.
2. Click **Add SM** or **BHS** to add SM in a sector.



3. Enter all parameters under following categories:
    - **Common parameters:** Device Name, Device Type, MAC Address, and MSN.
    - **Location related parameters**: Latitude, Longitude, Height and Height Type, Horizontal Accuracy, and Vertical Accuracy.
    - **Antenna related parameters**: Integrated Antenna Gain, Beam width, Azimuth, and Down Tilt.
    - **Add CPI Certificate**: Certificate File, File Password, and CPIR Name.
4. Click **Add** to add an SM.

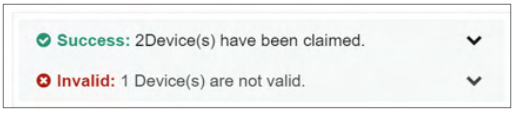
Import SMs

1. Navigate to **Services > CBRS > Management Tool** and select a sector**.**
2. Click **Import** button to import SMs into a sector.
3. Enable the **ReImport Devices** to overwrite the previous imported data and deregister all existing devices.

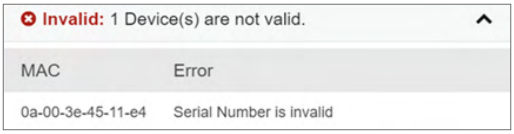


4. Click **Download Template** if user does not have Import Sector template. Users can download two different template formats:
   - PMP: Excel or ODS
   - LTE: Excel or ODS
5. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or Open Document Spreadsheet (ods) formats.
6. Enter the following CPI credentials:
   - Upload CPI Certificate File by clicking **Import Certificate** button.
   - Enter CPI File Password.
   - Enter CPI Registered Name.
7. Click **Import**.

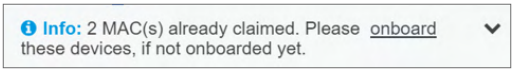
   Import status will be shown under **Success, Info,** and **Invalid** sections.



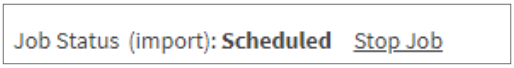
8. Details of **Success**, **Info** and **Invalid** can be seen by clicking .



9. If the devices is already claimed, it can be onboarded by clicking the **onboard** link.



10. Once the user clicks **Import**, a job is scheduled.

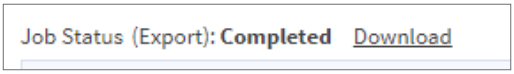


Export Sector

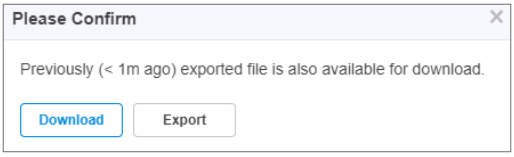
1. Navigate to **Services** > **CBRS** > **Management Tool** and then select a sector.
2. Click **Export** button to export the sector (export as xlsx).



3. Once the user clicks **Export**, a job is scheduled.

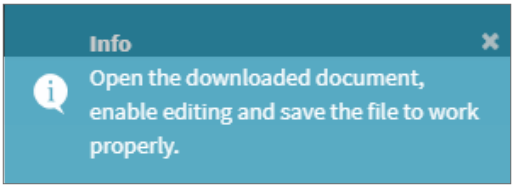


4. Once the Job status is Completed, **Download** the Sector xlxs.



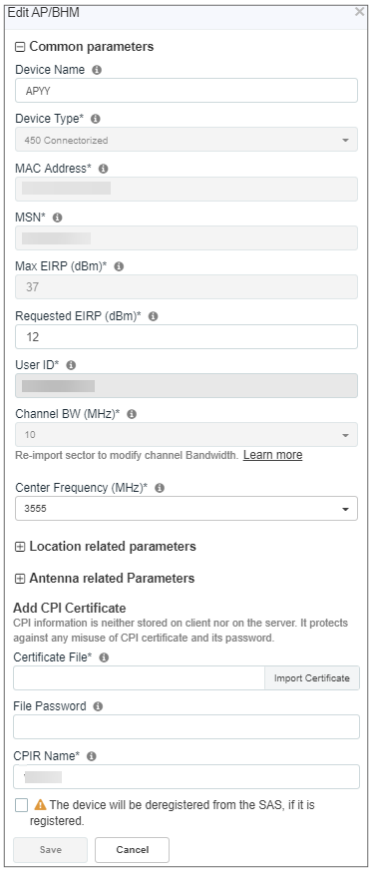
> **Note**
>
> **Download** button is enabled only for two hours after the export job completes.

5. User can use the .xlxs file for importing back into the sector. To import, save the file as shown in the below figure.



Edit Device

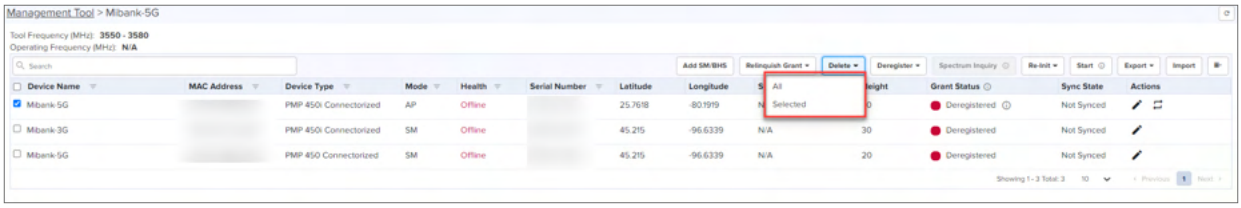
1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector**.**
2. Click **Stop** button if the CBRS procedure is running.
3. Click **Edit** button to edit device parameters.
4. Enter CPI credentials:
   - Upload CPI Certificate File by clicking **Import Certificate** button.
   - Enter CPI File Password.
   - Enter CPI Registered Name.
5. After editing the device. The device should go to derigestered state.



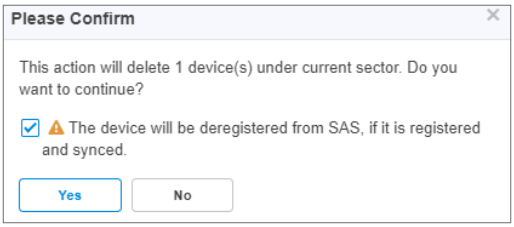
6. Click **Save**.

Delete Device

1. Navigate to **Services > CBRS > Management Tool** and select a sector**.**
2. Click **Stop** button if the CBRS procedure is running (the CBRS procedure is running if the START procedure described below has been invoked, and if all devices in AUTHORIZED state).
3. Deleting SM:
   - Select SM to deregister if it is not in UNREGISTERED state (Refer to the CBRS State Diagram).
4. Once the SM selected click **Delete** and display popup **All** or **Selected.** click **Selected:**
   - **All**: Deletes all registered SM devices.
   - **Selected**: Deletes the selected devices.



5. Click **Yes** to confirm.



6. Once the user clicks **Yes**, a job will be scheduled.



7. Deleting AP:

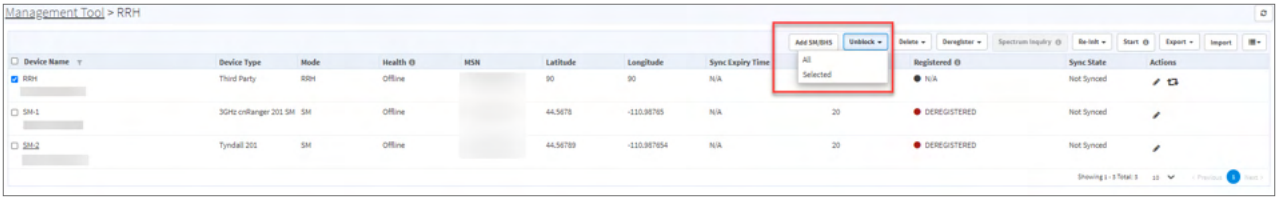
   All SMs of the sector must be deregistered and deleted before deleting the AP. Refer to the Deregistration procedure to deregister all SM devices.

8. Select the AP of the sector to delete.
9. Click **Delete**.

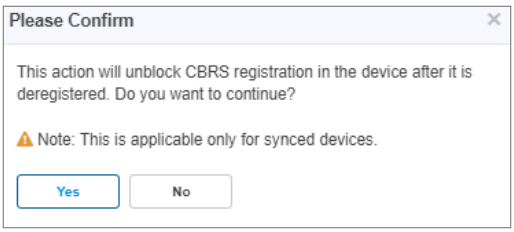
> **Note**
>
> If the procedure is started for the device and it is registered, then, while deleting the device, you must select the **Deregister** checkbox, otherwise the deletion will fail.

Unblock Device

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector.
2. If LTE device is **Config Synced**, and if device deregister flag is enabled, unblock removes the deregistartion flag on the device.
3. Once the device is selected, click **Unblock** and choose **All** or **Selected** from the drop-down**.**
   - **All**: Unblocks all registered devices.
   - **Selected**: Unblocks the selected devices.



4. Click **Selected** display the **Please Confirm** window.

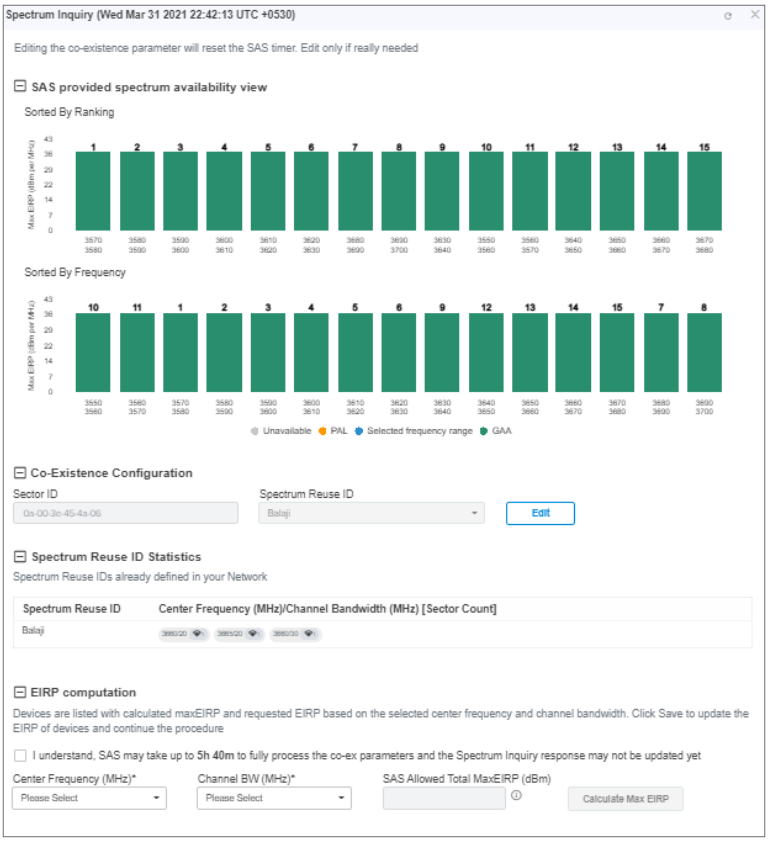


5. Click **Yes** to confirm the action.

Start CBRS Procedure

The Start button starts the CBRS procedure for a sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Start** to start CBRS procedure of a sector.
3. Once the user clicks start, the **Spectrum Inquiry** window pops up.

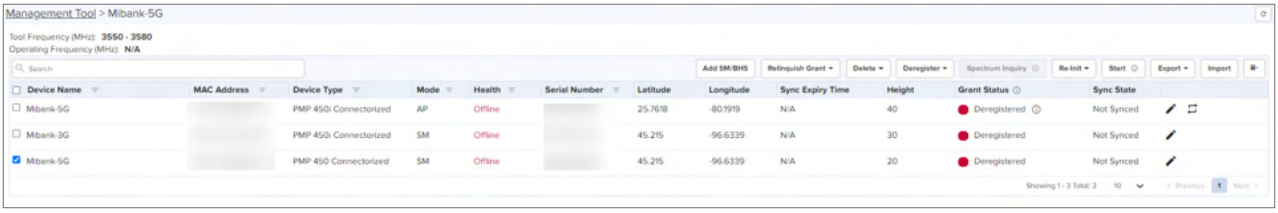


Note

- Multi-Grant is enabled by default.
- **Sorted By Ranking** is applicable for users selecting Google or Federated Wireless SAS.
- User can enable or disable the multigrant only if the device version is less than 21, if device version is 21 and above only multigrant is possible.

4. User can disable the Multi-Grant feature by disabling the checkbox **This feature will enable multi grant on the tool**. For more details refer Multiple Grant.
5. Click **Edit** to edit **Co-Existence Configuration** and **EIRP Computation.**
   - **Spectrum Reuse ID Statistics** displays the devices running on different sector, channels, and bandwidth based on the **Spectrum Reuse ID**.
6. Once the Spectrum Inquiry is verified, click **Save**.

   The Sector is created displays as shown below:



Note

- If the device is already synced with the Management Tool, the CBRS Start and Stop procedures are not applicable for all the synced devices.
- If user does not see the **Start** button, it means the CBRS procedure is already running.
- If all devices of the sector are in AUTHORIZED or HALT status and the user tries to start the CBRS procedure, the **Start** button will go to Stop state (as CBRS procedure is completed for all devices).

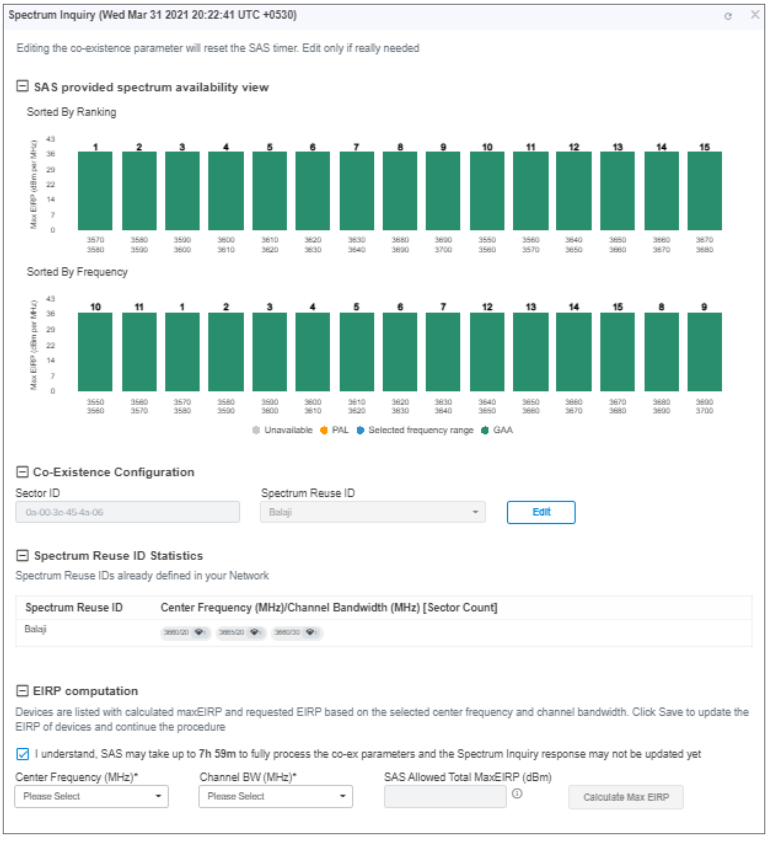
Multi-Grant

Multi-Grant feature divides selected channel bandwidth into multiple of 10 MHz channels. If the selected channel bandwidth is 5 MHz or low/high frequency contains 5 MHz raster, the slice would be in 5 MHz channel. Each slice will initiate a separate Grant procedure.

To enable Multiple Grant for a new sector:

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector.
2. Click **Start** to start CBRS procedure of a sector.
3. Once the user clicks **Start**.

   The Spectrum Inquiry window pops up as shown below.



Note

- Multi-Grant is enabled by default.
- Include User ID is applicable only for PMP devices, if user selects SAS is either Federated Wireless.

4. Click **Edit** to edit Co-Existence Configuration and EIRP Computation.
    - Spectrum Reuse ID Statistics displays the devices running on different sector, channels, and bandwidth based on the Spectrum Reuse ID.
5. Accept the checkbox process of the Co-Existence parameters.

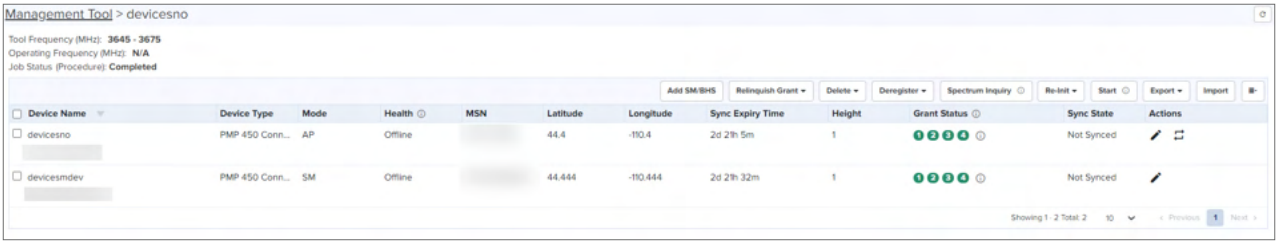


Note

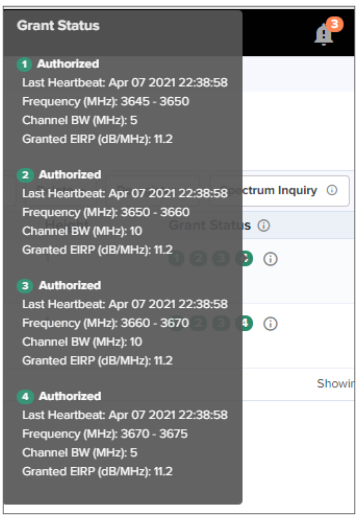
The Federated Wireless or Google SAS might need hours to fully process the Co-Existence parameters in the Registration, (before they are properly reflected in the Spectrum Inquiry Response). For more details see the CBRS Standalone Procedures Guide.

6. Once the Spectrum Inquiry is verified, click **Save**.

   A Sector created with Multiple Grants will be displayed as shown below:



7. To view the Grant Status click the info (ⓘ) icon.



Relinquish Grant

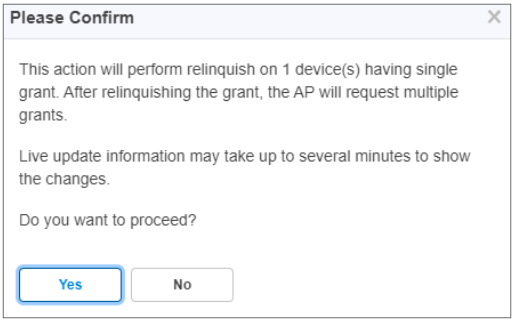
Relinquish Grant relinquishes all grants of selected sector. This will make devices enter the Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on it.

To Relinquish Grant Perform as follows:

1. Navigate to **Services > CBRS > Management Tool** and select a sector with Single Grant.
2. Once the SM is selected, click **Relinquish Grant** to display **All** or **Selected.** Click **Selected.**
    - **All**: relinquish all the registered devices.
    - **Selected**: relinquish the selected device.



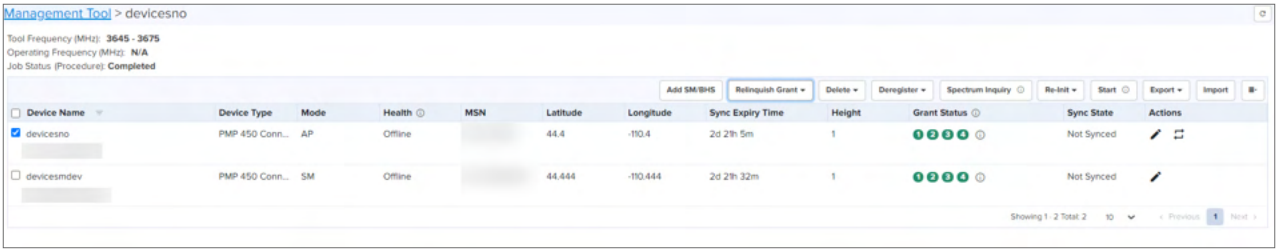
3. Click **Yes** to confirm the action.



Note

Live update information may take upto several minutes to display the changes of reflected relinquish status.

4. Once the user clicks **Yes**, **Wider Grant** gets converted to the **Multiple Grants** as shown below:



Stop CBRS Procedure

The **Stop** button stops the CBRS procedure for a sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector**.**
2. Click **Stop** button to stop CBRS procedure.

Note

- If the device is already synced with the Management Tool, the CBRS Start and Stop procedures are not applicable to the synced devices.
- If user does not see the **Stop** button, it means the CBRS procedure is already in stopped state, **Start** and **Stop** are toggles.
- If all devices of the sector are in AUTHORIZED state, the CBRS procedure will automatically stop.

Reinitialize CBRS Procedure

The **Re-init** button allows the user to start the CBRS procedure for a sector and reinitialize selected devices (Reinitialize = Start of sector + Reinitialization of user selected devices). At least one device must be selected in order to enable the **Re-init** button. Clicking **Re-init** reinitializes selected devices to UNREGISTERED (irrespective of previous CBRS state).

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector.
2. Click **Stop** if the CBRS procedure is already running.
3. Select one or more devices to be reinitialized.

Note

You might notice some delay in enabling **Re-init** button after pressing **Stop.** It is due to a delay in properly stopping the CBRS procedure.

4. Click **Re-init** to start the reinitialization procedure
5. Confirmation window pops up:
   - Click **Continue** or
   - Select **Spectrum Inquiry** to edit the **EIRP values** as shown in Start procedure.



Note

- Synced devices cannot be reinitialized.
- Reinitialize modifies or corrects the parameters. For example, if a device is in HALT state due to a parameter error, the user can stop the CBRS procedure and reinitialize the device after modifying device parameters.

Deregistration

The deregistration procedure allows user to deregister the devices from the SAS server .

1. Navigate to **Network Services** > **CBRS** > **Management Tool** and select a sector.
2. Click **Stop** button if the CBRS procedure is already running.
3. Select one or many devices which need to be deregistered.
4. Click **Deregister** button to deregister selected devices.

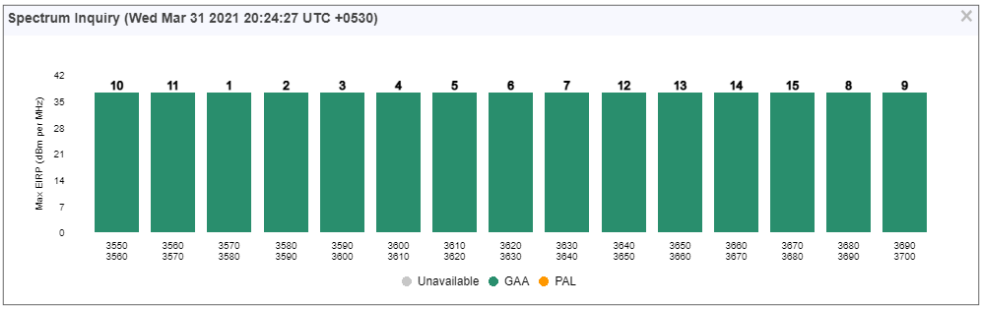
   Once the user clicks **Deregister**, a job is scheduled**.**

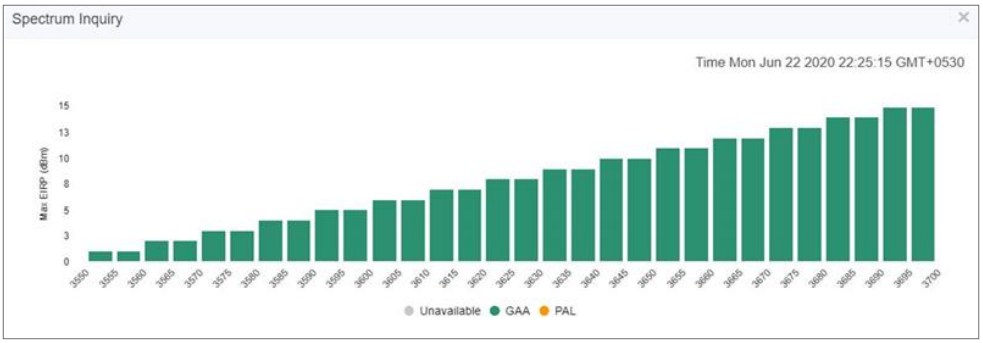
5. If the deregistration fails, the reasons will be indicated under .

Spectrum Inquiry

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a Sector.
2. Click **Spectrum Inquiry** button.
3. **Spectrum Inquiry** status button is enabled once the device is registered (REGISTERED state) to the SAS.
   - If the selected SAS is not Google, EIRP is unsupported, and Spectrum Inquiry is displayed as shown below:



- If the users is selected SAS is **Google,** it supports **EIRP.** Spectrum Inquiry displays as below:



- **GAA**: General Authorized Access
- **PAL**: Priority Access License

Spectrum availability can be checked by hovering over frequencies.

Device Sync

The Sync procedure allows user to transfer grant information from Management Tool to respective device.

For a PMP sector, the Sync action can only be performed on an AP or BHM. The SM and BHS gets synced automatically when it comes online.

For an LTE sector, which supports a Cambium SM with a 3rd party BBU and RRH, the sync action will sync the Cambium SMs in this sector.

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector.
2. Click **Sync** button to perform sync procedure.
3. Click **Yes** on the pop-up or click **NO** to cancel the sync procedure.

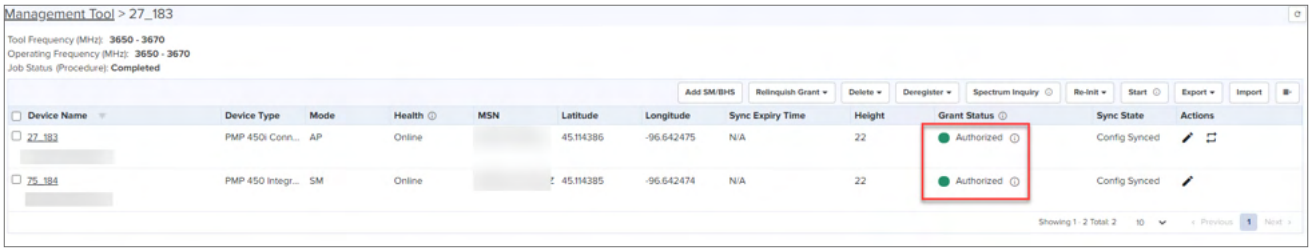
Once **Yes** is clicked, the Management Tool will check the accessibility of AP/BHM before proceeding with sync.

Note

- PMP SM cannot be manually synced. It is only synced automatically.
- Once the device is synced, for both PMP and LTE devices, primary management is transferred from the tool to the device itself. However, some actions and procedures are still supported on the tool. See the CBRS Consolidated Procedures Guide for more details.
- Sync procedure copies complete CBRS parameters to device and enables CBRS to transmit with configured parameters.

Live Status Update

Once the device is **Config synced**, CBRS details like CBSD ID, Grant ID, CBSD Grant State, and Last Heartbeat Time are read from the device every 5 minutes.



It displays the possible single Grant state such as:

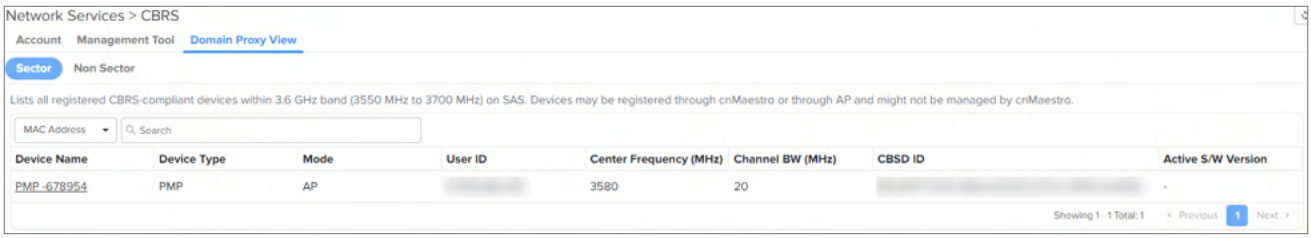
- Authorized
- Deregistering
- Grant
- Grant Suspended
- Grant Terminate
- Registered
- Registering
- Relinquished Spectrum
- Relinquishing Spectrum
- Unregistered
- Unknown

Domain Proxy View

Note

Domain Proxy View is available only on cnMaestro Cloud and the Cloud Anchor account.

In Domain Proxy view, Sectors and Non-Sector page helps check CBRS-complaint devices connected through this server and On-Premises server using the token ID of this server. This page displays all the devices connected to CBRS.



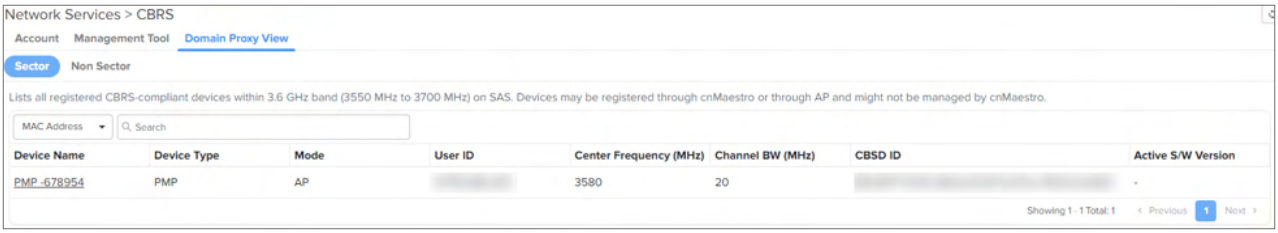
- **Sectors Page**: displays the devices according to the parenting AP list.
- **Non-Sector Page**: displays each individual AP and SM of **LTE** and **PMP**.

Searching a Domain Proxy Sector

To search a sector:

1. Navigate to **Services** > **CBRS** > **Domain Proxy View > Sector** page.
2. Select search option **CBSD or MAC.**

- For **CBSD**: Search by CBSD ID
- For **MAC**: Search by MAC ID.



3. Enter text in search box.



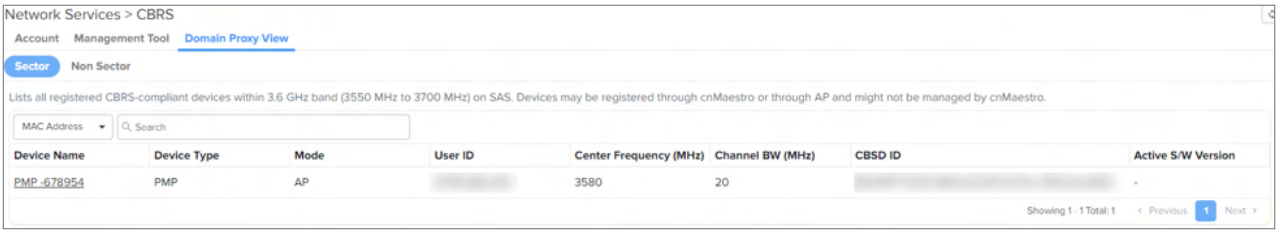
Note

- If AP device is entered , it displays the both AP devices and the related SM device in the search result.
- If SM devices is entered , it displays only the SM devices in the search result.

4. Filtered device can be cleared by clicking **Clear** button.

Domain Proxy Sector view

1. Click a Sector from Sector AP column to get the list of devices.
2. All the devices of the sector will be displayed.



3. CBSD state shows current status of device and whether it is registered or deregistered with SAS.
4. Click **Deregister** to deregister the device from CBRS.
5. The Sectors view displays the following columns by default:

   Device Name, Device Type, Mode, User ID, Center Frequency (MHz), Channel BW (MHz), CBSD ID, and Active S/W Version.

Searching a Domain Proxy in Non Sector View

To search for a device in the non-sector view, complete the following steps:

1. Navigate to **Services** > **CBRS** > **Domain Proxy View** > **Non Sector** page.
2. Select one of the following search options from the drop-down list—**CBSD**, **MAC Address**, or **Heartbeat Status**.
   - For **CBSD**, search by the CBSD ID
   - For **MAC Address**: search by the MAC address of the device
   - For **Hearbeat Status**, search by the heartbeat status of registered devices:

- Heartbeating
- Not Heartbeating for Last 24 Hours
- Not Heartbeating for Last 7 Days
- Not Heartbeating for Last 30 Days
- Not Heartbeating for Last 60 Days
- Not Heartbeating for Last 90 Days



Note

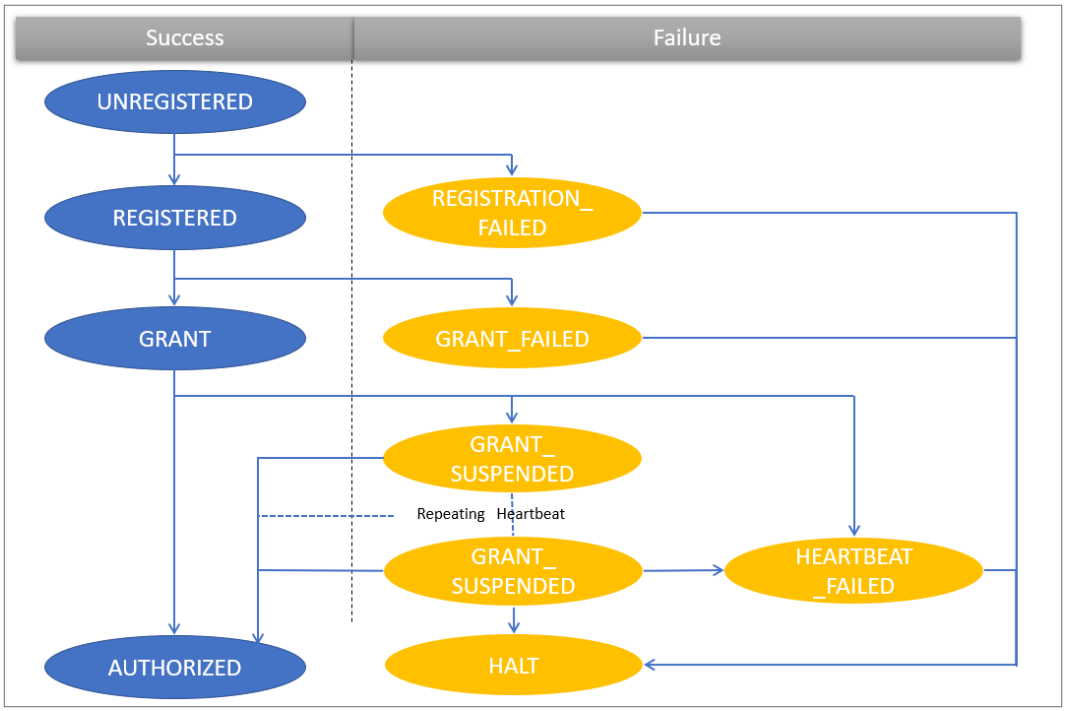
Information in the **Heartbeat Status** and **Last Heartbeat** columns is displayed only for registered devices.

cnMaestro checks the heartbeat status of a CBRS device every 12 hours. The following statuses are updated in the **Heartbeat Status** column, based on whether the device is online or offline:

- **Heartbeating**: When the device is online and the heartbeat check is successful.

  Also, the last successful heartbeat time is updated in the **Last Heartbeat** column.
- **Not Heartbeating**: When the device is offline for 24 hours or more.

CBRS State Diagram



Note

GRANT_SUSPENDED is a temporary suspend state where HEARTBEAT message is sent for an extended period of time prior to obtaining the AUTHORIZED state.

CBRS Device Parameters

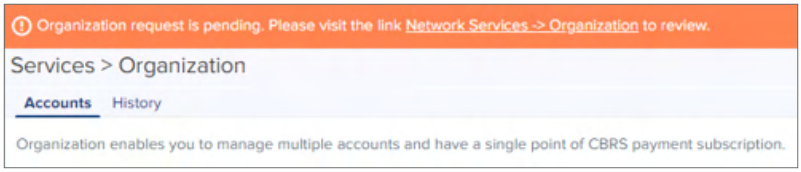
Category	Parameter	Details
Common	Channel BandWidth (MHz)	Channel Bandwidth of AP or BHM in MHz.
	Center Frequency (MHz)	Center frequency of AP or BHM in MHz.
	Device Name	Name given to device on SAS Admin (A maximum of 120 characters are supported. However, this name is not copied to the device when synchronized.)
	Device Type	Drop-down selection of supported devices types.
	MAC Address	MAC address of the device.
	MSN	Serial number of device.
	User ID	Unique identifier is assigned by the SAS. The User ID is part of the registration request message. The wrong User ID leads to REGISTRATION_FAILED.
Location	Height	Device antenna height in meters.
	Height Type	Should be AGL or AMSL as follows: • AGL height is measured relative to the ground level. • AMSL height is measured relative to the mean sea level.
	Horizontal Accuracy	A positive number in meters to indicate the accuracy of the device antenna horizontal location.
	Latitude	Latitude of the device antenna location in degrees.
	Longitude	Longitude of the CBSD antenna location in degrees.
	Vertical Accuracy	A positive number in meters to indicate the accuracy of the device antenna vertical location.
Co-Existence Related Parameters	Sector ID	The default AP MAC address (allows editing the default MAC).
	Spectrum Reuse ID	The Spectrum Reuse ID defined in the network.
	Include User ID	Prefixes the User ID to the Sector ID and Spectrum reuse ID.
ECGI Related Parameters	PLMN ID	Public and Mobile Network Identifier.
	ECI	E-UTRAN Cell Identifier. It is a length of 28 bits and contains the eNodeB-ID.
	ECGI	Enter the both PLMN ID and ECI parameters and it displays in the ECGI field.
	Azimuth (degrees)	Boresight direction of the horizontal plane of the antenna in degrees with respect to True North.

Category	Parameter	Details
Antenna Parameters	Beamwidth (degree)	3-dB antenna beam width of the antenna in the horizontal-plane in degrees.
	Downtilt (degrees)	Antenna downtilt in degrees.
	External Antenna Gain (dBi)	Peak gain of external antenna connected to device in dBi.
	Integrated Antenna Gain (dBi)	Peak gain of integrated antenna in dBi.
Add Certificate	Certificate File	CPI (Certified Professional Installer) certificate.
	CPIR Name	CPI registered name.
	File Password	CPI private password.

Actions for Existing CBRS On-Premises Users

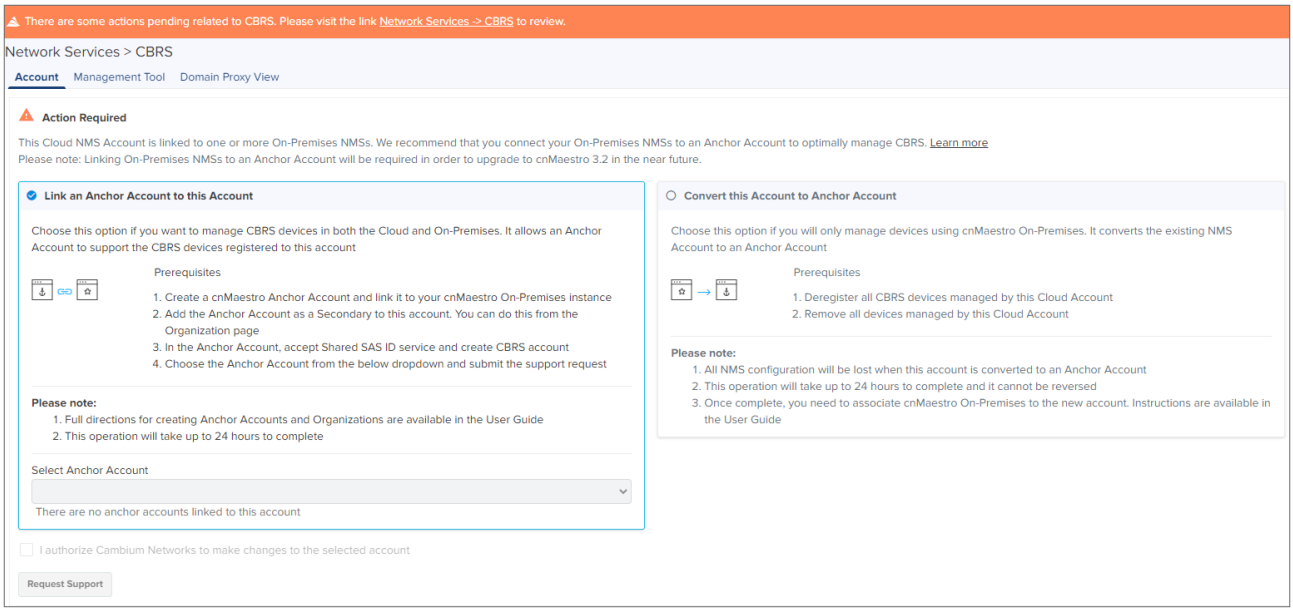
Current CBRS On-Premises customers maintain their CBRS billing and SAS configuration in an NMS Account. This must be updated to support Anchor accounts. To create an anchor account, refer to Manage Instances.

If an action is required for existing Cloud NMS users, the UI will display the following notification:



After clicking the notice, navigate to **Services.**

- **Link an Anchor Account to this Account:** Select if managing CBRS devices in both Cloud and On-Premises. It creates an Organization that shares configuration between a Primary NMS account and a Secondary Anchor account (without deregistering existing CBRS devices).
- **Convert this Account to Anchor Account:** Select only if managing devices On-Premises and NMS do not have any devices. It converts the existing NMS Account to an Anchor Account.



Link an Anchor Account to this Account

Select this to manage CBRS devices in both Cloud and On-Premises. An Anchor account must be created to manage the CBRS On-Premises devices without deregistration.

Note

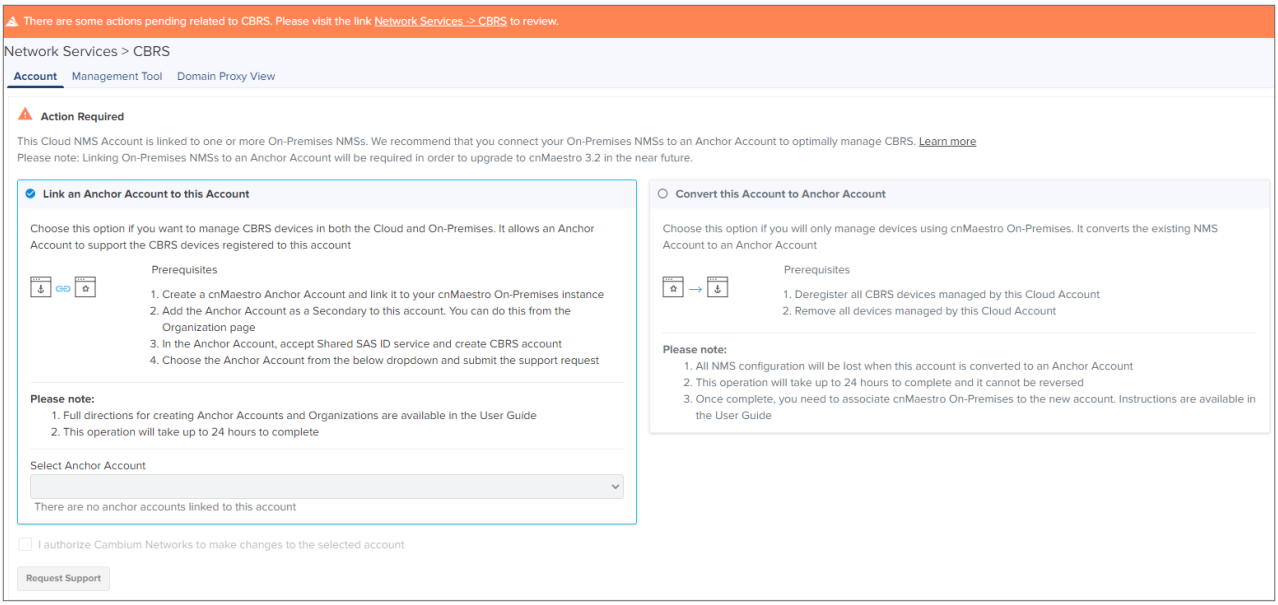
Cambium recommends selecting this option when the user is managing devices in both cnMaestro Cloud and On-Premises.

Before linking an Anchor account, please do the following:

- Ensure the cnMaestro Anchor account is linked to the cnMaestro On-Premises instance(s).
- Add the Anchor account as a Secondary account to Primary NMS account. Refer to Create Organization.

To convert the existing account:

1. Navigate to **Services** > **CBRS** > **Account** page.

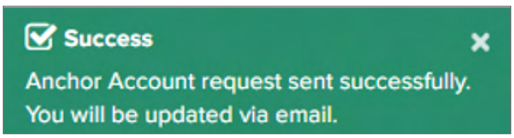


2. Select **Anchor Account** from the drop-down list.

Note

Users are allowed to select only one Anchor account from the drop-down list.

3. Enable **I authorize Cambium Networks to make changes to the selected account**.
4. Click **Request Support** and a **Success** window pops up.



Note

The Cambium Support team validates the request and creates an Organization from the NMS and Anchor accounts within 24 hours. Alternately, you can create the Organization yourself using the directions specified earlier in this document.

Convert this Account to Anchor Account

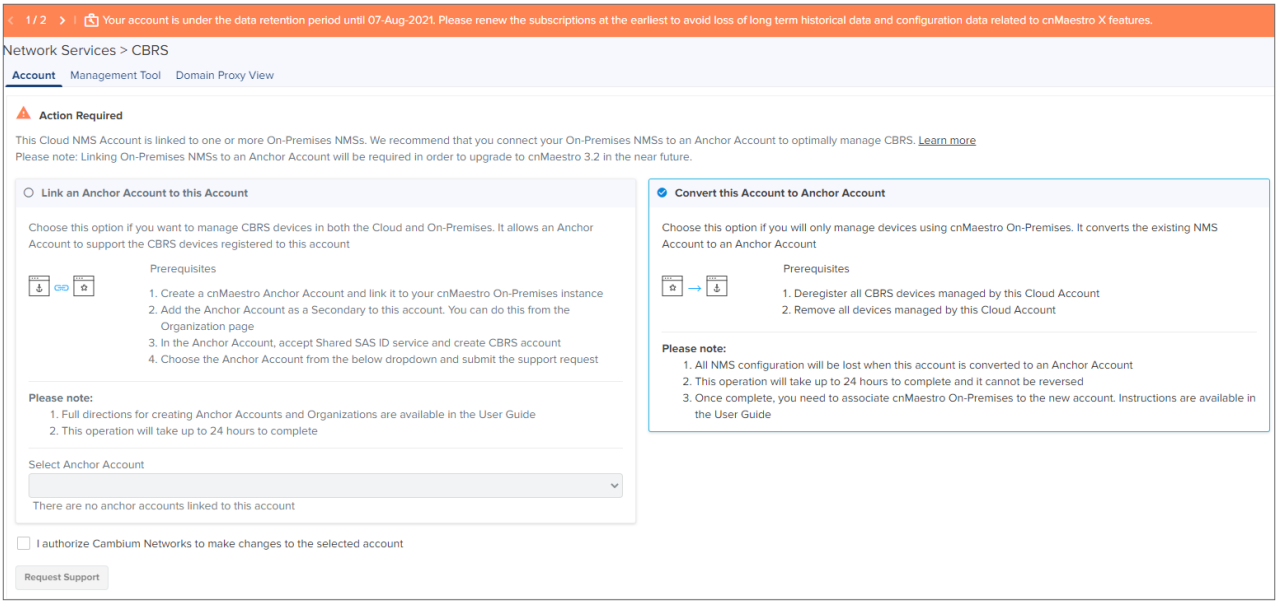
Select this to manage CBRS devices in On-Premises only. It converts an existing NMS account to an Anchor account.

Note

Cambium recommends selecting this option when the user only plans to manage devices using cnMaestro On-Premises. Cloud account devices must be deregisted and deleted from the NMS account and registered back to On-Premises before the conversion.

To convert the existing account:

1. Navigate to **Services** > **CBRS** > **Account** page.

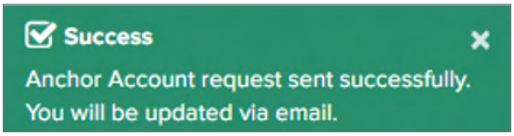


2. Select **Convert this Account to Anchor Account.**

Note

- Deregister and remove all devices from the NMS account before the conversion.
- All NMS configuration will be lost when the account is converted to Anchor, including:
  - Guest Access Portal
  - Templates
  - Performance Graph Data, etc.
- The process of converting an NMS account to an Anchor account cannot be reversed.

3. Provide your consent by selecting the **I authorize Cambium Networks to make changes to the selected account** checkbox.
4. Click **Request Support** and the following success message is displayed.



The Cambium Support team validates the request and creates an Organization from the NMS and Anchor accounts within 24 hours.

Organizations for CBRS

An Organization allows multiple accounts to share CBRS billing and SAS ID. The Primary Account owns this configuration, and the Secondary Account can optionally share it. Both accounts must authorize the sharing.

Note

- There is only one Primary Account in an Organization.
- CBRS configuration can be set in the Primary Account and optionally shared to Secondary Accounts.

This chapter provides the following information:

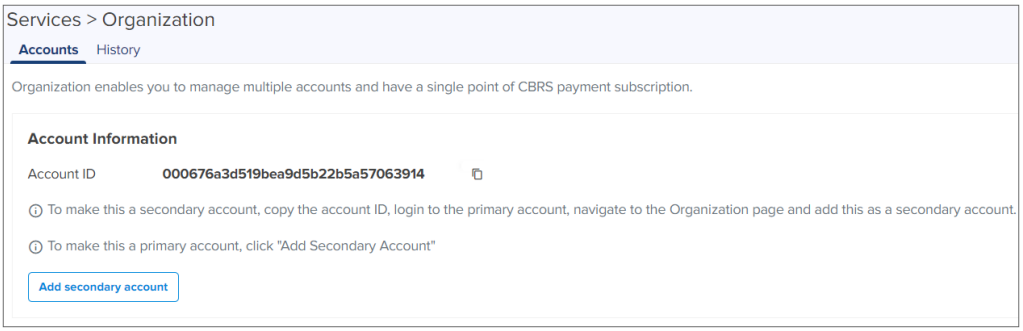
- Create an Organization
- Remove Accounts
- Disable Secondary Account Services
- Edit Services
- Share CBRS Configuration with the On-Premises Instance
- Organization History

Create an Organization

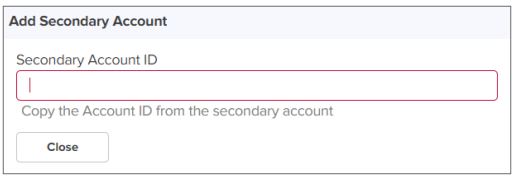
Primary Account

Perform the following steps on the Primary Account:

1. Navigate to **Network Services** > **Organization** > **Accounts**.

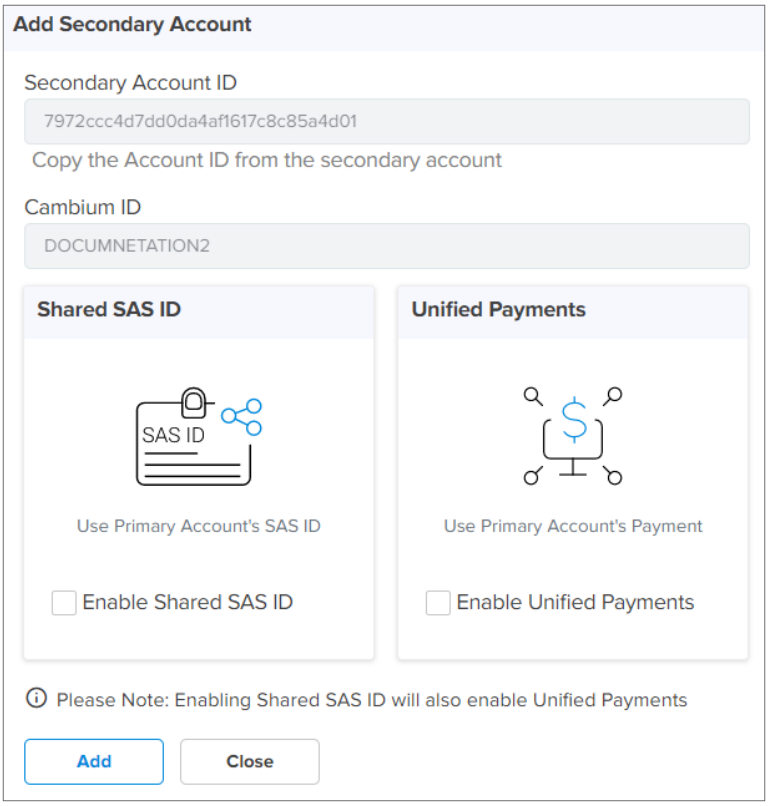


2. Click **Add Secondary Account**.



   Navigate to the planned Secondary Account and copy the Account ID of the Secondary Account using the Copy to Clipboard.

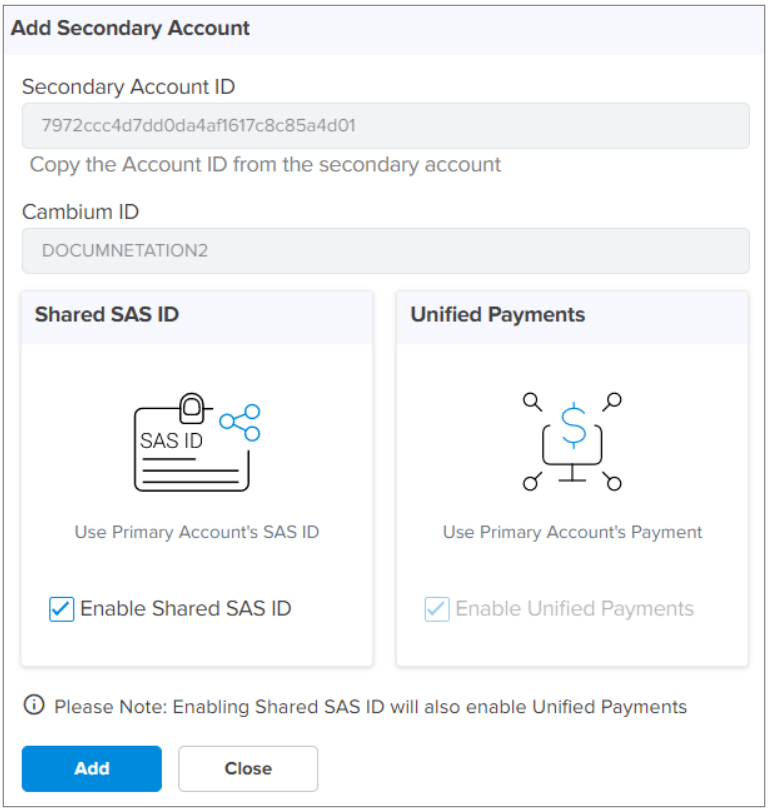
3. Paste the copied **Account ID** in the **Secondary Account ID** text box.
4. Once the Secondary Account is validated, the **Cambium ID** is displayed as shown below.



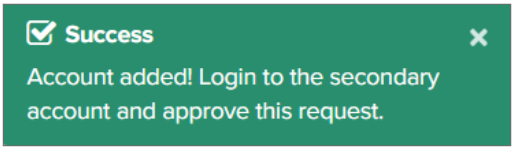
5. The Primary Account can offer services such as:
   - **Shared SAS ID**: This allows the Secondary Account to use the CBRS SAS ID configured in the Primary Account.
   - **Unified Payments**: This allows the Secondary Account to use payment details configured in the Primary Account.

> **Note**
>
> Sharing the SAS ID automatically enables **Unified Payments**.

6. Enable the Services **Shared SAS ID** or **Unified Payments**.



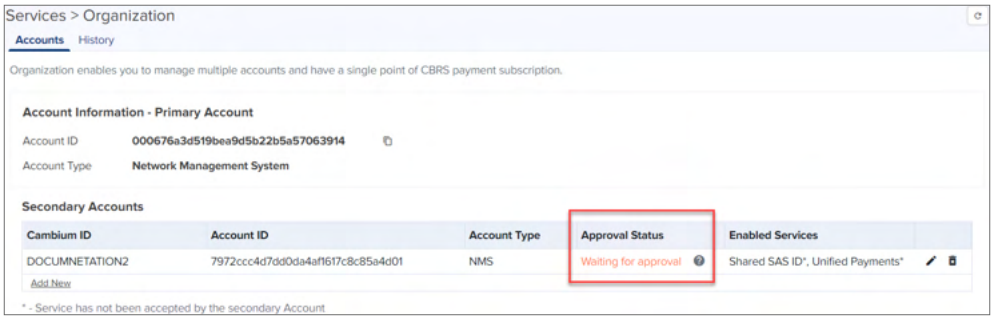
7. Click **Add**. It displays the **Success** message as shown below:



Note

The Secondary Account administrator must approve this request from the Primary Account to join the Organization.

8. 1. In the **Secondary Accounts** table, the **Approval Status** is displayed as **Waiting for approval**.

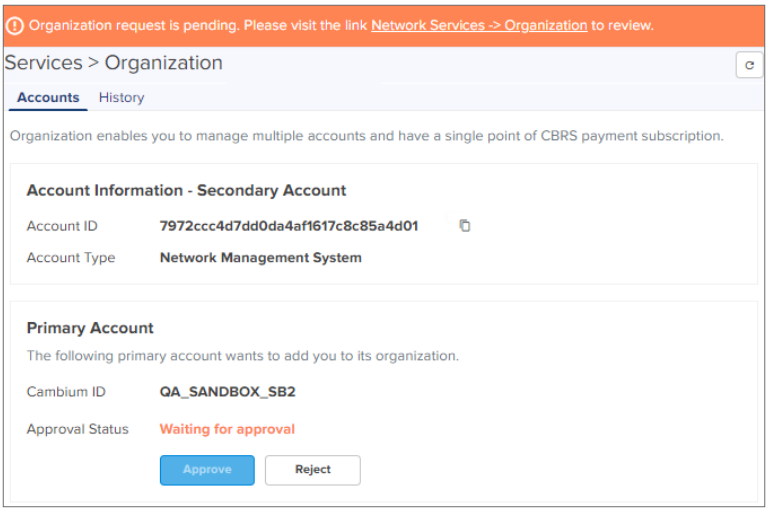


Secondary Account

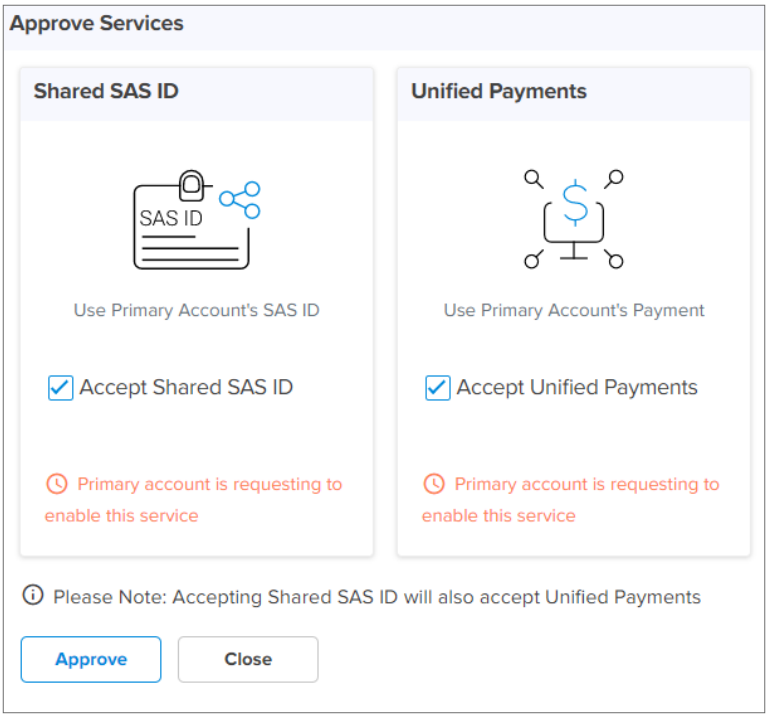
Login to the Secondary Account to complete Organization creation. The Secondary Account must approve the request and authorize the shared services. The Secondary Account can also request additional services (which must be approved by the Primary Account).

Perform the following steps in the Secondary Account:

1. Navigate to **Network Services** > **Organization** > **Accounts**.
2. Click **Approve**.



3. The **Approve Services** window pops up. Review the services requested and click **Approve**.



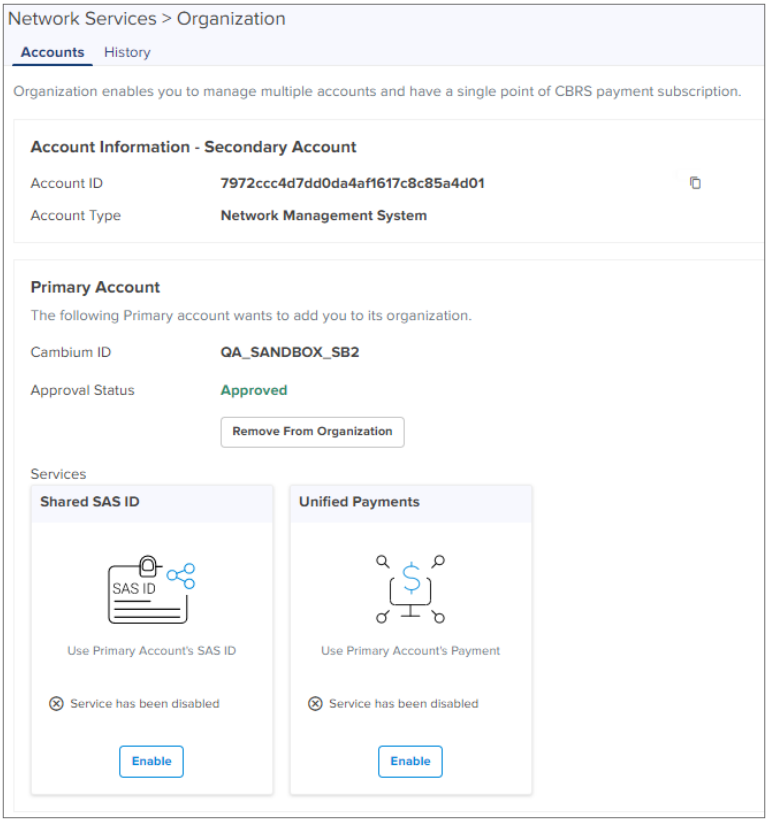
Additional service requests from the Secondary Account

Additional services can be added after the Secondary Account joins the Organization, such as including the Unified Payments Service.

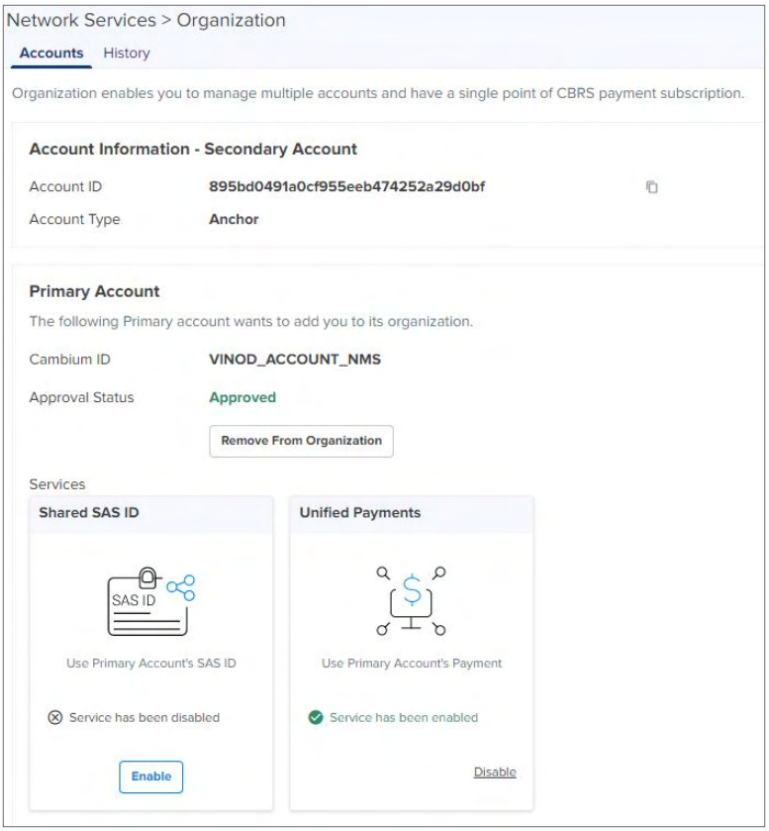
Perform the following steps on the Secondary Account:

1. Navigate to **Network Services** > **Unified Payments** and click **Enable.**

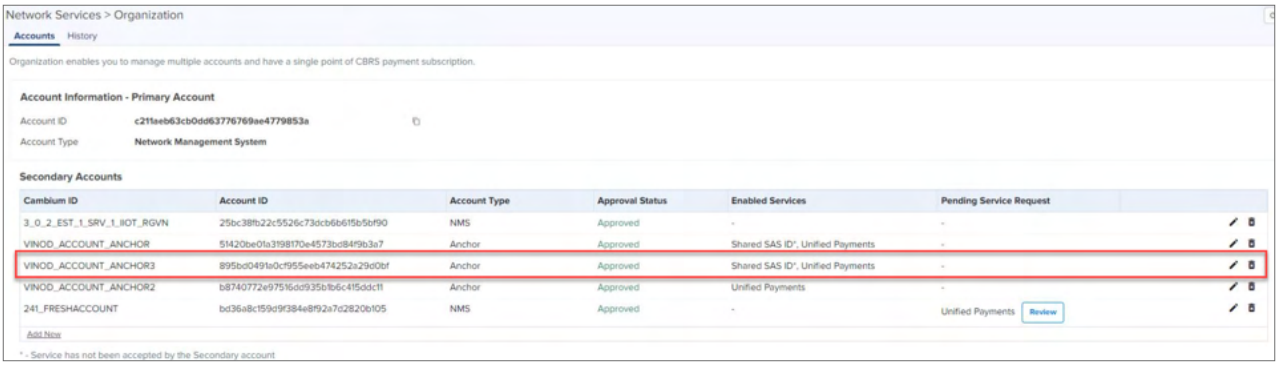
> **Note**
>
> This generates a request to the Primary Account to provide support for Unified Payments.



2. Once the services are enabled and approved in the Primary Account, the following displays in the Secondary Account.



3. The enabled services will be displayed in the Primary Account.

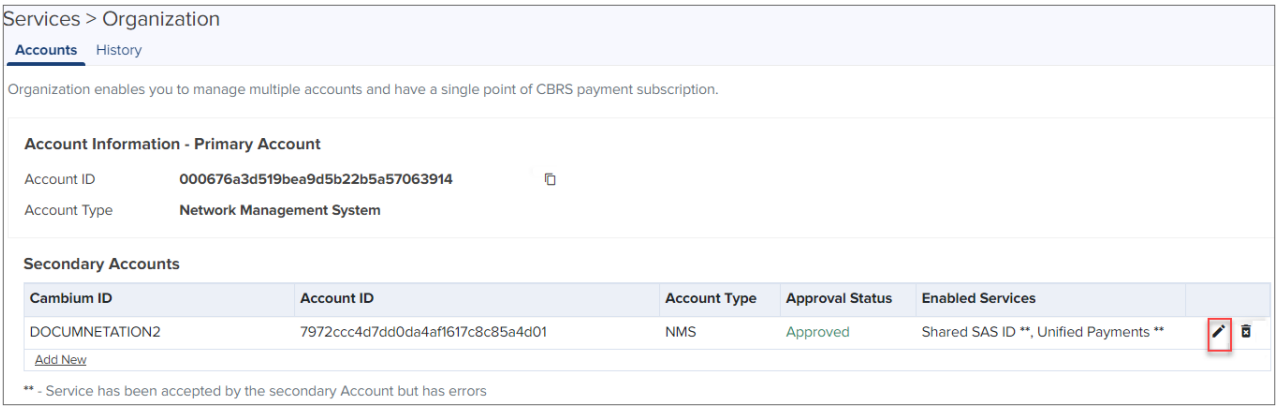


Removing Accounts

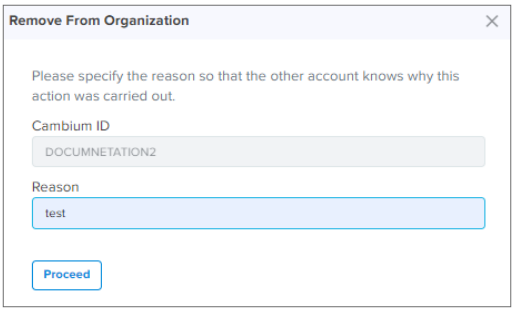
Remove through Primary Account

Perform the following steps on the Primary Account to remove the Secondary Account:

1. Navigate to **Network Services** > **Organization** > **Accounts**.
2. In the **Secondary Accounts**, click Delete ( ) icon.



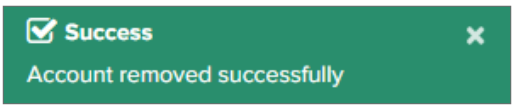
3. The **Remove From Organization** window pop up.



4. Enter the **Reason.**
5. Click **Proceed.**

Without Active Services

- If services such as **Shared SAS ID** or **Unified Payments** are inactive in the Secondary Account, it can be deleted without any approval.
- The following message displays if successful.



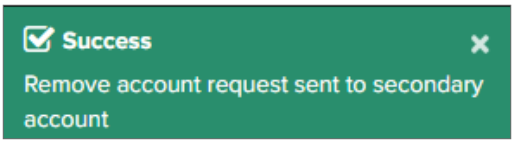
With Active Services

- If services such as **Shared SAS ID** or **Unified Payments** are active in the Secondary Account, the services need to be disabled from the Secondary Account, and the request must be approved by the Secondary Account administrator.

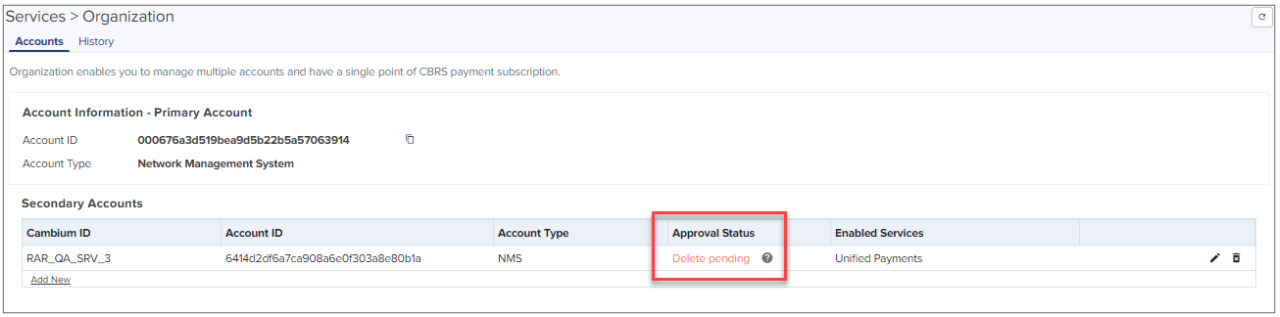
Note

- User needs to disable the active services such as Shared SAS ID and Unified Payments before removing the Secondary Account, or an Error message is shown.
- Shared SAS ID can be removed by contacting Cambium support to deactivate the current CBRS account to stop using Shared SAS ID.
- Active Services will be highlighted in **Green** color.

- The following message displays if successful.



- In the **Secondary Accounts** table, the UI displays the **Approval Status** as **Delete Pending**.

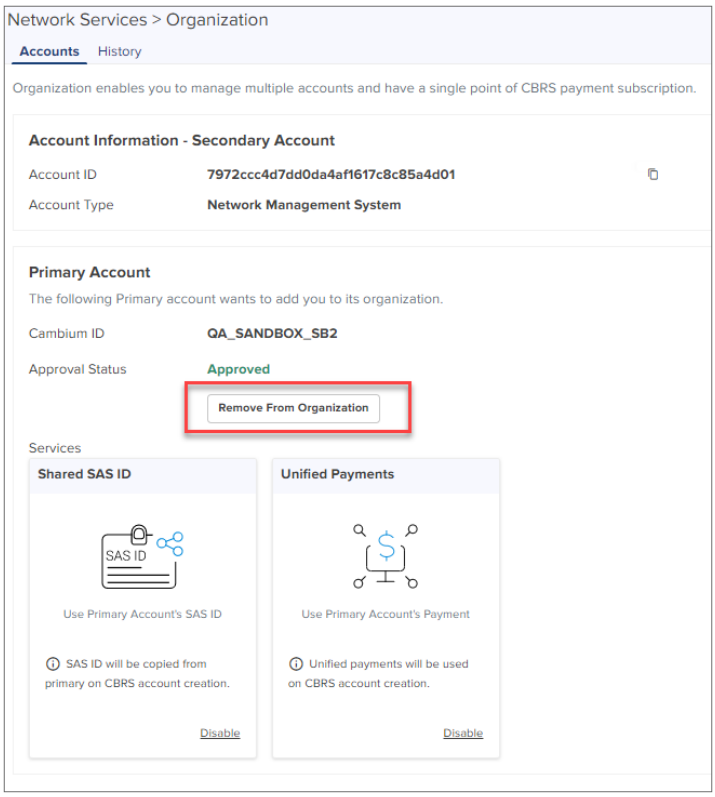


The Secondary Account administrator must approve the remove request from the Primary Account. For more details, refer to Approve Remove Request (with active services).

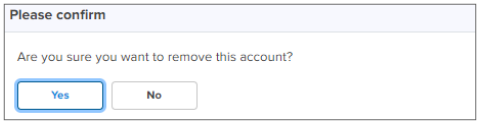
Remove Organization from Secondary Account

Perform the following steps on the Secondary Account to remove an Organization:

1. Navigate to **Network Services** > **Organization** > **Accounts**.
   a. Click **Remove From Organization** (without active services).
      - To remove the Secondary Account from an Organization with no active services.



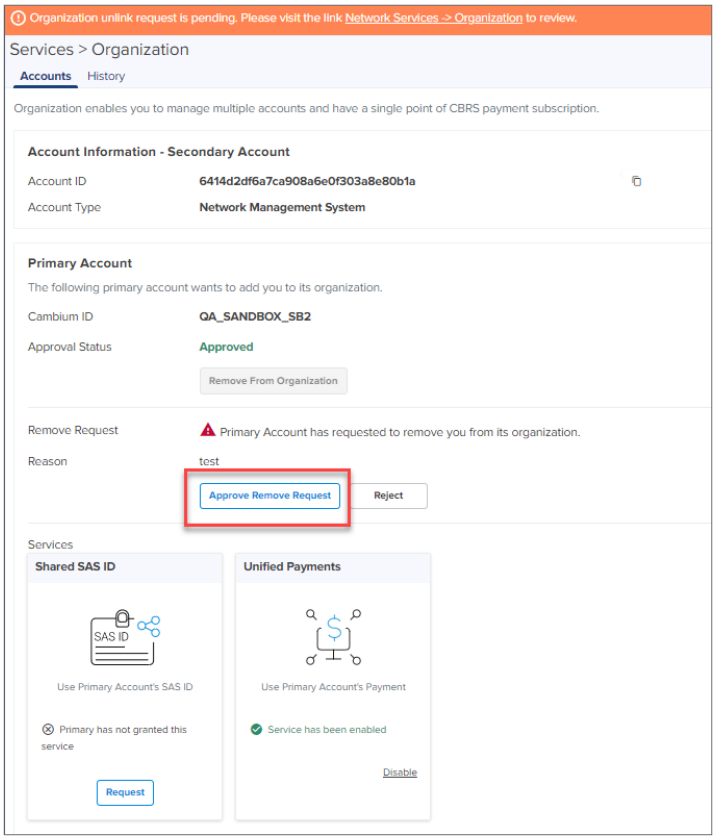
- Click **Yes** in **Please confirm** window to remove this account.



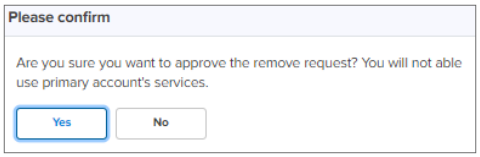
b. **Approve Remove Request** (with active services).

> **Note**
>
> Disable active services before **Approve Remove Request**.

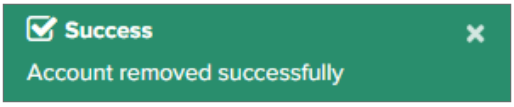
- If the Secondary Account is using services such as **Shared SAS ID** or **Unified Payments**, the following message displays.



- Click **Yes** in **Please confirm** window to approve the request.



2. The following message displays if successful.

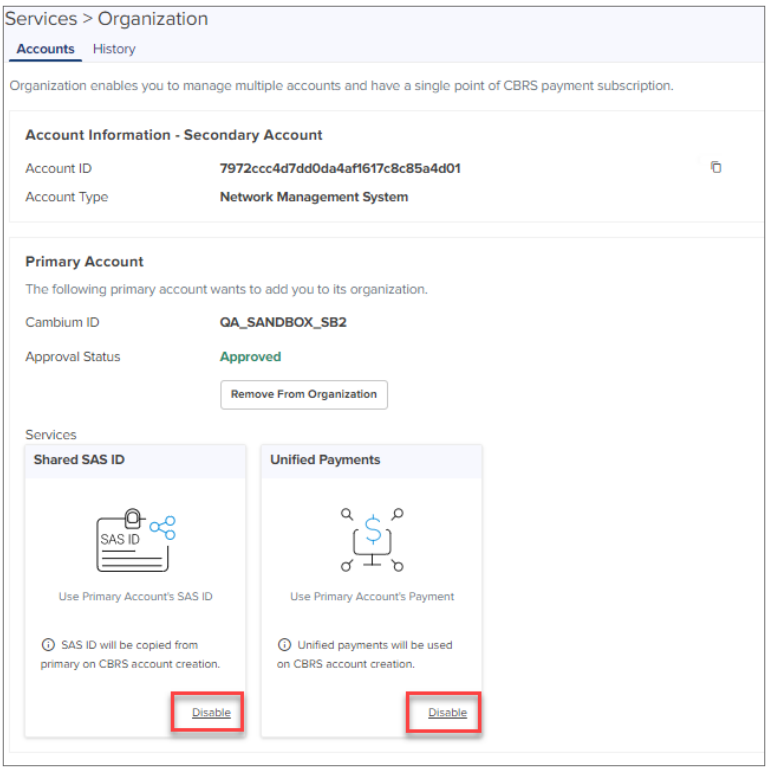


Disable Secondary Account services

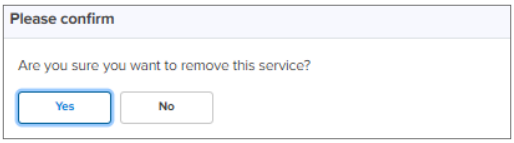
With no active services

The Secondary Account user can disable services without leaving the Organization.

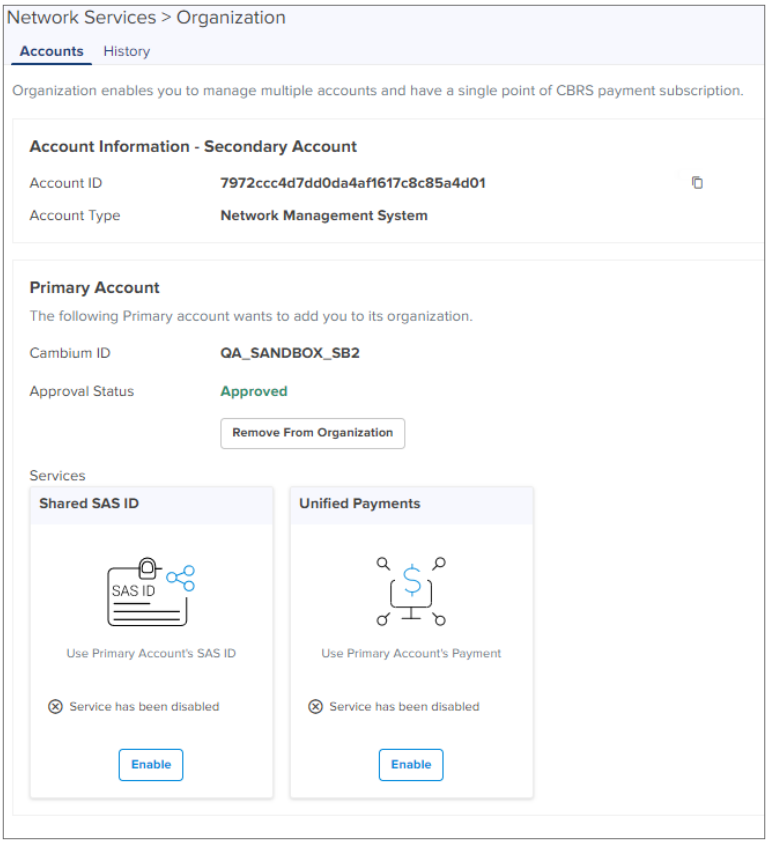
1. Navigate to **Services** > **Organization** > **Accounts** and select **Services.**
2. Click **Disable**.



3. Click **Yes** in the **Please confirm** window.



4. After disabling, the following displays.



5. Click **Enable** to reactivate the services.

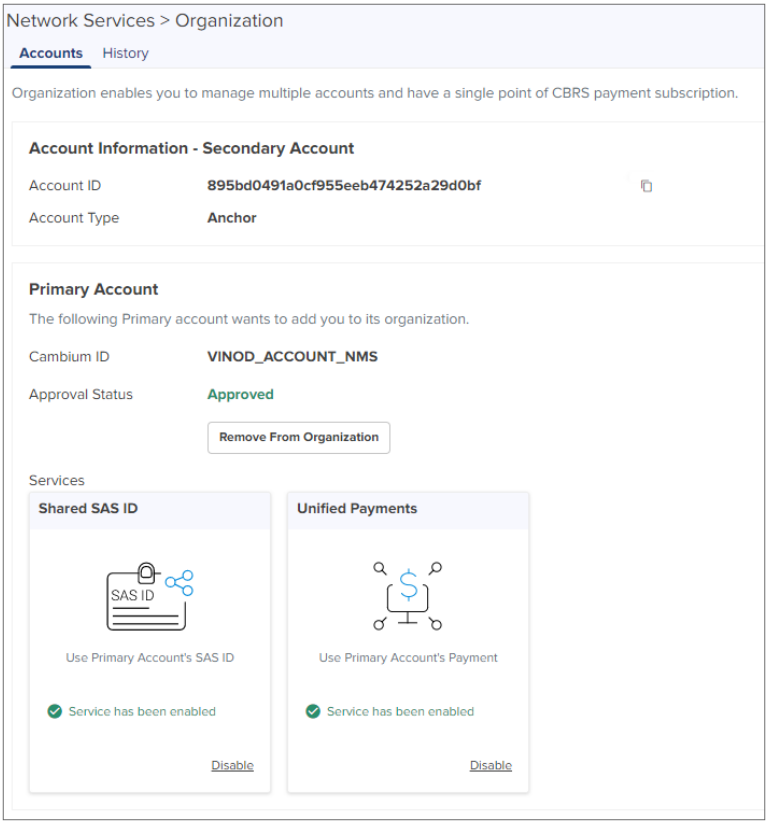
With active shared SAS ID services

Note

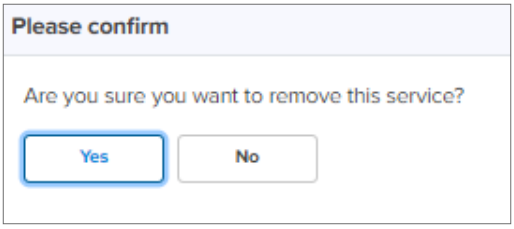
Active Services are highlighted in **Green** color.

The Secondary Account user can disable the **Shared SAS ID** services.

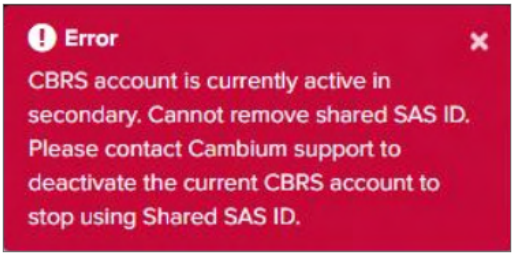
1. Navigate to **Services** > **Organization** > **Accounts** and select **Services.**



2. Click **Disable** in the **Shared SAS ID.**
3. Click **Yes** in the **Please confirm** window.



4. If CBRS account is active in Secondary Account, while disabling it displays the following error message.



If an **Error** message pops up, the user needs to raise a request to Cambium Support for the SAS vendor cancellation. Cambium Support will disable the CBRS services and deregister all devices associated to the Secondary Account.

Once disabled, the Secondary Account user can view the SAS vendor page and create a new CBRS account as shown below.



For further information on creating a new CBRS account, refer to CBRS.

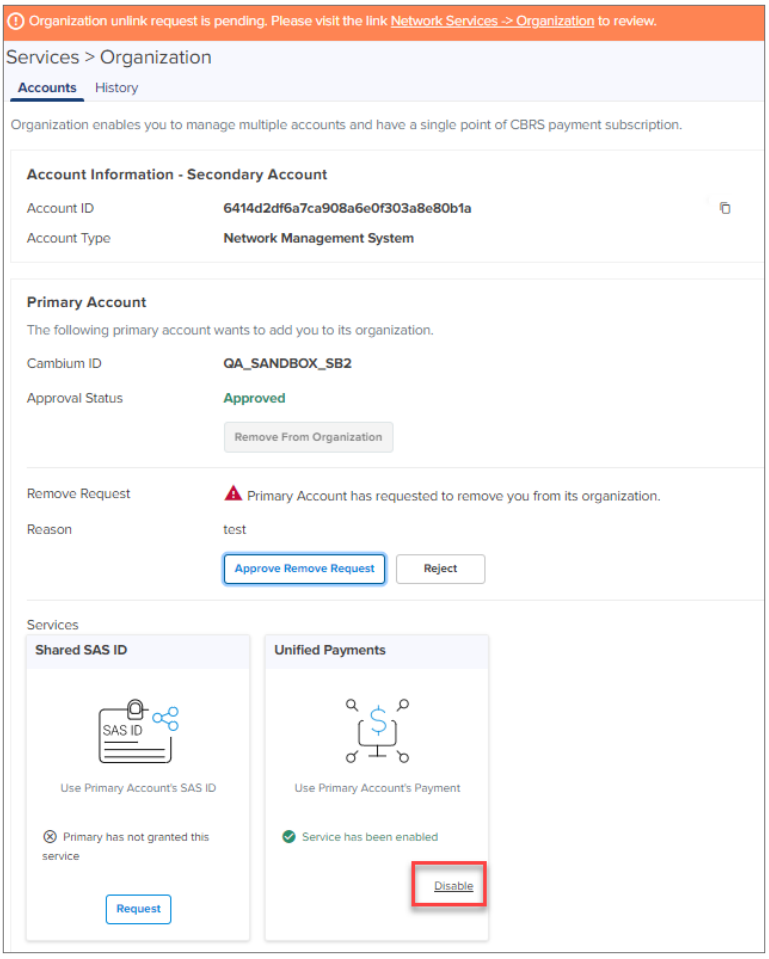
Note

Services in the Secondary Account cannot be disabled unless CBRS is inactive in Secondary Account. Contact Cambium Support to disable CBRS operation or change SAS Vendor.

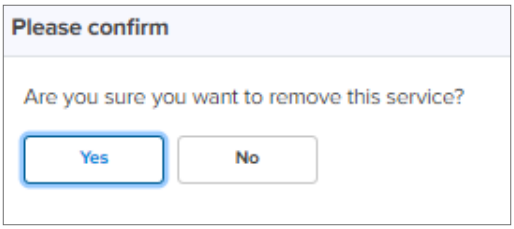
With active Unified Payments

The Secondary Account user can disable Unified Payments.

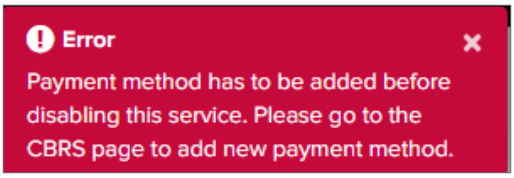
1. Navigate to **Services > Organization > Accounts** and select **Services.**



2. Click **Disable** within **Unified Payments**.
3. Click **Yes** in **Please confirm** window.



4. If **Unified Payments** is active in CBRS of the Secondary Account, it displays an **Error** message.



If this happens, the user needs to add new CBRS payment details into the Secondary Account.



For further information on Payment details, refer to CBRS.

The user can disable the **Unified Payments** once the new payment details are added successfully to the Secondary Account.

Edit Services

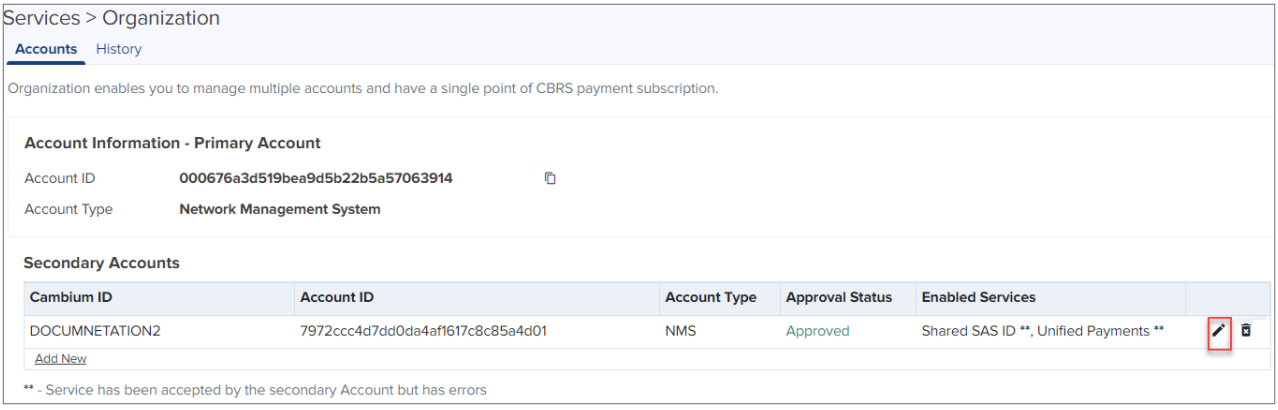
Enable services in the Primary Account

The Primary Account can edit or disable services shared with the Secondary Account as shown below:

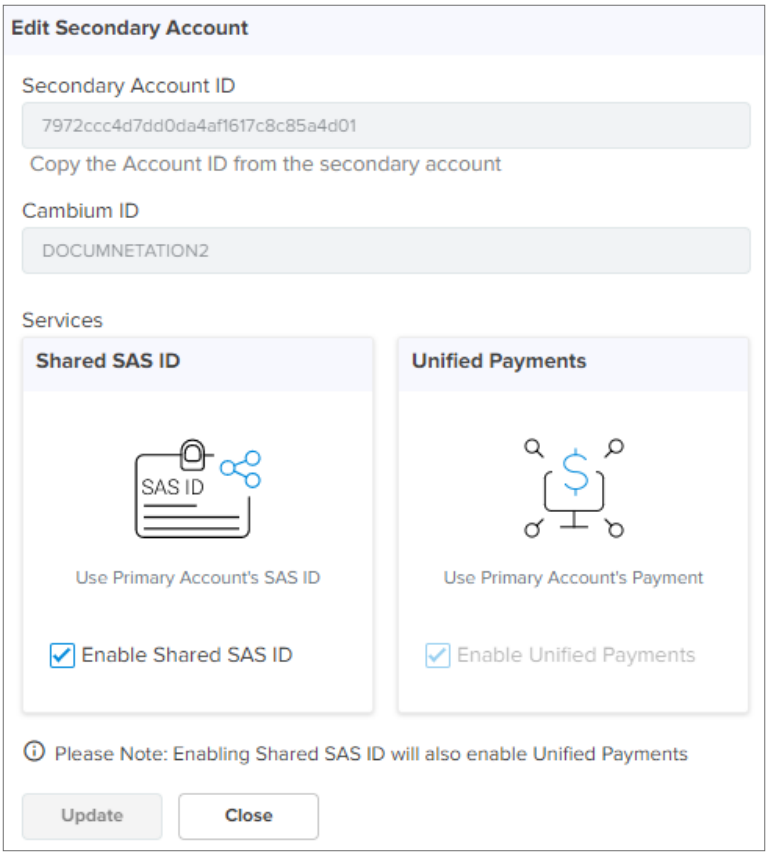
Note

When the services are active in CBRS of the Secondary Account, the Primary Account cannot disable those services.

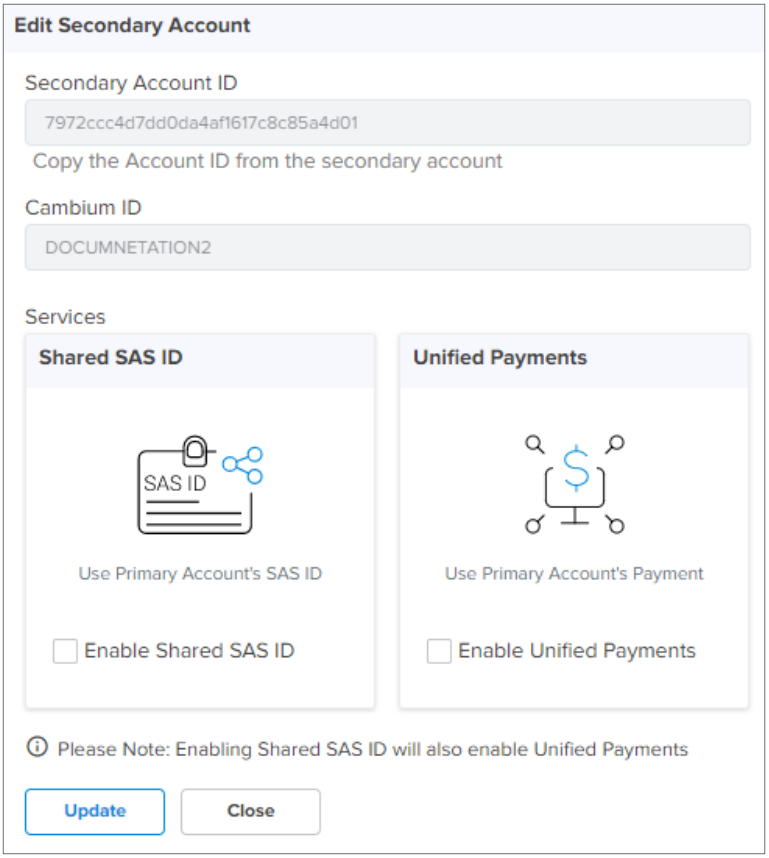
1. Navigate to **Accounts** > **Secondary Accounts** tab.
2. Click Edit (✎) icon.



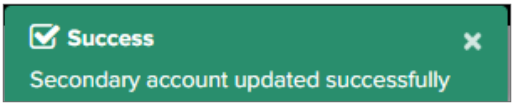
3. **Edit Secondary Account** window pops up.



4. Disable the **Services** and click **Update**.



5. The following message displays if successful.

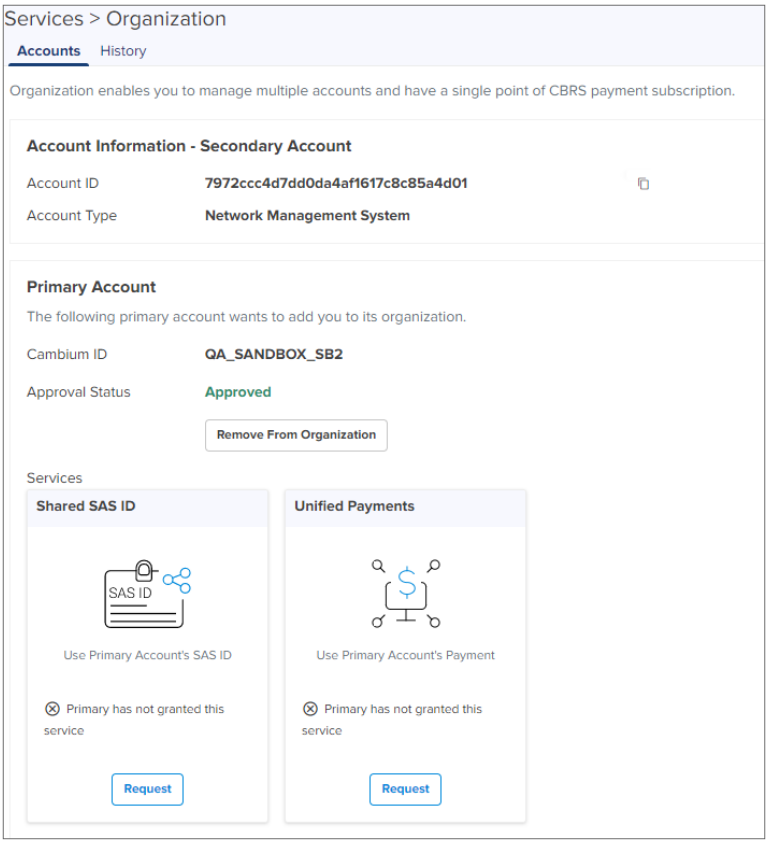


Request services from Secondary Account

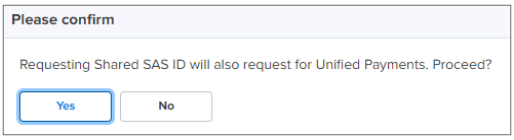
If the services are disabled, the Secondary Account needs to make a request to the Primary Account to activate them.

To request activation, perform the following on the Secondary Account:

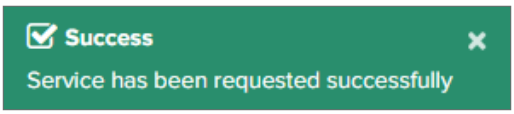
1. Navigate to **Network Services** > **Organization** > **Accounts**.
2. Click **Request**.



3. Click **Yes** in **Please confirm** window.



4. It displays the **Success** message as shown below:



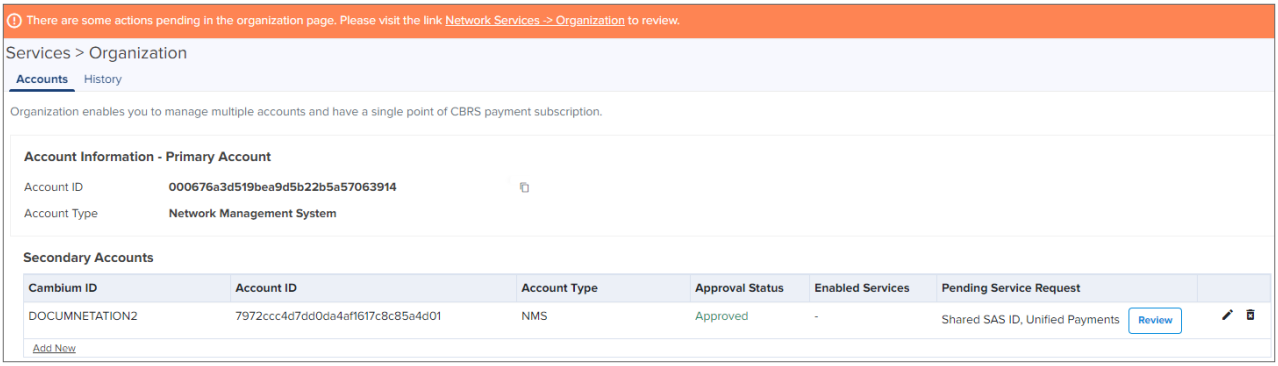
5. Once requested, login to the **Primary Account** page and **Approve** the request.

The Primary Account administrator must approve this request from the Secondary Account in order to enable the services.

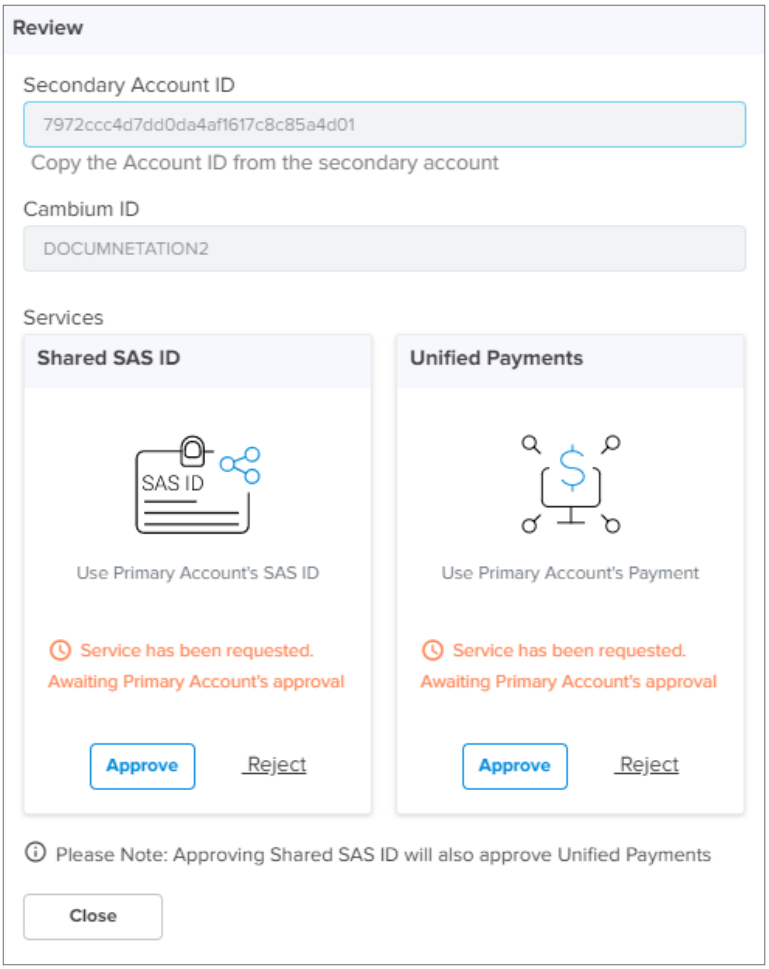
Review service request in Primary Account

Perform the following steps on the Primary Account.

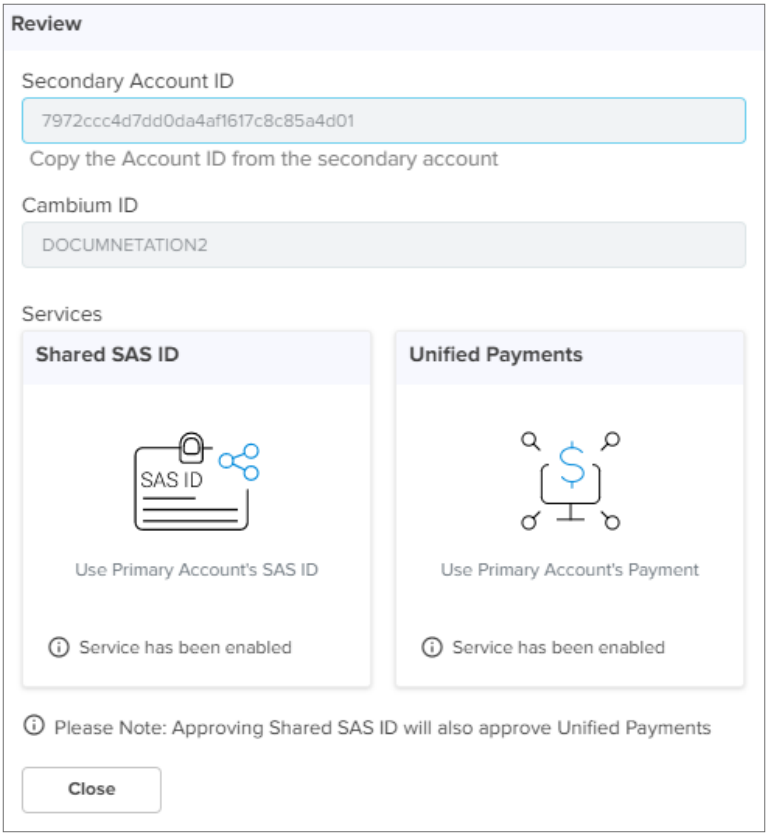
1. Navigate to **Services** > **Secondary Accounts** tab.
2. Click **Review** in **Pending Service Request**.



3. The **Review** window pops up. Click **Approve**.



4. Once approved, the requested services are enabled in the **Secondary Account.**

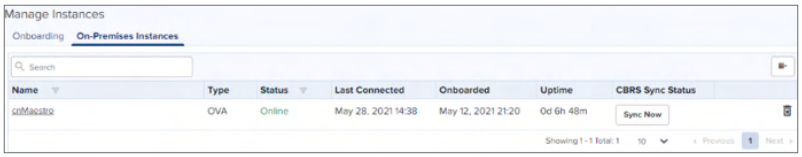


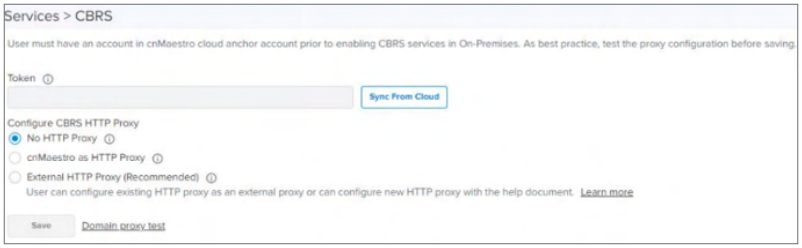
Share CBRS Configuration with the On-Premises Instance

Note

Starting with version 3.0.3, cnMaestro supports synchronizing CBRS Configuration to On-Premises instance.

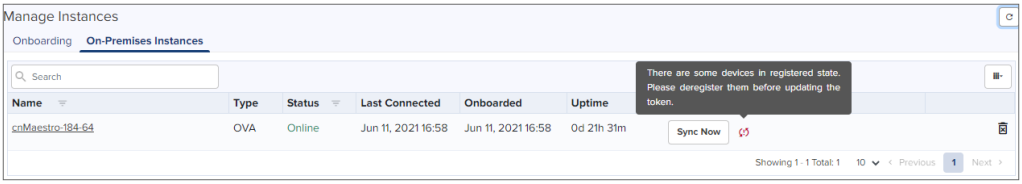
Once On-Premises is connected to the Anchor Account, the user can synchronize CBRS details (SAS ID, Token) to the cnMaestro On-Premises instance to register CBRS devices.





- If the user shares (sync) CBRS details configured on Anchor account to connected On-Premises and if any devices are registered in On-Premises with different CBRS token or SAS ID it displays the deregister error as

shown below.

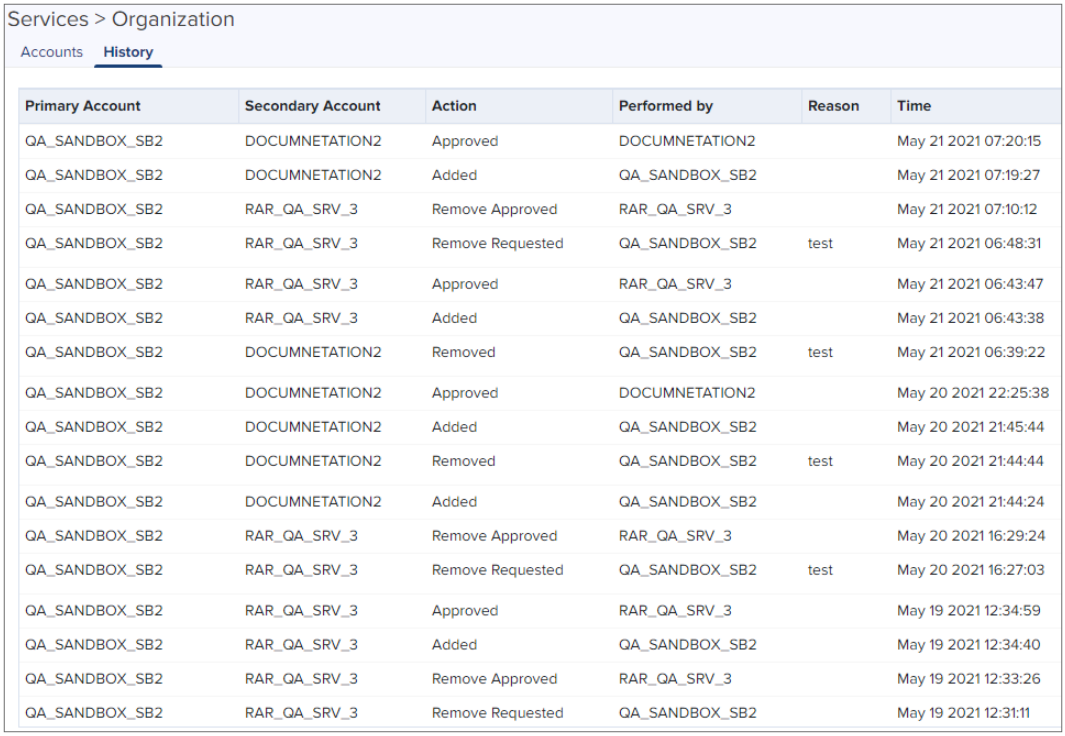


Organization History

In Organization History user can view changes to the Organization status over time. This includes details of Primary Account, Secondary Account, Action, Performed by, and Reason.

To view Organization History:

Navigate to **Network Services** > **Organization** > **History** tab.



Primary Account	Secondary Account	Action	Performed by	Reason	Time
QA_SANDBOX_SB2	DOCUMNETATION2	Approved	DOCUMNETATION2		May 21 2021 07:20:15
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 21 2021 07:19:27
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 21 2021 07:10:12
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2	test	May 21 2021 06:48:31
QA_SANDBOX_SB2	RAR_QA_SRV_3	Approved	RAR_QA_SRV_3		May 21 2021 06:43:47
QA_SANDBOX_SB2	RAR_QA_SRV_3	Added	QA_SANDBOX_SB2		May 21 2021 06:43:38
QA_SANDBOX_SB2	DOCUMNETATION2	Removed	QA_SANDBOX_SB2	test	May 21 2021 06:39:22
QA_SANDBOX_SB2	DOCUMNETATION2	Approved	DOCUMNETATION2		May 20 2021 22:25:38
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 20 2021 21:45:44
QA_SANDBOX_SB2	DOCUMNETATION2	Removed	QA_SANDBOX_SB2	test	May 20 2021 21:44:44
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 20 2021 21:44:24
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 20 2021 16:29:24
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2	test	May 20 2021 16:27:03
QA_SANDBOX_SB2	RAR_QA_SRV_3	Approved	RAR_QA_SRV_3		May 19 2021 12:34:59
QA_SANDBOX_SB2	RAR_QA_SRV_3	Added	QA_SANDBOX_SB2		May 19 2021 12:34:40
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 19 2021 12:33:26
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2		May 19 2021 12:31:11

LTE

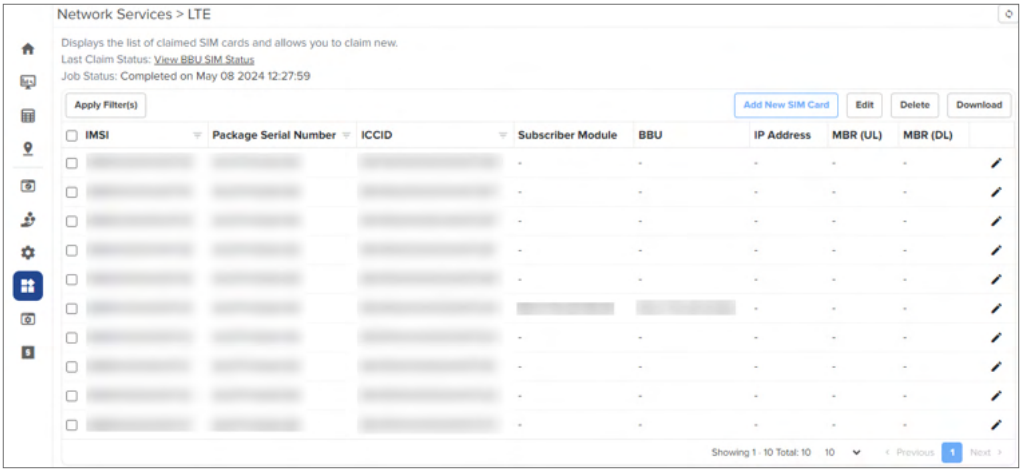
cnMaestro supports LTE as part of its cnMaestro deployment. LTE allows customers to onboard the SM with IMSI into cnMaestro.

System access in cnRanger is dependent on installation of SIM credentials on every BBU in the operator network. To ease the operations aspects of SIM card management, cnMaestro provides utilities for claiming, managing, and distributing Cambium Networks cnRanger SIM card credentials (3rd party SIM cards are not currently supported on cnRanger).

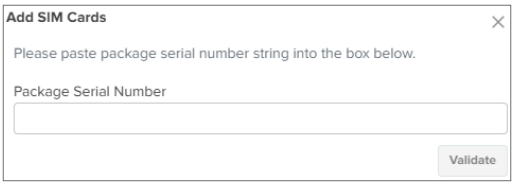
Adding SIM Cards

To add a SIM card, complete the following steps:

1. Navigate to **Network Services > LTE**.



2. Click **Add New SIM Card**. The following window appears.



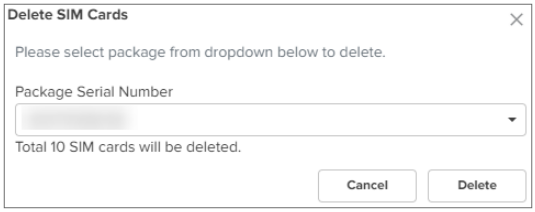
3. Enter appropriate **Serial Number** of SIM package and click **Validate**.
4. After successful validation of the serial number, click **Add**.

Note

User can download the .CSV file from the Cloud account once the Serial Number is validated from the cnMaestro Cloud database.

Delete SIM Cards

To delete a SIM card from the list, click **Delete**. The following window appears.



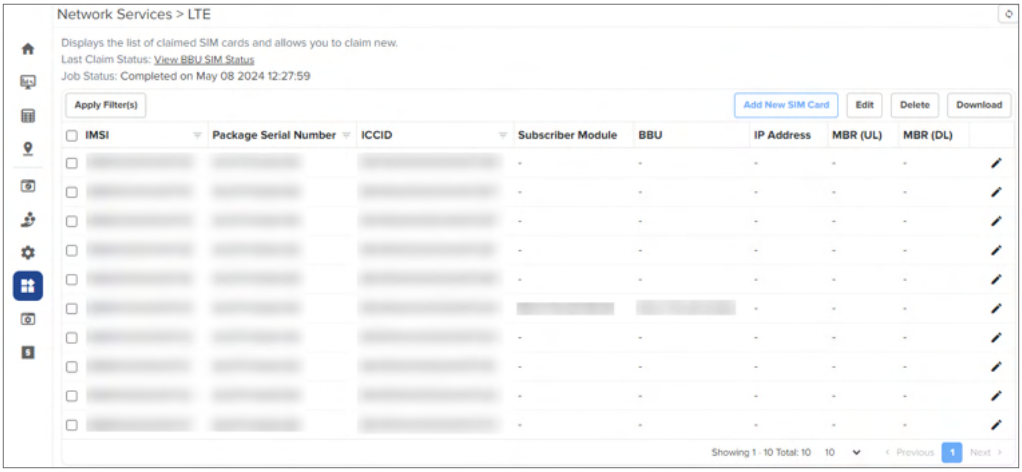
Note

IMSI numbers get deleted with the mapped Serial Number.

Update SIM Details

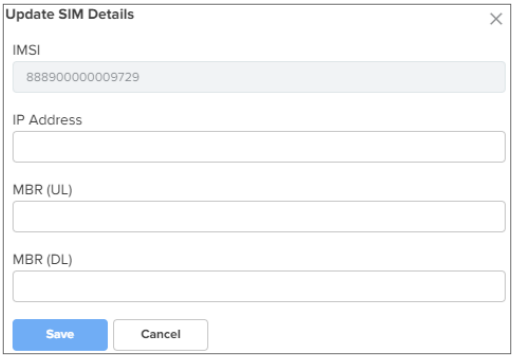
User can edit the SIM details as follows.

1. Navigate to **Network Services > LTE**.



2. Click the edit ( ) icon for the IMSI that you want to edit.

   The **Update SIM Details** window pops-up.

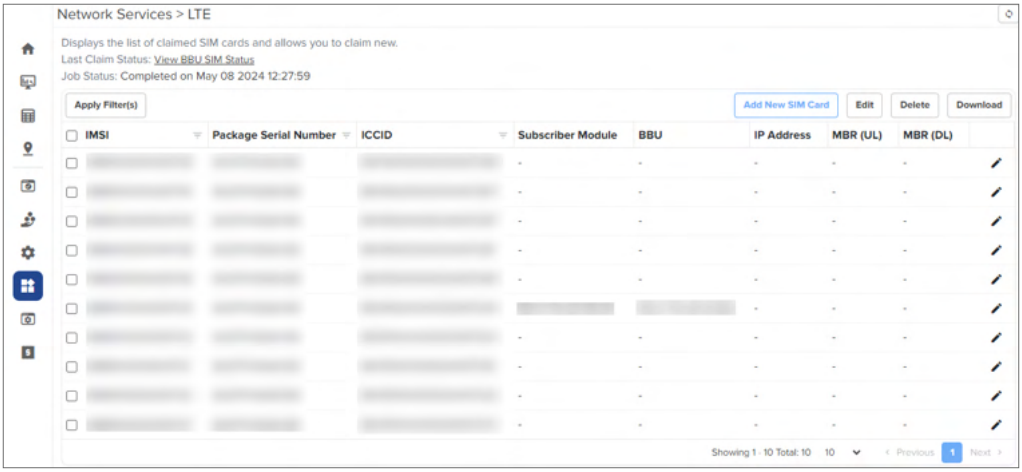


3. Enter a valid **IP Address**.
4. Enter the **MBR (UL)** and **MBR (DL)**.
5. Click **Save**.

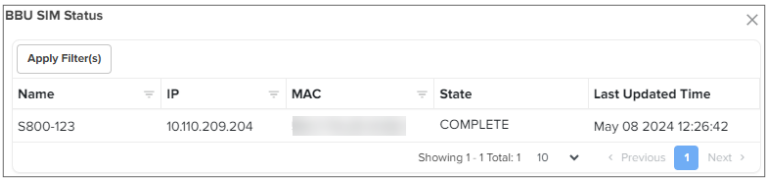
Viewing BBU SIM Status

Allows the users to view the status of the SIM connected to the BBU.

1. Navigate to **Network Services > LTE.**



2. Click **View BBU SIM Status.**



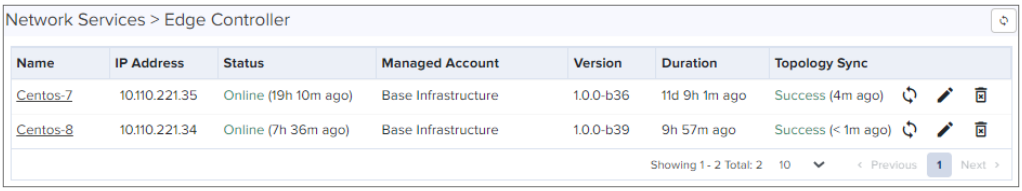
Managing Edge Controller

This chapter provides the details about how Edge Controllers are configured to discover PTP 820/850 devices in a network using SNMP protocol. To view the onboarded Edge Controllers in cnMaestro, perform the following steps:

1. Navigate to **Network Services** > **Edge Controller**.

   A list of onboarded Edge Controllers in a table format is displayed, as shown in Figure 555.

   Figure 555 *Edge Controllers*



   The following parameters are available to view in a table format: Name, IP Address, Status, Managed Account, Version, Duration, and Topology Sync Status. You can perform the following actions in the Edge Controller page.

   - Topology Sync
   - Edit
   - Delete

   Select the required Edge Controller name in the page, to perform the following actions:

   - Topology Sync

- Edit
- Delete

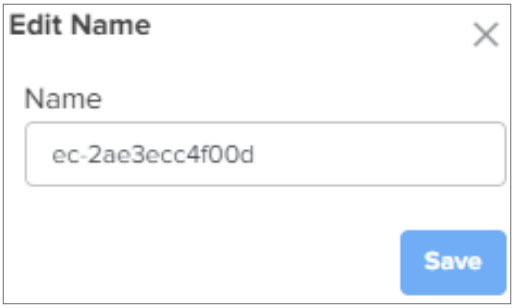
Topology Sync

Click on the **Topology Sync** ( ) icon to run topology synchronization for the required Edge Controller.

Edit

1. Click the edit ( ) icon in the Edge Controller page.

   The **Edit name** window appears, edit the name of the Edge Controller.

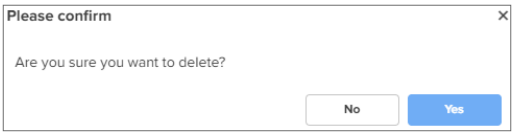


2. Click **Save**.

Delete

1. Click the delete ( ) icon in the Edge Controller page.

   The delete confirmation window appears.



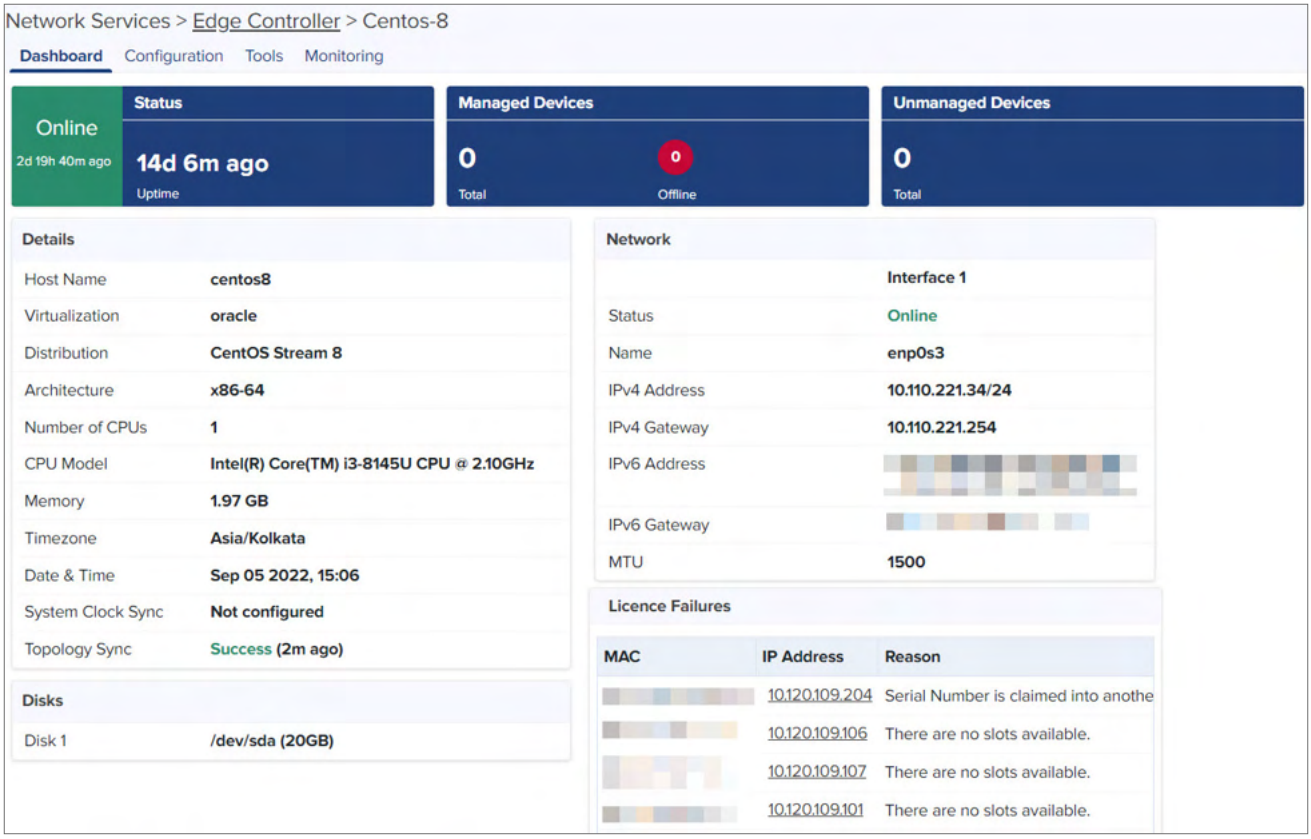
2. Click **Yes**.

In the Edge Controller page, you can navigate to the following tabs:

- Dashboard
- Configuration
- Tools
- Monitoring

To view the Edge Controller dashboard, click on the name of the Edge Controller. The Edge Controller dashboard page appears as shown in Figure 556.

Figure 556 *The Edge Controller dashboard*



Dashboard

The dashboard page displays status of managed and unmanaged PTP 820/850 devices, details of Edge Controller, disk space availability, and network details of Edge Controller as shown in Table 154.

Figure 557 *Edge Controller and PTP 820/850 devices status*

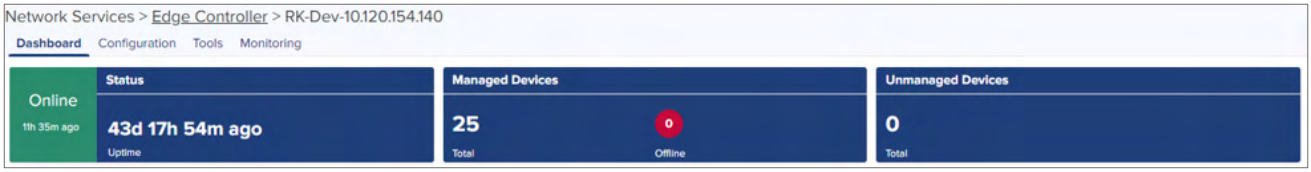


Table 154 *Fields in the Edge Controller dashboard*

Field	Description
Host name	Name of the host.
Virtualization	Type of virtualization such as VMware or Oracle.
Distribution	Type of distribution such as Ubuntu and CentOS versions.
Architecture	CPU and Operating System installed.
Number of CPUs	Total number of CPUs utilized.
CPU Model	Type of CPU model.
Memory	Available memory.
Timezone	Current timezone.

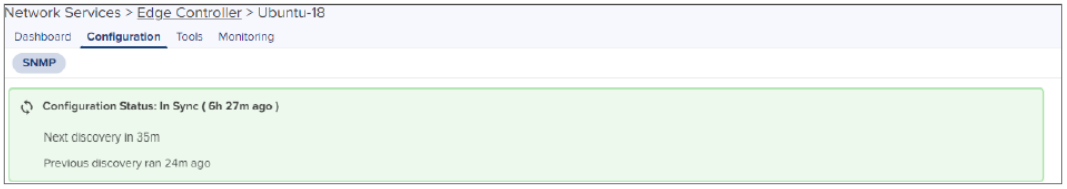
Table 154 *Fields in the Edge Controller dashboard*

Field	Description
Date & Time	Current date and time.
System Clock Sync	Configuration of System Clock Synchronization.
Disk	Current Disk space usage.
Status	Status of Network Interface Online or Offline.
Name	Name of the Network Interface.
IPv4 Address	Configured IPv4 Address.
IPv4 Gateway	Configured IPv4 Gateway.
IPv6 Address	Configured IPv6 Address.
IPv6 Gateway	Configured IPv6 Gateway.
MTU	Maximum Transmission Unit of network interface of Edge Controller.
License Failures	Displays MAC, IP Address, and Reason. The reasons for license failure are as follows: When the discovery exceeds the slot availability. When the individual devices are already onboarded in other Cloud account.
Topology Sync	Status of Topology Sync.
Version	Software version of the device.

Configuration

In the **Configuration** page, you need to configure SNMP rules to discover and onboard PTP 820/850 devices. The **SNMP** tab in the **Configuration** page displays **Configuration Status.** The**Configuration Status** displays when the Edge Controller is **In Sync** or **Not Sync** with cnMaestro. The synchronization status is shown in days, hours and minutes. **Next discovery** and **Previous discovery** ran is displayed in minutes as shown in Figure 558.

Figure 558 *Configuration Status*



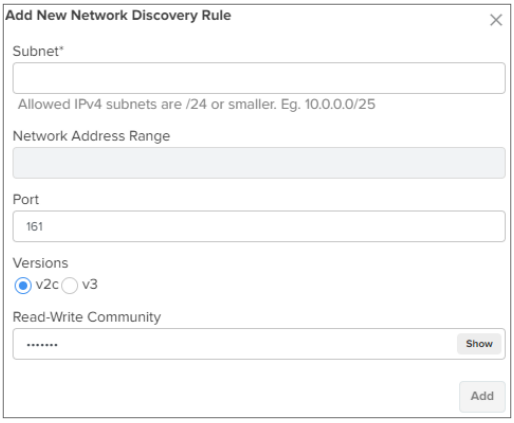
Rules

To add a new rule, perform the following steps:

1. Click **Add New**.



The **Add New Network Discovery Rule** window appears.



2. Type **Subnet** range in CIDR format (for example, 10.204.88.0/28) to discover PTP 820/850 devices.

   The range of IP addresses in the **Network Address Range** field is displayed.

3. Type **Port** number.

4. Choose SNMP **Version**:

   For SNMP version **v2c**, perform the following:

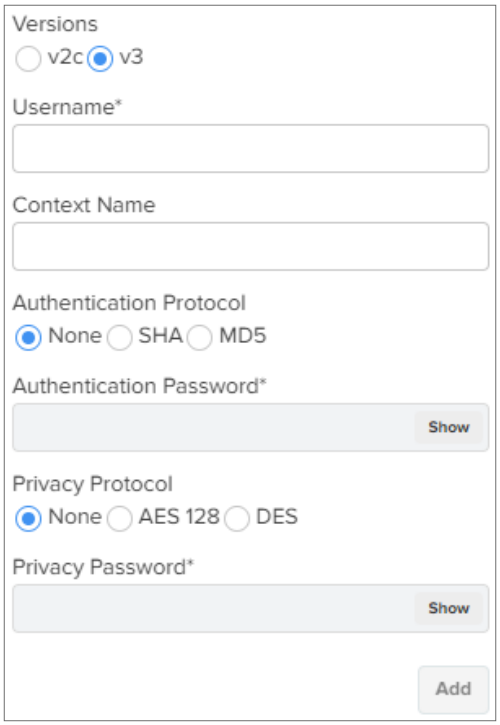
   a. Enter preferred community string when you create a SNMP discovery rule.

   b. Click **Add.**

> **Note**
>
> Default community string is private.

   For SNMP Version **v3,** perform the following:

   a. Choosing SNMP v3 version allows you to enter the parameters as shown in the following figure.



b. Enter the following fields:

- **Username**.
- **Context Name** field is optional.

c. Choose any one of the **Authentication Protocol.**

- None
- SHA
- MD5

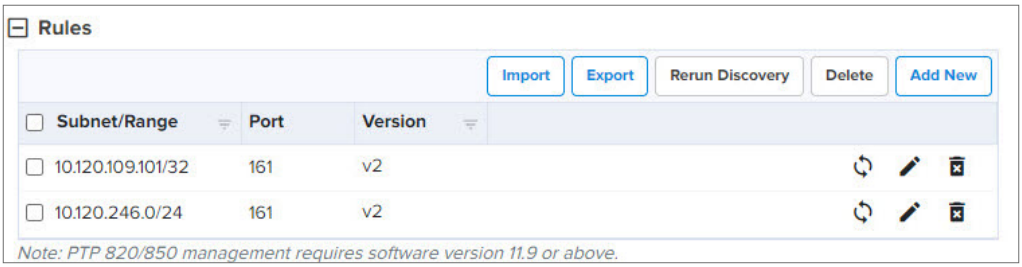
d. Choose any one of the **Privacy Protocol**.

- None
- AES128
- DES

e. Type **Privacy Password**.

f. Click **Add**.

SNMP Rules added are listed in the Rules table as shown in the following figure.



5. Click **Rerun Discovery** to start SNMP discovery for the rules added in the table or select specific **Subnet/Range** in the table and manually run **Rerun Discovery** (↻) icon.

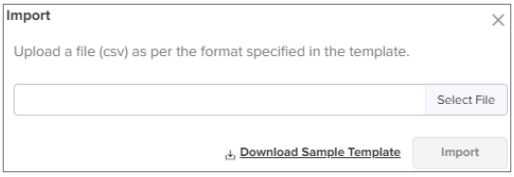
Import

To import SNMP rules, perform the following steps:

1. Click **Import.**

   Import window appears.

2. Browse to **Select File** or **Download Sample Template** to change or configure the SNMP as per the requirements in **Downloaded Sample Template.**

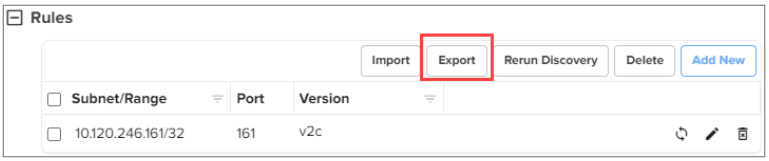


3. Click **Import**.

Export

To export SNMP rules, perform the following steps:

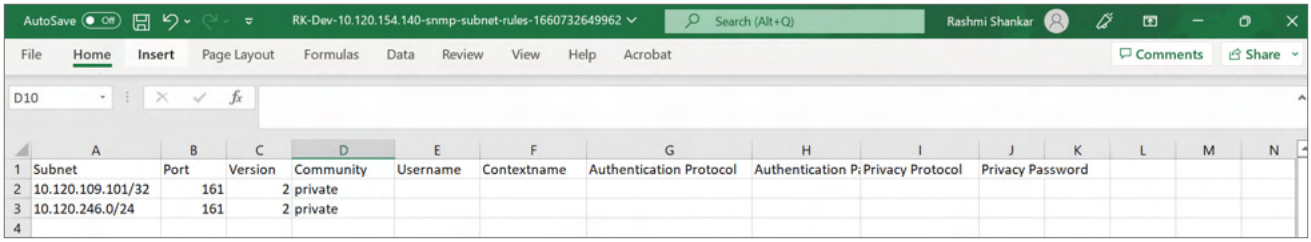
1. Select one or more SNMP rules required to export.
2. Click **Export**.



3. It exports the rules in the CSV file format as shown in the following figure.

Note

By default all SNMP rules are exported, if none of the rules are selected from the table.



Delete

To delete SNMP rules in the table, perform the following steps:

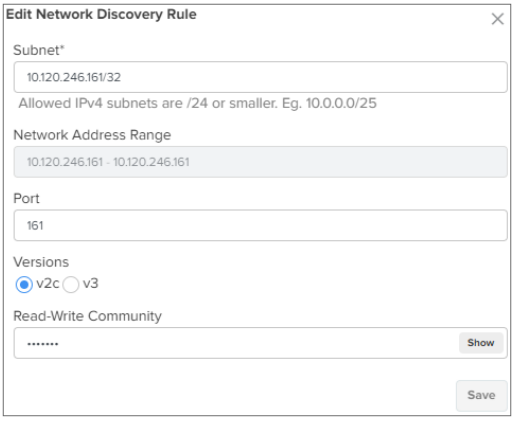
1. Select one or more SNMP rules in the table.
2. Click **Delete**, to delete one or more entries in the table or click **Delete** (🗑) icon to delete specific rule in the table.

Edit

To edit SNMP rule in the table, perform the following steps:

1. Click Edit (✎) icon to edit SNMP rule.

   Edit Network Discovery Rule window appears. Edit the required field values.

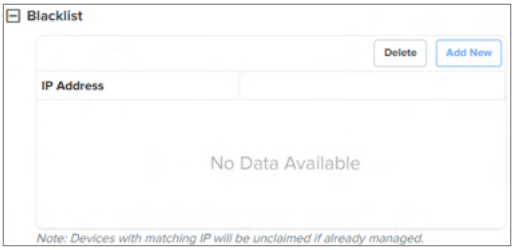


2. Click **Save**.

Blacklist

To blacklist PTP 820/850 devices, perform the following steps:

1. Click **Add New.**



Add Blacklist IP Address window appears.



2. Type **IP Address.**
3. Click **Save.**

Blacklisted IP Addresses are displayed in the table.



4. Select one or more blacklisted IP addresses in the table.
5. Click **Delete**, to delete one or more entries in the table or click **Delete** (🗑) icon to delete specific blacklist entry in the table.

Advanced Settings

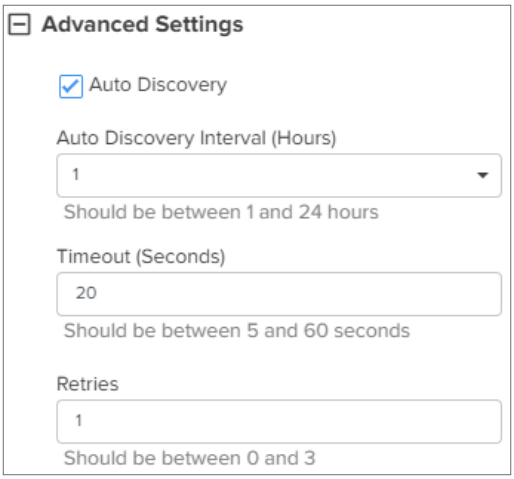
In **Advanced Settings** section, configure the following parameters:

Note

- By default, **Auto Discovery** option is disabled.
- By default, **Auto Discovery Interval** option is 24 hours, when enabled and fields are auto-filled.

Enable **Auto Discovery** if you want to run SNMP discovery rules manually and perform the following steps:

1. Select **Auto Discovery Interval** option from the drop-down.
2. Enter **Timeout** in seconds between 5 to 60 seconds.
3. Enter **Retries** values between 0 and 3.



4. Click **Save**.

Tools

The Tools page allows you to perform the following actions:

- Diagnostics
- Operations
- Services

Diagnostics

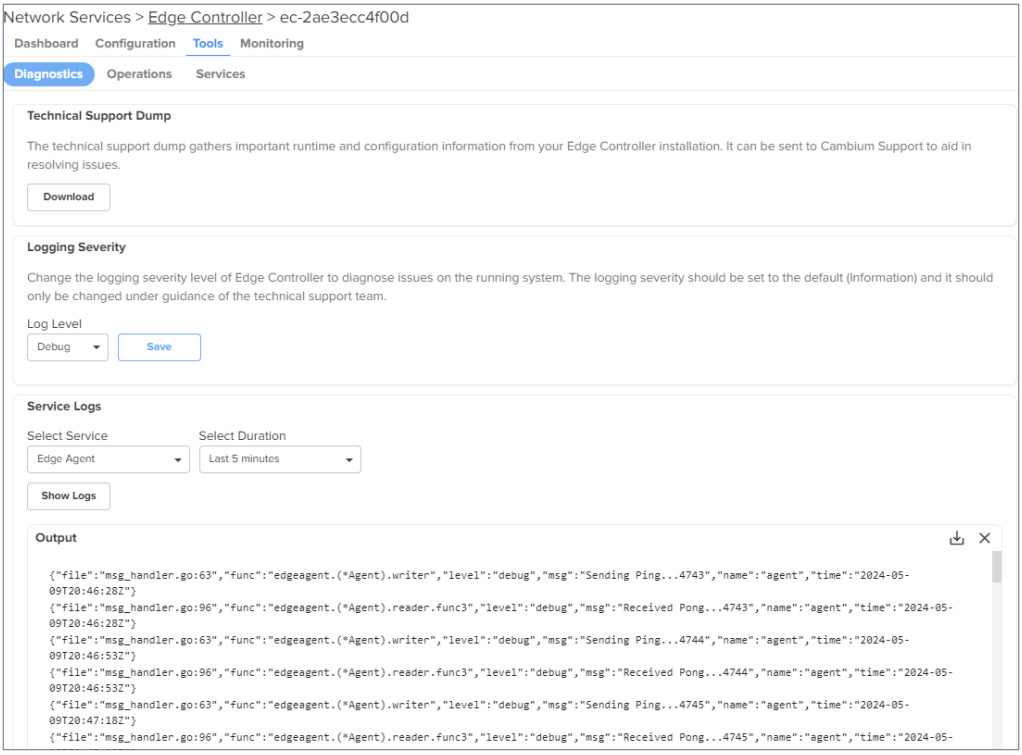
Diagnostics page allows you to gather technical support dump which can be downloaded and sent to Cambium Networks support team.

Technical Support Dump

The Technical Support Dump gathers important runtime and configuration information from the Edge Controller. It can be sent to Cambium Support to aid in resolving issues.

1. Navigate to **Edge Controller** > **Tools** > **Diagnostics**.
2. Click **Download** under Technical Support Dump**.**

Diagnostics

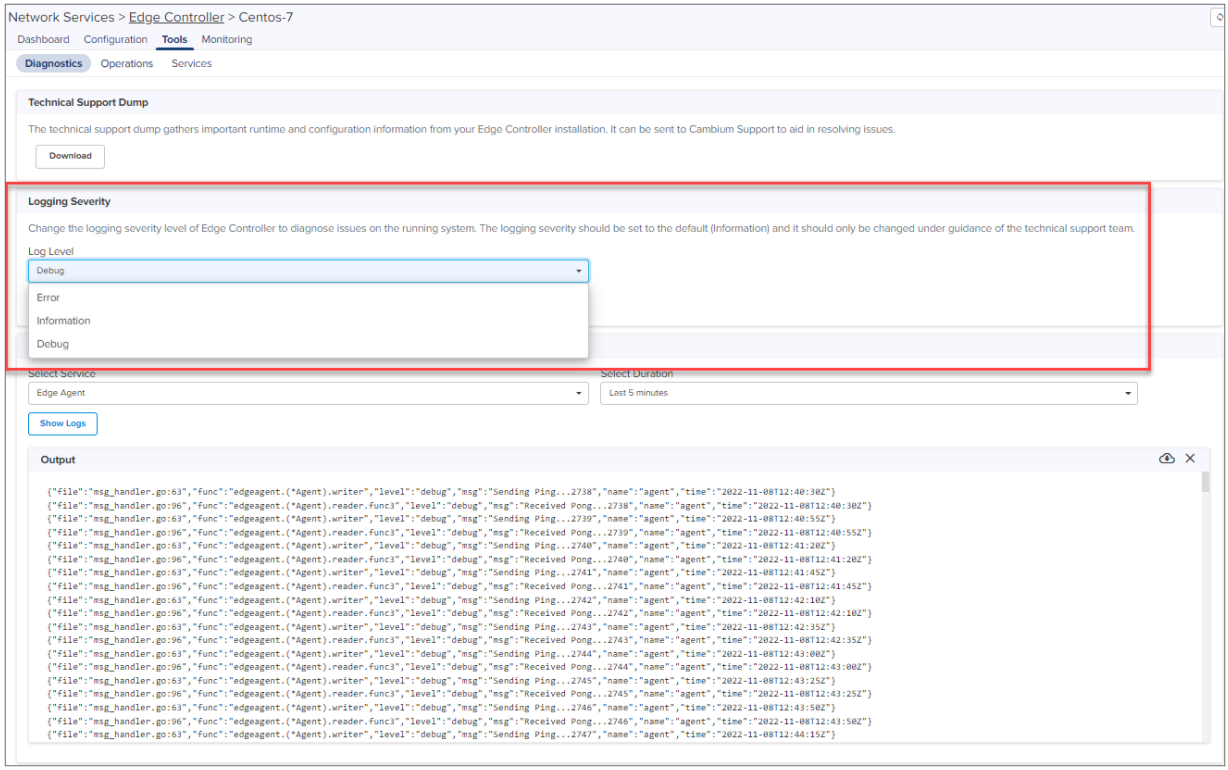


Logging Severity

The Logging Severity level of Edge Controller diagnose issues on the running system. The logging severity should be set to the default (Information) and it should only be changed under guidance of the technical support team.

1. Navigate to **Edge Controller** > **Tools** > **Diagnostics.**
2. In **Logging Severity** section, select one of the log level from **Log level** drop-down.
    - Error
    - Information

- Debug



3. Click **Save.**
4. Click **Reset** to revert to the previous **Log level** option.

Service Logs

The Service Logs allows you to diagnose any issues in the services running in the Edge Controller.

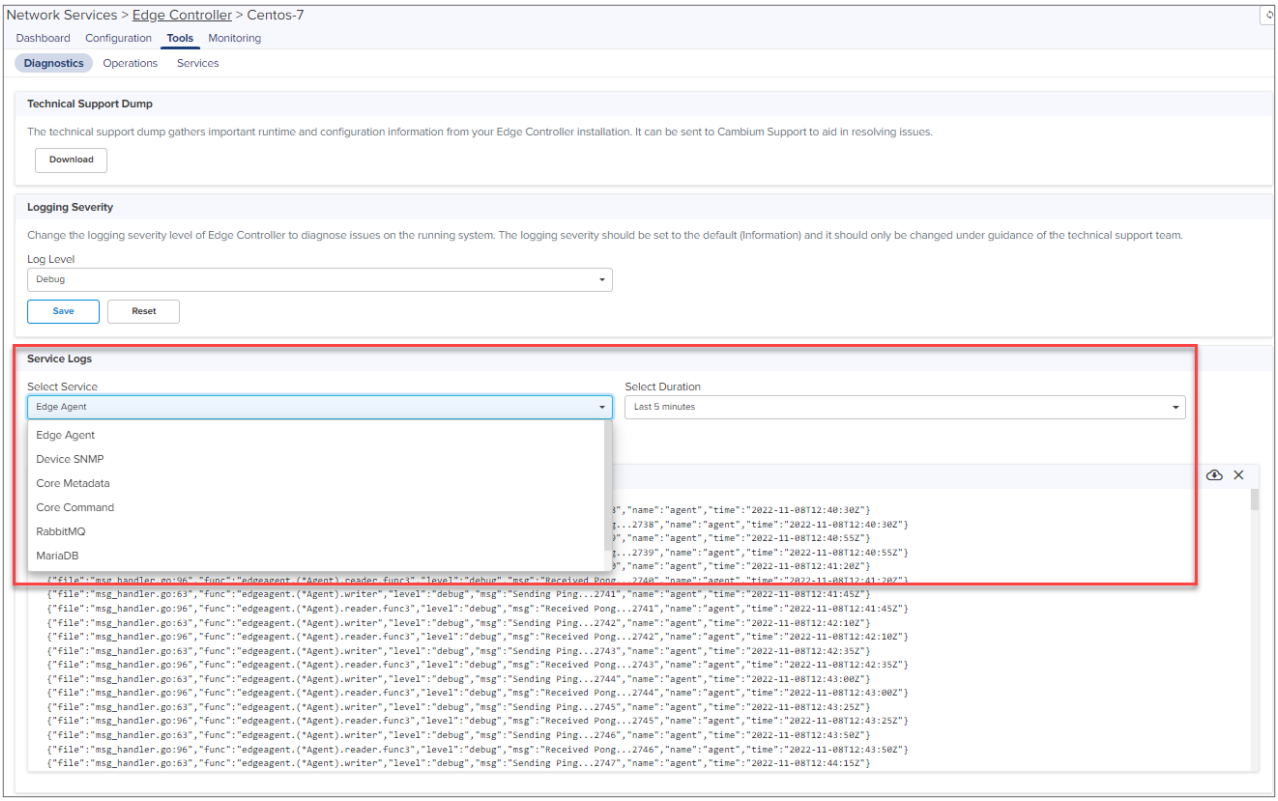
1. Select **Service** and **Duration** from the drop-down.

   The following list of service and duration (5 minutes, 15 minutes, 30 minutes and last 1 hour) are available from the drop-down:

   - Edge Agent
   - Device SNMP
   - Core Metadata
   - Core Command
   - RabbitMQ
   - MariaDB
   - SFTP

2. Click **Show Logs.**

   The output for the selected criteria appears as shown:

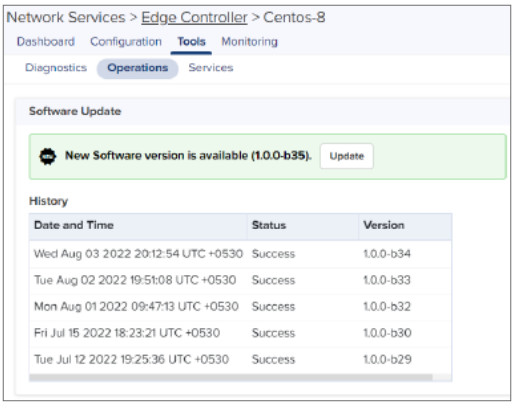


3. Click download ( ) icon to download the generated output.
4. Click clear (✕) icon to clear the output.

Operations

In the **Operations** page, you can view the current software version of the Edge Controller. You can also view history of the last five software updates.

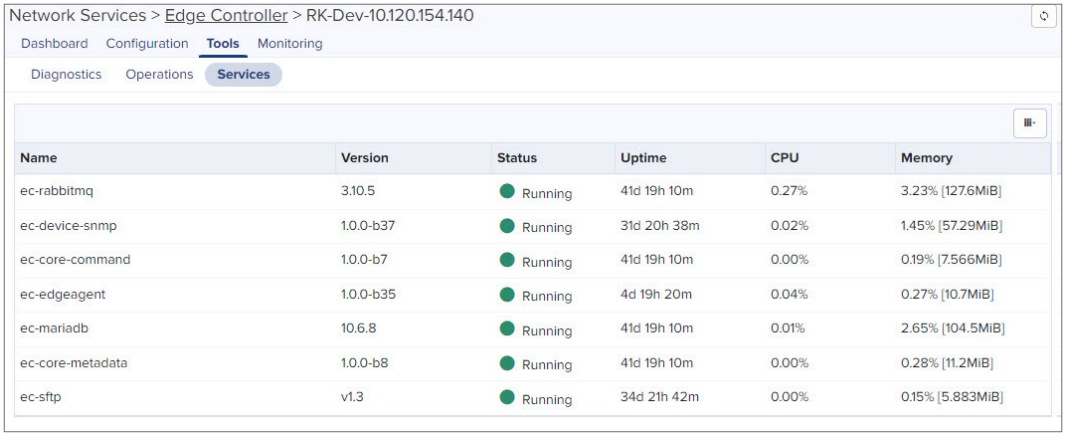
1. 1. Navigate to **Tools > Operations**.
2. 2. Click **Check for new software update**, checks for any new available software update.



Services

In **Services** page you can view the services running in the Edge Controller.

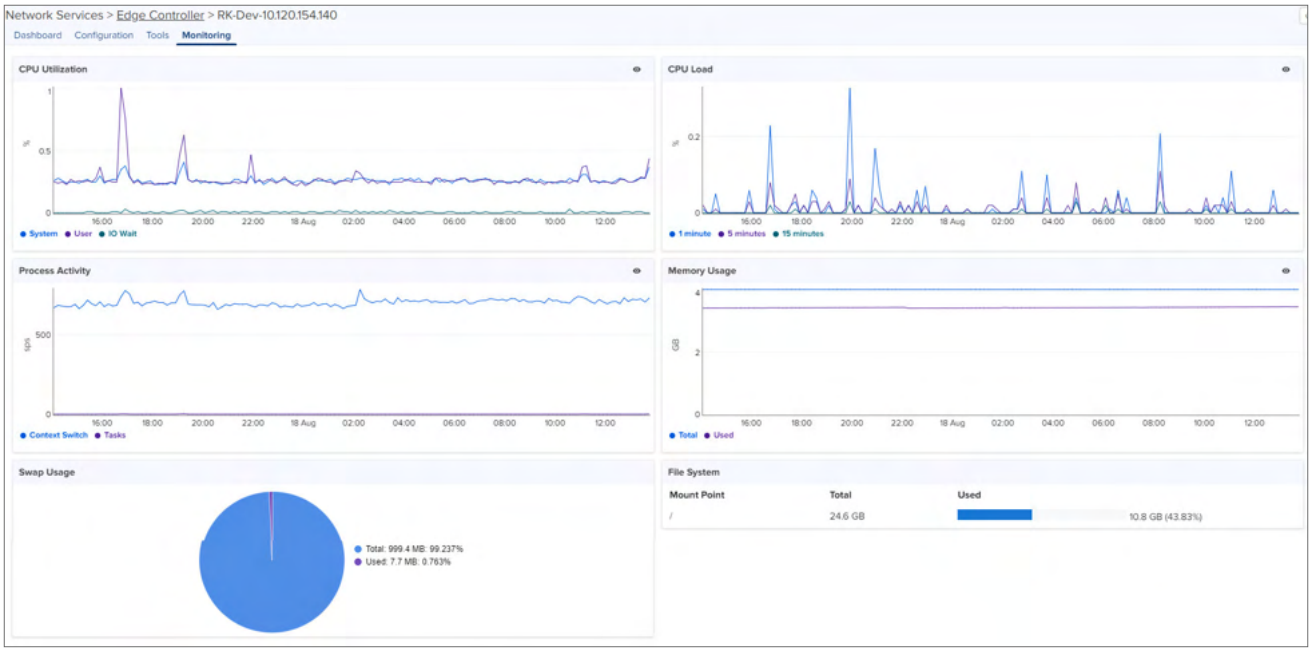
Figure 559 *Services*



Name	Version	Status	Uptime	CPU	Memory
ec-rabbitmq	3.10.5	Running	41d 19h 10m	0.27%	3.23% [127.6MiB]
ec-device-snmp	1.0.0-b37	Running	31d 20h 38m	0.02%	1.45% [57.29MiB]
ec-core-command	1.0.0-b7	Running	41d 19h 10m	0.00%	0.19% [7.566MiB]
ec-edgeagent	1.0.0-b35	Running	4d 19h 20m	0.04%	0.27% [10.7MiB]
ec-mariadb	10.6.8	Running	41d 19h 10m	0.01%	2.65% [104.5MiB]
ec-core-metadata	1.0.0-b8	Running	41d 19h 10m	0.00%	0.28% [11.2MiB]
ec-sftp	v1.3	Running	34d 21h 42m	0.00%	0.15% [5.883MiB]

Monitoring

In the **Monitor** page, you can view details of CPU utilization, CPU Load, Process Activity, Memory Usage, Swap Usage, and File System.



cnArcher Installation Summary

cnArcher is a mobile application used to install PMP Subscriber Modules (SMs), ePMP (SMs), and cnRanger SMs. The installation summary provides an overview of the data collected by cnArcher during the installation process.

Note

- cnArcher Installation Summary is a cnMaestro X feature.
- cnArcher Installation summary of PMP SM is available for users in cnMaestro Cloud and OnPremises from 3.1.0 release.
- cnArcher Installation summary of ePMP SM is available for users in cnMaestro Cloud and OnPremises from 3.1.1 release.
- ePMP PTP 550 (two radio devices) and ePMP Elevate are not supported for cnArcher Installation

Summary.

To view the installation summary:

1. Navigate to **Network Services** > **cnArcher Installation Summary.**

   The **cnArcher Installation Summary** page appears.

2. You can **Search** cnArcher Summary details by using **MAC Address**, **Name at Installation**, **Date** and **Time**, **Added By**, and **Comments.**

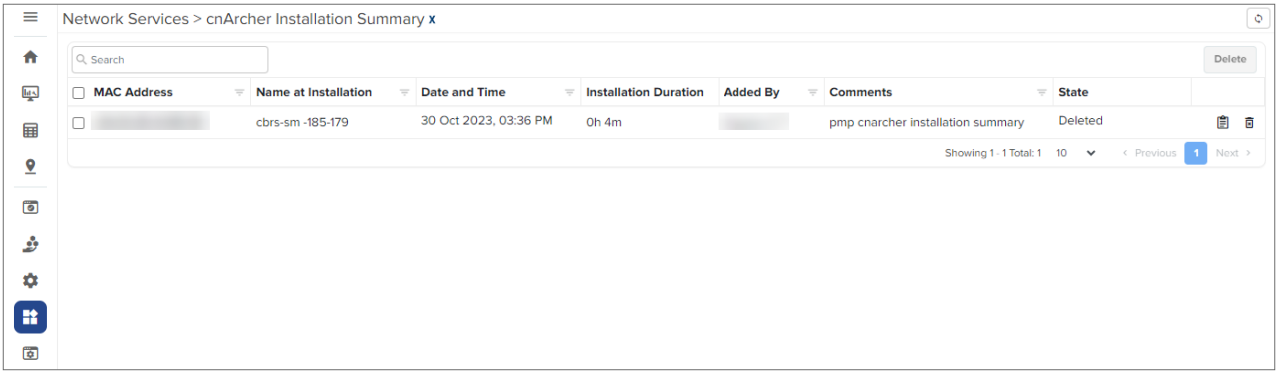


Table 155 *Fields in cnArcher Installation Summary*

Field	Description
MAC Address	MAC address of the device.
Name at Installation	Name given to the device when installed.
Date and Time	Date and time of installation.
Installation Duration	Duration of installation.
Added By	Name of the user adding the device.
Comments	Comments about the installation.
State	Current state of the device such as Managed or Deleted.

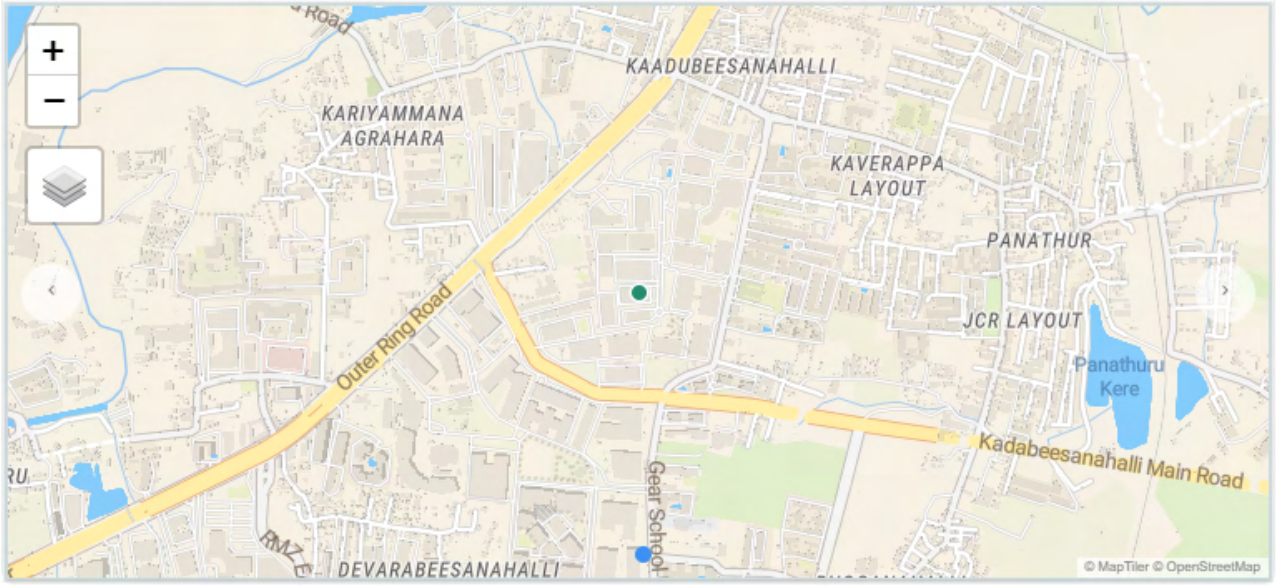
3. Click **View Details** icon to view detailed Installation Summary.

Installation Summary : cbrs-sm -185-179 on 30 Oct 2023, 03:36 PM

Summary	
SM Name	cbrs-sm -185-179
MAC Address	
MSN	
Product	PMP 450 SM 3.6 GHz
Software Version	CANOPY 22.1 SM
RSSI	-35.4 dBm
SSR	1.4
External Antenna	No External Antenna
Start Timestamp	30 Oct 2023, 03:32 PM
End Timestamp	30 Oct 2023, 03:36 PM
Added By	
Comment	pmp cnarcher installation sum...

Configuration	
IP Address/Setting	/Static
Subnet	
Gateway	
DNS	
Management VLAN	Not Configured
Data VLAN	Not Configured
Security	none
PSK	-
Status	Already Onboarded
Software Update	Not Configured
Template	Not Configured
Onboarding Details	SM was already cloud manag...

Photos & Location: Map



Link Test Result

Time	Mode	Throughput Uplink/Downlink	Modulation Uplink/Downlink
30 Oct 2023, 03:35 PM	Extrapolated	1.7 Mbps / 38.5 Mbps	8 X / -

AP Scan Result

AP MAC	AP Bandwidth	AP Frequency	Registered
	30 MHz	3580.0 MHz	Yes

Copyright © 2015 - 2024 Cambium Networks, Ltd. All rights reserved | Version 5.0.0-r23 | Community | Support | Help

Table 156 *Summary fields in cnArcher Installation*

Field	Description
SM Name	Name of the device.
MAC Address	MAC address of SM.
MSN	Serial number of device.
Product	Device model and type.
Software Version	Software version of device.
RSSI	Receiver Signal Strength Indicator (RSSI) of SM.
SSR	Signal Strength Ratio (SSR).
External Antenna	Peak gain of external antenna connected to the device.
Start Timestamp	Start time of the summary.
End Timestamp	End time of the summary.
Added By	Name of the user adding the device.
Comment	Comments about the installation process.

Configuration

Table 157 *Configuration fields in cnArcher Installation*

Field	Description
IP Address/Setting	IP settings such as for DHCP or Static IP allocation.
Subnet	Subnet mask of the device.
Gateway	IP address of the gateway.
DNS	Name of the DNS server.
Management VLAN	Configured Management VLAN.
Data VLAN	Configured Data VLAN.
Security	Security settings.
PSK	Type of PSK (Pre-Shared Key): WPA or WPA2.
Status	Current SM state such as Onboarded or Already Onboarded.
Software Update	Software version provided to upgrade.
Template	Name of the configuration template to apply.
Onboarding Details	Onboarding details related to SM.

Photos and Location

Photos and Location displays the photos taken during installation. You can view a maximum of four photos at a time.

Link Test Result

Link Test Result displays the link related test results with respect to throughput.

Table 158 *Link Test Results fields*

Field	Description
Time	Time at which the link test was performed.
Mode	Modes such as Extrapolated Link Test or Link Test with Bridging.
Throughput Uplink/Downlink	Uplink and Downlink Throughput.
Modulation Uplink/Downlink	Uplink and Downlink Modulation.

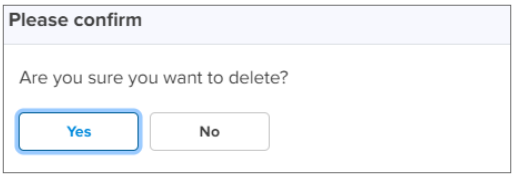
AP Scan Result

AP Scan Result displays a list of scanned APs.

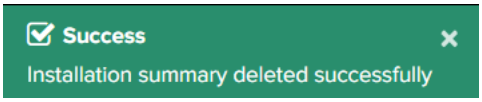
Table 159 *Fields in AP Scan Result*

Field	Description
AP MAC	MAC address of the AP.
AP Bandwidth	Bandwidth of the AP.
AP Frequency	Frequency of the AP.
Registered	Details of the registered SM.

1. Click the delete (🗑) icon to delete single or multiple entries from the **cnArcher Installation Summary** page.
2. Click **Yes** to delete.



3. A confirmation message is displayed on a successful delete.



Note

cnArcher uploads Installation Summary with cnMaestro when Internet connection is available to users mobile device. This feature is support only in Android.

Spectrum Analyzer X

The Spectrum Analyzer feature monitors and analyzes wireless spectrum for PMP AP and SM devices, allowing users to optimize network performance.

Note

- The Spectrum Analyzer is a cnMaestro X feature.
- Spectrum Analysis is supported on devices running PMP software version 22.1.0 and above.
- Spectrum Analyzer feature is available for users in cnMaestro Cloud and On-Premises.

To view Spectrum Analyzer page:

1. Navigate to **Network Services** > **Spectrum Analyzer**.
2. You can view the Spectrum Analyzer details by using **Name**, **Status**, **Type**, **Sector Count**, **Start Time**, and **End Time**.

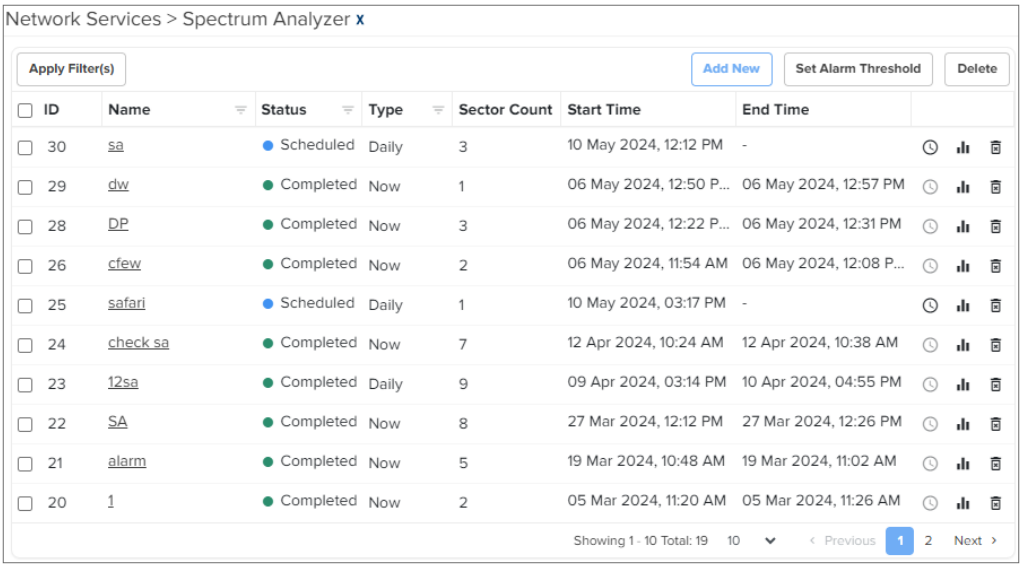


Table 160 *Fields in Spectrum Analyzer*

Field	Description
Name	The user-defined name for the spectrum analysis job or scan.
Status	The current status of the spectrum analysis.
Type	The type of analysis performed (for example, Now, Weekly).
Sector Count	The number of sectors or wireless areas analyzed in the spectrum scan.
Start Time	The scheduled start time for the spectrum analysis job.
End Time	The scheduled end time for the spectrum analysis job.

3. Click **View Result** icon on top right corner to view the detailed Spectrum Analyzer summary.

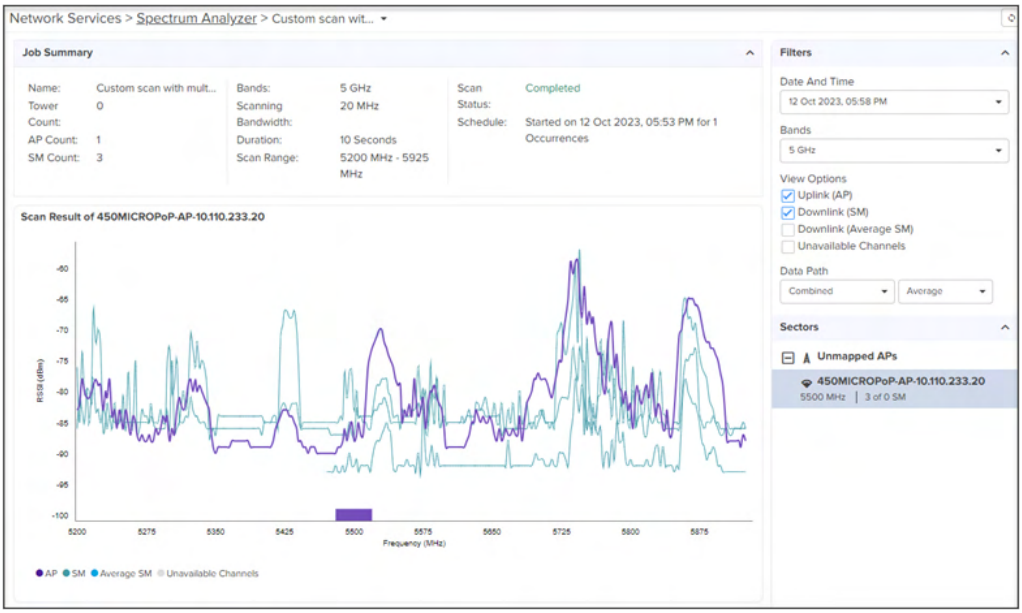


Table 161 *Job Summary parameters*

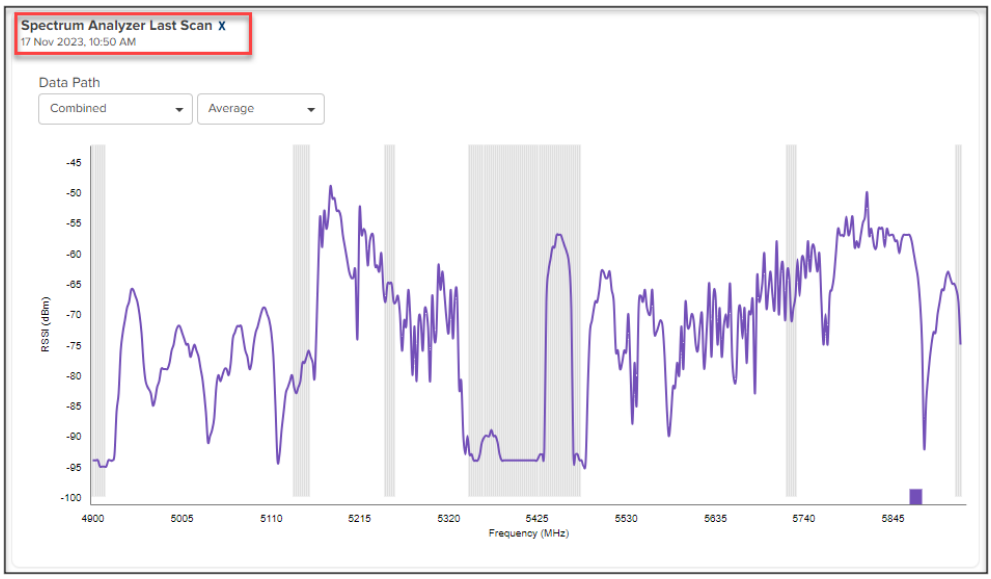
Field	Description
Name	The user-assigned name for the analysis job.
Tower Count	The number of towers included in the analysis.
AP Count	The number of APs in the analysis.
SM Count	The number of SMs in the analysis.
Bands	The frequency bands under analysis.
Scanning Bandwidth	The width of the frequency band being scanned.
Duration	The duration of the analysis job.
Scan Range	The spectrum range analyzed.
Scan Status	The current status of the analysis job.
Schedule	The scheduling details for the analysis job.

Table 162 *Filters parameters*

Field	Description
Date and Time	The specific date and time when the spectrum analysis is conducted.
Bands	The frequency bands included in the analysis.
View Options	The viewing options for analyzing the spectrum. • Uplink (AP) • Downlink (SM) • Downlink (Average SM) • Unavailable Channels
Data Path	The data path used for the analysis. • **Combined**: Combines data from Path A and Path B for analysis. • **Average**: Calculates the average and maximum values for the analysis data.

4. **Scan Result** displays the scanning result graph.
5. To view the last scan results at the device level:

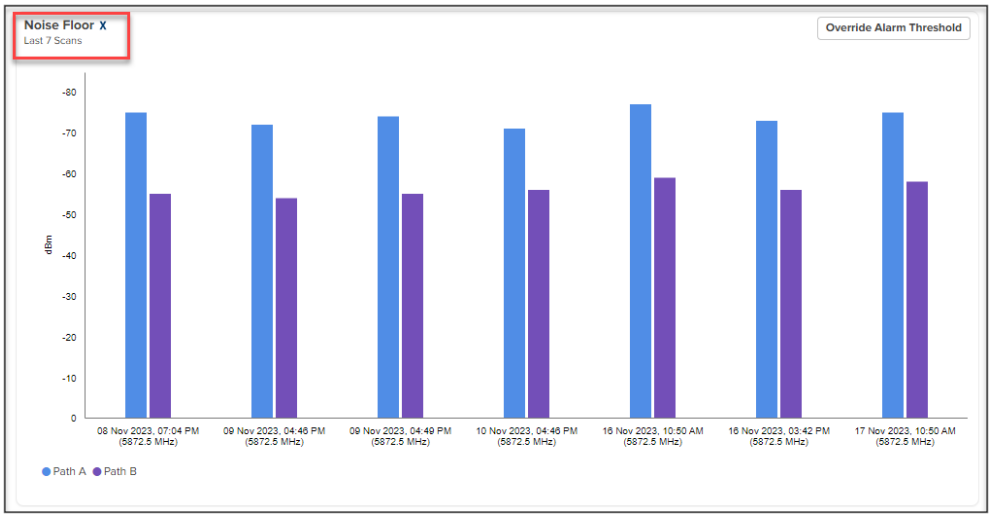
a. Navigate to PMP device **Dashboard** > **Spectrum Analyzer Last Scan**.



b. The dashboard automatically generates the appropriate graph for AP and SM based on the device type.

c. The default data path for displayed graphs is **Combined**, and users can customize it to their preferences.

d. The dashboard displays **Noise Floor**, which provides noise floor information for both **Path A** and **Path B**. These two graphs are displayed for both AP and SM that are part of the scan.

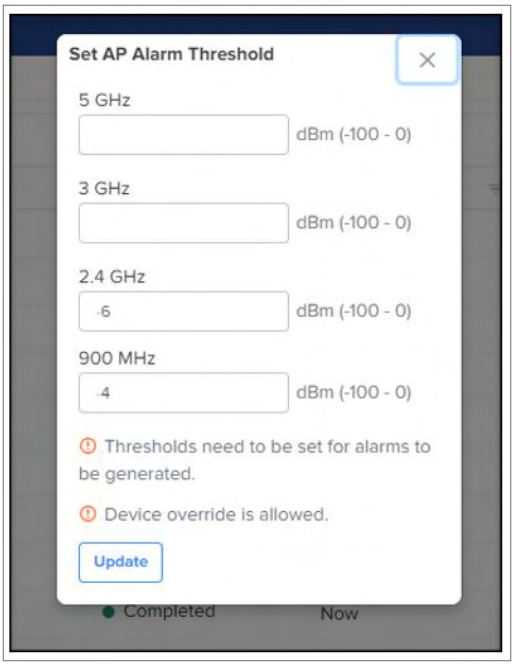


e. **Unmapped APs** display any APs that are not assigned to a tower.

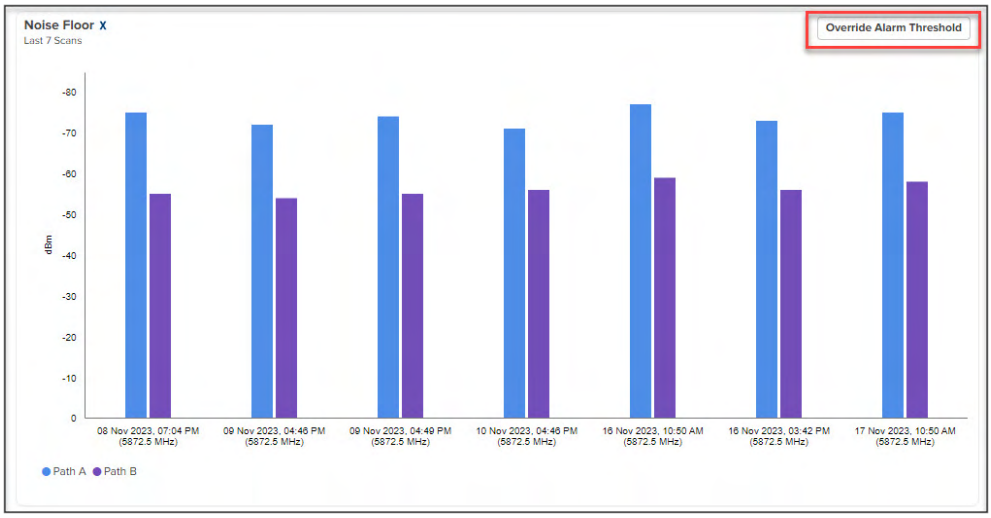
f. Click **Delete** icon on the top right corner to delete a job.

To set Alarm Threshold:

1. Navigate to **Network Services** > **Spectrum Analyzer**.
2. Click on the **Set Alarm Threshold** on the top right corner of the Spectrum Analyzer page.



3. Users can set band-specific alarms by configuring threshold values and alarm triggers for specific frequency bands (for example, 5 GHz, 3 GHz, 2.4 GHz, and 900 MHz).
4. These alarms are applied globally to all PMP devices operating in the same frequency band.
5. After configuration, the alarms are displayed on the alarm page, enabling easy monitoring and timely responses to network issues.
6. User can override alarm threshold for AP at the device level:
   a. Navigate to **Dashboard** > **Override Alarm Threshold**.



   b. Before overriding, users can review the global alarm threshold values that apply to the entire network.



c. Choose the specific AP device for which you want to set custom alarm thresholds.

d. Configure and set individual threshold values for the selected device, overriding the global thresholds only for that specific device.

To create a new job:

1. Navigate to **Network Services** > **Spectrum Analyzer**.
2. Click on **Add New** on the top right corner of the Spectrum Analyzer page.

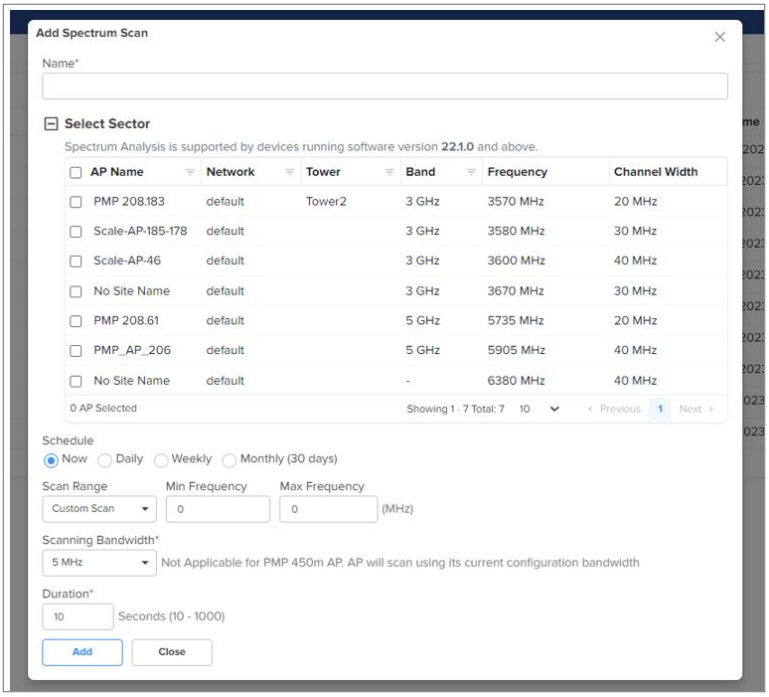


Table 163 *Add Spectrum Scan parameters*

Field	Description
Name	Job name to distinguish the analysis job within the Spectrum Analyzer.
Schedule	Scheduling options, including: • **Now**: Immediate execution of the spectrum analysis. • **Daily**: Set up a daily schedule for the analysis job. • **Weekly**: Configure a weekly schedule for the analysis job. • **Monthly**: Create a monthly schedule for the analysis job.
Scan Range	The desired scan range from a drop-down with two options:

Table 163 *Add Spectrum Scan parameters*

Field	Description
	• **Full Scan**: Performs a comprehensive analysis of the entire spectrum. • **Custom Scan**: Set the Min Frequency and Max Frequency to precisely choose the frequency range for a more accurate spectrum analysis.
Scanning Bandwidth	The specific scanning bandwidth from the available options to adjust the spectrum analysis.  **Note** Scanning Bandwidth is not applicable for PMP 450m AP.
Duration	The analysis duration in seconds, ranging from 10 to 1000 seconds.

3. After creating the job, it appears on the home page with a **Scheduled** status.

Administration

This section includes the following topics:

- Managing Users
- Cloud Anchor Account
- Settings
- Audit Logs

Users

This chapter provides the following details:

- Managing Users
- Session Management

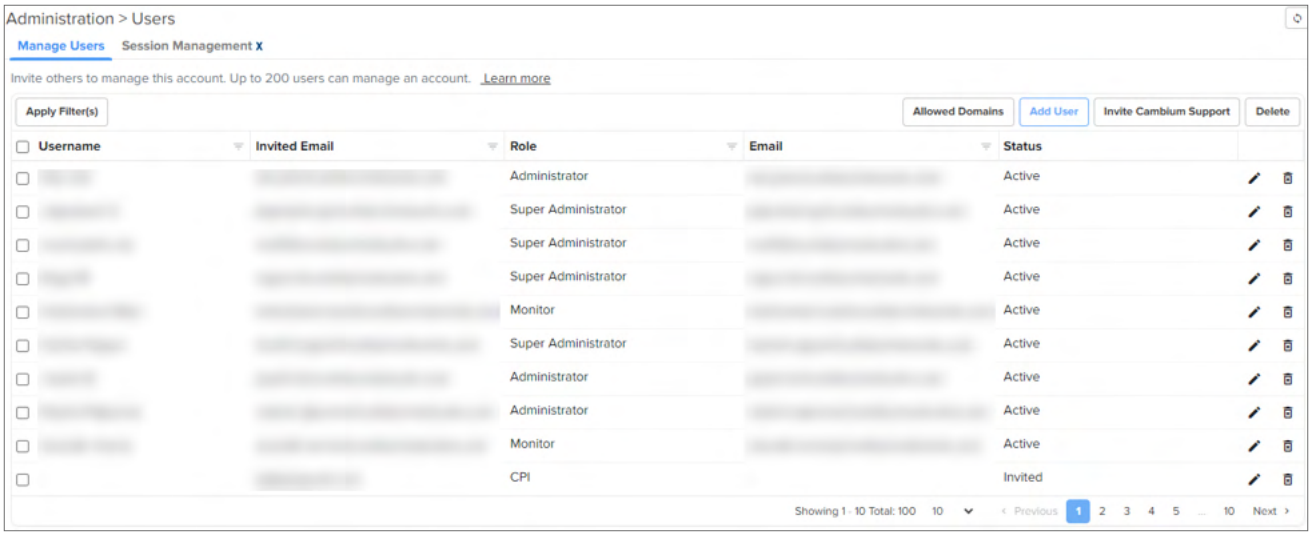
Managing Users

cnMaestro allows you to add Users using the **Administration > Users** page.

Note

- cnMaestro X account supports up to 200 users.
- cnMaestro Essentials account supports only up to 10 users.

Figure 560 *Adding Users*



Role-Based Access

cnMaestro supports the following user Roles:

- **Super Administrator** – Super Administrators can perform all operations.
- **Administrator** – Administrators can modify cnMaestro application functionality, but they are not able to edit User, API, or Server configuration.
- **Operator** – Operators are able to configure device-specific parameters and view all configuration.
- **Monitor** - Monitors have only the view access.
- **CPI -** CPI can perform onboarding the devices using the CBRS tool and has the view access only.



Note

- cnMaestro allows one to limit the number of concurrent sessions for each Role and display current active user sessions.
- CPI role is authorized only when the **CBRS** is Enabled.

Role-Mappings

The table below defines how Roles are authorized to access specific features.

Table 164 *Role-Mappings*

Feature	Description
Access Control Policies	Configure policies to control users connectivity to the network. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Application Operations	Application level operations such as to create, update and delete operations for Networks, Towers/Sites. Bulk device configuration. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Application Settings	Change global application configuration and onboarding key. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Assists	Scan device configurations and generate assists scores, which in turn helps in isolating configuration issues in a deployment. • Super Administrator - All • Administrator - All

Table 164 *Role-Mappings*

Feature	Description
	• Operator - All • Monitor - All (**Fix Now** is not allowed) • CPI - All (**Fix Now** is not allowed)
Citizen Broadband Radio Service Subscription (CBRS)	Support CBRS-compliant devices in the 3.6 GHz band (from 3550 MHz to 3700 MHz) • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - All
cnArcher Installation Summary	View installation summary of PMP ePMP, and cnRanger SMs installed using the cnArcher Mobile Application. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - View
Configuration/Software Update	Manage configuration/software update jobs. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Custom Applications	Configure applications with a specific IP address or a domain name, and apply filter rules. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Device Operations	Device operations such as reboot device, link test, connectivity test, tech support file download, and Wi-Fi performance test. • Super Administrator - All • Administrator - All • Operator - All

Table 164 *Role-Mappings*

Feature	Description
	• Monitor - None • CPI - None
Device Overrides	Per-device configuration, including updating AP Group and applying configuration. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
EasyPass	Create captive portal using EasyPass to allow clients to access the network through Free Tiers, Vouchers, or Paid Access types. • Super Administrator - All • Administrator - All • Operator -View • Monitor - View (Sessions Only) • CPI - None
Floor Plan	Floor Plan configuration • Super Administrator - All • Administrator - All • Operator - View • Monitor - View • CPI - None
Global Configuration	The ability to create and apply configuration for global features such as Templates, WLANs, AP Groups, and bulk sync configuration. • Super Administrator - All • Administrator - All • Operator -View • Monitor - None • CPI - None
Guest Portal	Guest Portal configuration. • Super Administrator - All • Administrator - All • Operator -View • Monitor - View (Sessions Only) • CPI - None

Table 164 *Role-Mappings*

Feature	Description
LTE	Manage cnRanger LTE devices. • Super Administrator - All • Administrator - All • Operator - View and Edit SIM credentials only • Monitor - None • CPI - None
Monitoring	Display of monitoring data at all levels. • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - View
Notifications	Alarms and Events management. • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - View
Onboarding	Device approval, modifying individual device configuration, and performing software update. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - All
Reporting	Report generation. • Super Administrator - All • Administrator - All • Operator - All • Monitor - All • CPI - All
Session Management	Capability to view and logout other users sessions. • Super Administrator - All • Administrator - All

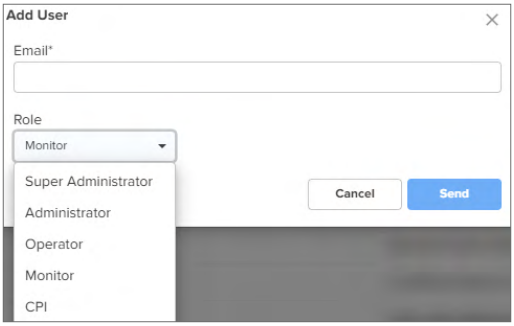
Table 164 *Role-Mappings*

Feature	Description
	• Operator - None • Monitor - None • CPI - None
Software Upgrade	Upgrade the device with the latest software. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Spectrum Analyzer	Analyze and monitor wireless spectrum for optimizing network performance on PMP devices. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
User Management	User management operations such as manage users and roles. • Super Administrator - All • Administrator - View • Operator - None • Monitor - None • CPI - None

Creating Users and Configuring User Roles

To add an administrator:

1. Navigate to **Administration** > **Users** page.
2. Click **Add User** button. The following window is displayed:



3. Enter the email address in the **Email** box.

4. To configure the User Role, select any one of the role for the user from the **Role** drop-down list:
    - Super Administrator
    - Administrator
    - Operator
    - Monitor
    - CPI
5. Click **Send** button to add this user.

To edit or delete a user, click the Edit icon or the Delete icon against the user in the **Administration > Users** page.

Whitelisting specific domains

Using the **Administration > Users** page, you can allow (or whitelist) a specific domain (for example, gmail.com). When users from the whitelisted (or allowed) domain are added, an invite email is sent directly to them. When the users accept the invite, they are allowed to access a particular cnMaestro UI account.

You can also blacklist or disallow a specific domain to prohibit all users of that domain from accessing the UI account.

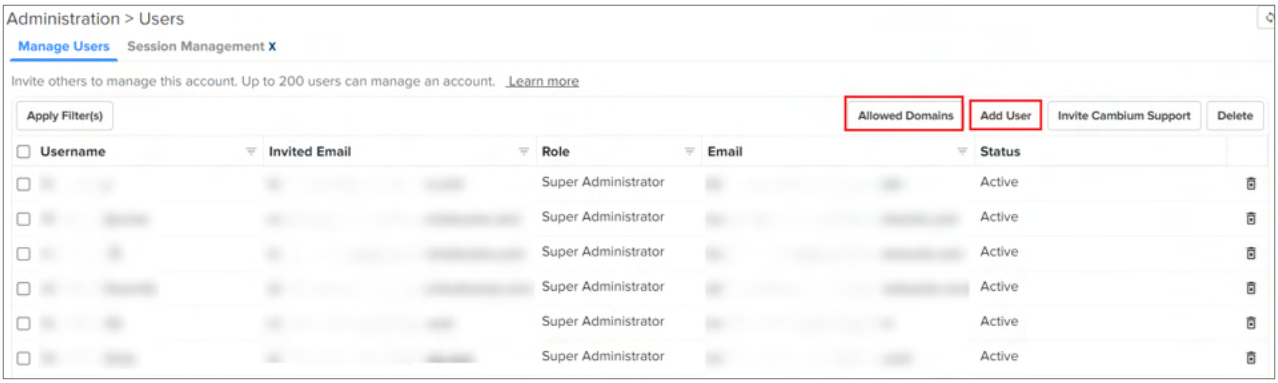
Note

- Domain whitelisting is not applicable to NFR User accounts.
- For users from the whitelisted domains, you can create the MSP user account.

To whitelist or blacklist a specific domain, perform the following steps:

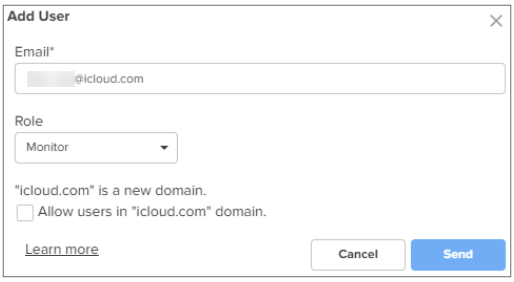
1. Navigate to **Administration > Users** page.

    The **Manage Users** page appears.



2. To add a new domain (for example, a gmail ID), click on the **Add User** button.

    The **Add User** window appears. You must set the fields, as described in the Creating Users and Configuring User Roles section. The **Add User** window also displays that the email ID used is a new domain, as shown in the following example (in this case, gmail.com is the new domain):



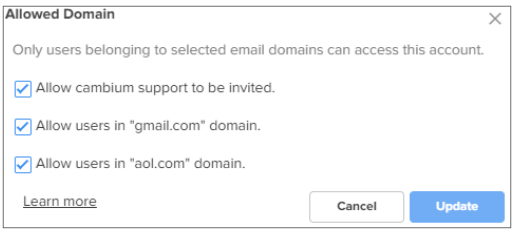
3. Select the **Allow users in "gmail.com" domain** check box (the domain name varies based on the email ID you add).

   The new domain is added to the database.

   When users who belong to this allowed domain (for example, gmail.com) are added (using the **Add User** button), an invite email is directly sent to the users. When the users accept the invite, they can access a particular cnMaestro UI account. The **Allow users in "gmailail.com" domain** checkbox is available only when you are adding a new domain.

4. To blacklist or disallow a specific domain, click on the **Allowed Domains** button on the **Manage Users** page.

   The **Allowed Domain** window appears with a list of whitelisted domains.



5. Uncheck the required domain check box to blacklist hat specific domain.
6. 1. Select **Update**.

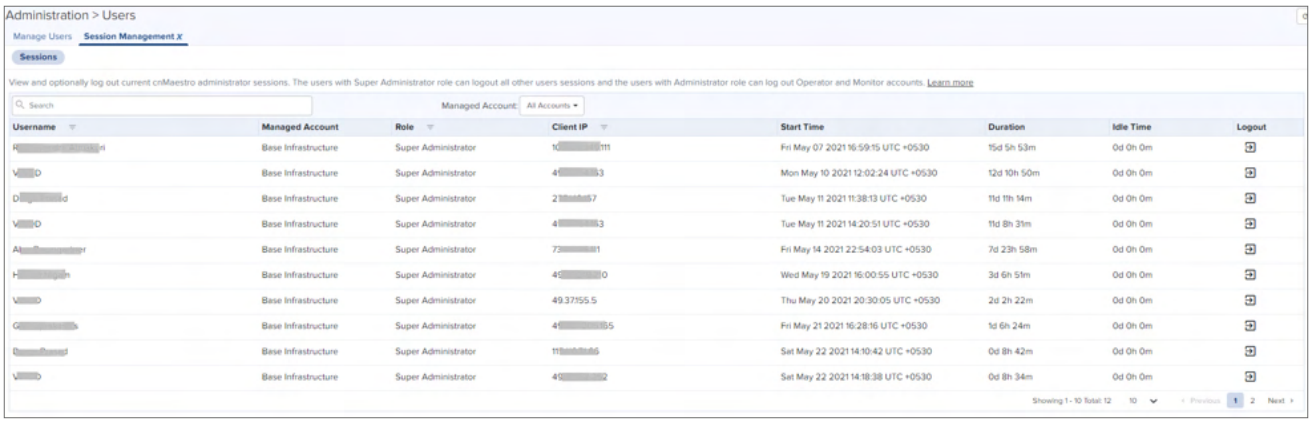
All users from that blacklisted domain are not allowed to access the UI. To allow the blacklisted domain, you must check the required domain check box on the **Allowed Domain** window.

Session Management

View and optionally log out current cnMaestro administrator sessions. The users with Super Administrator role can logout all other users sessions and the users with Administrator roles can logout Operator and Monitor accounts.

Sessions

Displays the detailed information on the user sessions.



Cloud Anchor Account

This chapter provides the following details:

- Manage Instances
- Inventory
- Administration
- Network Services
- Manage Subscriptions

Manage Instances

Registration of On-Premise customer accounts to Cloud is addressed by this feature. This will allow us to do many synchronization things in On-Premises instances, similar to Cloud will have the inventory stats from instances.

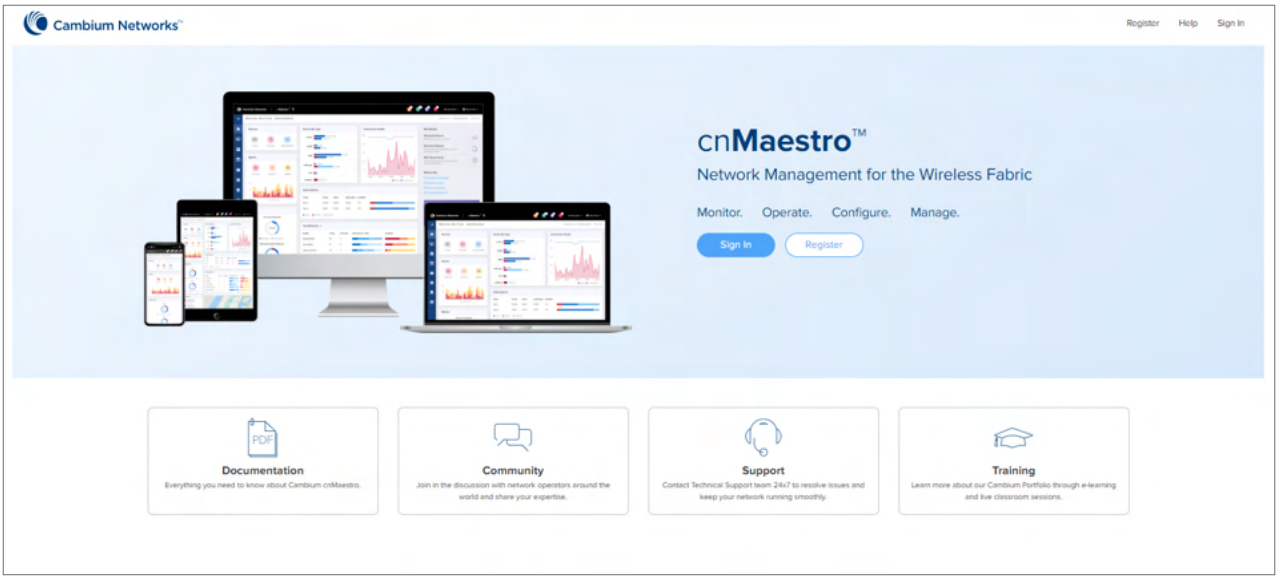
Manage Instances describes the following

- Onboarding
- On-Premises Instances
- Notifications

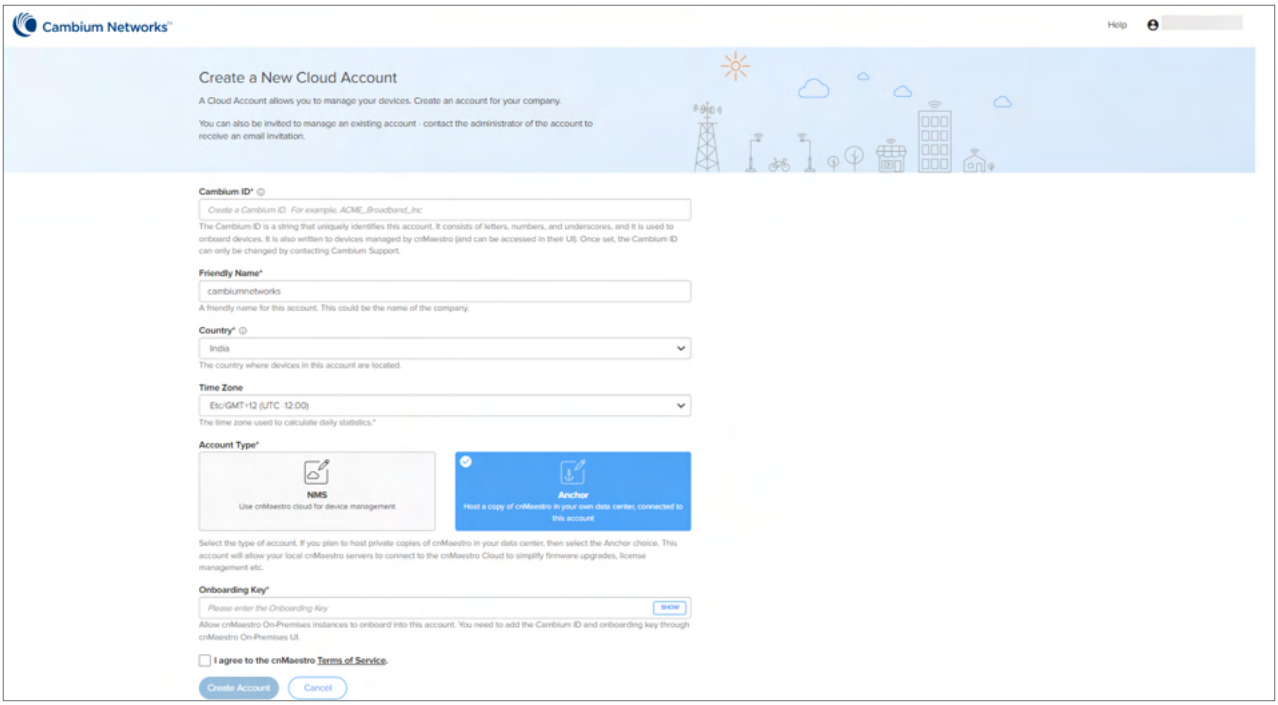
Onboarding

To onboard the devices to the Cloud Anchor Account, you need to create the Cloud account before connecting to cnMaestro On-Premises:

1. Log in to the cnMaestro UI, https://cloud.cambiumnetworks.com.

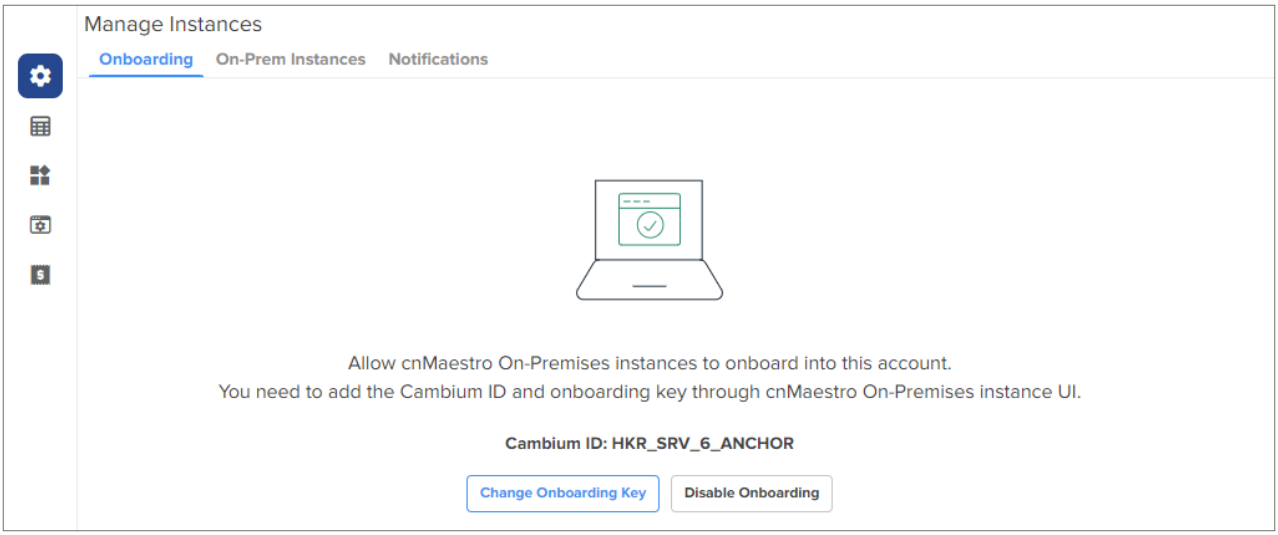


2. In **Account Type**, select **Anchor**.



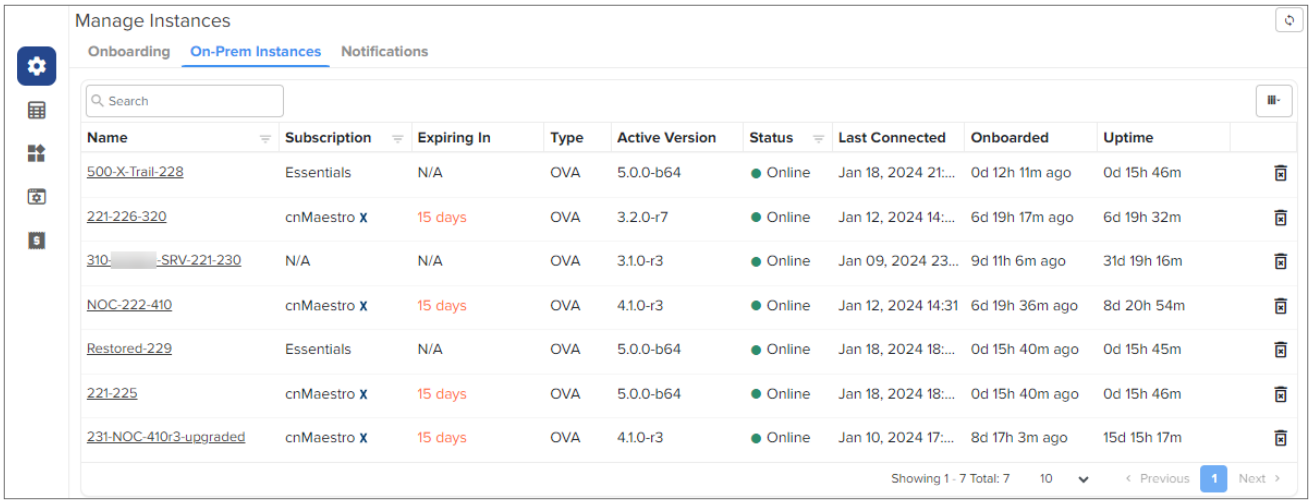
3. Enter the On-Premises **Onboarding Key**.
4. Click I agree to the cnMaestro **Terms of Service**.
5. Click **Create Account**.
6. When the Anchor Account is created, an Onboarding Key must be set to allow On-Premises instances to connect.
7. Navigate to the **Manage Instances** page as shown below and allows you to change the **Onboarding Key** and **Disable Onboarding**.

   This key needs to be entered in the cnMaestro On-Premises UI to connect to the Anchor Account.

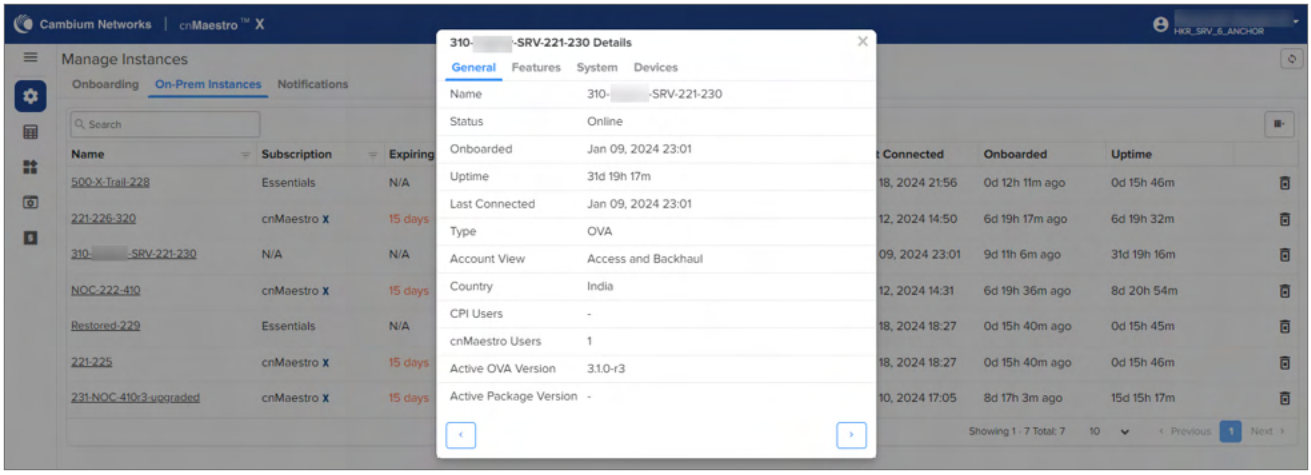


On-Premises Instances

Once the On-Premises server has been onboarded with the Key, it will be included in the **On-Prem Instances** page. Multiple On-Premises installations can be added to a single Anchor Account.

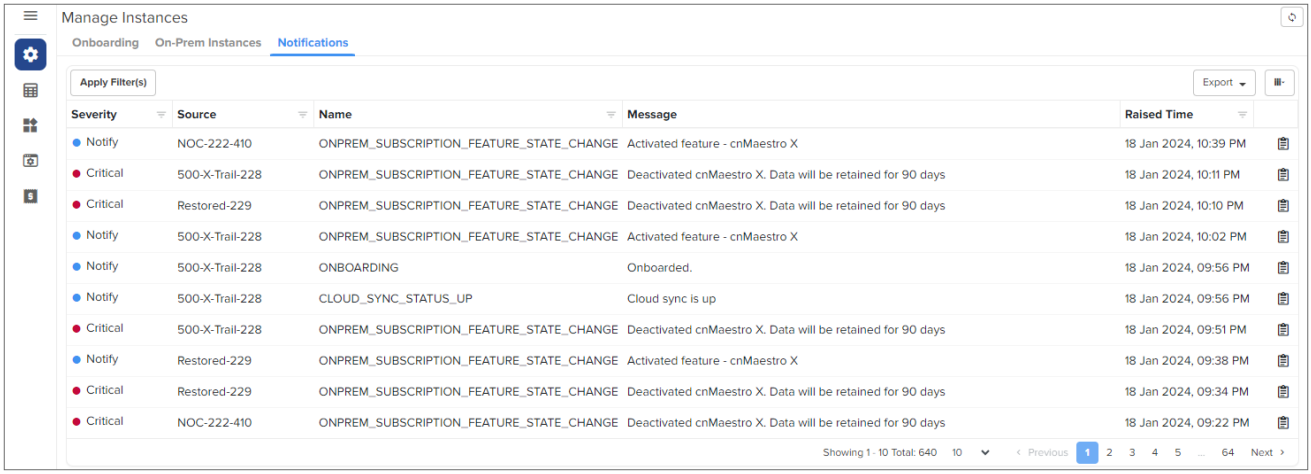


By clicking the instance host name, you can see the On-Premises server details such as General, Features, System, and CBRS:

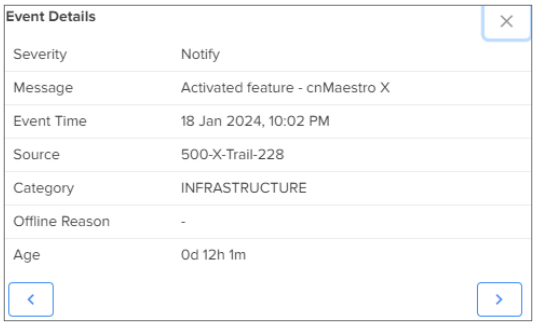


Notifications

Notification page displays the history of the most recent events notification of On-Premises instances with **Severity**, **Source**, **Name**, **Raised Time**, and **Message**.

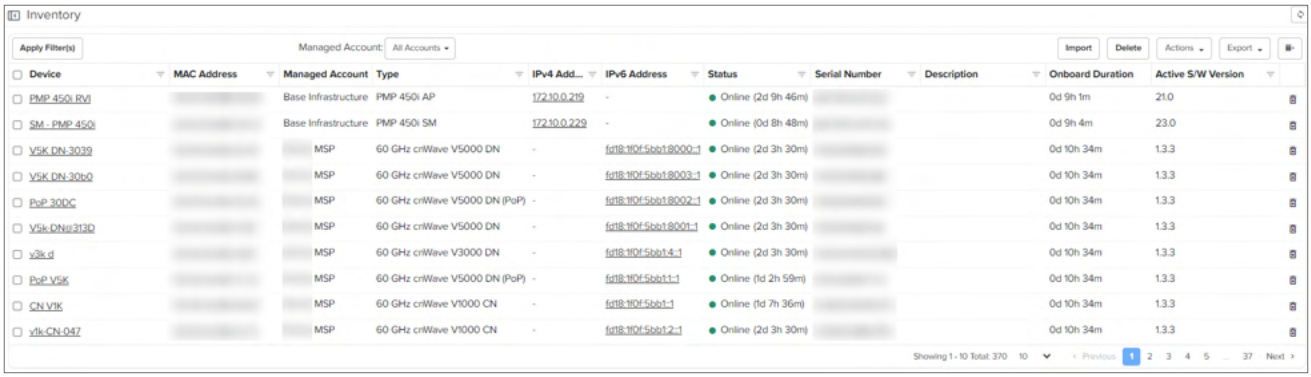


Click View Details to view the Event Details as shown below:



Inventory

The **Inventory** page displays a list of devices under the selected Node. It presents health and maintenance information provides a tabular view that allows for sorting and filtering. When selected for a single device, it presents a detailed customized page of that device.



Administration

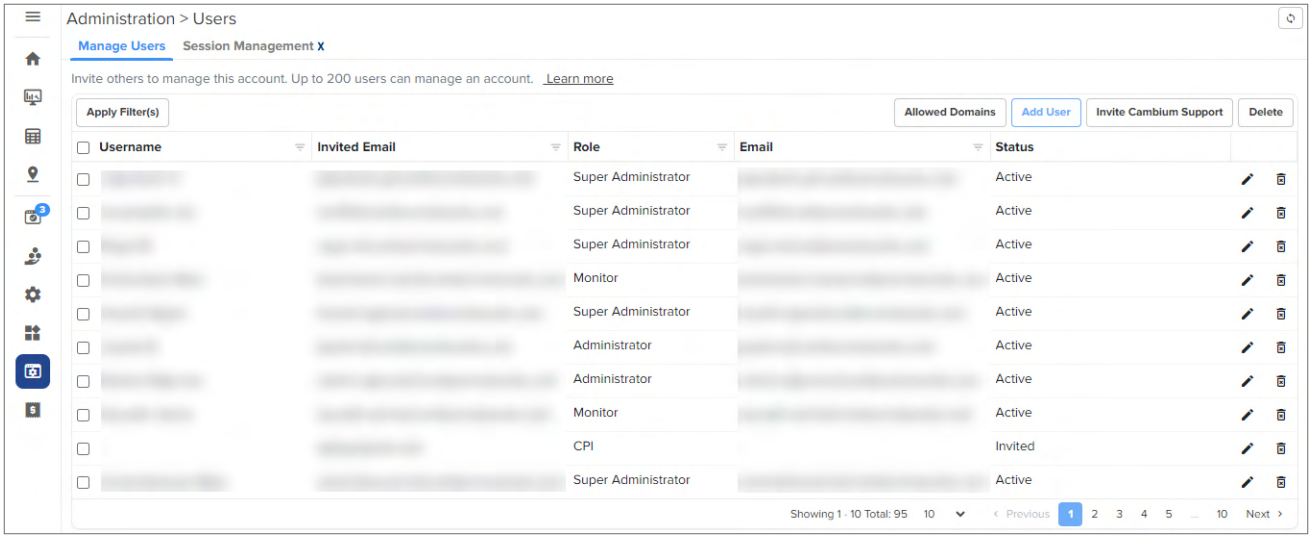
Administration provides the following details:

- Users
- Audit Logs

Users

cnMaestro allows to add Users using the **Administration > Users** page. A maximum of ten users are currently allowed in the system.

Figure 561 *Adding Users*



Role-Based Access

On successful authentication, every request from this user is processed in light of their Role.

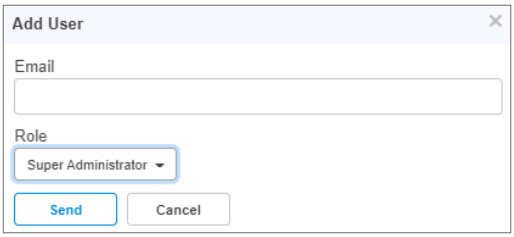
cnMaestro supports the user Role:

- **Super Administrator** – Super Administrators can perform all operations.

Creating Users and Configuring User Roles

To add an administrator:

1. Navigate to **Administration > Users** page.
2. Click **Add User** button. The following window is displayed:

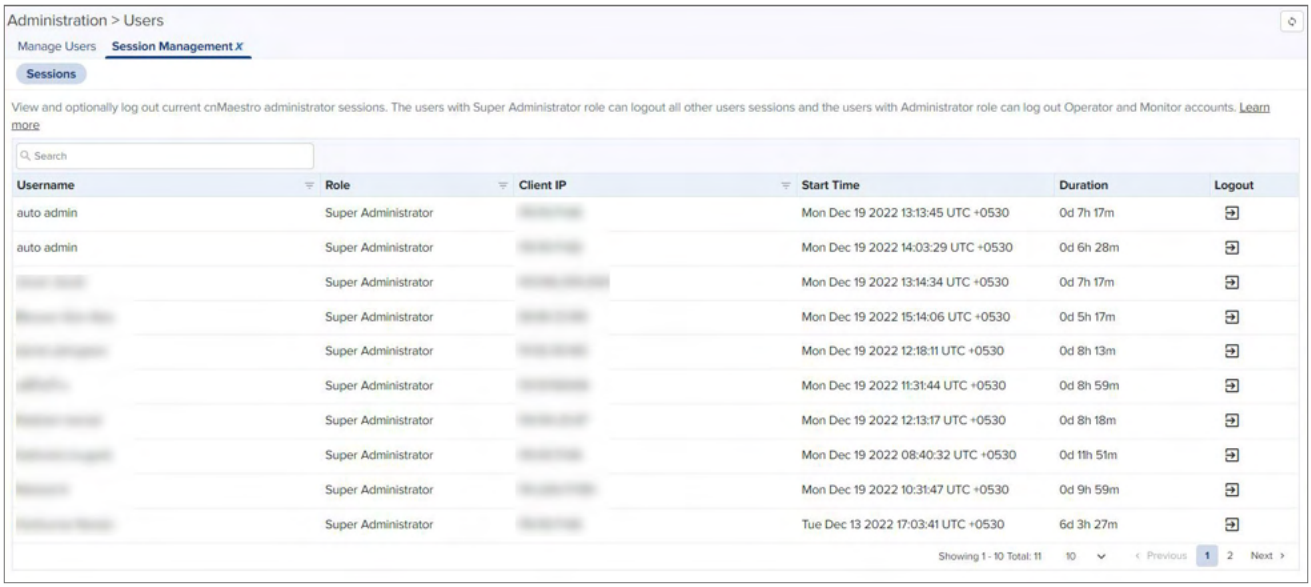


3. Enter the ID in the **Email** text box.
4. Click **Send** button to add this user.

To delete, click the delete icon against the user in the **Administration > Users** page.

Session Management

View and optionally log out current cnMaestro administrator sessions. The users with Super Administrator role can logout all other users sessions and the users with Administrator role can log out Operator and Monitor accounts.



Network Services

Network Services provide the following details:

- CBRS
- Organization

CBRS

Citizens Broadband Radio Service subscription for the CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz).

For further information, refer to CBRS.

Organization

An Organization allows multiple accounts to share CBRS billing and SAS ID. The Primary account owns this configuration, and the Secondary account can optionally share it. Both accounts must authorize the sharing.

For further information, refer to Organization.

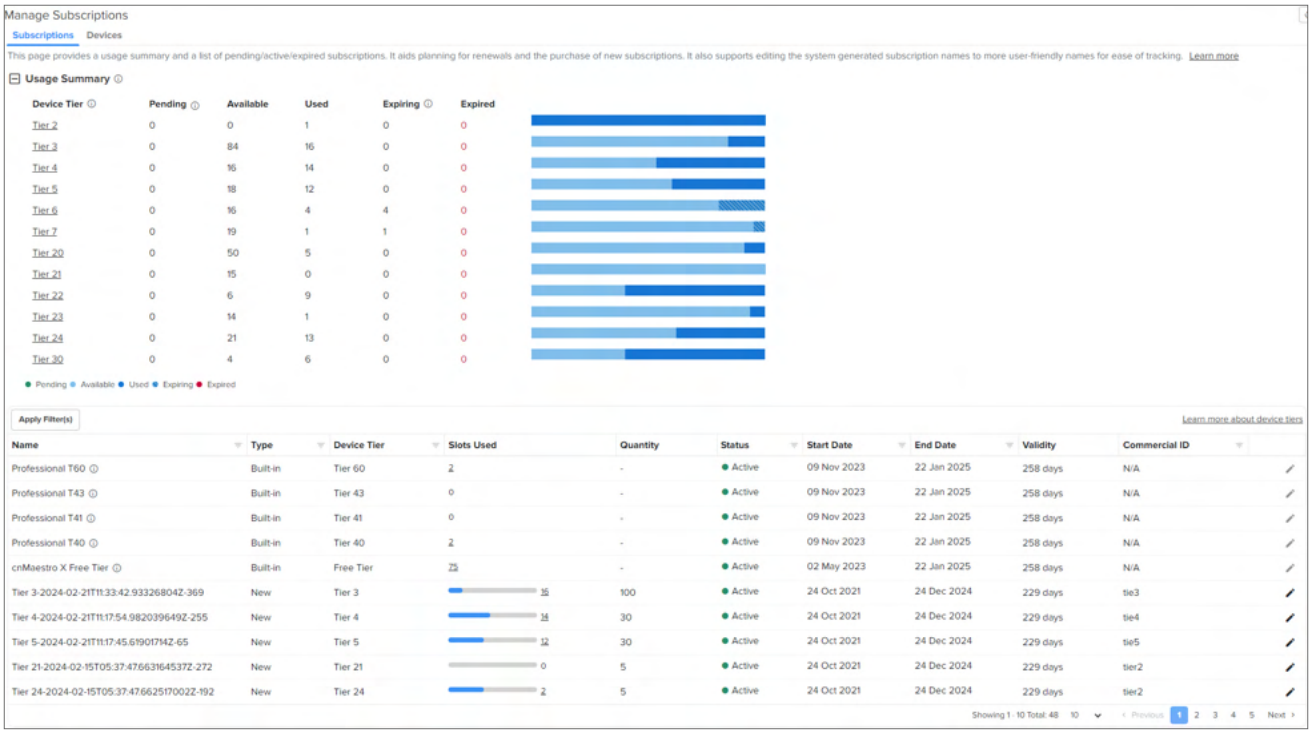
Manage Subscriptions

Manage Subscriptions provide the following details:

- Subscriptions
- Devices
- On-Premises Instances

Subscriptions

Subscriptions page describes about the usage summary and a list of pending, active, and expired subscriptions. It aids planning for renewals and the purchase of new subscriptions.

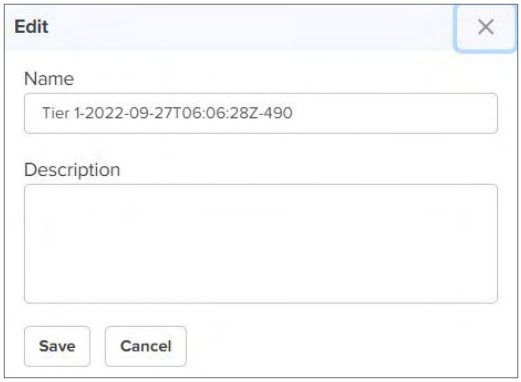


It also supports editing the system generated subscription names to more user-friendly names for ease of tracking.

To edit the **Subscriptions** perform the following steps:

1. click edit (✎) icon.

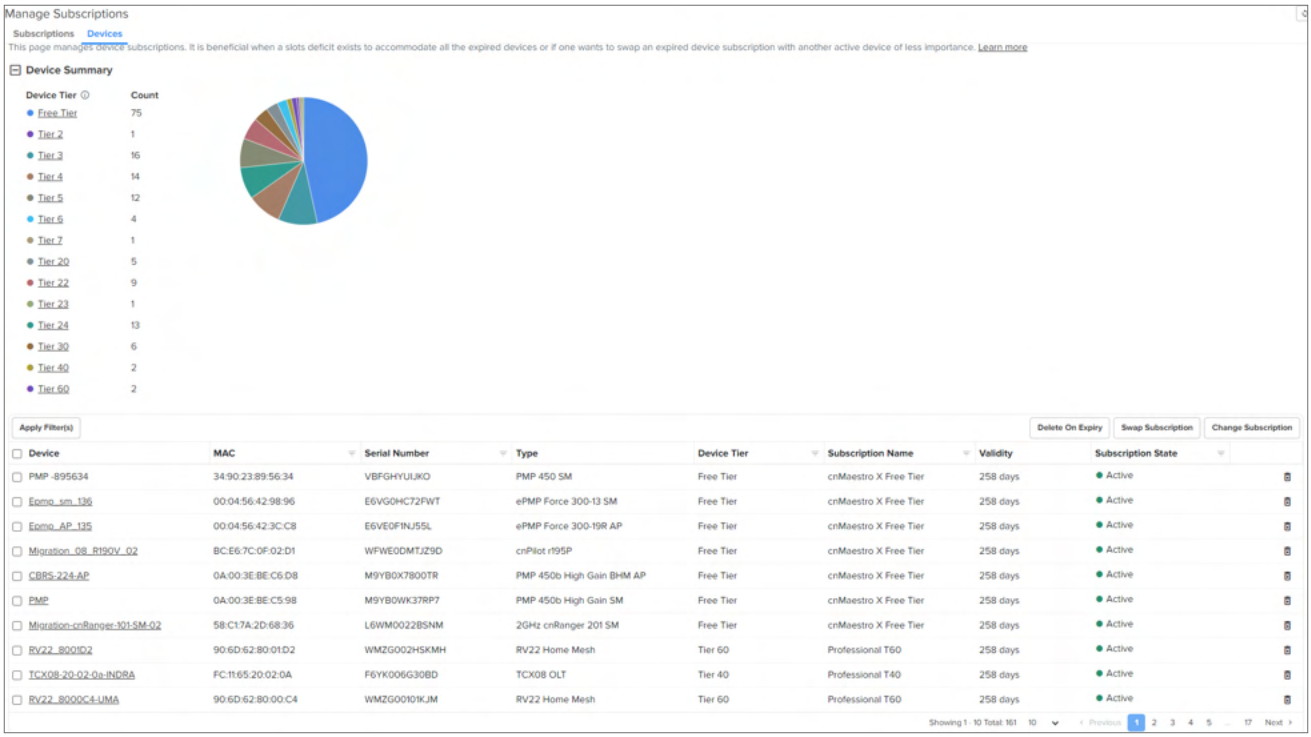
   Edit window pops up as shown below.



2. Enter **Name** and **Description**.
3. Click **Save**.

Devices

Devices page manages device subscriptions. It is beneficial when a slots deficit exists to accommodate all the expired devices or if one wants to swap an expired device subscription with another active device of less importance. For more info refer to Subscription Management.



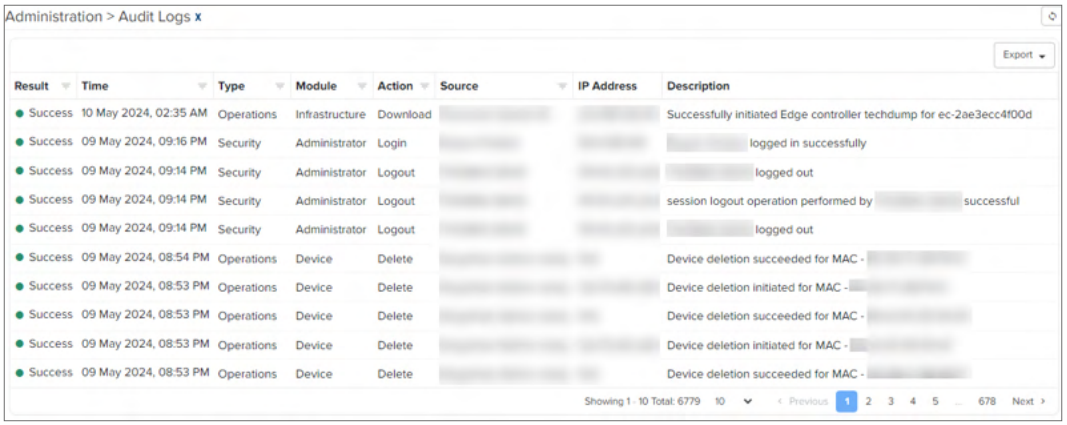
Audit Logs

Note:

Audit Logs are supported only for cnMaestro X subscribers.

Audit Logs record administration activities through both the Web UI and the RESTful API. Audit Log entries usually include destination and source addresses, a timestamp and user login information. User can access Audit Logs in the **Administration** > **Audit Logs** page.

Figure 562 *Audit Logs*



The following table describes the Audit Logs parameters and their descriptions.

Table 165 *Audit Log Parameters*

Parameter	Description
Action	Displays the action performed by the user (create, delete, download, etc).

Table 165 *Audit Log Parameters*

Parameter	Description
Description	Textual description of the task.
Export	Enable export as CSV or PDF.
IP Address	IP address of the Web browser or API application.
Module	Module generating entry (AAA, administrator, alarm).
Result	The result of the audit log as **Success** or **Failed**.
Source	Administrator or API client name.
Time	The time when the action was performed.
Type	Type of the log entry (configuration, operation, onboarding, security).

Log Action

An action log contains a set of transactions. Each transaction contains one or more Actions. Each Action has a name and input parameters. Some Actions have output parameters.

The following Actions will be supported for individual Audit Log entries. Each activity performed in the server is detailed in this table.

Table 166 *Log Action Parameters*

Parameter	Description
Claim	Claim a device in the network operator.
Cloud-Connect	Provides the status of the On-Premises to Cloud account connection.
Create	Create an object in the network device.
Delete	Delete an object in the network device.
Download	Download a file.
Edit	Edit an existing device detail.
Link Test	Perform a Link Test.
Login	Login to a device.
Logout	Logout from a device.
Mail	Mail ID of a device.
Move	Move a device from the server.
Reboot	Reboot a device.
Reset	To reset a device
Upload	Upload a file on the server.

Audit Modules

Auditing activity is mapped to individual modules within cnMaestro. A breakdown of the available modules is listed below.

Module	Type (s)	Description
ACL	provisioning	Adding Editing Removing the ACL Entries.
administrator	provisioning operations security	User Management: Login, Users, Roles, Email, etc.

Module	Type (s)	Description
alarm	provisioning	Alarms and Alarm History.
api	provisioning	API Management: API Clients and Webhooks.
auditing	provisioning	Auditing Infrastructure.
auto-provision	provisioning	Auto-Provisioning.
CBRS	Services	CBRS.
Cloud- Sync	Services	Synchronizing the Cloud to On-Premises Instances.
data-tunnel	provisioning	Data Tunneling.
device	provisioning operations	Device management.
Email-Notifications	operations	Add or edit Email notification.
guest-portal	provisioning	Guest Portal.
infrastructure	provisioning	Site, Network, Tower Management.
jobs	provisioning operations	Jobs Infrastructure.
license	licensing	Update license details.
MSP	operations	Operations covering Managed Services and Managed Account.
onboard	provisioning operations	Onboarding Queue.
report	provisioning operations	Data Reports.
Profile	provisioning	Create or update a profile.
SIM	provisioning	SIM claim and delete.
system	provisioning operations security	System Services: VM management, change log level, system upgrade, system monitoring, software images, system settings.
template	provisioning	Template-Based Configuration.
tools	provisioning operations	Technical support dump, networking operations, etc.
webhooks	provisioning	Webhooks configuration and management.
Wi-Fi	provisioning operations security	AP Groups, WLANs: edit W-Fi configuration objects.

Settings

Email Notifications

The Email Notifications feature allows the Super Administrator and the Administrator users to add subscribers (Email IDs) for receiving different types of alerts by means of Emails.

Note

- Only 2 email recipients can be added per cnMaestro Essentials account.
- Up to 10 email recipients can be added per MSP, Base Infra, and system level scope.

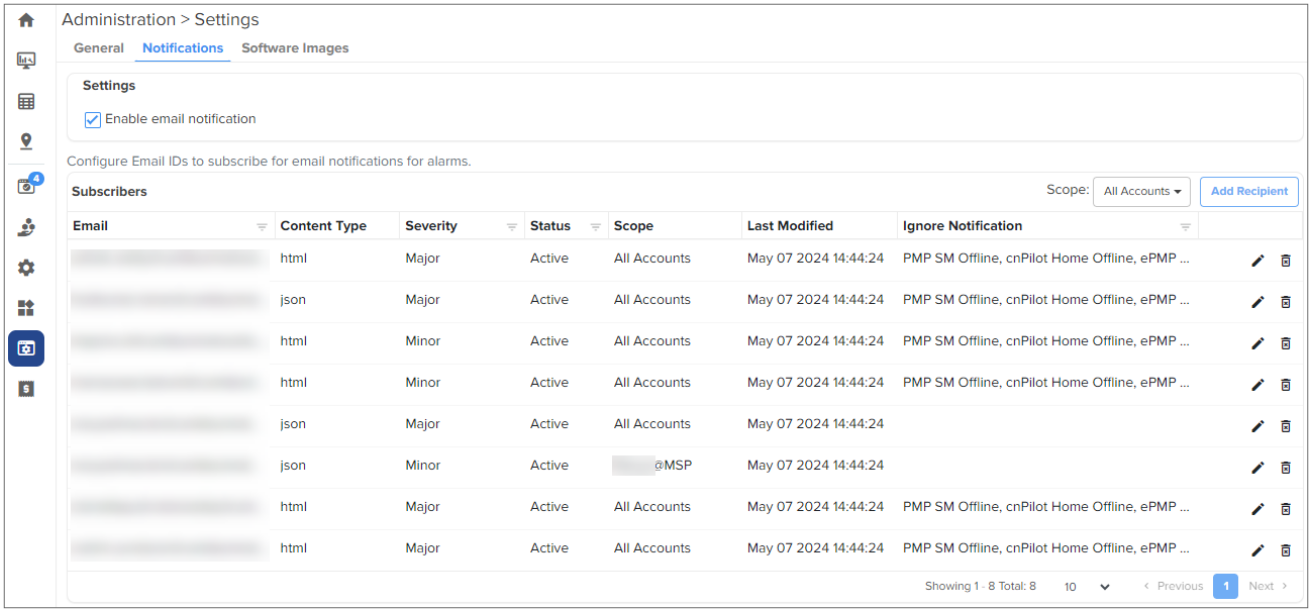
  For example, if there is one MSP, you can create 10 recipients at MSP, 10 at Base Infra, and 10 at system level (All accounts scope).

The severity of alerts are classified as follows:

- Critical
- Major
- Minor

The content of the email alert will be in JSON or HTML format. The subscriber will get email alert only when the global setting is enabled.

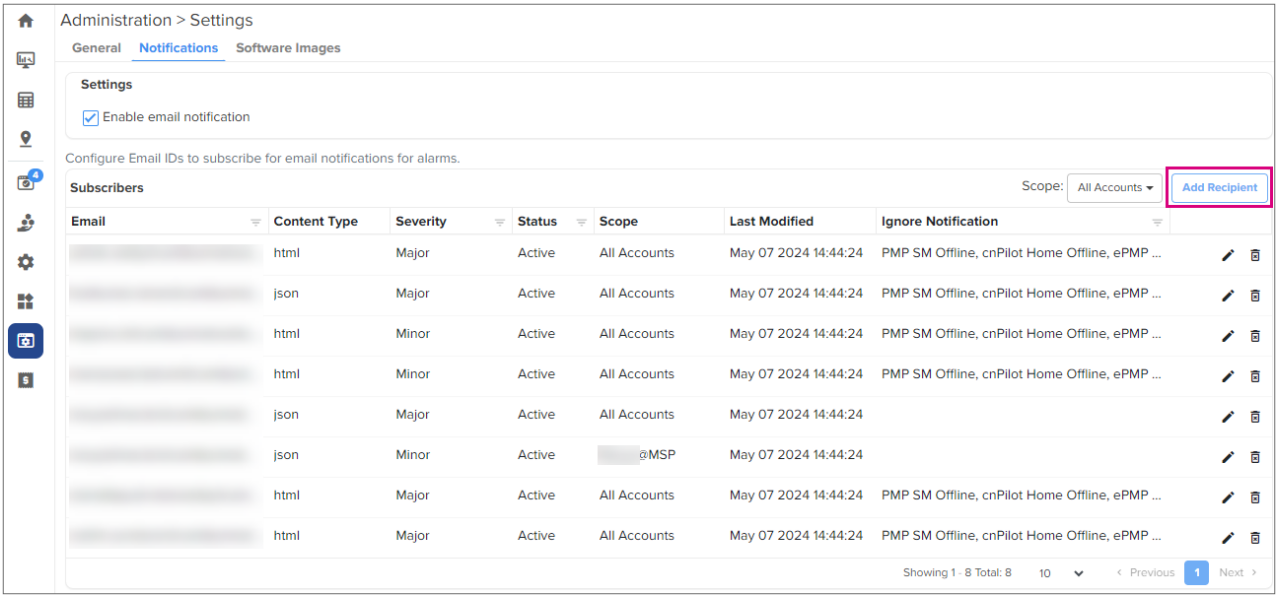
Figure 563 *Email notifications page*



Adding Recipient to Subscriber Table

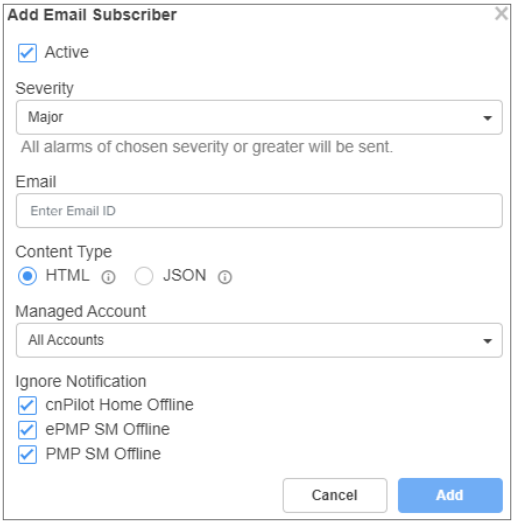
1. Navigate to **Administration > Settings > Notifications** page.

   Figure 564 *Adding Subscribers*



2. Click **Add Recipient**.

   The following window is displayed:

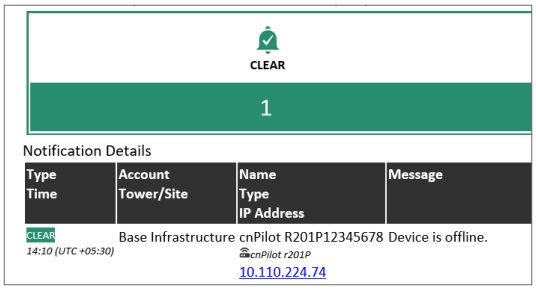


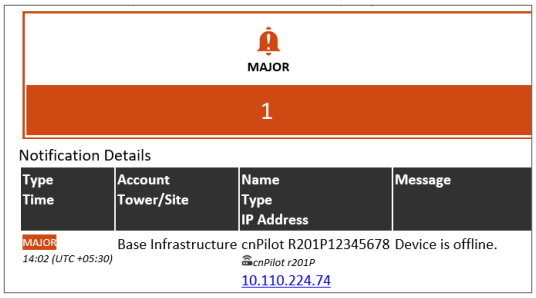
3. Enter the Email ID of the subscriber in the **Email** textbox.
4. Select the severity level from the **Severity** list.
5. Select the Managed Account type from the **Managed Account** list.
6. Choose **HTML** or **JSON** radio button for the **Content Type**.
7. Select the appropriate option (s) for **Ignore Notification.**
8. Click **Add** and the entry reflects in the subscriber table.

All alarms of chosen severity and above are sent through email as explained below:

- If severity **Critical** is selected, then we receive only critical alarms.
- If severity **Major** is selected, then we receive critical and major alarms.
- If severity **Minor** is selected, then we receive critical, major, and minor alarms.

HTML Email Example





JSON Email Example



Account Type

cnMaestro supports three separate account types, based upon the composition of devices installed. The type is set when the account is created initially, but it can be changed later through the **Administration > Settings** page.

For more information, refer Navigating the cnMaestro UI.

Managing Device software images under Automatically Update Device Software section

cnMaestro cloud allows one to update the device software during onboarding and for managed devices.

Adding update device software is a manual process as follows:

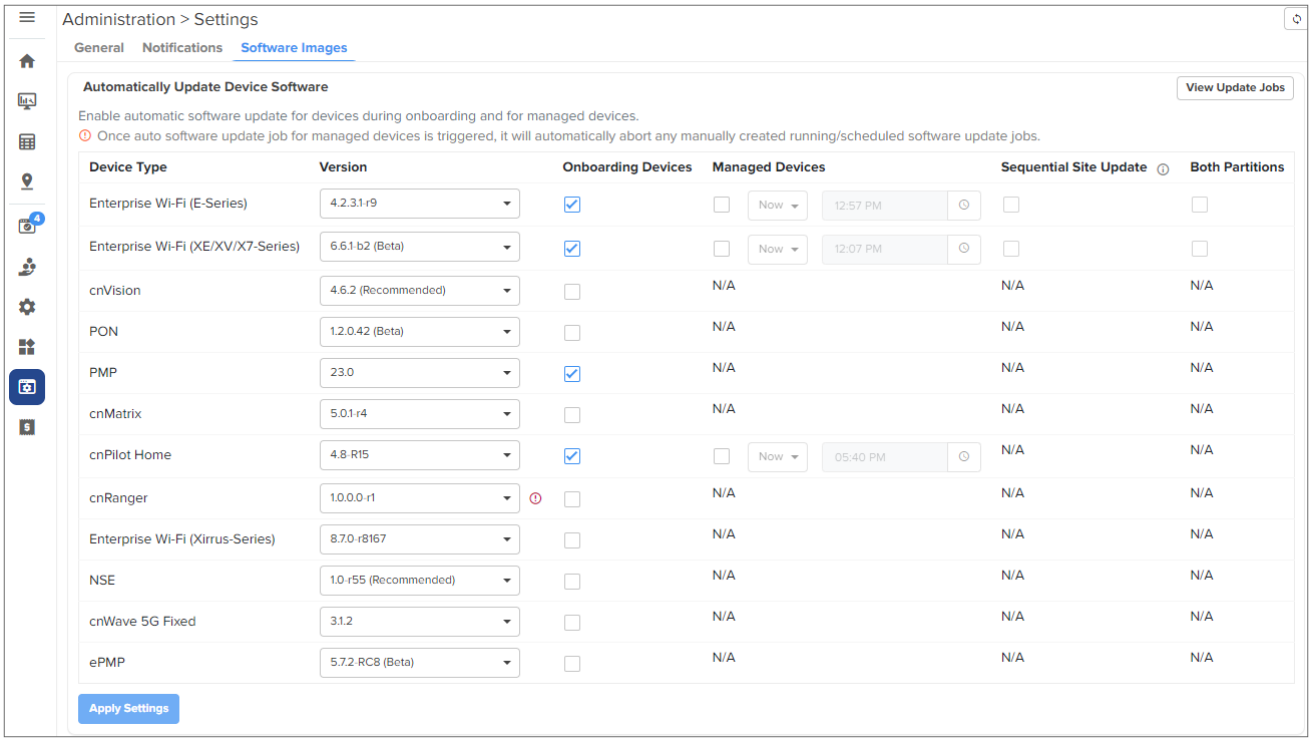
1. Navigate to **Administration > Settings > Software Images** > **Automatically Update Device Software** tab.
2. Select the version file and then click **onboarding/Managed Devices** checkbox.

> **Note**
>
> Enable the onboarding checkbox, in order to avoid the failure of onboarding devices with minimum supported version rather than the recommended version.

3. Enable the checkbox as follows:
   - Enable **Managed Devices** flag only for Wi-Fi devices (E-Series, R-Series and XE/XV/X7-Series).
   - Enable **Sequential Site Update** and **Both Partitions** flag only for only E-Series and XE/XV/X7-Series devices.
4. click **Apply Settings.**

> **Note**
>
> - Once auto software update job for managed devices is triggered, it will automatically abort any manually scheduled software update jobs.
> - In order to avoid failures in onboarding devices having minimum supported version other than recommended version, enable the onboarding check.

Figure 565 *Software Images*



Appendix

This section includes the following topics:

- Network Port Requirements
- XMS-Enterprise to cnMaestro X
- Converting Tier 2 Unused Slots

Network Port Requirements

Network Port Requirements for Outbound

The following table provides information about network port requirements for outbound:

Table 167 *Outbound Port Details*

Port Number	Port Type	Purpose
443	TCP	HTTPS Web Access and Device communication

XMS-Enterprise to cnMaestro X

This section describes the process of migration from XMS-Enterprise (XMS-E) to cnMaestro X.

Before you begin migration, upgrade the following to the latest version:

- XMS-E to version 8.4.0
- Xirrus APs to version 8.7.0

Perform the following steps for migration:

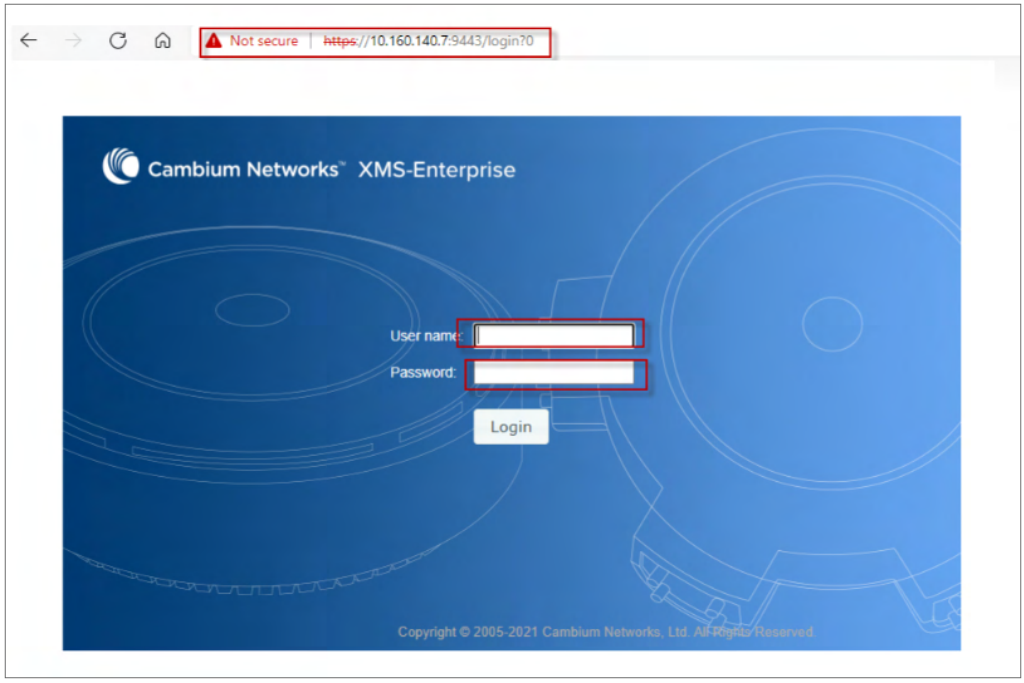
1. In XMS-E, perform the following actions:
   - Export Golden Configuration
   - Migrate to cnMaestro X
2. In cnMaestro X, perform the following actions:
   - Create Wi-Fi AP Group
   - Approve APs into Wi-Fi AP Group
   - Import and Apply AP configuration

XMS-E System

To login to XMS-E, complete the following steps:

1. Launch the Web login page.
2. Enter the username and password.

3. Click **Login**.

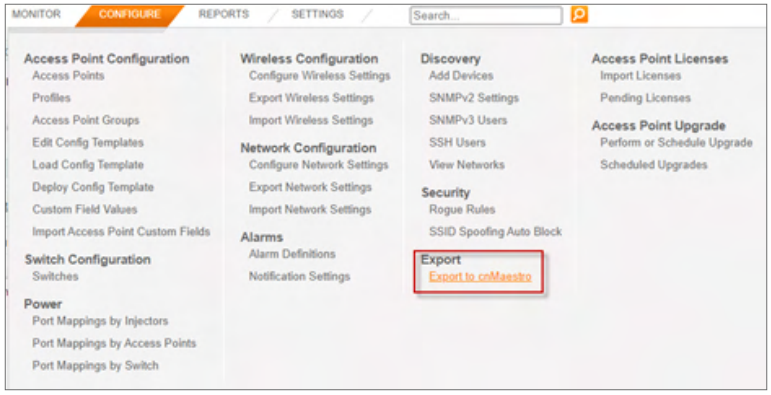


Export Golden Configuration

Export Golden Configuration for one of the APs. It is saved as a zipped file in the local file system.

To start export golden configuration in XMS-E, navigate to **Configure** tab > **Export**.

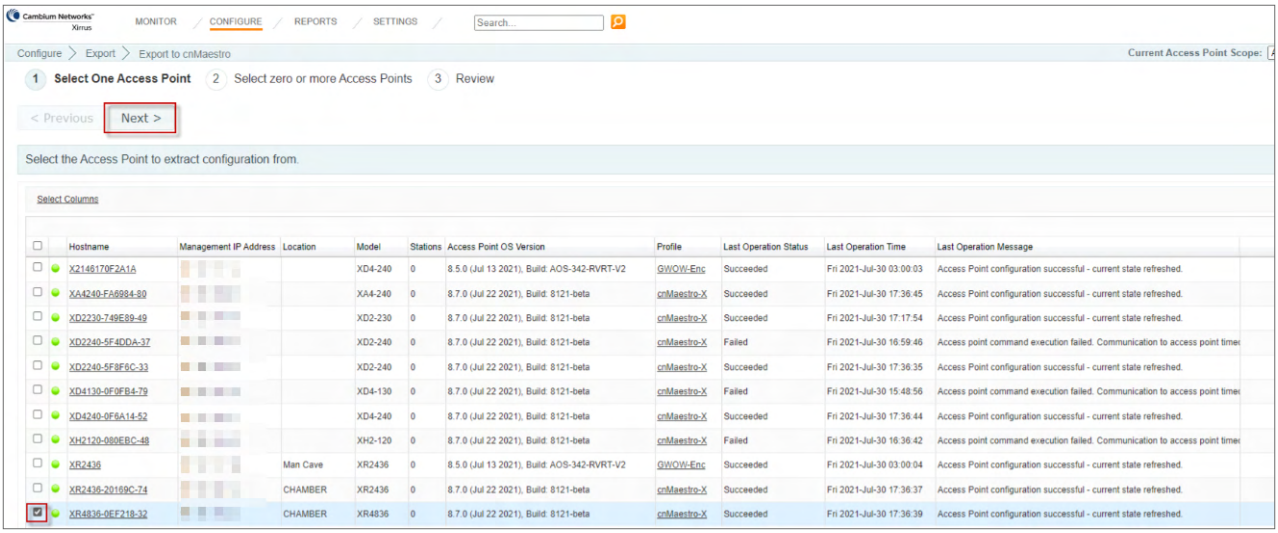
1. Select **Export to cnMaestro**.



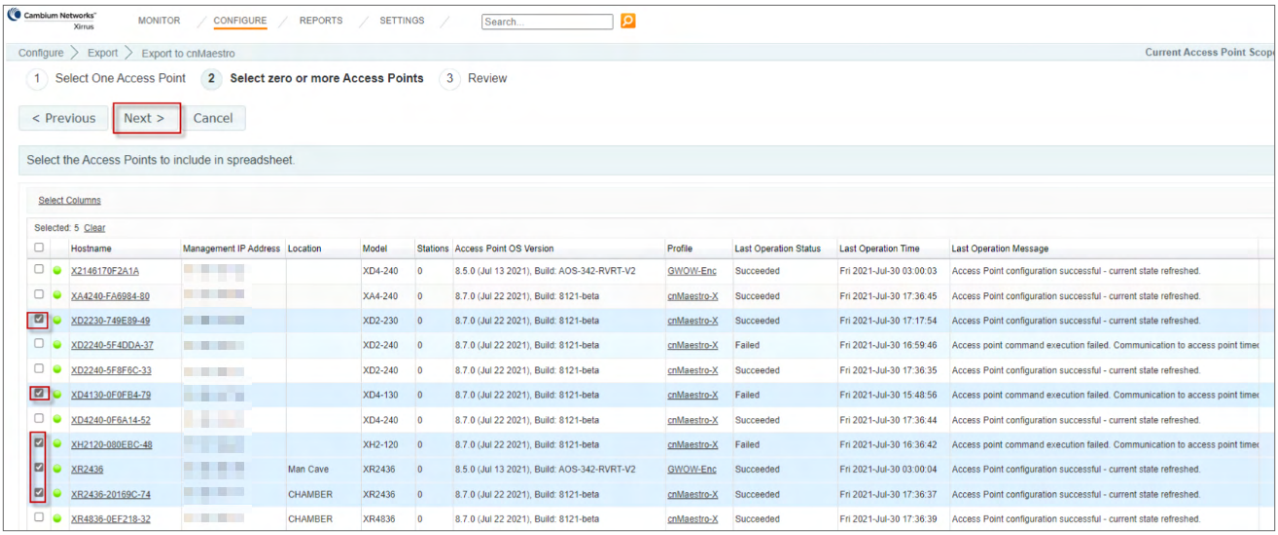
2. Select the AP to create the golden configuration for a group of APs and click **Next**.

Note

- Select the AP with the maximum radios and the highest capability.
- During the migration of an AP from XMS-E to cnMaestro, the AP configurations are not modified.



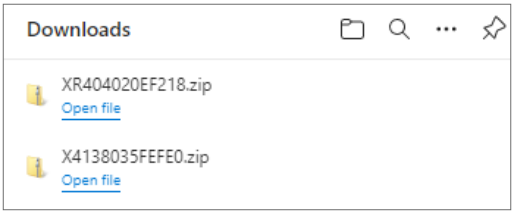
3. Select group of APs to be added to the spreadsheet and click **Next**.



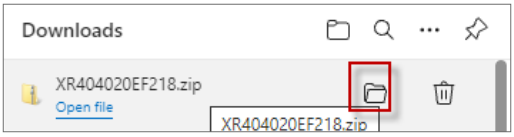
4. Click **Export**.

   In Local System unzip the directory and files to local directory.

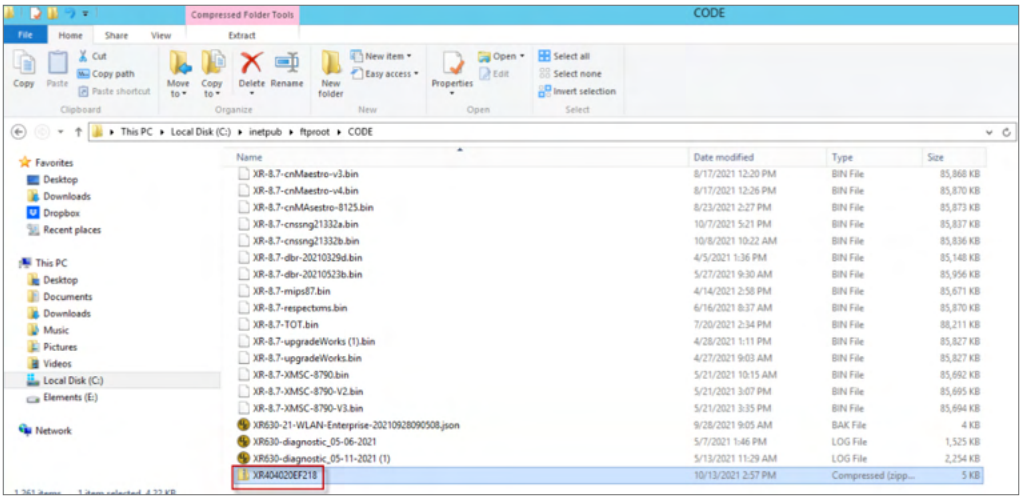
5. Download the zip files from the browser window.



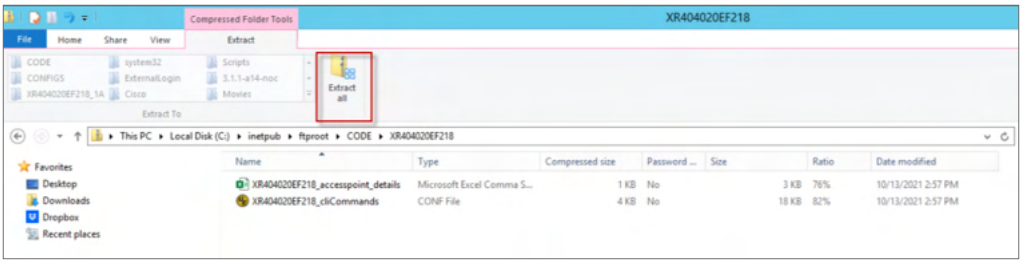
6. Go to the folder where the zipped files are saved and extract the contents to a folder.



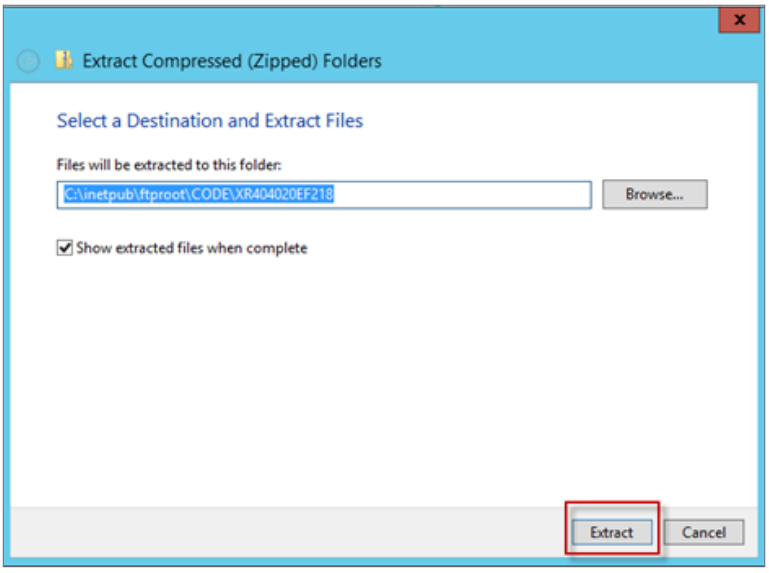
7. Open the directory path where the file has been stored and double-click on the zipped file.



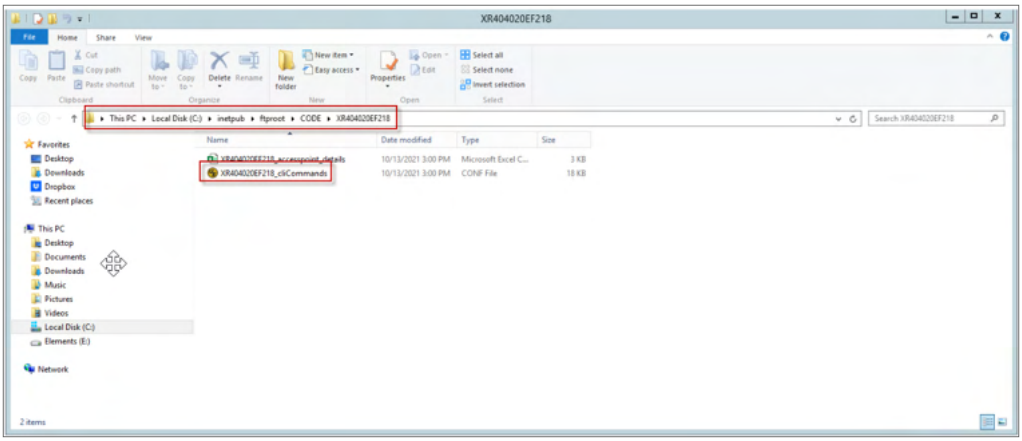
8. Click **Extract all**.



9. Extract the folder to the path.



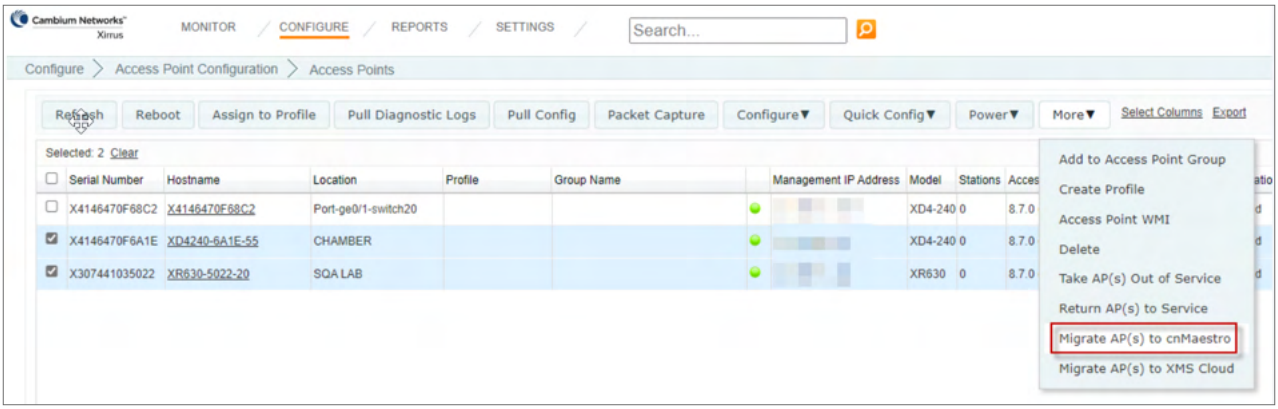
10. Make a note of the folder or file location as you will require this file later.



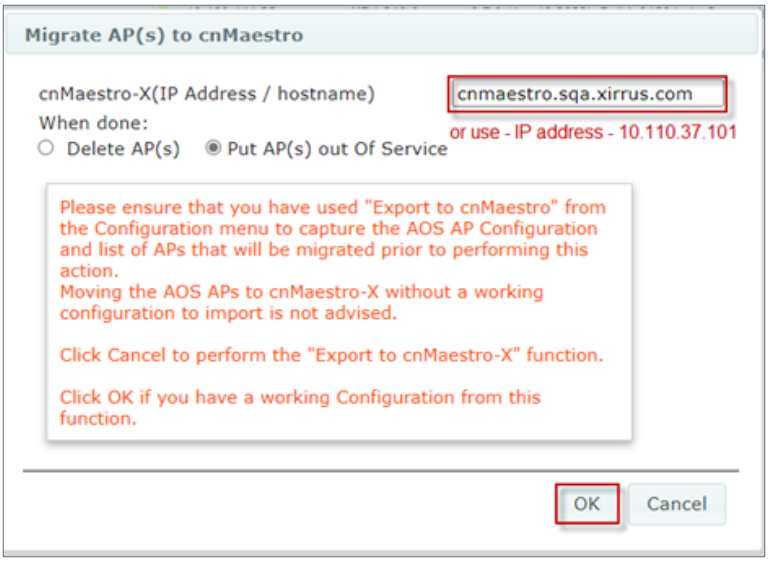
Migrate to cnMaestro X

Select APs to migrate to cnMaestro X. Perform the following steps:

1. Navigate to the **More** menu > select **Migrate APs to cnMaestro.**



2. Enter the IP address or Hostname mapped in DNS for cnMaestro X.
3. Select **Delete AP** or **Put AP(s) out of Service** and click **OK.**



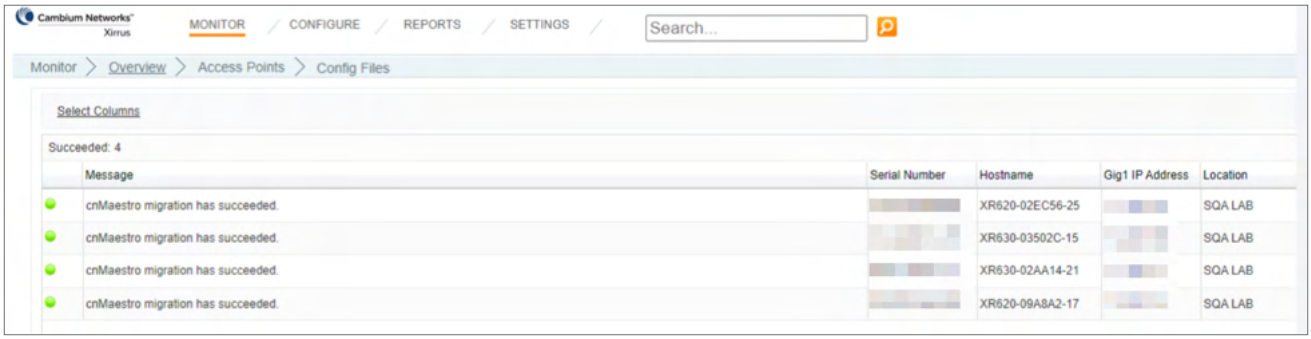
Note

- Out of service APs are not removed from XMS-E, so if there is an issue, select the **Return APs to**

Service option and they will return to XMS-E.

- You must reset using the `snmp trap host 1 Xirrus-XMS` AP CLI command on the AP for the return to service to work.
- If you select **Delete APs**, they will be removed and you must rediscover them on the network to return them to XMS-E.
- You should also remove the Device Network from the Device discovery section to clean up XMS-E.

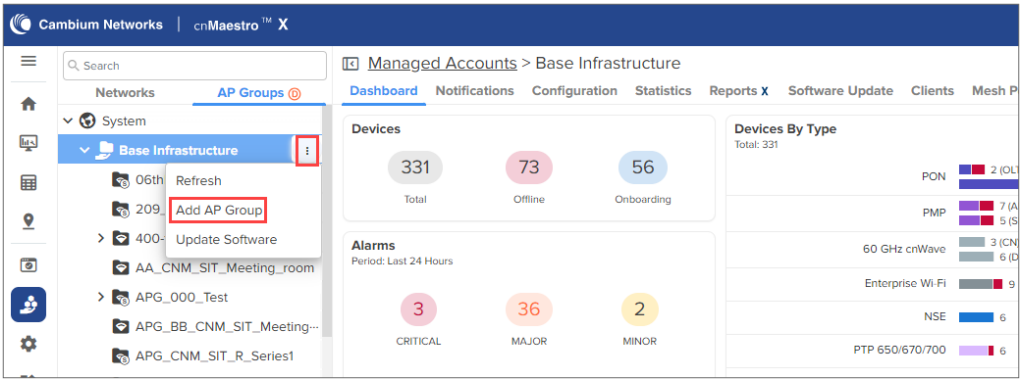
A success message from XMS-E for each of the APs migrated to cnMaestro X is displayed.



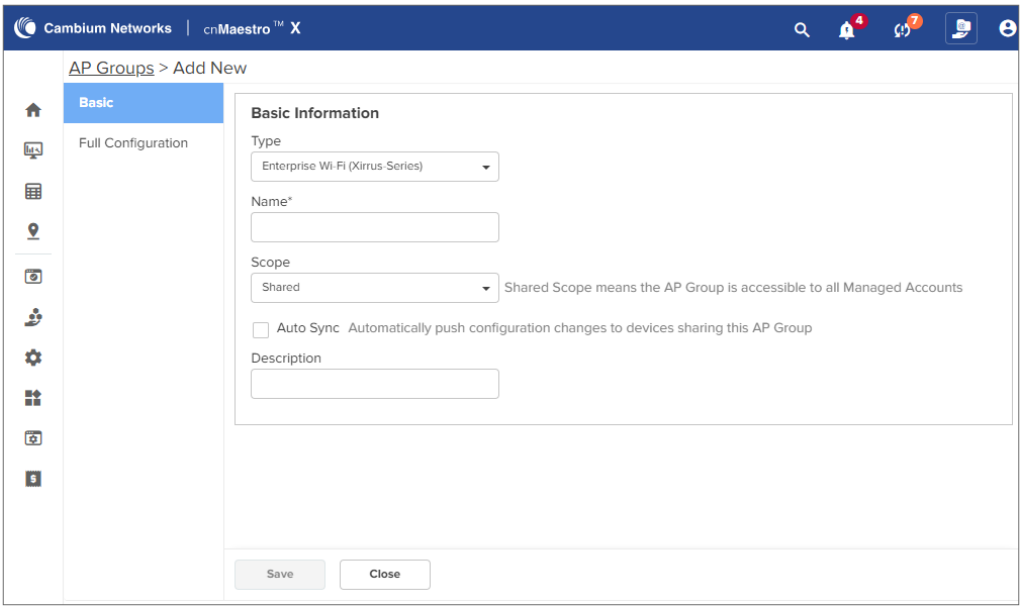
Create Wi-Fi AP Group

Create Wi-Fi AP Group and Import CLI command file from exported directory.

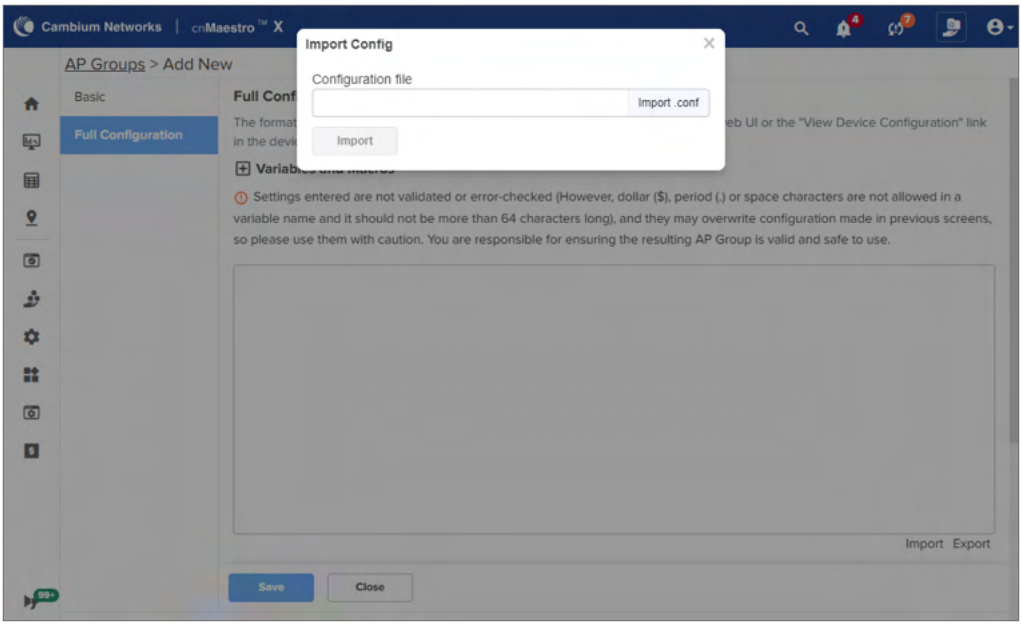
1. Navigate to **Wi-Fi AP Group** > **Base Infrastructure** > click action (⋮) icon to add **Add AP Group**.



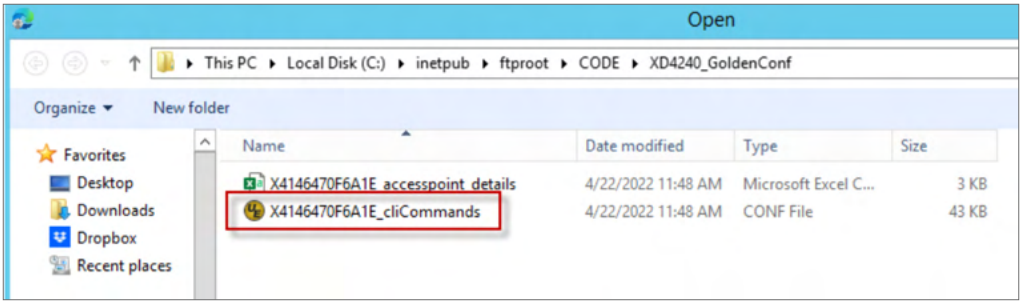
2. In the **Basic Information** page, select Type as **Enterprise Wi-Fi (Xirrus-Series)** from the drop-down.
3. Select the **Auto-Sync.**
4. Click **Save.**



5. In the **Full Configuration** page, click the **Import** option.



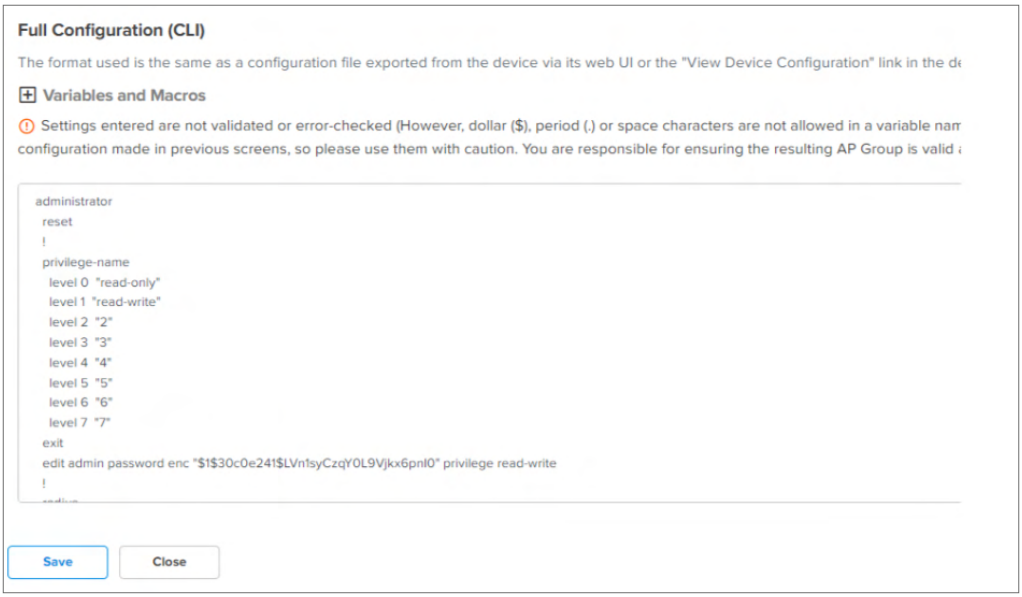
6. Select the CLI command file from the unzipped directory.



7. Click **Import**.



The configuration file is displayed.



8. Click **Save**.

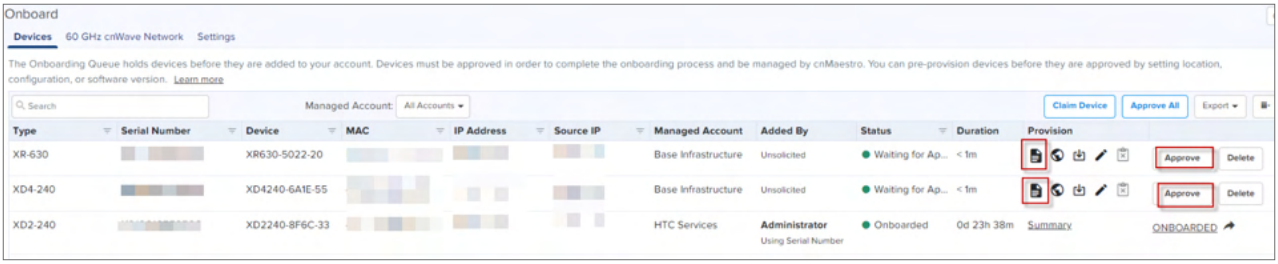
Approve APs into Wi-Fi AP Group

APs pending for approval in cnMaestro X based on the **Migrate APs to cnMaestro X** steps as described above.

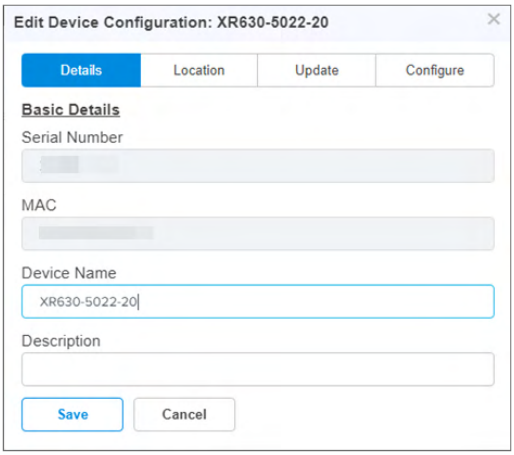
You can claim APs to approve from the **Onboard** > **Devices** page.

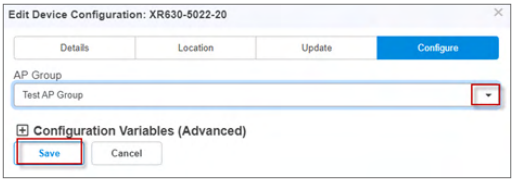
Perform the following steps to approve APs from the **Onboard** > **Devices** page.

1. Navigate to the **Onboard** > **Devices** page and click **Approve All** (to approve all devices at once) or **Approve** (to approve devices individually.)



2. Enter the required details, provision the device for location, and assign to an AP Group.

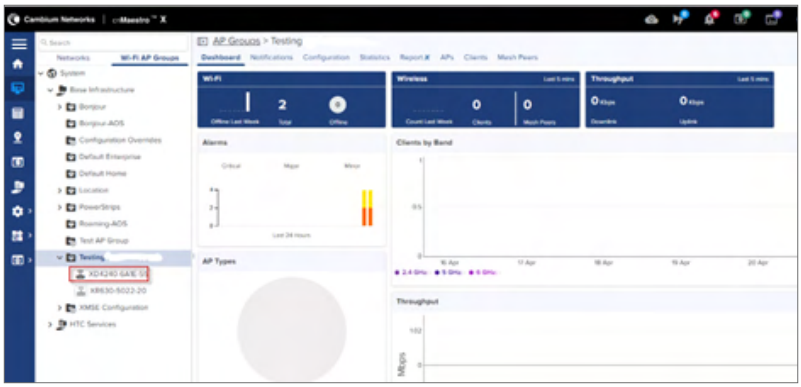




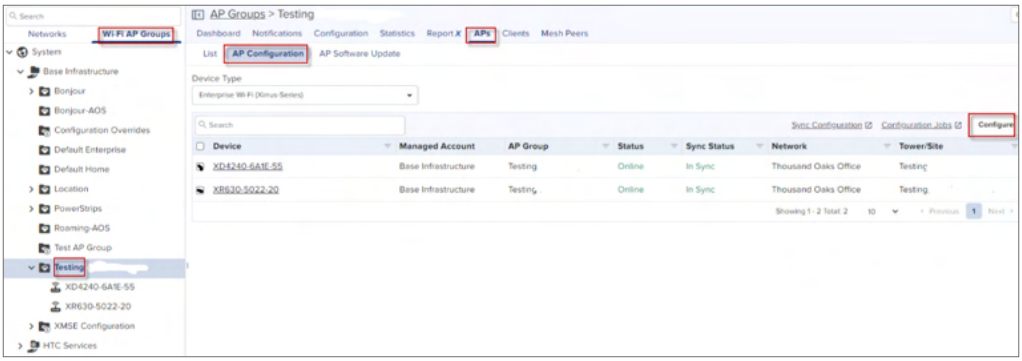
3. Click **Save.**
4. In the **Onboard** > **Devices** page, select **Approval All** (to approve all devices at once) or **Approve** (to approve devices individually.)

Import and Apply AP configuration

APs imported are ready for basic configuration. Import AP configuration using the CSV file from the exported directory.

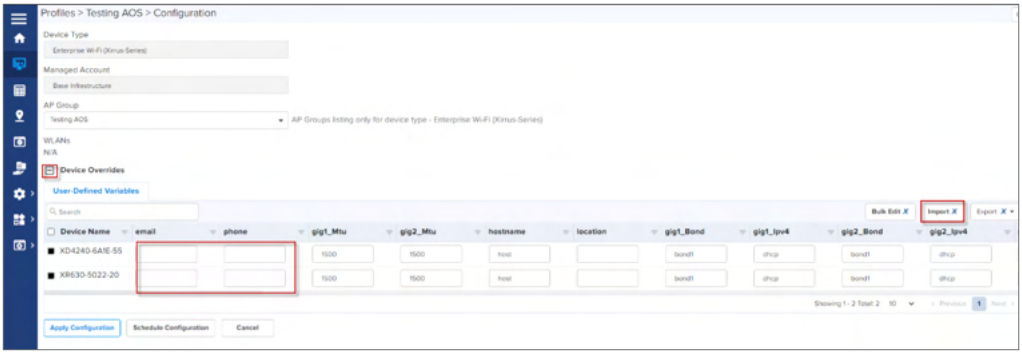


1. Navigate to **Wi-Fi AP Group** > select **AP Group** > **AP Configuration**.
2. Select all APs to configure, click **Configure.**



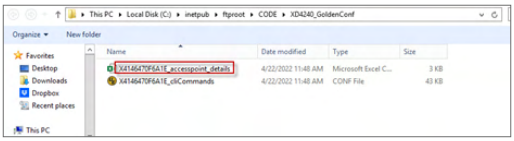
3. In Device Override table, verify AP details and click **Import.**

> **Note**
>
> Email and Phone fields are auto populated from the .csv file.

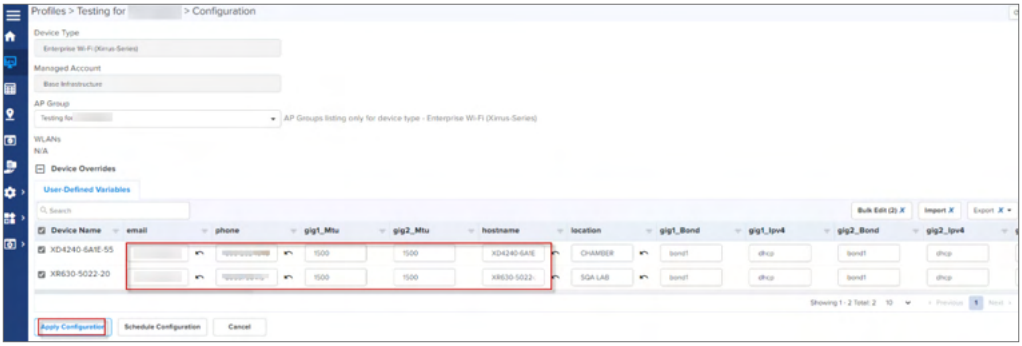


4. Select the .csv import file from the unzipped directory folder and click **Apply**.

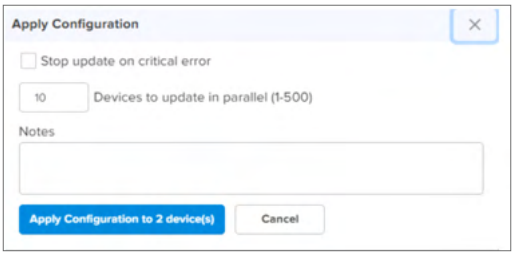




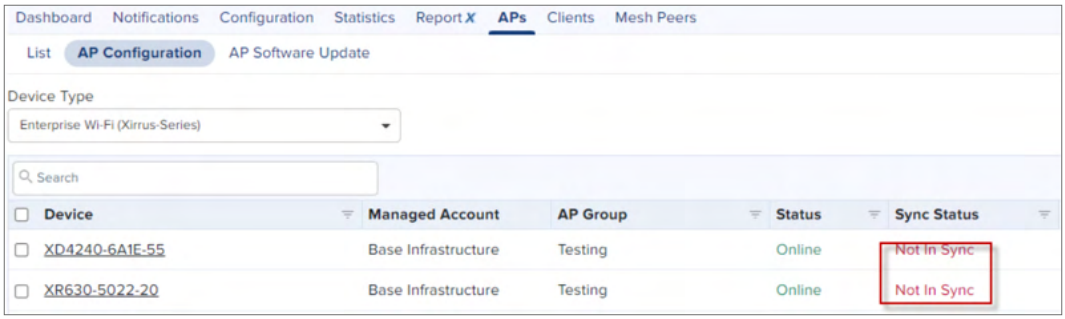
All the configuration values from the CSV file are populated for each AP. The data is auto populated to the **User Defined Variables** tab. The APs receive complete configurations including all IAP settings.



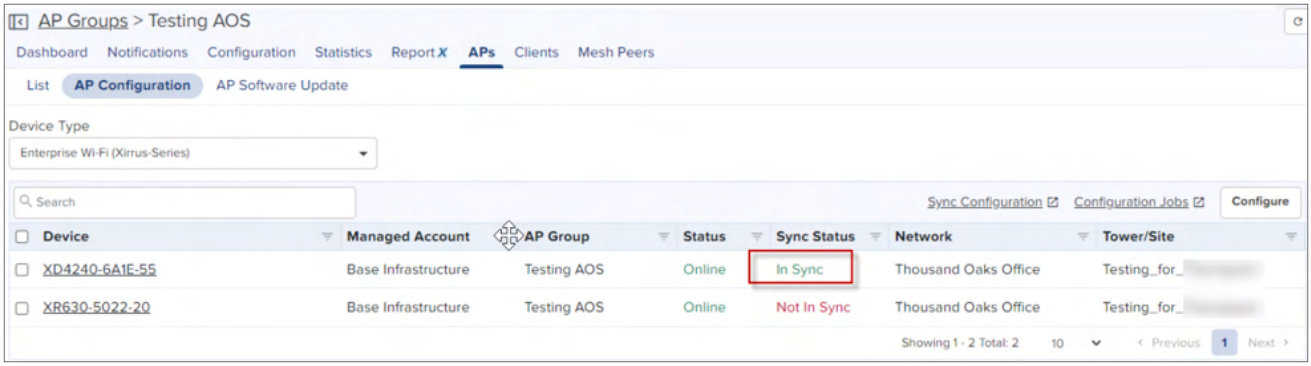
5. Click **Apply Configuration.**



When the APs are completely configured, **Sync Status** is displayed as **In Sync**.



You have to refresh the page to view the updated **Sync Status.**



Converting Tier 2 Unused Slots

Cambium Networks has introduced new product family-based cnMaestro X SKUs and pricing for devices such as Fixed Wireless Broadband APs, cnRanger, cnReach, cnVision, PMP, ePMP, and PTP. Earlier, the Tier 2 subscription was used to control these devices (pricing). To simplify the purchase and onboarding for these devices, Cambium Networks has decided to remove the Tier 2 subscription and introduce new four tiers (Tier 21, Tier 22, Tier 23, and Tier 24).

The Tier 2 subscription is no longer valid now. Due to Tier 2 subscription removal, there can be unused Tier 2 slots in your account (purchased during the Tier 2 subscription). As a solution, Cambium Networks provides an option to convert these unused Tier 2 slots into new tiers based on the device family and requirements. You can manually convert the unused Tier 2 slots to Tier 21, Tier 22, Tier 23, and Tier 24 using the ⓘ icon located on the **Manage Subscriptions** page (cnMaestro UI). This solution helps in better mapping and device management.

Note

The Convert Tier 2 option is effective from March 1, 2024 for Fixed Wireless Broadband APs, cnRanger, cnReach, cnVision, and PTP devices. You must convert the unused Tier 2 slots in your account to the new Tier 2x slots before onboarding the devices.

When you convert the unused Tier 2 slots into new tiers, you cannot change the new tiers back to Tier 2.

You can convert the unused Tier 2 slots to new tiers, for example, as described in Table 168.

Table 168 *Example of converting unused Tier 2 slots*

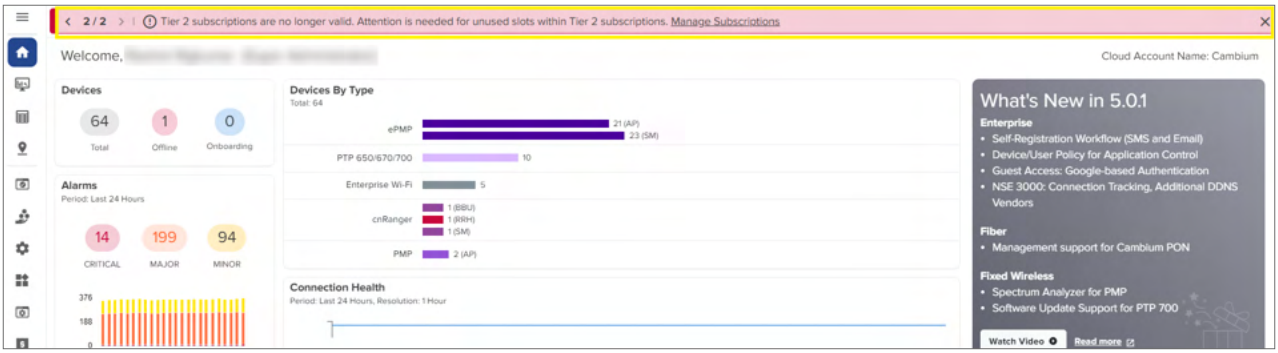
New Tier	Device Family and Type	
Tier 21	cnVision	FLEXr, HUB360
	ePMP	All AP Models
Tier 22	PMP	All AP Models except 450m and 450mv
Tier 23	PMP	450m
Tier 24	cnRanger	All BBU Models
	cnReach	All cnReach Models
	PTP	All PTP Models

To manually convert the unused Tier 2 slots for a device family, complete the following steps:

1. Log in to your respective cnMaestro UI account.

   The **Home** page appears with a banner, as shown in Figure 566.

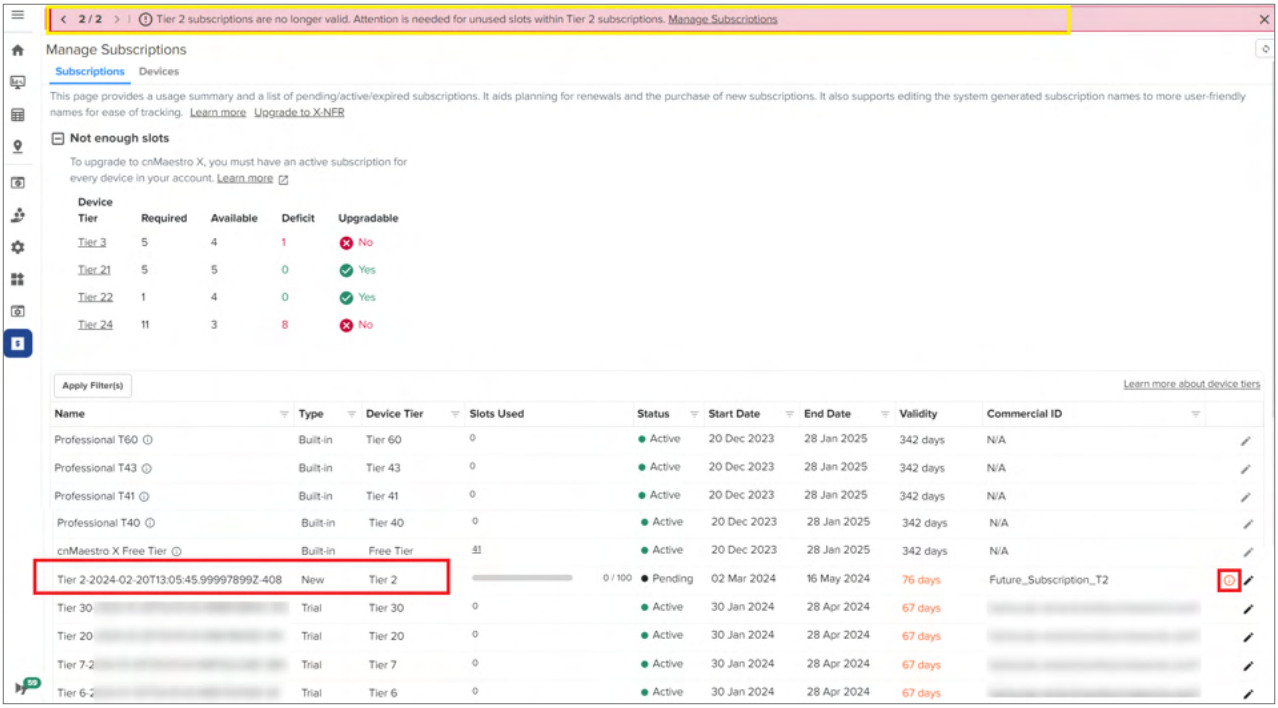
   Figure 566 *The Tier 2 conversion-specific banner*



2. From the home page, navigate to the **Manage Subscriptions** page.

   The **Manage Subscriptions** page appears (as shown in Figure 567), displaying the same banner and details of tiers.

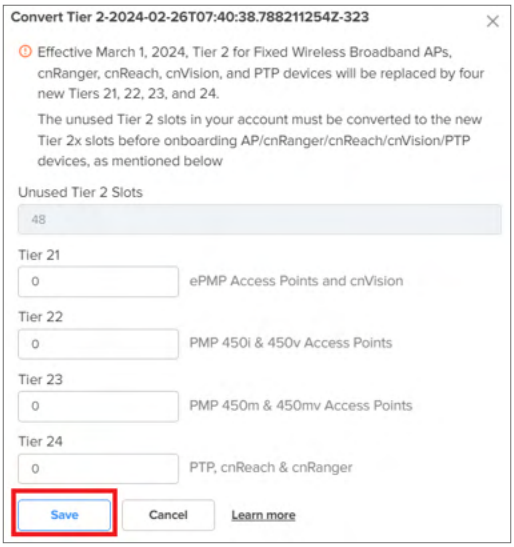
Figure 567 *The Manage Subscriptions page with tier information*



3. Select the Tier 2 subscription and click the corresponding ⓘ icon (as shown in Figure 567).

   The Tier 2 subscription window appears with details of unused slots and options to convert to new tiers (Tier 21, Tier 22, Tier 23, and Tier 24).

Figure 568 *The Convert Tier 2 window*



4. Check the unused slot count and enter a valid value (in integers) in Tier 21, Tier 22, Tier 23, or Tier 24 text boxes (based on your requirements).
5. Click the **Save** button (as shown in Figure 568) to apply the changes.

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places, and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Support website	https://support.cambiumnetworks.com
Support inquiries	
Technical training	https://learning.cambiumnetworks.com/learn
Main website	http://www.cambiumnetworks.com
Sales inquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list	http://www.cambiumnetworks.com/contact-us/
User Guides	http://www.cambiumnetworks.com/guides
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom

Cambium Networks™ www.cambiumnetworks.com

Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

Copyright © 2024 Cambium Networks, Ltd. All rights reserved.





Cambium Networks™









USER GUIDE

cnMaestro On-Premises



Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”).

This product is not restricted in the EU. Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

© 2021 Cambium Networks Limited. All Rights Reserved

Contents

Contents 3
Introduction 14
Supported Devices and Features 14
cnMaestro shared features 14
Differences with cnMaestro Cloud 18
Supported browsers 20
Supported Virtualization Infrastructures 20
Device software 22
Quick Start 26
Installation 26
Virtualization 26
Desktop virtualization 26
Bare metal hypervisor 26
cnMaestro deployment 26
Onboard devices 37
DHCP Options (Linux) 43
UI Navigation 47
Account View 47
Access and Backhaul View 48
Enterprise View 48
Industrial Internet View 48
Home page 48
Page structure 49
Page navigation 51
Access and Backhaul View 51
Overview 51
Enterprise View 57
Overview 57
System 57
Devices 57
AP groups and WLANs 58
Sites 58
Side menu 59
Section tabs 59

System status 60
Logout 60
Architecture 62
Overview 62
Networking 62
Device Onboarding 64
Overview 64
60 GHz E2E Controller Onboarding 64
Pre-Configuration and Approval of Devices (Optional) 64
Device Authentication 65
Claiming the Wi-Fi Devices from AP Group 65
Claiming the Wi-Fi Devices from Site Dashboard 66
60 GHz E2E Controller Onboarding 68
Overview 68
High Availability (HA) 72
Overview 72
Primary vs Secondary 72
Shared (Floating) IP Address 72
Network Ports 72
Recommendations 73
Dual Interfaces 73
Add eth1 Network Adapter 73
HA Cluster Setup 75
Bootstrap (Primary) 75
Accept (Primary) 75
Join (Secondary) 75
Basic HA Cluster Creation Flow 76
Secondary Server 77
HA Menu 78
High Availability Cluster Menu (Pre-Bootstrap) 78
High Availability Menu (Post-Bootstrap) 79
New Cluster 79
Accept Join Requests 80
Join Existing Cluster 80
Validate SSH Fingerprints 80
HA Cluster Status 81

Delete Node 83
Leave Cluster 83
Information 83
Behaviour of cnMaestro features when HA is Enabled 84
Monitoring 86
Network Monitoring 86
Dashboard 86
KPI (Key Performance Indicators) 86
Device Health 86
Connection Health 87
Charts and Graphs 87
Notifications 88
Overview 88
Events 88
Alarms 90
Statistics and Details 91
Performance 99
Maps 111
Geolocation Map Settings 112
Map Navigation 113
Mode 113
Tools 115
60 GHz cnWave Tools 116
cnMatrix Tools 116
cnPilot Home Tools 121
cnRanger Tools 122
cnReach Tools 123
cnVision Tools 124
Enterprise Wi-Fi Tools 126
ePMP Tools 133
Machfu 137
PMP Tools 137
Tower-to-Edge view 139
WIDS 140
Detecting Rogue APs 140
cnPilot Dashboards 144

Device Dashboard 144
Overview 144
Clients 144
Dashboard 147
Network Info 150
Mesh Peers 152
Neighbors 153
Site Dashboard 153
Wi-Fi Devices Availability (Total and Offline) 154
Wireless 154
Throughput 154
RF Quality 154
AP Types 155
Top Wi-Fi APs 155
Channel Distribution by Band 155
Radio/WLAN Distribution by Band 156
Clients by SNR 156
Clients by Performance 156
Clients Graph 157
Throughput Graph 157
Statistics 157
Wireless Clients 158
Floor Plan 158
Inventory 160
Inventory Export 160
Bulk Delete 160
Bulk Reboot 161
Schedule Reboot 162
CSV Configuration Import 162
Sample Configuration File 163
Sample Configuration File (60 GHz cnWave) 163
Uploading a Configuration File 164
Reports 167
Generating Reports 167
Device Report 167
Performance Report 173

Active Alarms Report 179
Alarms History Report 179
Events Report 179
Clients Report 180
Mesh Peers Report 181
Guest Access Login Events 181
Remote Upload 182
Report Jobs 183
Provisioning 184
Software Update 184
Software Update Overview 184
Create Software Update Job 185
Software Update while Onboarding 187
Software Update through Managed Devices 188
Viewing Running Jobs in Header 192
cnReach Bulk Software Upgrade 192
Fixed Wireless Configuration 194
Overview 194
Configuration Templates 194
Configuration Variables 195
Macros 195
Variable Caching 196
Device Type-Specific Configurations 196
Variable Validation 196
Sample Templates 196
Template File Creation 196
Template 196
Configuration Update 198
Device Selection 198
Device Type 198
Device Table 198
Configuration Update Steps 200
Configuration Backup 200
Jobs 203
Configuration Update 204
Wireless LAN Configuration 205

cnPilot Home and Enterprise Wi-Fi 205
Configure cnPilot using cnMaestro 205
Create an AP Group 211
Pre-Defined Overrides 216
User-Defined Overrides 216
User-Defined Variables 216
Bulk Overrides 217
Synchronize (Sync) Configuration 223
Configuration Job Status 224
Factory Reset 224
Association ACL 225
Overview 226
Configuring Association ACL 226
cnMatrix Switches 227
Switch Groups Configuration 227
Synchronize (Sync) Configuration 233
Policy Based Automation(PBA) 235
Switches 237
Switch Ports 242
Device Details 249
60 GHz cnWave Network Configuration 253
Managing E2E Network 253
Site Configuration 291
Node Configuration 295
PoP Node 303
DN/CN Node 323
Auto-Provisioning 334
Creating Auto-Provisioning Rule 334
Services 336
Managed Service Provider (MSP) 336
Overview 336
Managed Accounts 336
Managed Service 337
Managed Service Provider (MSP) 338
Managed Service Users (Administrators) 339
Configuring Managed Services 341

Enable Managed Service Provider (MSP) 341
Create Managed Services 342
Create Managed Account 344
Validate Managed Account Administrators 345
Managed Services Administration 348
Overview 348
System Dashboard 349
Managed Account Administration 350
Device Management 351
Disabling Managed Service Provider Feature 353
API Client 354
Overview 354
API Clients 354
RESTful API Specification 355
Authentication 355
Swagger API 356
Introduction 356
Sample Swagger UI Screenshot 357
Client ID and Client Secret Generation 357
cnMaestro User Interface 357
API Session 358
Introduction 358
Retrieve Access Token 358
Access Resources 360
API Details 360
HTTP Protocol 360
REST Protocol 361
Parameters 363
Access API 368
Token (basic request) 368
Token (alternate request) 369
Validate Token 370
Selected APIs 371
Overview 371
cnMaestro v2 API 371
Devices API Response (v2 Format) 372

Statistics API Response (v2 format) 374
Performance API Response (v2 format) 386
External Guest Access Login API 394
60 GHz cnWave RESTful API 396
cnPilot Guest Access 399
Configuration 399
Create the Guest Access Portal in cnMaestro 399
Mapping the Device to Guest Access Portal in cnMaestro 409
Access Types 411
Guest Access using Social Login 411
SMS Authentication 422
Generic SMS Gateway Configuration 422
cnPilot GRE Tunnels 429
Overview 429
Typical Deployment Model (Two Port Solution) 429
Multicast/Broadcast Handling with Multiple APs on Tunnel Concentrator 430
Inter AP Wireless Client Communication (through Concentrator) 430
Access Control List (ACL) Configuration 430
MAC Layer ACL 431
IP Layer ACL 431
Transport Layer ACL 432
SNMP 433
Overview 433
Enable SNMP 433
Configure SNMP Parameters 433
cnMaestro MIB (Management Information Base) 434
RADIUS Proxy 435
Overview 435
Minimum cnMaestro On-Premises Version Requirements 435
RADIUS Proxy Configuration 435
Citizen Broadband Radio Service (CBRS) 437
Enabling CBRS in Cloud 437
Enabling CBRS in On-Premises 442
Share CBRS Configuration to the On-Premises Instance 443
CBRS HTTP Proxy Configuration Options 444
Management Tool 446

Using a HTTP Proxy Server for CBRS Connectivity 468
Proxy Suggestions for CBRS Connectivity 468
External Proxy Requirements 468
Squid as External Proxy 468
HA for Squid external proxy 469
LTE 470
Adding SIM Cards 470
cnArcher Installation Summary 472
Configuration 474
Photos and Location 474
Link Test Result 474
AP Scan Result 475
Administration 476
User Management 476
Authentication 476
Local Users 476
Creating Users and Configuring User Roles 481
Changing Password 482
Authentication Servers 483
Session Management 492
Server Management 493
Monitoring 493
Settings 493
Operations 499
Update cnMaestro Software 500
System Backup 500
In-System Upgrade 502
Diagnostics 504
SSL Certificate 505
Certificate Management 506
Manage Software Images 509
Webhooks 514
Integrations 514
Limits 515
cnMaestro Webhooks Configuration 515
Types of Variables 518

Error and Retransmission 519
Viewing Configured Webhooks 519
Status Check 520
Custom Template Examples 520
Audit Logs 535
Syslog 538
Cloud Connectivity 542
Overview 542
Connecting cnMaestro On-Premises to Anchor Account 543
Software Images 544
cnMaestro System Update 545
Appendix 547
Maintenance 547
Command Line Alternatives 547
Export cnMaestro Data 547
Import cnMaestro Data 547
Technical Support Dump 548
Apply OVA Upgrade 548
Apply Package Update 548
SSH Access 548
Enabling SSH Access 548
Data Backup 551
Overview 551
cnMaestro backups 551
Full Backups 551
Virtualization System specific Backup Methods 552
Extending the Data Disk 553
VMware Workstation Disk Expansion 553
VirtualBox Disk Expansion 554
Partition and File System Updates 554
Account Recovery 554
Virtual Machine (Console) Account Recovery 554
cnMaestro Application Account Recovery 556
Application Account Recovery 556
Configure Network Time Protocol (NTP) 558
Disabling NTP Support 558

Statistics API Response (v1 Format) 559
Performance API Response (v1 Format) 570
Deployments 579
VMware ESXi Installation 579
cnMaestro VM Deployment 579
Oracle VirtualBox 5 Installation 582
VMWare Workstation 583
KVM Installation 585
Deployment 585
Windows DHCP 589
Configuring Option 60 589
Windows DHCP Server Configuration 589
Configuring Option 43 590
Windows DHCP Server Configuration 590
Configuring Option 15 590
Windows DHCP Server Configuration 591
Configuring Vendor Class Identifiers 591
Configuring the Policies at the SCOPE Level 592
Citrix Hypervisor Installation 596
Overview 596
Import using Citrix Hypervisor 596
Access cnMaestro 600
SSH Access 600
HTTPS Access 601
Advanced Options 601
Expand the Data Disk 601
Expand the volume through Citrix Hypervisor 601
Expand the file system within cnMaestro 602
Network Requirements 603
Inbound Ports 603
Outbound Ports 603
Custom Network Scripts 604
Contact Cambium Networks 605

Introduction

cnMaestro On-Premises is a standalone network management platform that can be installed in a data center. It is distributed as a virtual machine. The on-premises functionality is nearly identical to the cloud version.

This section covers the following topics:

- Supported Devices and Features
- Quick Start
- UI Navigation
- Architecture
- Device Onboarding
- High Availability

Supported Devices and Features

cnMaestro shared features

Table 1 lists the features shared between the on-premises and cloud deployments.

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
✔	✔	60 GHz cnWave	Manage 60 GHz cnWave Networks.
✔	✔	Advanced Troubleshooting	Display tower-to-edge status in a single graphic, which is used to: • Troubleshoot client connectivity directly on the AP. • View Wi-Fi client details and health.
✔	✔	AP Group Configuration	Configure Enterprise Wi-Fi and cnPilot Home devices.
✔	✔	AP Group Dashboard	Display aggregate Wi-Fi AP statistics for the configured AP Group.
	✔	Audit Logs	Record administrator activities.
	✔	Auto Manage Routes	Support automated IPv6 routes for cnWave Distribution Node (DN) and Client Node (CN) based on topology and status of Point of Presence (PoP) Node.
✔	✔	Automatic Device Software Updates	Automatically update device software during onboarding or reconnection.

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
✔	✔	Bulk Image Upgrade	Schedule software image upgrades across sectors or device groups.
✔	✔	Citizen Broadband Radio Service Subscription (CBRS)	Support CBRS-compliant devices in the 3.6 GHz band (from 3550 MHz to 3700 MHz).
	✔	Client Dashboard	Allows methods to control, or block applications or terminate based on consumption of applications.
✔	✔	Cloud Connectivity	Automatically download device software from the cloud.
	✔	cnArcher Installation Summary	It displays installation summary of PMP SMs.
	✔	Data Reports	Export device, performance, alarm, and event statistics data in CSV formats.
✔	✔	Device Inventory	Aggregate inventory data at the System, Network, Tower, Sector, or Site level. It supports data export in PDF or CSV formats.
✔	✔	Email Notifications	Send email alerts when the alarm status changes.
✔	✔	Enterprise View	Display a simplified UI tailored for Enterprise Wi-Fi devices.
✔	✔	Guest Access Portal	Allow Wi-Fi Clients to access wireless service using a free model or vouchers.
	✔	Guest Access Portal (Paid Access)	Allow Wi-Fi Clients to connect to wireless service through paid access.
✔	✔	Hierarchical Dashboards	Visualize devices from tower-to-edge through customized dashboards for each device type.
✔	✔	IPv6 Support	Provide IPv6 support for cnPilot Enterprise devices.
	✔	Long Term Historical Data	Display long-term performance graphs for the following: • Fixed Wireless Broadband up to 2 years. • Wi-Fi APs, IIoT, and cnMatrix up to 1 year.

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
✔	✔	LTE	Manage cnRanger LTE devices.
	✔	Managed Server Provider (MSP)	Split an installation into separate Managed Accounts with independent administration and configuration.
✔	✔	Maps and Map Modes	Position devices and visualize their health and connectivity on the map. Also, change the map mode to display wireless key performance indicators.
✔		Mesh Peers	Display the details of available Mesh clients.

✔	✔	Multiple UI View	Support the following tailored views in the cnMaestro UI:
			• **Access and Backhaul View**: Used for managing Fixed Wireless and Wi-Fi deployments, including the following:
			  ◦ 60 GHz cnWave
			  ◦ cnMatrix
			  ◦ cnPilot Home (cnPilot R-Series)
			  ◦ cnRanger
			  ◦ cnVision
			  ◦ Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot)
			  ◦ ePMP
			  ◦ PMP
			  ◦ PTP
			• **Enterprise View**: Used for managing Enterprise Wi-Fi (E-Series and XV-Series), cnPilot Enterprise (ePMP 1000 Hotspot), and cnMatrix.
			• **Industrial Internet View**: Used for managing Fixed Wireless, Wi-Fi, and IIoT deployments, including the following:
			  ◦ 60 GHz cnWave
			  ◦ cnMatrix
			  ◦ cnPilot Home (cnPilot R-Series)

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
			• cnRanger • cnReach • cnVision • Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) • ePMP • Machfu • PMP • PTP
✔	✔	Notifications	Communicate immediate status with stateful alarms and events. Notifications help troubleshoot customer issues.
	✔	RADIUS Proxy	Proxy RADIUS packets are sent through cnMaestro (On-Premises) instead of directly to the RADIUS server from the AP.
	✔	RESTful API	Support HTTPS RESTful API for inventory, monitoring, performance, notification, and basic provisioning.
✔	✔	Role-Based Access	Assign the following roles to users: • Super Administrator • Administrator • Operator • Monitor • CPI
✔	✔	Scheduled Configuration Update	Specify a time to configure devices.
✔	✔	Scheduled Software Update	Specify a time to install device software.
✔	✔	Site Dashboard	Aggregate Wireless LAN AP statistics by location.
✔	✔	Statistics and Trending	Present historical radio and network statistics.

Table 1: Primary features supported by cnMaestro

Essentials	X	Feature	Description
✔	✔	Switch Groups	Share configuration across cnMatrix switches.
✔	✔	Syslog	Forward audit and event logs to a configured external Syslog server.
✔	✔	Template-Based Configuration	Schedule configuration of single devices or a group of devices across the network using templates for cnMatrix, cnPilot Home Series, cnReach, cnVision, ePMP, and PMP devices.
	✔	User Session Management	Track current cnMaestro users and support forced logoff.
✔	✔	Zero Touch Onboarding	Enable cnVision Client, PMP SMs, and ePMP SMs to automatically appear in the onboarding queue if the parent AP is already onboarded.

Differences with cnMaestro Cloud

The majority of features in cnMaestro On-Premises are identical to cnMaestro Cloud, but there are some differences.

Table 2 lists the feature differences between Cloud and On-Premises supported by cnMaestro.

Table 2: Differences with Cloud

Essentials	X	Feature	Description
✔	✔	Account Recovery	Password and account recovery issues are resolved locally.
	✔	Auto-Provisioning	New devices, such as cnPilot, cnVision, ePMP, and PMP, can automatically be approved and onboarded using the subnet.
✔	✔	Certificate Management	SSL certificate management is available for the UI and Guest Access Portal.
✔	✔	cnMaestro Software Upgrade	Enable three types of software upgrade: • **Virtual machine upgrade** requires the customer to replace the entire virtual machine with a new instance. The configuration and the data are exported from the old instance and imported to the new. • **Package upgrade** only updates the cnMaestro software. It does not require a virtual machine reinstallation.

Table 2: Differences with Cloud

Essentials	X	Feature	Description
			• **OVA upgrade** only overwrites the OS partition. For more information, refer to OVA Image.
✔	✔	Configuration Backup	Backup configuration from fixed wireless devices (cnVision, PMP and ePMP) and cnReach devices that are currently online.
✔	✔	Deployment	• The Cloud version is fully hosted and maintained by Cambium Networks at https://cloud.cambiumnetworks.com. • The On-Premises version is released as an OVA (Open Virtualization Archive) file that needs to be installed on either VMware or VirtualBox.
✔	✔	Device Connectivity	• In the Cloud version, all devices can be accessed through https://cloud.cambiumnetworks.com. • In the On-Premises, version, devices contact the local cnMaestro server. The devices must be configured to access the server before they can be managed. Alternatively, DHCP options can be configured to provide the cnMaestro URL when the device boots up.
✔	✔	Device Image Management	• In the Cloud, device images are automatically available. • In On-Premises, new images need to be downloaded from Support Center and added to the cnMaestro server.
✔	✔	Local and Authentication Server Administrators	Multiple types of administration access for local administrators (with a username and password maintained by cnMaestro) or authentication services (including TACACS+, RADIUS, LDAP, and Active Directory).
✔	✔	Onboarding	• In the Cloud version, devices onboard using either the device Manufacturer Serial Number (MSN) or through the Cambium ID or Onboarding Key (entered on the device). • In the On-Premises version, all devices contacting cnMaestro are added to the Onboarding Queue, where they are approved and managed.

Table 2: Differences with Cloud

Essentials	X	Feature	Description
✔	✔	On-Premises Console	Configure networking parameters and update the system password using the CLI available through the virtual machine console.
✔	✔	Server Management	Monitor virtual machine parameters such as disk, memory, and CPU utilization through the UI.
	✔	SNMP	Basic SNMP for inventory and alarms.
✔	✔	System Events	System events for On-Premises server instance.
✔	✔	System Log	Forward events to a remote system log server.
	✔	Webhooks	Send alarm notifications to the external servers.
✔	✔	Wireless LAN Speed Test	Test the speed between the wireless LAN APs and cnMaestro.

Supported browsers

Table 3 lists the browsers supported by cnMaestro on different operating systems.

Table 3: Supported browsers

Operating System	Browser	Version
Linux	Chrome	49 and above
	Firefox	45 and above
macOS	Safari	9 and above
MS Windows	Chrome	49 and above
	Firefox	45 and above
	Microsoft Edge	44.17763.1.0

Supported Virtualization Infrastructures

cnMaestro On-Premises is released as an Open Virtualization Archive (OVA) file.

	**NOTE:** cnMaestro On-Premises is also available as an Amazon Machine Image (AMI) that can be accessed through the AWS Marketplace. For more details, visit https://aws.amazon.com/marketplace/pp/prodview-tfe6lkwozpdho.

Table 4 lists the platforms supported by cnMaestro:

Table 4: Supported virtualization infrastructures

Platform	Version
VMware ESXi	Version 6.0.0 Update 3 (Build 7967664) or higher (this is the preferred platform)
VMware Workstation/Player	Version 16

Hardware requirements

cnMaestro On-Premises is preconfigured with two virtual drives of approximately 120 GB total size. The image supports up to 10,000 devices, including cnMatrix, cnReach, cnPilot, ePMP, PMP, and PTP.

	**NOTE:** Virtual hardware is different than physical hardware. Virtual hardware executes the cnMaestro application, and physical hardware executes the VMware virtualization infrastructure and the cnMaestro application (and other independent applications).

	**NOTE:**
	• Cambium Networks recommends using a recent Intel Core i7 or Xeon CPU with the following Geekbench Multi-Core score:
	  ◦ 4,500 for 100 devices
	  ◦ 8,000 for 4,000 devices
	  ◦ 13,400 for 10,000 devices.
	• If RADIUS Proxy is enabled, system resources like vCPUs and RAM must double the requirements in Table 5.
	• If a user enables NBI APIs and generates multiple performance reports, system resources like vCPUs and RAM must increase by 1.5 times the requirements in Table 5.
	• Cambium Networks recommends using a SSD drive to improve performance.

Table 5 lists the hardware requirements supported by cnMaestro.

Table 5: Hardware requirements

Number of Devices	Wireless Clients	Number of vCPUs	RAM Size (GB)	Hard Disk (GB)
1 - 100	Up to 1500	2	4	80
101 – 1,000	Up to 15,000	4	4	100
1,001 - 4,000	Up to 60,000	4	8	150
4,001 - 10,000	Up to 150,000	8	16	250

Device software

The cnMaestro OVA contains the latest versions of device software. Download new device software to your local computer using the steps described in the Supported Devices and Features section.

Device software is available from Cambium Support Center at: https://support.cambiumnetworks.com/files.

Table 6 lists the device model and the minimum software version supported by cnMaestro (not the recommended version).

Table 6: Supported devices and minimum software versions

Device	Minimum Software Version
60 GHz cnWave V1000	1.1
60 GHz cnWave V3000	1.1
60 GHz cnWave V5000	1.1
cnMatrix	2.0.4-r1
cnPilot e400/e500	3.2.1-r6
cnPilot e425H/e505	4.0
cnPilot e430W/e410/e600	3.5.2-r4
cnPilot e501S	3.2.1-r6
cnPilot e502S	3.2.1-r6
cnPilot e510	3.11.4-r9
cnPilot e700	3.7-r9
cnPilot r190	4.4.2-R2

Table 6: Supported devices and minimum software versions

Device	Minimum Software Version
cnPilot r195P	4.7
cnPilot r195W	4.5.2
cnPilot r200/r201	4.4.2-R2
cnPilot XE3-4	6.4
cnPilot XV2-2	6.1
cnPilot XV2-2	6.4
cnPilot XV2-2T0	6.3.5-r4
cnPilot XV3-8	6.0
cnRanger Sierra 800	1.0.1.0-r1
cnRanger Tyndall 101	1.0.1.0-r1
cnRanger Tyndall 201	2.0-r1
cnReach N500	5.2.17e
cnVision Client	4.6
cnVision Hub	4.6
E2E Controller	1.0.1-r2
ePMP 1000	2.6.2
ePMP 1000 Hotspot	3.2.1-r6
ePMP 2000	3.0.1
ePMP 3000	4.4.1
ePMP Elevate	3.2
ePMP Elevate SXGLIT5/LHG5	4.3.2.1
ePMP Elevate XM/XW	3.2
ePMP Force 130 2.4 GHz	4.4
ePMP Force 130 5 GHz	4.3.2

Table 6: Supported devices and minimum software versions

Device	Minimum Software Version
ePMP Force 180/200	2.6.2
ePMP Force 190	3.5
ePMP Force 200L	4.7.0
ePMP Force 300	4.1
ePMP Force 300-13	4.4
ePMP Force 300-13L	4.5.2
ePMP Force 300-13LC	4.6
ePMP Force 300-19	4.4
ePMP Force 300-19R	4.4
ePMP Force 300-22L	4.6
ePMP Force 300-25L	4.6
ePMP Force 300 CSM	4.3.2
ePMP Force 400	5.1.0.18
ePMP Force 425	5.1.0.18
ePMP MP 3000	4.5
ePMP PTP 550	4.1
ePMP PTP 550E	4.4.2
Machfu	7.1.2-1.1.0.5
PMP	15.0.1
PMP 450 MicroPoP Omni	16.2.1
PMP 450 MicroPoP Sector	16.2.1
PMP 450b Retro	16.2.2
PTP 650	01-47
PTP 670 (650 Emulation)	01-47
PTP 670, PTP 700	02-67



NOTE:

By default, Cambium Networks does not update device builds during OVA or package upgrades. The user must upload device software by clicking the **Add** button in **Administration** > **Server** > **Software Images > Manage Software Images**. Software can also be downloaded through an Anchor account.

For further information, refer to Manage Software Images.

Quick Start

Installation

The default passwords for cnMaestro are:

Table 7: Default passwords

Component	Username/Password
cnMaestro UI	admin /admin
Virtual Machine Console	cambium /cnmaestro



NOTE:
Please change your passwords after logging in for the first time.

Virtualization

On-Premises supports two types of virtualization:

- Desktop virtualization
- Bare metal hypervisor

Desktop virtualization

Desktop virtualization executes within an existing operating system environment (Windows, Mac, or Linux). The virtualization software (such as VMware Workstation or Oracle VirtualBox) executes in tandem with other desktop applications. cnMaestro can be installed as a virtual machine on one of these platforms.

The desktop environment is the easiest way to get cnMaestro up-and-running quickly. You can download a trial version of VMware Workstation Player from VMware.

Bare metal hypervisor

A bare metal hypervisor takes over the entire physical machine and uses it to host virtual instances. This type of virtualization is best for production environments, but takes time to set up correctly. VMware vSphere ESXi is an example of this type of virtualization, and it is discussed in detail in the Appendix. You can download ESXi here.

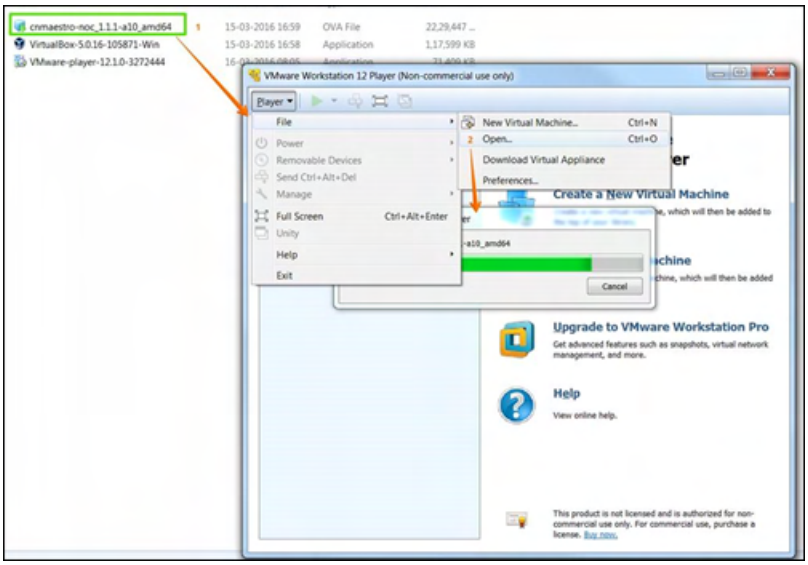
cnMaestro deployment

This document describes cnMaestro deployment using VMware Workstation Player. Directions for VMware vSphere ESXi and VirtualBox are found in the Appendix. VMware Workstation Player (and Oracle VirtualBox) are the easiest to install and evaluate, and ESXi is preferred for production.

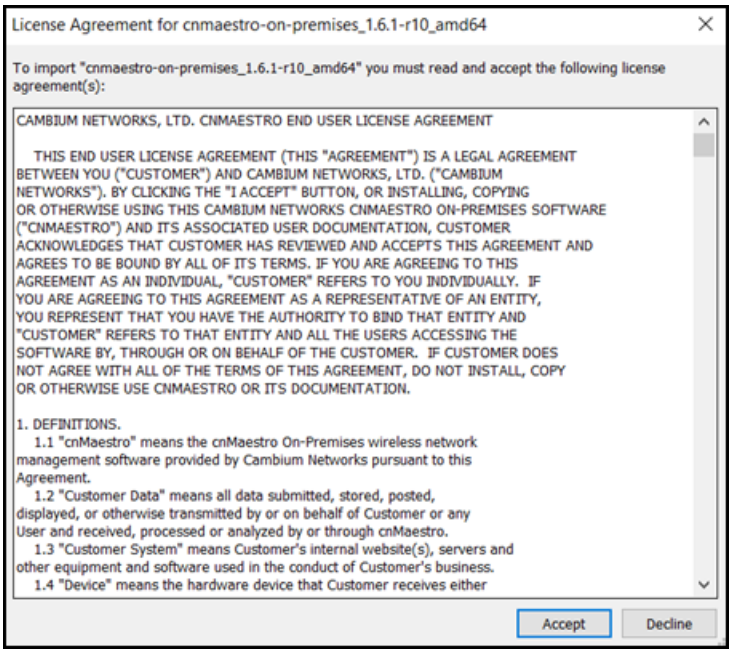
VMware Workstation Player

Follow the steps below to import cnMaestro On-Premises into VMware Workstation Player:

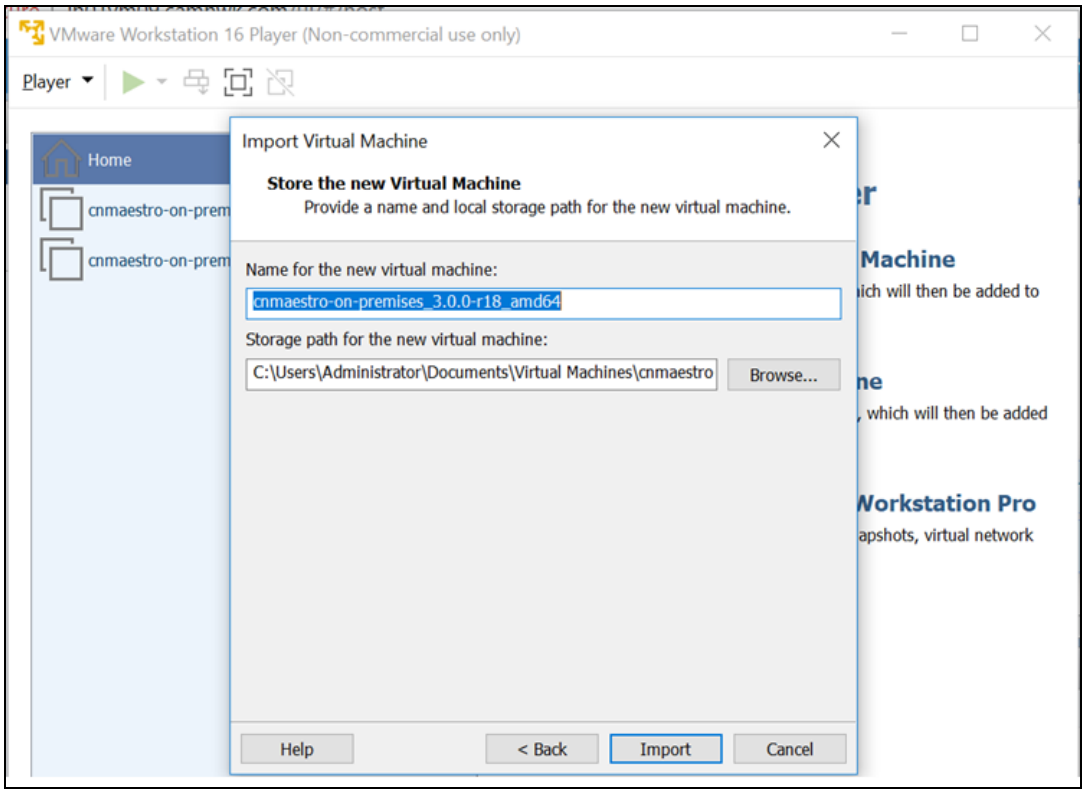
1. Download the cnMaestro On-Premises OVA file from Cambium Support Center.
2. Open VMware Workstation Player and navigate to **Player** > **File** > **Open**. Import the cnMaestro OVA.



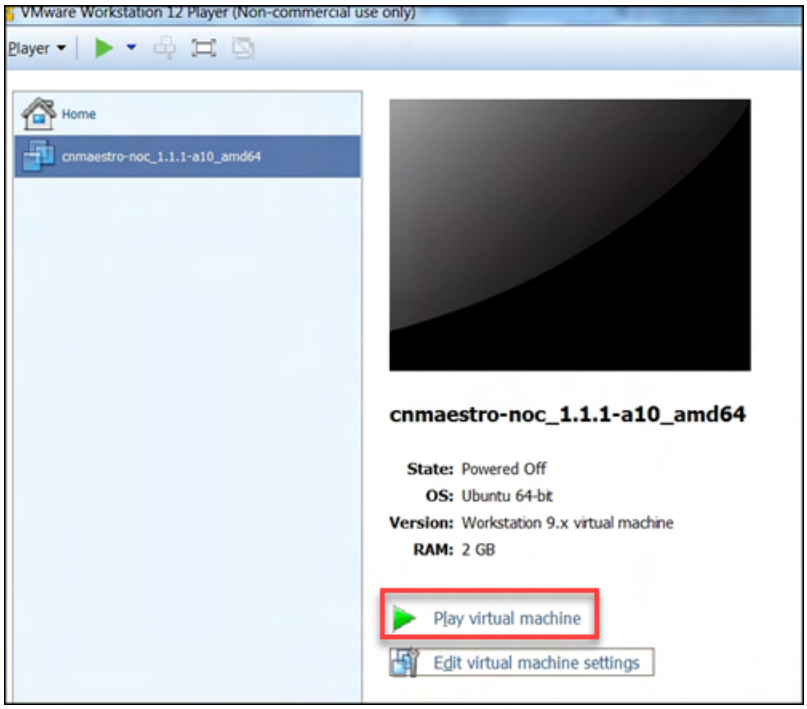
3. **Accept** the cnMaestro EULA.



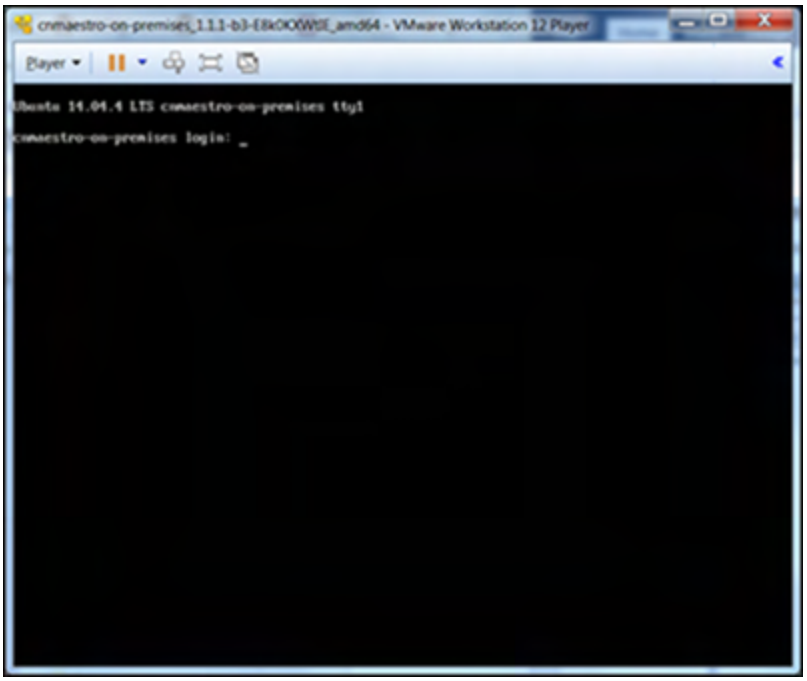
4. Click **Import** to start the deployment. This process could take a couple of minutes.



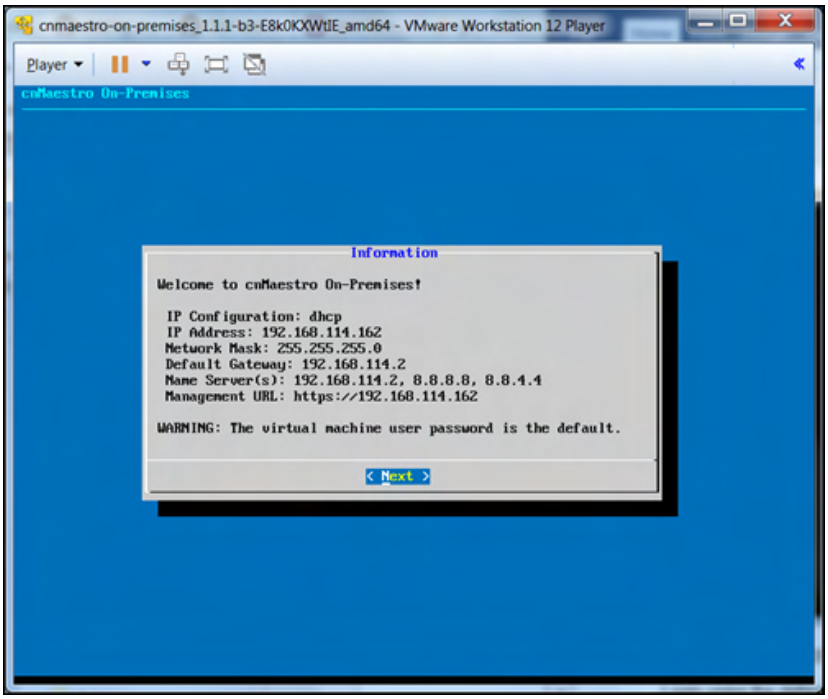
5. Click **Play** to start the Virtual Machine.



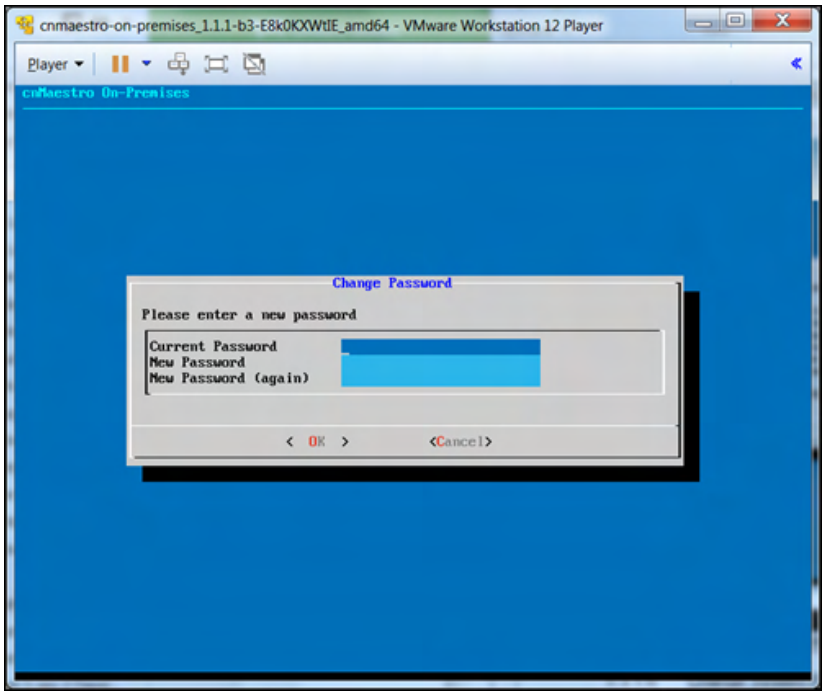
6. Login to the cnMaestro Console using the default username/password (cambium/cnmaestro). The Console is the primary way to access the cnMaestro CLI (Command Line Interface).



7. The **Information** page displays the current network settings.



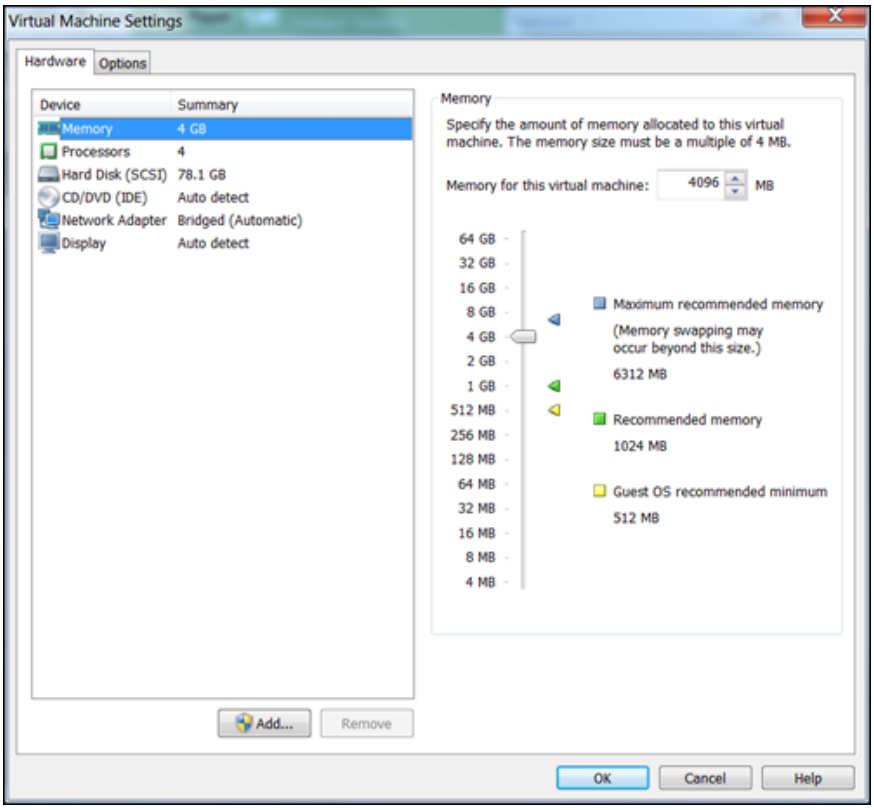
8. Click **Next** and navigate to the **Password** page to update the password.



Update virtual machine hardware

cnMaestro by default is configured to use 2 CPUs, 4 GB memory, and NAT. To change these parameters, you should stop the virtual machine, update the virtual machine settings in VMware, and then restart. Click **Edit Virtual Machine Settings** from the VMware home screen. From there you can update the virtual hardware.

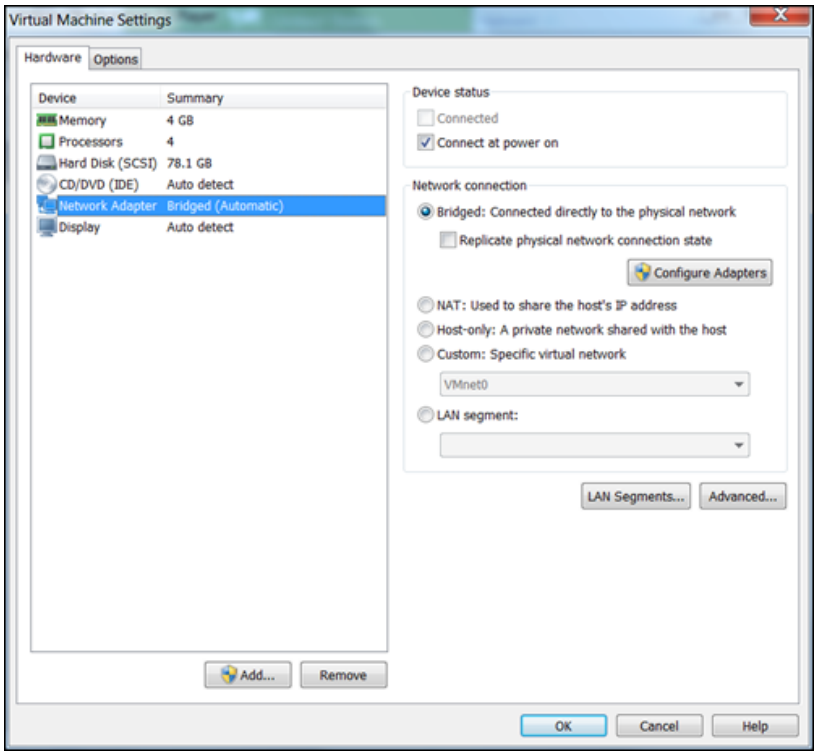
	NOTE: If you are evaluating more than 100 devices, we recommend to use at least 4 GB of memory and 4 processors.



Configure network adapter

By default, cnMaestro acquires its IP address from a DHCP Server. With desktop virtualization, the DHCP server is in a private network localized in the host device, and therefore the IP address of cnMaestro will not be accessible from the external LAN. VMware should instead be configured so the virtual machine network interface is shared with the device.

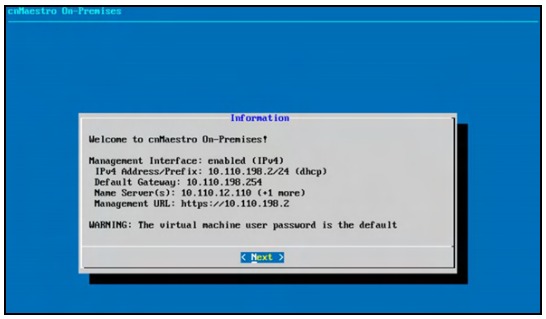
1. In the VMware settings, select **Bridged** for the Network Adapter state and select the **Network Adapter** > **Configure Adapter** to choose the external LAN adapter.



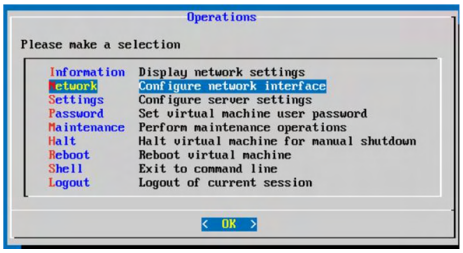
2. Restart cnMaestro.

Configure cnMaestro networking

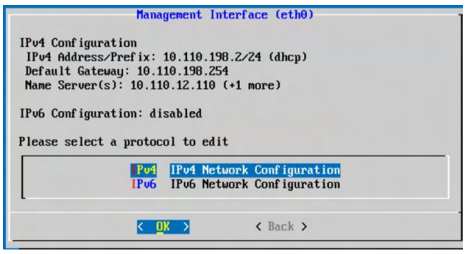
1. After logging back in, the **Information** page displays the IP address from the LAN instead of the private network.



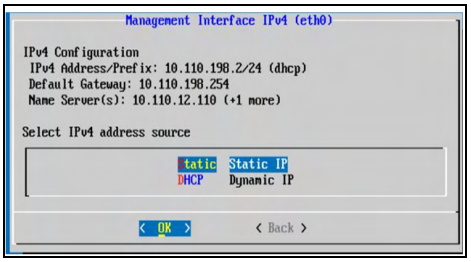
2. Click **Next** to view the **Operations** menu and select **Network.**



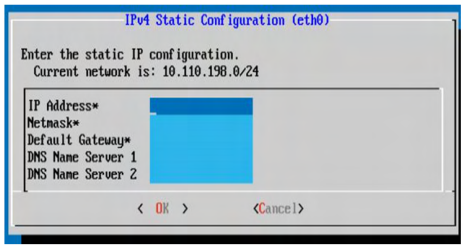
3. The **Management Interface (eth0)** window appears.



4. Select **IPv4** then **Static** to configure a static IP address.



5. Set **IPv4 Static Configuration** parameters.



Network configuration

By default, cnMaestro is configured with a single eth0 interface. You can extend this to support a second eth1 interface for control (device) traffic. Details for configuring two interfaces are specified later in this document.

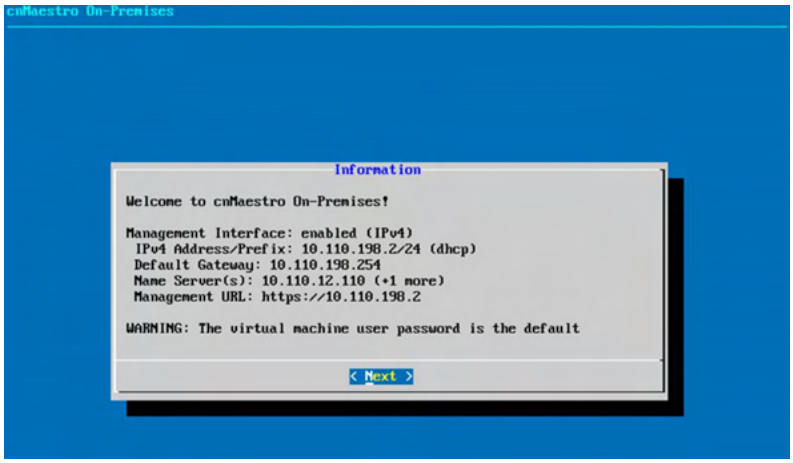
Single interface (eth0)

Name	Interface	Details
Management/Cluster/Device	eth0	User interface, cluster, API, device controller traffic.

Protocols (IPv4, IPv6)

cnMaestro supports both IPv4 and IPv6. The eth0 interface requires IPv4 (for the system IP address and clustering configuration) and optionally supports IPv6.

Validate the changes. You can validate your update by navigating back to the **Information** page and viewing the current network configuration.

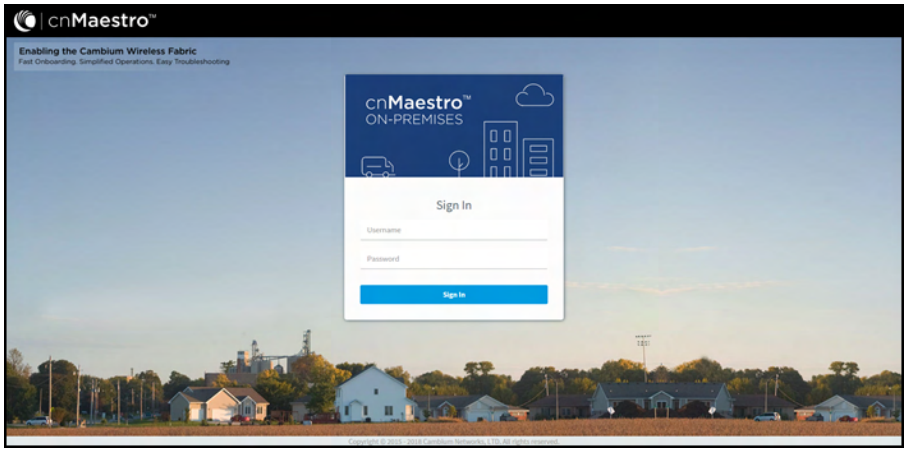


cnMaestro UI access

Access the UI using the **Management URL** specified in the **Information** page.

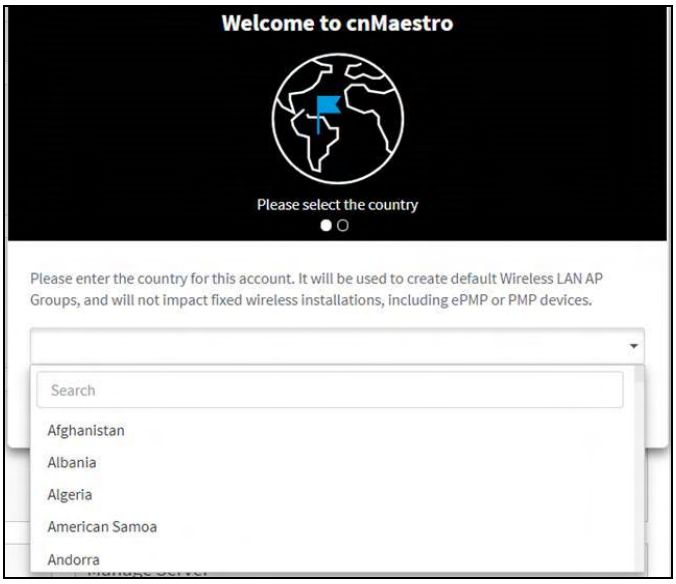
The default username/password are admin/admin.

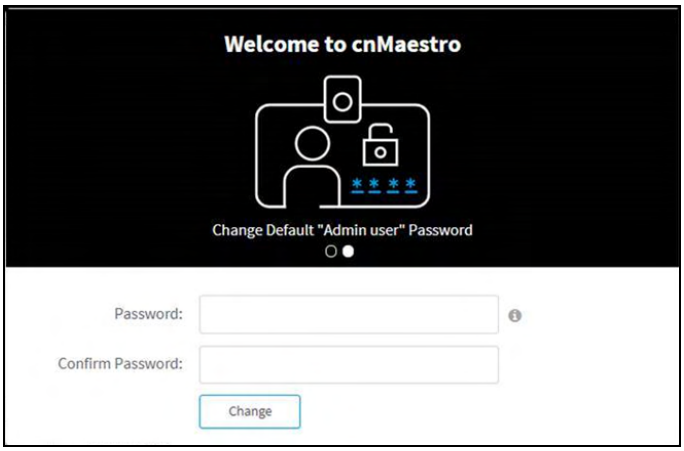
	NOTE: The browser displays an untrusted certificate error when you access cnMaestro On-Premises. This is because it uses a self-signed certificate. You can upload your own Root CA and Signed Certificates to suppress the error.



First login

1. Upon first login, cnMaestro will request initial configuration and require changing the default password.



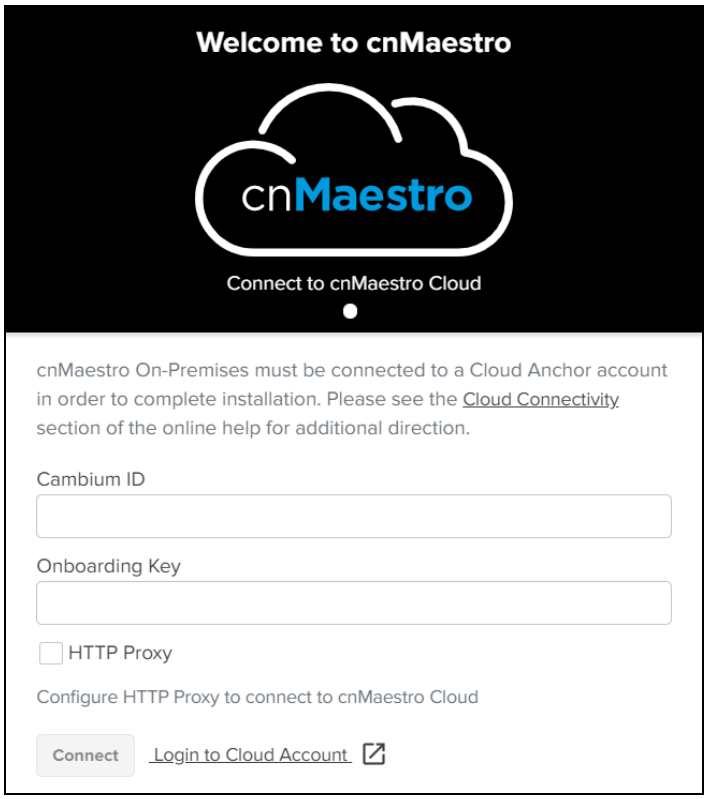


User can connect to Cloud account using Enforce Anchor account.

	NOTE: Enforce Anchor account connectivity is available only for new 3.1.0 installations.

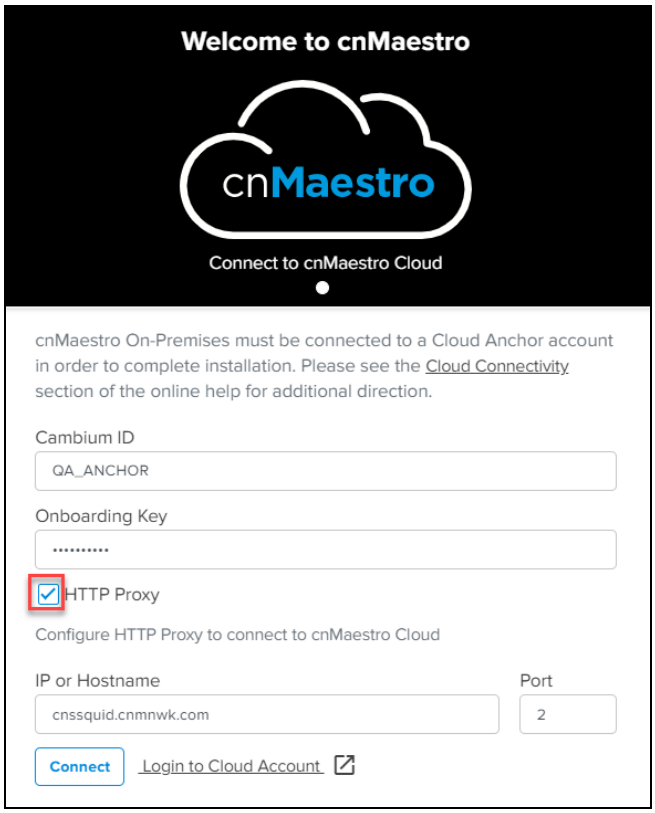
Perform the following steps to connect to the Cloud account.

1. Enter the **Cambium ID** and **Onboarding Key**.



Configure HTTP Proxy to connect to cnMaestro Cloud.

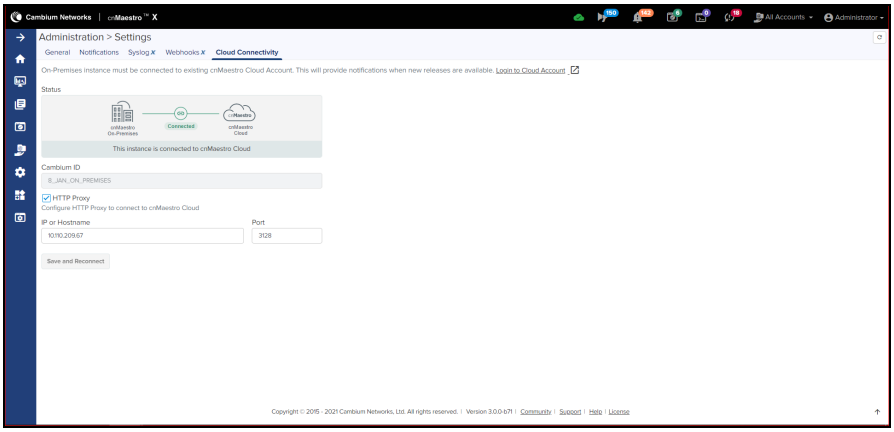
2. Select **HTTP Proxy.**
3. Enter **IP** or **Hostname.**
4. Enter **Port** number and click **Connect**.



For more details to connect with Cloud Anchor account, refer to Cloud Connectivity.

Once the initial configuration is complete, you will have access to the entire UI.

5. Navigate to **Administration** > **Settings** > **Cloud Connectivity** to connect the Cloud Anchor account with On-Premises.



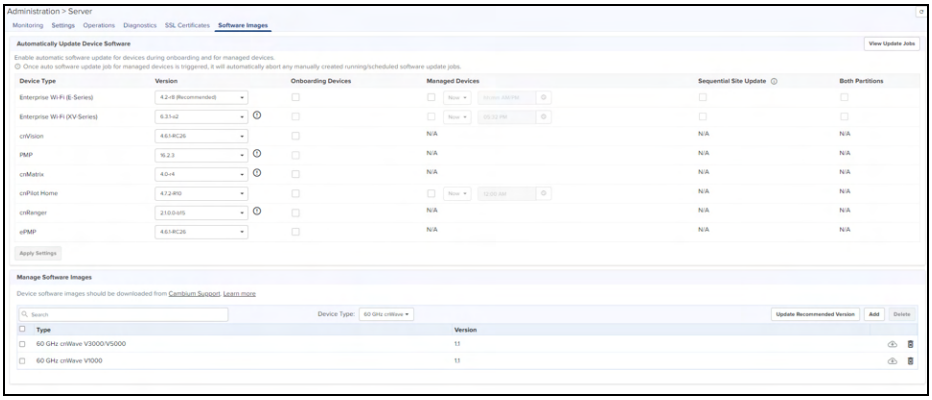
6. Navigate to **Administration** > **Server** to monitor and manage cnMaestro On-Premises.

Onboard devices

Devices must have the correct software installed in order to access cnMaestro. These images are hosted on the Cambium Networks website, and they can also be downloaded directly from cnMaestro On-Premises. The minimum software requirements are listed in the Release Notes. The cnMaestro OVA contains the latest software versions at the time of build.

Navigate to **Administration** > **Server** > **Software Images**. Select your device type to display the available images, and then click the download icon ( ).

Figure 1 Device software



Once the device is updated with the correct software version, it can be onboarded.

In order to access cnMaestro, devices must be configured with the cnMaestro On-Premises URL. There are three ways to do this (listed in priority order)

1. Configure the cnMaestro URL on the device

2. Configure DHCP Option 43 on the DHCP server

3. Configure DHCP Option 15 on the DHCP server

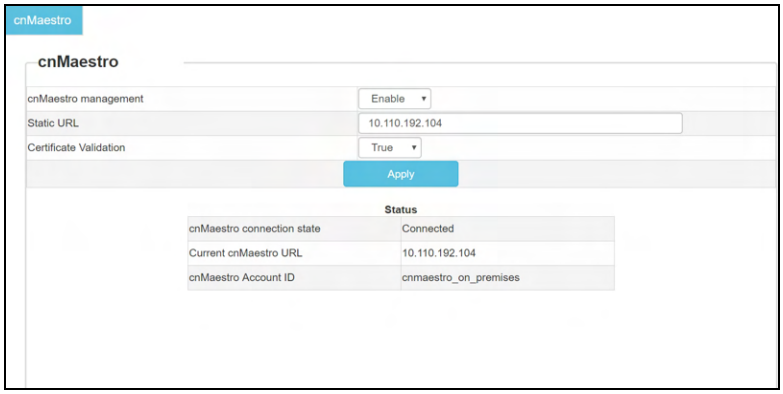
If none of these are present, the default action on the device is to access the cnMaestro Cloud URL: https://cloud.cambiumnetworks.com.

Static URL

If a static URL is configured in the device UI, the device will always connect using it. The below sections details where to set the cnMaestro URL on various device types. The Cambium ID and Onboarding Key can optionally be used in some devices for added security.

cnMatrix

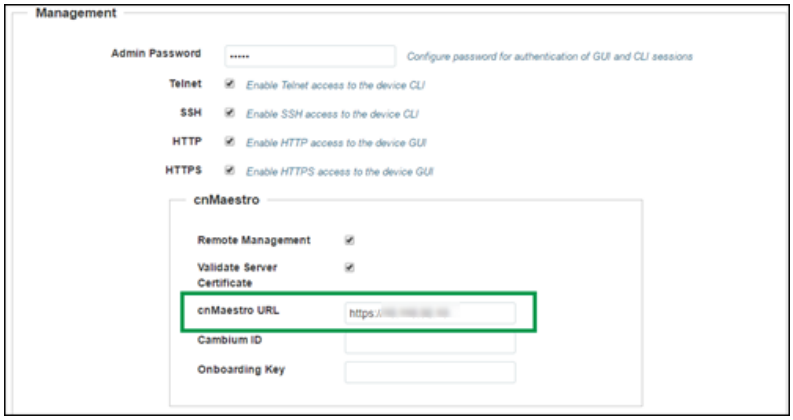
1. Navigate to **System** > **cnMaestro** tab.
2. Enter **Static URL**.



cnPilot Enterprise

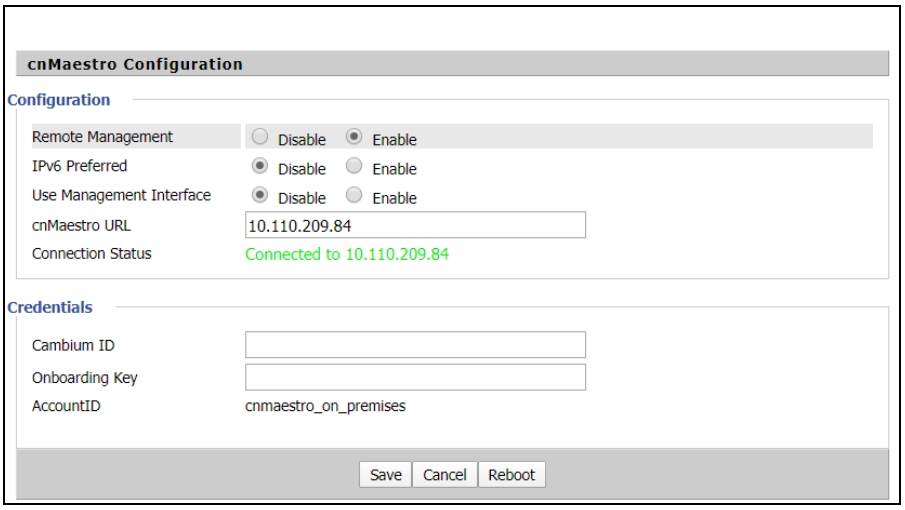
1. Navigate to **Configure** > **System** > **Management** tab.

2. Enter **cnMaestro URL**.



cnPilot Home

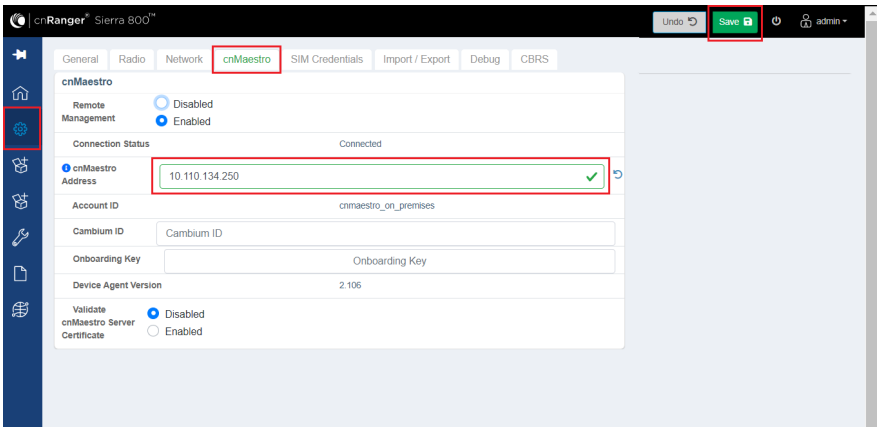
1. Navigate to **Administrator** > **cnMaestro** tab.
2. Enter **cnMaestro URL.**



cnRanger

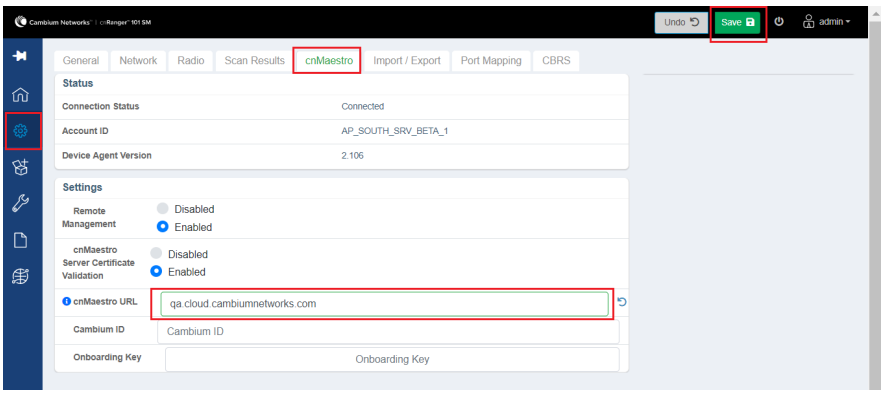
Setting static URL for cnMaestro on Sierra 800

1. Navigate to **Configuration** > **cnMaestro** tab.
2. Under cnMaestro section, enter URL in the **cnMaestro Address**.
3. Click **Save**.



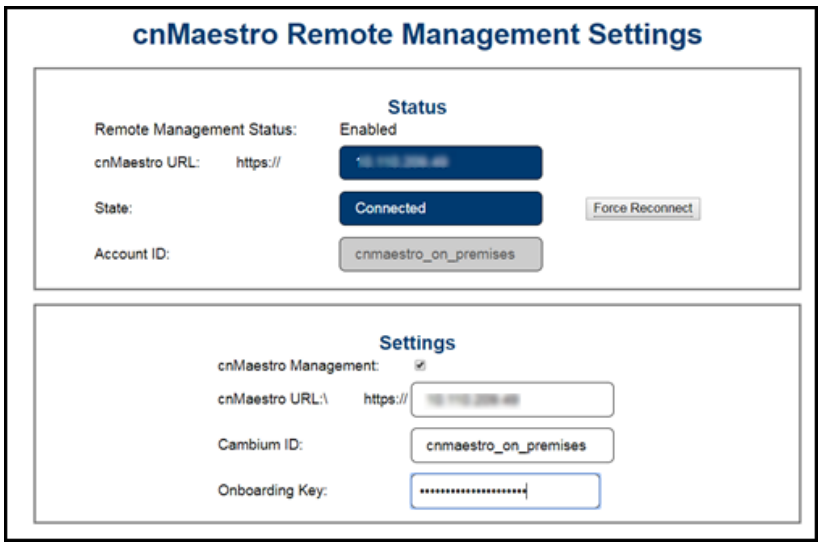
Setting static URL for cnMaestro on Tyndall 101

1. Navigate to **Configuration** > **cnMaestro** tab.
2. Under cnMaestro section, enter URL in the **cnMaestro URL**.
3. Click **Save.**



cnReach

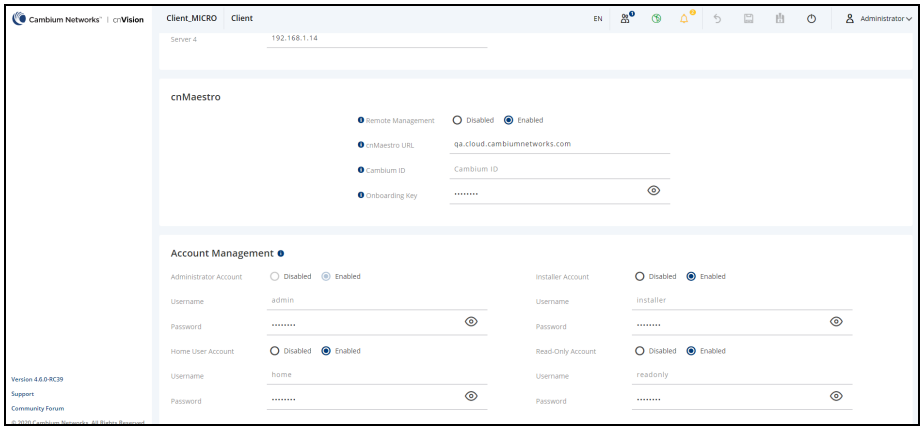
1. Navigate to **cnMaestro** > **Management Settings** > **Settings**.



2. Click **cnMaestro Management** check box.
3. Enter **cnMaestro URL.**

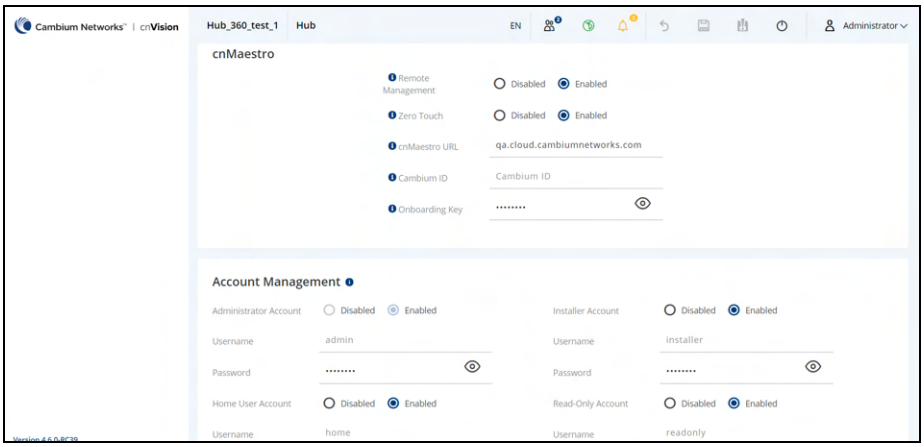
cnVision Client

1. Navigate to **Configuration** > **System** > **Device Management** tab.
2. Under cnMaestro section, enter **cnMaestro URL**.
3. Click **Save**.



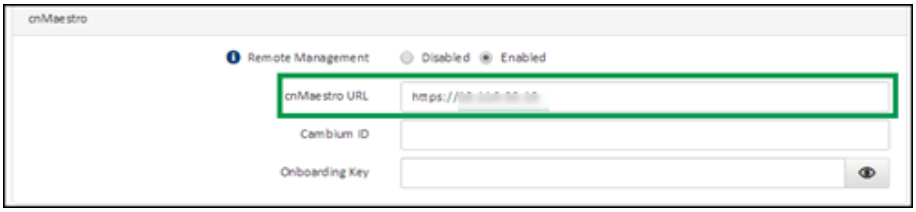
cnVision Hub

1. Navigate to **Configuration** > **System** > **Device Management** tab.
2. Under cnMaestro section, enter **cnMaestro URL**.
3. Click **Save**.



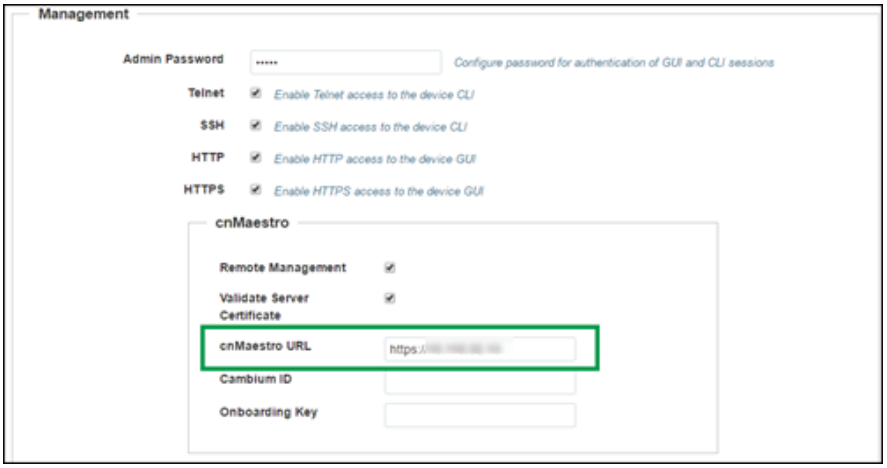
ePMP 1000 AP/SM

1. Navigate to **Configuration** > **System** > **cnMaestro** tab.
2. Enter **cnMaestro URL.**



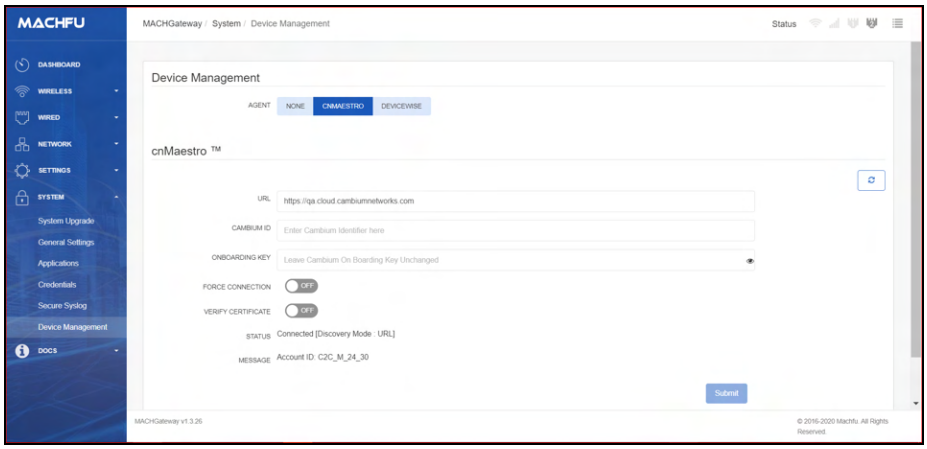
ePMP 1000 Hotspot

1. Navigate to **Configure** > **System** > **Management** tab.
2. Enter **cnMaestro URL.**



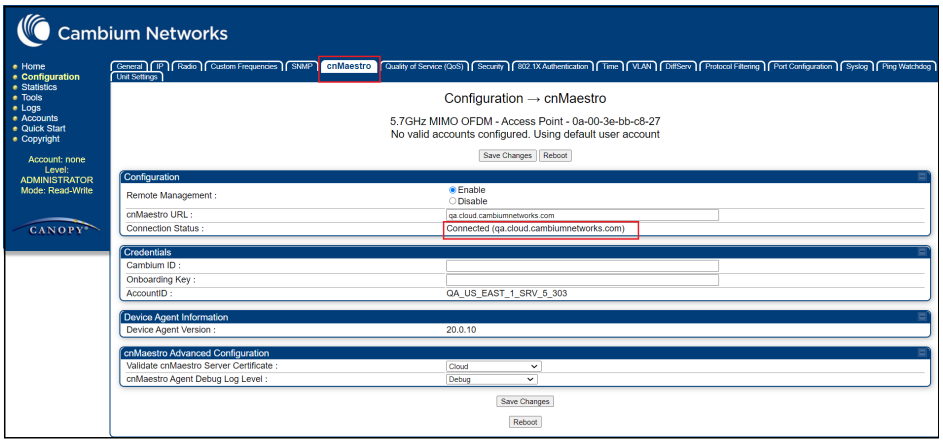
Machfu

1. Navigate to **System** > **Device Management** tab.
2. Under cnMaestro section, enter cnMaestro **URL**.
3. Click **Save**.



PMP

1. Navigate to **Configuration** > **cnMaestro** tab.
2. Enter **cnMaestro URL**.
3. To check the cnMaestro connection status, navigate to **Configuration** > **cnMaestro** > **Connection Status.**



PMP configuration prerequisites

Please make sure the following configuration requirements are met in PMP before onboarding to cnMaestro.

SM (not using NAT)

- LAN 1 network interface should have 'public' accessibility.
- IP address should be public IP address: either static IP address or obtained via DHCP.
- DNS server configuration should be filled: either static IP address or obtained via DHCP.

SM using NAT

- Remote Management interface with standalone config should be enabled.
- Remote Management IP address should be public IP address.
- DNS server should be configured.

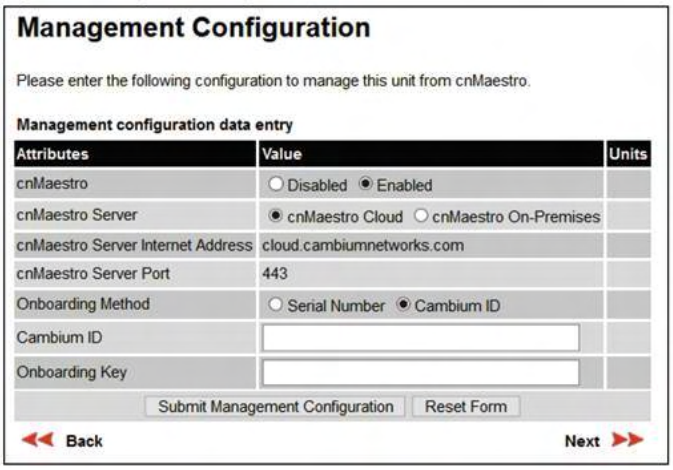
AP

- IP address should be public.
- DNS server should be configured.

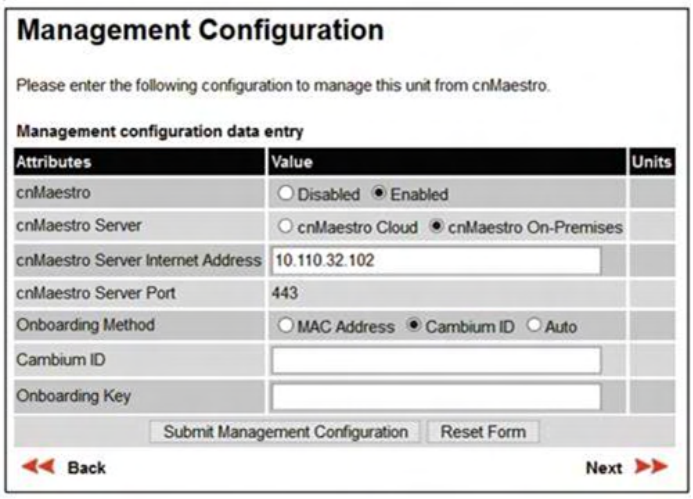
PTP

1. Navigate to **Installation** and click **run Installation wizard** button.

2. In the **Management Configuration** window, under cnMaestro, select **Enabled.**



3. Select **cnMaestro On-Premises** radio button.



DHCP Options (Linux)

A DHCP Server can be used to configure the IP Address, Gateway, and DNS Servers for Cambium Networks devices. If you administer the DHCP Server, you can also configure DHCP Options to direct devices how to access cnMaestro automatically (so the URL does not need to be set on each device). Cambium Networks devices support DHCP Options 43 and 15 for setting the cnMaestro On-Premises URL.

The following configuration is for Linux-based systems. Refer to Appendix: Windows DHCP Options Configuration for configuring DHCP options for Windows.

NOTE:
DHCP Options are available from the following builds:

- cnMatrix: 2.0.4-r1
- cnPilot e400/e500/e502S/e501S: 3.2.1-r6
- cnPilot e425H/e505: 4.0
- cnPilot e430W/e410/e600: 3.5.2-r4
- cnPilot e510: 3.11.4-r9
- cnPilot e700: 3.7-r9
- cnPilot r190: 4.4.2-R2
- cnPilot r195P: 4.7
- cnPilot r195W: 4.5.2
- cnPilot r200P/r201P: 4.4.2-R2
- cnReach: 5.2.17e
- ePMP 1000, ePMP Force 180/200: 3.1
- ePMP 1000 Hotspot: 3.2.1-r6
- ePMP 2000: 3.0
- ePMP 3000: 4.5
- ePMP Elevate: 3.2
- ePMP Force 190: 3.5
- ePMP Force 300: 4.1
- ePMP PTP 550: 4.1
- Machfu 7.1.2-1.1.0.5
- PMP: 15.0.1
- PTP 650, PTP 670 (650 Emulation): 02-67

The priority order for determining the cnMaestro URL is the following:

1. Static URL manually set through the Device UI.
2. DHCP Option 15.
3. DHCP Option 43.
4. Default Cambium Cloud URL (https://cloud.cambiumnetworks.com).

NOTE:

cnRanger, cnReach, PTP 650, PTP 670, and PTP 700 do not support DHCP Options for onboarding.

Using DHCP Option 43

DHCP Option 43 returns the cnMaestro On-Premises URL as a Vendor-Specific Option. DHCP Option 43 is returned in tandem with DHCP Option 60 (the Vendor Class Identifier, or VCI).

The VCI for the individual Cambium products is listed below:

Table 8: VCI (DHCP Option 60)

Product	VCI (DHCP Option 60)
cnMatrix	Cambium-cnMatrix-EX2K
cnPilot r190	Cambium-cnPilot r190
cnPilot r195	Cambium-cnPilot r195
cnPilot r200P	Cambium-cnPilot r200P
cnPilot r201P	Cambium-cnPilot r201P
cnPilot e400/e410/e430W cnPilot e425H/e505 cnPilot e500/e501S/e502S/e510 cnPilot e700/e600	Cambium-WiFi-AP
ePMP	Cambium
ePMP 1000 Hotspot	Cambium-WiFi-AP
PMP 430 SM	Cambium PMP 430 SM
PMP 450 AP	Cambium PMP 450 AP
PTP 450 BHM	Cambium PTP 450 BHM
PMP 450 BHS	Cambium PTP 450 BHS
PMP 450 SM	Cambium PMP 450 SM
PMP 450b SM	Cambium PMP 450b SM
PMP 450i AP	Cambium PMP 450i AP
PMP 450i BHM	Cambium PTP 450i BHM
PTP 450i BHS	Cambium PTP 450i BHS
PMP 450i SM	Cambium PMP 450i SM
PMP 450m APs	Cambium PMP 450m AP

Typically, Option 43 is the preferred mechanism to configure the cnMaestro URL. Example configuration for the ISC DHCP Server is presented below (from the /etc/dhcp/dhcpd.conf file).

```
option option-43 code 43 = string;

# ePMP/PMP Devices
class "Cambium" {
    match if option vendor-class-identifier = "Cambium";
    # DHCP server MUST return the device's Vendor Class back, in the offer.
    option vendor-class-identifier "Cambium";
    # cnMaestro On-Premises IP is 192.168.0.100
    option option-43 "https://192.168.0.100";
}

# WiFi Devices
class "Cambium-WiFi-AP" {
    match if option vendor-class-identifier = "Cambium-WiFi-AP";
    option vendor-class-identifier "Cambium-WiFi-AP";
    option option-43 "https://192.168.0.100";
}

# cnPilot R200P Devices
class "Cambium-cnPilot R200P" {
    match if option vendor-class-identifier = "Cambium-cnPilot R200P";
    option vendor-class-identifier "Cambium-cnPilot R200P";
    option option-43 "https://192.168.0.100";
}

# cnPilot R201P Devices
class "Cambium-cnPilot R201P" {
    match if option vendor-class-identifier = "Cambium-cnPilot R201P";
    option vendor-class-identifier "Cambium-cnPilot R201P";
    option option-43 "https://192.168.0.100";
}
```

Using DHCP Option 15

DHCP Option 15 allows the device to derive the cnMaestro URL from the domain name. For example, if the domain name in DHCP Option 15 is **mycompany.com**, the device will try to access the cnMaestro server at **cnmaestro.mycompany.com** (essentially the string **cnmaestro** is prepended to the domain). The domain itself, and the IP address of cnMaestro, must be configured in the DNS server for this to work correctly.

Sample configuration for the ISC DHCP Server is presented below (from the /etc/dhcp/dhcpd.conf file).

```
option domain-name "mycompany.com";
```

UI Navigation

cnMaestro On-Premises provides a number of ways to navigate its content.

This section includes the following topics:

- Account View
- Home page
- Page structure
- UI Navigation
- Access and Backhaul View
- Enterprise View
- Side menu
- Section tabs
- System status
- Logout



NOTE:

- Only Super Administrator and Administrator can change the Time Zone.
- The Time Zone setting is applicable only for Email Notifications, Webhooks, and RESTful APIs only.

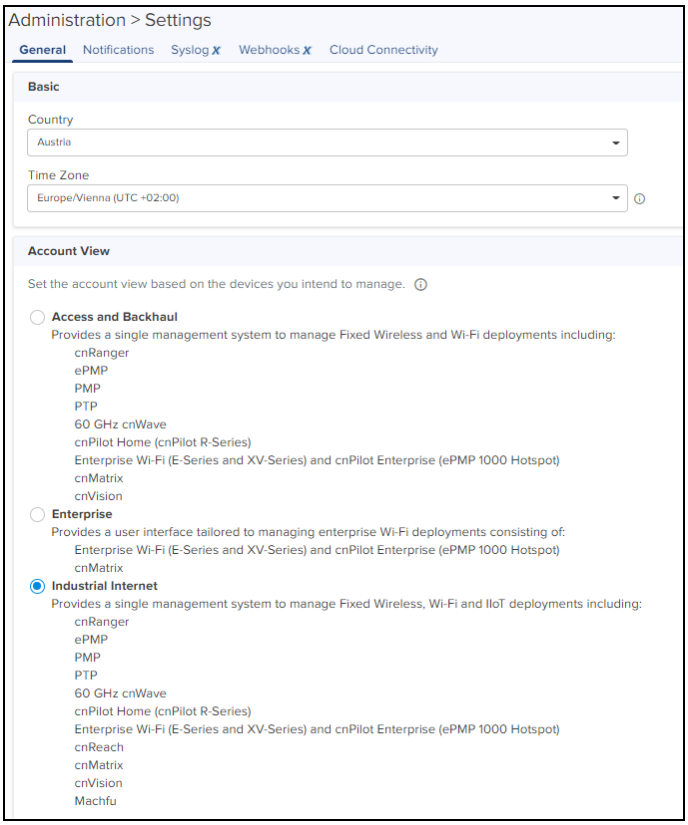
Account View

cnMaestro supports three different account views, based upon the composition of devices.

- Access and Backhaul view
- Enterprise view
- Industrial Internet view

The account view is selected when the account is created but it can be changed later through the

Administration > **Settings** page.



Access and Backhaul View

The Access and Backhaul View supports all Fixed wireless and Wi-Fi devices. The device types include 60 GHz cnWave, cnMatrix, cnPilot Enterprise (ePMP 1000 Hotspot), cnPilot Home, cnRanger, cnVision, Enterprise Wi-Fi (E-Series and XV-Series), ePMP, PMP, and PTP.

Enterprise View

The Enterprise View supports the Enterprise Wi-Fi portfolio, which includes the , cnPilot Enterprise APs (ePMP 1000 Hotspot), cnMatrix, and Enterprise Wi-Fi APs (E-Series and XV-Series). It provides a simplified UI for Wi-Fi components (hiding fixed wireless features such as Towers).

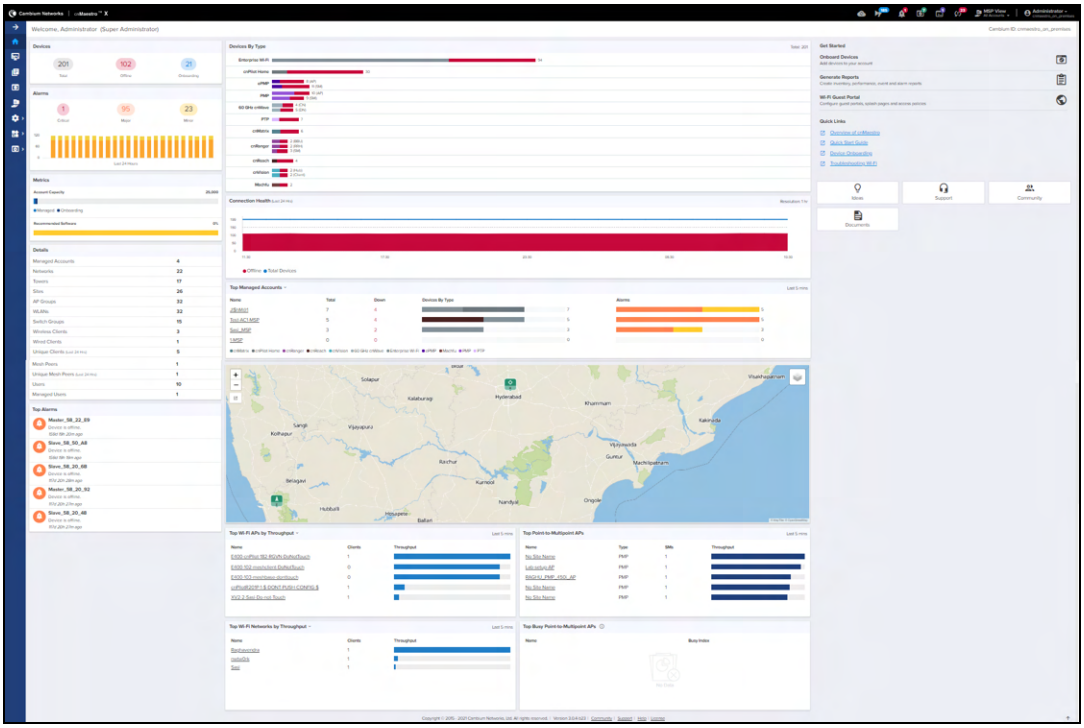
Industrial Internet View

Industrial Internet View provides a interface for Fixed Wireless, Wi-Fi, and cnReach deployments. The device types include 60 GHz cnWave, cnMatrix, cnPilot Home (cnPilot R-Series), cnRanger, cnReach, cnVision, Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) and ePMP.

Home page

The Home page is displayed when the user logs into the cnMaestro. It provides links to the core functional areas in the UI, such as **Cambium Support Center**, **Community**, **Documents**, and **Licensing**.

Figure 2 cnMaestro On-Premises - Home page



Page structure

cnMaestro follows a standard page structure, which consists of a left-side menu and a content area. On many pages, tabs provide additional content navigation.

Figure 3 cnMaestro On-Premises - page structure

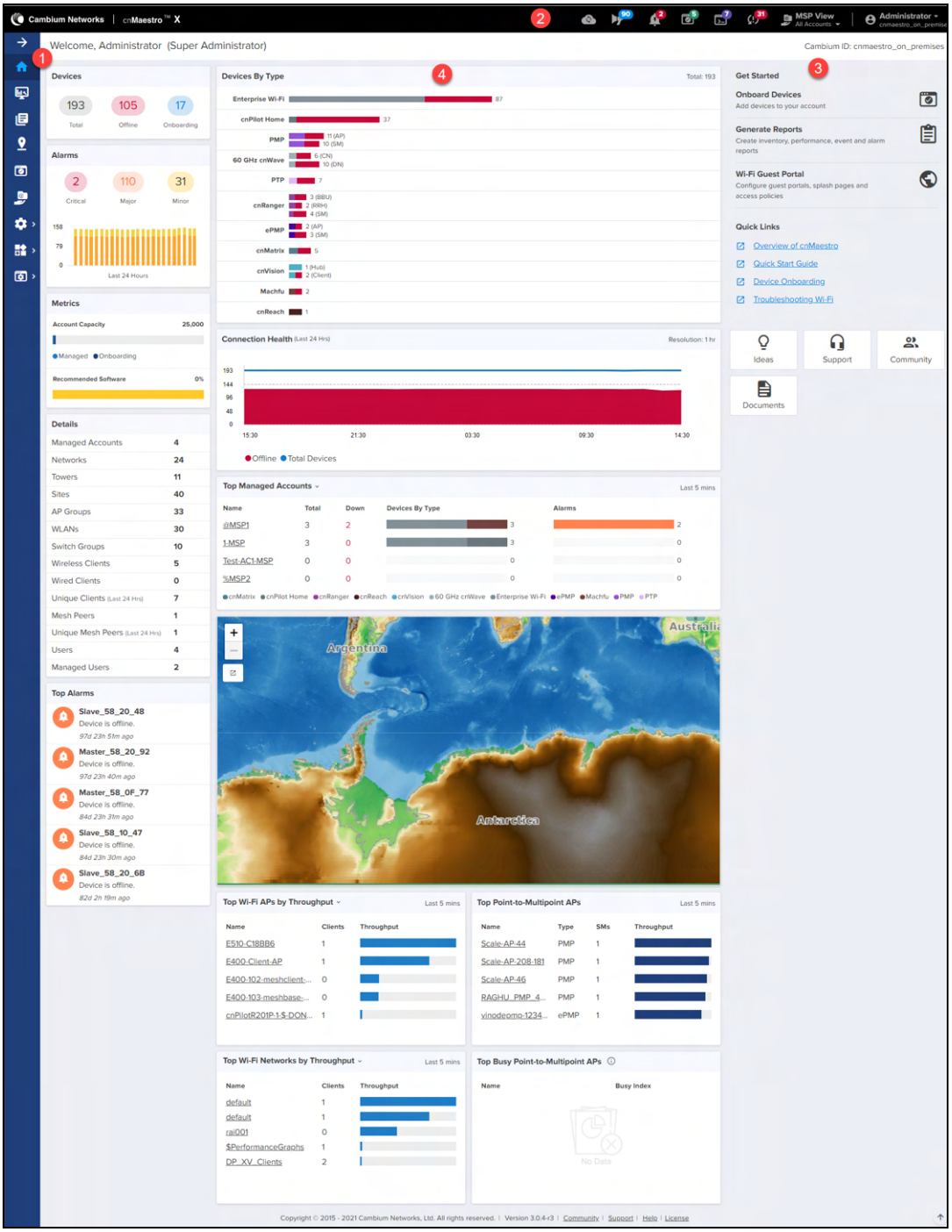


Table 9: UI description

Number	Elements	Description
1.	Left menu	Shows the functional areas of the UI. This menu can be expanded or collapsed to view the submenu by clicking the top arrow.
2	Header	Shows the basic counters for **Major Alarms**, **Devices Awaiting for Approval**, **Software Updates Jobs**, and **Out of Synch Devices**.
3	Right menu	Provides links to Cambium **Ideas**, **Support**, **Community**, **Documents**, and **Licensing** .
4	Functional area	Shows the detailed view of the section selected in the left menu.

Page navigation

The cnMaestro pages include items such as **Dashboard, Notifications, Configuration, Statistics, Report, Software Update, Map, Clients**, and, **Mesh Peers**.The content of a page differs depending upon its context. For example, a Dashboard page will be different at the **System/Network/Tower/Site/Device** levels. The context, or level in the hierarchy, is selected in the Device tree as shown below.

Access and Backhaul View

Overview

The Access and Backhaul view leverages a hierarchical tree to display device installations. In this view, customers can group their fixed wireless devices into Networks, and display their Point-to-Multipoint devices in Tower-based sectors. Navigation is performed using the tree. The device tree is segmented into two tabs: Network and Wi-Fi AP Groups.

Networks tab

The Network tab displays a hierarchical view of the devices. It consists of Systems, Networks, Towers, Sites, and, Devices. There is a strict ordering for how nodes can fit in the hierarchy, and as one navigates through and selects nodes, the pages display the node chosen.

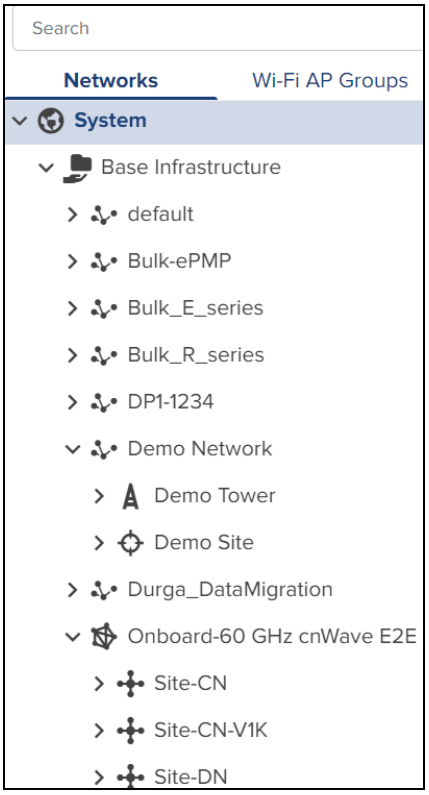
Selecting an arrow icon will expand the node and display the next level of hierarchy.



NOTE:

Opening the node does not automatically select a node in the new hierarchy, instead the desired node needs to be clicked.

Figure 4 Device tree navigation



The structured hierarchy has the following devices:

Table 10: Structured hierarchy nodes

Icon	Name	Description
	60 GHz cnWave CN	CN is mapped to a **Site** in E2E Network.
	60 GHz cnWave DN	DN is mapped to a **Site** in E2E Network.
	60 GHz cnWave External E2E Network	60 GHz cnWave devices are located within a **Network** deployed through the external E2E controller.
	60 GHz cnWave Onboard E2E Network	60 GHz cnWave devices are located within a **Network** deployed through the Onboard E2E controller.
	60 GHz cnWave PoP	PoP is mapped to a **Site** in E2E Network and deployed through the External E2E controller.
	60 GHz cnWave PoP Onboard E2E Network	PoP is mapped to a **Site** in E2E Network and deployed through the Onboard E2E controller.
	60 GHz cnWave Site	**Sites** are located within E2E Networks. A site maps to a single area and represents a location on a map that has 60 GHz cnWave devices.

Table 10: Structured hierarchy nodes

Icon	Name	Description
	cnMatrix	cnMatrix devices are located within a **Network**. Optionally they can also be mapped standalone to a **Tower** or to a **Site**.
	cnPilot Home	Wi-Fi devices are generally matched to a local SM and inherits its **Network**. They can also be mapped standalone to a **Network** or to a **Site**.
	cnRanger RRH	cnRanger RRH access points are located in a **Network** and are mapped to a **BBU**.
	cnRanger Sierra 800	cnRanger Sierra 800 are located in a **Network** and are optionally mapped to a **Tower**.
	cnRanger SM	cnRanger SM devices are located in a **Network** and are optionally mapped to a RRH.
	cnReach	cnReach device which could have zero, one, or two radios and support one or two roles, including Point-to-Point (PTP), Point-to-Multipoint (AP or EP) (PTMP), or IO Expander.
	cnVision Client	cnVision Client Subscriber Modules are located in a **Network** (if they are standalone, which is only used for bootstrapping) or they are associated with an AP. The SM will inherit the **Network** and **Tower** of the AP to which it is associated.
	cnVision Hub	cnVision Hub are located in a **Network** and are optionally mapped to a **Tower**.
	Enterprise Wi-Fi	Enterprise Wi-Fi devices are generally matched to a local SM and inherits its **Network**. They can also be mapped standalone to a **Network** or to a **Site**.
	Machfu	Machfu devices are located within a **Network**. Optionally they can also be mapped standalone to a **Network** or to a **Tower**.
	Network	All devices are placed within **Networks**. Networks represents the geographical regions or collections of devices with a shared responsibility. Accounts can have one network or many networks. Networks allow one to provide structure to accounts with many devices and also provides aggregation buckets for cnMaestro On-Premises statistics (essentially the system pre-calculates statistics, so they are displayed quickly).
	PMP AP	Point-to-Multipoint access points are located in a **Network** and are optionally mapped to a **Tower**.
	PMP SM	Point-to-Multipoint Subscriber Modules (SM) are located in a **Network** (if they are standalone, which is only used for bootstrapping) or they are associated with an AP. The SM will inherit the **Network** and **Tower** of the AP to which it is associated.
	PTP Master	Point-to-Point (PTP)Master device located in a network and optionally mapped to a Tower.

Table 10: Structured hierarchy nodes

Icon	Name	Description
	PTP Slave	Point-to-Point (PTP) Slave device located in a network and optionally mapped to a Tower.
	Site	**Sites** are located within networks and hold wireless access points. A site maps to a single area and represents a location on a map that has APs or a building.
	System	The **System** node is at the top-level of the hierarchy, though it does not have an explicit node in the tree. It's pages are displayed when the user logs in for the first time, when one selects the **System** button in the hierarchical tree (displayed when Networks are show), or selects the **System** node in the breadcrumbs. The System level aggregates data from all devices within the account.
	Tower	**Towers** are located within networks and hold cnRanger, PTP devices or Point-to-Multipoint APs. All the devices on a Tower are mapped to the same Network, and all their children devices such as Subscriber Modules or Home APs are also mapped to the same network.

Default network

cnMaestro On-Premises has a Default network into which unmapped devices will be placed. These can remain in the default network or moved to a named network. The Default network cannot be deleted, but it can be renamed.

Tree menu

Each node in the device tree has a menu icon (⋮) that supports node-specific actions. For example, the system node lets you **Add Network** or launch the **Update Software** page, while individual devices allow you to **Edit** their cnMaestro settings, **Reboot**, or even **Delete** the device from management (so it can be transferred to another account). The actions supported across the tree include the following:

Table 11: Tree menu

Action	Node	Description
All Devices		
Add Network	System	Add a new Network as a child to the System node.
Add Site	Network	Add a new Site as a child to the Network node.
Add Tower	Network	Add a new Tower as a child to the Network node.
Delete	Most Nodes	Delete a node from the tree. This is available for all nodes except System and the default network. Deleted devices will be removed entirely from the management system (along with their historical statistics). In order to delete a container, such as Network or Site, all nodes inside the container must be deleted first.
Edit	Most Nodes	Edit the cnMaestro settings, including node name and location. This is available for all nodes except System. For 60 GHz cnWave, edit option applies for E2E Network and nodes. Node name can be edited.

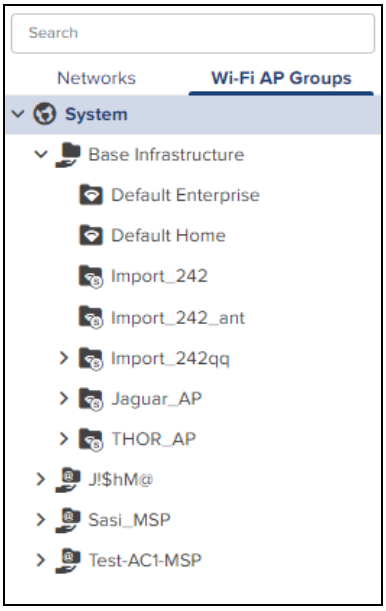
Table 11: Tree menu

Action	Node	Description
Flash LEDs	Enterprise Wi-Fi	The LEDs of the device enables to identify and locate the device.
Reboot	Devices	Reboot the device.
Refresh	All	Refresh the node in the tree. This refreshes the node and its children only, not the entire tree.
60 GHz cnWave Network		
Add Link	Network and Most Nodes	Add a new link to the System.
Add Node	Site	Add a new Node as a child to the Site.
Download PoP (s) Onboarding Config	Network and PoP Nodes	Download PoP(s) Onboarding Configuration data.
Hide or Show Sites		It allows to hide or show sites in E2E Controller Network tree menu.
Replace Node	CN/DN Nodes	Replace Node by changing the MAC address of th faulty node.
Sync Topology	Network	To sync the Topology of E2E Network.
Update Software	Network and Nodes	Allows the user to update the 60 GHz cnWave nodes software.

Wi-Fi AP Groups tab

The **Wi-Fi AP Groups** tab displays the Wi-Fi AP Groups configured in cnMaestro (and the devices mapped to them). AP Groups allow one to share configuration across many access points. They also display the aggregated statistics for the devices managed and present them within the AP Groups dashboard.

Figure 5 Wi-Fi AP Groups



Map navigation

Maps are presented in Main menu with dedicated Map display. Maps often show Towers and Devices located in proximity. You can double-click the map nodes to navigate to the Device, Site, or Tower. By selecting a node in the map, the Device tree gets updated to reflect that node.

Figure 6 Map navigation



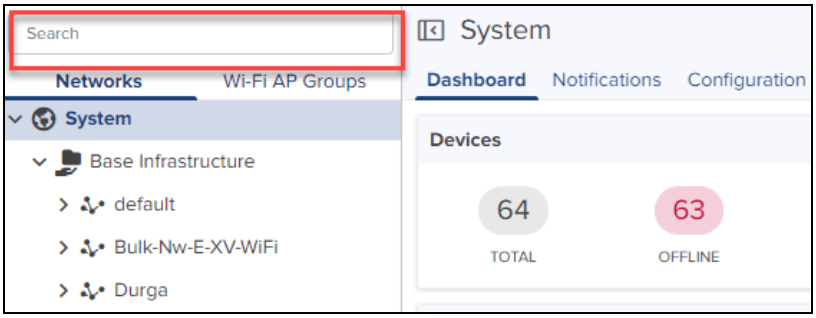
Table navigation

Some tables display **Networks**, **Towers**, **Site,** or **Devices** and allow the user to click the node and navigate to the location of the node in the tree.

Node search

Administrators can search for nodes within the device tree using the **Search** box. It allows the user to search based upon Device Name and MAC Address. Once the node is found and selected, one can navigate to it in the hierarchical tree.

Figure 7 Node search



Enterprise View

Overview

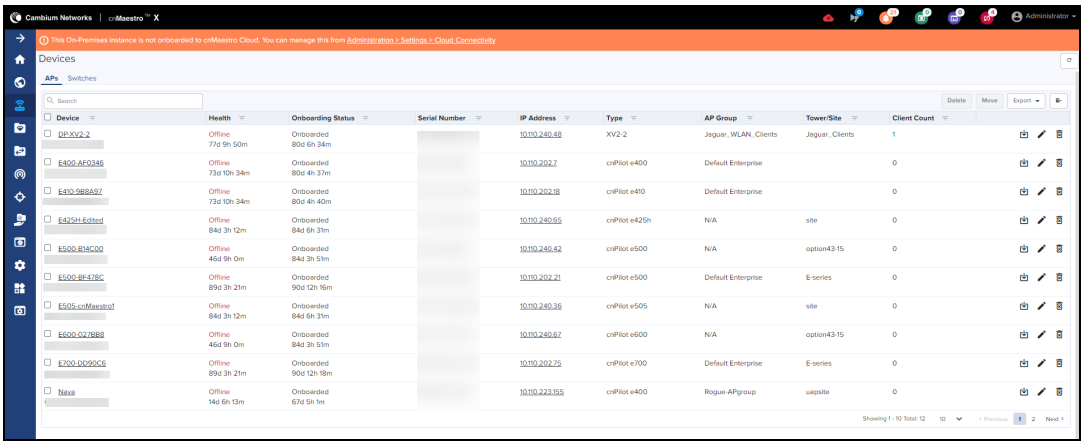
The Enterprise account differs from Access and Backhaul in that it is largely table-driven. It does not have the Quick Buttons or the Device Tree, instead, it has direct navigation for Devices, AP Groups, WLANs, Switch Groups, and Sites. Each of these is presented in tabular form.

System

Global functionality is presented in the System menu. It aggregates data across the entire installation.

Devices

The **Devices** section provides a searchable table listing all the devices in the system.



Selecting a device launches its management page.



AP groups and WLANs

AP Groups and WLANs manage shared configuration across APs. AP Groups also aggregate data for all the APs that map to them. This includes consolidating statistics and events/alarms and presenting AP Group-centered pages for Dashboard, Notifications, Configuration, Statistics, Report, Software Update, Clients, and Mesh Peers.

Figure 8 AP groups

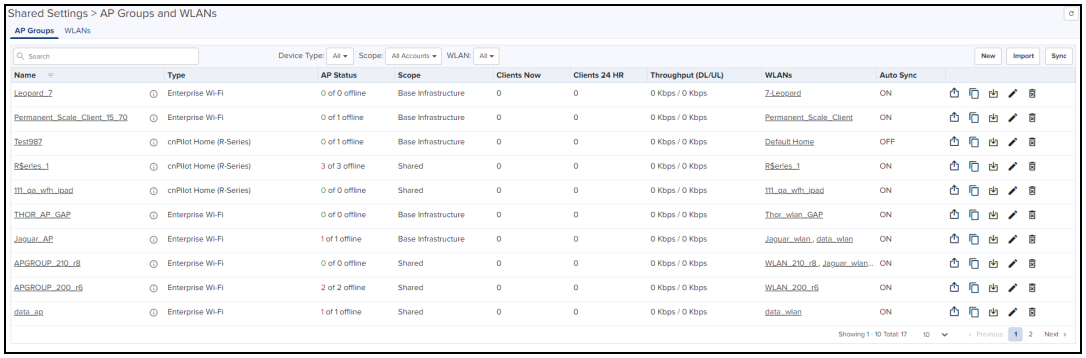
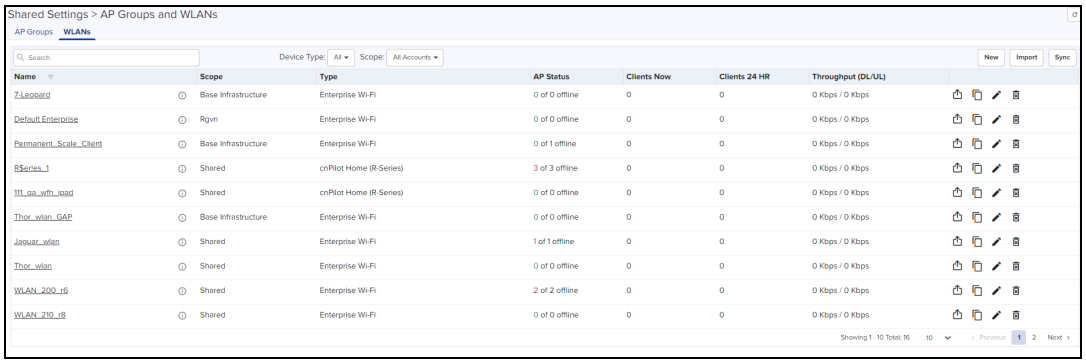


Figure 9 WLANs



Sites

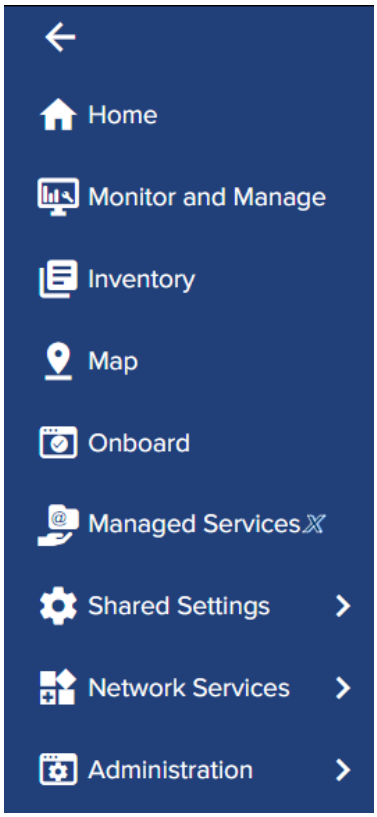
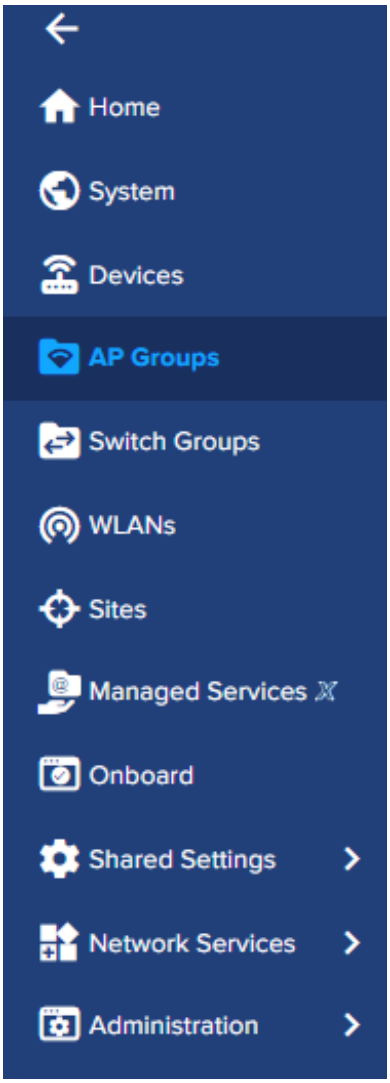
Sites are similar to AP Groups in that they aggregate statistics from many APs. The difference is a site represents APs installed at a single physical location (and mapped to a Floor Plan). Sites also have their own dashboard and aggregation pages.

Side menu

The side menu provides high-level navigation through the cnMaestro UI. You can expand or collapse the menu bar by clicking the arrow icon at the top.

The side menu for the **Access and Backhaul View** and **Industrial Internet** and **Enterprise View** is shown below:

Figure 10 Side menu

Side Menu for Access and Backhaul View and Industrial Internet	Side Menu for Enterprise View
	

Section tabs

All management sections are displayed in context of the managed item, including System, AP, AP Group, and Site. The options vary depends upon the items selected. A breakdown is below:

Table 12: Section tabs

Page	Tabs
System	Dashboard | Notifications | Configuration | Statistics | Report | Software Update | Clients| Map | Mesh Peers
Site	Dashboard | Notifications | Configuration | Statistics | Report | Floor Plan | APs | Clients | WIDS | Mesh Peers

System status

The UI header has the following System status icons.

Table 13: System status icons

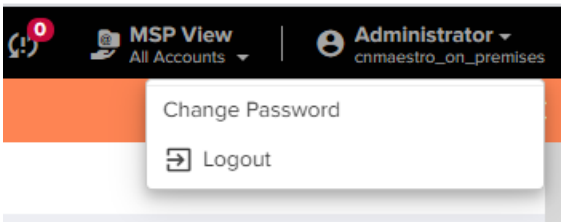
Icon	Name	Description
	Active Software Upgrade Jobs	The number of devices in the onboarding queue that are registered to the account but which need to be manually accepted prior to completing their onboarding.
	Announcements	If cnMaestro Cloud is synced with the On-Premises announcement notifies the latest Device Software images, Package, or OVA to upload from Cloud.
	Cloud Connectivity Status	It notifies that cnMaestro Cloud is Synced or not with the On-Premises.
	Critical Alarms	The count of critical alarms currently raised in the system (if no critical alarms are raised, then the major alarm count will be displayed).
	Devices Waiting for Approval	The count of jobs in the queue. It includes both running and pending jobs.
	Major Alarms	The count of major alarms currently raised in the system.
	Out-of-Sync Devices	The number of Wi-Fi devices with unsynchronized configuration (which can occur when automatic synchronization is disabled in the AP Group, or the configuration is changed directly on the device).

Clicking the icons directs the user to the relevant management page.

Logout

Log out of cnMaestro by clicking on the user icon in the upper-right corner and selecting **Logout.**

Figure 11 Logout



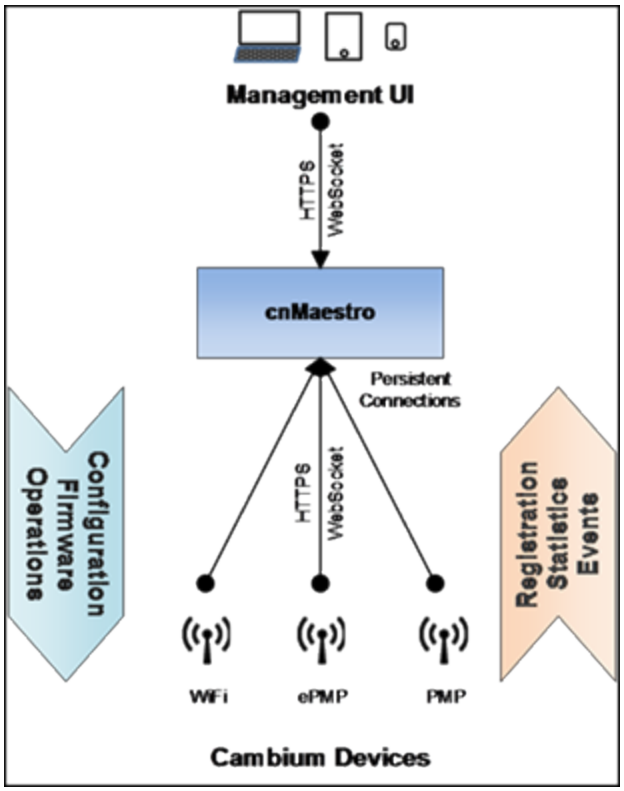
Architecture

Overview

The diagram below presents a simplified view of the cnMaestro architecture. Both devices and users contact cnMaestro over a secure HTTPS connection. The device connection uses WebSockets and is persistent. The device periodically sends data to cnMaestro (such as metrics and events), and cnMaestro directs the device to update configuration and software (among other operations).

In cnMaestro On-Premises, devices must be configured to contact the cnMaestro instance (by default, they access cloud.cambiumnetworks.com). This can be done either by configuring the device through its UI, or by setting DHCP Options (described in the Appendix).

Figure 12 On-Premises architecture



Networking

Most connection issues occur because the device is unable to contact cnMaestro. If devices do not enter the Onboarding Queue it may not be able to reach cnMaestro. Use the Ping and Traceroute tools on the device to troubleshoot.

NOTE:

1. Devices must have a route to the cnMaestro On-Premises server.
2. A static IP address or hostname for cnMaestro server, so it will persist over time.
3. An outbound connection from the device must be allowed for port 443.
4. An outbound connection will also be required for port 80 for legacy software on some devices. If your devices are running an image older than the one listed below, outbound connectivity over port 80 is needed for software update. The versions listed (and later) support port 443.

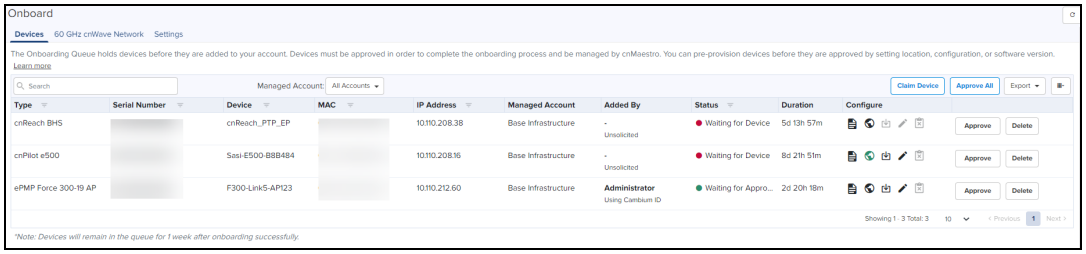
- 60 GHz cnWave (External Controller) 1.0.1
- 60 GHz cnWave (Onboard Controller) 1.0.1
- cnPilot E-Series / ePMP 1000 Hotspot: 3.2.1-r6
- cnPilot R-Series: 4.4.2-R2
- cnRanger 1.0.1.0-r1
- cnReach: All versions
- Enterprises Wi-Fi 6 APs: 6.0
- ePMP: 3.2
- PMP: 15.0.1
- PTP: All versions

Device Onboarding

Overview

By default, all devices contacting cnMaestro On-Premises will be placed in the Onboarding Queue, where they persist until Approved (after which they become Managed). The Onboarding Queue (**Onboard > Devices**) is shown below.

Figure 13 Onboarding Devices



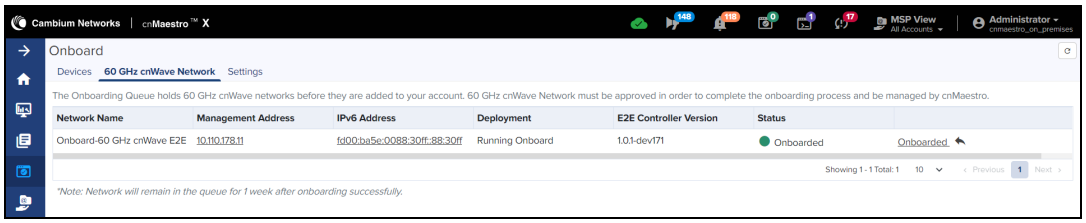
Onboarding devices is different between On-Premises and Cloud.

- In On-Premises, when a device contacts cnMaestro, it is placed in the Onboarding Queue by default, from which it can be approved into the account.
- In Cloud, the user needs to enter the serial number (MSN) of the device to claim it through the **cnMaestro UI**, or enter the Cambium ID and the Onboarding Key to claim it through the **Device UI**.

60 GHz E2E Controller Onboarding

The Onboarding Queue has a separate tab for 60 GHz cnWave E2E Networks. They must be approved by the user before they are added to cnMaestro and can manage 60 GHz cnWave devices. This approval can be done either by accessing through the **Onboard** page or **Tree** menu.

Once the onboarding process is approved the 60 GHz cnWave E2E Network (and its devices) can be managed by cnMaestro.



> **NOTE:**
> If **Auto Generate IPv6 Addresses** is enabled, E2E Controller fetches the IPv6 addresses automatically.

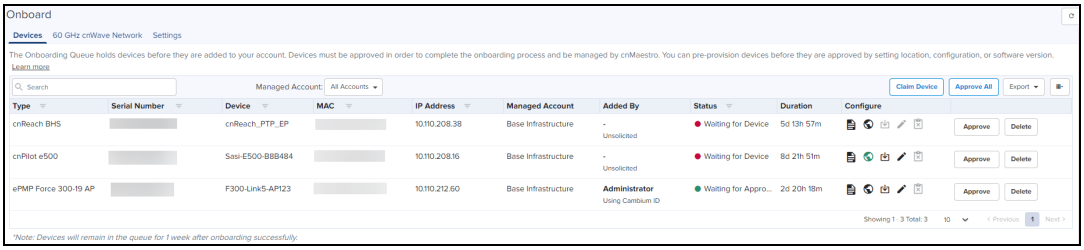
Refer 60 GHz E2E Controller Onboarding chapter for details on how to onboard E2E devices.

Pre-Configuration and Approval of Devices (Optional)

To preemptively configure and approve devices when they access cnMaestro, add the MAC address of the device to the **Onboard > Settings**. Adding devices here places them in the Onboarding Queue, where they can be pre-configured and/or pre-approved.

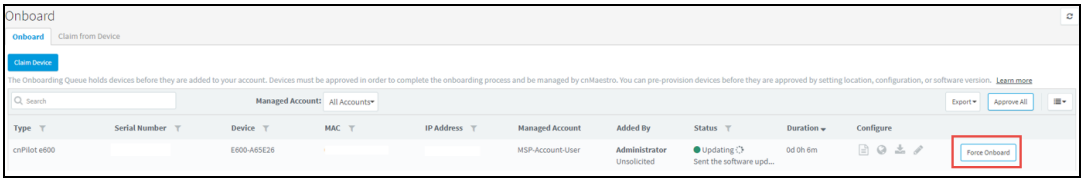
If this step is not done, the devices automatically show up in the Onboarding Queue, where they can be approved.

Figure 14 Pre-Configuration and Approval of Devices





NOTE:
If the device gets struck in the Onboarding Queue, the **Force Onboard** button will automatically enable. Click **Force Onboard** to onboard the device.



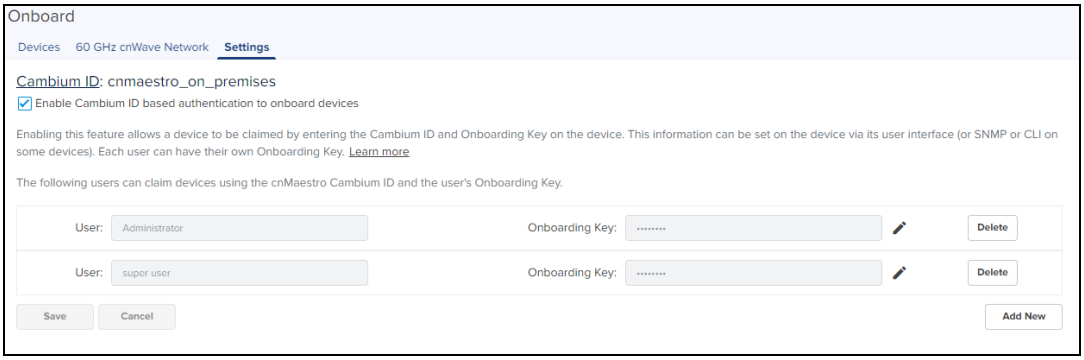
Device Authentication

To require devices to authenticate with cnMaestro before they are added to the Onboarding Queue, enable Cambium ID based authentication at **Onboard > Settings**. During configuration, the Onboarding Key must also be created. Each user can have their own Onboarding Key. The Onboarding Key needs to be entered into the Device UI before cnMaestro allows it into the Onboarding Queue.



NOTE:
When Cambium ID authentication is enabled, the Device UI requires both a Cambium ID and an Onboarding Key. For cnMaestro On-Premises, the Cambium ID is ignored. This mechanism is optional, and it should only be used to force device authentication before adding to the Onboarding Queue.

Figure 15 Device Authentication

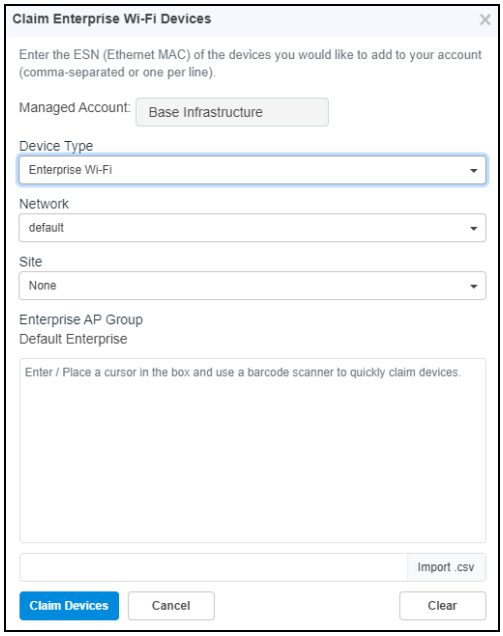


Claiming the Wi-Fi Devices from AP Group

To claim multiple devices from the AP Group, perform the following steps:

1. Navigate to the **Wi-Fi AP Groups** tree view and click the drop-down menu for the selected **AP Group**.
2. Click the **Claim Devices** option.

3. Select the **Device Type**, **Network** and **Site** under which these devices should be placed. By default, the devices claimed will have the configuration settings as the AP Group.



> **NOTE:**
> In Network and Site the **Search** option is enabled.

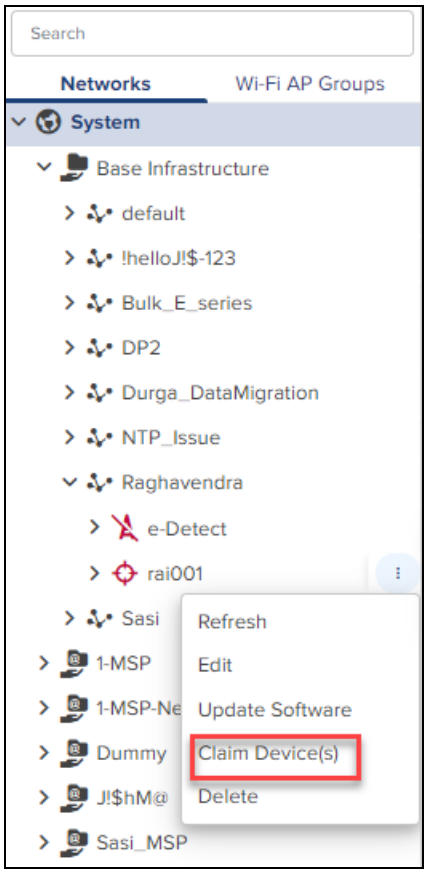
4. Specify the MAC Address of the devices line-by-line or comma-separated, or click **Import .csv** to import the MAC addresses of the device from a file.
5. Click **Claim Devices** to add to the selected AP Group with the configuration applied.

> **NOTE:**
> In cnMaestro Cloud the procedure is same as On-Premises, but instead of MAC Address, the user enters the MSN of the device.

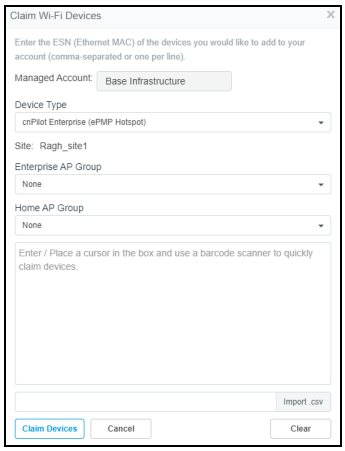
Claiming the Wi-Fi Devices from Site Dashboard

To claim multiple devices from the Site dashboard, perform the following steps:

1. Navigate to **Manage > Networks** tree view and select the drop-down menu for the Site.
2. Click **Claim Devices** from the drop-down.



3. Select the AP Group that should be applied for cnPilot E (Enterprise) and R (Home) devices. The devices claimed under the Site will have the configuration settings from the selected AP Group.



4. Specify the MAC Address of the devices line-by-line or comma-separated, or use the **Import .csv** option to import the MAC of the devices from a file.
5. Click **Claim Devices** to add the devices to the selected AP Group and **Apply Configuration**.

	NOTE: In cnMaestro Cloud, the procedure is the same as On-Premises, but instead of MAC Address the user should use the MSN of the device.

60 GHz E2E Controller Onboarding

Overview

There are two ways to deploy 60 GHz E2E Controller:

- External E2E Controller
- Onboard E2E Controller

External E2E Controller

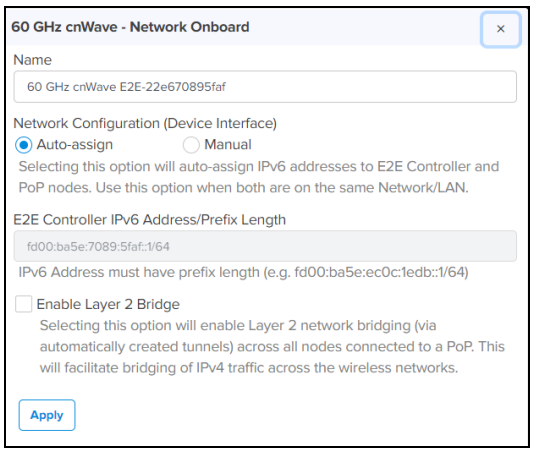
External E2E Controller is an OVA file which can be deployed in ESXi or VMware. The External E2E Controller discovers cnMaestro after it is deployed and ready.

The E2E Controller will also be placed in the **Tree** prior to approval (in addition to the Onboarding Queue). To Onboard the E2E Controller Network through the **Tree**, perform the following steps:

1. Navigate to the Controller in the tree and select the **Monitor and Manage** tab.
2. Click **Approve.**



60 GHz cnWave – Network Onboard window pops up.

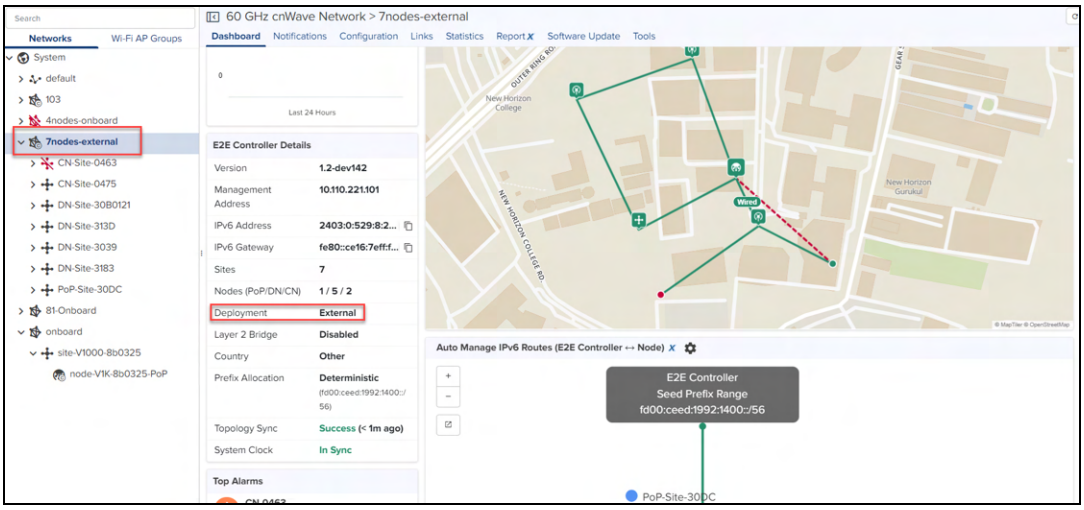


3. By default **Auto-assign** is selected however, the user can select **Auto-assign** or **Manual** to update the IPv6 address in the E2E Network. It takes a while for the IPv6 address to update (after which, the user can optionally **Enable Layer 2 Bridge**).
4. Click **Apply.**

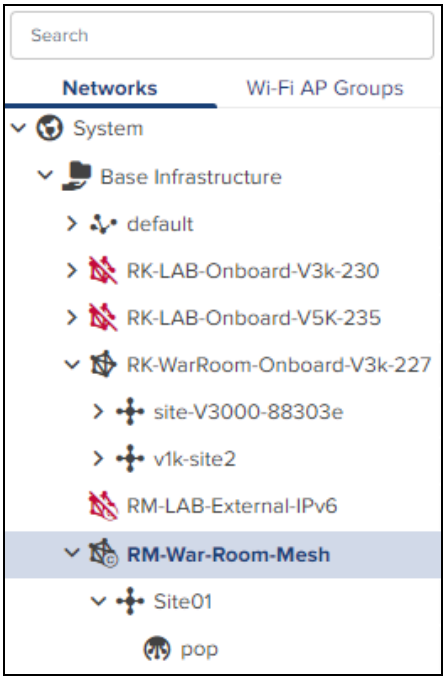
5. Wait until the network onboard completes.



6. E2E Network **Dashboard** in cnMaestro is shown below:



External E2E Controller network icon will be displayed .



Onboarding E2E Controller

The Onboard E2E Controller is hosted on a 60Hz cnWave device. (E2E Controller option to be enabled in the device UI).

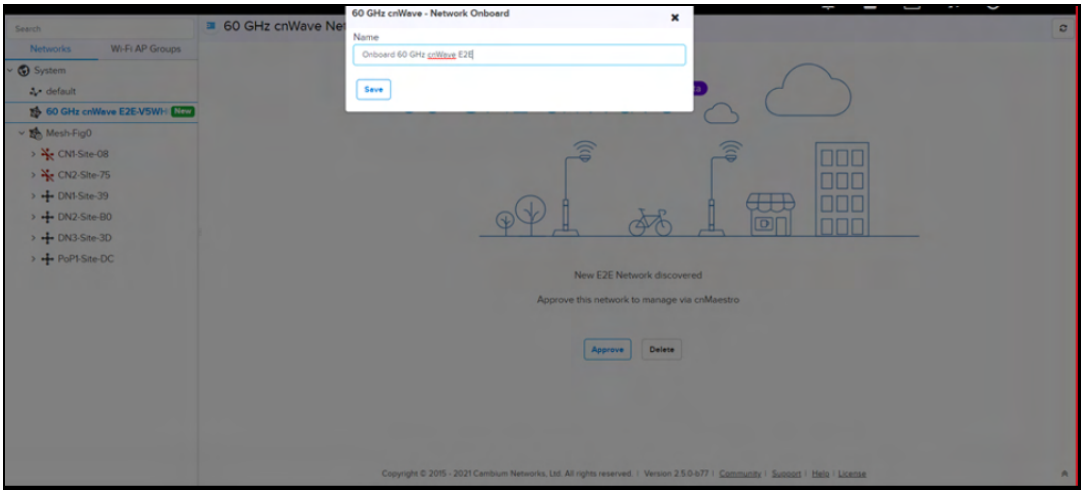
To approve, proceed as follows:

1. Navigate to **Manage > Network >** select **60 GHz cnWave E2E Network.**
2. Click **Approve.**

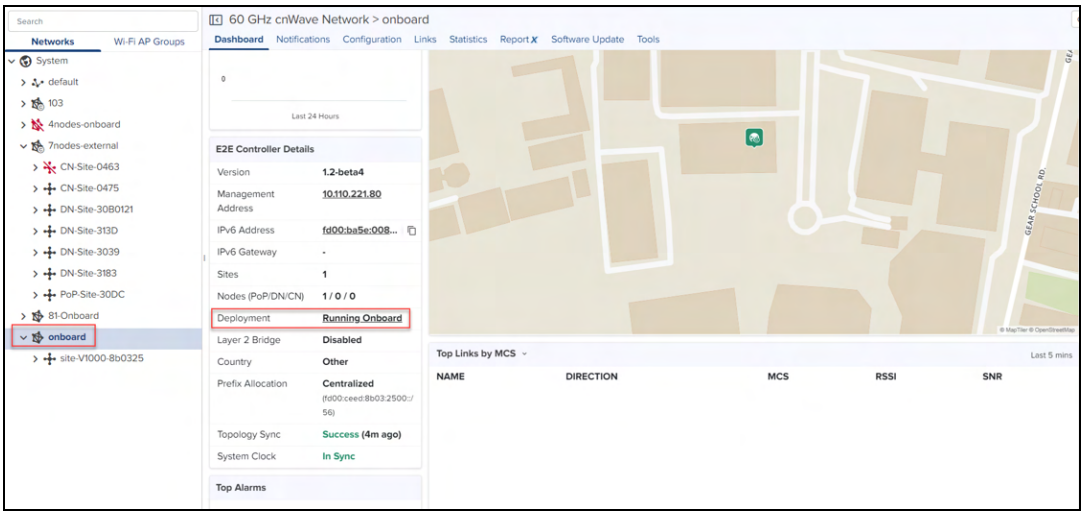


60 GHz cnWave-Network Onboard window pops up and provides option to **Edit** Network name.

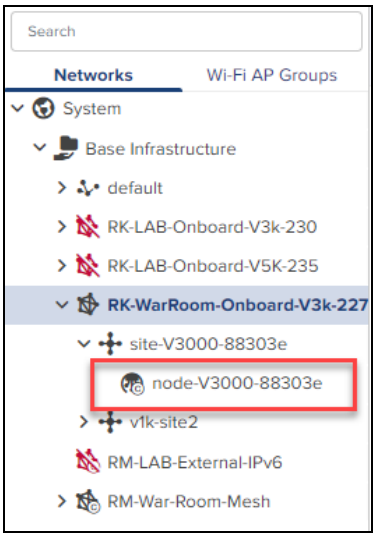
3. Click **Save**.



4. After the successful Onboard E2E Network, it can be managed through cnMaestro. The E2E Network **Dashboard** for an Onboard Controller is shown below:



If PoP Node is running the Onboard E2E Controller then, the PoP icon will be indicated with as shown below:


Search
Networks
Wi-Fi AP Groups
System
Base Infrastructure
default
RK-LAB-Onboard-V3k-230
RK-LAB-Onboard-V5K-235
RK-WarRoom-Onboard-V3k-227
site-V3000-88303e
node-V3000-88303e
v1k-site2
RM-LAB-External-IPv6
RM-War-Room-Mesh

High Availability (HA)

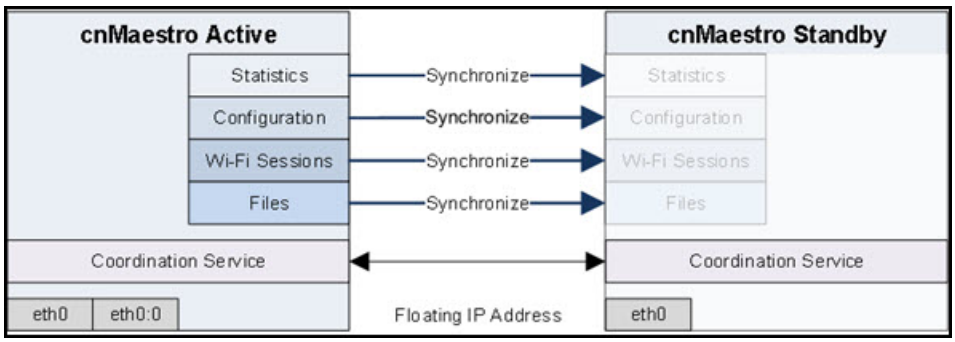
This section includes the following topics:

- Overview
- HA Cluster Setup
- HA Menu

Overview

cnMaestro On-Premises supports Layer 2 HA through an active-standby (1+1) architecture. The default HA installation has a single management interface (eth0) and a shared (floating) management IP address. The basic deployment is highlighted below:

Figure 16 Overview of High Availability



Primary vs Secondary

The Primary server always has up-to-date configuration and data, and it hosts the cnMaestro application. The Secondary replicates data from the Primary and enters standby state when fully synchronized.

Shared (Floating) IP Address

A Shared IP address is used to access the cnMaestro application. It is configured in devices or typed into a Web browser to launch the cnMaestro UI. Since the shared IP migrates between the two installations, it must be on the same subnet as both static IPs.

Network Ports

The following ports/protocols must be accessible between the two systems:

Ports	IP Type	Details
22	TCP	Data Replication
8300	TCP	Distributed Synchronization
8301	TCP, UDP	Distributed Synchronization

Recommendations

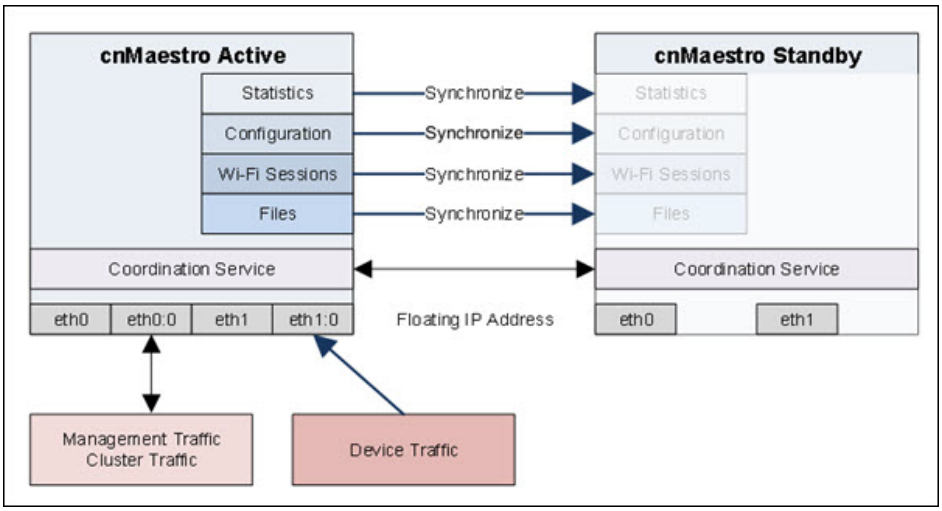
Cambium Networks recommends backing up virtual machines prior to starting HA. To take daily automated backups of cnMaestro configuration, navigate to **Administration > Server > System Backup and Restore**. For larger installations, and to backup statistics, refer section on backing up the data disk.

Dual Interfaces

cnMaestro can be configured with two interfaces, eth0 and eth1, on VMware workstation and ESXi. These allows traffic to be segmented into Management/Cluster and Device/Control. Starting with 3.1.0 release, this traffic separation will be strictly enforced. The implementation allows deployments with separate management and control subnets to integrate more easily with cnMaestro.

Traffic Type	Interface	Details
Management/Cluster	eth0	User interface, Cluster, API, outbound traffic to Internet
Device/Control	eth1	Device control traffic

A high-level overview of the separation is below:



Add eth1 Network Adapter

To add eth1, the virtual machine needs to be stopped, and a second Network Adapter added manually. Adding multiple adapters to a virtual machine leads to issues with PCI ordering, which determines how eth0 and eth1 are mapped to the running VM: the PCI ordering does not necessarily follow the order of interface addition. The section below details how to make sure the PCI ordering is correct.

Network Interface PCI Ordering

In a two-interface configuration, VMware may apply Network Interfaces in an order different than that presented in the UI. This may result in a second interface mapped to eth0 instead of eth1. In order to resolve this, you may need to update VMware configuration.

VMware Workstation

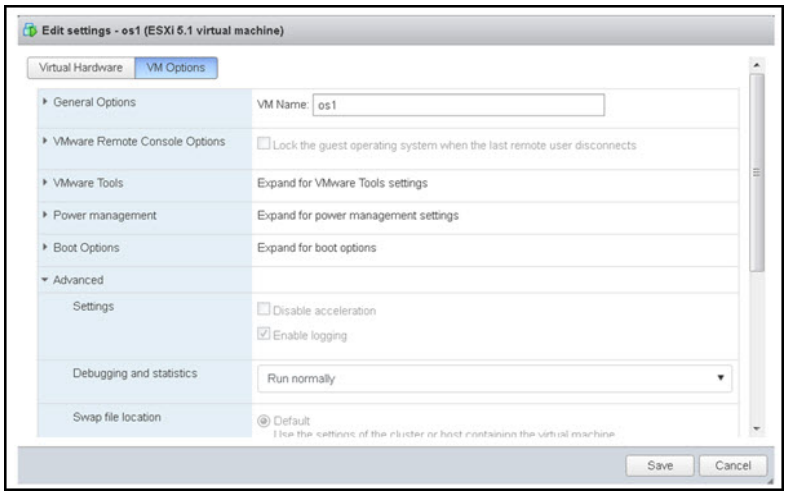
In VMware Workstation, edit the configuration file (ending in .vmx) in the virtual machine home directory. After shutting down the VM, change the following two entries, so the eth0 PCI number is lower than eth1.

```
ethernet0.pciSlotNumber = "33"
ethernet1.pciSlotNumber = "34"
```

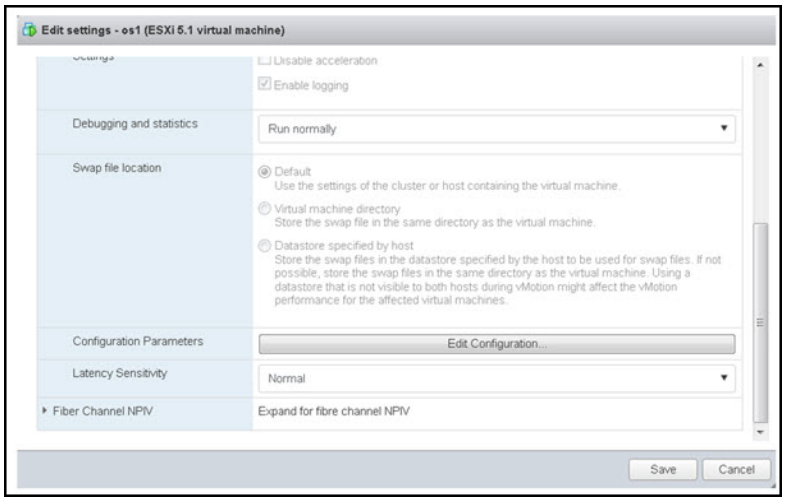
VMware ESXi

The same operation is required for VMware ESXi, but it can be performed through the UI.

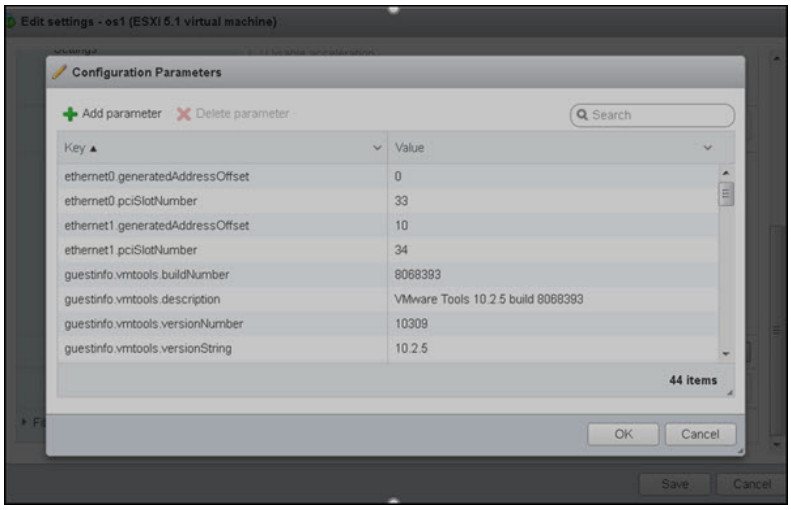
1. Select **Edit Settings** of the VM and choose **VM Options > Advanced**.



2. Scroll down and select **Edit Configuration**.



This launches a screen that allows updating the PCI numbers.



HA Cluster Setup

HA Cluster Setup requires bootstrapping the Primary system and then adding the Secondary. The high-level steps are defined below. All cluster operations are performed through the cnMaestro Console.

Bootstrap (Primary)

The first step is to enable high availability on a cnMaestro instance – effectively creating a HA cluster and initializing high availability processes. The bootstrapped instance is called the Primary, and it hosts the shared IP address.

Accept (Primary)

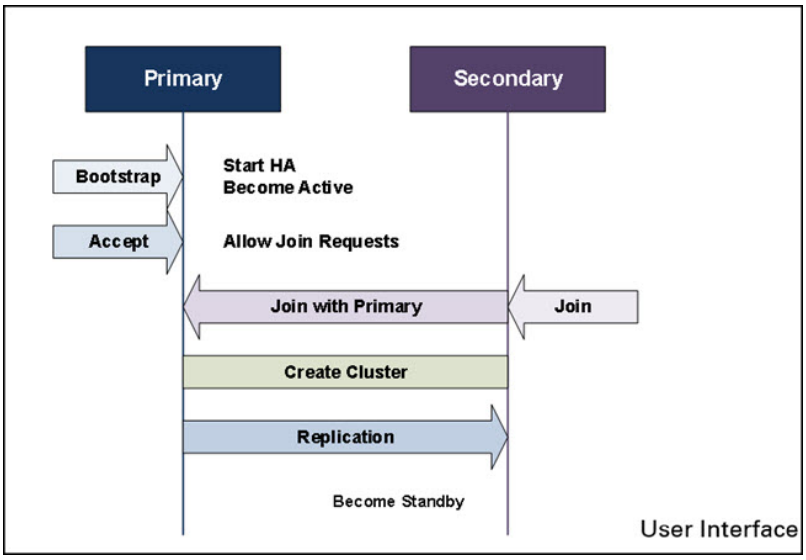
The Primary server then configures a shared secret to allow a Secondary system to join the cluster. The secret is used for authentication, and it is valid for 30 minutes.

Join (Secondary)

The Secondary joins the Primary using the shared secret, and extends the Cluster. At this point, the Secondary begins replicating data (which could take many minutes). Once fully replicated, the Secondary becomes standby and is able to fail-over.

	NOTE: The Join process uses SSH (port 22) to connect to the Primary. It is important to review the fingerprint displayed during the Accept and Join operations, to make sure they are the same (and protect against man-in-the-middle attacks).
	WARNING: All data on the Secondary will be overwritten during the operation.

Figure 17 Accept Join

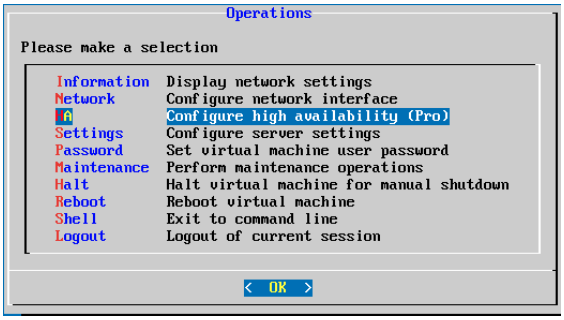


Basic HA Cluster Creation Flow

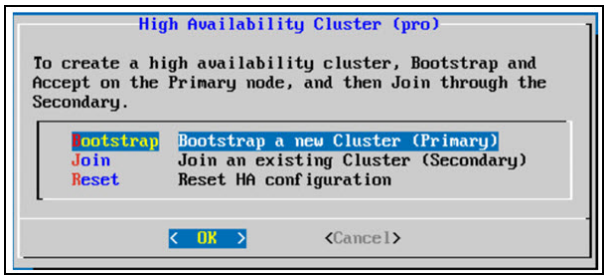
A general HA configuration flow is presented below. Each page will be discussed independently in later sections.

Primary Server

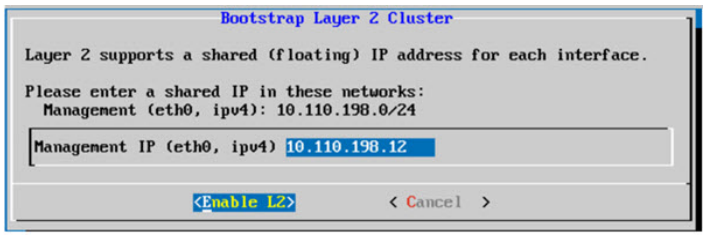
1. After logging into cnMaestro console, from **Operations** tab, select **HA** and click **OK**.



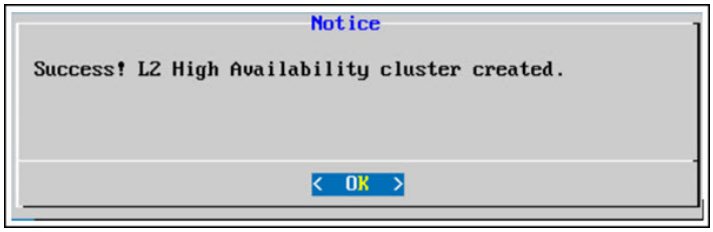
2. From **High Availability Cluster** tab, select **Bootstrap** and click **OK**.



3. From the **Bootstrap Layer 2 Cluster** tab, enter **Management IP** and click **Enable L2**. The Management IP must be on the same subnet as the eth0 interface.



L2 High Availability Cluster is created, success window pops up as shown below.



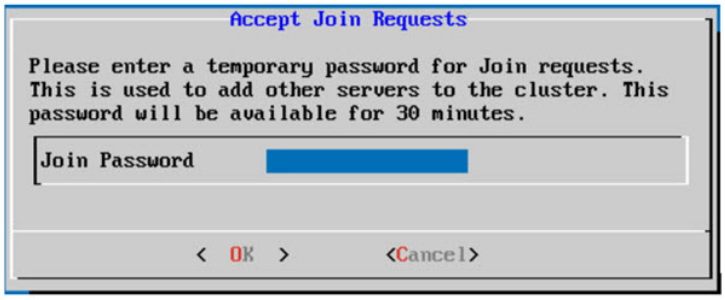
The Primary Bootstrap is successfully completed.

4. Click **OK**.

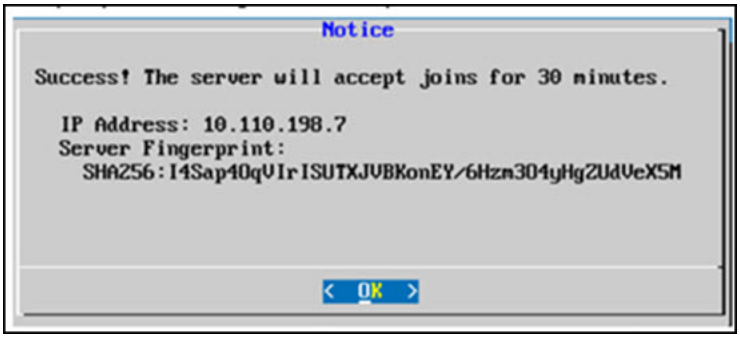
Accept Join Requests page displays.

5. Enter a temporary password for Join requests.

This password is used by the Secondary system to authenticate and join, the Cluster. It is valid for 30 minutes.

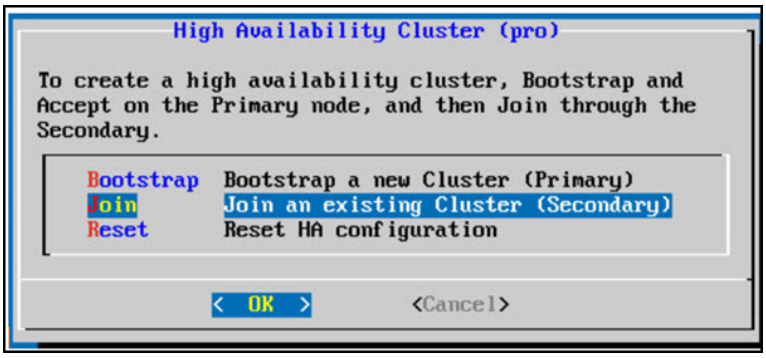


6. After the **Join Password** is set, click **OK** to initialize the system for 30 minutes.
7. A SSH Fingerprint is generated. Match the fingerprint to the one displayed during the Join process.

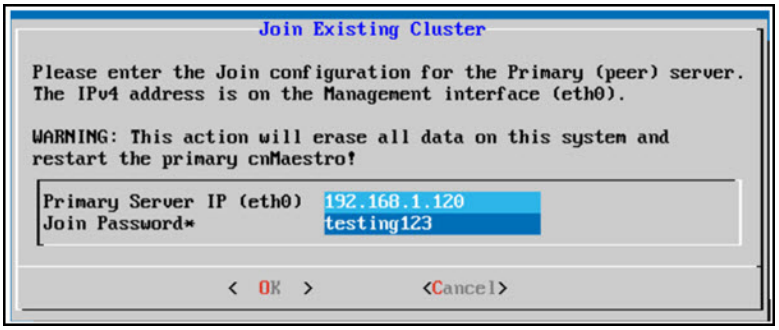


Secondary Server

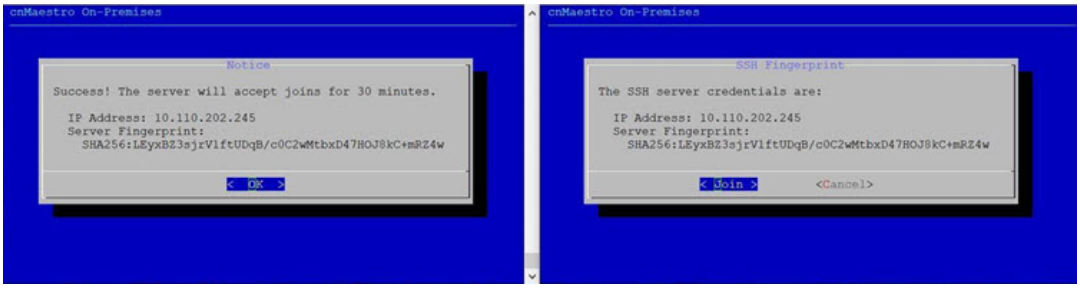
1. On the Secondary cnMaestro server, from the **High Availability Cluster** menu, select **Join** and click **OK**.



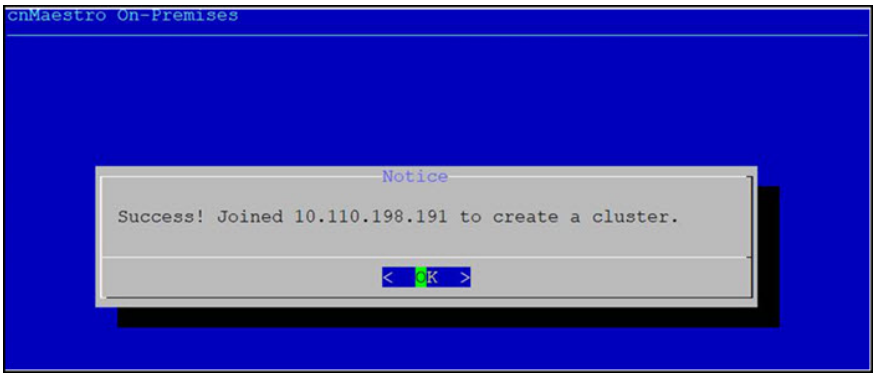
2. **Join Existing Cluster** window appears. Enter the **Primary Server IP (eth0)** and the **Join Password**, click **OK**.



A pop-up window displays the fingerprint of the Primary server. Validate the fingerprint shown on the Secondary exactly matches the fingerprint of the Primary (when it is accessed directly). If the fingerprints are different, the Primary server is incorrect, and the Join should be cancelled.



3. After verifying and continuing, the successfully joined cluster window appears.

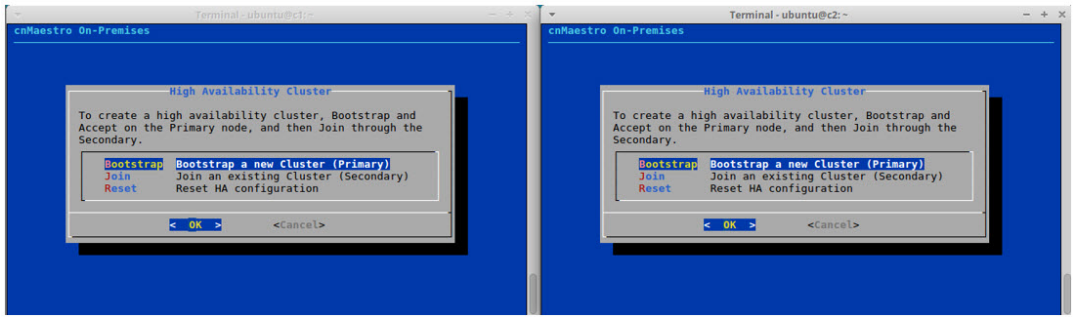


HA Menu

This section walks through the different HA tabs available in the console.

High Availability Cluster Menu (Pre-Bootstrap)

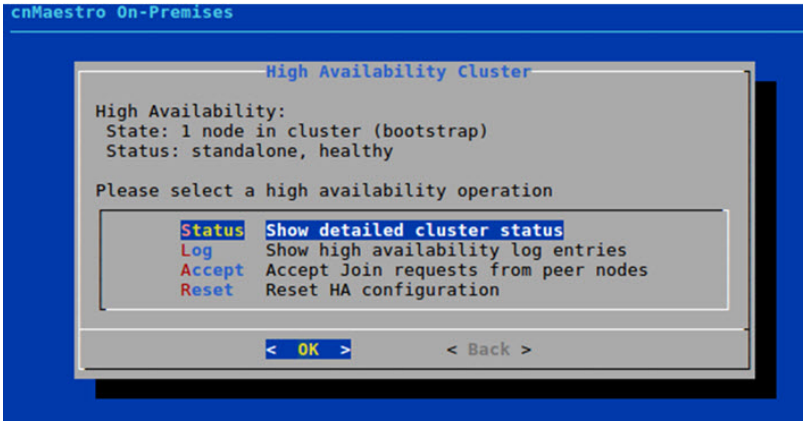
This menu is available before HA is enabled and the cluster has been created.



Field	Description
Bootstrap	Convert into a standalone HA Cluster.
Join	Join a standalone HA Cluster to create a replication Cluster.
Reset	Reset HA infrastructure to default. This option is provided as a failsafe.

High Availability Menu (Post-Bootstrap)

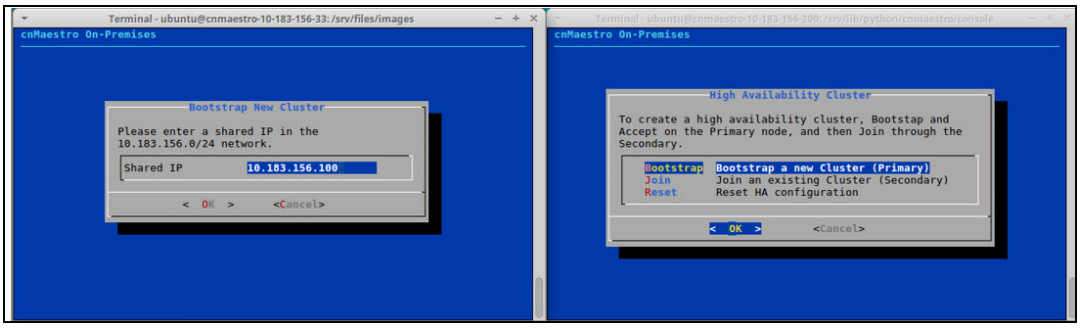
This menu is available after a successful Bootstrap.



Field	Description
Accept	Join requests from the peer nodes.
Log	Log entries of High Availability.
Reset	Reset HA configuration.
Status	Overall status for the Cluster.

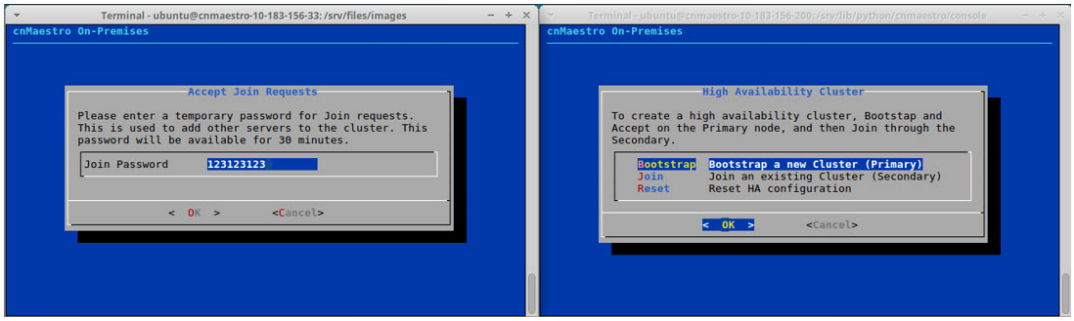
New Cluster

An HA Cluster requires the eth0 interface be configured with a static IP address. Once the Cluster is created, the IP address cannot be changed without dissolving the Cluster. During the bootstrap process, a shared IP address is configured in the same subnet as eth0. This address floats between the active cnMaestro system, and it should be used for cnMaestro access.



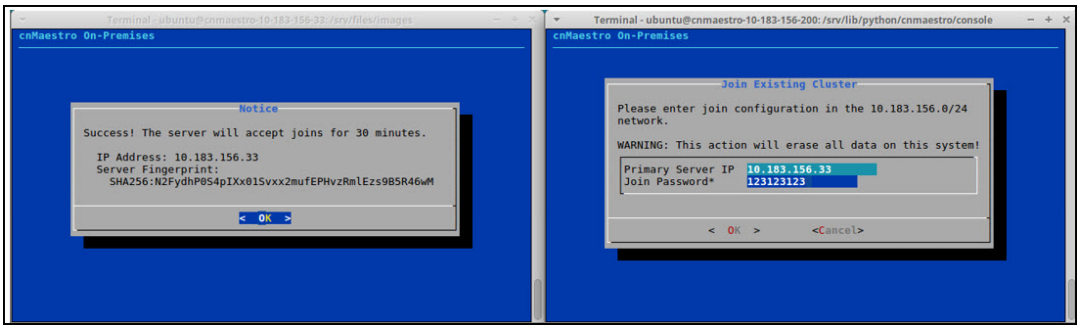
Accept Join Requests

As part of the Bootstrap process, create a shared password used during the Join. The password will be available for 30 minutes after creation.



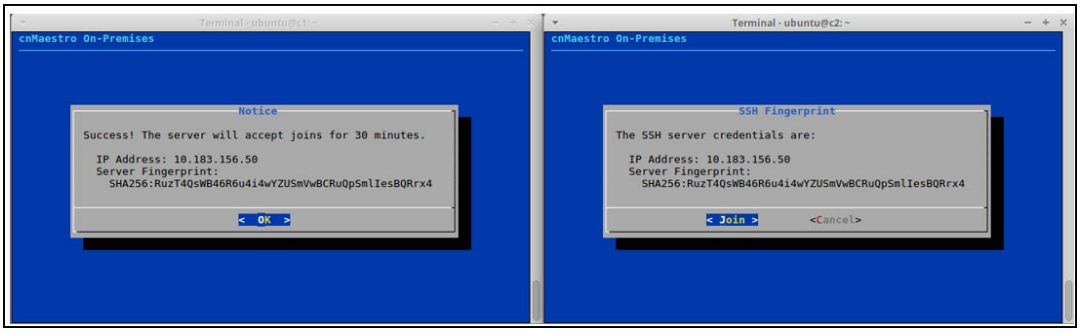
Join Existing Cluster

To join another system to the Cluster, select the Join option of the HA menu on the Secondary Server. The IP address is the eth0 address for the Primary server (only the eth0 IPv4 address is used to create a cluster). The Password is the same created during Accept.



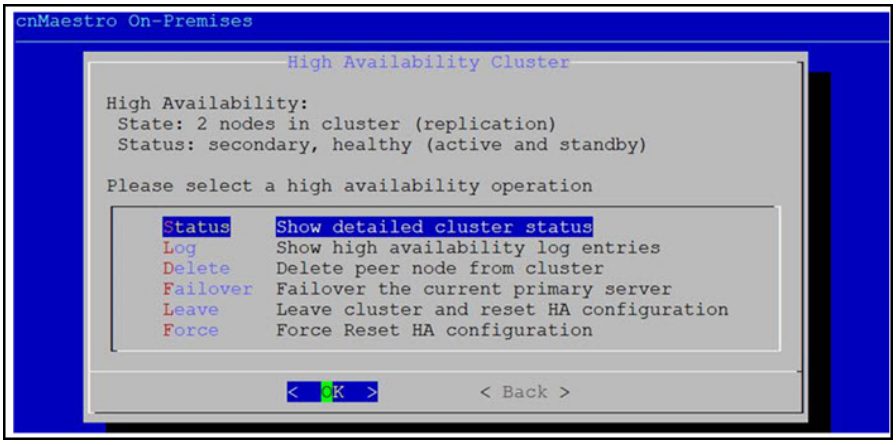
Validate SSH Fingerprints

Customers should validate the fingerprint before joining. If the fingerprint on the Primary is different than the fingerprint displayed at the Secondary, the Join should be cancelled, because the Primary server is incorrect. In the graphic below, the Primary server is on the left, and the Secondary server is on the right.



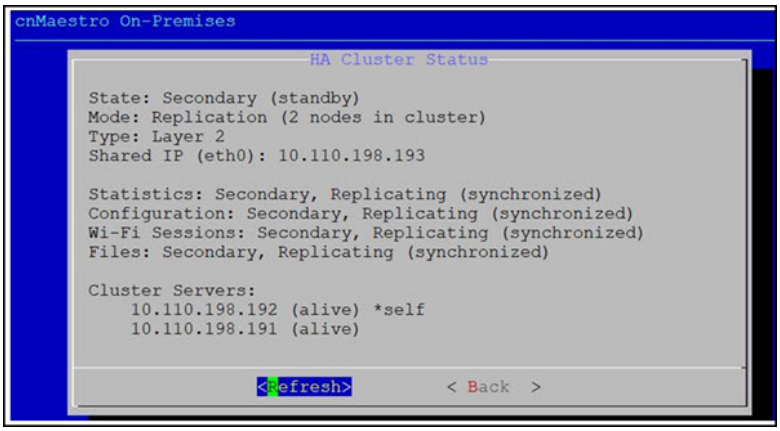
HA Cluster Status

The HA Cluster Status tab details the current HA state, including the replication status. After a cluster operation, it may take a few minutes for the page to show full details.

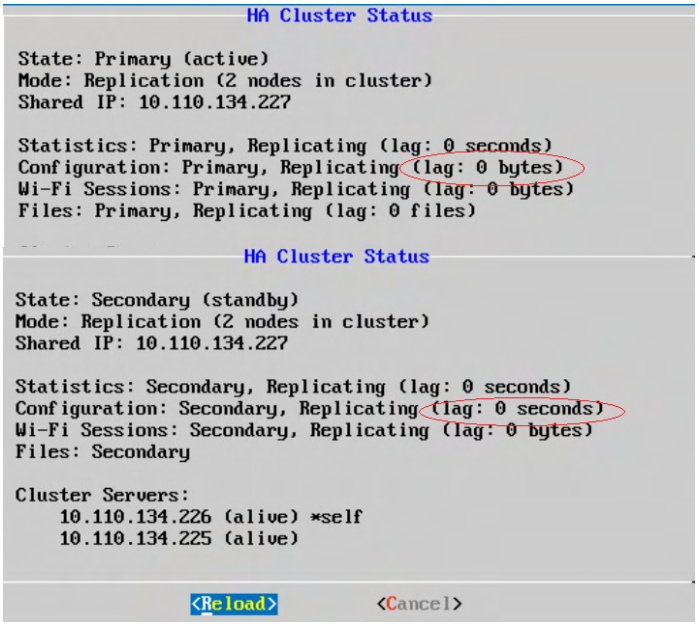


Field	Description
Accept	Set a password used by another system to join the Cluster.
Delete	Delete a node from the Cluster.
Failover	Failover to the current Standby node. This is not visible while standalone.
Force/Reset	Forcibly Reset HA configuration. This causes a non-graceful reset of the current node, and it does not delete the node from the Peer. This operation should only be used if the Leave operation fails.
Leave	Leave the Cluster. This deletes all HA configuration and puts the device into a default state.
Status	Overall status for the Cluster.

Select **Status** and click **OK**. The following window appears:



Field	Description
Configuration	Status of configuration replication.
Files	Status of file system replication (including floor maps, etc.).
Statistics	Status of statistics data replication (this tends to take the longest).
Wi-Fi Sessions	Status of Wi-Fi session replication.



	NOTE: There may be discrepancy in the Primary and Secondary lag values it may display the results in bytes or seconds.

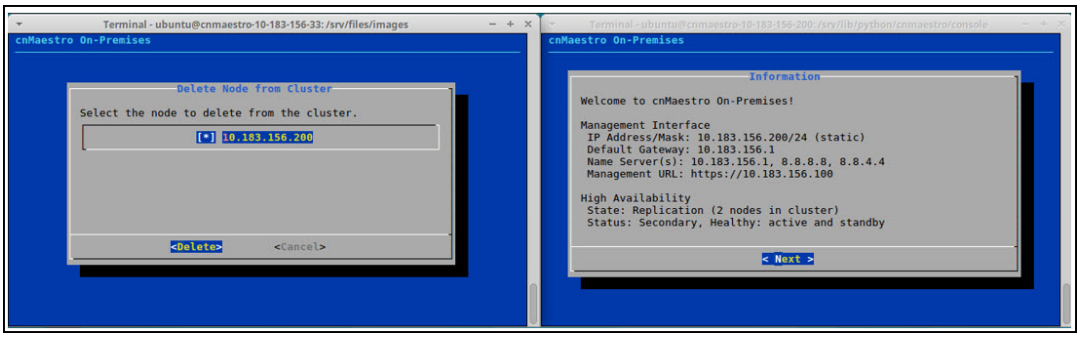
Delete Node

Delete from Cluster

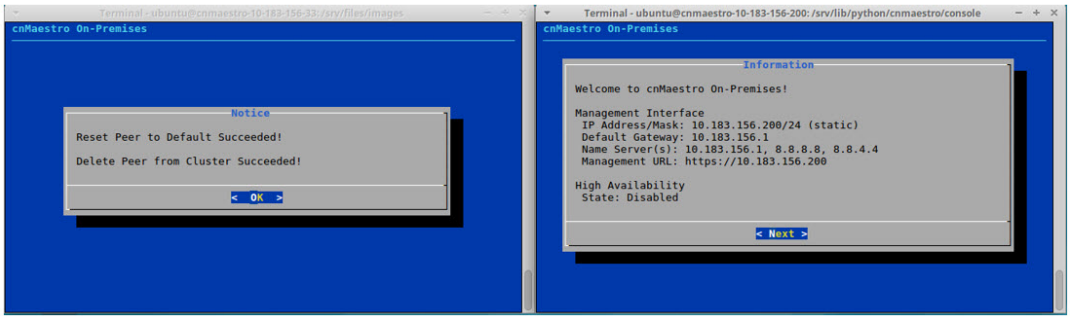
Deleting removes the peer node from the cluster. Navigate to **Operations > HA**, select **Delete** and click **OK**.

Use the space bar to select the Node and select **Delete** and click **Enter**.

Deleting a Node Resets the HA configuration of the node and removes it from the Cluster (as long as the node is still online). If the node is down, or unresponsive, it needs to be manually removed by accessing the node itself and selecting **Leave**.



After deletion, HA has been reset on the deleted node, and the current node becomes Standalone.



	NOTE: After node deletion, it is recommended to perform Force/Reset operation under HA menu.

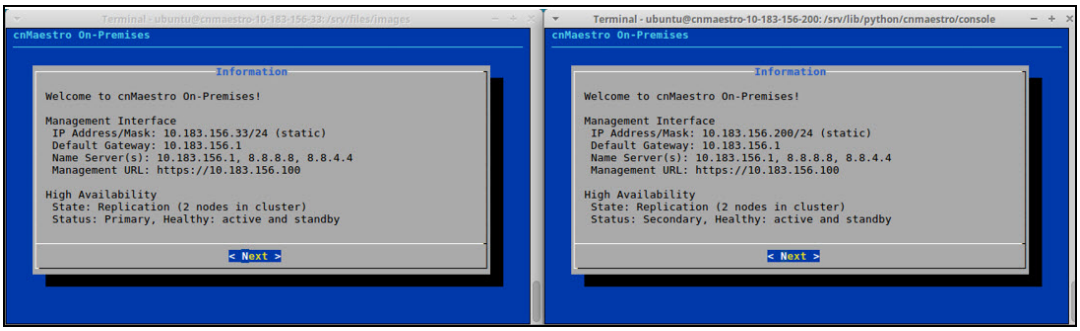
Leave Cluster

Leaving removes the current node from the cluster. It first tries to delete the node from the peer; then it resets the current node to default. If the delete fails (for example, if there is no network connectivity), it needs to also be deleted manually through the peer Console.

	NOTE: After cluster deletion, it is recommended to perform Force/Reset operation under HA menu.

Information

The Information page provides global status for the system at initial login. It has a High Availability section at the bottom.



Behaviour of cnMaestro features when HA is Enabled

This section lists the behavioral changes of cnMaestro features when HA is enabled:

Feature	Observations	
Device Approval from Onboarding Queue	If the fail over happens when Device Approval is In-Progress, then the **Device Approval** will get struck. You have to re-initiate the **Approval All**	
Software Update Jobs	If the fail over happens when the Software Update job is **In-Progress**, then the devices software update will be Timeout after fail over.	
	Software Update break up	**Impact after failover**
	Software update to 50 devices with **Devices to update in parallel** set as 10	10 devices which were in parallel updated will get impacted. After failover job will get timed out after 5 minutes. You have to retrigger software update for these 10 devices
	Software update to 50 devices with **Devices to update in parallel** set as 50	All 50 devices which were in parallel update will get impacted. After failover job will get timed out after 5 minutes.You have to retrigger software update for 50 these devices.
Configuration push jobs in running state	If the fail over happens when the Configuration Update is **In-Progress**, then the configuration update will be Timeout.	
	Configuration update to 50 devices with **Devices to update in parallel** set to 10	10 devices which were in parallel update will get impacted. After fail over job will get Time out after 5 minutes. You have to retrigger Config update for these 10 devices.
	Configuration update to 50 devices with **Devices to update in parallel** set to 50	50 devices which were in parallel update will get impacted. After fail over job will get Time out after 5 minutes. You have to retrigger Config update for these 50 devices.
OVA Upgrade	If failover happens when the OVA upgrade is in progress, then you have to re-intiate OVA upgrade	
	OVA upgrade	**Impact after failover**
	Failover happens during OVA file upload	File upload is canceled. You have to retrigger it

Feature	Observations	
	Failover happens during 10% to 100% OVA upgrade	OVA upgrade is canceled You have to retrigger it
	Failover happens after 100% of OVA upgrade and before **Apply**	File upload is canceled. You have to retrigger it
	Failover happens during 10% to 100% OVA upgrade	OVA upgrade is canceled You have to retrigger it

Monitoring

This section includes the following topics:

- Network Monitoring
- cnPilot Dashboard
- Inventory
- Reports

Network Monitoring

The Monitoring tab displays the monitoring panel for cnMaestro On-Premises. This includes the following sections:

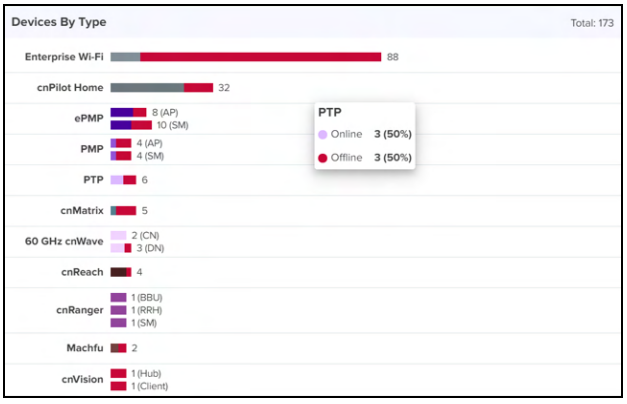
- Dashboard
- Notifications
- Statistics and Details
- Performance
- Maps
- Tools
- WIDS

Dashboard

Dashboard pages are customized for each device type and aggregation level (such as System, Network, Tower, and Site). Pages representing devices provide information on location, significant configuration parameters, and performance. System, Network, Tower, and Site nodes aggregates dashboard data for the devices they contain.

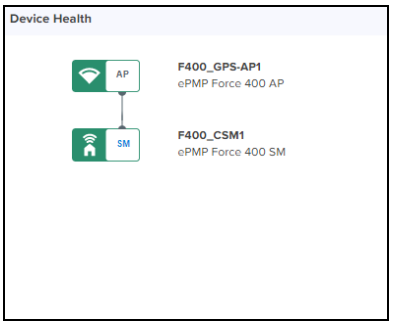
KPI (Key Performance Indicators)

Each page has a set of KPIs tailored to the node type. These displays a current value and often historical trend data.



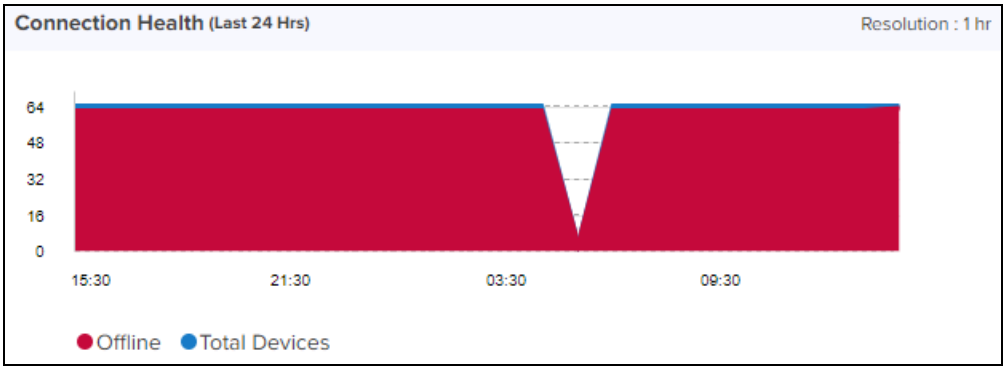
Device Health

Device Health displays the health of the network from the tower to the edge Device Health.



Connection Health

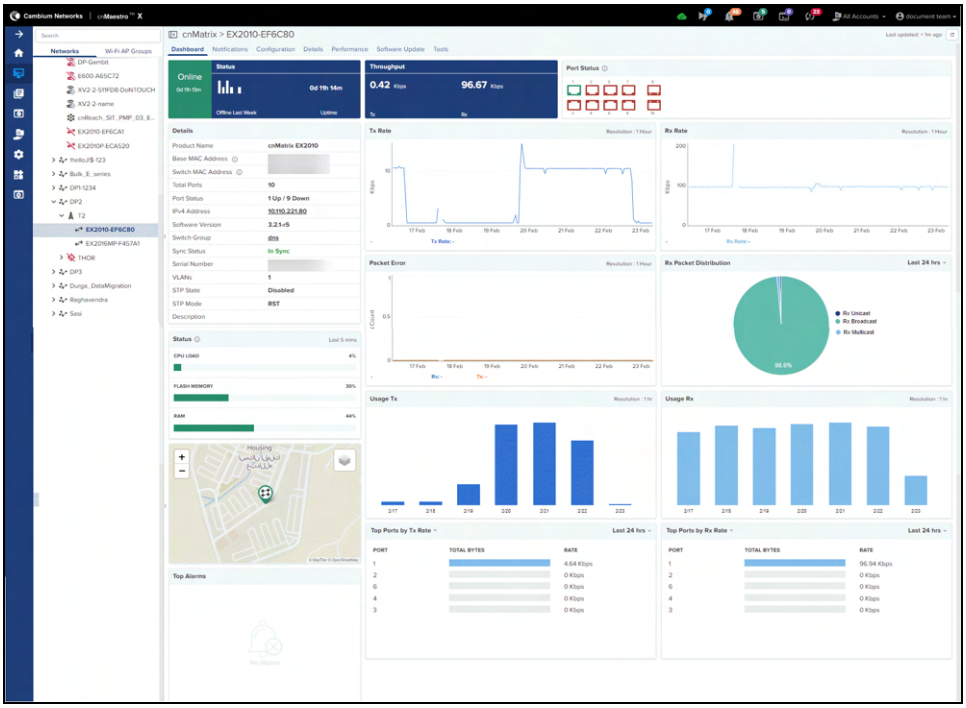
Connection Health displays the health of the devices connected to the network.



Charts and Graphs

Contextual charts and graphs provides details on important dashboard metrics.

Figure 18 Charts and Graphs



Notifications

Overview

Notifications consist of Events, Alarm History, and Alarms. They are asynchronous messages that provides real-time system status.

Table 14: Notification Overview

Type	Description
Alarms	Alarms have state and persist as long as the problematic activity continues; they reflect the current health of the devices in the network. **NOTE:** After every server reboot or restart, alarm displays as shown below: • cnMaestro takes up to 10 minutes to reflect the alarm count. • Email Notification subscribers status up and down major alarms is blocked for 30 minutes. • Webhooks will not send the device status up and down major alarms for next 30 minutes.
Alarm History	Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts.
Events	Events are stateless, transient messages that occur in response to an input or action, such as the CPU exceeds a threshold or a device association fails. Events are fire-and-forget; they are stored in an Event Table and provide a history of device activity.

Event/Alarm Source

Identity of the source device for the event or alarm.

Aggregation

Notifications are visible at every level of the device tree. Higher levels consolidate notifications for all devices at lower levels in the hierarchy. For example, the network level displays the events and alarms for all devices within that network. This aggregation is only available for System, Networks, Towers, and Sites. When a device is selected, such as an AP, the notifications will only be for it, and not its associated SMs (even though they are lower in the tree).

Storage

Events and Alarms are stored in cnMaestro for an extended period. They will be removed when the total count for each across the account surpasses 1,000 multiplied by the number of devices in the account. The oldest entries will be cleared first.

Events

The Event Table stores a history of the most recent events for the selected node.

Event Severity

Event Severity is mapped to the following levels:

Table 15: Event Severity

	Severity	Definition
	Critical	Catastrophic problem that makes the product/feature unusable.
	Major	Issue that greatly degrades the product/feature, but it is still usable.
	Minor	Limited issue that alters product functionality in a targeted way.
	Notify	Message used primarily for notification which includes type of reboot of cnPilot Wi-Fi devices.

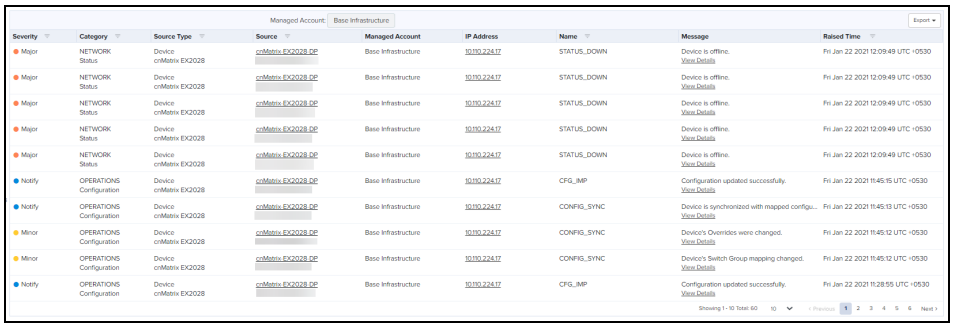
Event Export

The event data in a table can be exported in a CSV or PDF file format.

Support for System Events

The source type can be System, Device, or Client. Events generated by the application will be filtered using the source type **System**.

Figure 19 System Events



The following table describes the different types of event categories and their descriptions.

Table 16: Event Types and Definitions

Event Category	Description
Infrastructure	Events related to infrastructure management – such as HA state, System resources (e.g CPU, Disk, Memory), etc. Source: cnMaestro
Network	Events related to networking issues, such as link up/down. Source: Device
Operations	Events related to system-level processes, such as pushing configuration, installing images, etc. Source: Device
Other	Events unrelated to the above categories. Source: Device
Registration	Events related to managing/unmanaging devices. Source: Device

Table 16: Event Types and Definitions

Event Category	Description
Security	Events related to logging into the devices and establishing secure links. Source: cnMaestro, Device and Client
Services	Events related to additional services added to the product. Source: cnMaestro and Device
Wireless	Events related to issues/notifications with the PTP/PMP radio connectivity, Wi-Fi Clients, etc. Source: Device and Client

Alarms

Alarm Life Cycle

The basic alarm life cycle has the following states:

Table 17: Alarm Life Cycle

State	Description
Acknowledged	Active alarms can be acknowledged, which signifies they are known and being handled. Acknowledgment alarms are not included in the total alarm count.
Active	The alarm remains active until the combination of inputs that generated it are cleared.
Expired	Expired Alarms are placed in the Alarm History.
Inactive	Inactive alarms remain visible in the active alarm table for 10 minutes, then they are moved to alarm history. An alarm becomes inactive when the inputs that generated it are no longer present. An Inactive alarm can be pulled back to Active/Acknowledged states if a new event reactivates the alarm.
Raised	The creation of the alarm.

Alarm Severity

Alarms have a severity that determines how they are handled.

Table 18: Alarm Severity

	Severity	Definition
	Critical	Catastrophic problem that makes the product/feature unusable.
	Major	Significant issue that greatly degrades the product/feature, but it is still usable.
	Minor	Limited issue that alters product functionality in a targeted way.
	Notify	It represents clear and is used for inactive alarms.

Alarm Types

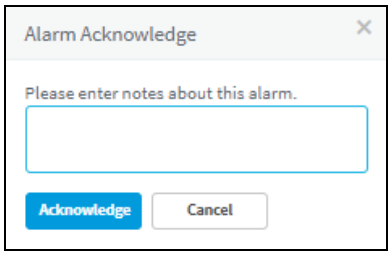
Table 19: Alarm Types

Alarm Type	Definition
Configuration	Tracks issues encountered during a device configuration update.
DFS State	Tracks issues related to DFS operational status.
GPS State	Tracks issues related to GPS synchronization.
Link State	Tracks issues related to the status of device interfaces.
Status	Tracks when connectivity between cnMaestro On-Premises and a device is lost.
Upgrade	Tracks issues encountered during device software upgrade.

Alarm Acknowledgment

Active alarms can be acknowledged in the alarm table. Acknowledgment makes the alarm less visible in the table, and the administrator can further add a note describing how the alarm is being resolved. Acknowledging an alarm will also remove it from the alarm counts.

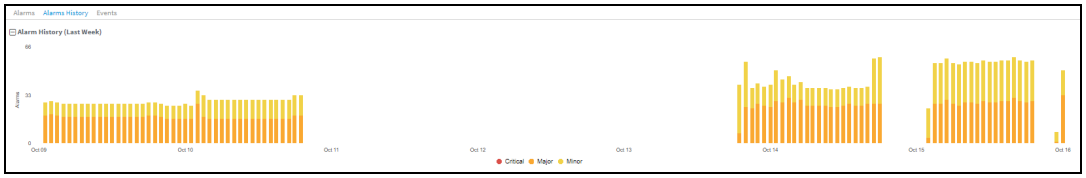
Figure 20 Alarm Acknowledge



Alarm History

Expired alarms are added to the Alarm History. The Alarm History displays historical active alarm counts. Clicking the bar chart filters the table data underneath, allowing one to view which alarms were active at a specific time in the past.

Figure 21 Alarm History



Statistics and Details

Statistics provide a tabular aggregation of data, including general information on the devices monitored, as well as Wireless, Network, and Traffic metrics. Details pages provide information on a single device, generally in a page format.

The table below highlights the type of information generally found in cnMaestro Statistics and Details sections (separated by Device Type).

Table 20: Device Statistics

Device Statistics	Fields
60 GHz cnWave Nodes	**General** • Device • IPv6 Address • Main Aux SFP • Mode • Model • Network • PoP Node • Radio Channel • Serial Number • Site • Software Version • Status • Status Time • Sync Mode • Zone **GPS** • Fix Type • Height • Latitude • Longitude • Satellites Tracked
cnMatrix	**General** • Device • IP Address • Product Name • Serial Number • Status **Traffic** • Throughput (DL) • Throughput (Rx)
cnPilot Home	**General** • Device • IP Address • Product Name • Serial Number • Status **Wireless** • Radios (Channel)
cnRanger BBU	**General** • Device • IP Address • Registered SM Count • Serial Number • Status **Traffic**

Table 20: Device Statistics

Device Statistics	Fields
	• Throughput (DL) • Throughput (UL)
cnRanger SM	**General** • Device • IMSI • IP Address • Serial Number • Status **Traffic** • Throughput (DL) • Throughput (UL) **Wireless** • Bandwidth • Frequency • MCS (DL) • MCS (UL) • RSRP • RSRQ • RSSI
cnReach	**General** • Device • IP Address • Neighbors • Radio • Role • Status **Radio** • Average Noise • Radio Temperature • RSSI • SNR • Tx Power **Traffic** • Throughput (DL) • Throughput (UL)
cnReach XIO	**General** • Active S/W Version • Device • IP Address • Product Name • Serial Number • Status
cnVision Client	**General** • Device • DFS Status

Table 20: Device Statistics

Device Statistics	Fields
	• Distance • IP Address • Serial Number • Session Time • Status **Network** • LAN Interface • LAN Interface 2 • WAN IP Address **Traffic** • Retransmission Rate (DL) • Retransmission Rate (UL) • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Connected AP • MCS (DL) • MCS (UL) • Quality Capacity • RSSI (DL) • RSSI (UL) • SSID • Tx Power • Wireless MAC
cnVision Hub	**General** • Device • DFS Status • IP Address • Registered SM Count • Reregistration Count • Serial Number • Status **Network** • LAN Interface • LAN Interface 2 **Traffic** • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Bandwidth • DL/UL Ratio • Max Range • Frequency • SSID • Tx Power

Table 20: Device Statistics

Device Statistics	Fields
Enterprise WiFi	**General** • Device • IP Address • Product Name • Serial Number • Status **Wireless** • Radios (Channel)
ePMP AP	**General** • Device • DFS Status • IP Address • Registered SM Count • Reregistration Count • Serial Number • Status **Network** • LAN Interface • LAN Interface 2 **Traffic** • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Bandwidth • DL/UL Ratio • Frequency • Maximum Range • SSID • Tx Power
ePMP SM	**General** • Device • DFS Status • Distance • IP Address • Serial Number • Session Time • Status **Network** • LAN Interface • LAN Interface 2 • WAN IP Address **Traffic** • Retransmission Rate (DL) • Retransmission Rate (UL)

Table 20: Device Statistics

Device Statistics	Fields
	• Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Capacity • Connected AP • MCS (DL) • MCS (UL) • Quality • RSSI (DL) • RSSI (UL) • SSID • Tx Power • Wireless MAC
Machfu	**Cell** • Cell Enabled • Cell ICCID • Cell IMEI • Cell IMSI • Cell IP • Cell Link • Cell Manufacturer • Cell Network Type • Cell RSSI • Cell Rx Rate • Cell Sw Version • Cell Tx Rate **Ethernet** • Ethernet • Ethernet Enabled • Ethernet Gateway • Ethernet IP Address • Ethernet Link • Ethernet Link Speed • Ethernet MAC • Ethernet Mask • Ethernet Mode • Ethernet Rx Rate • Ethernet Tx Rate **General** • Device • IP Address • Status **GPS** • GPS Accuracy • GPS Altitude • GPS Fix Time • GPS Satellites in use • GPS Status

Table 20: Device Statistics

Device Statistics	Fields
	• GPS Time **VPN** • VPN IP • VPN Link • VPN Server • VPN Type **Wireless Client** • WC Enabled • WC Gateway • WC IP • WC Link • WC MAC • WC Mask • WC RSSI • WC Rx Rate • WC SSID • WC Tx Rate **Wireless Access Point** • WAP Enabled • WAP IP • WAP Link • WAP MAC • WAP Mask • WAP Mode • WAP Rx Rate • WAP SSID • WAP Tx Rate
PMP AP	**General** • Device • DFS Status • IP Address • Registered SM Count • Reregistration Count • Serial Number • Status **Network** • LAN Interface **Traffic** • Busy Index (DL) • Busy Index (UL) • Frame Utilization (DL) • Frame Utilization (UL) • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Bandwidth

Table 20: Device Statistics

Device Statistics	Fields
	• Color code • DL/UL Ratio • Frequency • Maximum Range • Tx Power
PMP SM	**General** • Device • DFS Status • Distance • IP Address • Serial Number • Session Time • Status **Network** • LAN Interface • WAN IP Address **Traffic** • Packet Loss (DL) • Packet Loss (Error Drop) (DL) • Packet Loss (Overcapacity) (DL) • Packet Loss (UL) • Packet Loss (Overcapacity) (UL) • Packet Loss (Error Drop) (UL) • Throughput (DL) • Throughput (UL) **Wireless** • Antenna Gain • Color Code • Connected AP • Horizontal SNR (DL) • Horizontal SNR (UL) • LQI (DL) • LQI (UL) • Modulation (DL) • Modulation (UL) • RSSI (DL) • RSSI Imbalance • Tx Power • Vertical SNR (DL) • Vertical SNR (UL)
PTP	**General** • Device • IP Address • Product Name • Status **Network** • Aux Interface • Main PSU Interface

Table 20: Device Statistics

Device Statistics	Fields
	• SFP Interface **Wireless** • Antenna Gain • Bandwidth • Errored Seconds • Licensed Country • Maximum Transmit Power • Receive Frequency • Severely Errored Seconds • Transmit Frequency • Unavailable Seconds

Performance

Performance pages display a synchronized view of time series data for devices. The data can be filtered using the interval ranges in the upper left (last 4 hours to last week for Essentials customers), or by dragging the cursor on the graph to select a specific range. The data presented varies based upon device type.

The following images represents the sample performance graphs for 60 GHz cnWave, cnMatrix, cnPilot Enterprise, cnPilot Home, cnRanger,cnReach, ePMP AP, ePMP SM, PMP AP, PMP SM, and PTP.

Table 21: Performance Graph

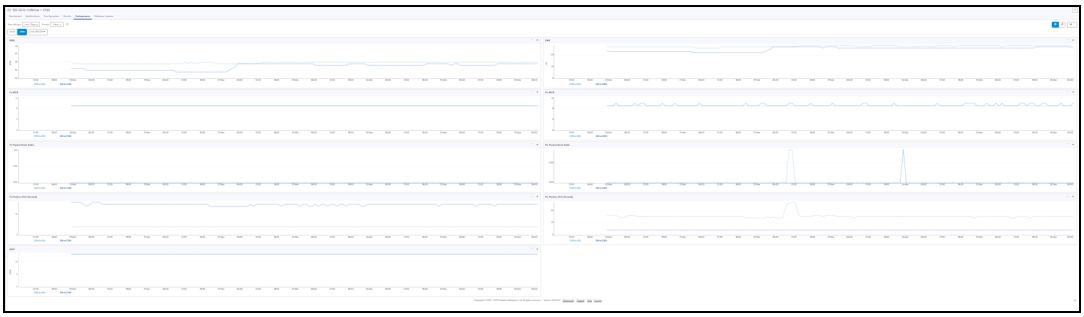
Device	Fields
60 GHz cnWave (Node)	Displays the following graphs: • Available Memory • CPU Utilization 
60 GHz cnWave (Links)	Displays the following graphs: • EIRP • RSSI • Rx Frames (Per Second) • Rx MCS • Rx Packet Error Ratio • SNR • Tx Frames (Per Second) • Tx MCS • Tx Packet Error Ratio 
cnMatrix	Displays the following graphs: • CPU • Packet Error • Rx Packets • Throughput • Tx Packets

Table 21: Performance Graph

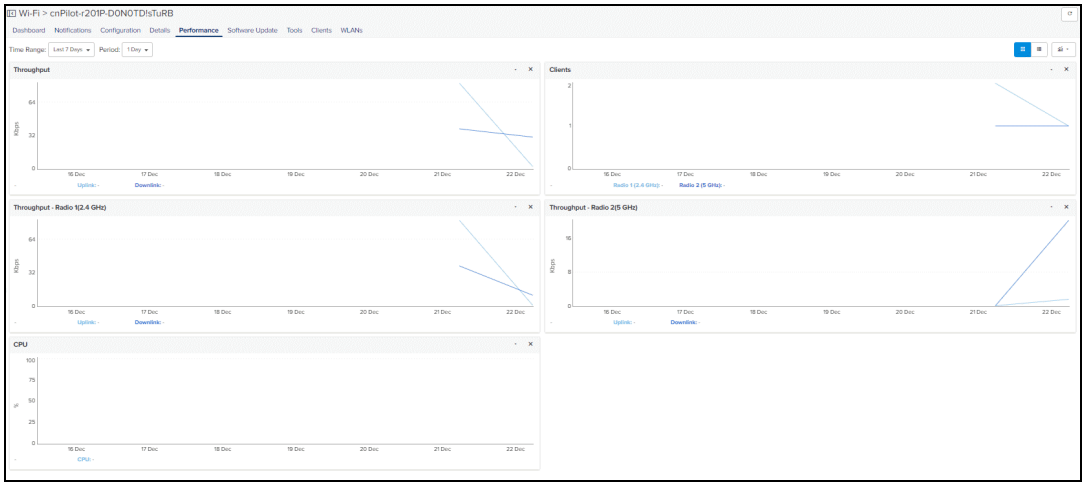
Device	Fields
	
cnPilot Home	Displays the following graphs: • Clients • CPU • Throughput • Throughput - Radio 1 (2.4 GHz) • Throughput - Radio 2 (5 GHz) 
cnReach	Displays the following graphs: • Neighbors • Noise • RSSI • Throughput • Transmit Power

Table 21: Performance Graph

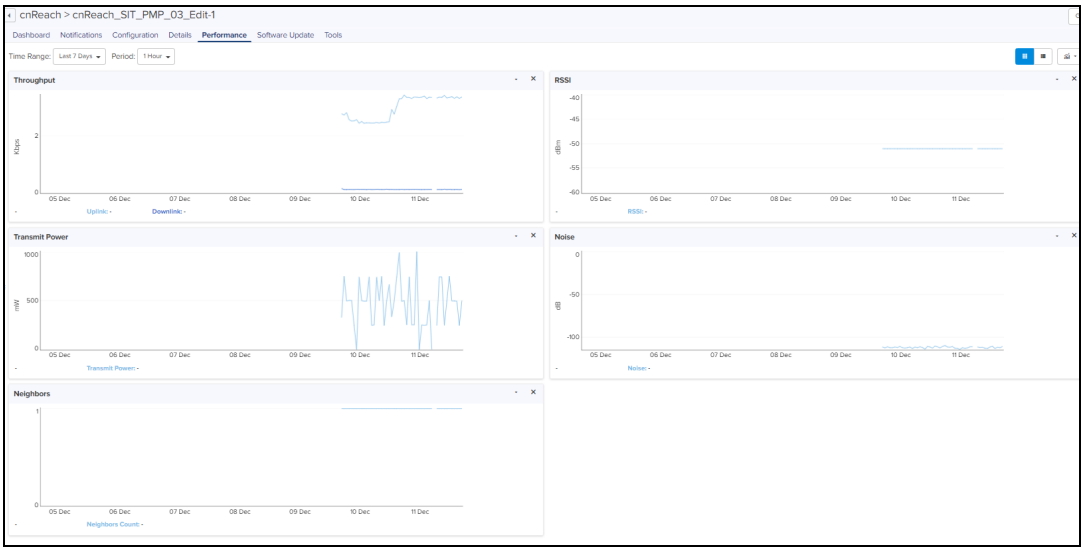
Device	Fields
	
cnRanger BBU	Displays the following graphs: • Available Memory • Interface (eth1) • Interface (eth2) • SMs Registered • Temperature • Throughput 
cnRanger RRH	Displays the following graphs: • Ambient Temperature • CPU • Die Temperature • Frame Utilization • SMs Registered • Throughput

Table 21: Performance Graph

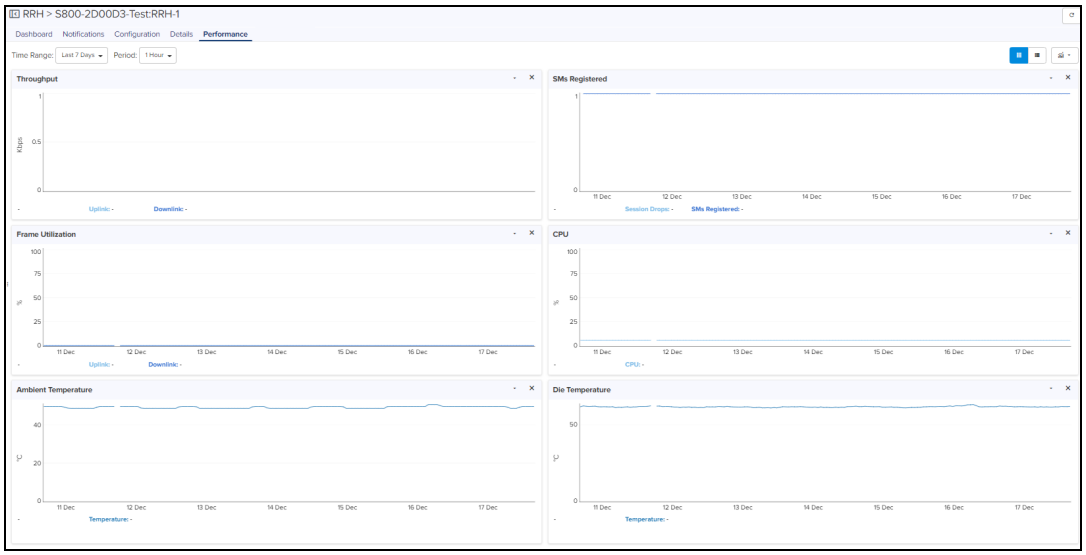
Device	Fields
	
cnRanger SM	Displays the following graphs: • Available Memory • CPU • MCS • RSRP • RSRQ • RSSI • SINR • Throughput

Table 21: Performance Graph

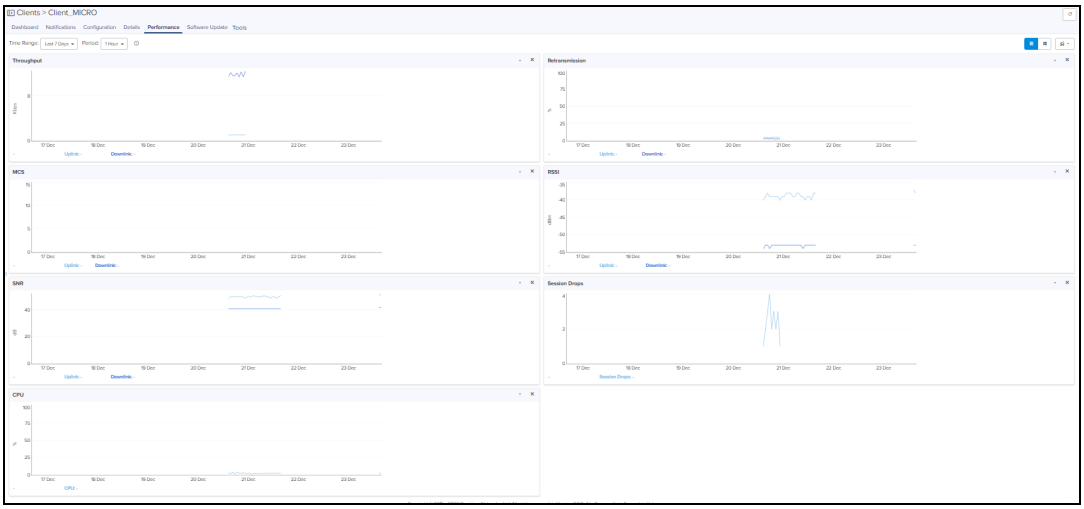
Device	Fields
	
cnVision Client	Displays the following graphs: • CPU • MCS • Retransmission • RSSI • Session Drops • SNR • Throughput 

Table 21: Performance Graph

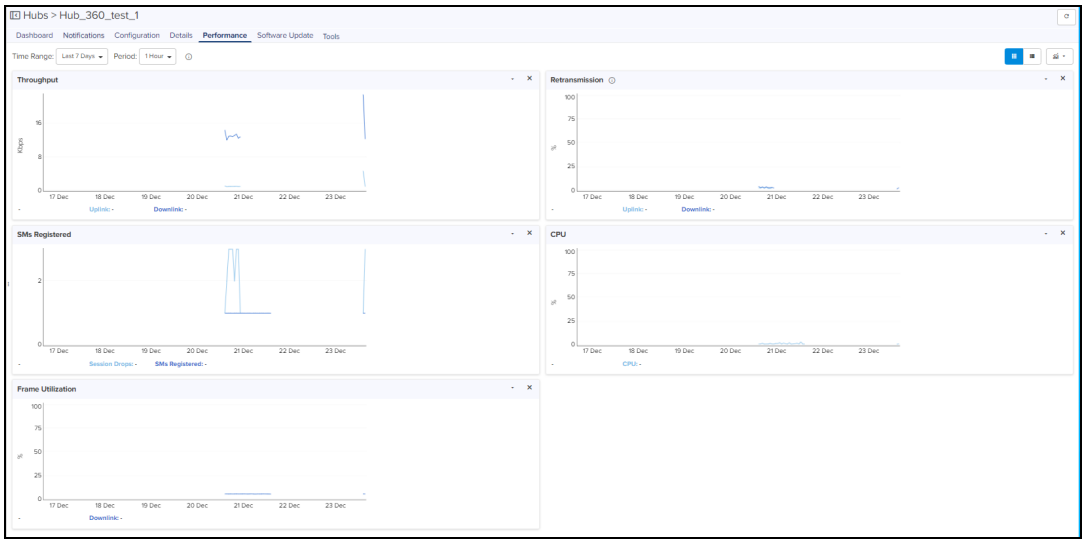
Device	Fields
cnVision Hub	Displays the following graphs: • CPU • Frame Utilization • Retransmission • SMs Registered • Throughput 
Enterprise Wi-Fi	Displays the following graphs: • Airtime (2.4 GHz) • Airtime (5 GHz) • Available Memory • Clients • CPU • Interference • Noise Floor • Packet Rate • Throughput • Throughput - Radio 1 (2.4 GHz) • Throughput - Radio 2 (5 GHz)

Table 21: Performance Graph

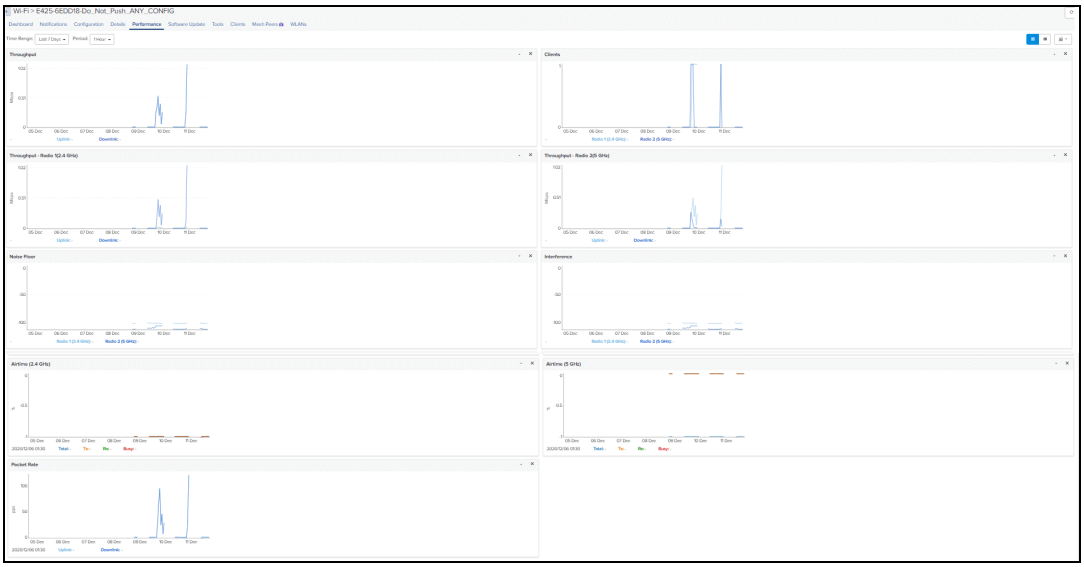
Device	Fields
	
ePMP AP	Displays the following graphs: • CPU • Frame Utilization • Retransmission • SMs Registered • Throughput 
ePMP SM	Displays the following graphs: • CPU • MCS • Retransmission • RSSI • Session Drops • SNR • Throughput

Table 21: Performance Graph

Device	Fields
	
Machfu	Displays the following graphs: • Cellular RSSI • Cellular Throughput • CPU Load • Disk Storage • Ethernet 1 Throughput • Ethernet 2 Throughput • Flash Memory • Wi-Fi Access Point Throughput • Wi-Fi Client RSSI • Wi-Fi Client Throughput

Table 21: Performance Graph

Device	Fields
	
PMP AP	Displays the following graphs: • CPU • Frame Utilization • SMs Registered • Throughput 
PMP SM	Displays the following graphs: • CPU

Table 21: Performance Graph

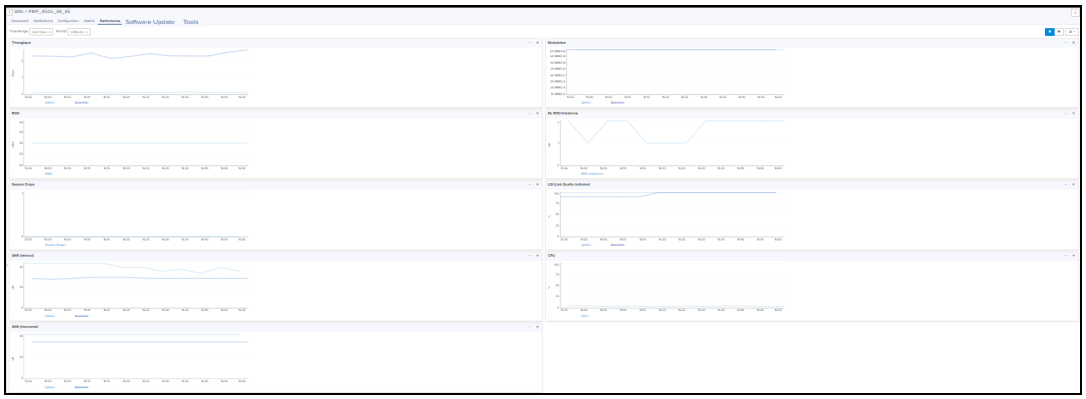
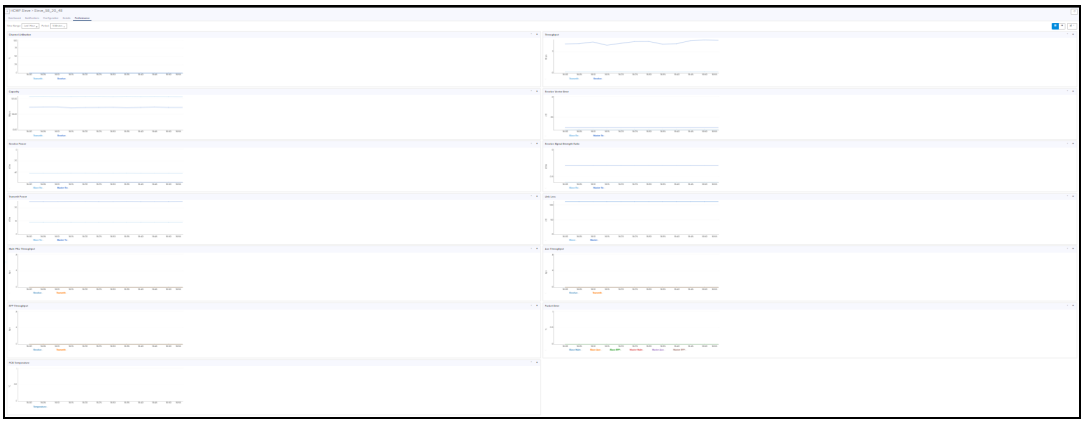
Device	Fields
	• DL RSSI Imbalance • LQI (Link Quality Indicator) • Modulation • RSSI • Session Drops • SNR (Horizontal) • SNR (Vertical) • Throughput 
PTP and HCMP Masters	Displays the following graphs: • Aux Throughput • Capacity • Channel Utilization • Link Loss • Main PSU Throughput • Packet Error • PCB Temperature • Receive Power • Receive Signal Strength Ratio • Receive Vector Error • SFP Throughput • Throughput • Transmit Power

Table 21: Performance Graph

Device	Fields
	
PTP and HCMP Slaves	Displays the following graphs: • Aux Throughput • Channel Utilization • Capacity • Main PSU Throughput • Link Loss • Packet Error • PCB Temperature • Receive Vector Error • Receive Power • Receive Signal Strength Ratio • SFP Throughput • Throughput • Transmit Power 

Maps

Maps provide a visualization for Towers, Sites, and Devices. They display proximity to other devices, connectivity between devices, device health, and selectable status parameters. An example map is presented below.

Two views are supported in System Maps and Network/Tower Dashboard Map:

- Street view
- Satellite view

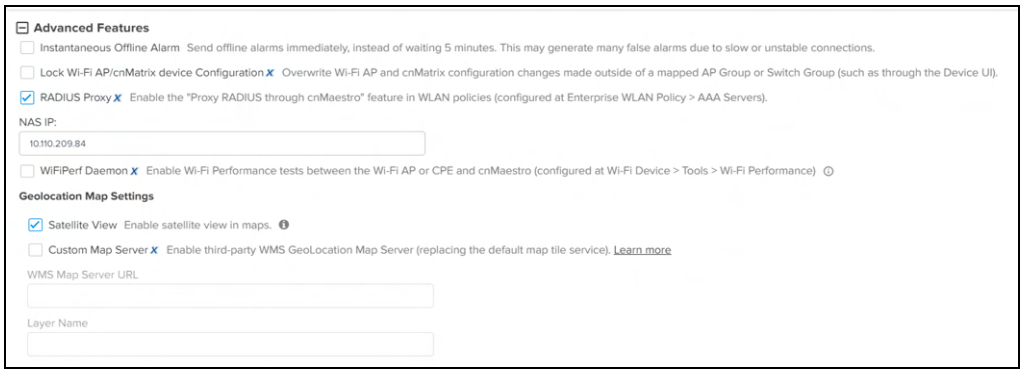
Figure 22 Map Street View





To enable Satellite View, perform the following steps:

1. Navigate to **Administration > Settings > Advanced Features**.
2. Click **Satellite View** checkbox.



The Satellite view is supported in limited US and EU regions.

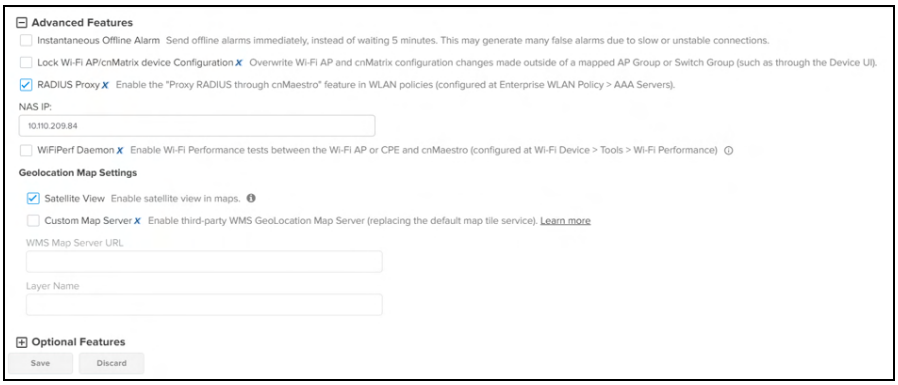
Figure 23 Map Satellite View



Geolocation Map Settings

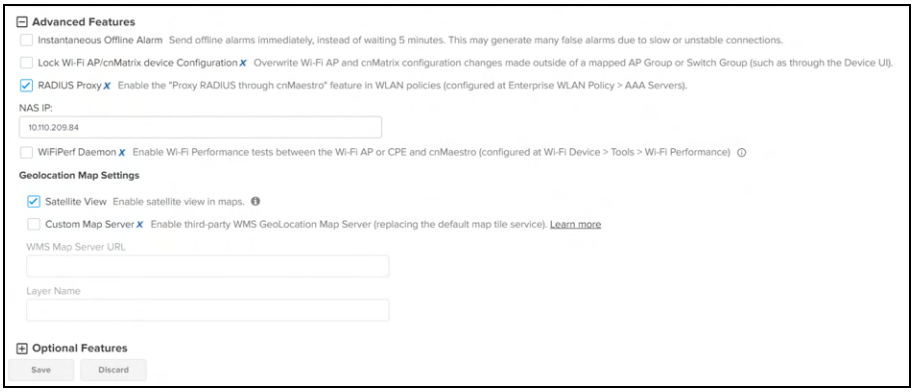
Geolocation Map Settings allows you to custom the **Map** using a Web Map Service (WMS) map server. Map can be customized using the WMS map server URL and the Layer Name provided by the service provider.

Example: If you are using the URL http://ows.mundialis.de/services/service? in the WMS Map server, then enter the layer Name **TOPO-WMS** or **TOPO-OSM-WMS** provided by the map service provider.



To enable Geolocation Map Settings, perform the following steps:

1. Navigate to **Administration** > **Settings** > **Geolocation Map Settings**.
2. Enable **Custom Map Server**.



3. Enter **WMS Map Server URL**.
4. Enter **Layer Name**.
5. Click **Save**.

If you enable the **Geolocation Map Settings**, it displays the custom tile map as shown below:



Map Navigation

There are a various ways to navigate through the map display.

Action	Description
Double-Click	Double-Click on the following items on the Map, the UI will auto-navigate to the Dashboard of that item: • ePMP SM • Site • Tower
Hover	Hovering over a tower or device will pop-up a tool tip that provides basic status information. Hovering over an RF link will display status on the link.
Click	Click the following items on the Map, auto-select the same item in the Tree: • ePMP SM • Tower
Standard Components	In the upper-left corner are generic map navigation components that allow one to zoom in and out. User can also use the mouse to drag and reposition the view as well as turn on satellite display.

Mode

The map can be placed in a number of different modes for the devices of PMP/ePMP SMs only, which define how the device status is presented.

Table 22: Mode

Mode	Details
Alarm Status	Highlights devices based upon alarm count (Critical, Major, Minor).
Average MCS (ePMP only)	Displays the Uplink or Downlink average MCS per device.
Device Status	Displays whether a device is Up (Green) or Down (Red).
Frequency	Displays the sector frequency.
Link Quality Indicator (PMP only)	Displays the Uplink or Downlink average indicator per device.
Reregistration Count	Displays the nodes based upon the number of reregistrations in the last 24 hours. The more reregistration, the larger the node is displayed.
Retransmission Percentage (ePMP only)	Displays the percentage of packets retransmitted between ePMP SM and AP on the wireless link.

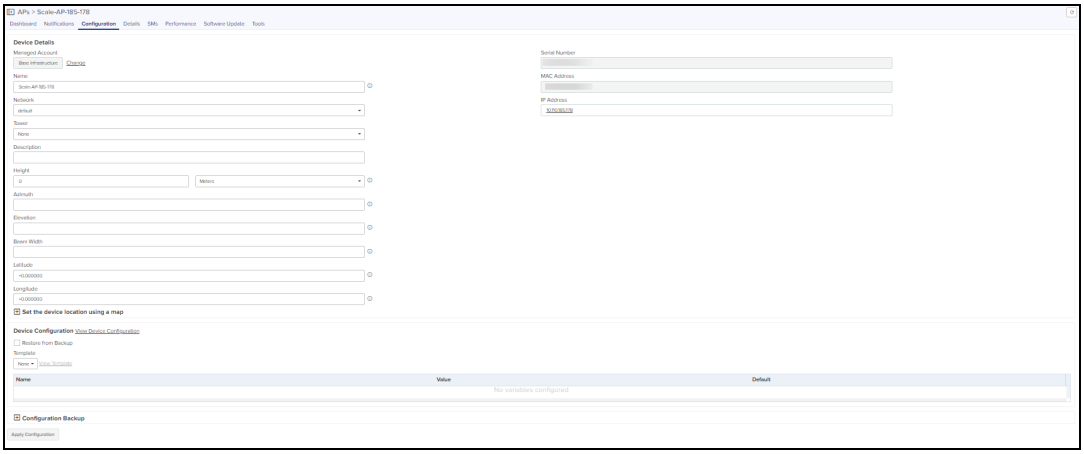
Embedded Maps

Maps are embedded into some additional UI views (most notably, the Dashboard). These embedded maps do not provide the full features of the map view.

Sector Visualization

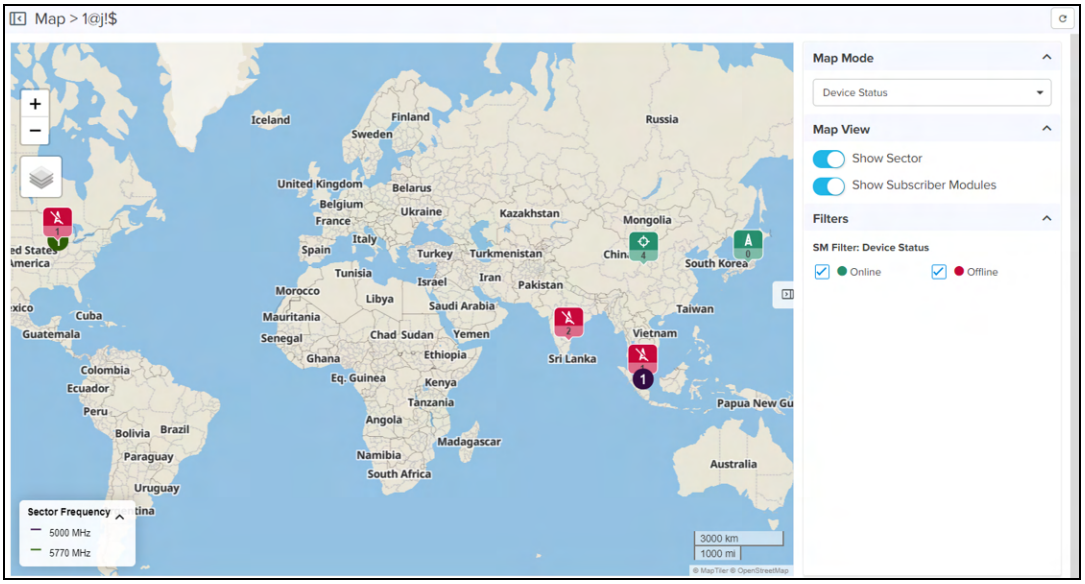
cnMaestro is able to present a basic sector View for ePMP and PMP fixed wireless devices. This requires configuration of Height, Azimuth, Elevation and Beam Width under ePMP/PMP AP configuration. This configured data is used to generate the Sector View. The presentation is not based upon link planning or geographic topology.

Figure 24 AP Configuration Page



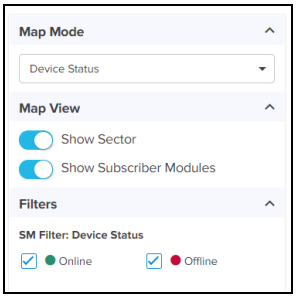
Sector Visualization is available in **Map View**. By selecting the **Show Sector** option, the following map is displayed:

Figure 25 Sector Visualization



Show Subscriber Modules option is available at System, Network, Tower, and AP levels. User can also choose to set the color of SMs based upon frequency or Online/Offline status.

	NOTE: By default **Show Subscriber Modules** is disabled.



Tools

This section provides the following details:

- 60 GHz cnWave Tools
- cnMatrix Tools
- cnPilot Home Tools
- cnRanger Tools
- cnReach Tools
- cnVision Tools
- ePMP Tools
- Enterprise Wi-Fi
- Machfu
- PMP Tools
- Tower-to-Edge View

60 GHz cnWave Tools

In E2E Network **Tools** tab you can view Operations, Diagnostics, Debug, Remote Command, Services, and Settings. Refer to E2E Network Tools.

In Nodes **Tools** tab you can view the Status, Debug, and Remote Command of the device. Refer to Node Tools.

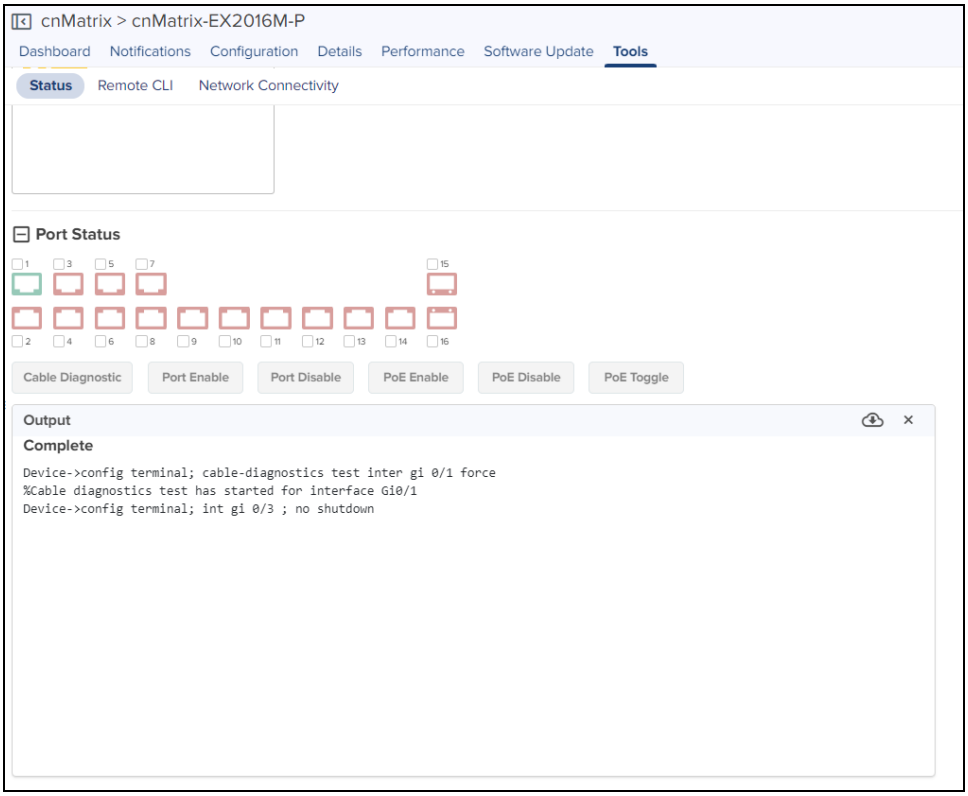
cnMatrix Tools

In **Status** tab you can view the status of the device either Online or Offline and you can reboot the device.

Table 23: cnMatrixTools

Field	Description
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Remote CLI	Remote CLI mode is enabled for Super Administrator and Administrator only. But only **Show** commands can be executed by the Operator.The user can provide the CLI command in the **Command** text box. The output will be displayed in the output window.
Status	Displays the Status and Port Status.

In **Status** tab, user can view the status of the device either Online or Offline, you can reboot the device.



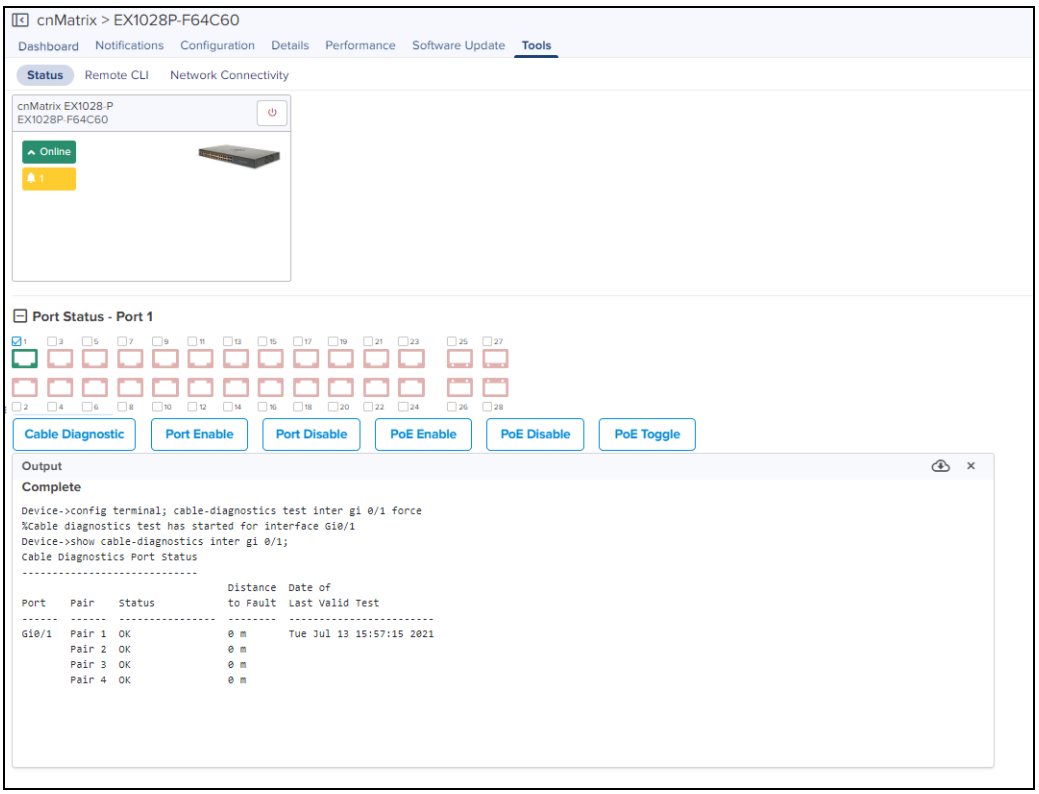
In **Port Status**, user can view the following port status for the **PoE Switches**:

- Cable Diagnostic
- Port Enable
- Port Disable
- PoE Enable

- PoE Disable
- PoE Toggle

Cable Diagnostic

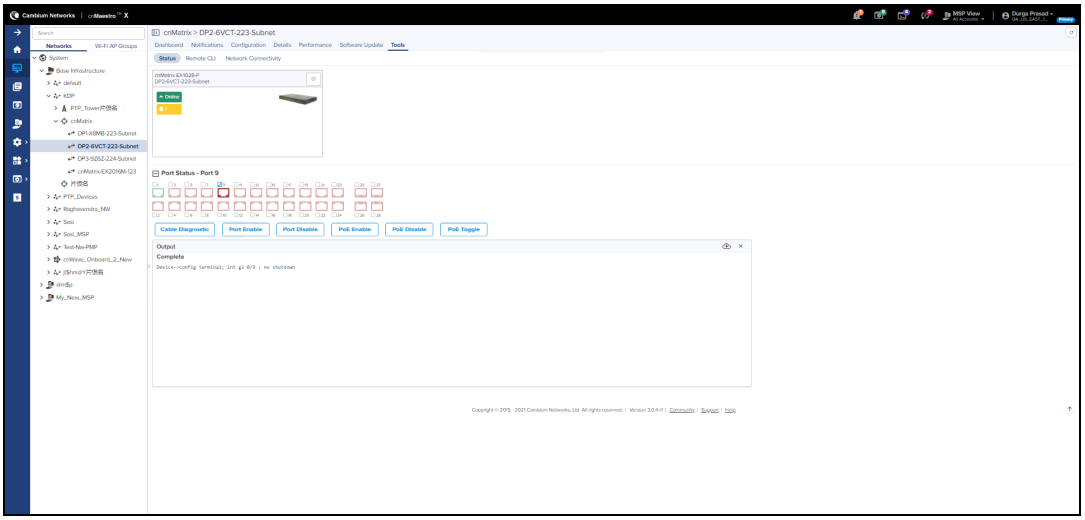
Navigate to **Tools > Status > Port Status**, select the Port and click **Cable Diagnostic**, the following output is displayed:



- You can download the generated output by clicking the download icon.
- You can clear the generated output by clicking the delete icon.

Port Enable or Port Disable

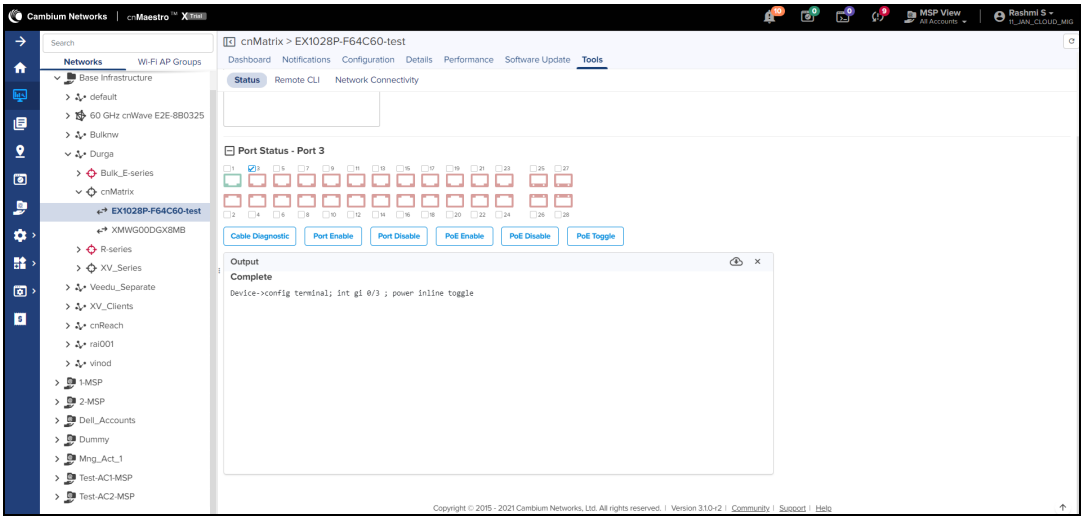
Navigate to **Tools > Status > Port Status**, select the Port and click **Port Disable** or **Port Enable**, the following output is displayed:



- You can download the generated output by clicking the download icon.
- You can clear the generated output by clicking the delete icon.

PoE Toggle

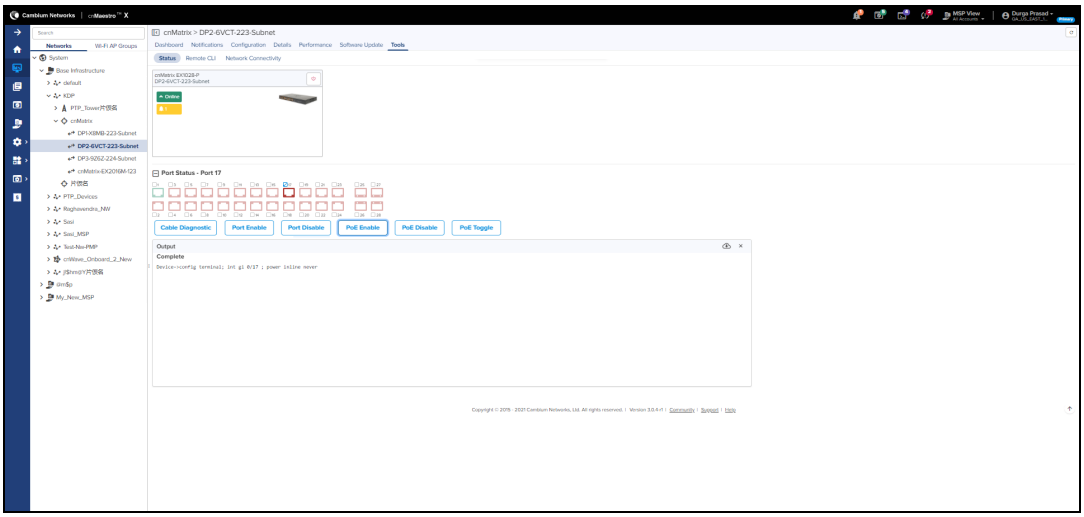
Navigate to **Tools > Status > Port Status**, select the Port and click **PoE Toggle**, the following output is displayed:



- You can download the generated output by clicking the download icon.
- You can clear the generated output by clicking the delete icon.

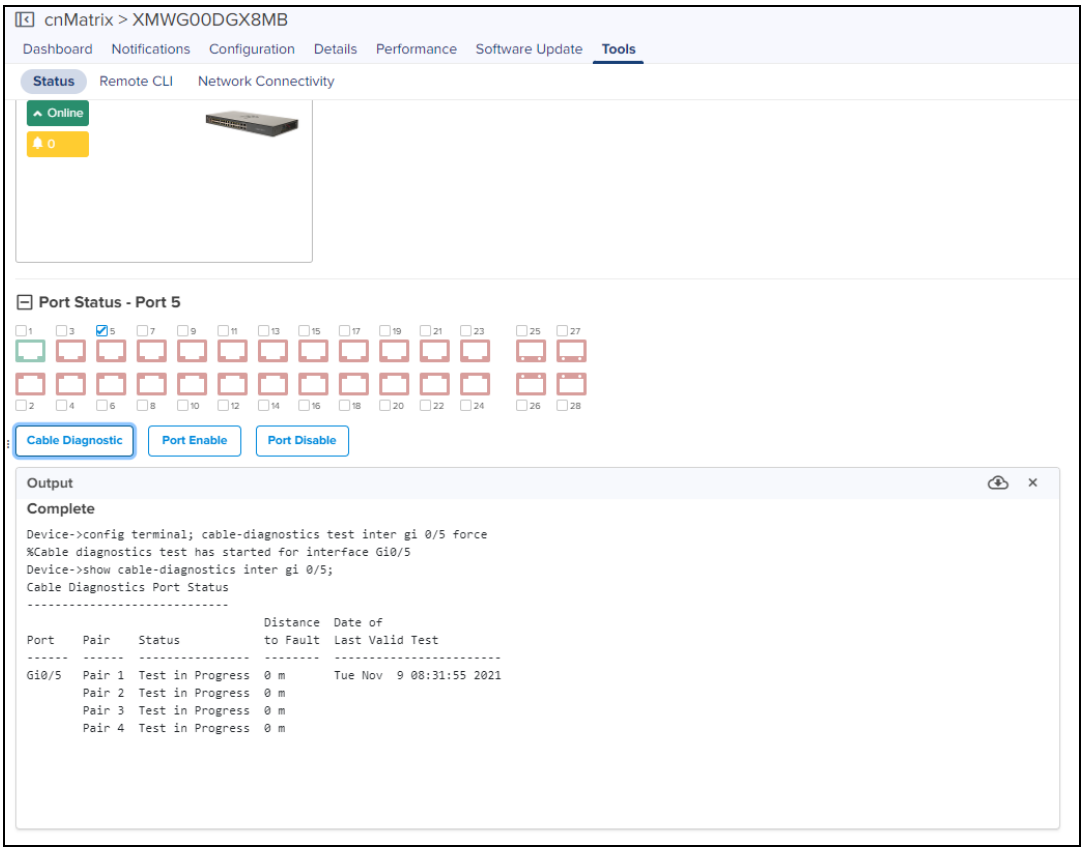
PoE Enable or PoE Disable

In **Tools > Status > Port Status**, select the Port and click **PoE Enable** or **PoE Disable**, the following output is displayed:



In **Port Status,** user can view the following port status for the **non-PoE Switches**:

- Cable Diagnostic
- Port Enable
- Port Disable



Remote CLI

Navigate to **Tools > Remote CLI**, when you select a command type and click **Run**, the following output is displayed:

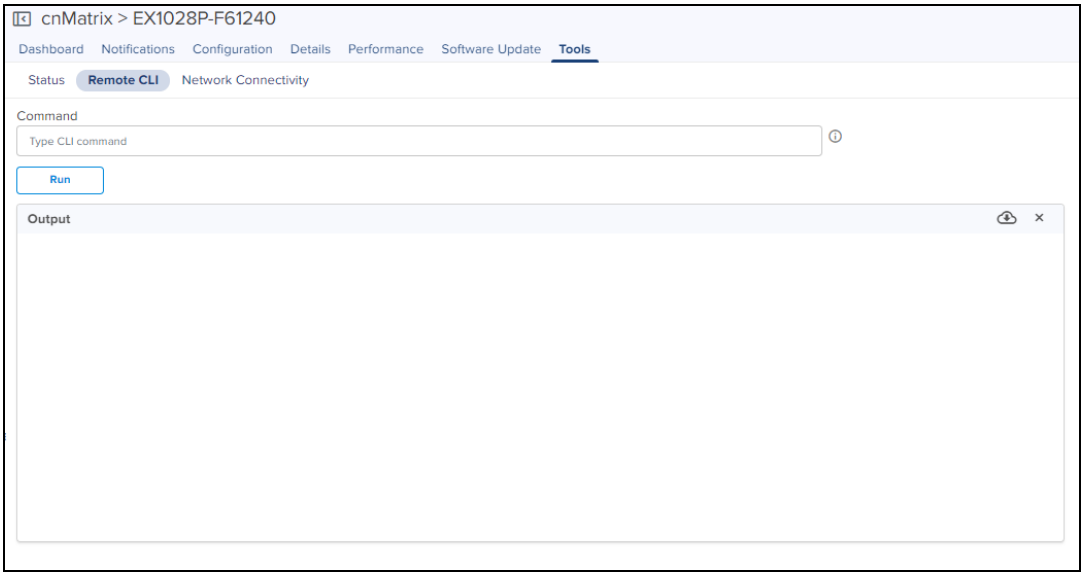
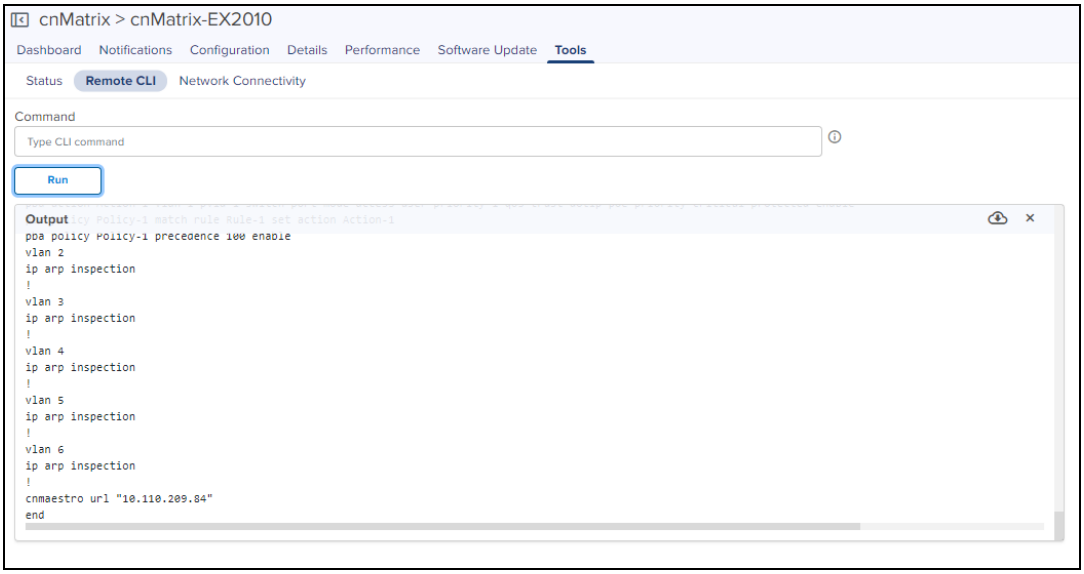
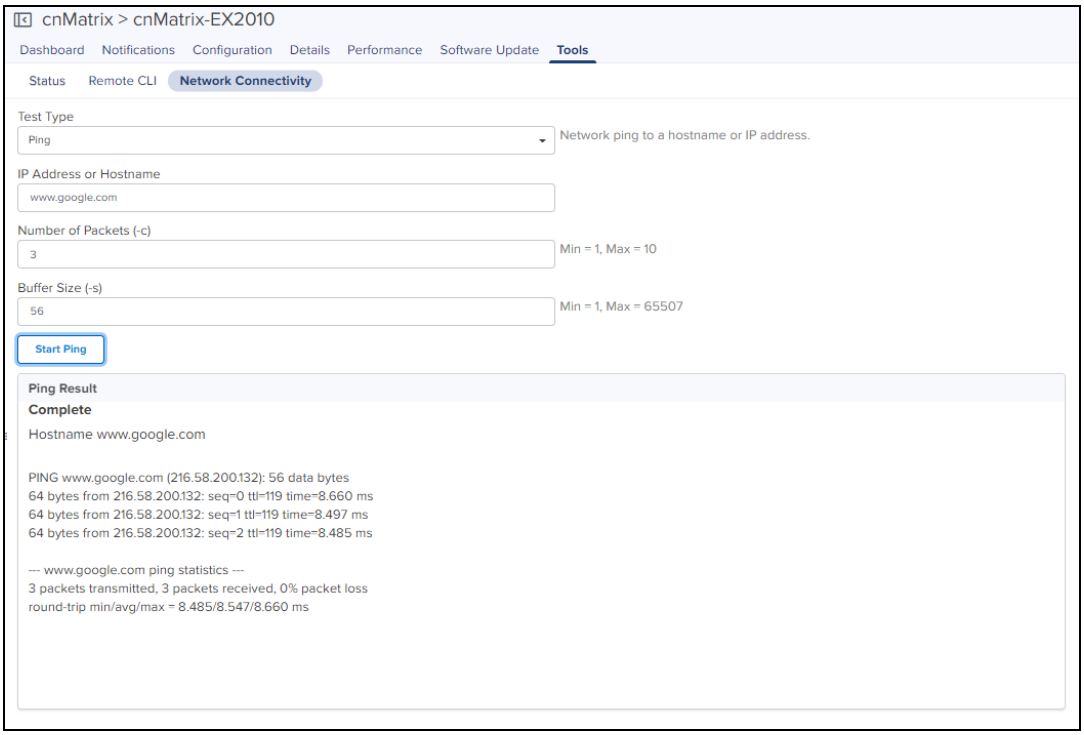


Table 24: cnMatrix Tools

Tools	Description
Remote CLI	Remote CLI mode is enabled for super admin and admin users only. But only show commands can be executed by operator. The user can provide the CLI command in the **Command** textbox. The output will be displayed in the output window.



- You can download the generated output by clicking the download icon.
- You can clear the generated output by clicking the delete icon.



cnPilot Home Tools

The Tools page for cnPilot Home devices consolidates a number of operations into a single troubleshooting interface.

The operations of cnPilot Home is listed below:

Table 25: cnPilot Home

Tools	Description
Debug	Displays the log details.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Packet Capture	Lists packet capture details.
Status	Displays the status of device.
Wi-Fi Analyzer	Displays radio traffic and signal.
Wi-Fi Performance	Wi-Fi performance measures the backhaul speed across devices with respect to cnMaestro.

Figure 26 cnPilot Tools Enterprise WiFi

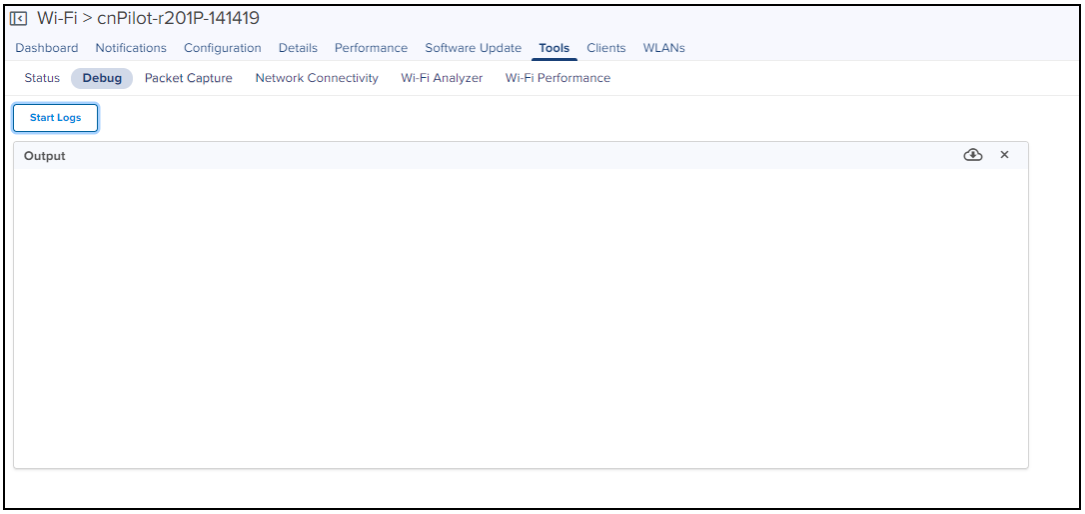
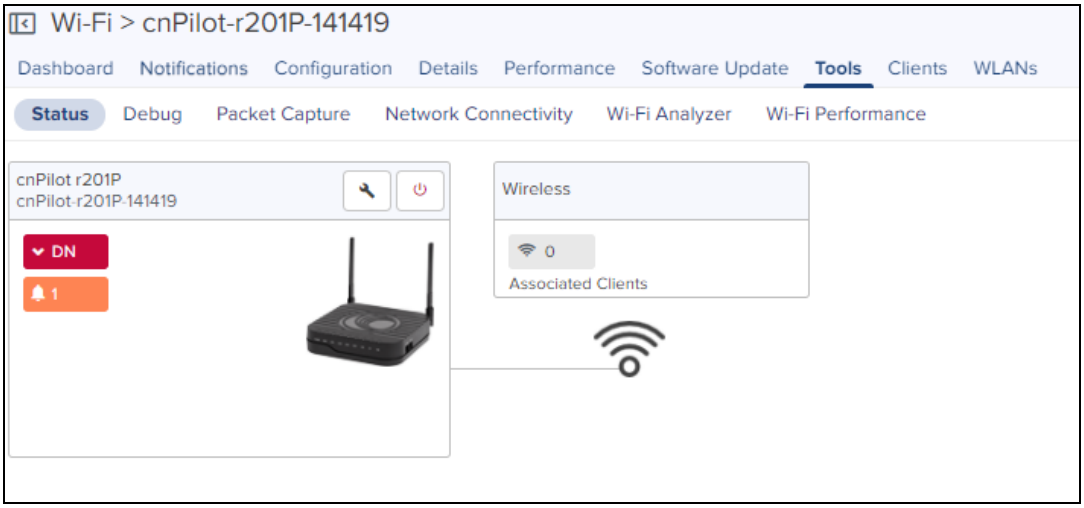


Figure 27 cnPilot Tools Status



cnRanger Tools

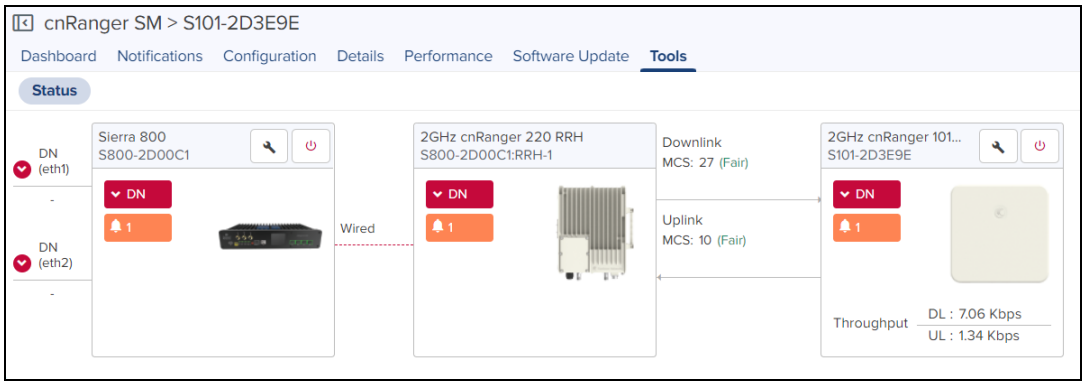
cnRanger BBU

In **Status** tab you can view the status of the device either Online or Offline, allows to download Tech Support File and can reboot the device.



cnRanger SM

In **Status** tab you can view the status of the device either Online or Offline, allows to download Tech Support File, displays the wired connectivity status, and can reboot the device.



cnReach Tools

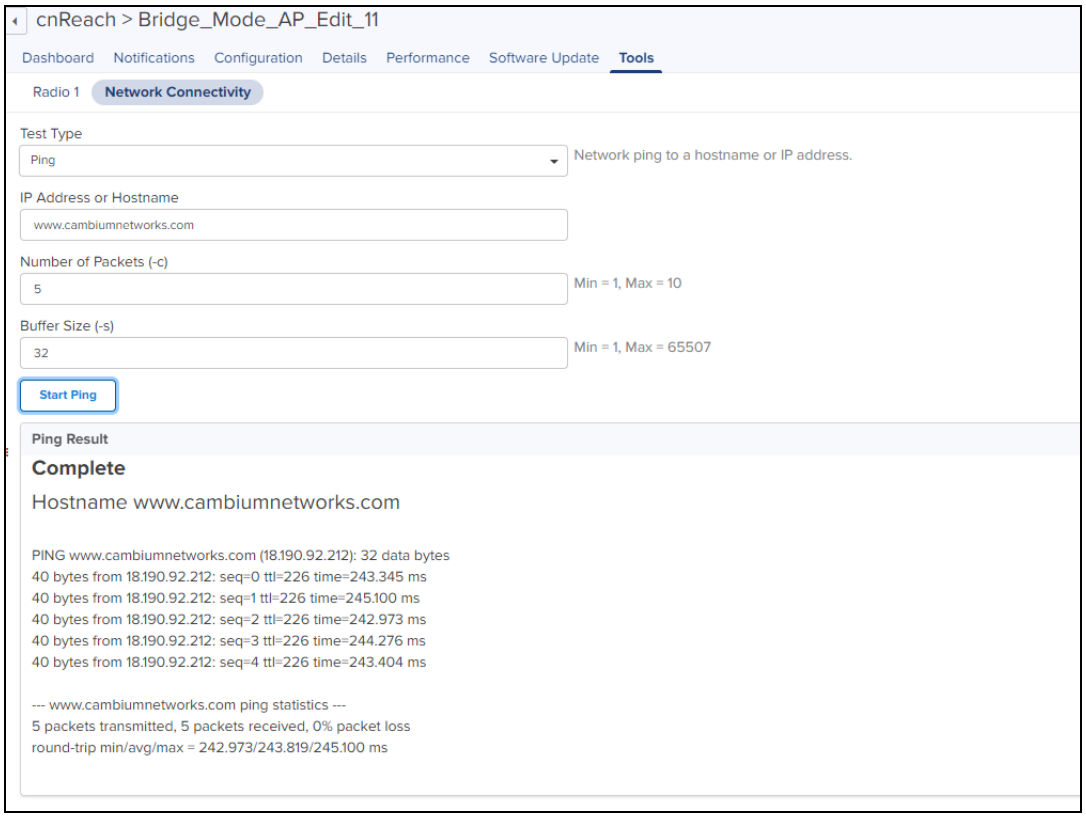
The Tools page for cnReach devices consolidates a number of operations into a single troubleshooting interface.

The operations are listed below:

Table 26: cnReach Tools

Tools	Description
Ping	Network ping to a hostname or IP address.
RF Ping	RF reachability test between local radios that provides details on signal quality.
RF Throughput	RF throughput test between local radios that provides details on throughput.

Figure 28 cnReach Tools



cnVision Tools

The Tools page for cnVision devices consolidates a number of operations into a single troubleshooting interface.

The operations are listed below:

Table 27: cnVision Tools

Field	Description
Debug	Displays the log details.
Network Connectiviy	Executes Ping, DNS, or Traceroute tests.
Status	Displays the Status.

Table 27: cnVision Tools

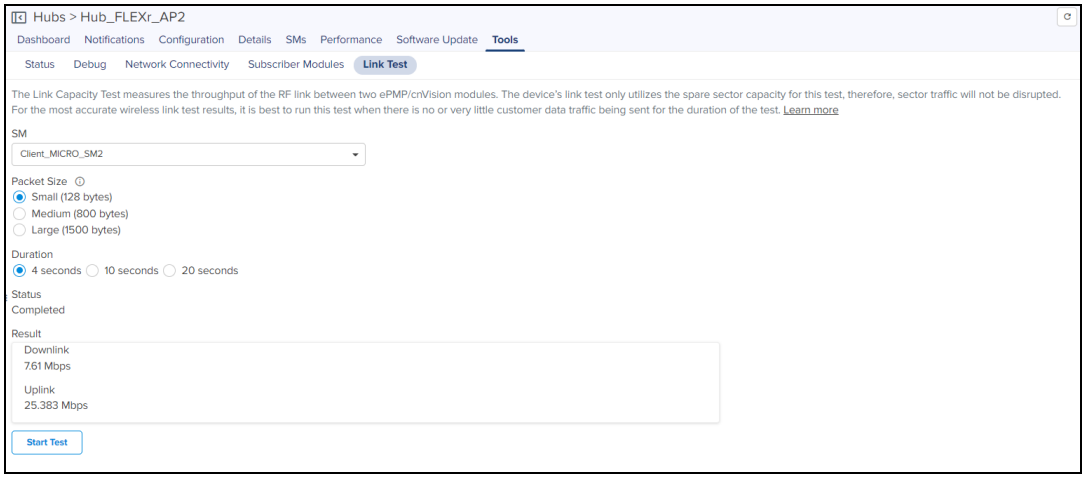
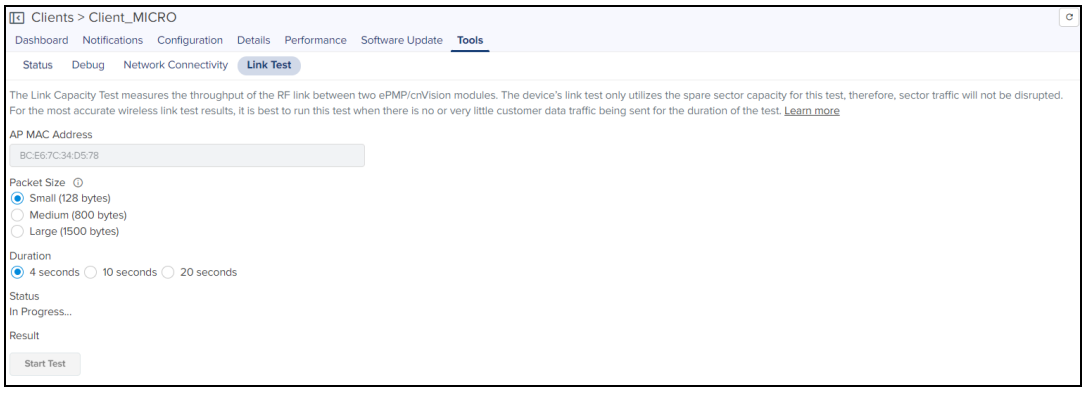
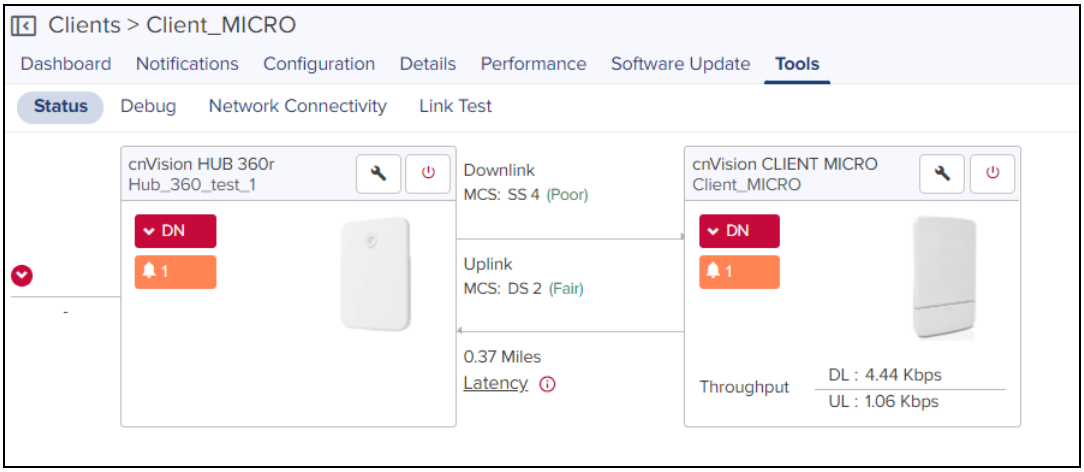
Field	Description
Subscriber Modules	Displays the SM linked to the Hub and allows to reboot and download the tech support file.
Link Test	The Link Capacity Test measures the throughput of the RF link between two cnVision modules. cnVision link test only utilizes the spare sector capacity for this test, therefore, sector traffic will not be disrupted. For the most accurate wireless link test results, it is best to run this test when there is no or very little customer data traffic being sent for the duration of the test. Displays the link related test result with respect to Throughput. Link Test can be performed on the cnVision Hub and its SM link. In order to run this operation, select the device and then the **Tools** tab. • If an cnVisiosn Hub is selected you can choose the SM from the list and start the test.  Displays the following fields: • **Packet Size**: Choose the Packet Size to use for the throughput test. • **Duration**: Choose the time duration in seconds to use for the throughput test. • If an cnVision Client is selected, click **Start** Test to run the link test.  Displays the following fields: • **Packet Size**: Choose the packet size to use for the throughput test. • **Duration**: Choose the time duration in seconds to use for the throughput test.

Figure 29 cnVision Tools



Enterprise Wi-Fi Tools

The Tools page for Enterprise Wi-Fi devices consolidates a number of operations into a single troubleshooting interface.

The operations of Enterprise Wi-Fi are listed below:

Table 28: Enterprise Wi-Fi Tools

Tools	Description
Debug	Displays the log details.
Flash LEDs (Only for E Series Device)	The LEDs of the device enables to identify and locate the device.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Packet Capture	Lists packet capture details.
Remote CLI	Remote CLI mode is enabled for super admin and admin users only. But only show commands can be executed by operator. The user can provide the CLI command in the **Command** textbox. The output will be displayed in the output window.
Status	Displays the status of device.
Wi-Fi Analyzer	Displays radio traffic and signal.
Wi-Fi Performance (wifiperf)	Wi-Fi performance measures the backhaul speed across devices with respect to cnMaestro.

Figure 30 Enterprise Wi-Fi Tools

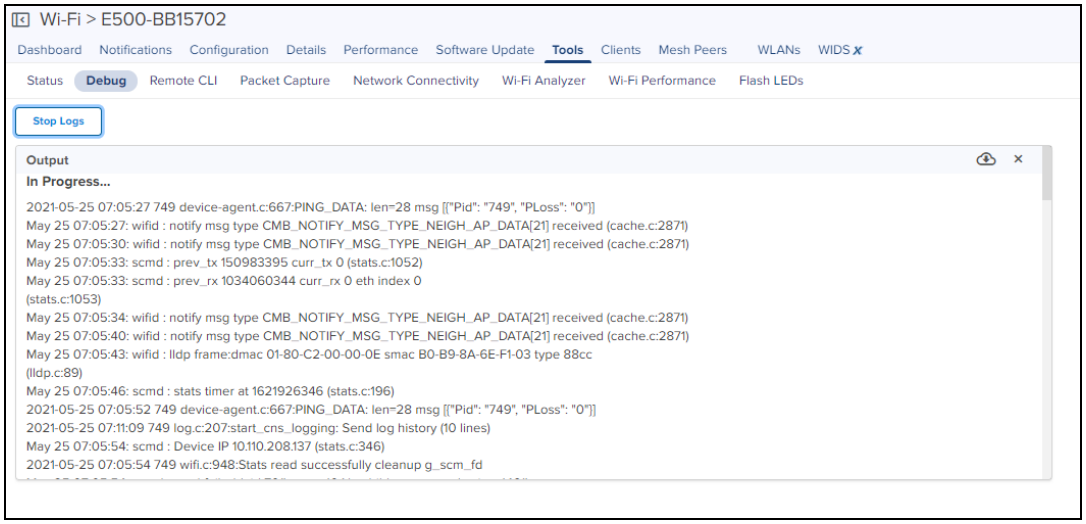


Figure 31 Enterprise Wi-Fi Remote CLI Tools

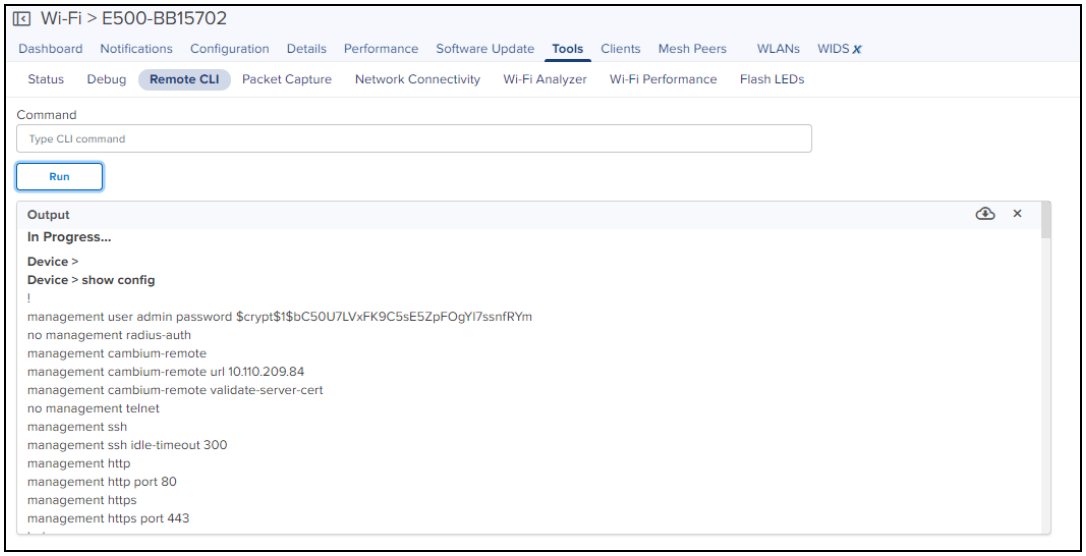
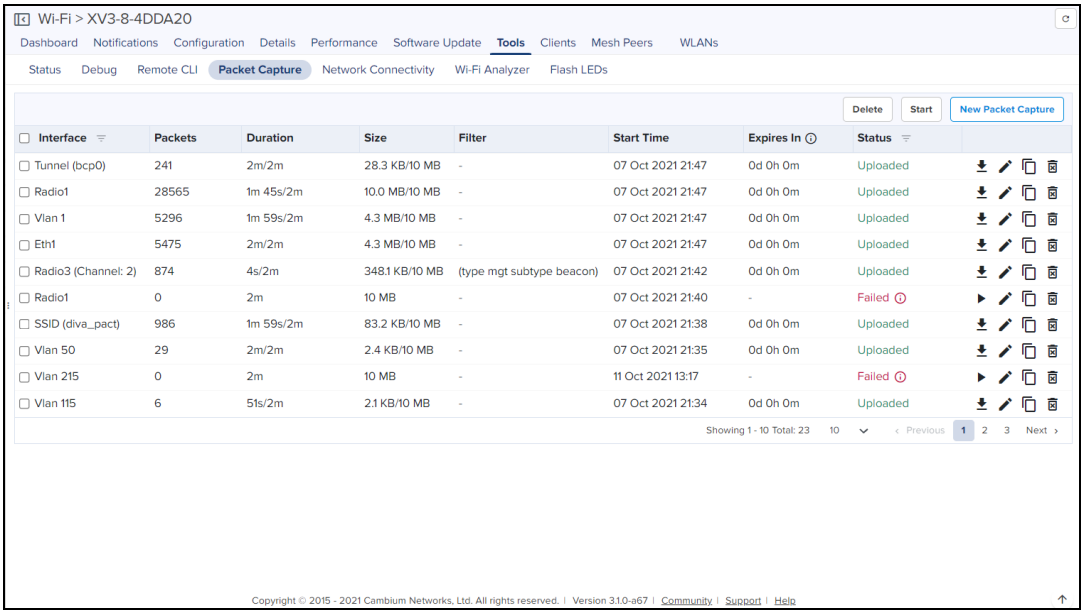


Figure 32 Enterprise Wi-Fi Packet Capture



Packet Capture

The Packet Capture allows the user to capture all packets on a specified interface simultaneously. The user can trigger packet capture on an interface (or multiple interfaces simultaneously). The main input for packet capture is by selecting type of interface and filter options.

NOTE:

Enhanced packet capture is available for version 6.4 or higher in Enterprise devices.

To view Packet Capture, navigate to **Network** or **Site** > **Wi-Fi AP** > **Tools** > **Packet Capture**.

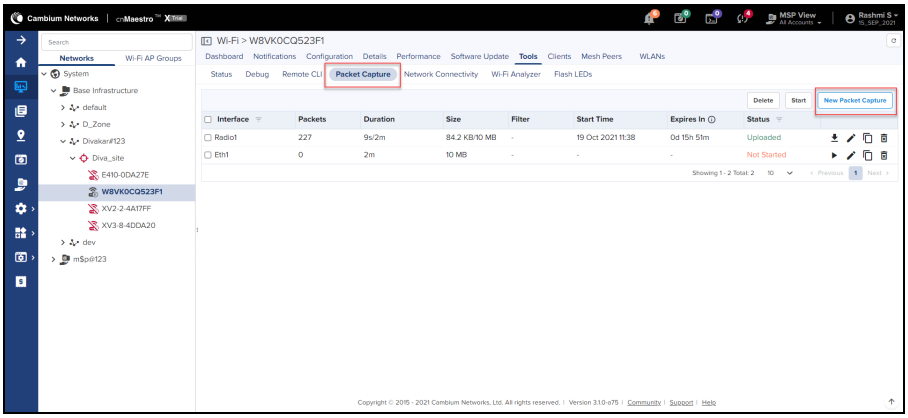


Table 29: Packet Capture field

Field	Description
Duration	Represents packet capture running duration in seconds versus maximum duration configured.
Expires In	Expiry time of packet capture. By default the packets captured expires in 24 hours.
Filter	Type of filter option opted by user.
Interface	The following interfaces supports the packet capture: • Ethernet • Radio • Wireless LAN • VLAN • SSID • TUNNEL • BRIDGE • PPPoE
Packets	Represents number of packets captured versus maximum limit of packet count configured.
Size	Current packet capture size versus maximum packet capture size configured.
Start Time	Start time of the capture.
Status	Status of packet captured is as follows: • Queued • Failed • Skipped • Aborted

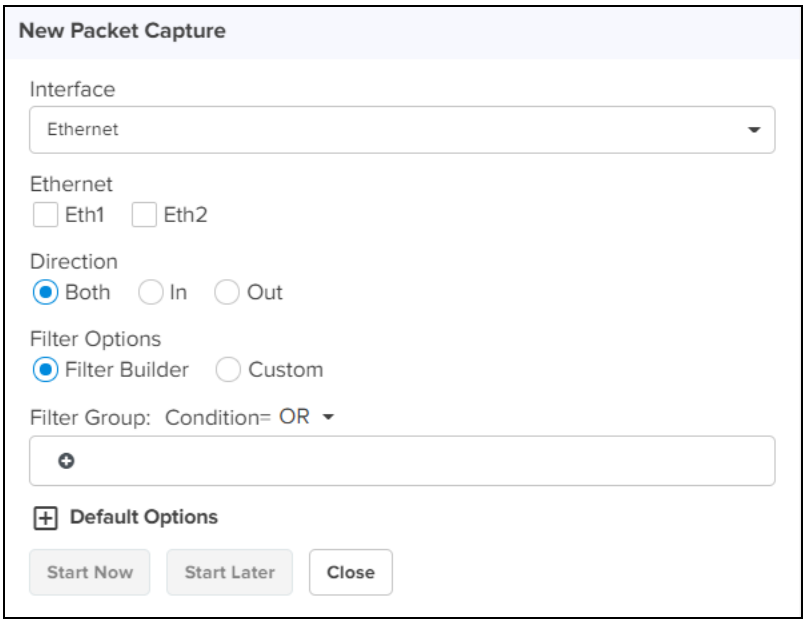
New Packet Capture

Perform the following steps to start a new packet capture:



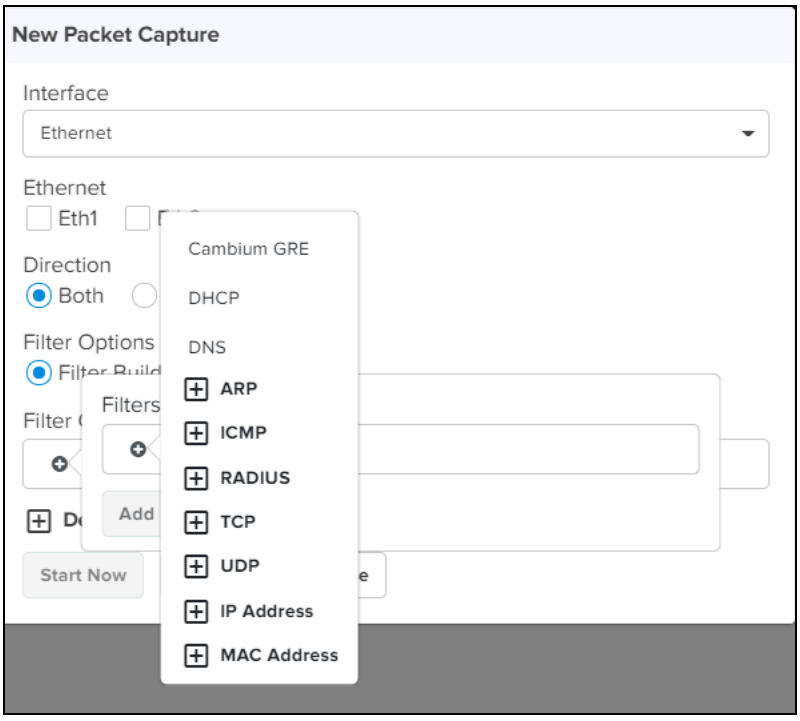
NOTE:
- Filter options vary for different interfaces (Radio, Wireless LAN, VLAN, SSID, TUNNEL, BRIDGE, and PPPoE. Radio, SSID has wireless 802.11 filters, other interfaces has wired 802.3 filters).
- User can also add custom filters if needed.

1. Click **New Packet Capture** to start packet capture.

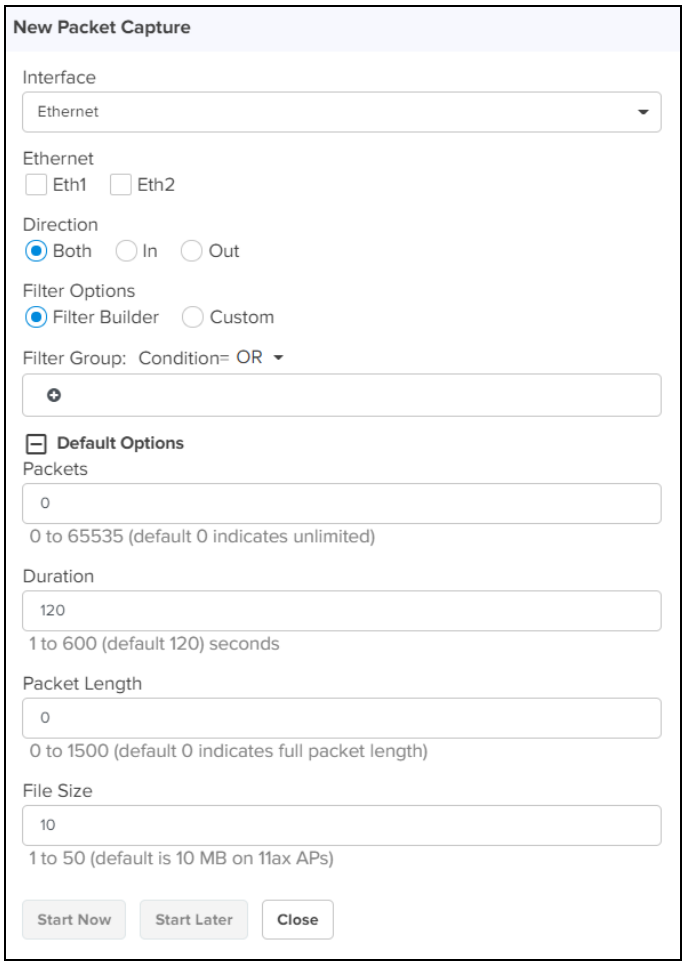


2. Select the **Interface** type from the drop-down list.
3. Select **Ethernet** as **Eth1** or **Eth2**.
4. Choose the **Direction** as **Both**, **In**, or **Out**.
5. Select **Filter options** as **Filter Builder** or **Custom**.

   You can filter the packets captured by specifying Cambium GRE , DHCP, DNS, ARP, ICMP, Radius, TCP, UDP , IP address, and MAC address.



6. Click **Default Options** to configure **Packets**, **Duration**, **Packet Length**, and **File Size**.

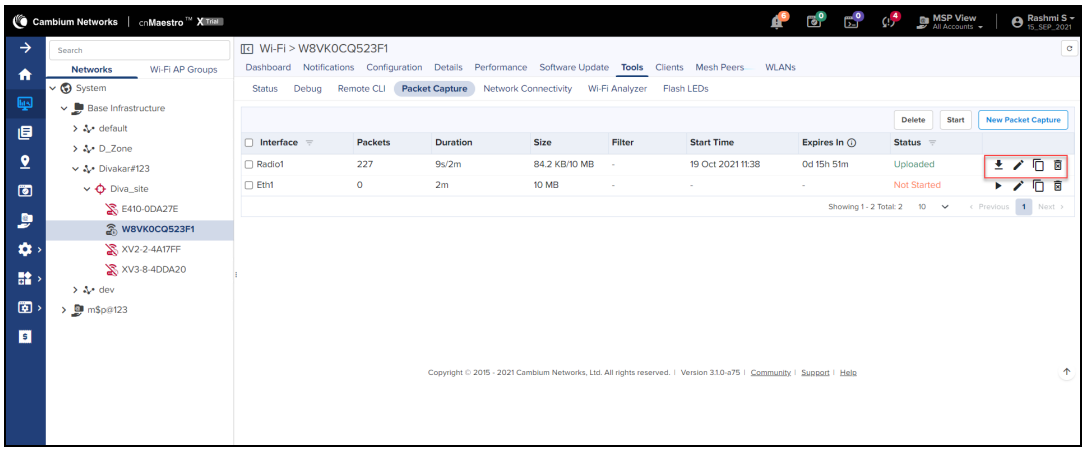


7. Click **Start Now** to capture the packets immediately or start the capture later by selecting **Start Later** option. The progress of packets captured can be seen in **Status** field.

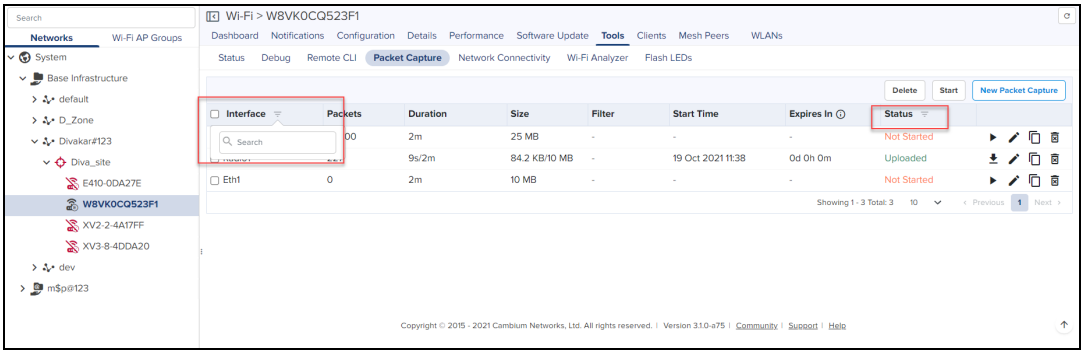
8. Click download icon to download the packets post completion in **PCAP** file format.

> **NOTE:**
>
> For cnMaestro X, a maximum of four sessions of packet capture is supported whereas for cnMaestro Essentails a maximum of two sessions of packet capture is supported.

The user can **Edit**, **Clone**, and **Delete** the packets captured. Packets captured can be cloned depending on the type of interface opted during the start of the capture.



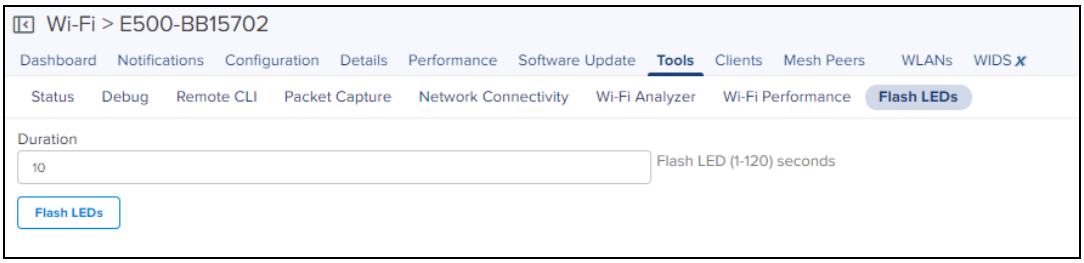
The user can search the packet capture by **Interface** type and **Status.**



NOTE:

- User can start packet capture by clicking **Play** button for packet capture stopped at **Not Started/Failed/ Expired**.
- **Bulk Start** and **Bulk Delete** can be done by selecting multiple packet capture settings.
- Expired packet capture is deleted from cnMaestro after 7 days.
- Packet capture is removed immediately, when device(AP) is deleted from cnMaestro.
- Packet capture cannot be started on same interface simultaneously.
- Only **Show** command works for user like Operator.

Figure 33 Flash LEDs

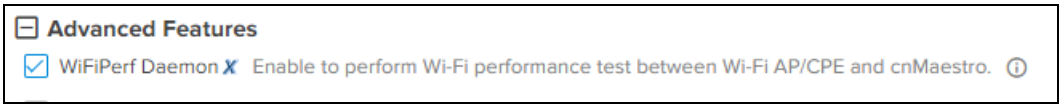


Wi-Fi Performance Test

Currently, Wi-Fi performance test feature is supported only on cnPilot devices. Wi-Fi performance test will be triggered between the AP and Wi-FiPerf Endpoint.

Wi-FiPerf Endpoint can be either the cnMaestro instance or a locally installed speed test server.

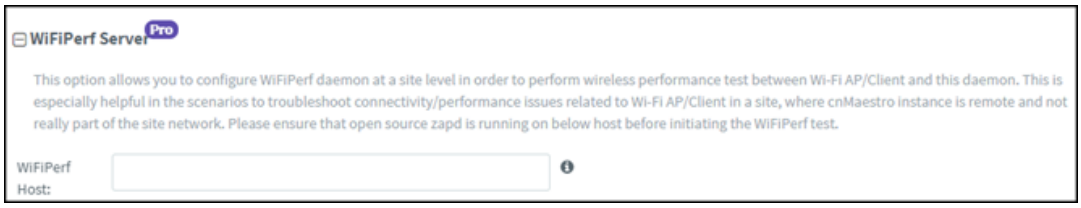
- **cnMaestro Instance :** To enable Wi-Fi performance test, navigate to **Administration > Settings > Advanced Features** page and enable **Wi-FiPerf Daemon** option.



- **Locally installed Wi-Fi Performance Server** : Wifiperf performance inter-operates with the open source zapwireless tool.

(https://code.google.com/archive/p/zapwireless/). So install zap on the local host on the site. This is especially helpful in the scenarios to troubleshoot connectivity/performance issues related to Wi-Fi AP/Client in a site.

To configure locally installed site level speed test server on cnMaestro, navigate to **Site > Configuration** > **Wi-FiPerf Server** page.



	NOTE: The Wifiperf manager running on cnMaestro establishes control session with AP (and other endpoint-local host) using TCP port number 18301. So it is mandatory that both the AP and the other endpoint is reachable from cnMaestro. Make sure that the NAT/firewall does not block the wifiperf traffic from cnMaestro to any endpoint or AP (also between the endpoints and AP). Ensure that the port number 18301 is not blocked in the network for TCP and UDP.
	NOTE: For more details on Wi-Fi performance (wifiperf) feature, refer here.

Performing the Test:

To run the Wi-Fi performance test, navigate to **Tools > Wi-Fi Performance** page.

It can be used to measure the following parameters with intervals of 10, 20 and 30 seconds:

Traffic Types

- TCP
- UDP

Traffic Direction

- Downlink
- Uplink

WiFiPerf Endpoint

- cnMaestro
- WiFi Perf Local Host

ePMP Tools

The Tools page for ePMP devices consolidates a number of operations into a single troubleshooting interface.

The operations are listed below:

Table 30: ePMP Tools

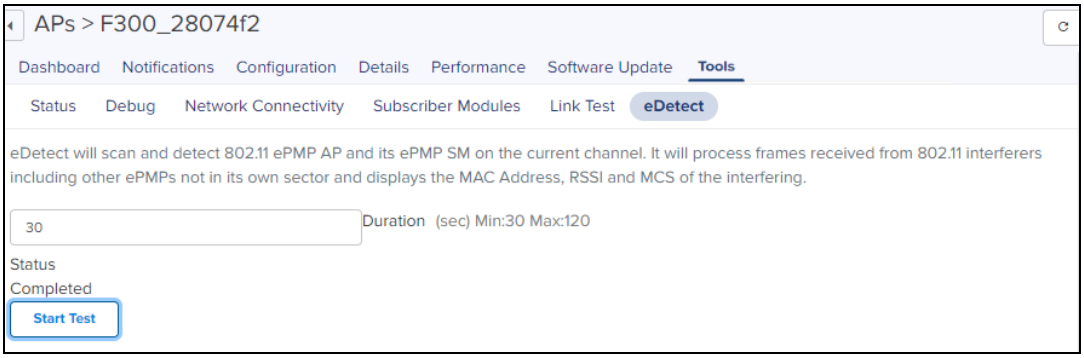
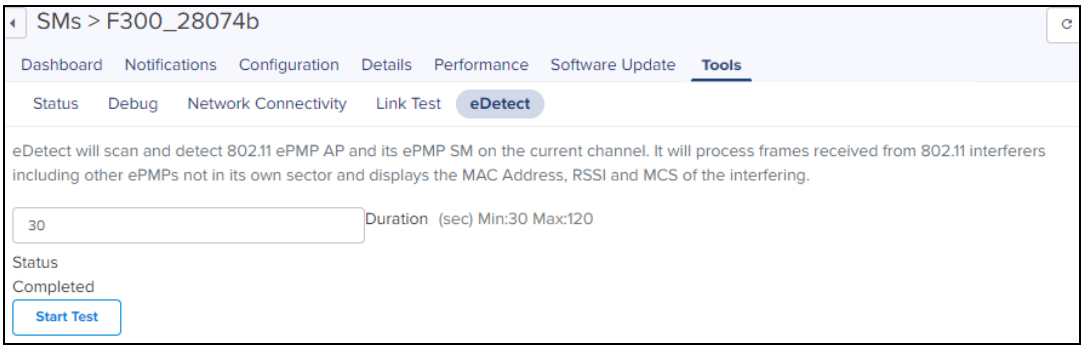
Tools	Description
Debug	Displays the log details.
eDetect	eDetect is supported on the ePMP AP or SM. It is also launched from the **Tools** tab. The eDetect tool (not available in ePMP Master/Slave mode) is used to measure the 802.11 interference at the ePMP radio or system when run from the AP or the SM, on the current operating channel. When the tool is run, the ePMP device processes all frames received from devices not connected to the ePMP system and collects the interfering frame's information such as MAC Address, RSSI, and MCS. Configure the duration for which the AP scans for interference.  Configure the duration for which the SM scans for interference. 
Link Test	The Link Capacity Test measures the throughput of the RF link between two ePMP modules. ePMP's link test only utilizes the spare sector capacity for this test, therefore, sector traffic will not be disrupted. For the most accurate wireless link test results, it is best to run this test when there is no or very little customer data traffic being sent for the duration of the test.. Displays the link related test result with respect to Throughput. Link Test can be performed on the ePMP AP and its SM link. In order to run this operation, select the device and then the **Tools** tab. • If an ePMP AP is selected you can choose the SM from the list and start the test.

Table 30: ePMP Tools

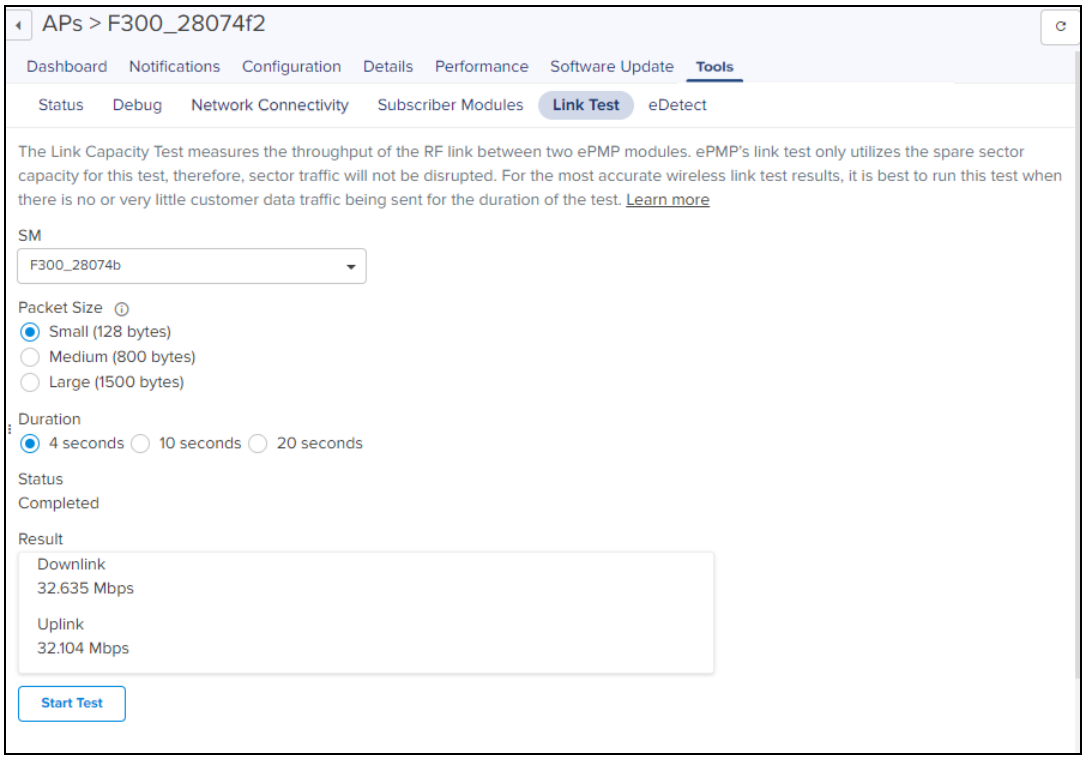
Tools	Description
	 Displays the following fields: • **Packet Size**: Choose the packet size to use for the throughput test. • **Duration**: Choose the time duration in seconds to use for the throughput test. • If an ePMP SM is selected, click **Start** Test to run the link test.

Table 30: ePMP Tools

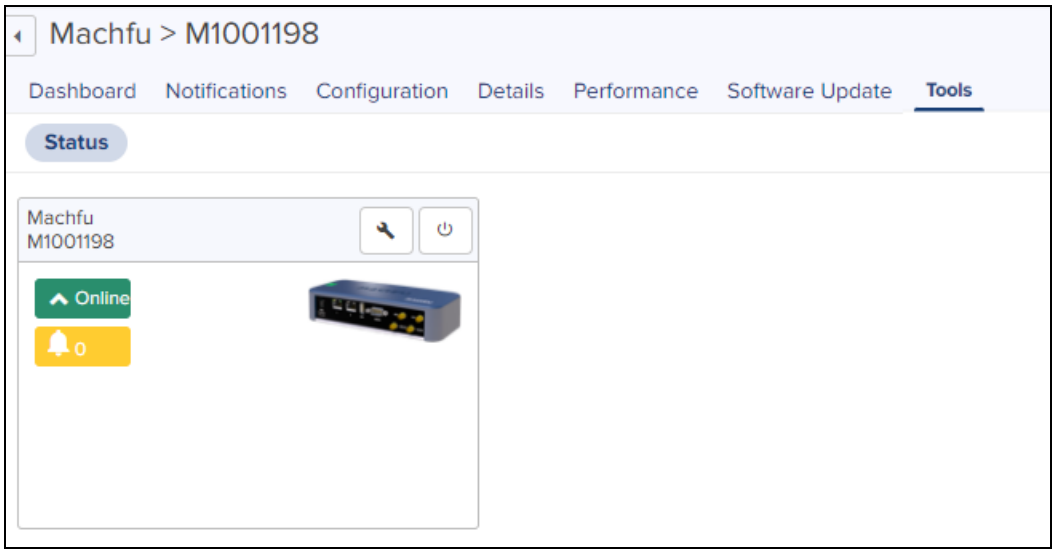
Tools	Description
	 Displays the following fields: • **Packet Size**: Choose the Packet Size to use for the throughput test. • **Duration**: Choose the time duration in seconds to use for the throughput test.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.

Figure 34 ePMP Tools



Machfu

In **Status** tab you can view the status of the device either Online or Offline, allows to download Tech Support File and can reboot the device.



PMP Tools

The Tools page for PMP devices consolidates a number of operations into a single troubleshooting interface.

The operations are listed below:

Table 31: PMP Tools

Tools	Description
Debug	Displays the log details.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.

Table 31: PMP Tools

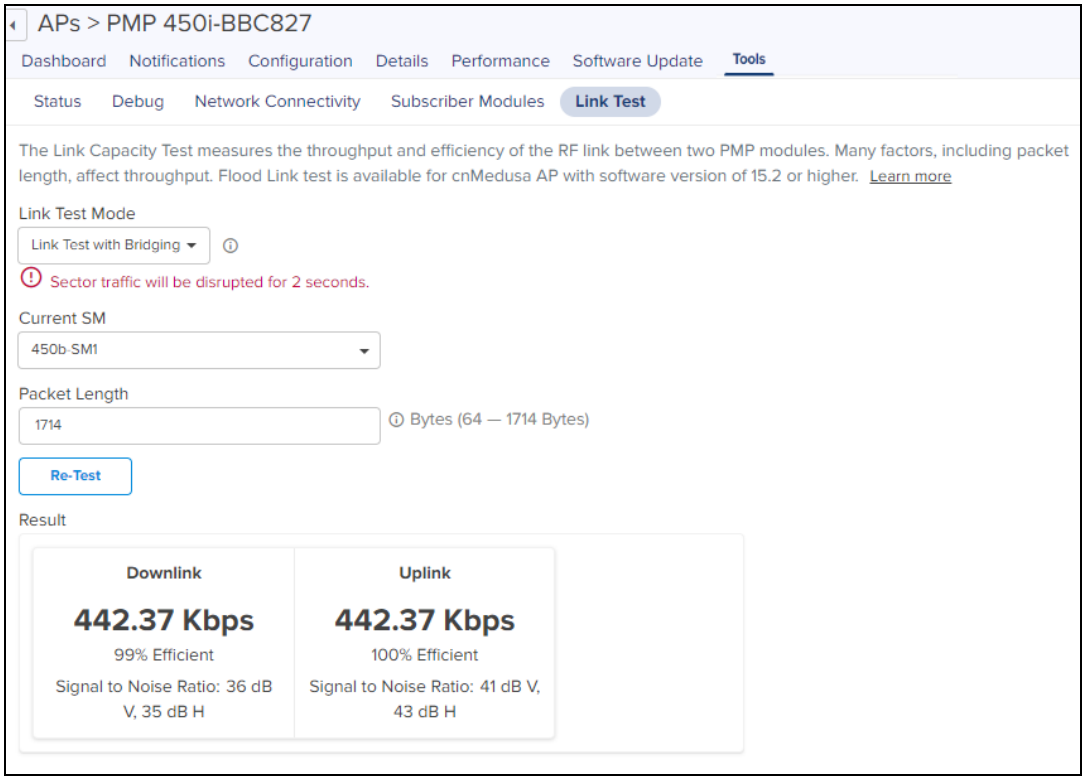
Tools	Description
Subscriber Modules	Lists all the SMs connected to the selected AP. This is available for PMP APs only.
Link Test	The Link Capacity Test measures the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. Packets are added to one or more queues in the AP in order to fill the frame. Throughput and efficiency are then calculated during the test The Link Capacity Test tool has following modes: • **Link Test without Bridging** - Tests radio-to-radio communication, but does not bridge traffic. • **Link Test with Bridging** - Bridges traffic to "simulated" Ethernet ports, providing a status of the bridged link. • **Link Test with Bridging and MIR -** Bridges the traffic during test and also adheres to any MIR (Maximum Information Rate) settings for the link. • **Extrapolated Link Test**: Estimates the link capacity by sending few packets and measuring link quality. Displays the link related test result with respect to Throughput and Interference. Link Test can be performed on the PMP AP and its SM link. In order to run this operation, select the device and then the **Tools** tab. • If a PMP AP is selected you can choose the SM from the list and start the test.  • If a PMP SM is selected, click **Start Test** to run the link test.

Table 31: PMP Tools

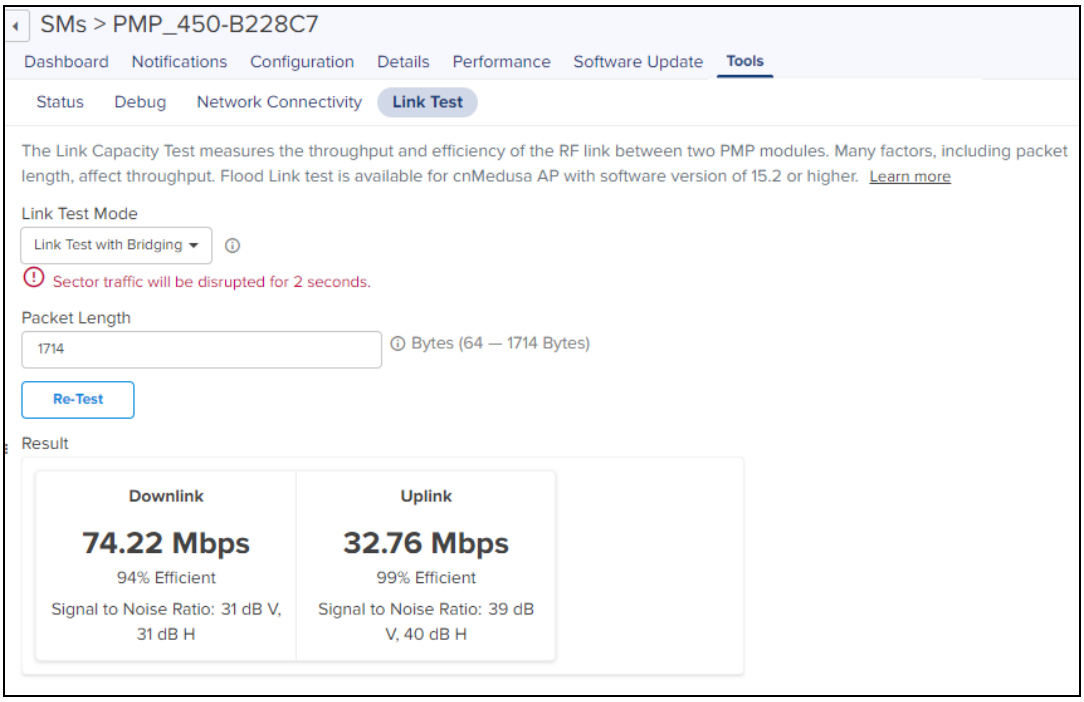
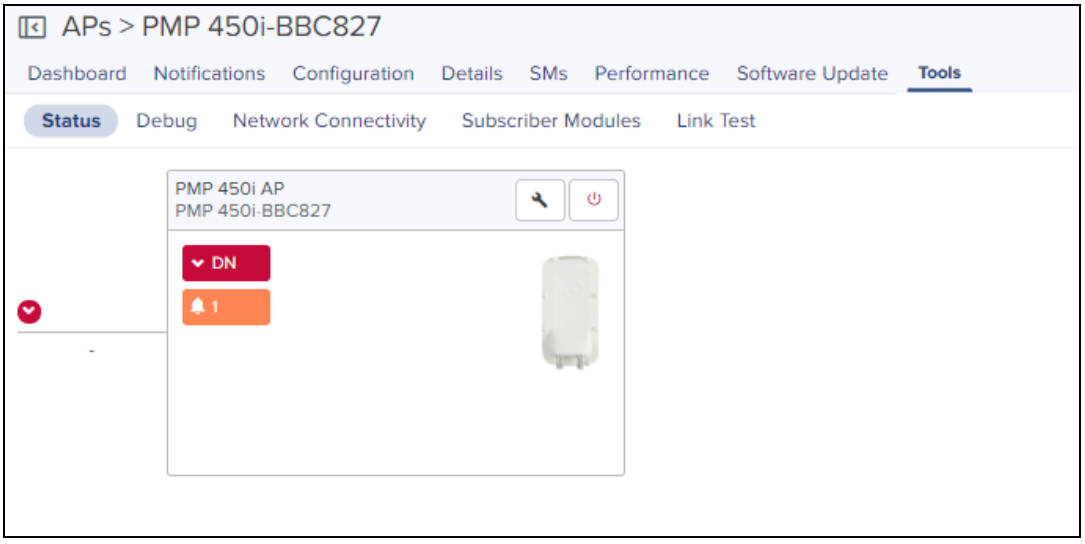
Tools	Description
	

Figure 35 PMP Tools



Tower-to-Edge view

This component displays the network from the Point-to-Multipoint AP to the edge Enterprises devices.

Figure 36 Tower-to-Edge view



WIDS

This section provides details on Rogue APs.

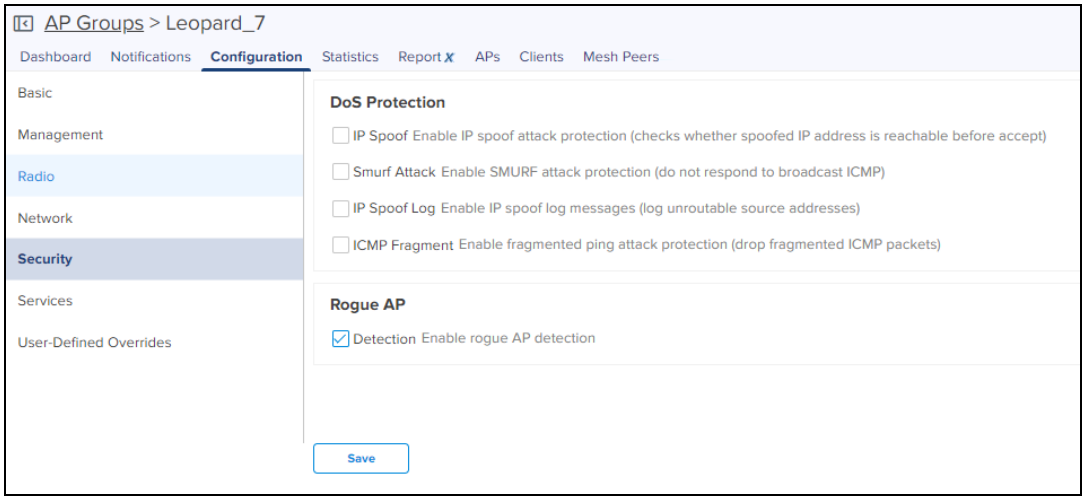
Detecting Rogue APs

A rogue AP is an unsanctioned AP, which is not onboarded to cnMaestro. The AP scans the channels, collects the details about the neighbor APs and sends them to cnMaestro.

Configuring Rogue AP

To enable Rogue AP feature:

1. Navigate to **AP Groups > Configuration > Security** page.
2. Select **Rogue AP Detection** checkbox.



To enable OCS (Off Channel Scan):

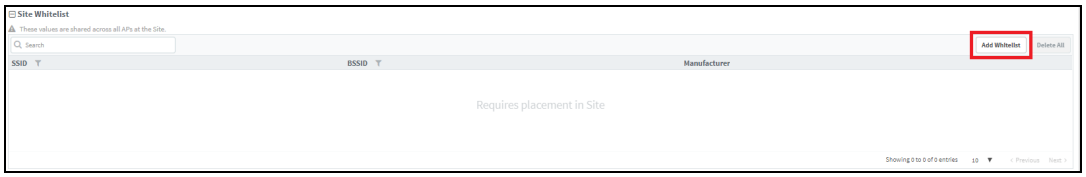
1. Navigate to **AP Groups > Configuration > Radio** (Available on both radio 2.4 GHz and 5 GHz) page.
2. Select the **Enable OCS** checkbox under **OCS** tab.



You can grant valid APs to provide secure access to the network by adding them to the Whitelist by providing their MAC address and SSID.

To add Rogue APs to whitelist:

1. Navigate to **APs > WIDS** page.
2. Click **Add Whitelist** under **Site Whitelist** tab.
3. Enter **MAC** and **SSID** of the device to be whitelisted.
4. Click **Save**.

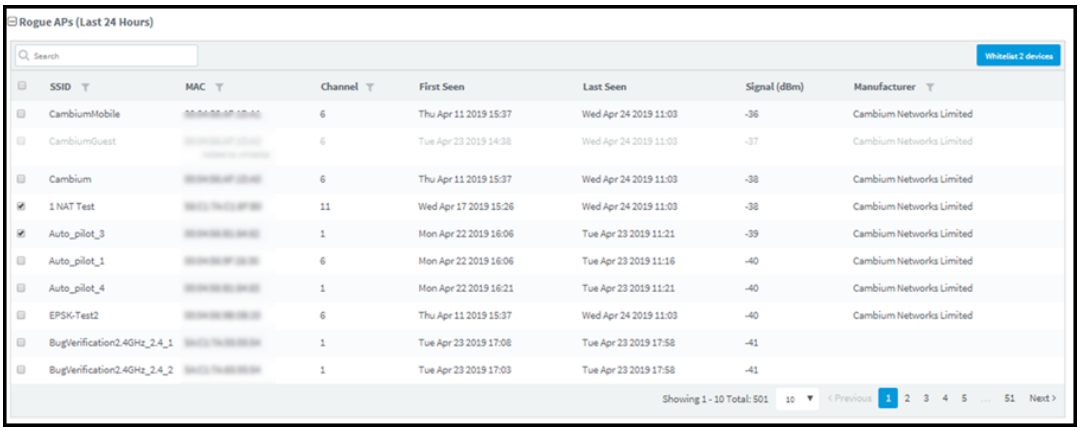


The whitelisted Rogue AP WLAN will be grayed out in Rogue AP list and it will be removed after 24 hours.

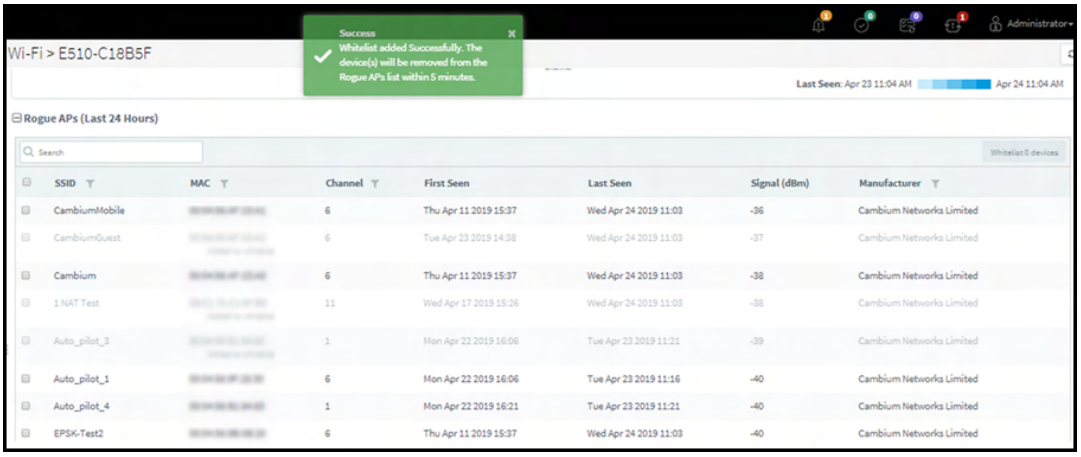


To whitelist multiple Rogue APs:

1. Select the Rogue APs in the list.
2. Click **Whitelist Devices.**

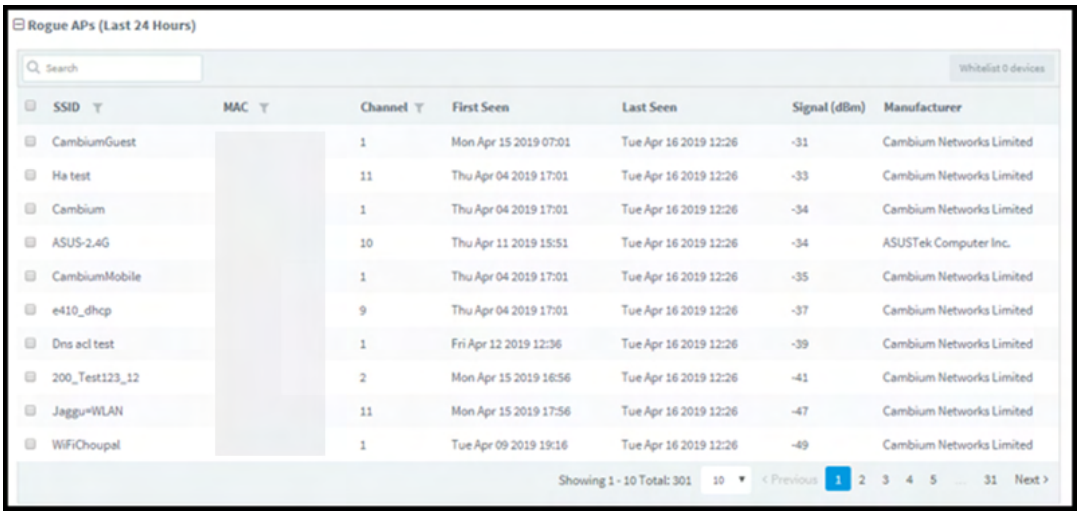


The following pop-up is displayed after successfully adding the Rogue APs to the whitelist.



View List of Rogue APs

The user can view list of Rogue APs at the device level in the Monitor page:

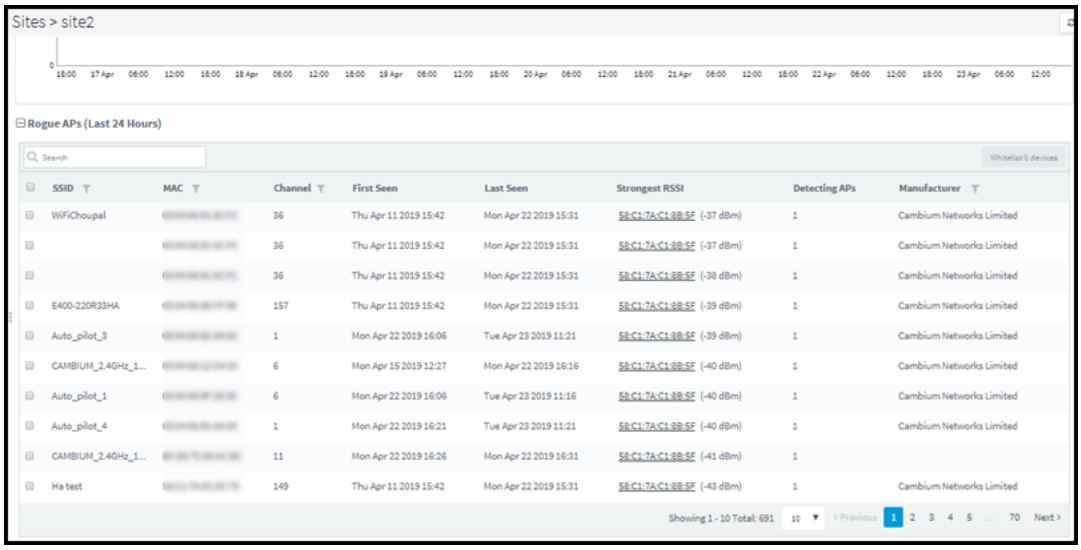


The following parameters are displayed:

- **SSID**: SSID of the Rogue AP.
- **MAC**: MAC address of the Rogue AP.
- **Channel**: Channel in which the Rogue AP operates.
- **First Seen**: Time at which the Rogue AP is detected for the first time.

- **Last Seen**: Time at which the Rogue AP is detected last.
- **Signal:** Signal strength of the Rogue AP detected by the device.
- **Manufacturer**: Manufacturer of the Rogue AP (Cambium, Cisco, Aruba, etc).

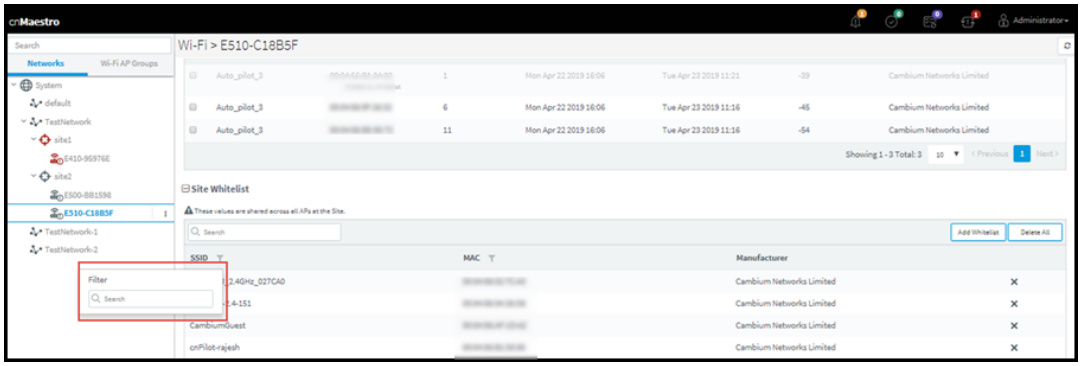
The user can view list of Rogue APs at the Site level in the Monitor page:



The following parameters are displayed:

- **SSID**: SSID of the Rogue AP.
- **MAC**: MAC address of the Rogue AP.
- **Channel**: Channel in which the Rogue AP operates.
- **First Seen**: Time at which the Rogue AP is detected for the first time.
- **Last Seen**: Time at which the Rogue AP is detected last.
- **Strongest RSSI:** Rogue AP RSSI which is detected strongest RSSI by AP.
- **Detecting AP:** Number of APs detecting the same Rogue AP.
- **Manufacturer**: Manufacturer of the Rogue AP (Cambium, Cisco, Aruba, etc).

You can search for a specific Rogue AP based on the MAC, SSID, Channel, and the Manufacturer by using the search option.



NOTE:

1. OCS (on both 2.4 GHz and 5 GHz) and Rogue AP detection should be enabled for WIDS option to work at site and device level in cnMaestro.

2. It takes 5 minutes to detect Rogue AP on AP boot up.

cnPilot Dashboards

Device Dashboard

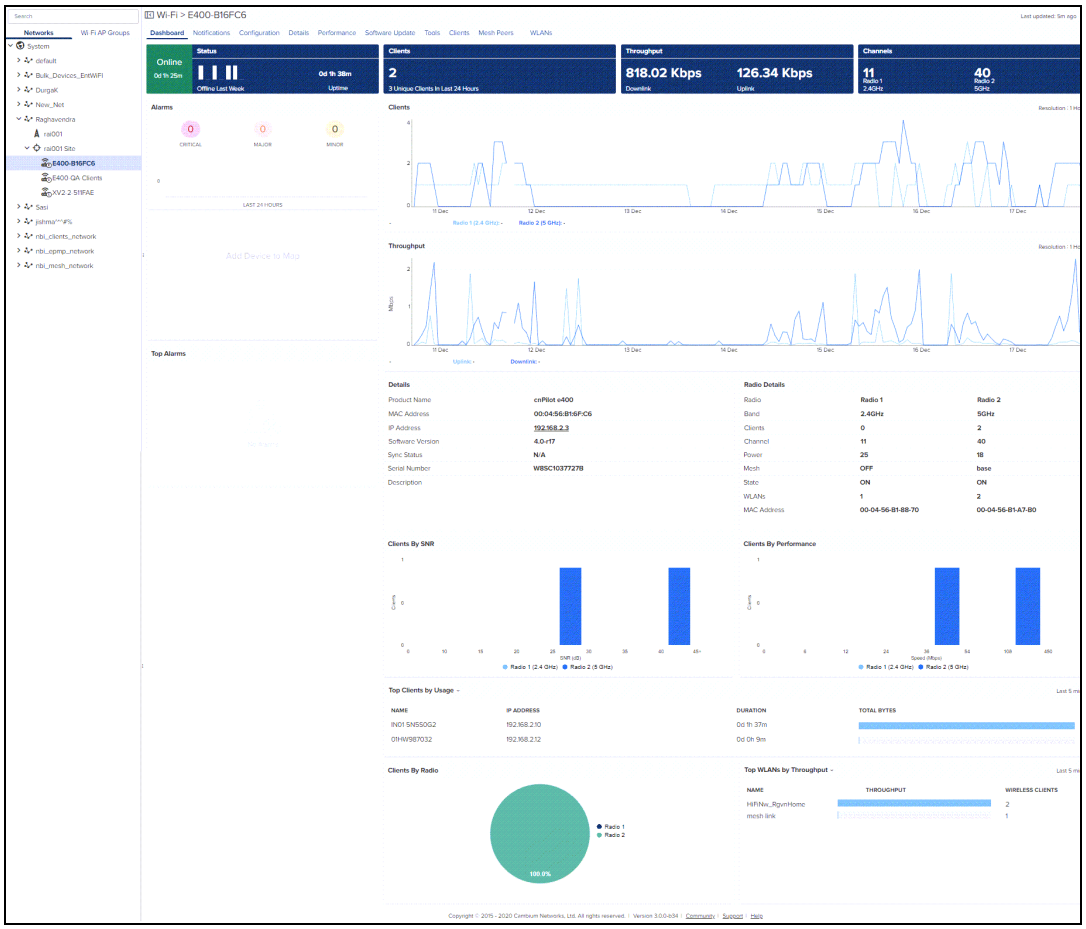
The Device Dashboard page displays details of all the Wi-Fi devices in cnMaestro. It mainly focuses on the following parameters:

- Overview
- Clients
- Network Info
- Mesh Peers
- Neighbors

Overview

The overview section displays the radio **Details, Clients, Throughput, Channels, Top Alarms, Clients by SNR, Clients by Performance, Clients by Radio, Top Clients by Usage,** and **Top WLANs by Throughput**.

Figure 37 Device Dashboard > Overview Page



Clients

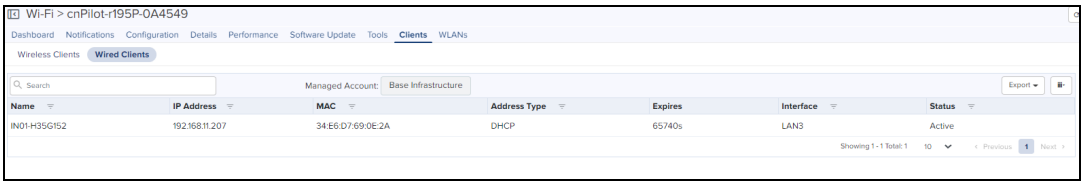
The **Clients** section displays the details of all the wireless and wired clients.

Following parameters are displayed for wired clients for cnPilot Home Series:

- Address Type

- Expires
- Interface
- IP Address
- MAC Address
- Name
- Status

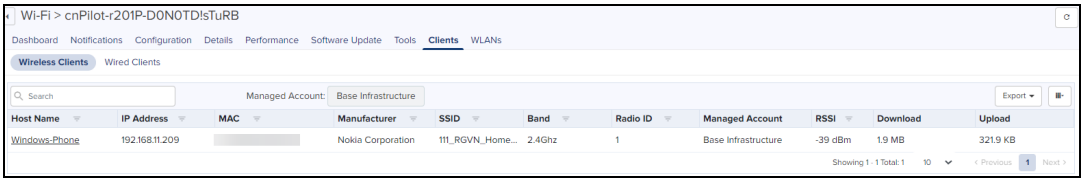
Figure 38 cnPilot Home: Device Dashboard > Wired Clients Page



Following parameters displays for Wireless Clients of R-Series:

- Band
- Download
- Host Name
- IP Address
- MAC
- Manufacturer
- RSSI
- WLAN
- Upload

Figure 39 cnPilot Home: Device Dashboard > Wireless Clients Page

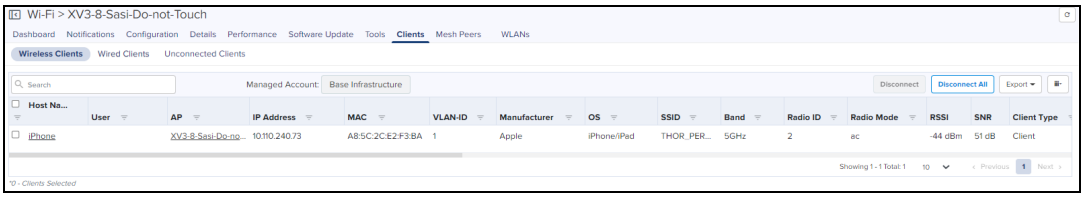


Following parameters displays for Wireless Clients of E-Series:

- Actions
- Authentication
- Band
- Client Type
- Download
- Download Quota
- Download Quota Balance
- GA Mode
- Guest Access Type
- Host Name
- IP Address
- MAC
- Manufacturer

- Managed Account
- Mode
- OS
- RSSI
- SNR
- Session Expiry
- Type
- User
- Upload
- Upload Quota
- Upload Quota Balance
- VLAN
- WLAN

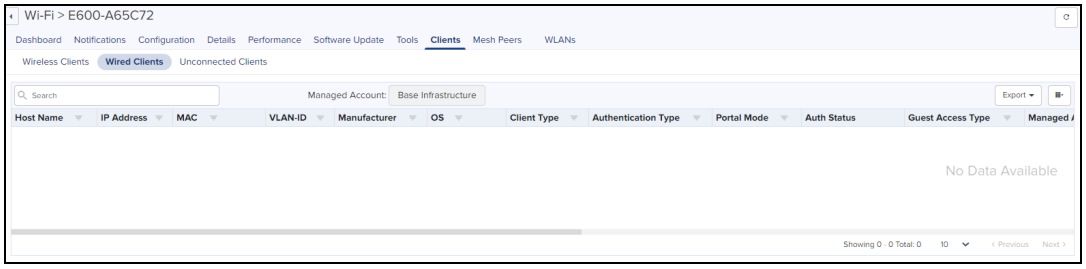
Figure 40 Enterprise Wi-Fi: Device Dashboard > Wireless Clients Page



Following parameters displays for Wired Clients of E-Series:

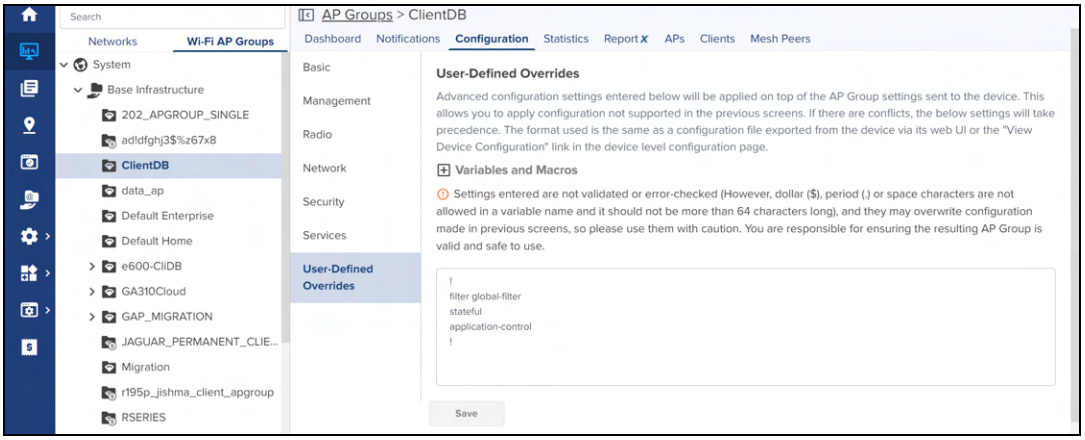
- Authentication
- Auth Status
- Client Type
- Download
- Download Quota
- Download Quota Balance
- Guest Access Type
- Host Name
- IP Address
- MAC
- Manufacturer
- OS
- Portal Mode
- Total Quota
- Total Quota Balance
- User
- Upload
- Upload Quota
- Upload Quota Balance
- VLAN

Figure 41 Enterprise Wi-Fi: Device Dashboard > Wired Clients Page



Dashboard

The user can view the applications used by client when the application visibility option is enabled as shown below:



The Client Dashboard displays the details of the clients connected to the Wi-Fi device.

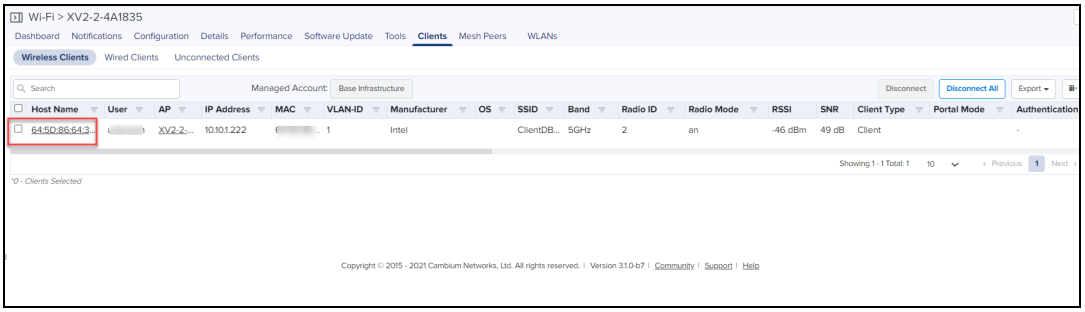
NOTE:

- Enable the Application Visibility feature to view **Application** page and supported only for XV-series devices.
- Dashboard is supported for all cnPilot devices.

To view the **Dashboard**, navigate to **Clients** > **Wireless Clients** and click **Host Name**.

It navigates to detailed client **Dashboard** as shown below:

Figure 42 XVseries: Device Dashboard > Wireless Client Page



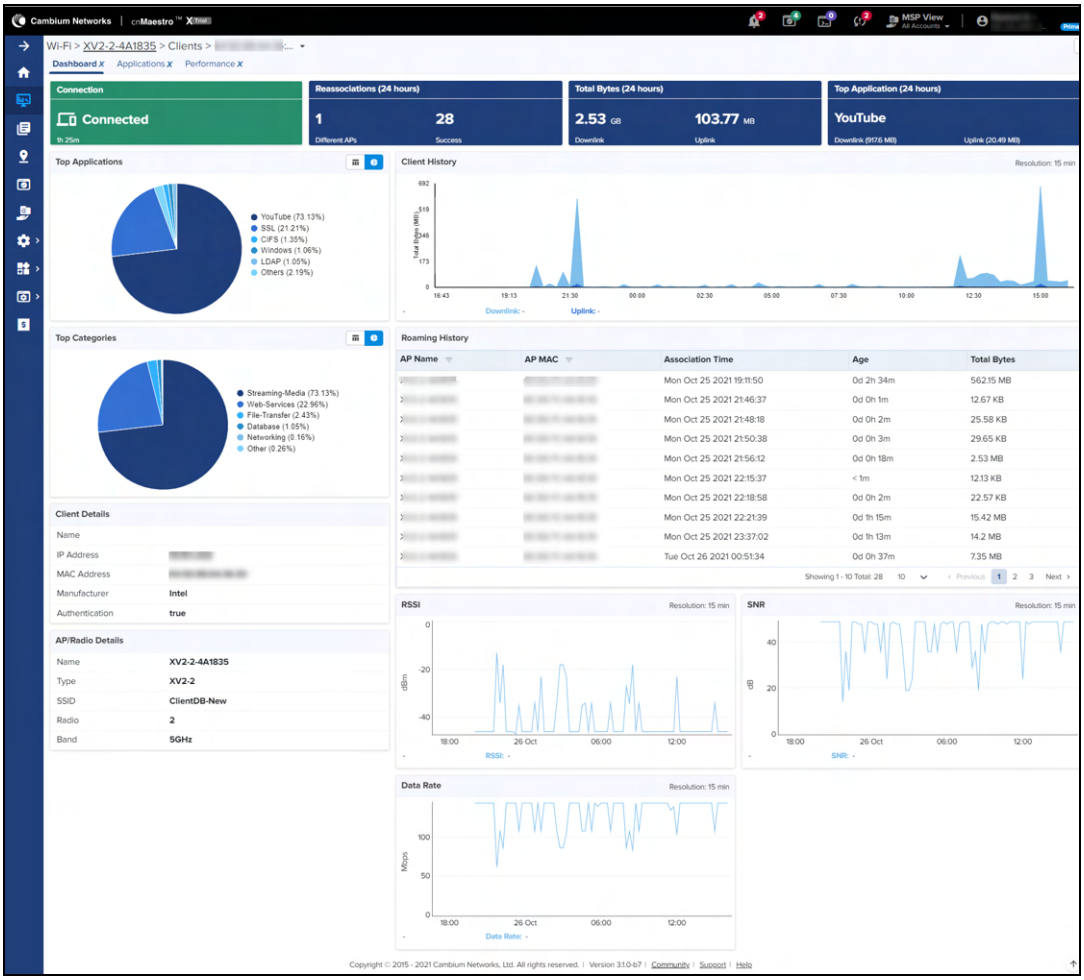
The following parameters are displayed for wireless clients for XV-series:

- AP/Radio Details
- Client Details
- Client History
- Connection

- Reassociations
- Roaming History
- Top Applications
- Top Application (24 hours)
- Total Bytes (24 hours)
- Top Categories

The client traffic distribution in Uplink and Downlink direction during last 24 hours is buffered every 5 minutes granularly.

User can hover over the piechart to view specific application usage and in linear graph to view date, timings, Downlink, and Uplink data statistics.



Application

The **Application** tab displays the details **Total Bytes**, **Top Application**, **Top Category**, and **Application History**.

The Application data is displayed for 24 hours or 7 days.

- **Total Bytes** - represents the Uplink and Downlink of the client data usage across applications.
- **Top Application** - represent top application.
- **Top Category** - represent single category specific to the top application.

NOTE:
- Advance Client Dashboard is applicable for cnMaestro X.
- Application usage data is applicable for only XV series of devices.

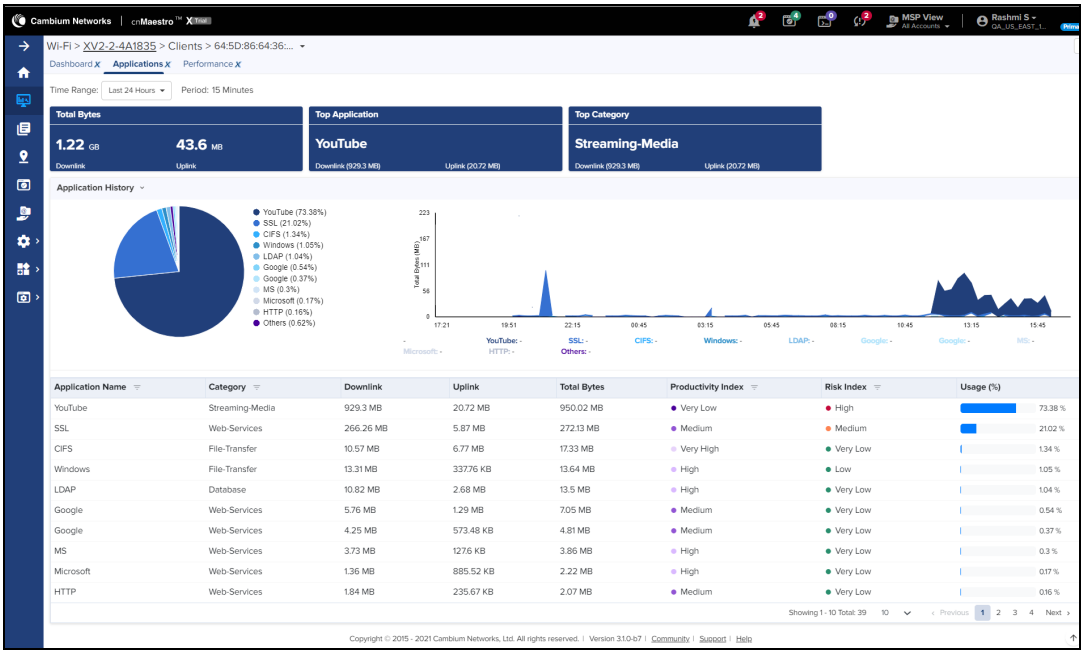
User can view the data usage in single format (pie chart). You can select type of history from the drop-down.

- **Application History** - displays data usage of top 10 and others applications in pie and linear graph format.
- **Category History** - displays data usage for list of categories in pie and linear graph format.

The following parameters are shown:

Table 32: Application fields

Field	Description
Application Name	Name of the application.
Category	Category of the application.
Downlink	Downlink of application data.
Productive Index	Index label for each application to reflect the overall productivity of network users.
Risk Index	Index label for each application to reflect undesirable content onto network.
Total Bytes	Total number of application data in bytes.
Uplink	Uplink of application data.
Usage	Percentage of data usage by application.



Performance

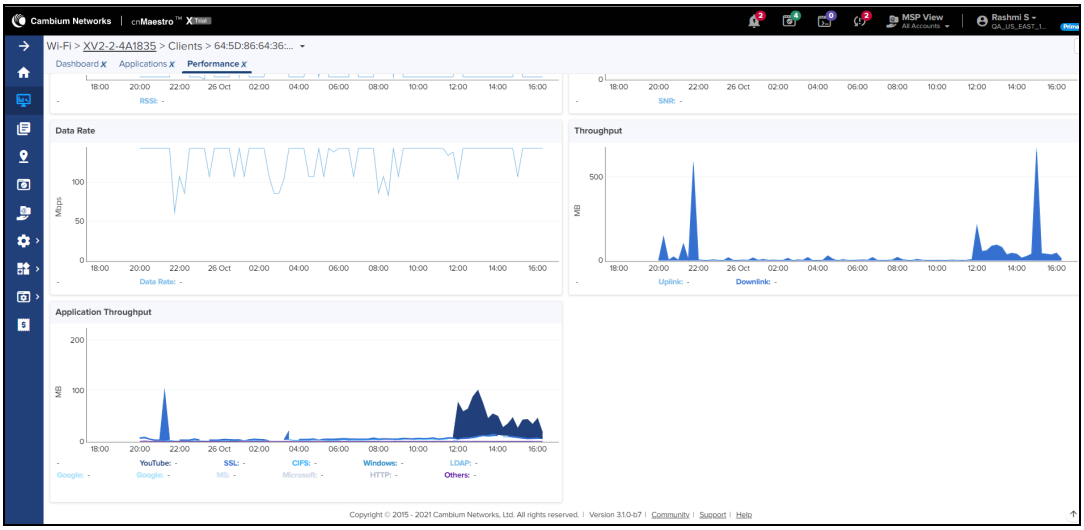
The **Performance** tab displays a synchronized view of time-series data which includes parameters for client's connection health, application usage.

The client data usage can be viewed based upon on **Time Range which is shown in four different quadrants.**

- User can select the Time Range by **Last 24 Hours** or **Last 7 Days.**
- User can hover over the pie chart to view specific application usage and in linear graph to view date, timings, Downlink, and Uplink values.

The following client data parameters are shown:

- Application Throughput
- Data Rage
- RSSI
- SNR
- Throughput



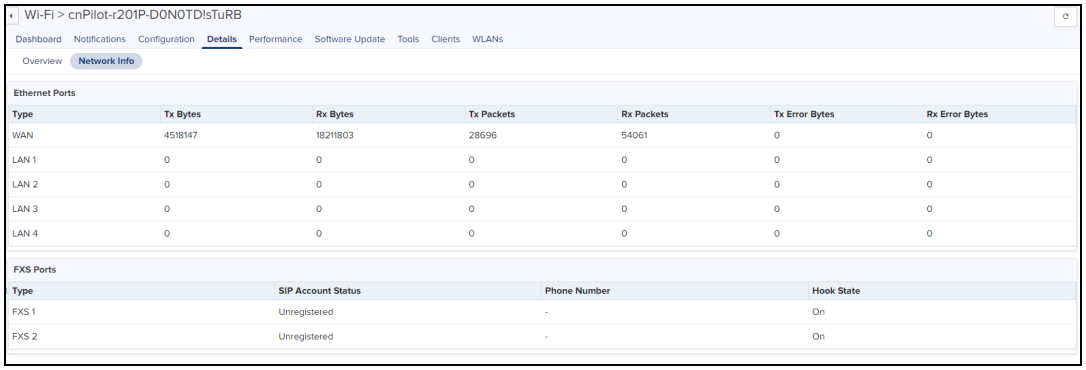
Network Info

The Network Info section displays the details of the Network.

Following parameters are displayed for cnPilot Home router:

- Ethernet Ports
  - Type
  - Tx Bytes
  - Rx Bytes
  - Tx Packets
  - Rx Packets
  - Tx Error Bytes
  - Rx Error Bytes
- FXS Ports
  - Type
  - SIP Account Status
  - Phone Number
  - Hook State

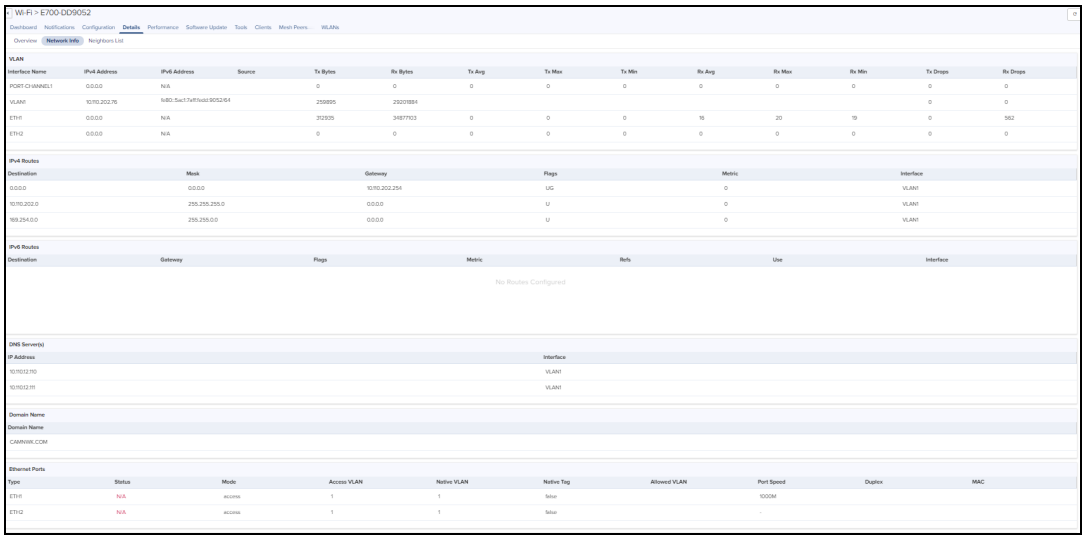
Figure 43 cnPilot Home: Device Dashboard > Network Info Page



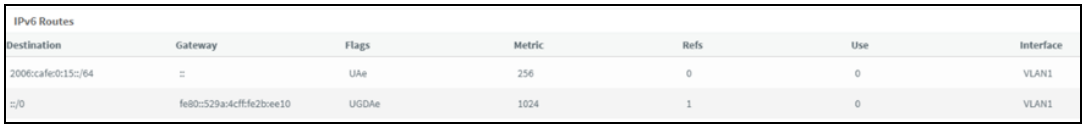
Following parameter details are displayed in E-Series:

- VLAN
- Routes
- DNS Server(s)
- Domain Name
- Ethernet Ports
- Tunnels
- PPPoE

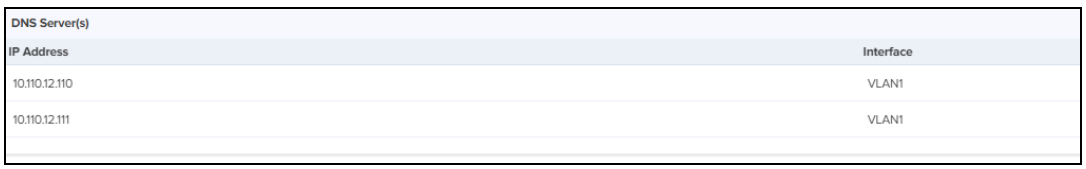
Figure 44 Enterprise Wi-Fi: Device Dashboard > Network Info Page



IPv6 Routes



DNS Servers



Following parameter details are displayed in E-Series:

- Port
- Tx Octets
- Rx Octets
- Tx Frames
- Rx Frames
- Rx Frames with Error
- Tx Broadcasts
- Rx Broadcasts
- Rx Frames Undersize
- Rx Frames Oversize

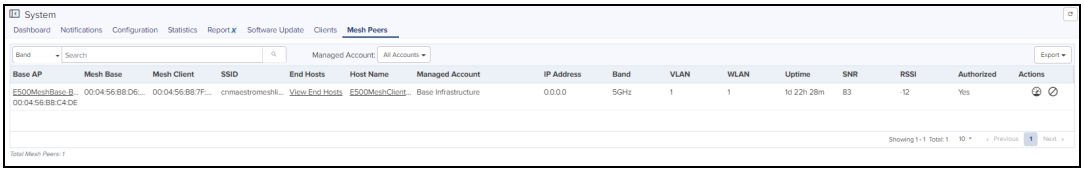
Figure 45 PTP: Device Dashboard > Network Info Page



Mesh Peers

The **Mesh Peers** tab displays information related to mesh clients and respective RF parameters such as SNR, RSSI, and Band. This tab helps the user to trigger Wi-Fi performance between the Mesh Client and Mesh Base.

Figure 46 Device Dashboard > Mesh Peers Page

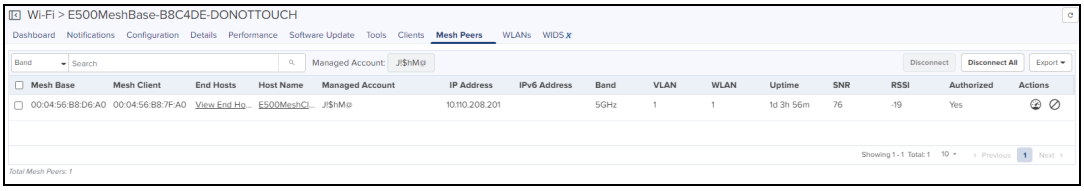


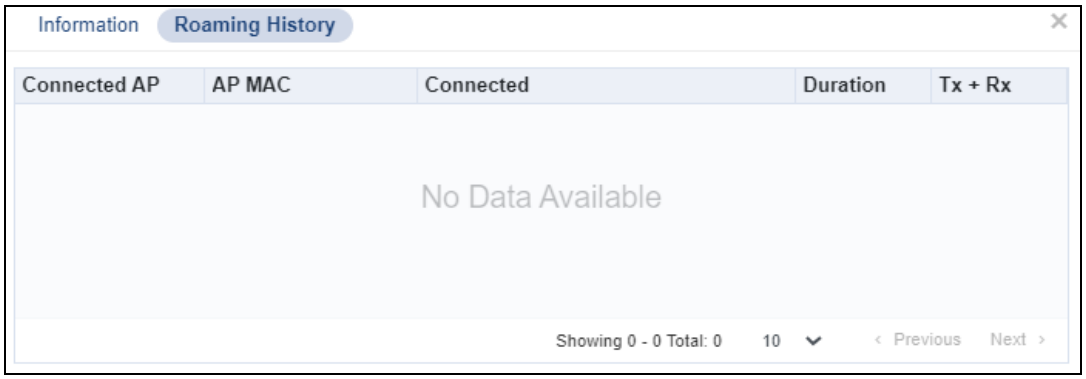
You can also perform the Wi-Fi performance test by clicking the icon in the **Action** field.

Roaming History for Mesh Peers

The roaming history provides details of the mesh clients such as **Connected AP, AP MAC, Duration**, number of packets transferred and received by the clients (Tx and Rx), duration etc during roaming from one mesh base to a different mesh base.

Figure 47 Roaming History for Mesh Peers

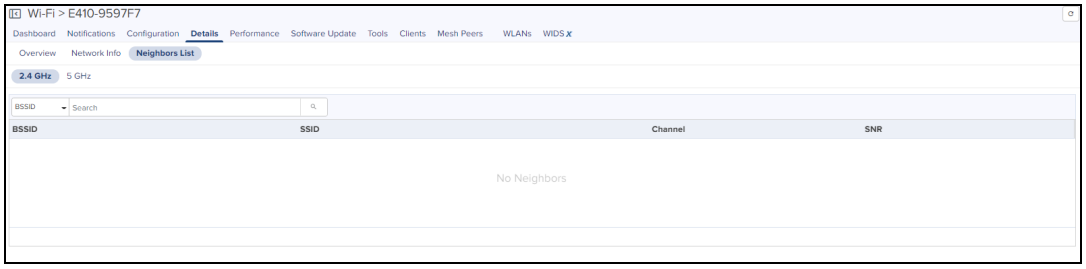




Neighbors

Displays the BSSID, SSID, Channel, RSSI details of neighboring 2.4 GHz and 5 GHz radios.

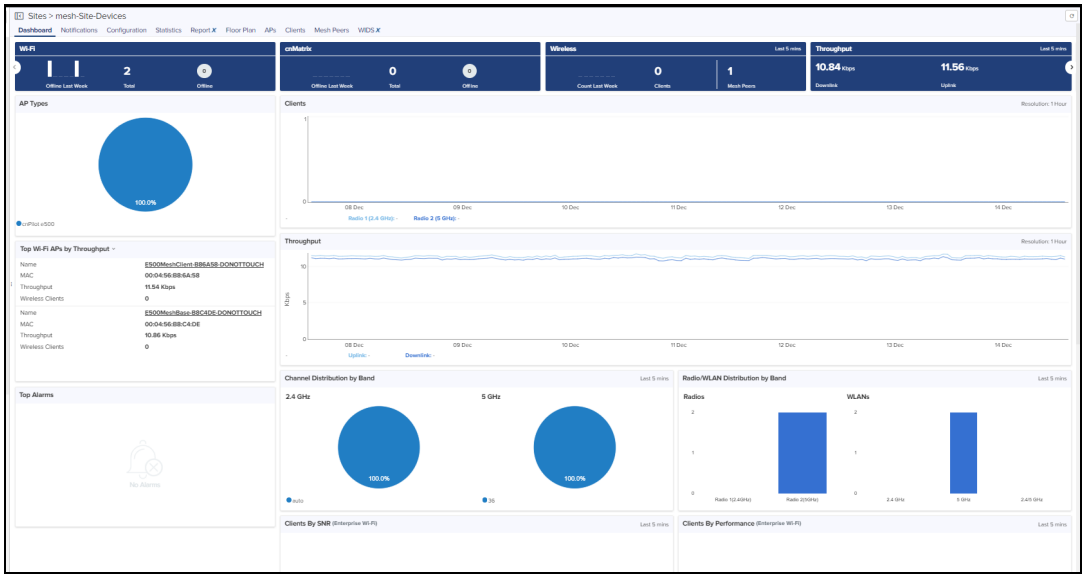
Figure 48 Device Dashboard > Neighbors Page



Site Dashboard

The Site dashboard page provides the overview of site related parameters and devices as shown below:

Figure 49 Site Dashboard



The Site Dashboard displays the following parameters:

- AP Types
- Channel Distribution by Band
- Clients by SNR

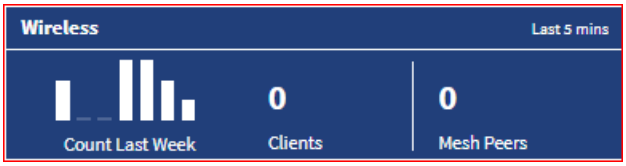
- Clients by Performance
- Floor Plan
- Radio/WLAN Distribution by Band
- RF Quality
- Throughput
- Top Wi-Fi APs
- Throughput Graph
- Wi-Fi Devices Availability (Total and Offline)
- Clients Graph
- Statistics
- Wireless Clients

Wi-Fi Devices Availability (Total and Offline)

Displays total number of access points in the site and the devices that are offline.



Wireless

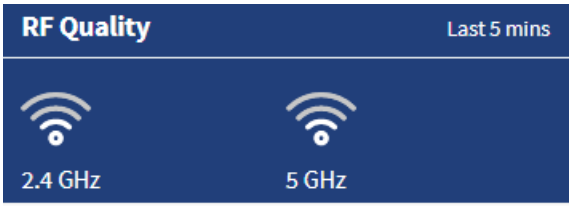


Throughput

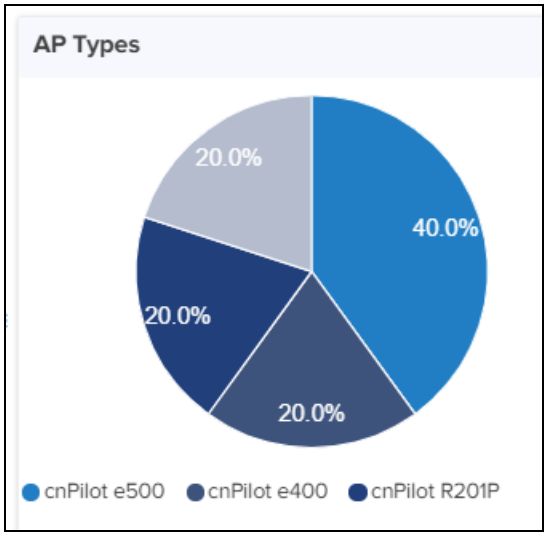
Displays aggregated throughput for all the clients.



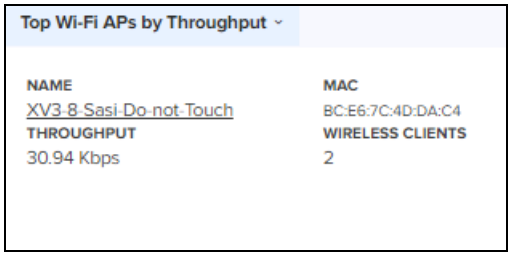
RF Quality



AP Types

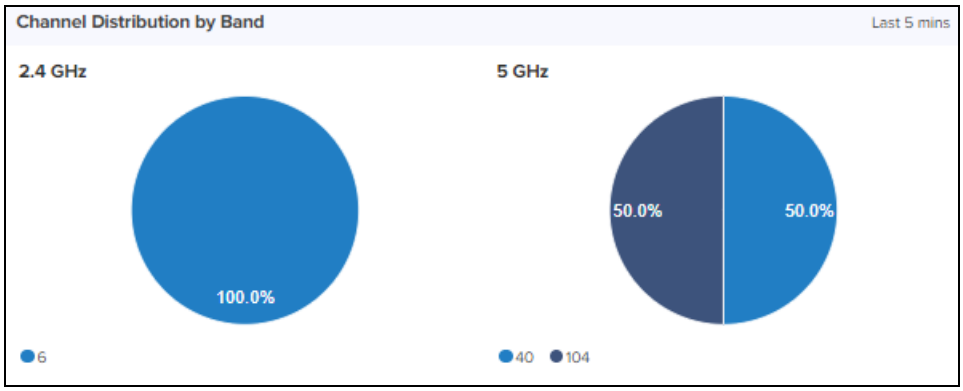


Top Wi-Fi APs

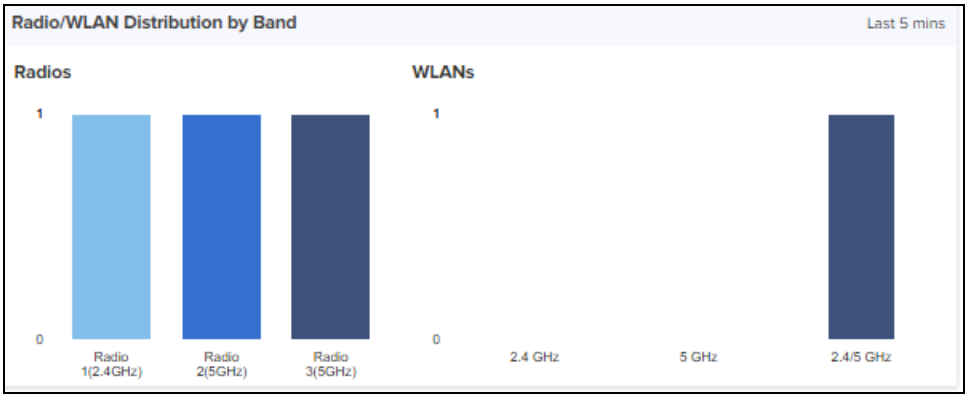


Channel Distribution by Band

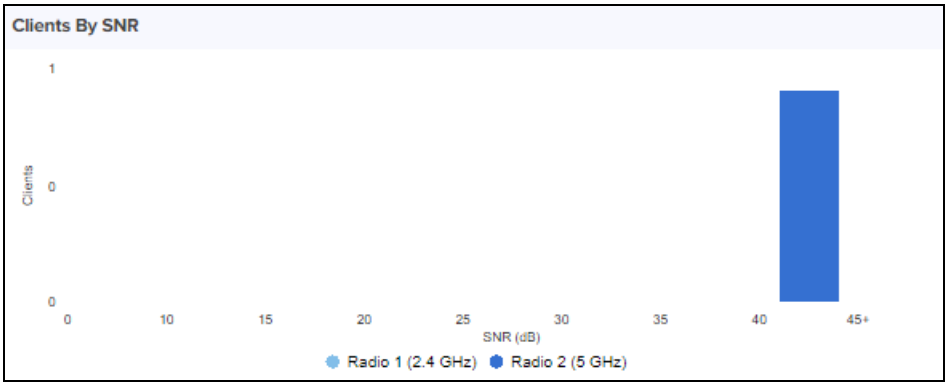
Channel Distribution by AP displays usage of channels in 2.4 GHz and 5 GHz. This helps users in planning and implementing WLANs within a high-density environment.



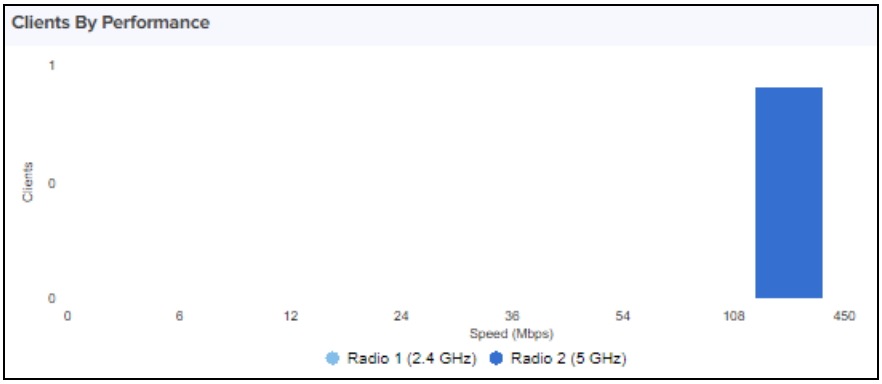
Radio/WLAN Distribution by Band



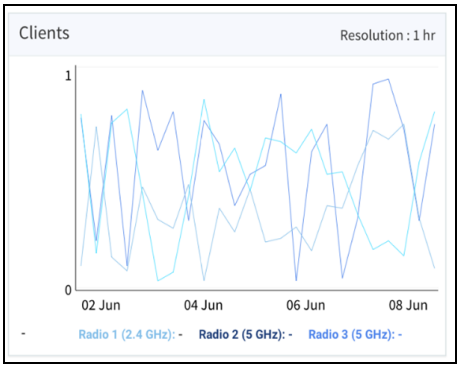
Clients by SNR



Clients by Performance

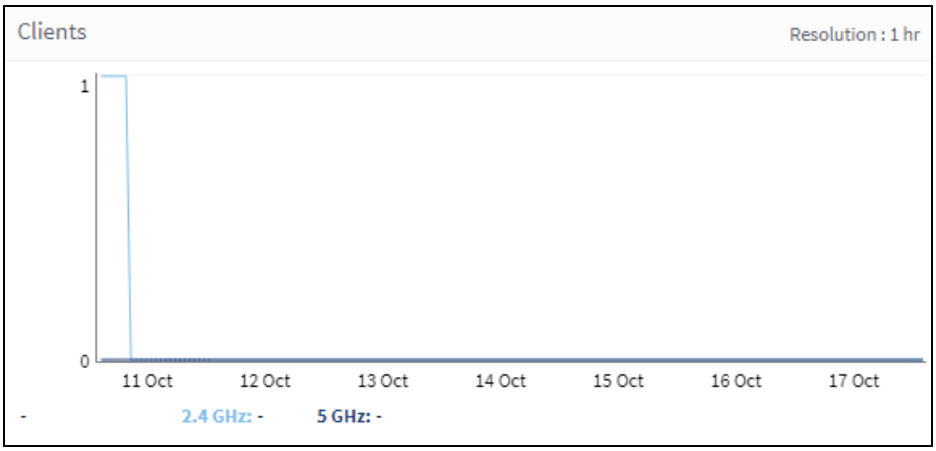


Clients By Performance (For XV3-8)



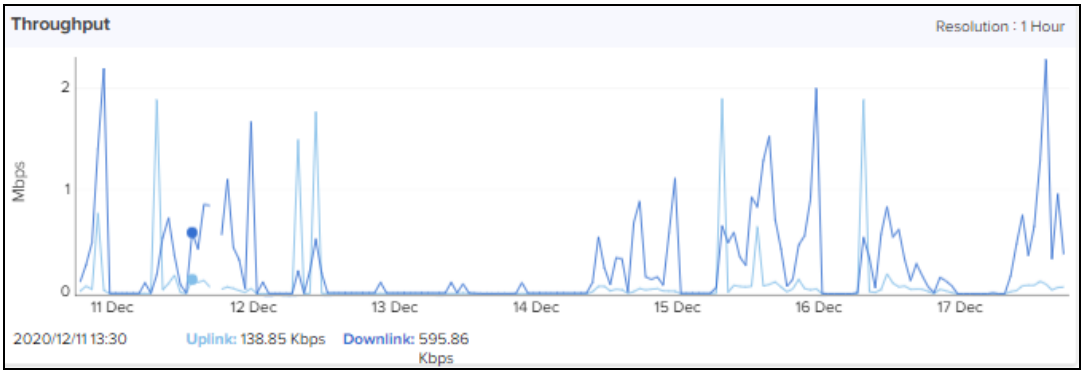
Clients Graph

Clients Graph displays clients that are connected in 2.4 GHz and 5 GHz for the last week.



Throughput Graph

Throughput Graph displays client traffic for the last week.

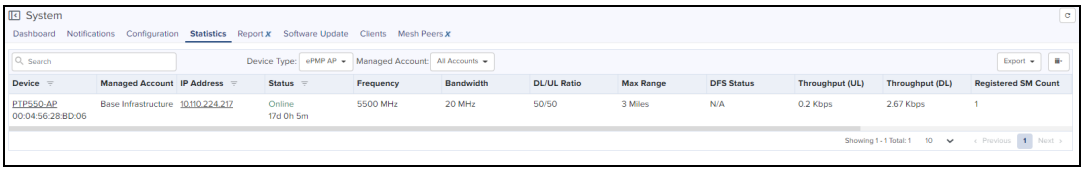


Statistics

Statistics displays following parameters:

- Channel
- Device
- IP Address
- Managed Account
- Power
- Product Name
- Status
- Throughput (DL)
- Throughput (UL)
- Type

User can **Export Statistics** data to PDF or CSV.

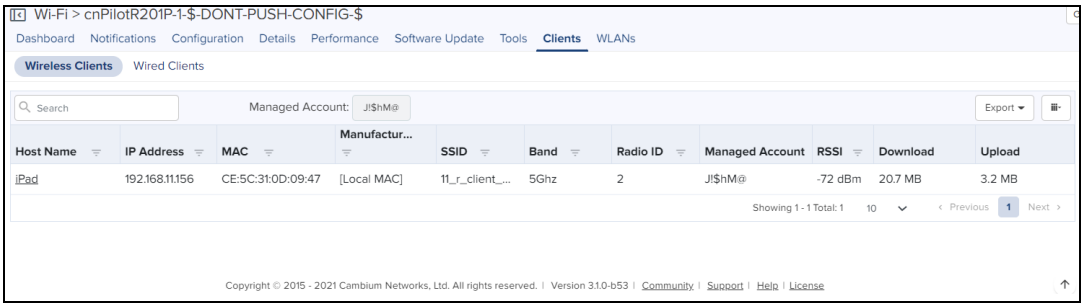


Wireless Clients

Wireless Clients displays following parameters:

- Auth Status
- Authentication Type
- Band
- Client Type
- Host Name
- IP Address
- MAC
- Manufacturer
- Mode
- OS
- Portal Mode
- RSSI
- SNR
- Session Expiry
- User
- VLAN-ID
- WLAN

The table can be exported as PDF or CSV.

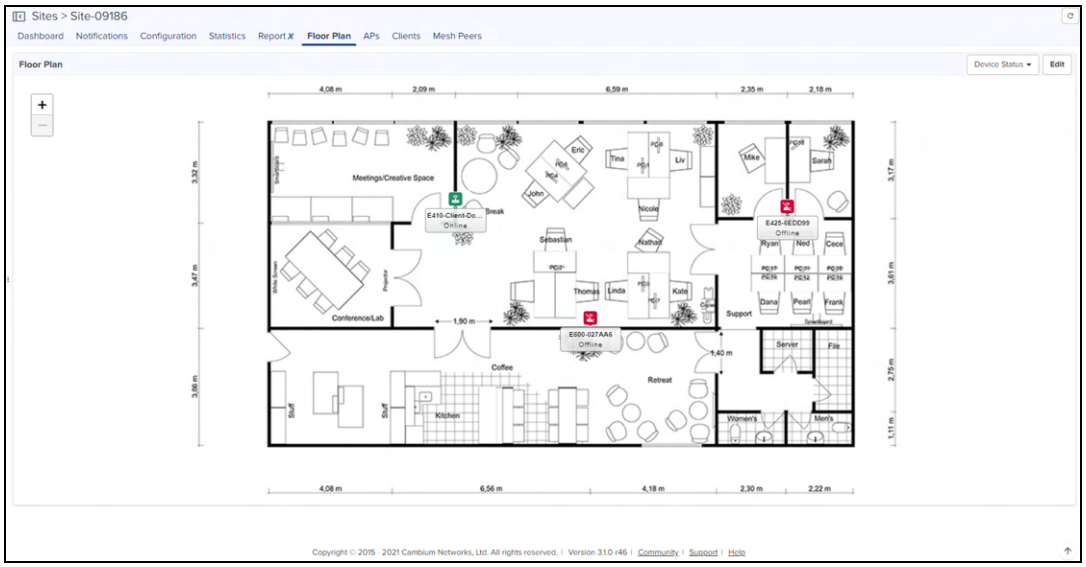


Floor Plan

Floor Plan is used to locate all APs on the map (and present device status, connected clients, and Tx power). This is done by uploading the map in **Site > Floor Plan > Edit > Upload** or floor map can be uploaded when site is created. Placing the APs on the floor map is done by clicking full-screen option and then click edit; then place the APs on the map and click **Save**.

NOTE:
While uploading the floor plan follow the recommended specifications such as:

- Resolution: 1024 px X 800 px
- Supported file types: jpeg, jpg, png, and gif
- File size: not more than 5 mb.



Inventory

The Inventory displays a list of devices under the selected node. It presents health and maintenance information that can be toggled through a button bar at the top. It aggregates children devices and provides a tabular view that allows for sorting and filtering. When selected for a single device, it presents a detailed page tailored to that device.

Navigate to **Inventory**.

Figure 50 Inventory - Access and Backhaul and Industrial Internet View

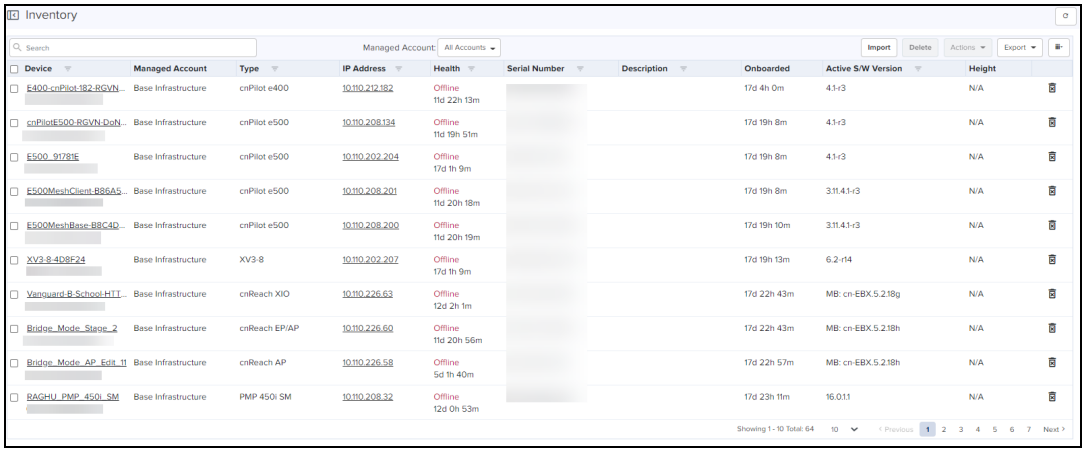
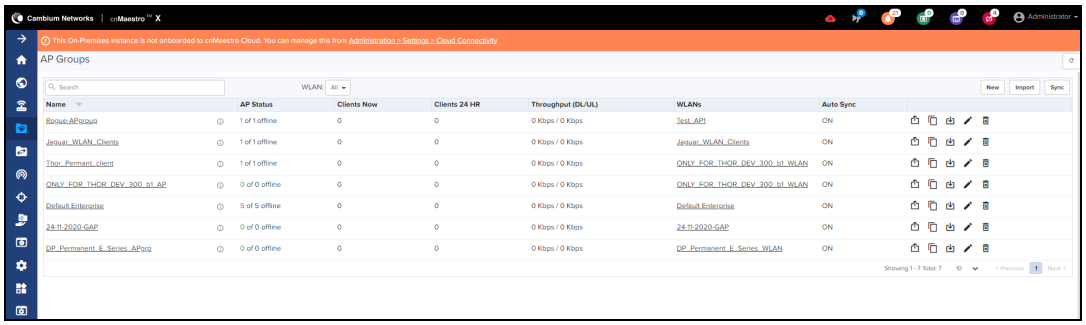


Figure 51 Inventory - Enterprise View



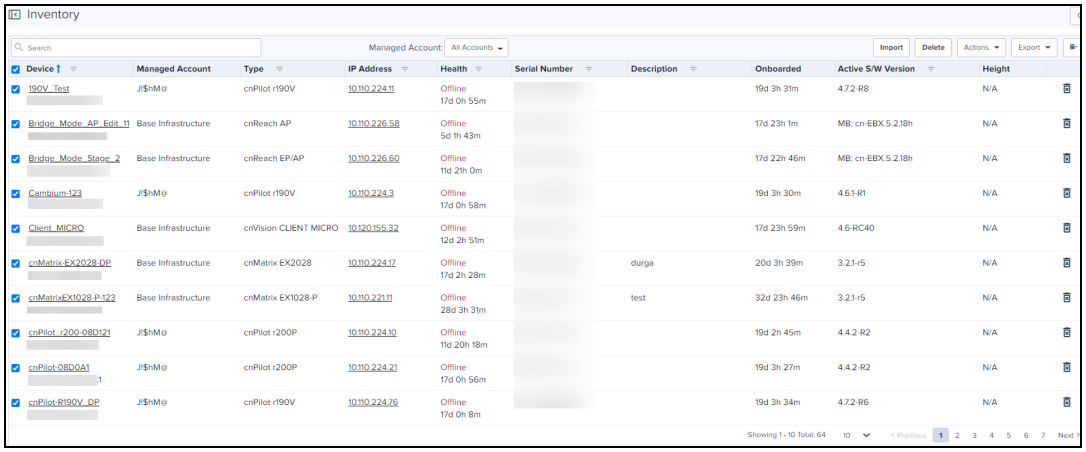
Inventory Export

The inventory can be exported in either CSV or PDF format. The values exported will match those in the selected table columns. You can customize the health and maintenance views to add or delete columns.

Bulk Delete

The **Bulk Delete** is available in the inventory page of System/Network/Tower/Site in cnMaestro On-Premises. This feature helps the users in bulk deletion of devices from System/Network/Tower/Site.

Figure 52 Bulk Delete



To delete devices using Bulk Delete, perform the following steps:

1. Navigate to **Inventory** page of System/Network/Tower/Site.
2. Select one or multiple devices as per the requirement.
3. Click **Delete**.

> **NOTE:**
>
> In Wi-Fi view, Bulk Delete can also delete the devices that are in waiting for approval state.

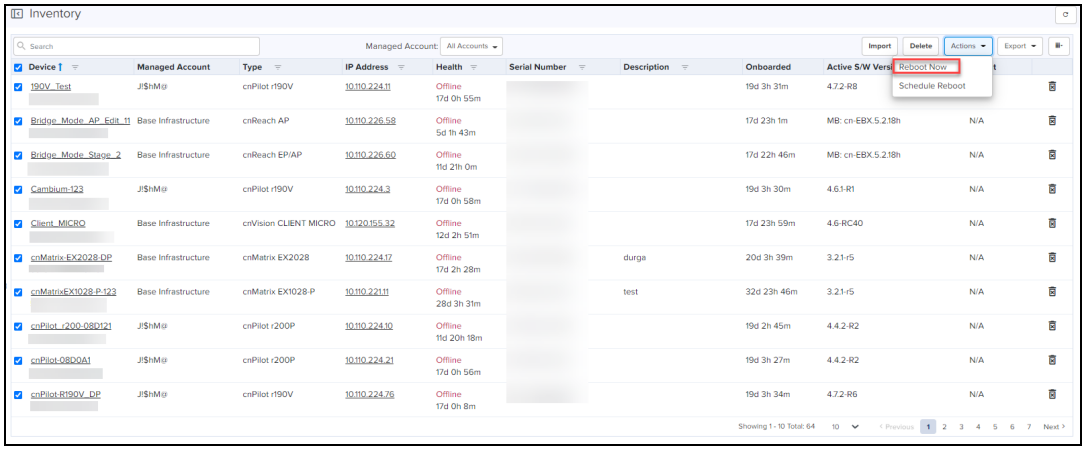
Bulk Reboot

The **Bulk Reboot** is available in the inventory page of Network/Tower/Site in cnMaestro On-Premises.

This feature helps the users in bulk reboot of devices.

When the devices are moved using the Bulk Reboot option, all the **Network/Tower/Site Dashboards, Graphs, Clients, Reports, and Mesh Peers** will also get updated accordingly.

Figure 53 Bulk Reboot

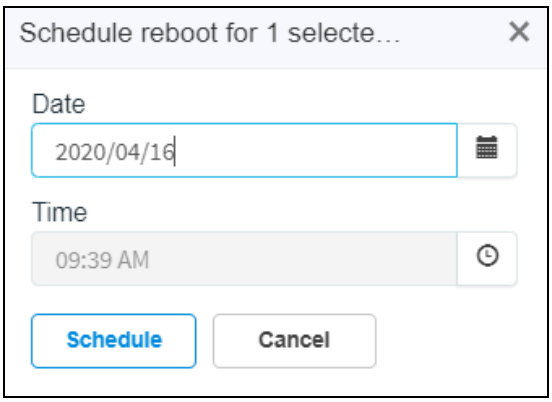


To reboot devices using Bulk Reboot:

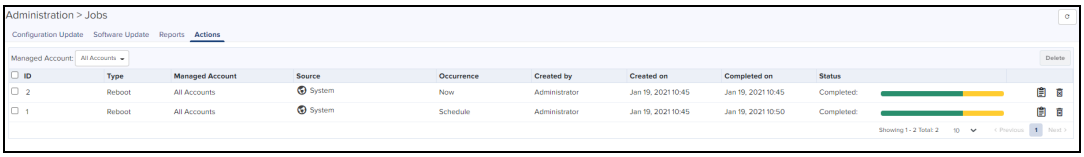
1. Navigate to **Inventory** page of Network/Tower/Site.
2. Select one or multiple devices as per the requirement.
3. Click **Actions** and choose **Reboot Now**.

Schedule Reboot

You can also schedule reboot of the device/devices by selecting **Schedule reboot** from **Actions** drop-down list, and by providing the **Date** and **Time**.



After creating a scheduled reboot job, you can view the status in the **Administration > Jobs > Actions** page.



CSV Configuration Import

Import device(s) configuration is available from inventory page at System/Network/Managed Account/ePMP or PMP AP device levels.

> **NOTE:**
>
> The Import Device configuration is supported only for the Access and Backhaul account and is applicable only on ePMP/PMP AP and SM devices.

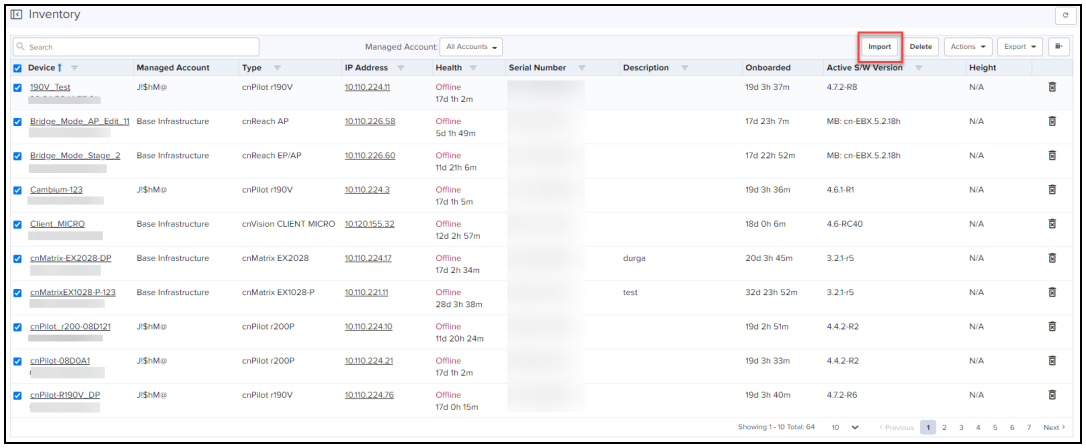
The following parameters are supported for ePMP/PMP AP in the CSV file:

- Azimuth
- Beam Width
- Elevation
- Height
- Latitude
- Longitude

The following parameters are supported for ePMP/PMP SM is in the CSV file:

- Latitude
- Longitude

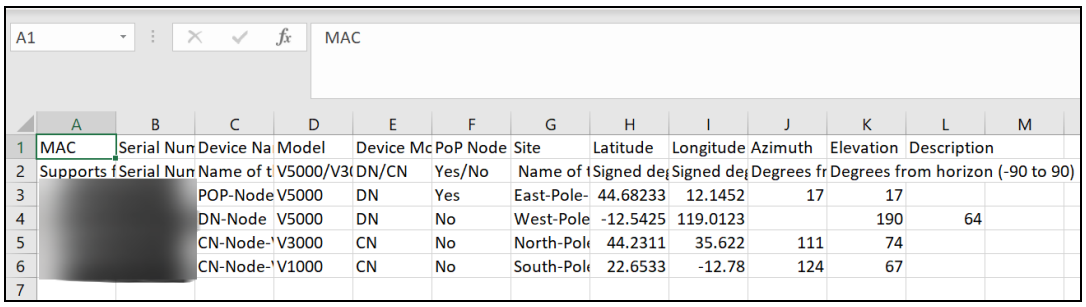
Figure 54 Import Device Configuration



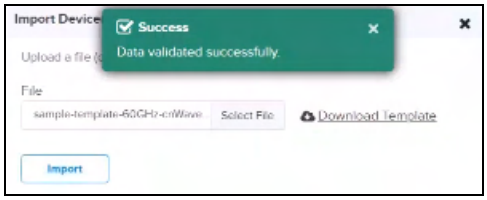
Sample Configuration File

MAC	LATITUDE	LONGITUDE	AZIMUTH	ELEVATION	BEAM WIDTH	HEIGHT	HEIGHT UNIT
Supports formats with ':', '-', 'no space', upper and lower case.	Signed degrees format (DDD.ddd).	Signed degrees format (DDD.ddd).	Degrees from North (0 to 360)	Degrees from horizon (-90 to 90)	Degrees from 1 to 360	Min=0, Max=5	Meters/Feet
[redacted]	16	19	17	17	130	1500	Feet
[redacted]	-90	119.0123	190	64	120	1000	feet
[redacted]	79.0123	11	111	74	112	110	Meters
[redacted]	-44	-12.78	124	67	177	190	meters

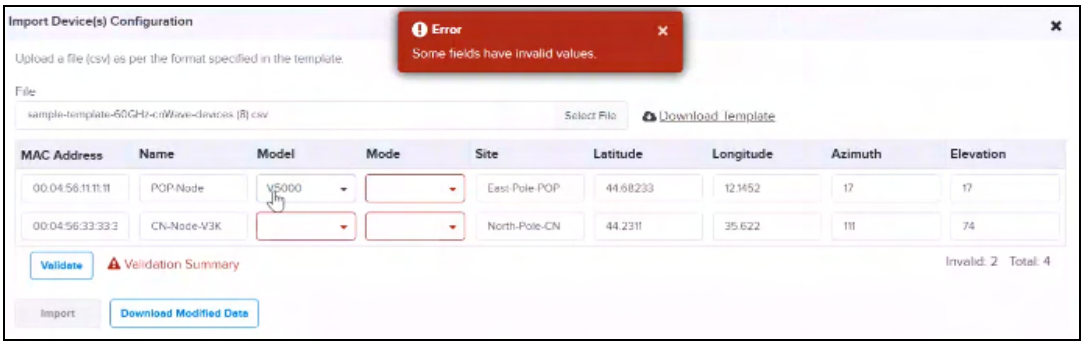
Sample Configuration File (60 GHz cnWave)



While importing the file it automatically validates the data as shown below.



If any invalid fields are found while validating it pops-up an error window as shown below:



Uploading a Configuration File

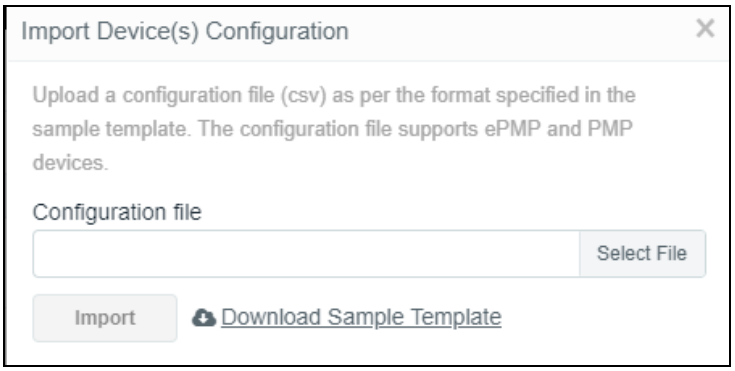
To upload a configuration file (CSV) as per the format specified in the sample template:

1. Download Sample Template or prepare a sheet in CSV file format with necessary column details.
2. Upload a configuration file (CSV) as per the format specified in the sample template.

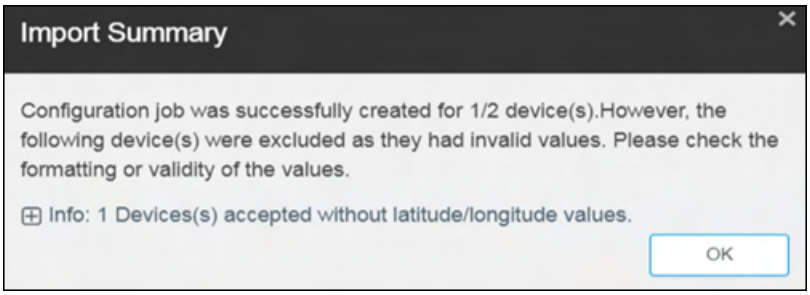
	NOTE: You must know the MAC address of the device to push the configuration.

3. Click **Import**.

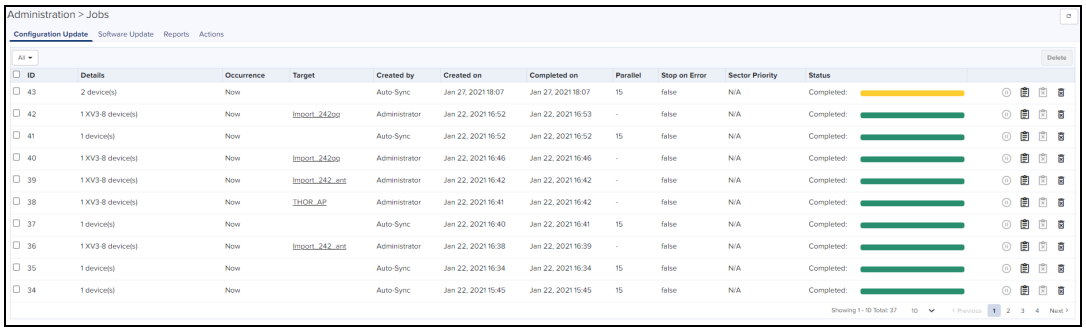
Figure 55 Uploading Configuration File



4. A configuration job will be created in the tower page.



5. You can view the completed status of import device (s) configuration in the Managed Account page.



The following table provides details on different errors that might occur while importing a CSV file:

Table 33: CSV Importing Error

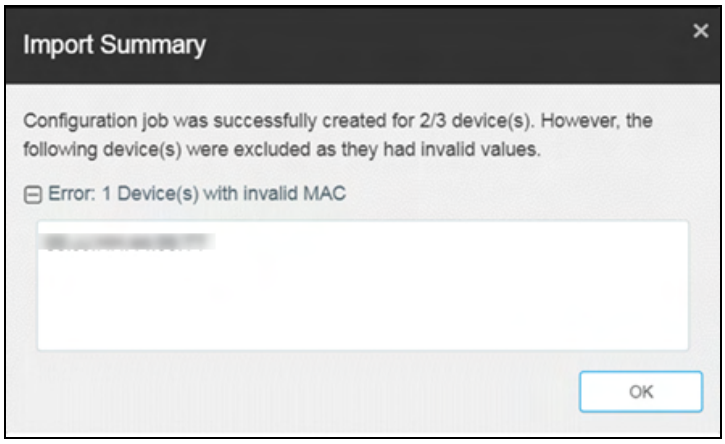
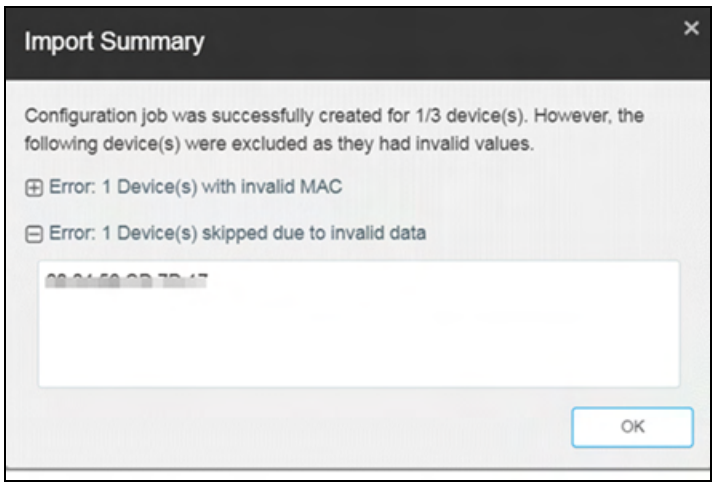
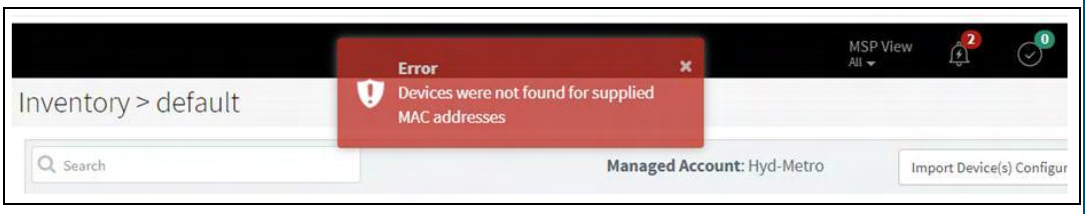
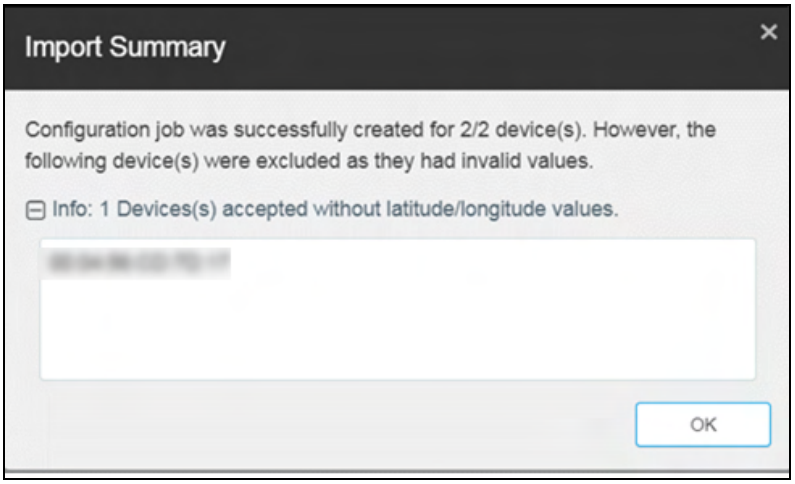
Error	Description
Error1: Error: {Count of Devices} Device(s) with invalid MAC	This error is displayed if the uploaded CSV file contains invalid MAC Address. 
Error2: {Count of Devices} Device(s) skipped due to invalid data	This error is displayed if the uploaded CSV file contains invalid Data or data not relevant for Latitude, Longitude, Azimuth, Height and Elevation. 
Error3: Devices were not found for supplied MAC Address	This error message is displayed if the devices were not found with supplied MAC address in the CSV file.

Table 33: CSV Importing Error

Error	Description
	
Error4: Info: 1 Devices(s) accepted without latitude/longitude values	This error is displayed when the latitude and longitude values are tried to push on to ePMP AP or PMP AP which are under a Tower. 

Reports

This section provides details on how to schedule and generate different types of data reports in cnMaestro On-Premises.

- Generating Reports
- Remote Upload
- Report Jobs

Generating Reports

The following reports can be generated such as:

- Device Report
- Reports
- Active Alarms Report
- Alarms History Report
- Events Report
- Clients Report
- Mesh Peers Report
- Guest Access Login Events Report

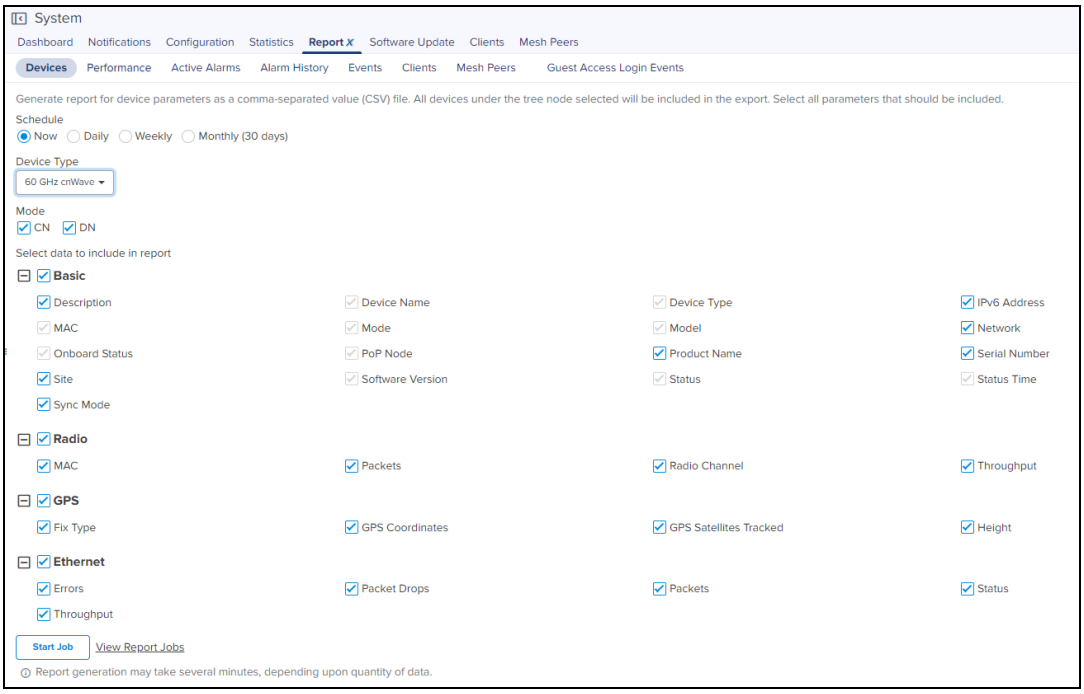
Device Report

To generate device reports:

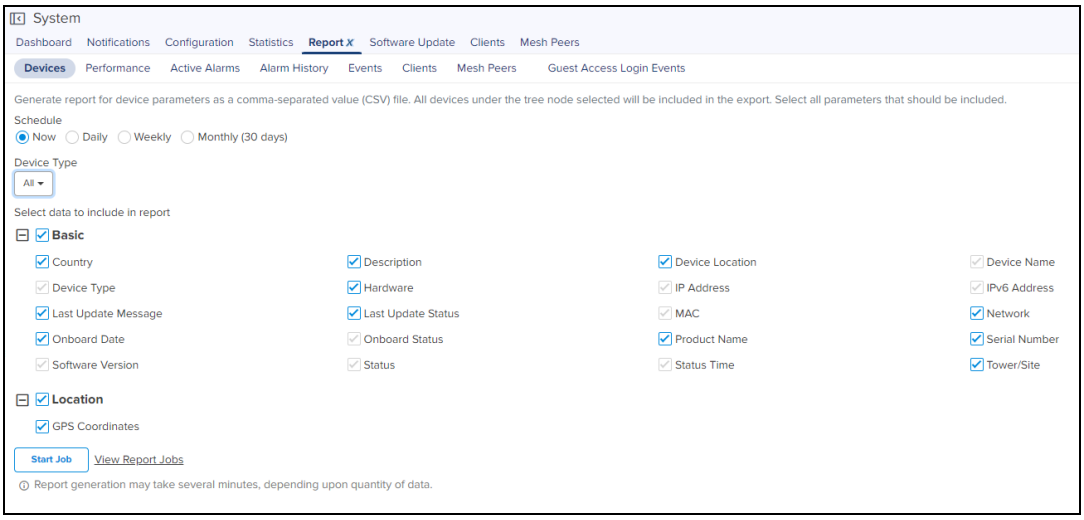
1. Navigate to **Report > Devices** tab.
2. Select the device type for which the user wants to generate the report or select **ALL** for generating the report for All device types.
3. Select data to include in report.
4. Click **Start Job** to generate report **Now** or you can **Schedule** based on schedule type (**Daily, Weekly** or **Monthly**).

Based on the device type selection the Data Export parameters will change.

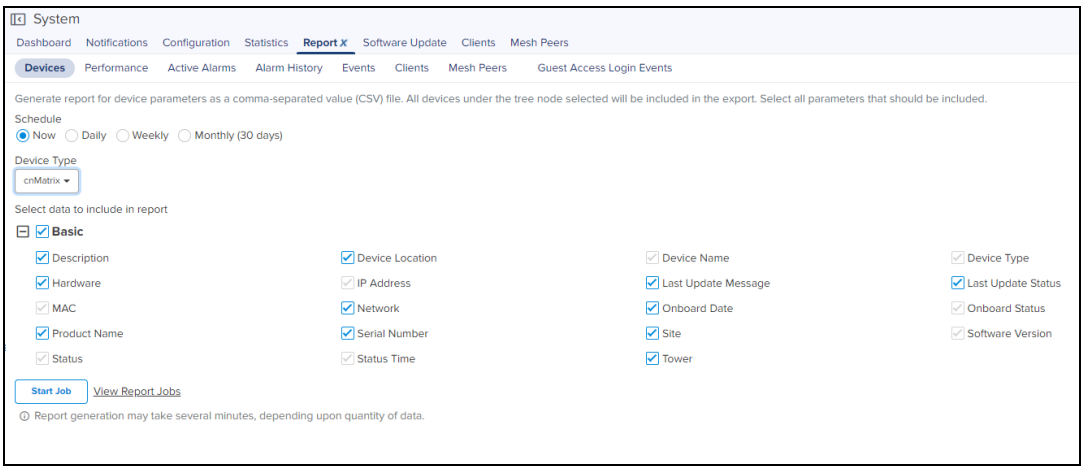
- If 60 GHz cnWave with enabling CN or DN or both is selected as the **Device Type**, then Basic, Radio, GPS, and Ethernet Data of CN or DN will be exported.



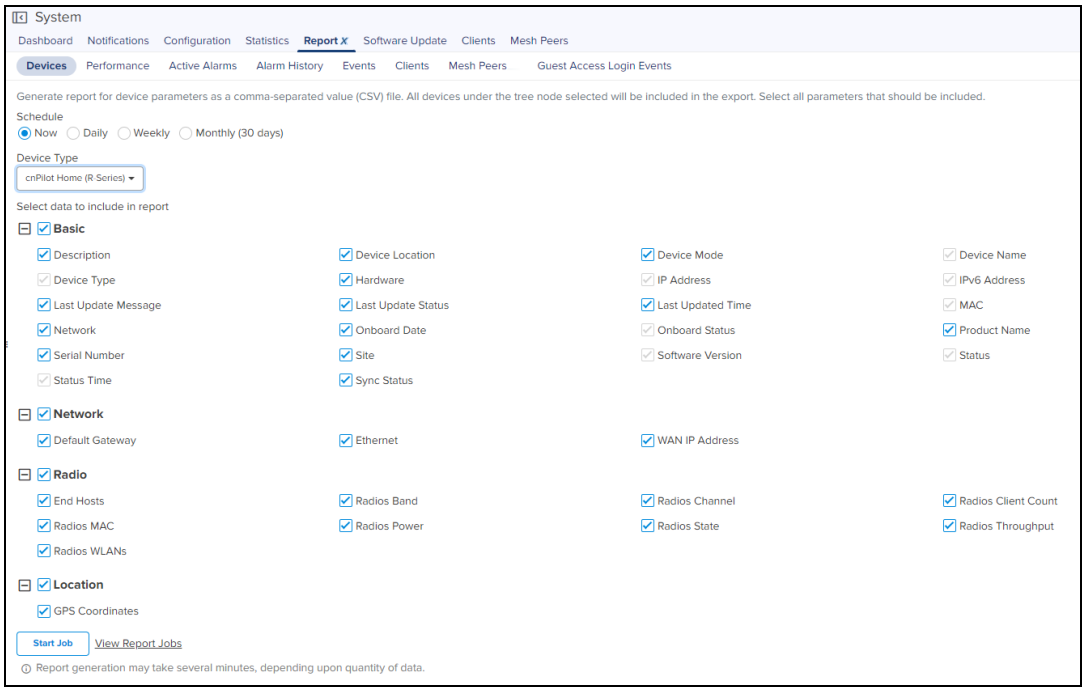
- If **ALL** is selected as the **Device Type**, the Basic Data Export parameters will be exported.



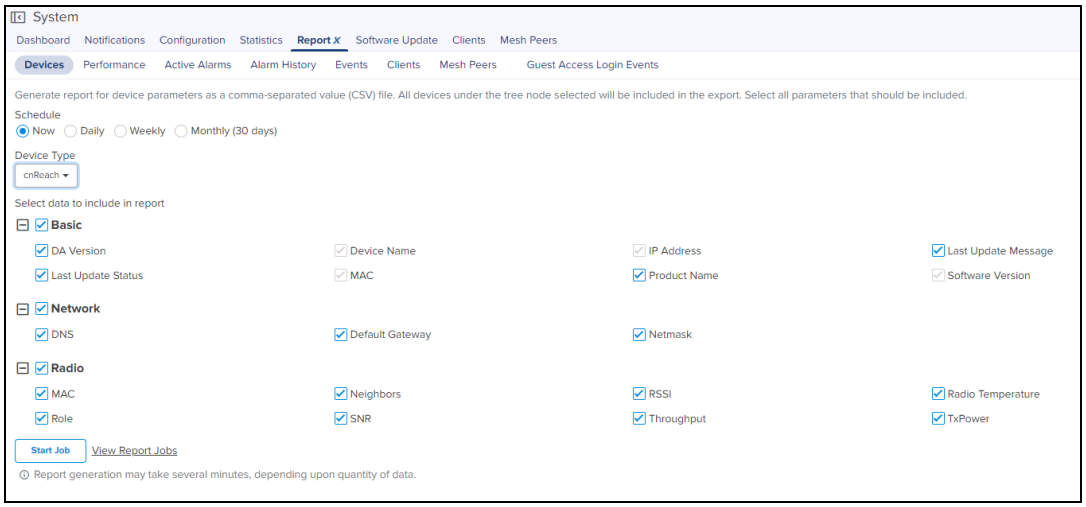
- If cnMatrix is selected as the **Device Type**, then Basic data will be exported.



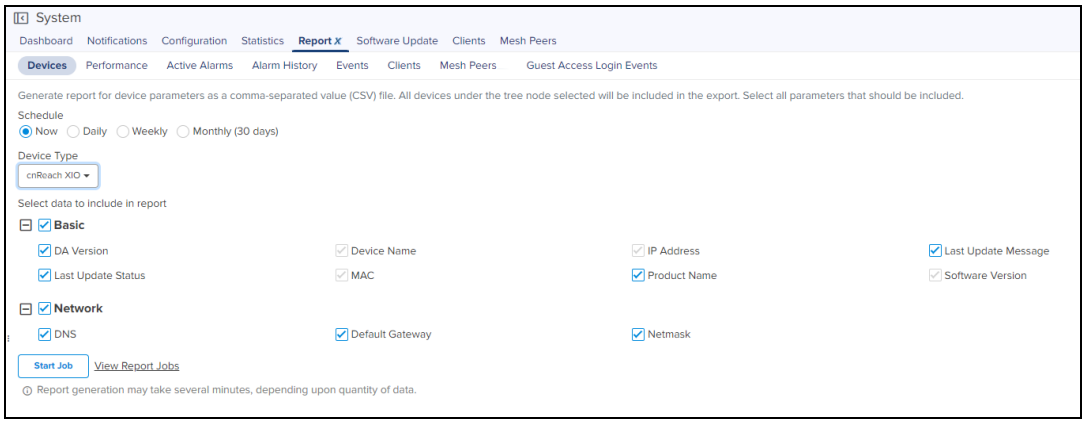
- If cnPilot Home (R-Series) is selected as the **Device Type**, then Basic, Network and Radio Data will be exported.



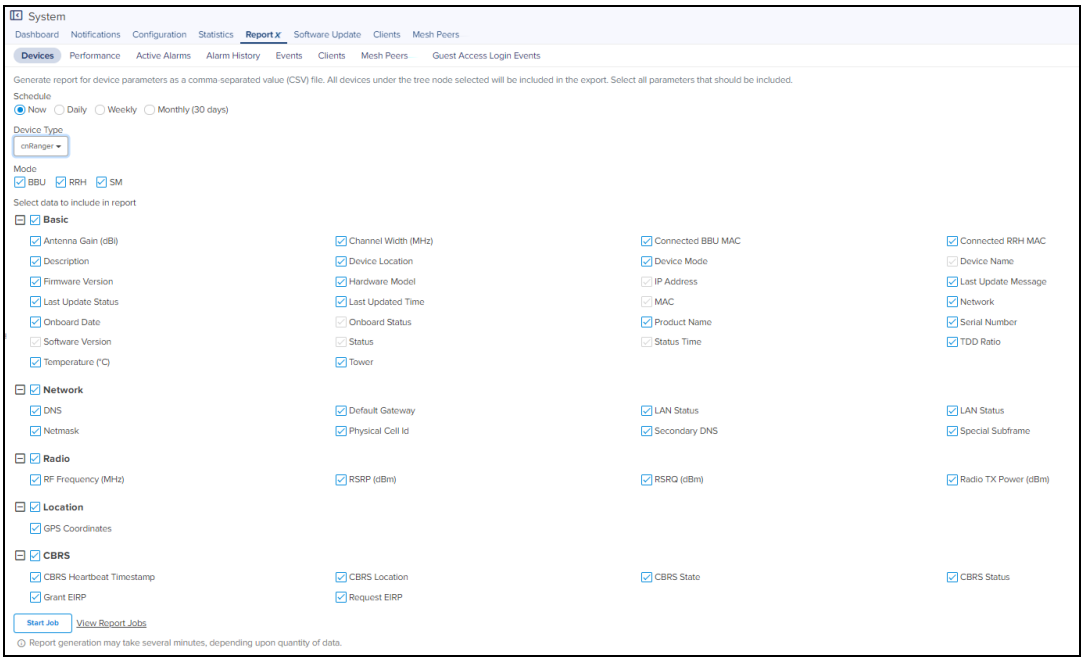
- If cnReach is selected as the **Device Type**, then Basic, Radio and Network Data will be exported.



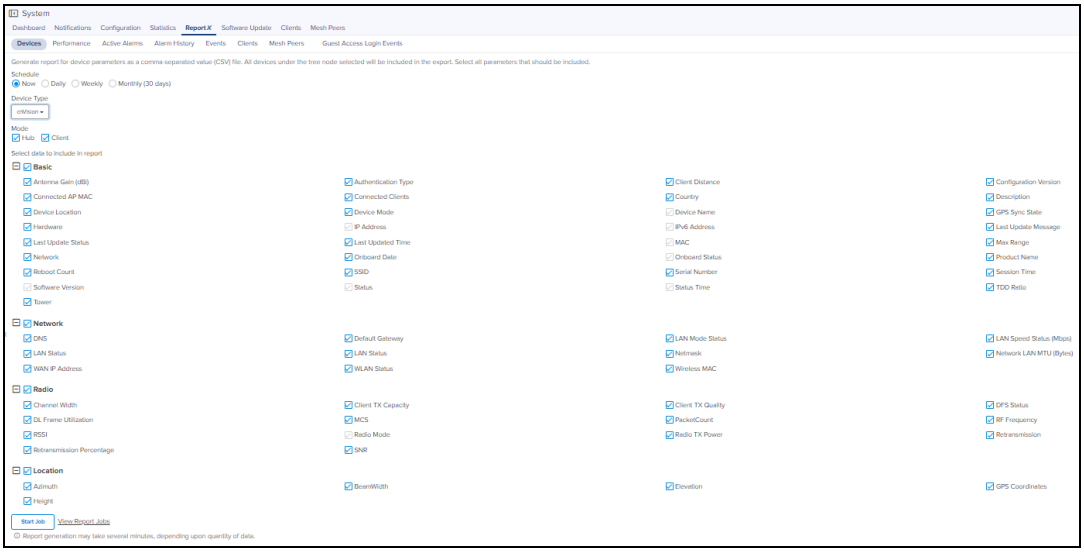
- If cnReach XIO is selected as the **Device Type**, then Basic, Radio and Network Data will be exported.



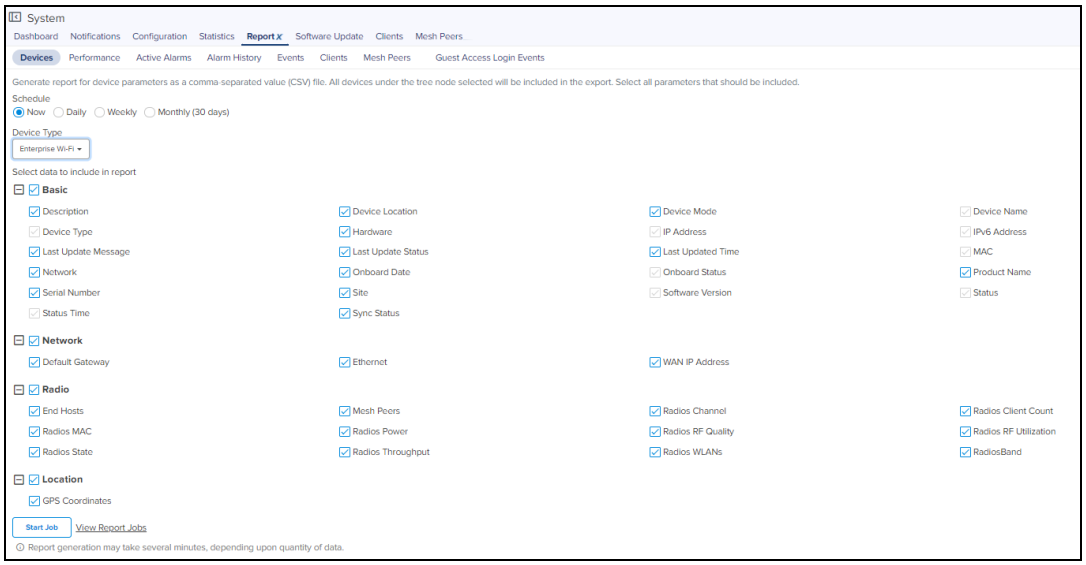
- If cnRanger is selected as the **Device Type**, then Basic, Radio, Location, CBRS, and Network Data will be exported.



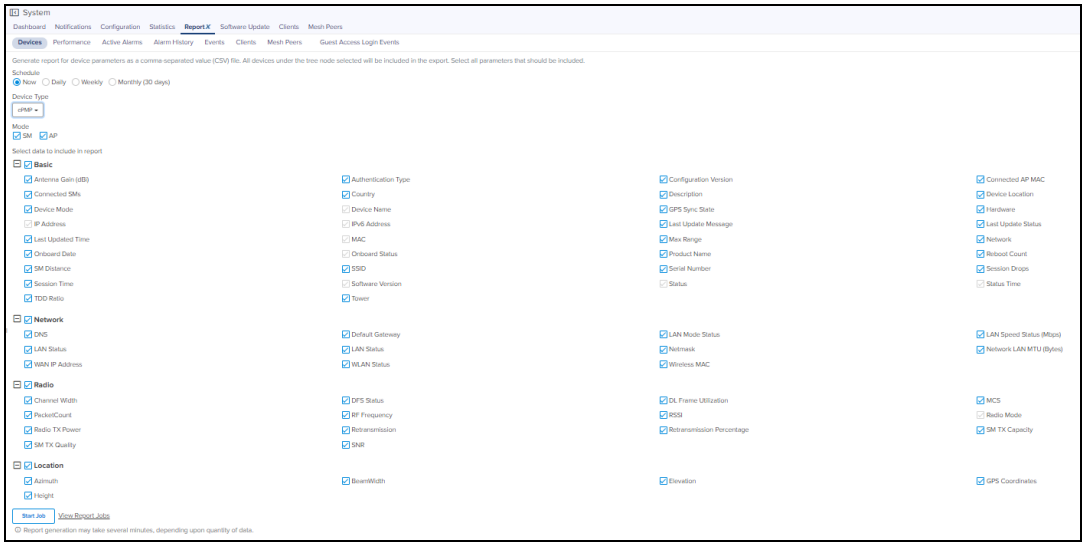
- If cnVision is selected as the **Device Type**, then Basic, Network, Location and Radio Data will be exported.



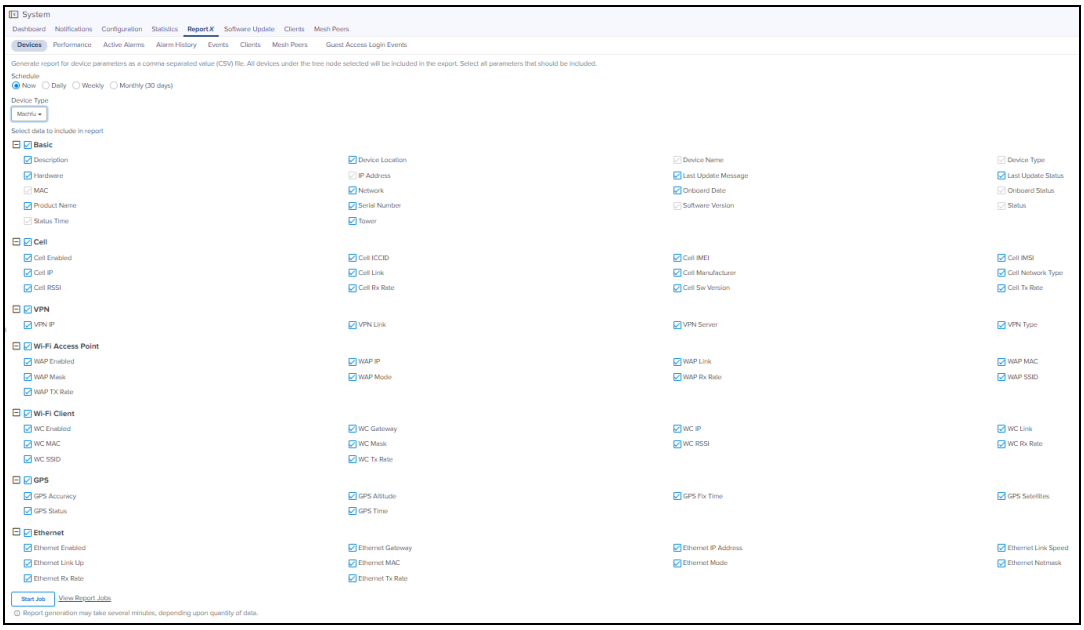
- If Enterprise Wi-Fi is selected as the **Device Type**, then Basic, Network, Location, and Radio Data will be exported.



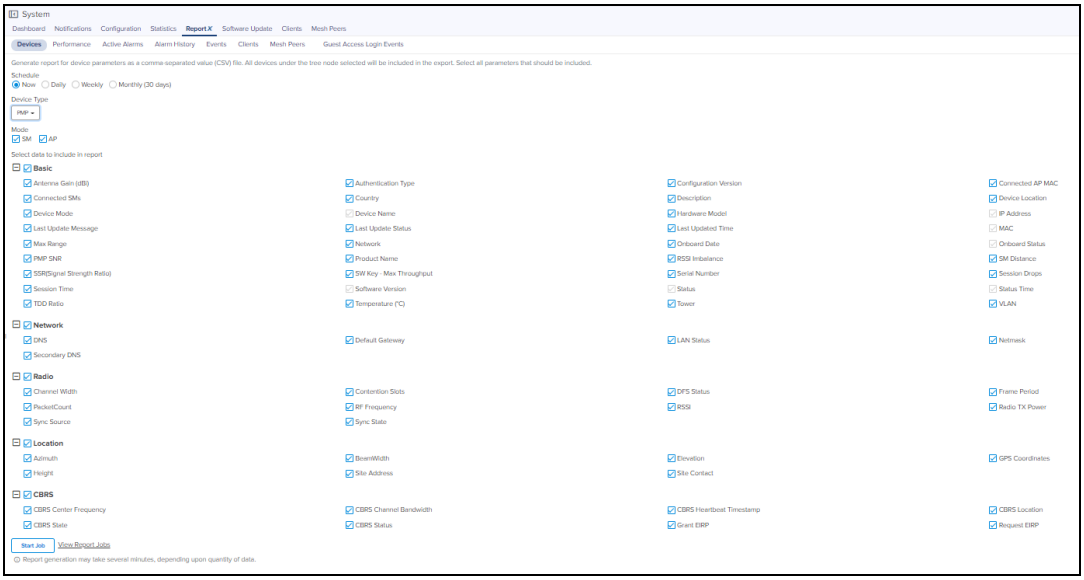
- If ePMP is selected as the **Device Type**, then Basic, Network, Location and Radio data will be exported. User can select to generate the report for either AP or SM or both. Based on the AP or SM selection, the data related to AP or SM will be exported.



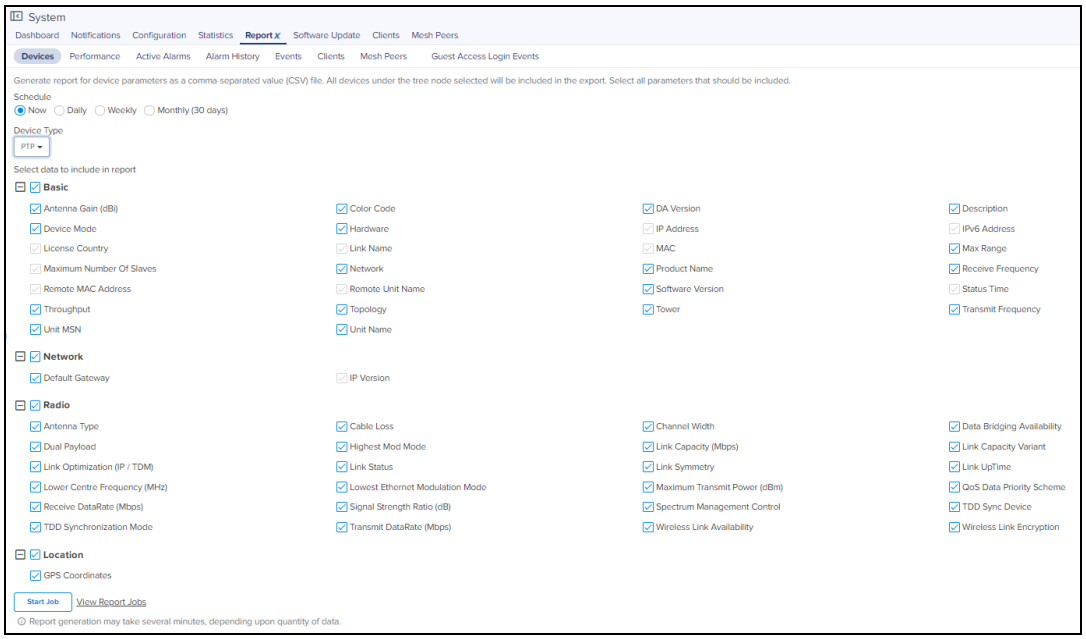
- If Machfu is selected as the Device Type, then Basic, Cell, VPN, Wi-fi Access Point, Wi-Fi Client, GPS and Ethernet data will be exported.



- If PMP is selected as the **Device Type**, then Basic, Network, Location and Radio data will be exported. User can select to generate the report for either AP or SM or both. Based on the AP or SM selection, the data related to AP or SM will be exported.



- If PTP is selected as the **Device Type**, then Basic, Network, Location and Radio data will be exported.



NOTE:
The data will be exported for the devices which are under the System/Managed Account/Network/Tower/Site/AP Group based on the selection made by the user in the LHS Tree.

Performance Report

To generate performance reports:

1. Navigate to **Report > Performance** tab.
2. Select **Time Range** based on which the report can be generated for **Last Day** or **Last Week** or **Custom Time Range**.
3. Select **Period** to report at either **5 Minutes** or **1 Hour** or **1 Day**.
4. Select **Device Type.**
5. Select data to include in report.
6. Click **Start Job** to generate report **Now** or you can **Schedule** based on schedule type **(Daily, Weekly** or **Monthly).**

NOTE:
Custom Interval is currently supported only for one week and in future releases it will be expanded for Monthly data.

60 GHz cnWave Performance Report

Figure 56 60 GHz cnWave Performance Report (Node Type)

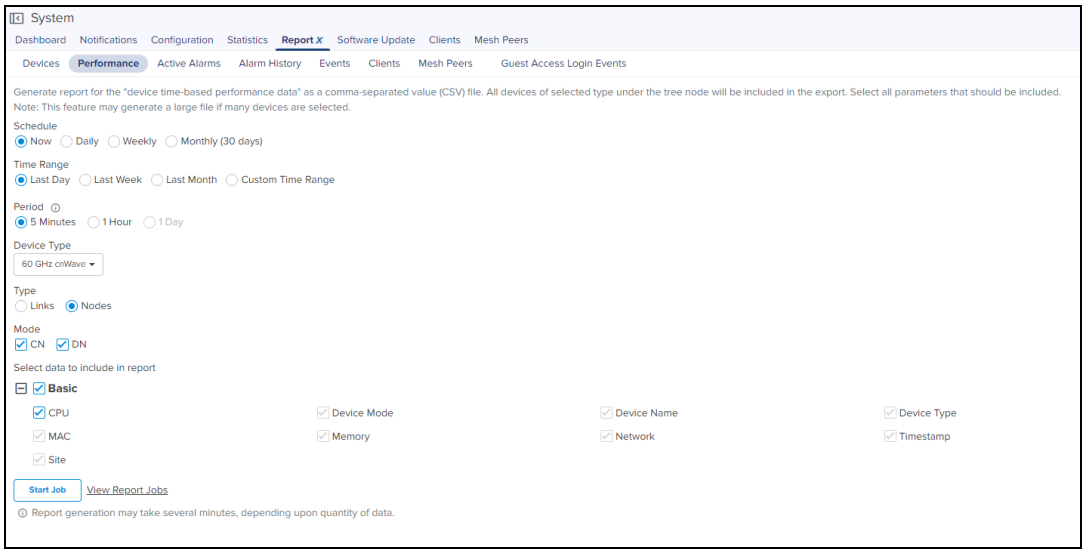
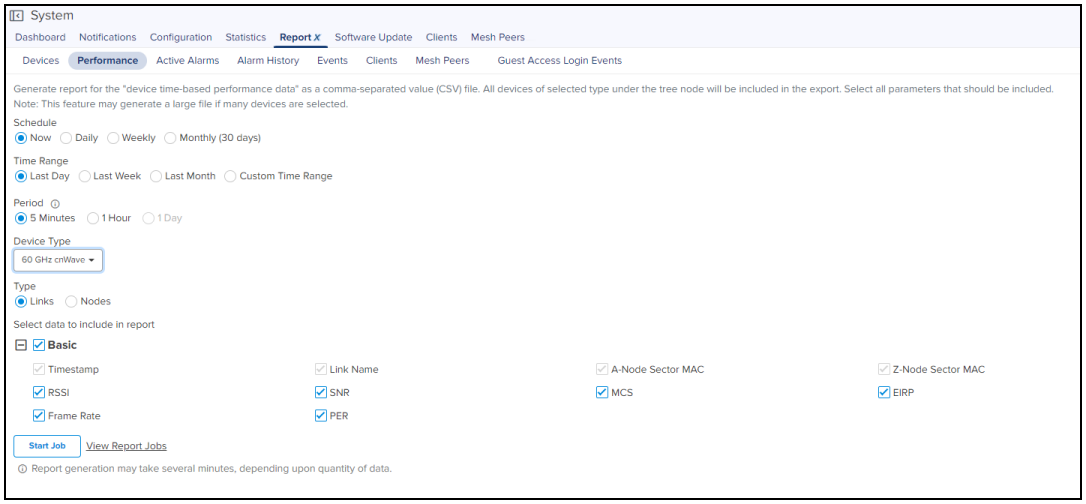
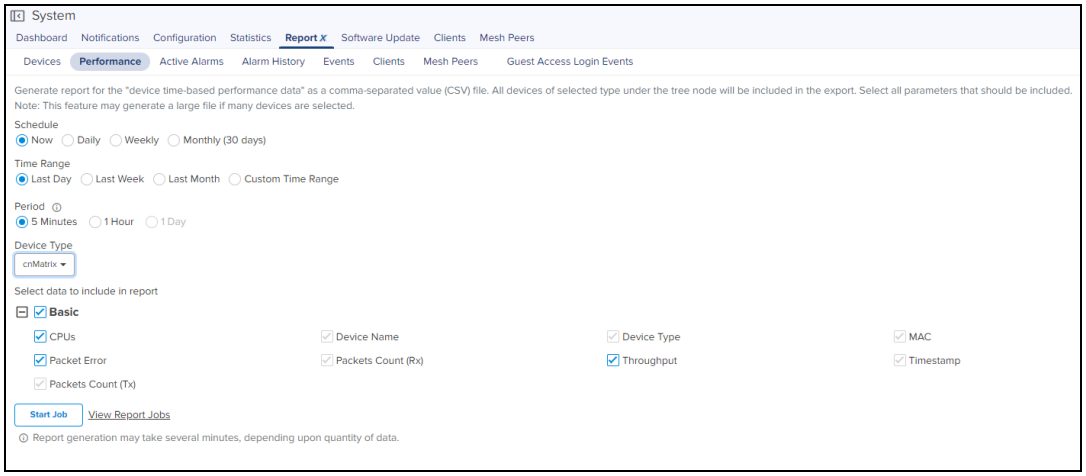


Figure 57 60 GHz cnWave Performance Report (Links Type)



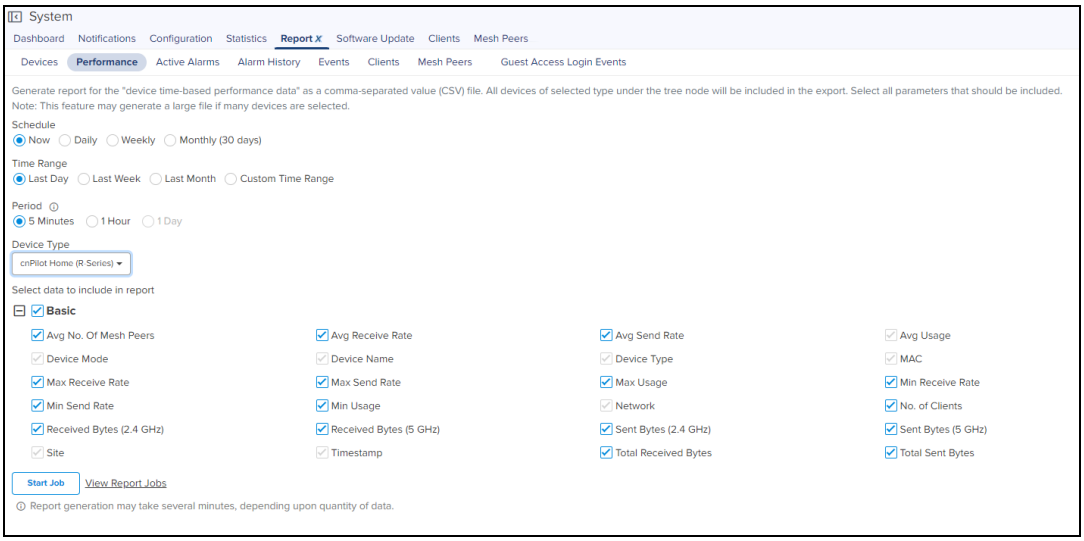
cnMatrix Performance Report

Figure 58 cnMatrix Performance Report



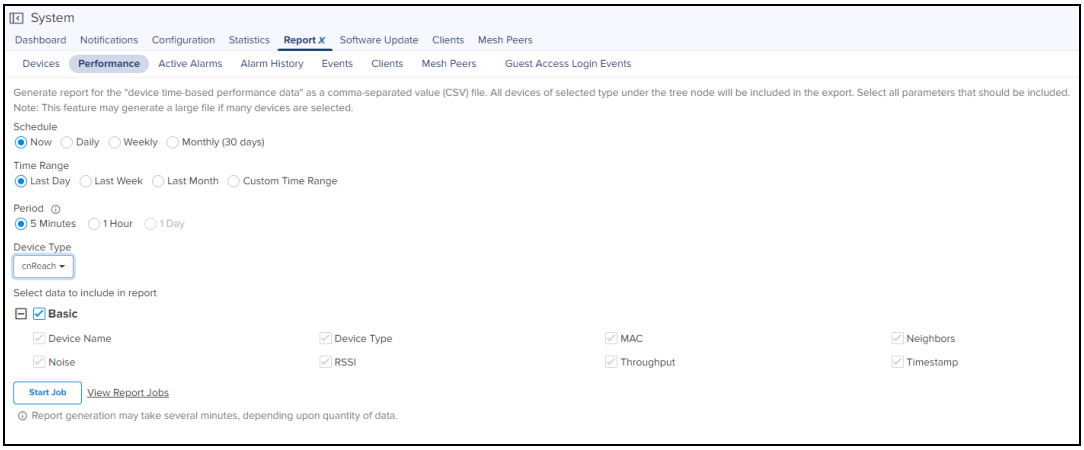
cnPilot Home (R-Series) Performance Report

Figure 59 cnPilot Home (R-Series) Performance Report



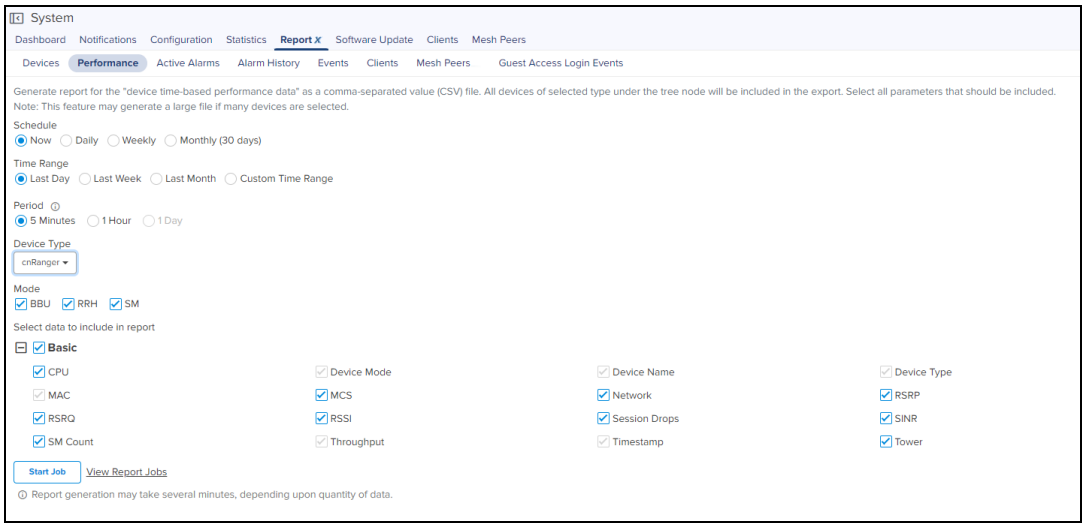
cnReach Performance Report

Figure 60 cnReach Performance Report



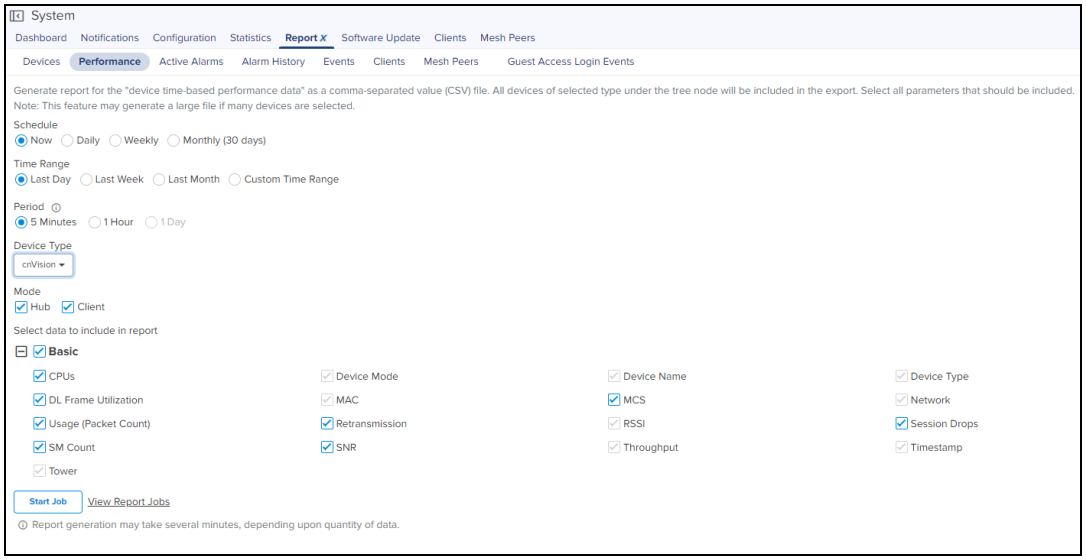
cnRanger Performance Report

Figure 61 cnRanger Performance Report



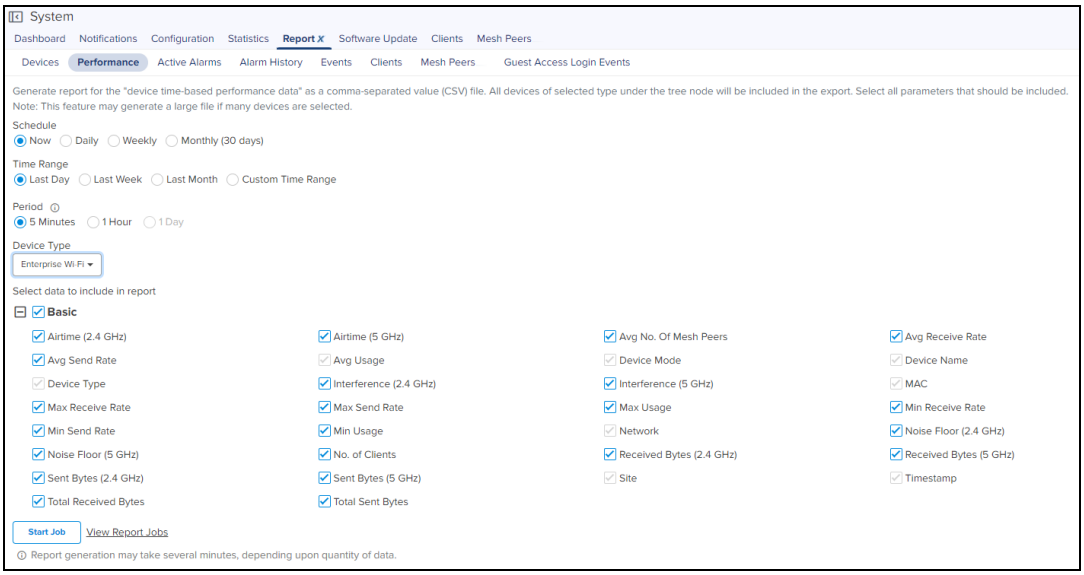
cnVision Performance Report

Figure 62 cnVision Performance Report



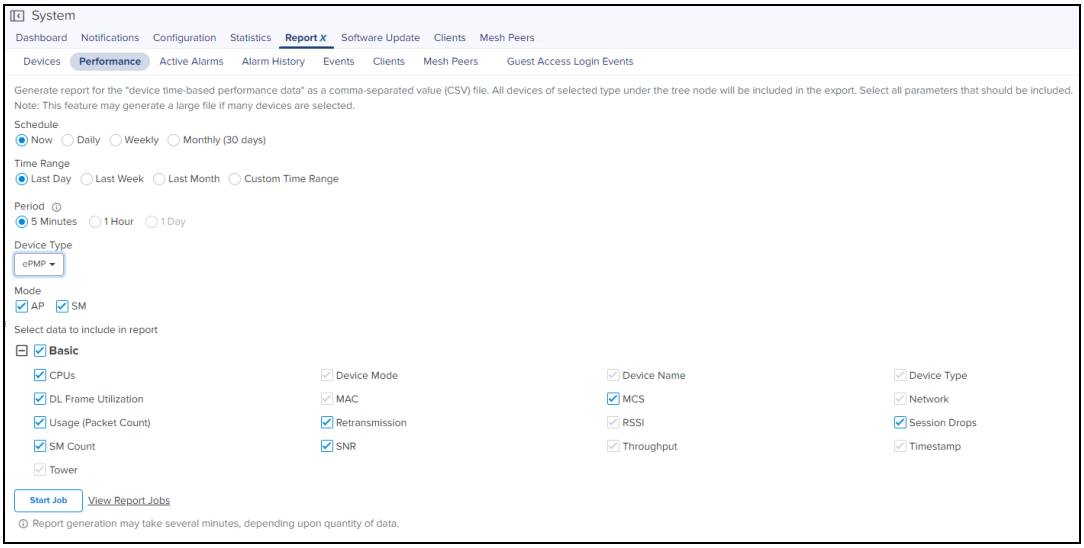
Enterprise Wi-Fi Performance Report

Figure 63 Enterprise Performance Report



ePMP Performance Report

Figure 64 ePMP Performance Report



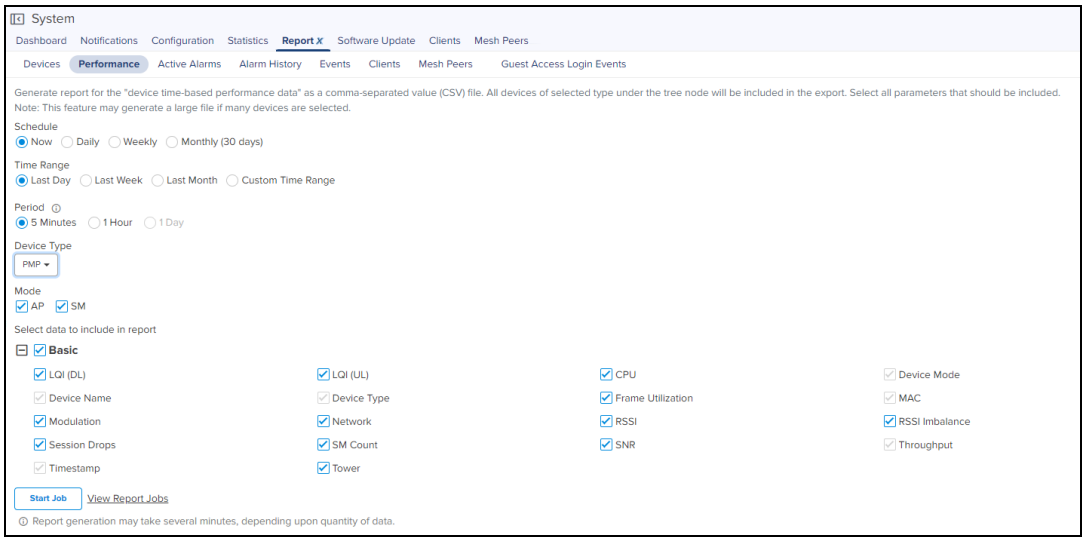
Machfu Performance Report

Figure 65 Machfu Performance Report



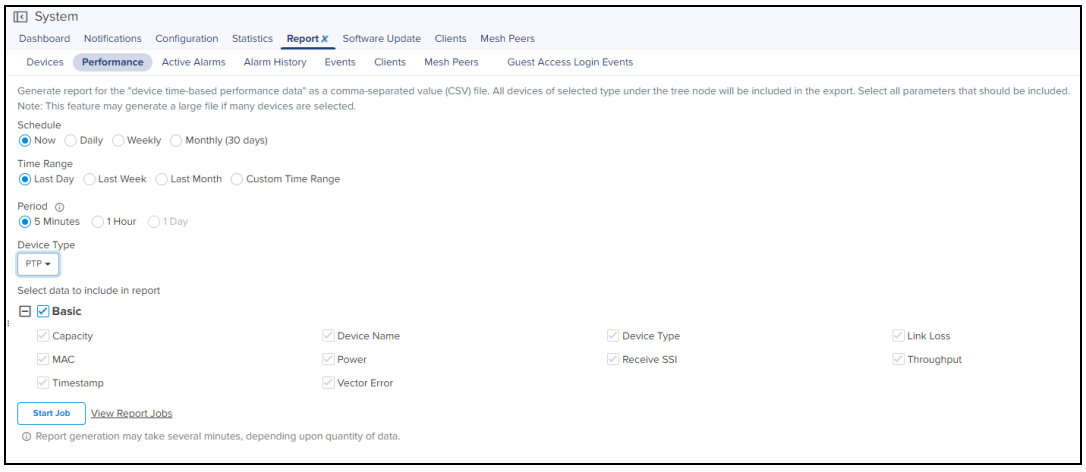
PMP Performance Report

Figure 66 PMP Performance Report



PTP Performance Report

Figure 67 PTP Performance Report

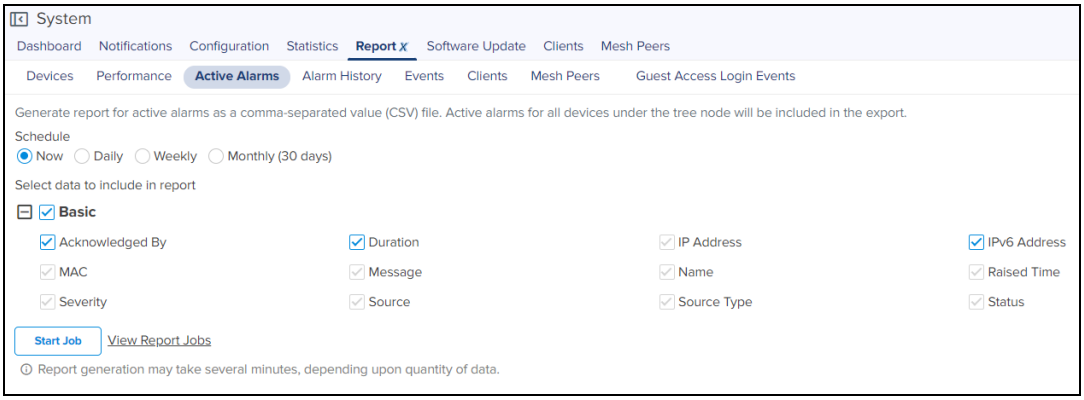


Active Alarms Report

To generate the Active Alarms reports, navigate to **Report > Active Alarms** tab.

This report will export the data for the Alarms which are currently active at the report generation time.

Figure 68 Active Alarms Report

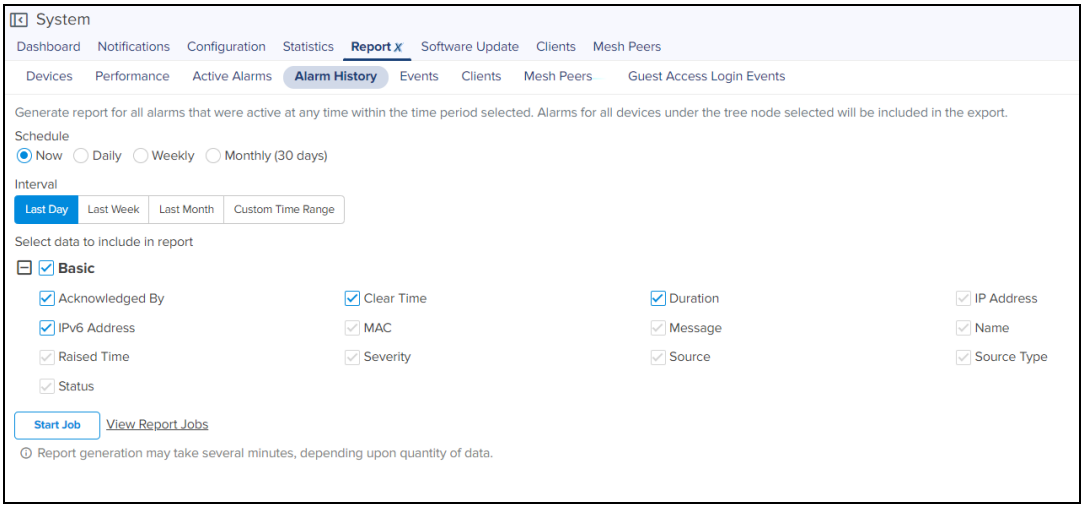


Alarms History Report

To generate the Active Alarms reports, navigate to **Report > Alarm History** tab.

This report will export the data for the Alarms which are currently active at the report generation time and the historical alarms for the specified time period and interval.

Figure 69 Alarms History Report

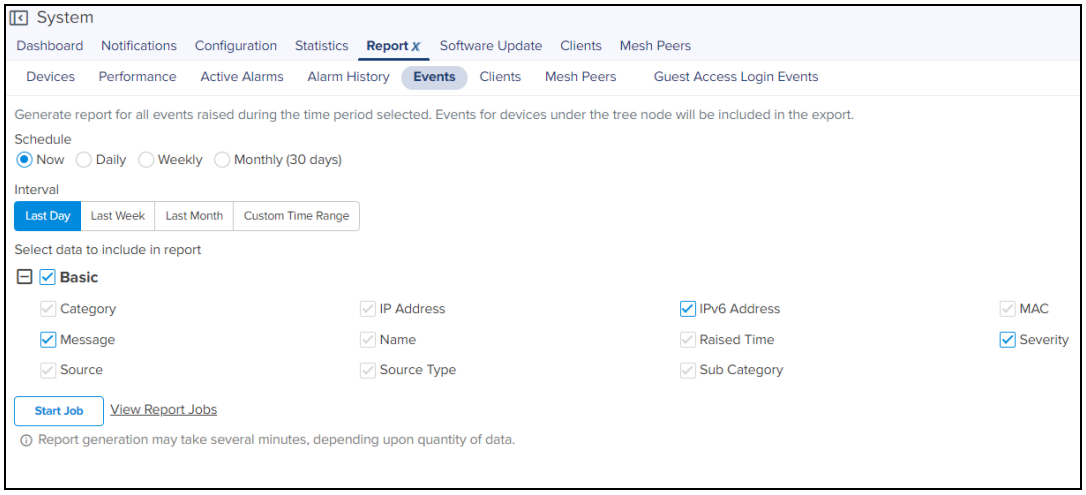


Events Report

To generate the Events reports:

1. Navigate to **Report** > **Events** tab.
2. Select **Schedule** as **Now**, **Daily**, **Weekly**, or **Monthly**.
3. Select **Interval** on which the report can be generated for **Last Day, Last Week**, **Last Month**, or **Custom Time Range**.
4. Select data to include in report.
5. Click **Start Job** to generate report **Now** or you can **Schedule** based on schedule type **(Daily, Weekly** or **Monthly).**

Figure 70 Events Report



The Events report will export the data for the events for the specified Time Period and Interval.

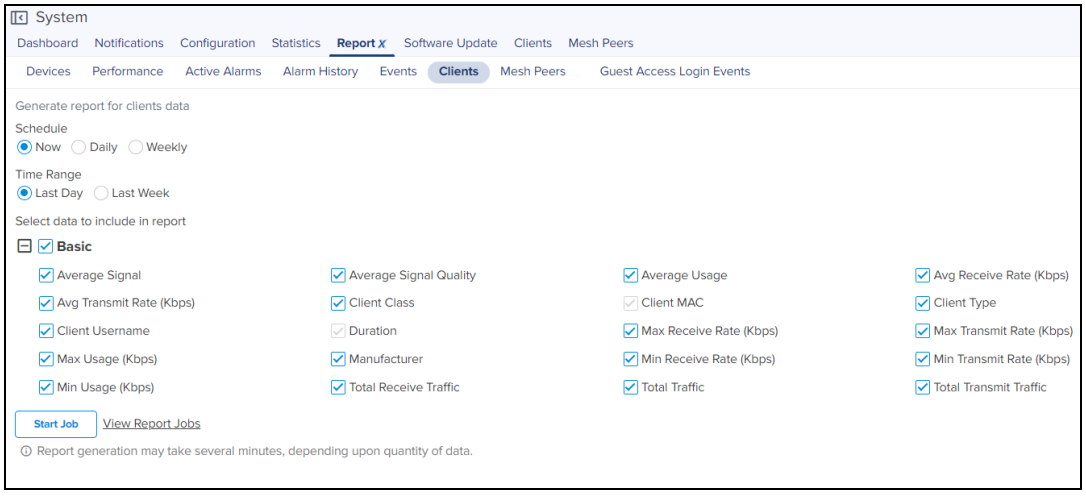
Clients Report

> **NOTE:**
>
> Clients Data is available for last day, last 24 Hrs and last week.

To generate the E-Series device reports of Client report:

1. Navigate to **Report > Clients** tab.
2. Select **Schedule** as **Now**, **Daily**, or **Weekly**. You can generate report based on schedule type **(Daily** or **Weekly).**
3. Select **Interval** on which the report can be generated. for **Last Day** or **Last Week**.
4. Select data to include in report.
5. Click **Start Job** to generate report **Now** and click **View Jobs** to view the Reports.

Figure 71 Clients Report



The **Clients** report exports the data for the clients for the specified Time Period and Interval.

Mesh Peers Report

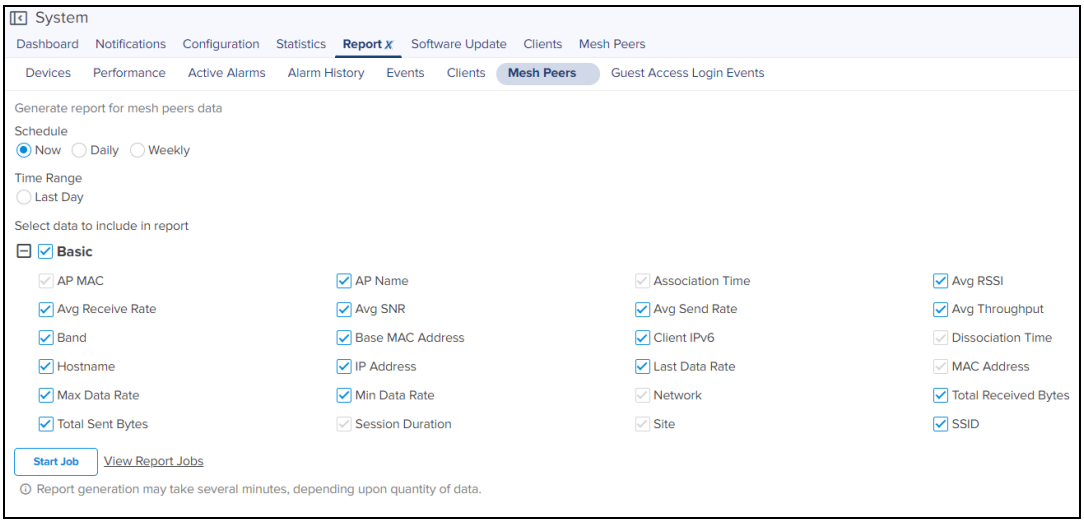
NOTE:

Mesh Peers report is available for last 24 Hrs and last week.

To generate the Mesh Peers report:

1. Navigate to **Report > Mesh Peers** tab.
2. Select **Schedule** as **Now**, **Daily**, or **Weekly**. You can generate report based on schedule type **(Daily** or **Weekly).**
3. Select **Interval** on which the report can be generated. for **Last Day** or **Last Week**.
4. Select data to include in report.
5. Click **Start Job** to generate report **Now** and click **View Jobs** to view the Reports.

Figure 72 Mesh Peers Report



NOTE:

1. Every report page has a **View Report Jobs** link that directs the user to the **Report Jobs** page under **Administration > Jobs > Reports**.
2. To schedule a report **Now**, click **Start Job** under the respective report section. cnMaestro downloads the report immediately for the current system time.

Daily report will generate reports on a daily basis depending upon the start and the end time. The weekly report generates report on seven days interval depending upon the start and the end time. Click **Schedule** button and configure start and end time to schedule daily or weekly reports under the respective Reports section.

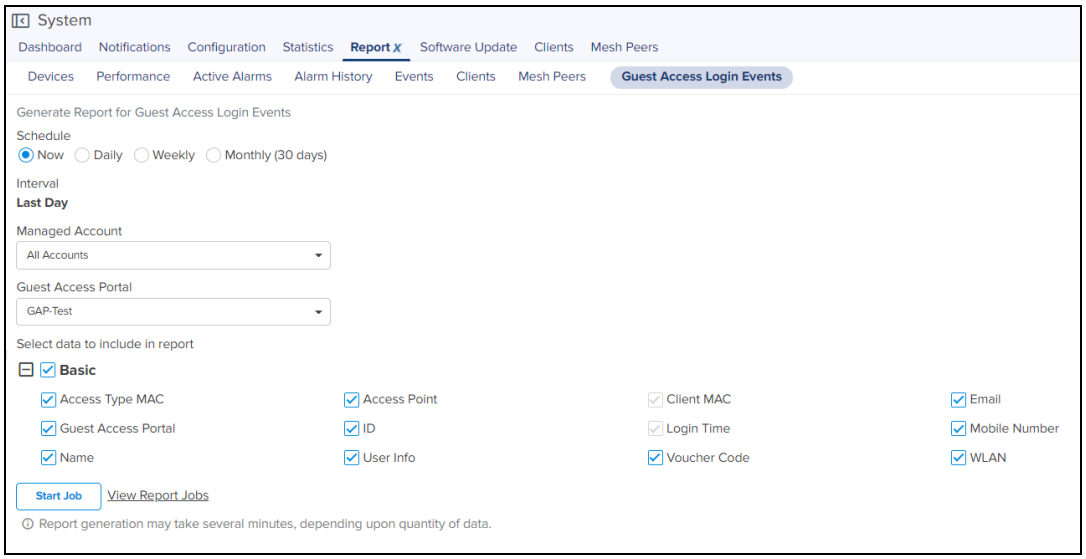
3. Export now option helps the user to create no of export jobs and these will be stored under **Administration > Jobs > Report** tab in the export page and can be downloaded with in seven days from the day of generation. This saves user's local memory from downloading each and every export report.

Guest Access Login Events

To generate the Guest Access Login Events reports:

1. Navigate to **Report > Guest Access Login Events** tab.

2. Select **Schedule** as **Now**, **Daily**, or **Weekly**. You can generate report based on schedule type **(Daily, Weekly,** or **Monthly).**
3. Select **Interval** the report can be generated for **Last Day.** By default Interval will be **Last Day**.
4. Select **Managed Account** and **Guest Access Portal** from drop-down.
5. Select data to include in report.
6. Click **Start Job** to generate report and click **View Jobs** to view the reports.



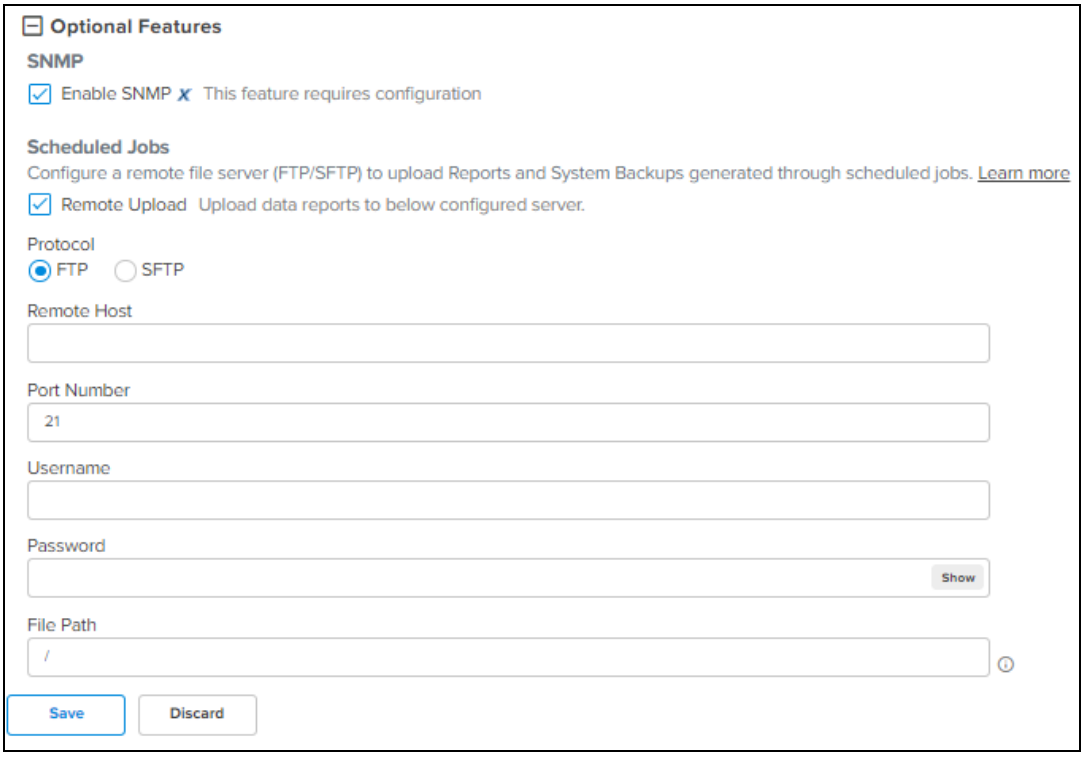
Remote Upload

Reports scheduled for **Now**, **Daily** or **Weekly** can be downloaded directly through the UI, or from an FTP or SFTP server.

To transfer reports to FTP or SFTP server:

1. Navigate to **Administration > Settings** page and select **Optional Features** tab.
2. Select the **Report Scheduler** check box to enable scheduling feature for data reports.
3. Select **Remote Upload** check box to upload the generated reports to the configured file server by FTP or SFTP.
4. Enter the **Remote Host**.
5. Enter the **Port Number**.
6. Enter the **Username**.
7. Enter the **Password**.
8. Enter the **File Path**.
9. Click **Save**.

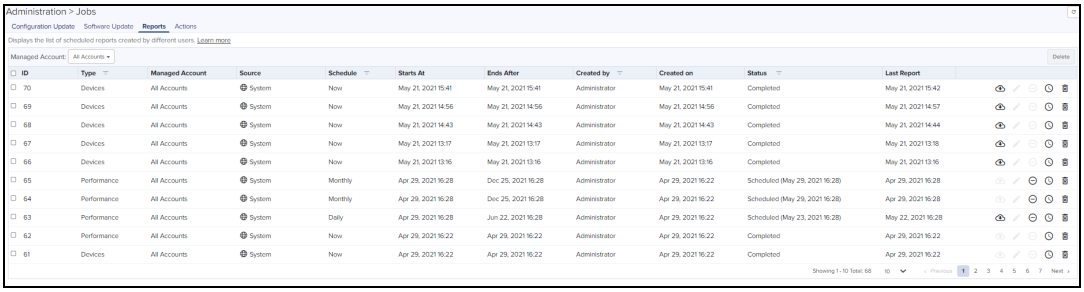
Figure 73 Scheduling Reports



Report Jobs

Displays the list of scheduled report job created by different users.

Figure 74 Report Jobs



A scheduled report job displays the following action buttons:

- **Edit**: Visible only for the active Jobs which are not yet run once. With this option, you can reschedule a job.
- **Terminate**: Stop the active Jobs.
- **Show History**: Display the detailed status of the generated reports and the file transfer status.
- **Delete**: Delete active and completed Jobs.
- **Instant Download**: User can instantly download the latest report directly once the download is complete without checking the show history.

Provisioning

This section includes the following topics:

- Software Update
- Fixed Wireless Configuration
- Wireless LAN Configuration
- Auto-Provisioning

Software Update

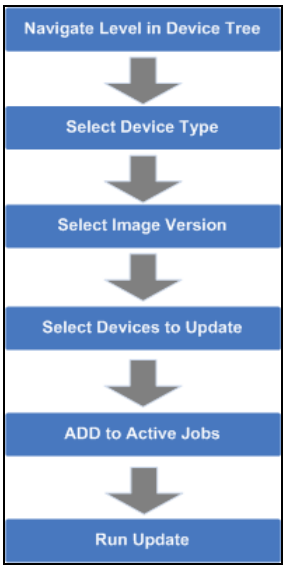
The **Software Update** tab displays the device update details for cnMaestro On-Premises. This section includes the following:

- Software Update Overview
- Create Software Update Job
- Viewing Running Jobs in Header
- cnReach Bulk Software Upgrade

Software Update Overview

The Software Update feature allows users to deploy the latest software images to devices. Software updates can be started at any level in the Device Tree, and individual devices can be selected for update. Updates are created as Jobs and placed into the jobs queue. When the update is ready to run, it can be started. The basic flow is the following:

Figure 75 Software Update Overview



When a Job finishes, it is placed in the completed Jobs table, where it remains for a week before it is deleted.

Create Software Update Job

Device Selection

Navigate the Device Tree to an appropriate level for the devices to be updated. For example, selecting an AP will filter the selectable devices to include itself and its children.

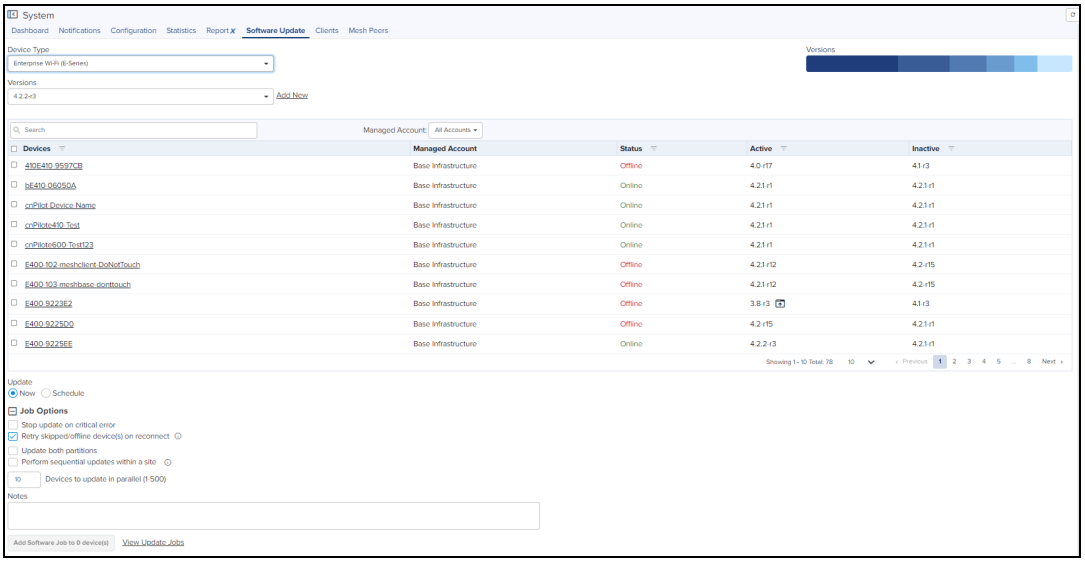
Device Type

Software Updates are executed on one device-type at a time. The type includes the specific hardware (Backhaul and Wi-Fi devices).

Software Update Dashboard

Once device type is chosen, the Software Update Dashboard displays the most recent software release version for that device type. It also displays a breakdown of the different software versions currently installed on the devices in the upgrade view.

Figure 76 Software Update Dashboard Enterprise Wi-Fi (E-Series)

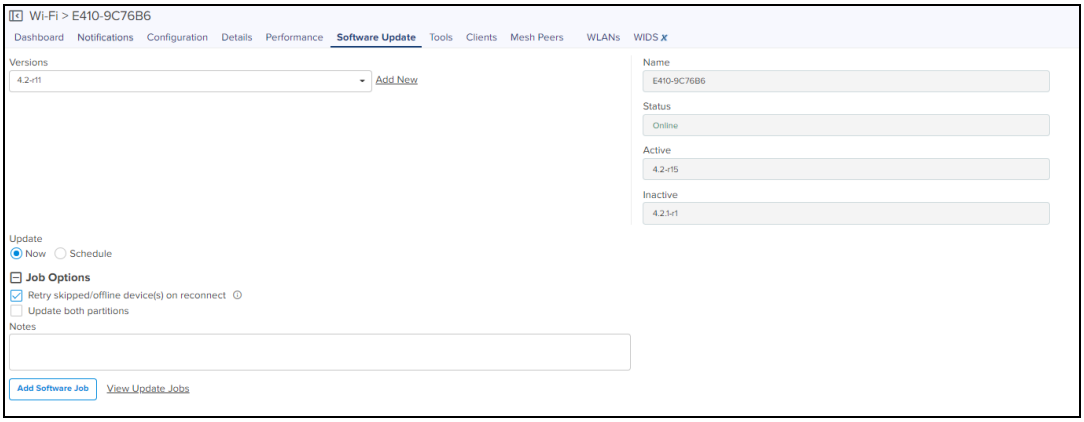


> **NOTE:**
>
> **Update both partition** option is available at System/Managed Account/Network/Site/Device levels.
>
> **Perform sequential updates within a site** option is available at System/Managed Account/Network/Site level except the device level.

If the **Update both partition is** enabled/disabled. In the device level of the software update will be displayed as follows:

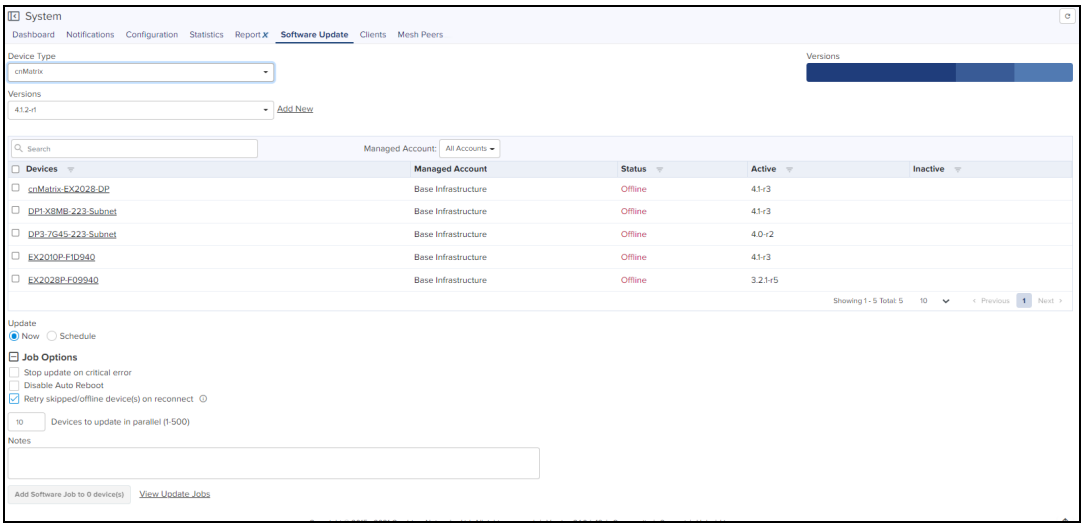
- **Enable:** The selected target image will be upgraded in both active and inactive portions of the device.
- **Disable:** The selected target image will be upgraded in only active portion of the device.

Figure 77 Software Update Dashboard Device level



If **Perform sequential updates within a site** is enabled the image upgrade will happen only on one device at a time in that particular site or upgrade will happen on all the devices.

Figure 78 Software Update Dashboard (cnMatrix)



Disable Auto Reboot option disables reboot after applying the new software image. User has to manually reboot the switch to complete the software update and boot with new version.

Figure 79 Software Update Dashboard (cnRanger)

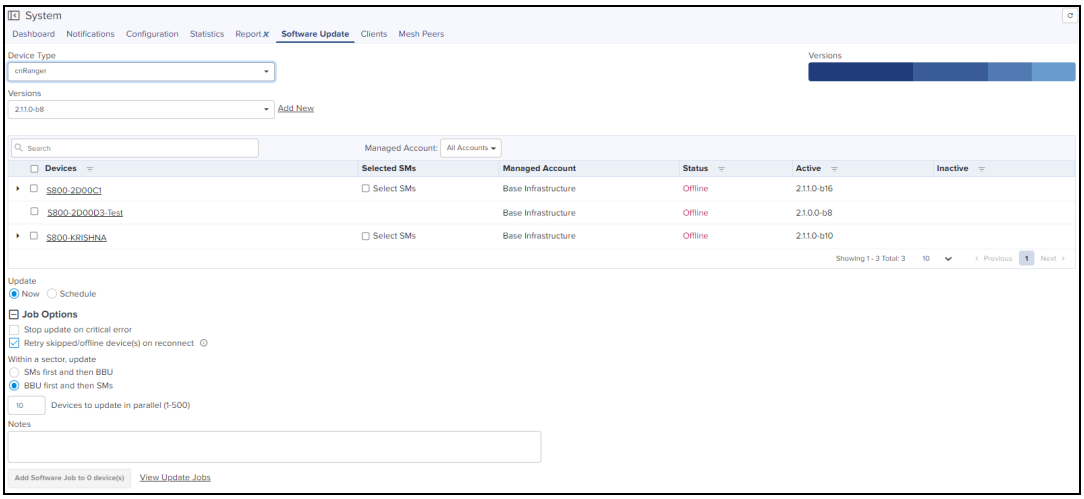
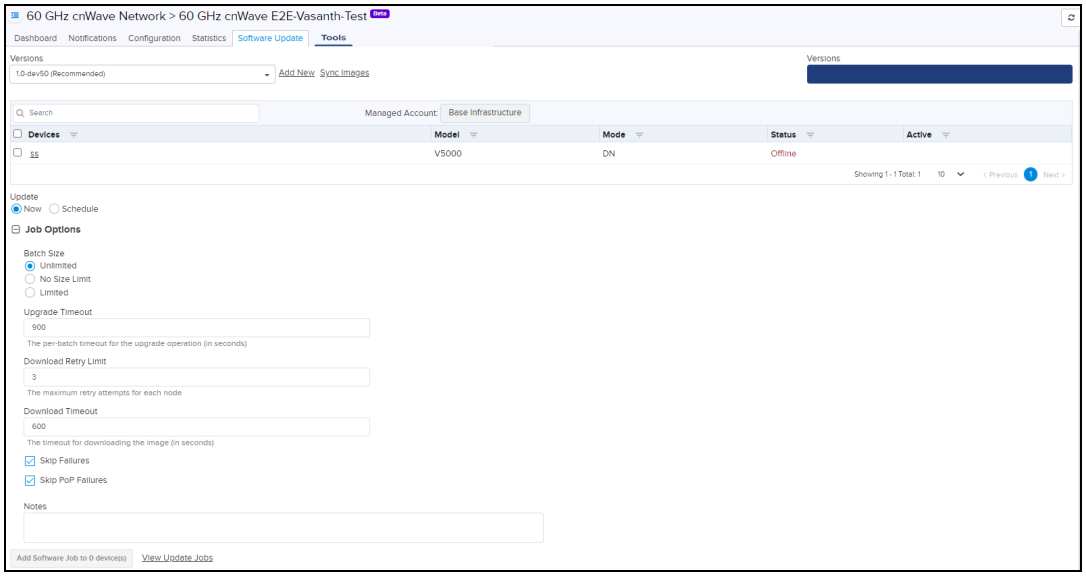


Figure 80 Software Update Dashboard (60 GHz cnWave)



Scheduling Software Update Job

You can now schedule a software update job on the devices by selecting **Schedule** radio button and providing the **Start Date** and **Start Time**.

Figure 81 Scheduling Software Update Job



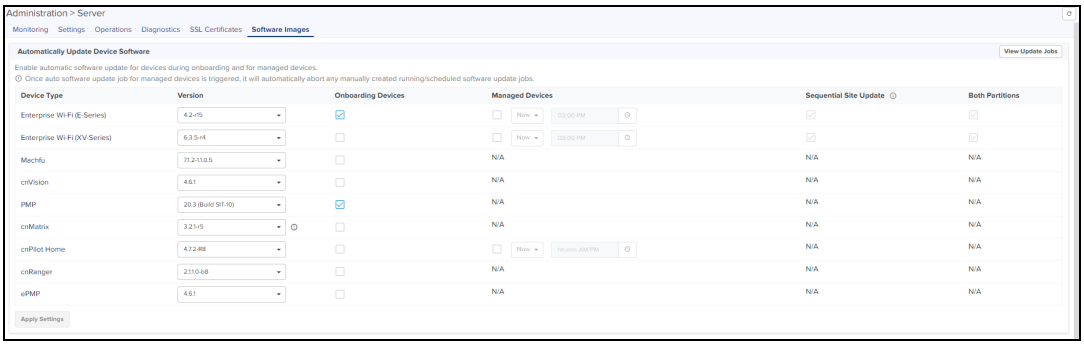
You can view the status of software update job in **Administration > Jobs > Software Update > Manual or Auto** page.

Software Update while Onboarding

The software version on the devices can be auto updated to the preferred version when the device first contacts cnMaestro.

To enable the device software feature update feature perform as follows:

1. Navigate to **Administration > Server > Software Images**.
2. Click the **Onboarding** checkbox for the particular device version.
3. Click **Apply Settings.**



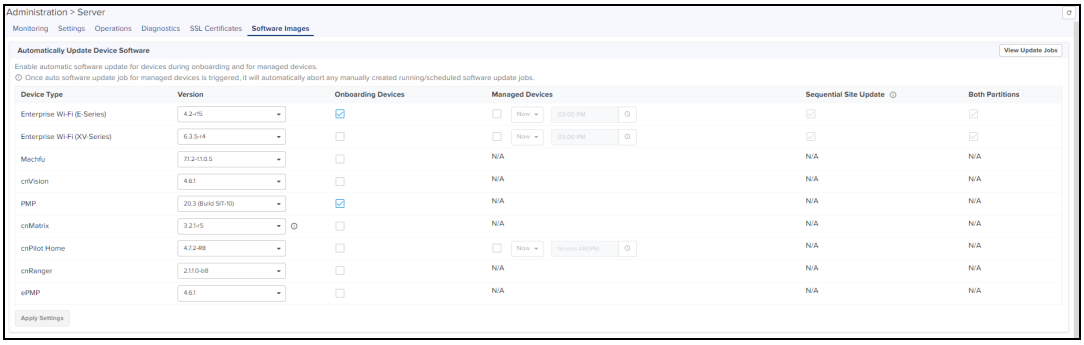
The device will get automatically upgraded based on the software selected while Onboarding.

Software Update through Managed Devices

The software version on the devices can be auto updated to the preferred version through the Managed Devices.

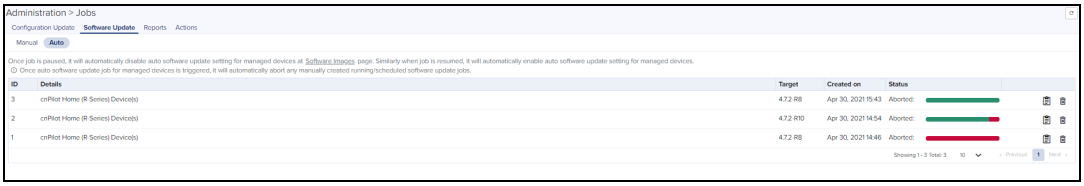
To enable the device software feature update feature perform as follows:

1. Navigate to **Administration > Server > Software Images**.
2. Click the **Managed Devices** checkbox for the particular device version.
3. Click **Apply Settings.**



Once the Setting is applied user can view the Jobs in **Administration > Jobs > Software Update> Auto** page.

Figure 82 Auto Update Page



	NOTE Auto update can be aborted during job is in-progress or idle state.

Device Table

Select the devices to upgrade in the Devices Table.

	NOTE: You can upgrade a device only when its status is Up. If you try to upgrade a device when it is Down, The selected device is down message is displayed in the UI. If the device is under the Auto Software upgrade, the manual software update is not possible.

The following parameters are visible (though some are only available for certain device types).

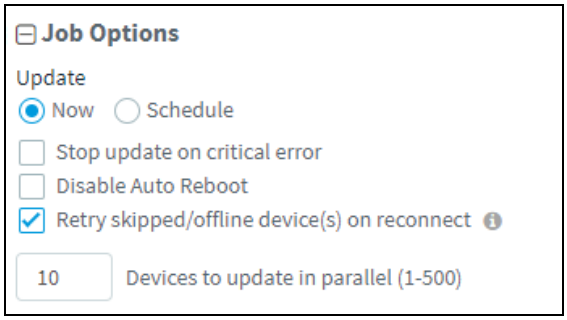
Table 34: Parameters Displayed in Device Table

Parameter	Description
Current Version	The version of the active software image running on the device.
Devices	The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree.
Selected SMs	If the AP is selected, the corresponding SMs will also be selected.
Status	The status of a particular device in a system. Devices that are not connected and cannot have images pushed to them.

Retry Software Update

The **Retry Software Update** option is available in every **Software Update** tab, and it is enabled by default.

Figure 83 Retry Software Update



If the software update job was skipped for a device as it was offline, an icon ( ) appears next to the active software version of the device. This indicates that the software update for the device will be done with the **Target** device version in the Job, whenever it reconnects to cnMaestro.

If the software update job was skipped while upgrading with the same version as the device active version, then the icon will not be displayed and the device will not update when it reconnects.

NOTE:
The device which undergoes **Retry Software Update**, does not create a new Job.

Options

Stop Updates on Critical Error

If one of the updates fails, then do not start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off, if desired.

Sector Upgrade Order

The recommended update ordering for devices within a sector will be pre-configured according to the recommendations for the device. It can be changed if desired.



NOTE:
Device updates occurs sector-by-sector. One sector needs to complete before a second sector is started.

Parallel Upgrades

Specify how many device upgrades to perform in parallel to complete the upgrade faster. However if the job is configured to halt on an error, all concurrent sessions will still be allowed to complete.

Upgrade Steps

To upgrade an ePMP (Sectors) device:

1. Navigate to **System** or **Network** or **Tower** or **Device** level. From the list, select the system or network or tower or device to which the device belongs.
2. Navigate to **Manage > Software Update > Select Devices** page.
3. Select **ePMP (Sectors)** from the following **Select Device Type** drop-down list:
   a. 60 GHz cnWave
   b. cnMatrix
   c. cnReach
   d. cnRanger
   e. cnPilot Home (R-Series)
   f. cnPilot Enterprise (ePMP Hotspot)
   g. cnVision
   h. Enterprise Wi-Fi (E-Series)
   i. Enterprise Wi-Fi (XV-Series)
   j. ePMP (Sectors)
   k. Machfu
   l. PMP (Sectors)
   m. PTP
4. Select the software image to update from the **Select Image Version** drop-down list.
5. Select the devices to update by clicking the **tick** icon.
6. Set desired **Job Options**.
7. Click **Add Software Job** button.

Software Update Parameters

The Software Update Jobs table lists all currently running, queued, and completed jobs. The jobs can be triggered immediately or can be run later.

(**Administration > Jobs > Software Update** tab)

The following table displays the list of parameters displayed in the **Software Update Jobs** tab:

Table 35: Parameters displayed in Software Update Jobs tab

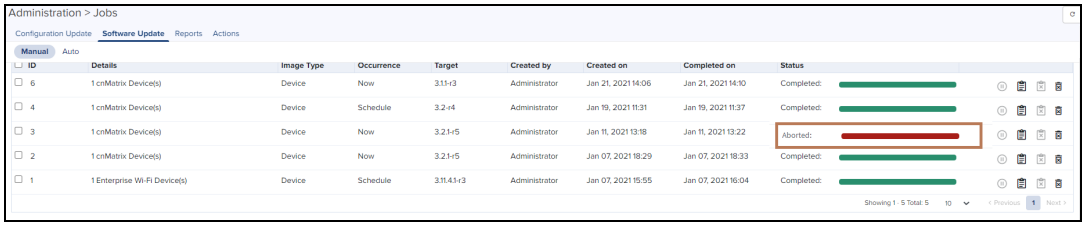
Parameter	Description
Created By	The user who has created this job.
Created On	Date and time on which the job is created.
Completed On	Date and time on which the job is
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Image Type	Displays the type of image selected for the device.
Occurrence	Displays the occurrence of the update like now, scheduled, etc.
Status	Status of update.
Target	Target software version to upgrade.
Managed Account	Displays the Managed Account Name.

The user can filter the jobs based on the running status. The user can also filter the devices in a particular job based on the parameters mentioned in the above table.

Abort Software Job

Abort operation will skip devices that are waiting for update to begin. Devices already being updated may continue, but cnMaestro will stop tracking their progress. Aborting a Software Job puts the device into a **Completed** state that cannot be manually restarted by the user. The **Pending** devices will not begin their updates.

Figure 84 Abort Software Job



NOTE:

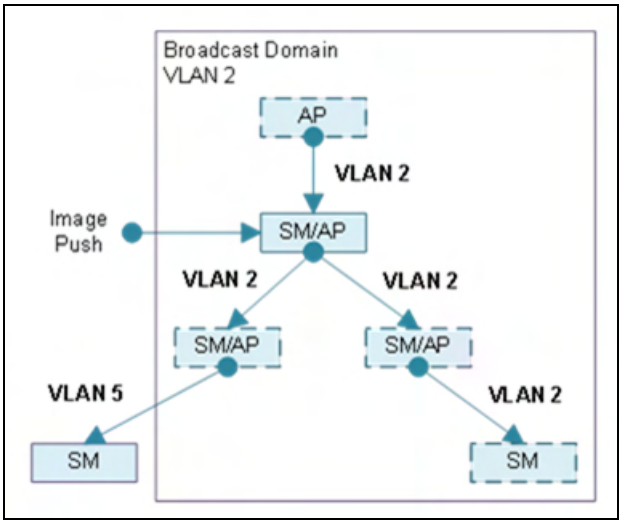
1. Devices which are already completed display as **Completed** with a message update complete along with the status as **Completed**.
2. Devices which are ongoing display as **Aborted** with a message **Manually Aborted** with the status as **Aborted**.
3. Devices which have not yet started display as "skipped" with a message "job was aborted" with the status as **Skipped**.
4. Software update jobs can be scheduled in parallel irrespective of other running Jobs as PRO account supports Parallel Jobs also If same devcie is used for config/ software job at a time only one operation will be done as the Job locks the device until it finishes.

Viewing Running Jobs in Header

Click the icon at the top right corner of the UI. This directs you to the **Jobs** page of the Software Update tab. For more information, see Software Update Parameters.

cnReach Bulk Software Upgrade

Distributing software to cnReach devices can take many hours, due to the relatively low RF bandwidth. In order to minimize wireless traffic, cnMaestro supports the cnReach mechanism by which a single AP coordinates the broadcast distribution of firmware to every cnReach device within its VLAN. In the below figure, the bulk upgrade operation transfers an image to the middle AP, which then distributes it to all APs with VLAN 2. The APs are not updated in this process; the firmware is just pushed into their storage, where it can be applied later (once the distribution completes). cnReach has a mechanism to handle offline devices during the distribution (which can take upwards of a day), or devices added midway through the transfer. Often this means the process repeats a second time, to handle any updates.



The **Bulk Software Upgrade** is optional, and meant to be used for efficiency. One can still use the standard Software Update mechanism to transfer images to cnReach devices one-at-a-time, though the distribution could be many hours or days.

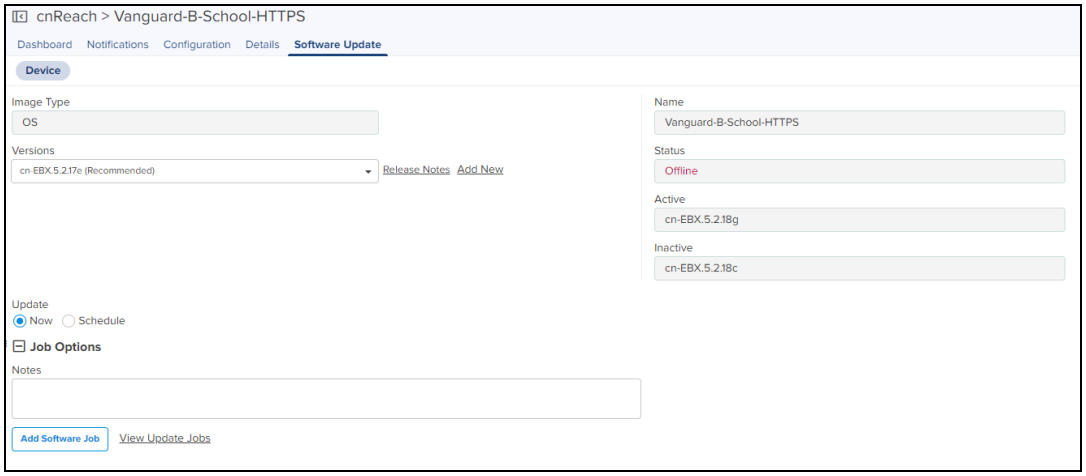
Firmware Versions (OS and Radio)

cnReach devices have two versions of software: one for the Motherboard OS, and another for the Radio. Each Radio can have a different version of firmware. When selecting software to distribute, one should choose either OS or Radio. During the Apply phase, when the image is updated, one or both Radios can be selected.

Bulk Upgrade

The Bulk Upgrade tab is accessed by selecting a cnReach AP then **Software Update > Bulk Upgrade**. The Motherboard (OS) or Radio software is available, and the distribution started and stopped. Once the bulk upgrade is started, the distribution continues until stopped, so be sure to manually stop the process when complete.

Figure 85 : Bulk Upgrade

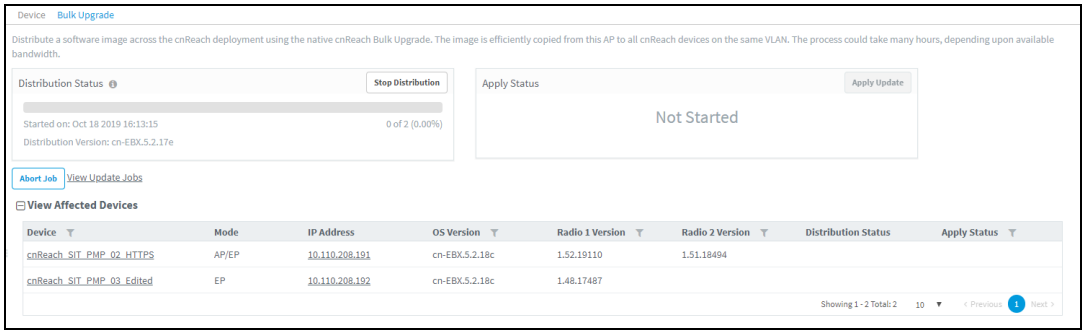


NOTE:

You must start the distribution on a single AP in a cnReach VLAN, and only run it from that AP. Executing Bulk Software Upgrade on more than one AP in a VLAN will not be prevented by cnReach devices, and it could lead to distribution failures.

Upgrade Tracking

The following page is displayed when an AP is actively distributing software. One can view other devices in the VLAN (and their current software versions), and the distribution status. Distribution can be stopped at any time, and images can be applied directly to the devices in the list.



Fixed Wireless Configuration

This chapter provides the following information:

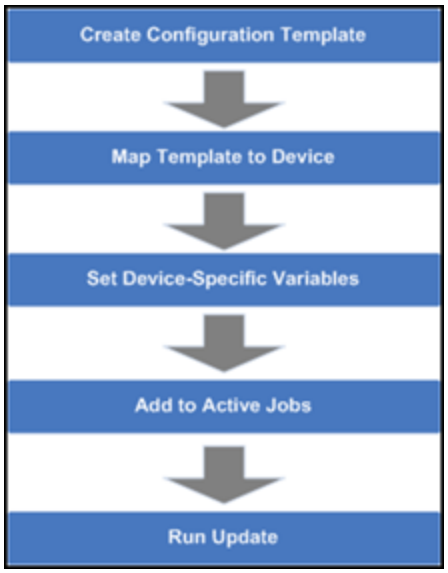
- Overview
- Configuration Templates
- Configuration Variables
- Configuration Update

Overview

Template configuration is supported for cnMatrix, cnPilot Home, ePMP, PMP, Machfu, cnVision and cnReach devices. Templates are textual representations of device settings that contain a full configuration or partial configuration. When a template is applied to a device, the only parameters changed are those in the template.

The below figure presents the basic template configuration flow:

Figure 86 Basic Template Configuration Flow



Configuration Templates

Templates can be pushed to a device manually through a configuration job. This is accomplished in the configuration management page. Templates can also be applied prior to onboarding, in which they would be provisioned in the **Onboarding** queue.

Some sample templates are listed below. The ellipses (...) represents additional content that has been excised from the example to limit the size of the text.

Sample ePMP Template

The ePMP template uses the exported ePMP configuration format, which is JSON-encoded.

Figure 87 Sample ePMP Template

```
"device_props": {
      "acsEnable":       "0",
      "acsScanMinDwellTime":   "200",
      "acsScanMaxDwellTime":   "300",
      "acsControl":      "0",
      "bcPriority":      "0",
      "cambiumInternetConnectionServerIP":       "",
      "centerFrequency":       "5670",
      "dataVLANEnable": "0",
      "dataVLANVID":     "",
      ...,
      "snmpTrapTable": [{
            "snmpTrapEntryIP":       "10.120.143.176",
            "snmpTrapEntryPort":     "162"
      }],
      ...
}
```

Configuration Variables

Administrators can embed variables into templates that will be replaced when the template is applied to a device. This allows one to leverage a shared, generic template, but to tailor it to individual devices when it is pushed. Template variables are added to a configuration file by replacing an existing parameter with a customer-defined string of the format ${VARIABLE}. An example configuration line with a single variable replacement is shown below:

“networkLanIPAddr”: $ {IP ADDRESS}

The above variable is named IP_ADDRESS. When the template is pushed to a device, this variable will be replaced with a value specific to the device. This value needs to be set for the device prior to the template application, else the configuration will not be pushed. Default values can also be specified for variables, as shown below:

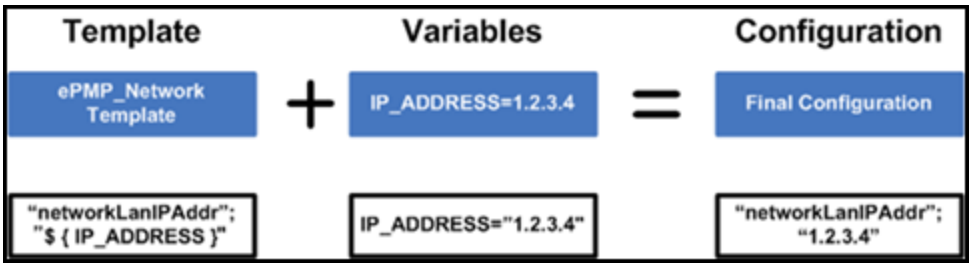
“networkLanIPAddr”: $ {IP ADDRESS="10.1.1.254"},

The default value is "10.1.1.254". In this case if the variable is not set for a device, the default value is used.

Variable Usage

The figure below highlights how **Templates** and **Variables** are merged to create the final configuration that is pushed to the device.

Figure 88 Variable Usage



Macros

Macros can be used in templates similar to configuration variables except they automatically take values provided by the device itself.

- %{ESN} will be replaced with the MAC address of the device
- %{MSN} will be replaced with the Serial Number of the device.

Variable Caching

Variables set for a particular device will be cached, so they can be re-used later. This means the next time you apply a template that leverages a variable with the same name as one used previously, its value will be pre-populated with the previous value. It is therefore beneficial to define a uniform variable naming and usage scheme for variables across different templates.

Device Type-Specific Configurations

The format and values of a configuration template are unique to the different device types. Templates that work with one type of device will not work with others, and all templates need to be mapped to a specific device type upon creation.

Device Mode Restrictions

Some devices, such as ePMP, executes in AP and SM modes. The ePMP templates can be configured so they can only be applied to devices that support a selected mode.

Variable Validation

All variables for a selected template must be mapped to a value in order to create a configuration job. If any variables are not mapped, an error will be generated. Variables that have default settings will not cause an error if they are unset.

Sample Templates

A number of sample templates are provided for each device type. These are not meant to be applied directly, but rather serve as an example of the configuration data format accepted by the device. See the documentation for your devices for full details.

Template File Creation

The typical process taken for creating your own configuration template text from scratch are below.

1. On a test device configure the parameters you are interested in pushing to devices with values that will be easy to search for. This can be done directly on the device web UI .
2. Export the device configuration. Via cnMaestro this is done by navigating to **Configuration > Templates**, selecting the device in the left-hand tree and then clicking the View Device Configuration link. This can also be done via the device GUI, typically in the Administration or Operations section where there will be an **Export** for configuration.
3. View the configuration file in a text editor like Notepad++ and search for the values you entered in step 1. You can also search for the parameter name to try to find the correct lines.
4. Copy and paste the relevant lines into a new file.
5. Optionally replace values with replacement variable text. This will allow you to set the value per device.
6. Once you have this partial template it can be copied into the template creation text field and saved.

Template

To create a configuration template:

1. Navigate to **Shared Settings >Templates** in the main menu.
2. Click the **Add Template**.
3. Choose a **Device Type**, **Name**, and **Description** for the template. For ePMP templates, you should select a **Device Mode**.

4. Either upload your template into the UI or paste the template.
5. After clicking **Save**, the template will be available in the selection menu on the configuration and onboarding pages, as long as the device type and mode match the device selected.
6. By selecting **Custom** option under **Template** type filter. All Default templates will be hidden.

> **NOTE:**
>
> When you navigate to the **Template** default template type filter will be custom. User needs to select **All** or **Default** in order to view other templates.

Figure 89 Template configuration (ePMP/PMP)

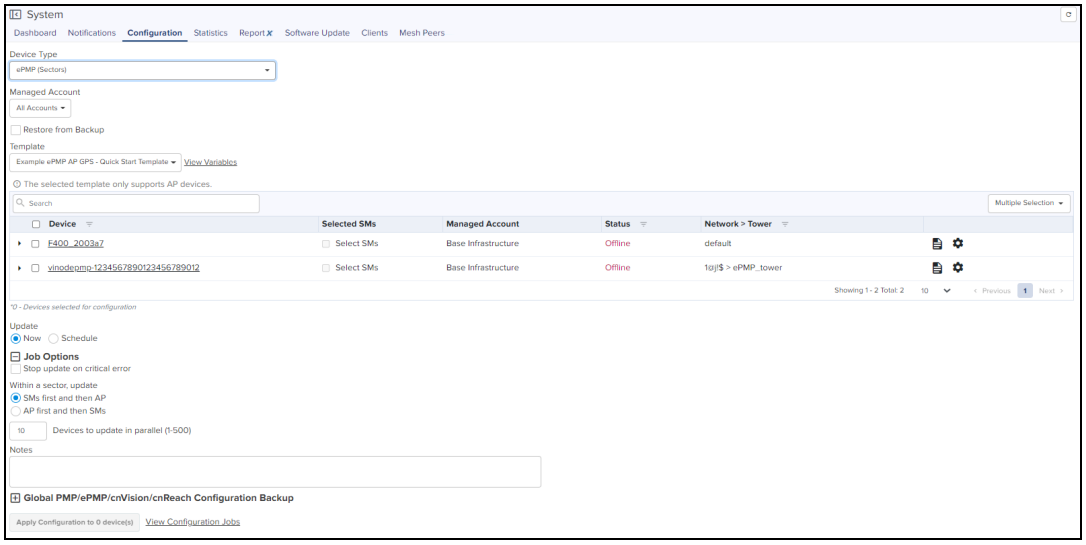


Figure 90 Template configuration (cnPilot Home R-Series)

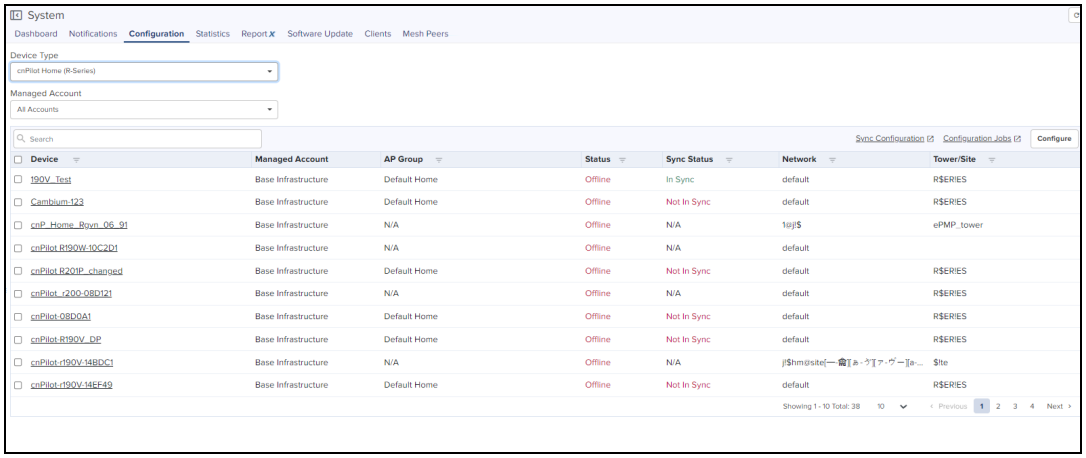


Figure 91 Template configuration (cnVision)

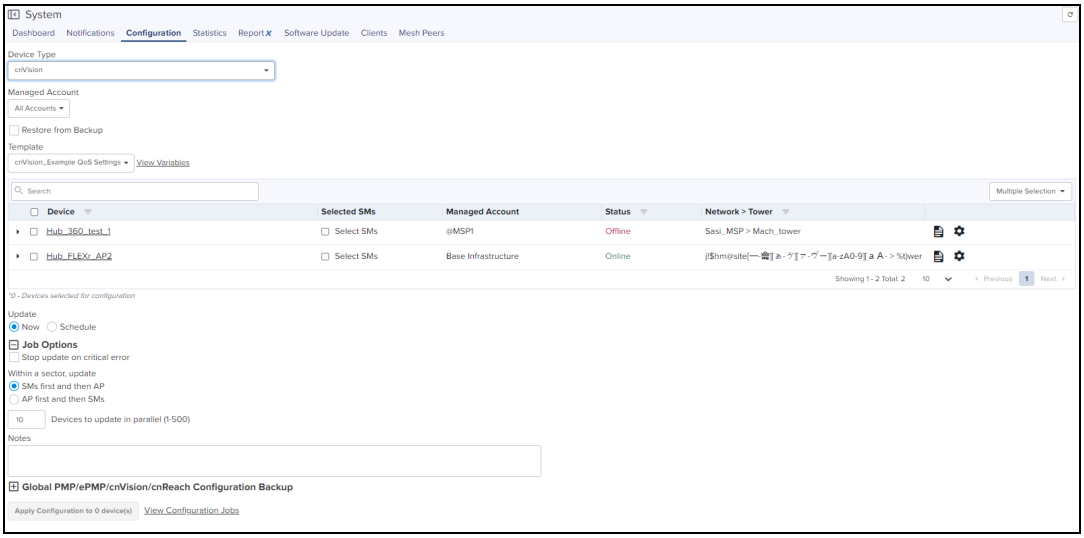
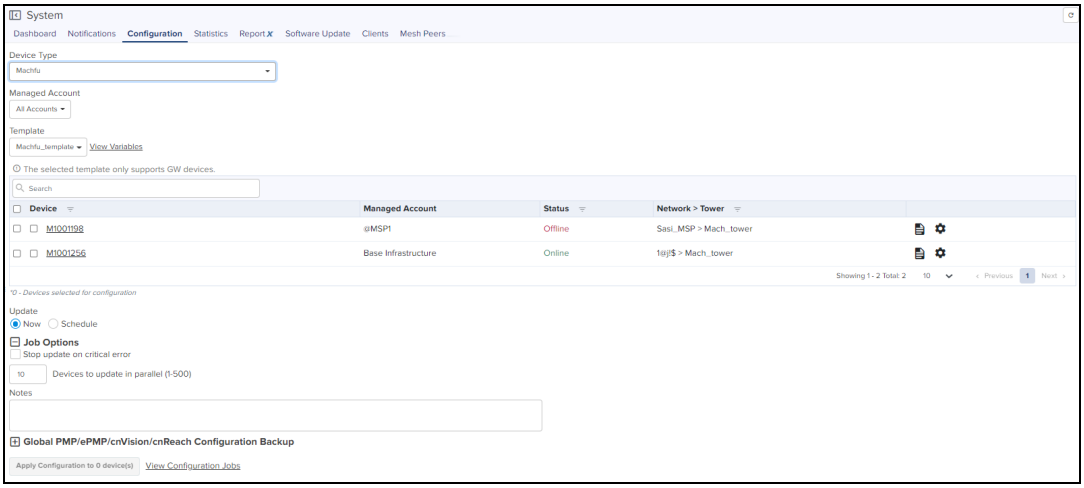


Figure 92 Template configuration (Machfu)



Configuration Update

Device Selection

First navigate to the **Configuration Update** tab, then navigate the Device Tree to the appropriate level for device selection. For example, selecting an AP will enable selection of the AP and all its SMs.

Device Type

Configuration jobs are created for a single device type. The type includes the specific hardware (ePMP, PMP) as well as the mode of the device (cnVision, PMP or PTP mode for ePMP for example).

Device Table

Select the devices to upgrade in the Devices Table. The following parameters are visible in the table:

Table 36: Parameters Displayed in the Device Table

Parameter	Description
Devices	The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree.
Network/Tower	The network and the tower on which the device is located.
Status	The status of a particular device in a system. Devices that are “Down” cannot have images pushed to them.

NOTE:

You can save and download the existing device configuration as template by clicking **View Device Configuration** link.

Options

Stop all Configuration on a Critical Error

If one of the configuration updates fails, then do not start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off.

Parallel Upgrades

Define how many configuration updates to perform in parallel.

Start Job Now

If enabled, attempts to automatically start the configuration job immediately after creation.

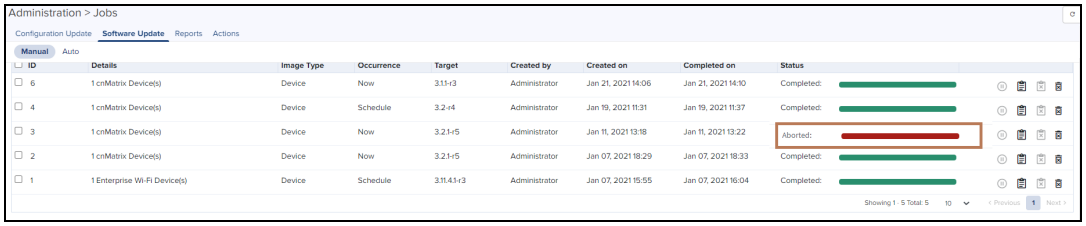
Update Ordering

Allows you to specify update ordering within a sector. Options are SMs first and then AP or AP first and then SMs.

Abort Configuration

Abort operation will skip devices that are waiting for update to begin. Devices already that are being updated may continue but cnMaestro will stop tracking their progress. Aborting a Configuration Job puts the device into a complete state that cannot be manually restarted by the user. The pending devices will not begin their updates.

Figure 93 Abort Configuration





NOTE:

1. Devices which are already completed display as "completed" with a message "update complete" along with the status as Completed.

2. Devices which are ongoing display as "Aborted" with a message "Manually Aborted" with the status as Aborted.

3. Devices which have not yet started display as "skipped" with a message "job was aborted" with the status as Skipped.

Configuration Update Steps

To update the configuration of an ePMP (Sectors) device:

1. Navigate to **Manage > Configuration > Device Details** in the main menu.
2. Navigate to **System > Network** in the Device Tree. From the list of available networks, select a network in which the device belongs.
3. Select ePMP (Sectors) from the following **Device Type** drop-down list:
   a. cnMatrix
   b. cnPilot Enterprise (ePMP Hotspot)
   c. cnPilot Home (R-Series)
   d. cnReach
   e. cnVision
   f. Enterprise Wi-Fi (E-Series, XV-Series)
   g. ePMP (Sectors)
   h. Machfu
   i. PMP (Sectors)
   j. PTP
4. Select the configuration template to upgrade from the **Template** drop-down list.
5. Select the device(s) to upgrade by clicking the tick icon.
6. Set any variables that are required for selected devices by clicking the gear icon under the "Configure" column on the right side of the table. The configuration upgrade cannot proceed until all required variables (those without default parameters) are set. If you attempt to create a configuration job without setting required variables, the gear icon will turn red for any devices not meeting this requirement.
7. Click **Apply Configuration**.



NOTE:

You can save and download the existing device configuration as template by clicking **View Device Configuration** link.

Configuration Backup

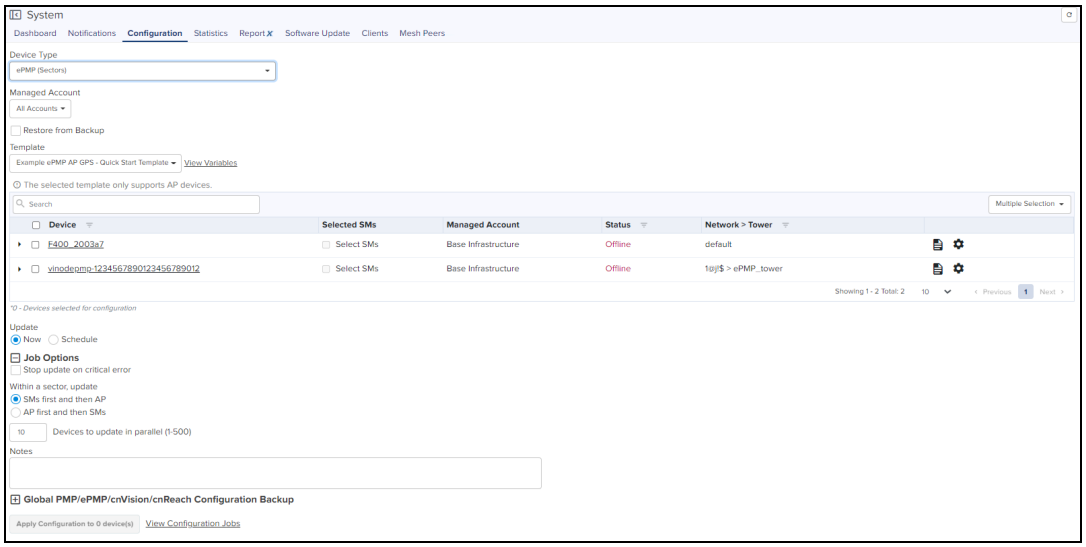
Configuration Backup pulls and stores configuration from Fixed Wireless devices (PMP and ePMP) and cnReach devices which are currently online.

The backup operations log can be done through:

- System level
- Device level

System Level

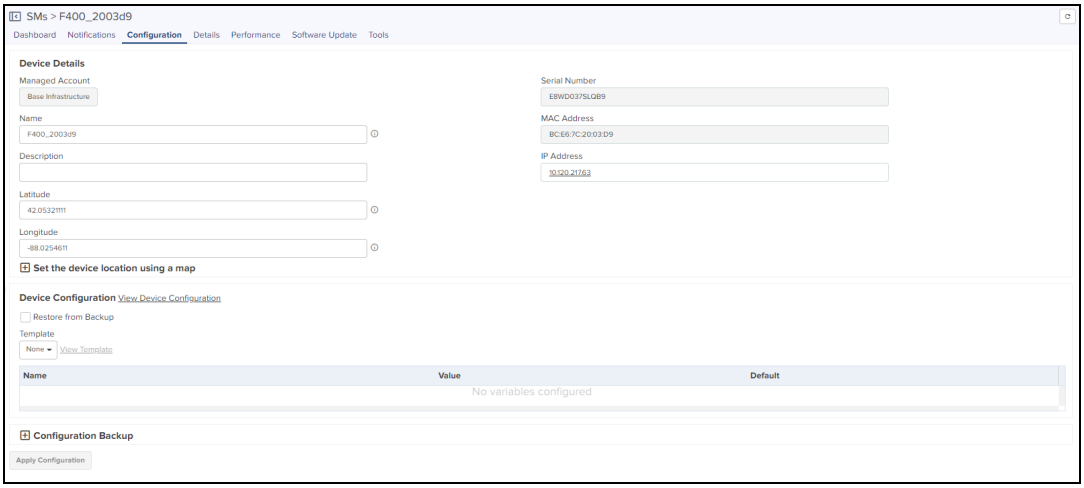
1. Navigate to **Manage > Configuration**.
2. Select cnReach/cnVision/PMP/ePMP (Sectors) from the following **Device Type** drop-down list:
3. In **Global cnReach/PMP/ePMP Configuration Backup** click **Backup Now.**



4. Last backup displays in the **Log from Last Execution** tab with the date and time.
5. Click **Export** to export the backup in **.json** format.

Device Level

1. Navigate to **Manage > System,** select cnReach/cnVision/PMP/ePMP **Network** in the Device Tree.
2. Navigate to **Configuration > Configuration Backup** click **Backup Now.**



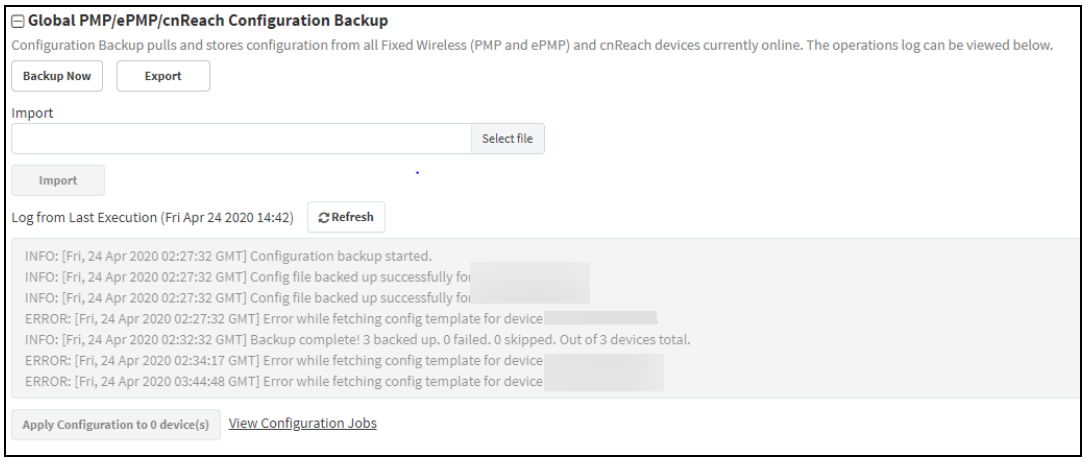
3. Click **View** to view the backup data.



Import Configuration Backup

Perform as follows to import the configuration backup of the device.

1. Navigate to **Manage > Configuration > Device Details** in the main menu.
2. Select cnReach/cnVision/PMP/ePMP (Sectors) from the following **Device Type** drop-down list:
3. In **Global cnReach/cnVision/PMP/ePMP Configuration Backup,** click **Select File** in import tab.



4. Once selected the file click **Import**.

Restore from Backup

Restore from backup operations can be done through:

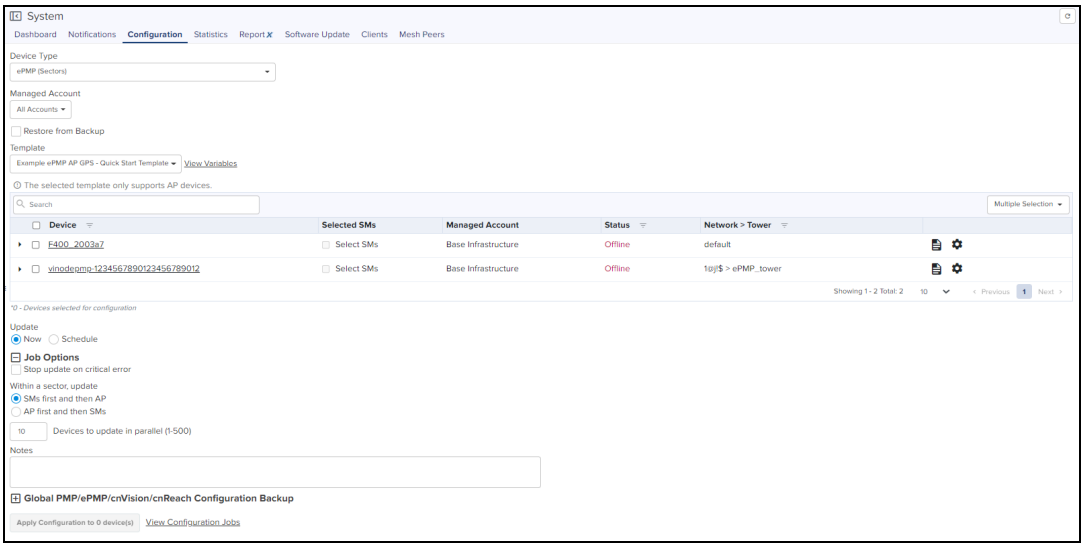
- System level

- Device level

System Level

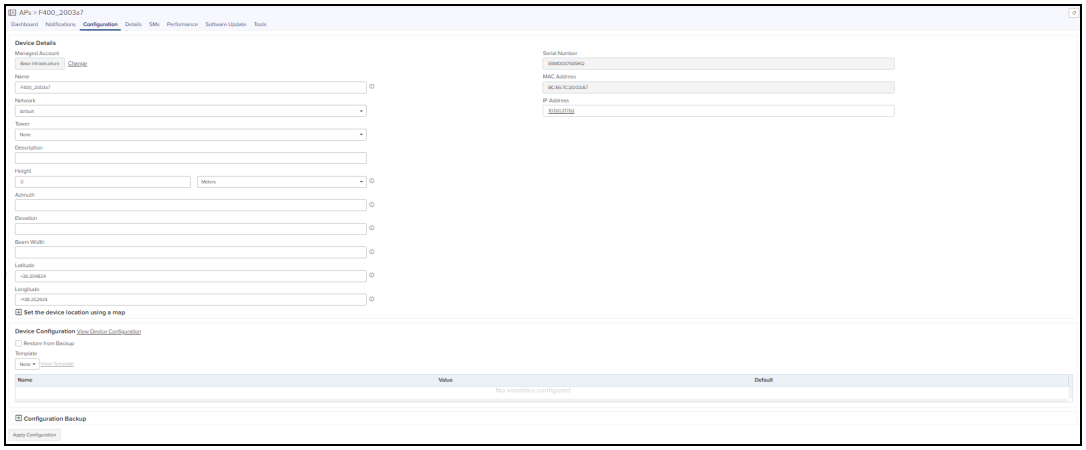
Perform as follows to restore the configuration backup of the device.

1. Navigate to **Manage,** select **System/Managed Account/ Network/Tower > Configuration** in the main menu.
2. Select cnReach/cnVision/PMP/ePMP (Sectors) from the following **Device Type** drop-down list.
3. Enable the **Restore from Backup.**
4. Select the Device from the list.
5. Click **Apply Configuration to devices.**



Device Level

1. Navigate to **Manage > System,** select **cnReach/cnVision/PMP/ePMP Network** in the Device Tree.
2. Navigate to **Configuration > Device Configuration >** click **Restore from Backup**.
3. Click **Apply Configuration to devices.**



Jobs

Administration > Jobs > Configuration Update tab lists all currently running, queued and completed jobs. The jobs can be triggered immediately or run later.

The following table displays the list of parameters in the **Jobs** tab:

Table 37: Parameters displayed in Configuration Update tab

Parameter	Description
Action	Use the **Start** or **Delete** button to manage the upgrade process. After upgrade has started, the **Pause** button will stop new upgrades from beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the **Resume** button.
Created By	The user who has created this job.
Created On	Date and time on which the job is created.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Parallel	Number of device to start in parallel.
Stop on Error	Stop the job, if any device in middle finds any error.
Sector Priority	For ePMP/PMP, cnVision Client/Hub, the priority of AP/SM to start.
Status	Status of update.
Target	Target software version to upgrade.
By selecting the **Show More** icon, you can view the following parameters:	
Device	Device for which the upgrade is initiated.
Message	The message displayed after the update.
Result	The upgrade status of the device.
Status	Status of the device.

Configuration Update

Administrators can apply configuration to devices during the onboarding process: prior to approving the device in the **Onboarding** queue, the configuration template and variables can be specified.These will then be pushed to the device during onboarding. For more details on onboarding, see Device Onboarding.

Wireless LAN Configuration

Wi-Fi configuration is handled through AP Groups (Fixed Wireless devices, such as cnMatrix, ePMP and PMP, use Templates).

This chapter provides the following details:

- cnPilot Home and Enterprise Wi-Fi
- Factory Reset
- cnMatrix Switches

cnPilot Home and Enterprise Wi-Fi

This section provides the following details:

- Configure cnPilot using cnMaestro
- Pre-Defined Overrides
- User-Defined Overrides
- User-Defined Variables
- Synchronize (Sync) Configuration
- Configuration Job Status

There are two types of cnPilot devices:

1. Enterprise Wi-Fi by Enterprise Wi-Fi (E-Series), Enterprise Wi-Fi (XV-Series) and cnPilot Enterprise (ePMP hotspot)

2. cnPilot Home by cnPilot R-Series devices.

Each WLAN or AP Group, prior to creation, is mapped to one of these device categories and can only be used with supported device types. Two categories are required, because the features available in Enterprise and Home are different.

Configure cnPilot using cnMaestro

cnPilot devices are configured by creating an AP Group, mapping it to shared WLANs, and then assigning it to a particular device through the **Configuration** tab. Once assigned, the configuration is pushed automatically if Auto Sync is enabled, or manually if disabled (this requires a manual sync).

Auto Synchronization

AP Groups can automatically synchronize device configuration whenever the AP Group or associated WLANs are updated. This is done by enabling **Auto Sync** in the AP Group configuration page.

Manual Synchronization

When a device is mapped to an AP Group without Auto Sync turned on, the device will be placed in an unsynchronized state until it is manually synchronized. This can be done by navigating to the device Configuration page and clicking the **Sync Now** button, or by navigating to the **Sync Configuration** page (**Administration > Sync Configuration**).

The process for creating a Wi-Fi device configuration is as follows:

1. Navigate to **Shared Settings > AP Groups and WLANs.**
2. Create an AP Group.

3. Select an AP Group Type. The choices are cnPilot Home (which represents the R-Series) and cnPilot Enterprise (which maps to the E-Series and ePMP Hotspot). The configuration options depend upon the AP Group Type.



NOTE:

The Wireless LAN view supports cnPilot Enterprise devices, so the cnPilot Home device type is not available.

4. Assign WLANs to the AP Group (you may want to update WLAN SSID and security parameters during this step).
5. Map devices to an AP Group by selecting the AP Group in the device **Configuration** tab.

AP Groups support all Wi-Fi devices, including: cnPilot R190/200/201, cnPilot E400/E410/E500, and ePMP 1000 Hotspot.

Creating a WLAN

To create a WLAN, navigate to **Shared Settings > AP Groups and WLANs** (or the WLAN page in the Wireless LAN View) and select **New WLAN**. As with AP Groups, WLANs are separated into cnPilot Home and cnPilot Enterprise types. cnPilot Enterprise WLANs are able to configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters. cnPilot Home WLANs can configure SSID, Scheduled Access, and Access parameters.

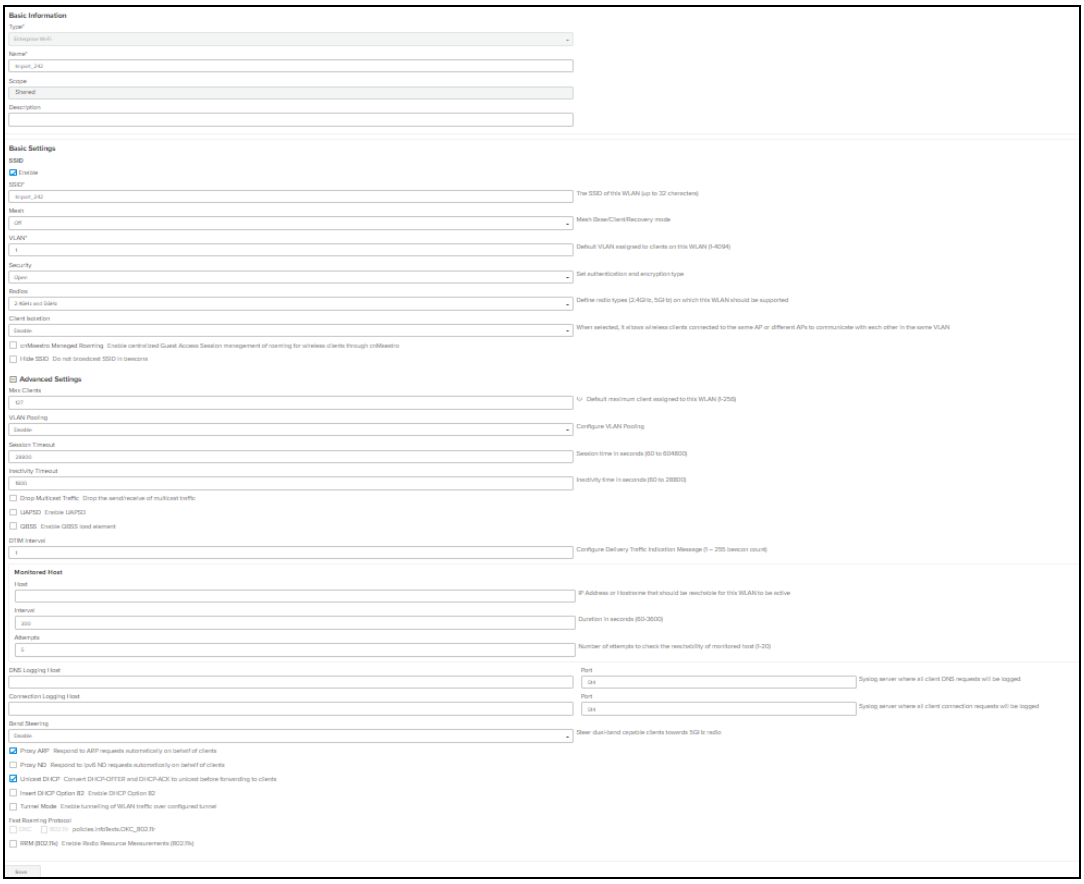


NOTE:

The special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z0-9_-*&%#@!<>.()[]^~`$). The user can also rename them if required.

Steps to create WLAN policy:

1. From homepage navigate to **WLANs.**
2. Click **New WLAN**, provide basic parameters to WLAN, and ensure **WPA2 Pre-Shared keys** is enabled in Security drop-down.



3. Click **Save**.

Creating a ePSK WLAN

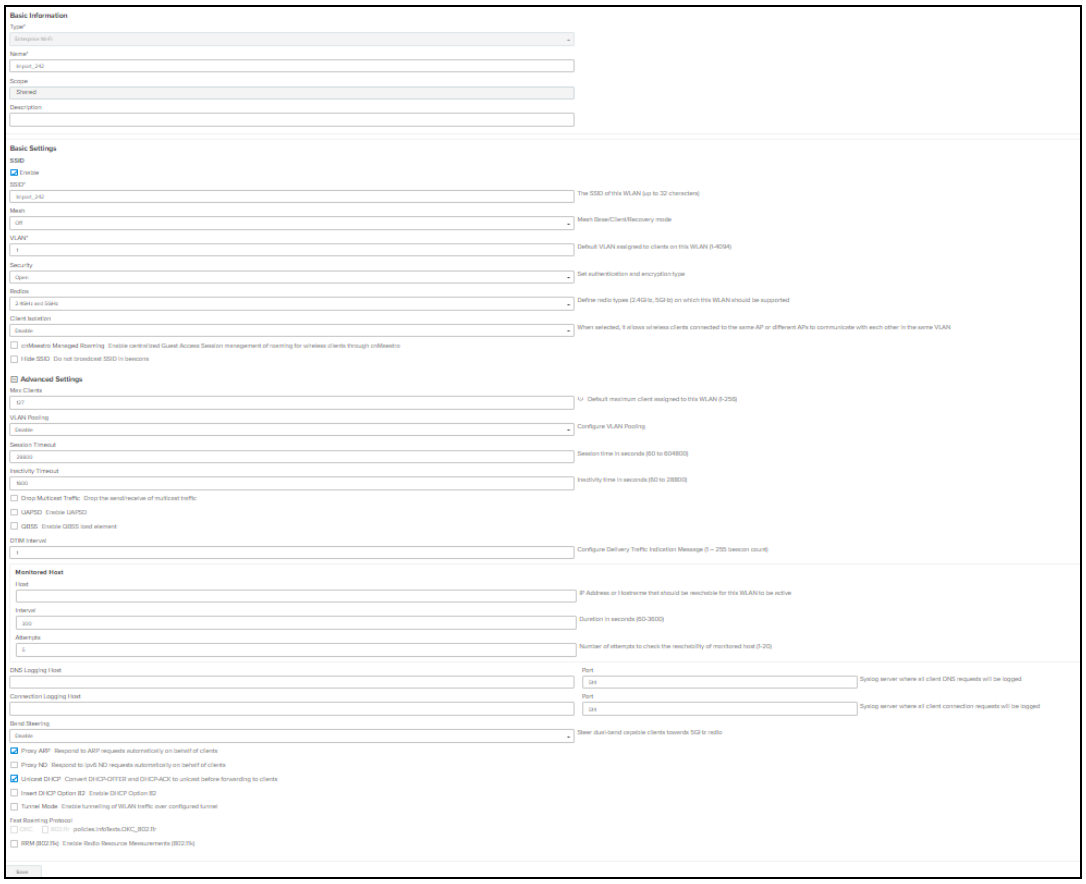
To create a WLAN, navigate to **Shared Settings > AP Groups and WLANs** (or the WLAN page in the Wireless LAN View) and select **New WLAN**. As with AP Groups, WLANs are separated into cnPilot Home and cnPilot Enterprise types. cnPilot Enterprise WLANs are able to configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters. cnPilot Home WLANs can configure SSID, Scheduled Access, and Access parameters.

NOTE:

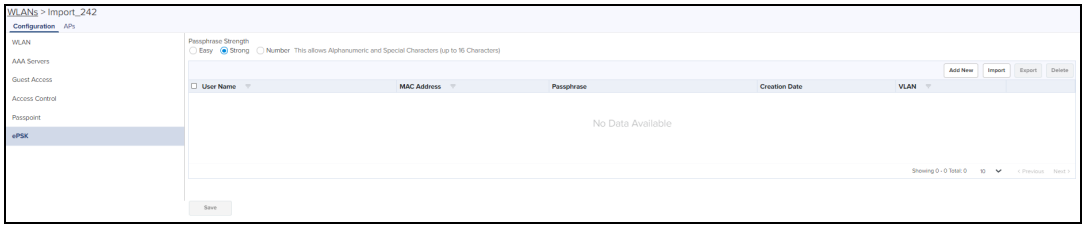
- The special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z0-9_-*&%#@!<>.()[]^~`$). The user can also rename them if required.
- In cnMaestro X pro user allowed to create 1024 espk per Wlan.
- By default password will not be configured. User has to configure the password for WLAN.

Steps to create WLAN policy:

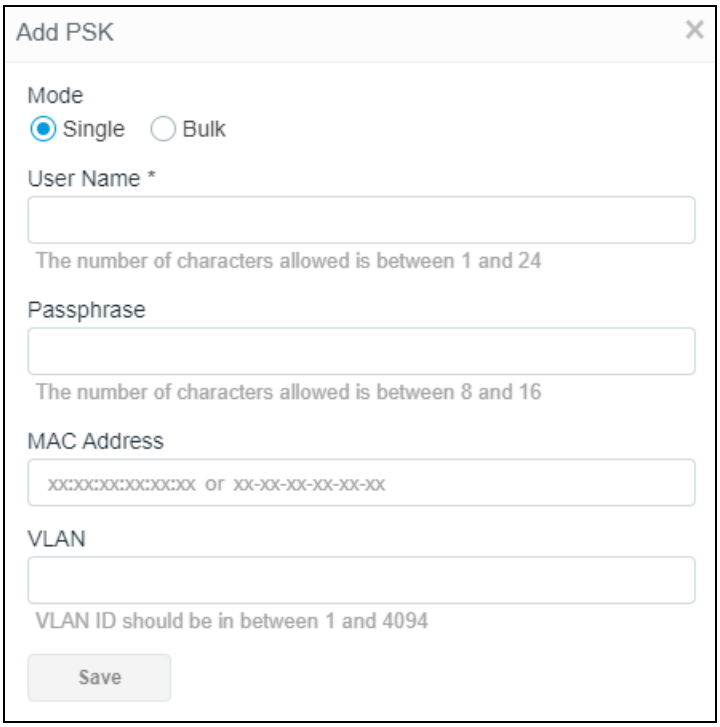
1. From homepage navigate to **WLANs.**
2. Click **New WLAN**, provide basic parameters to WLAN, and ensure **WPA2 Pre-Shared keys** is enabled in Security drop-down.



3. Click **Save**.
4. Navigate to **ePSK** tab. Select the **Passphrase Strength** as **Easy** or **Strong** or **Number**.



5. Click **Add New**. The Add PSK window pops-up where you can select the **Mode** as either **Single** or **Bulk**.
6. In Single Mode **User Name** is mandatory and rest of the entries are optional.

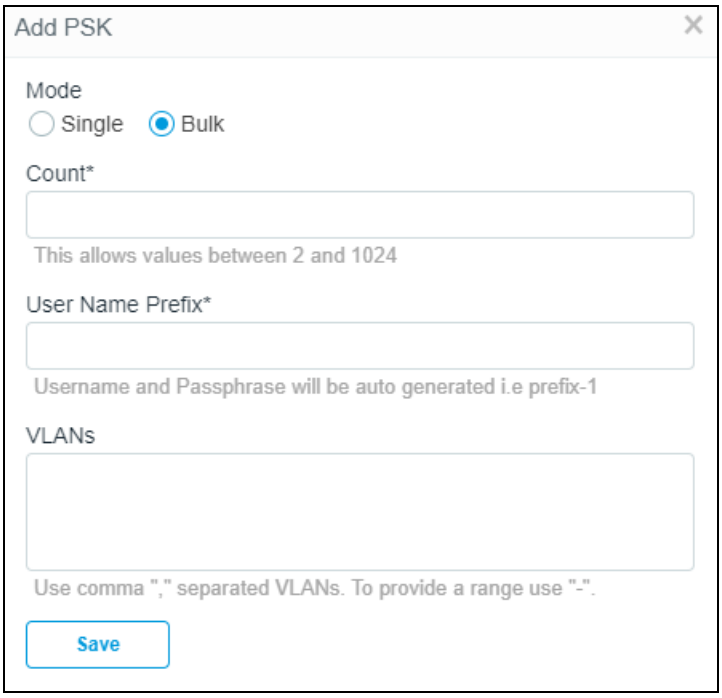


	NOTE: Passphrase is optional and it will be automatically generated based on the selected passphrase strength.

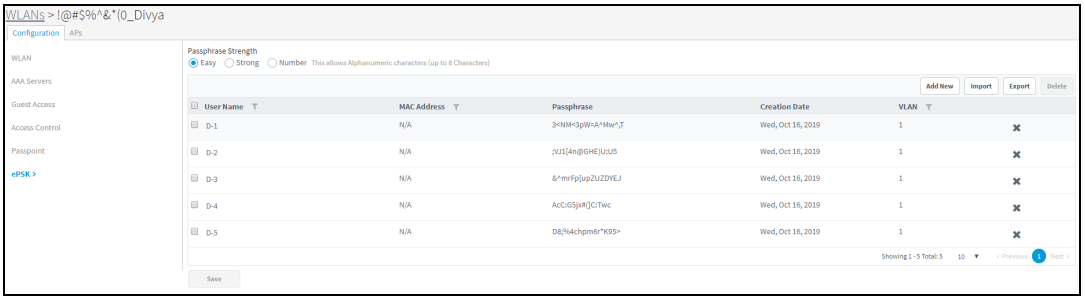
6. In **Single** Mode we can see single entry only.



7. In **Bulk** Mode, **Count** and **User Name Prefix** are mandatory fields. Enter the **Count** and **User Name Prefix**.

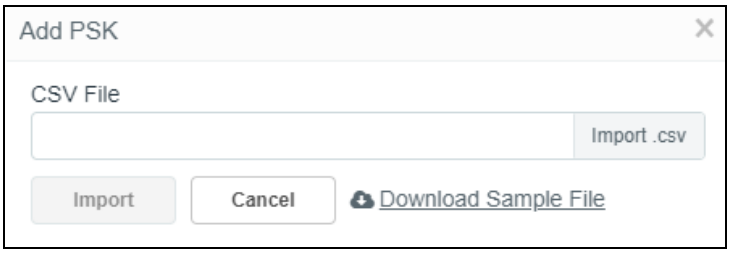


8. In **Bulk** Mode we can see many entries.

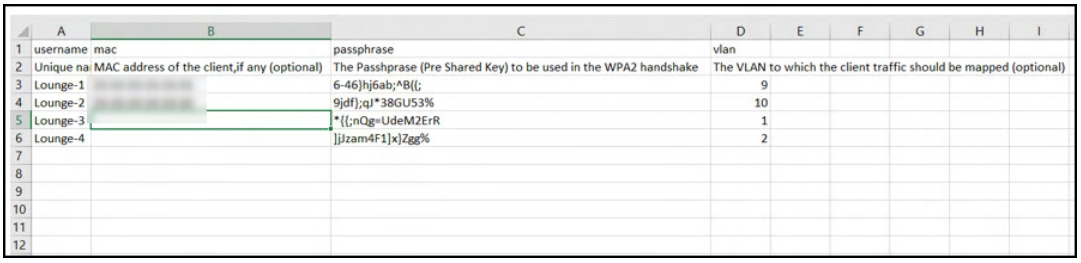


Import ePSK

1. Click **Import**. A dialogue box appears.
2. Select **import.csv** and import the file.



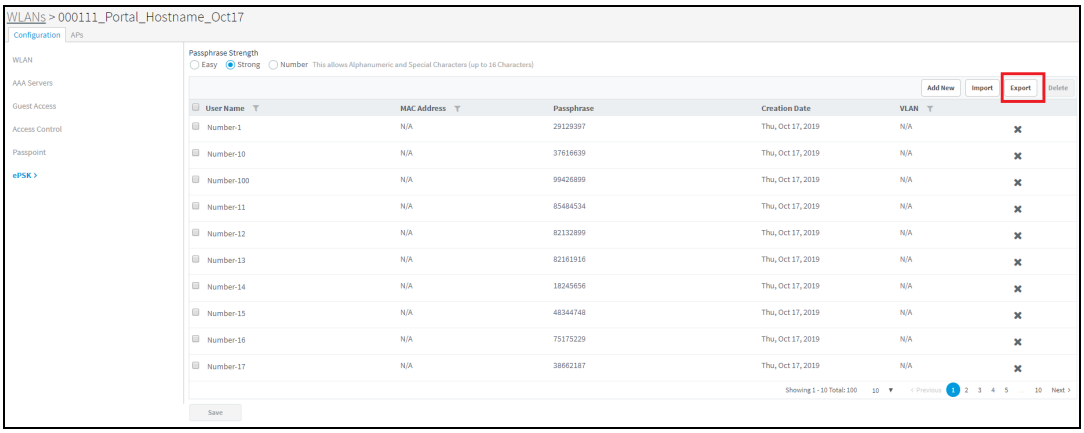
3. When you click **Download Sample File**, you can see Sample ePSK excel sheet.



	A	B	C	D	E	F	G	H	I
1	username	mac	passphrase	vlan					
2	Unique na	MAC address of the client,if any (optional)	The Passphrase (Pre Shared Key) to be used in the WPA2 handshake	The VLAN to which the client traffic should be mapped (optional)					
3	Lounge-1		6-46}hj6ab;^B((;	9					
4	Lounge-2		9jdf};qJ*38GU53%	10					
5	Lounge-3		*{{;nQg=UdeM2ErR	1					
6	Lounge-4		]jJzam4F1]x]Zgg%	2					
7									
8									
9									
10									
11									
12									

Export ePSK

1. Click **Export**. A dialogue box appears.
2. Select **export.csv** and export the file.

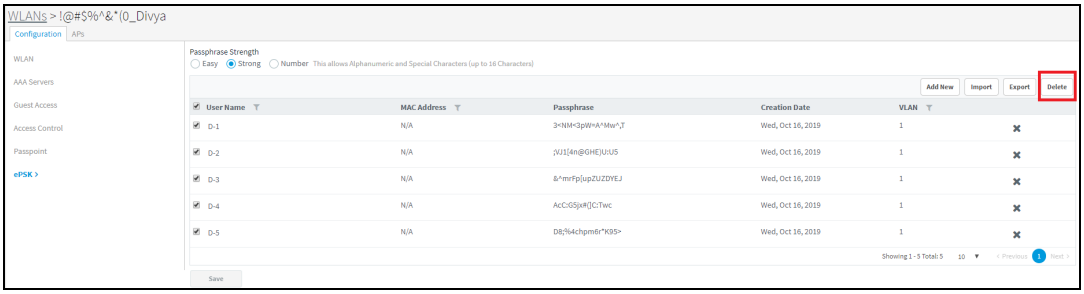


3. When you click **Download Sample File**, you can see Sample ePSK excel sheet.

	A	B	C	D	E	F	G	H	I
1	username	mac	passphrase	vlan					
2	Unique na	MAC addr	The Passh	The VLAN to which the client traffic should be mapped (optional)					
3	Room-1		WVghr8SmY_a;;Q(e						
4	Room-2		a{n5&HepkJ~=Qt%,						
5	Room-3		6q@Qk#WU8JzC.Br)						
6	Room-4		eX~g!n!sjj]tZw[j						
7	Room-5		y$cqds{!YAw5gJ;p						
8	Room-6		j;Ag]EBKk8kNRS*c						
9	Room-7		8H($F}u;m9C4_MQ=						
10	Room-8		_(hgH7;dzb]Ys~9w						
11	Room-9		7%[C5bqDMpt^()2]						
12	Room-10		3mq=xY~zg&fn!mN%						

Delete ePSK

To delete ePSK, select the ePSK and click **Delete**.



NOTE:

- You can group select or individually select ePSK entry and delete the same.
- ePSK feature is supported in cnPilot from System Release 3.11.1 onwards.

Create an AP Group

To create an AP Group, perform the following steps:

1. Navigate to **Configuration > AP Groups and WLANs** page **> AP Group** tab.
2. Click **New AP Group** tab.
3. Enter values of **AP Group name, Country name**, and **WLAN** parameters.
4. Click **Add WLAN** and select **WLAN** from the list.
5. Enter the **Administrator** password in the Management tab.
6. Click **Save**.

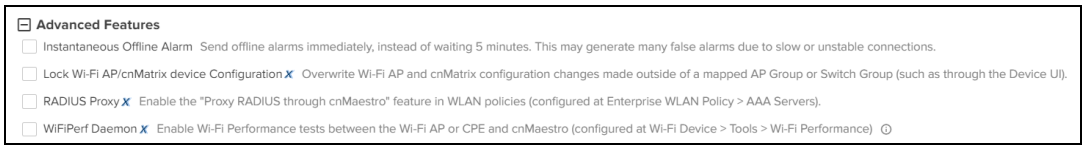
Map WLANs to AP Groups

WLANs are added to AP Groups in the AP Group configuration. Ensure that the WLANs are ordered correctly if Mesh mode is used.

> **NOTE:**
>
> Maximum of 16 WLAN policies are supported for E-Series and XV-Series devices and 8 WLAN policies are supported for ePMP 1000 Hotspot and Only one WLAN for cnPilot Home AP Group.

Lock cnPilot/cnMatrix device Configuration

This feature supports automatically restoring the configuration of devices to their mapped AP Group if their configuration is changed outside of cnMaestro. When this feature is enabled in cnMaestro, the configurations changed from the UI or CLI of the device are reverted back by pushing the existing AP Group configuration. The configuration will get pushed only if the device is in sync status.



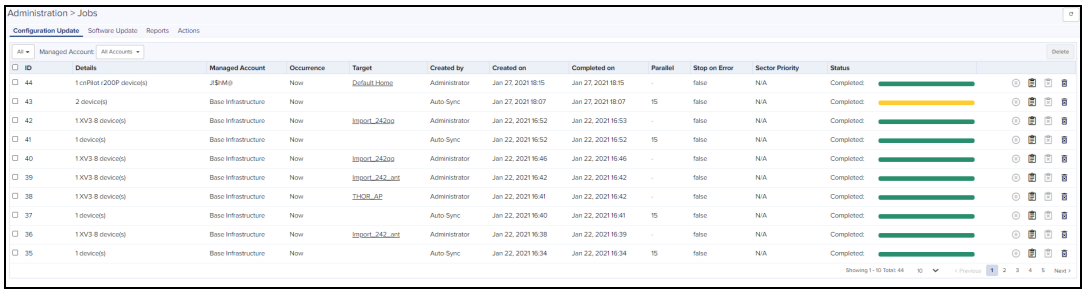
To enable this feature:

1. Navigate to **Administration > Settings > Advanced Features** page.
2. Enable the **Lock cnPilot/cnMatrix device Configuration** check box.

3. Click **Save**.

When a configuration change is made on the device via its UI or CLI, cnMaestro detects the change as **Device's configuration changed outside of cnMaestro** and the device is marked as **Not In Sync**. In this scenario, an Auto-Sync job is triggered automatically by cnMaestro to revert back the changes.

The Auto-Sync job can be viewed in **Administration > Jobs > Configuration Update** page.

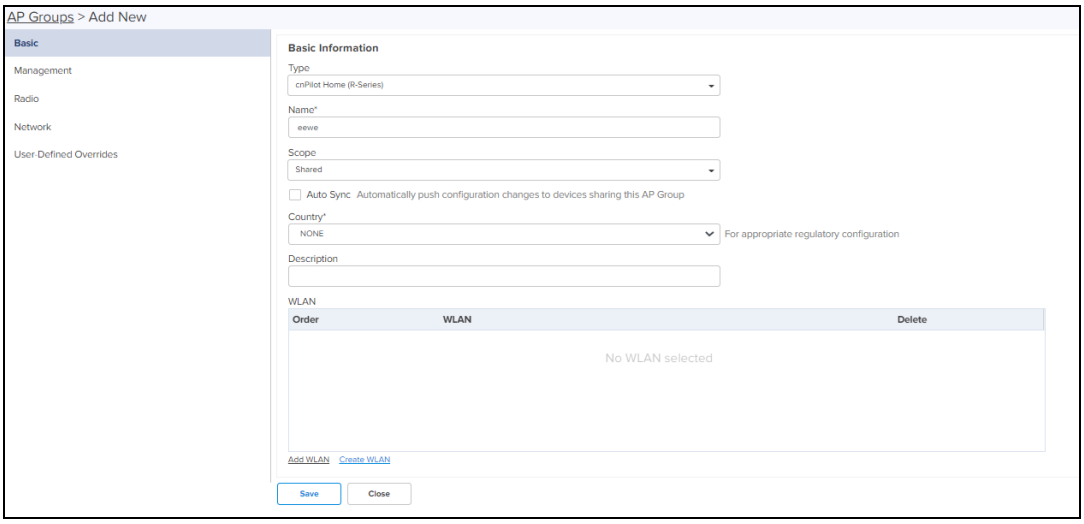


Retry Configure

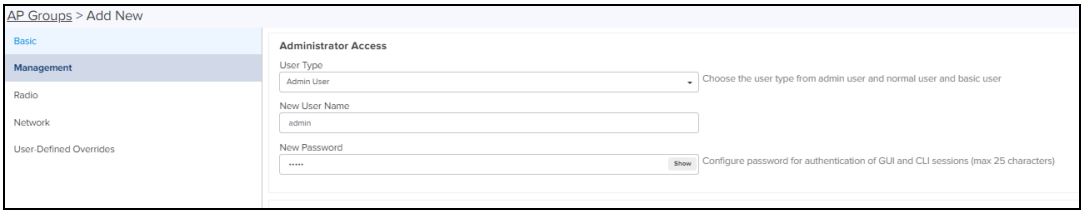
When the user tries to apply any AP Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as "Device was offline", in the **Jobs** page. In this case, when device comes up and connects to cnMaestro, then cnMaestro will create an Auto-sync job for that device and pushes the AP group. (It will not apply the AP group if the **Auto-Sync** was disabled in the AP group).

NOTE:

The config update (Auto-Sync) will happen only when the "Auto-Sync" option was enabled in the AP Groups page. If the device was skipped/failed because of any other reason other than the "Device was offline", then the device will not be updated.



Default password: **admin** of cnPilot R-series should be changed before upgrading to the build 4.6-RX.



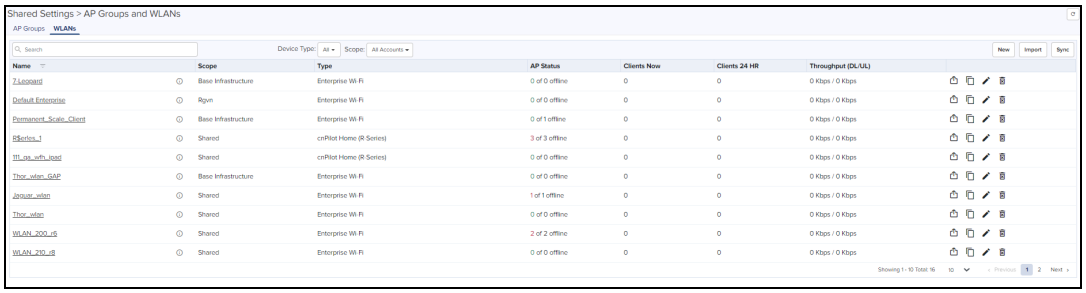
Once after the upgradation of build 4.6-RX, default password; **admin** becomes invalid and password needs to be reset through the WAN.

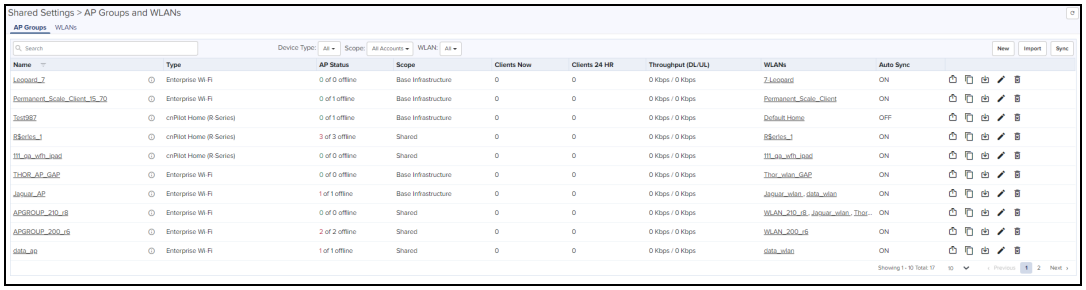
NOTE:

Default User Name: **admin** can be used after the upgradation.

Import/Export of AP Groups and WLANs

The AP Groups and WLANs are created for cnPilot Home and Enterprise devices. The configurations created for each AP Groups and WLANs in a server can be exported and imported to different servers. This will help the users reduce the effort of manually creating the WLAN and AP Group each time.





To export WLAN and AP Group,

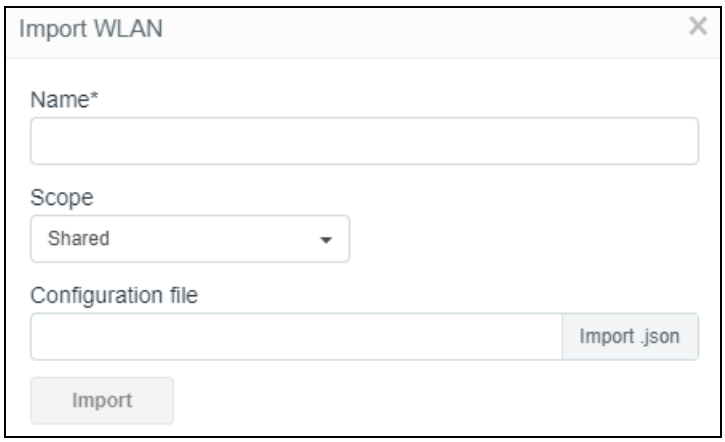
1. Navigate to **Shared Settings > AP Groups and WLANs page > WLAN** or **AP Group** tab (according to the choice).
2. Click **Export**.

NOTE:

- The AP Groups and WLANs should be exported separately as the associated WLANs are not exported while exporting an AP Group.
- The AP Groups and WLANs will be exported with proper name and time stamp.

To import WLAN and AP Group,

1. Navigate to **Shared Settings > AP Groups and WLANs page > WLAN** or **AP Group** tab (according to the choice).
2. Click **Import WLAN**.



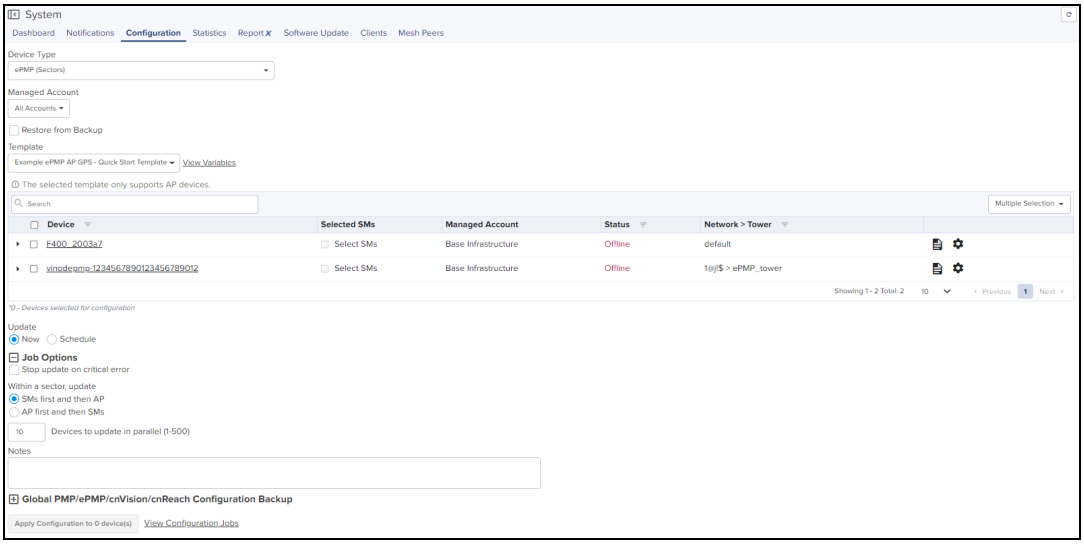
3. Enter the **Name.**
4. Select the **Configuration file** in Json format.
5. Click **Import**.

NOTE:

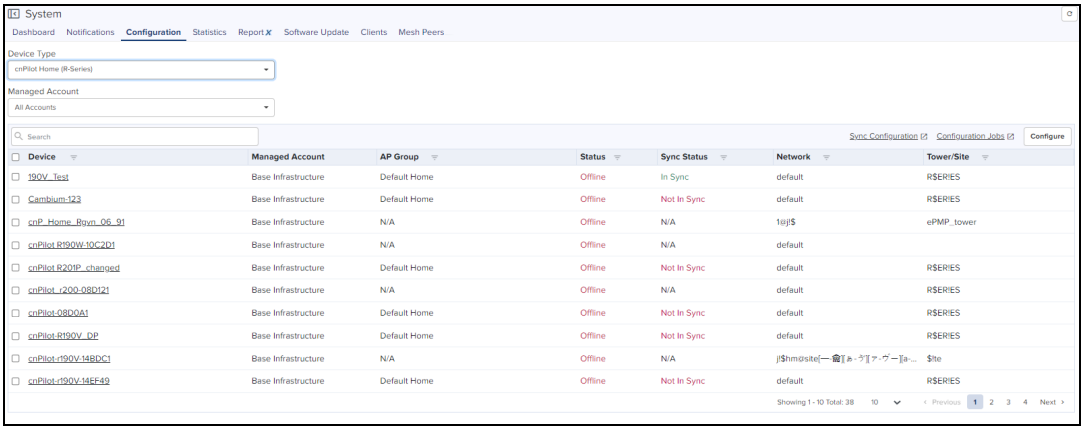
- To import an AP Group, ensure that all the associated WLANs in that AP Group are already imported. If the WLAN associated with the AP Group is unavailable, an error message will be displayed during AP Group import.
- If the name is not provided for WLAN or AP Group while importing, it will take the name of the file that is to be imported, automatically.
- If the name provided for the AP Group/WLAN while importing matches with the existing list of WLAN or AP Group in the system, an error " **The specified policy name already exists**" will be displayed.
- Importing WLAN and AP group type R-series are not allowed in Wi-Fi mode.

Create a Configuration Job

Configuration job can be created from **Monitor and Manage > System > Configuration**. Select a device type and a set of devices along with AP groups to which they will be mapped. This can be done in three steps:



1. Select the **AP Group**.
2. Select the list of Wi-Fi Devices.
3. Click **Apply Configuration.**

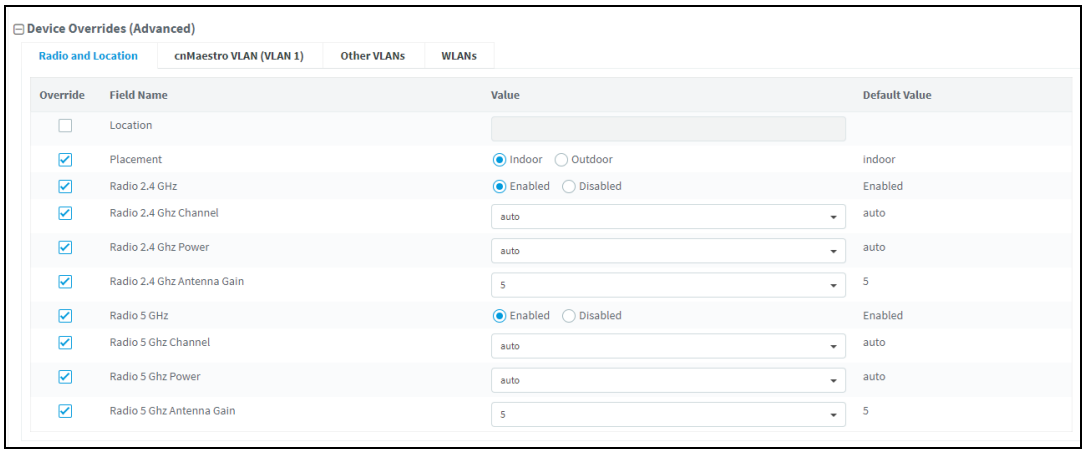


Pre-Defined Overrides

Some device configuration is generally specific to an individual device, and hence not easily shared through an AP Group. This includes IP Address, Radio Channel Settings, and WLAN details such as SSID, Enabling/Disabling SSID, Enabling/Disabling Radio 2.4 GHz and 5 GHz, and Passphrase. These items can be configured in the device Configuration tab, navigate to **Manage > Configuration** and select a device in the tree to update.

You can then choose/change different values from AP Group to be overridden. The icon to the left of a field must be selected first to override that parameter. After specifying override parameters, select **Apply Configuration** on the bottom right to save your changes to the server and create a job to push the new values to the device. This option is also applicable for Onboarding process queue.

By default, Enterprise Wi-Fi devices will have **Auto-set** from device enabled. This option reads several network related configuration fields from the device and uses those as override values to prevent overwriting values that would disconnect the device.



User-Defined Overrides

User-Defined Overrides can be entered into the end of an AP Group configuration. They will be merged into or appended to the AP Groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI, and they are considered as advanced operation that should rarely be used. The format of the commands would be same as with the device CLI.

For example, if a new version of the software had a feature unsupported in cnMaestro, it could can be pushed to the device using CLI commands through the User-Defined Override mechanism

This can be explained with the following example, in which country-code and hostname are appended to the end of the configuration, and will override any settings in the UI

```
country-code IN

hostname Wi-Fi_Device
```

User-Defined Variables

Override configuration also supports a programmatic concept called user-defined variables (which are also used with Fixed Wireless templates). User-Defined Variables can be embedded into the User-Defined Override text area. They require a value to be set for each device mapped to the AP Group before the configuration can be applied. This is either through a default value, or an explicit setting in the device configuration.

The syntax for user-defined variables is shown in the following example: the VariableName maps to an identifier set by each Device. If the value is not set, the optional DefaultValue will be used.

```
Parametername ${VariableName=DefaultValue}
```



NOTE:
You can also configure the user-defined variables in the Onboarding process queue page. They are mapped individually to each device.

Other Examples

Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP hotspot)

```
country-code ${countryname=US} // country name with US as default value
hostname ${hostname=ePMP_1000_Hostpot}
```

cnPilot Home R-Series

```
Parametername ${varaibleName=someDefaultValue}
```

Example

```
CountryCode=${countryName=IE}
RTDEV_CountryCode=${5GHz_CountryName=IE}
wan_ipaddr=${wan_ip=10.110.68.10}
```

Macros can be used in Advanced Configuration similar to User-Defined Overrides except they automatically take values provided by the device itself.

- %{ESN} will be replaced with the MAC address of devices.
- %{MSN} will be replaced with the Serial Number of devices.

Bulk Overrides

Bulk Overrides allows the user to edit the multiple configurations shared through an AP Group for one or more devices.

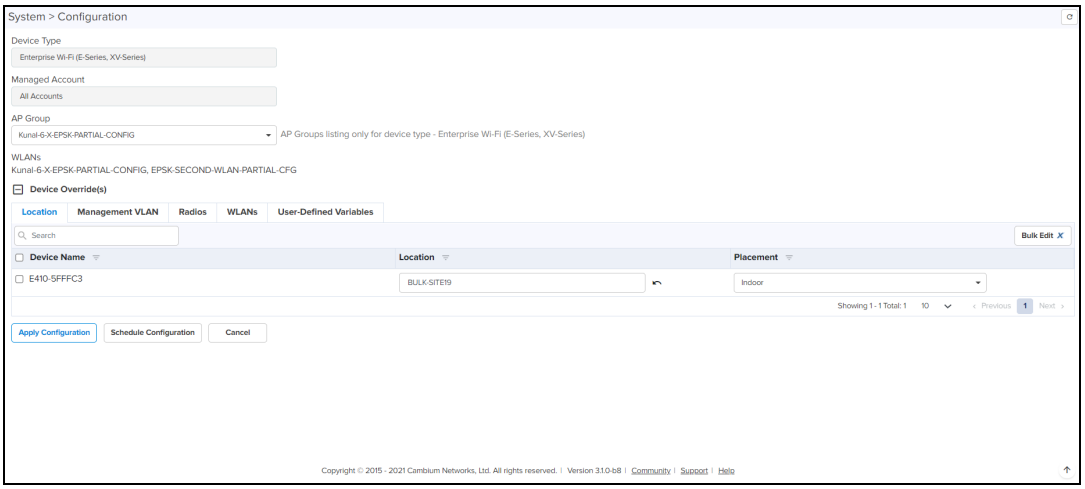


NOTE:

Bulk Edit option under **Configuration** > **Devices Overrides** is supported only for cnMaestro X.

The user can override for the following configurations:

- Location
- Management VLAN
- Radios
- WLANs
- User-Defined Variables

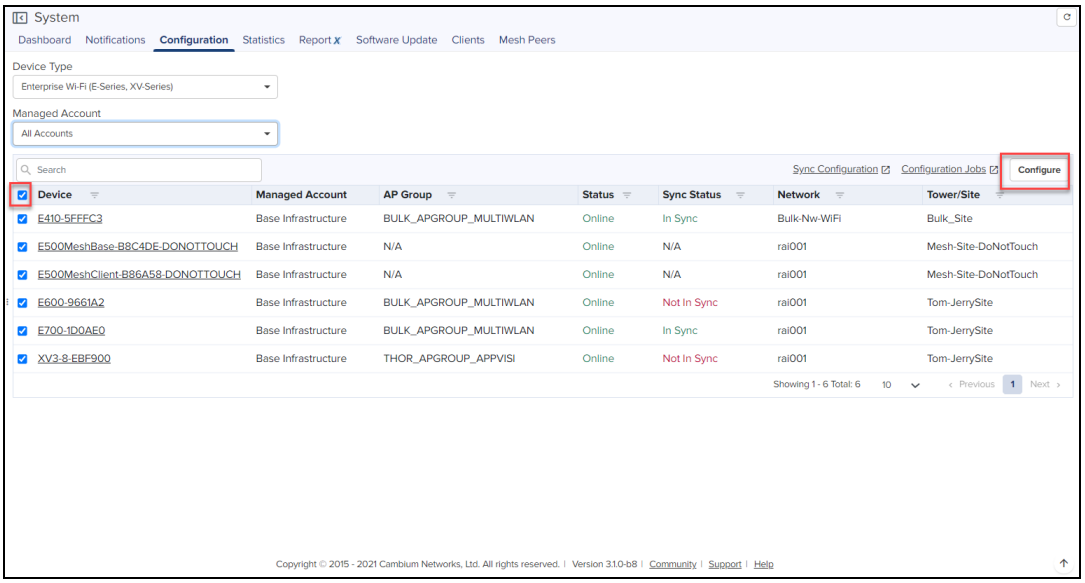


Perform the following steps to configure Bulk Overrides for the devices.

NOTE:

Configuration tab will be available from other container levels like Network/Site and also from AP group level..

1. Navigate to **Manage > System > Configuration.**
2. Select the **Device Type** from the drop-down.
3. Select **Device** from the list and click **Configure**.

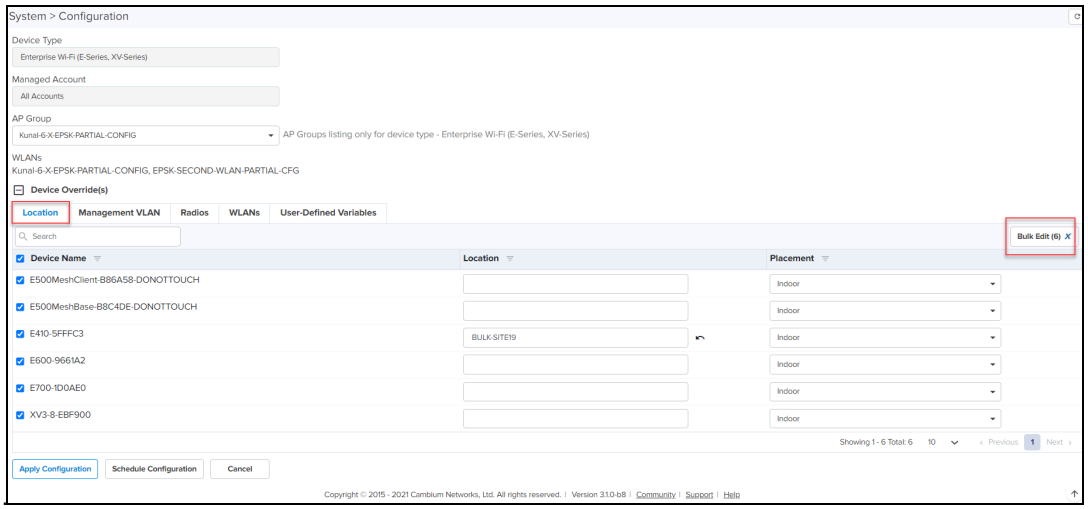


The bulk device configuration is displayed as shown below. Click (+) next to **Device Overide(s)** to view the list of devices.

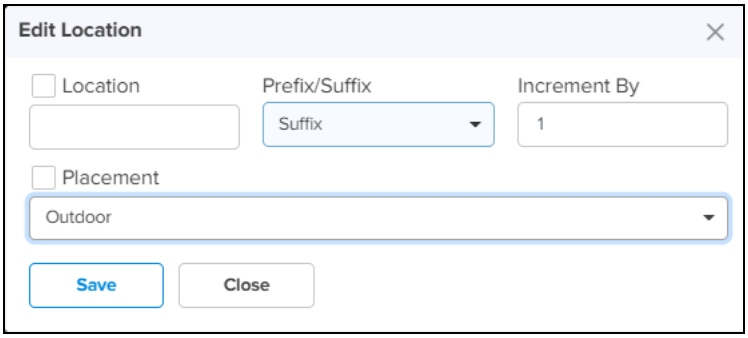


Location

1. In **Location** tab, select the devices from the list.
2. Click **Bulk Edit. Edit Location** window appears.

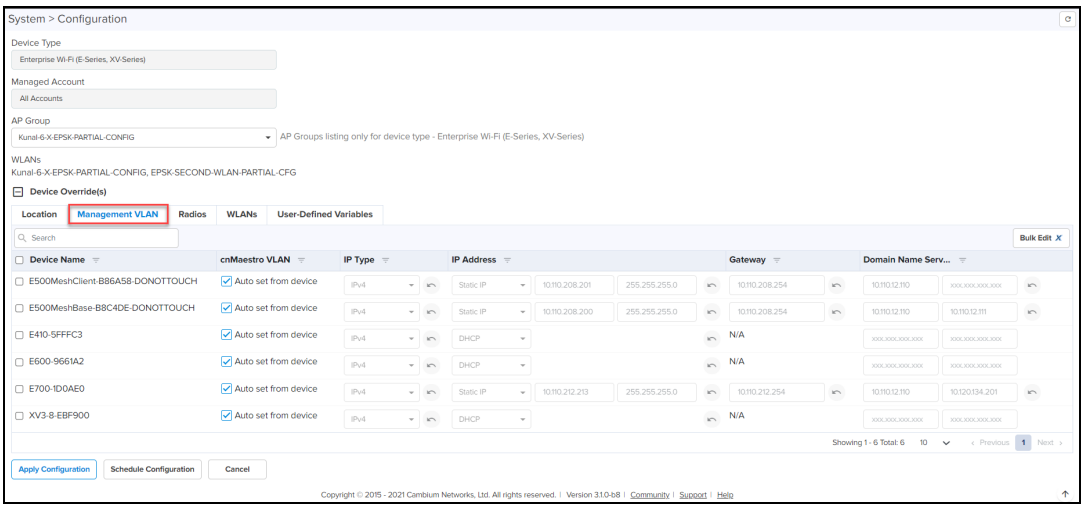


3. Edit the configuration details and click **Save**.

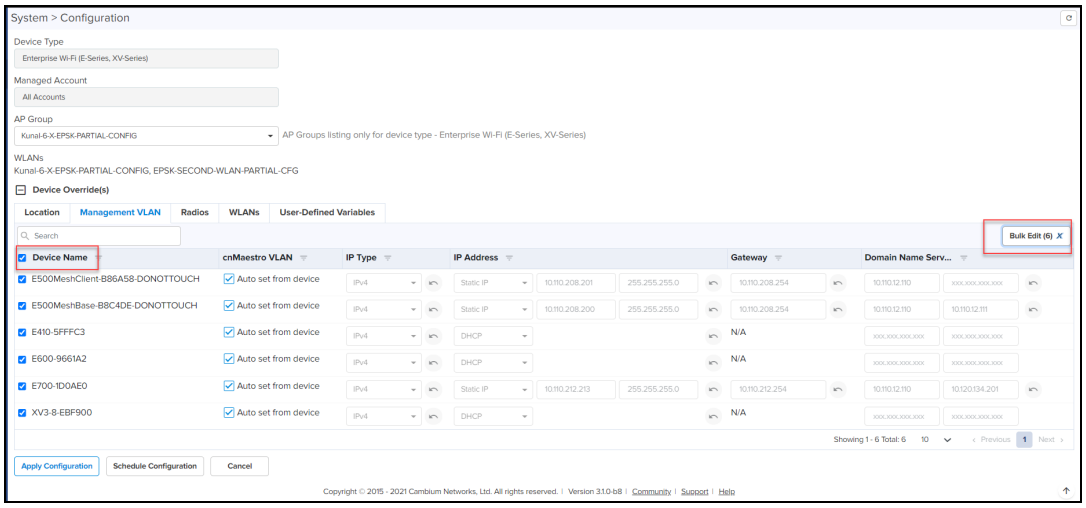


Management VLAN

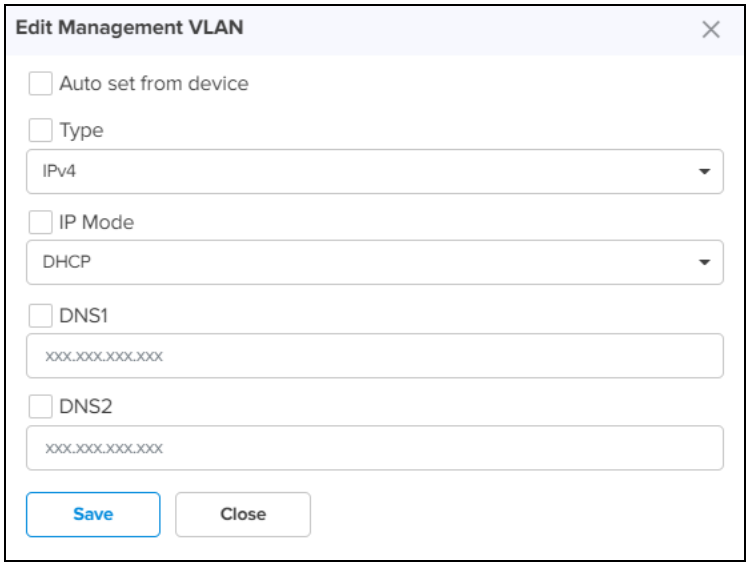
1. In **Management VLAN** tab, select the **VLAN** of the device from the list.



2. Click **Bulk Edit**. **Edit Management VLAN** window appears

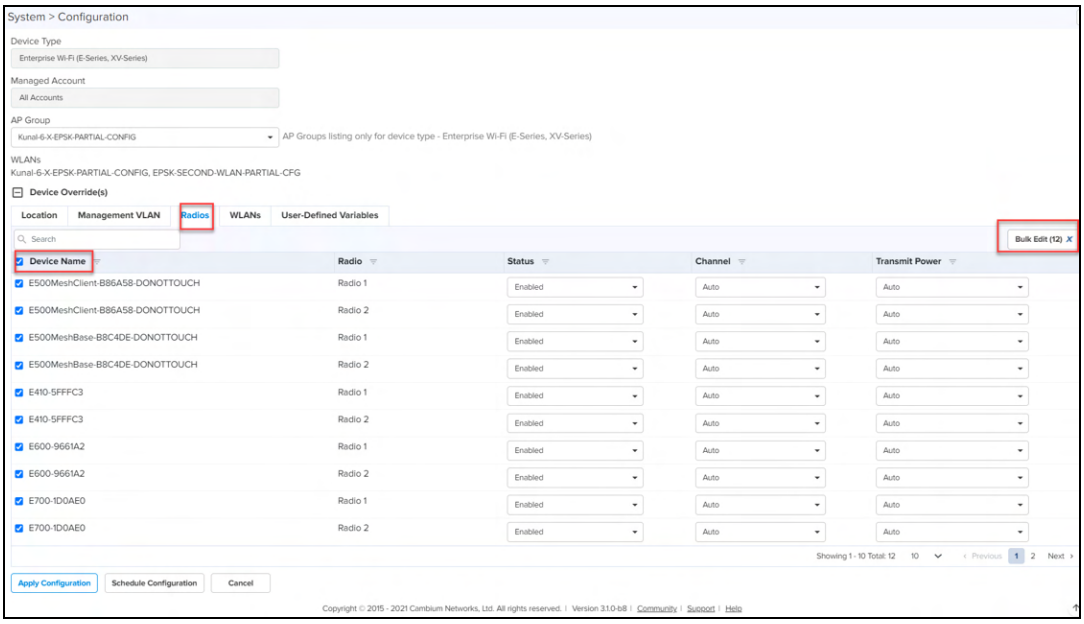


3. Edit the changes and click **Save**.

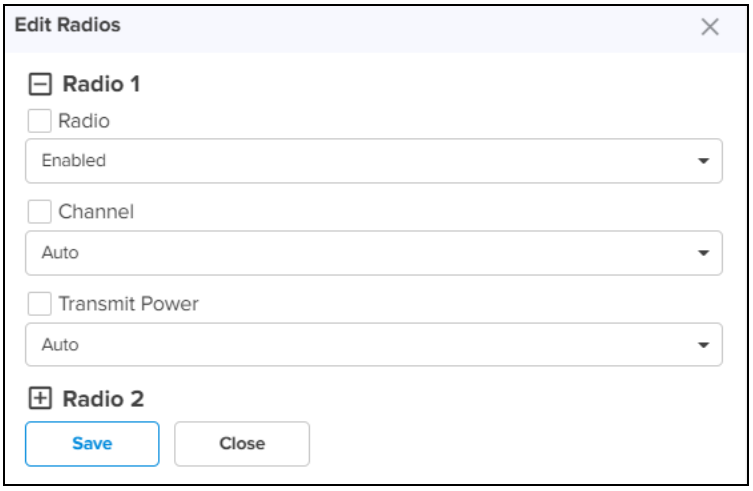


Radios

1. In **Radio** tab, select the radios from the device list.

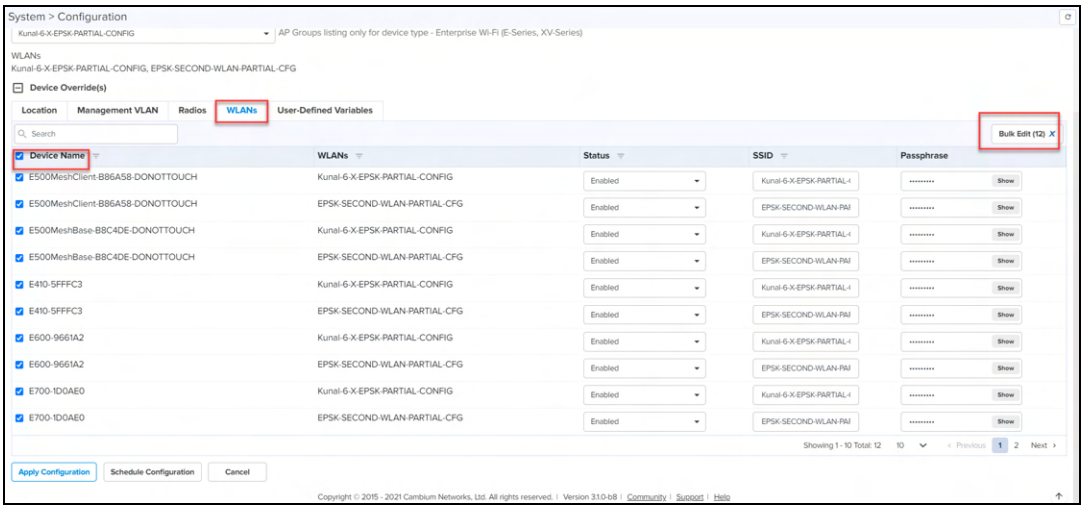


2. Click **Bulk Edit**. **Edit Radios** window appears.
3. Edit the configuration details and click **Save**.

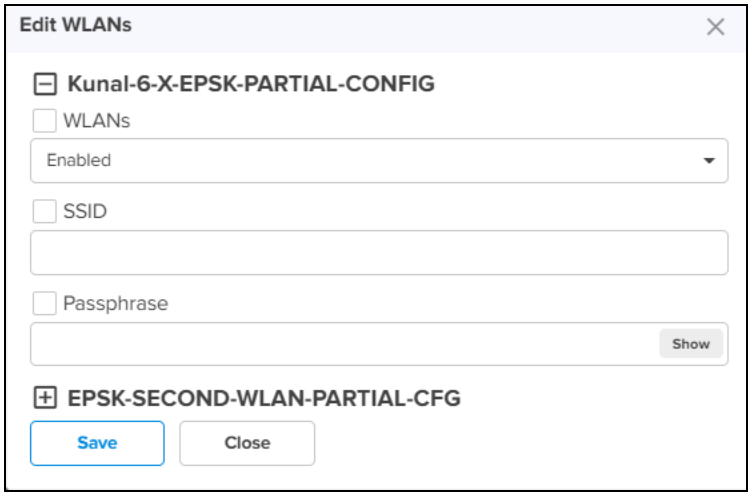


WLANs

1. In **WLANs** tab, select the WLAN of the devices from the list.

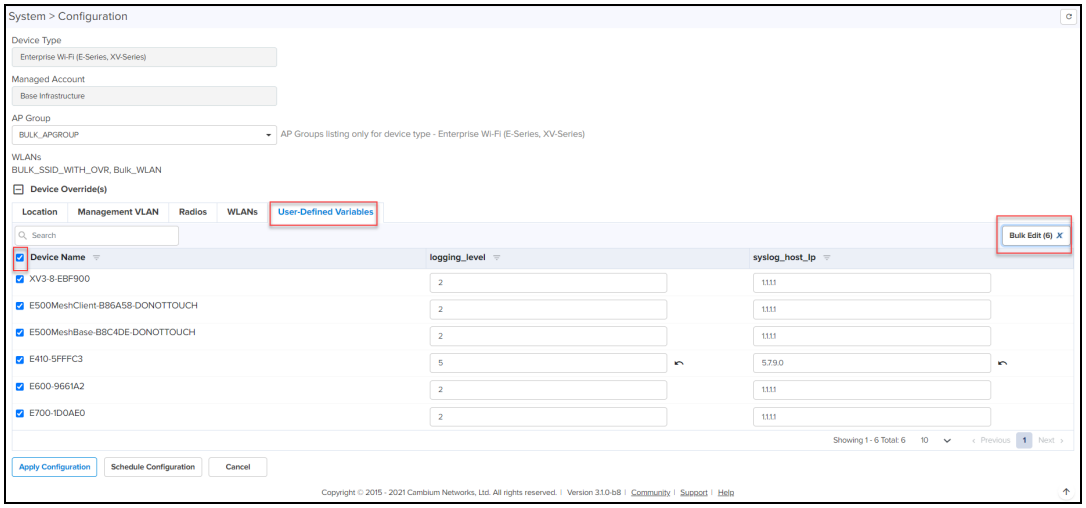


2. Click **Bulk Edit**. **Edit WLANs** window appears.
3. Edit the configuration details and click **Save**.



User-Defined Variables

1. In **User-Defined Variables** tab, select the devices from the list.



2. Click **Bulk Edit**. **Edit User Defined Variables** window appears.



3.Edit the configuration details and click **Save**.

NOTE:

For Bulk overrides to enable in **User Defined Overrides** tab, user has to define overrides in User Defined Overrides section of AP groups. For more details, refer to User-Defined Overrides

3. Click **Apply Configuration** to start immediately or click **Schedule Configuration** to schedule later.

Synchronize (Sync) Configuration

AP Groups can be configured to synchronize automatically or manually when they are updated. The setting is found in the AP Group configuration.

1. **Enterprise Wi-Fi AP Groups** by default synchronize automatically (so any change of AP Group or WLAN, followed by a Save, will immediately push configuration to the devices without manual intervention).
2. **cnPilot Home AP Groups** by default synchronize manually. Updates to them (or the WLANs to which they map) need manual synchronization to push configuration to the devices.

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately. Navigate to **Administration > Sync Configuration**.

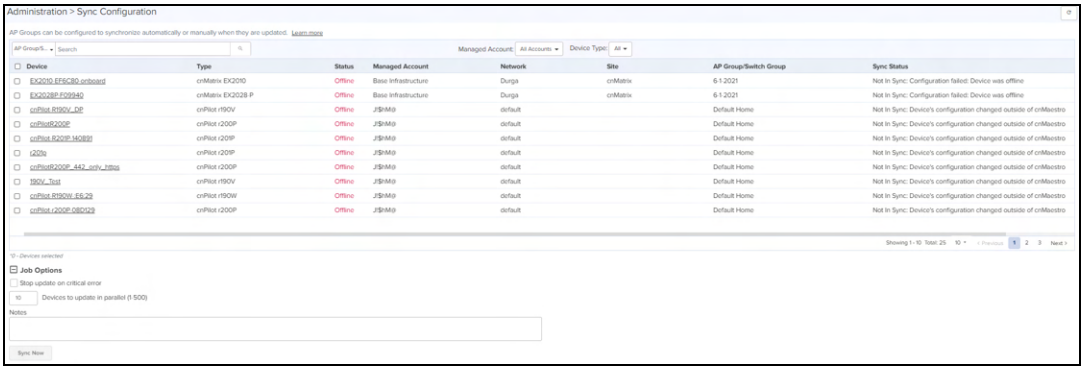
Sync Configuration only displays devices currently out-of-sync with a mapped AP Group .

Sync Configuration has the following fields:

- AP Group (AP Group to which device is mapped)
- Device (Hostname)
- Device Type
- Network (Network in which device is present)
- Status (Up/Down)
- Site (Site under which device is present)
- Sync Status (Sync status will tell whether job is completed or failed)

Steps to do Sync Configuration:

1. Click the **Sync Configuration** in the top right of the **Configuration > WLAN and AP Groups or Manage > Configuration > Device Details or Jobs** tab.
2. Select devices you wish to synchronize.

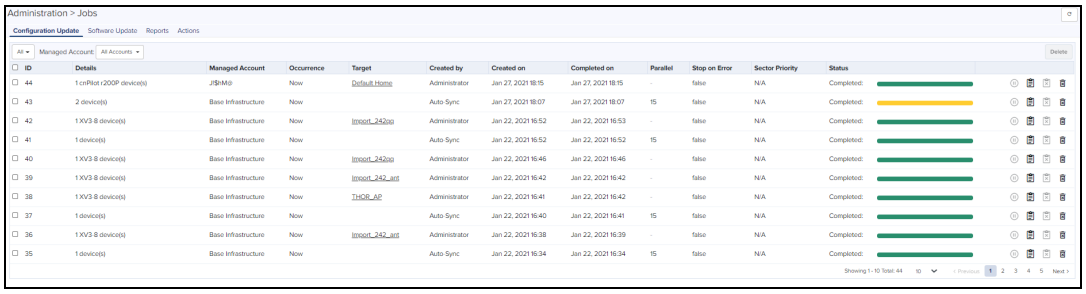


3. Click **Sync Now**.

	NOTE: Sync configuration can only be used if a AP Group is already mapped to the device. Software update jobs can be scheduled in parallel irrespective of other running Jobs as PRO account supports Parallel Jobs also If same devcie is used for config/ software job at a time only one operation will be done as the Job locks the device until it finishes.

Configuration Job Status

After applying configuration, navigate to **Administration > Jobs** to view configuration jobs (for Wireless LAN devices). When configuration is pushed from Sync Configuration, a Configuration job will be created in the background.



NOTE:

1. Configuration jobs will skip devices which are offline. With manual synchronization, they need to be synchronized by the administrator.

   For more information on Wi-Fi AP configuration, refer the following URLs:

   - Unique per-Device values in Profiles Using User-Defined Overrides
   - AP Groups and Overrides for Wi-Fi Devices.
   - Migrating from Templates to Profiles

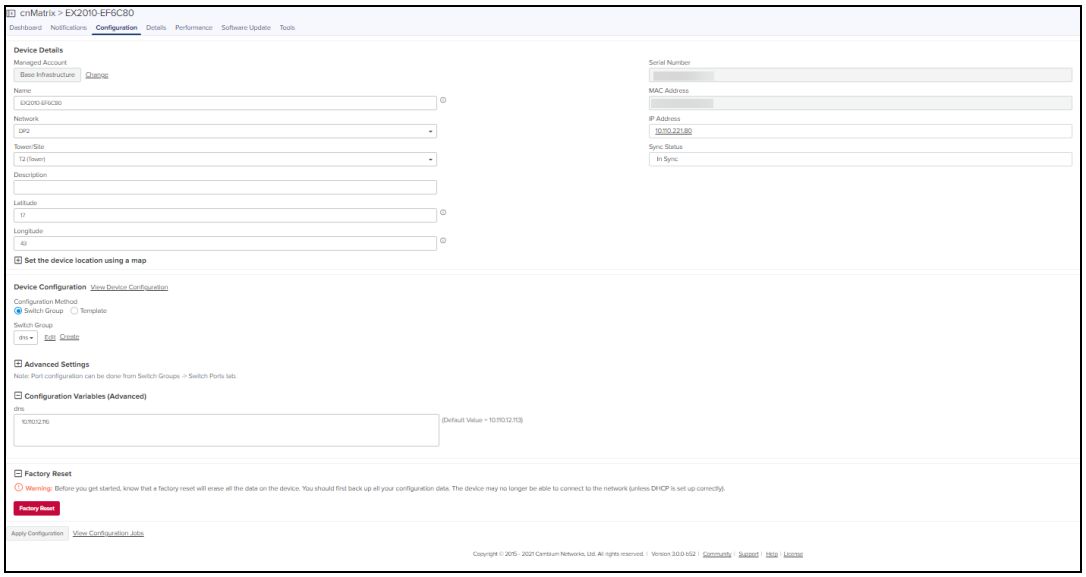
2. cnMaestro X account user can run any number of jobs in parallel.

Factory Reset

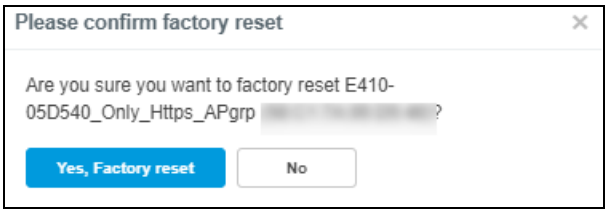
A factory reset erases all the data on the device. Factory reset is supported for two device models, Enterprise Wi-Fi with greater than 3.10-R6 version and cnMatrix with greater than 4.0 version.

To factory reset the device from cnMaestro:

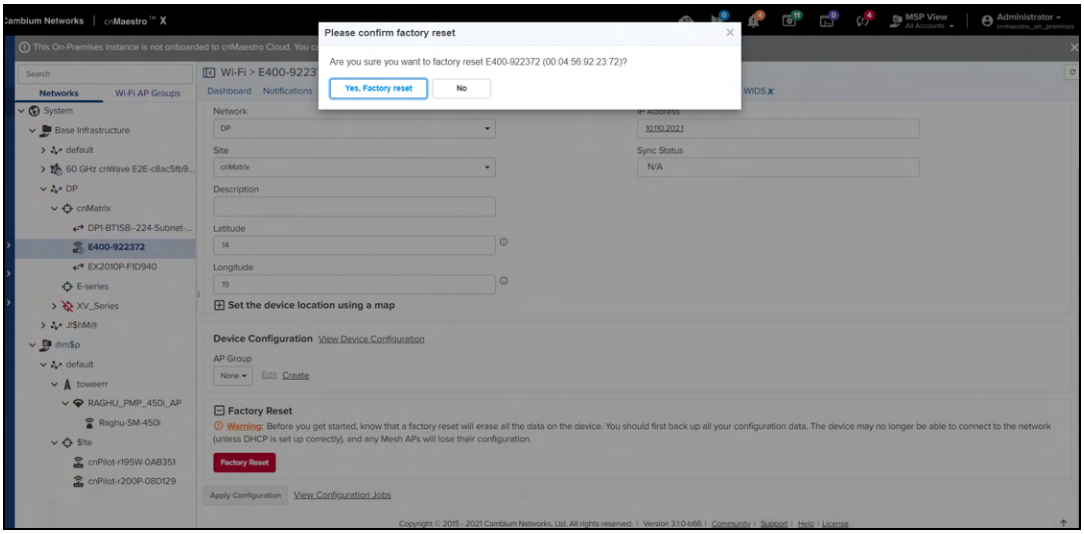
1. Navigate to the **Configuration** tab of the device.
2. Select **Factory Reset.**



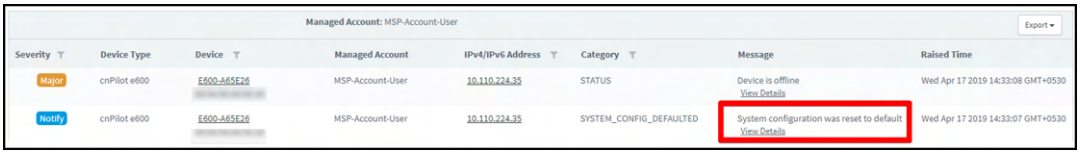
3. Click **Factory Reset**.



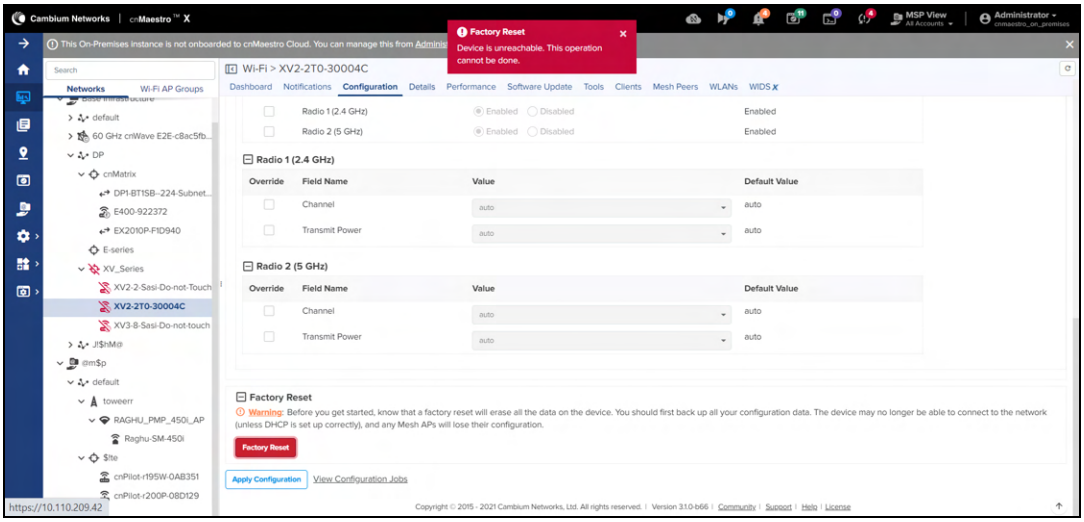
The following window pops-up if you click **Yes, Factory reset** option.



Once the Factory Reset is successful, the following message is displayed in the **Notifications** tab.



If the user does Factory Reset on an offline device it displays error as shown below:



Association ACL

This section describes how cnMaestro replies to AP's request to allow or disallow client associations. This feature allows you to configure MAC association list on the controller.

Overview

When a client requests to get connected to an AP,

1. The AP sends MAC authentication request along with the MAC Address of client and the Customer ID (CID) to the Controller. This is optional and occurs only if MAC ACL is configured for the WLAN on the AP and the policy for the MAC ACL is cnMaestro.

2. Controller checks and responds with an action to allow or deny the request.

3. AP allows or denies the client's request based on the response of the Controller.

Configuring Association ACL

To configure the Access Control List (ACL) in cnMaestro:

1. Navigate to **Shared Settings > Association ACL** page.
2. Click **Add**.



3. Enter the **MAC.**
4. Click the **Allow** check box.
5. Enter the **Description**.
6. Click **Save**.



4. Once the MAC is successfully configured, a pop-up **Association ACL default action is saved successfully** is displayed and lists the configured MAC in **Shared Settings > Association ACL** tab.



5. To configure MAC authentication as cnMaestro:

The Association ACL is shared among all Enterprise WLANs, but it must be explicitly mapped to each Enterprise Wireless LAN that uses it (at **Access Control > MAC Authentication**)



NOTE:

- If MAC is not configured under the policy (to allow/deny), the default action will be applied.
- To **edit/delete** Association ACL, click the respective icons.
- You can import Association ACL, by clicking **Import.csv** and export using the **Export**.

cnMatrix Switches

cnMatrix switches simplify the network deployment and operation. cnMaestro provides management, configuration and control, and security services for cnMatrix with deployment options such as policy-based automation (PBA) to streamline core operations and improve network security. Central to cnMaestro's orchestration of cnMatrix devices is the concept of Switch Groups.

Switch Groups Configuration

A Switch Group can also be considered a Virtual Stack. The Switch Group functionality enables the users to manage multiple switches with the same configurations.

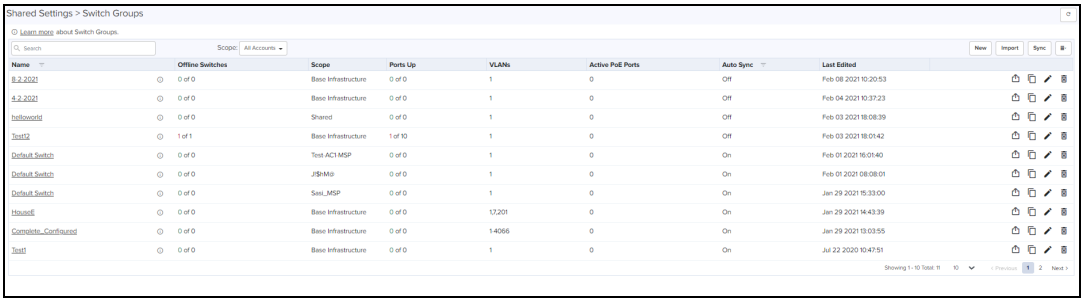
Configuration is common to all switches belonging to a Switch Group:

- Configuration changes are synchronized and applied for all the switches in a Switch Group.
- A subset of configuration attributes can be overruled for an individual switch.
- Switch ports across all physical switches are associated with a Switch Group and can be simultaneously bulk edited.

From the Switch Groups tab, the administrator can navigate to the Switches and the Switch Ports tabs for configuration. The Dashboard tab is used to monitor the health condition of the virtual stack.

The process for creating a new Switch Group configuration is as follows:

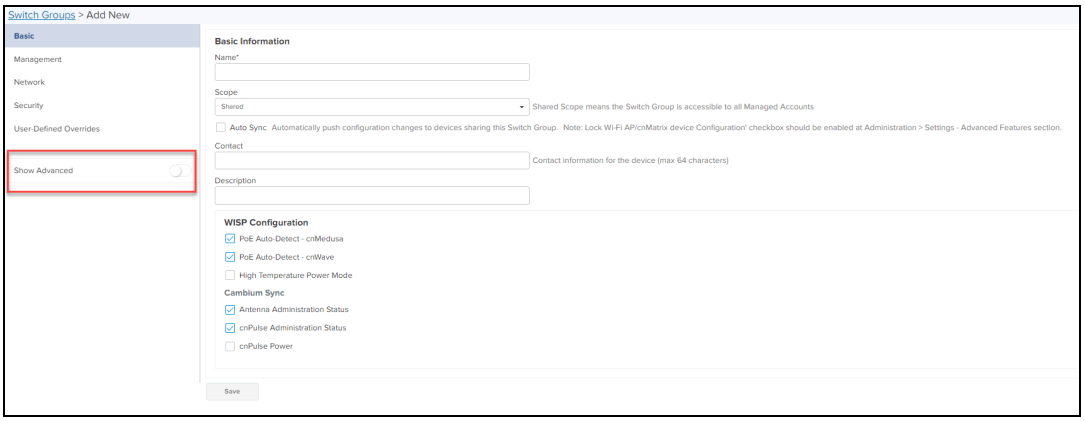
1. Navigate to **Shared Settings > Switch Groups.**
2. Click **New Switch Group**.



NOTE:

To Edit the Configuration of existing Switch group, click **Edit** icon > navigates to **Configuration** page.

3. Configure the following tab parameters to create a Switch groups:
   - Basic
   - Management
   - Network
   - Security
   - User-Defined Overrides



NOTE:

- Click **Show Advanced** to view the advanced options of the Switch Groups.
- Click **Save** on individual tab parameters or click once after entering all the four tab parameters.

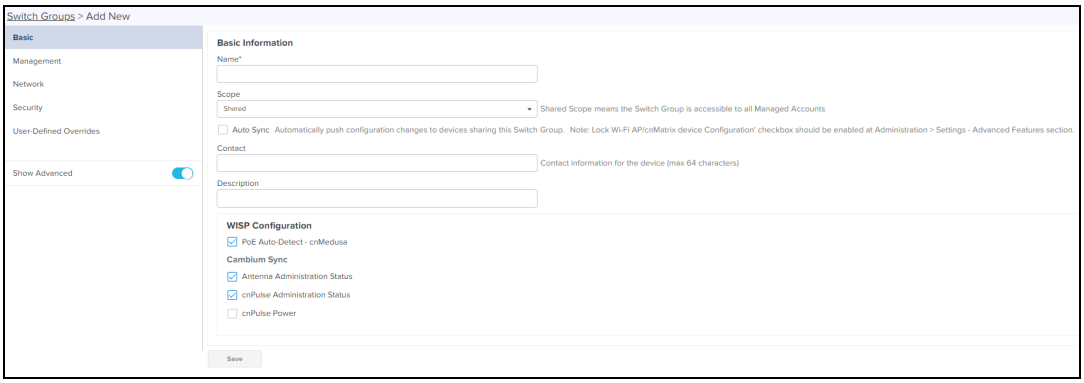
Basic

The Basic tab provides options to the user to configure the device name as well as other standard values used to identify a switch.

1. Navigate to **Configuration > Switch Groups > Basic.**
2. On the **Basic** page enter device identification data such as:
   - Name
   - Scope
   - Contact
   - Description
   - WISP Configuration

Note:

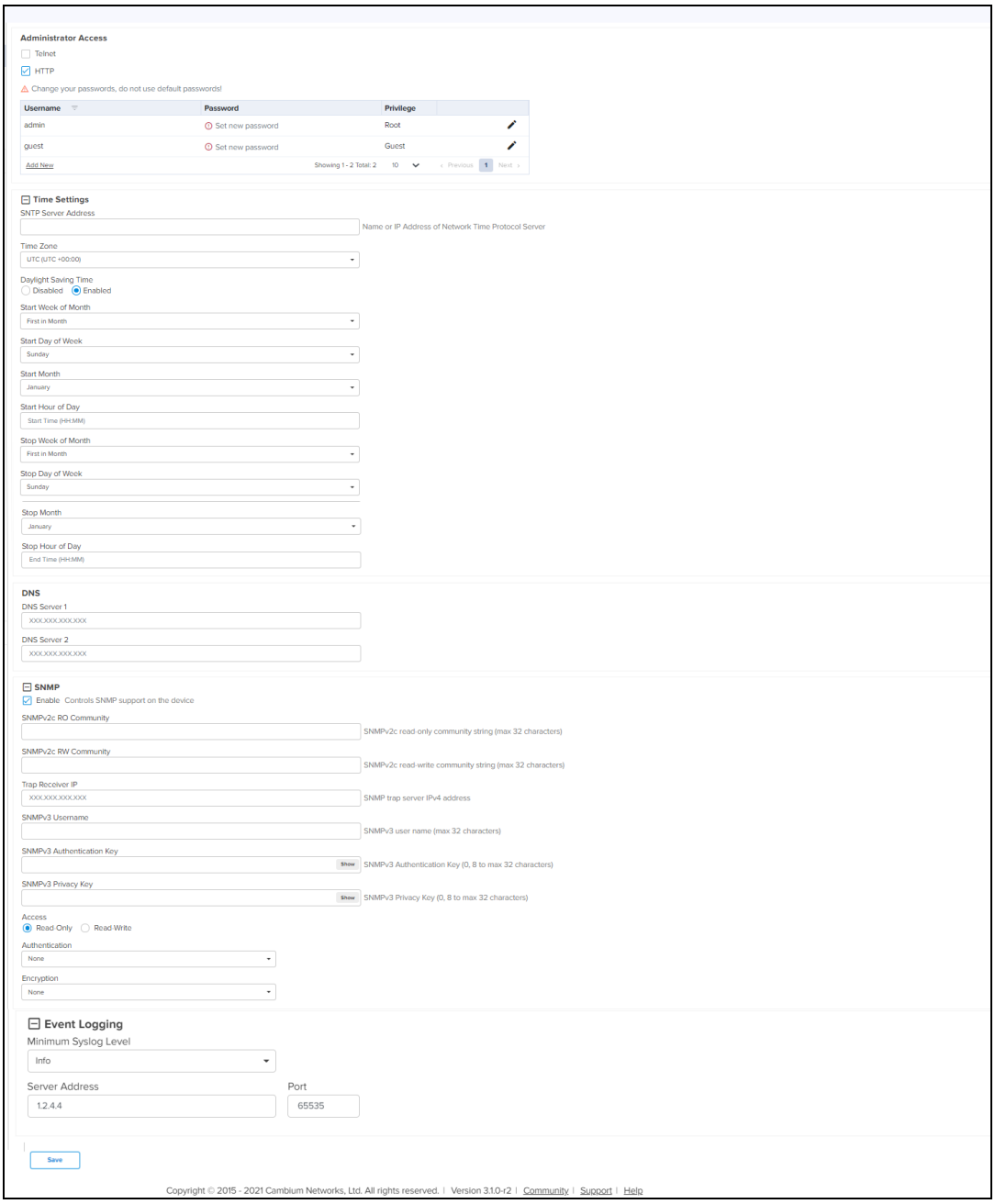
The special characters can be used to create names of Switch Groups (Eg: a-zA-Z_-*&%#@!<>.() []^~`$1234567890).



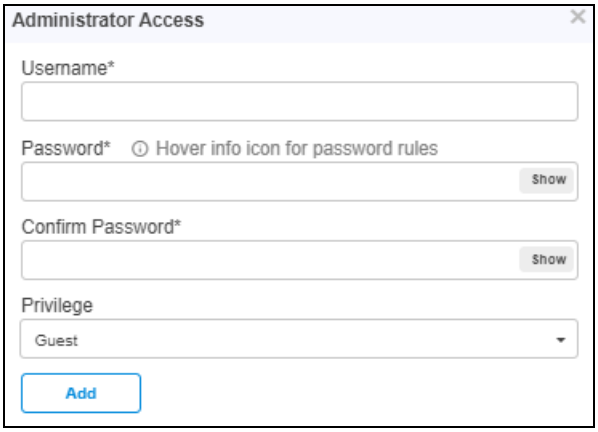
3. Click **Save**.

Management

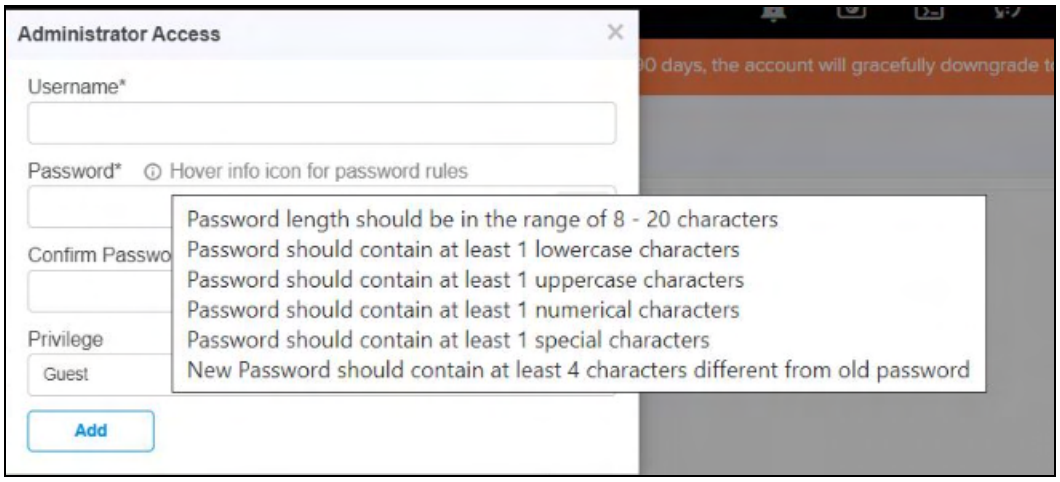
1. Navigate to **Management** page.
2. Enable the **Daylight Saving Time** and enter the details.



3. Click **Add New** to add **Administrator Access**, enter the details and click **Add.**



4. Password should match the special characters as shown below:

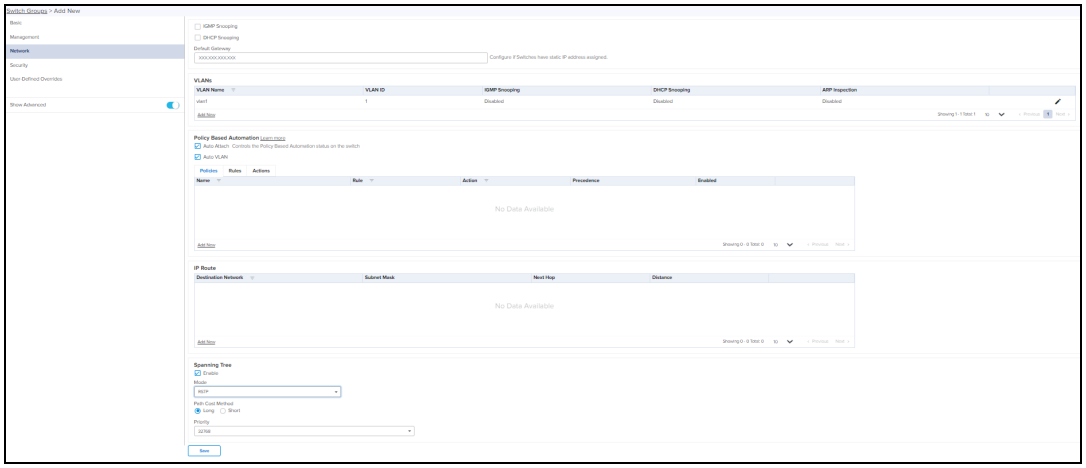


5. Click **Save.**

Network

The **Network** page allows the user to configure VLANs, PBA, IP Route, and Spanning Tree details.

1. Navigate to **Network,** enter the details of VLANs, Policy Based Automation, IP route, and Spanning Tree.

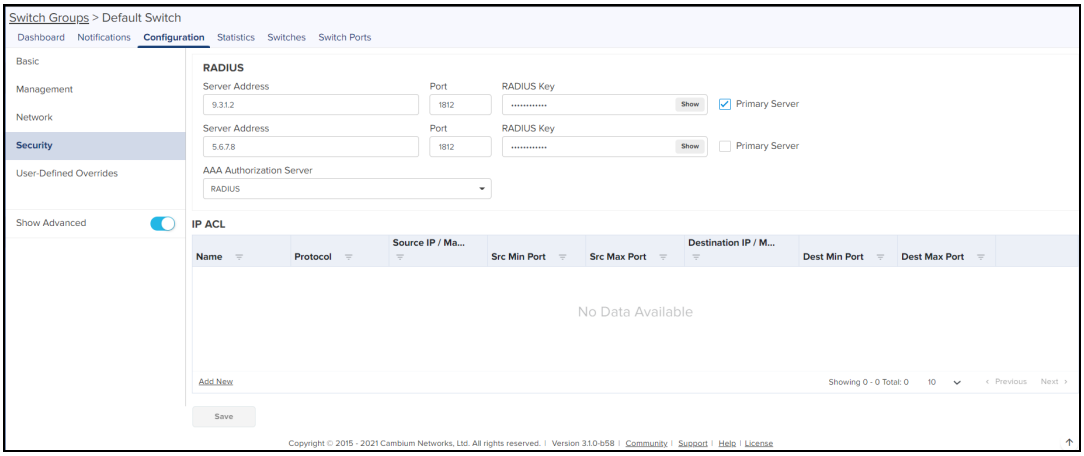


2. Click **Save.**

Security

The Security page allows the user to configure RADIUS and Access Control List (ACL) details.

1. Navigate to **Security** page and enter the details of **RADIUS** and **ACL IP**.

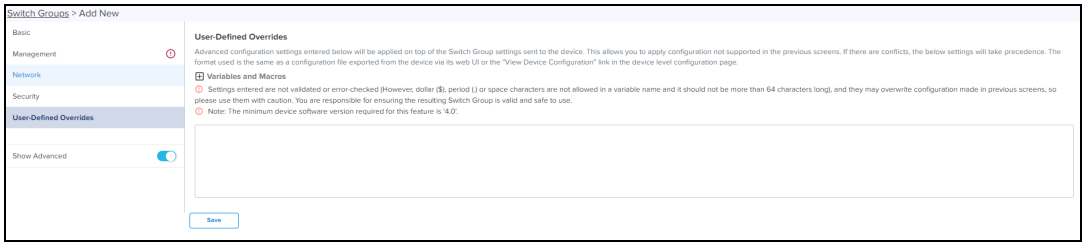


2. Click **Save**.

User-Defined Overrides

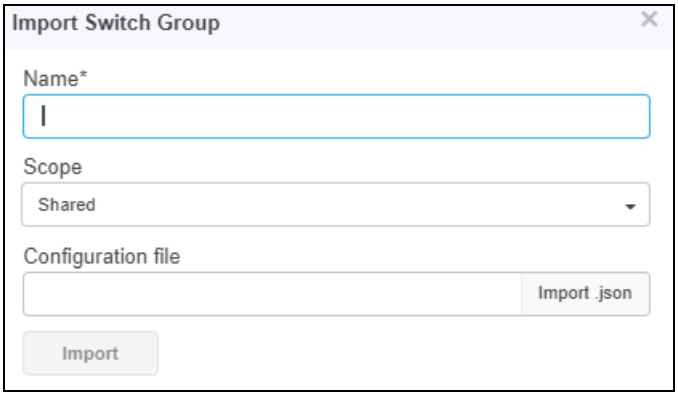
> **NOTE:**
>
> The minimum device software version required for this feature is 4.0.

User-Defined Overrides allows you to apply configuration in cnMatrix switches. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.



Import Switch Group

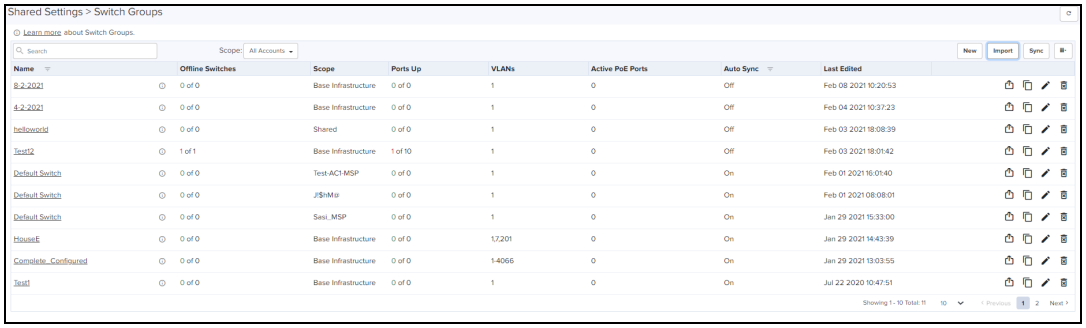
1. Click **Import Switch Group**. A dialogue box appears.
2. Select **import.json** and import the file.



3. When you click **Download Sample File**, you can see Sample excel sheet.
4. Click **Import**

Delete Switch Group

To delete Switch Group from the list click **Delete** icon of the specific device row.



Retry Configure

When the user tries to apply any Switch Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as " Device was offline", in the Jobs page. In this case, when device comes Up and connects to cnMaestro, then cnMaestro will create an Auto-sync job for that device and pushes the Switch Group. (It will not apply the Switch Group if the "Auto-Sync" was disabled in the Switch Group).

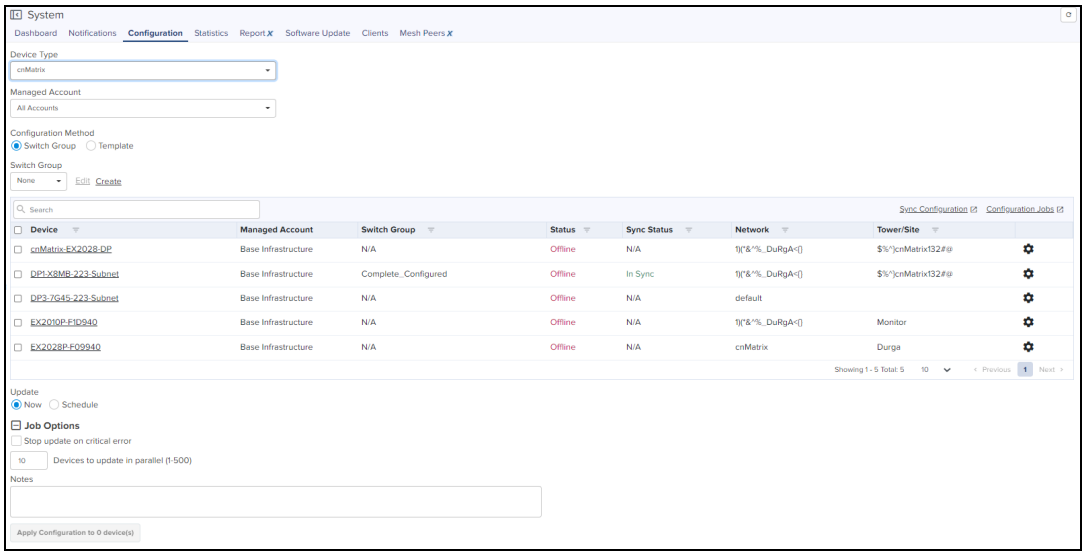
NOTE:

The config update (auto-sync) will happen only when the "Auto-Sync" option was enabled in the Switch Groups page. If the device was skipped/failed because of any other reason other than the "Device was offline", then the device will not be updated.

Create a Configuration Job

Configuration job can be created from **System/Network/Tower/Site/Device Configuration** page. Select a device type and a set of devices along with Switch Groups to which they will be mapped. This can be done in three steps:

1. Select the Switch Group that needs to be pushed from drop-down.
2. Select the list of Switch Group **Device**.
3. Select update **Now/Schedule**.
4. Click **Apply Configuration.**



Synchronize (Sync) Configuration

Switch Groups can be configured to synchronize automatically or manually when they are updated. The setting is found in the Switch Group configuration.

Switches by default synchronize automatically (so any change of Switch Group, followed by a Save, will immediately push configuration to the devices without manual intervention).

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately. The page is located at **Administration > SyncConfiguration**.

Sync Configuration has the following fields:

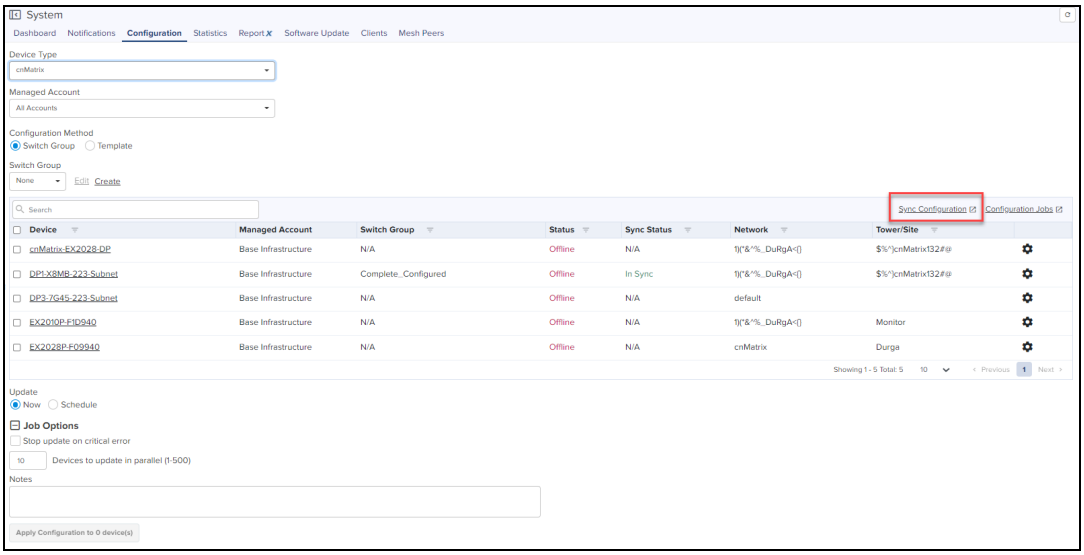
- Device (Hostname)
- Type

- Status (Online/Offline)
- Network (Network in which device is present)
- Site (Site under which device is present)
- AP Group/Switch Group (AP Group/Switch Group to which device is mapped)
- Sync Status (Sync status will tell whether job is completed or failed)

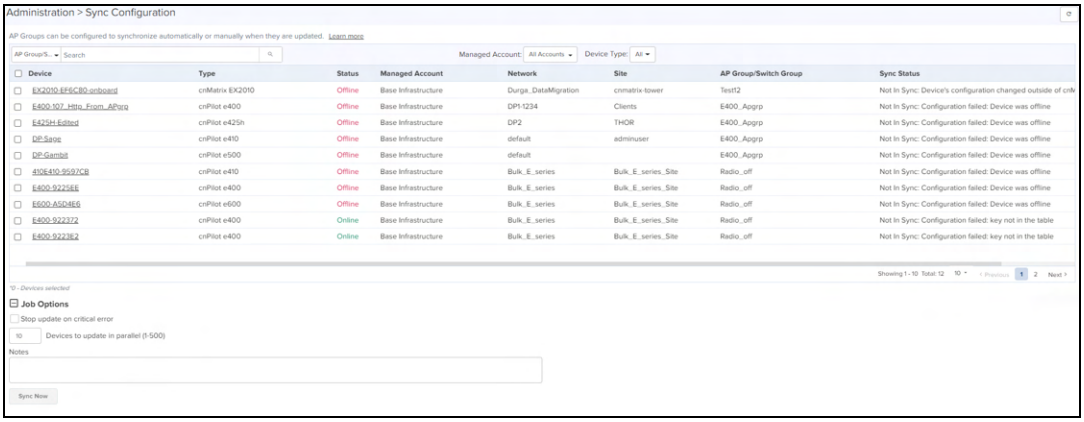
Steps to do Sync Configuration:

Navigate to **Manage > Network > Configuration > Device Details or Jobs** tab.

1. Select devices to synchronize and click the **Sync Configuration**.



2. Automatically it navigates to **Administration > Sync Configuration** and select devices to synchronize.



3. Click **Sync Now**.

	NOTE: Sync configuration can only be used if a Switch Group is already mapped to the device.

Policy Based Automation(PBA)

Cambium Networks PBA functionality fully automates certain commonly performed operations, improving network security while eliminating potential configuration errors. It allows the user to automatically configure switch port settings based on the device currently connected to the port. These dynamic PBA settings remain in-use for the duration of the device connection and are automatically cleared when the device disconnects from the switch.

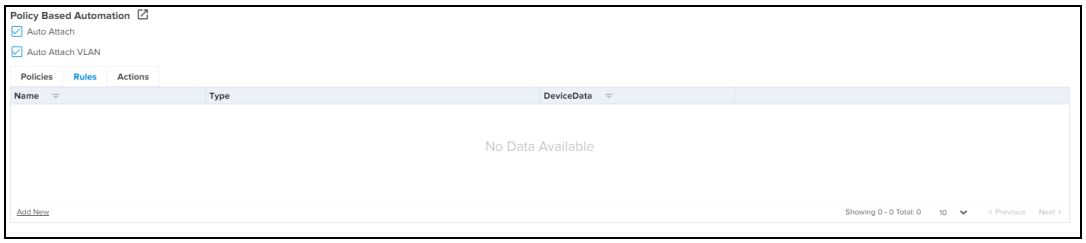
PBA configuration is common to all switches within a switch group.

NOTE:

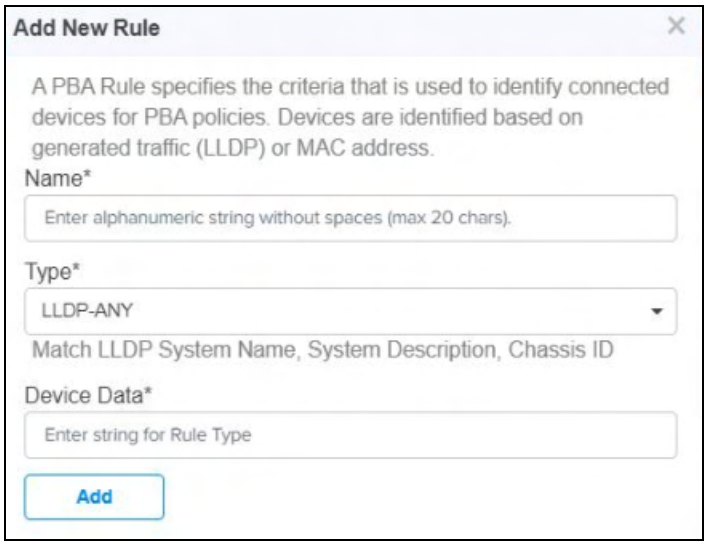
Dynamic PBA updates are indicated by asterisk * on the Switch Dashboard and on the Switch Ports pages.

Configure the PBA as follows:

1. Navigate to **Switch Groups > Configuration > Network > Policy Based Automation.**
2. Navigate to **Rules tab.**



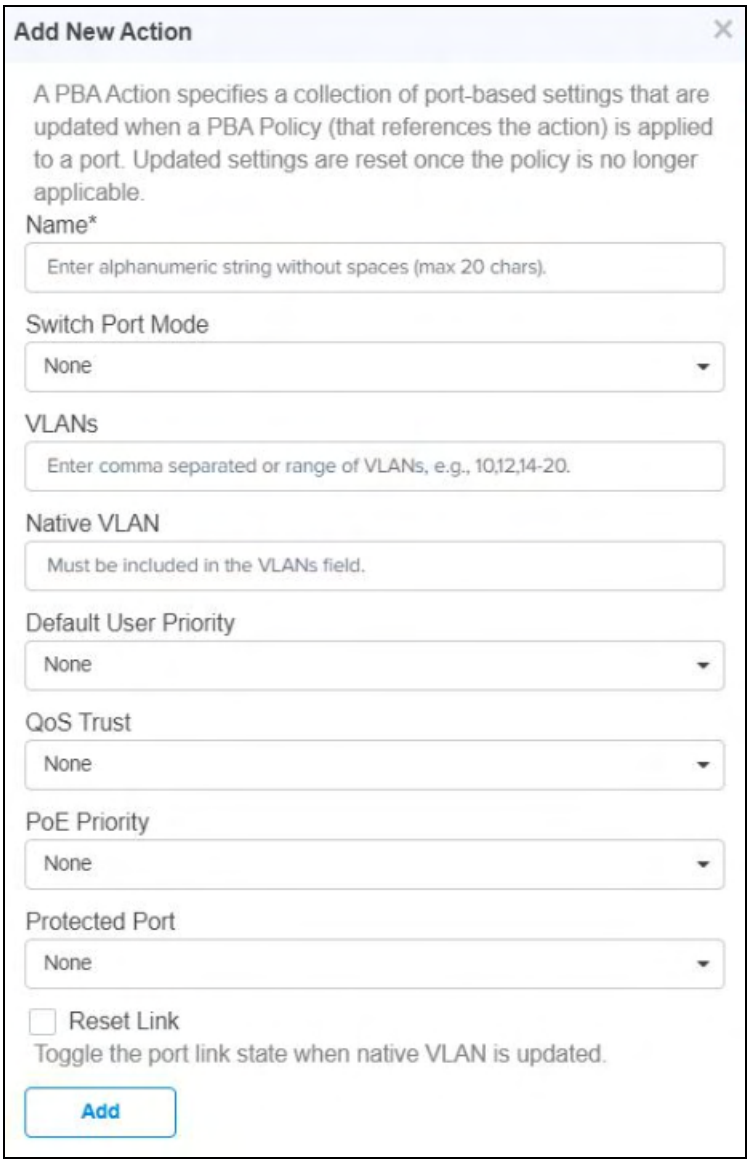
3. Click **Add New** to set the rules.



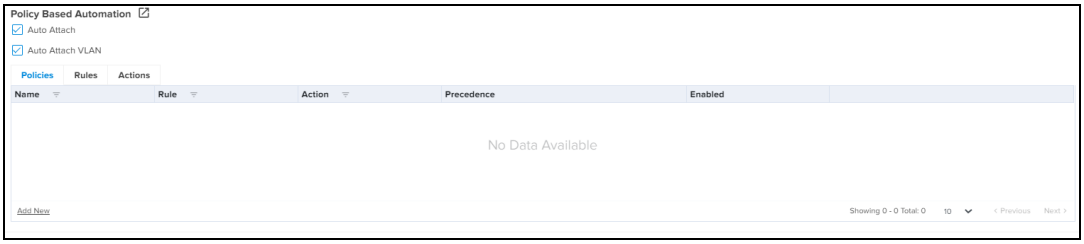
4. Click **Add.**
5. Navigate to **Actions** tab.



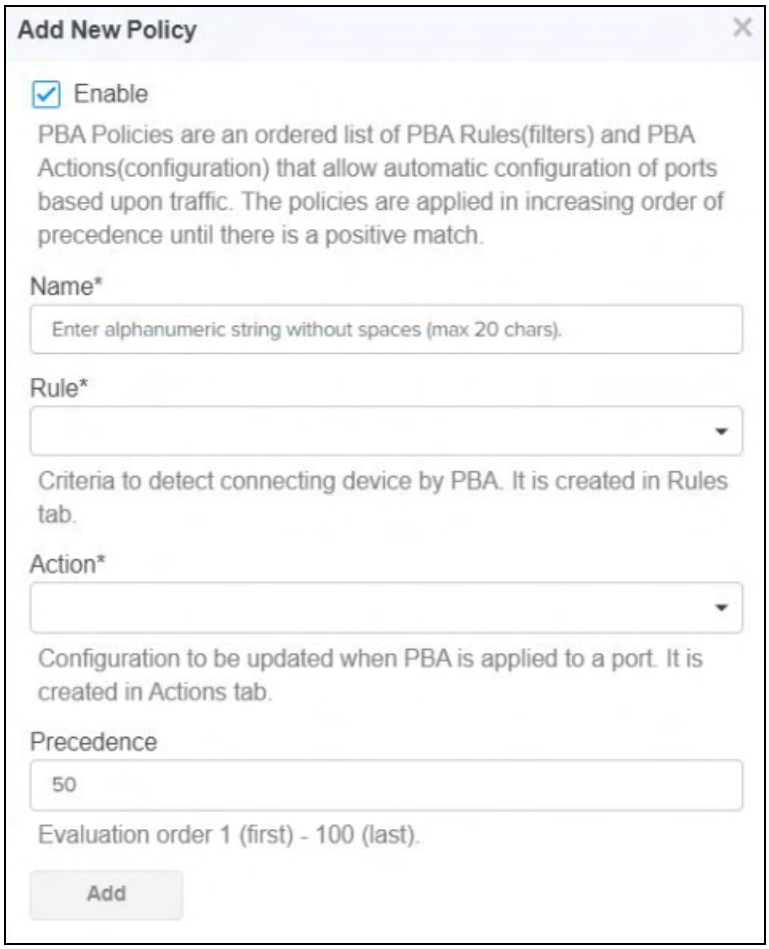
6. Click **Add New** to set the actions.



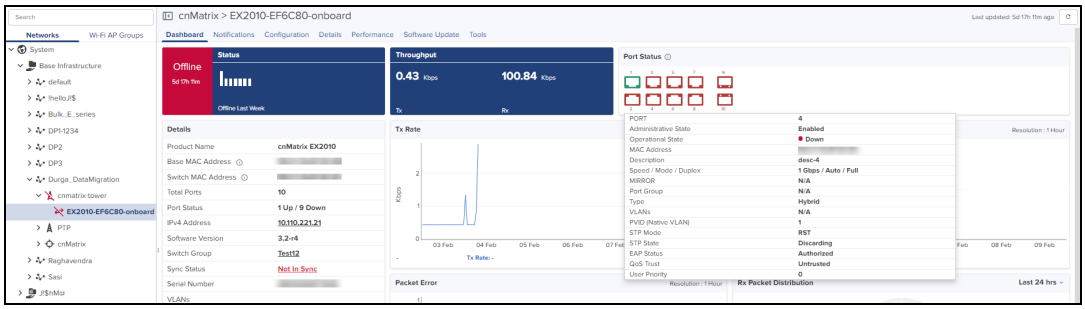
7. Click **Add**.
8. Navigate to **Policies.**



9. Click **Add New** to set the policies.



10. The VLANs Action which is set with the Device Data rules and policies is displayed in the System Dashboard Port Status under each port.



Switches

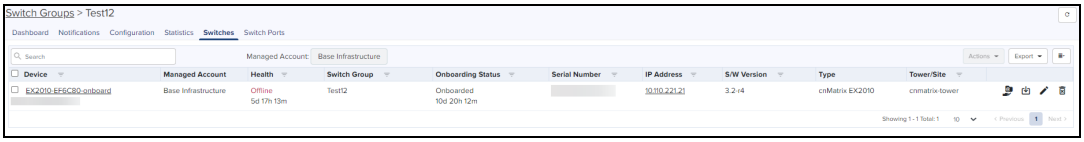
The Switches page is accessed by selecting the **Switch Groups > Switches** tab lists all of the physical switches assigned to the Switch Group. The switch dashboard and switch override configurations settings are accessible through this page.

Switch overrides allow certain attributes for each switch to be configured individually.

	NOTE: For configuration, a switch must belong to a Switch Group.

Configure the Switch Group as follows:

- Navigate to **Switch Groups >** select the switch from the list and click **Switches** page to view and edit the onboarded switches.

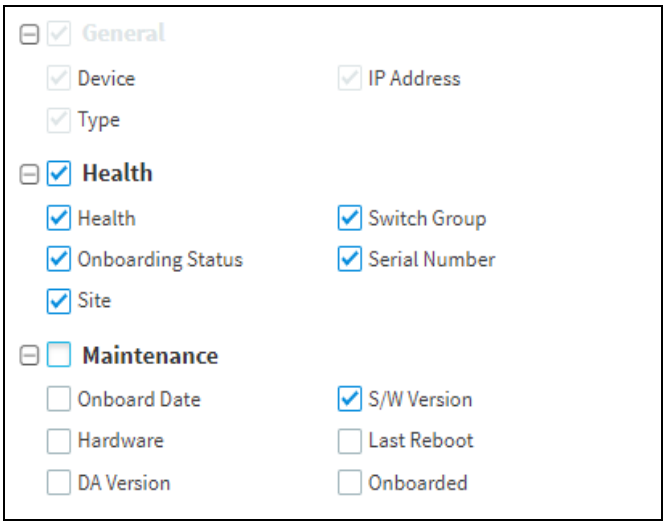


The Switches details view displays following fields by default:

- Device, Health, Onboarding Status, Serial Number, IP Address, Switch Group, Type, Site and Action tab.

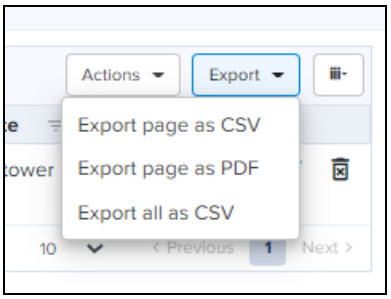
Action column can be used to edit or delete any device of the Switches.

User can click on top bar to include additional fields in Switches Detail view.



Export Switches

1. Click **Export**. A dialogue box appears.

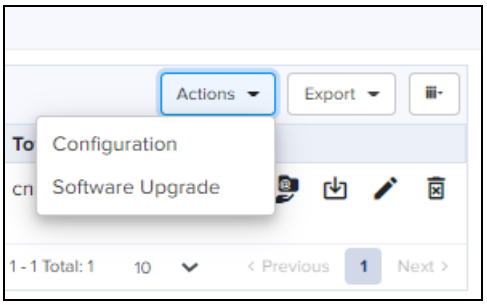


2. Select **Export page as CSV/PDF/all as CSV** and export the file.

Action

Action column can be used to edit or delete any device of the Switches.

1. Click **Action**. A dialogue box appears.



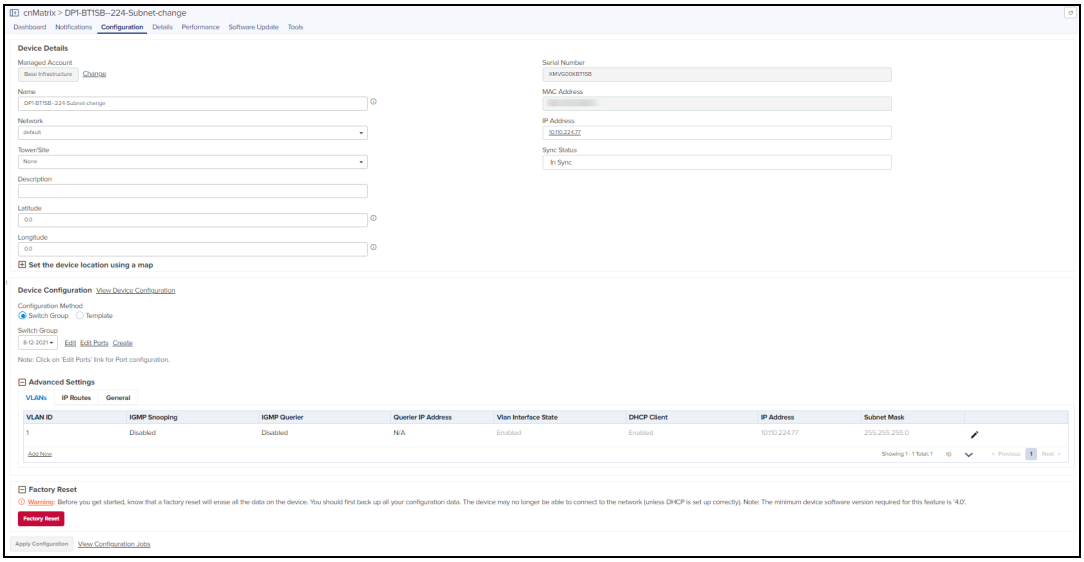
2. Select **Configuration** to edit the device details or click Edit icon
3. Select **Software Upgrade** to update the device software or click
4. Click to delete the selected device from the list.

Switch Configuration

To edit or configure the switches, click the **Edit** or **Configuration** from the **Action** drop-down.

Navigates to the Device **Configuration** page.

1. Enter the **Device Details, Set the service location** and **Device Configuration.**



2. Click **Apply Configuration**.

Device Configuration

Device Configuration allows the customer to configure the Configuration Method as Switch Group.

Switch Group Configuration Method

Enable the **Switch Group** and select a device from the **Switch Group** drop-down.



To Edit or Create a Switch Group, refer to the Switch Groups Configuration.

Navigate to the **Advanced Settings** and configure the following parameters:

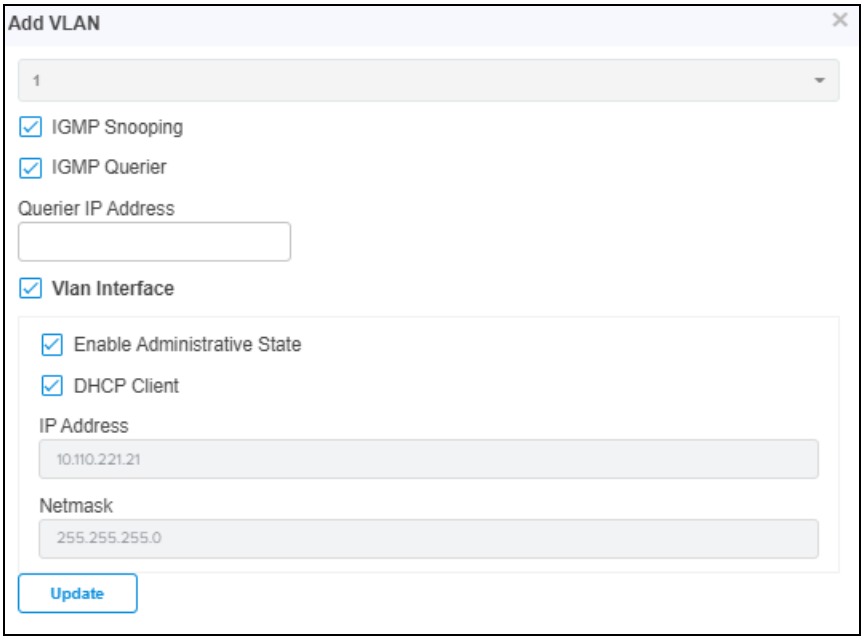
Vlan Interface

VLAN Interface allows the user to edit/Add the VLAN details such as **Vlan ID, IGMP Snooping, IGMP Querier, Querier IP Address, DHCP Client, IP Address**, and **Subnet Mask.**

1. Click **Advanced Settings** in **Configuration** page and navigate to**Vlan Interface** tab.



2. Click Edit Icon or Add New.
3. Enter the required details and click **Add**

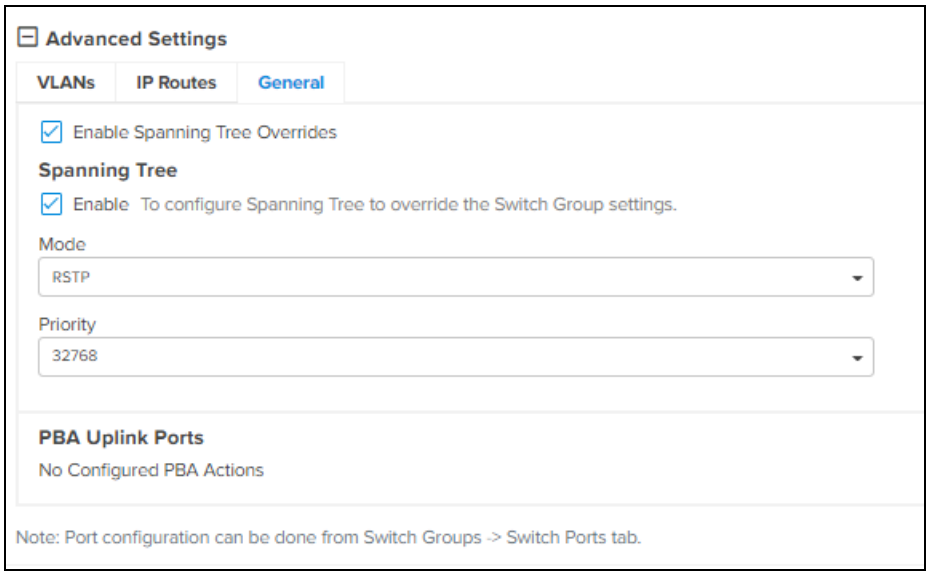


General

Certain configurations are different for each Switch, and these are highlighted within cnMaestro as overrides.

Configure the Overrides as follows:

1. Click **Advanced Settings** in **Configuration** page and navigate to **General** tab.
2. Click **Enable Spanning Tree Overrides.**
3. Select the **Spanning Tree** parameters.



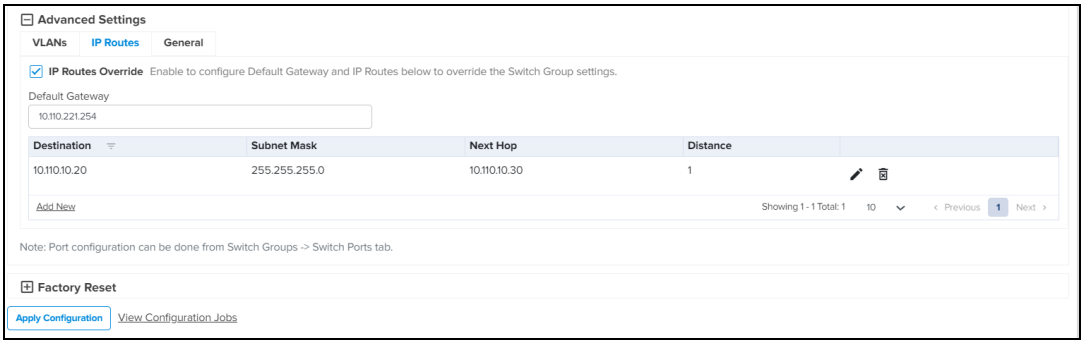
NOTE:

If Spanning Tree is disabled the overrides feature will be disabled on the Switch configuration.

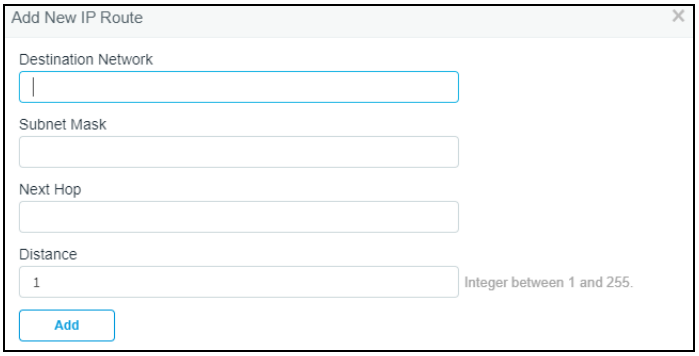
IP Routes

IP Routes allows the user to configure the Default Gateway and IP Routes to override the Switch Group.

- Configure the IP Route as follows:
- Enable the **IP Routes Override** and enter the **Default Gateway.**



1. Click **Add New**.
2. Enter the parameters such as Destination Network, Subnet Mask, Next Hop, and Distance.
3. Click **Add.**



Default gateway IP will override the all IP's of the Switch Groups.

Switch Ports

Switch Ports tab displays the list of the Ports and the port channel assigned to the specific switch.

The Switch Ports tab allows the administrators to configure the port settings by port ID for all ports within the switch group. By default, a port ID identifies the switch (by switch name) and port number, example., EX2028P-EC9541: 1.

It supports bulk editing of switch port settings across all physical switches.

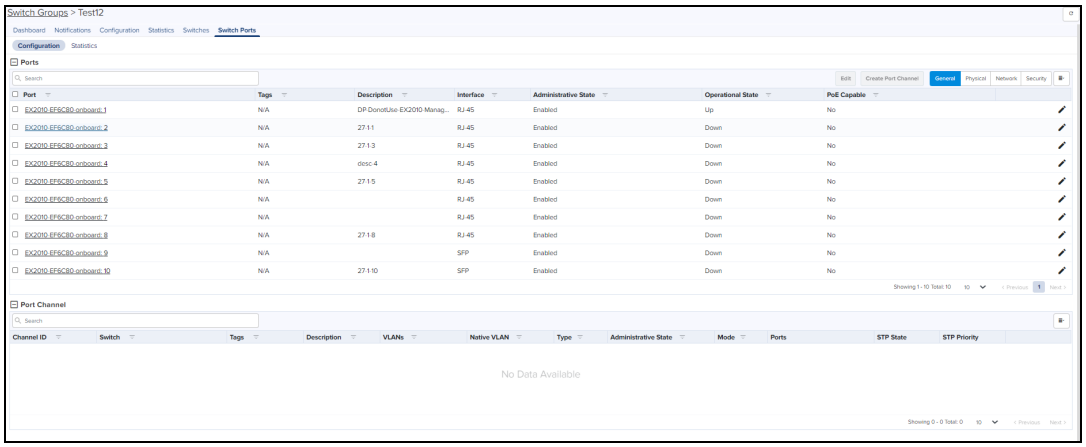
To view the Switch Ports, navigate to **Shared Settings > Switch Groups > Switch Ports**.

Ports

cnMaestro **Switch Ports Configuration** tab allows the user to configure the following parameters:

- General
- Physical
- Network
- Security

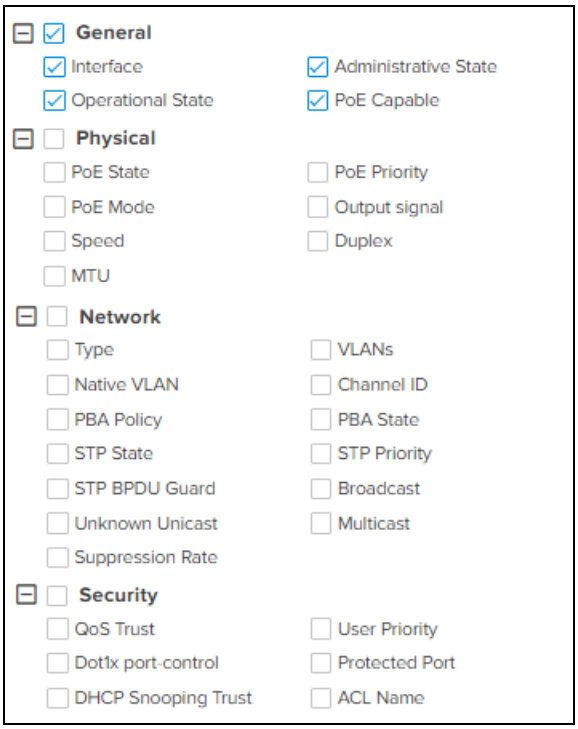
General Tab



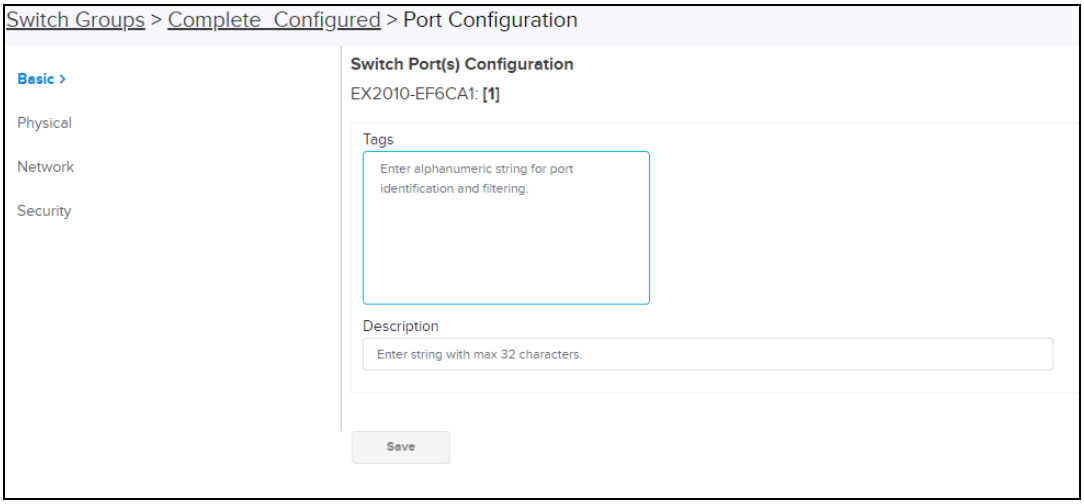
The **Ports General** details view displays following fields by default:

- Port, Tags, Description, Interface, Administrative State, Operational State, PoE Capable, and Edit.

User can click on top bar to include additional fields in **Ports** General Detail view.



1. Click Edit icon or Port device in the list to edit the **Ports Configuration** General tab details.
2. Navigates to **Switch Groups > Switches > Port Configuration.**

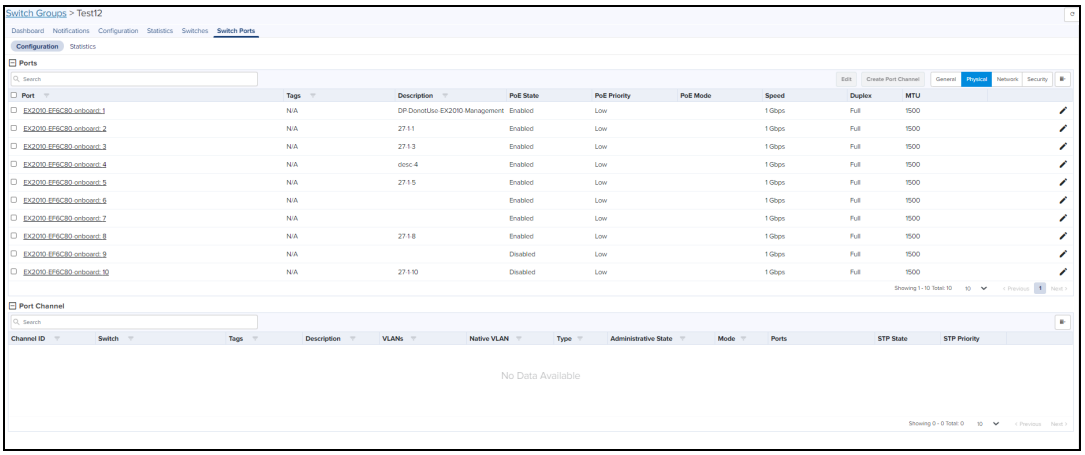


3. Enter the **Tags** and **Description** details.
4. Click **Save**.

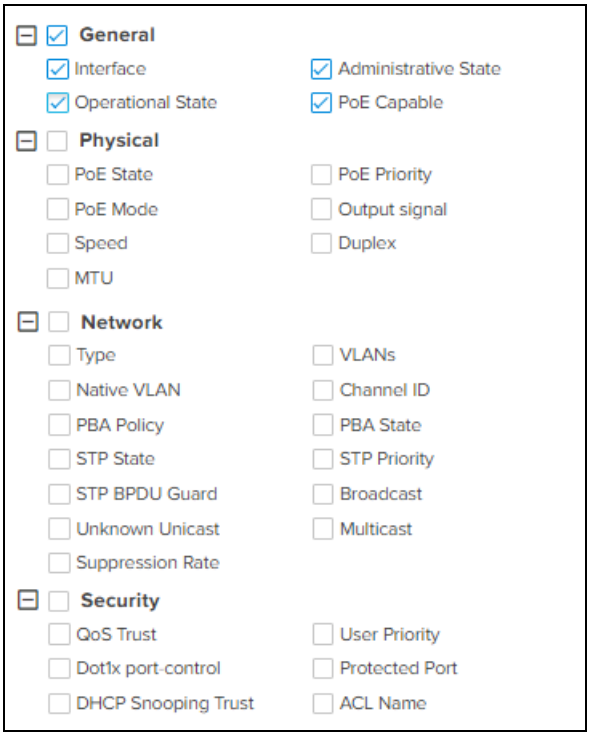
Physical Tab

The **Ports Physical** details view displays following fields by default:

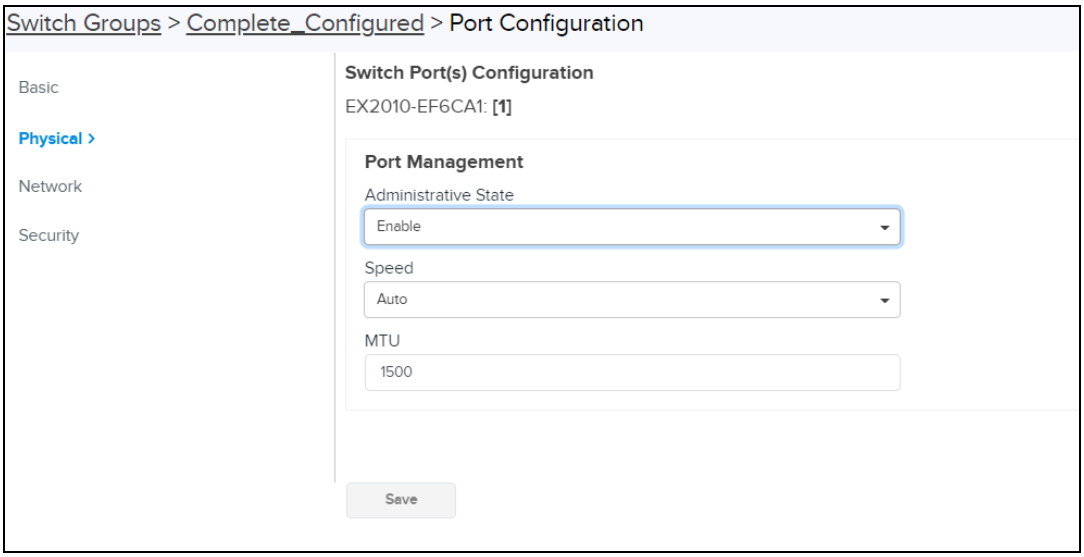
- Port, Tags, Operational State, PoE State, PoE Priority, Speed, Duplex, MTU, and Edit.



User can click  on top bar to include additional fields in **Ports Physical** Detail view.



1. Click Edit  icon or Port device in the list to edit the **Ports Configuration** Physical tab details.

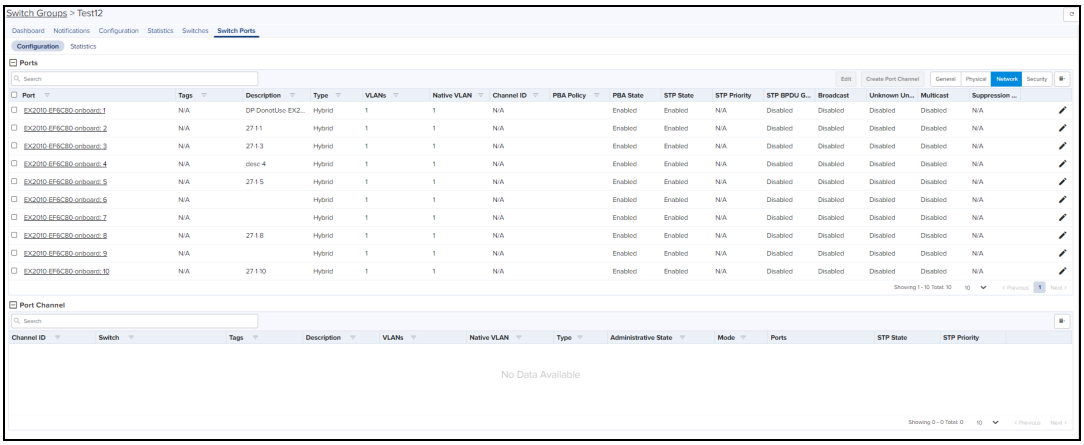


2. Enter the **Port Management** and **PoE** details.
3. Click **Save.**

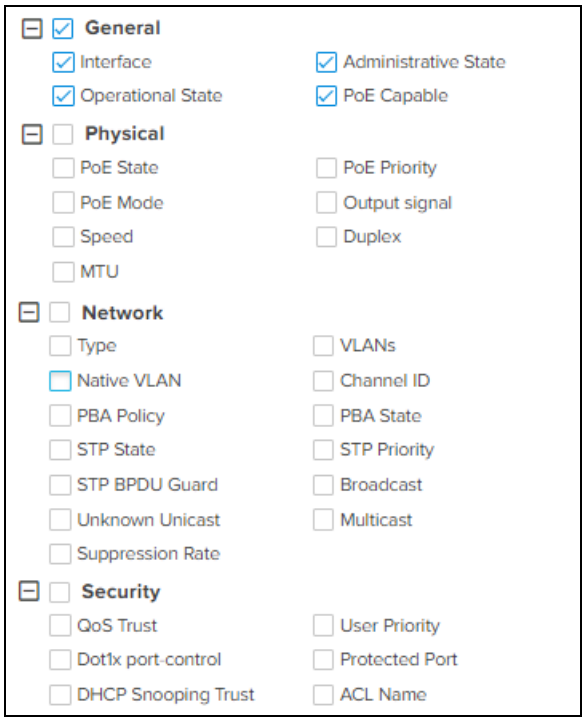
Network Tab

The **Ports Network** details view displays following fields by default:

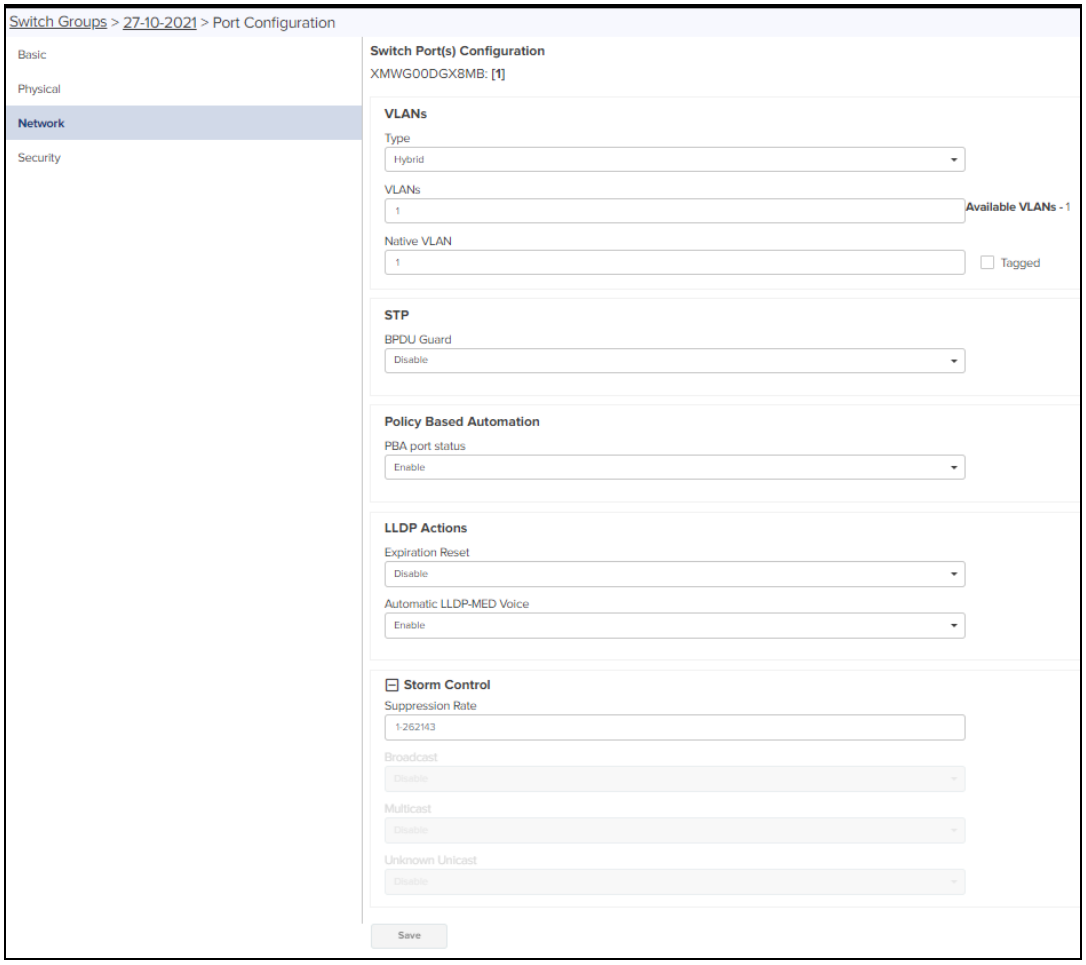
- Port, Tags, Type, VLANs, Native VLAN, Channel ID, PBA Policy, PBA State, STP State, STP Priority, and Edit.



User can click  on top bar to include additional fields in **Ports Network** Detail view.



1. Click Edit icon or Port device in the list to edit the **Ports Configuration** Network tab details.

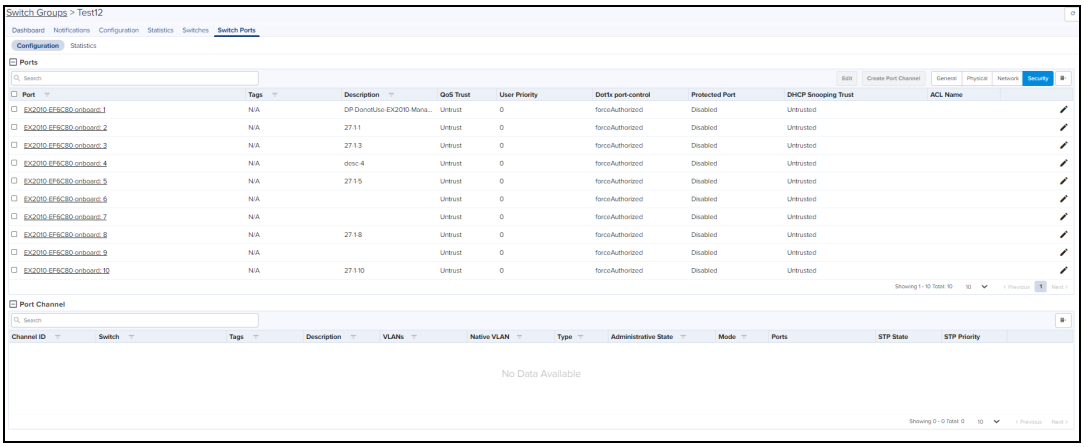


2. Enter **VLANs, STP, Policy Based Automation,** and **Strom Control** details.
3. Click **Save.**

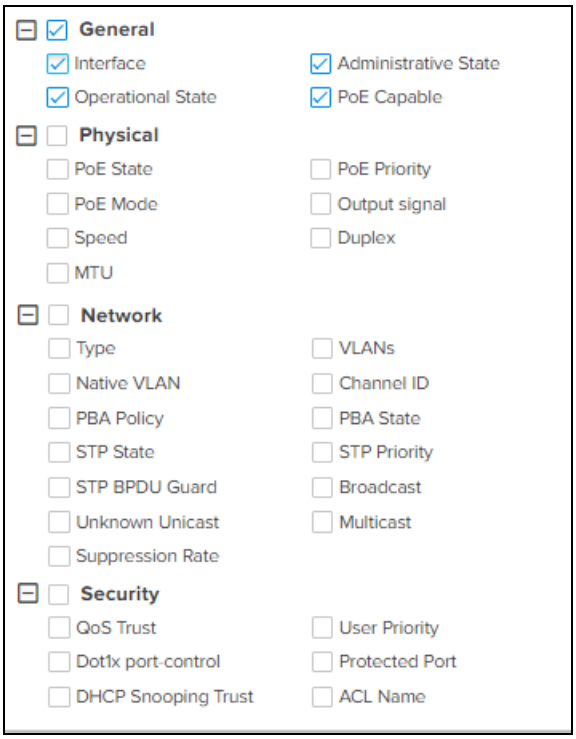
Security Tab

The **Ports Security** details view displays following fields by default:

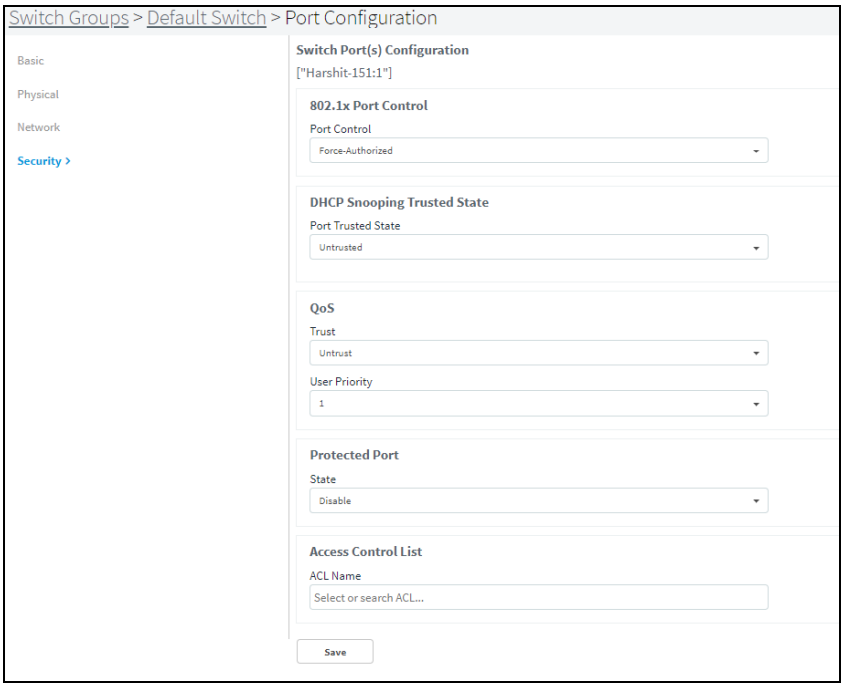
- Port, Tags, QoS Trust, User Priority, Dot1x port-control, Protected Port, DHCP Snooping Trust, ACL Name, and Edit.



User can click  on top bar to include additional fields in **Ports** Network Detail view.



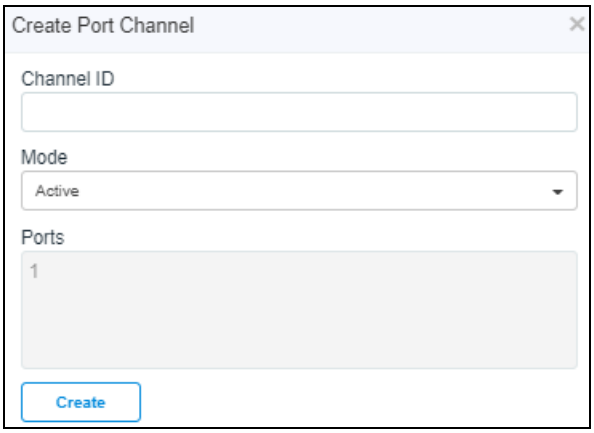
1. Click Edit  icon or Port device in the list to edit the Ports Configuration Security tab details.



2. Enter **802.1xPort Control, DHCP Snooping Trusted State, QoS, Protected Port, Access Control List** details.
3. Click **Save.**

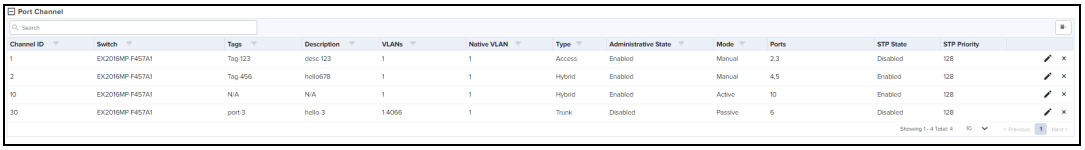
Port Channel

1. To create a Port Channel, select a **Port** from the list under the specific parameters and click **Create Port Channel**.
2. **Create Port Channel** window pops-up, enter details.
3. Click **Create**.

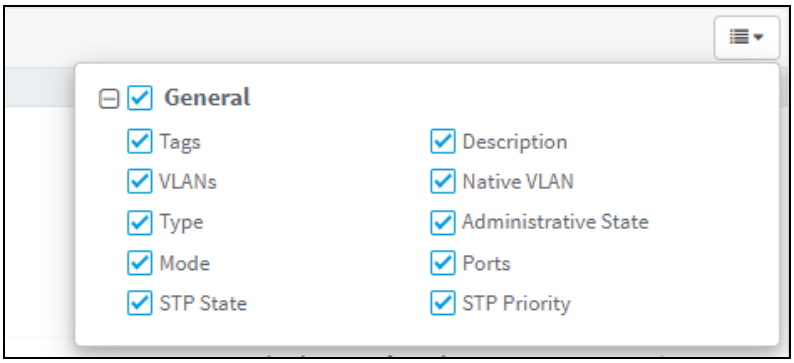


The **PortChannel** details view displays following fields by default:

- Channel ID, Switch, Tags, Description, VLANs, Native VLAN, Type, Administrative State, Mode, Ports, STP State, and STP Priority.



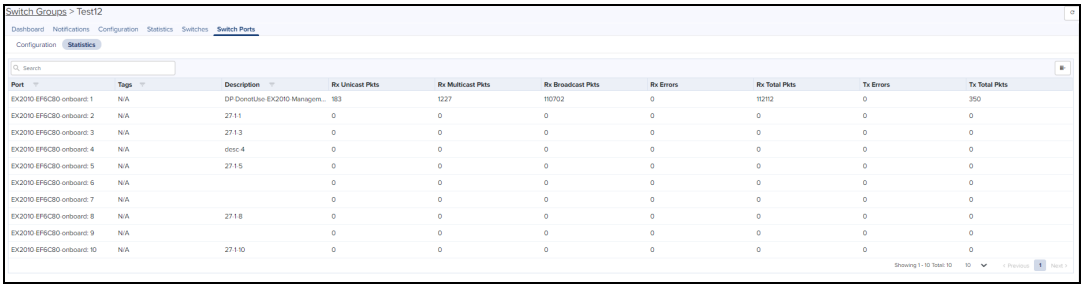
User can click on top bar to include additional fields in **Port Channel** Detail view.



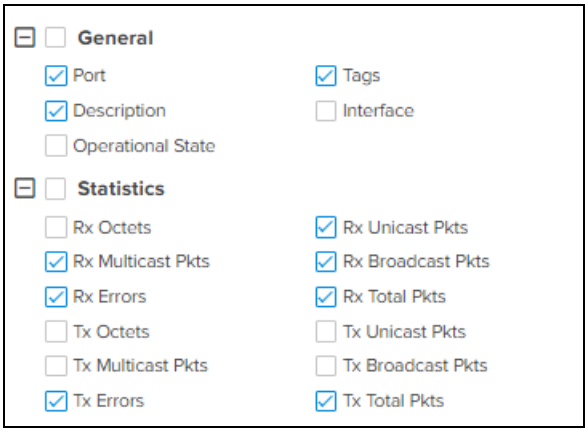
Statistics

The **Statistics** page displays the latest data and statistics of each Port. Port statistics match the Client statistics and generate the Client View.

To view the Switch Ports Statics navigate to **Shared Settings > Switch Groups > Switch Ports > Statistics**.

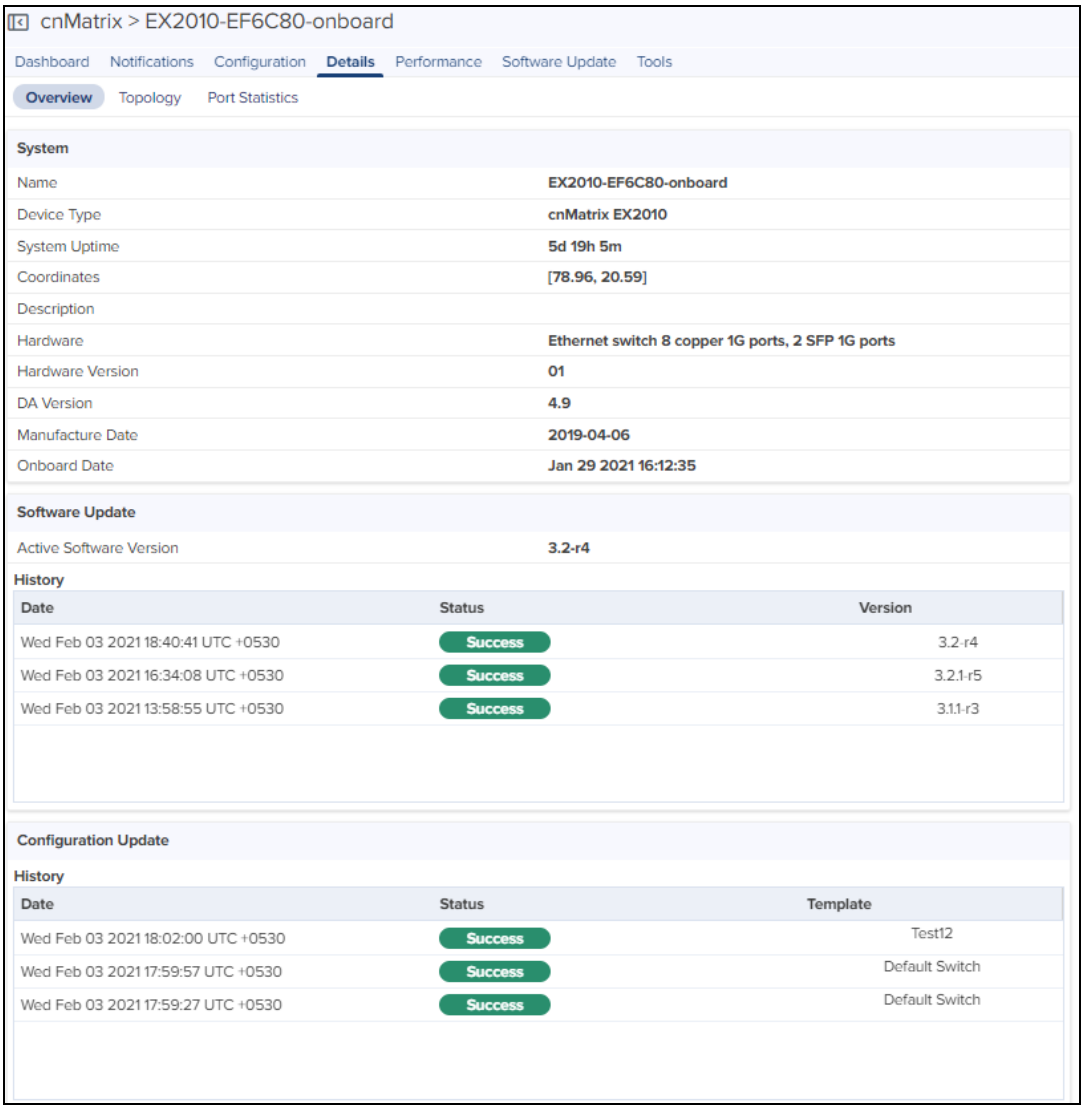


User can click  on top bar to include additional fields in **Statistics** Detail view.



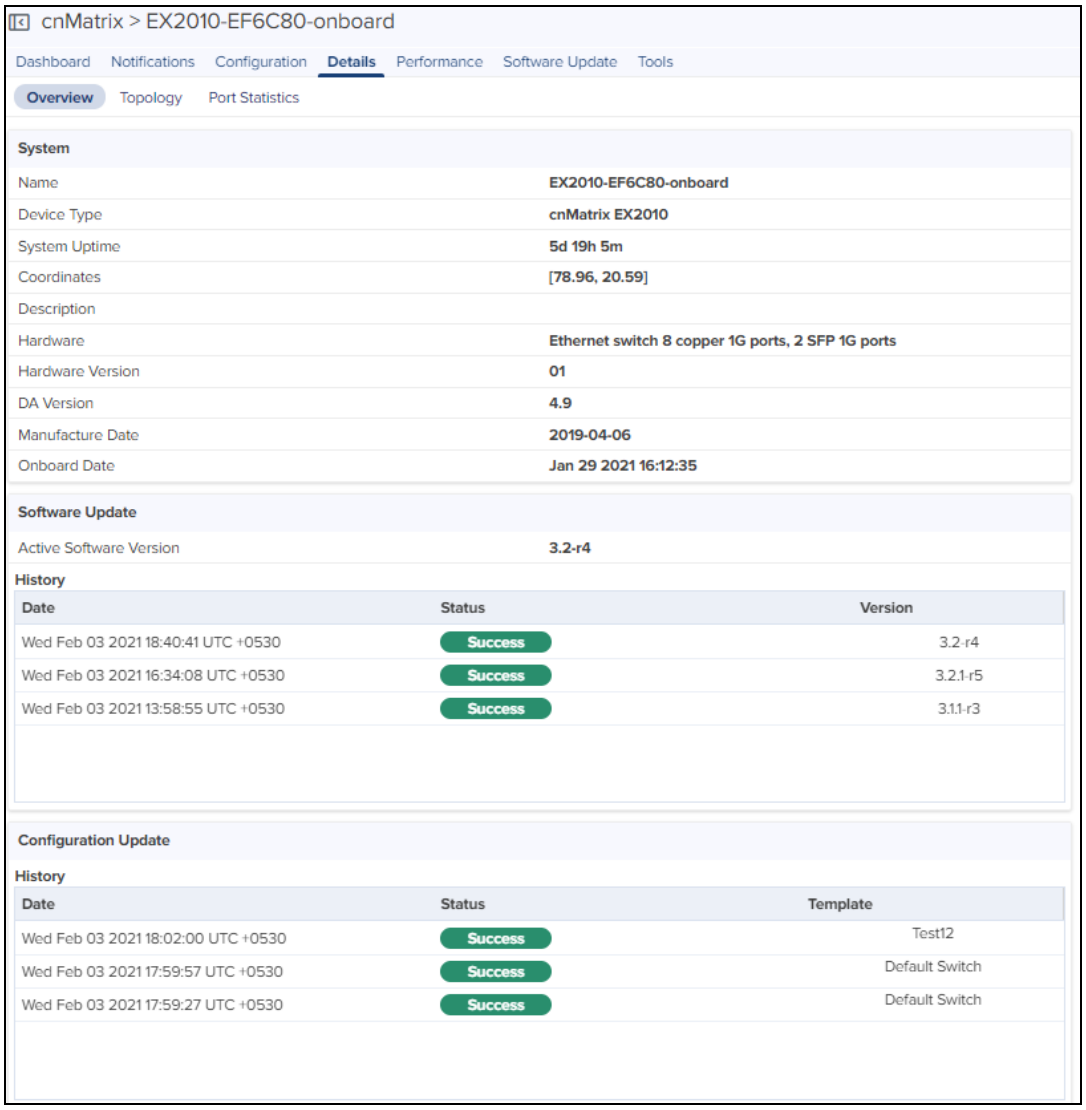
Device Details

Details page provide the information about the switches **Overview**, **Topology**, and **Port Statistics**.



Details Overview

To view the details of the overview page, navigate to the **Details > Overview** tab.



Topology

To view the details of the Topology page, navigate to the **Details > Topology** tab.



Port Statistics

To view the details of the Port Statistics page, navigate to the **Details > Port Statistics** tab.



Port	Tags	Description	Rx Unicast Pkts	Rx Multicast Pkts	Rx Broadcast Pkts	Rx Errors	Rx Total Pkts	Tx Errors	Tx Total Pkts
EX2010 EF6C80 onboard: 1	N/A	DP DonotUse-EX2010-Mana...	183	1227	110702	0	112112	0	350
EX2010 EF6C80 onboard: 2	N/A	27.1.1	0	0	0	0	0	0	0
EX2010 EF6C80 onboard: 3	N/A	27.1.3	0	0	0	0	0	0	0
EX2010 EF6C80 onboard: 4	N/A	desc 4	0	0	0	0	0	0	0
EX2010 EF6C80 onboard: 5	N/A	27.1.5	0	0	0	0	0	0	0
EX2010 EF6C80 onboard: 6	N/A		0	0	0	0	0	0	0
EX2010 EF6C80 onboard: 7	N/A		0	0	0	0	0	0	0
EX2010 EF6C80 onboard: 8	N/A	27.1.8	0	0	0	0	0	0	0
EX2010 EF6C80 onboard: 9	N/A		0	0	0	0	0	0	0
EX2010 EF6C80 onboard: 10	N/A	27.1.10	0	0	0	0	0	0	0

60 GHz cnWave Network Configuration

60 GHz cnWave operates with Cambium Networks cnMaestro management system. cnMaestro simplifies device management by offering full network visibility and zero-touch provisioning. Using cnMaestro, user can view network status and perform a full suite of wireless network management functions in real time including optimizing system availability, maximizing throughput, and meeting the emerging needs of business and residential customers.

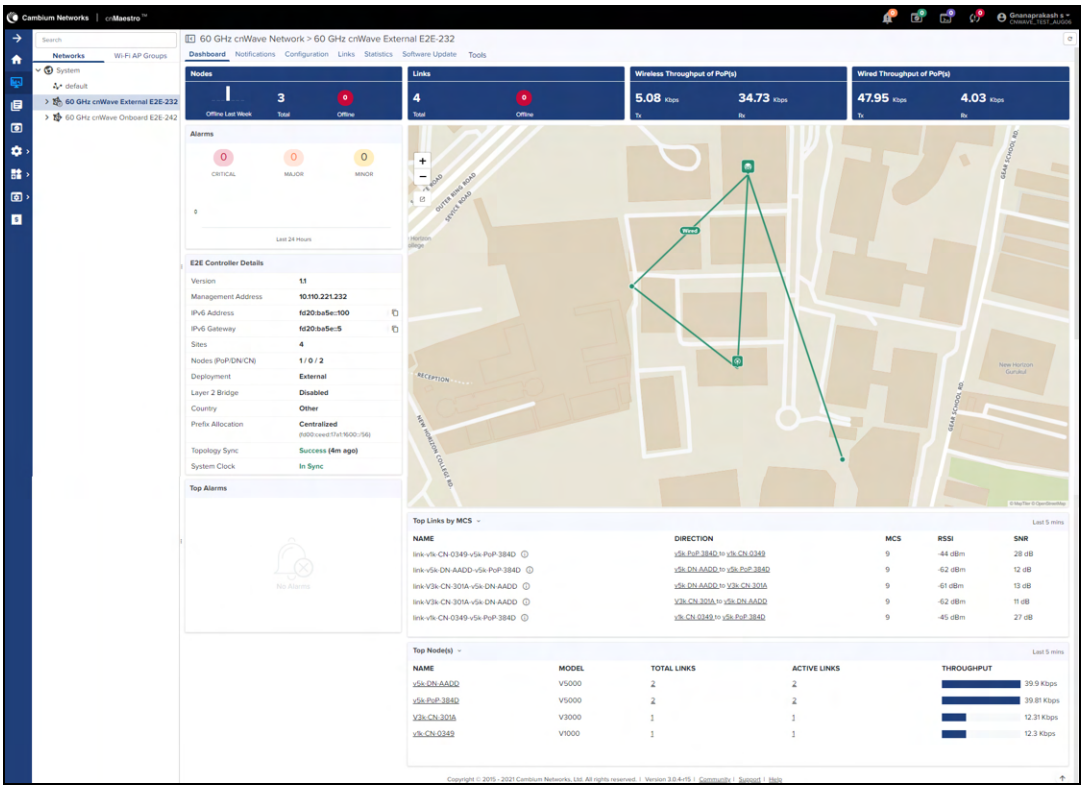
Managing E2E Network

The Monitoring tab displays the monitoring panel of 60 GHz cnWave for cnMaestro On-Premises. This section includes the following:

- Dashboard
- Notifications
- Configuration
- Links
- Statistics
- Software Update
- Reports
- Map
- Tools

Dashboard

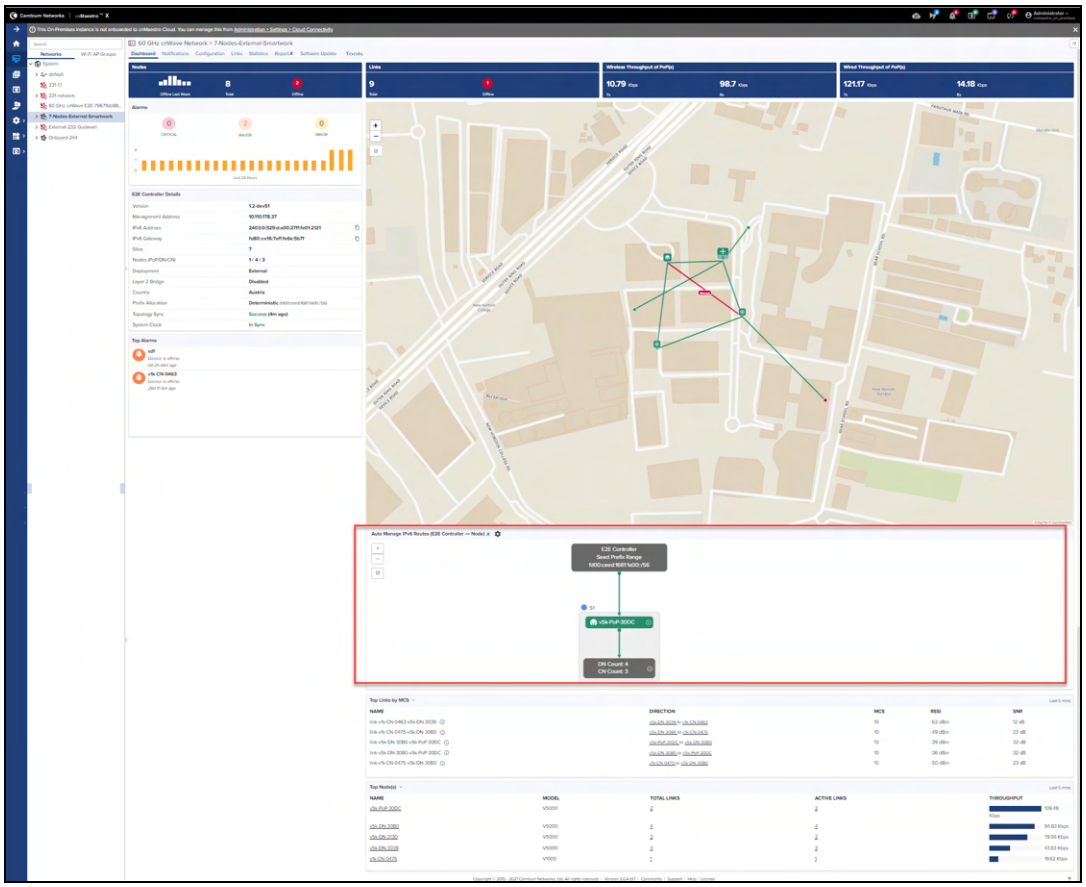
Dashboard pages are customized for each device type and aggregation level (such as E2E Network, Node, and Site). The dashboard section displays the **Nodes, Links, Auto Manage IPv6 Routes, Wireless Throughput of PoP(s), Wired Throughput of PoP(s), Alarms, E2E Controller Details, Top Alarms, Map, Top Links by MCS, Top Links by RSSI, Top Links by SNR, Top Node(s),Top PoP(s), Top DN(s),** and **Top CN(s).**



Auto Manage IPv6 Routes (E2E Controller↔ Node)

The E2E Controller Network dashboard page displays the **Auto Manage IPv6 Routes (E2E Controller ↔ Node)** tab, if you enable **Auto Manage Routes** in the **Tools > Settings** page of **External E2E Network**.

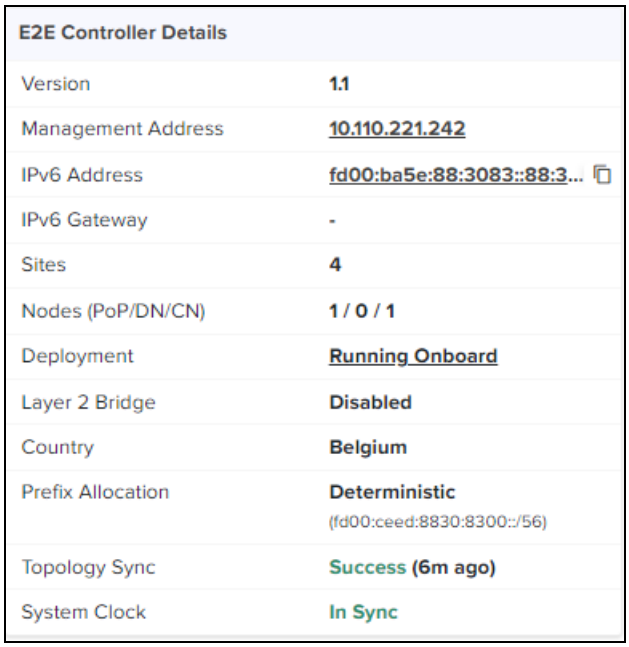
This feature automates IPv6 routes for DNs and CNs based on status of the topology and PoP nodes. It is applicable only if PoP nodes and E2E Controller are in the same Network or containing the same prefix length.



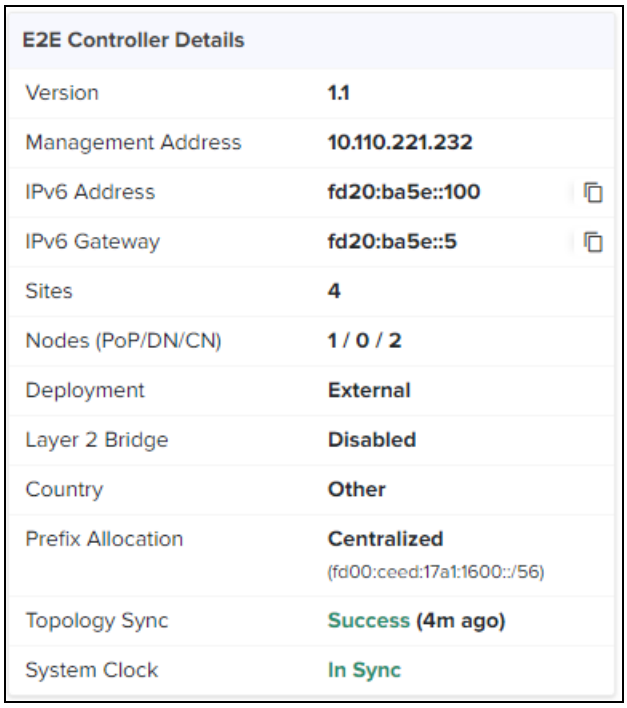
E2E Controller Details

E2E Controller Details displays the details such as **Version**, **Management Address, IPv6 Address, IPv6 Gateway, Sites, Nodes, Deployment, Layer 2 Bridge, Country, Prefix Allocation, Topology Sync,** and **System Clock**

- If Onboard E2E controller is enabled in device and managed by cnMaestro, it displays deployment as **Running Onboard.**

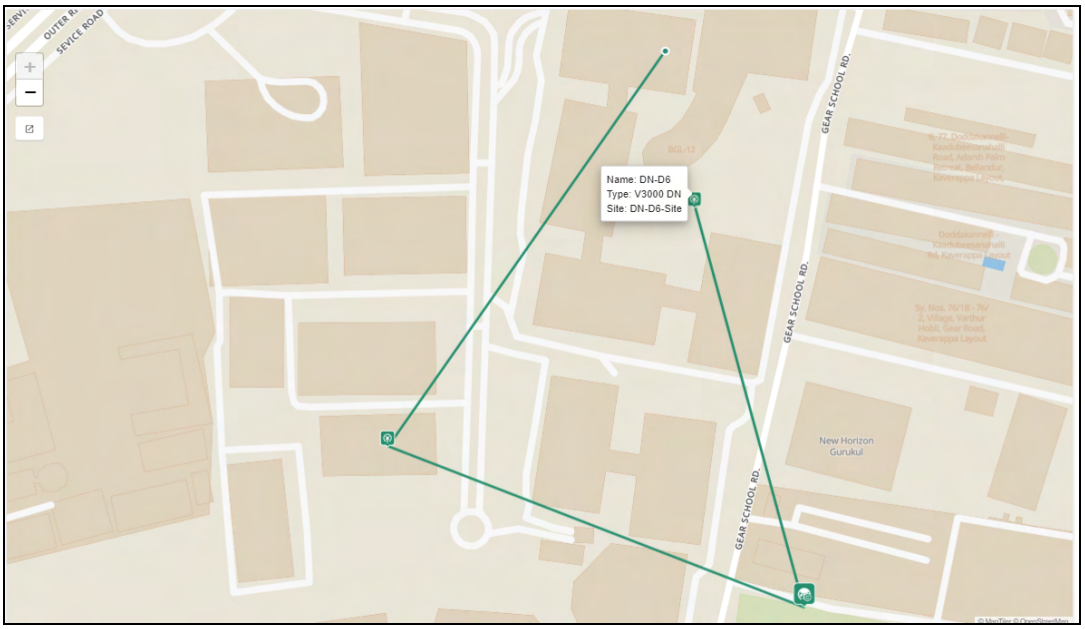


- If External E2E controller is managed by cnMaestro, it displays deployment as **External.**

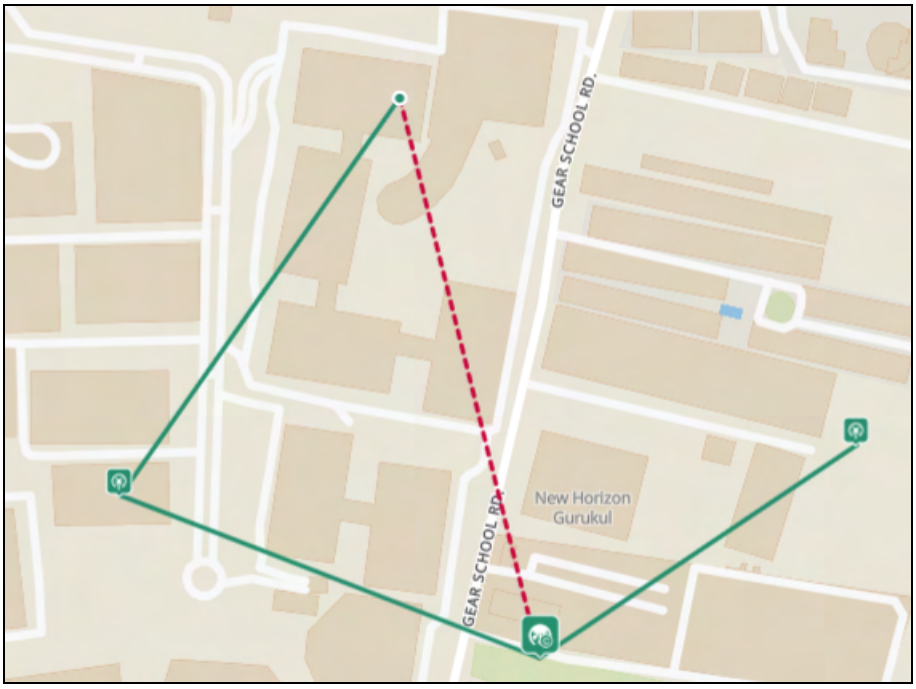


Dashboard Maps

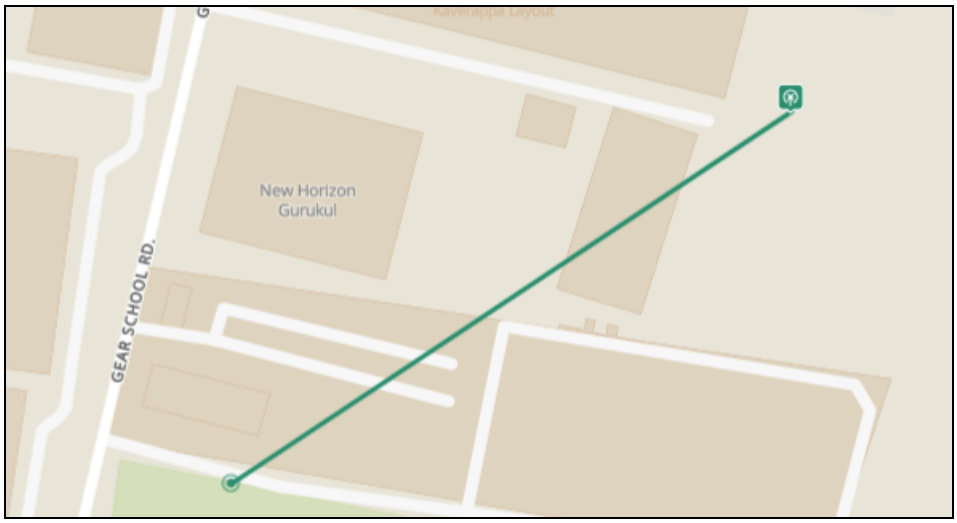
In the dashboard map, when user hover on particular link or node, it pops-up link or node basic details.



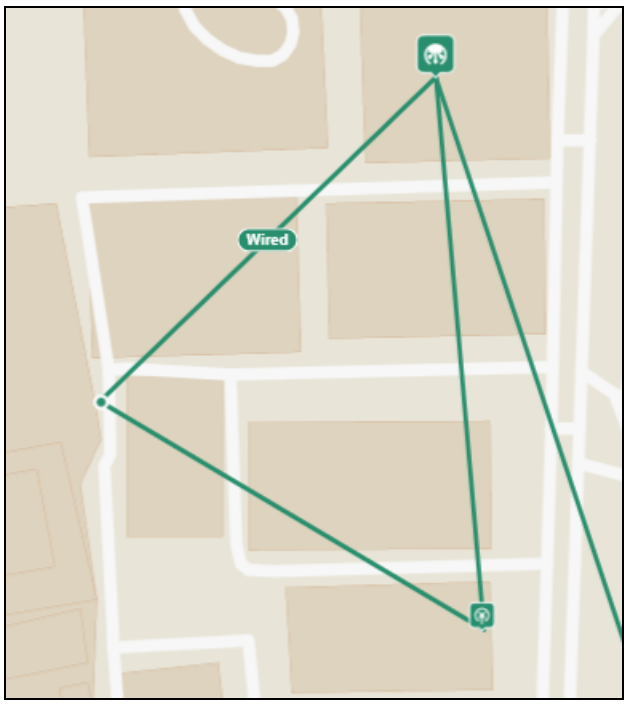
- Dotted line displays the Backup CN link between the DN and CN.



- Continuous line displays the wireless link between PoP, DN or CN.



- Continuous line with **Wired** tag displays the wired link between PoP, DN or CN.



To navigate to the Maps page click the Map view .

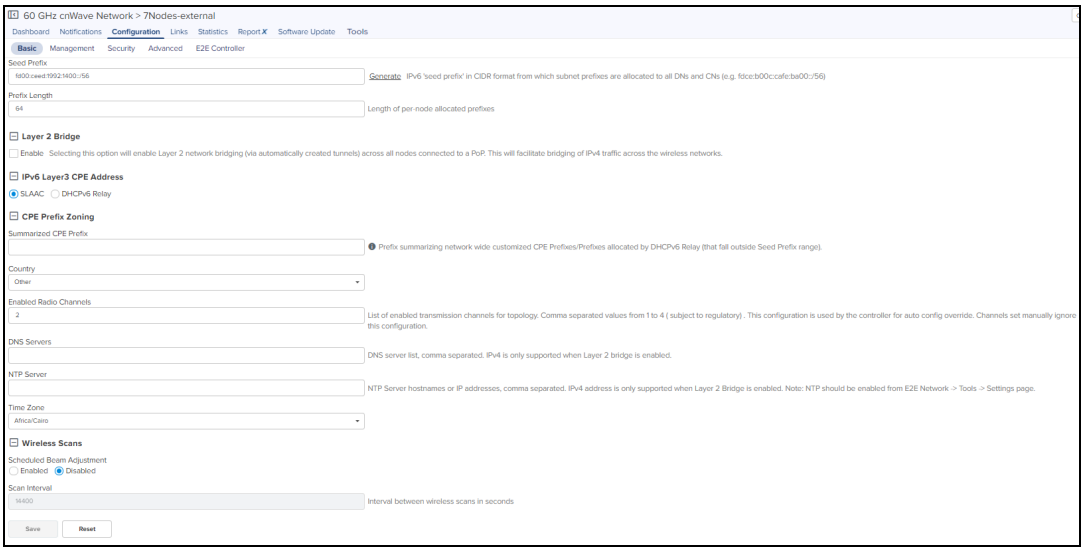
Notifications

Notifications are same as shown above for other devices, refer Notification for more details.

Configuration

Configure the following after onboarding the 60 GHz cnWave E2E controller:

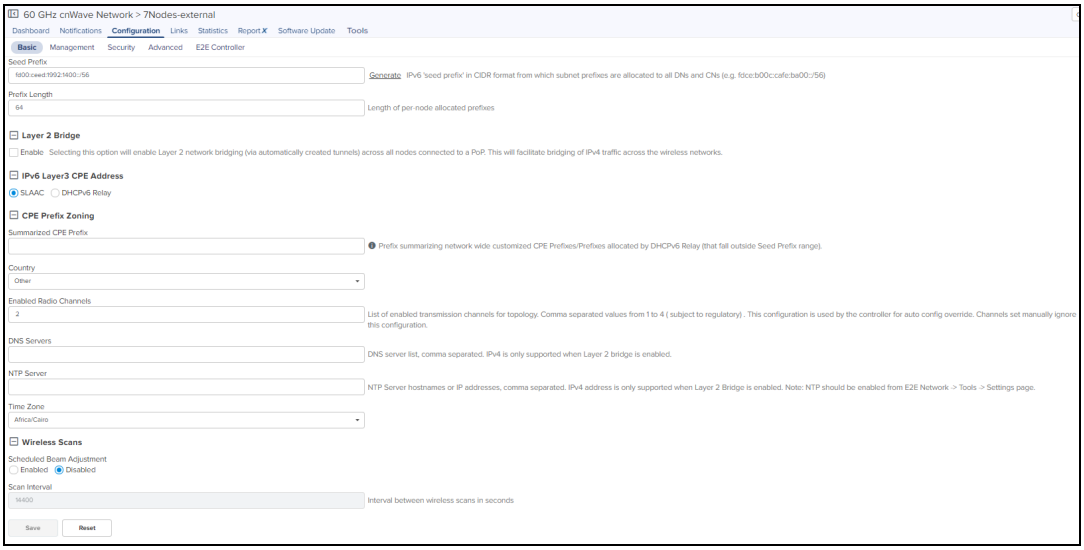
- Basic
- Management
- Security
- Advanced
- E2E Controller



NOTE:
Once user selects the **Auto-assign** IPv6 Addresses while configuring E2E Controller and PoP node. Uses the same IPv6 during the prefix allocation.

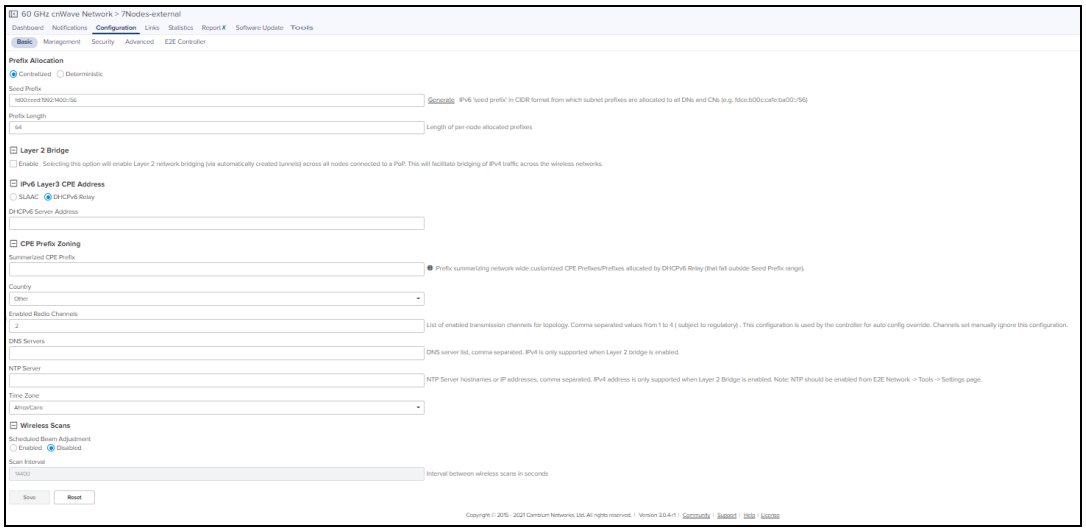
Basic Configuration

1. Navigate to **Configuration** > **Basic** to configure basic settings of E2E Controller.

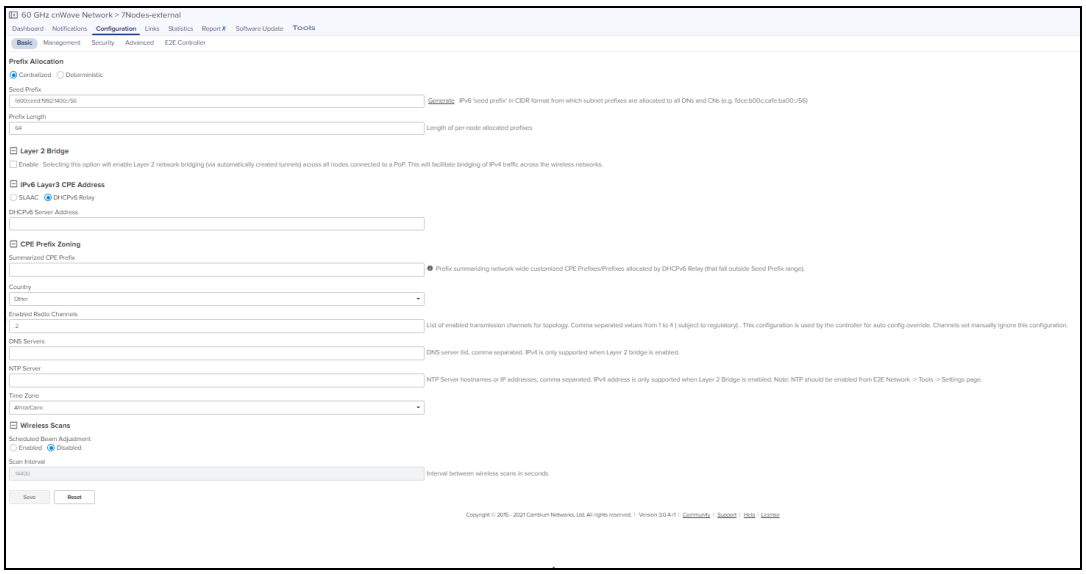


NOTE:
Prefix allocation automatically gets updated, when E2E Controller is managed by cnMaestro.

2. In the **Prefix Allocation**, select **Centralized** or **Deterministic** to allocate the IP for the nodes.



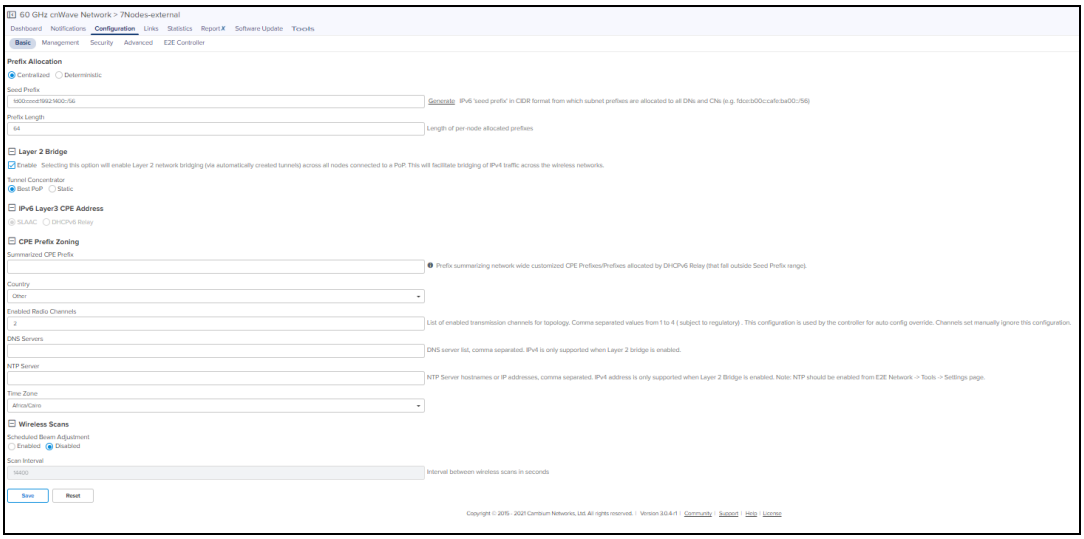
3. Enter the **Seed Prefix** and **Prefix Length**.



4. Enabling **Layer 2 Bridge** is optional.

   Enabling this option will enable Layer 2 network bridging (via automatically created tunnels) connected across all nodes and facilitates bridging of IPv4 traffic across the wireless networks. It also enables the configuration of VLAN Management and Ports on all PoP, DN, and CN Nodes.

   In **Layer 2 Bridge**, select the check box to enable Layer2 Network Bridging, choose **Tunnel Concentrator** as **Best PoP** or **Static.**



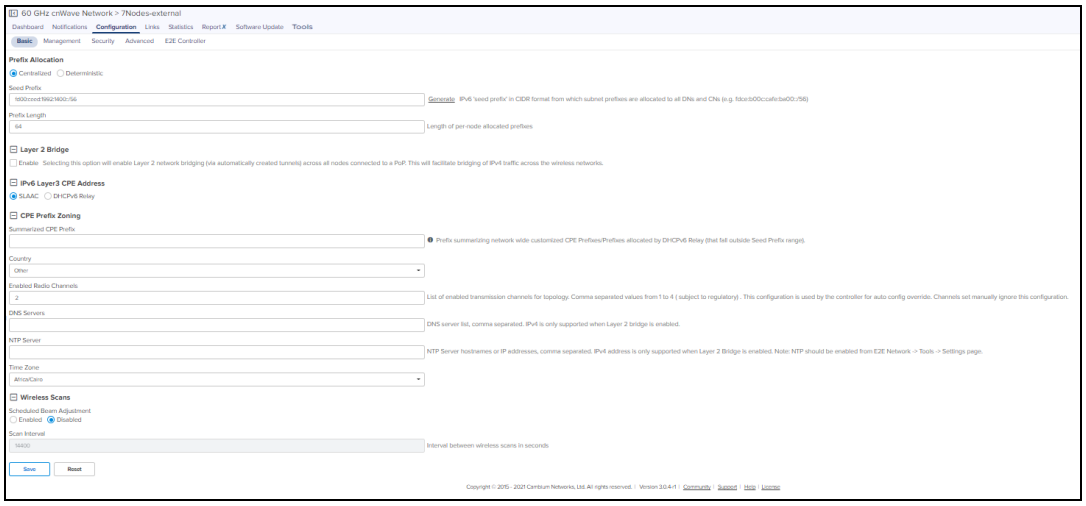
- If user selects **Tunnel Concentrator** as **Static.**
- Enter the Concentrator can be an external switch/router when static is selected.



	NOTE: **IPv6 Layer3 CPE Address** can be enabled when E2E Controller is running 1.1 verison and Layer 2 Bridge is disabled.

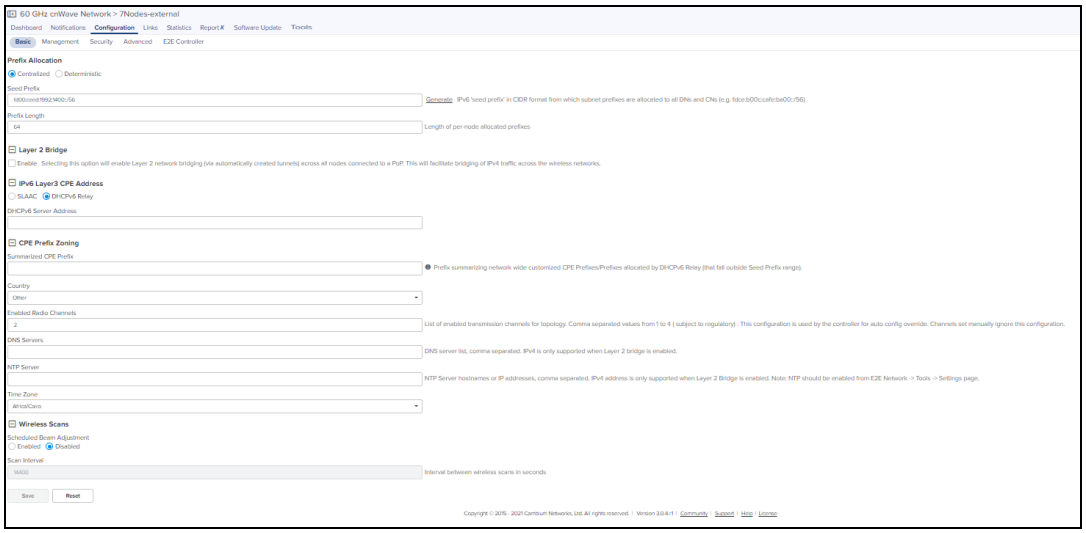
5. Select the **IPv6 Layer3 CPE Address** as **SLAAC** or **DHCPv6 Relay.**

   CPE sends a DHCP request. DHCPv6 server assigns address and the CN node uses the Address and Prefix from the corresponding DHCP pool.



- If user selects **IPv6 Layer3 CPE Address** as **DHCPv6 Relay.**

  User can configure the DHCPv6 server address.

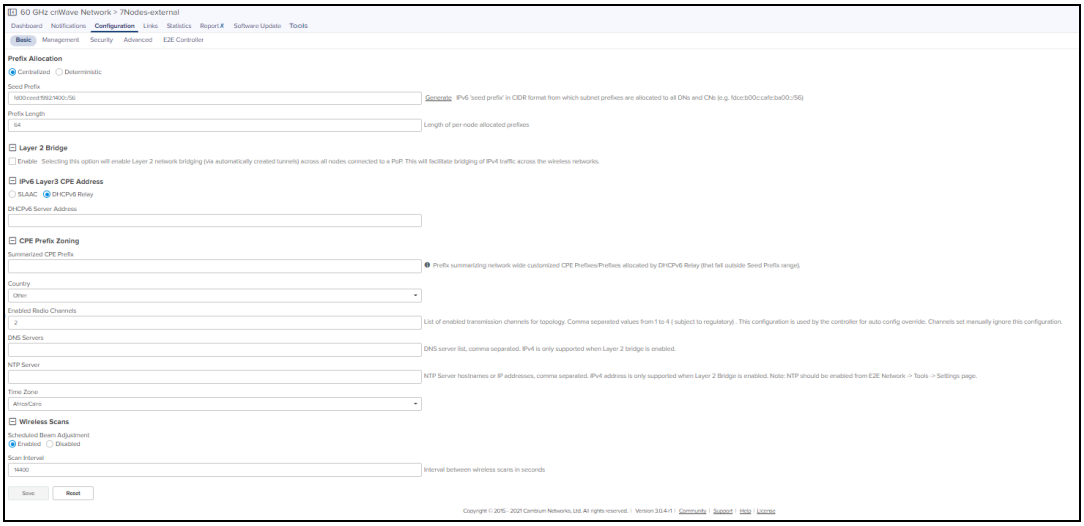


> **NOTE:**
>
> - By default **Country** is **Other**, user can configure it.
> - By default **Enabled Radio Channels** is 2, user can configure channel if required.
> - Enter the **Hostnames** or **IP address** of NTP server

6. In **CPE Prefix Zoning** enter **Summarized CPE Prefix**.
7. Select the **Country** from the drop-down.
8. Enter the channel number in **Enable Radio Channels** and **DNS Servers.**
9. Enter **NTP Server.**
10. Select the **Time Zone** from the drop-down.

> **NOTE:**
>
> By default **Wireless Scans** will be disabled.

11. In **Wireless Scans** enable the **Scheduled Beam Adjustment** and configure **Scan Interval** as required.

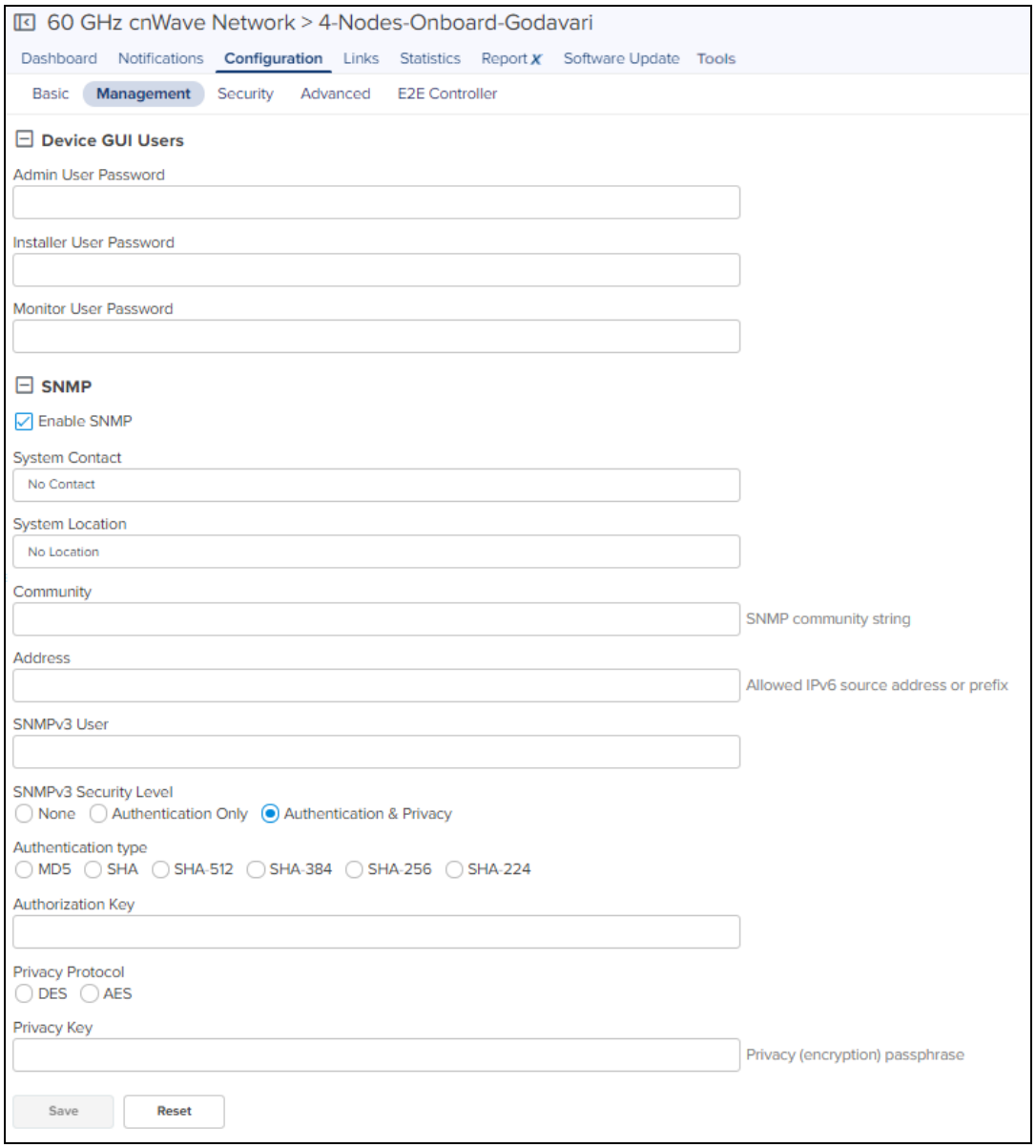


12. Click **Save.**

Management

Management configuration allows user to configure and manage the credentials of the administrator and it allows enable **SNMP**.

1. Navigate to **Configuration** > **Management** to set the **Device GUI Passwords** and to enable the **SNMP**.



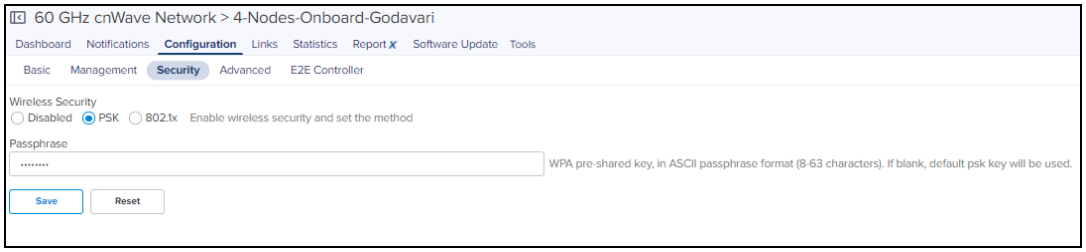
2. Click **Save.**

Security

Security page allows the user to enable the wireless security **PSK** or **802.1x.** Disabling option unscure the devices.

To Enable PSK :

1. Navigate to **Configuration** > **Security** tab.
2. Select **PSK** in **Wireless Security**.



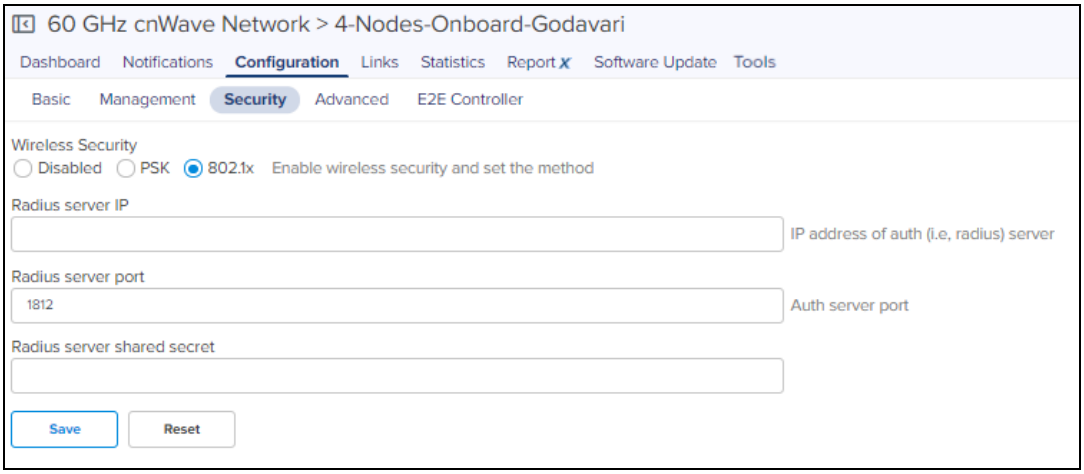
3. Enter the **Passphrase**.

	NOTE: If passphrase is left blank, default psk_key will be used.

4. Click **Save.**

To Enable 802.1x

1. Navigate to **Configuration** > **Security.**
2. Select **802.1x** in **Wireless Security**.



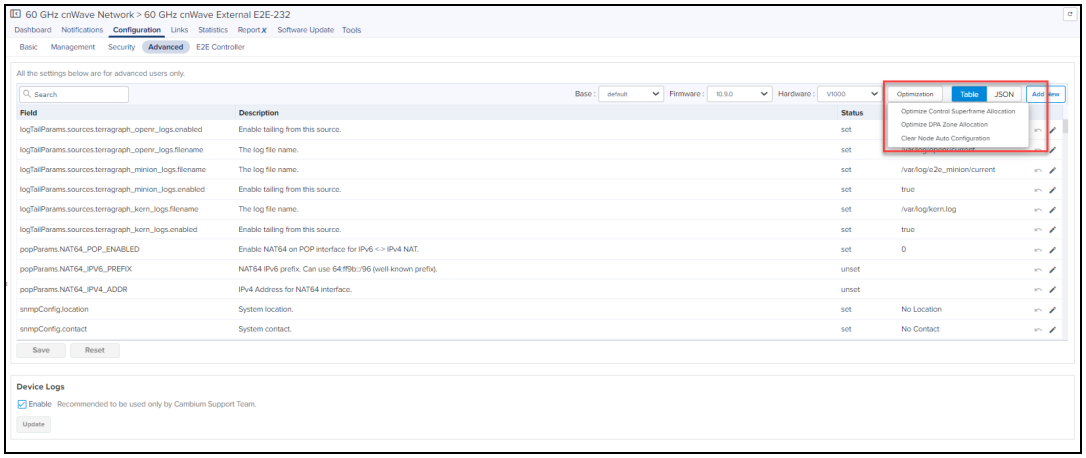
3. Enter the **Radius server IP.**
4. Enter the **Radius server port.**
5. Enter the **Radius server shared secret.**
6. Click **Save**.

Advanced

Advanced tab allows the advanced user to edit the settings of the Table and JSON format of the E2E Controller.

It also allows to optimize the network using the following options:

- Optimize Control Superframe Allocation
- Optimize DPA Zone Allocation
- Clear Node Auto Configuration

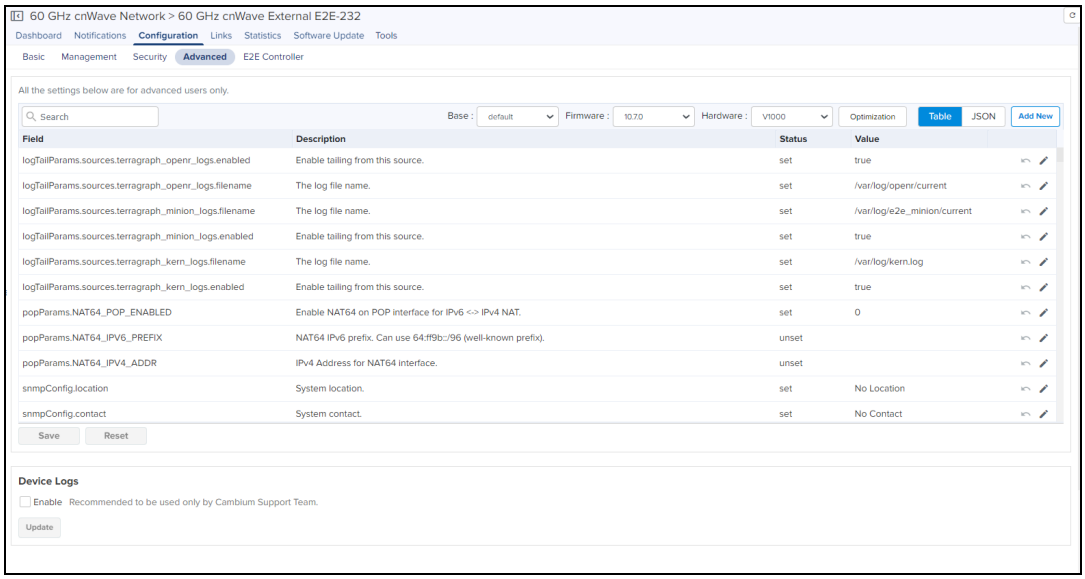


Table

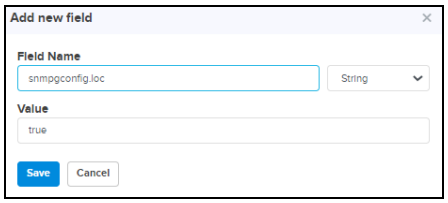
In the **Table** advanced user can able to view, add, and edit **Field Name** and **Value**.

To add a field:

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



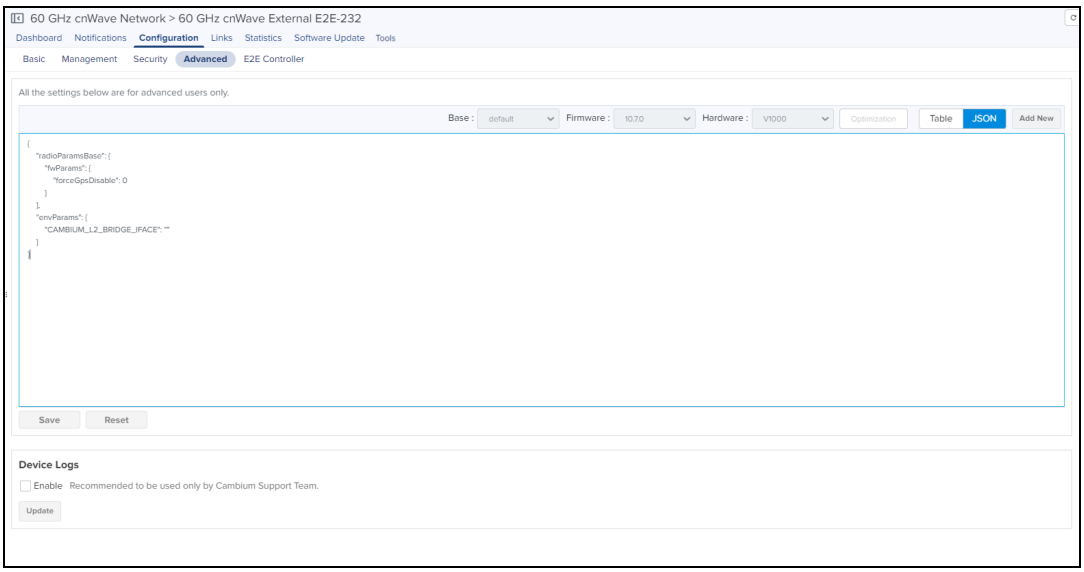
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

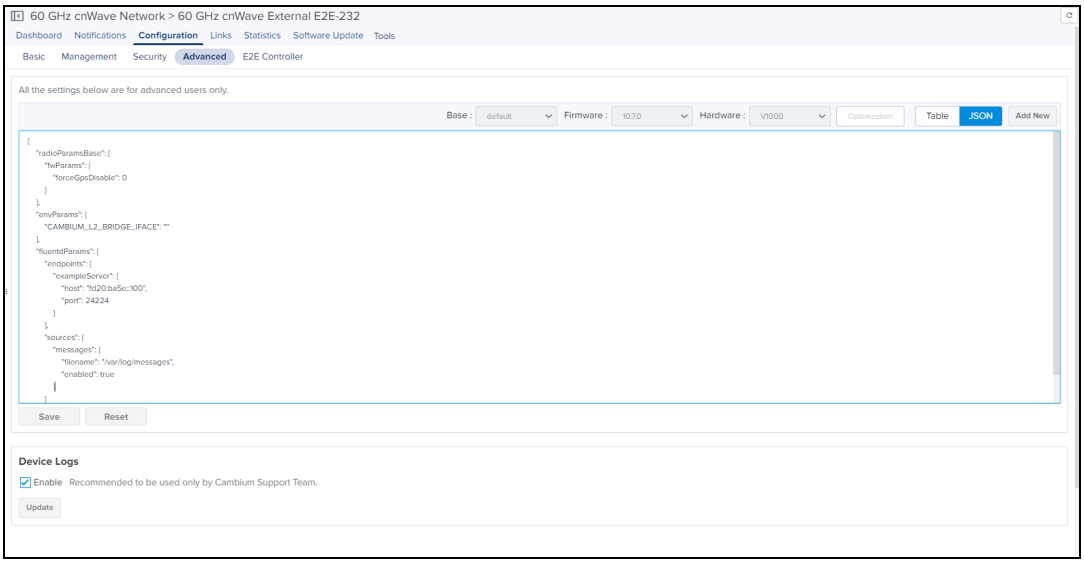
JSON

JSON allows Advanced user can view and edit json format.



To view or edit the JSON file:

1. Navigate to **Configuration** > **Advanced > JSON.**



	NOTE: Enabling the Device Logs is supported only for External E2E Controller devices and it allows the Support team can view the logs.

2. Enable **Device Logs**.
3. Click **Update.**

E2E Controller

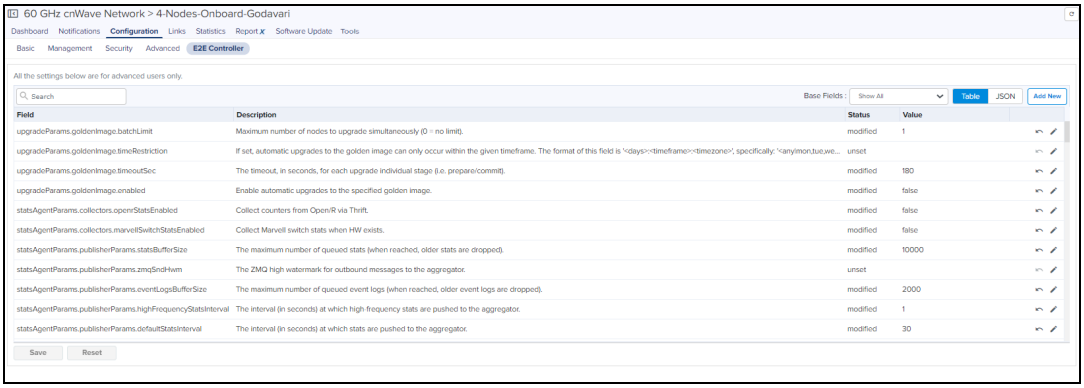
E2E Controller allows the advanced user to set the **Table** and download the **JSON** file.

Table

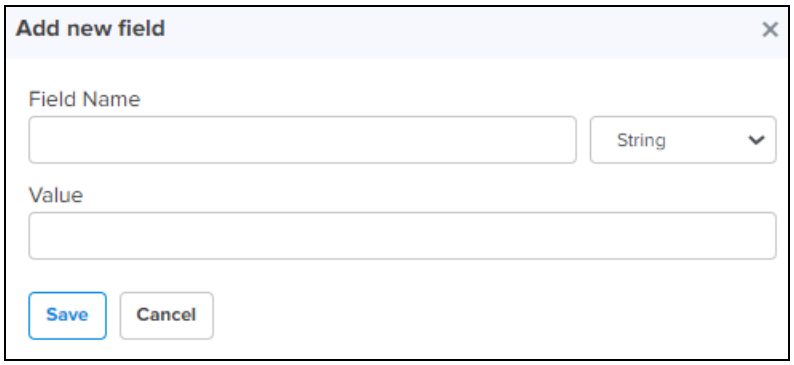
In **E2E Controller Table** user can view, edit and add **Field Name** and **Value.**

To Add Field:

1. Navigate to **Configuration** > **E2E Controller.**
2. Click **Add New.**



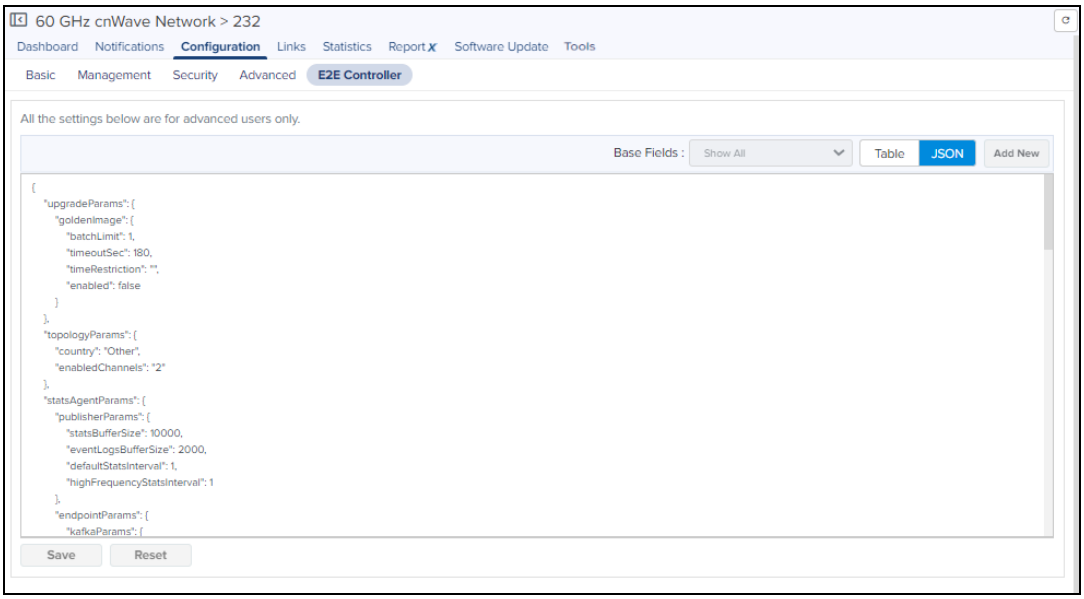
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

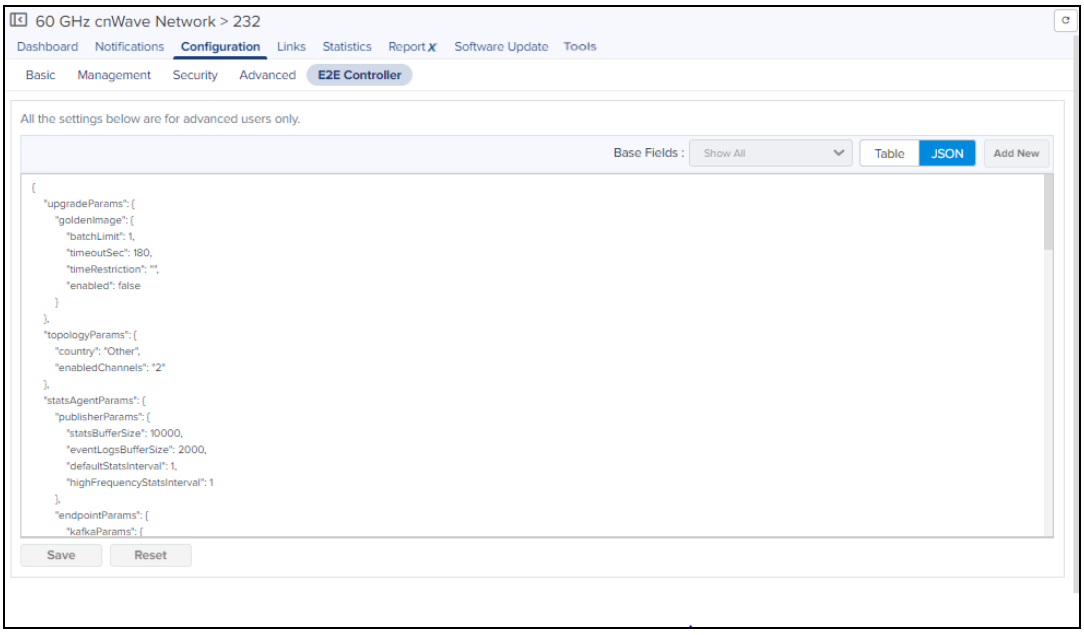
JSON

JSON allows Advanced user to view and edit json format.



To view or edit the JSON file:

1. Navigate to **Configuration** > **E2E Controller > JSON**



Links



NOTE:

Backup CN Link option gets enabled when E2E controller is running on Version 1.1.

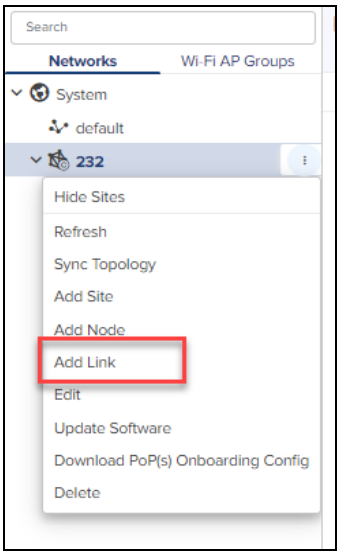
Links provide the details about the link established between the nodes and also provides the option to create a new Wireless, Statistics, Events, Wired and CN backup link.

- List
- Statistics
- Events

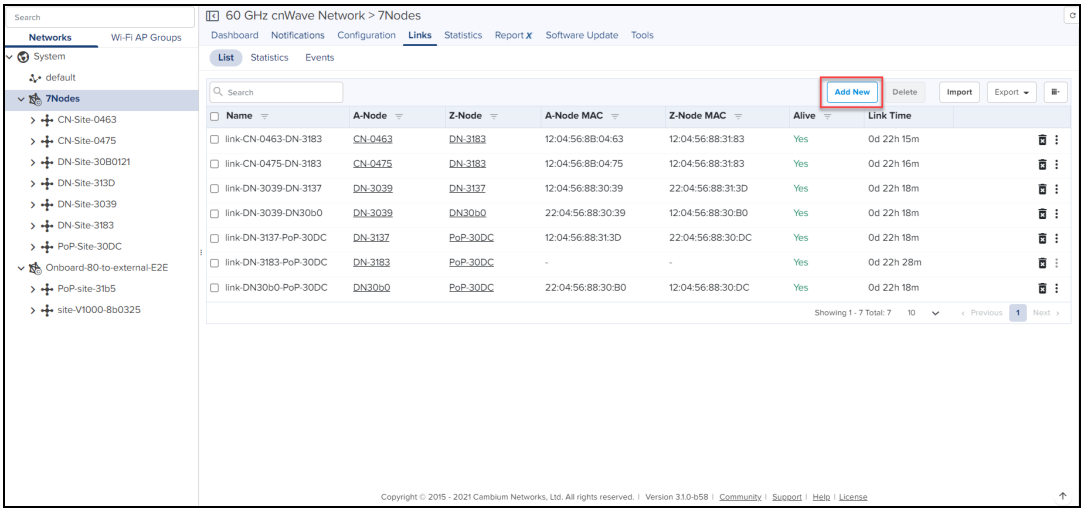
List

To add a link:

1. Navigate to the E2E Network tree menu click ⋮ icon and select **Add Link** or

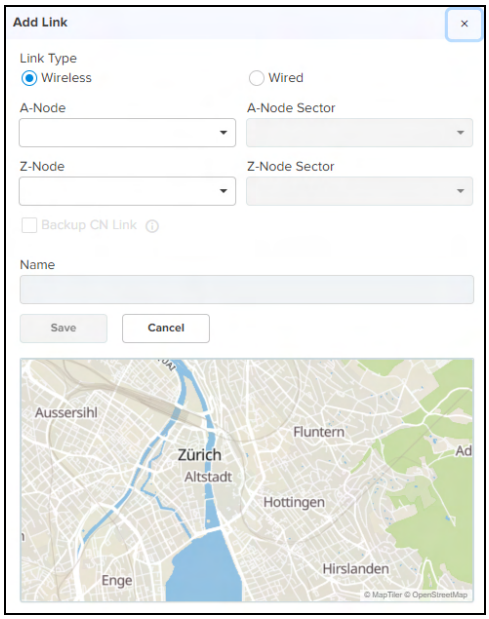


Navigate to **Network > Links > List > Add New**.



Add Link window pops-up.

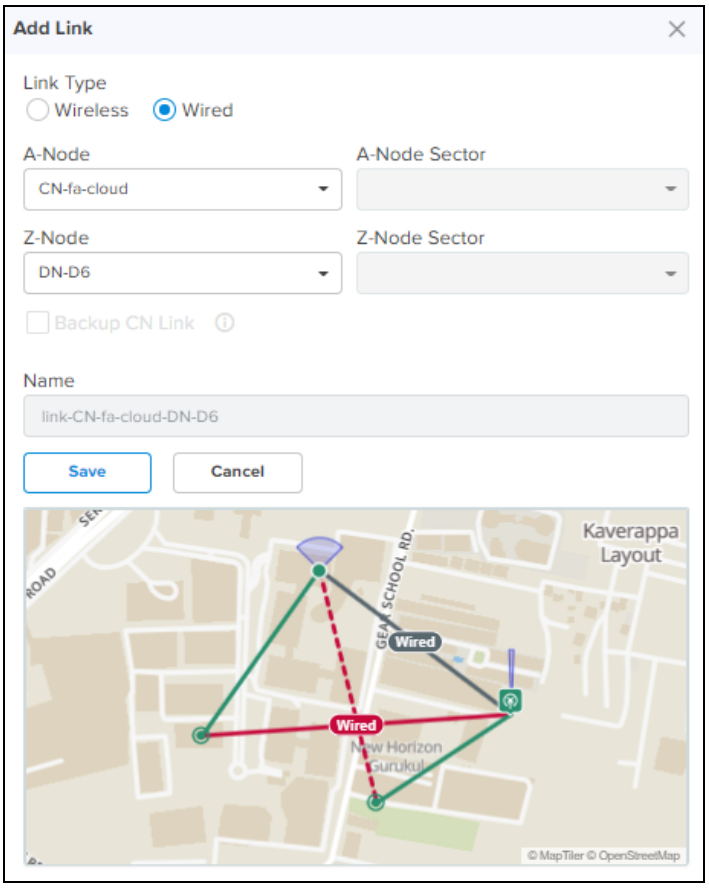
Figure 94 Wireless



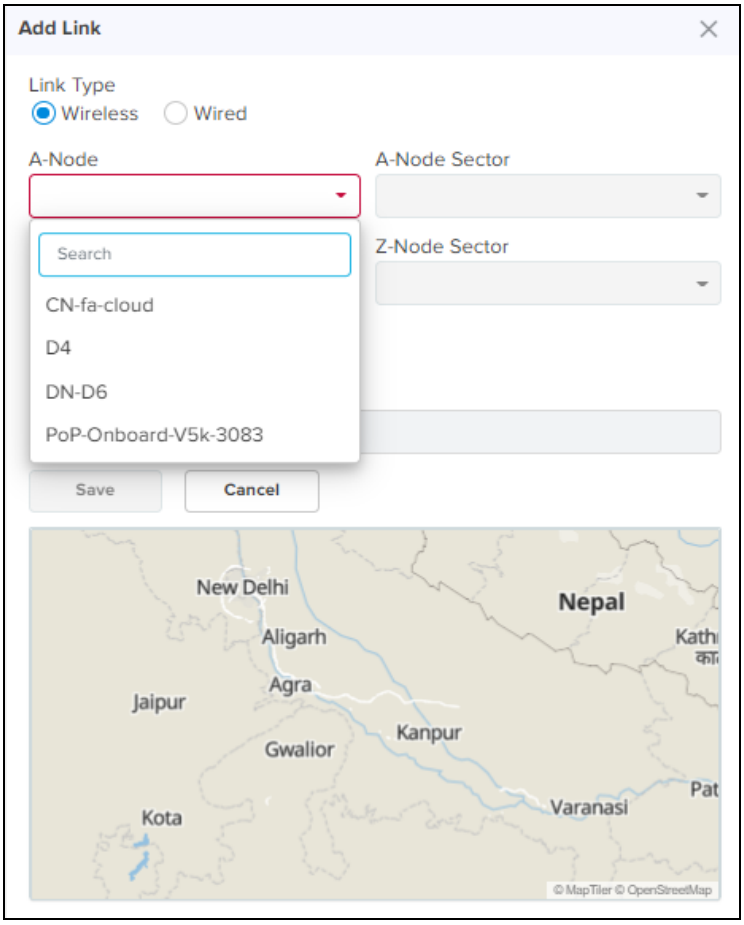
2. Select **Link Type** Wireless or Wired.

Figure 95 Wired

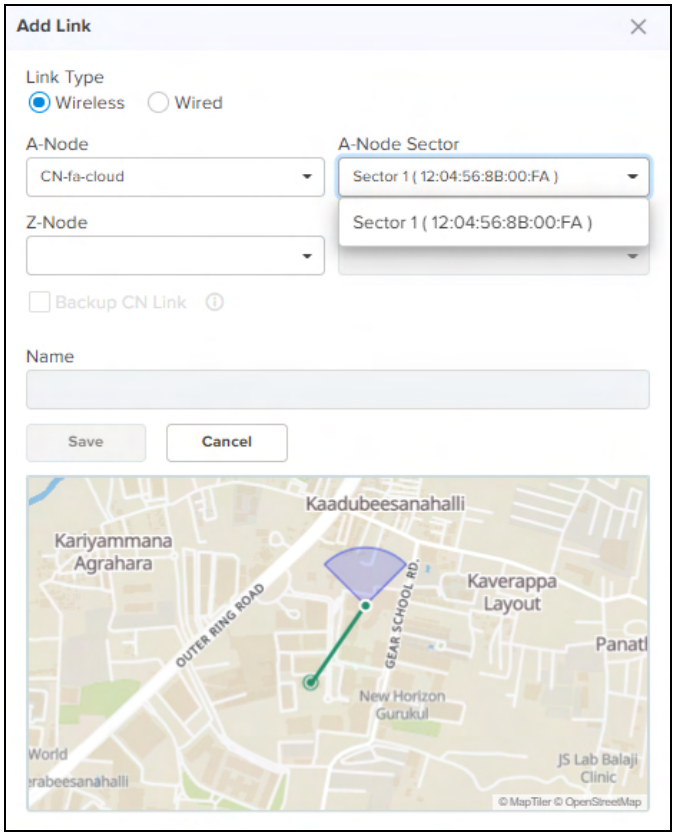
	NOTE: In Wired Link Type Sector will be disabled.



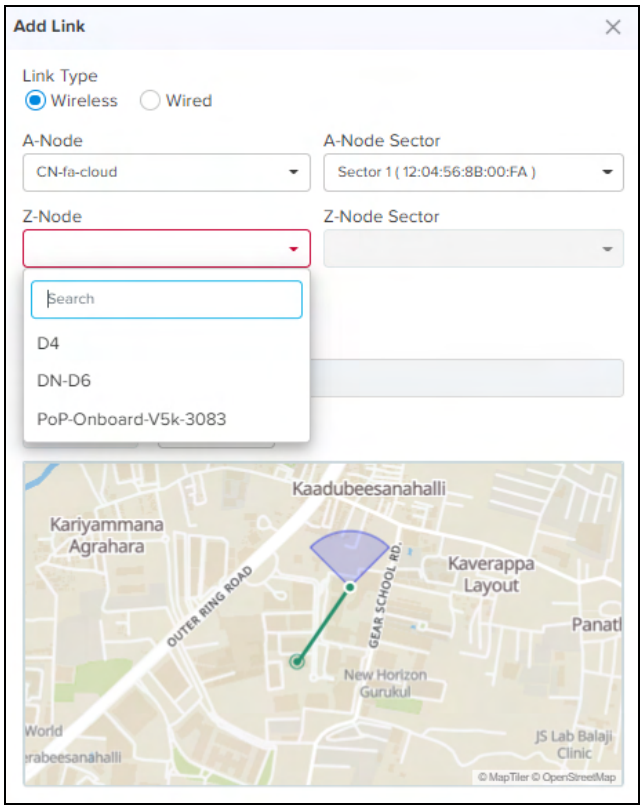
3. Select the **Node** from the drop-down in **A-Node.**



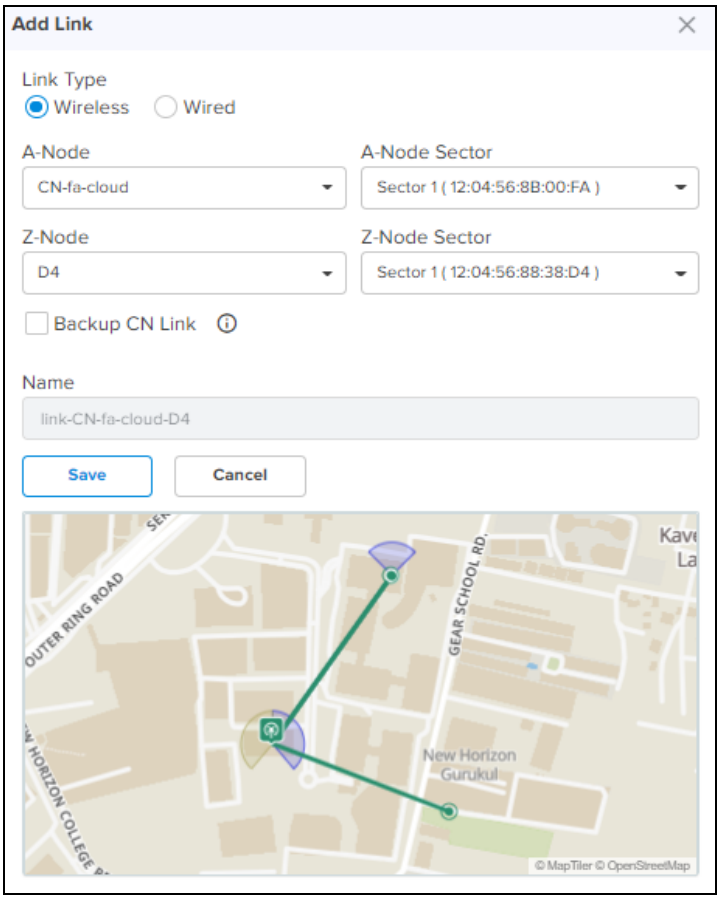
4. Select the **Sector** of the node from the drop-down in **A-Node Sector.**



5. Select the **Node** from the drop-down in **Z-Node.**



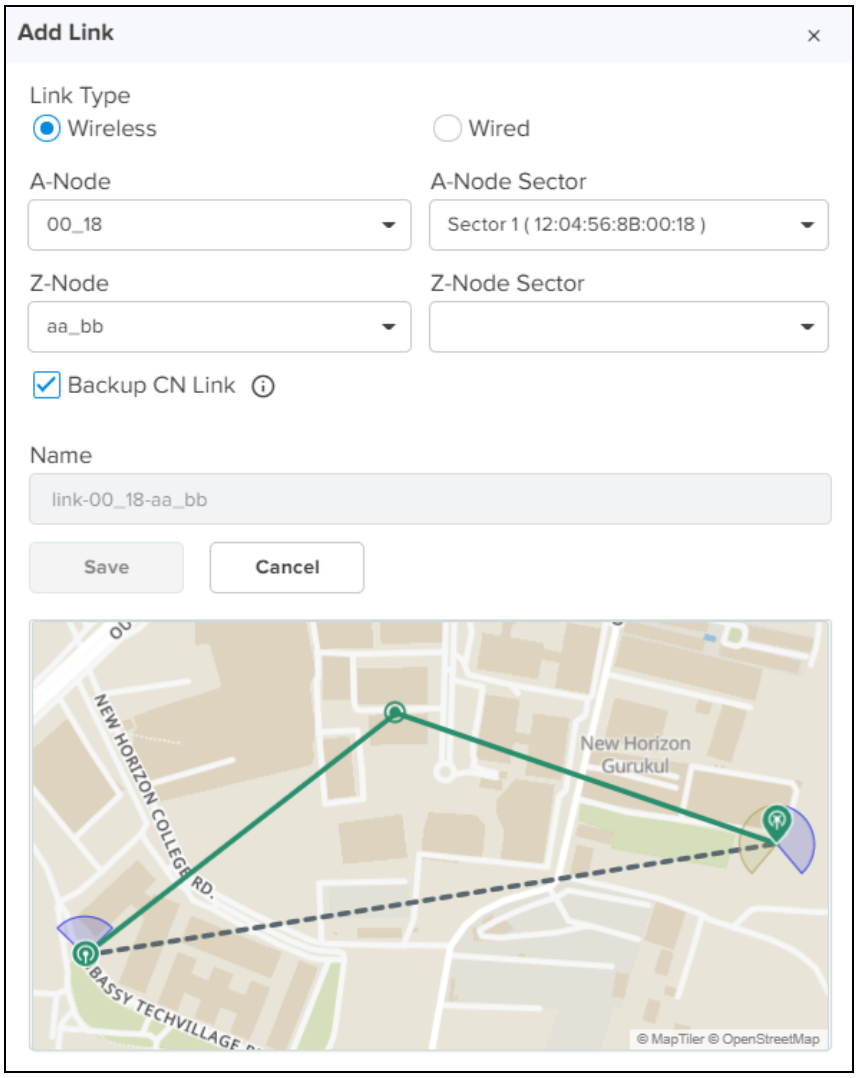
6. Select the **Sector** of the node from the drop-down in **Z-Node Sector.**



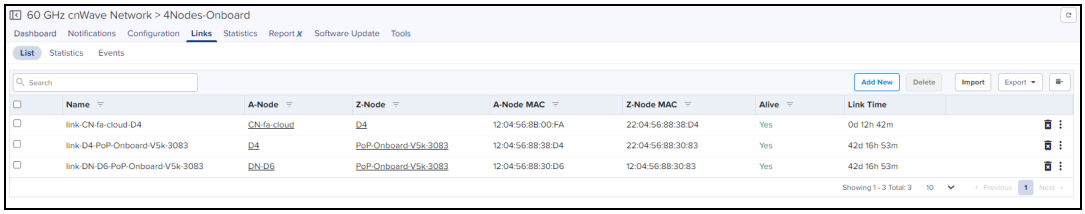
NOTE:

. Backup CN link is optional.

7. Enable the **Backup CN Link**.
   - If the link between PoP or DN and CN gets disconnected. This Backup CN link provides the backup connectivity from DN or PoP to particular CN.

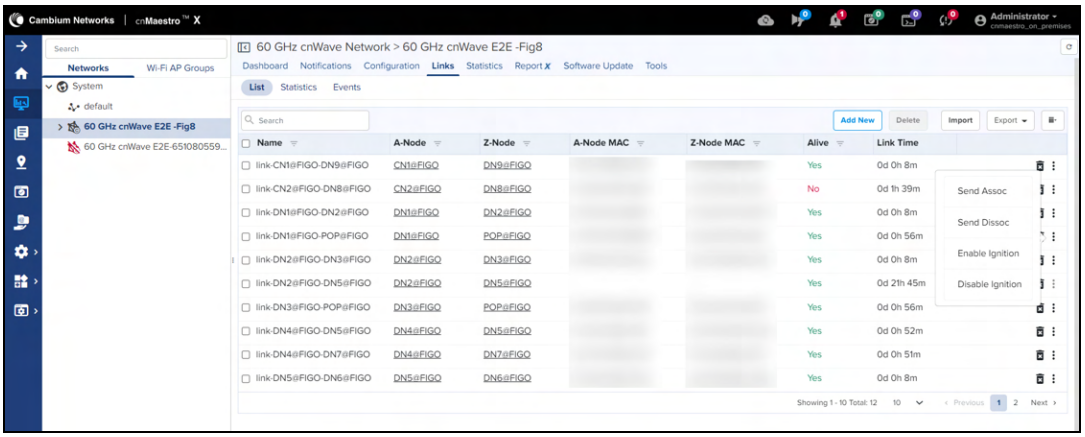


8. Click **Save**.
9. Once the link is successful it displays the **Alive** status as **Yes**.



Available link options are:

- Send Assoc
- Send Dissoc
- Enable Ignition
- Disable Ignition

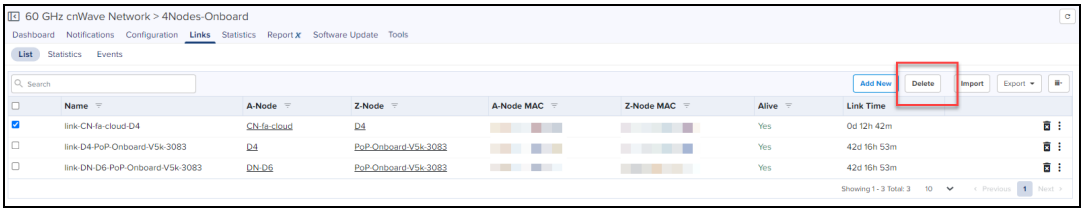


Delete Links

In **Links** tab you can delete the each individual links by clicking delete icon or multiple links can be deleted by selecting the links and click delete.

To delete the links:

1. Navigate to **Links** > **List.**
2. Select the links to delete.



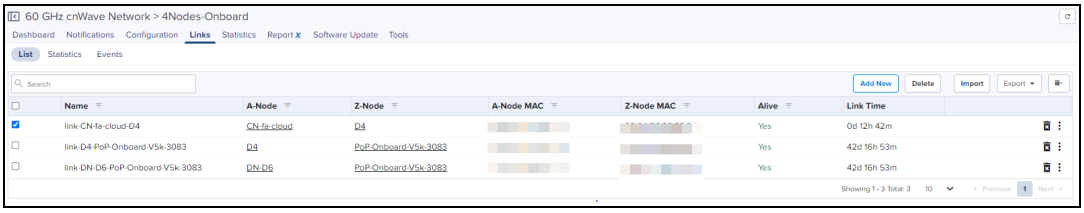
3. Click **Delete**.

Import Links

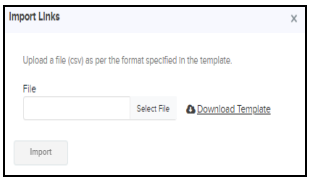
In **Links** tab you can import the E2E Controller Network Links.

To import the links:

1. Navigate to **Links > List.**
2. Select **Import.**



Import Links pops up.



3. Click **Download Template** to download the .CSV format file.

	A	B	C	D	E
1	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of the device	Sector 1/2 MAC Address	Z node name of the device	Sector 1/2 MAC Address	Wireless or Wired
3	POP	12:04:56:44:55:66	DN1	22:04:56:33:44:55	wireless
4	DN1	12:04:56:33:44:55	CN1	12:04:56:11:22:33	wireless
5	DN1		CN2		wired
6					
7					

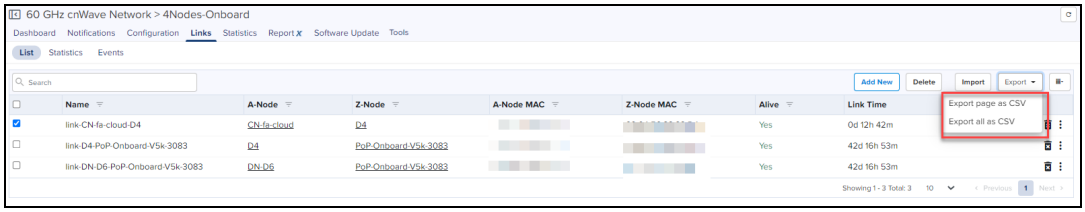
4. Select the file and click **Import**.

Export Links

In **Links** tab you can export the E2E Controller Network Links.

To export the links:

1. Navigate to **Links** > **List** > select **Export.**

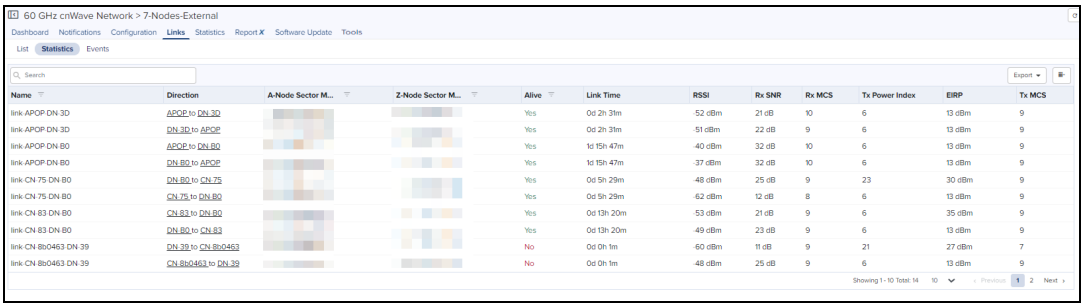


2. It exports .csv file format as shown below.

	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of t	Sector 1/2 MAC	Z node name of tl	Sector 1/2 MAC	Wireless or Wired
3	CN-2c	12:04:56:8B:00::	pop	12:04:56:AA:BB	Wireless
4	CN	12:04:56:AA:BC:	DN2	12:04:56:88:30:	Wireless
5	DN	22:04:56:AA:BB:	DN2	12:04:56:88:30:	Wireless
6	DN	12:04:56:AA:BB:	pop	22:04:56:AA:BB	Wireless
7	DN2	22:04:56:88:30:(	dn-44	12:04:56:88:31:	Wireless
8	DN2	22:04:56:88:30:(	v3000	12:04:56:88:30:	Wireless
9	dn-44	22:04:56:88:31:4	pop	12:04:56:AA:BB	Wireless

Statistics

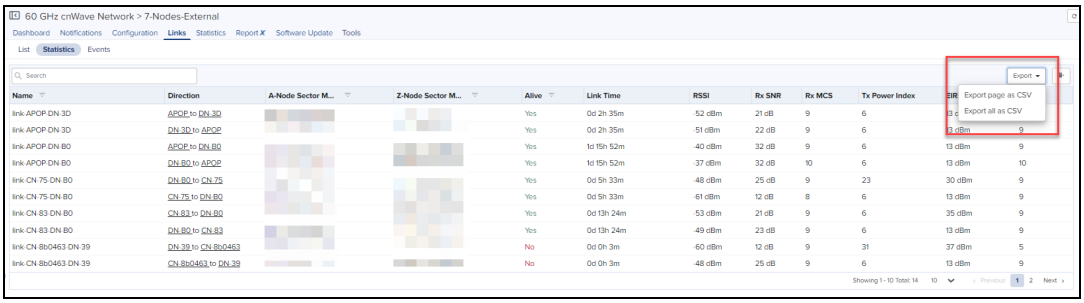
Links Statistics pages provides details of **Name, Direction, A-Node Sector MAC, Z-Node Sector MAC, Alive, Link Time, RSSI, Tx Power Index, A-node, Z-node, Type, Distance, Azimuth, Rx MCS, Tx MCS, Rx PER, Tx PER, Rx SNR, Rx Beam Index, Tx Beam Index, EIRP, Rx Errors, Tx Errors, Rx Frames, Tx Frames** on a single link of the node, generally in a page format.



Export Statistics

To export the Statistics :

1. Navigate to **Links > List >** > select **Export.**



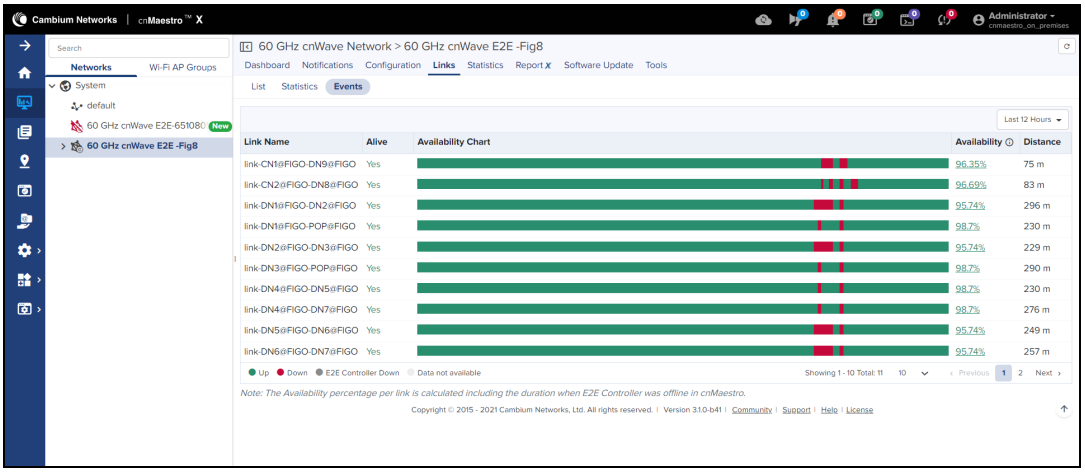
2. It exports .csv file format as shown below.

LINK_NAME	DIRECTION	A_NODE_I	Z_NODE_I	A_NODE_I	Z_NODE_I	ALIVE	TYPE	DISTANCE	AZIMUTH	RSSI	Rx_SNR	Rx_MCS	Rx_PER	Rx_BEAM	Tx_POWE	EIRP	Tx_MCS	Tx_PER	Tx_BEAM	Rx_ERROR	Rx_FRAME
link-APOP-DN-3D	APOP to DN-3D	APOP	DN-3D	22:04:56:8	12:04:56:8	Yes	Wireless	147	83	-52	21	9	0.17	64	6	13	10	0.19	64	290	20975
link-APOP-DN-3D	DN-3D to APOP	APOP	DN-3D	22:04:56:8	12:04:56:8	Yes	Wireless	147	83	-51	22	9	0.2	84	6	13	9	0.21	84	374	1488
link-APOP-DN-B0	APOP to DN-B0	APOP	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	94	-178.1	-40	32	9	0	32	6	13	9	0	35	92	30630
link-APOP-DN-B0	DN-B0 to APOP	APOP	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	94	-178.1	-37	32	10	0	0	6	13	10	0	0	1332	9183
link-CN-75-DN-B0	DN-B0 to CN-75	CN-75	DN-B0	12:04:56:8	12:04:56:8	Yes	Wireless	171	-151.2	-48	25	9	0.31	0	23	30	9	0.38	0	0	0
link-CN-75-DN-B0	CN-75 to DN-B(	CN-75	DN-B0	12:04:56:8	12:04:56:8	Yes	Wireless	171	-151.2	-61	12	8	0.42	0	6	13	9	0.35	0	1944	443425
link-CN-83-DN-B0	CN-83 to DN-B(	CN-83	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	71	52.7	-53	21	9	0.81	58	6	35	9	0.06	58	385	2043
link-CN-83-DN-B0	DN-B0 to CN-8:	CN-83	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	71	52.7	-49	23	9	0.04	112	6	13	9	0.08	112	0	339
link-CN-8b0463-D	DN-39 to CN-8b	CN-8b046	DN-39	12:04:56:8	22:04:56:8	No	Wireless	199	-45.2	-60	12	9	0	44	31	37	5	0.01	44	95	2856
link-CN-8b0463-D	CN-8b0463 to D	CN-8b046	DN-39	12:04:56:8	22:04:56:8	No	Wireless	199	-45.2	-48	25	9	0.04	45	6	13	9	0.56	45	54	62
link-DN-39-DN-3D	DN-39 to DN-3(	DN-39	DN-3D	12:04:56:8	22:04:56:8	Yes	Wireless	155	20.5	-40	32	9	0	15	6	13	9	0	24	23	504
link-DN-39-DN-3D	DN-3D to DN-3:	DN-39	DN-3D	12:04:56:8	22:04:56:8	Yes	Wireless	155	20.5	-43	30	9	0	0	6	13	10	0	0	164	232
link-DN-39-DN-B0	DN-B0 to DN-3:	DN-39	DN-B0	12:04:56:8	12:04:56:8	Yes	Wireless	100	-70.5	-45	28	9	0.06	35	6	13	9	0.02	34	73	567
link-DN-39-DN-B0	DN-39 to DN-B(	DN-39	DN-B0	22:04:56:8	12:04:56:8	Yes	Wireless	100	-70.5	-48	25	9	0.3	55	6	13	10	0.01	54	331	303

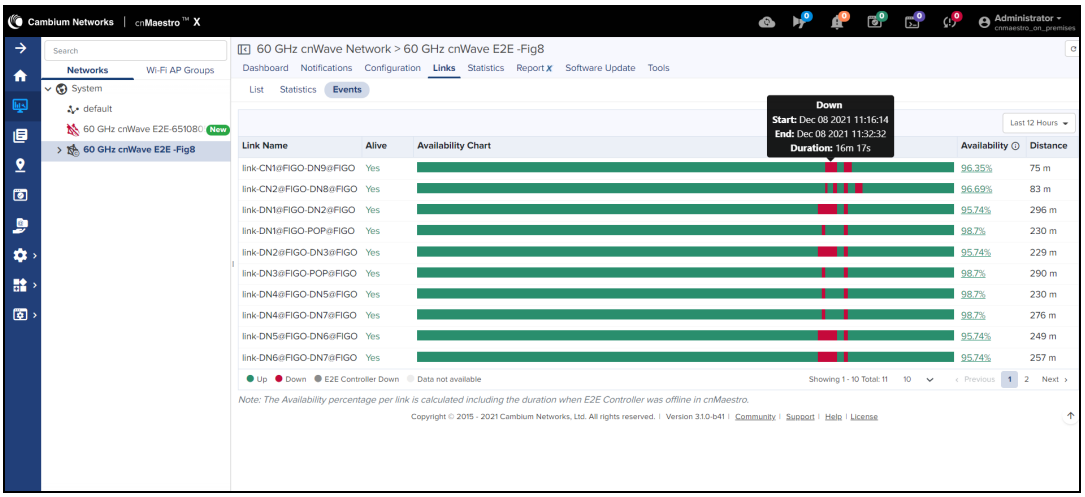
Events

Events provides the details of links availability and health from last 1 hour to 7 Days Period.

Figure 96 Links Events



It also calculates the Availability percentage per link, including the duration when E2E Controller was offline in cnMaestro.



Statistics

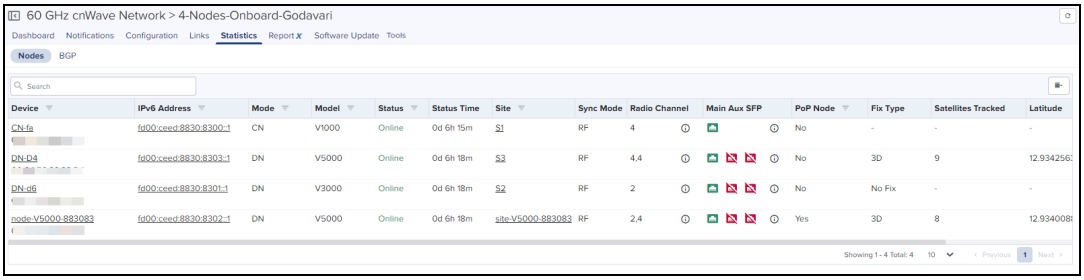
E2E Controller Statistics provides the following details:

- Nodes Statistics
- BGP

Nodes Statistics

Nodes provide a tabular aggregation of data, including General information on the nodes monitored, as well as Wireless, Network, and Traffic metrics. Node Statistics pages provide information of **Device, IPv6 Address, Mode, Model, Status, Status Time, Site, Radio channel, Main Aux SFP, PoP Node, Software Version, Serial Number, Sync Mode, Zone, Fix Type, Satellites Tracked, Latitude, Longitude, and Height** on a single device, generally in a page format.

Figure 97 Nodes Statistics

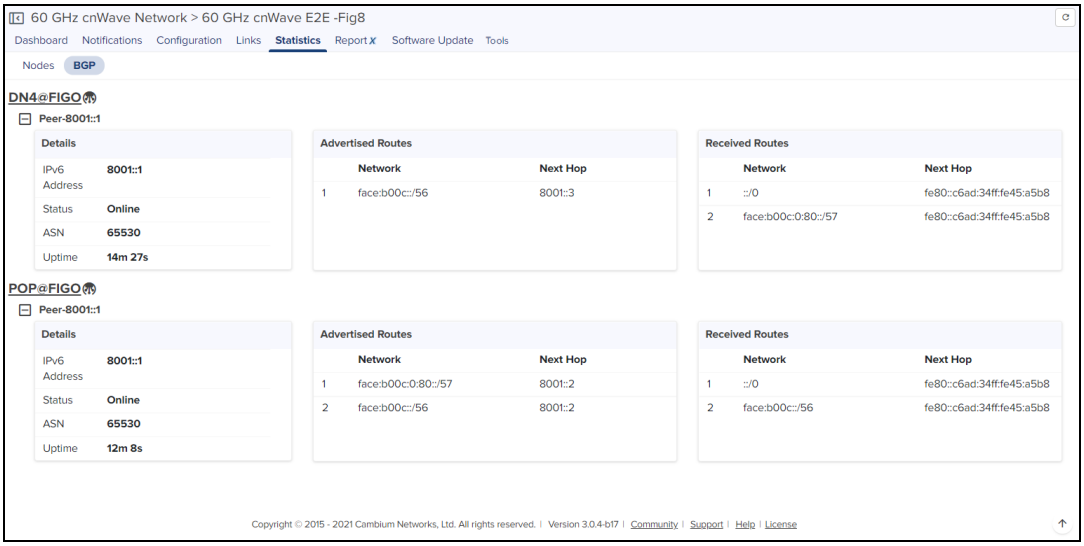


BGP

> **NOTE:**
>
> BGP statistics displays only if BGP option is enabled in Routing in PoP configuration.

BGP provides the details of **Advertised Routes, Received Routes,** and **Details of IPv6 Address.**

Figure 98 BGP



Reports

Reports page provides details on how to schedule and generate different types of data reports such as Devices, Active Alarms, Alarm History and Events. For further details, refer to Reports.

Software Update

Allows the user to update with the latest device software.

To update the software, perform the below steps:

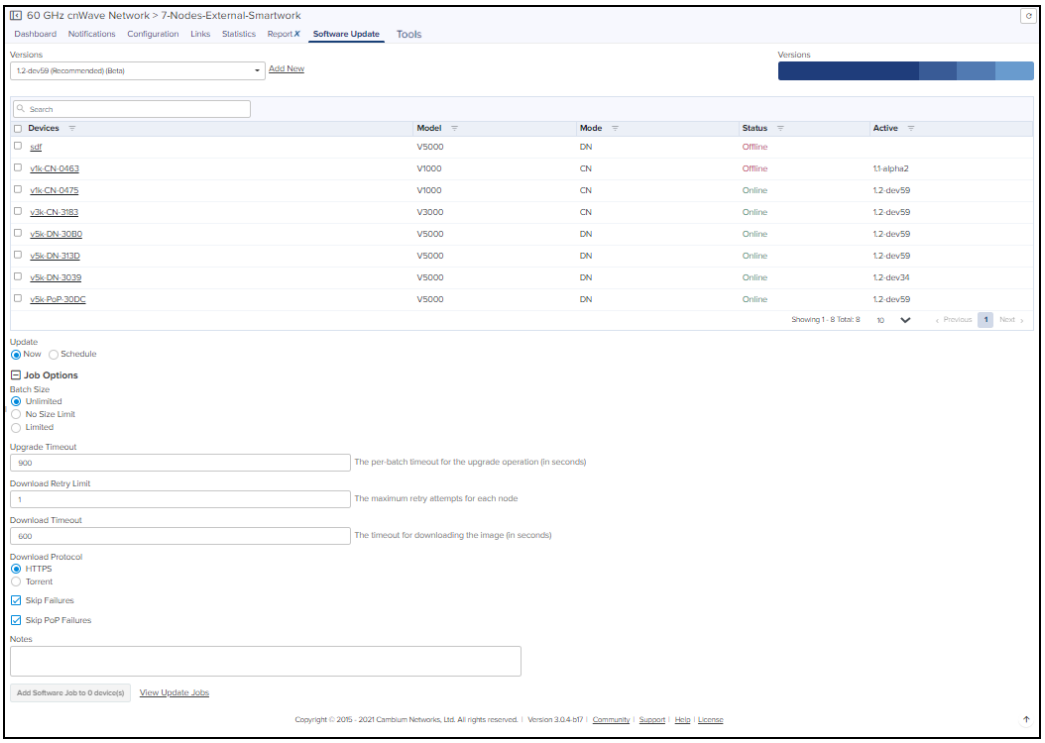
1. Select the **Network** and navigate to the **Software Update** tab.
2. In **Software Update** tab select the desired Versions from drop-down in **Versions** tab.
3. Select the **Device(s)** for the software update.
4. Click **Update Now** or **Schedule**.
5. In **Job options**:

    - Select type of **Batch Size** as Unlimited, No Size Limit, or Limited.
    - Enter **Upgrade Timeout.**
    - Enter **Download Retry Limit.**
    - Enter **Download Timeout.**
    - Select the Download Protocol as **HTTPS** or **Torrent.**

    > **NOTE:**
    >
    > If E2E Controller version is 1.2 or above, HTTPS or Torrent options will be available.

    - Enable the **Skip Failures** or **PoP Failures**.

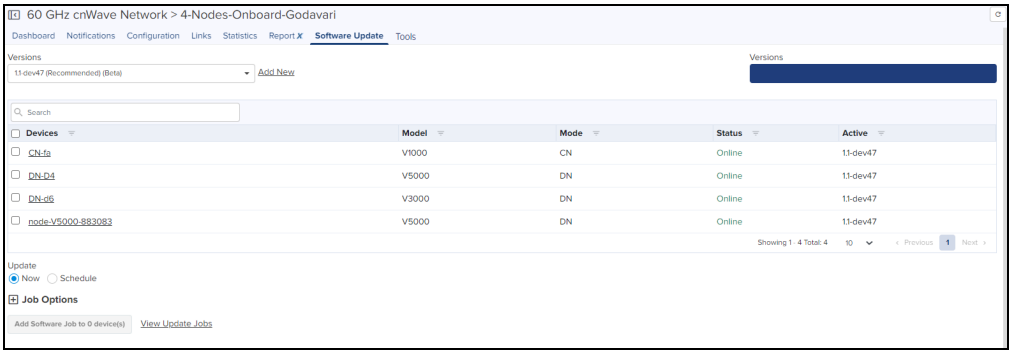
6. Click **Add Software Job to device.**



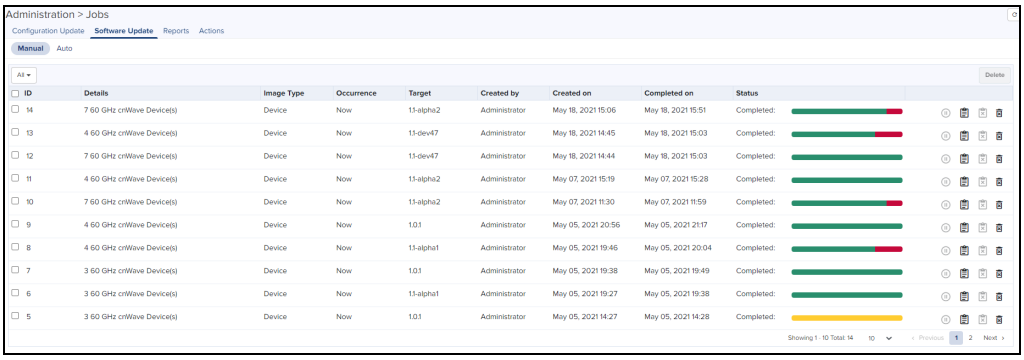
> **NOTE:**
> Onboard E2E controller will support only one synced software image. If user needs to sync another image, select the image from **Versions** drop down and click **Sync Selected Image.**

View Update Jobs

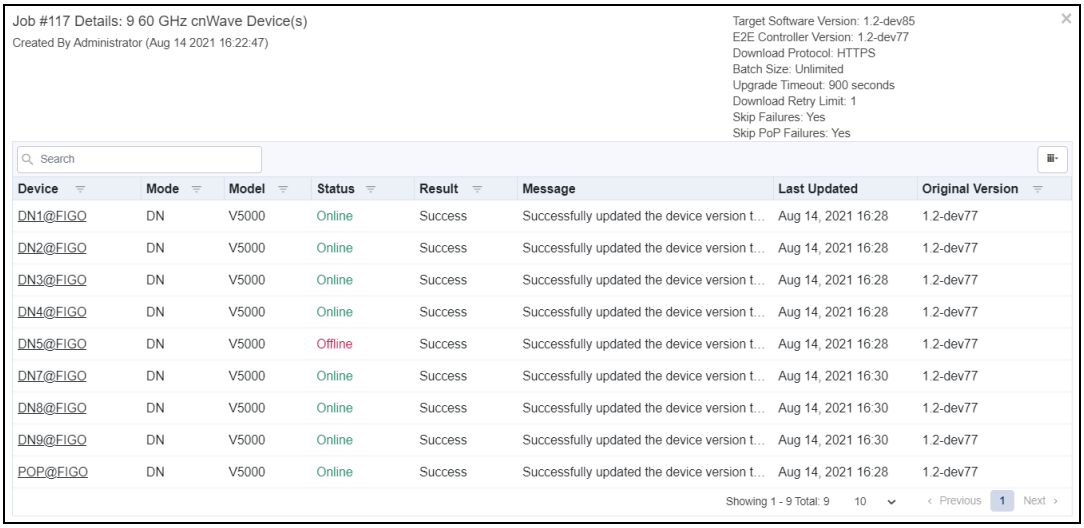
After adding the new Software Images, click **View Update Jobs.**



1. Navigate to the **Administration > Jobs > Software Update**.

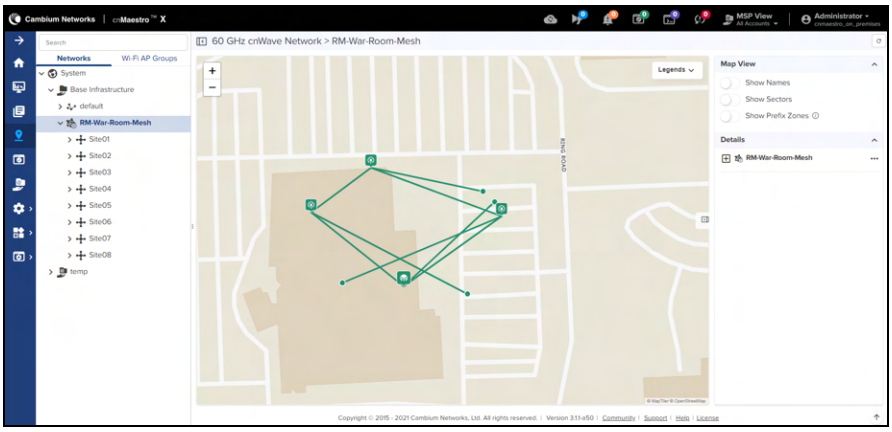


2. Click **Show More** to view the Job Details.

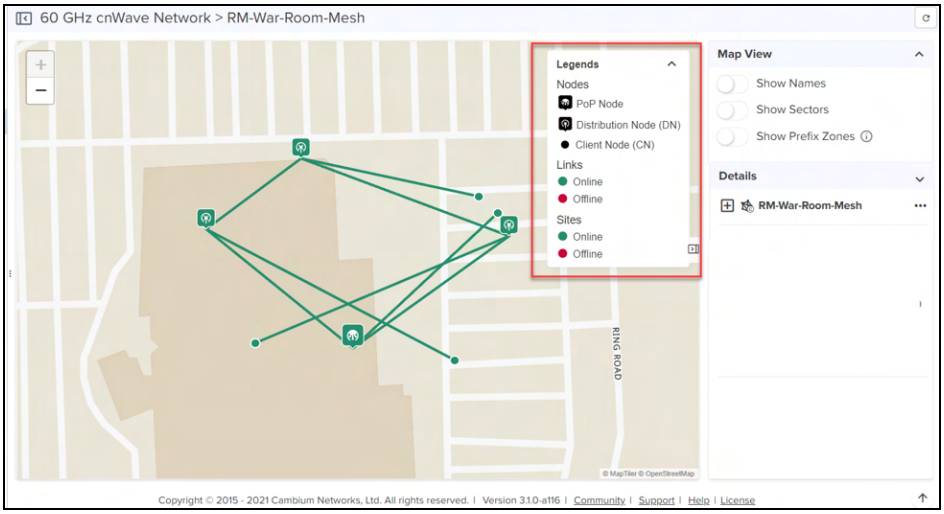


Map

User can view E2E Network and the 60 GHz cnWave devices in Map as shown below. Navigate to E2E Network and then select Map from left pane to view 60 GHz cnWave devices.



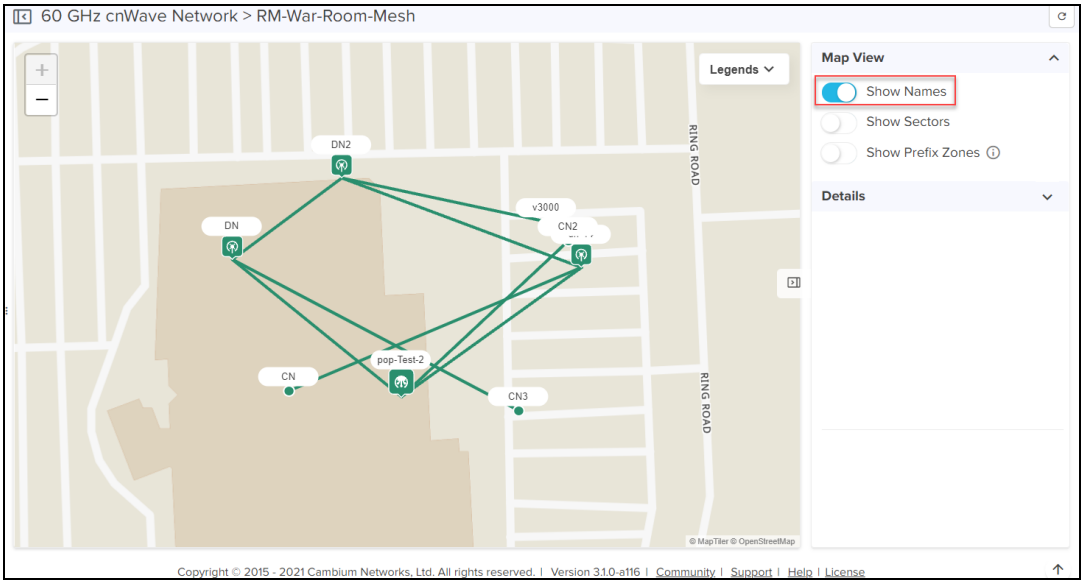
Click down arrow next to **Legends** to view the map legend.



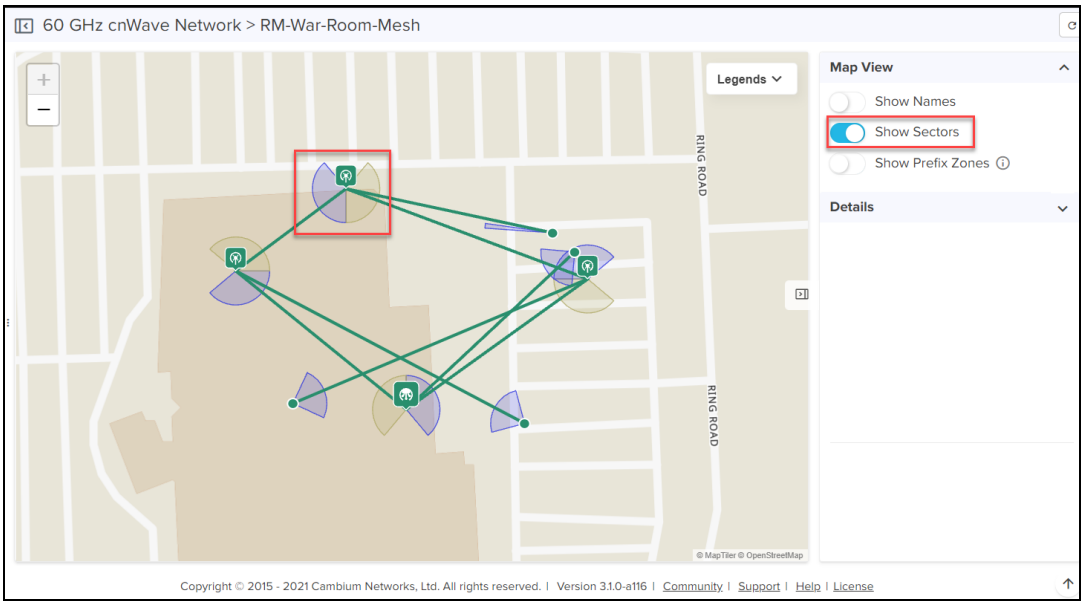
Map View

Map is viewed by **Names**, **Sectors**, and **Prefix Zones**. For **Map View** slide the button next to the field name as shown below.

- **Show Names** - shows the name of the nodes in the network.



- **Show Sectors** - shows the basic sector visualization of the nodes in the network.

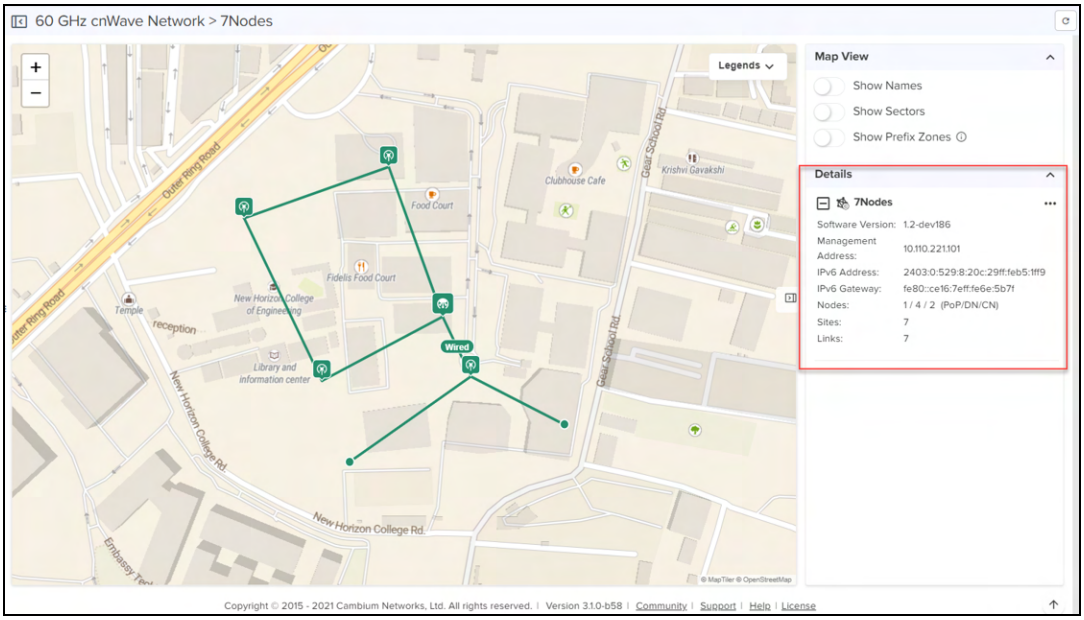


- **Show Prefix Zones** - shows the prefix zone of each PoP communicating with each other.

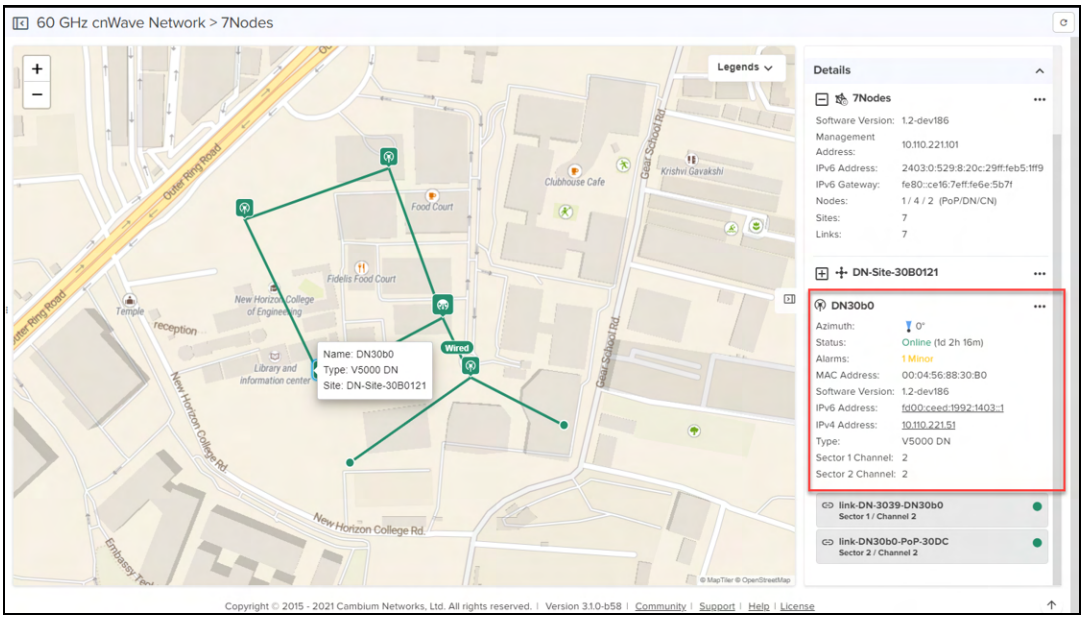
	NOTE: **Show Prefix Zones** is enabled only if **Prefix Allocation** is set to **Deterministic**.

E2E Network Details

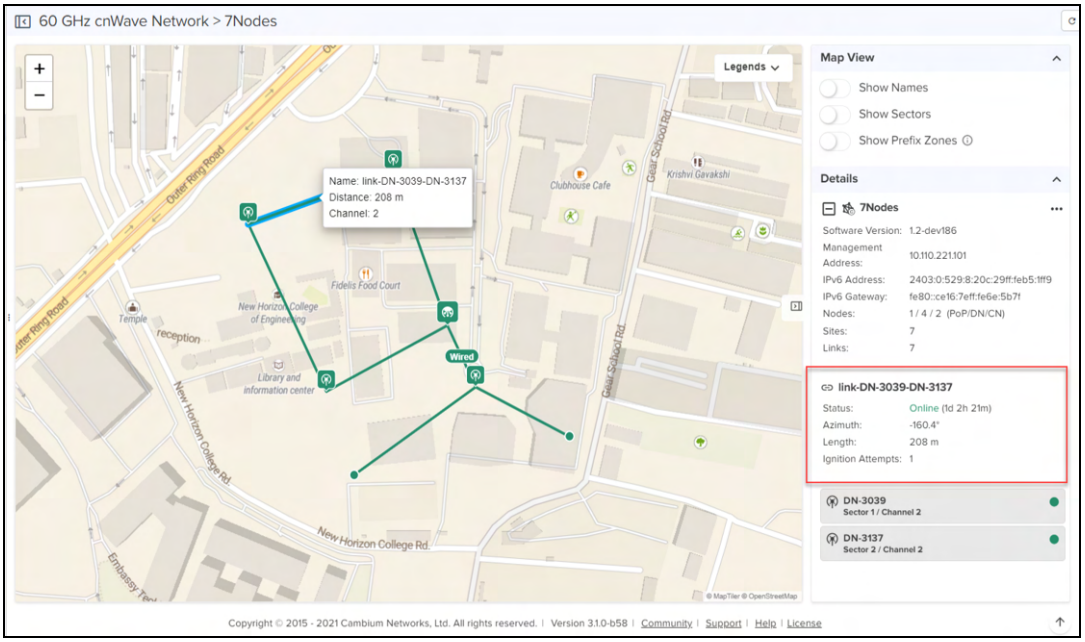
Click the down arrow next to **Details** to view E2E Network details in map. The following E2E Network details is as shown below.



Hover the cursor on the node, you can view the node **Name**, **Type**, and **Site**. Node details is shown when node is selected in the map. Node details is also shown in the right pane as shown below:



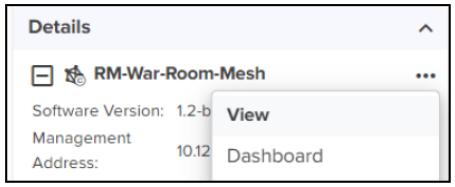
Hover the cursor on the links connected to the node, you can view the link **Name**, **Distance** and **Channel.** Link details is shown when link line in the map is selected**.** Link details is shown in the right pane as shown below:



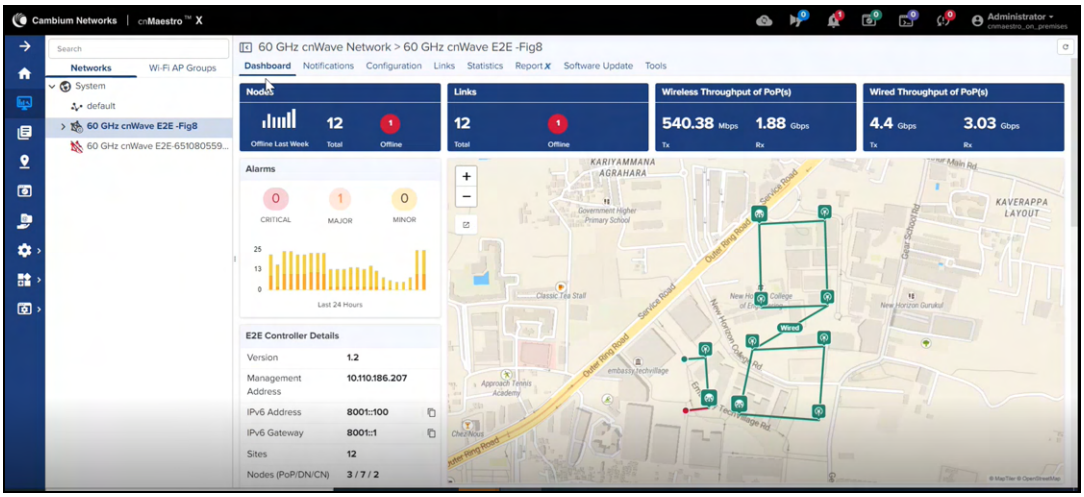
Links connected to nodes are represented in colors depending on the status of the link Green when Online or Red when Offline.

E2E Network Dashboard

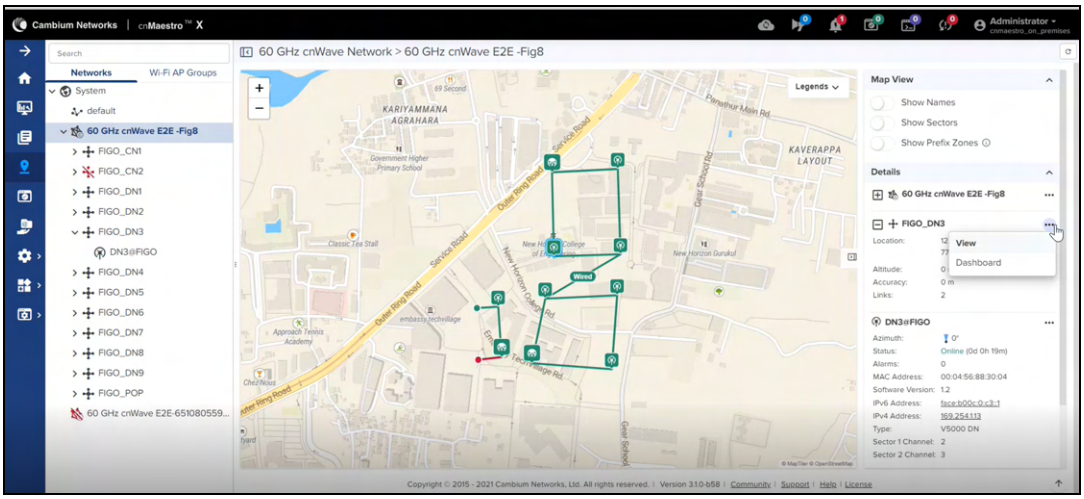
To view Dashboard of E2E Network click ••• next to E2E Network in the right pane as shown below.



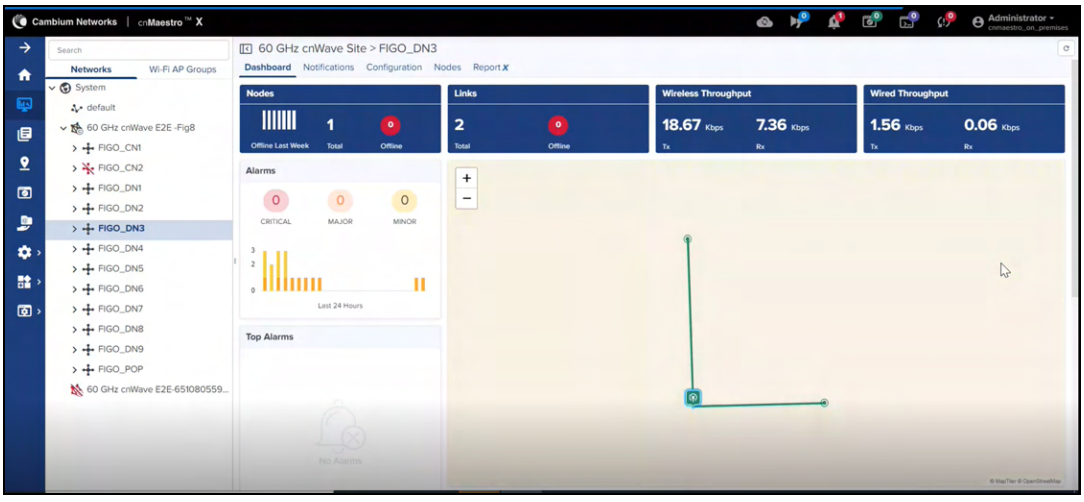
You will be directed to the 60 GHz cnWave Network Dashboard as shown below.



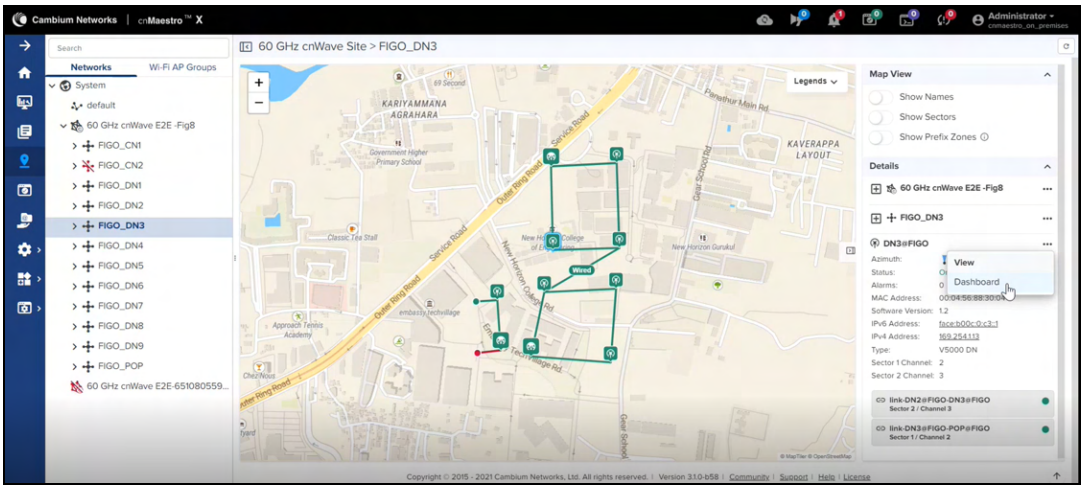
To view Dashboard of Site click ••• next to Site in the right panel as shown below.



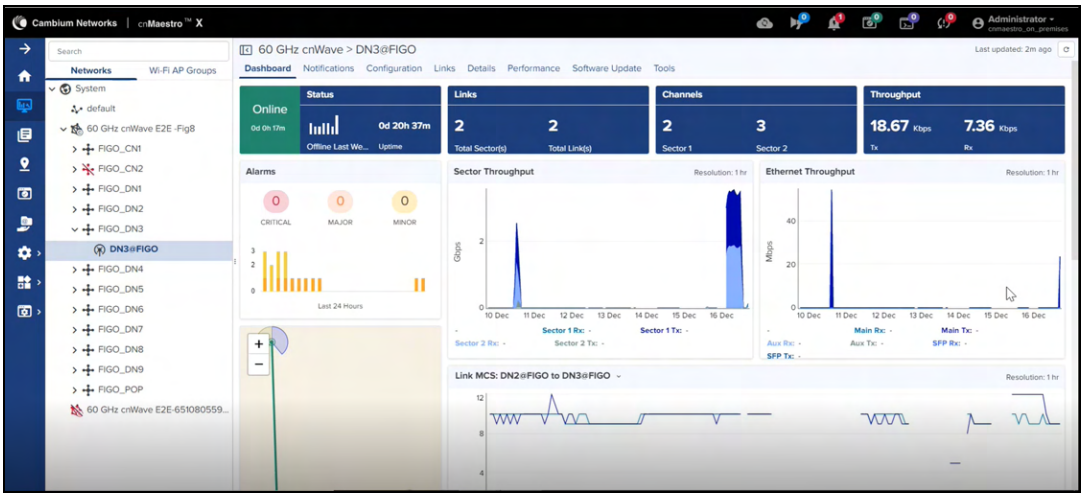
You will be directed to the 60 GHz cnWave Site Dashboard as shown below.



To view Dashboard of Device click ••• next to Device in the right pane as shown below.



You will be directed to the 60 GHz cnWave Device Dashboard as shown below.



Tools

In Tools page it allows the user to perform the following actions:

- Operations
- Diagnostics
- Debug
- Remote Command
- Services
- Settings

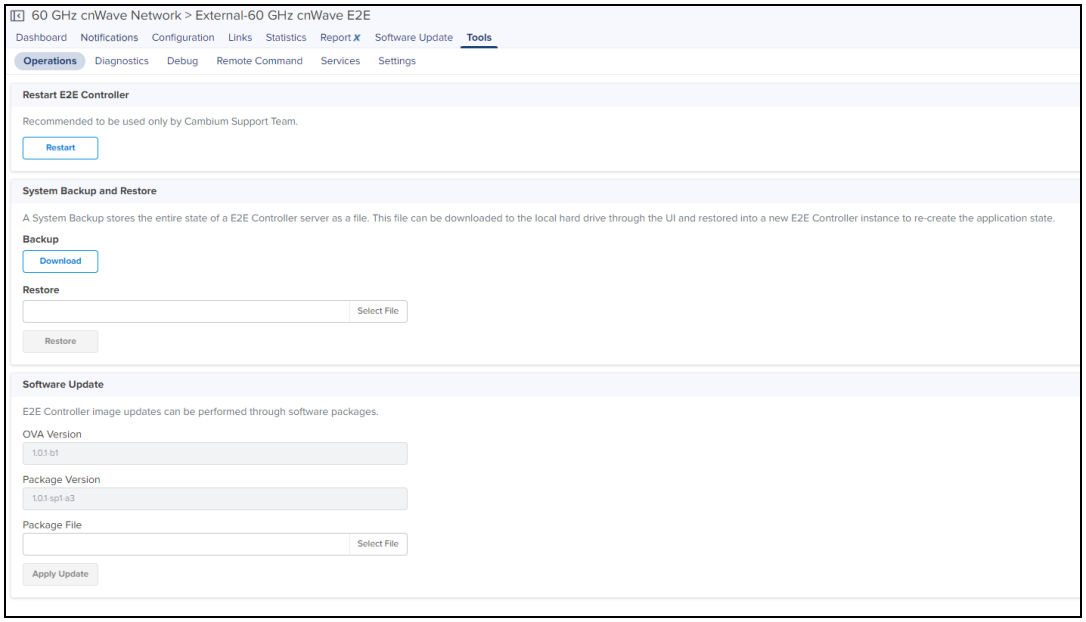
Operations

External E2E Controller deployment

If the nodes are deployed through **External E2E Controller** it displays the operations page as follows:

- **Restart E2E Controller** performs the **Restart.**
- A **System Backup and Restore** the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create.

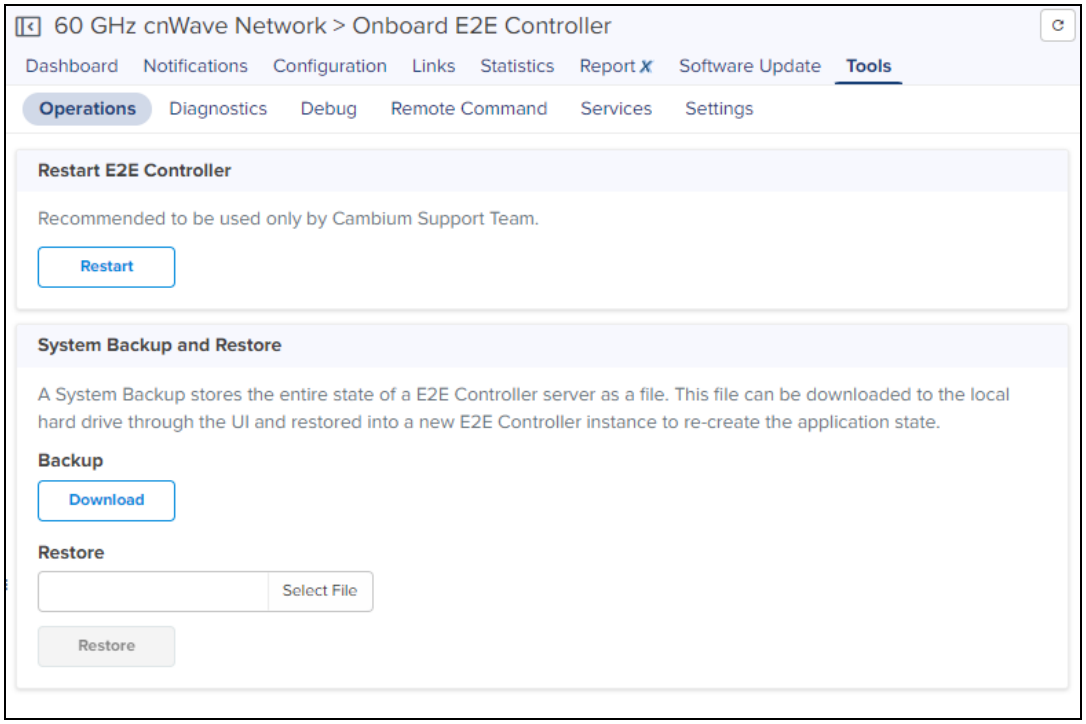
- The **Software Upgrade** is to upgrade E2E controller and can be done through E2E controller package.



Onboard E2E Controller deployment

If the nodes are running **Onboard E2E Controller** it displays the operations page as follows:

- **Restart E2E Controller** performs the **Restart.**
- A **System Backup and Restore** the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create.

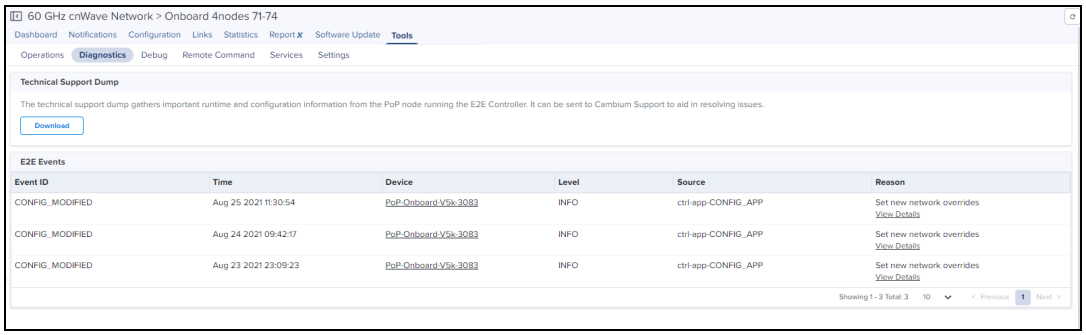


Diagnostics

Diagnostics page allows the user to gather **Technical Support Dump** and can be downloaded and sent to cambium support team.

All the events information of E2E controller can be viewed under E2E Events. In **E2E Events** tab user can view the **Event ID, Time, Device, Level, Source** and **Reason** of the E2E Network.

Figure 99 Diagnostics



Debug

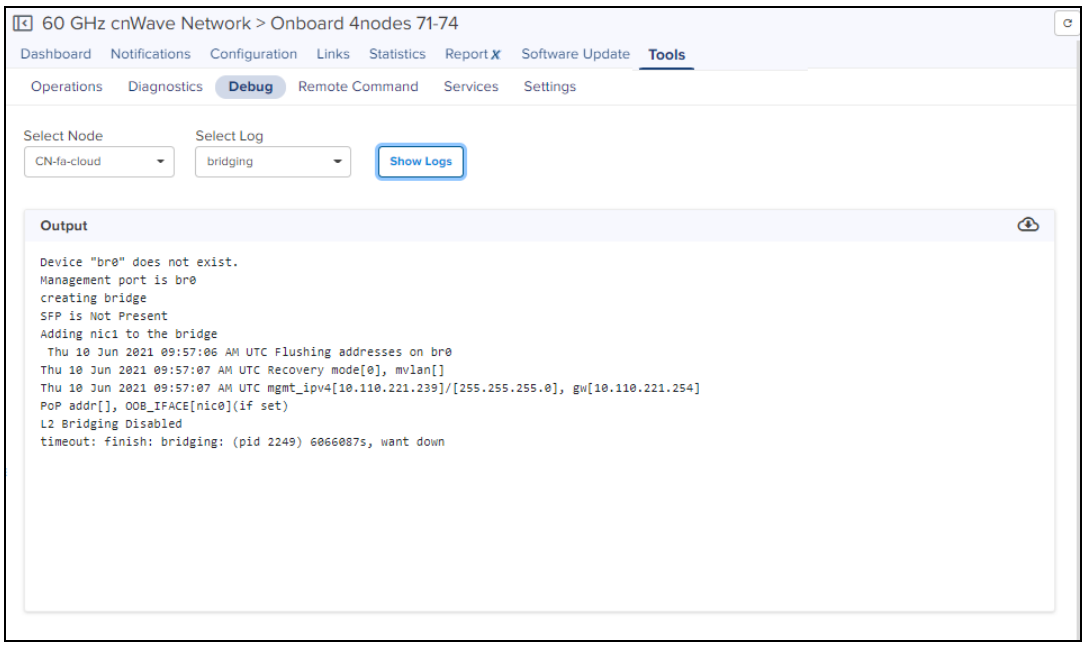
In **Debug** tab user can able to view or download the Node logs by executing the following log:

- bridging
- pop_config
- e2e_minion
- openr
- exabgp

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select a node name from the **Select Node** drop-down list box.
3. Select the required log name from the **Select Log** drop-down list box.
4. Click **Show Logs.**

The output for the selected criteria appears as shown:



- Click the download icon to download the generated output.

Remote Command

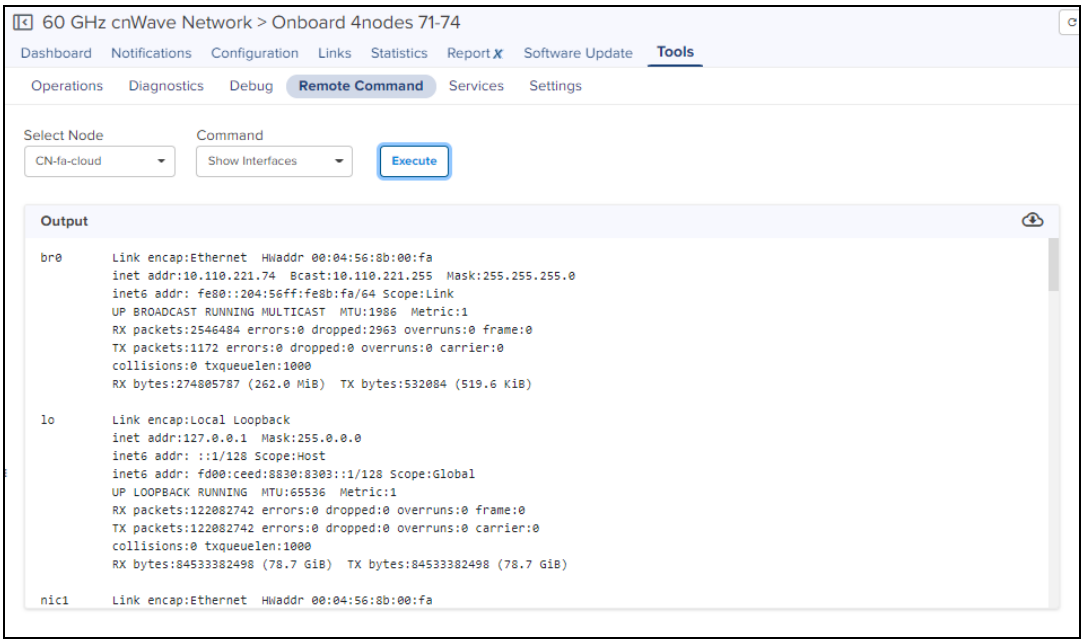
In **Remote command** tab user can able to view or download Command logs by executing the following command:

- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 and V3000)

To Execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select a node name from the **Select Node** drop-down list box.
3. Select the required command from the **Command** drop-down list box.
4. Click **Execute.**

The output for the selected criteria appears as shown:

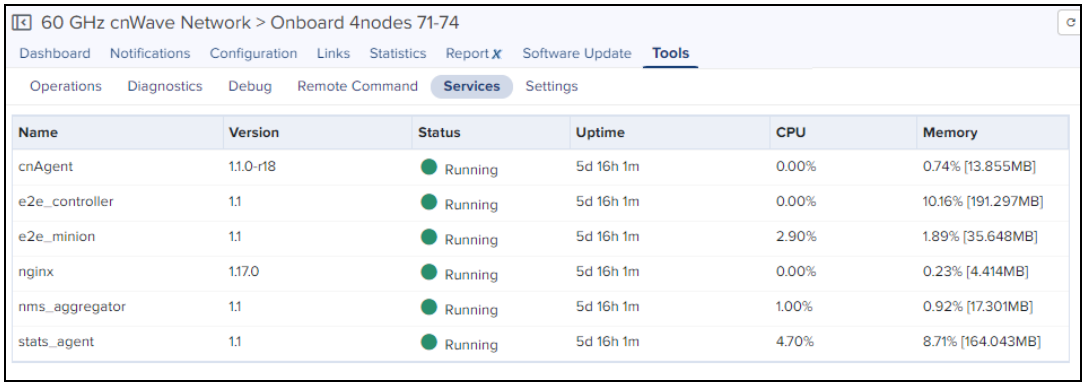


- Click the download icon to download the generated output.

Services

In **Services** page user can view the services running in E2E Controller.

Figure 100 Services

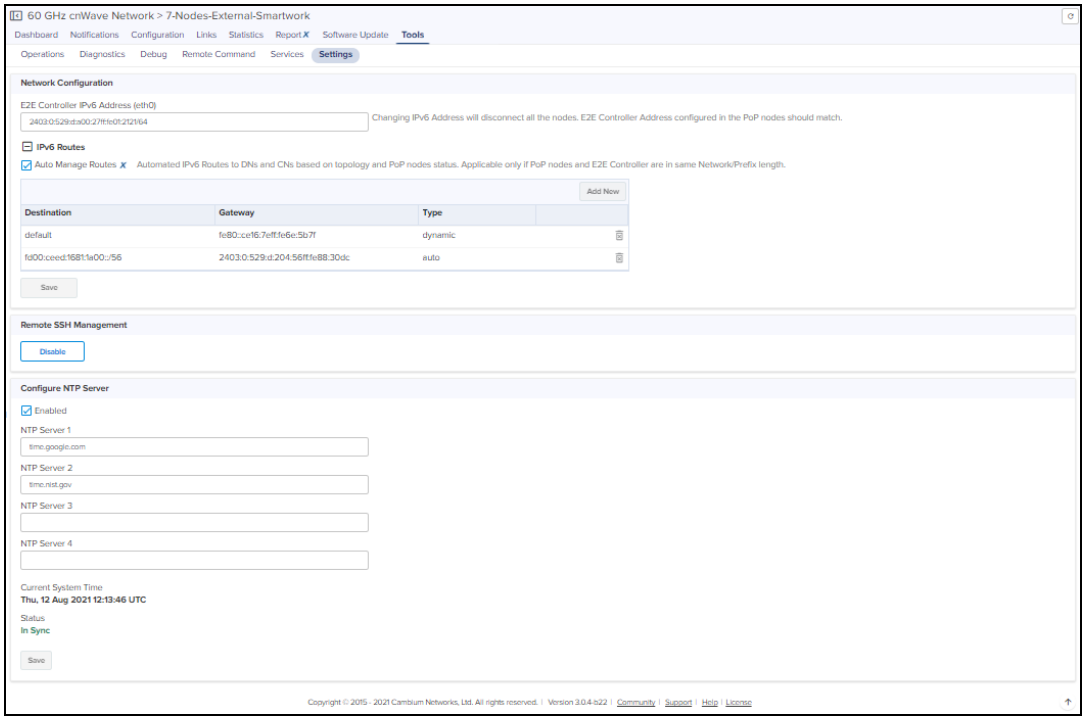


Settings

	NOTE: E2E Settings are not applicable for Onboard E2E Controller deployment.

External E2E Controller deployment

In **External E2E Controller Settings** page you can configure the **Network Configuration, IPv6 Routes, Remote SSH Management,** and **NTP Server**.



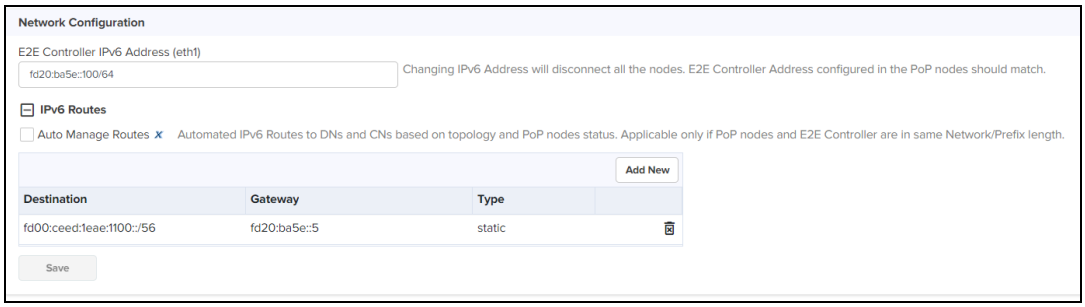
In **Network Configuration** user can configure the **E2E Controller IPv6 Address** and **IPv6 Routes**.

	NOTE: Auto Manage Routes supports only for the cnMaestro X feature.

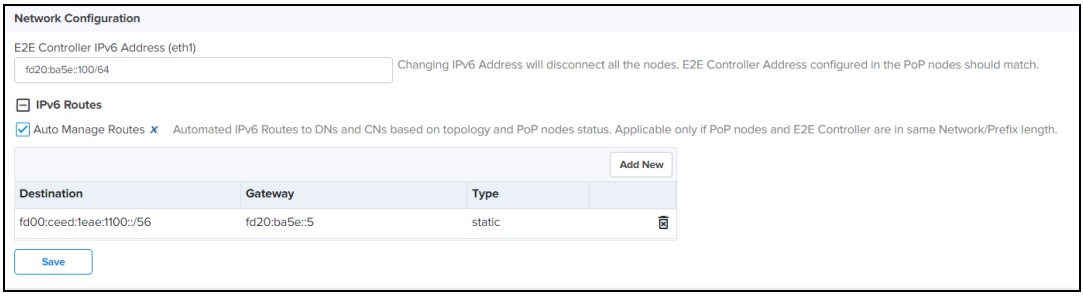
User can also enable the **Auto Manage Routes**. This automates IPv6 Routes to DNs and CNs based on the topology and PoP nodes status. It is applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

To Enable **Auto-Managed Routes:**

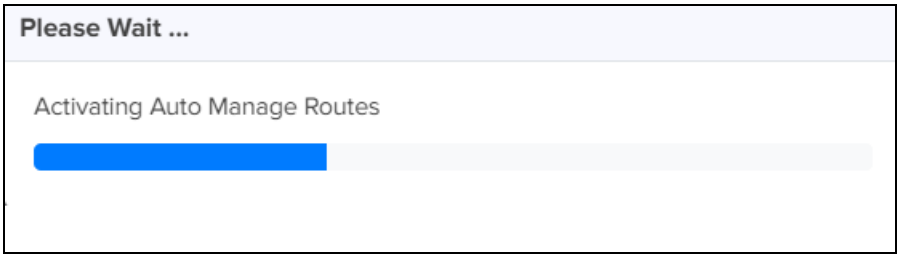
1. Navigate to **Tools > Settings > IPv6 Routes** tab.



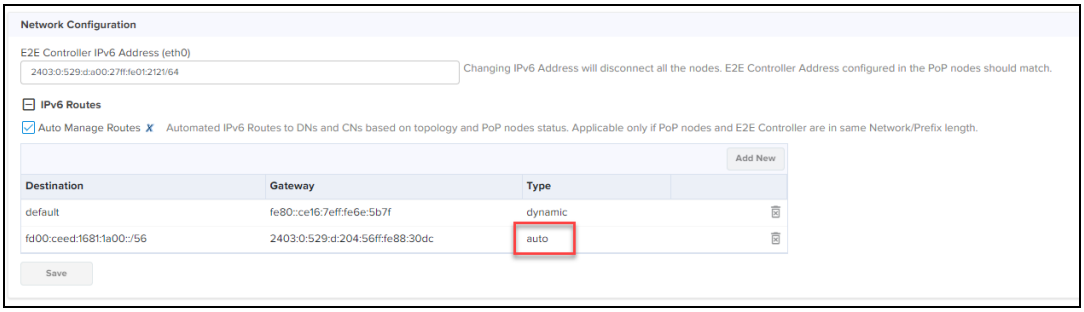
2. Enable **Auto-Managed Routes.**



3. Click **Save**.
4. **Please Wait** window pops-up.



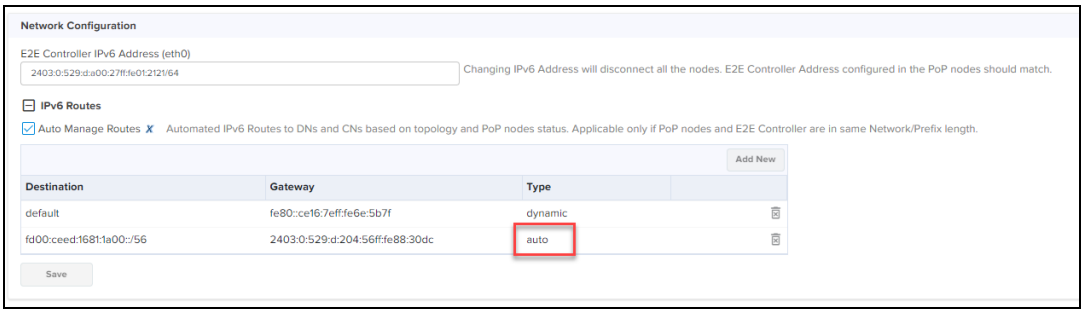
If IPv6 routes is managed through auto manage routes in type it displays as **Auto**.



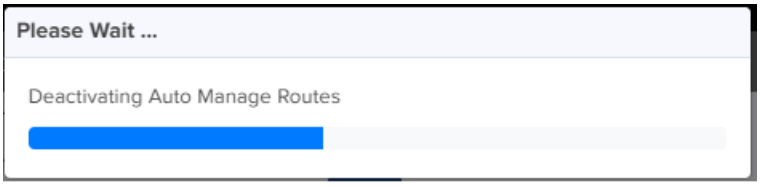
If cnMaestro X account is downgraded to Essential or if Auto Manage Routes is disabled. User can retain auto-managed routes of IPv6.

To Retain Auto-Managed Routes:

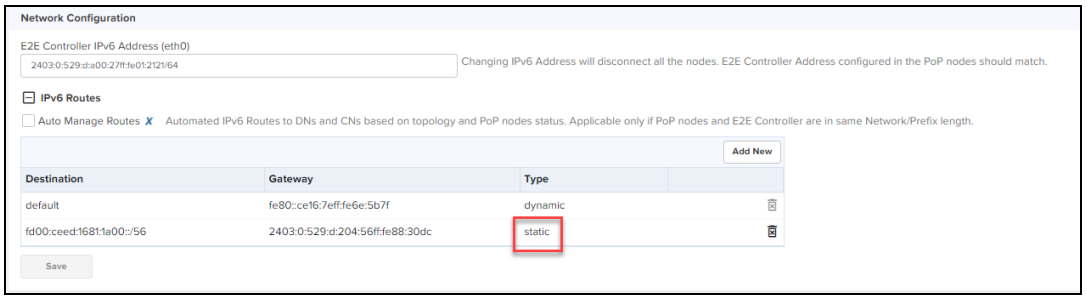
1. Navigate to **Tools > Settings > IPv6 Routes** tab.



2. Enable **Retain Auto-Managed Routes.**
3. Click **Save**.
4. Please wait pops-up.



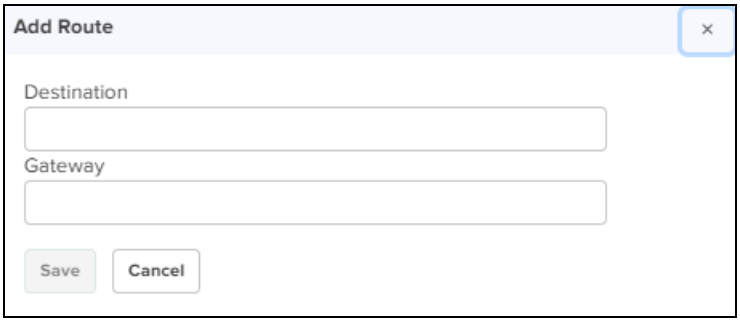
Once the Auto Manage Routes is disabled, IPv6 routes can be managed through static routes and in type it displays as **Static**.



5. Enter the **IPv6 Interface.**
6. Click **Save**.

To add new **Static Routes**:

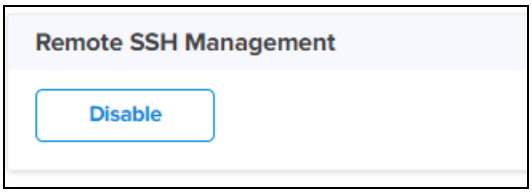
1. Click **Add New**.



2. Enter **Destination** and **Gateway**.
3. Click **Save.**

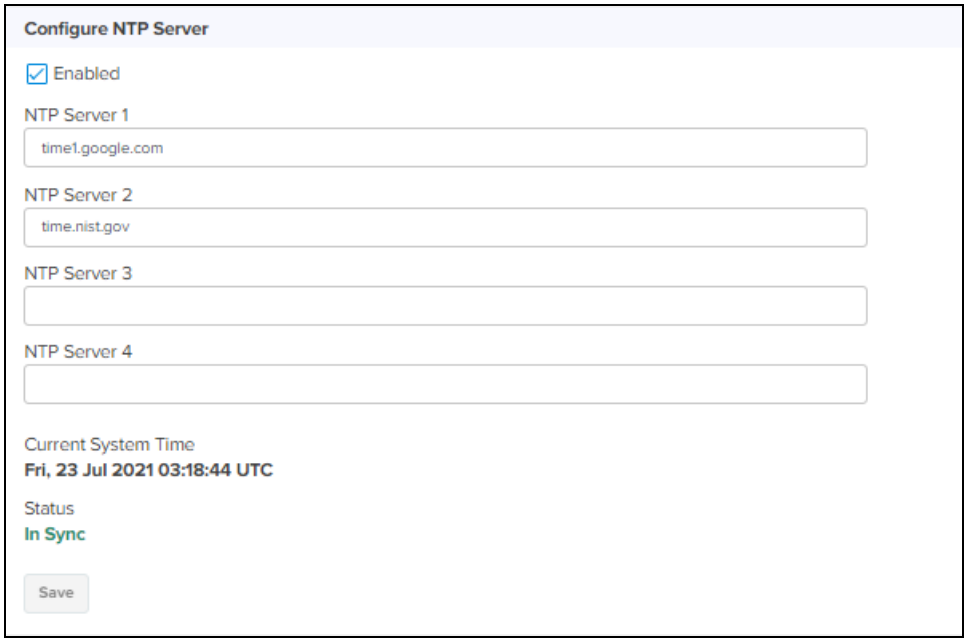
The user can configure the **NTP Settings** to configure the time configuration of the server with hostname or IP address.

Remote SSH Management allows the user to **Enable** and **Disable** Remote SSH Management.



To configure the NTP server:

1. Navigate to **Tools** > **Settings** > **NTP Settings** tab.
2. Enable the **NTP Settings**.
3. Enter **Host Name** or **IP Address**. It displays **Current System Time** and **Status** of the server.

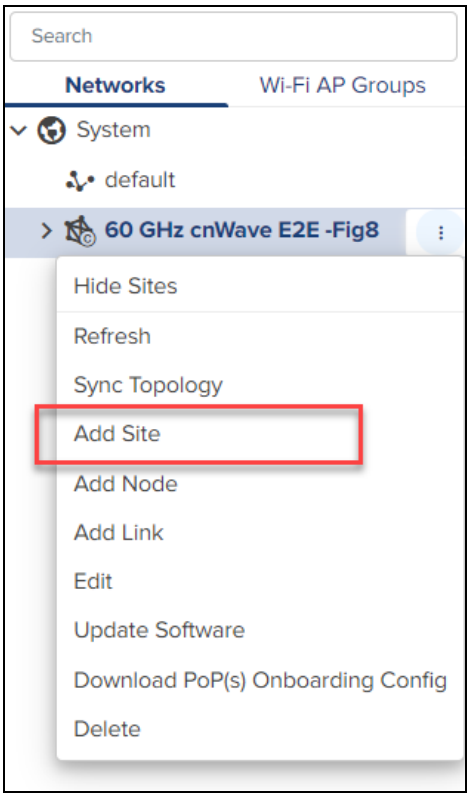


Site Configuration

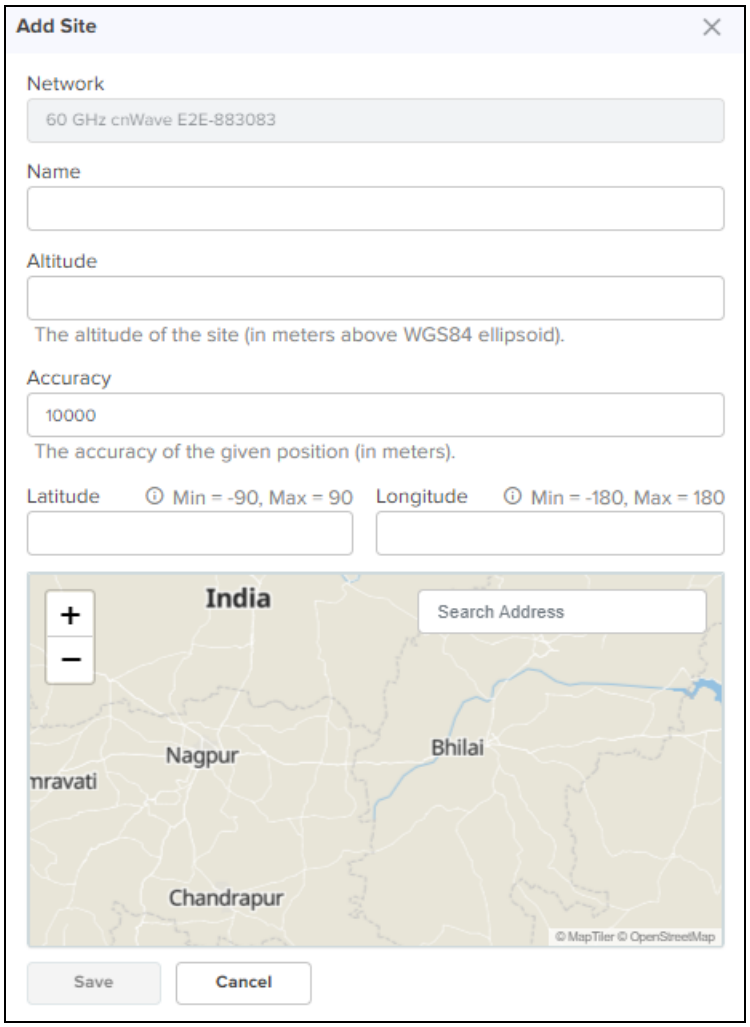
Sites are located within the networks and wireless access points attached to it.

To Add a Site

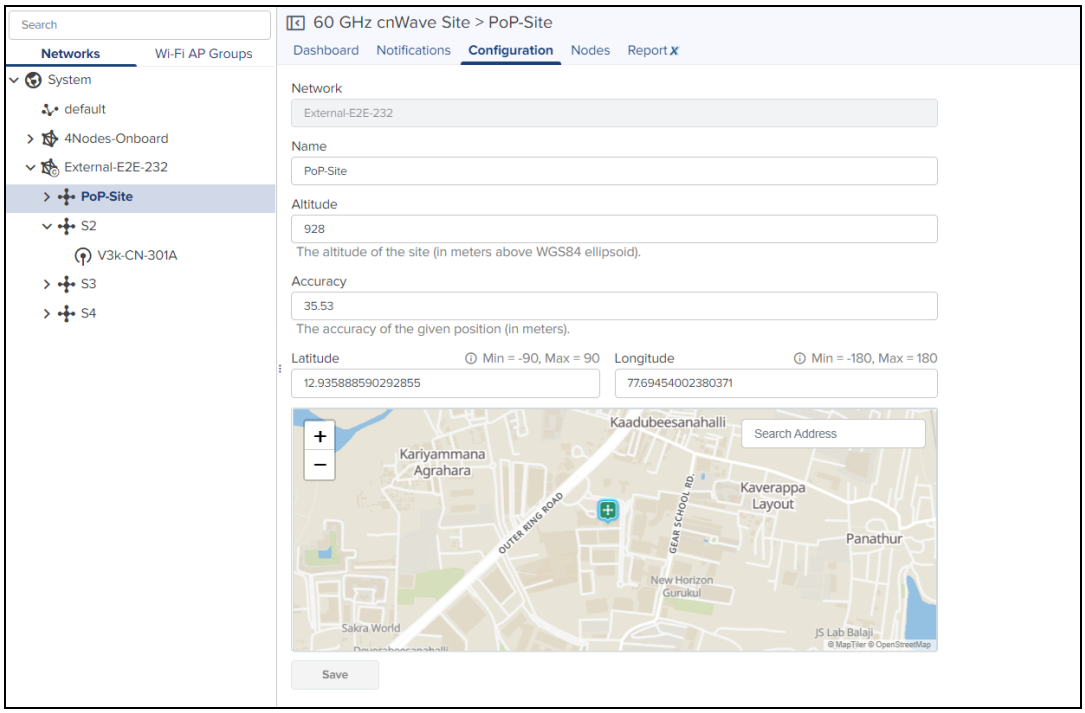
1. Navigate to **Network** and click the icon ⋮.
2. Select **Add Site** from the drop-down.



3. Enter the **Name**, **Altitude**, and **Accuracy.**
4. Once the address is entered in the Map, **Latitude** and **Longitude** gets fetched automatically. You can also enter the details Manually.

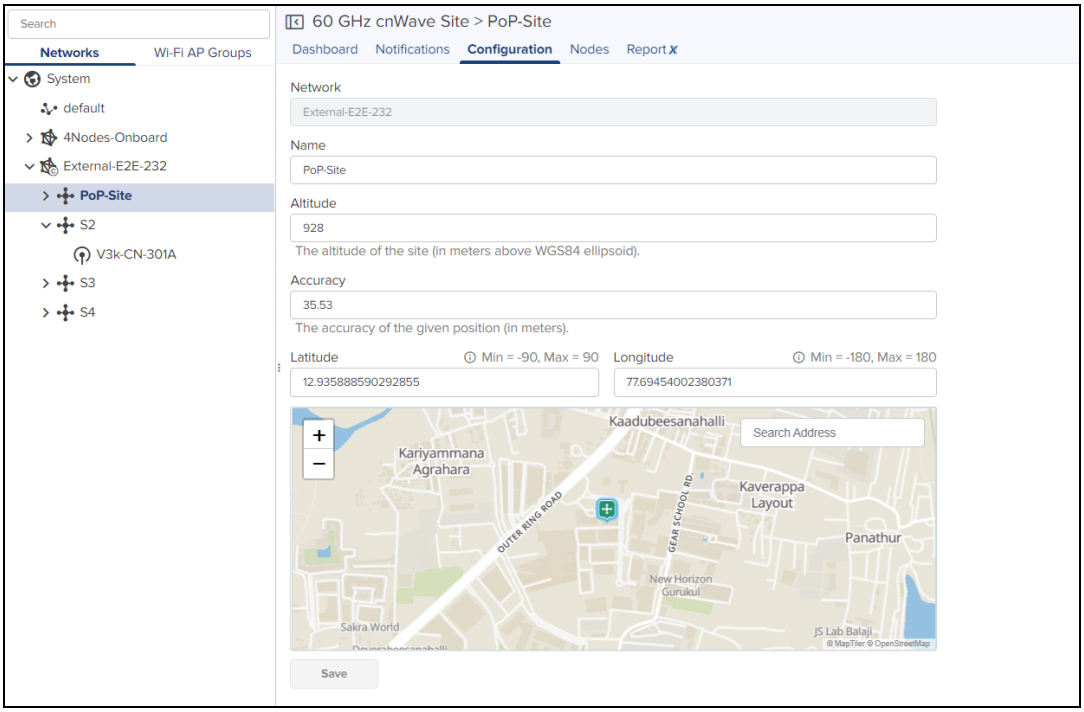


5. Click **Save**. Once the Site is configured it gets added under the E2E Network.



To edit the **Site**, perform the following:

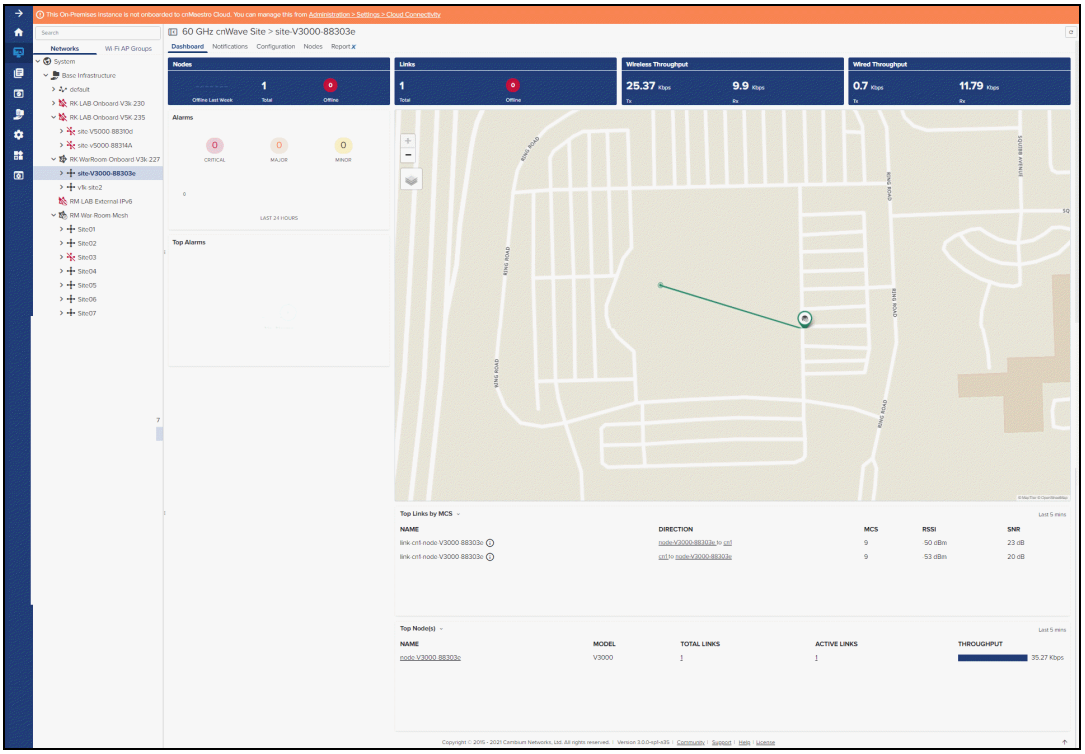
1. Navigate to **Network** > **Site** > **Configuration**.
2. Edit the details and click **Save.**



Site Dashboard

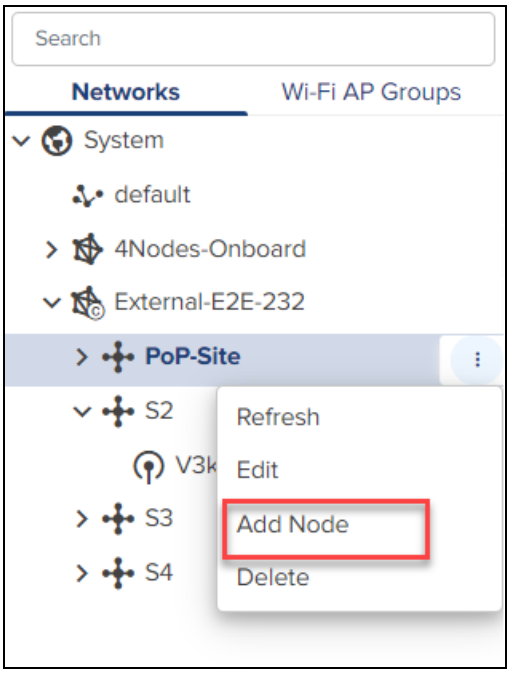
Dashboard pages are customized for each device type and aggregation level. The Site dashboard section displays the **Nodes, Links, Wireless Throughput, Wired Throughput, Alarms, Top Alarms, Top Links by MCS, Top Links by RSSI, Top Links by SNR, Top Node(s), Top PoP(s), Top DN(s), and Top CN(s).**

Figure 101 Site Dashboard

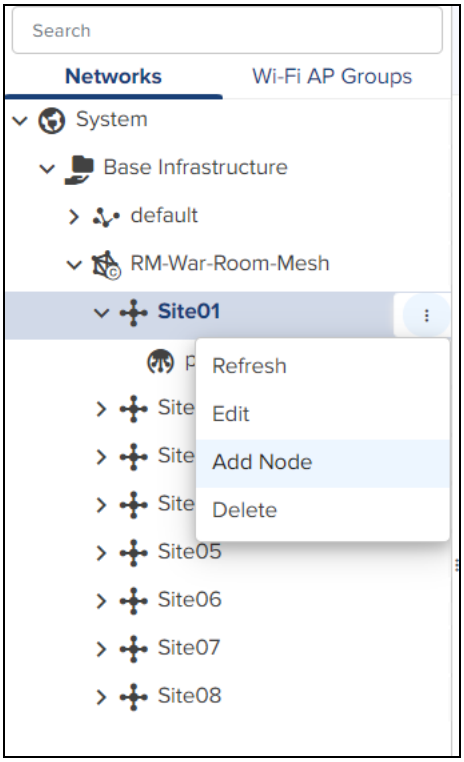


Node Configuration

Node can be configured through **Network** tree and **Site**. Select the **Network** click ⋮ select **Add Node.**

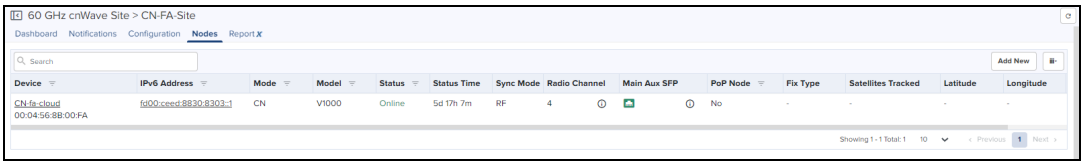


Select the **Site** click ⋮ select **Add Node.**

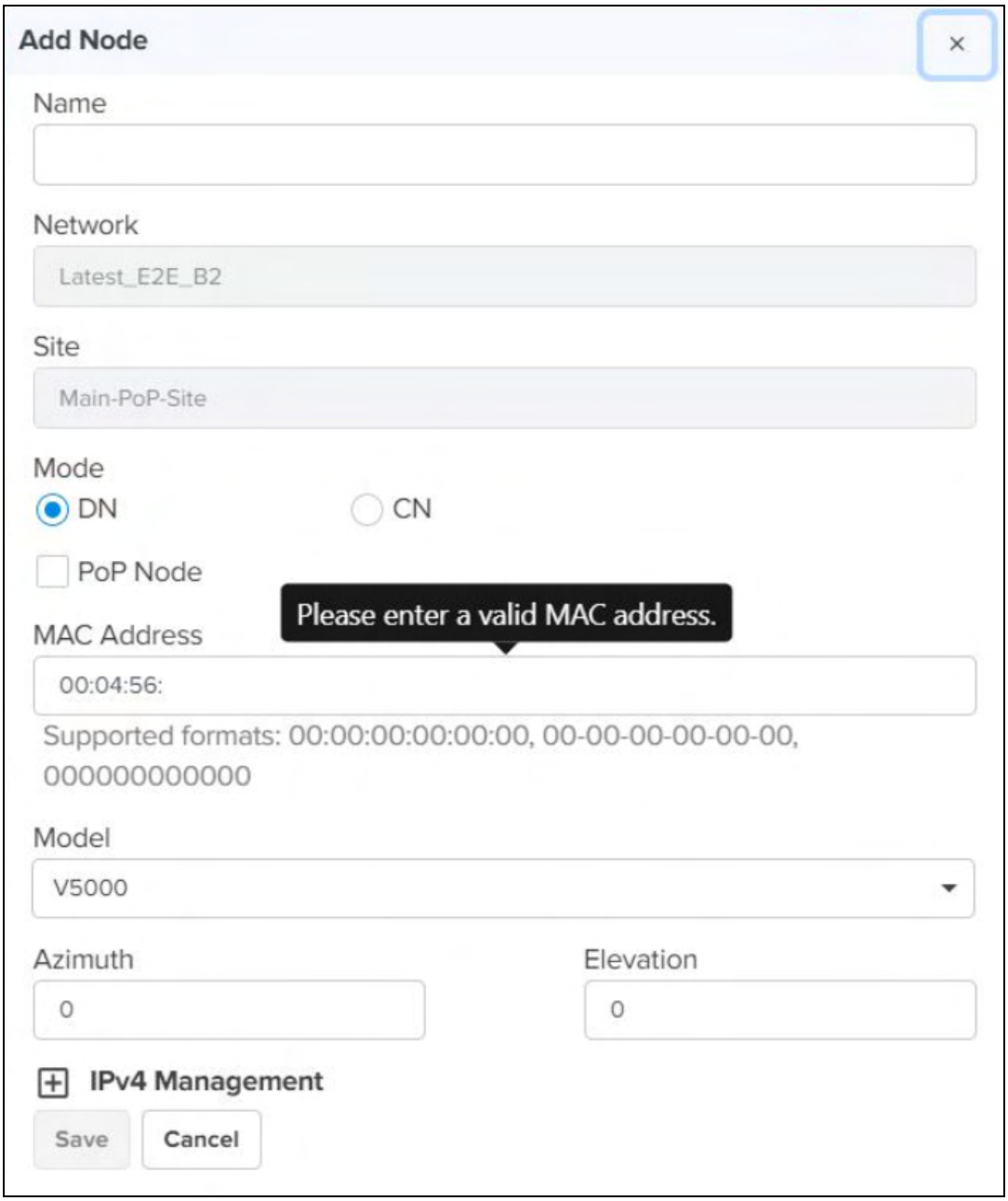


To Add a Node, perform the following steps:

1. Navigate to the **Network** > **Site** > **Nodes.**



2. **Add Node** window pops-up once the user clicks **Add new.**



Adding the Node allows the user to create the different Nodes as shown below:

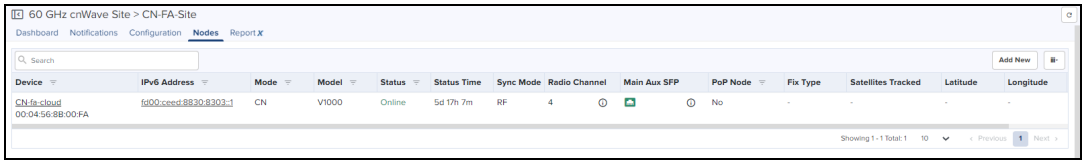
- PoP Node
- DN
- CN

PoP Node configuration

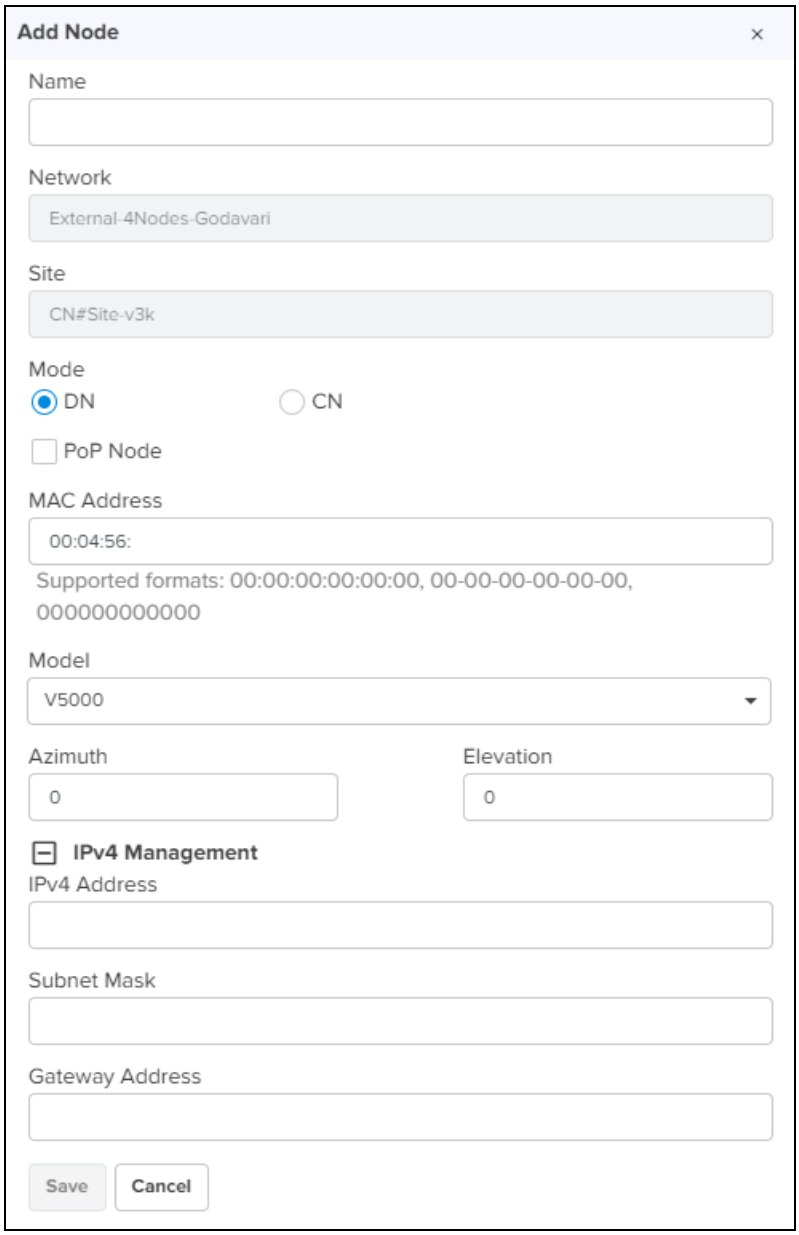
To add a PoP Node, perform the following steps:

1. Navigate to the **Network** > **Site** > **Nodes.**

2. Click **Add New.**



3. **Add Node** window pops-up.

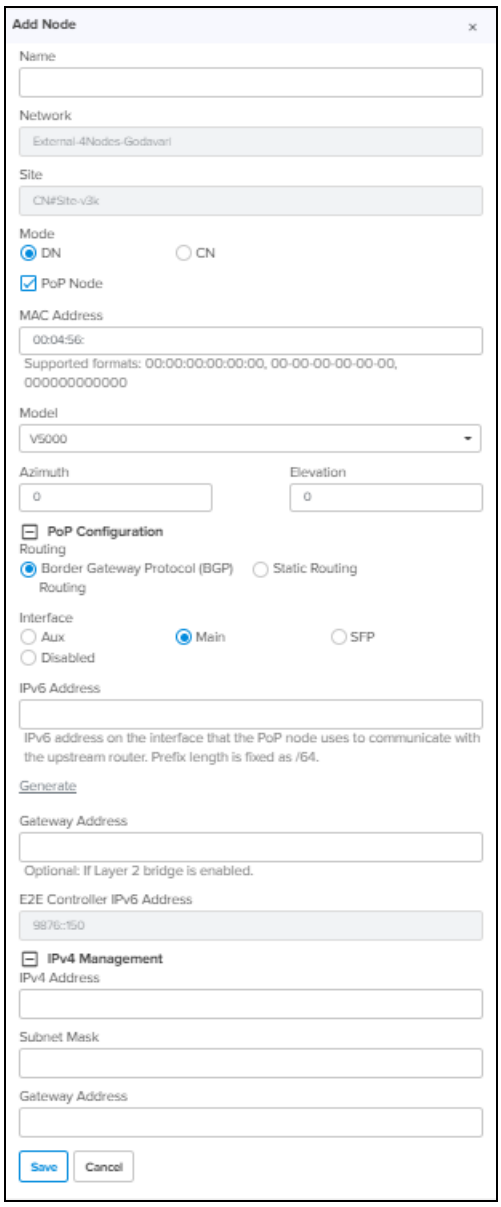


4. Enter the **PoP Name**, select the Mode **DN.**
5. Enable **PoP Node**.

	NOTE: Once the PoP Node is enabled user needs to select the **Routing** and **Interface** details.

6. Enter the **MAC Address** and select the device **Model** from the drop-down.
7. Enter the **Azimuth** and **Elevation**.

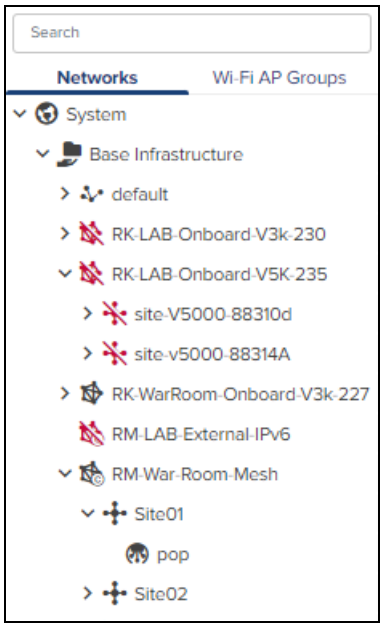
8. In the **PoP Configuration**, select **BGP** or **Static Routing**.
9. In **Interface,** select **Aux** or **Main** or **SFP** or **Disabled**.



10. Enter the **IPv6** and **Gateway Addresses.**
11. In IPv4 Management, enter the **IPv4 Address, Subnet Mask** and **Gateway Address**.
12. Click **Save.**

	NOTE: Once the PoP Node is configured, **PoP(s) Onboarding Config.json** file gets downloaded automatically, that can be used to import and configure in the PoP Node UI.

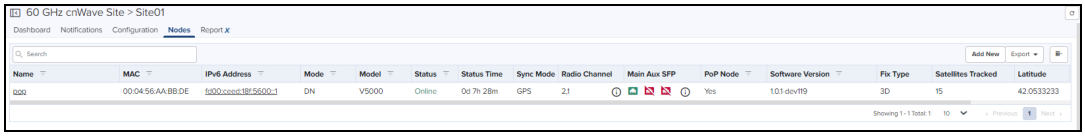
Once the **PoP** node is configured, it get listed under the **Site.**



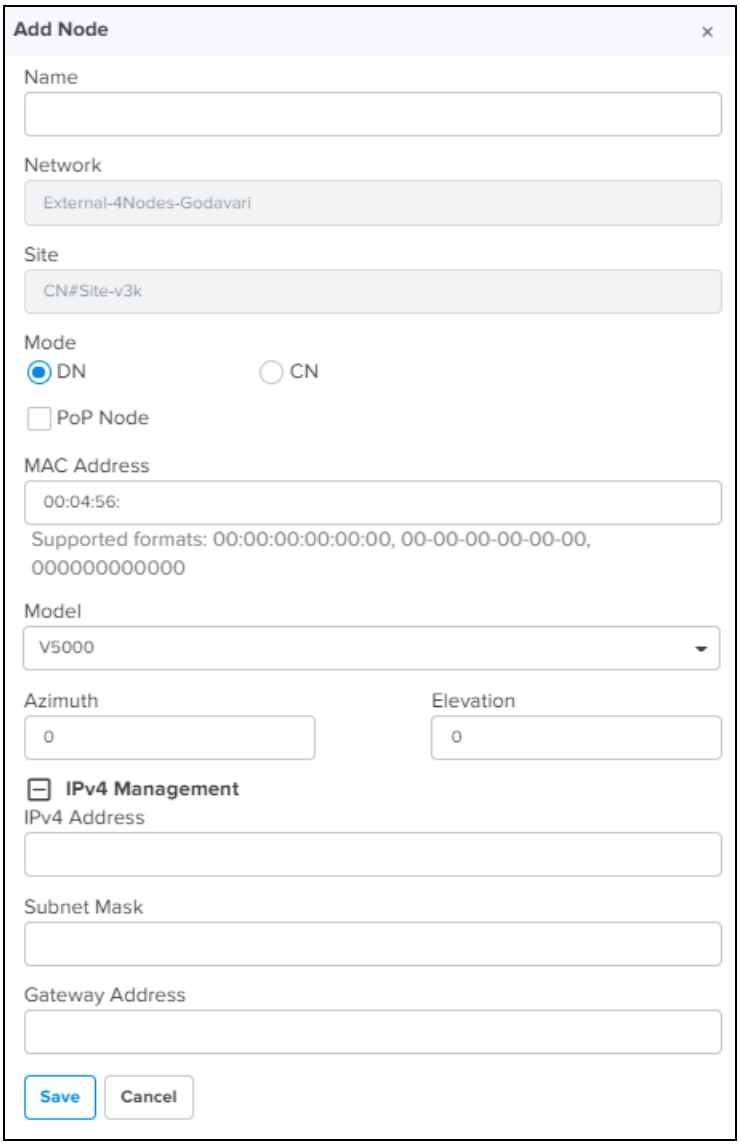
DN/CN Node configuration

To add DN/CN node:

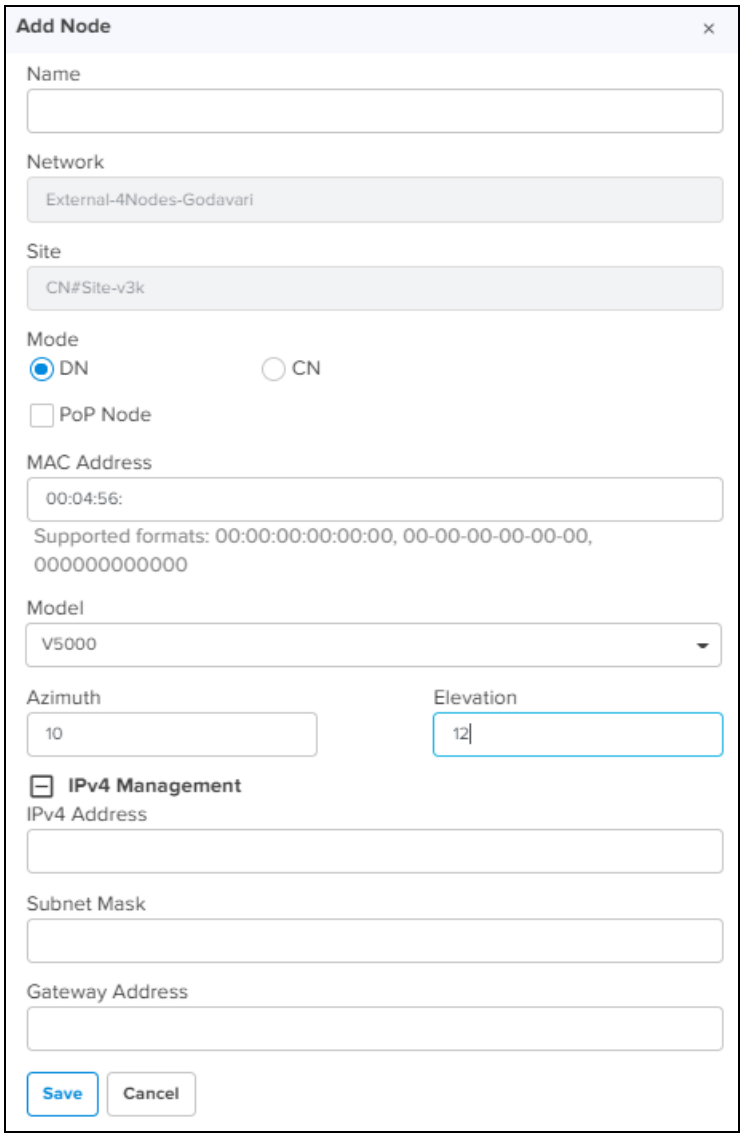
1. Navigate to the **Network** > **Site** > **Nodes.**
2. Click **Add New.**



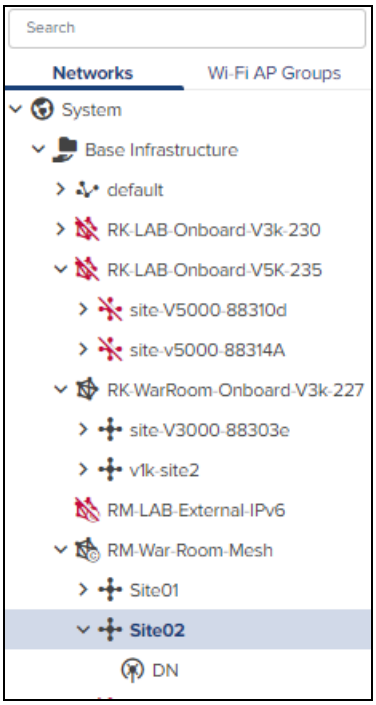
3. **Add Node** window pops-up.



4. Enter the **Node Name**, select the Mode **DN** or **CN.**
5. Enter the **MAC Address**, and select the device **Model** from the drop-down.
6. Enter the **Azimuth** and **Elevation**.



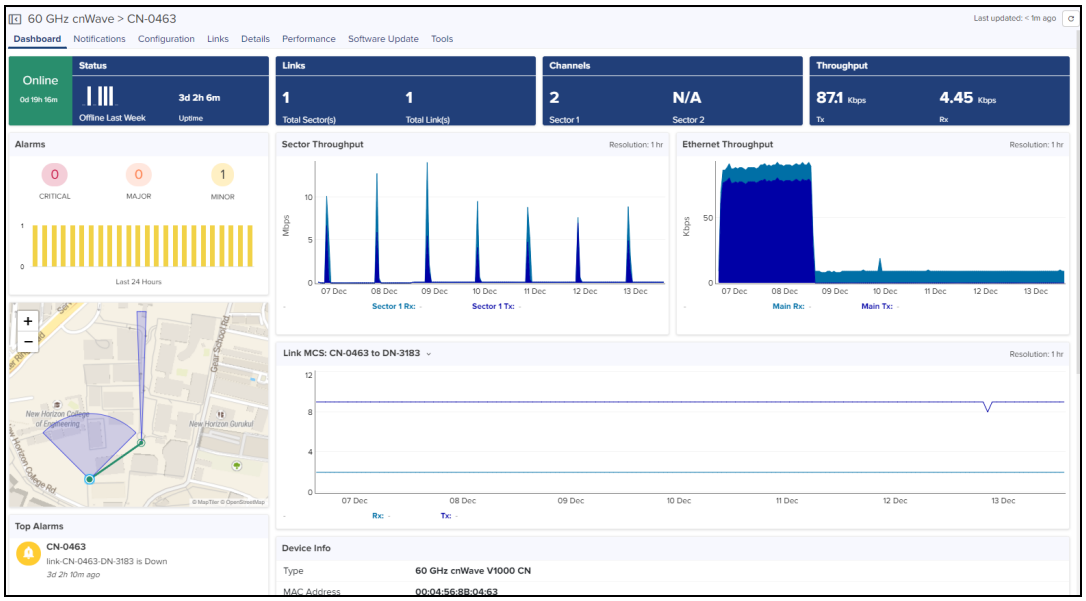
7. In IPv4 Management, enter the **IPv4 Address, Subnet Mask** and **Gateway Address**.
8. Click **Save.**
9. Once the **DN/CN** node is configured, it gets listed under the Site.



Replace Node

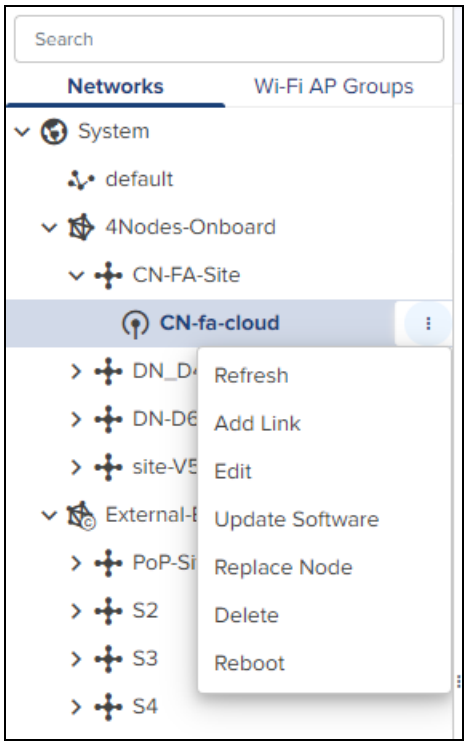
Replace Node allows to replace the existing faulty nodes with new nodes along with the configuration and links of existing faulty nodes.

	NOTE: New node should be replaced with same model as existing node.

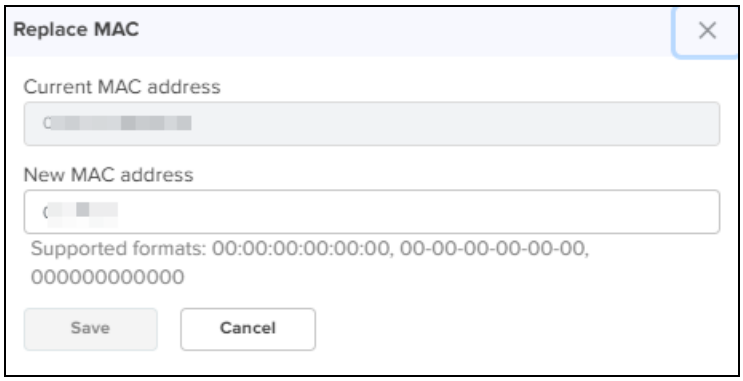


To replace Node, perform the following steps:

1. Navigate to **Node** tree menu and select the node.



2. Click icon, Select **Replace Node** from the drop-down.
3. **Replace MAC** window pops-up.



4. Enter the **New MAC address**.
5. Click **Save**.

PoP Node

Once the PoP node is configured it displays the monitoring panel of the PoP node.

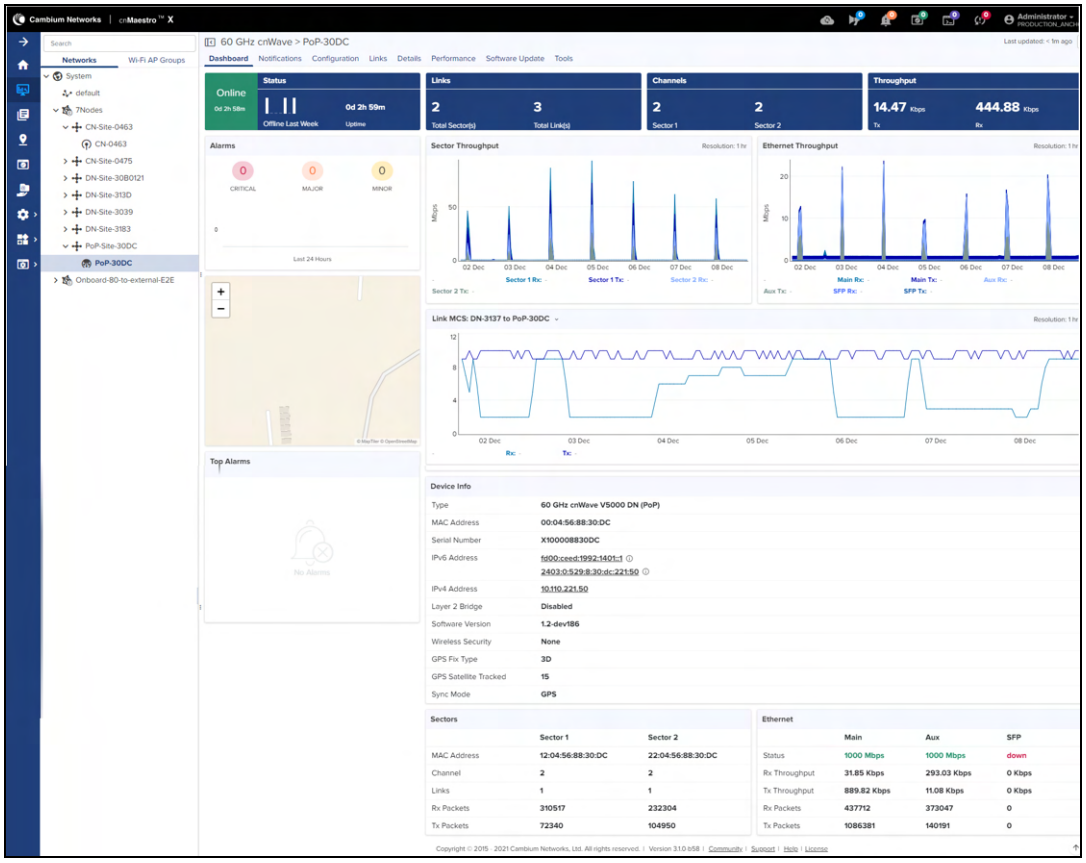
Dashboard

Dashboard pages can be customized for each device type and aggregation level. The PoP node dashboard section displays the **Status, Links, Channels, Throughput (sector1), Throughput (sector2), Throughput (Main), Throughput (AUX), Throughput (SFP), Alarms, Top Alarms, Links MCS, Device Info, Sectors, and Ethernet**.

NOTE:

- Throughput (sector1) for V3000 and V1000.
- Throughput (sector1 and sector2) for V5000.
- Throughput graph with Main for V1000.
- Other throughput graph with Main, Aux, SFP for V5000 and V3000.

Figure 102 PoP Node Dashboard

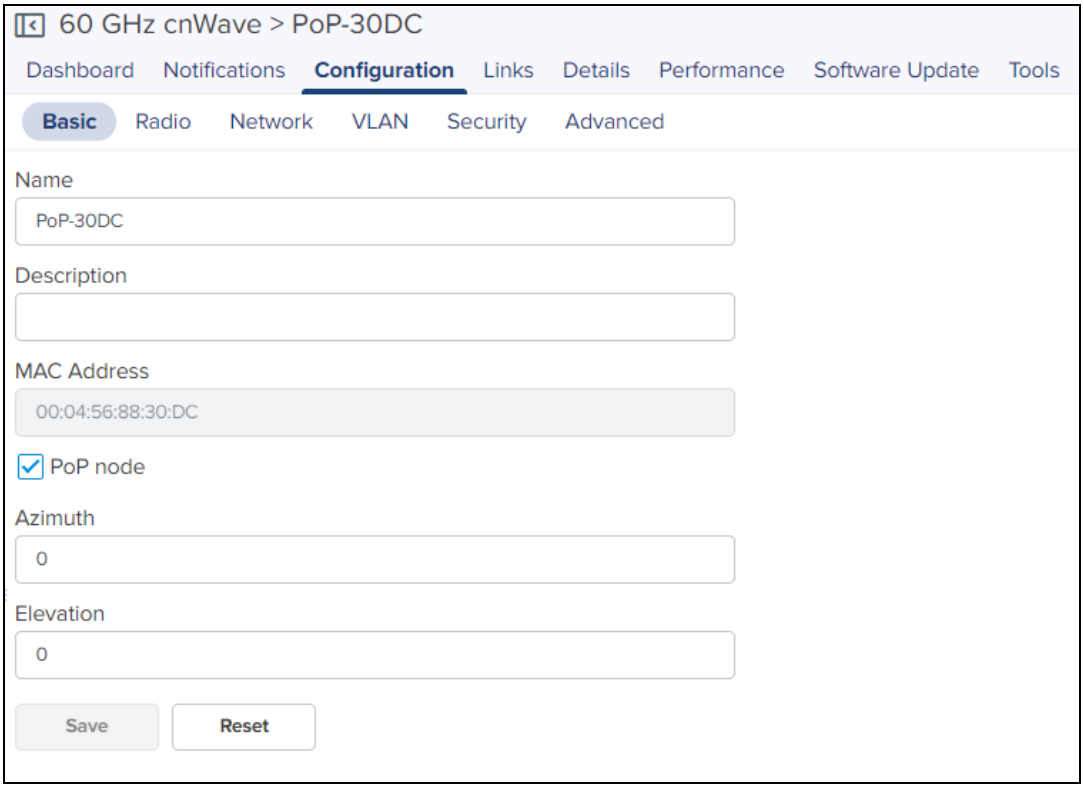


Configuration

Basic

In Basic page you can able to view and edit the details of PoP node such as **Name, Description, MAC Address, Azimuth,** and **Elevation**.

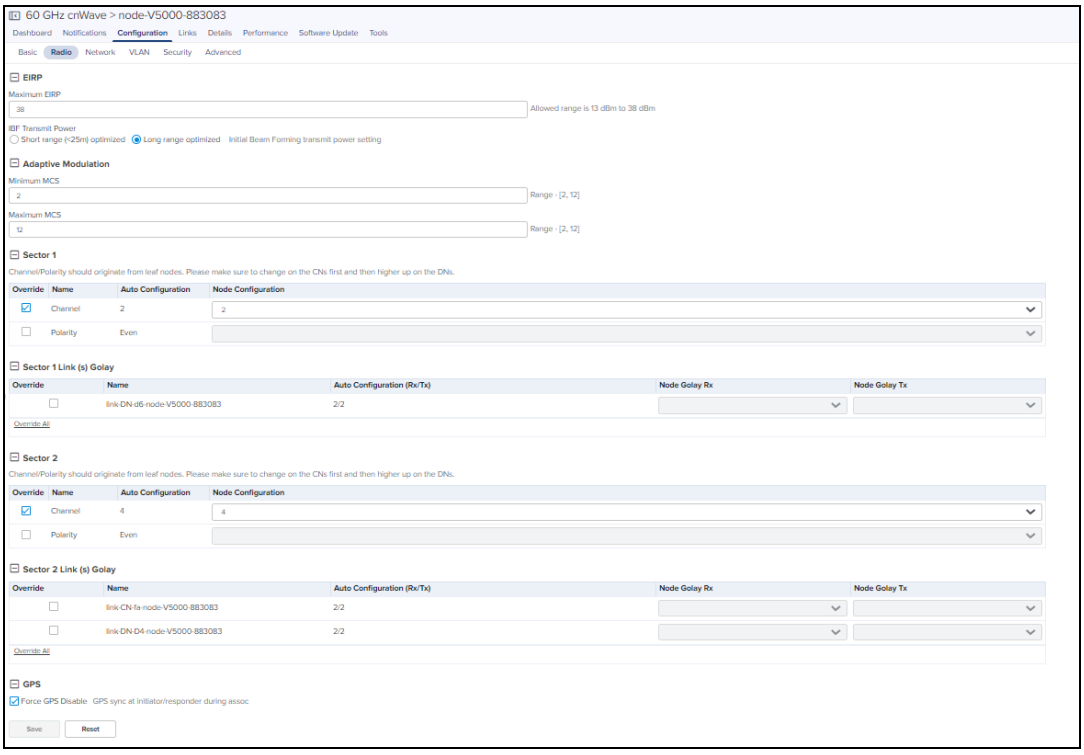
Figure 103 Basic



Radio

It allows the user to configure the **EIRP**, **Adaptive Modulation**, **Sectors (channels, Polarity and Link(s) Golay)**, and **GPS**.

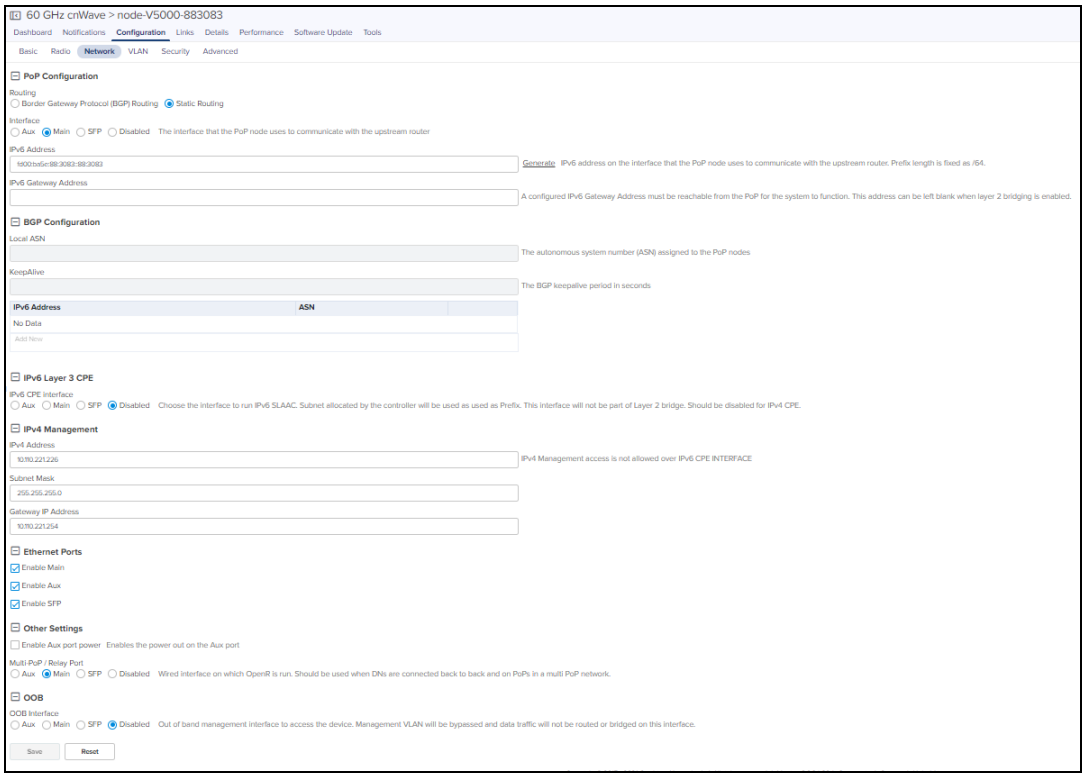
Figure 104 Radio



Network

Network tab allows the user for the **PoP configuration**, **E2E Controller Configuration**, **BGP Configuration**, **IPv6 Layer 3 CPE**, **IPv4 Management, OOB**, **Other Settings (Multi-PoP or Relay Port, Enable Aux port power)** and **Ethernet Ports.**

Figure 105 Network

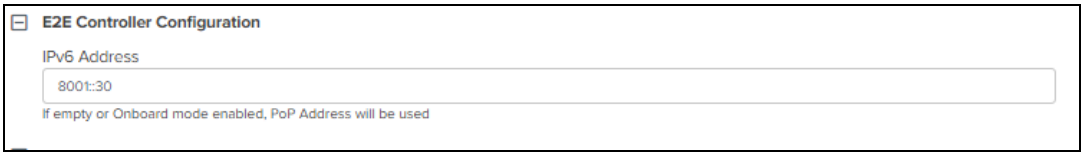


Configure the Network as shown below:

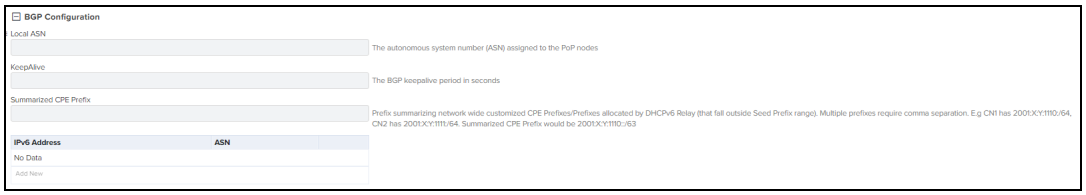
1. Navigate to the **Configuration** > **Network.**
2. In **PoP Configuration:**
    - Select the appropriate option in **Routing** and **Interface**.
    - Enter **IPv6 Address.**
    - Enter **IPv6 Gateway Address** its optional.



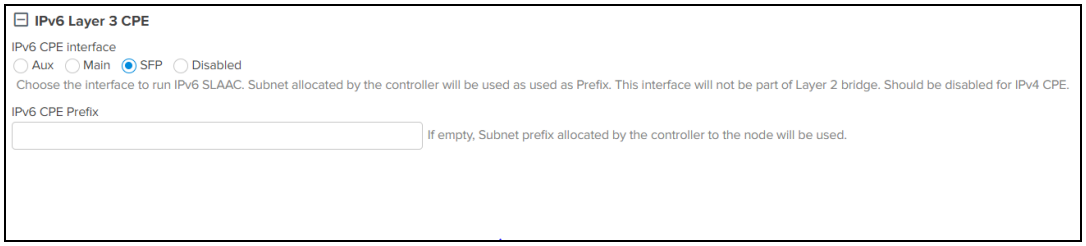
3. In **E2E Controller Configuration**, enter the **IPv6 Address.**



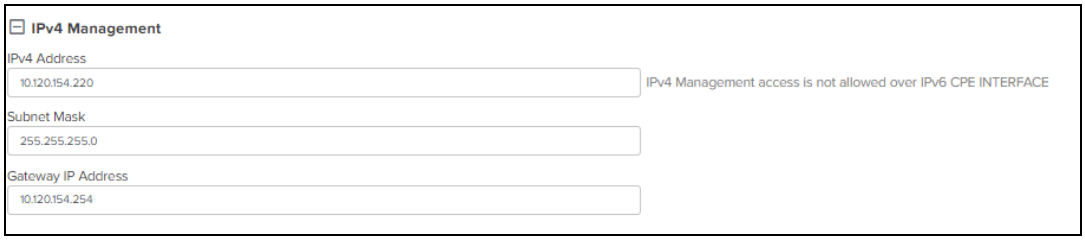
4. In **BGP Configuration** add IPv6 Address.



5. In **IPv6 Layer 3 CPE**
    - Select **IPv6 CPE interface** as Aux, Main, or SFP.
    - Enter **IPv6 CPE Prefix.**



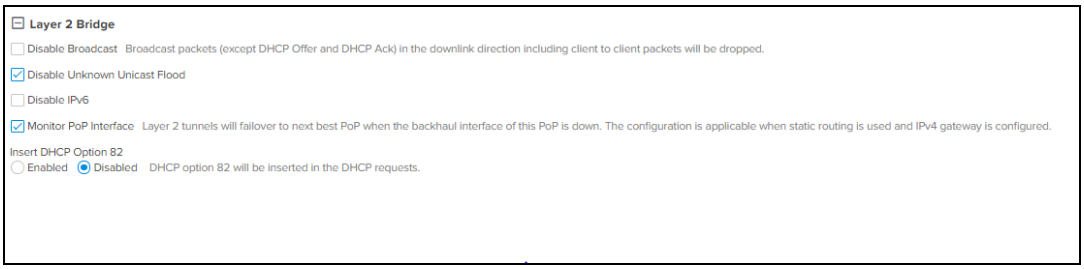
6. In **IPv4 Management**:
    - Enter **IPv4 Address.**
    - Enter **Subnet Mask**.
    - Enter **Gateway IP Address**.



7. In **Ethernet Ports** enable the appropriate option **Main** or **Aux** or **SFP.**
8. In **Layer 2 bridge** enable the appropriate options such as:
    - Disable Broadcast Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be dropped.
    - Disable Unknown Unicast Flood.
    - Disable IPv6.
    - Monitor PoP Interface Layer 2 tunnels will failover to next best PoP when the backhaul interface of this PoP is down.

	NOTE: The configuration is applicable only when static routing is used and IPv4 gateway is configured.

    - Insert DHCP Option 82



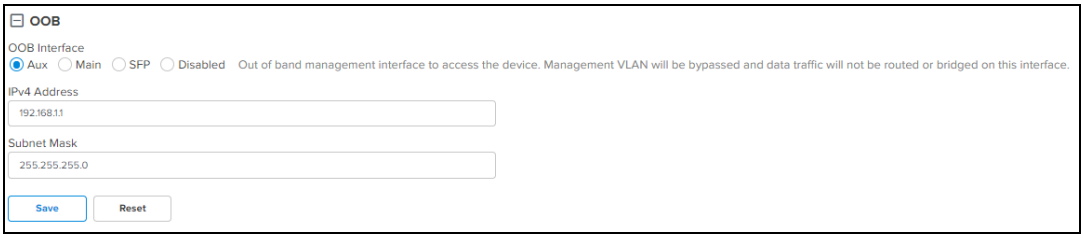
9. In Other Settings.

   - Enable Aux port power
   - Select **Multi-PoP / Relay Port** as Aux, Main, or SFP.



10. In **OOB Interface** enable the appropriate option **Main** or **Aux** or **SFP.**

    - Enter **IPv4 Address.**
    - Enter **Subnet Mask**.



11. Click **Save.**

	NOTE: Once the configuration is updated successfully in cnMaestro, the same parameters needs to be entered in the UI of the **PoP Node GUI**.

VLAN

	NOTE: From Software Update Version 1.1 of all nodes, supports configuration of the VLAN Management and Ports.

Virtual Local Area Networks (VLANs) is a broadcast domain in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set and traffic will be tagged when transporting over wireless.

NOTE:

Only PoP node Management VLAN can be configured, if Layer 2 Bridge is not enabled in **E2E Network > Configuration > Basic** page.

Node running version 1.0.1:

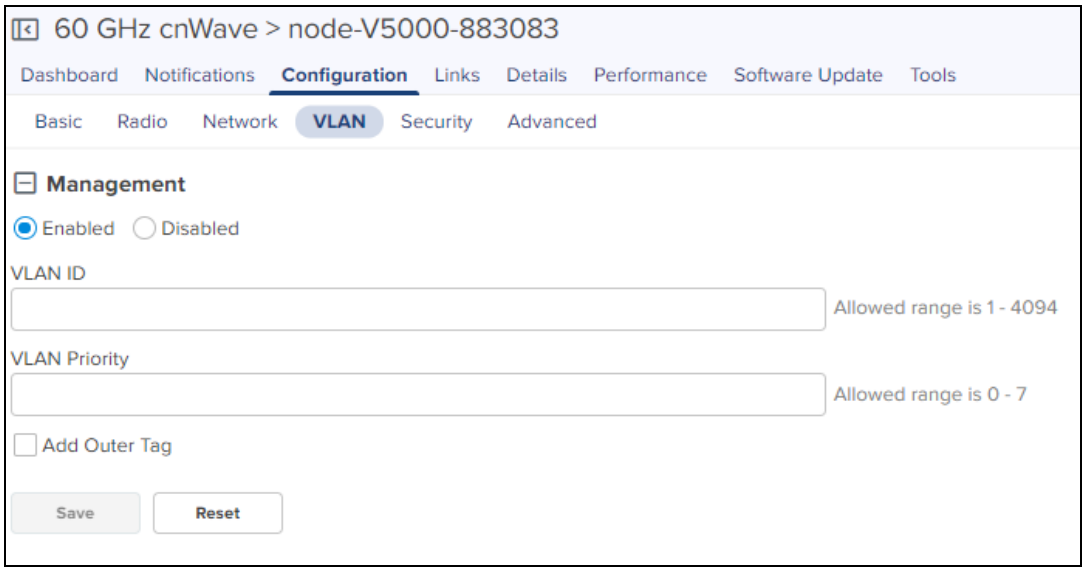
- When Layer2 bridge is disable, Only PoP node Management VLAN ID can be configured.
- When Layer2 bridge is enable, all nodes Management VLAN ID can be configured.

Node running version 1.1:

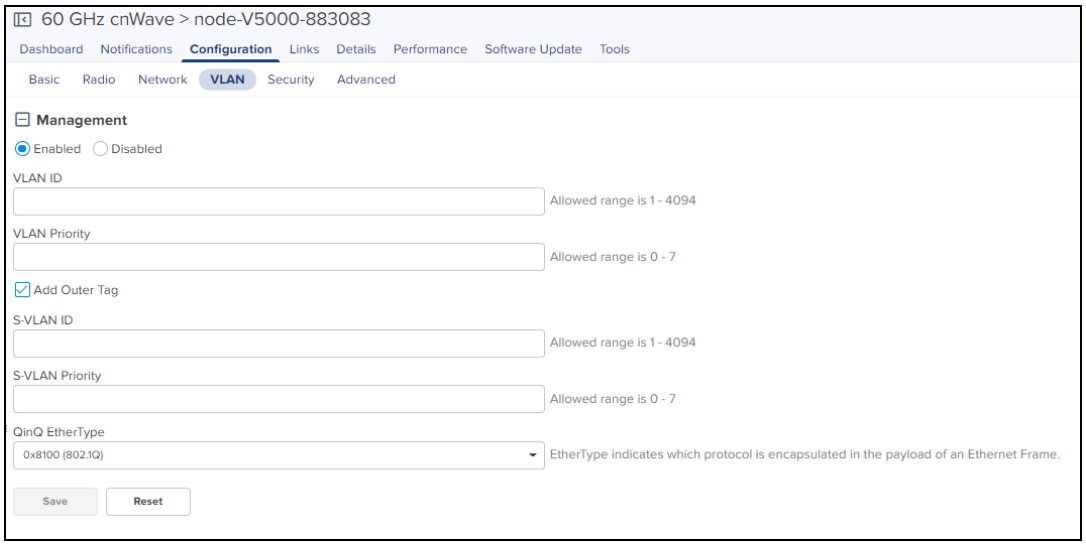
- When Layer2 bridge is disable, Only PoP node Management VLAN ID, Priority with Outer Tag can be configured.
- When Layer2 bridge is enable, all node management VLAN and ports can be configured.

To add a Management VLAN:

1. Navigate to **Configuration > VLAN.**
2. Click **Enabled**.



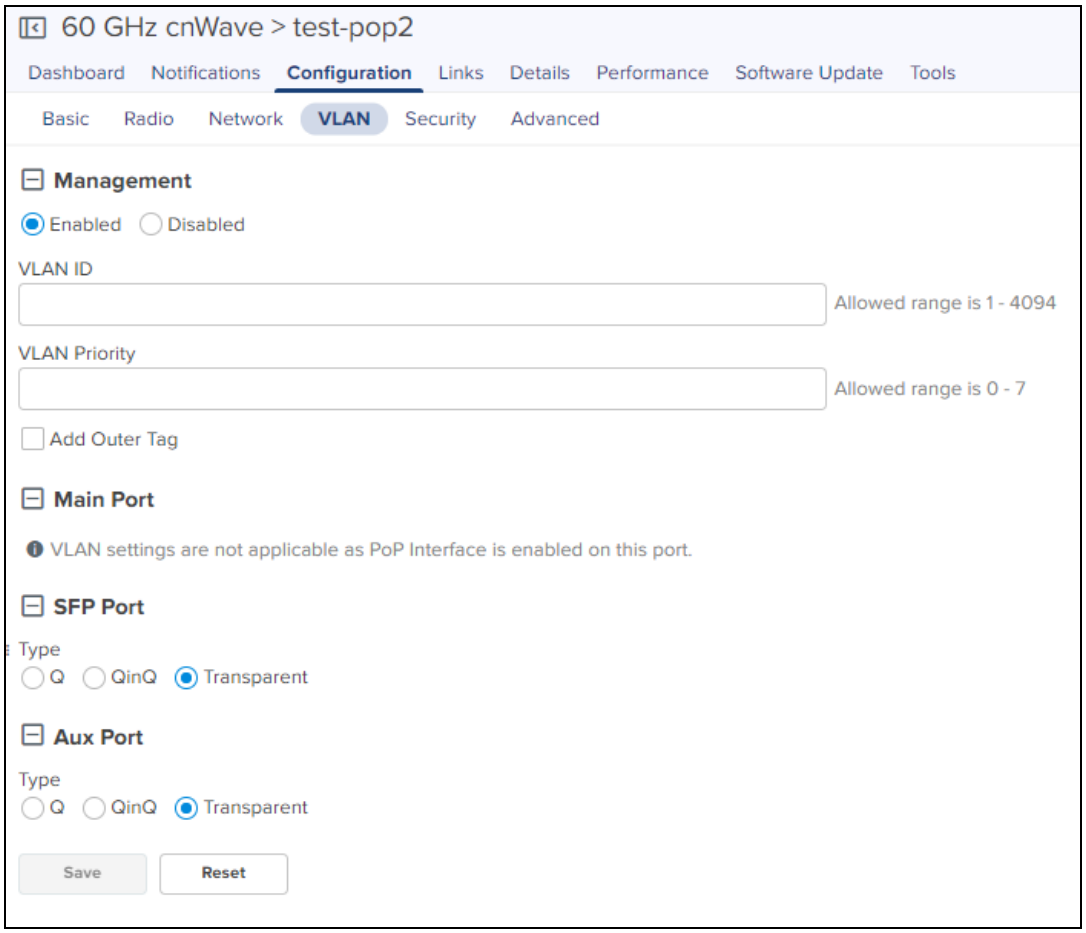
3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.



5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**
7. Enter **QinQ EtherType.**
8. Click **Save.**

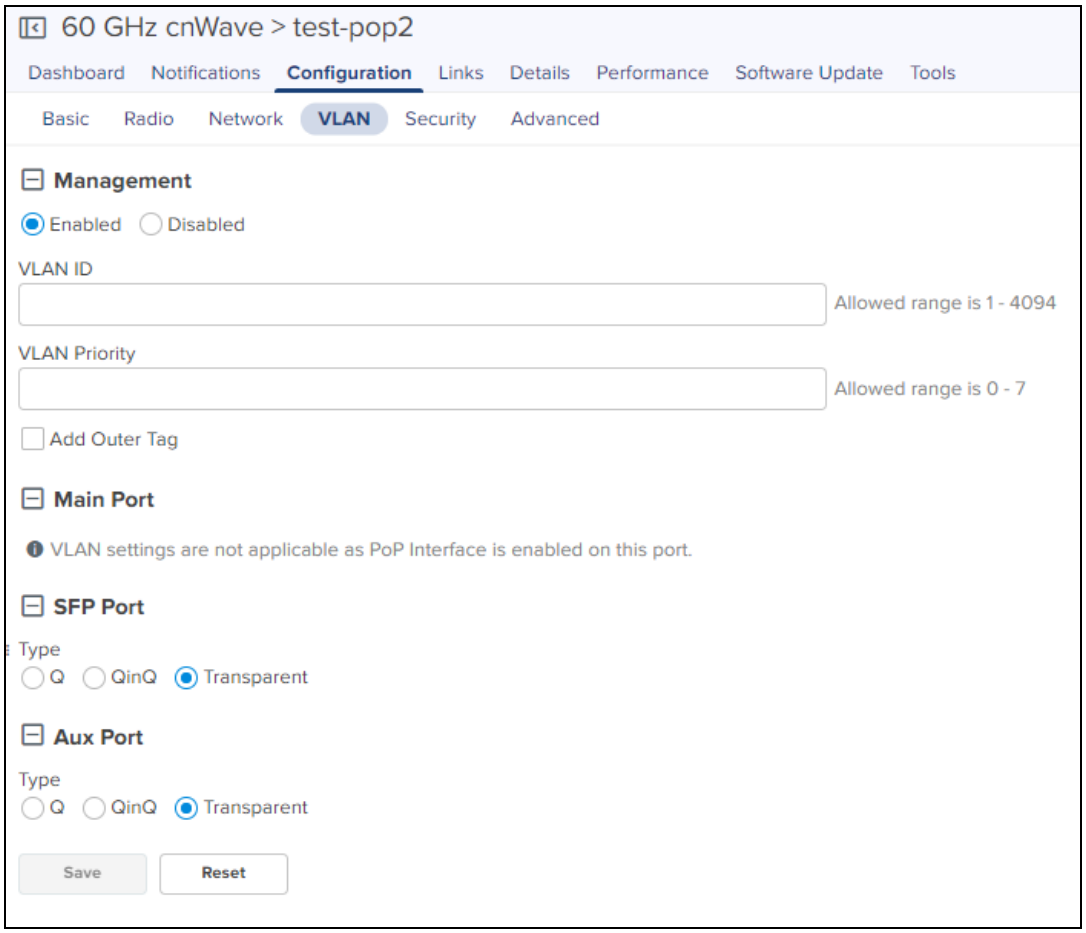
If Layer 2 Bridge is enabled in **60 GHz cnWave Network > Configuration > Basic** page, then the user can configure Management VLAN and Ports of PoP node, DN and CN.

	NOTE: VLAN settings are not applicable if Relay Port, SFP Port, or Aux Port is enabled on Network page.

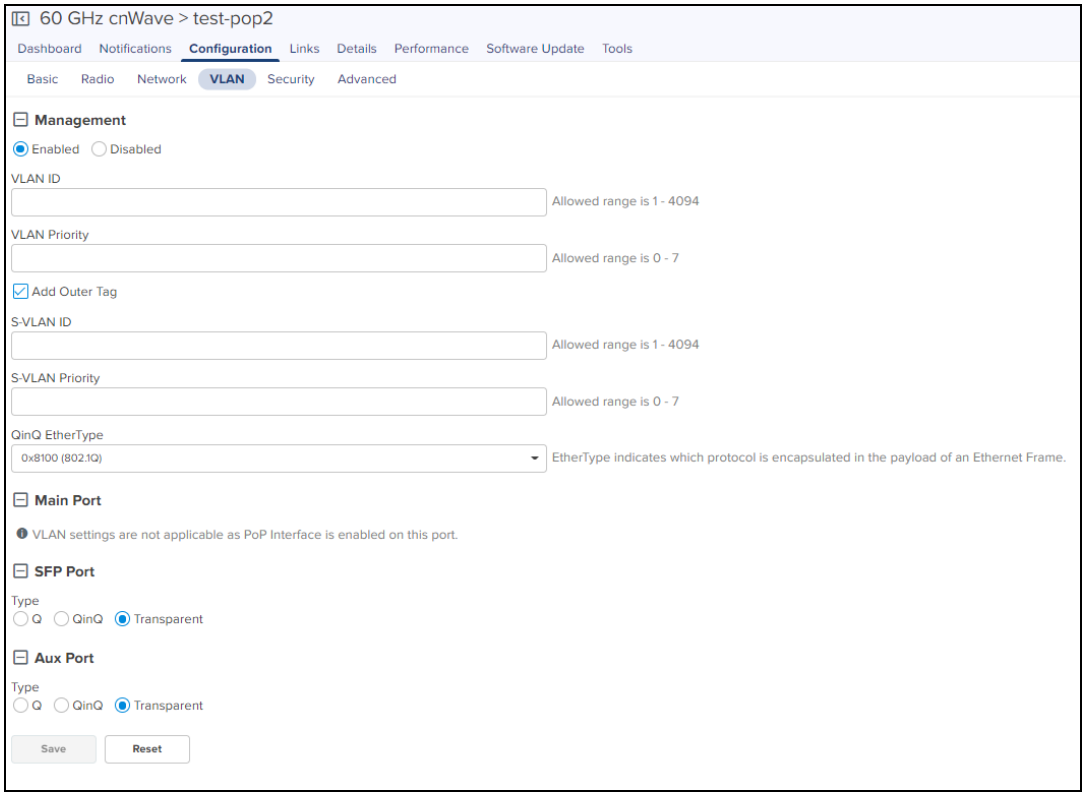


To add a VLAN, perform the following steps:

1. Navigate to **Configuration > VLAN.**
2. Click **Enabled**.



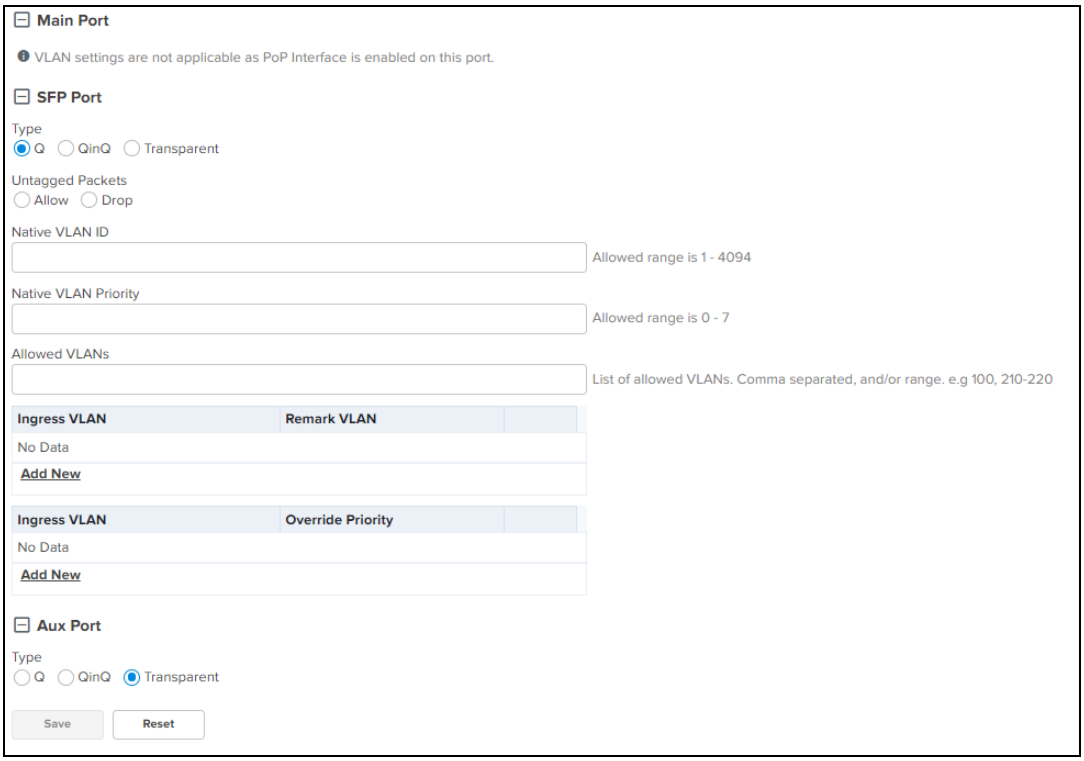
3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.



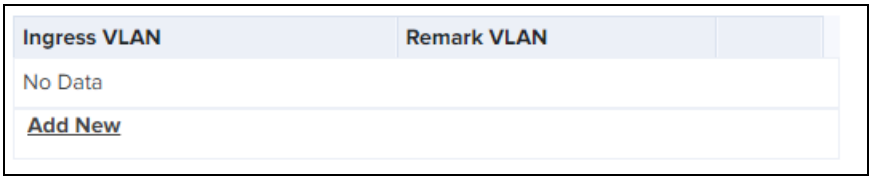
5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**
7. Enter **QinQ EtherType.**

	NOTE: VLAN settings configuration of Main Port, SFP Port, or Aux Port is similar.

8. Select Port **Q** or **QinQ** types.
   a. If user selects **Q type** perform as follows:



   - Select **Untagged Packets** Allow or Drop.
   - Enter **Native VLAN ID.**
   - Enter **Native VLAN Priority**.
   - Enter **Allowed VLANs**.
   - To add new **VLAN Remarking.**



   - Click **Add New**.



- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- To add new **VLAN Priority Override**.



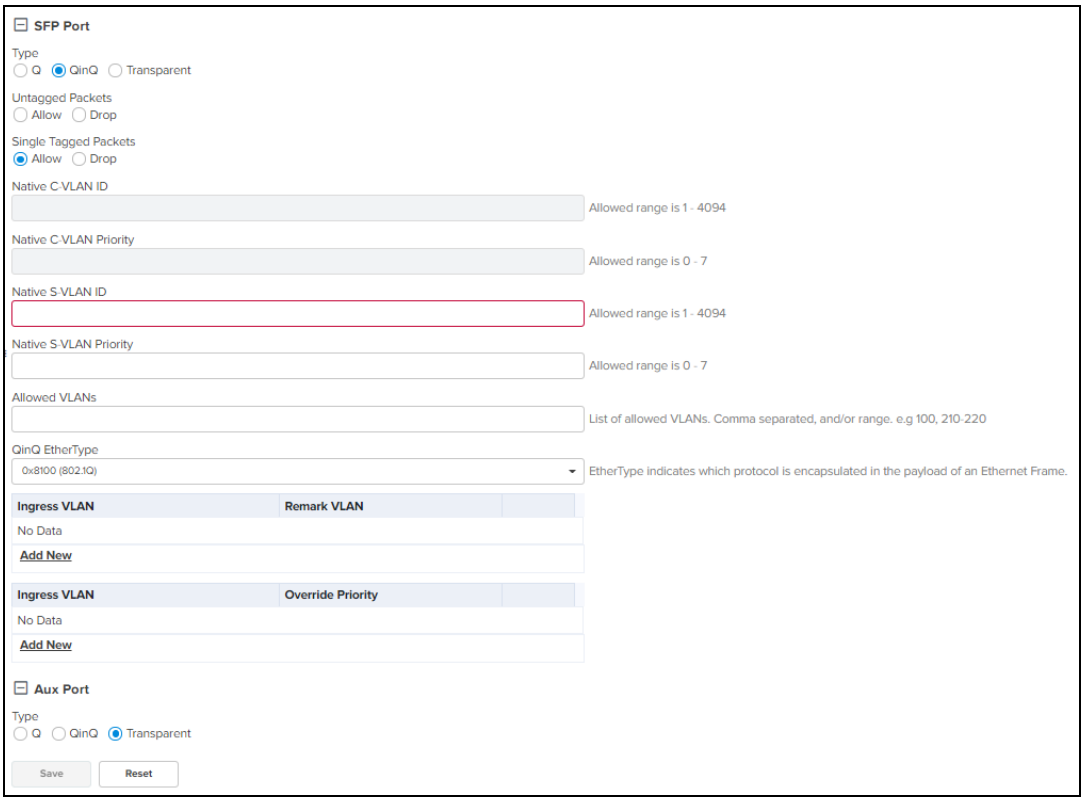
- Click **Add New**.



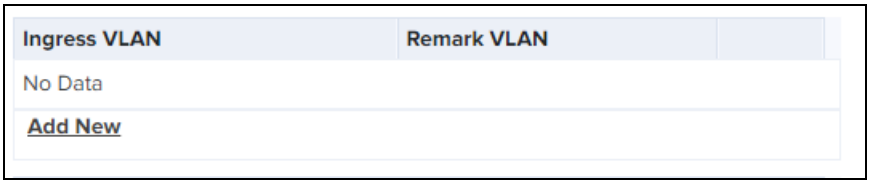
- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- Click **Save**.

b. If user selects **QinQ** type, then perform as follows:



- In **Untagged Packets** select **Allow** or **Drop.**
- In **Single Tagged Packets** select **Allow** or **Drop.**
- Enter **Native C-VLAN ID.**
- Enter **Native C-VLAN Priority**.
- Enter **Native S-VLAN ID**.
- Enter **Native S-VLAN Priority**.
- Enter **Allowed VLANs**.
- Enter **QinQ EtherType**.
- To add new **VLAN Remarking.**

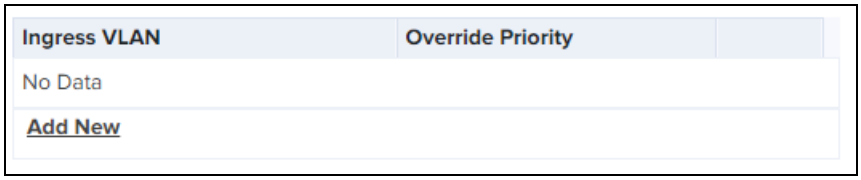


- Click Add New



- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- To add new **VLAN Priority Override**.



- Click **Add New**.



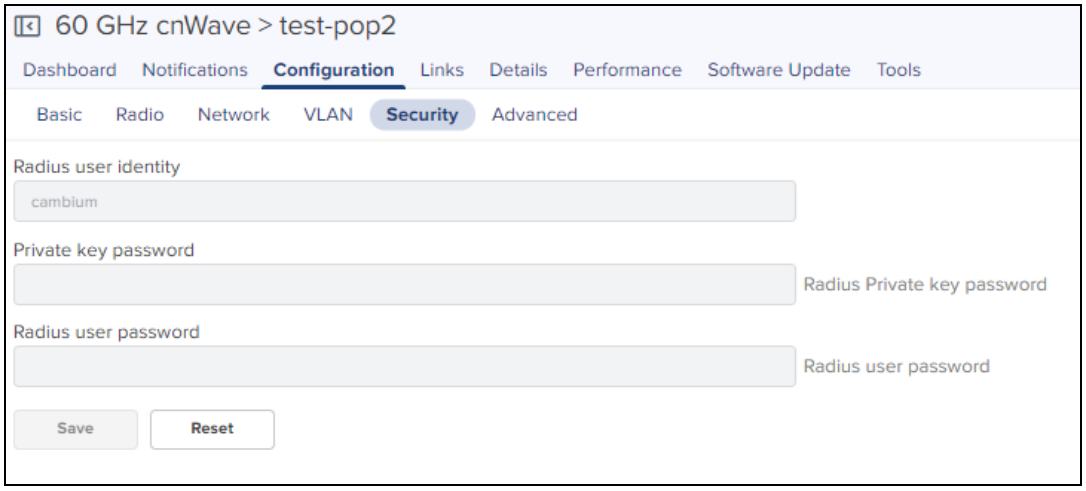
- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- Click **Save**.

Security

Security tab allows to reset the identity and password of the Radius user.

Figure 106 Security



Advanced

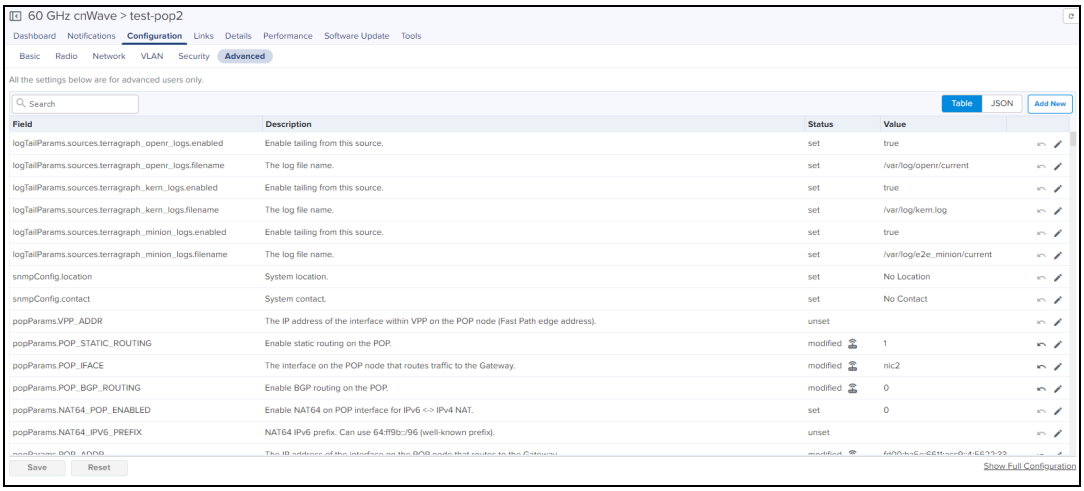
Advanced tab allows the advanced user to edit the settings of the Table and JSON format of the PoP Nodes.

Table

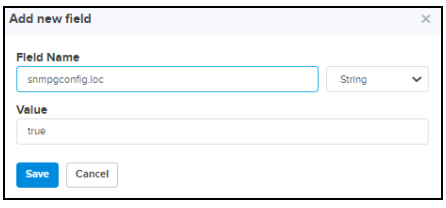
In the **Table** user can able to view and edit **Field Name** and **Value**.

To add a field, perform the following steps:

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



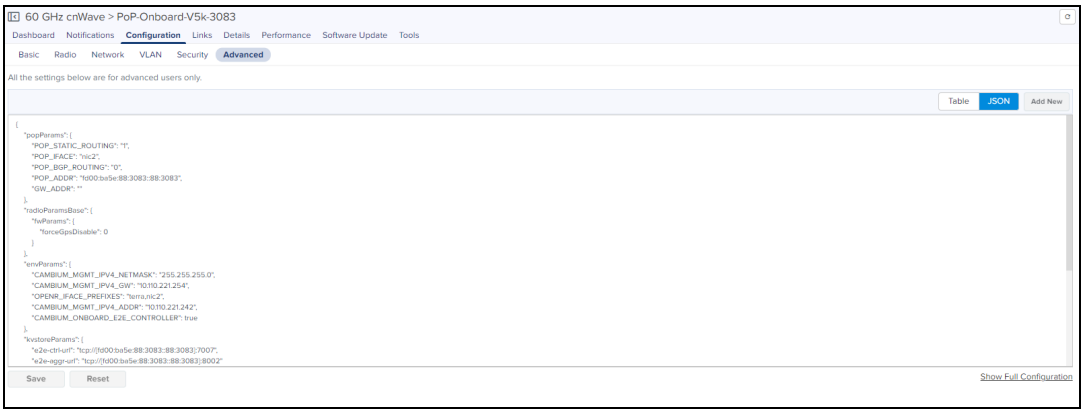
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

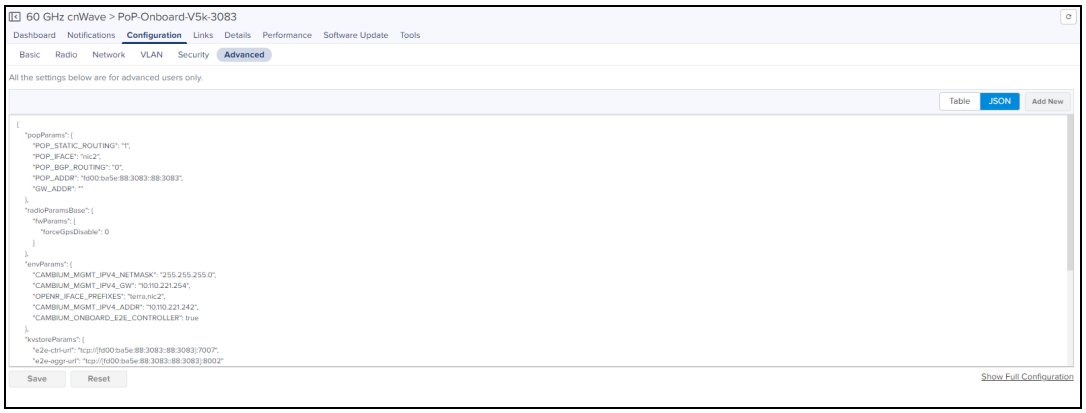
JSON

JSON allows Advanced user to download or view the JSON format.



To download the file, perform the following steps:

1. Navigate to **Configuration** > **Advanced > JSON**



2. Click **Show Full Configuration.**
3. **View Device Existing Configuration** pops-up.



4. Click **Download**.

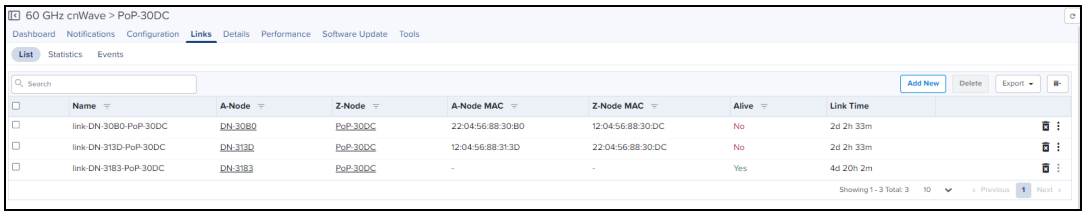
Links

Links provide the details about the links between nodes, status and also provides the option to create a new link. User can delete the links in bulk by selecting the particular devices.

List

List provide the details about the links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular links.

Figure 107 List



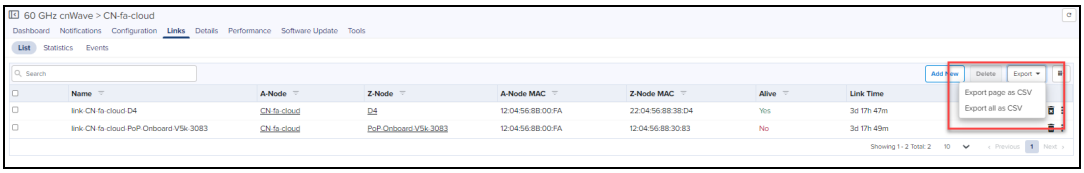
> **NOTE:**
>
> Once the PoP node is configured successfully user needs to create a Site and DN to link the PoP as shown in the DN/CN Node link.

Export Link List

Export list allows the user to export the PoP links list.

To export the links, perform the following steps:

1. Navigate to **Links** > **List** > select **Export.**

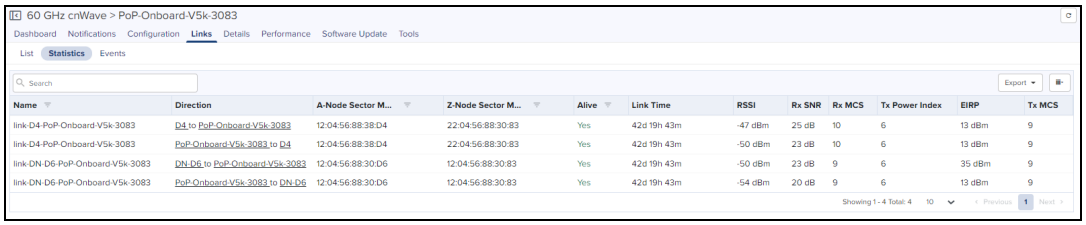


2. It exports .csv file format as shown below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	LINK_NAME	A_NODE_I	A_NODE_I	Z_NODE_I	Z_NODE_I	LINK_TYPE	ALIVE	IGNITION_	DISTANCE	AZIMUTH	BACKUP_C	IGNITION_	TIMESTAMP		
2	Link Name	A node nai	Sector 1/2	Z node nai	Sector 1/2	Wireless o	Yes/No	Ignition At	Distance b	Azimuth (D	Yes/No	Enabled/D	Timestamp		
3	link-CN-fa-cloud-D4	CN-fa-clou	12:04:56:8	D4	22:04:56:8	Wireless	Yes	16	996	54.9	No	Enabled	2021-07-23T02:49:06.317Z		
4	link-D4-PoP-Onboard-V5k-3083	D4	12:04:56:8	PoP-Onbo	22:04:56:8	Wireless	Yes	0	988	158.8	No	Enabled	2021-07-23T02:49:06.317Z		
5	link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	12:04:56:8	PoP-Onbo	12:04:56:8	Wireless	Yes	0	979	105.2	No	Enabled	2021-07-23T02:49:06.317Z		

Statistics

Links Statistics pages provides details of **Name, Direction, A-Node Sector MAC, Z-Node Sector MAC, Alive, Link Time, RSSI, Tx Power Index, A-node, Z-node, Type, Distance, Azimuth, Rx MCS, Tx MCS, Rx PER, Tx PER, Rx SNR, Rx Beam Index, Tx Beam Index, EIRP, Rx Errors, Tx Errors, Rx Frames, Tx Frames** on a single device, generally in a page format.



Export Statistics

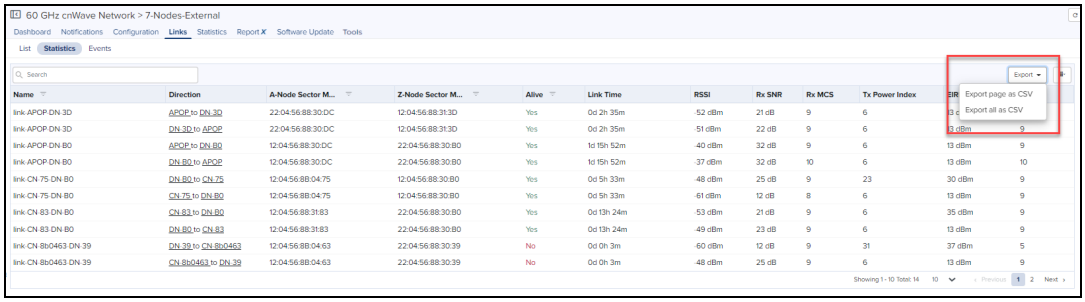
Export list allow the user to export the PoP links Statistics.

To export the Statistics :

1. Navigate to **Links > List >** select **Export.**



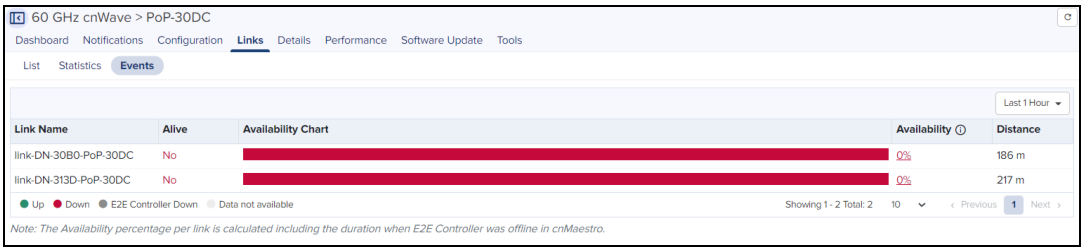
2. It exports .csv file format as shown below.



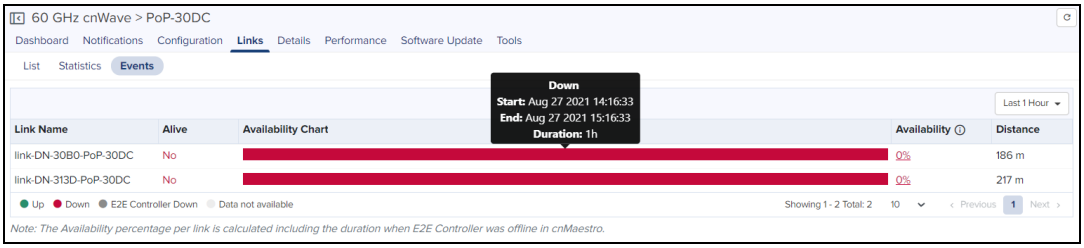
Events

Events provides the details of the links from last 1 hour to 7 Days Period.

Figure 108 Events



It also calculates the Availability percentage per link, including the duration when E2E Controller was offline in cnMaestro.



Details

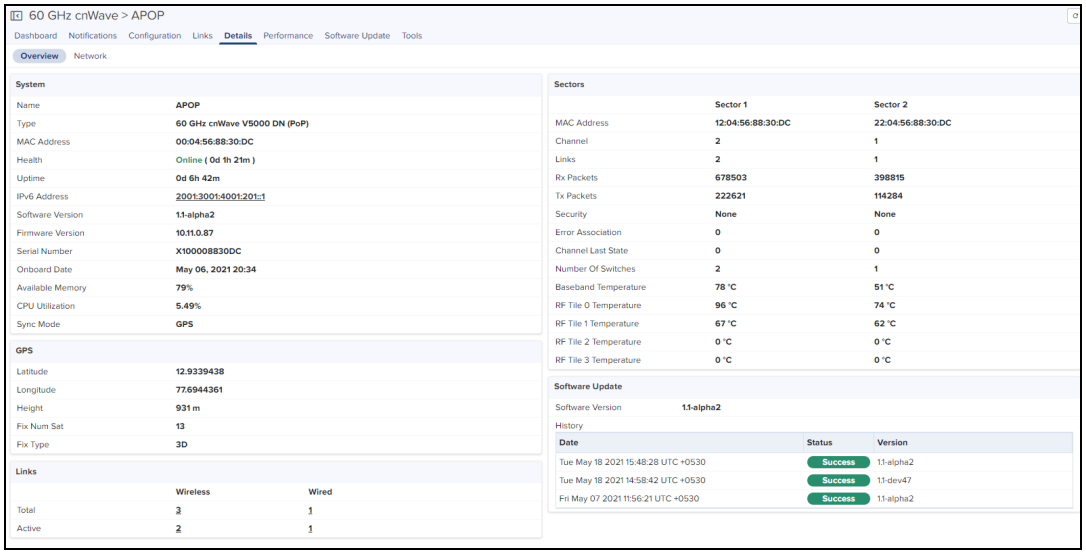
Details page provides the following device information:

- Overview
- Network

Overview

Overview page provides the device details and it also details of the last 3 software update history.

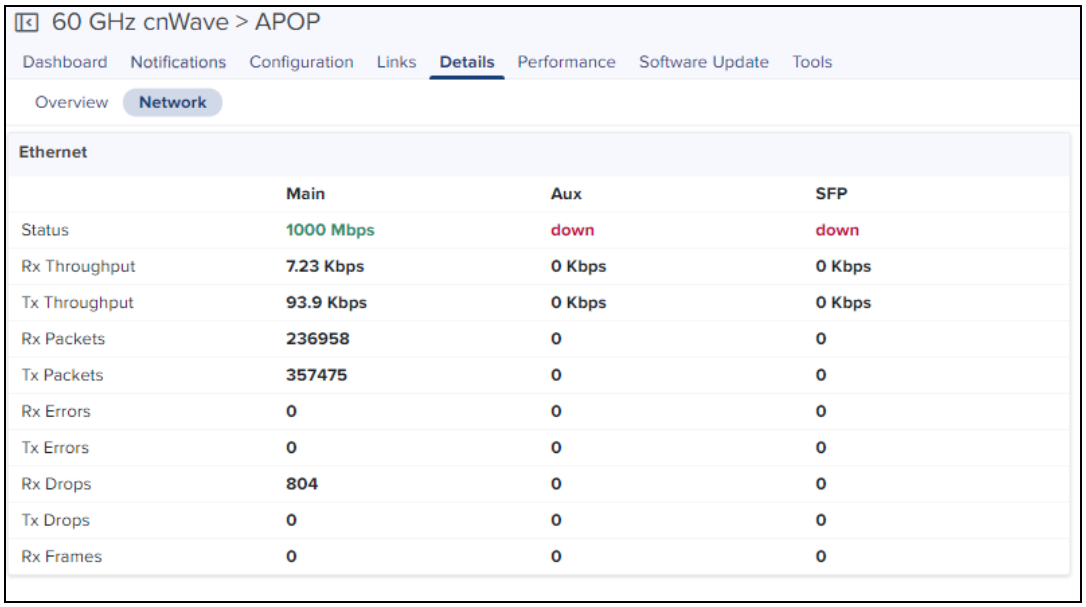
Figure 109 Details Overview Page



Network

Network page provides the **Ethernet** details of **Main, Aux**, and **SFP**.

Figure 110 Details Network Page



Tools

In Tools page user can able to view the **Status**, **Debug,** and **Remote Command** of the device.

Status

In **Status** tab you can view the status of the device:

- Critical alarms
- Download Tech Support File
- Online or Offline
- Reboot the device.
- Restart Minion



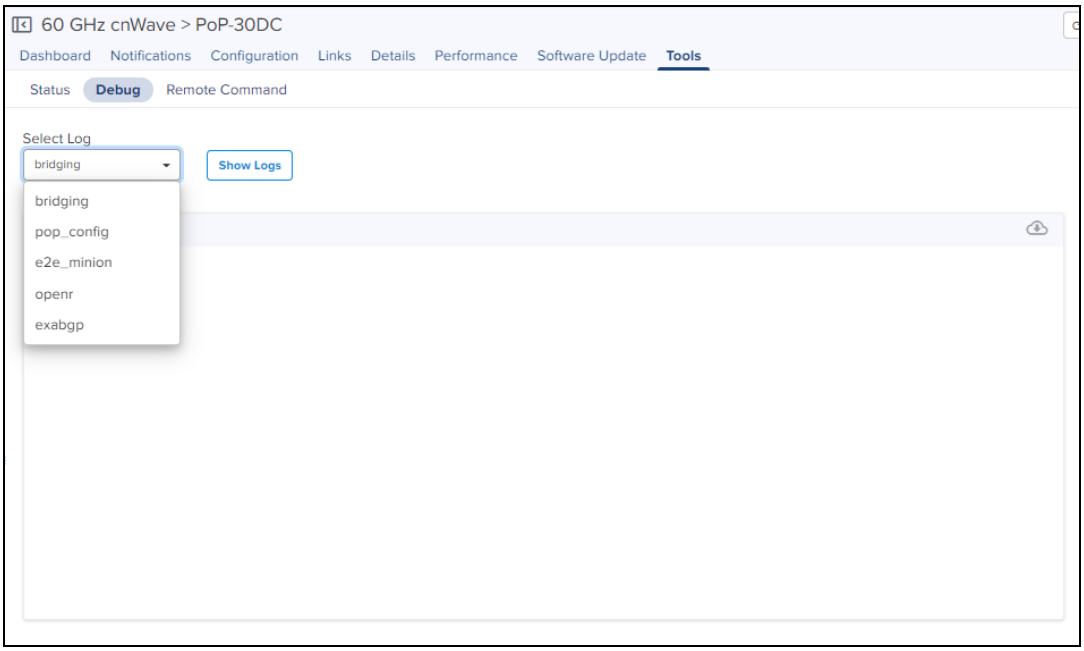
Debug

In **Debug** tab user view or download the PoP logs by executing the following log commands:

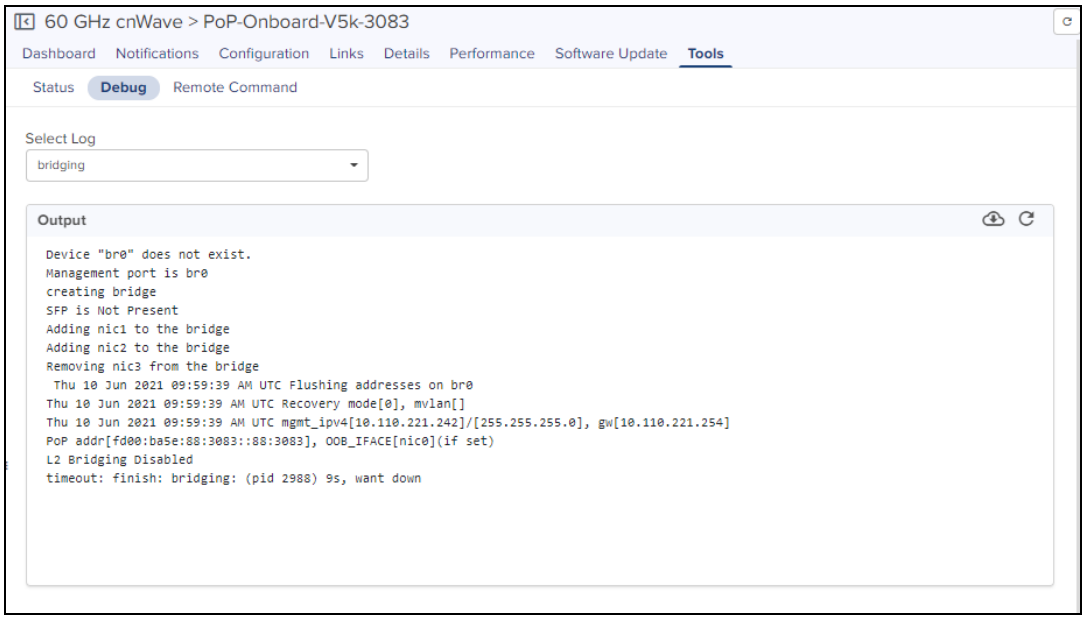
- Bridging
- pop-config
- e2e_minion
- openr
- exabgp

To view the logs, perform the following steps:

1. Navigate to **Tools > Debug**.
2. Select the required log name from the **Select Log** drop-down list box.



Once command is selected, it displays the output as shown below:



- Click icon to download the generated output.
- Click icon to refresh the generated output.

Remote Command

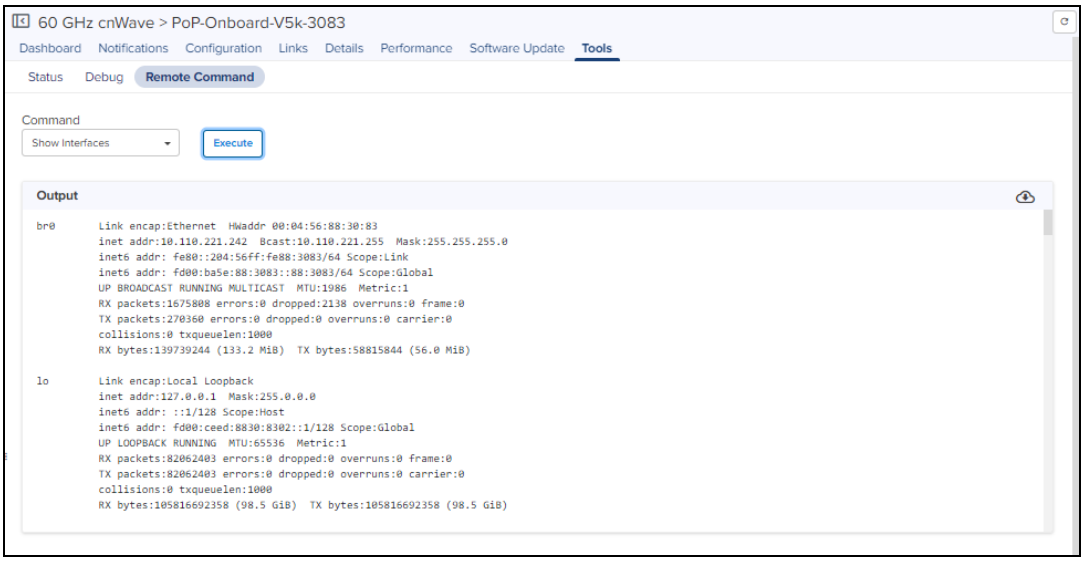
In **Remote command** tab user view or download Command logs by executing the following commands:

- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 and V3000)

To Execute the command:

1. Navigate to **Tools > Debug**.
2. Select the required command from the **Command** drop-down list box.
3. Click **Execute.**

The output for the selected critera appears as shown:



- Click the download icon to download the generated output.

DN/CN Node

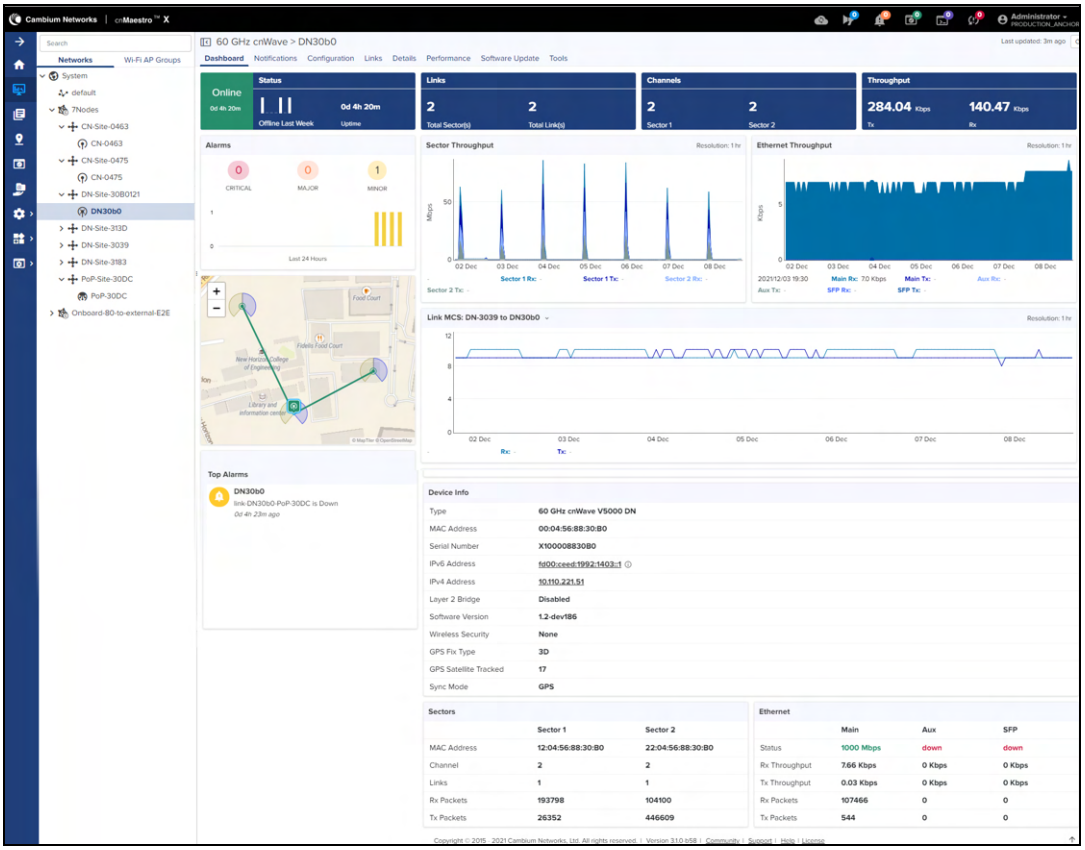
To create a new site, refer to Site.

To create a sub Node, refer to DN/CN.

Dashboard

Dashboard pages are customized for each device type and aggregation level. The DN/CN node dashboard section displays the **Status, Links, Channels, Throughput (Sector 1), Throughput (Sector 2), Throughput (Main), Throughput (Aux), Throughput (SFP), Alarms, Top Alarms, Links MCS, Device Info, Sectors,** and **Ethernet**.

Figure 111 DN/CN Node Dashboard



Configuration

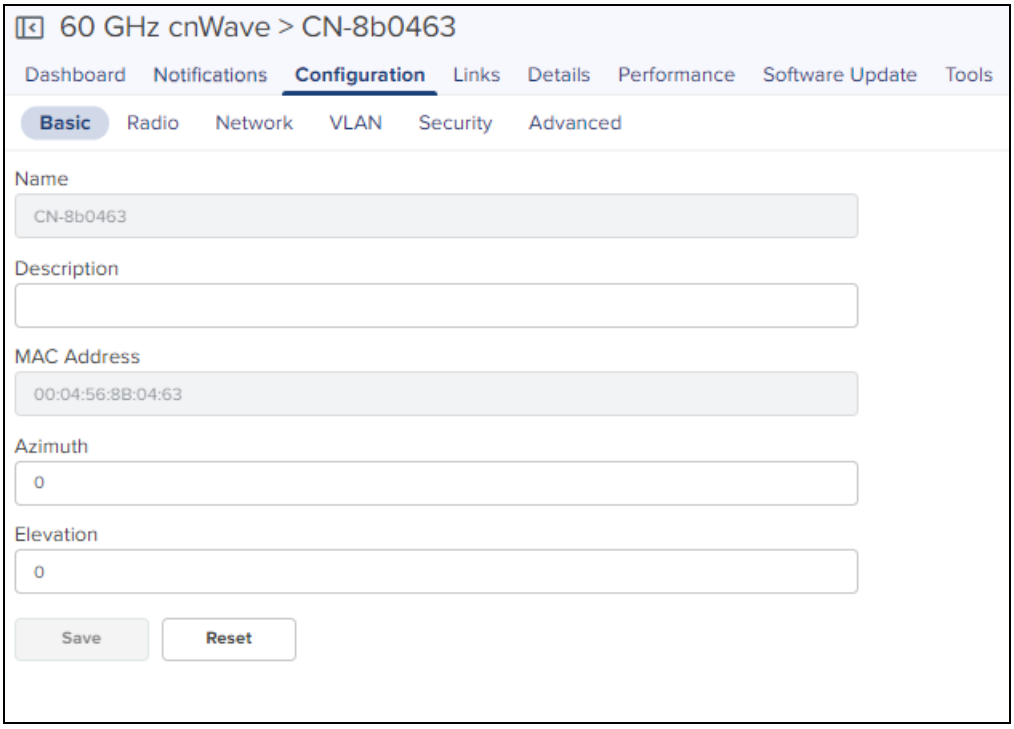
Configuration page allows the user to configure the following details of CN/DN:

- Basic
- Radio
- Network
- VLAN
- Security
- Advanced

Basic

It allows to configure and reset the basic details of DN/CN node such as **Description, Azimuth**, and **Elevation**.

Figure 112 Basic

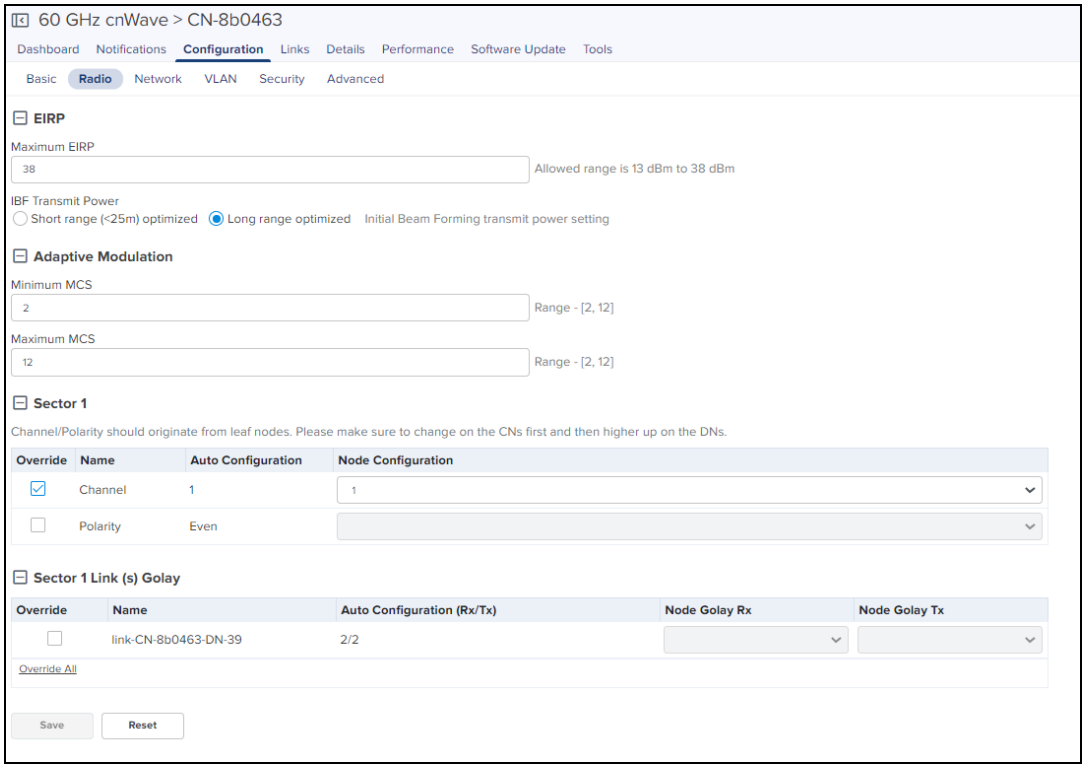


Radio

	NOTE: GPS option is not enable for v1000.

It allows the user to configure the **EIRP**, **Adaptive Modulation**, **Sectors (Channels and Golay)**, and **GPS**.

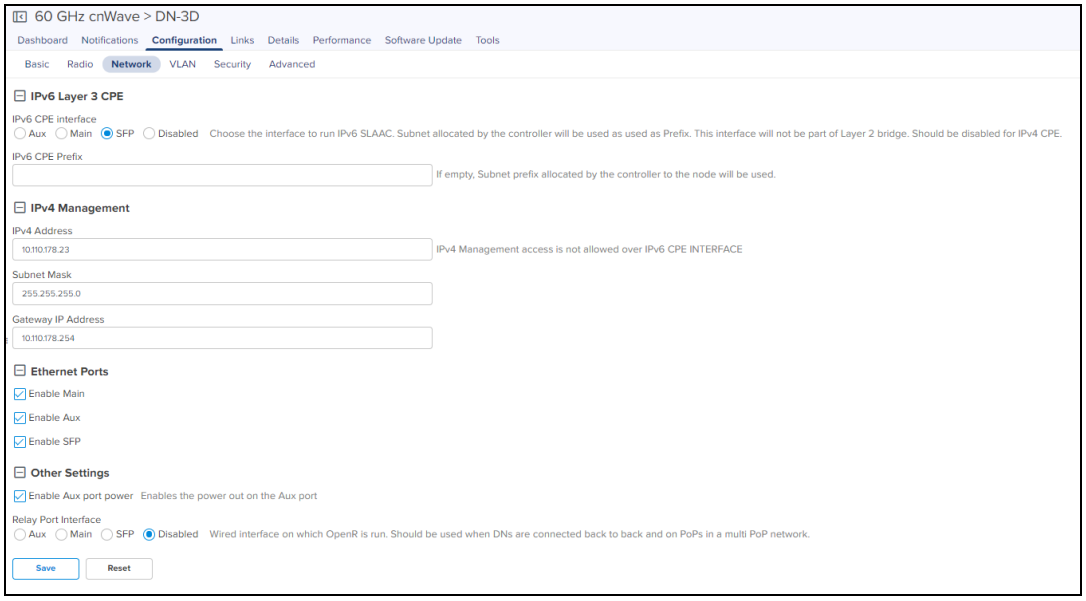
Figure 113 Radio



Network

Network tab allows the user to edit the **Layer 3 CPE, IPv4 Management**, **Ethernet Ports,** and **Other Settings.**

Figure 114 Network



VLAN

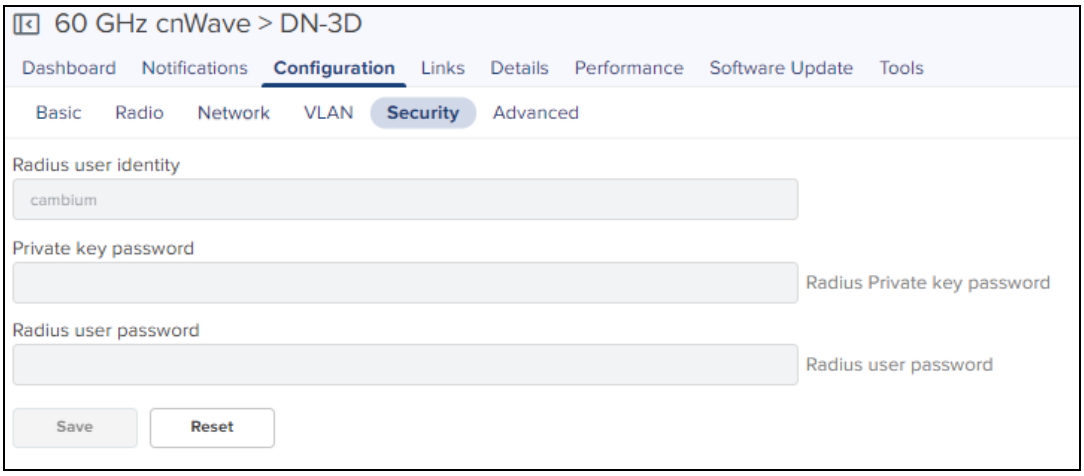
VLAN configuration of CN/DN is same as PoP Node VLAN as shown above.

	NOTE: Enable Layer 2 Bridge in **60 GHz cnWave > Configuration > Basic** page to configure the CN/DN VLAN.

Security

Security tab allows to reset the identity and password of the Radius user.

Figure 115 Security



Advanced

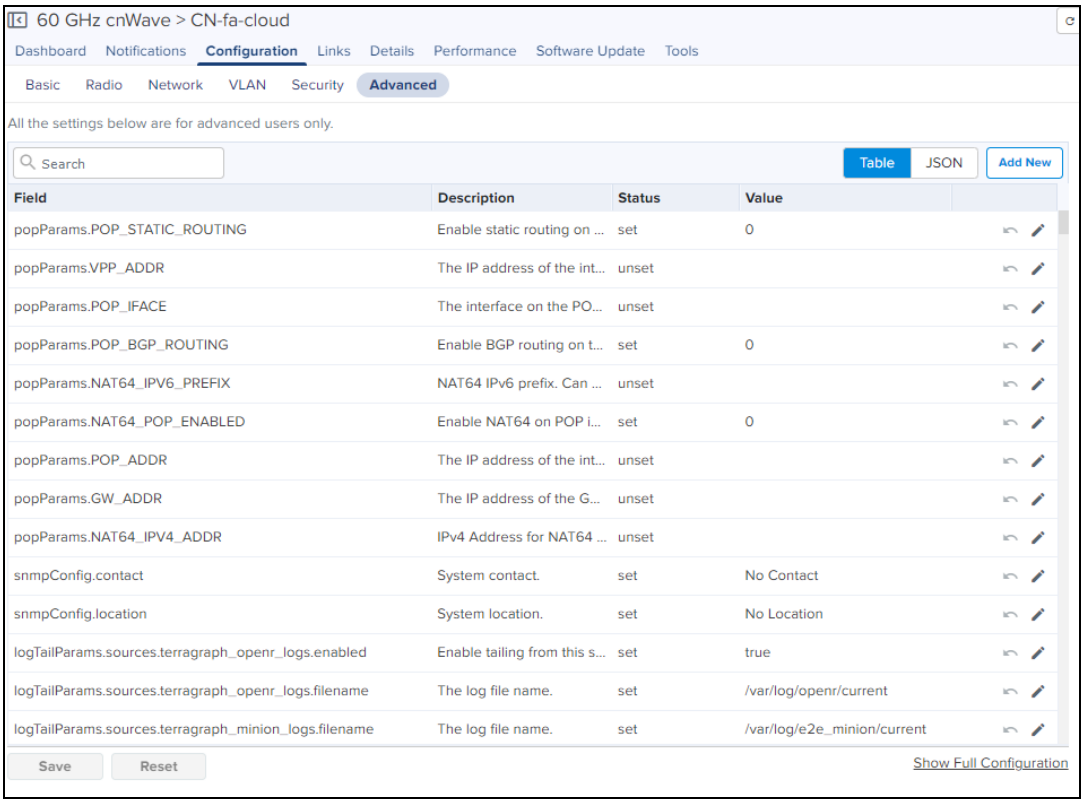
Advanced tab allows the advanced user to edit the settings of the Table and JSON format of the PoP Nodes.

Table

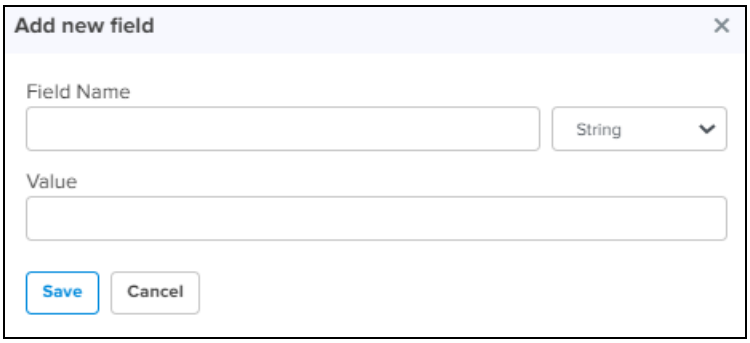
In the **Table** user can able to view, add, and edit **Field Name** and **Value**.

To add a field:

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



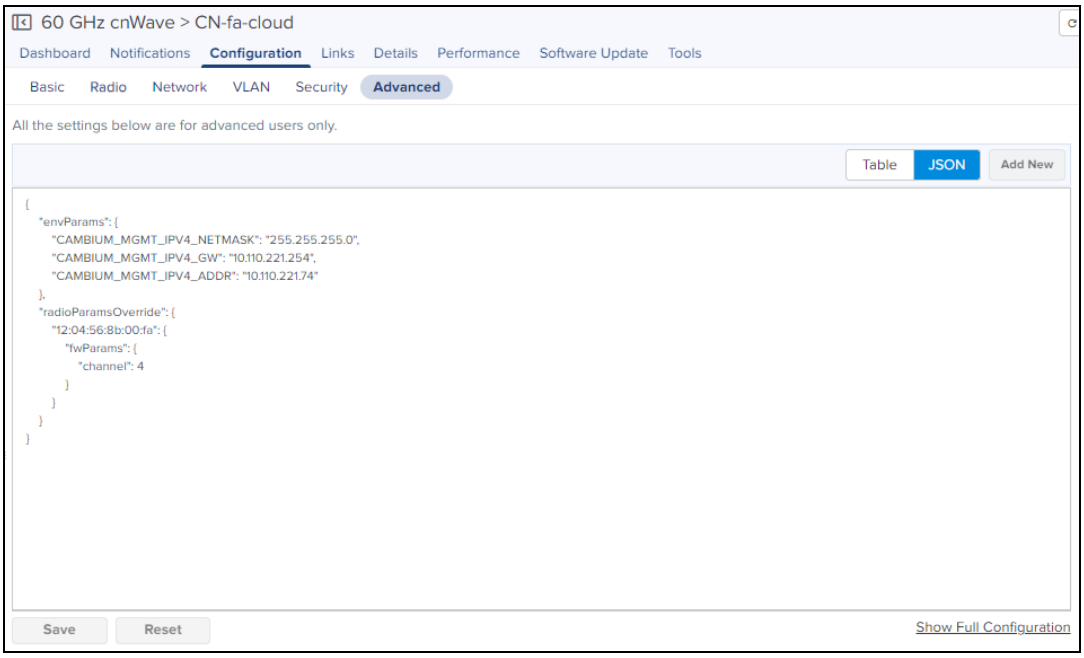
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

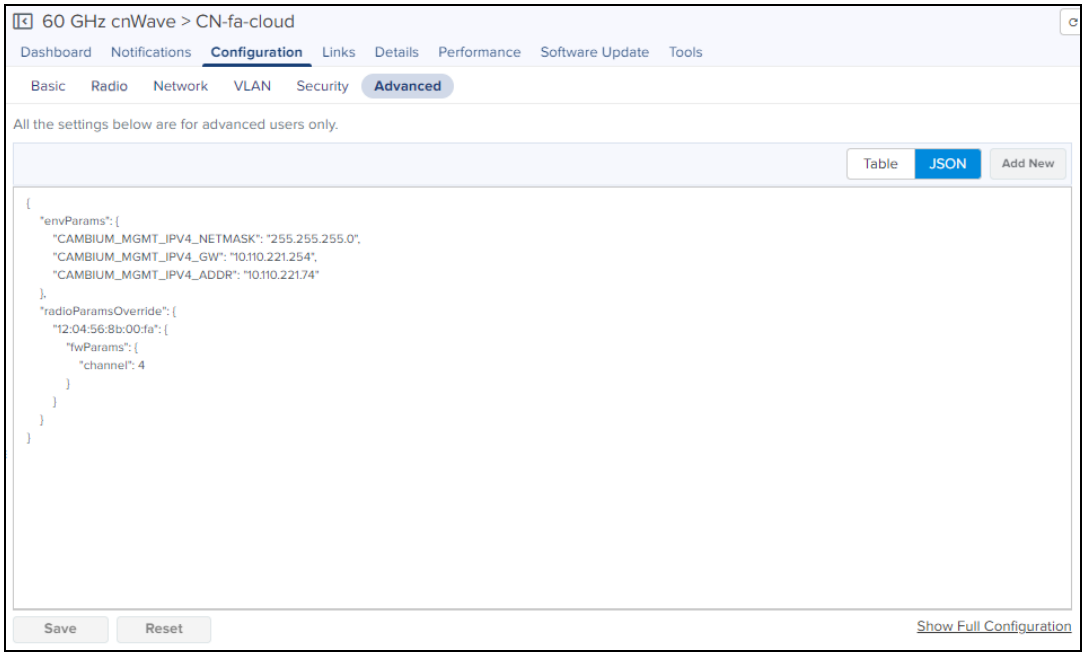
JSON

JSON allows Adavanced user to view the JSON format.



To download the file, perform the following steps:

1. Navigate to **Configuration** > **Advanced > JSON**



2. Click **Show Full Configuration.**
3. **View Device Existing Configuration** pops-up.



4. Click **Download**.

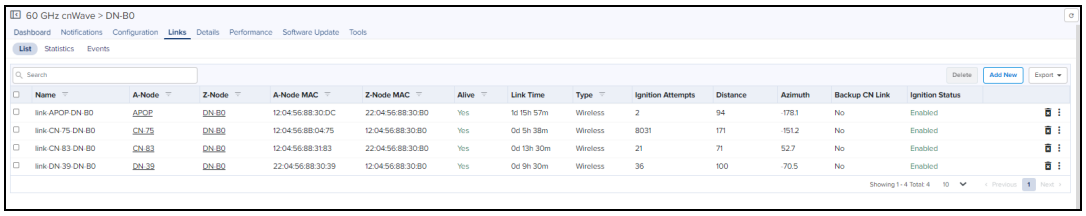
Links

Links provide the details about links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular devices.

List

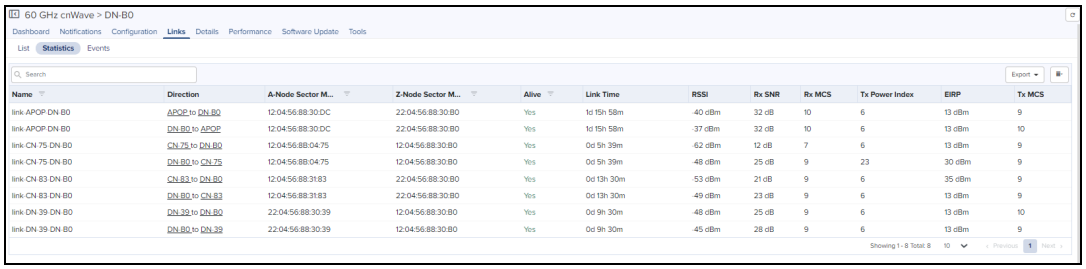
List provide the details about the links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular link.

Figure 116 List



Statistics

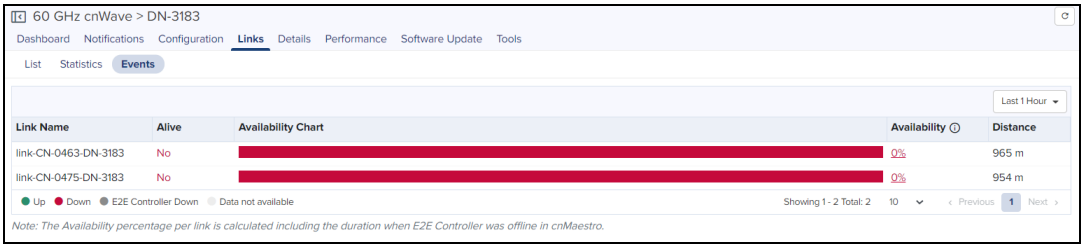
Links Statistics pages provides details of **Name, Direction, A-Node Sector MAC, Z-Node Sector MAC, Alive, Link Time, RSSI, Tx Power Index, A-node, Z-node, Type, Distance, Azimuth, Rx MCS, Tx MCS, Rx PER, Tx PER, Rx SNR, Rx Beam Index, Tx Beam Index, EIRP, Rx Errors, Tx Errors, Rx Frames, Tx Frames** on a single device, generally in a page format.



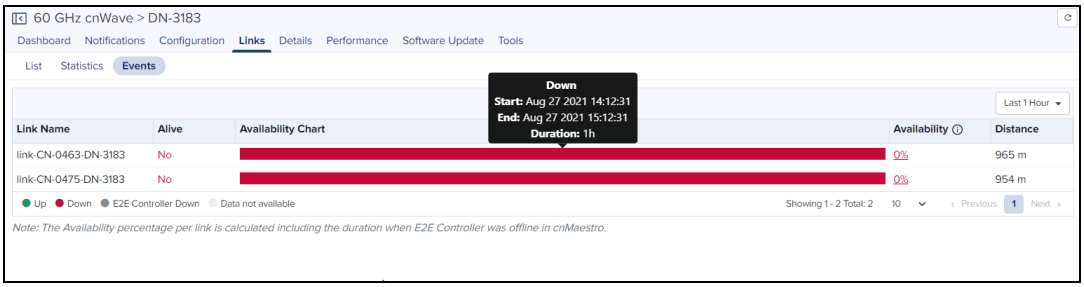
Events

Events provides the details of the links from last 1 hour to 7 Days, Ignition Attempts and Distance.

Figure 117 Events



It also calculates the Availability percentage per link, including the duration when E2E Controller was offline in cnMaestro.



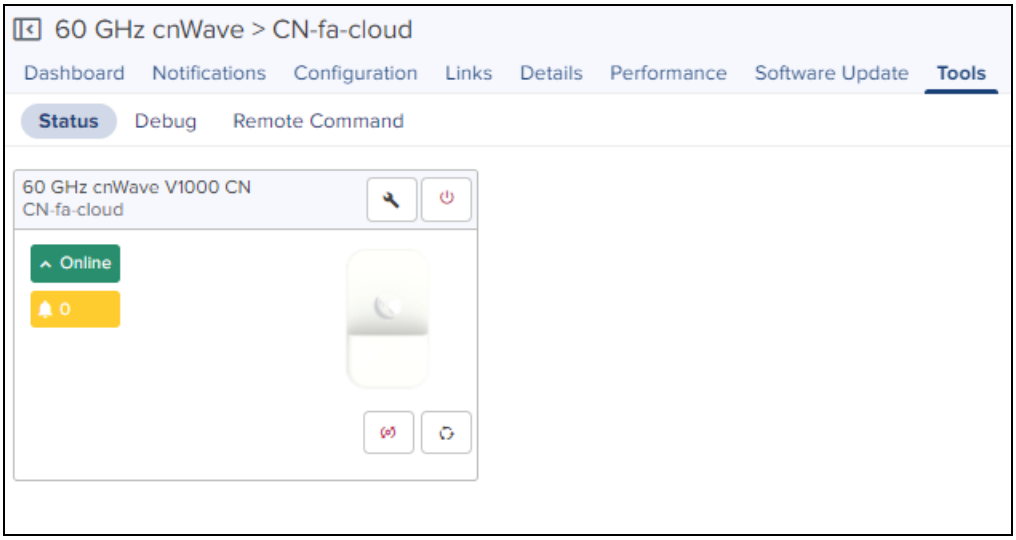
Tools

In Tools page user can able to view the **Status, Debug** and **Remote Command** of the device.

Status

In **Status** tab you can view the status of the device:

- Critical alarms
- Download Tech Support File
- Online or Offline
- Reboot the device.
- Restart Minion
- Factory reset



Debug

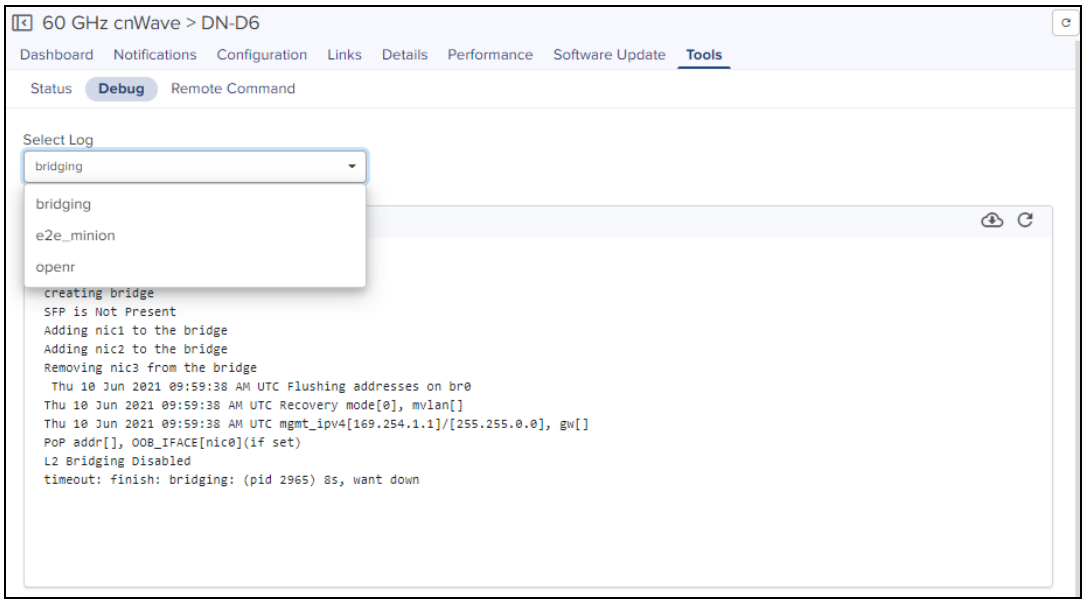
In **Debug** tab user can able to view or download the DN or CN logs by executing the following log commands:

- Bridging
- e2e_minion
- openr

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select the required log name from the **Select Log** drop-down list box.

The output for the selected criteria appears as shown:



- Click the download icon to download the generated output.
- Click the refresh icon to refresh the generated output.

Remote Command

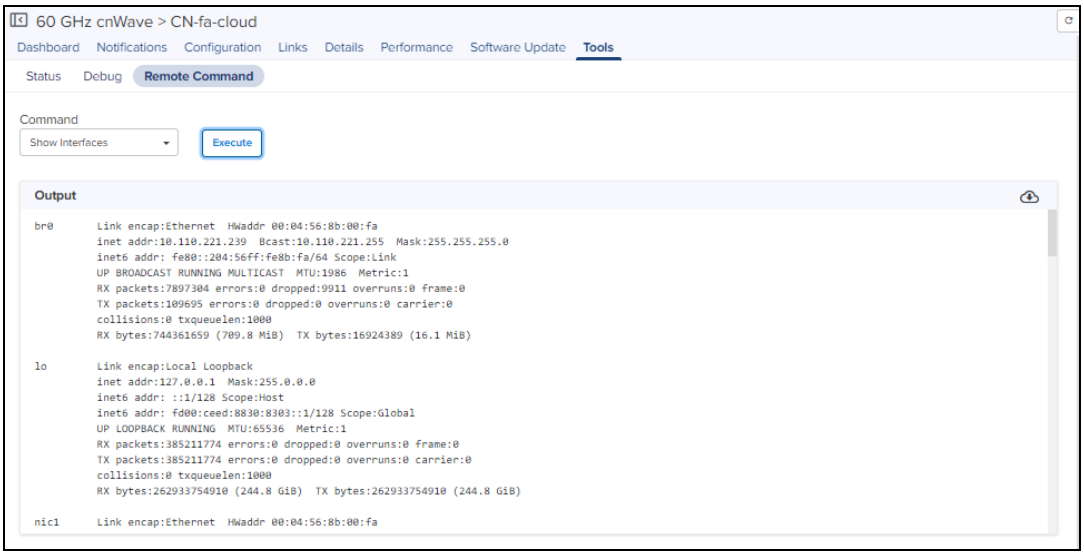
In **Remote command** tab user can able to view or download Command logs by executing the following commands:

- Show Interfaces
- Show Routes
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show SFP Power Details (applicable for V5000 an V3000)

To Execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select the required command from the **Command** drop-down list box.
3. Click **Execute.**

The output for the selected criteria appears as shown:



- Click the download icon to download the generated output.

Auto-Provisioning

cnMaestro On-Premises supports Auto-Provisioning for Wireless LAN devices (cnVision, Wi-Fi, and ePMP 1000 Hotspot) and fixed devices (PMP and ePMP). It is enabled at **Shared Settings > Auto-Provisioning**, and it allows one to automatically configure and approve devices based upon IP address.

	NOTE: Auto-Provisioning is supported only for cnMaestro On-Premises.

Creating Auto-Provisioning Rule

To create a rule for Auto-Provisioning, perform the following steps:

1. Navigate to **Shared Settings > Auto-Provisioning** page.



2. Click **Add** and following window appears.

Figure 118 Auto-Provisioning - Wireless Devices

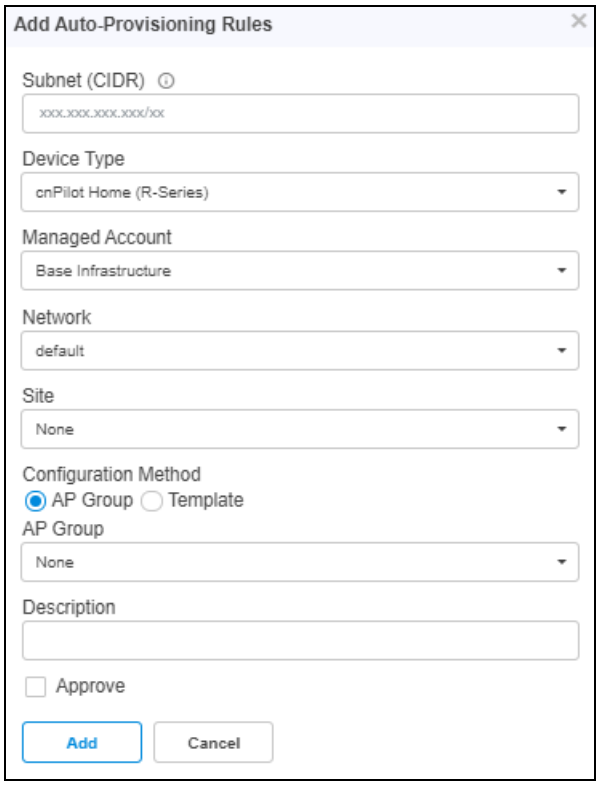
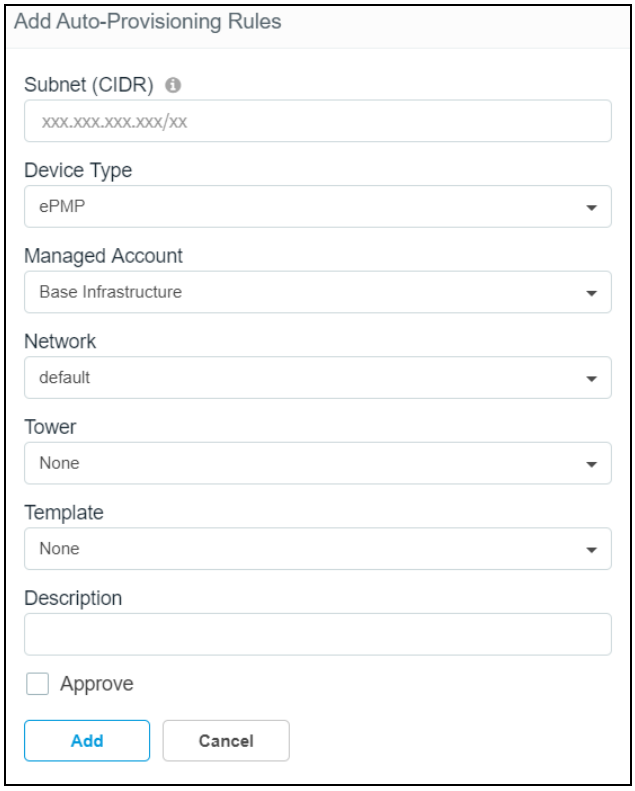


Figure 119 Auto-Provisioning - Fixed Devices



3. Enter the following details:
   - **Subnet:** The subnet with CIDR of the devices to which the rule has to be applied.
   - **Device Type:** Select the rule to be created for Enterprise Wi-Fi, cnVision, Home (R-Series), ePMP, or PMP devices.
   - **Managed Account:** Select the Managed Account from the list.
   - **Network:** To which network the device should be onboarded, once device contacts the server.
   - **Site:** Under which site the device should be onboarded, once device contacts the server, applicable for Enterprise (E) or Home (R).
   - **Tower:** Under which site the device should be onboarded, once device contacts the server, applicable for ePMP AP or PMP AP.
   - **Template:** To which template to be applied on the device when onboarding, once device contacts the server, applicable for ePMP AP or PMP AP.
   - **AP Group:** To which AP Group to be applied on the device when onboarding, once device contacts the server, applicable for Enterprise (E) or Home (R).
   - **Description:** Type the information to add additionally.
   - **Approve:** The device should be auto-approve or needs manual approval for onboarding.
4. Click **ADD**.

Services

This section includes the following topics:

- Managed Service Provider (MSP)
- API Client
- cnPilot Guest Access
- cnPilot Data Tunnels
- SNMP
- RADIUS Proxy

Managed Service Provider (MSP)

This section includes the following topics:

- Overview
- Configuring Managed Services
- Managed Services Administration

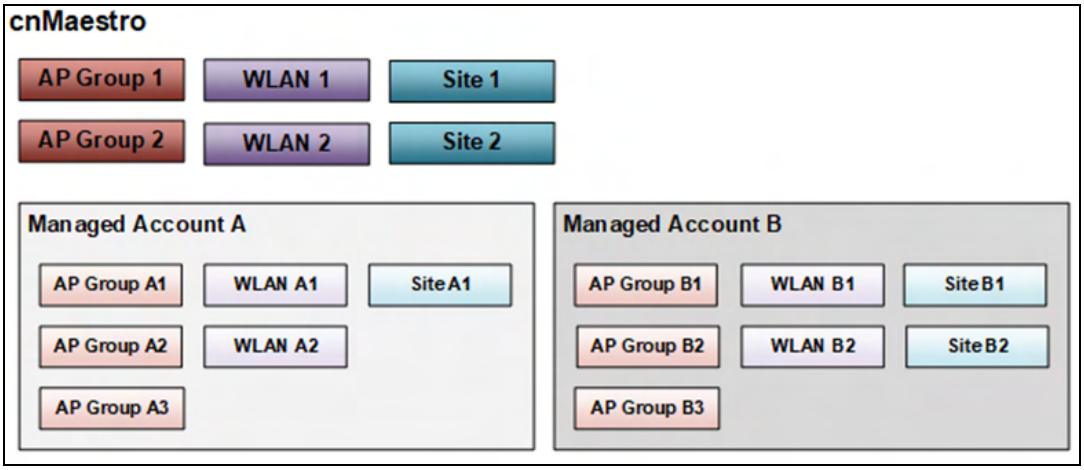
Overview

Managed Service Provider (MSP) allows a cnMaestro account owner to partition their installation into separate Managed Accounts – each with its own independent administration and configuration. This feature is for managed service providers who want to provision a full cnMaestro infrastructure for their customers but still maintain control over the individual deployments.

Managed Accounts

Managed Accounts group cnMaestro devices and configuration objects (such as AP Groups, WLANs, and Sites) into administration domains within a single cnMaestro instance. Managed Accounts are independent, and the devices added to them are configured using the objects in the Managed Account.

Figure 120 Managed Accounts



Scope

An account with MSP enabled has three scopes:

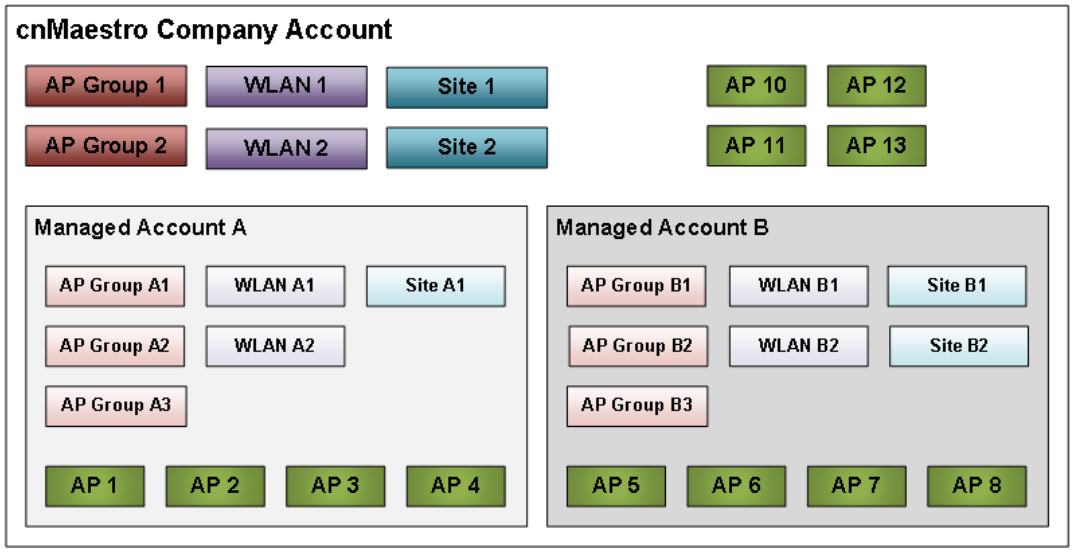
1. Global Scope for entities (Devices, Networks, Sites, etc.) that exist outside of Managed Accounts and are only available to Global cnMaestro Administrators.
2. Managed Account Scope for entities in Managed Accounts and accessible to Global Administrators and Managed Account Administrators.
3. Shared Scope applies to management objects such as AP Groups, WLANs, and Switch Groups. Shared Scope objects can be used across all Managed Accounts but not modified by them, though they can be copied into the Managed Account and then changed.

Access Points

Access Points exist in the global cnMaestro application, or they can be added to a single Managed Account.

	NOTE: The Managed Service Provider feature supports all device types available within cnMaestro.

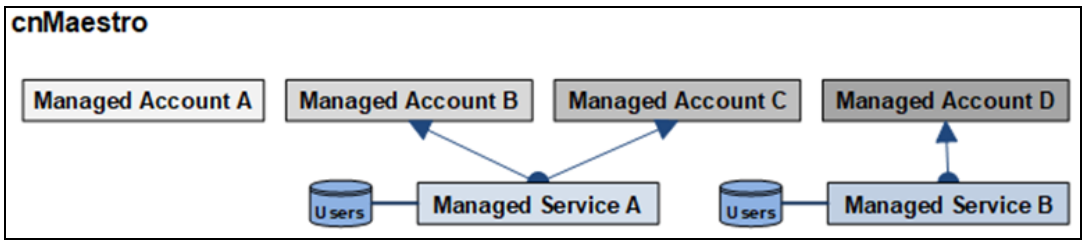
Figure 121 Access Points



Managed Service

A Managed Service creates customized version of the cnMaestro UI and assigns Managed Accounts. Each Managed Service can be mapped to many Managed Accounts.

Figure 122 Managed Service



Each Managed Service adds the following support to a Managed Account:

Support	Details
Administrator Database	Each Managed Service has its own independent database of users who can be assigned to multiple Managed Accounts.
Custom Login URL	The path of the Login URL used by Managed Service Administration can be tailored to represent the Managed Service. The path must be unique across all cnMaestro.
Managed Account UI	The Managed Account UI is customized for the Managed Service through graphics, colors, and text.

Managed Account UI

The Managed Account UI can be customized to represent the brand. A sample Managed Account UI is shown below:

Figure 123 Managed Account UI - Sample 1

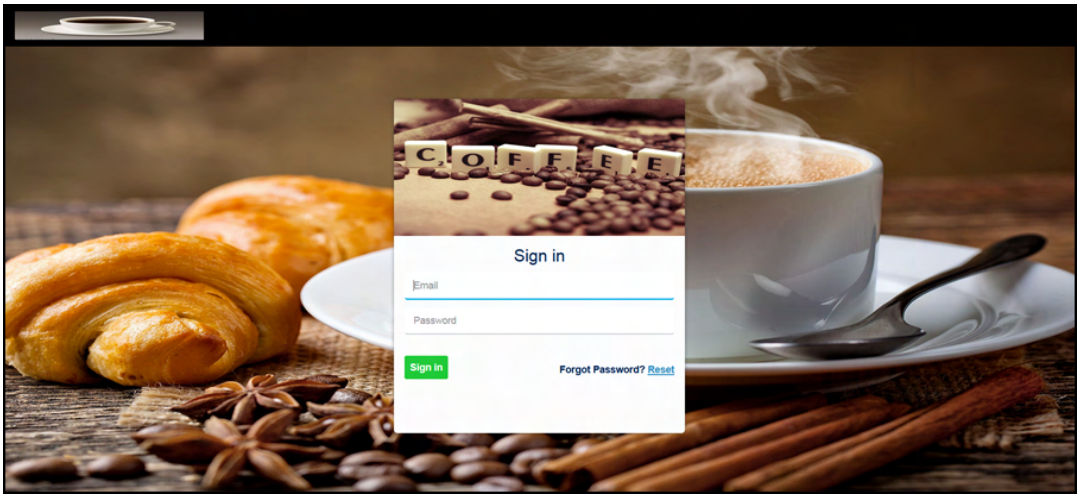
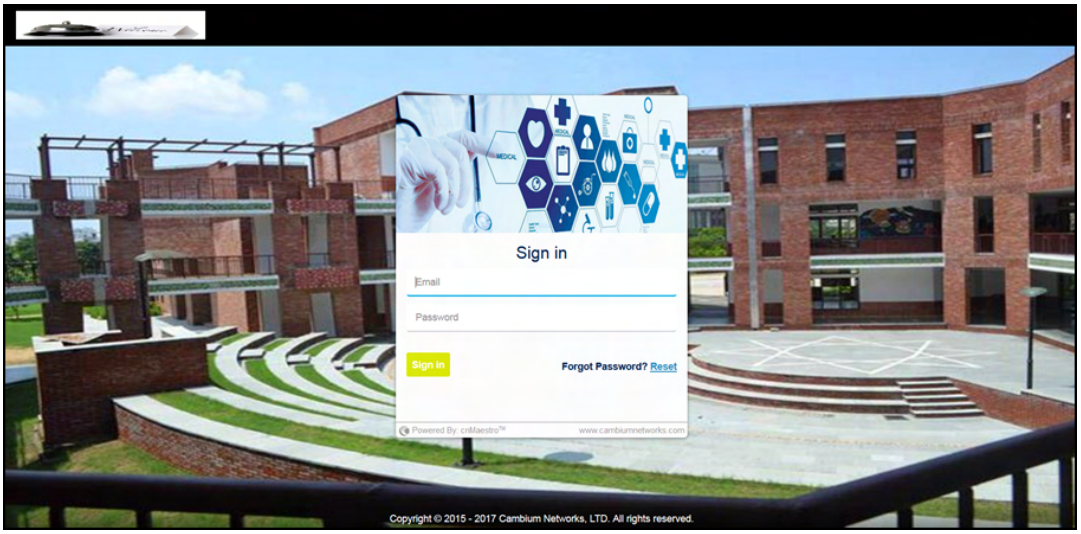


Figure 124 Managed Account UI - Sample 2



Managed Service Provider (MSP)

The MSP feature combines Managed Accounts with Managed Services.



Managed Service Users (Administrators)

Managed Service Users are assigned to Managed Accounts. They access nearly all the same features as the Global cnMaestro Administrators, except they are only allowed to manage the subset of devices and objects (AP Groups, WLAN, Sites, etc.) in their account.

Managed Service Users (Administrators) Roles

Managed Service Administrators can be assigned one of three roles as shown below for each account:

- Administrator
- Monitor
- Operator

The authorizations for each role are listed in the table below:

Table 38: Tenant Administrator Roles

Feature	Description	Administrator	Operator	Monitor
AAA Services (Global cnMaestro Administrator only)	Add AAA services	None	None	None
Administration Settings (Global cnMaestro Administrator only)	Change global application configuration, onboarding settings like password change	None	None	None
API Management (Global cnMaestro Administrator only)	Create API Clients	None	None	None
Application Operations 1	Networks, Tower, and Site creation	All	All	View
Application Operations 2	Tech Dump, import/export server data, account type change (backhaul and Wi-Fi)	None	None	None
Association ACL	Configure MAC list on the controller	All	View	None
Auto-Provisioning (Global cnMaestro	Support for global auto-provisioning rules	None	None	None

Table 38: Tenant Administrator Roles

Feature	Description	Administrator	Operator	Monitor
Administrator only)				
Audit logs	Log administration updates	All	All	All
Data Tunnel (Global cnMaestro Administrator only)	Data Tunnel configuration	None	None	None
Device Operations	Reboot device, Link Test, Connectivity Test	All	All	None
Device Override	Per-device configuration changes	All	All	View
Global Configuration	Templates and AP Groups; ability to apply configuration	All	View	View
Guest Portal	Guest Access	All	View	View (Sessions)
Monitoring	Statistics data from device	All	All	View
Notifications	Alarms and Events	All	All	View
Onboarding	Device approval	All	All	View
Reporting	Report generation view	All	All	All
Software Images (Global cnMaestro Administrator only)	Download device software images	All	None	None
System Operations	Reboot VM, change log level, system upgrade, system monitoring	None (Except System Monitoring)	None (Except System Monitoring)	None (Except System Monitoring)
Software Upgrade	Upgrade device	All	All	View
User Management	Manage users, roles, sessions	All	None	None

Configuring Managed Services

This section provides the following configuration details for Managed Services:

- Enable Managed Service Provider (MSP)
- Create Managed Services
- Create Managed Account
- Validate Managed Account Administrators

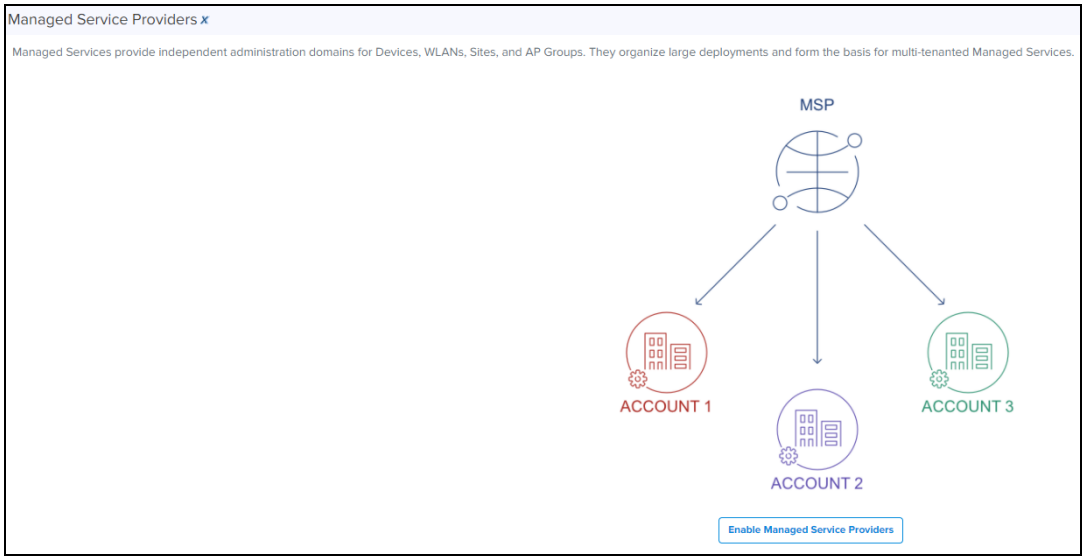
Enable Managed Service Provider (MSP)

By default, MSP is disabled in the cnMaestro UI.

To enable MSP:

1. Navigate to **Managed Service Providers** in the side-menu.
2. Click **Enable Managed Services**.

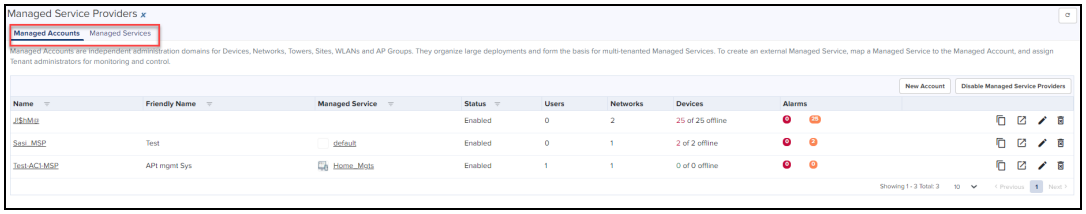
Figure 125 Enabling Managed Services



Additions in the cnMaestro UI when Managed Services is Enabled

- Once Managed Services is enabled, **Managed Account** and **Managed Services** tabs appears in the cnMaestro UI. The Managed Services page is replaced with Managed Accounts and Managed Services tables as shown below:

Figure 126 Managed Account and Managed Services Tabs



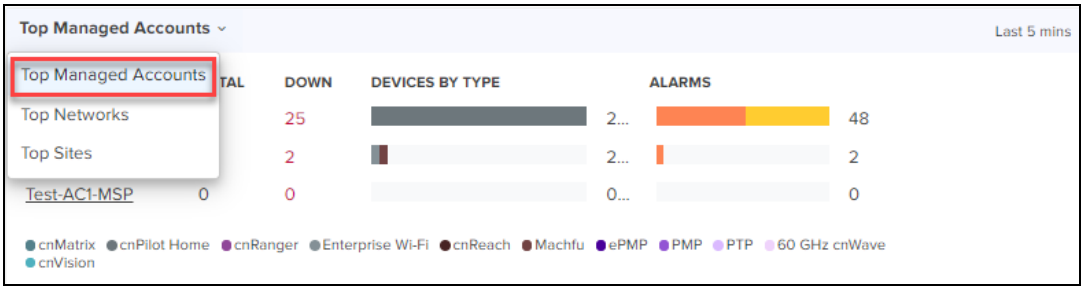
- The Header adds a select box that allows the global administrator to enter the context of Managed Accounts.

Figure 127 MSP Component in Header



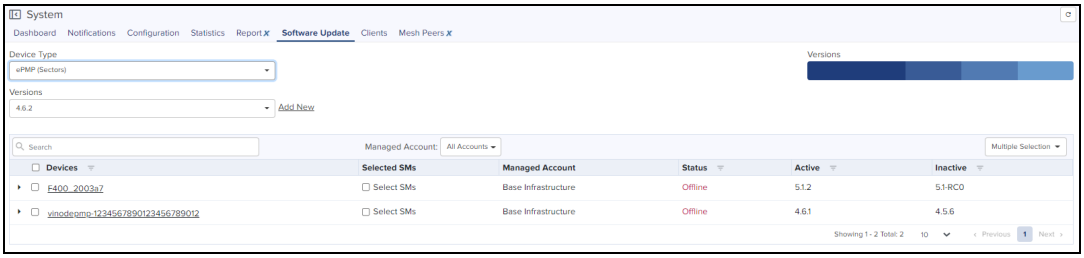
- The System Dashboard adds a Health component for Managed Accounts.

Figure 128 Dashboard > Managed Accounts



- Global tabs in the UI are updated with a Managed Account column.

Figure 129 Managed Account column



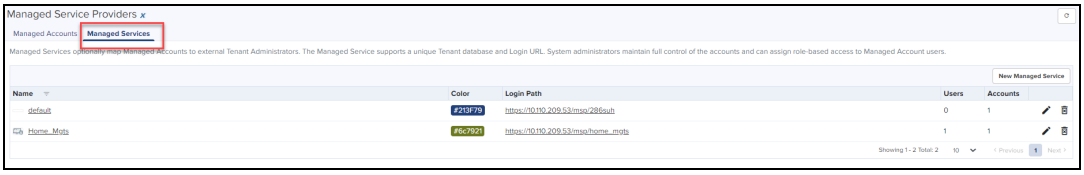
Create Managed Services

The user can create a Managed Service and map it to a Managed Account. The Managed Service supports an independent user database and a customized user interface. There is a default Managed Service, so creating a new service is optional.

Perform the following steps to create a Managed Service:

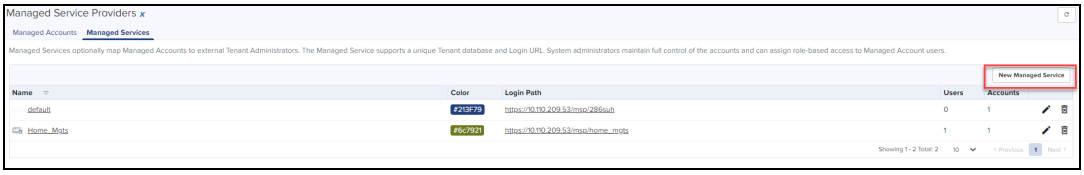
1. Select **Managed Service Providers** in the side-menu and select the **Managed Services** tab.

Figure 130 Managed Services tab



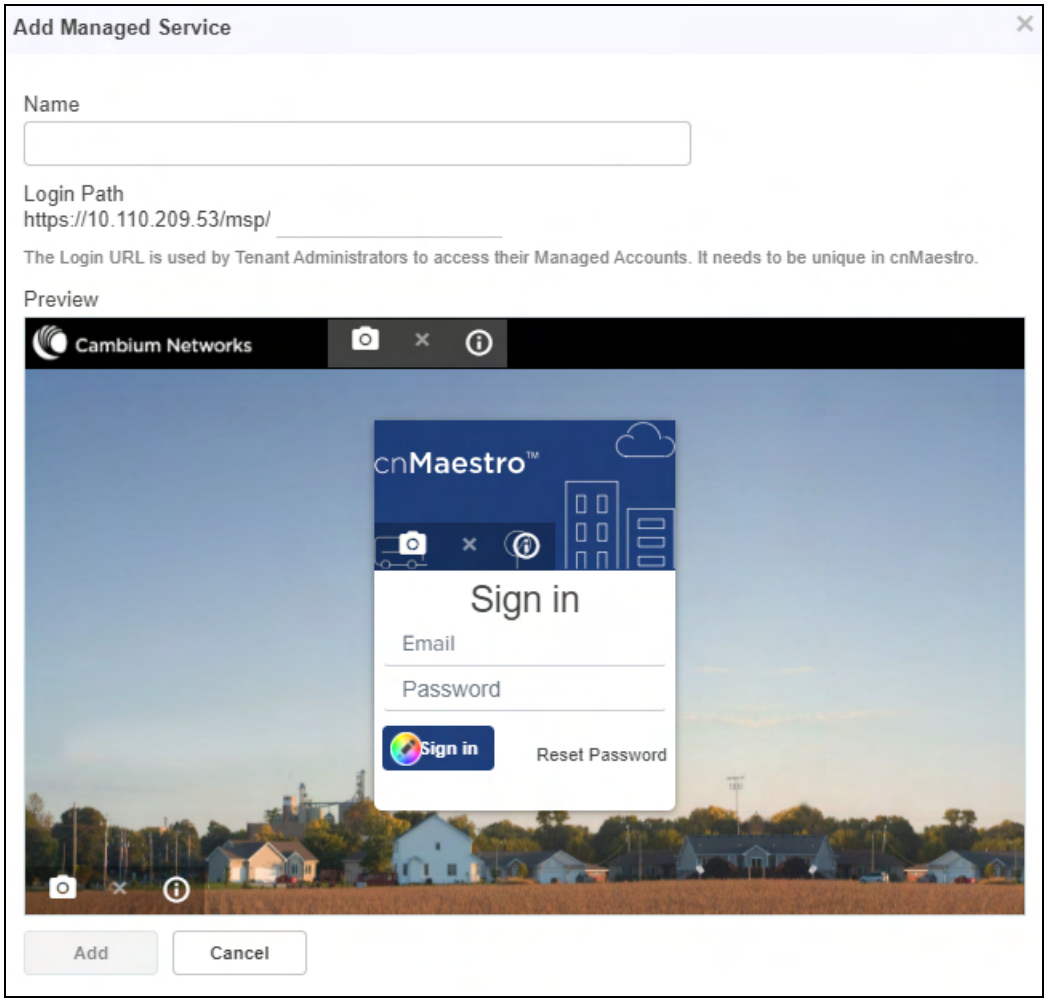
2. Click **Managed Service**.

Figure 131 Adding a New Managed Service



The following window appears.

Figure 132 Add New Managed Service window



3. Enter the following details:

Table 39: New Managed Service parameters

Parameter	Description
Name	Name of the service. This name is visible to Managed Account Administrators. A maximum of 64 characters are supported for the name.
Login Path	Managed Account Administrators log into cnMaestro using a standard URL with an additional Path that defines the Managed Service. For example: https://<cnmaestro on-premises ip>/msp/<Managed_service_path> **Note:** • The Path name must be unique across all Managed Service accounts when cnMaestro is hosted in the Cambium Cloud. • A maximum of 16 characters are supported for the path.

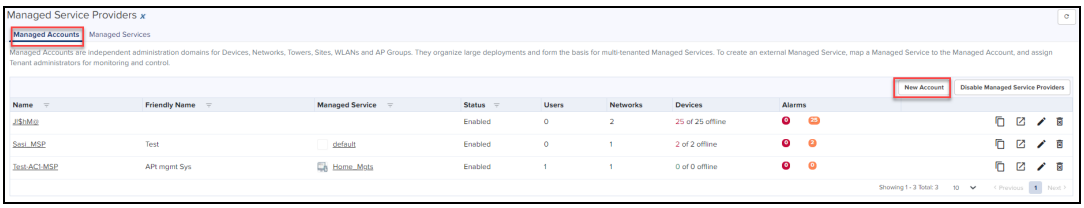
4. Click **Add**.

Create Managed Account

Perform the following steps to create a Managed Account:

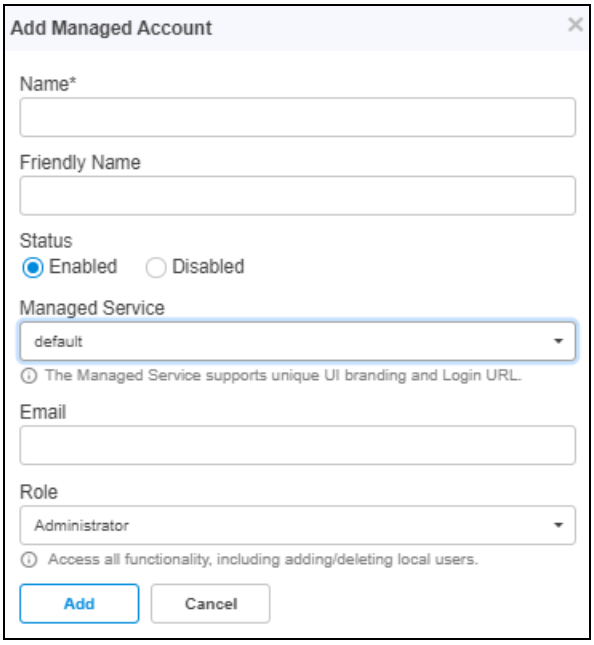
1. Select **Managed Service Providers** in the side-menu and select the **Managed Account** tab.
2. Click **New Account**.

Figure 133 Managed Account tab



The following window appears:

Figure 134 Add Managed Account window



3. Enter the following details:

Table 40: Managed Account parameters

Parameter	Description
Name	Name of the Managed Account. This is sent in the invitation email when Managed Account Administrators are invited to the account.
Friendly Name	The Friendly Name will be sent in the invitation email.
Status	Determines whether the account is enabled or disabled. When an account is disabled, all Managed Account Administrators are logged out.

Table 40: Managed Account parameters

Parameter	Description
Managed Service	The Managed Service used for Managed Account Administrator.
Email	The email address of the first Managed Account Administrator. You can add more Users after the account has been created.
Role	The role of the Managed Account Administrator (Administrator, Operator, Monitor).

4. Click **Add**.

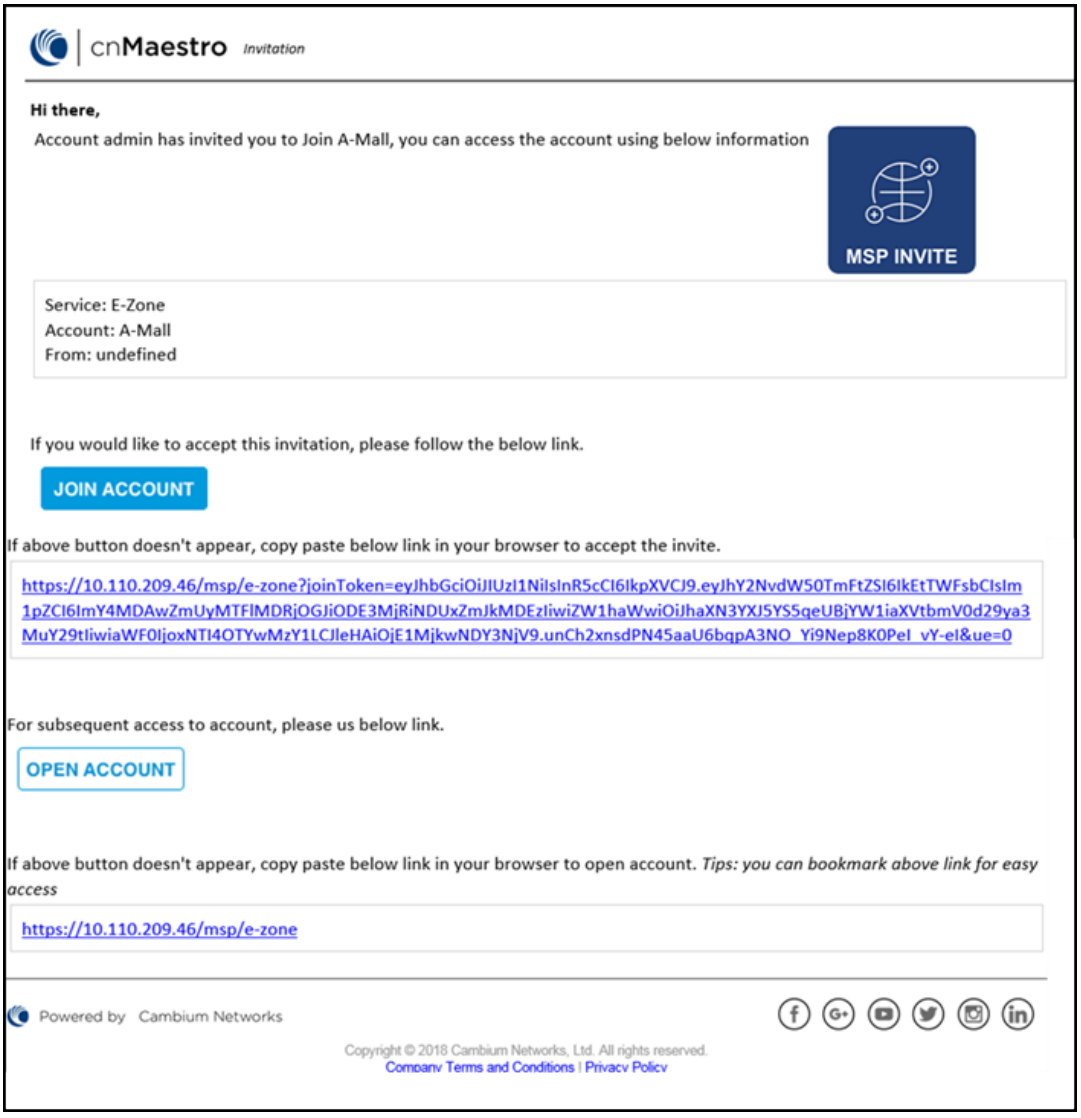


NOTE:
Users are allowed to edit the existing name of the Managed Account before validating the account.

Validate Managed Account Administrators

Once a Managed Account is created, the Managed Account Administrator is sent an email invitation. The email provides directions on how to access the Managed Account UI and set their password.

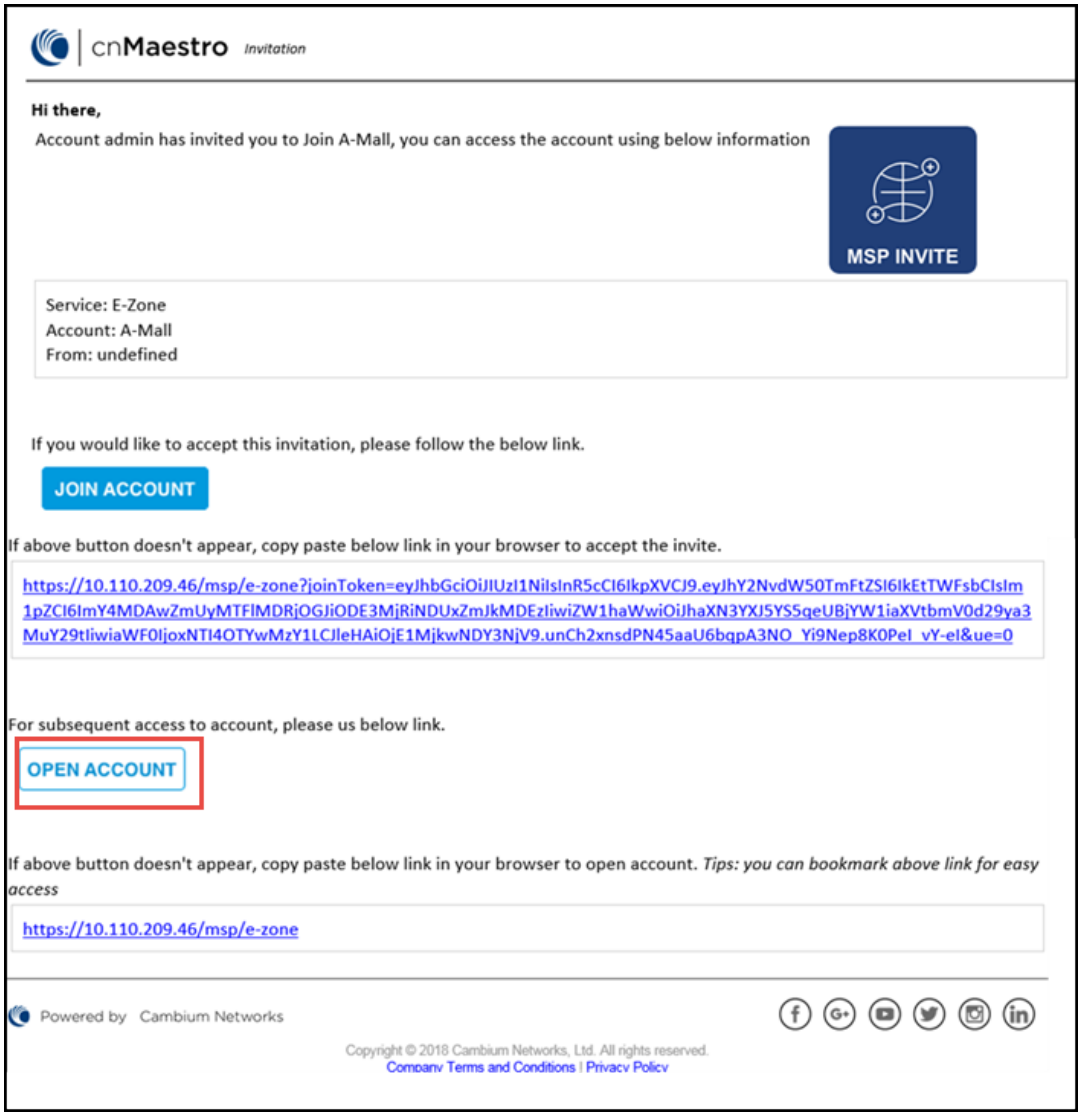
Figure 135 Sample Email invitation



Check Email for invite

An email is sent inviting the Managed Account Administrator to view their new Managed Service account. It has a link that must be clicked to enable access.

Figure 136 Checking Managed Account Administrator User Email



Create Account in Branded Service

Clicking the link prompts the user to create a new account or use an existing account.

> **NOTE:**
> If a user already has an account in the Managed Service, they can use their existing email login to accept the invite for the new account. Switching between accounts is accomplished using the choice box in the UI header (upper-right).

Login to the Managed Account UI

Once the Managed Account Administrator (User) is created, use the Managed Service URL to login.

Figure 137 A Sample Login URL



Managed Services Administration

Overview

Once Managed Services is enabled, there are three ways for administrator to Managed Accounts.

- System View
- Managed Account View
- Managed Account Administrator (User) View

Important Points to Remember

Please note the following points for managed services administration:

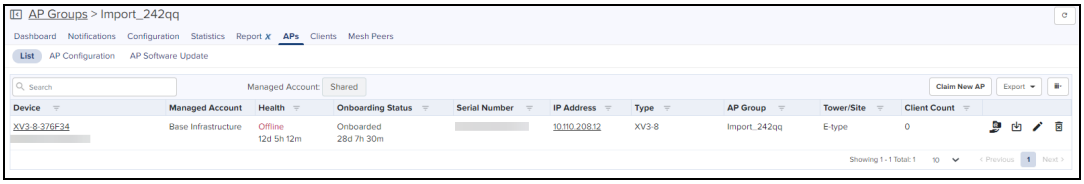
NOTE:

- When a device is moved from one Managed Account to other, it goes offline for one minute before appearing online. Only active alarms are moved to the new account and other data is retained in the old account.
- The Managed Service Provider feature can be disabled only if all devices in Managed Accounts are deleted or moved to Base Infrastructure account.
- Administrators of any Managed Accounts do not have access to the settings page of the On-Premises server to change the account type.
- When Global Super Administrators trigger Configure/Software/Reports Jobs, the Managed Account users cannot view them in any of the Managed Accounts.
- When Managed Account users trigger Configure/Software/Reports Jobs, they are reflected under the Global Super Administrator view along with respective Job IDs enrolled in the respective Managed Accounts.
- The devices that have not started Software/Configure Jobs cannot be moved across Managed Accounts.
- The Global Super Administrator and the Managed Account Administrator cannot trigger a Software or Configure Job simultaneously on the same device.
- The Lock AP configuration can be enabled only by the Global Super Administrator. But whenever a device configuration is changed outside of cnMaestro by either a Global Super Administrator or a Managed Account Administrator, the Auto Synchronization Job starts automatically with the configuration job ID as in Managed Account and reflects in both the Global Super Administrator and Managed Account Administrator accounts.

System View

At the System level, one can view APs, AP Groups, or Sites across all Managed Services in a single, unified table. This allows one to review the status of all accounts in context to each another. The following figure displays the AP table, and specifies which APs are mapped to the Managed Accounts.

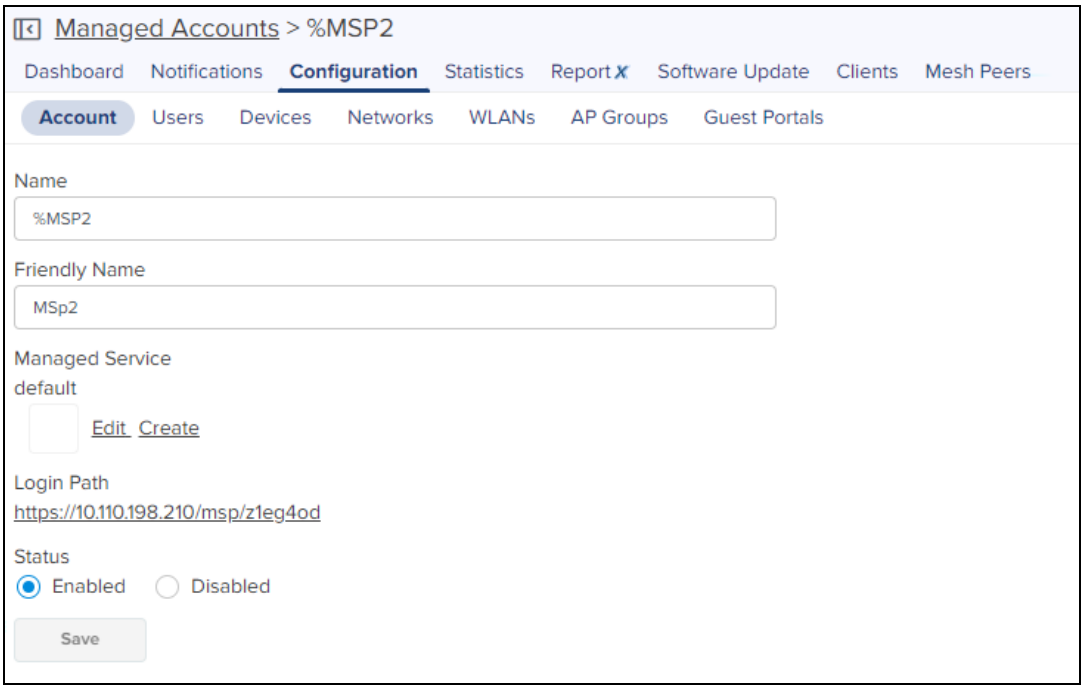
Figure 138 System View



Managed Account View

The Managed Accounts page allows you to select the Managed Account, which launches the Managed Account View. This provides full status and configuration for all components of the Managed Account, including Dashboard, Notifications, Configuration, Software Update, Reports, Clients, etc.

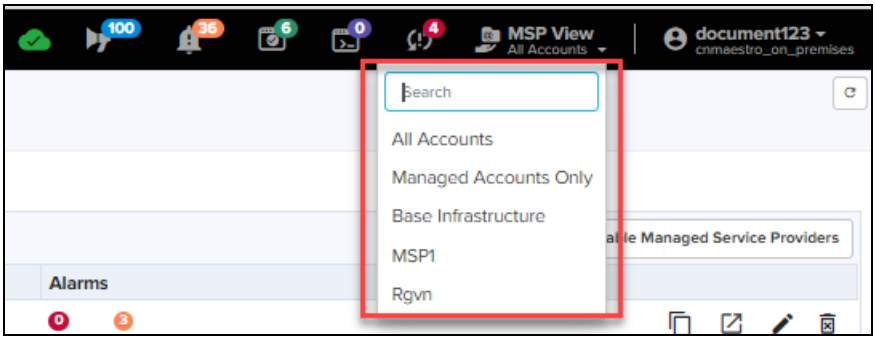
Figure 139 Managed Account View



Managed Account Administrator (User) View

The Managed Account Administrator View presents the branded Managed Account UI, without having to explicitly log into it. It is accessed through the Managed Account drop-down in the UI header. Selecting a specific Managed Account (rather than "All") updates the UI to the Managed Account Administrator's view. From here, the Global Administrator can update the configuration and monitor issues.

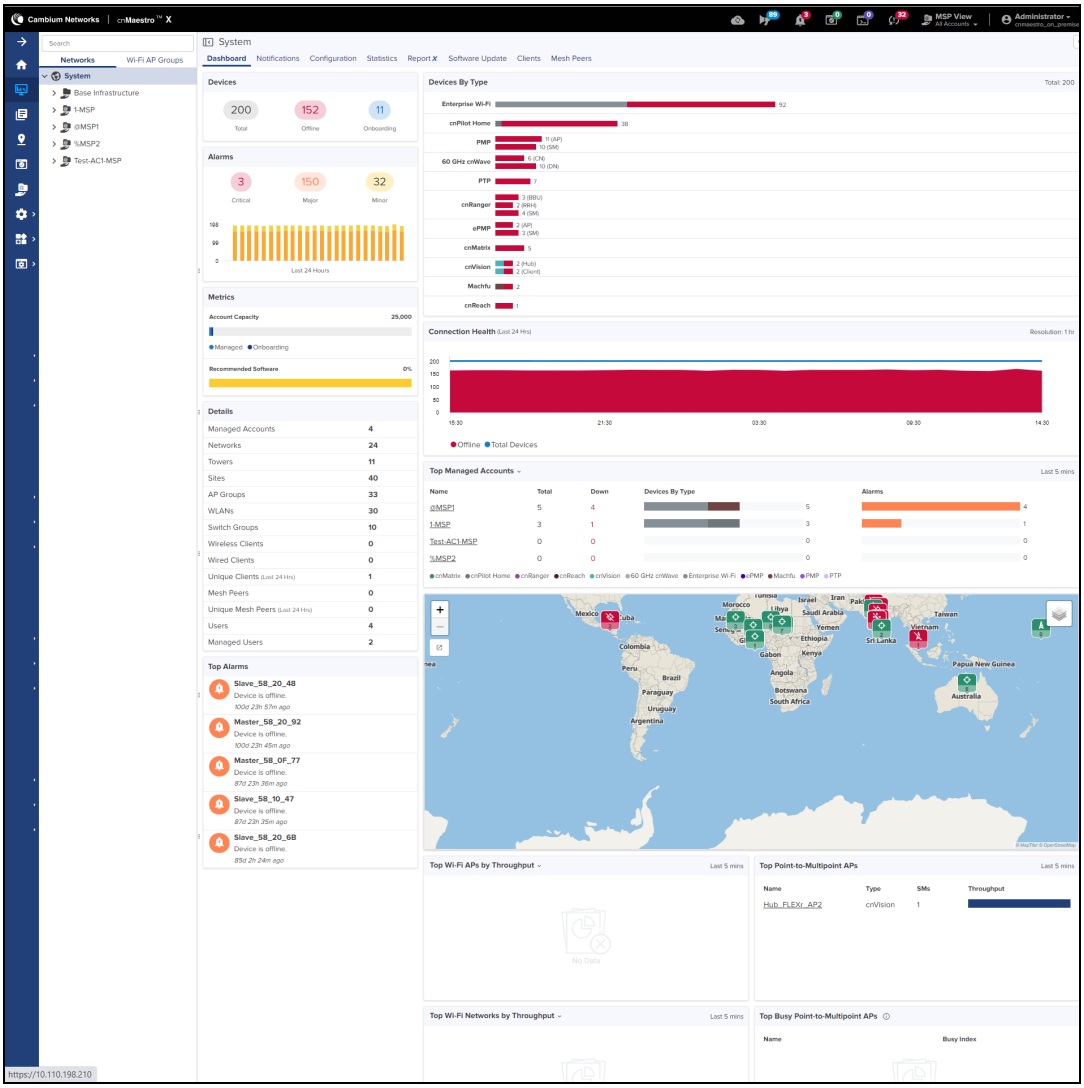
Figure 140 Managed Account View



System Dashboard

The System Dashboard integrates Managed Accounts into the global health component. It ranks the top Managed Accounts based upon device count.

Figure 141 System Dashboard



Managed Account Administration

Object Scope

AP Groups, WLANs, and Switch Groups have three types of accessibility scope as shown below:

Table 41: Accessibility Scopes

State	Description
Base Infrastructure	The object is only available for the Global account.
Managed Account	The object belongs to a Managed Account.
Shared	The object is shared among all Managed Accounts. It can be mapped to devices in the Managed Account, but it cannot be modified. To change the configuration, it needs to be copied into the Managed Account and then update.

NOTE:
Once the scope has been configured on an object it cannot be changed.

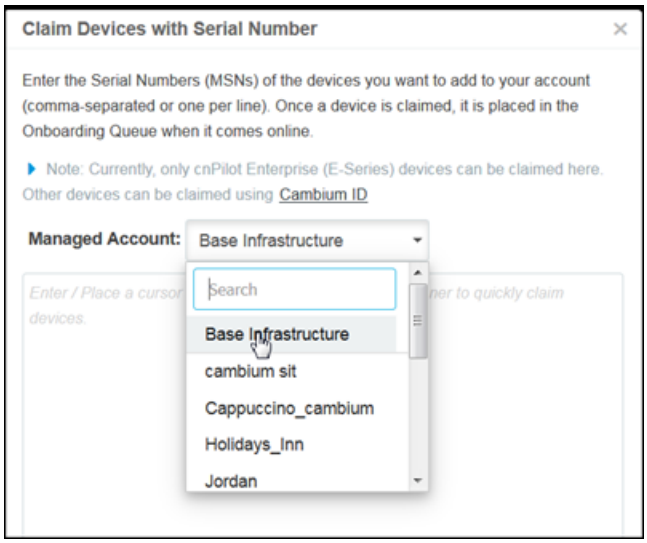
Device Management

Devices are added at the global System level or within Managed Accounts. Devices added at the System level can be moved into Managed Accounts at a later time.

System Onboarding

Onboarding at the global System level supports both MSN and Cambium ID. In the example below, a Managed Account can be selected for all devices onboarded in the MSN batch.

Figure 142 System Onboarding



Management Account Onboarding

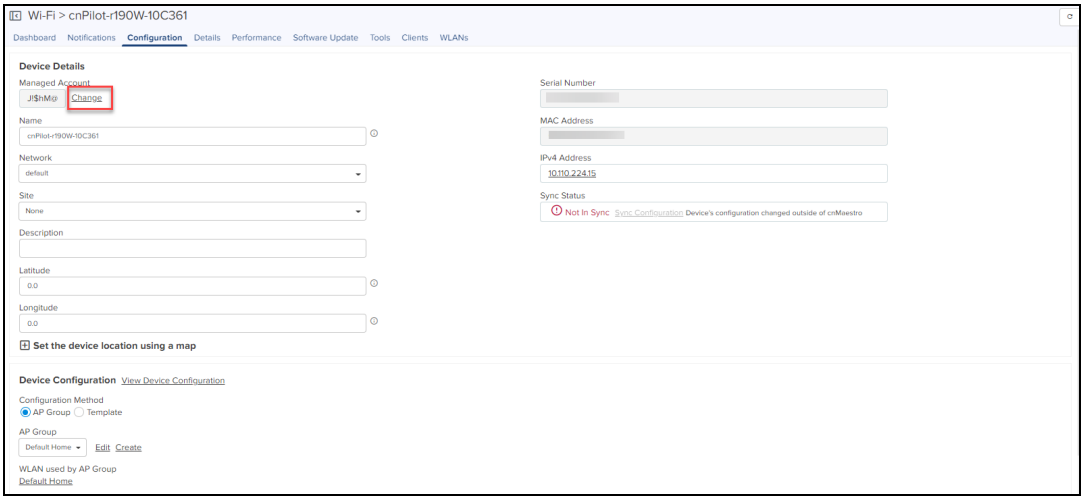
Onboarding through the Managed Account UI automatically places the devices in the Managed Account.

NOTE:
cnMaestro supports onboarding through either MSN or Cambium ID. Within Managed Accounts, only MSN onboarding is supported.

Moving a Device Between Managed Accounts

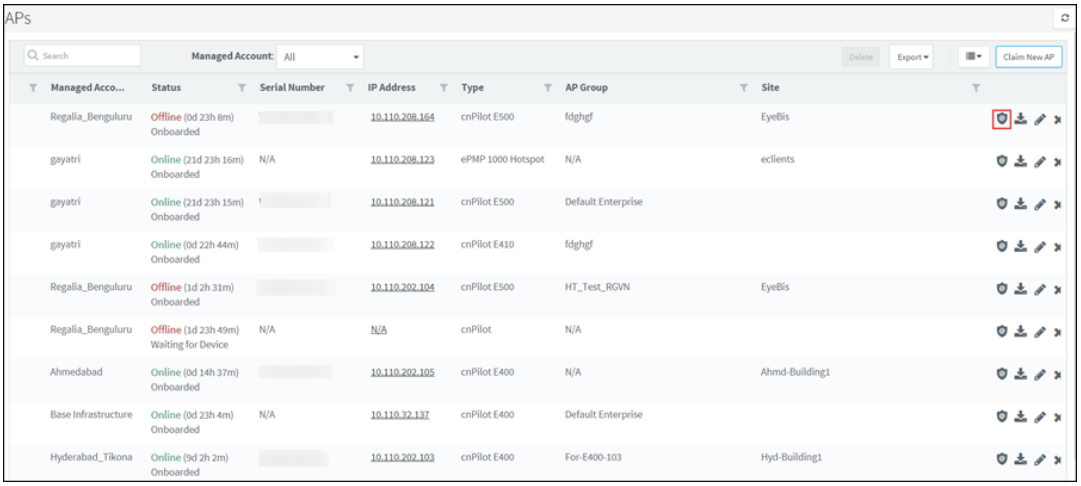
You can move a device from one Managed Account to another by using the **Change** option in account device managed page.

Figure 143 Moving a Device Between Managed Accounts



In Enterprise View, the device can be moved between Managed Accounts using a **Managed Account** icon in the Inventory tab.

Figure 144 Moving a device between Managed Accounts in Enterprise View



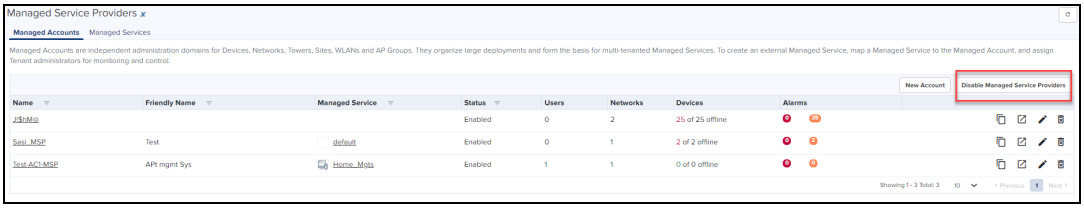
Managed Account Deletion



NOTE:
All devices must be removed from the Managed Account before deleting it.

To delete a Managed Account, navigate to **Managed Services** page and click the **delete** icon.

Figure 145 Managed Account Deletion



Disabling Managed Service Provider Feature

The Managed Service Provider feature can be disabled within the system only after all the devices are deleted or moved to the Global context. By disabling Managed Services, the Managed Account field will be disabled across all the tables such as Clients, Notifications, Inventory etc.



NOTE:
In the current release, only the global administrator of On-Premises account has control on the following features:

- Association ACL
- Auto-Provisioning
- Scheduled Backup
- Server Settings
- SMTP Server
- SNMP Configuration

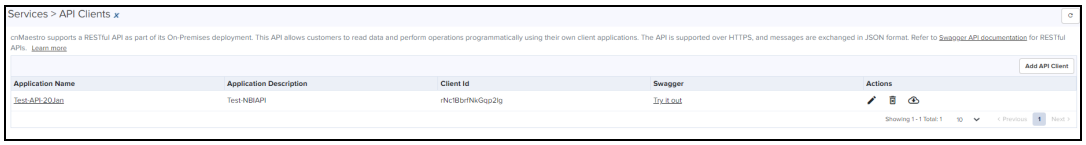
API Client

Overview

cnMaestro supports a RESTful API as part of its On-Premises deployment. This API allows customers to read data and perform operations programmatically using their own client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Modern programming languages have rich support for RESTful interfaces.

API Clients

API Clients are external applications that access the RESTful API over HTTPS using OAuth 2.0 Authentication. They require a Client ID and Client Secret for access, both of which are detailed later in this section. They are configured by navigating to **Services > API Clients**.

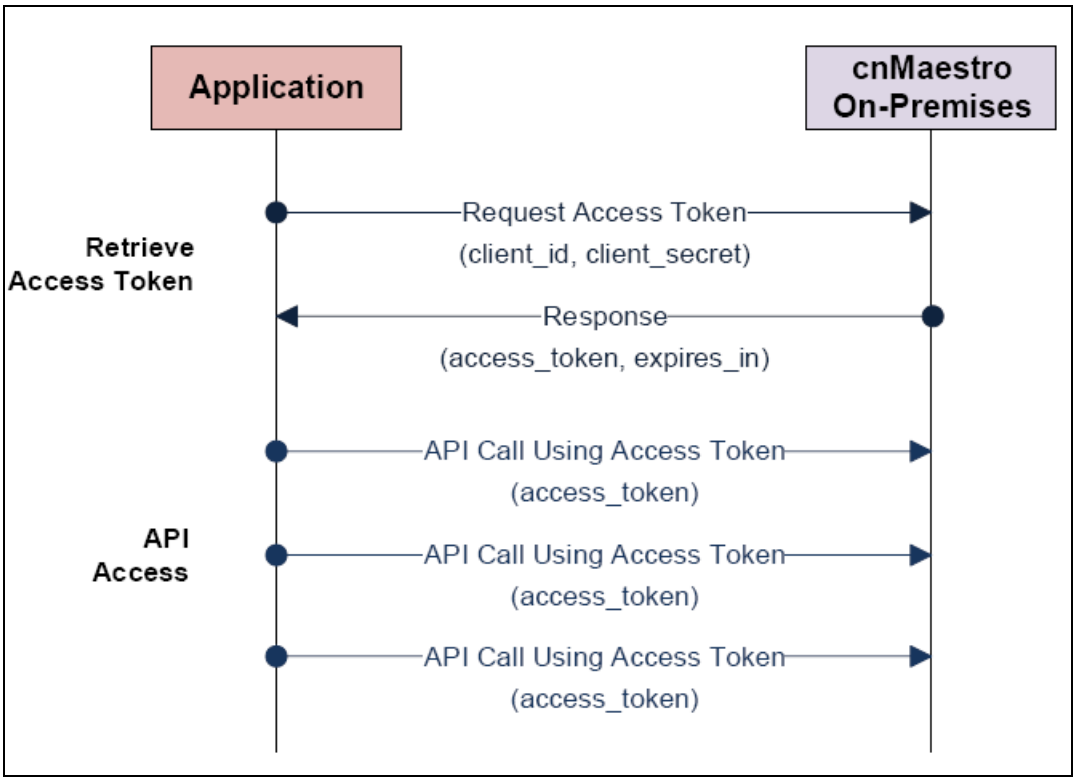


RESTful API Specification

	NOTE: The cnMaestro API is changing to v2 in the 3.0 Release. v1 continues to be supported through 3.1.x. Cambium Networks recommends using v2 on any new API applications and updating from v1 as soon as possible. The changes to the v2 API are limited and described later in this chapter.

Authentication

API Authentication uses OAuth2. The client retrieves an Access Token to start the session. It then sends API requests until the Access Token times out, at which point the token can be regenerated.



Establishing Session

A session is created by sending the Client ID and Client Secret to the cnMaestro server. These are generated in the cnMaestro UI and stored with the application. The Client ID defines the cnMaestro account and application, and the Client Secret is a private string mapped to the specific application. The Client Secret should be stored securely.

If the session is established successfully, an Access Token is returned along with an expiration string. The Access Token is used to authenticate the session. The expiration is the interval, in seconds, in which the Access Token remains valid. If the Access Token expires, a new session needs to be created.

API Access

With the Access Token, the application can make cnMaestro API calls. The token is sent in an Authentication header on each API request. Details are provided later in this document.

Session Expiration

If a token expires, an expiration error message is returned to the client. The client can then generate a new token using the Client ID and Client Secret. Tokens will expire immediately if the Client API account that created them is deleted. The default expiration time for a token is 3600 seconds (1 hour). This is configurable in the UI.

Concurrent Access

Each client supports a single Access Token or multiple Access Tokens. Multiple Access Tokens allows concurrent access.

Single Access Token

If only one Access Token is enabled at a time, whenever a new Access Token is generated from the Client ID and Client Secret, the previous Token will immediately expire.

Multiple Access Tokens

If multiple access tokens are supported, then many clients can concurrently access the API. If another Access Token is created, the previous will remain valid until their original expiration.

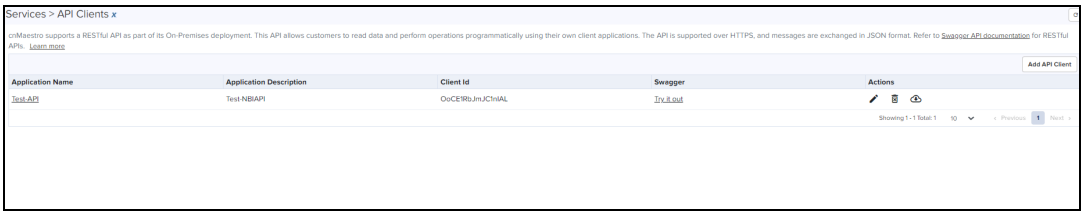
Rate Limiting

Request Rate Limiting is not enabled in the On-Premises version of cnMaestro. It is up to the application owner to make sure requests do not overtax the system.

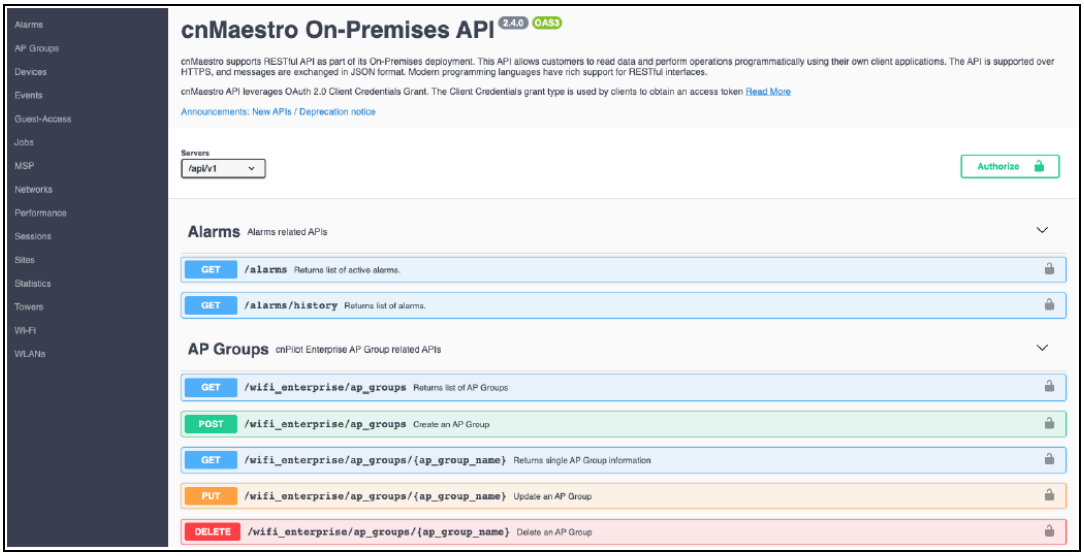
Swagger API

Introduction

The RESTful API documentation is now supported through Swagger. Swagger UI allows visualization and interaction with the API resources. You can access Swagger by navigating to **Services > API Clients** grid and clicking on **Swagger API documentation**.



Sample Swagger UI Screenshot

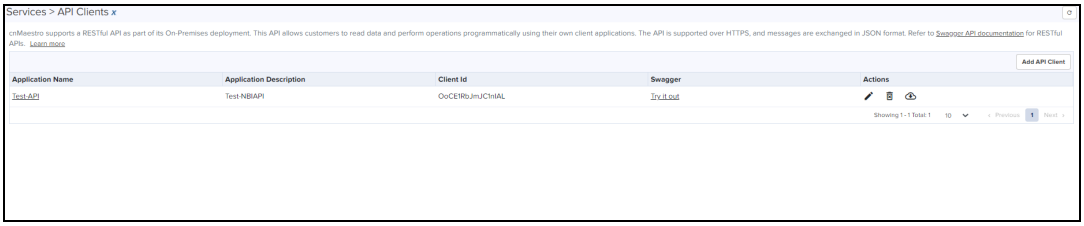


Client ID and Client Secret Generation

cnMaestro User Interface

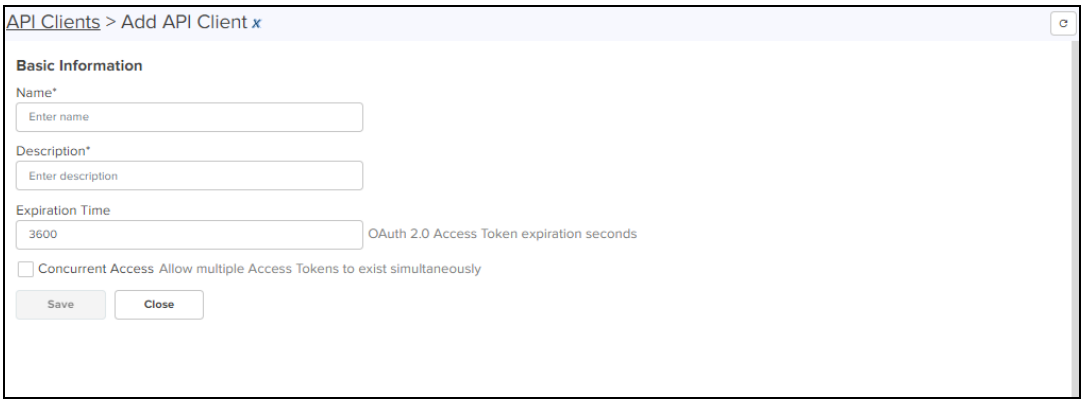
The Client Id and Client Secret are created in the cnMaestro UI by navigating to **Services > API Client**. Each client application should be added as an API Client.

Step 1: Navigate to Services > API Clients



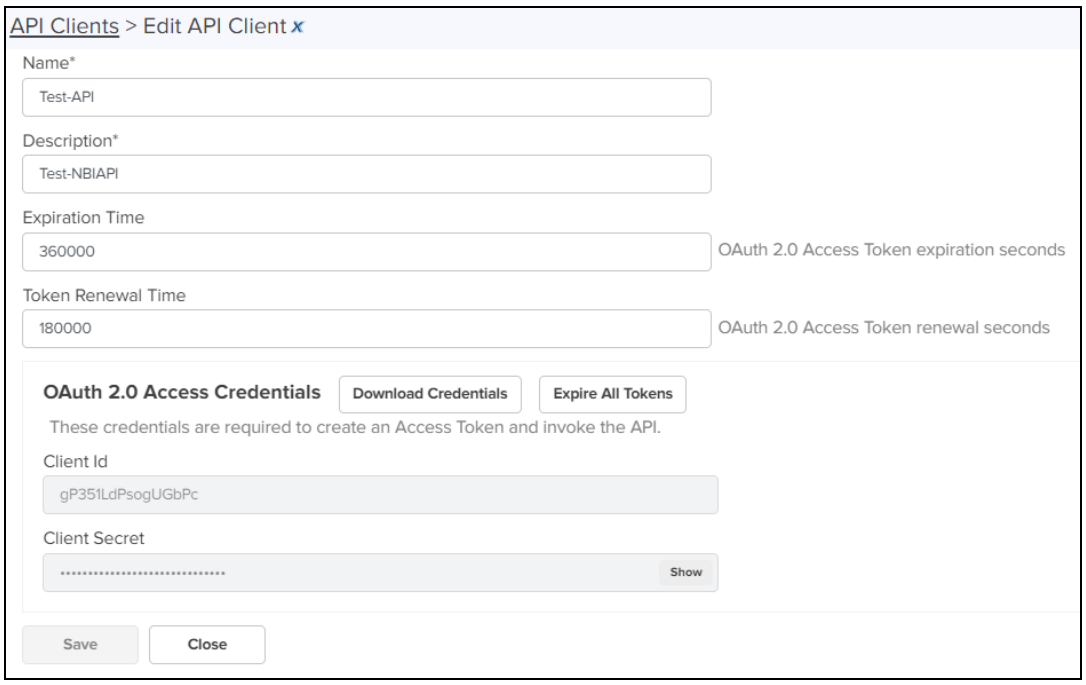
Step 2: Create a New API Client

Select **Add API** Client to add a client, then fill in the requested details, and click **Save**.



Step 3: Download the Client ID and Client Secret

Download and store the Client ID and Client Secret by clicking **Download Credentials**. Both are required to create an API session.



API Session

Introduction

The cnMaestro API leverages the Client Credentials section of the OAuth 2.0 Authorization Framework (RFC 6749). An API session can be created using any modern programming language. The examples below highlight how messages are encoded and responses returned.

Retrieve Access Token

> **NOTE:**
>
> The steps below are for the On-Premises release of cnMaestro.

Access Token Request (RFC 6749, section 4.4.2)

In order to generate a session, the client should retrieve an access token from cnMaestro. This is done by base64 encoding the **client_id** and **client_secret** downloaded from the cnMaestro Web UI and sending them to the cnMaestro server. The **Authorization** header is created by base64 encoding these fields as defined below. Note the fields are separated by a colon (:):

```
Authorization: Basic BASE64(<client_id>:<client_password>)
```

In the body of the **POST** the parameter **grant_type** must be set to **client_credentials.**

```
POST /api/v2/access/token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials
```

Alternatively, instead of using the **Authorization** header, the credentials can be passed within the body of the **POST**:

```
POST /api/v2/access/token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&client_id=s6BhdRkqt3&client_secret=7Fjfp0ZBr1KtDRbnfVdmIw
```

Access Token Response (RFC 6749, section 4.4.3)

The response returned from cnMaestro includes the access_token that should be used in subsequent requests. The expires_in field defines how many seconds the token is valid.

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token":"2YotnFZFEjr1zCsicMWpAA",
  "token_type":"bearer",
  "expires_in":3600
}
```

Error Response (RFC 6749, section 5.2)

If there is an error, an HTTP 400 (Bad Request) error code is returned along with one of the following error messages:

Message	Details
invalid_request	Required parameter is missing from the request.
invalid_client	Client authentication failed.
unauthorized_client	The client is not authorized to use the grant type sent.
unsupported_grant_type	The grant type is not supported.

An example error response is below:

```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
   "error": "invalid_request"
}
```

Access Resources

Once the **access_token** is retrieved, API requests are sent to cnMaestro server using the format below. The **access_token** is sent within the HTTP **Authorization** header.

```
GET /api/v2/devices
Accept: application/json
Authorization: Bearer ACCESS_TOKEN
```

API Details

HTTP Protocol

HTTP Response Codes

The following response codes are supported in cnMaestro and may be returned through the HTTP protocol.

Code	Description	Use in cnMaestro
400	Bad Request	Status field in request validation related errors.
502	Bad Gateway	Internal server error that may require a reboot.
403	Forbidden	An authenticated user tries to access a non-permitted resource.
500	Internal Server Error	A server-side error happened during processing the request.
405	Method Not Allowed	A method (GET, PUT, POST) is not supported for the resource.
404	Not Found	Server could not locate the requested resource.
501	Not Implemented	The request method is not recognized.
200	OK	Standard response for successful HTTP requests.
413	Payload Too Large	The request is larger than the server is willing to handle
431	Request Header Fields Too Large	The header fields are too large to be processed.
503	Service Unavailable	Internal server error that may require a reboot.
429	Too Many Requests	The client has sent too many requests in a given interval.
401	Unauthorized	User tried to access a resource without authentication.
422	Unprocessable Entity	The server understands the request but cannot process it.

HTTP Response Codes

Request Headers

Header	Details
Authorization	Used in every API request to send the Access Token. Example: Authorization: Bearer <Access-Token>
Accept	Set to application/json
Content-Type	Set to application/json

REST Protocol

Resource URLs

The format for cnMaestro path and parameters are the following:

Access a collection of resources:

```
/api/{version}/{resource}?{parameter}={value}&{parameter}={value}
```

Access a single resource:

```
/api/{version}/{resource}/{resource_id}?{parameter}={value}&{parameter}={value}
```

Access a sub-resource on a collection (this is also possible on single resources):

```
/api/{version}/{resource}/{sub-resource}?{parameter}={value}&{parameter}={value}
```

For example – read the statistics for MAC, Type, and IP on all devices:

```
/api/v2/devices/statistics?fields=mac,type,ip_wan
```

Version

The version is equal to v2 in this release.

Resource

Resources are the basic objects in the system

Context	Details
alarms	Current active alarms.
alarms/history	Historical alarms, including active alarms.
devices	Devices, including ePMP, PMP, and WiFi.
events	Historical events.
msp	MSP managed services.

Context	Details
networks	Configured networks.
sites	Configured WiFi sites.
towers	Configured Fixed Wireless towers.

Sub-Resources

Sub-Resources apply to top-level resources. They provide a different view of the resource data, or a filtered collection based upon the resource. They include:

Context	Details
alarms	Alarms mapped to the top-level resource.
alarms/history	Historical alarms mapped to the top-level resource.
clients	Wireless LAN clients mapped to the top-level resource.
devices	Devices mapped to the top-level resource.
events	Events mapped to the top-level resource.
mesh/peers	Wireless LAN mesh peers mapped to the top-level resource.
operations	Operations available to the top-level resource
performance	Performance data for the top-level resource.
statistics	Statistics for the top-level resource.

Responses

Successful Response

In a successful HTTP 200 response, data is returned using the following structure. The actual payload is presented in JSON format. The request URL is:

```
/api/v2/devices?fields=mac,type&limit=5
```

```
{
 "paging": {
   "offset": 0,
   "limit": 5,
   "total": 540
 },
 "data": [
   {
     "mac": "C1:00:0C:00:00:21",
     "type": "wifi-home"
   },
   {
     "mac": "C1:00:0C:00:00:18",
     "type": "wifi-home"
   },
   {
     "mac": "C1:00:0C:00:00:12",
     "type": "wifi-home"
   },
   {
     "mac": "C1:00:0C:00:00:15",
     "type": "wifi-home"
   },
   {
     "mac": "C1:00:0C:00:00:06",
     "type": "wifi-home"
   }
  ]
}
```


Error Response

Error responses return a message and an error cause. If the start_time and stop_time are mandatory query parameters and someone missed to provide them in the url gives the following error response with message and cause.


```
{
  "error": {
    "message": "Missing required property: stop_time \n Missing required property: start_
time",
    "cause": "InvalidInputError"
  }
}
```


Parameters

Most APIs can be modified to filter the data and limit the number of entries returned. The parameter options are listed below. The specific fields, and the appropriate values, vary for each API.

Field Selection

Field selection is supported through the optional “fields” parameter, which can specify the specific data to return from the server. If this parameter is missing, all available fields will be returned.

Parameter	Details
fields	Define exactly what fields should be returned in a request. The names are provided as a comma-separated list.

Fields can limit which JSON parameters are returned.

Example: To retrieve name, type and location information for all devices.

Request:

```
/api/v2/devices?fields=mac,type
```

Response:

```
{
  "paging": {
    "total": 3,
    "limit": 100,
    "offset": 0
  },
  "data": [
    {
      "mac": "00:44:E6:34:89:48",
      "type": "wifi-enterprise"
    },
    {
      "mac": "00:44:16:E5:33:E4",
      "type": "wifi-enterprise"
    },
    {
      "mac": "00:44:26:46:32:22",
      "type": "wifi-enterprise"
    }
  ]
}
```

Filtering

A subset of fields support filtering. These are defined as query parameters for a particular resource, and they are listed along with the API specification. Some of the standard filtering parameters are below:

Field	Details
network	(Devices) Configured Network name.
severity	(Alarms, Events) Alarm or Event severity (critical, major, minor, notice).
site	(Devices) Configured Site name.
state	(Alarms) Alarm state (active, cleared).

Field	Details
status	(Devices) Device status [online, offline, onboarding]
tower	(Devices) Configured Tower name.
type	(Devices) Device type [60ghz-cnwave, cnreach, cnmatrix, epmp, pmp, wifi-enterprise, wifi-home, wifi, ptp] (wifi includes wifi-home and wifi-enterprise).

Filters can be used simultaneously for Resources and Sub-Resources.

Example: Retrieve all WiFi devices that are online.

Request:

```
/api/v2/devices?type=wifi&status=online
```

Response:


```
{
  "paging": {
    "total": 1,
    "limit": 100,
    "offset": 0
   },
   "data": [
     {
       "ip": "233.187.212.38",
       "location": {
         "type": "Point",
         "coordinates": [
           77.55310127974755,
           12.952351523837196
         ]
       },
       "mac": "C1:00:0C:00:00:24",
       "msn": "SN-C1:00:0C:00:00:24",
       "name": "Hattie",
       "network": "Bangalore",
       "product": "cnPilot R201",
       "registration_date": "2017-05-23T21:28:37+05:30",
       "status": "online",
       "site": "Bangalore_Industrial",
       "type": "wifi-home",
       "hardware_version": "V1.1",
       "software_version": "2.4.4",
       "status_time": 1495560086
     }
   ]
}
```


Time Filtering

Events, Alarms, and Performance data can be filtered by date and time using ISO 8601 format.

Example: January 12, 2015 UTC would be encoded as **2015-01-12.**

Example: January 12, 2015 1:00 PM UTC would be encoded as **2015-01-12T13:00:00Z.**

The parameters are below. If they are not specified, then the start or stop times will be open-ended.

Parameter	Details
start_time	Inclusive start time of interval.
stop_time	Inclusive stop time of interval.

Sorting

Sorting is supported on a selected subset of fields within certain requests. sort is used to specify sorting columns. The sort order is ascending unless the path name is prefixed with a '-', in which case it would be descending.

Parameter	Details
sort	Used to get the records in the order of the given attribute.

Example: To retrieve devices in sorted (ascending) order by name.

Request:

```
/api/v2/devices?sort=name
```

Example: To retrieve devices in sorted (descending) order by mac.

Request:

```
/api/v2/devices?sort=-mac
```

Pagination

The limit and offset query parameters are used to paginate responses.

Parameter	Details
limit	Maximum number of records to be returned from the server.
offset	Starting index to retrieve the data.

Example: To retrieve the first 10 ePMP devices

Request:

```
/api/v2/devices?offset=3&limit=1
```

Response:


```
{
  "paging": {
    "total": 6,
    "limit": 1,
    "offset": 3
  },
  "data": [
    {
      "status": "online",
      "product": "cnPilot E400",
      "network": "Mumbai",
      "software_version": "3.3-b14",
      "registration_date": "2017-04-28T08:57:33+00:00",
      "site": "Central",
      "hardware_version": "Force 200",
      "status_time": "3498",
      "msn": "Z834275ABCDH",
      "mac": "00:04:36:46:34:AA",
      "location": {
        "type": "Point",
        "coordinates": [
          0,
          0
       ]
     },
     "type": "wifi-enterprise",
     "name": "E400-4634AA"
    }
  ]
}
```


Internal Response Limits

When clients try to access a resource type without pagination, the server will return the first 100 entries that match the filter criteria. The response will always carry a metadata to convey total count and current offset and limit. Maximum number of results at any point is 100 even though limit provided is more than 100.

Example: To retrieve all devices.

Request:

```
/api/v2/devices
```

Response:


```
{
  data: {devices: [ {name: 'ePMP_5566', type:'ePMP', location:'blr'} , {….}… ] },
  paging:{
    "limit":25,
    "offset":50,
    "total":100
  }
}
```


The response returns the following values in the paging section:

Parameter	Details
limit	Current setting for the limit.
offset	Starting index for the records returned in the response (begins at 0).
total	Total number of records that can be retrieved.

Access API

Token (basic request)

POST

`/api/v2/access/token`

The access API generates token using the Client ID and Client Password created in the cnMaestro UI. The token can be leveraged for API calls through the expiration time. Only one token is supported for each Client ID at any given time.

Request

Headers

Header	Value
Accept (optional)	application/json
Authorization	Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type	application/x-www-form-urlencoded

The client_id and client_secret are encoded and sent in the Authorization header. The encoding is:

```
BASE64(client_id:client_secret)
```

Body

The body needs to have the grant_type.

```
grant_type=client_credentials
```

Response

The response returns credentials for API access.

Body

Name	Details
access_token	Access token to return with each API request.
expires_in	Time in seconds that the API session will remain active.
token_type	This will always be bearer.

```
{
   "access_token":"2YotnFZFEjr1zCsicMWpAA",
   "token_type":"bearer",
   "expires_in":3600
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/token \

```
 -X POST -k \
 -u 8YKCxq72qpjnYmXQ:pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF \
 -d grant_type=client_credentials
```

Response

```
{"access_token":"d587538f445d30eb2d48e1b7f7a6c9657d32068e","token_type":"
 bearer","expires_in":86400}
```

Token (alternate request)

POST

`/api/v2/access/token`

An alternative form is supported in which the client_ID and client_secret are sent in the body, rather than the Authorization header.

Request

Headers

Header	Value
Accept (optional)	application/json
Content-Type	application/x-www-form-urlencoded

Body

```
grant_type=client_credentials&client_id=s6BhdRkqt3&client_secret=7Fjfp0ZBr1KtDRbnfVdmIw
```

Response

The response to both forms is the same.

Body

Name	Details
access_token	Access token to return with each API request.
expires_in	Time in seconds that the API session will remain active.
token_type	This will always be bearer.

```
{
   "access_token":"2YotnFZFEjr1zCsicMWpAA",
   "token_type":"bearer",
   "expires_in":3600
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/token \

```
 -X POST -k \
 -d grant_type=client_credentials \
 -d client_id=8YKCxq72qpjnYmXQ \
 -d client_secret=pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF
```

Response

```
{"access_token":"ee4e077cf457196eb4d27cf6f02686dc07763059","token_type":" bearer","expires_
in":86400}
```

Validate Token

GET

`/api/v2/access/validate_token`

Verify an Access Token is valid and return the time remaining before it expires.

Request

HTTP Headers

Header	Value
Accept (optional)	application/json
Authorization	Bearer <ACCESS_TOKEN>

Response

Body

Name	Details
expires_in	Time in seconds that the API session will remain active.

```
{
   'expires_in': 86399
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/validate_token \

```
 -X GET -k \
 -H "Authorization: Beareree4e077cf457196eb4d27cf6f02686dc07763059"
```

Response

```
{"expires_in":85643}
```

Selected APIs

Overview

cnMaestro APIs are defined within the Swagger specification, accessed here https://docs.cloud.cambiumnetworks.com/api/3.0.0/index.html#/. This section only presents additional details for the Device, Statistics and Performance APIs, which have unique responses based upon Device Type, and are difficult to present within Swagger.

cnMaestro v2 API

Beginning with cnMaestro 3.0.0, the API version changes from **v1** to **v2**. The **v1** version will be supported through 3.1.0, but Cambium recommends updating existing API code to use **v2**. For most commands, swapping v1 in the URL with v2 should be sufficient. However, the following APIs may need to be rewritten while moving to v2.

- AP Groups
- Devices
- Statistics
- Performance
- Mesh Peers
- Operations

There are Unique API responses such as:

- Device API Response (v2 Format)
- Statistics API Response (v2 Format)

Devices API Response (v2 Format)

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	cnMatrix	60 GHz cnWave
ap_group	AP Group			X					
cbrs_state	CBRS state		X						
cbrs_status	CBRS status		X						
config.sync_reason	Configuration synchronization reason	X	X	X	X	X	X	X	
config.sync_status	Configuration synchronization status	X	X	X	X	X	X	X	
config.variables	Device is mapped to configuration variables	X	X	X	X	X	X	X	
config.version	Current configuration version	X	X	X	X	X	X	X	
country	Country	X	X	X		X			
country_code	Regulatory band						X		
description	Description	X	X	X	X	X	X	X	X
hardware_version	Hardware version	X	X	X	X	X	X	X	X
inactive_software_version	Inactive software version	X	X	X	X	X	X	X	
ip	IP address	X	X	X	X	X	X	X	X
ipv6	IPv6	X		X		X			X
last_reboot_reason	Reason for the last reboot (see 24.1)	X	X	X	X	X	X	X	

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	cnMatrix	60 GHz cnWave
link_symmetry	Link symmetry						X		
location	Location	X	X	X	X	X	X	X	X
mac	MAC address	X	X	X	X	X	X	X	X
managed_account	Managed account name	X	X	X	X	X	X	X	X
maximum_range	Maximum range (KM)	X	X			X	X		
msn	Manufacturer serial number	X	X	X	X	X	X	X	X
name	Device name	X	X	X	X	X	X	X	X
network	Network	X	X	X	X	X	X	X	X
product	Product name	X	X	X	X	X	X	X	X
registration_date	Registration date	X	X	X	X	X	X	X	X
role							X		
site	Site			X				X	X
site_id	Site unique identifier			X				X	X
software_version	Active Software version	X	X	X	X	X	X	X	
status	Status (online, offline, onboarding)	X	X	X	X	X	X	X	X

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	cnMatrix	60 GHz cnWave
status_time	Uptime/downtime time interval (sec)	X	X	X	X	X	X	X	X
tower	Tower	X	X		X	X	X	X	
type	Device type (epmp, pmp, wifi-home, wifi-enterprise, cnreach, ptp, cnmatrix, 60ghz-cnwave)	X	X	X	X	X	X	X	X

Statistics API Response (v2 format)

Statistics API Response v2 format are shown for the following devices:

- 60 GHz cnWave
- cnMatrix
- cnReach
- Fixed Wireless
- PTP
- Wi-Fi

60 GHz cnWave

General

Name	Details	Mode
cpu	CPU utilization	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
memory	Available memory	All
mode	Device mode	All
name	Device name	All
network	Network	All

Name	Details	Mode
site	Site name	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
sync_mode	Radio Sync mode [RF, GPS, None]	All
type	Device type	All

Networks

Name	Details	Mode
ipv6	IPv6 address	All

Radios (Array format)

Name	Details	Mode
radios[].channel	Channel	All
radios[].id	Radio Id	All
radios[].mac	Radio MAC	All
radios[].rx_bps	Receive bits/second	All
radios[].tx_bps	Transmit bits/second	All
radios[].sync_mode	Radio Sync mode [RF, GPS, None]	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx_pkts	Received packets	All
ethports[].tx_pkts	Transmitted packets	All
ethports[].speed	Port speed and duplex	All

cnMatrix

General

Name	Details
cpu	CPU utilization
config_version	Configuration version
last_sync	Last synchronization (UTC Unix time milliseconds)
mac	MAC address
managed_account	Managed account name
memory	Available memory
mode	Device mode
name	Device name
network	Network
site	Site name
site_id	Site unique identifier
status	Status [online, offline, claimed, waiting, onboarding]
status_time	Uptime/downtime interval (seconds)
tower	Tower name
type	Device type

Networks

Name	Details
ip	IP address

cnReach

General

Name	Details	Mode
config_version	Configuration version	All
connected_sms	Connected SM count	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
tower	Tower name	All
type	Device type	All

Networks

Name	Details	Mode
ip	IP address	All

Radios (Array format)

Name	Details	Mode
radios[].device_id	Device ID	Radios
radios[].id	Radio Id	Radios
radios[].linked_with	Linked with	Radios
radios[].mac	Radio MAC	Radios
radios[].margin	Margin	Radios
radios[].mode	Radio mode [ap, ep, rep]	Radios

Name	Details	Mode
radios[].neighbors	Radio neighbors	Radios
radios[].network_address	Network address	Radios
radios[].noise	Average noise (dB)	Radios
radios[].power	Transmit power	Radios
radios[].rssi	RSSI value (dB)	Radios
radios[].rx_bytes	Receive bytes	Radios
radios[].software_version	Current software version	Radios
radios[].temperature	Radio temperature	Radios
radios[].type	Radio type [ptp, ptmp]	Radios
radios[].tx_bytes	Transmit bytes	Radios

Fixed Wireless (ePMP and PMP)

General

Name	Details	ePMP	PMP
ap_mac	AP MAC	SM	SM
config_version	Configuration version	AP/SM	AP/SM
connected_sms	Connected SM count	AP	AP
cpu	CPU utilization		AP/SM
distance	SM distance (KM)	SM	SM
gain	Antenna gain (dBi)	AP/SM	AP/SM
gps_sync_state	GPS synchronization state	AP/SM	
last_sync	Last synchronization (UTC Unix time milliseconds)	AP/SM	AP/SM
mac	MAC address	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM

Name	Details	ePMP	PMP
network	Network	AP/SM	AP/SM
reboots	Reboot count	AP/SM	
status	Status [online, offline, claimed, waiting, onboarding]	AP/SM	AP/SM
status_time	Uptime/downtime interval (seconds)	AP/SM	AP/SM
temperature	Temperature		AP/SM
tower	Tower name	AP	AP
vlan	VLAN		AP/SM

Networks

Name	Details	ePMP	PMP
default_gateway	Default gateway	AP/SM	AP/SM
ip	IP address	AP/SM	AP/SM
ipv6	IPv6 address	AP/SM	
ip_dns	DNS	AP/SM	AP/SM
ip_dns_secondary	Secondary DNS		AP/SM
ip_wan	WAN IP	AP/SM	
lan_mode_status	LAN mode status [no-data, half, full]	AP/SM	
lan_mtu	MTU size	SM	
lan_speed_status	LAN speed status	AP/SM	
lan_status	LAN status [down, up]	AP/SM	AP/SM
netmask	Network mask	AP/SM	AP/SM

Radios

Name	Details	ePMP	PMP
radio.auth_mode	Authentication mode	SM	
radio.auth_type	Authentication type ePMP [open, wpa1, eap- ttls] PMP [disabled, enabled]	AP/SM	AP/SM
radio.channel_width	Channel width ePMP [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP [...]	AP/SM	AP/SM
radio.color_code	Color code		AP/SM
radio.dfs_status	DFS status ePMP: [not-applicable, channel- availability-check, in-service, radar- signal-detected, alternate-channel- monitoring, not-in- service] PMP: [Status String]	AP/SM	AP/SM
radio.dl_err_drop_pkts	Downlink error drop packets	SM	
radio.dl_err_drop_pkts_ percentage	Downlink error drop packets percentage	SM	
radio.dl_frame_utilization	Downlink frame utilization		AP
radio.dl_lqi	Downlink Link Quality Indicator		SM
radio.dl_mcs	Downlink MCS	SM	
radio.dl_modulation	Downlink Modulation		SM
radio.dl_pkts	Downlink packet count	AP/SM	AP/SM
radio.dl_pkts_loss	Downlink packet loss		AP/SM
radio.dl_retransmits	Downlink Retransmission	AP/SM	
radio.dl_retransmits_pct	Downlink Retransmission percentage	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance		AP
radio.dl_snr	Downlink SNR (dB)	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal		SM

Name	Details	ePMP	PMP
radio.dl_snr_v	Downlink SNR (dB) vertical		SM
radio.dl_throughput	Downlink throughput	AP/SM	AP/SM
radio.frequency	RF frequency	AP/SM	AP/SM
radio.frame_period	Frame period		AP
radio.mac	Wireless MAC	AP/SM	
radio.mode	Radio mode [eptp-master, eptp- slave, tdd, tdd-ptp, ap/sm]	AP/SM	
radio.sessions_dropped	Session drops	AP	AP/SM
radio.software_key_throughput	Software key – max throughput		SM
radio.ssid	SSID	AP/SM	
radio.sync_source	Synchronization source		AP
radio.sync_state	Synchronization state		AP
radio.tdd_ratio	TDD ratio ePMP [75/25, 50/50, 30/70, flexible] PMP [...]	AP	AP
radio.tx_capacity	SM transmit capacity	SM	
radio.tx_power	Radio transmit power	AP/SM	AP/SM
radio.tx_quality	SM transmit quality	SM	
radio.ul_err_drop_pkts	Uplink error drop packets	SM	
radio.ul_err_drop_pkts_ percentage	Uplink error drop packets percentage	SM	
radio.ul_frame_utilization	Uplink frame utilization		AP
radio.ul_mcs	Uplink MCS	AP/SM	
radio.ul_modulation	Uplink Modulation example [2X MIMO-B)]		SM
radio.ul_lqi	Uplink Link Quality Indicator		SM
radio.ul_pkts	Uplink packet count	AP/SM	AP/SM
radio.ul_pkts_loss	Uplink packet loss		AP/SM

Name	Details	ePMP	PMP
radio.ul_retransmits	Uplink Retransmission	SM	
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM
radio.ul_snr	Uplink SNR (dB)	SM	
radio.ul_snr_h	Uplink SNR (dB) horizontal		SM
radio.ul_snr_v	Uplink SNR (dB) vertical		SM
radio.ul_throughput	Uplink throughput	AP/SM	AP/SM
radio.wlan_status	WLAN status [down, up]	AP/SM	

PTP

General

Name	Details	Mode
config_version	Configuration version	All
connected_sms	Connected SM count	Master
gain	Antenna gain (dBi)	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode [AP, SM]	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
temperature	Temperature	All
tower	Tower name	All
type	Device type	All
vlan	VLAN	All

Networks

Name	Details	Mode
default_gateway	Default gateway	All
ip	IP address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
lan_status	LAN status [down, up]	All
netmask	Network mask	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx_frames	Ports receive frames oversize	All
ethports[].rx_util	Ports receive bandwidth utiliization	All
ethports[].speed	Ports speed and duplex	All
ethports[].tx_util	Ports transmit bandwidth utiliization	All

Radios

Name	Details	Mode
radio.byte_error_ratio	Byte Error Ratio	All
radio.channel_width	Channel width ePMP: [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP: [...]	All
radio.color_code	Color code	All
radio.rx_frequency	Receive frequency	All
radio.tx_frequency	Transmit frequency	All
radio.tx_power	Radio transmit power	All

Wi-Fi

	NOTE: Mode is Enterprise, Home, or All.

General

Name	Details	Mode
config_version	Configuration version	All
cpu	CPU utilization	All
mac	MAC address	All
managed_account	Managed account name	All
memory	Available memory	All
mode	Device mode	All
name	Device name	All
network	Network	All
parent_mac	Parent MAC	All
site	Site name	All
site_id	Site unique identifier	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
type	Device type	All

Networks

Name	Details	Mode
ip	IP address	All
ipv6	IPv6 address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
ip_wan	WAN IP	All

Name	Details	Mode
lan_mode_status	LAN mode status [no-data, half, full]	Enterprise
lan_speed_status	LAN speed status	All
lan_status	LAN status [down, up]	Home
netmask	Network mask	All

Radios (Array format)

Name	Details	Mode
radios[].airtime	Airtime	All
radios[].band	Radio band	All
radios[].bssid	Radio mac	Enterprise
radios[].channel	Channel	All
radios[].id	Radio Id	All
radios[].multicast_rate	Multicast rate	Enterprise
radios[].noise_floor	Noise floor	Enterprise
radios[].num_clients	Number of clients	All
radios[].num_wlans	Number of WLANs	Enterprise
radios[].power	Transmit power	All
radios[].quality	RF Quality description	Enterprise
radios[].radio_state	Radio state	Enterprise
radios[].rx_bps	Receive bits/second	All
radios[].rx_bytes	Receive bytes	All
radios[].tx_bps	Transmit bits/second	All
radios[].tx_bytes	Transmit bytes	All
radios[].unicast_rates	Unicast rates	Enterprise
radios[].utilization	Radio utilization	Enterprise

Performance API Response (v2 format)

Performance API Response v2 Format are shown for following devices:

- 60 GHz cnWave
- cnMatrix
- cnReach
- Fixed Wireless
- PTP
- Wi-Fi

60 GHz cnWave

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
site	Site	All
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].id	Radio ID	All
radios[].rx_bps	Receive bits/second	All
radios[].tx_bps	Transmit bits/second	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].max_rx	Ports maximum receive bytes	All
ethports[].max_tx	Ports maximum transmit bytes	All
ethports[].min_rx	Ports minimum receive bytes	All
ethports[].min_tx	Ports minimum transmit bytes	All

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx	Ports receive bytes	All
ethports[].tx	Ports transmit bytes	All

cnMatrix

General

Name	Details
mac	MAC address
managed_account	Managed account name
mode	Device mode
name	Device name
network	Network
site	Site
timestamp	Timestamp
tower	Tower
type	Device type

Switch

Name	Details
switch.rx.broadcast_pkts	Receive broadcast packets
switch.dl_kbits	Downlink usage (in kbits on hour or minute basis)
switch.dl_throughput	Downlink throughput (Kbps)
switch.ul_kbits	Uplink (in Kbits on hour or minute basis)
switch.rx.multicast_pkts	Receive multicast packets
switch.ul_throughput	Uplink throughput (Kbps)
switch.rx.pkts_err	Receive Packet error
switch.rx.unicast_pkts	Receive unicast packets

Name	Details
switch.tx.broadcast_pkts	Transmit broadcast packets
switch.tx.multicast_pkts	Transmit multicast packets
switch.tx.pkts_err	Transmit packet error
switch.tx.unicast_pkts	Transmit unicast packets

cnReach

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
sm_count	Connected SM count	All
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].id	Radio ID	Radios
radios[].neighbors	Radio neighbors	Radios
radios[].noise	Average noise	Radios
radios[].power	Transmit power	Radios
radios[].rssi	RSSI value	Radios

Name	Details	Mode
radios[].rx_bytes	Receive bytes	Radios
radios[].throughput	Total throughput	Radios
radios[].tx_bytes	Transmit bytes	Radios

Fixed Wireless (ePMP and PMP)

General

Name	Details	ePMP	PMP
mac	MAC address	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM
network	Network	AP/SM	AP/SM
online_duration	Duration of device connection with server (seconds)	AP/SM	AP/SM
sm_count	Connected SM count	AP	AP
sm_drops	Session drops	AP/SM	AP
timestamp	Timestamp	AP/SM	AP/SM
tower	Tower	AP/SM	AP/SM
type	Device type	AP/SM	AP/SM
uptime	Device online time (seconds)	AP/SM	AP/SM

Radios

Name	Details	ePMP	PMP
radio.dl_frame_utilization	Downlink frame utilization		AP
radio.dl_kbits	Downlink usage (in Kbits on hour or minute basis)	AP/SM	
radio.dl_mcs	Downlink MCS	SM	

Name	Details	ePMP	PMP
radio.dl_modulation	Downlink modulation		SM
radio.dl_pkts	Downlink packet count	AP/SM	
radio.dl_pkts_loss	Downlink packet loss		AP/SM
radio.dl_retransmits_pct	Downlink retransmission percentage	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance		SM
radio.dl_snr	Downlink SNR	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal		SM
radio.dl_snr_v	Downlink SNR (dB) vertical		SM
radio.dl_throughput	Downlink Throughput (Kbps)	AP/SM	AP/SM
radio.ul_frame_utilization	Uplink frame utilization		AP
radio.ul.kbits	Uplink usage (in Kbits on hour or minute basis)	AP/SM	
radio.ul_mcs	Uplink MCS	SM	
radio.ul_modulation	Uplink modulation		SM
radio.ul_pkts	Uplink packet count	AP/SM	
radio.ul_pkts_loss	Uplink packet loss		AP/SM
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM
radio.ul_snr	Uplink SNR	SM	
radio.ul_snr_h	Uplink SNR (dB) horizontal		SM
radio.ul_snr_v	Uplink SNR (dB) vertical		SM
radio.ul_throughput	Uplink Throughput (Kbps)	AP/SM	AP/SM

PTP

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
sm_count	Connected SM count	Master
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].max_rx	Ports maximum receive bytes	All
ethports[].max_tx	Ports maximum transmit bytes	All
ethports[].min_rx	Ports minimum receive bytes	All
ethports[].min_tx	Ports minimum transmit bytes	All
ethports[].pkt_error	Ports packet error	All
ethports[].port	Port name	All
ethports[].rx	Ports receive bytes	All
ethports[].tx	Ports transmit bytes	All

Ethernet

Name	Details	Mode
ethernet.link_loss	Link loss	All
ethernet.pcb_ temperature	PCB temperature	All
ethernet.rx_channel_util	Receive channel utilization	All
ethernet.rx_capacity	Receive capacity	All
ethernet.ssr	Signal strength ratio	All
ethernet.rx_power	Receive power	All
ethernet.sfp_interface.tx	SFP transmit bytes	All
ethernet.rx_throughput	Receive throughput	All
ethernet.tx_channel_util	Transmit channel utilization	All
ethernet.tx_capacity	Transmit capacity	All
ethernet.tx_power	Transmit power	All
ethernet.tx_throughput	Transmit throughput	All
ethernet.vector_error	Vector error	All

Wi-Fi

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
site	Site	All

Name	Details	Mode
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].clients	Number of clients	All
radios[].id	Radio ID	All
radios[].rx_bps	Receive bits/second	All
radios[].throughput	Total throughput	All
radios[].tx_bps	Transmit bits/second	All



NOTE:

The specification for the equivalent v1 APIs is available in the Appendix.

- Statistics API Response (v1 Format)
- Performance API Response (v1 Format)

External Guest Access Login API

Integrates an external captive portal with the Cambium Networks AP while posting directly to cnMaestro. This API provides the support for the external captive portal to make login requests.

POST `/api/v2/ext-portals/login`

Request:

curl -X

```
/api/v2/ext-portals/login" -H "accept: */*" -H "Authorization: Bearer
e88916f5b663c1ea966af835c8a0a19c20d17686" -H "Content-Type: application/json"-d
```

Body

```
"{\"ga_ap_mac\":\"11-22-33-44-55-66\",\"ga_cmac\":\"11-22-33-44-55-65\",\"ga_
Qv\":\"eUROBR86HBgAGDEEVgQAGw4UWRUCACYVMgFPMV5ZWVFfUVdGX1ZFJXxZR1dLBhMUMww\",\"ga_
user\":\"test-user\",\"ga_pass\":\"test-pass\"}"
```

Response:

```
{
"data": {
         "mType": 3,
         "msgId":28,
         "status":<integer values>,
         "prefixQs":<true/false>,
         "expiry":<integer values>,
         "action":<integer values>,
         "cmac":<client mac>,
         "msg":<Radius Returned Message>,
         "extURL":<external url string>
         }
}
```

The status value description is provided in the table below.

Status	Description
0	Login is successful.
1	Invalid login request, the client is not currently associated to the AP which is being requested for login here.
2	RADIUS reject due to invalid username/password.
3	RADIUS timeout, AP didn't received the RADIUS response.
4	Missing RADIUS server config on the WLAN config of the AP.
5	If LDAP configured on the AP for authentication then LDAP server responded back with reject.
6	LDAP timeout happened on the AP for the request.
7	Missing LDAP configuration on the WLAN configuration of the AP.
8	Logout is successful.
9	Logout failed due to missing session on the AP. Most likely client session is already deleted from this AP.

The response parameter name and details is shown below.

Name	Details
prefixQs	True: Add query strings to landing URL on success. False: Remove query strings from landing URL on success. `prefixQs` and `action` values are driven based on WLAN configuration.
action	0: On success action redirects the user to AP onboard logout page. 1: On success redirects user to an external URL. 2: On success redirects user to its original URL.
msg	Message is based on RADIUS attribute reply message (18) in the RADIUS Access Accept or Reject message.
expiry	Displays the session time for the given guest session.
cmac	MAC address of the client.

60 GHz cnWave RESTful API

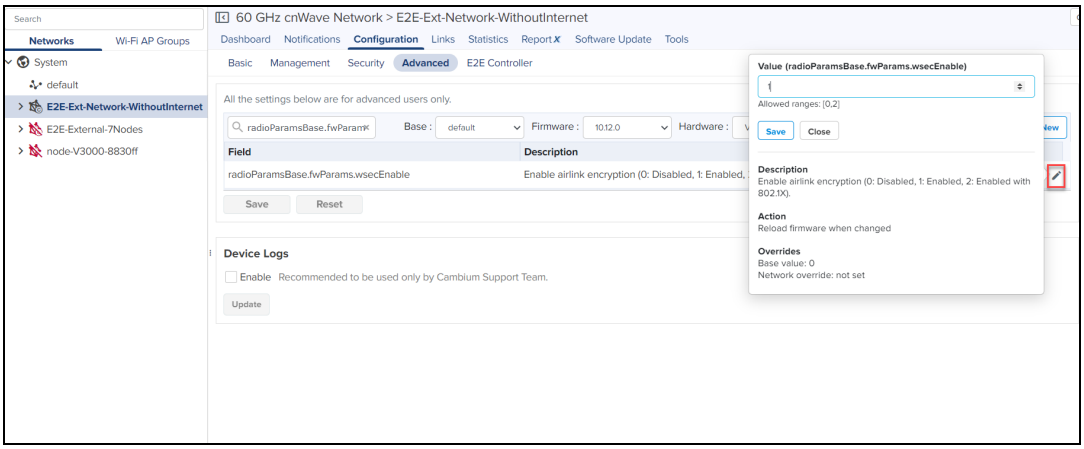
cnMaestro supports configuration overrides for 60 GHz cnWave E2E Network, E2E Controller, and Node(s) using the RESTful API.

E2E Network

To determine the configuration parameters available in an E2E Network, navigate to **E2E Network** > **Configuration** > **Advanced**. Search for the desired **Field**, and review its **Description**, allowed **Values**, and **Override status**. Use the RESTful API to override single or multiple fields.

GET `/api/v2/cnwave60/networks/{network_id}/configuration`

PUT `/api/v2/cnwave60/networks/{network_id}/configuration`



Field names are separated by dots. Each substring between dots will be converted to objects and the last substring will be the key and value.

Example

In case of field name `radioParamsBase.fwParams.wsecEnable`, payload will be:

```
{
  "radioParamsBase": {
    "fwParams": {
       "wsecEnable": 1
    }
  }
}
```



WARNING:

Partial update is not allowed. Always send full configuration that needs to be pushed to E2E Network.

Device (Node) Configuration

To update Device configuration, navigate to **Node** > **Configuration** > **Advanced**. Search for the **Field**, and review its **Description**, allowed **Values**, **and Overrides status**. Use the RESTful API to override those fields.

GET `/api/v2/cnwave60/networks/{mac}/configuration`

PUT `/api/v2/cnwave60/networks/{mac}/configuration`

Field names are separated by dots. Each substring between dots will be converted to objects and the last substring will be the key and value.

Example

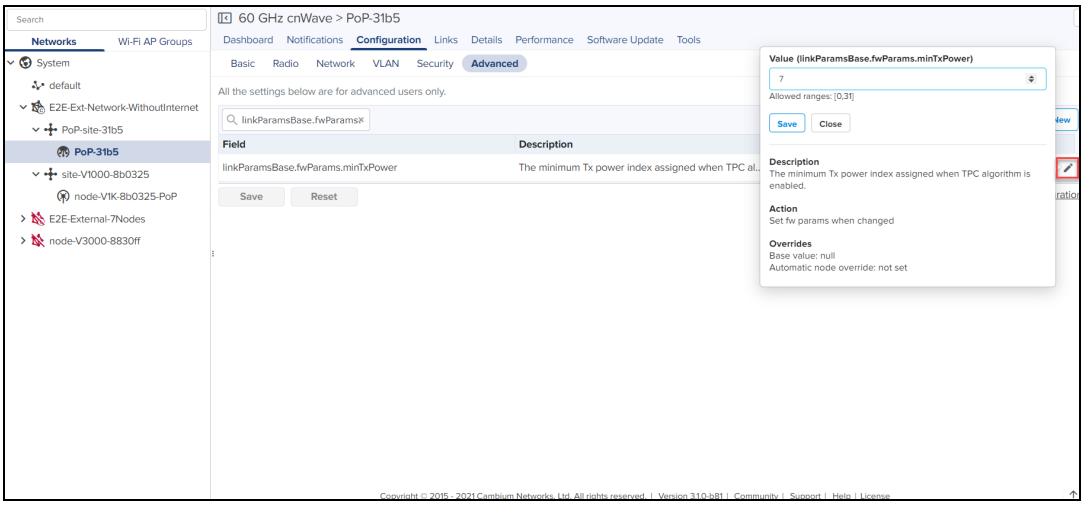
In case of field name `linkParamsBase.fwParams.minTxPower`, object to send in the API payload will be:

```
{
    "linkParamsBase": {
        "fwParams": {
            "minTxPower": 6
            "maxTxPower": 8
         }
      }
}
```

The below two APIs are introduced in Release 3.1.0 to update multiple device configurations overrides.

GET `/api/v2/cnwave60/networks/{network_id}/devices/overrides`

PUT `/api/v2/cnwave60/networks/{network_id}/devices/overrides`





WARNING:

Partial update is not allowed. Always send full configuration that needs to be pushed to 60 GHz cnWave Devices.

The example payload for PUT request is seen from cnMaestro UI.

Example

```
{
  "device1_name": {
    "radioParamsBase": {
     "fwParams": {
       "txPower": 6
     }
    }
   },
   "device2_name": {
     "popParams": {
      "POP_IFACE": "nic2"
     }
    }
  }
```

NOTE:

You can download the full config of the node by clicking on the **Show Full Configuration** as well and then get the JSON key and pass in RESTful API.

E2E Controller

To update E2E Controller configuration, navigate to **E2E Network** > **Configuration** > **E2E Controller**. Search for the desired **Field**, and review its **Description**, allowed **Values**, and **Override status**. Use the RESTful API to override those fields.

GET `/api/v2/cnwave60/networks/{network_id}/controller/configuration`

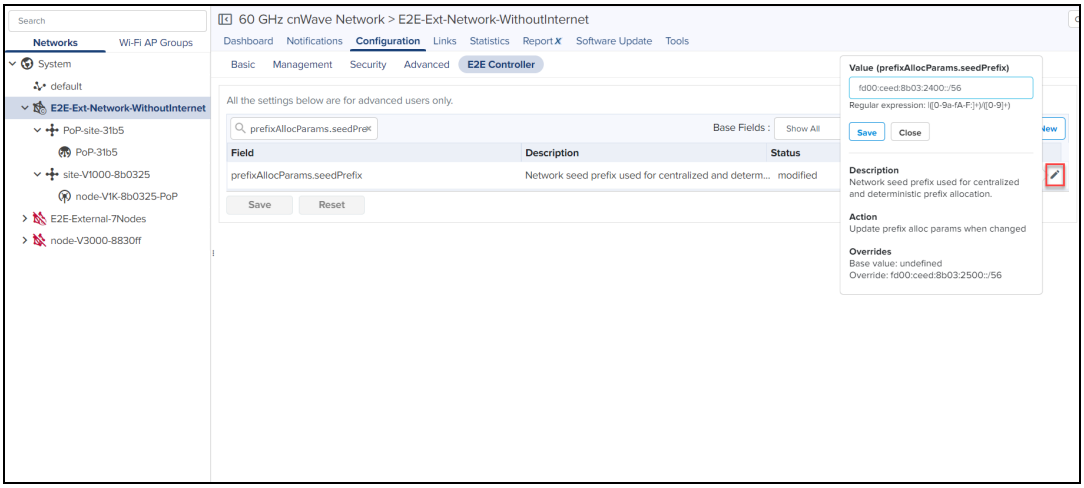
PUT `/api/v2/cnwave60/networks/{network_id}/controller/configuration`

Field names are separated by dots. Each substring between dots will be converted to objects and the last substring will be the key and value.

Example

In case of field name `prefixAllocParams.seedPrefix`, payload will be:

```
{
    "prefixAllocParams": {
     "seedPrefix": "fd00:ceed:1992:1400::/56"
    }
}
```



WARNING:

Partial update is not allowed. Always send full configuration that needs to be pushed to the E2E Controller.

cnPilot Guest Access

This section describes how to configure Guest Access using cnMaestro. This feature allows the clients to connect through Free Tier, Buying Vouchers or Paid Access types.

The Guest Access feature creates a separate network for guests by providing Internet access to guest wireless devices (mobiles, laptops, etc).

	NOTE: The Guest Access feature is supported on cnPilot E-series Enterprise devices.

Configuration

- Create the Guest Access Portal in cnMaestro
- Map the device to cnMaestro

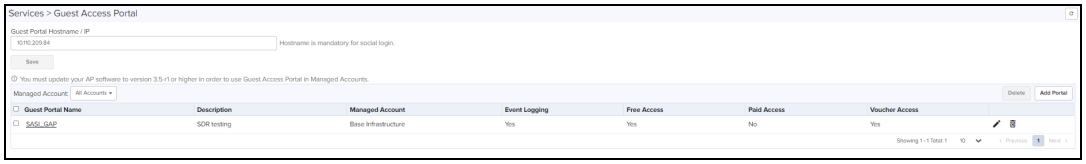
Create the Guest Access Portal in cnMaestro

1. Basic details
2. Access Portal
3. Splash page
4. Sessions

Procedure for creating Guest Access

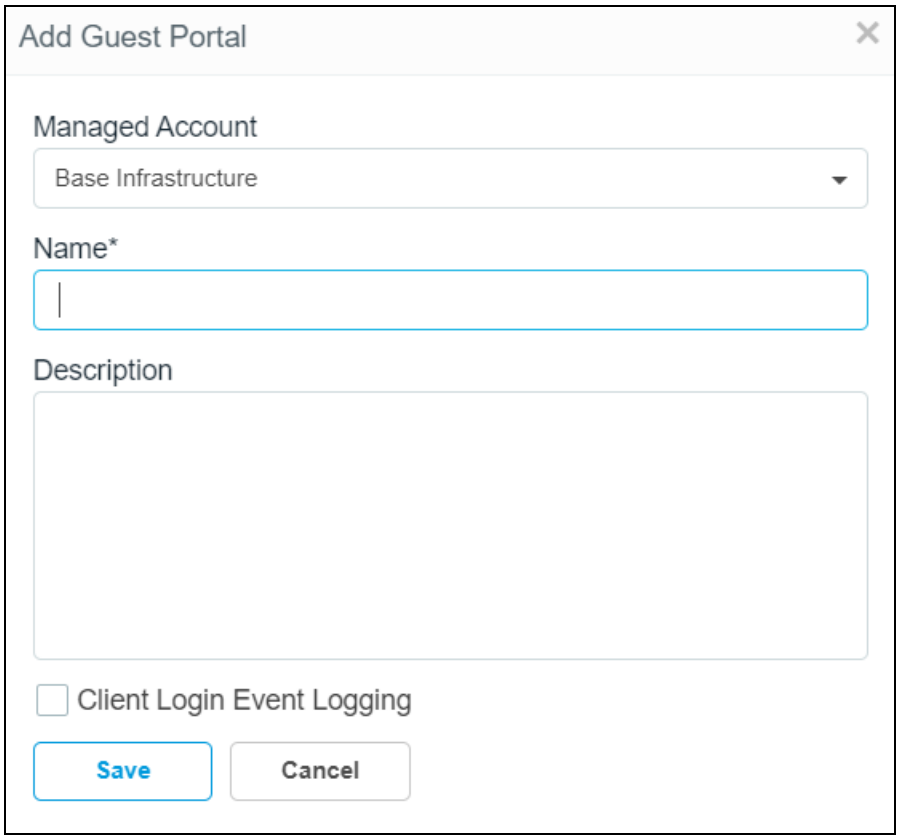
Prerequisites

1. Navigate to **Services > Guest Access Portal**.



	NOTE: The Floating Management IP should be used to access the Guest Access Portal. This means DNS should be mapped to the Floating Management IP, and not to one of the unique IP addresses of the cnMaestro instances.

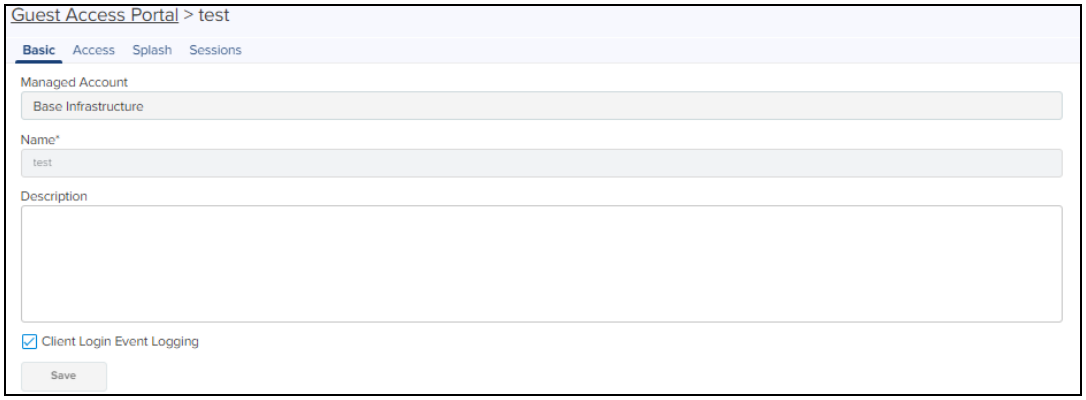
2. Click **Add Portal**. A maximum of four portals can be created per account.
3. Enter **Name** and **Description**.



4. Click **Save.**

Basic Details

The **Basic** Details page contains the Managed Account Type Name and Description.



NOTE:

A name once created for the Portal cannot be changed.

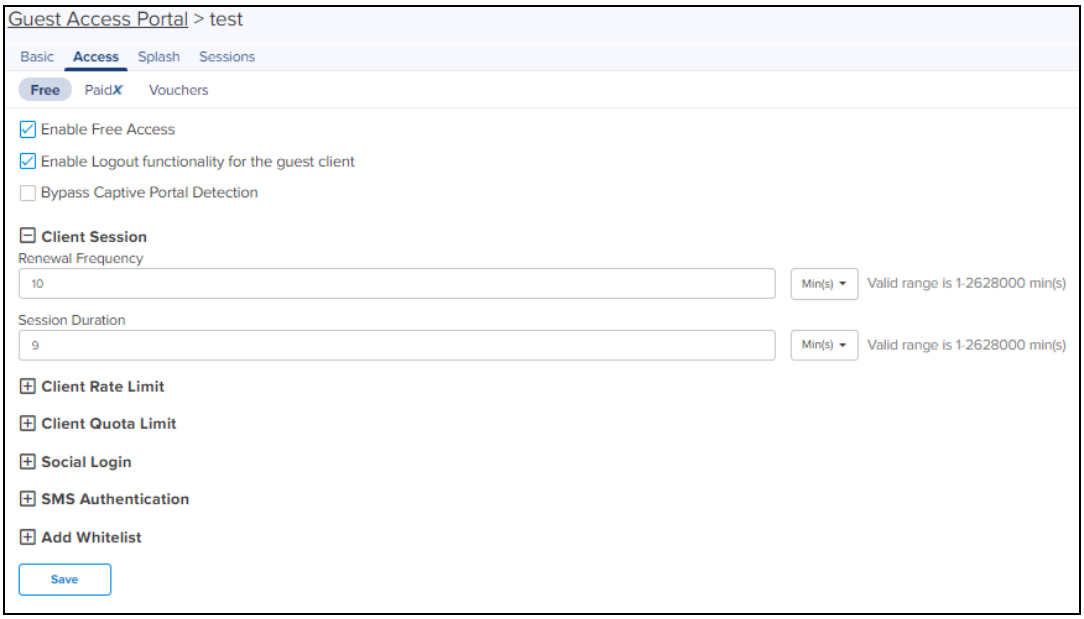
Access Portal

The Access Portal tab has three different access types:

- Free
- Paid
- Vouchers

The parameters under each access method can only be configured once the corresponding access method is enabled.

Free Access Type Configuration



Free access type contains **session validity, renewable frequency, client rate limits**, and **social login configurable parameters**.

You can select authentication using Google, Facebook, Twitter, and Office 365, or all. Enter the App ID of your social login app. If you enable Facebook login you will also need to enter your Facebook App secret.

Table 42: Free Access Type Parameters

Parameter	Description
Add Whitelist	It contains options for configuring the IP address or the domain name.
Client Rate Limit	It contains options for configuring downlink and uplink parameters in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied.
Client Quota Limit	The data quota limit feature has been added for RADIUS-based as well as for controller-based guest portals. For controller-based, it is either directional or total data quota limit. Once the client logins as a guest, the data quota limit is enforced and the values are sent to the accent point to which the client is connected. The access point keeps track of the data limits Access Point also sends client statistics to the controller every thirty minutes. In case of multiple devices allowed for a given policy then the data quota limits enforcement has some limitations and works with the latency of thirty minutes during which the cumulative data quota limits of the devices can be exceeded beyond the configured data quota limits. The similar behavior is supported through RADIUS attributes for RADIUS-based onboard guest access clients. RADIUS_VENDOR_ID_CAMBIUM 9 (17713) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP (151) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN (152) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP_GIGWORDS (153) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN_GIGWORDS (154) RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL (155)

Table 42: Free Access Type Parameters

Parameter	Description
	RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL_GIGWORDS (156) The gigwords attributes are used for supporting data quota limits above 4GB when required.
Renewable Frequency	Once the session duration for the client expires, the client needs to wait for the period specified by renewal frequency before logging in again.
Session Duration	The duration for which the client is provided access.
Social Login	Consists of the following options: • Domain URL: The redirected URL in client when trying to access the Internet. • Google: Consists of ID and Secret options to configure, which admin can create from https://console.developers.google.com/iam-admin/projects • Facebook: Consists of ID and Secret options to configure, which admin can create from https://developers.facebook.com/apps/ • Twitter: Consists of consumer key, consumer secret key, and callback URL. • Office 365: Consists of ID and reply back URL.
SMS Authentication	SMS OTP supports Twilio, SMS Country, and SMS Gupshup SMS gateway providers. Any one of the gateway providers can be used to support the SMS OTP to be delivered to the cell phone of the end user. Once OTP is received the client can enter the OTP to get Internet access.

NOTE:

- Renewal frequency should be greater than session expiration.
- Client will get Social login options only when enabled in Access Control page in portal.
- If Social login is enabled, it is mandatory in free access method for client to login through Google/Facebook/Twitter/Office 365.

Paid Access Type Configuration

Paypal has been added as a payment gateway support where end users can purchase Internet connection using either the credit card or their existing paypal accounts. For purchasing the Internet plans, the clients are directed to paypal portal where they purchase the plan and then they are automatically redirected to guest access portal where the purchased Voucher is displayed. The user should ensure to save this Voucher information if he plans to use it on multiple devices.

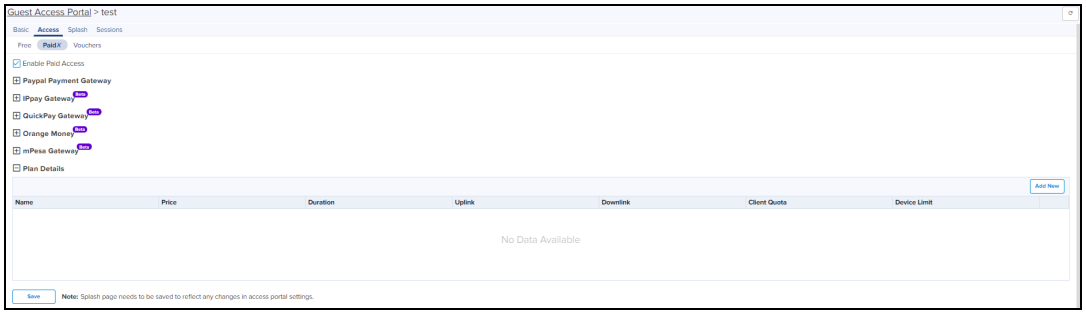
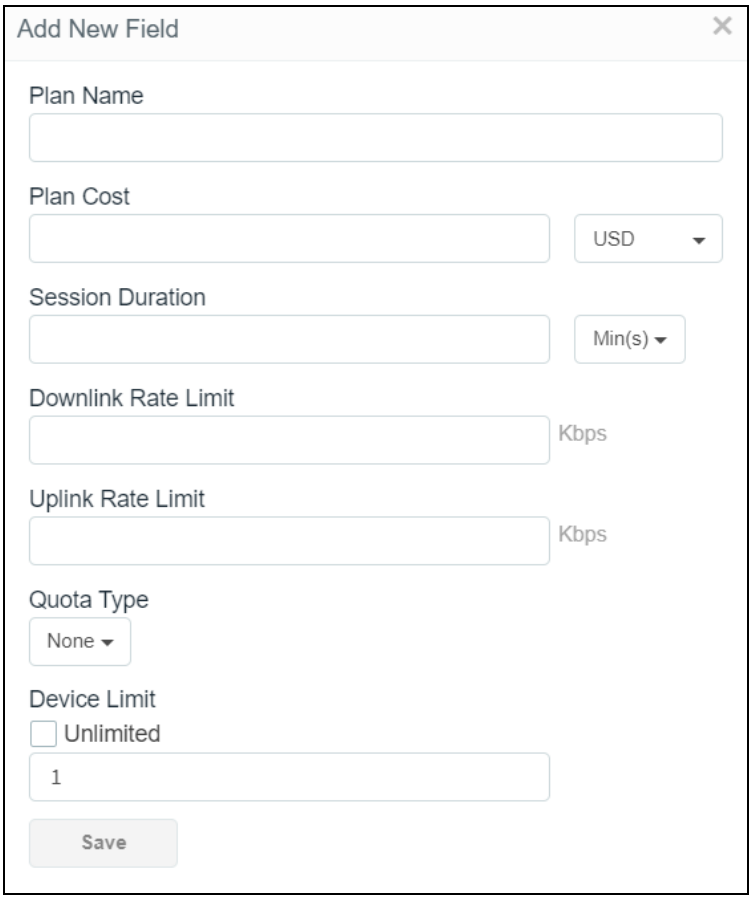


Table 43: Paid Access Type Parameters

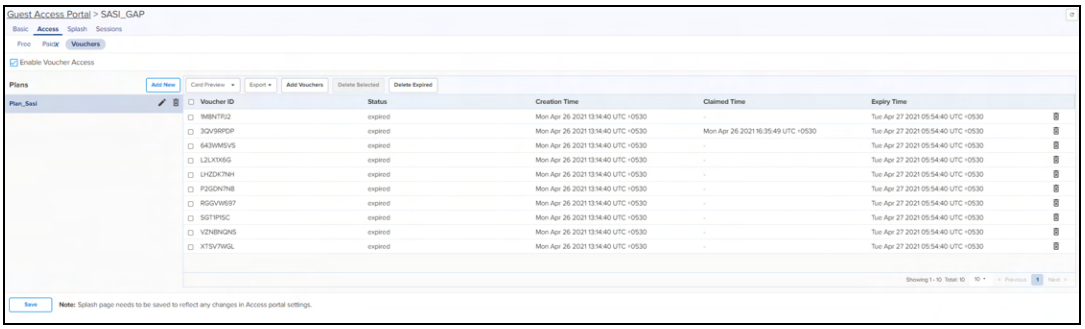
Parameter	Description
General	• **Plan Name**: The name of the plan. • **Session Duration:** The duration for which the client is allowed network access. • **Client Rate Limit**: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied. • **Device Limit:** The device limit allow that number of devices to be connected or select the unlimited to connect any number of devices.



Voucher Access Type Configuration

Important Points to Remember

- Vouchers can only be generated after enabling **Vouchers** and creating at least one **Voucher plan**.
- A maximum of 50,000 Vouchers per portal can be created on cnMaestro On-Premises.
- A maximum of 1,000 Vouchers per portal can be created on the Cloud-hosted version. (cloud.cambiumnetworks.com).
- Total number of generated Vouchers = Vouchers Unclaimed + Vouchers Claimed + Vouchers Expired.
- The admin can export all/valid/current page Voucher codes as PDF/CSV document.



Voucher contains options to add new plans and Vouchers. Based on user requirements, the plans can be created with different validity and rate limits.

1. **Create a plan**
   a. Navigate to **Services > Access Control Portal** page and select **Access Control** tab.
   b. Enable **Vouchers**
   c. Click **Add New Plan**.
      The window with general and design parameters for the plan is displayed.

Table 44: Voucher Access Type Parameters

Parameter	Description
Design	• **Color:** There are options to modify colors for the title, message, code, and background. • **Background Image:** You can browse and select a background image for this page. • **Title**: The tiltle of the voucher plan. • **Message:** Detailed information about the plan. • **Access Code Message:** 8 digit access code will be provided to use the voucher. With all the above parameters, administrators can create their own design for the card with text, color and message to be displayed on card.
General	• **Name**: The name of the plan. • **Session Duration:** The duration for which the client is allowed network access. • **Voucher Expiry**: The expiry time for the generated vouchers. Once this time lapses, the Vouchers cannot be used. • **Client Rate Limit**: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a **Client Rate Limit** parameter is blank, no limits are applied.

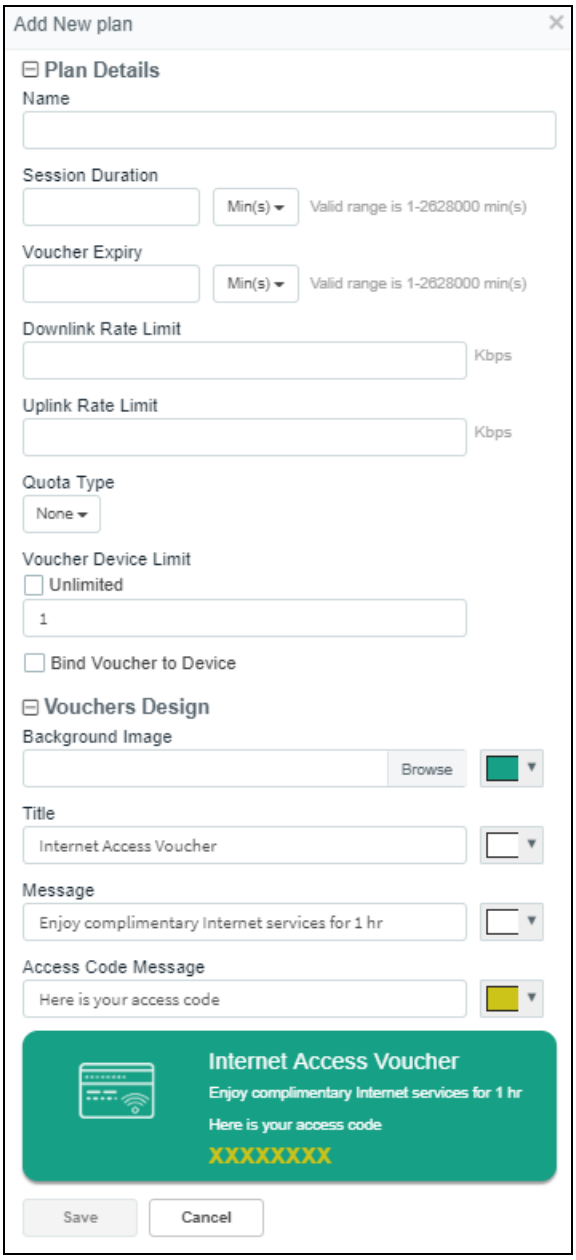
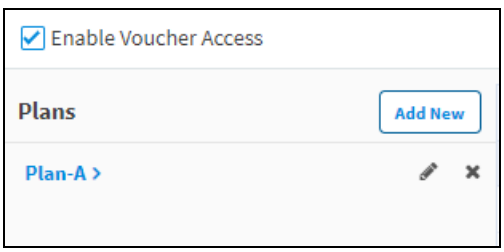


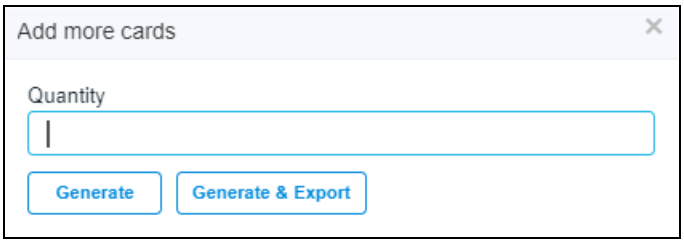
Table 45: Adding Vouchers

Once a plan is configured, vouchers can be generated for it. Each Voucher is a unique, randomized alphanumeric code.

a. **Select a plan.**



b. **Add Vouchers.**



Once the plan is created and the Vouchers are generated, the following page is displayed:



c. **Sample Voucher Code.**



NOTE:
The modified values in the Access Portal page reflectes on the splash page only when the splash page is saved after making the changes.

Splash Page

The Splash page refers to the page to which a wireless client is redirected when it connects to the guest portal. Administrators can create their own splash page by modifying the default logo, background, and text to be displayed in the splash page with different colors and fonts.

- If **Free** is selected in **Access Portal**, the client only sees free access related parameters.
- If **Voucher** is selected in **Access Portal**, the client only sees Voucher related parameters with a text box to enter the **Voucher code**.
- If both **Free** and **Voucher** are enabled, then the client sees both Free and Voucher related parameters.

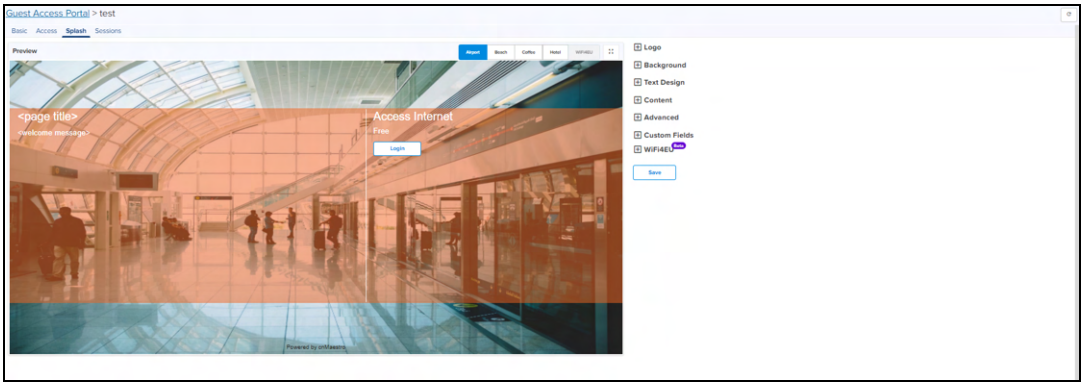


Table 46: Splash Page Parameters

Parameter	Description
Accept Terms Message	Text to appear as the accept terms message.
Advanced	Expand Advanced option. Browse and select the advanced fields.
Background	Browse and select the image that needs to be appear as the background.
Background Placement	Choose the option from the drop-down list for placing the background image in the splash page.
Custom Fields	Expand **Custom Field** option. The user can customize the fields in the Splash page by choosing the **Custom Field** option in the **Guest Access Portal** page and clicking **Add New** button.
Enter Voucher Code Message	Enter the text to appear in Voucher Code Message.
Free Label	Enter the text that should appear on the free label.
Footer	Enter the text to appear as the footer of the page. You can choose the font style and size for the footer.
Logo	Browse and select the logo the needs to be appear on the splash page.
Login Title	Text to appear for login.
Login Success Message	Message to appear after successful login.
Login Failure Message	Message to appear any error while login.
Login Button	Enter the text that should appear on the window to submit.
Message	Text to appear as the welcome text. You can choose the font style and size for the welcome text.
Opacity	The transparency of background image.
On Success Redirect to URL	Enter the URL to be redirected to the page like Google, Twitter, and Facebook, etc.
Page Title	Text to appear as the title of the page. You can choose the font style and size for the title.
Please wait Message	Text to appear in the waiting screen.
Repeat Background	Enable the check box if you want the background image to be repeated.
Server Error Message	Text to appear if there is an error while contacting server.
Select Plans Label	Enter the text to appear in the label to select plan.
Text Design	Choose the appropriate colors for the background, logo in the background, content area, and for the text.

Table 46: Splash Page Parameters

Parameter	Description
Terms Agree Button	Text to appear in the terms agree button.
Terms Cancel Button	Text to appear in the terms cancel button.
Voucher Code	Enter the text to appear in Voucher Code, Voucher Label, Enter Voucher Code Message, and Voucher Code Error Message.
Voucher Label	Enter the text to appear in Voucher Label.
Voucher Code Error Message	Enter the text to appear in Voucher Code Error Message.
WIFI4EU	WiFi4EU provides free, high-quality Internet access only across the European Union.

WIFI4EU

WiFi4EU provides the free, high-quality Internet access across the European Union. Administrator can enable the **WiFi4EU** check box to provide access to the free Internet.

Table 47: WiFi4EU Type Parameters

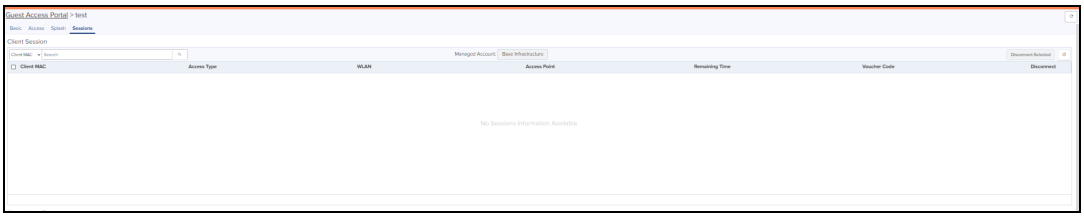
Parameter	Description
General	• **Network UUID**: Universally Unique Identifier (UUID) that the EC attribute is generated when the network installation is created in the Installation. • **Language:** Allows to select the preferred language. • **Enable Self Test Mode**: Allows the browsers background script verification. • **Show Logo:** Displays the WiFi4EU logo provided by the European union.



Sessions

Sessions tab contains Client MAC address, Access Point MAC address, Access Type as Free (Google or Facebook) or Voucher, WLAN-SSID of client connected AP, Remaining time and Disconnect option.

Administrator can check how many clients are connected, Access Type (Free/Voucher) of the client, and can disconnect the clients.



Client Login Events table creates events of client login sessions. It maintains the login events for 7 days. This table has Client MAC address, Portal Name, SSID, Access point MAC, Voucher code (if client connected with Voucher), Access type (Google/Facebook/Voucher).

Admin can export the client login events as PDF / CSV.

Table 48: Sessions Parameters

Parameter	Description
Access Point	MAC address of the Access Point.
Access Type	Access type as Free or Voucher.
Client MAC	MAC address of the client.
Disconnect	Displays if the client is disconnected from the network.
Remaining Time	The time left for the client to access the Internet. It depends upon the session duration configured in the Access Portal.
Voucher	Displays the valid applied voucher.
WLAN	SSID of the network.

NOTE:

For **Free** Access method, the client MAC address is displayed even after the free session duration expires. Delete the MAC address of the client after the Renewable Frequency completes.

Mapping the Device to Guest Access Portal in cnMaestro

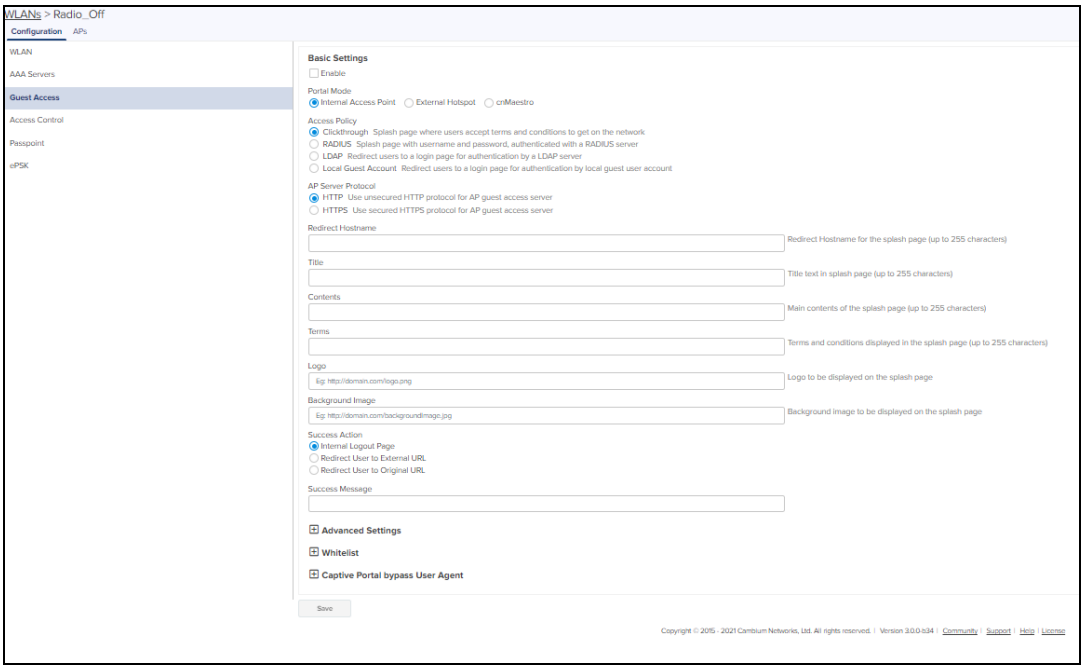
The administrator needs to configure the name of the Guest Access Portal in the device which redirects the device to cnMaestro for client connectivity.

NOTE:

The client gets the fully configured splash page for login only if the Access Point is onboarded into the server.

Configuration at Device Side

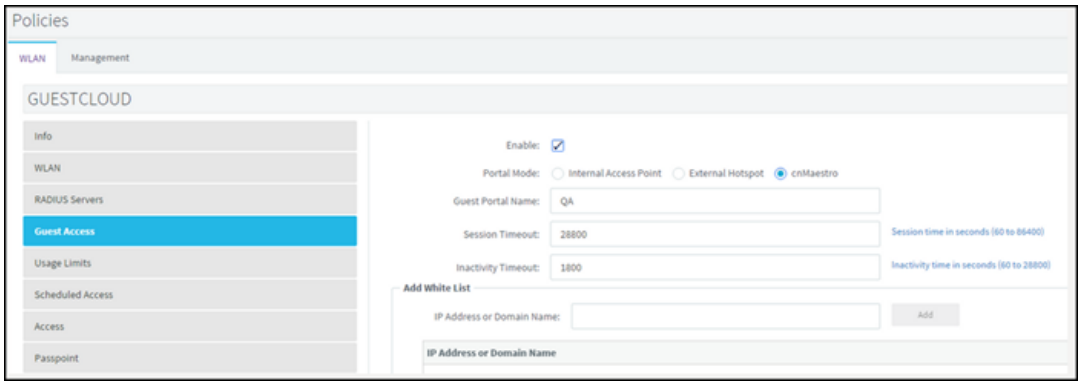
1. Login to the device.
2. Navigate to **Configuration > WLAN > Guest Access**.

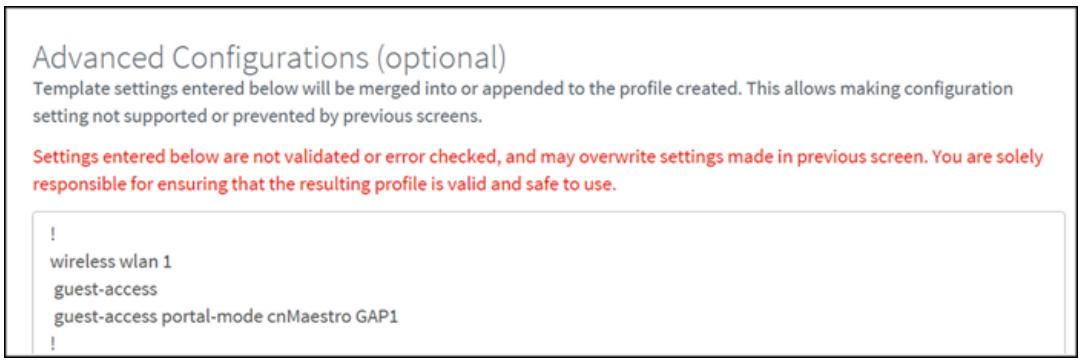


3. Select the check box to enable Guest Access.
4. Choose the **Portal Mode** radio as **cnMaestro**.
5. In the **Guest Portal Name** text box, select the name of the portal that was created in cnMaestro and enter the respective parameters.

Configuration at cnMaestro Side

The administrator can push the configuration from cnMaestro through policy or advanced configuration.

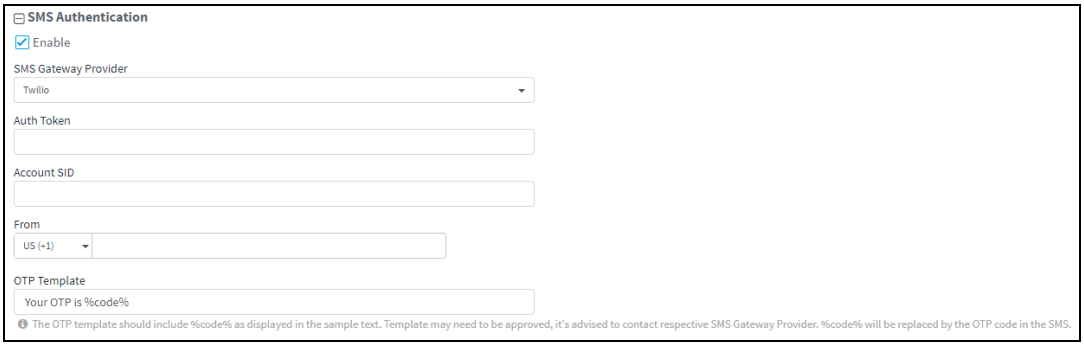




Access Types

The following table describes the parameters in configuring SMS authentication:

Parameter	Description	SMS Gateway Provider				
		Fast SMS	SMS Country	SMS Gupshup	Twilio	Victory Link SMS
Enable	It indicates to enable the SMS Authentication feature.	✓	✓	✓	✓	✓
Username	Indicates the username of the vendor.	✓	✓	✓	X	✓
Sender ID	It is the name or number which flashes on the recipients mobile phone when they receive SMS. This is Optional not mandatory.	✓	✓	✓	X	✓
API Key	It's a token which is provided by vendors.	✓	X	X	X	X
Account Type	It shows type of accounts such as International, OTP, Promotional and Transaction.	✓	X	X	X	X
OTP Template	The template with which SMS has to be sent.	✓	✓	✓	✓	✓
Password	It indicates the password.	X	✓	✓	X	✓
Country Code	It enables to select country code based on deployments.	X	✓	✓	X	X
Auth Token	It acts as a password.	X	X	X	✓	X
Account SID	It acts as a username.	X	X	X	✓	X
From	It enables to select the country code.	X	X	X	✓	X
Language	It indicates the Language.	X	X	X	X	✓



To configure SMS Authentication on cnMaestro:

1. Enable SMS Authentication feature.
2. In SMS Gateway provider, select your required gateway from the drop-down list.
3. Enter the **User Name**.
4. Enter the **Sender ID**. This field is optional. This allows user to send SMS through the ID which he chooses.
5. Enter **API Key**.
6. Select your **Account Type** from the drop-down list.
7. Enter the OTP Template. The OTP template should include "%code%. %code% replaces the OTP code in the SMS.

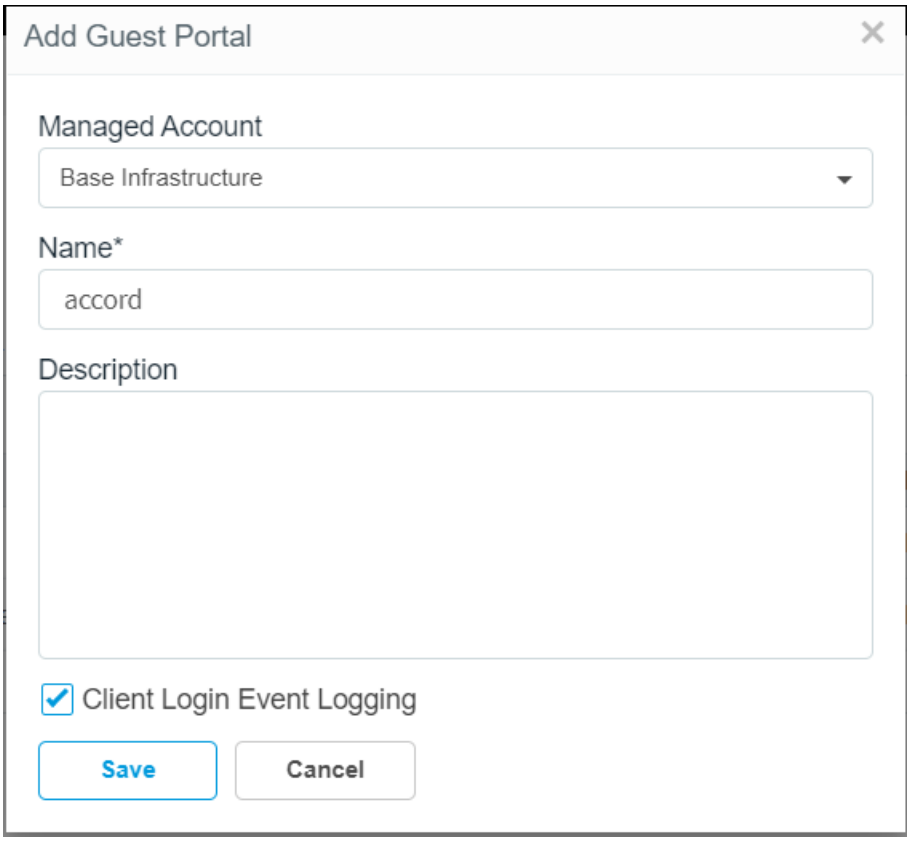
Guest Access using Social Login

Configuration

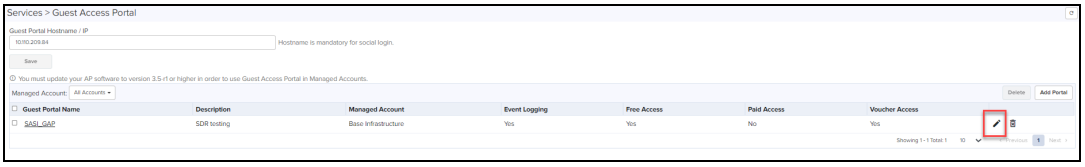
To achieve cnMaestro Guest Access using Social Logins like Google, Twitter, Facebook, Office 365, perform the following steps:

Create Guest Access profile on cnMaestro:

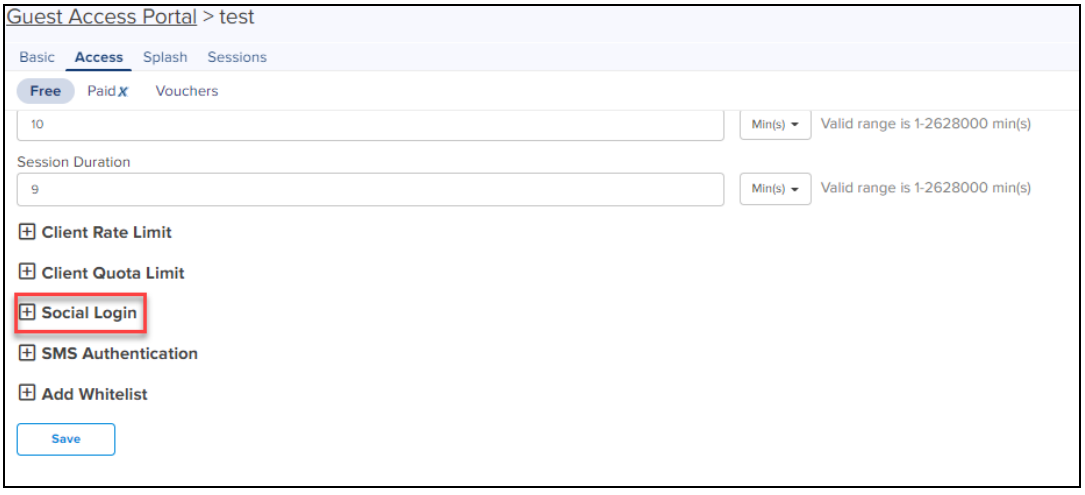
1. Login to cnMaestro and navigate to **Services Guest Access Portal** > **Add Portal.**
2. Enter Portal Name, Description, enable logging for client login events.
3. Click **Save**.



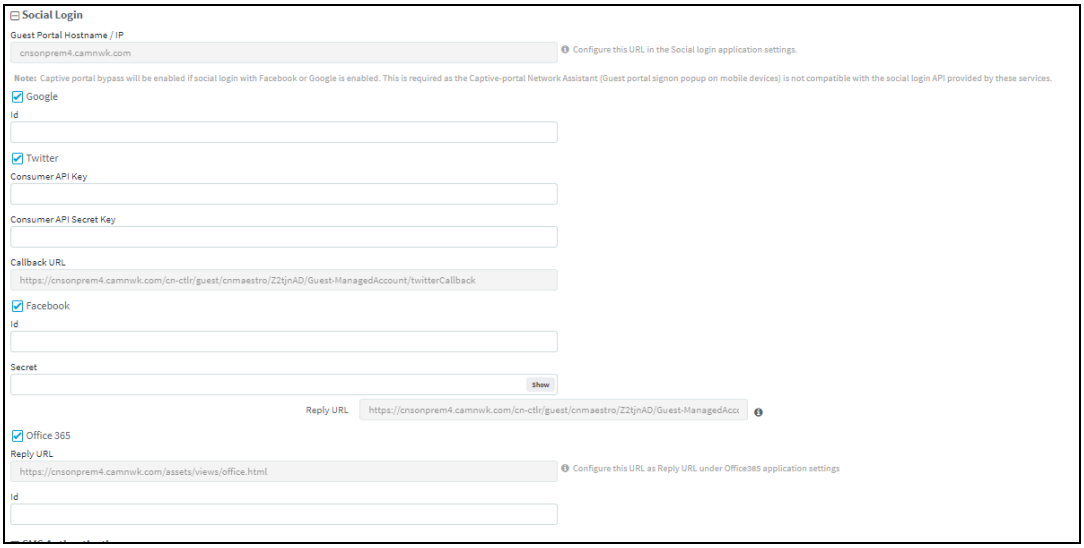
4. Click **Edit Guest Portal Details.**



5. Navigate to **Access** tab and expand **Social Login**.



6. Select Google, Twitter, Facebook, Office 365 based on your requirement.



API Key Generation

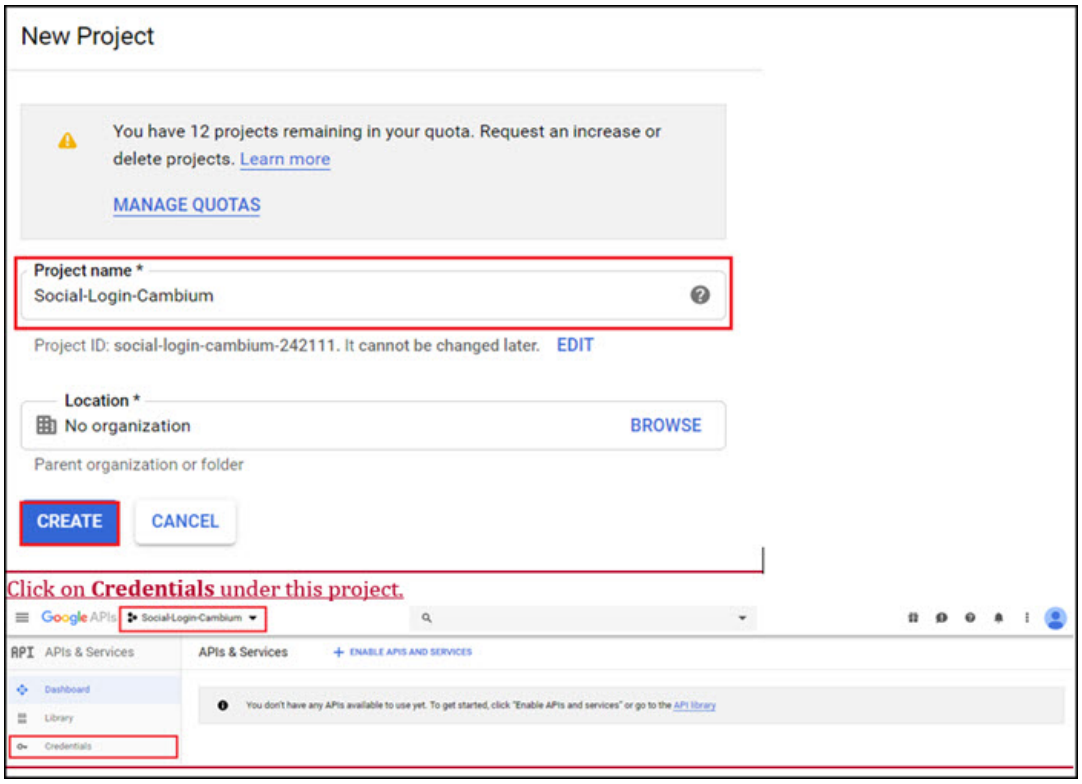
Creating APIs to integrate cnMaestro with Google, Twitter, Facebook, and Office 365.

Google

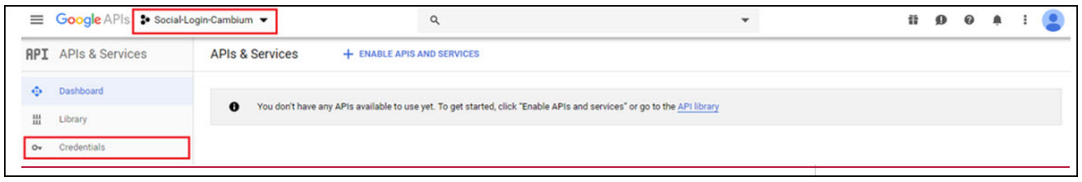
1. Login to Google Account and navigate to https://console.developers.google.com.
2. Click **Select a Project** and then click **New Project.**



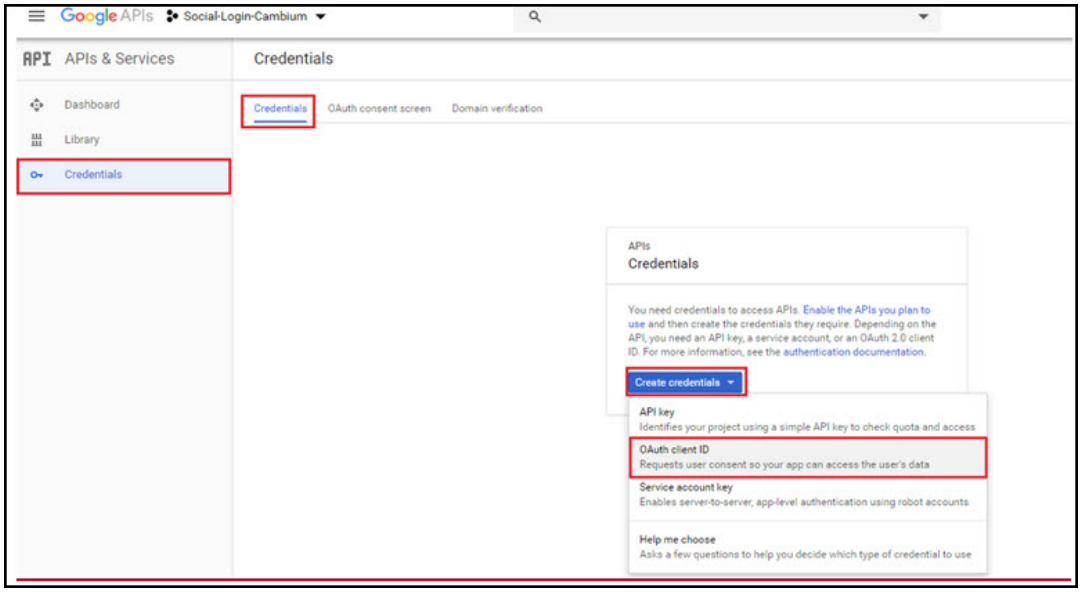
3. Enter a **Name** and click **CREATE**.



4. Click **Credentials** under this project.



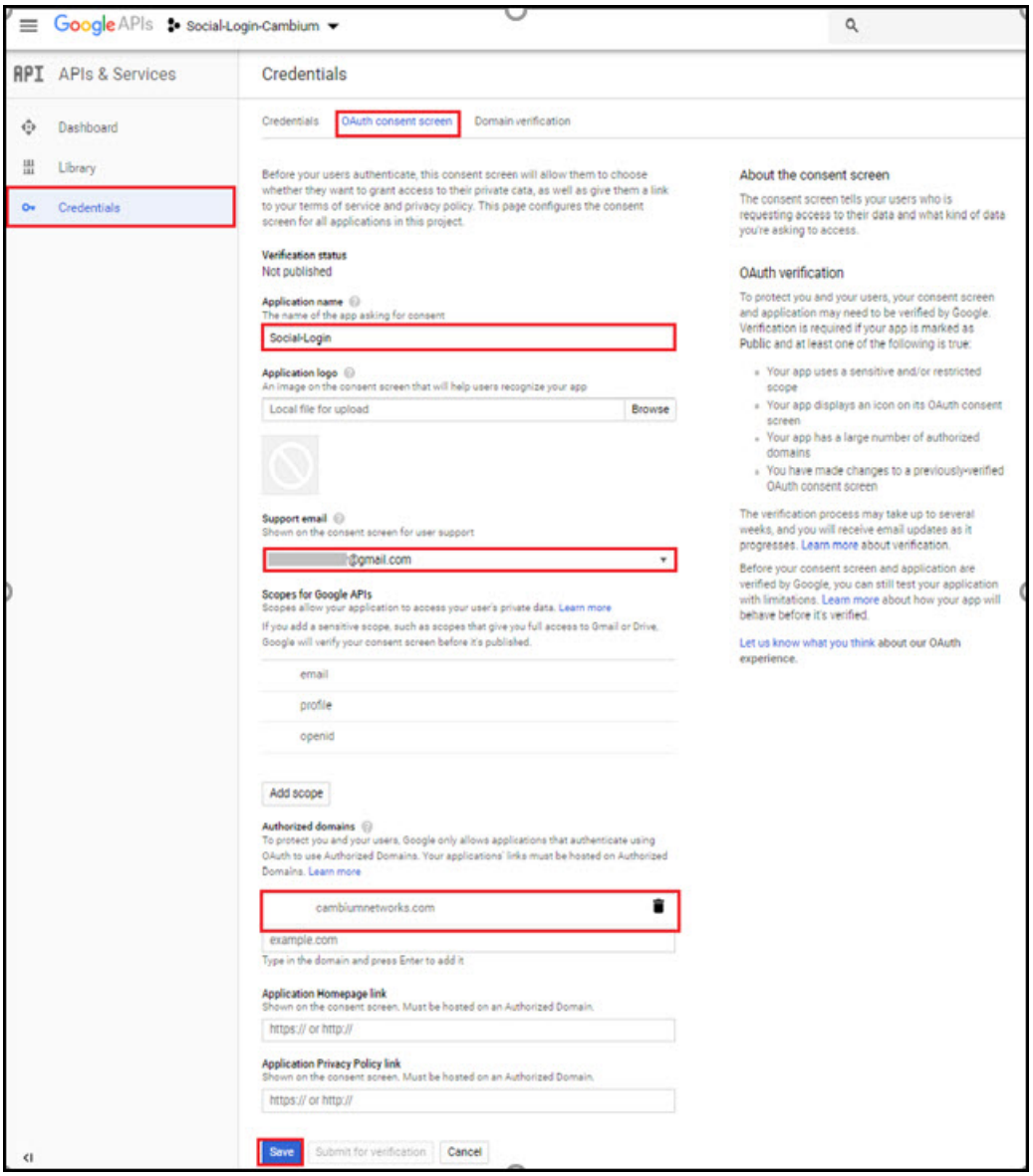
5. Under **Credentials** tab create OAuth Client ID.



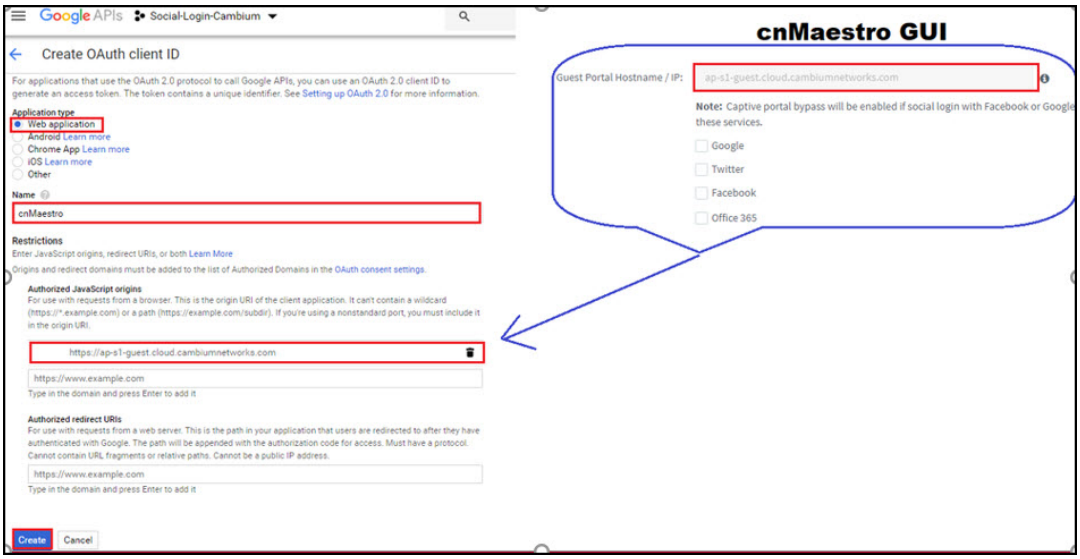
6. Click **Configure Consent Screen**.



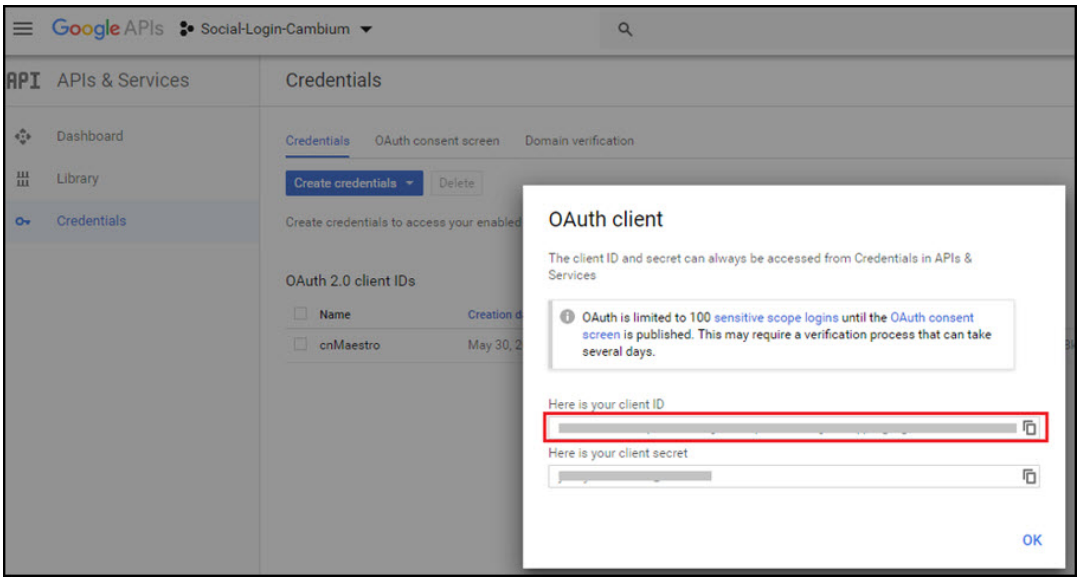
7. Assign a name to the application, map to the email ID, add cambiumbnetworks.com to the authorized domain and click **Save**.



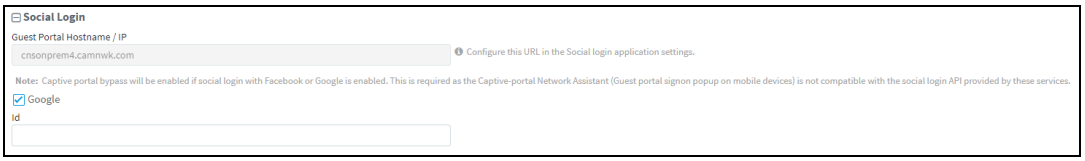
8. It redirects to creation of OAuth Client ID.
9. Select **Application type** as **Web Application**, give a Name, add Guest Portal Hostname url/IP which cnMaestro UI provides and click **Create**.



10. It redirects to the screen showing Client ID and Client Secret.

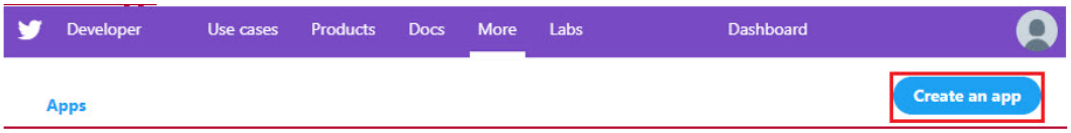


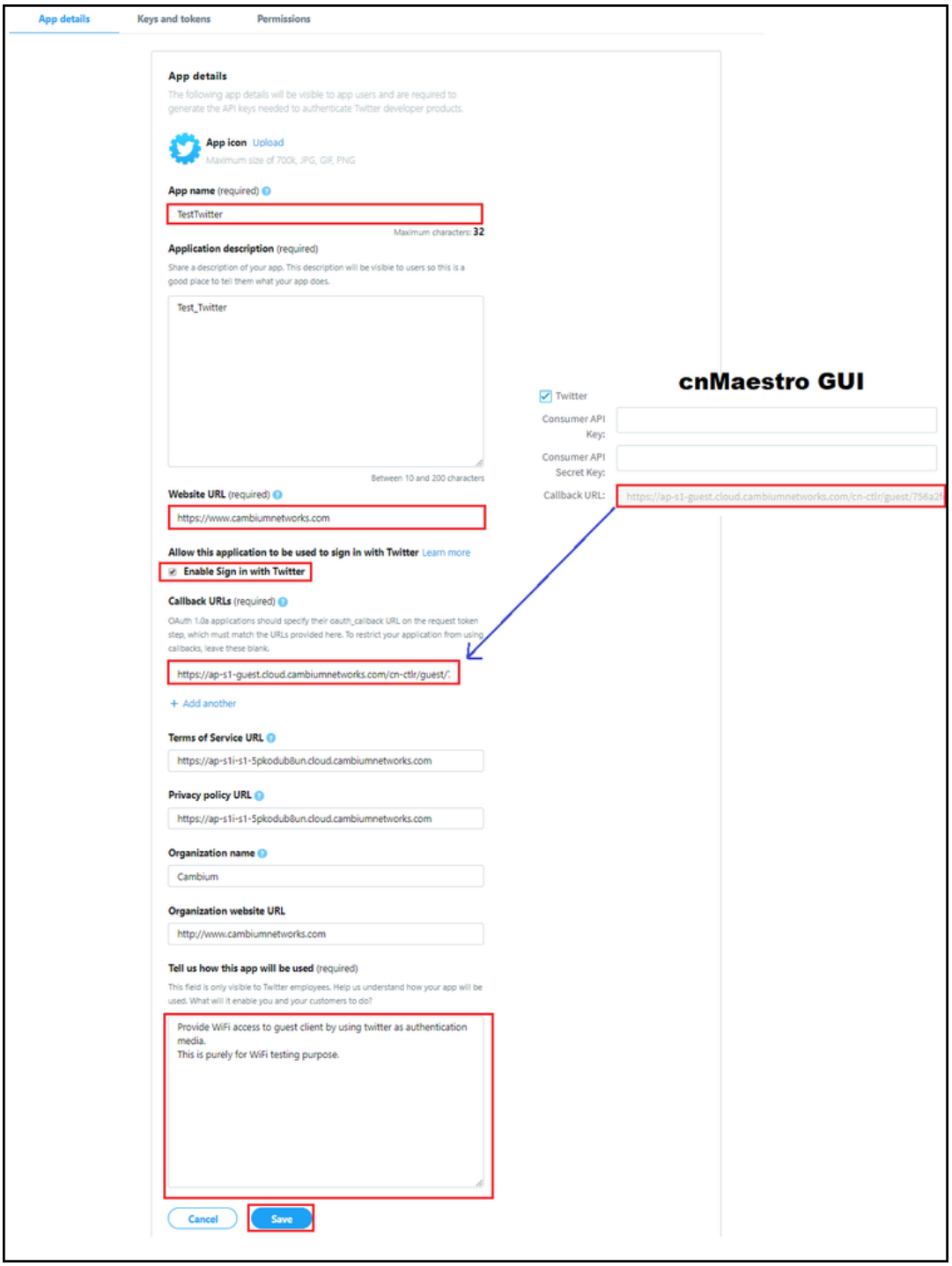
11. Copy the Client ID and paste it to the cnMaestro enabling Google under Social Logins and click **Save**.



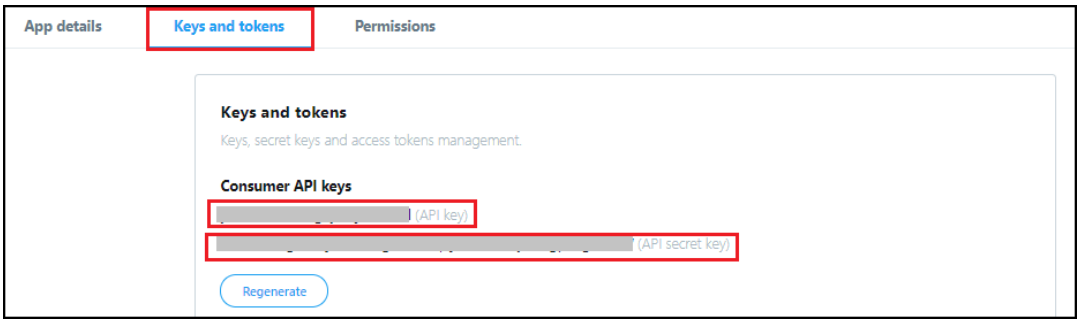
Twitter

1. Login to Twitter Account and access **https://developer.twitter.com/en/apps**, and click **Create an App**.





2. Click **Keys** and **Tokens** and copy Consumer API Key and Consumer API Secret Key.

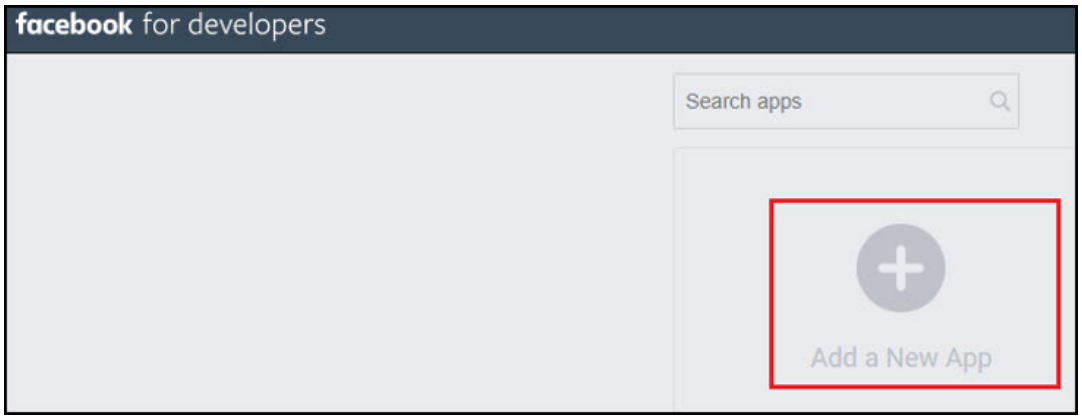


3. Paste them to cnMaestro UI for Twitter social login.

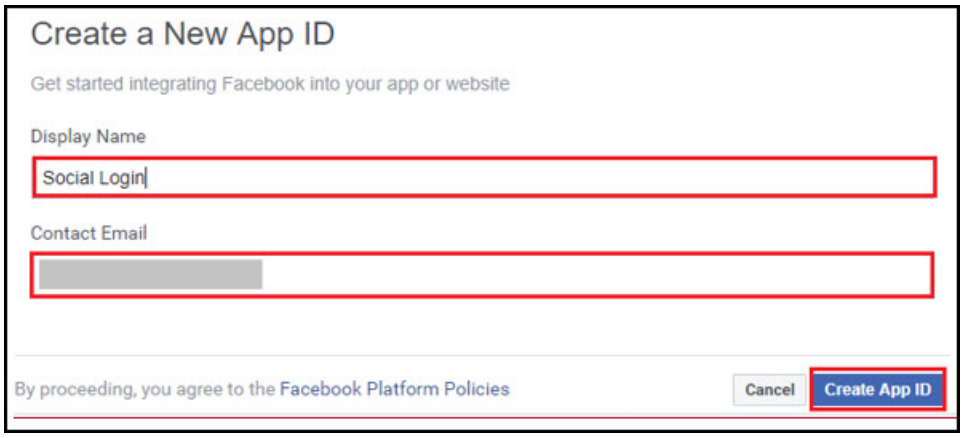


Facebook

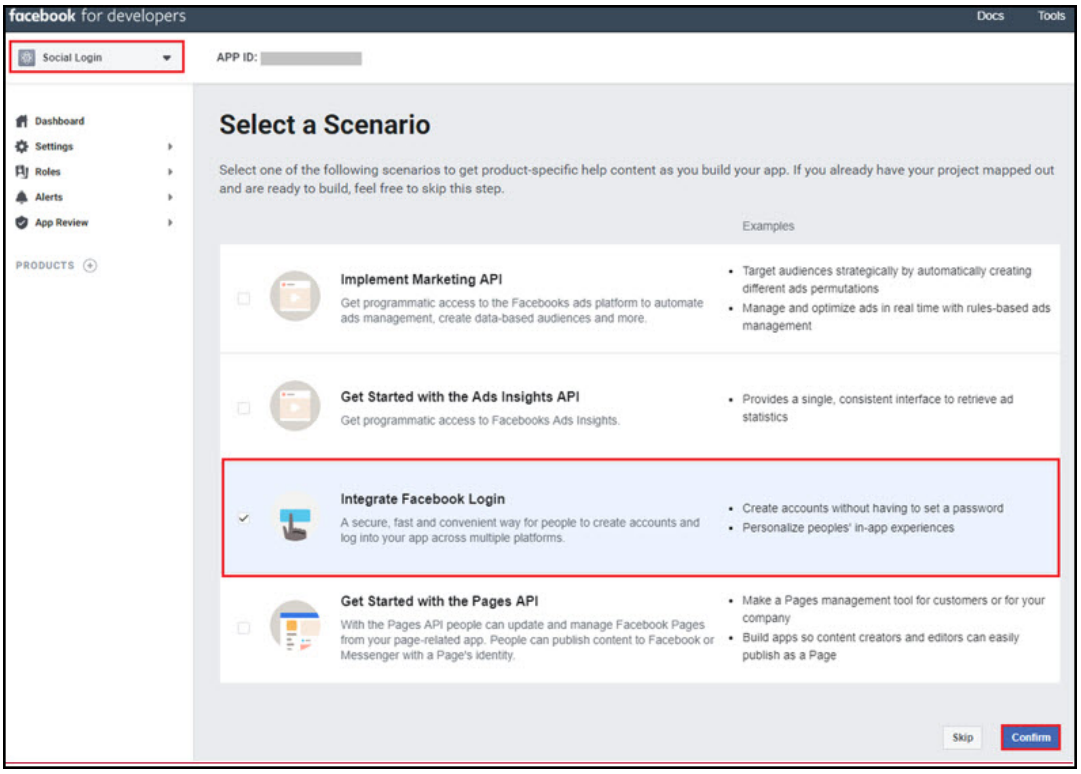
1. Login to Facebook Account and access **https://developers.facebook.com/apps/**, and click **Add a New App**.



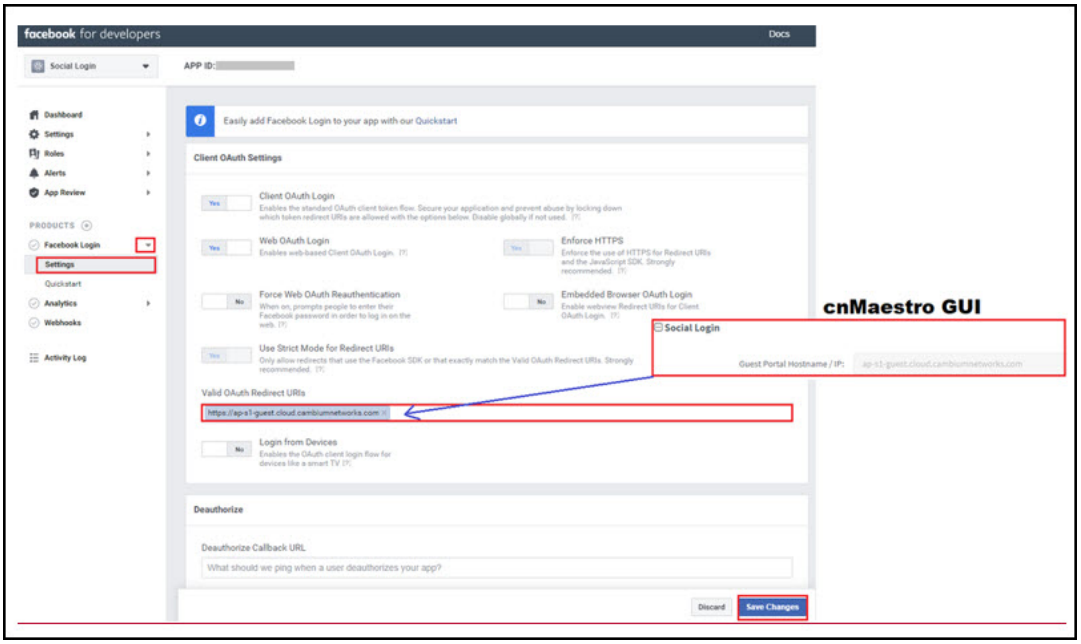
2. Enter App Display Name, Contact Email and click **Create App ID**.



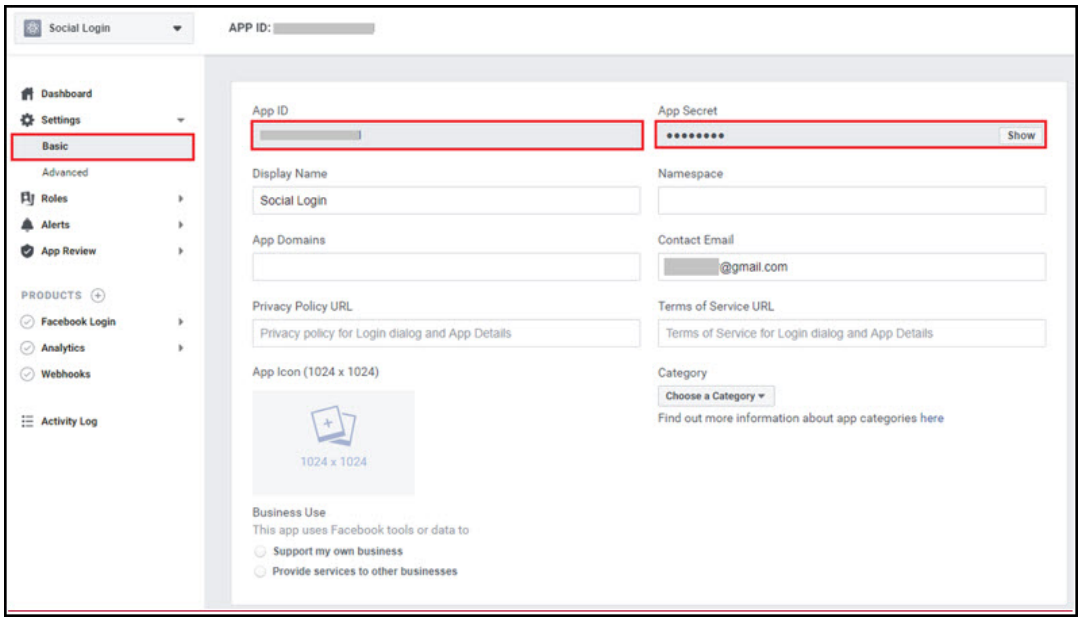
3. Select a Scenario as Integrate Facebook Login and click **Confirm.**



4. Navigate to **Settings** tab under Facebook Login and add Guest Portal Hostname from cnMaestro to valid OAuth Redirect URLs section and click **Save Changes**.



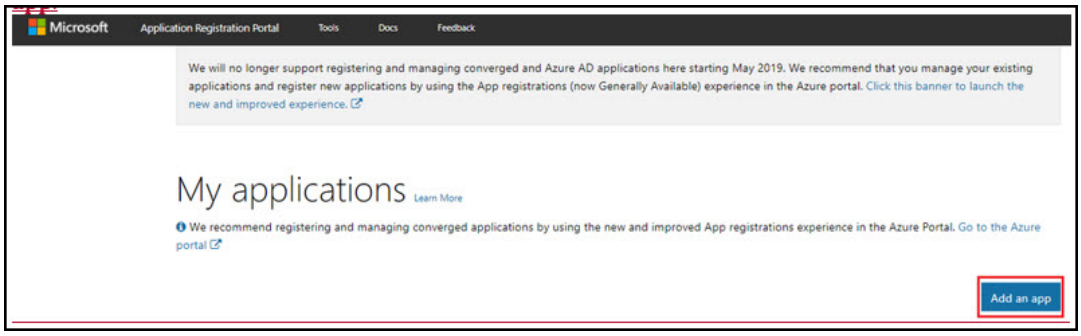
5. Navigate to **Settings** > **Basic** and copy **App ID** and **App Secret**.

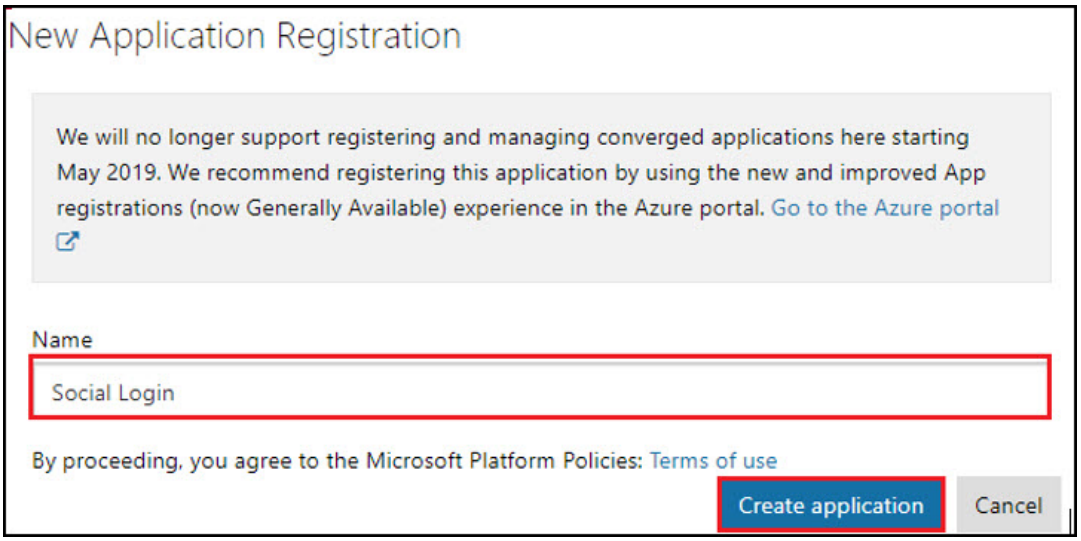




Office 365

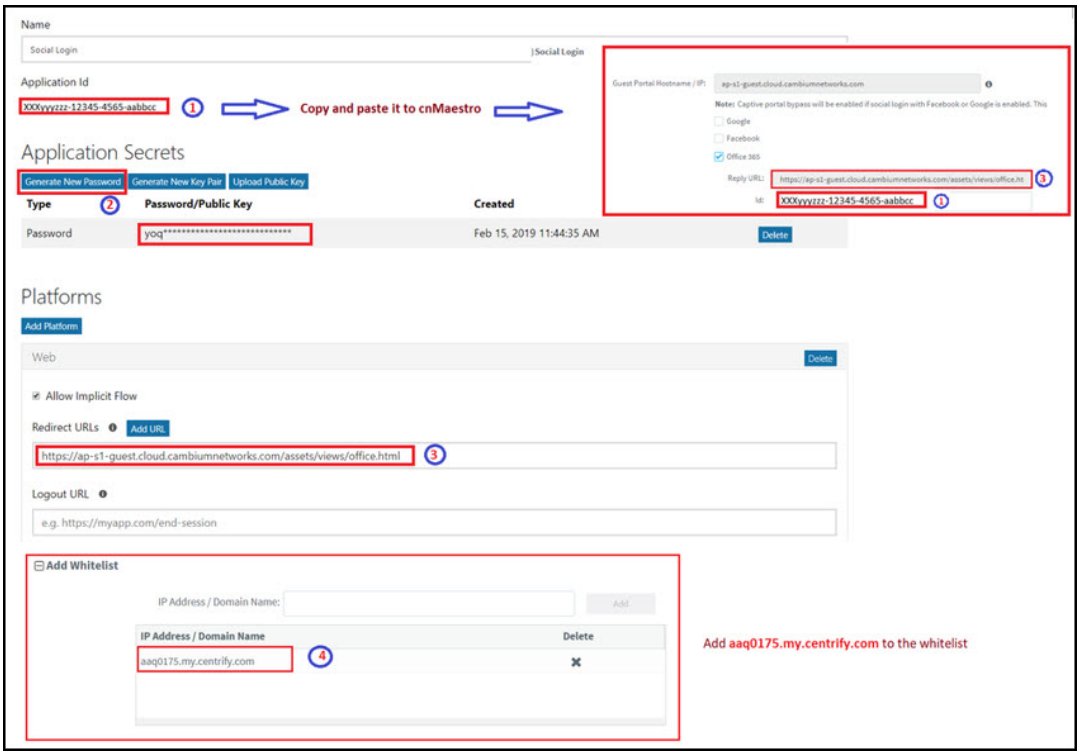
1. Login to Office 365 Account and access https://apps.dev.microsoft.com/ and click **Add an App**.





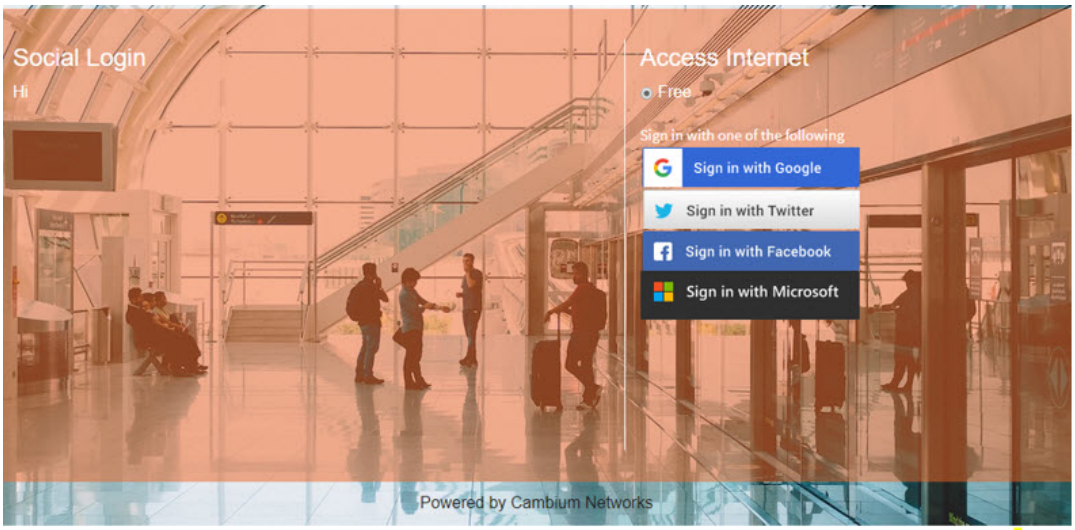
After adding your App name and clicking Create application, it redirectes to App page.

1. Copy Application ID and paste it to cnMaestro Guest Access page under Office 365.
2. Click **Generate New Password**.
3. Copy reply URL from cnMaestro and paste it under Redirect URLs.
4. Add my.centrify.com to the Whitelist on the cnMaestro.



Sample Template

Sample client login page is displayed as shown below:



SMS Authentication

The gateway provider sends a text SMS containing the OTP to end users phone number. Once OTP is received the client can enter the OTP and get the Internet access.

Twilio, SMS Country, and SMS Gupshup are the SMS gateway providers that support the SMS OTP. Also there is a generic SMS gateway option, which provides flexibility to configure any preferred SMS gateway by cnMaestro users. Configuring SMS Gateway through this generic SMS gateway does require a little more involvement by cnMaestro user to go through the Integration specifications of the given SMS gateway. Please follow the guidelines as mentioned on the Generic SMS Gateway Configuration section.

Generic SMS Gateway Configuration

SMS Service providers expose SMS API which typically works over HTTP GET or HTTP POST requests. Most of the SMS Gateways use username and password in the API requests to validate a given SMS send a request and some use special authorization token in the HTTP Headers.

Apart from that many API have specific tokens that need to be passed into the request along with the authentication part. To start off one has to first go through the SMS API document of the given SMS provider and understand what all components does it need to be provided in the HTTP request and try to build the corresponding cnMaestro configuration.

In general, all SMS API documents show some example curl commands which can be used to create an SMS request with the server. Curl examples clearly show the required components in the request and helps to find the right configuration for the cnMaestro Guest Portal Generic SMS API.

The cnMaestro Generic SMS API configuration is split into multiple components which makes it easy to configure the static and the dynamic part of the SMS API request. It also provides a way to handle the SMS API response and validate the API success or failure case. How to handle the reply can be found under the Advanced options.

SMS Gateway Provider Name

Provide the SMS Gateway name which is used for reference purposes. This is not part of API request so please just provide some meaningful name to identify this SMS Gateway service provider.

HTTP Request Type

Based on the SMS gateway provider and the API document information, identifies the SMS API. The SMS API uses “HTTP GET or HTTP POST” requests for communication with the SMS gateway server.

Example HTTP GET API Request

https://smsapiserver.com/service/sms/send?user=xxx&password=yyyyy&message=”Your OTP is ABCD”&mobileNumber=123456789&dnd=yes&sid=SenderID&v=1.1&messagType=N

Curl command to do HTTP GET request

Curl -v https://smsapiserver.com/service/sms/send?user=xxx&password=yyyyy&message=’Your OTP is ABCD’&mobileNumber=123456789&dnd=yes&sid=SenderID&v=1.1&messagType=N

Example HTTP POST Request

HTTP POST URL

https://smsapiserver.com/service/sms/send

HTTP POST Form Content

user=xxx&password=yyyyy&message=”Your OTP for Internet Access is QW123”&mobileNumber=123456789&dnd=yes&sid=SenderID&v=1.1&messagType=N

Curl command to do HTTP POST request

```
curl -v “https://smsapiserver.com/service/sms/send” -H "Content-Type: application/x-www-form-urlencoded" -X POST \
--data-urlencode 'user=xxx' \
--data-urlencode 'passwd=yyyyy' \
--data-urlencode 'mobilenumber=1234567789' \
--data-urlencode 'message=Your OTP for Internet access is QW123' \
--data-urlencode 'sid=Sid' \
--data-urlencode 'v=1.1' \
--data-urlencode 'mtype=N' \
--data-urlencode 'dnd=yes' \
--data-urlencode 'DR=Y'
```

If the SMS Gateway is using an authorization token, then below example curl request shows how the “Authorization” field is added into a HTTP header.

```
curl -v -H "Authorization: Bearer nZYIoU7QoUxfD03ct1CC2YvInqI7DmUAH6RYz01K1" \
"https://smsapiserver.com/service/sms/send?\
from=Test&\
to=123456789&\
message=’Your OTP for Internet access is QW123’&\
format=json"
```

All the SMS API have some components as follows:

- Static components which are part of the request.
- Two dynamic components which are the part of the mobile number, to which the SMS needs to be sent and the message which contains the OTP.

Static Components

API URL

Based on our above curl request example the URL configures as https://smsapiserver.com/service/sms/send where the request needs to be sent.

API URL Information

From the example curl request please find the static components of the URL. Based on our above example this configures as “user=xxx&password=yyyyy&dnd=yes&sid=SenderID&v=1.1&messagType=N”.

So what we have done here is removed the message and mobile number query strings from that URL and configured rest all. This is what a static component is for a given SMS API so identify what all options are required for the SMS API request and add it here in this given format of “key1=value1&key2=value2...”.

HTTP Request Header Key

Based on the above example, If the SMS Gateway Provider API uses some HTTP header field like authorization token, etc. Then the corresponding HTTP header field name will be configured as **Authorization**.

HTTP Request Header Key Value

Based on the above example, the SMS gateway API config settings expose some authorization token or auth token and the provided HTTP header key value will be configured as “Bearer nZYIoU7QoUxfD03ct1CC2YvInqI7DmUAH6RYz01K1” in this configuration.

Dynamic Components

Message Parameter Name

From the example curl request or the SMS gateway provider the parameter name used for the message key component where the OTP is added. It could be something like “message”|”text”|”msg” or whatever custom parameter name is used for sending the message component.

In our example curl request, we have used “message” and this is what configures based on the example curl request.

Mobile Number Parameter Name

From the example curl request or the SMS gateway provider the parameter name used for the mobile number key component where the OTP has to be sent. It could be something like “To”|”mobile”|”mobile” number” or whatever custom parameter name is used for sending the mobile number component.

In our example curl request, we have used “mobile number” and this is what configures based on the example curl request.

Advanced Options

If you care for adding functionality for parsing the SMS API response on the cnMaestro and find if the request was successful or if the server returned an error. Then one can use this advanced configuration to let cnMaestro parse the SMS API reply.

The usual HTTP response code is anyway handled by default and this advanced config parses the reply content is configured. This should be configured by advanced users only and in case if there is any failure seen in SMS functionality then disable this and report the issue to cambium Networks support.

Reply Type

The SMS gateway API sends back a response to let the client know about the request results, this result could be in text format or in json/xml format. So based on the SMS API document select the reply type here as “ TEXT”.

Success

Configure the text to match the success case as follows:

- Typically, servers may respond with a text message in reply like “success” or “sent”, then configure the exact message which should be matched in the response.
- If a server response is like “success, sent message to xxxxx”, then configure just “success” which matches in the reply.

Error

Configure the text which matches the failure case as follows:

- Typically, servers may respond with a text message in reply like “Error” or “failure”, then configure the exact message which should be matched in the response.
- If a server response is like “ERROR, failed to send SMS to xxxxx, out of credit”, then configure just “ERROR” which matches in the reply to mark it as an error.

Reply Type “JSON”

JSON Reply Success Key Name

Please look for the SMS gateway provider API document in detail and find the JSON examples for the reply and identify the key which contains the successful response status value.

cnMaestro guest portal generic SMS supports nested JSON too and one has to configure the complete path for the given result key which contains the SMS message sent status. Example JSON replies are given below to be configured for this config:

Example 1

```
{
  "messages": {
  "to": "123456789",
  "status": {
  "id": 0,
  "groupId": 0,
  "groupName": "ACCEPTED",
  "result": [
 {
  "status": "MESSAGE_ACCEPTED"
 }
],
  "description": "Message accepted"
 },
  "smsCount": 1,
  "messageId": "2250be2d4219-3af1-78856-aabe-1362af1edfd2"
 }
}
```

Success Key Name to be configured based on the above example messages.status.result[0].status.

Example 2

```
{
  "count": 1,
  "list": [
 {
  "id": "14609785729139684440",
  "points": 0.16,
  "number": "48500500500",
  "date_sent": 1460978579,
  "submitted_number": "48500500500",
  "status": "QUEUE"
  }
 ]
}
```

Success Key Name to be configured based on the above example list [0]. Status.

Example 3

```
{
 “status”: “Sent”
```

```
}
```

Success Key Name to be configured based on the above example is status.

JSON Reply Success Key Value

The success status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message successfully sent or successfully queued, which is also a success case that the queued message sents out shortly.

Based on our examples the status or the result field can be mapped to multiple values like as follows:

- Sent
- Queued
- Success
- Message Accepted

So in this configuration one can add multiple such values that should be matched for the success case for the value as received for the “JSON Reply Success Key Name” field.

JSON Reply Failure Key Name

Look for the SMS Gateway Provider API document in detail and find the JSON examples for the reply and identify the key which contains the Error/Failure response status value.

cnMaestro guest portal generic SMS supports nested JSON too and one has to configure the complete path for the given result key which contains the SMS message sent failure field. Example JSON replies are given below to be configured for this config:

Example

```
{
  "invalid_numbers": [
{
  "number": "456456456",
  "submitted_number": "456456456",
  "message": "Invalid phone number"
  }
],
  "error": 13,
  "message": "No correct phone numbers"
}
```

JSON Reply Failure Key Name to be configured based on the above example is error.

JSON Reply Failure Key Value

The error/failure status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message sent error or multiple error codes for the corresponding error.

Based on our examples the error can be mapped to multiple values like 13|12|-1 etc. So in this configuration, one can add multiple such values which should be matched for the failure case for the value as received for the “JSON Reply Failure Key Name” field. Reply Type “XML”.

Reply Type “XML”

XML Reply Success Element

Look for the SMS gateway provider API document in detail and find the XML examples for the reply and identify the elements which contain the successful response status value.

cnMaestro guest portal generic SMS supports nested XML too and one has to configure the complete path for the given result element which contains the SMS message sent status. Example XML replies are given below to be configured for this config:

Example 1

```
<items>
<item id="0001" type="result">
<status>Success</status>
</item>
</items>
```

Success Element Name to be configured based on the above example is items/item/status.

Example 2

```
<?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://tempuri.org/">-11</int>
```

Success Element Name to be configured based on the above example.

XML Reply Success Element Value

The success status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message successfully sent or successfully queued, which is also a success case that the queued message sents out shortly.

Based on our examples the status or the result field can be mapped to multiple values like as follows:

- Sent
- Queued
- Success
- Message Accepted

So in this configuration one can add multiple such values that should be matched for the success case for the value as received for the “XML Reply Success Element” field.

SMS message sent failure field. Example XML replies are given below to be configured for this configuration:

Example 1

```
<items>
<item id="0001" type="result">
<error>-12</status>
</item>
</items>
```

XML Reply Failure Key Name to be configured based on the above example is items/item/error.

Example 2

```
<items>
<item id="0001" type="result">
<status>Error</status>
</item>
</items>
```

XML Reply Failure Key Name to be configured based on the above example is items/item/status.

Example 3

```
<?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://tempuri.org/">-11</int>
```

XML Reply Failure Key Name to be configured based on the above example is int.

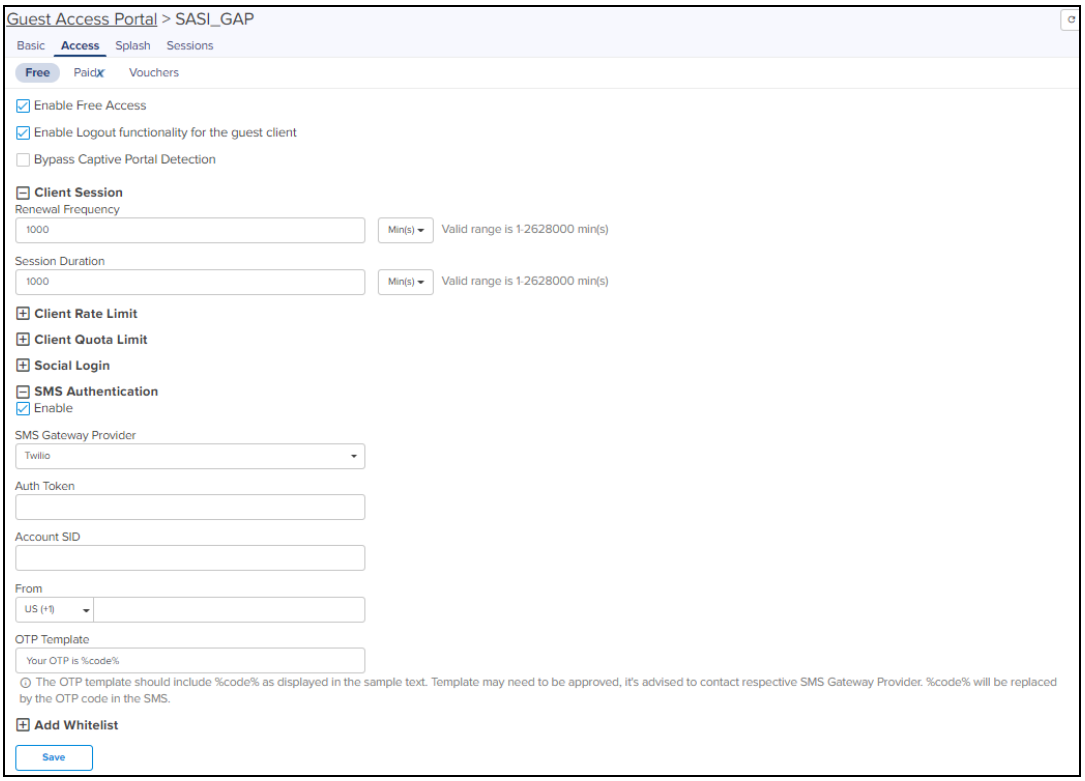
XMl Reply Failure Element Value

The error/failure status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message sent error or multiple error codes for the corresponding error.

Based on our examples the error can be mapped to multiple values like 13|12|-1 etc so in this configuration, one can add multiple such values which should be matched for the failure case for the value as received for the “XML Reply Failure Element” field.

Sample Configuration in the cnMaestro

Figure 146 : Guest Access Portal



cnPilot GRE Tunnels

This chapter provides the following information:

- Overview
- Typical Deployment Model (Two Port Solution)
- Access Control List (ACL) Configuration

	NOTE: GRE Tunnels feature is deprecated in release 3.0.0 and will be removed in a future release 3.1.0.

Overview

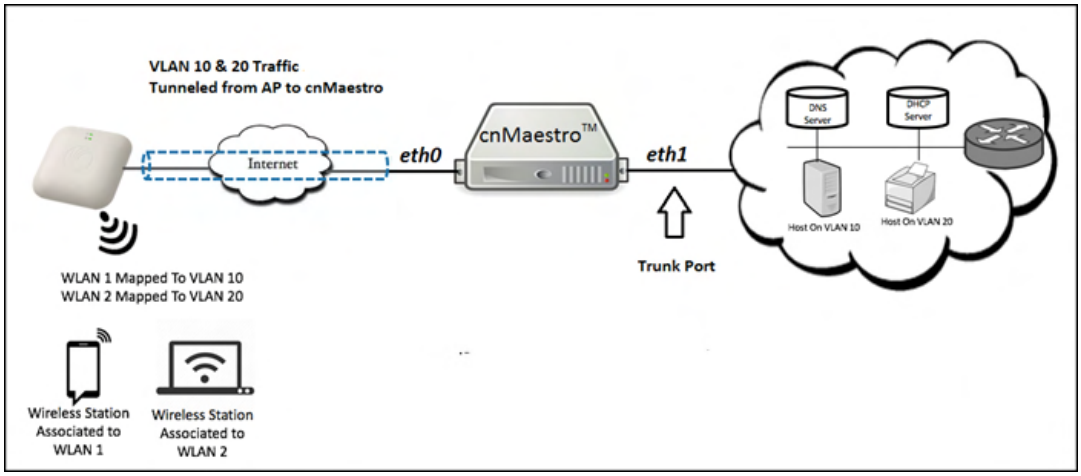
While deploying access points, the ability to tunnel wireless traffic from the APs to a tunnel concentrator (L2GRE/EoGRE) often plays a key role. By using the tunnel feature, the following can be avoided:

- Reconfiguration of switches and routers (for VLANs)
- Networking issues that arise when the clients IP range is not routable

The APs support L2GRE tunnel feature starting with release 3.1.1-r16. The cnMaestro On-Premises accepts tunneled traffic from the APs. With end to end tunnel solution from Cambium Networks, it is easy to get up the network fast and in reliable way.

Typical Deployment Model (Two Port Solution)

Figure 147 Typical Deployment Model (Two Port Solution)



In this deployment model, cnMaestro is equipped with two ports:

- **Primary Ethernet port (eth0)** is configured with cnMaestro IP address and all the communication between the APs and the cnMaestro On-Premises takes place at this port.
- In **Aux/bridge port (eth1)**, all the wireless clients traffic received from the APs will be transferred after removing the tunnel headers. This port comes up as a trunk port with allowed VLANs and other relevant configurable parameters from the cnMaestro UI.

Multicast/Broadcast Handling with Multiple APs on Tunnel Concentrator

In any type of deployment, multiple APs creates tunnel with the concentrator. In such scenario, the multicast/broadcast traffic (such as DHCP discovers, ARP Requests) generated by the wireless clients needs to be forwarded to aux/bridged port of the concentrator as well as to all the APs connected to the concentrator. Similarly, when any multicast/broadcast traffic is received on the aux/bridged port of the concentrator it needs to be sent to all the connected APs. In many situations, this broadcast can impact the performance and is better to restrict such traffic to flow out to all the APs.

Tunnel Concentrator is equipped with ACL feature which allows to restrict such traffic. There are many different ways by which ACL can drop the traffic. Each restriction is defined by an ACL rule. Refer ACL Configuration section for detailed information.



NOTE:

Default rules in the ACL prevents the unnecessary broadcast and multicast to go out towards the APs.

Inter AP Wireless Client Communication (through Concentrator)

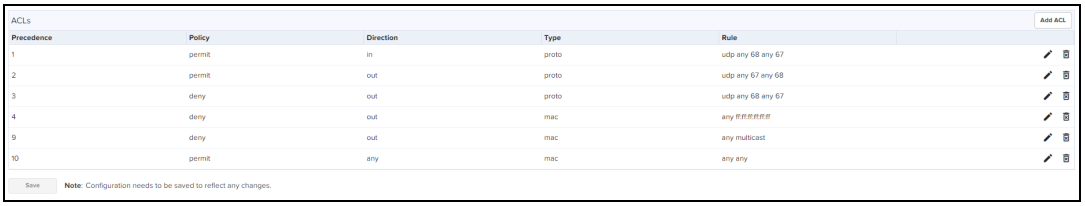
Different wireless clients on different APs can be configured to use same or different VLANs. When clients on different APs but on same VLAN try to communicate with each other, then the concentrator bridges the traffic received from one AP to other(s) access point(s) (if not restricted by ACL rules). However, when clients on different APs are using different VLANs (different subnets) then concentrator does not forward traffic from one AP to another AP.

Access Control List (ACL) Configuration

ACL provides mechanism to filter out the unwanted traffic passing through the tunnel as well as traffic going between the APs. ACL provides many options to deny or permit the traffic. Traffic can be denied / permitted based on MAC layer, IP layer, and Protocol layer along with direction of flow. ACL is configured with the help of rules, each of them comes with a precedence. In these rules, **IN** direction refers to traffic coming from APs to the concentrator and **OUT** direction refers the reverse.

ACL comes up with default rules that prevent unnecessary broadcast and multicast to go out towards APs. With these rules, the inter AP communication is blocked.

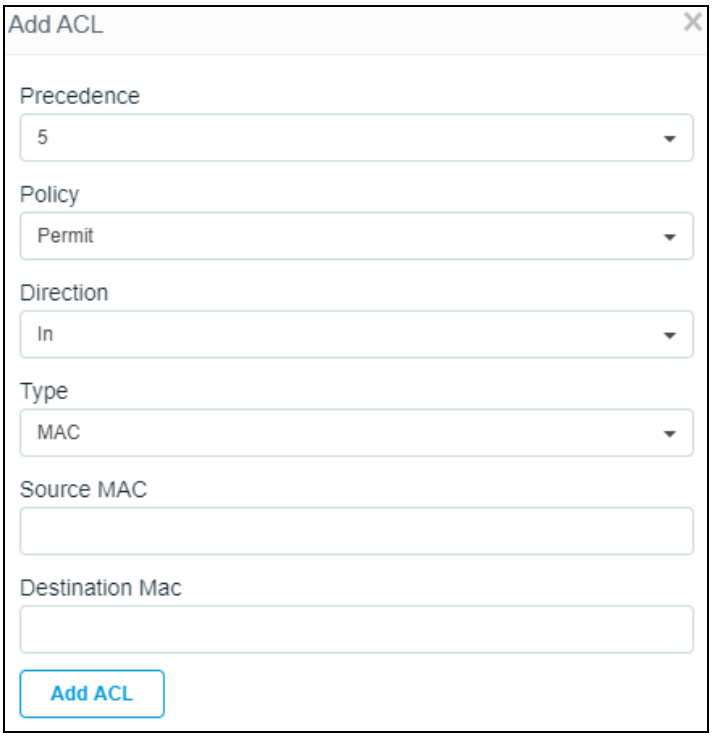
Figure 148 ACL Configuration



The following are the screenshots for the different ACL rule categories:

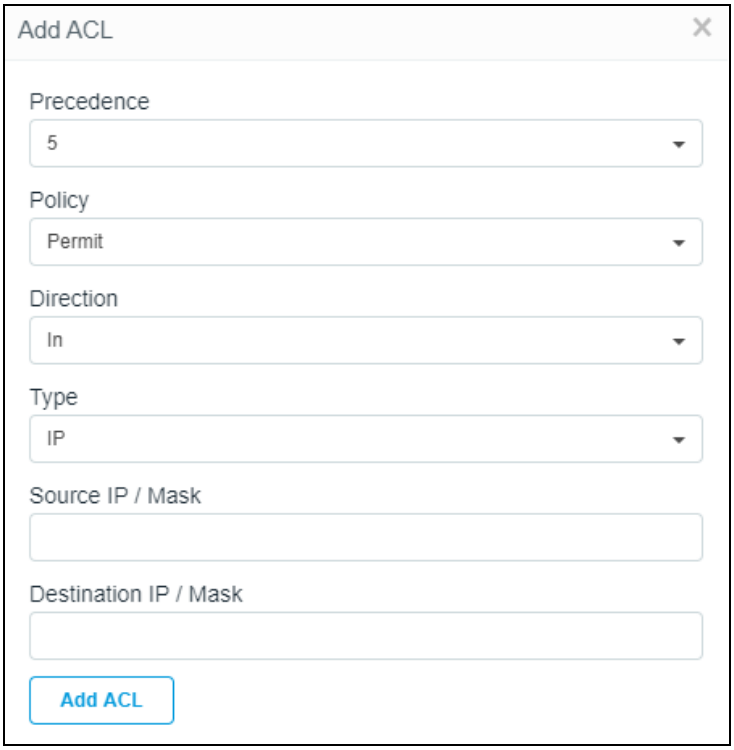
MAC Layer ACL

Figure 149 MAC Layer ACL



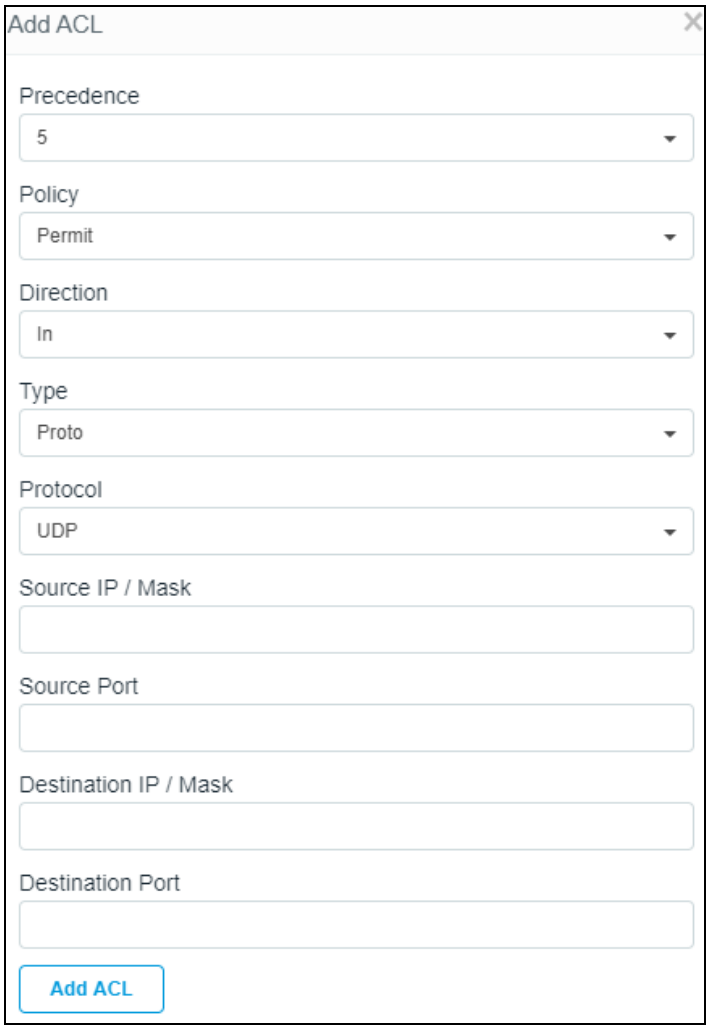
IP Layer ACL

Figure 150 IP Layer ACL



Transport Layer ACL

Figure 151 Transport Layer ACL



SNMP

This chapter provides the following information:

- Overview
- Enable SNMP
- Configure SNMP Parameters
- cnMaestro MIB (Management Information Base)

Overview

Currently, cnMaestro On-Premises supports SNMPv2c for basic monitoring data and online/offline traps and is a cnMaestro X feature.

	NOTE: SNMP uses UDP port 161 for GET requests and UDP port 162 for TRAPs.

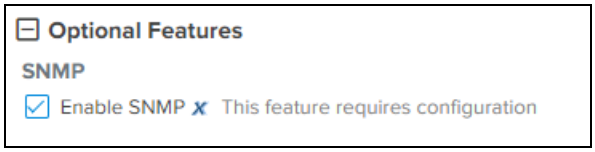
Enable SNMP

To enable SNMPv2c, navigate to **Administration > Settings > Optional Features** and enable **SNMP management.**

This turns on SNMP functionality within the UI; however, the server itself does not start until the SNMP Configuration is completed.

	NOTE: SNMP Services does not start until a valid configuration exists.

Figure 152 Enable SNMP

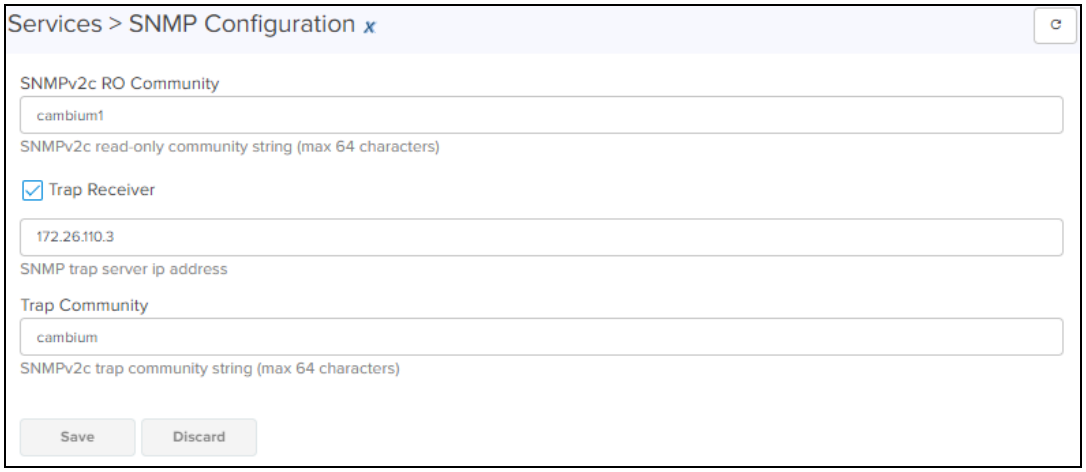


Configure SNMP Parameters

To configure SNMP Parameters, perform the following:

1. Navigate to **Services > SNMP Configuration** (this tab is only visible if SNMP is enabled).

Figure 153 Configure SNMP



2. Enter the **SNMPv2c RO Community String** name (maximum limit is 64 characters).
3. Enable the **Trap Receiver** check box and enter the IP Address.

> **NOTE:**
> The user can configure the desired Trap Community string value in the cnMaestro SNMP configuration page.

4. Enter the **SNMPv2c Trap Community** string name (maximum limit is 64 characters).
5. Click **Save**.

> **NOTE:**
> If there are thousands of devices in your cnMaestro account, you should set your MIB browser or snmpget command to use a minimum timeout of 20 minutes.

cnMaestro MIB (Management Information Base)

The cnMaestro MIB can be downloaded from Cambium Support Center.

By default, the following OIDs are supported when SNMPv2 is enabled in cnMaestro On-Premises:

- .1.3.6.1.2.1 (mib-2)
- .1.3.6.1.4.1.2021 (UCD)
- .1.3.6.1.6.3.1.1 (snmpV2 - snmpMIB)
- .1.3.6.1.6.3.1.2 (snmpV2 - snmpMIBConformance)
- .1.3.6.1.4.1.17713.23 (CAMBIUM - cnMaestro)

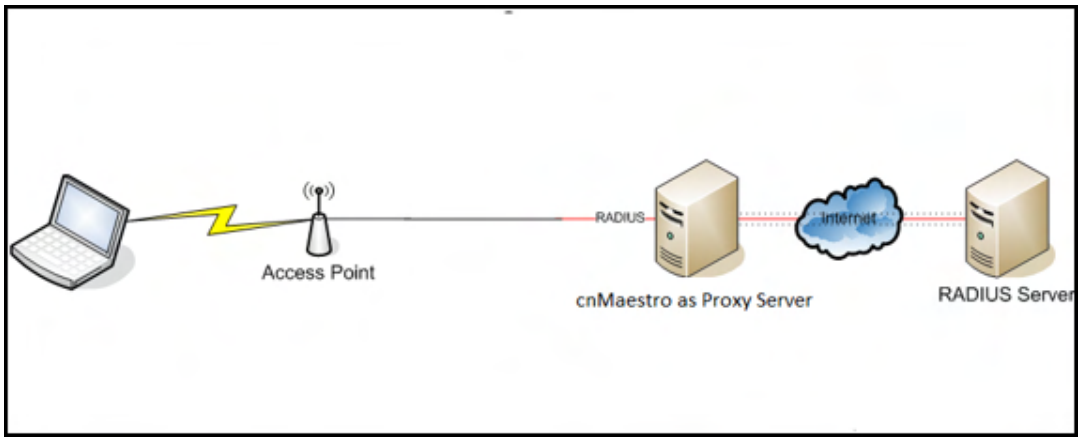
RADIUS Proxy

Overview

cnMaestro On-Premises can act as a proxy server to authenticate RADIUS requests for cnPilot Wi-Fi devices. In this scenario, cnMaestro acts as Network Access Server (NAS) for the RADIUS server.

In the below scenario, the Access Point sends RADIUS packets to cnMaestro On-Premises, and cnMaestro sends them to the RADIUS server. cnMaestro can act as a proxy for either authentication or accounting messages.

Figure 154 RADIUS Proxy on cnMaestro On-Premises



	NOTE: RADIUS Proxy is cnMaestro X feature.

Minimum cnMaestro On-Premises Version Requirements

- Minimum cnMaestro On-Premises release version required: 1.4.1-b1.
- Minimum cnPilot AP release required: 3.3.

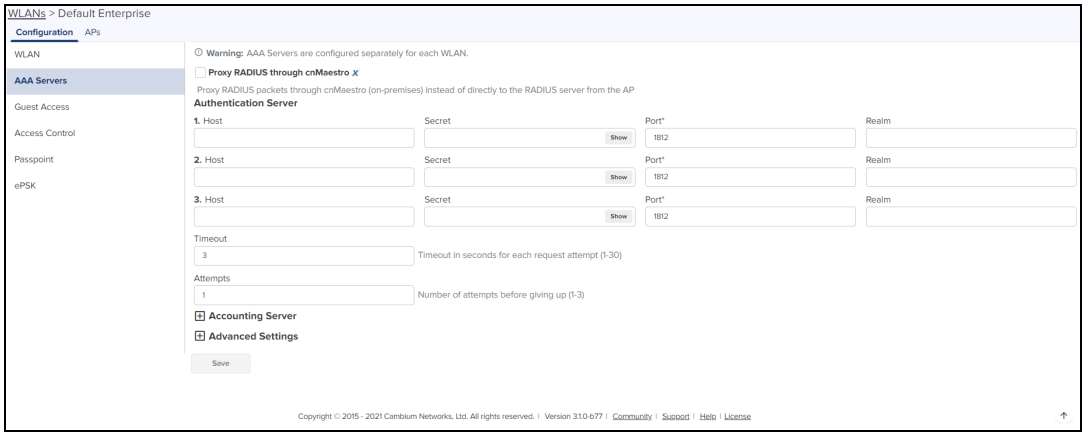
	NOTE: This feature is not available on the cnMaestro Cloud version.

RADIUS Proxy Configuration

Follow the below procedure to configure RADIUS proxy on cnMaestro On-Premises:

1. Navigate to **Shared Settings > AP Groups and WLANs** page.
2. Select **Enterprise WLAN** to edit, and then select **AAA Servers**
3. Under AAA servers, select **Proxy RADIUS through cnMaestro** check box .
4. Configure Authentication Server details.
5. Configure Accounting Server details.
6. Configure NAS-Identifier. For this, include NAS-Identifier attribute to use in RADIUS Request packets and Default to system name.
7. Push the configuration from cnMaestro to AP.

Figure 155 RADIUS Proxy Configuration



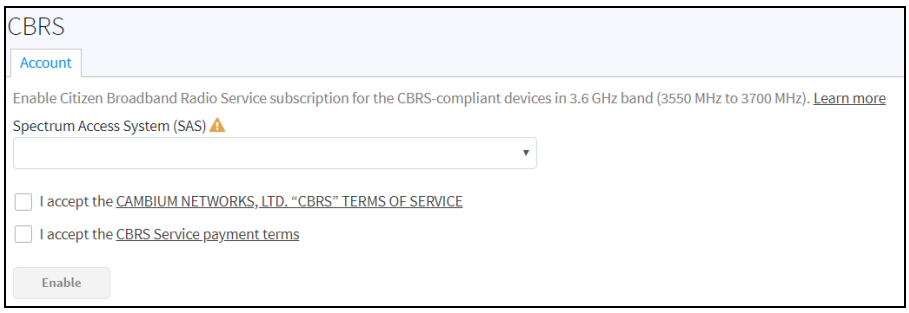
Citizen Broadband Radio Service (CBRS)

Citizen Broadband Radio Service subscription for CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz).

	NOTE: User must have an account in cnMaestro Cloud prior to enabling CBRS services in On-Premises.

Enabling CBRS in Cloud

1. Login to cnMaestro Cloud account https://cloud.cambiumnetworks.com/.
2. Navigate to **Services > CBRS** page.
3. Select preferred **Spectrum Access System (SAS)** vendor.



4. Click **I accept the CAMBIUM NETWORKS, LTD. "CBRS" TERMS OF SERVICES/I accept the CBRS Service payment terms** to activate **Enable**.
5. Click **Enable.**
6. In **Billing Information** window pops up; enter the following:

   Business Contact

   - First Name
   - Last Name
   - Email
   - Phone
   - Street Address
   - Zip Code
   - Country
   - State

   Technical Contact

   Enable **Same as Business Contact**.or enter a separate Technical Contact.

   - First Name
   - Last Name
   - Email

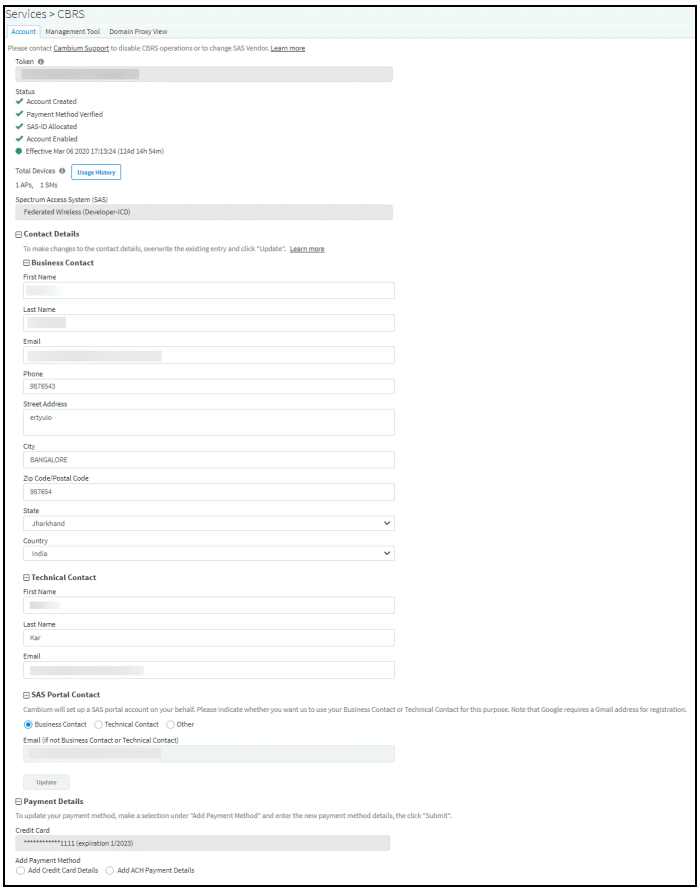
   SAS Portal Contact

   Cambium Networks creates the SAS portal account on behalf of the operator.

   - Click **Save.**



7. The **Account** page displays:
    - Token
    - Status
    - Total Devices
    - SAS
    - Contact Details
    - Payment Details



a. **Token:**

   Token used for authenticated communication with the SAS through Cambium Domain Proxy. It is generated automatically once CBRS is enabled for the Cloud account.

b. **Status:**

- Displays the account status.

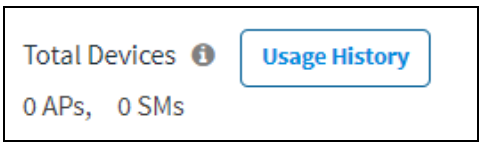
Pending Status	Sucess Status
Status Account Created Payment Method Verification Pending SAS-ID Allocation Pending Effective Jul 07 2020 16:54:10 (< 1m) Total Devices Usage History 0 APs, 0 SMs	Status Account Created Payment Method Verified SAS-ID Allocated Account Enabled Effective Mar 19 2020 15:02:02 (110d 2h 0m) Total Devices Usage History 3 APs, 68 SMs

1. **Account Creation**:Displays as Created once the account is enabled. Refer to **Step f** for entering contact information and enabling account.
2. **Payment Method**: Displays as Verified once the Payment Details are approved. Refer to **Step g** Payment Details.
3. **SAS ID**: Once the payment details are verified, the SAS ID is allocated automatically.

> NOTE
>
> It may take 1 day to get the SAS ID.

4. **Effective:**
    - **Grey** : indicates the **Pending Status**.
    - **Green** : indicates **Success**.
    - **Red** : indicates the account has been **Deactivated**.

c. **Total Devices**: Displays the count of **Total Devices** registered with the SAS using the **Token ID**. **Usage History** provides the list of devices registered with **Month** and **Year.**



> NOTE
>
> Initially the device counts will be 0 APs and 0 SMs.

d. **SAS:** Displays the SAS vendor preferred by the operator.

> NOTE
>
> Contact Cambium support to disable CBRS operation or to change SAS Vendor.

e. **SAS:** An operator needs to select which SAS vendor they prefer.

f. **Contact Details:**

For new CBRS account migrations, this information would have already been entered in **Step 6**. Review and update if necessary, else press ahead to **Step g**.

Cambium Networks selectively communicates with both the **Business Contact** and the **Technical Contact** with changes of interest: such as SAS administrator updates, CBRS initiative changes from the CBRS Alliance and WInnForum, and announcements of new Cambium CBRS features and options.

Business Contact

Cambium Networks communicates with the **Business Contact** for all commercial aspects of the CBRS Service such as invoicing, payment, change in terms, change in pricing, etc. This page requires:

- **First Name**
- **Last Name**
- **Email**
- **Phone**
- **Street Address**.
- **City**
- **Zip code/Postal Code**
- **State**
- **Country**

Technical Contact

Cambium Networks communicates with the **Technical Contact** such as software updates, publication of release notes, learning guides, technical issues, etc.

- **First Name**
- **Last Name**
- **Email**

SAS Portal Contact

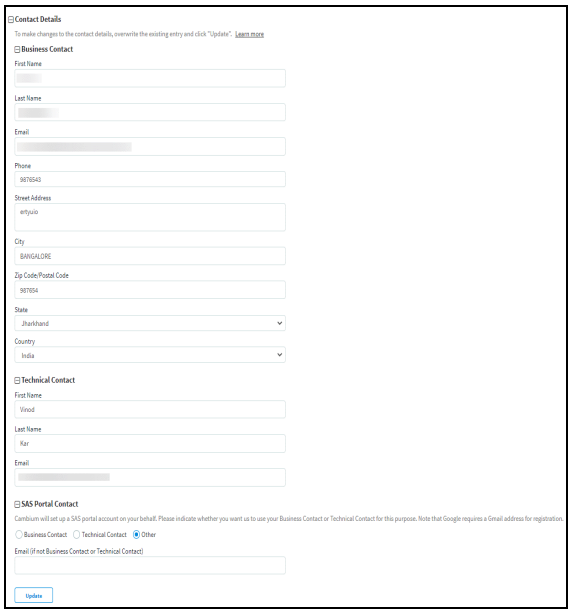
Cambium Networks sets up the SAS portal account on behalf of the operator. Please select whether you want us to use the **Business Contact, Technical Contact,** or **Other.**



NOTE

Google requires a Gmail address for registration.

- Click **Update.**

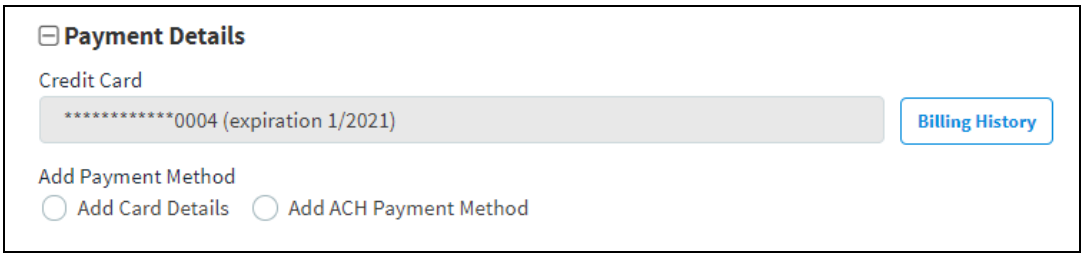


	NOTE Clicking update the Account Page will overwrite the current entries.

g. **Payment Details**

Select one of the payment methods below:

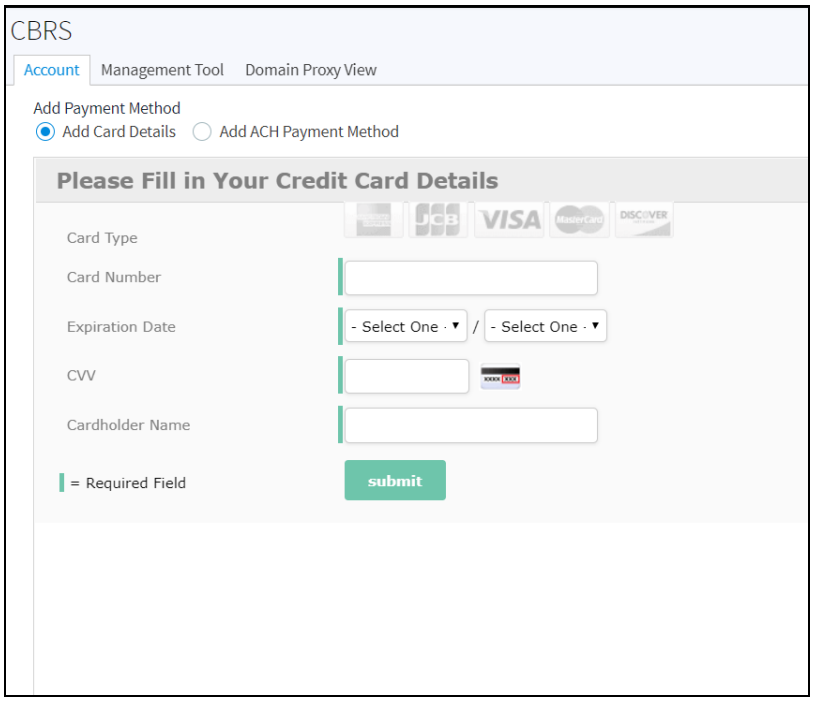
- Add Credit Card Details
- Add ACH Payment Method



Add Credit Card Details

Enter the following and click **Submit**:

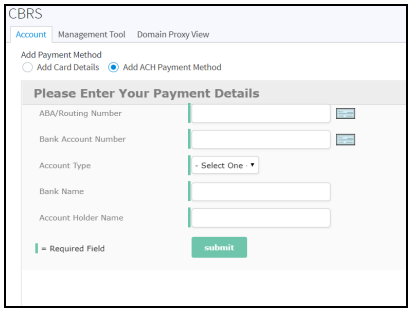
- 16 digit Credit **Card Number**.
- **Expiration Date** and **Year** on the card.
- **CVV** and **Cardholder Name**.



Add ACH Payment Method

Enter the following and click **Submit**:

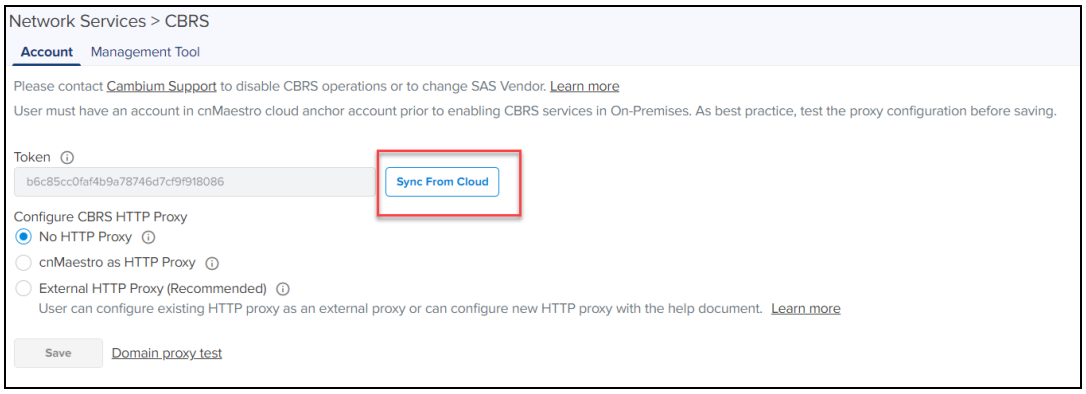
- **ABA/Routing Number**.
- **Bank Account Number**.
- Select one of the following **Account Type:**
  - Checking
  - Saving
  - Business Checking
- **Bank Name** and **Account Holder Name**.



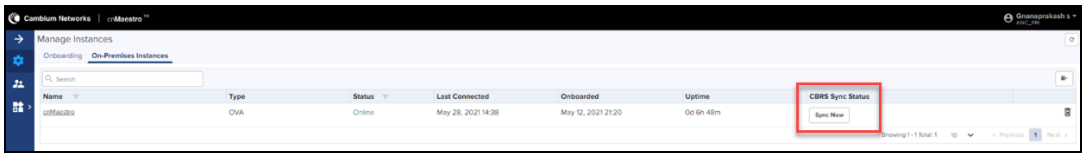
Enabling CBRS in On-Premises

Perform the following to enable CBRS:

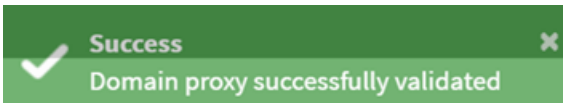
1. On successful activation of the CBRS service in the Cloud Anchor account, cnMaestro generates a Token.
2. Onboard the On-Premises to Anchor account.
3. User can Sync the CBRS token from On-premises or Anchor account
   a. In On-Premises CBRS accounts page click **Sync From Cloud** to synchronize the CBRS token.



b. Navigate to the **Anchor account > Manage Instances > On-Premises Instances** and click **Sync Now** on CBRS sync status.



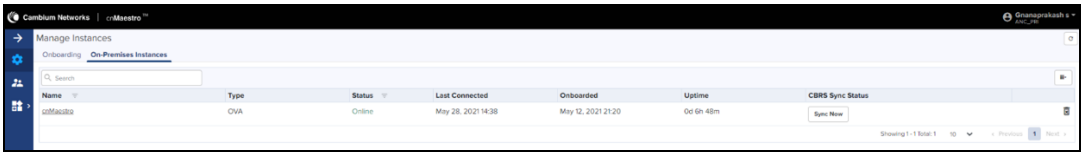
4. Select HTTP Proxy mode for SAS communication (refer to CBRS HTTP Proxy Configuration Options).
5. Click **Save token**. CBRS service will be enabled.
6. Click **Domain Proxy Test** to test Domain Proxy connectivity. If the test is successful, it will display the following message:

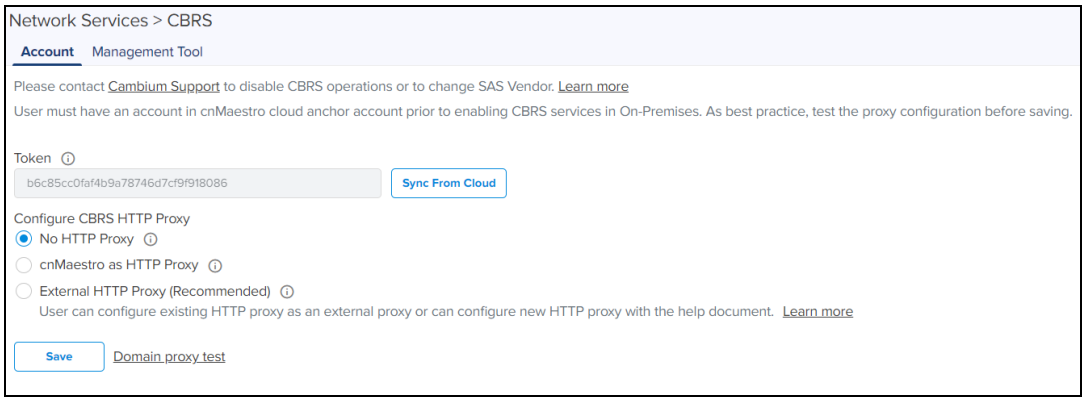


Share CBRS Configuration to the On-Premises Instance

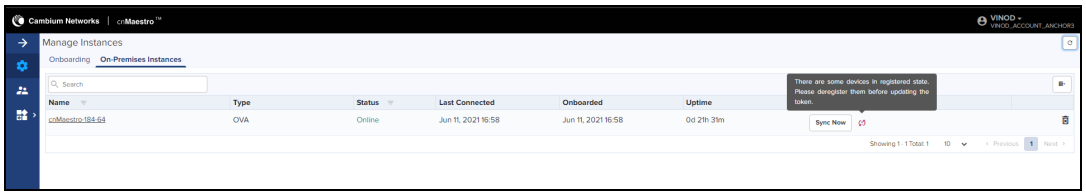
	NOTE: From version 3.0.3 cnMaestro supports Synchronize CBRS Configuration to On-Premises instance.

Once On-Premises is connected to the Anchor Account, the user can synchronize CBRS details (SAS ID, Token) to the cnMaestro On-Premises instance to register CBRS devices.





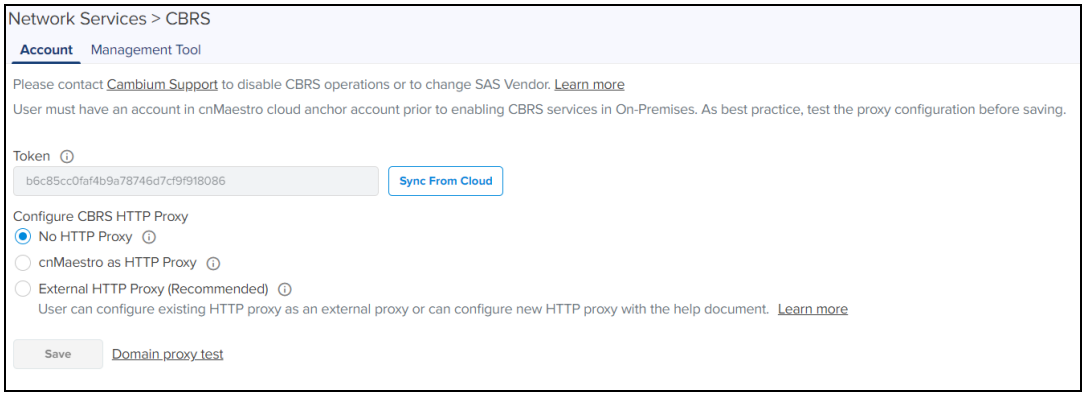
If the user shares (sync) CBRS details configured on Anchor account to connected On-Premises and if any devices are registered in On-Premises with different CBRS token or SAS ID it displays the deregister error as shown below.



CBRS HTTP Proxy Configuration Options

Cambium recommends using External HTTP Proxy for a highly available deployment, because cnMaestro software updates may take a few minutes to complete, during which time communication with SAS through the Domain Proxy will be affected.

No HTTP Proxy

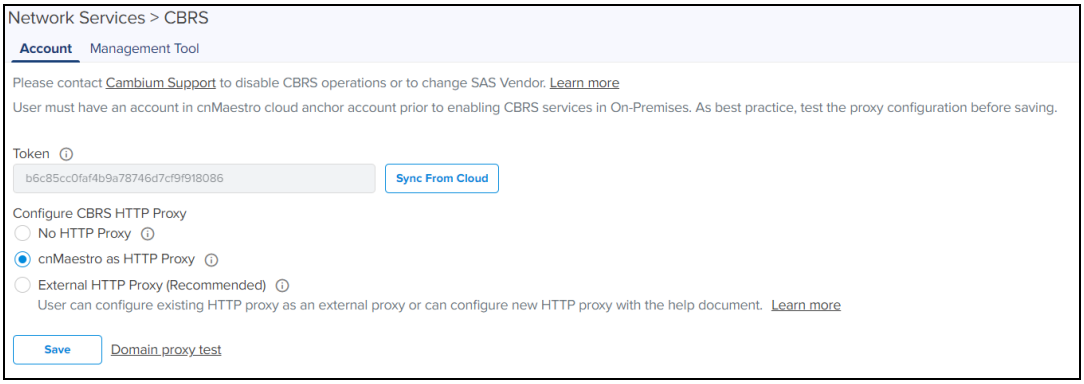


- In On-Premises **No HTTP Proxy** is selected by default.
- CBRS-compliant devices communicate with the Domain Proxy directly through the Cambium Domain Proxy.

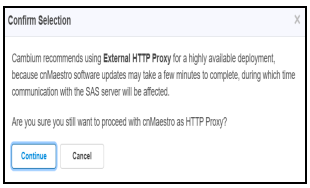
NOTE:

The On-Premises server and CBRS devices must have Internet access to communicate directly to the Cambium Domain Proxy.

cnMaestro as HTTP Proxy



- Select **cnMaestro as HTTP Proxy** and a window pops-up. Click **Yes.**



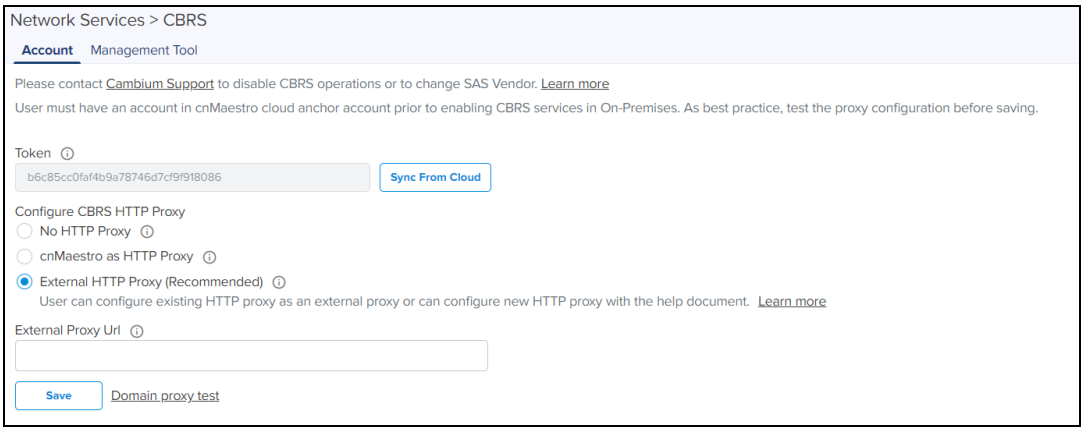
Warning:

Cambium recommends using External HTTP Proxy for a highly available deployment, because cnMaestro software updates may take a few minutes to complete, during which time communication with SAS through the Domain Proxy will be affected.

- CBRS-compliant devices communicate with the Cambium Domain Proxy through the local cnMaestro On-Premises HTTP Proxy.

NOTE:
cnMaestro On-Premises must have Internet access.

External HTTP Proxy



CBRS-compliant devices can communicate with the Cambium Domain Proxy through an External HTTP Proxy such as HA Proxy. Cambium recommends configuring High Availability on the HTTP Proxy.

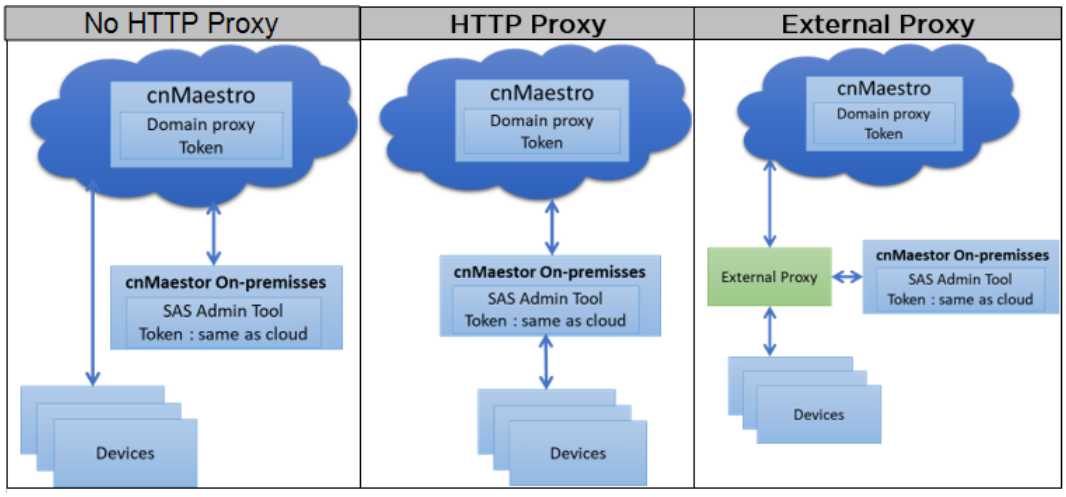
NOTE

The External HTTP Proxy method is preferred, because upgrades to cnMaestro could result in proxy downtime and lost CBRS connectivity.

- Configure the external HTTP Proxy to access the SAS Server through the Domain Proxy.
- Set the External HTTP Proxy as http://proxy-ip:port number.

  Example: http://11.110.0.101:9090

For more details, refer Using a Domain Proxy for CBRS connectivity.



Management Tool

The Management Tool allows one to register CBRS devices to the SAS provider before physically connecting CBRS-complaint devices to the network. The following Cambium CBRS-compliant devices operate in 3.6 GHz band frequency, ranging from 3550 to 3700 MHz:

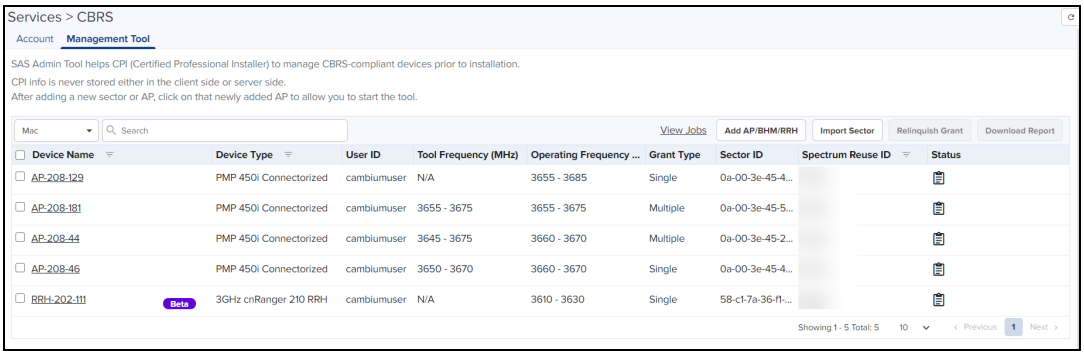
NOTE

The CBRS Multi-Grant feature is first supported in cnMaestro 3.0.2 and PMP 20.2.

- PMP 450b 3 GHz
- PMP 450m AP 3 GHz
- PMP 450i AP and SM 3 GHz
- PMP 450 AP and SM 3.6 GHz
- PTP 450i BHM and BSHS 3 GHz
- PTP 450 BHM and BHS 3.6 GHz
- LTE 3 GHz cnRanger 201 SM
- LTE 3 GHz cnRanger 210 RRH

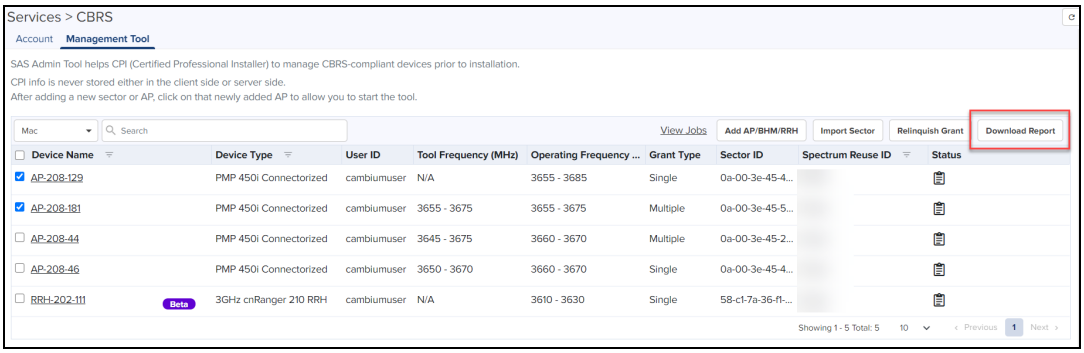
The CBRS procedure can be started and managed by an authorized CPI (Certified Professional Installer). CPIs are required to enter necessary credentials to run and modify the CBRS parameters.

A CBRS sector view is shown below:



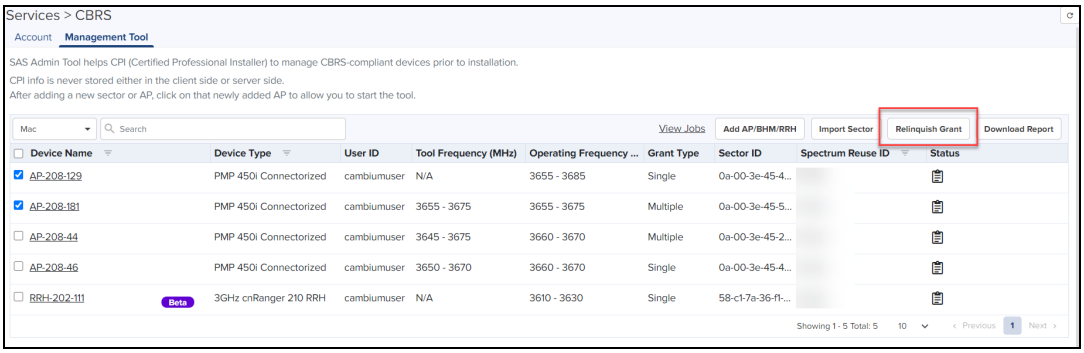
Download Report

The Download Report allows the user to download multiple device reports in a **.CSV** format.



Relinquish Grant

The Relinquish Grant relinquishes all grants of selected sector and places devices in the Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on device.



NOTE

- Relinquish Grant can be performed only for the Config_Synced devices which are running in Single Grant.
- PMP devices should be upgraded to release 20.2, that supports the Multi-Grant feature.

Creating a Management Tool Sector

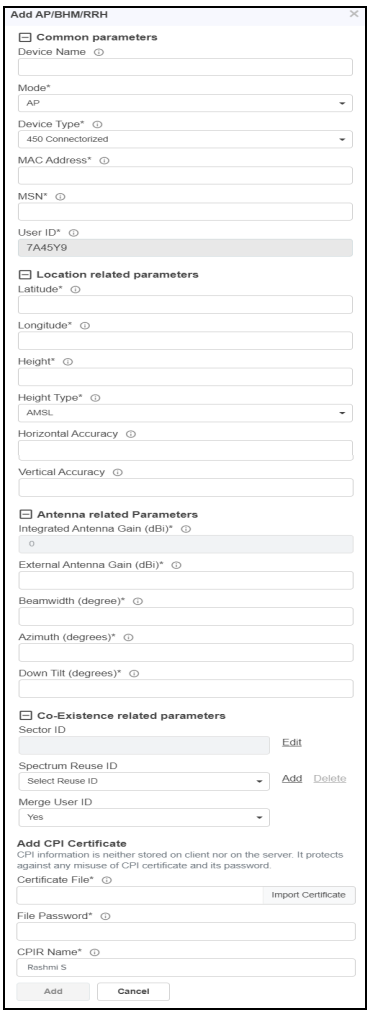
A sector can be created in two ways:

- Add AP/BHM/RRH : Adding all parameters manually of an AP/BHM/RRH.
- Import Sector: Upload a file with all sector device details.

Add AP/BHM

1. Navigate to **Services > CBRS > Management Tools** and click **Add AP/BHM/RRH**.
2. Enter all parameters under the following categories when the user selects the **Mode** as **AP/BHM**:

- **Common Parameters**: Device Name, Mode, Device Type, MAC Address, and MSN.
- **Location Related Parameters:** Latitude, Longitude, Height and Height Type, Horizontal Accuracy and Vertical Accuracy.
- **Antenna Related Parameters**: External Antenna Gain, Beamwidth, Azimuth and Down Tilt.
- **Co-Existence Related Parameters:** Sector ID, Spectrum Reuse ID, and Merge User ID.
- **Add CPI Certificate**: Certificate File, File Password, CPIR Name.



- Click **Add** to add a sector.

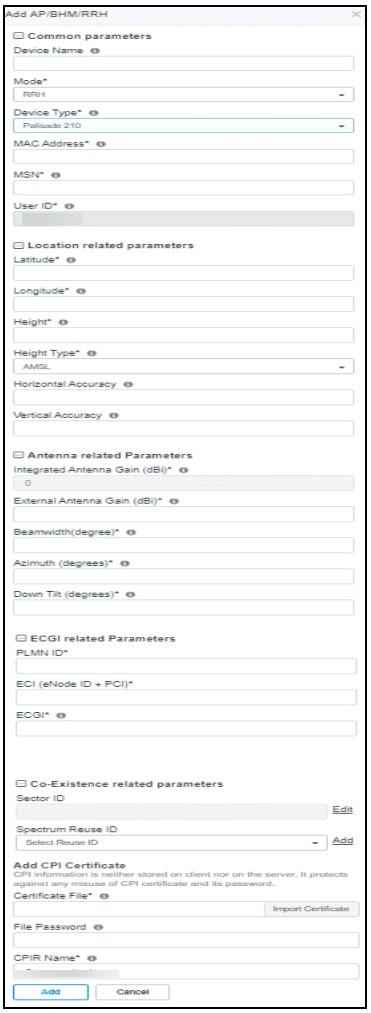
> **NOTE:**
>
> Merge User ID is applicable only for PMP devices, when SAS is Federated Wireless or CommScope.

Add RRH

1. Navigate to **Services > CBRS > Management Tools** and click **Add AP/BHM/RRH**.
2. Enter all parameters under the following categories when the user selects the **Mode** as **RRH**:

- **Common Parameters**: Device Name, Mode, Device Type, MAC Address, and MSN.

- **Location Related Parameters:** Latitude, Longitude, Height and Height Type, Horizontal Accuracy and Vertical Accuracy.
- **Antenna Related Parameters**: External Antenna Gain, Beam-width, Azimuth and Down Tilt.
- **ECGI Related Parameters** : PLMN ID, ECI (eNode ID + PCI) and ECGI.
- **Co-Existence Related Parameters:** Sector ID and Spectrum Reuse ID.
- **Add CPI Certificate**: Certificate File, File Password, CPIR Name.



> **NOTE:**
> Refer to CBRS Device Parameters for additional details.

Import Management Tool Sector

To import a sector, perform the following steps:

1. Navigate to **Services > CBRS > Management Tool** and click **Import Sector**.



2. Click **Download Template** if user does not have Import Sector template. Users can download two different template formats:
   - PMP: Excel or ODS
   - LTE: Excel or ODS
3. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or OpenDocument Spreadsheet (ods) formats.
4. Enter CPI credentials:
   a. Upload CPI Certificate File by clicking **Import Certificate**.
   b. Enter **CPI File Password**.
   c. Enter **CPI Registered Name**.
5. Enter the **Sector ID**.
6. Select **Spectrum Reuse ID** from the drop-down.
7. Select **Merge User ID**.

- Selecting **Yes** to **Merge User ID** prefixes the User ID to the Sector ID and Spectrum Reuse ID in the registration message of the SAS.

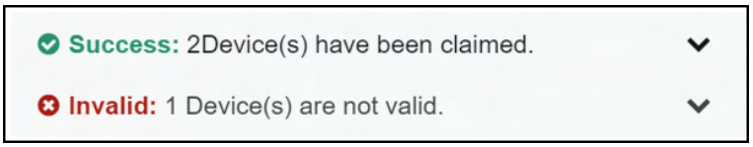


NOTE

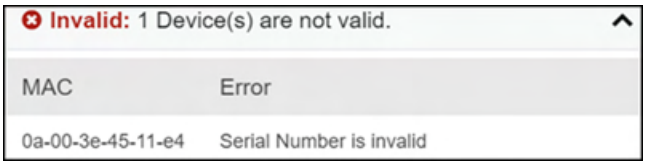
- **Merge User ID** is applicable only for PMP devices, when SAS is selected as **Federated Wireless** or **CommScope**.
- See the CBRS Consolidated Procedures Guide and the Cambium PMP Release 20.3 training slides for more details on when to select **Yes** or **No.**

8. Click **Import**.

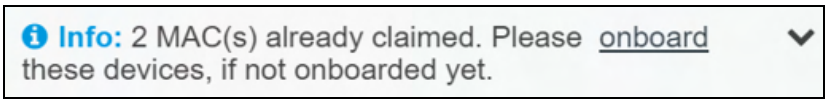
Import status is displayed as **Success, Info,** and **Invalid.**



9. Details of Success, Info and Invalid can be seen by clicking arrow ( ).



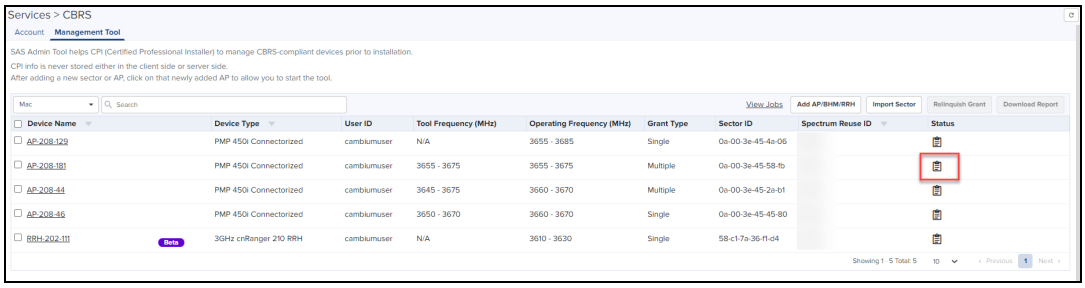
10. If the device is already claimed, it can be onboarded by clicking the **onboard** link.



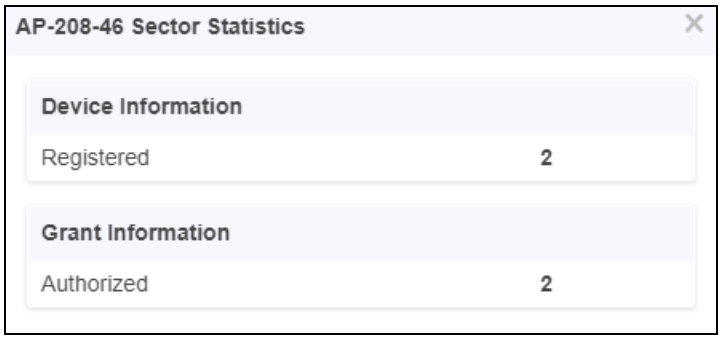
Management Tool Sector Statistics

To view Sector Statistics, perform the following steps:

1. Navigate to **Services > CBRS > Management Tool.**
2. Click **View Sector Statistics** under **Status**.



3. **Sector Statistics** window pops up.



NOTE:

Refer to the Live Status Update for additional details.

Search Management Tool Sector

To search for a sector:

1. Navigate to **Services > CBRS > Management Tool.**
2. Select search option **CBSD** or **MAC:**

- For **CBSD**: Search by CBSD ID.
- For **MAC**: Search by MAC Address

3. Enter text in search box to display filtered records.



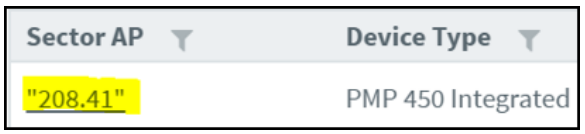
NOTE:

- If an AP device is entered in the search option, it displays the both AP devices and the related SM device.
- If an SM devices is entered in the search option, it displays only the SM devices.

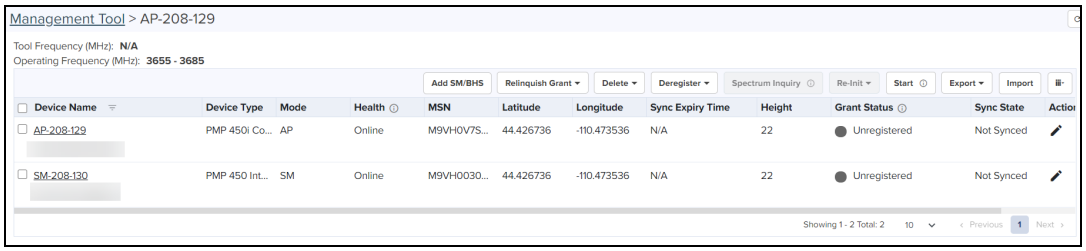
4. Filtered AP or sectors can be cleared by clicking or **Clear** button.

Sector View

1. Click a sector from the Sector AP column to get the list of devices.

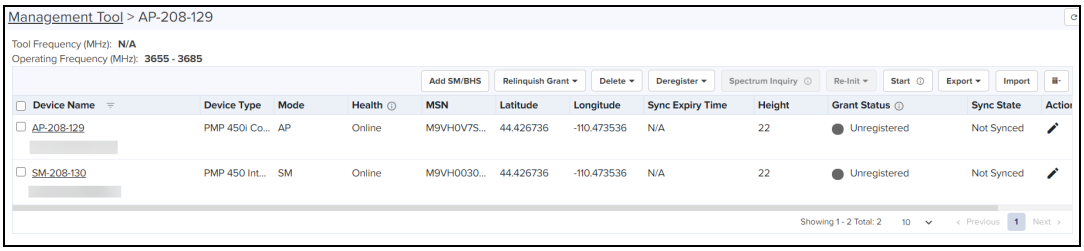


2. All devices of sector is displayed.



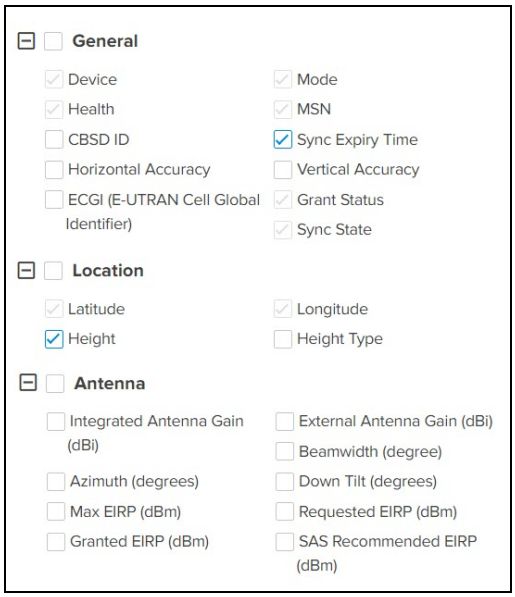
Sector Details View

- The Sector Details view displays the following fields by default:
  - Device Name, Device Type, Mode, Health, MSN, Latitude, Longitude, Sync Expiry Time, Height, Grant Status, Sync State, and Actions.

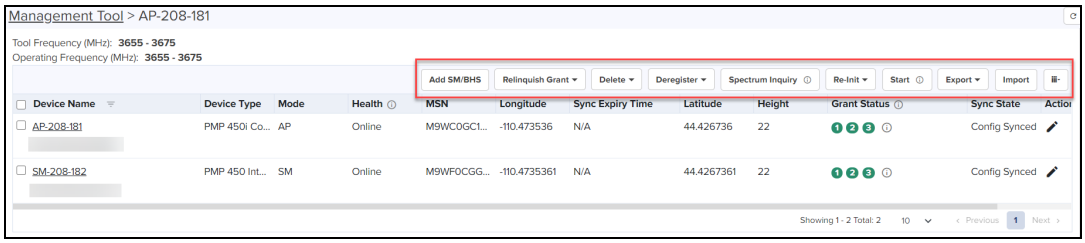


- SM can be added in the sector by manually entering all parameters using the **Add SM** button or uploading a file containing SM details using the **Import SMs** button.

- Action column can edit or delete any device in the sector. Edit and Delete buttons will available depending of device state. Refer to Edit Device and Delete Device for more details.
- Click on top bar to include additional fields in Sector Details view.



- Use the following buttons to control CBRS procedure:



  - **Start** and **Stop** manage the CBRS procedure of a sector.
  - **Reinitialize**: restarts the CBRS procedure and reinitializes the devices.
  - **Deregister:** deregisters the device (single or multiple).
  - **Spectrum Inquiry**: checks the availability of frequencies.
  - **Delete**: deletes device (single or multiple).
  - **Unblock**: clears the de-registered state on an LTE, allowing a registration or reregistration request.
  - **Export**: exports the sector data in .xlsx format.
  - **Import:** imports the SM in the sector.
  - **Relinquish Grant:** relinquishes grants which generated in Wide-Grant mode.

- Once the sector is authorized (enters the AUTHORIZED state), button transfers grant details from Management Tool to real devices.

Add SM or BHS

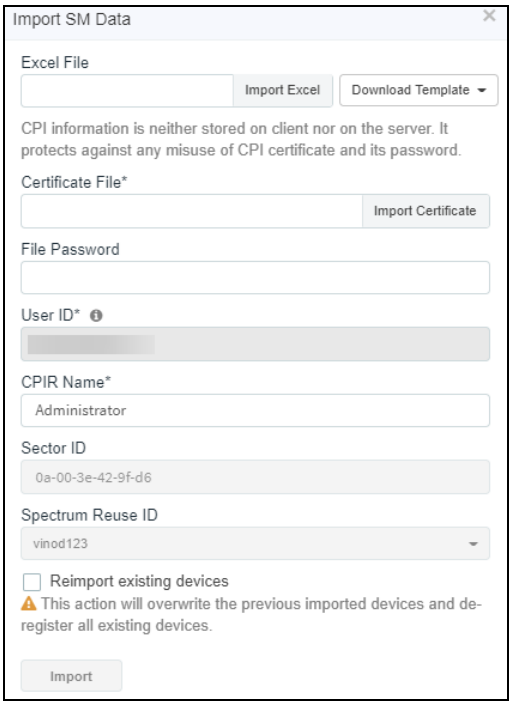
1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Add SM/BHS** button to add SM in a sector.



3. Enter all parameters under following categories:
   a. **Common:** Device Name, Device Type, MAC Address, and MSN.
   b. **Location:** Latitude, Longitude, Height and Height Type, Horizontal Accuracy and Vertical Accuracy.
   c. **Antenna Parameters:** Integrated Antenna Gain, External Antenna Gain, Beam width, Azimuth and Down Tilt.
   d. **Add Certificate:** Certificate File, File Password and CPIR Name.
4. Click **Add** to add an SM.

Import SMs

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Import SMs** button to import SMs in a sector.
3. Enable the **ReImport Devices** to overwrite the previous imported data and deregister all existing devices.

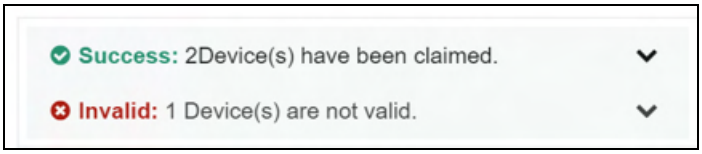


4. Click **Download Template** if user does not have Import Sector template. Users can download two different template formats:
   - PMP: Excel or ODS
   - LTE: Excel or ODS
5. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or OpenDocument Spreadsheet (ods) formats.
6. Enter CPI Credentials:

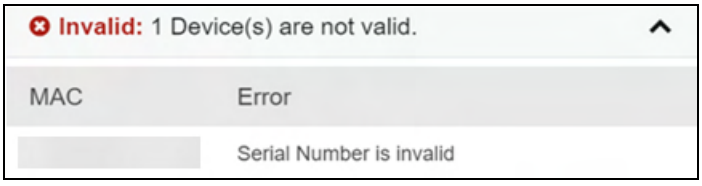
- Upload CPI Certificate File by clicking **Import Certificate** button.
- Enter CPI File Password.
- Enter CPI Registered Name.

7. Click **Import**.

Import status is displayed under **Success**, **Info** and **Invalid** sections.



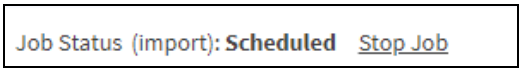
8. Details of Success, Info and Invalid can be seen by clicking .



9. If the device is already claimed, it can be onboarded by clicking **onboard** link.

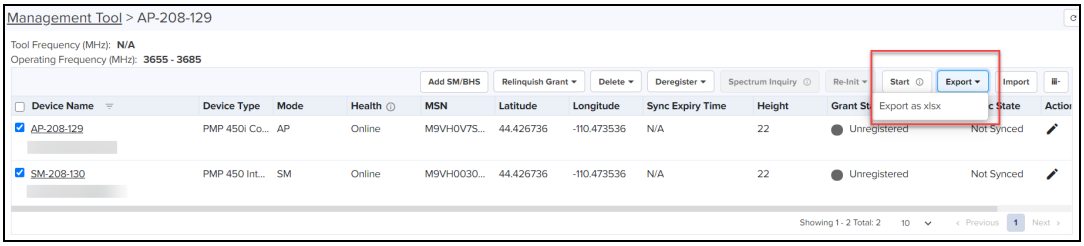


10. Once the user clicks **Import**, a job will be scheduled.

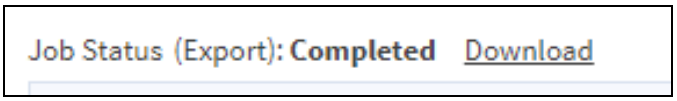


Export Sector

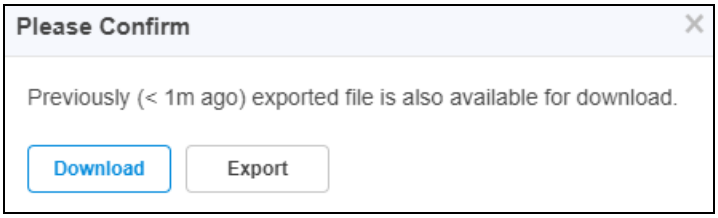
1. Navigate to **Services > CBRS > Management Tool** and then select a **sector**.
2. Click **Export** button to export the sector(export as xlsx).



3. Once the user clicks as **xlsx**, a job will be scheduled.

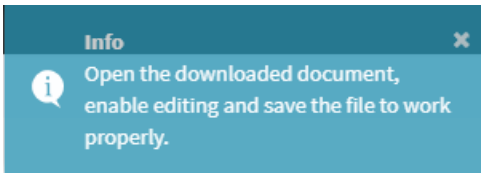


4. Once the Job status is Completed, click **Download** to download the Sector xlxs.



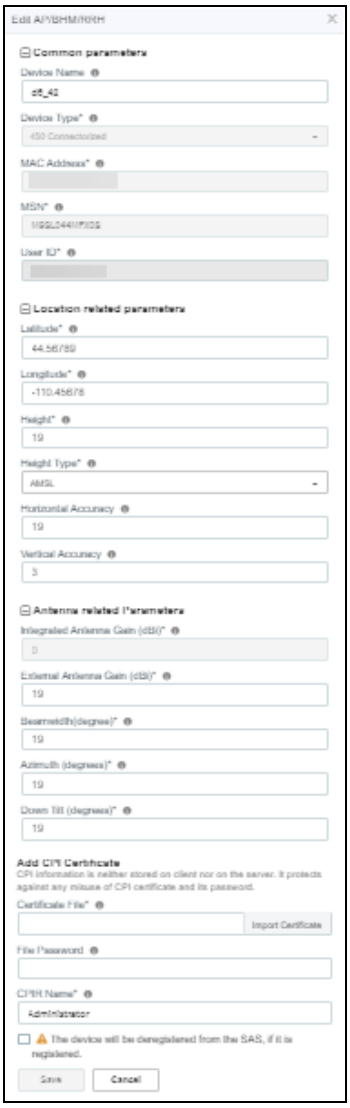
> **NOTE:**
>
> **Download** button is enabled only for two hours after the export job completes.

5. User can use the downloaded .xlxs file for importing into the sector. To import, save the file as shown in the below figure.



Edit Device

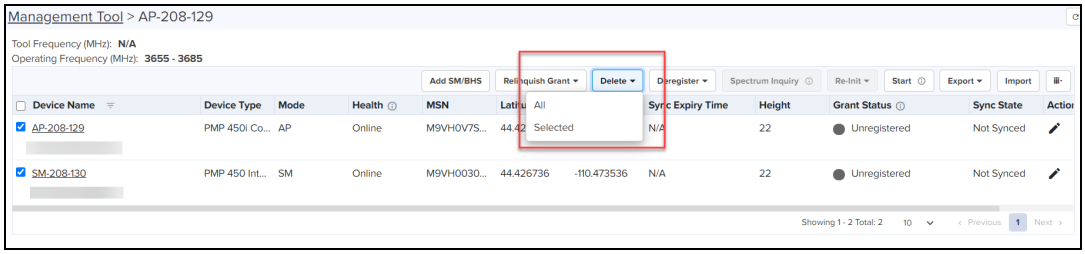
1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** button if the CBRS procedure is running.
3. Click **Edit** button to edit device parameters.
4. Enter CPI credentials:
   - Upload CPI Certificate File by clicking I**mport Certificate** button.
   - Enter CPI File Password.
   - Enter CPI Registered Name.



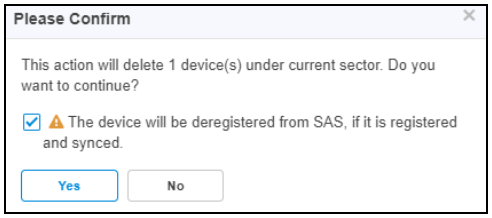
5. Click **Save.**

Delete Device

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** button if the CBRS procedure is running (the CBRS procedure is considered running if the START procedure described below has been invoked, and if all devices in AUTHORIZED state).
3. Deleting SM:
   - Select SM to deregister if it is not in UNREGISTERED state (refer to CBRS State Diagram).
4. Once the SM is selected, click **Delete** to display **All** or **Selected.** Click **Selected.**
   - **All** : delete the complete registered SM devices.
   - **Selected** : delete the selected device.



5. Click **Yes** to confirm.



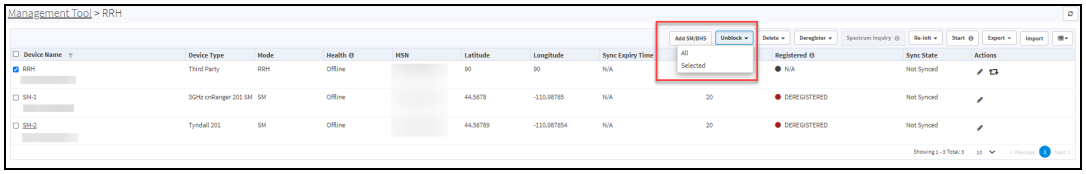
6. Once the user clicks **Yes**, a job will be scheduled.



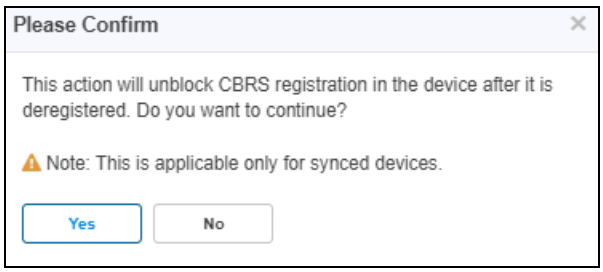
7. Deleting an AP:
   - All SMs of the sector must be deregistered before deleting an AP. Refer to Deregistration procedure to deregister all SM devices.
   - Select AP of the sector to delete. Start CBRS procedure.
   - Click **Delete**.

Unblock Device

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. If LTE device is **Config Synced** ,and if device deregister flag is enabled, unblock removes the deregistartion flag on the device.
3. Once the device is selected, click **Unblock** and choose **All** or **Selected** from the drop-down.
   - **All** : unblock the complete registered devices.
   - **Selected** : unblocks the selected single device.



4. Click **Selected** display the **Please Confirm** window.



5. Click **Yes** to confirm the action.

Start CBRS Procedure

The Start button starts the CBRS procedure for a Wider-Grant sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Start** to start CBRS procedure of a sector.
3. Once the user clicks start, the **Spectrum Inquiry** window pops up.

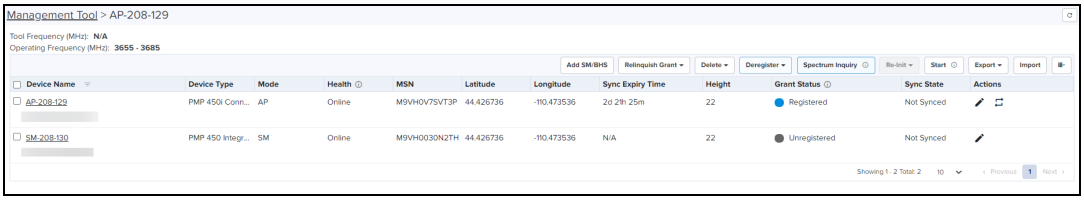


NOTE:

- Multi-Grant is enabled by default.
- Sorted By Ranking is applicable for users selecting Google or Federated Wireless SAS.

4. User can disable the Multi-Grant feature by disabling the checkbox **This feature will enable multi grant on the tool.** For more details refer to Multiple Grant.
5. Click **Edit** to edit **Co-Existence Configuration** and **EIRP Computation.**
   - **Spectrum Reuse ID Statistics** displays the devices running on different sector, channels, and bandwidth based on the **Spectrum Reuse ID**.
6. Once the Spectrum Inquiry is verified, click **Save**.

Once the Sector is created it displays as shown below:



NOTE:

- If the device is already synced with the Management Tool, the CBRS Start and Stop procedures are not applicable for all the synced devices.
- If user does not see the **Start** button, it means the CBRS procedure is already running.
- If all devices of the sector are in AUTHORIZED or HALT status and the user tries to start the CBRS procedure, the **Start** button will go to Stop state (as CBRS procedure is completed for all devices).

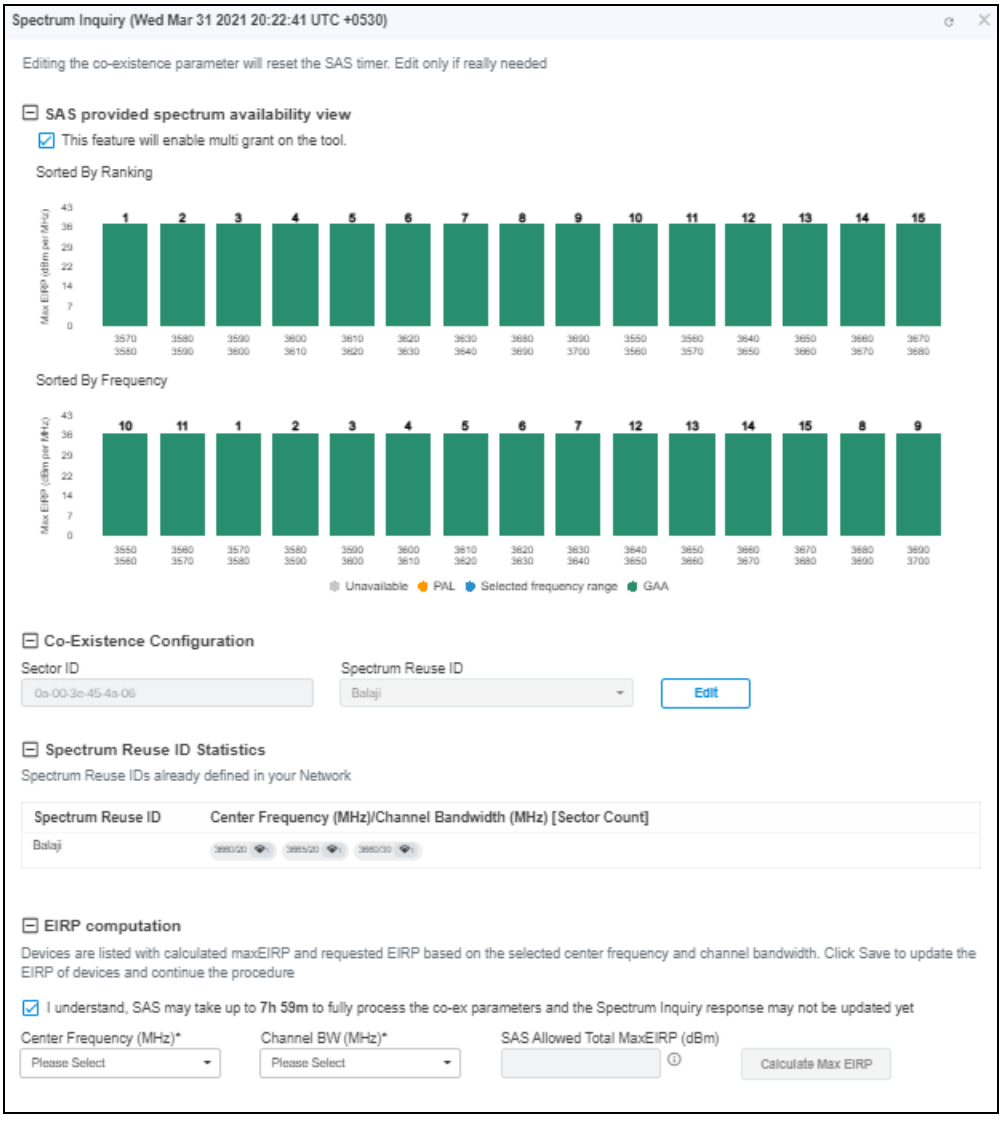
Multi-Grant

Multi-Grant feature divides selected channel bandwidth in multiple of 10 MHz channel. If the selected channel bandwidth is 5 MHz or low/high frequency contains 5 MHz raster, the slice would be in 5 MHz channel. Each slice will initiate a separate Grant procedure and status will be updated accordingly..

To enable Multiple Grant for new sector:

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Start** to start CBRS procedure of a sector.
3. Once the user clicks **Start**.

The Spectrum Inquiry window pops up as shown below:



NOTE:

- Multi-Grant is enabled by default.
- Merge User ID is applicable only for PMP devices, if user selects SAS is either Federated Wireless or CommScope.

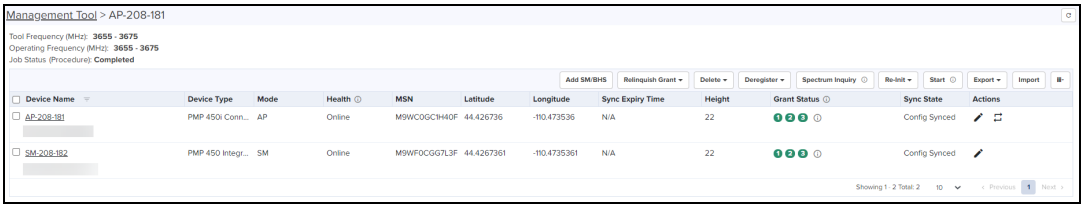
4. Click **Edit** to edit **Co-Existence Configuration** and **EIRP Computation.**
   - **Spectrum Reuse ID Statistics** displays the devices running on different sector, channels, and bandwidth based on the **Spectrum Reuse ID**.
5. Accept the checkbox process of the Co-Existence parameters.

NOTE:

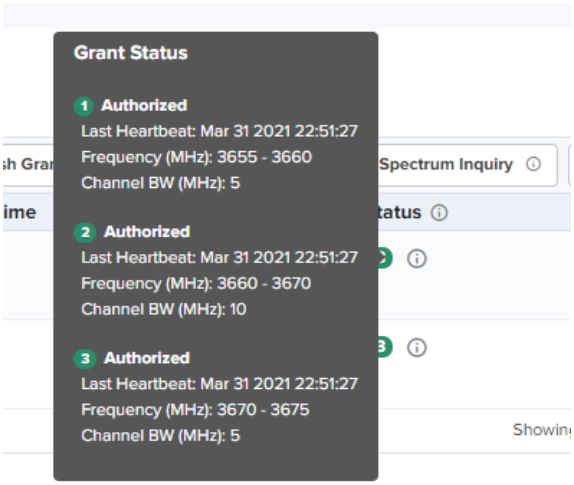
The Federated Wireless or Google SAS might need hours to fully process the Co-Existence parameters in the Registration, (before they are properly reflected in the Spectrum Inquiry Response). For more details see the CBRS Standalone Procedures Guide.

6. Once the Spectrum Inquiry is verified, click **Save**.

Once the Sector is created with Multiple Grants will be displayed as shown below:



To view the Grant Status click the info icon



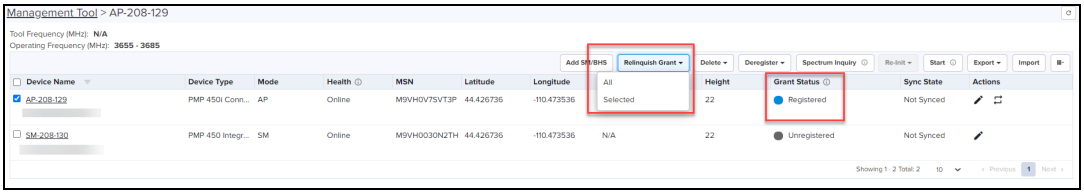
Relinquish Grant

The Relinquish Grant relinquishes all grants of selected sector. This will make devices to go to Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on device.

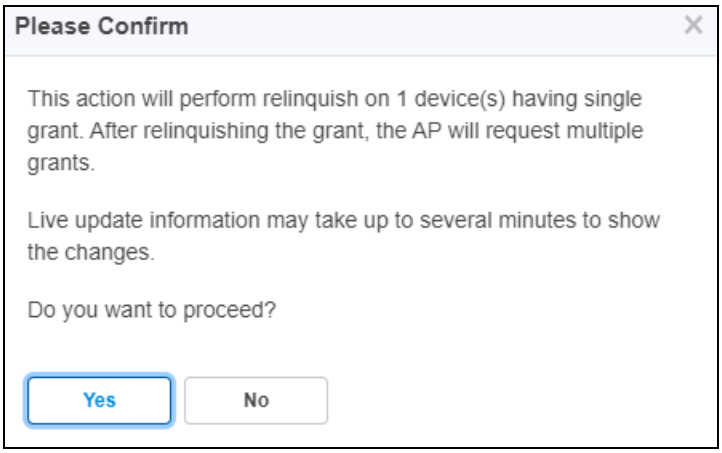
To Relinquish Grant Perform as follows:

1. Navigate to **Services > CBRS > Management Tool** and select a sector with Single Grant.
2. Once the SM is selected, click **Relinquish Grant** to display **All** or **Selected.** Click **Selected.**
   - **All** : Relinquish all the registered SM devices.

- **Selected** : Relinquish the selected device.



3. Click **Yes** to confirm the action.

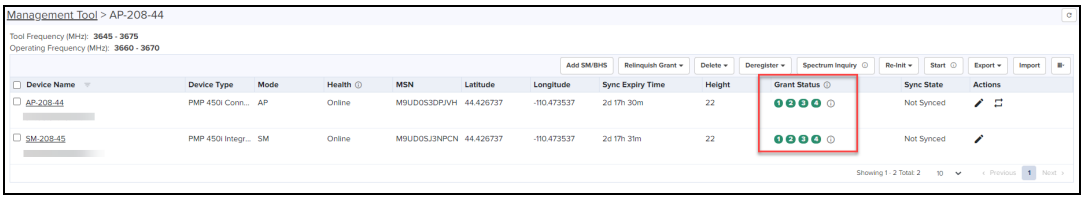




NOTE:

Live update information may take upto several minutes to display the changes of reflected relinquish status.

Once the user clicks **Yes**, **Wider Grant** gets converted to the **Multiple Grants** as shown below:



Stop CBRS Procedure

The **Stop** button allows the user to stop the CBRS procedure for a sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** button to stop CBRS procedure of a sector.



NOTE:

- If the device is already synced with the Management Tool, the CBRS Start and Stop procedures are not applicable to the synced devices.
- If user does not see the **Stop** button, it means the CBRS procedure is already in stopped state, **Start** and **Stop** are toggles.
- If all devices of the sector are in AUTHORIZED state, the CBRS procedure will automatically stop.

Reinitialize CBRS Procedure

The **Re-init** button allows the user to start the CBRS procedure for a sector and reinitialize selected devices (Reinitialize = Start of sector + Reinitialization of user selected devices). At least one device must be selected in order to enable **Re-init** button. Clicking **Re-init** reinitializes selected devices are reinitialized to UNREGISTERED (irrespective of previous CBRS state).

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** if the CBRS procedure is already running.
3. Select one or more devices to be reinitialized.

> **NOTE:**
>
> You might notice some delay in enabling **Re-init** button after pressing **Stop** button. It is due to a delay in properly stopping the CBRS procedure.

4. Click **Re-init** to start the reinitialization procedure.
5. Confirmation window pops up:
   - Click **Continue** or
   - Select **Spectrum Inquiry** to edit the **EIRP values** as shown in Start procedure.

> **NOTE:**
>
> - Synced devices cannot be reinitialized.
> - Reinitialize modifies or corrects the parameters. For example, if a device is in HALT state due to a parameter error, the user can stop the CBRS procedure and reinitialize the device after modifying device parameters.

Deregistration

The deregistration procedure allows the user to deregister devices from the Domain Proxy.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** if the CBRS procedure is already running.
3. Select one or more devices which need to be deregistered.
4. Click **Deregister** to deregister selected devices.
5. Once the user clicks **Deregister**, once a job will be scheduled.

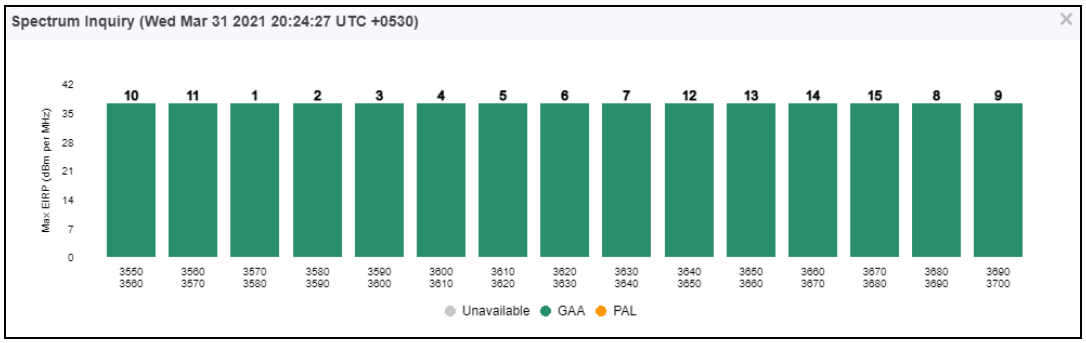


6. If deregistration fails, the reasons will be indicated under  .

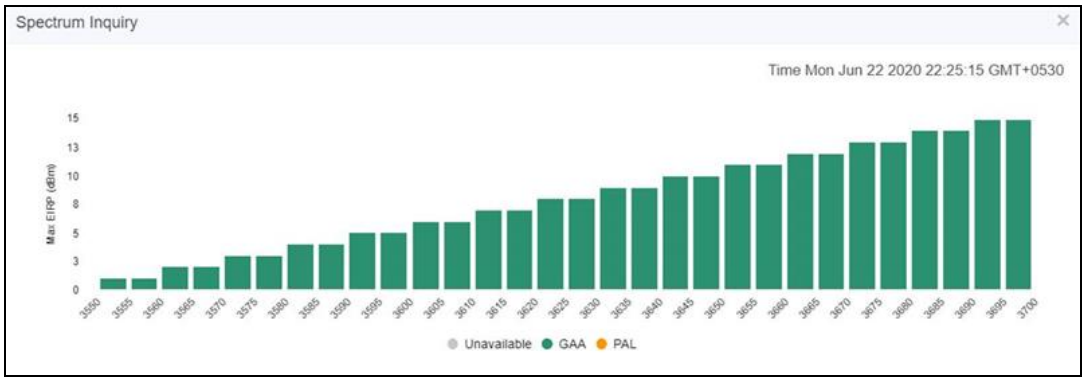
Spectrum Inquiry

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Spectrum Inquiry** button.
3. **Spectrum Inquiry** status button is enabled once the device is registered (REGISTERED state) to the SAS.

- If the selected SAS is not Google, EIRP is unsupported, and Spectrum Inquiry is displayed as shown below:



- If the users is selected SAS is **Google,** it supports **EIRP.** Spectrum Inquiry displays as below:



- **GAA**: General Authorized Access
- **PAL**: Priority Access License

Spectrum availability can be checked by hovering over frequencies.

Device Sync

The Sync procedure allows user to transfer grant information from Management Tool to respective device.

For a PMP sector, the Sync action can only be performed on an AP or BHM. The SM and BHS gets synced automatically when it comes online.

For an LTE sector, which supports a Cambium SM with a 3rd party BBU and RRH, the sync action will sync the Cambium SMs in this sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Sync** button to perform sync procedure.
3. Click **Yes** on the pop-up or click **NO** to cancel the sync procedure.

Once **Yes** is clicked, the Management Tool will check the accessibility of AP/BHM before proceeding with sync.

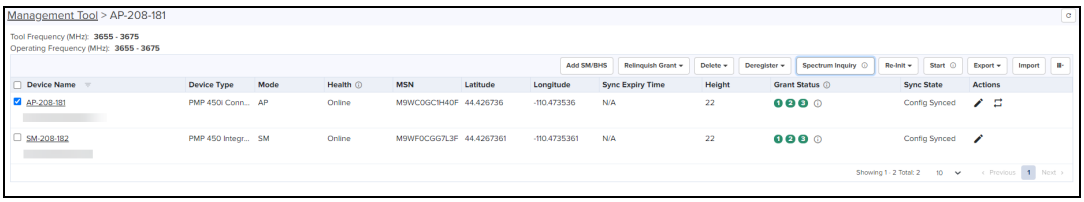


NOTE:

- PMP SM cannot be manually synced. It is only synced automatically.
- Once the device is synced, for both PMP and LTE devices, primary management is transferred from the tool to the device itself. However, some actions and procedures are still supported on the tool. See the CBRS Consolidated Procedures Guide for more details.
- Sync procedure copies complete CBRS parameters to device and enables CBRS to transmit with configured parameters.

Live Status Update

Once the device is Config synced, displays the CBRS details like CBSD ID, Grant ID, CBSD Grant State and Last Heartbeat Time from the devices every 5 minutes.



It displays the possible single Grant state such as:

- Authorized
- Deregistering
- Grant
- Grant Suspended
- Grant Terminate
- Registered
- Registering
- Relinquished Spectrum
- Relinquishing Spectrum
- Unregistered
- Unknown

Management Tool Sync

The Sync procedure allows the user to transfer grant information from the Management Tool to a real device. The Sync action can only be performed on an AP or BHM. The SM and BHS are synced automatically when they come online. Once the AP/BHM/SM/BHS are synced, no further action is taken from Management Tool.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Sync** to perform the synchronization procedure.
3. Click **Yes** to enable CBRS on AP/BHM after successful sync or click **No** to cancel synchronization procedure.

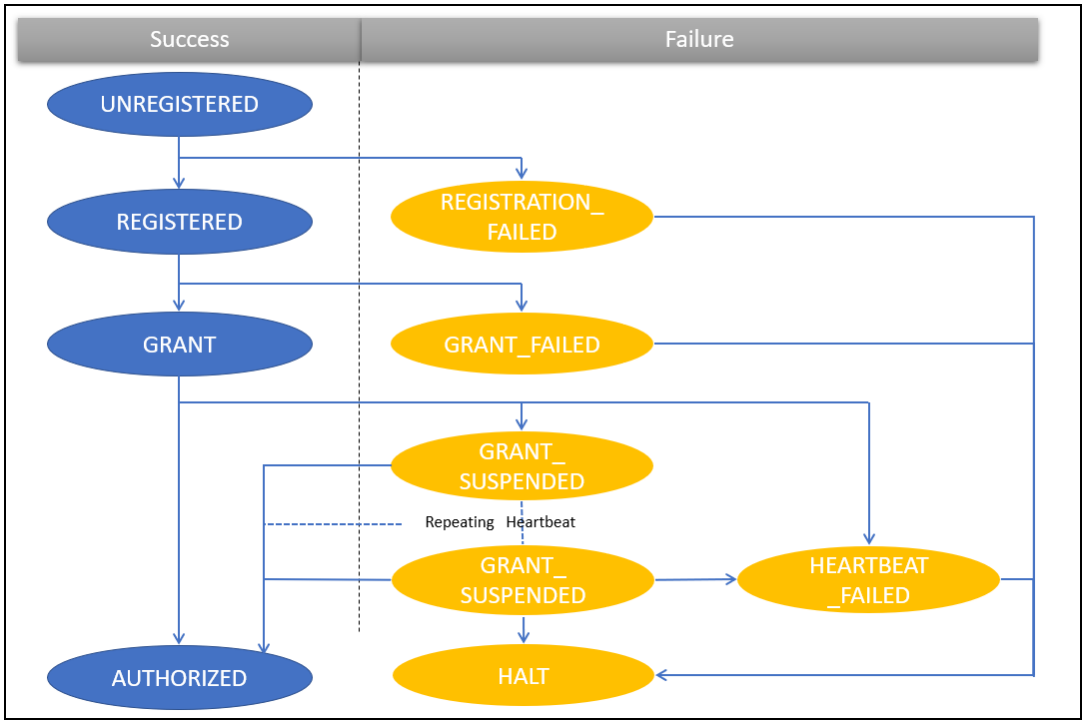
Once **Yes** is clicked, the Management Tool checks the accessibility of AP/BHM and proceeds with sync.



NOTE:

- AP or BHM requires manual Sync whereas SM or BHS does not require manual Sync. The latter two are synced automatically.
- Once the device is synced, it cannot be administered by the Management Tool.
- The Sync procedure copies CBRS parameters to the device and enables CBRS to transmit with configured parameters.

CBRS State Diagram



NOTE:

GRANT_SUSPENDED is a temporary suspend state where HEARTBEAT messages are sent for an extended period prior to getting AUTHORIZED.

The CBRS procedure has the following states:

CBRS Device Parameters

Category	Parameter	Details
Common	Channel BandWidth (MHz)	Channel Bandwidth of AP or BHM in MHz.
	Center Frequency (MHz)	Center frequency of AP or BHM in MHz.
	Device Name	Name given to device on SAS Admin (max 120 characters. This is to identify device on SAS Admin: it does not get copied to the device via sync.
	Device Type	Drop-down selection of supported devices.
	MAC Address	MAC address of the device.
	MSN	Serial number of device.
	User ID	Unique identifier is assigned by the SAS. The User ID is part of the registration request message. The wrong User ID leads to REGISTRATION_

Category	Parameter	Details
		FAILED.
Location	Height	Device antenna height in meters.
	Height Type	Should be AGL or AMSL as follows: • AGL height is measured relative to the ground level. • AMSL height is measured relative to the mean sea level.
	Horizontal Accuracy	A positive number in meters to indicate the accuracy of the device antenna horizontal location.
	Latitude	Latitude of the device antenna location in degrees.
	Longitude	Longitude of the CBSD antenna location in degrees.
	Vertical Accuracy	A positive number in meters to indicate the accuracy of the device antenna vertical location.
Co-Existence Related Parameters	Sector ID	The default AP MAC address and allows editing the default MAC address.
	Spectrum Reuse ID	The Spectrum Reuse ID defined in the network.
	Merge User ID	Prefixes the User ID to the Sector ID and Spectrum reuse ID.
ECGI Related Parameters	PLMN ID	Public and Mobile Network Identifier.
	ECI	E-UTRAN Cell Identifier. It is a length of 28 bits and contains the eNodeB-ID.
	ECGI	Enter the both PLMN ID and ECI parameters and it calculates displays in the ECGI field.
Antenna Parameters	Azimuth (degrees)	Boresight direction of the horizontal plane of the antenna in degrees with respect to True North.
	Beamwidth (degree)	3-dB antenna beam width of the antenna in the horizontal-plane in degrees.
	Downtilt (degrees)	Antenna downtilt in degrees.
	External Antenna Gain (dBi)	Peak gain of external antenna connected to device in dBi.
	Integrated Antenna Gain (dBi)	Peak gain of integrated antenna in dBi.
	Certificate File	CPI's (Certified Professional Installer) certificate.

Category	Parameter	Details
Add Certificate		
	CPIR Name	CPI's registered name.
	File Password	CPI's private password.

Using a HTTP Proxy Server for CBRS Connectivity

Proxy Suggestions for CBRS Connectivity

We do not recommend against using cnMaestro On-Premises, as a HTTP Proxy for CBRS connectivity. Normally, upgrades to cnMaestro that result in a small amount of downtime do not impact network devices under management. In the case of CBRS even a brief outage of the proxy during upgrade will result in a network outage.

External Proxy Requirements

If you already use a forward proxy in your network, continue to use it rather than set up a new one. Connections will be made using HTTP CONNECT to sas.cbrs.cambiumnetworks.com and your proxy needs to allow this. A TLS intercepting proxy (such as a security gateway) will break connectivity.

Squid as External Proxy

The following configuration will work for an external proxy configuration, but it does not offer high-availability, and it may not be in line with your network standards. We have tested this configuration using on fresh installs of:

- Ubuntu 20.04 / Squid Cache: Version 4.10
- Centos 7 / Squid Cache: Version 3.5.20

```
## WARNING:
## While this config may work for your use case,
we encourage you to follow your own best practices and modify this file for your network.
## Tested on squid version 4.10
## This localnet ACL is not useful unless you want to use this proxy for anything other than
a cbrs proxy.
#acl localnet src 10.0.0.0/8   # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
#acl localnet src fc00::/7       # RFC 4193 local private network range
#acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
## This cbrs ACL limits connections to sas.cbrs.cambiumnetworks.com only.
acl cbrs dstdomain sas.cbrs.cambiumnetworks.com
## Updates require access to destinations under cloud.cambiumnetworks.com
## This is a separate ACL for readability, but can be combined with the cbrs ACL if
preferred.
acl cloud dstdomain .cloud.cambiumnetworks.com
## This group blocks http CONNECT to non-standard https ports
acl SSL_Ports port 443
acl CONNECT method CONNECT
http_access deny CONNECT !SSL_Ports
## Allow access only to the sas and cloud acls. Add your own ACLs here if needed
http_access allow CONNECT cbrs
http_access allow CONNECT cloud
http_access deny all
## We dont need any cache for proxying cbrs traffic cache deny all Port config, change this
to suit your requirements
http_port 3128
```

HA for Squid external proxy

Since a standalone proxy is a single point of failure, we recommend using an HA setup for Squid. This can be done using Pacemaker or DRDB.

LTE

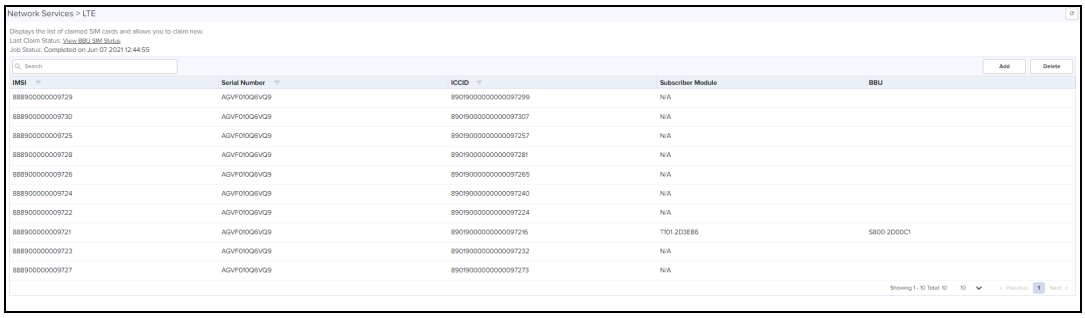
cnMaestro supports LTE as part of its On-Premises deployment. LTE allows customers to onboard the SM with IMSI into cnMaestro.

System access in cnRanger is dependent on installation of SIM credentials on every BBU in the operator network. To ease the operations aspects of SIM card management, cnMaestro provides utilities for claiming, managing, and distributing Cambium Networks cnRanger SIM card credentials (3rd party SIM cards are not currently supported on cnRanger).

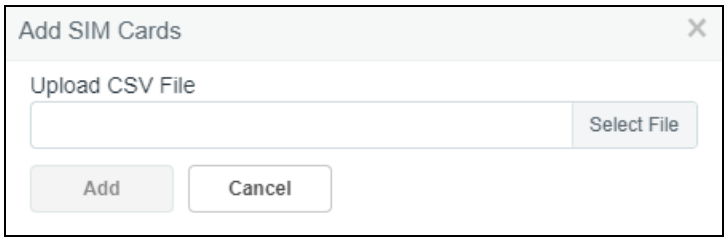
Adding SIM Cards

To add a SIM card:

1. Navigate to **Services > LTE.**



2. Click **Add.** The following window appears:

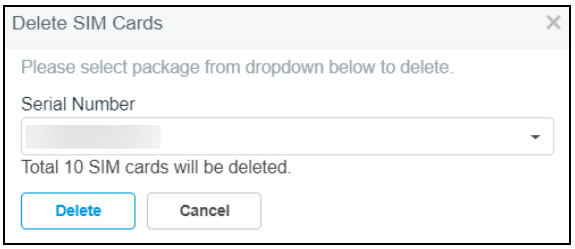


3. Select the CSV file and click **Add**.

> **Note:**
>
> User can download the .CSV file from the Cloud account once the Serial Number is validated from the cnMaestro Cloud data base.

Delete SIM Cards

To delete a SIM card from the list, click **Delete.** The following window pops-up.



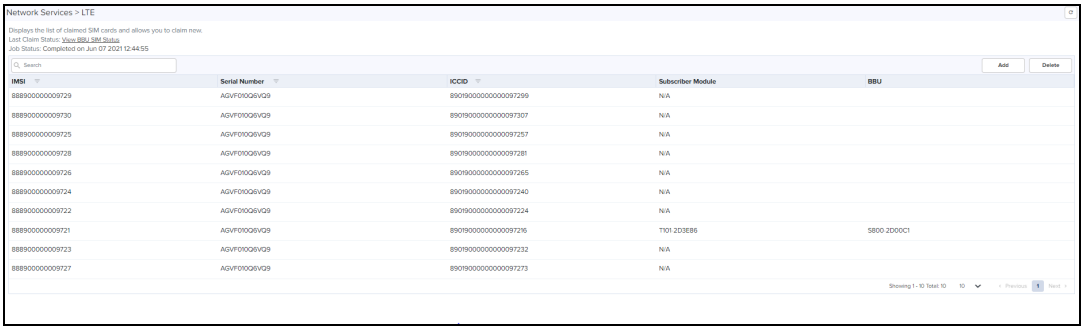
Note:

IMSI numbers are deleted with the mapped Serial Number.

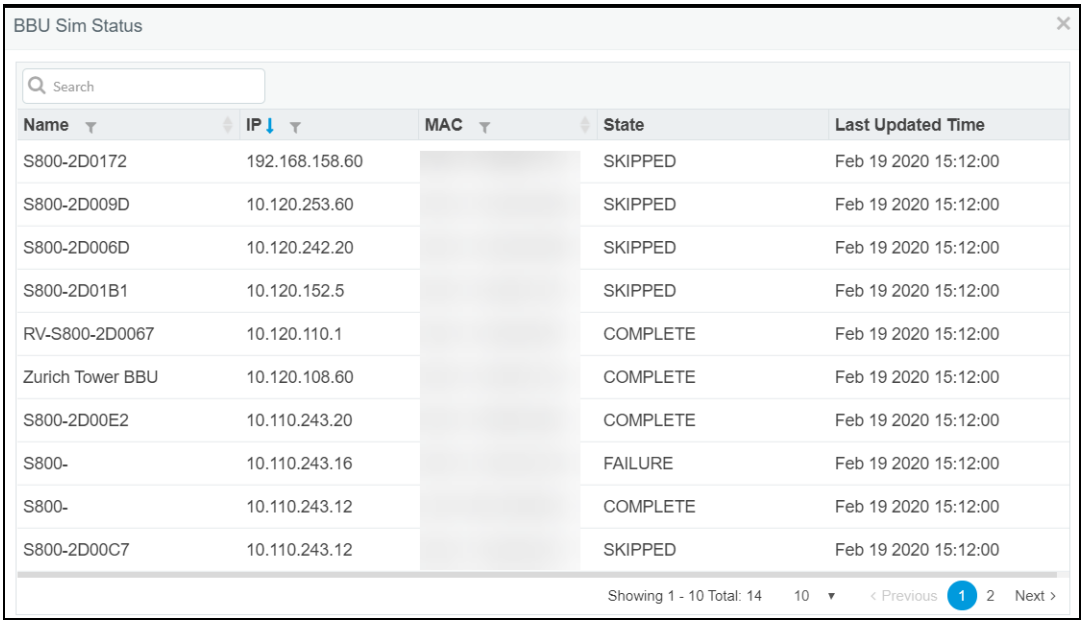
Viewing BBU SIM Status

Allows the users to view the status of the SIM connected to the BBU:

1. Navigate to **Services > LTE.**



2. Click **View BBU SIM Status.**



cnArcher Installation Summary

cnArcher is a mobile application used to install PMP Subscriber Modules (SMs), ePMP (SMs), and cnRanger SM. The installation summary provides an overview of the data collected by cnArcher during the installation process.

NOTE

- cnArcher Installation Summary is a cnMaestro X feature.
- cnArcher Installation summary of PMP SM is available for users in cnMaestro Cloud and OnPremises from 3.1.0 release.

To view the installation summary:

1. Navigate to **Network Services** > **cnArcher Installation Summary.**

   The **cnArcher Installation Summary** page appears.

2. You can **Search** cnArcher Summary details by using **MAC Address**, **Name at Installation**, **Date** and **Time**, **Added By**, and **Comments.**

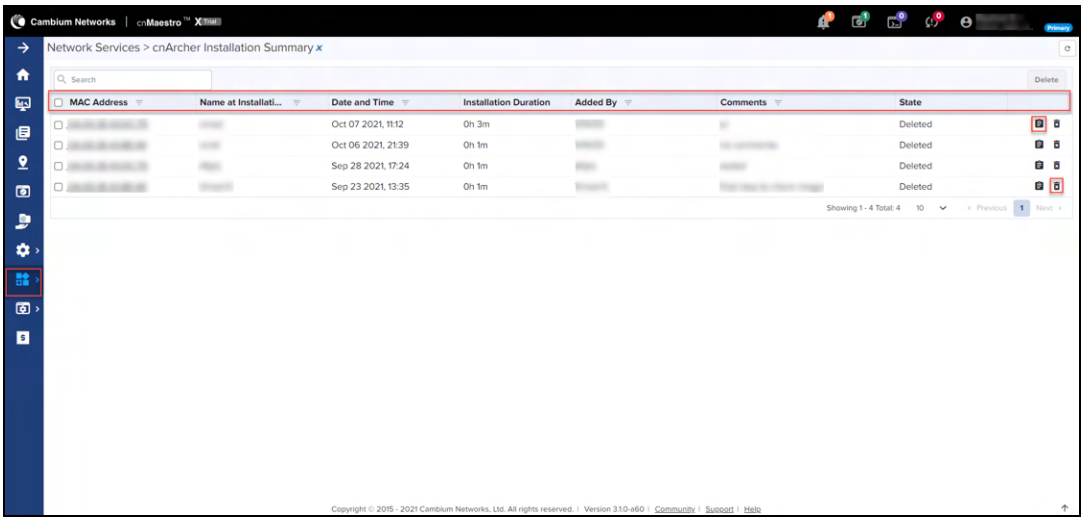


Table 49: Fields in cnArcher Installation Summary

Field	Description
MAC Address	MAC address of the device.
Name at Installation	Name given to the device when installed.
Date and Time	Date and time of installation.
Installation Duration	Duration of installation.
Added By	Name of the user adding the device.
Comments	Comments about the installation.
State	Current state of the device such as Managed or Deleted.

3. Click **View Details** icon to view detailed Installation Summary.

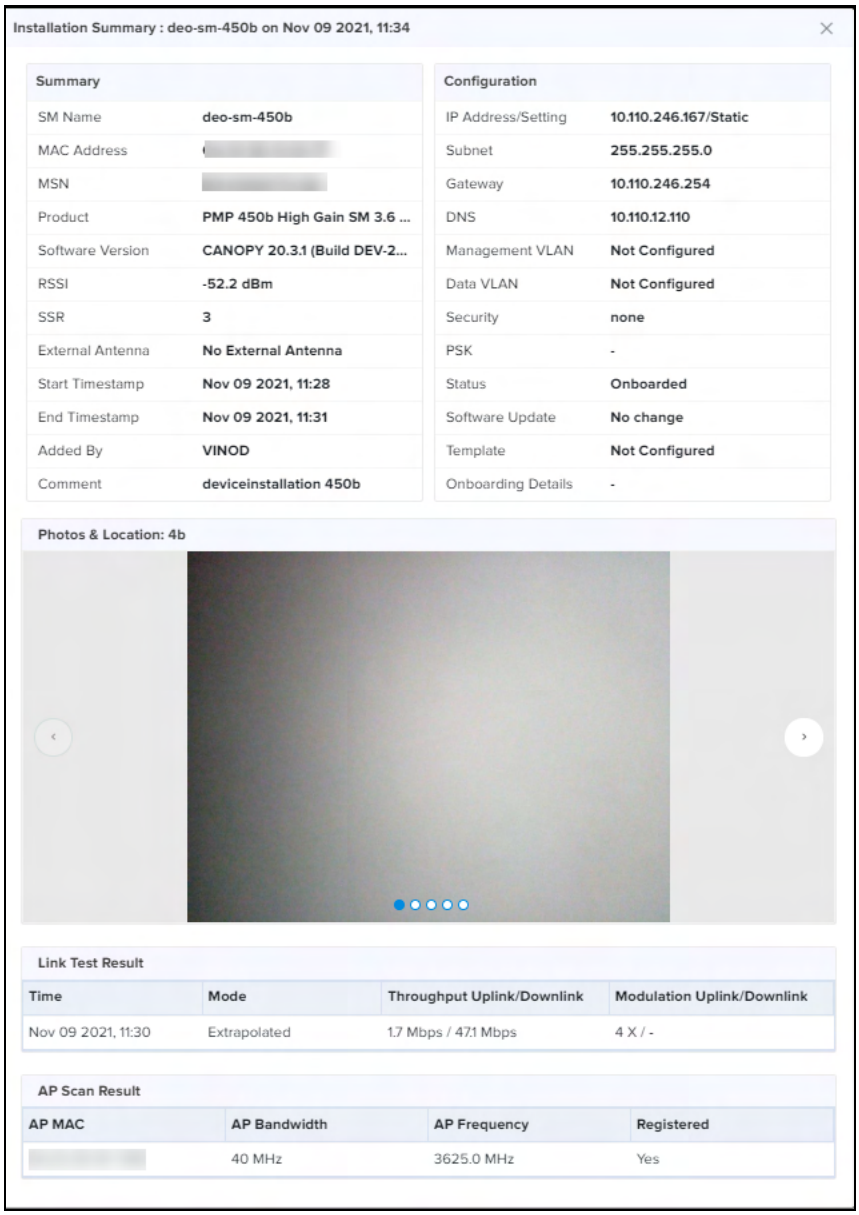


Table 50: Summary fields in cnArcher Installation

Field	Description
SM Name	Name of the device.
MAC Address	MAC address of SM.
MSN	Serial number of device.
Product	Device model and type .
Software Version	Software version of device.
RSSI	Receiver Signal Strength Indicator (RSSI) of SM.
SSR	Signal Strength Ratio (SSR).

Table 50: Summary fields in cnArcher Installation

Field	Description
External Antenna	Peak gain of external antenna connected to the device.
Start Timestamp	Start time of the summary.
End Timestamp	End time of the summary.
Comment	Comments about the installation process.

Configuration

Table 51: Configuration fields in cnArcher Installation

Field	Description
IP Address/Setting	IP settings such as for DHCP or Static IP allocation.
Subnet	Subnet mask of the device.
Gateway	IP address of the gateway.
DNS	Name of the DNS server.
Management VLAN	Configured Management VLAN.
Data VLAN	Configured Data VLAN.
Security	Security settings.
PSK	Type of PSK (Pre-Shared Key): WPA or WPA2.
Status	Current SM state such as Onboarded or Already Onboarded.
Software Update	Software version provided to upgrade.
Template	Name of the configuration template to apply.
Onboarding Details	Onboarding details related to SM.

Photos and Location

Photos and Location displays the photos taken during installation. You can view a maximum of four photos at a time.

Link Test Result

Link Test Result displays the link related test results with respect to throughput.

Table 52: Link Test Results fields

Field	Description
Mode	Modes such as Extrapolated Link Test or Link Test with Bridging.
Modulation Uplink/Downlink	Uplink and Downlink Modulation.
Time	Time at which the link test was performed.
Throughput Uplink/Downlink	Uplink and Downlink Throughput.

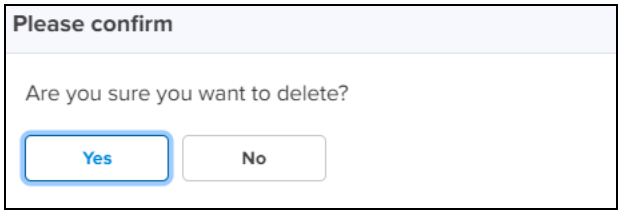
AP Scan Result

AP Scan Result displays a list of scanned APs.

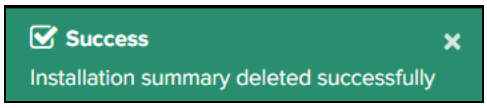
Table 53: Fields in AP Scan Result

Field	Description
AP MAC	MAC address of the AP.
AP Bandwidth	Bandwidth of the AP.
AP Frequency	Frequency of the AP.
Registered	Details of the registered SM.

4. Click **Delete** icon to delete single or multiple entries from the **cnArcher Installation Summary** page.
5. Click **Yes** to proceed to delete.



6. A confirmation message is displayed on a successful delete.





NOTE

cnArcher uploads Installation Summary with cnMaestro when Internet connection is available to users mobile device. This feature is support only in Android.

Administration

This section includes the following topics:

- User Management
- Server Management
- Syslog
- Webhooks
- Audit Logs

User Management

This chapter provides the following details:

- Authentication
- Local Users
- Authentication Servers
- Session Management

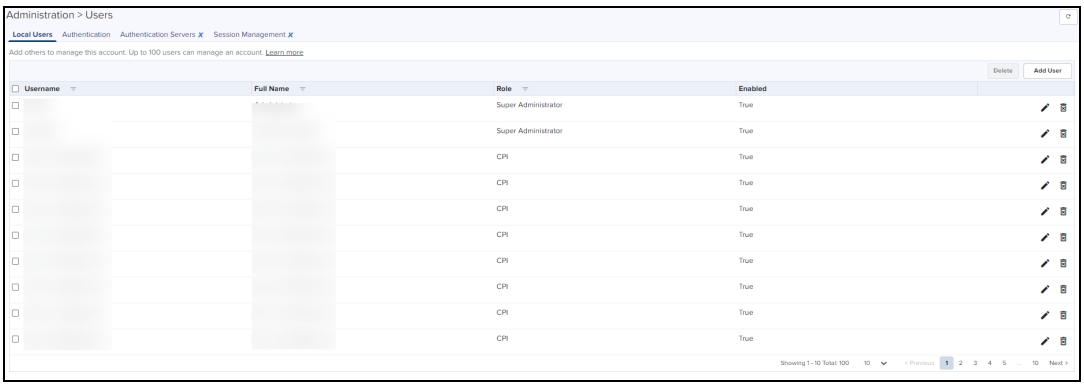
Authentication

cnMaestro On-Premises supports a Primary mode of authentication and an optional Secondary mode. If the Primary mode is Local Users (users specified in cnMaestro in the Users tab), no Secondary mode is available. If the Primary mode is an Authentication Server, then the Secondary mode will be set to Users and cannot be changed.

Local Users

To add Local Users, navigate to **Administration > Users**.

Figure 156 Adding Users



Role-Based Access

Each user is assigned a Role that defines their authorization. On successful authentication, every request from this user is processed in light of their Role.

cnMaestro supports the following user Roles:

- **Super Administrator** – Super Administrators can perform all operations.

- **Administrator** – Administrators can modify cnMaestro application functionality, but they are not able to edit User, API, or Server configuration.
- **Operator** – Operators are able to configure device-specific parameters and view all configuration.
- **Monitor** - Monitors have only view access.
- **CPI** - CPI can perform onboarding the devices using the CBRS tool and has the view access only.



NOTE:

- cnMaestro On-Premises allows the user to limit the number of concurrent sessions for each Role and display current active user sessions.
- CPI role is authorized only when the **CBRS** is enabled.

Role-Mappings

The table below defines how Roles are authorized to access specific features.

Table 54: Role-Mappings

Feature	Description
Authentication Services	Create and configure Authentication servers. • Super Administrator - All • Administrator - None • Operator - None • Monitor - None • CPI - None
API Management	API Client. administration. • Super Administrator - All • Administrator - None • Operator - None • Monitor - None • CPI - None
Application Operations	Application level operations such as to create, update and delete operations for Networks, Towers/Sites. Bulk device configuration. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Application Settings	Change global application configuration and onboarding key. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None

Table 54: Role-Mappings

Feature	Description
Configuration/Software Update and Scheduled Report Jobs	Manage configuration/software update and scheduled report related jobs • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Data Tunnel	Data tunnel configuration. • Super Administrator - All • Administrator - All • Operator - View • Monitor - View (Statistics tab only) • CPI - View (Statistics tab only)
Device Operations	Device operations such as reboot device, link test, connectivity test, technical support file download, and Wi-Fi performance test. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None (except Wi-Fi Performance test which is supported in On-Premises only) • CPI - None (except Wi-Fi Performance test which is supported in On-Premises only)
Device Overrides	Per-device configuration, including updating AP Group and applying configuration. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Global Configuration	The ability to create and apply configuration for global features such as Templates, WLANs, AP Groups, auto-provisioning, and bulk sync configuration. • Super Administrator - All • Administrator - All • Operator -View • Monitor - None • CPI - None
Guest Portal	Guest Portal configuration.

Table 54: Role-Mappings

Feature	Description
	• Super Administrator - All • Administrator - All • Operator -View • Monitor - View (sessions only) • CPI - View (sessions only)
Monitoring	Display of monitoring data at all levels, VM Monitoring • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - View
Managed Service Provider (MSP)	MSP operations such as modification of branded service, managed account and user invitations. • Super Administrator - All • Administrator - View • Operator - None • Monitor – None • CPI - None **Note:** Operator/Monitor users are not permitted to move devices across managed accounts.
Notifications	Alarms and Events management. • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - None
Onboarding	Device approval, modifying individual device configuration, and performing software update. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - All
Reporting	Report generation. • Super Administrator - All • Administrator - All • Operator - All

Table 54: Role-Mappings

Feature	Description
	• Monitor - All • CPI - All
Session Management	Capability to view and logout other users sessions. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Software Images	Upload and delete device software images. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Software Upgrade	Upgrade the device with the latest software. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None

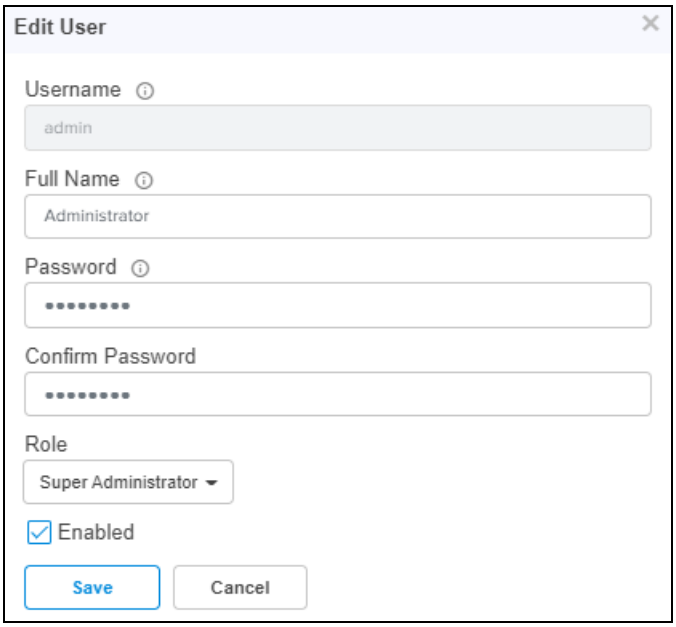
Table 54: Role-Mappings

Feature	Description
SNMP Configuration	SNMPv2c configuration parameters. • Super Administrator - All • Administrator - All • Operator -View • Monitor - None • CPI - None
System Operations	System operations such as Reboot VM, change log level, system upgrade, system monitoring, uploading SSL certificate, import/export server data and server tech dump, and upload/delete device software images. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
User Management	User management operations such as manage users and roles. • Super Administrator - All • Administrator - View • Operator - None • Monitor - None • CPI - None

Creating Users and Configuring User Roles

To add a user:

1. Navigate to **Administration > Users**.
2. Click **Add User**. The following window is displayed:



3. Enter the **Username**.
4. Enter the **Full Name**.
5. Enter the **Password**.
6. Confirm the Password by entering the same password.

To configure User Roles:

7. Select any one of the role for the user from the Role drop-down:

- Super Administrator
- Administrator
- Operator
- Monitor
- CPI

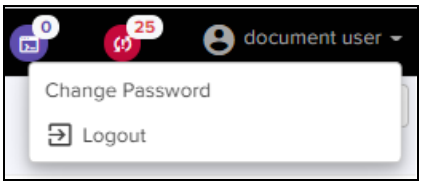
8. Choose the **State** as Enabled or Disabled.
9. Click **Save**.

To edit or delete a user, click the Edit icon or the Delete icon against the user in the **Administration > Users** page.

Changing Password

Change Password option is available only for local users.

Figure 157 Changing Password



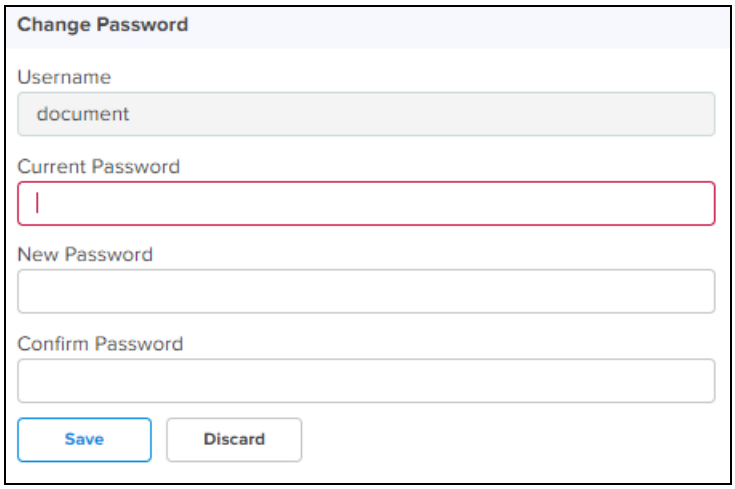
Ensure the primary Authentication must be local users to **Change Password** option. After changing the password, the current session will get logged out.

Also, ensure that there are no parallel sessions with the same users before going for **Change Password** option.

To change password:

1. Click the drop-down icon next to the username in the top right corner of the UI.
2. Enter the following details:
   a. The Current Password.
   b. A new password for this user.
   c. Confirm the Password by entering the same password.
3. Click **Save**.

Figure 158 Changing Password Parameters



Authentication Servers

cnMaestro supports authentication and authorization with TACACS+, RADIUS, LDAP, and Active Directory servers, and is a cnMaestro X feature.

Authentication Server

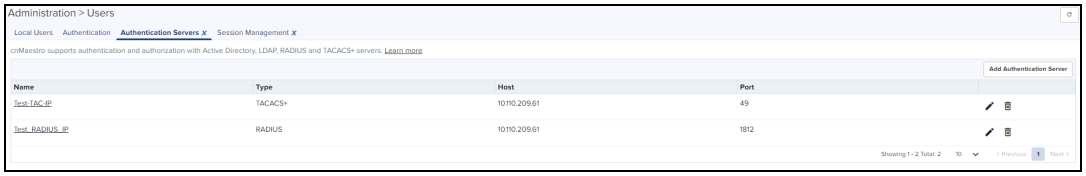
Authentication Servers can be configured by cnMaestro Super Administrators. The following operations are available:

- List All Authentication Servers
- Create New Authentication Server Configuration
- Secondary Server Authentication
- Edit an Existing Authentication Server Configuration
- Delete an Existing Authentication Server Configuration
- Verify the Role of the User
- Show User Groups for Active Directory

List All Authentication Servers

To view all the Authentication servers which are configured in cnMaestro, navigate to **Administration > Users > Authentication Servers**.

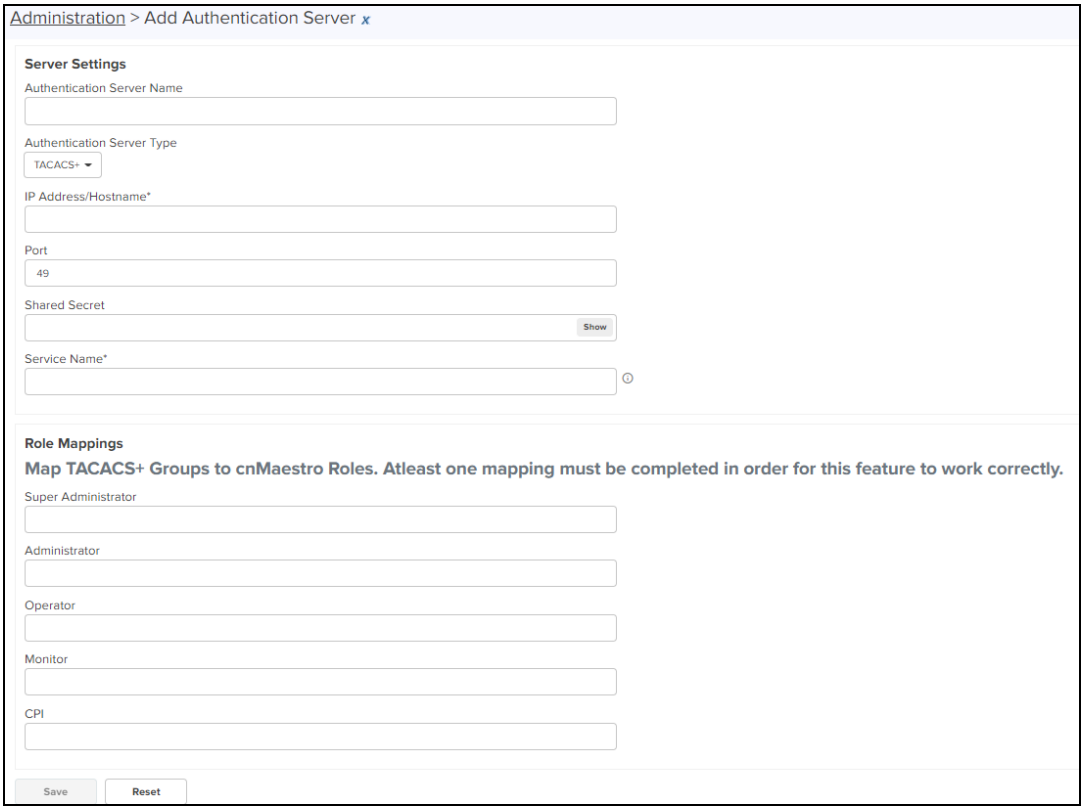
Figure 159 List of Authentication Servers



Create New Authentication Server Configuration

1. Navigate to **Administration > Users > Authentication Servers**.
2. Click **Add New Authentication Server**.

Figure 160 Authentication Server



TACACS+

The fields that are present when TACACS+ server is selected are listed below:

Table 55: TACACS+ Parameters

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server
IP Address/Host name	Enter the FQDN (Fully Qualified Domain Name) of the server or the IP address of the server.
Port	TCP port of the server. (Default value is 49)

Table 55: TACACS+ Parameters

Parameter	Description
Shared Secret	Shared secret key for communicating with the server.
Service Name	Name defined in the service configuration table configured by TACACS+ server administrator. This is used to configure service and corresponding user groups.
Role Mappings	TACACS+ user groups should be mapped to one or more cnMaestro Roles. Refer Role-Based Access section to view the supported Roles on cnMaestro. Enter the role strings that are configured in the TACACS+ server. Atleast one mapping must be completed for this feature to work correctly.

NOTE:
TACACS+ server administrator should setup the service name and corresponding user group as per the configuration.

RADIUS

The fields present when RADIUS is selected are listed below:

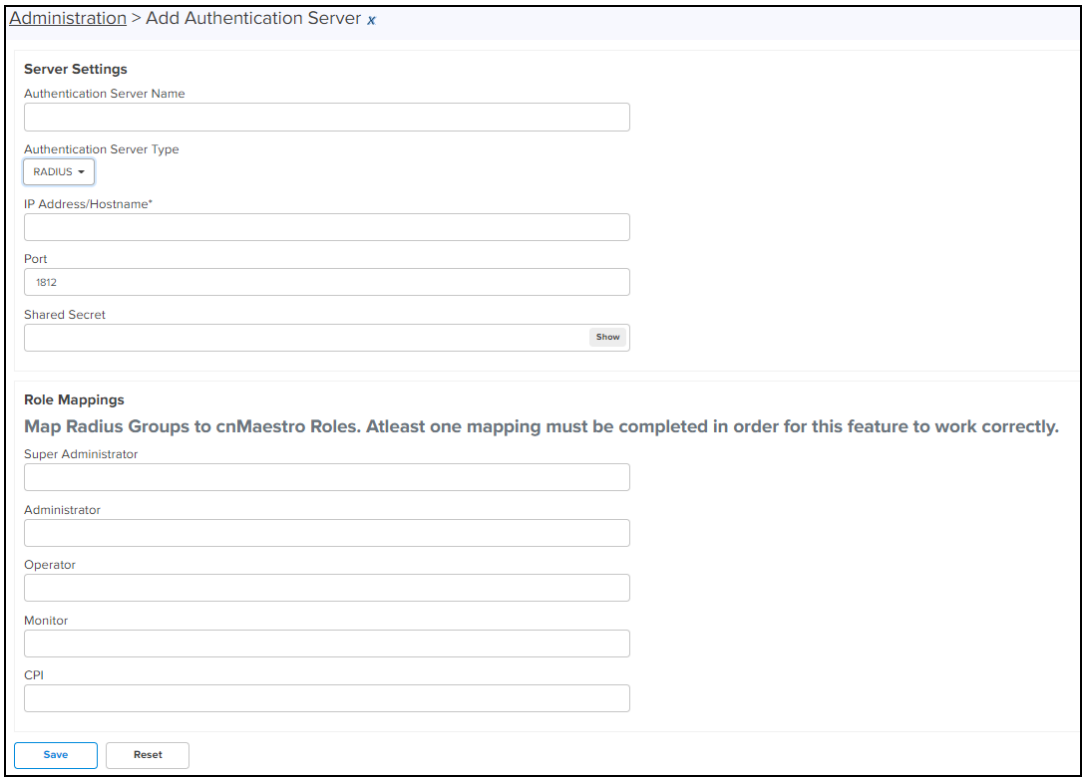


Table 56: RADIUS Parameters

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server.
IP Address/Hostname	Enter the FQDN (Fully Qualified Domain Name) of the server or the IP address of the server.
Port	UDP port of the server (Default is 1812).
Shared Secret	Shared secret key for communicating with the server.
Role Mappings	Radius user groups should be mapped to one or more cnMaestro Roles. Refer the Role-Based Access section to view cnMaestro supported Roles. Enter the role strings that are configured in the Active Directory server. At least one mapping must be completed for this feature to work correctly.



NOTE:

The RADIUS administrator should setup user group as per configuration. The RADIUS administrator can choose a user group and the same should be configured on cnMaestro Authentication server configuration.

Active Directory

The fields present when Active Directory is selected are listed below:

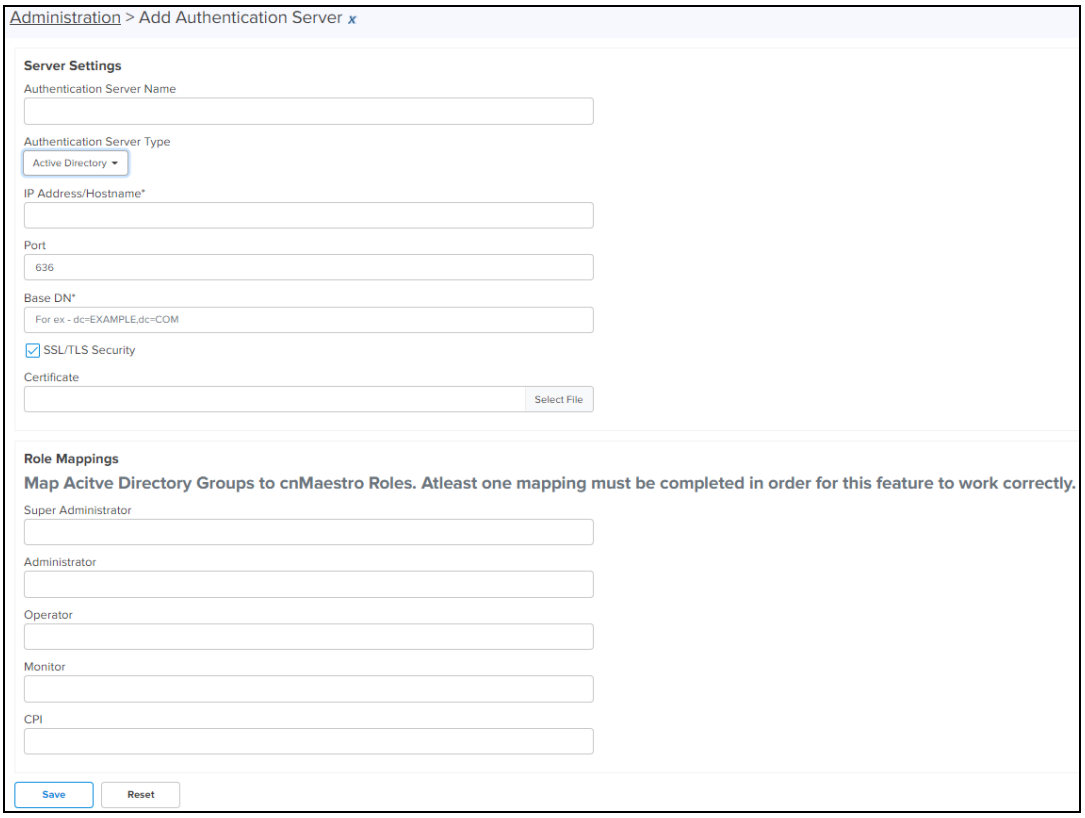


Table 57: Active Directory Parameters

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server.
BASE DN	Distinguished Name for Active Directory.
IP Address	IP address of the server.
Port	TCP port of the server. (default 389). When SSL/TLS option is enabled, the port will automatically change to 636.
SSL/TLS	Select this check box if Active Directory connection should be secured over SSL/TLS as LDAPS. Browse and select the Root certificate of the Active Directory server in .PEM format.
Role Mappings	Active Directory user groups should be mapped to one or more cnMaestro Roles. Refer the Role-Based Access section to view cnMaestro supported Roles. Enter the role strings that are configured in the Active Directory server. Atleast one mapping must be completed in order for this feature to work correctly.

	NOTE: The Active Directory administrator should setup user group as per configuration. The Active Directory administrator can choose a user group and the same should be configured on cnMaestro Authentication server configuration. Examples: CN=super-admin CN=admin CN=network CN=operator
	NOTE: If Role is not configured in TACACS+/RADIUS server or group is not configured in Active Directory, you cannot login to cnMaestro.
	NOTE: A user with valid credentials will not be to able to login if: 1. cnMaestro role to Authentication server's user group mapping is missing in Authentication server configuration 2. User group of the user is not configured in Authentication server and is a required field for cnMaestro login.

LDAP

The fields present when LDAP is selected are listed below:

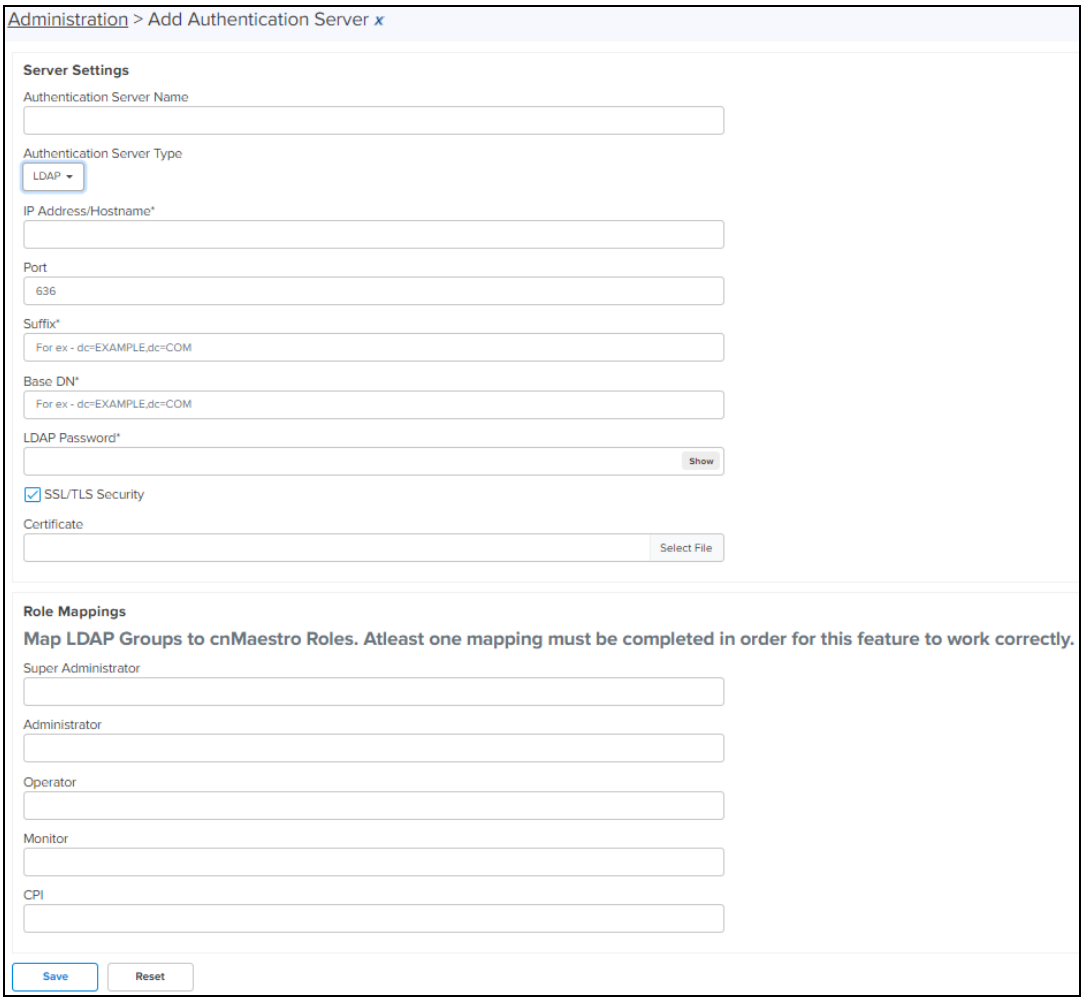


Table 58: LDAP Parameters

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server.
Base DN	Base DN is generally the Admin DN used to log in to LDAP server. For example: cn=admin,dc=xyz,dc=com.
Certificate	Browse and update with root certificate in .PEM format.
IP Address/Hostname	Provide IP address for LDAP and hostname of server if SSL/TLS is enabled.
LDAP Password	LDAP Password is the admin password used by Admin DN to log in.
Port	TCP port of the server. (Default for LDAP is 389 and for LDAPs is 636)

Table 58: LDAP Parameters

Parameter	Description
Suffix	Suffix is the DNS name. For example: dc= xyz, dc=com.
SSL/TSL Security	Select this check box LDAP connection should be secured over SSL/ TLS as LDAPS. Browse and select the Root certificate of the Active Directory server in .PEM format. **Note:** ■ If you enable **SSL/TSL Security** check box, the default port will appear as **636** in the **Port** text box. ■ If you disable **SSL/TSL Security** check box, the default port will appear as **389** in the **Port** text box.
Role Mappings	RADIUS user groups should be mapped to one or more cnMaestro Roles. Refer the Role-Based Access section to view cnMaestro supported Roles. Enter the role strings that are configured in the Active Directory server.At least one mapping must be completed for this feature to work correctly.

Secondary Server Authentication

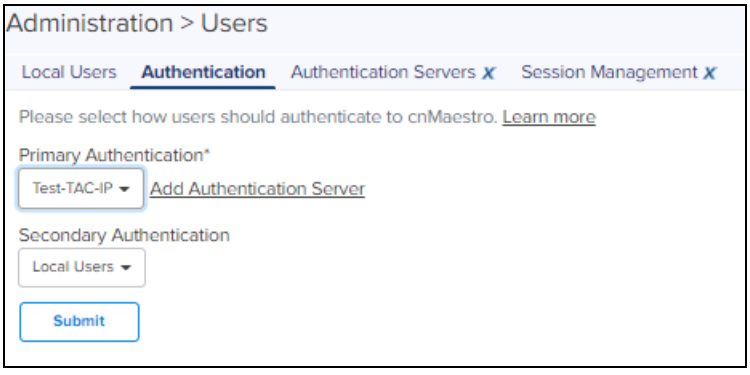
In addition to the primary server authentication, cnMaestro On-Premises now supports configuration for secondary external server for authentication. Secondary authentication and primary authentication servers should be different.



NOTE:
Same authentication will not be shown on the server. For example, If we select primary as Test-TAC-IP, then we cannot select the same in secondary authentication.

Tertiary authentication is always default to the local users. Local users logs in only when primary and secondary are not reachable or when the services are not being run on authentication server. If the primary server is not reachable then fallback happens to the secondary authentication server. If the secondary authentication server is not reachable then fallback happens to tertiary authentication. If primary authentication server is running properly then users belonging to primary authentication server can only be logged in. If secondary authentication server is running properly then users belonging to secondary authentication server can only be logged in.

Figure 161 Secondary Server Authentication

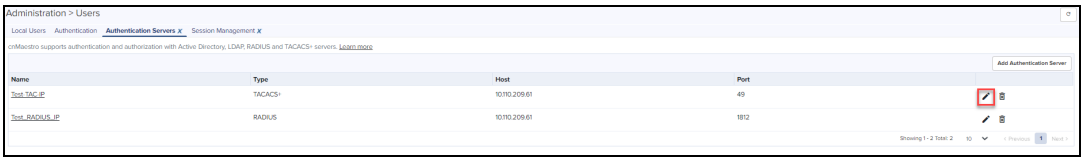


Edit an Existing Authentication Server Configuration

To edit an existing Authentication Server configuration:

1. Navigate to **List all Authentication Servers** page.

2. Click the name of the server or **Edit** icon( ).



Refer Create New Authentication Server Configuration section for explanation of fields on **Edit** page.

Delete an Existing Authentication Server Configuration

To delete an existing Authentication Server configuration:

1. Navigate to **List all Authentication Servers**.

2. Click **delete**.

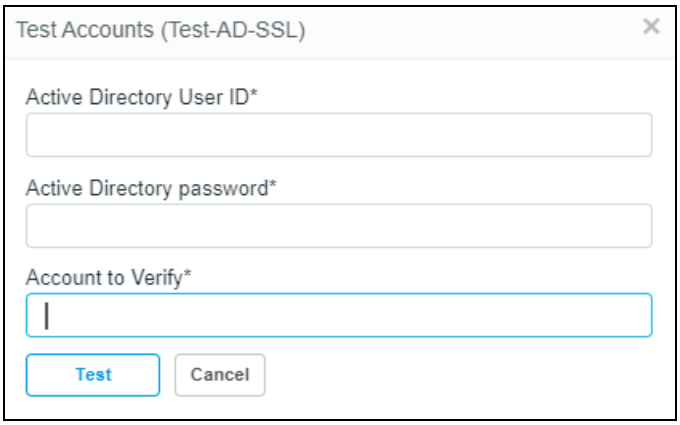
Primary authentication order will change as Local Authentication if this server is setup as Primary Authentication under **Manage Authentication Server Authentication** section.

Verify the Role of the User

- To know and verify the role of the **Active Directory** user:

1. Navigate to **List all Authentication Servers** page.

2. Click the **test** icon ( ) next to any of the Active Directory type. The following window appears:



3. Provide the following details:

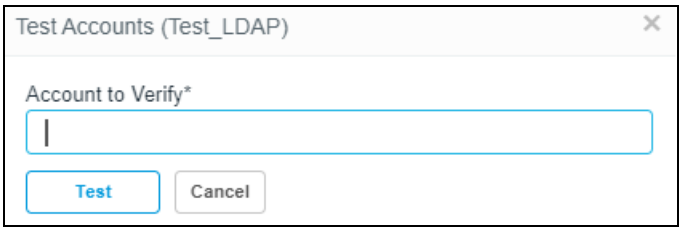
- Active Directory User ID
- Active Directory Password
- Account to Verify

4. Click **Test**.

- To know and verify the role of the **LDAP** user:

1. Navigate to **List all Authentication Servers** page.

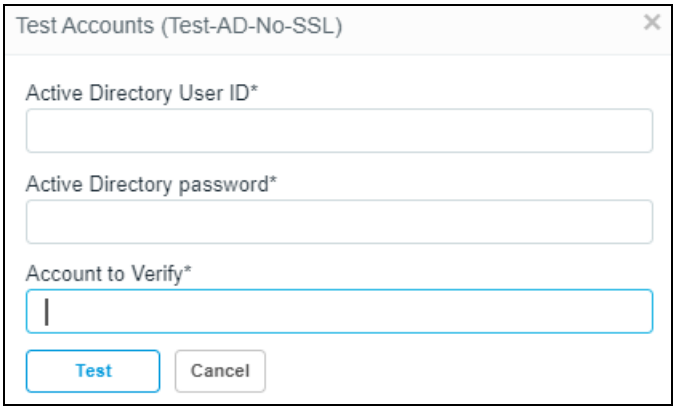
2. Click the **test** icon ( ) next to any of the LDAP type. The following window appears:



5. Enter the name of the **Account to Verify**.
6. Click **Test**.

Show User Groups for Active Directory

cnMaestro administrator can view user groups for Active Directory server type configuration by providing valid user credentials to login to Active Directory. The user details can then be viewed as shown below:



1. Enter **Active Directory User ID**. The User ID should be a valid string (Eg: user@example.com).
2. Enter **Active Directory password**.
3. Enter **Account to Verify**.

For searching the group of the user, the Users ID should follow the user@example.com format.

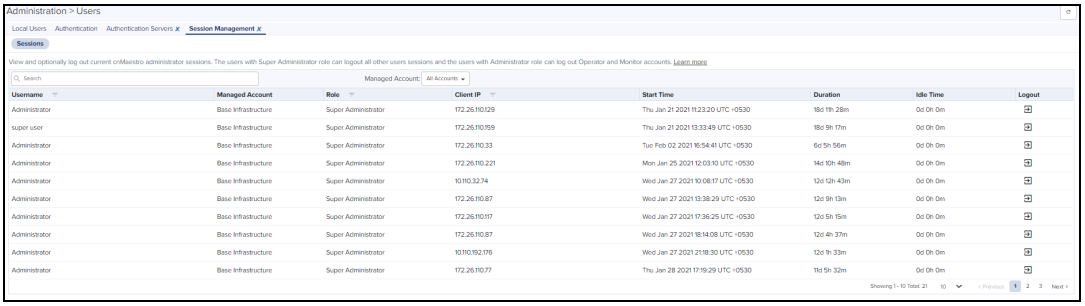
Session Management

View and optionally log out current cnMaestro administrator sessions. The users with Super Administrator Role can logout all other users sessions and the users with Administrator Roles can log out Operator and Monitor accounts.

Sessions

Displays the detailed information on the user sessions.

Figure 162 Session Management > Sessions



Server Management

This chapter provides the following details:

- Monitoring
- Settings
- Operations
- SSL Certificate
- Syslog

Monitoring

The Server tab provides monitoring and operations for the virtual machine instance.

Navigate to **Administration > Server.**

Figure 163 Monitoring cnMaestro Server Instance



Settings

This section provides the following details:

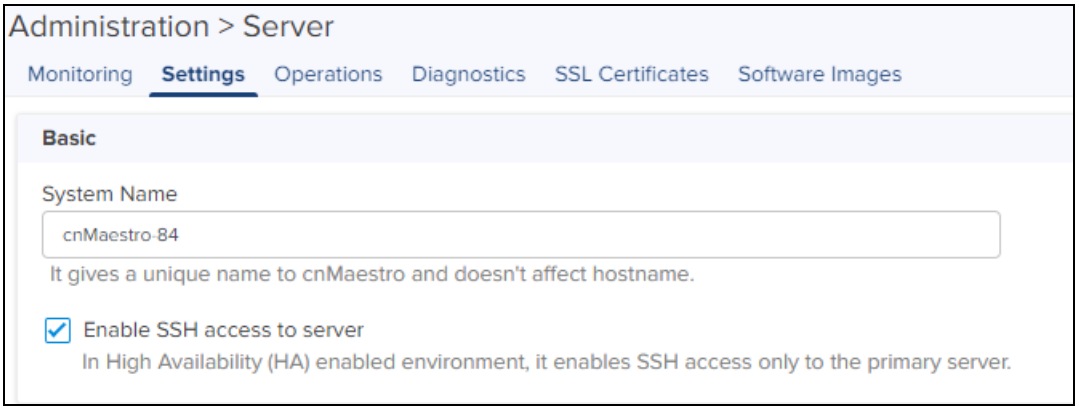
- Basic
- Configure NTP Server
- Configure Email Server
- Login Security Banner

Basic

The user can enter the **System Name** and enable the **SSH access to cnMaestro server**.

	NOTE: In High Availability (HA) enabled environment, it enables SSH access only to the primary server.

Figure 164 System Name

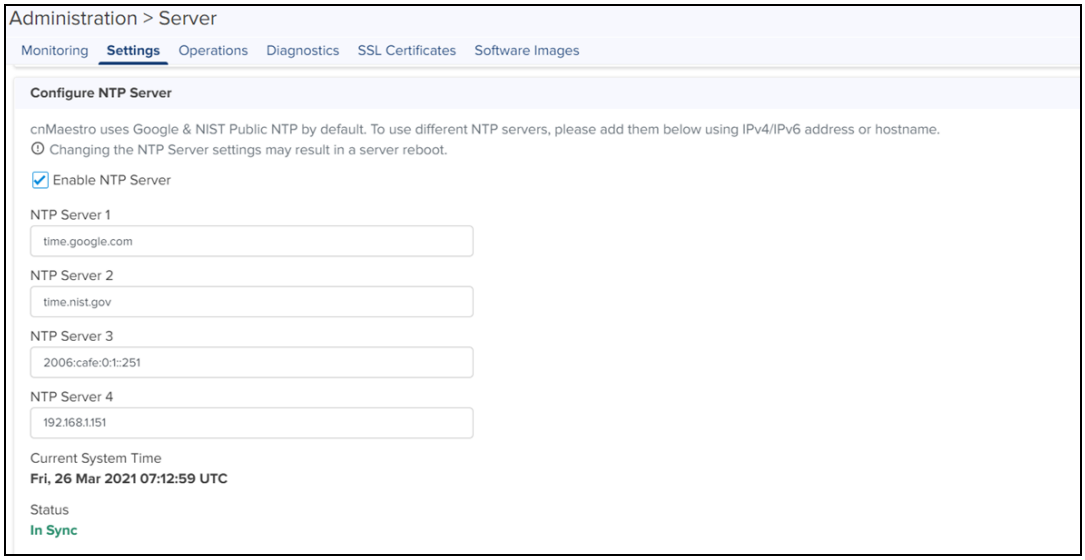


Configure NTP Server

The user can configure the NTP Server to configure the time configuration of the server with hostname or IP address.

To configure the NTP server:

1. Navigate to **Administration > Server > Settings> Configure NTP Server** tab.
2. Enable the **NTP Server**.
3. Enter **Host Name** or **IP Address**. It displays **Current System Time** and **Status** of the server.



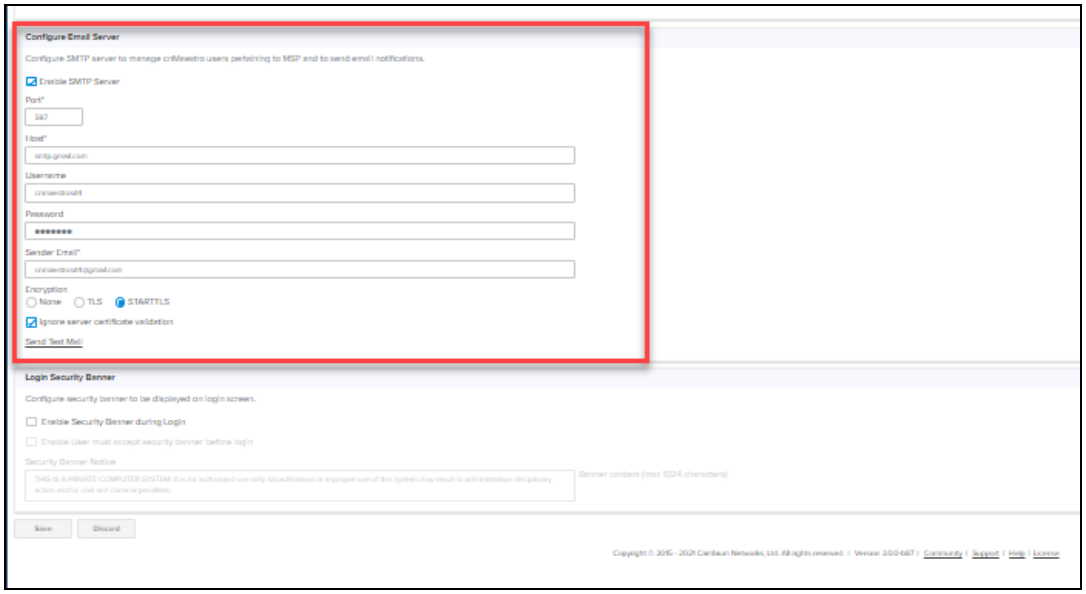
Configure Email Server

The user can configure the email server to send and receive email messages.

To configure the email server:

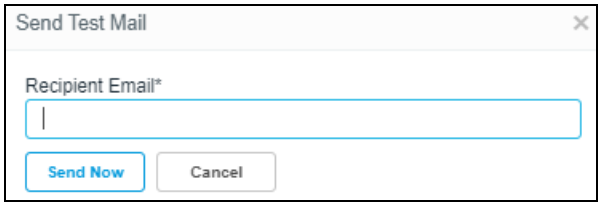
1. Navigate to **Administration > Server > Settings > Configure Email Server** tab.

Figure 165 Email Server



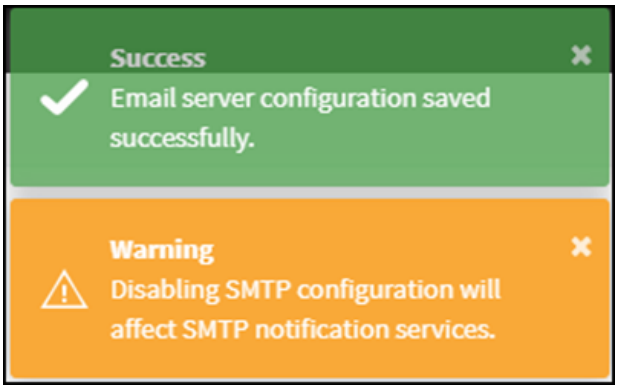
2. Select the **Enable SMTP Server** check box.
3. Enter the **Port number**.
4. Enter name of the **Host**.
5. Enter the **Username**.
6. Enter the **Password**.
7. Enter the **Sender Email**.
8. To send the email in an encrypted format, select any one of the following:
   - **None:** Uses port number 587 for communication which is not secured.
   - **TLS:** Uses port number 465 for encrypted communication. When this option is selected, upload CA certificate.
   - **STARTTLS**: For encrypted communication on port number 587, choose STARTTLS option. When this option is selected, upload CA certificate.
9. Select the **Ignore Server Certificate Validation** checkbox.
10. Click **Send Test Email**.

Figure 166 Specifying email address



11. Enter the **Recipient Email**.
12. Click **Send Now**.

	NOTE: When user tries to disable SMTP configuration a warning message pops-up.



Email Notifications

The Email Notifications feature allows the Super Administrator and the Administrator users to add subscribers (Email IDs) for receiving different types of alerts by means of Emails.

	NOTE: Email Subscribers are limited to two per account.

The severity of alerts are classified as follows:

- Critical
- Major
- Minor

The content of the email alert is in JSON or HTML format. The subscriber gets an email alert only when the global setting is enabled.

To receive email notifications, the user need to enable **Notification** checkbox. If SMTP settings are disabled, then below notification message does not pop-up.

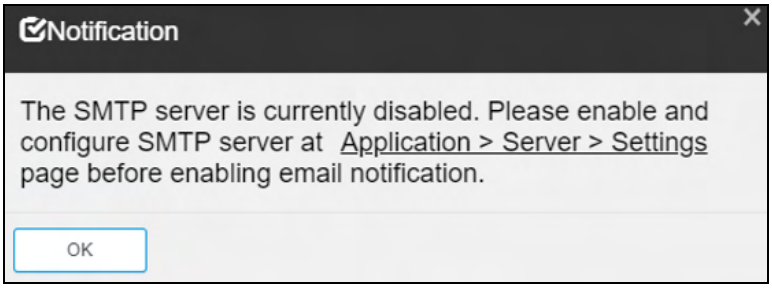
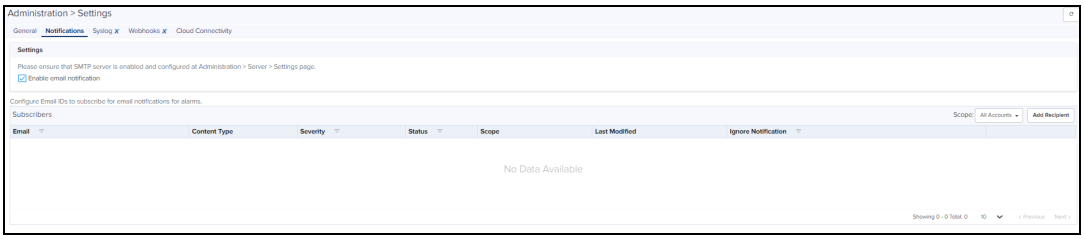


Figure 167 Email notifications



You can use the filter option for the following fields:

- Email
- Severity

- Status
- Ignore Notification

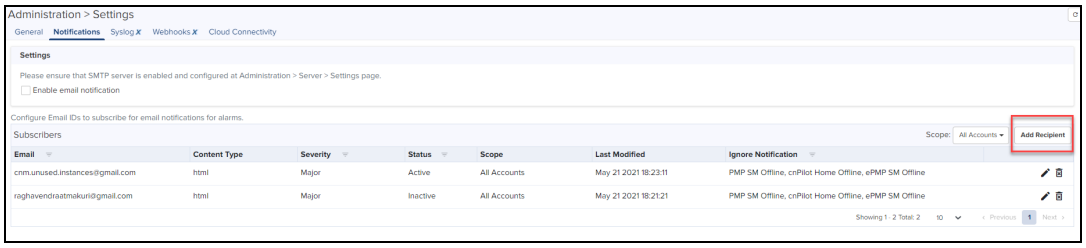
You can use the sorting option for the following fields:

- Content Type
- Last Modified Date

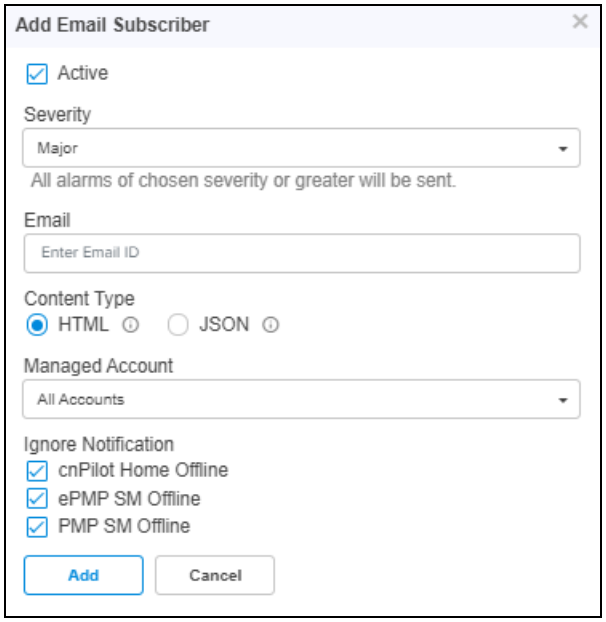
Adding Recipient to Subscriber Table

1. Navigate to **Administration > Settings > Notifications** and click **Add Recipient**.

Figure 168 Adding Subscribers



The following window is displayed:



NOTE:

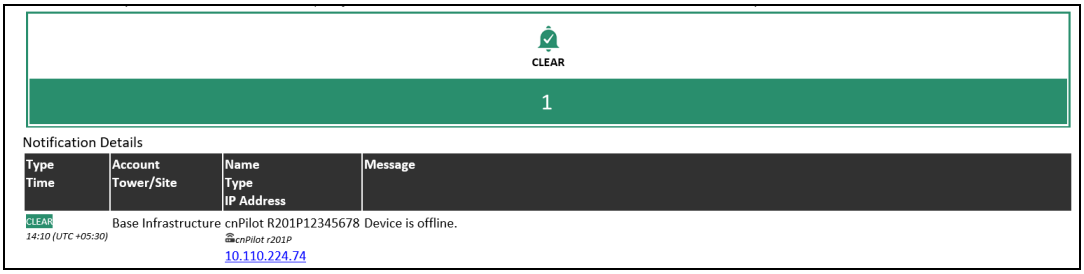
Managed Account option will appear only if MSP feature is enabled.

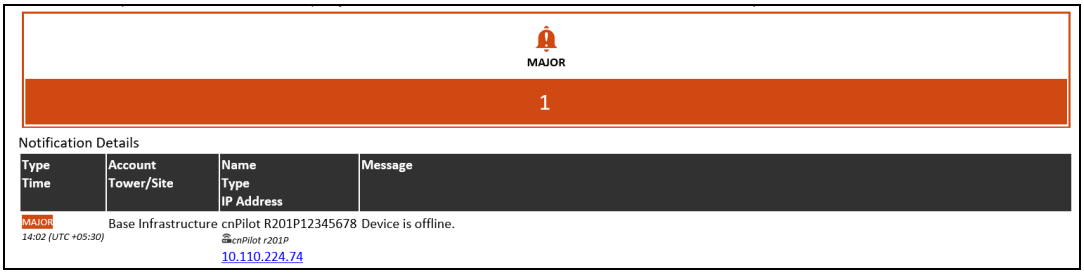
2. Select the **Severity** level.
3. Enter **Email**.
4. Select the **Content Type** as **HTML** or **JSON** .
5. Select the **Managed Account** list.
6. Select the appropriate option (s) for **Ignore Notification.**
7. Click **Add**.

All alarms of chosen severity and above are sent through email as explained below:

- If severity **Critical** is selected, then we receive only critical alarms.
- If severity **Major** is selected, then we receive critical and major alarms.
- If severity **Minor** is selected, then we receive critical, major, and minor alarms.

HTML Email Example





JSON Email Example



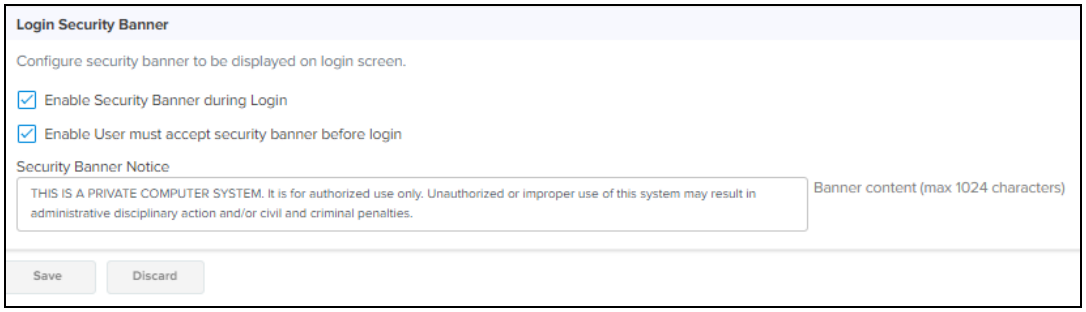
Login Security Banner

For security purpose, a banner will be displayed before the login window appears in cnMaestro On-Premises. If the user needs to be aware of any critical information, it is displayed within the security banner.

To enable :

1. Navigate to **Administration > Server > Settings > Security Banner**.

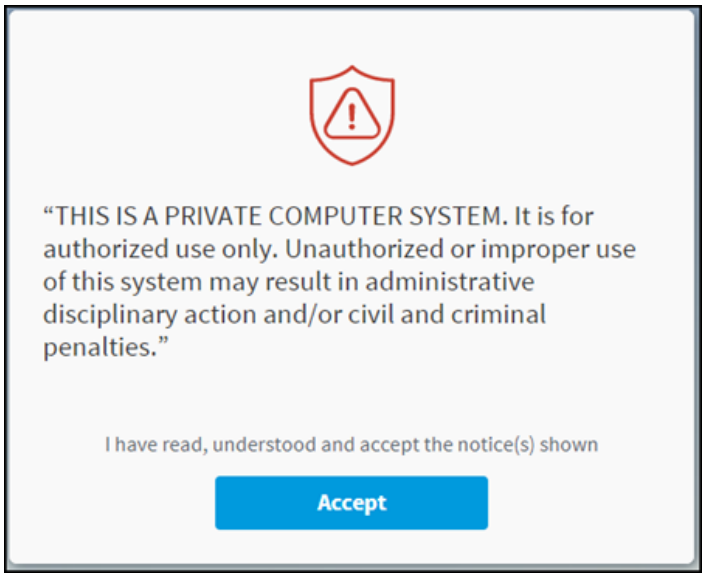
Figure 169 Enabling Security Banner



2. Enable the following options:
   - Enable Security Banner during Login
   - User must accept security banner before Login (If enabled, the user should accept the banner before login else the user can directly login, with the banner that is displayed.)
3. Enter the **Security Banner Notice**.
4. Click **Save.**

A sample security banner window is shown below:

Figure 170 Security Banner



Click **Accept**. The login window is displayed.

Operations

This section provides the following details:

- Reboot Virtual Machine
- Update cnMaestro Software
- System Backup
- In-System Upgrade

Reboot Virtual Machine

Warning:
All devices goes offline when the virtual devices is rebooted.

Update cnMaestro Software

Package Types

cnMaestro On-Premises software is released in two forms:

OVA Image

The OVA image contains all software needed to run the cnMaestro application. It is installed on a virtual machine and releases intermittently to update system software. Moving to a new OVA image requires an in-system upgrade of the current OVA (no import and export of data is required after the 2.0 release). The OVA is approximately 3.0 GB in size.

Package Upgrade

The package file is installed on top of an OVA image; and updates the cnMaestro application. Packages releases more frequently and provide a faster upgrade path for enhancements. Packages can be installed by downloading them from Cambium and uploading them through the UI (at **Administration** > **Server** > **Operations**).

NOTE:

1. The general update flow will be an OVA file followed by package releases. For significant system-level updates, a new OVA file will be generated.
2. Refer to Cloud connectivity page for download of software from cnMaestro Cloud.

System Backup

Cambium recommends customers periodically backup their system as a precautionary measure. To Backup navigate to **Server** > **Operations** > **System Backup and Restore**. Backups can be done manually, in real-time, or scheduled to execute daily or weekly. cnMaestro can also automatically transfer backup files off-box using FTP or SFTP (this support is configured under **Settings** > **Optional Features** > **Scheduled Jobs**).

A System Backup stores the entire state of cnMaestro On-Premises as a file. This file can be downloaded to the local hard drive through the UI and imported into a new cnMaestro instance to recreate the application state. Only one System Backup is available at any time, and a later entry overwrites an earlier one.

Generate Backup

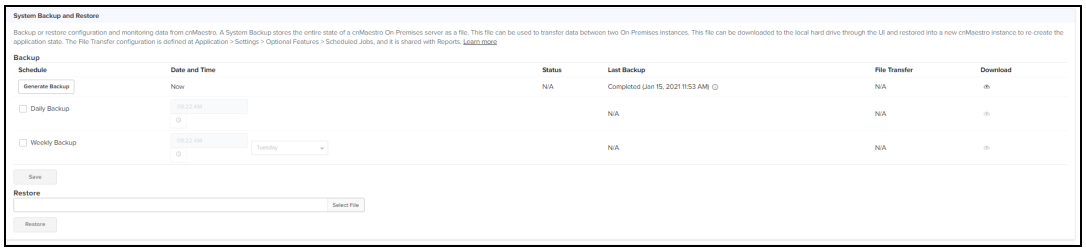
NOTE:

From 3.0.0 release, backup generated by On-Premises instance will have configuration data and historical monitoring data only for current month excluding client's data. It is suggested to take backup at the last day of the month if needed. Please refer to Data Backup for more information.

The user can create a system backup through a system backup job at **Administration > Server > System Backup and Restore**. The created backup file can be downloaded to the user's local machine for archiving.

To generate the system backup job:

1. Navigate to **Administration > Server > Operations > System Backup and Restore**.



2. Select any one of the following:

- **Daily Backup:** You can set time exceeding the current system time. The backup files will be generated every data at the scheduled time.
- **Weekly Backup**: The backup files will be generated for a specified day and time on a weekly basis .

You can download the last backup file using the download icon in the table. The file transfer configuration is defined at **Administration** > **Settings** > **Optional Features** > **Scheduled Jobs** and it is shared with Reports. If FTP is enabled, then a copy of each backup file will be stored in the configured FTP/SFTP server. The FTP column table displays the status of the upload to the FTP/SFTP server.

3. Click **Generate Backup** button.

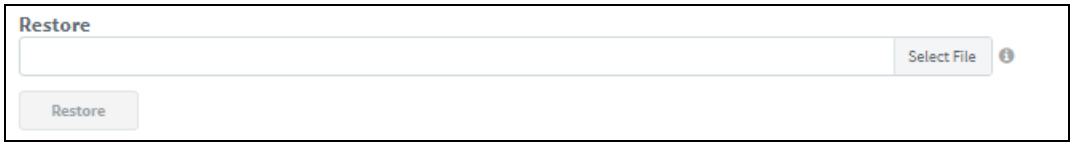
> **NOTE:**
>
> Only the latest backup is retained in the disk and available to download. The old backup is deleted once the new backup is generated.

To view the system backup job:

Click **View System Backup Jobs** link in **Operations** > **System Backup and Restore** or navigate to **Administration** > **Jobs** > **System Backups**.

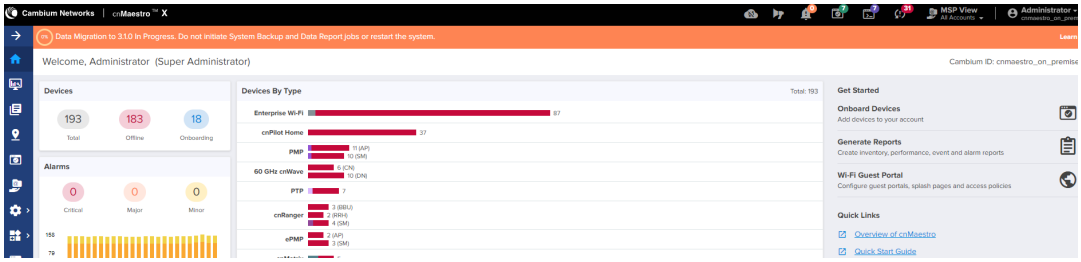
Restore Backup

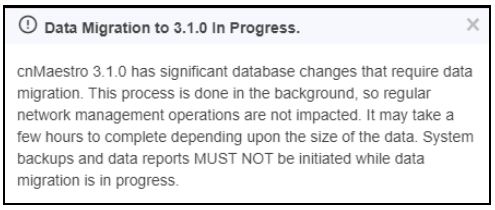
The user can now restore the downloaded system backup file to the new cnMaestro instance to recreate the application state under **Manage** > **Server** > **Operations** > **System Backup and Restore**.



To restore backup files, select the file from **Restore From Backup** option and click **Restore**.

Data migration to 3.1.0 from lower version takes some amount of time depending upon the size of backup file. During migration, the below banner is displayed:





In 3.1.0 release, when we import the backup data, the following banner displays in the top of cnMaestro On-Premises UI and it will be there until the indexing is completed.



NOTE:

- The indexing will happen whenever the user navigates to different UI pages. For example, when the user navigates to WLAN-AP group page, the respective indexing will be created and the banner will be displayed in the top of the UI.
- Database indexing pauses during the database migration and emails once indexing the webhooks.
- Do not Import data or Export data when the Migration banner is running.

OVA Update Process

Updating an OVA image can be managed through the following process (which assumes the hardware has enough hard disk space for two instances of cnMaestro.

1. Export the cnMaestro Server data from the old instance.
2. Stop the old instance.
3. Start the new instance (using the directions presented above).
4. Import the data into the new instance.
5. Set the IP address of the new instance to that of the old instance.

Clone Virtual Machine

Cambium also recommends backing up (or cloning) the virtual machine prior to updating cnMaestro software.

In-System Upgrade

In-System Upgrade is the ability to update the cnMaestro software without performing a system export followed by an import. Essentially all updates are performed within a single VM image. In-System Upgrade works in both Standalone and High Availability environments. The mechanism of the upgrade should be transparent to the user: they specify to upgrade the system on one instance, and the upgrade is propagated to both instances. The coordination happens automatically.

Software Update

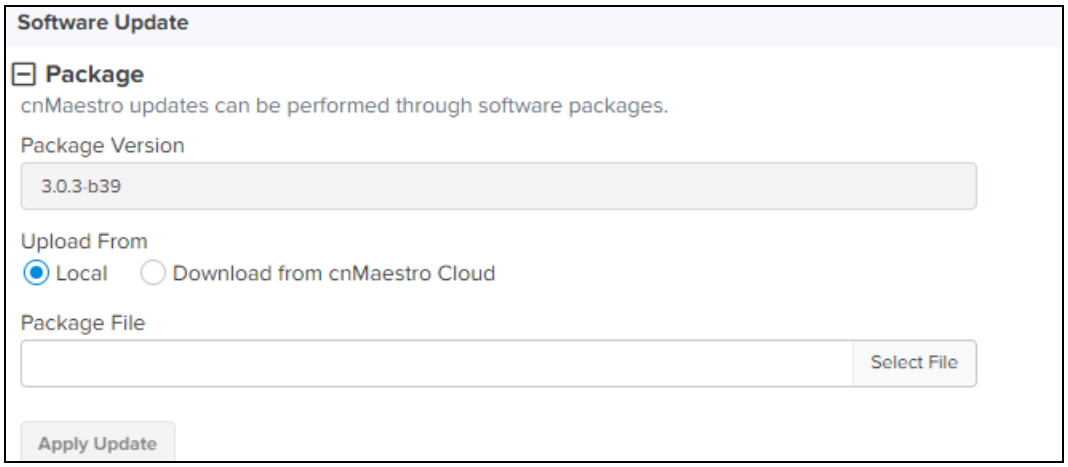
The basic UI allows the user to upload a new OVA, and install it. This process is used for both standalone and HA installations. The Software Upgrade can be done through OVA or package.

Package Upgrade

1. Navigate to **Administration > Server > Operations > Software Update**.
2. Click **Package**.

3. Browse and select the "cnmaestro-package_2.5.0.tar.gz file". You can upload the file from **Local** or **Download from cnMaestro Cloud.**
4. Click **Apply Update** or **Download and Apply.**

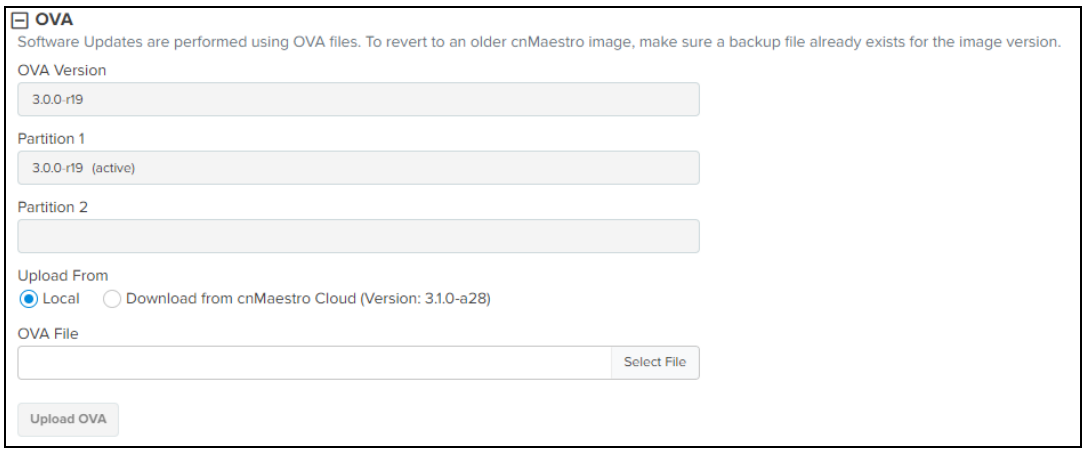
Figure 171 Package Upgrade



OVA Upgrade

> **NOTE:**
>
> Ensure to have minimum of 1 GB free RAM in the cnMaestro On-Premises server for the OVA to upgrade successfully.

1. Navigate to **Administration > Server > Operations > Software Update**.
2. Click **OVA**.
3. Browse and select the "cnmaestro-on-premises_3.0.0-b30_amd64.ova" file. You can upload the file from **Local** or **Download from cnMaestro Cloud.**



4. Click **Upload OVA**. or **Download OVA**. After upload it will progress with Staging.

OVA Upgrade Using CLI

1. Copy the OVA file into the location "/srv/storage/tmp"
2. Execute the command **sudo /srv/bin/sudo cnmaestro-image stage /srv/storage/tmp/<OVA file name>**
3. Staging Status can be verified in UI under **Server** > **Operation** > **OVA**.

In the CLI, it can be verified by executing the command sudo /srv/bin/cnmaestro-image status

If you are unable to apply the upgrade OVA using the UI, there is a command line mechanism that can be used as a failsafe. See **Appendix > Maintenance > Command Line Alternatives > Apply OVA Upgrade** for more details.

Diagnostics

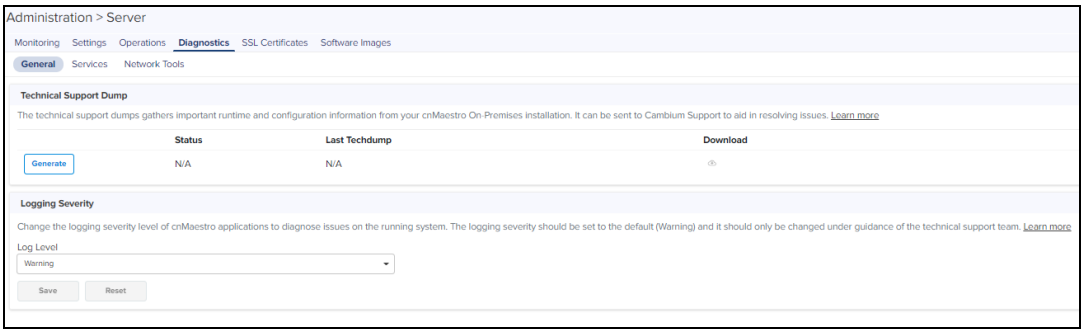
This section provides the following details:

- Server Technical Support Dump
- Logging Severity
- Services

Server Technical Support Dump

The technical support dump gathers important runtime information on the cnMaestro instance. It is accessed at **Administration > Server > Diagnostics** and can be used by Cambium Networks Support to aid in resolving issues.

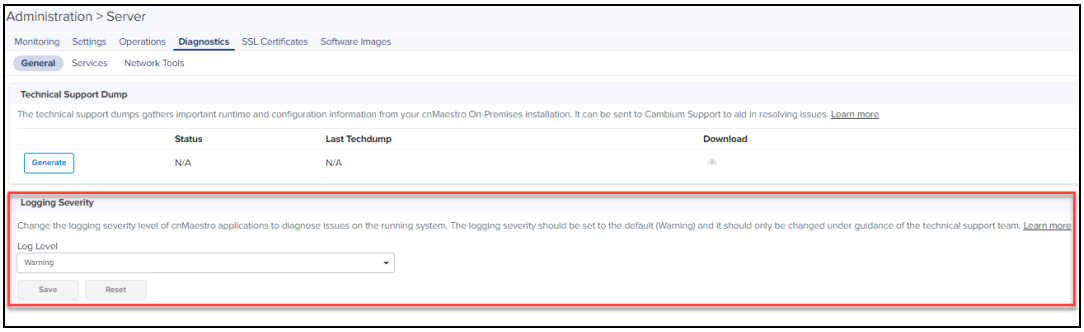
Figure 172 Technical Support Dump



Logging Severity

Change the severity level of the messages logged by the cnMaestro system. These messages are not accessible directly, but can be downloaded as part of the Technical Support Dump. The Log Level Severity can be changed at runtime and it does not require reboot of server to take effect.

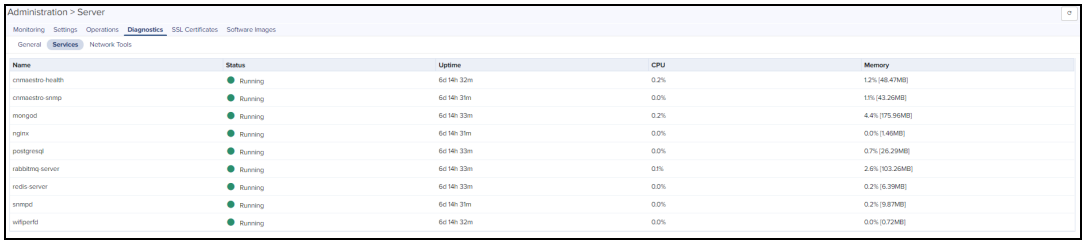
Figure 173 Logging Level



Services

Real time display of the status of critical cnMaestro services.

Figure 174 Services



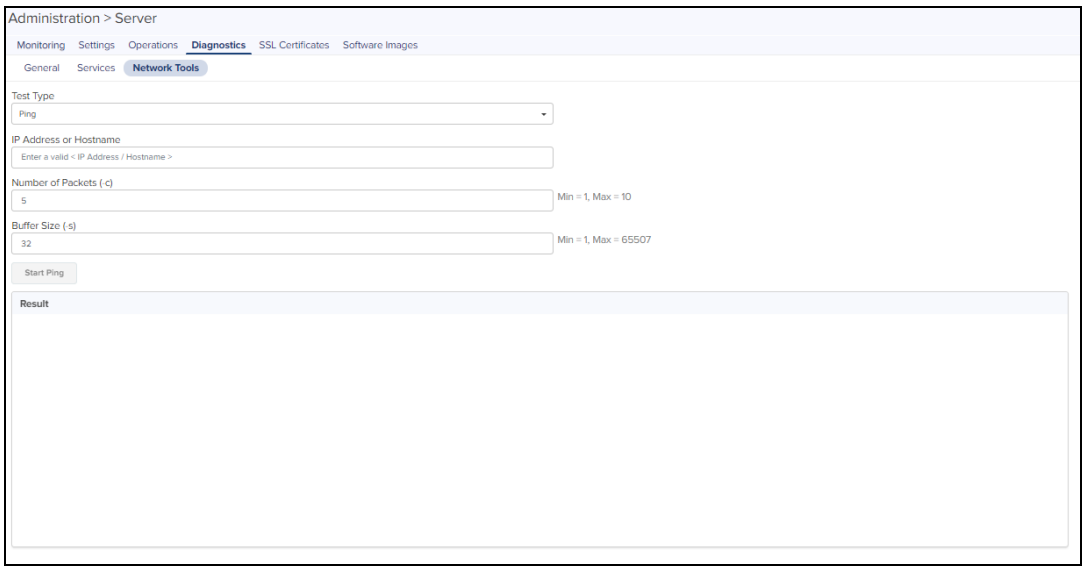
Network Tools

The Network Tools page consolidates a number of operations that can be performed on cnMaestro On-Premises. The operations are listed below:

Table 59: Network Tools

Tools	Description
DNS Lookup	Lists the DNS records for a domain in priority order.
Ping	Network ping to a hostname or IP address.
Traceroute	Lists the hosts or IP addresses showing the route of the test packets starting from the selected monitoring location to the destination Domain or IP.

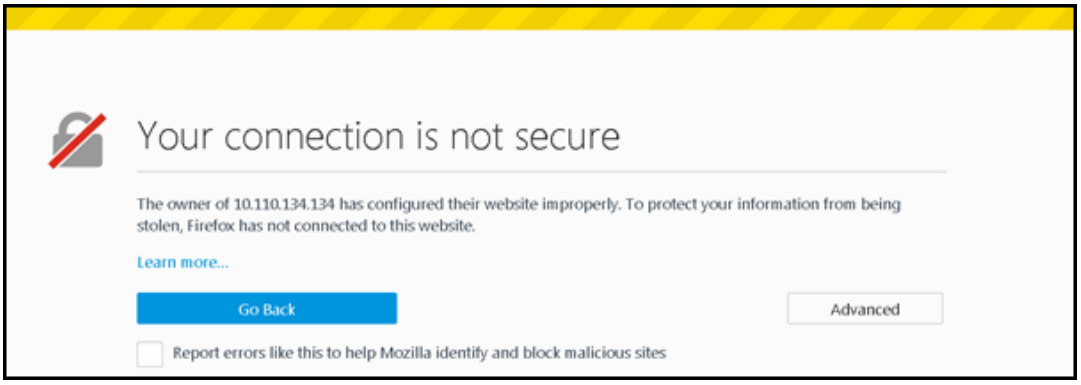
Figure 175 Network Tools



SSL Certificate

cnMaestro On-Premises generates a self-signed certificate when it boots the first time. Because the root CA is not present in standard browsers, cnMaestro users (administrators or Captive Portal customers) receive an SSL error message as shown below:

Figure 176 SSL Error Message



Certificate Management

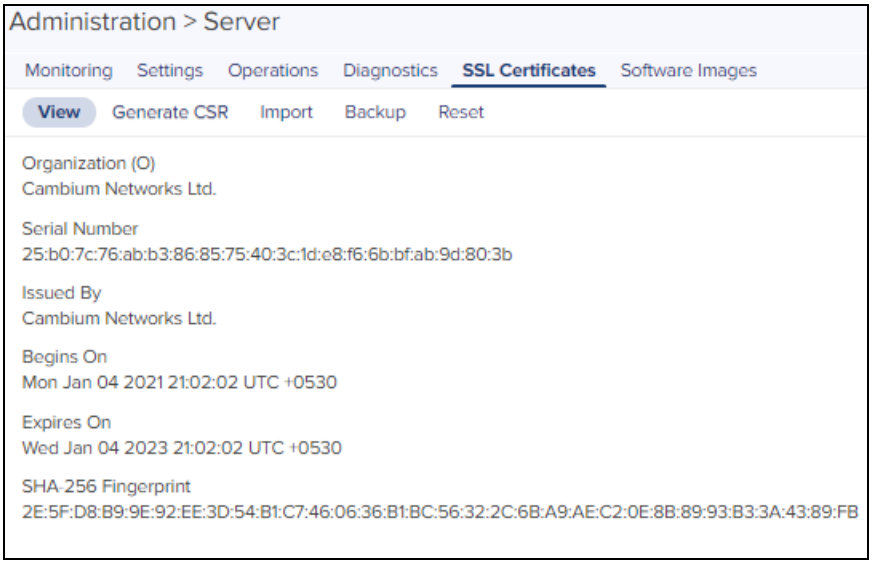
To fix the browser error, cnMaestro needs to host a certificate from a trusted certificate authority, and map the FQDN (fully qualified domain name) used to access cnMaestro. This requires the administrator to export a CSR (Certificate Signing Request) and import the signed Certificate back into cnMaestro.

The following options are available to manage the certificates:

- View Certificate
- Generate a Certificate Signing Request (CSR)
- Import a Certificate
- Backup Management
- Reset

View Certificate

To view the certificate details, click **View** tab.



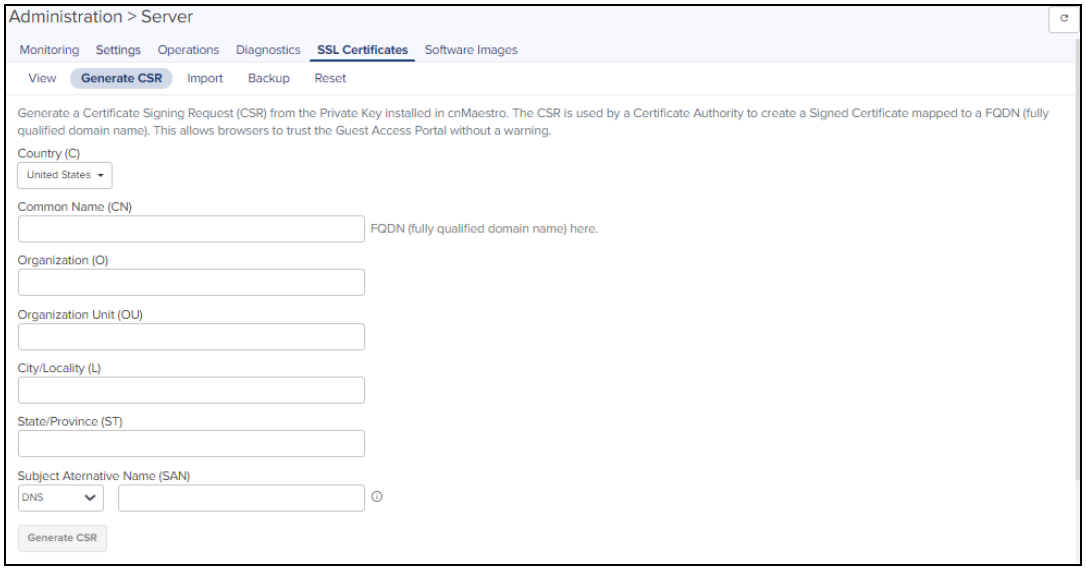
Generate a Certificate Signing Request (CSR)

A certificate-signing request leverages the current Private Key and exports a CSR that can be forwarded to any Certificate Authority.

To generate a CSR:

1. Navigate to **Administration** > **Server** > **SSL Certificates**.

2. Select **Generate CSR** tab.



3. Specify the parameters as in the below table:

Table 60: Configuring CSR Parameters

Parameter	Description
Common Name	Enter FQDN name of the cnMaestro server. This is either the Domain Name or the IP Address.
Organization (O)	Enter the name of the organization.
Organization Unit (OU)	Enter the name of the organization unit.
City/Locality (L)	Enter the name of the city.
State/Province (ST)	Enter the name of the state.
Subject Alternative Name (SAN)	Enter DNS or IP Address.
Country (C)	Select the name of the country from the drop-down list.

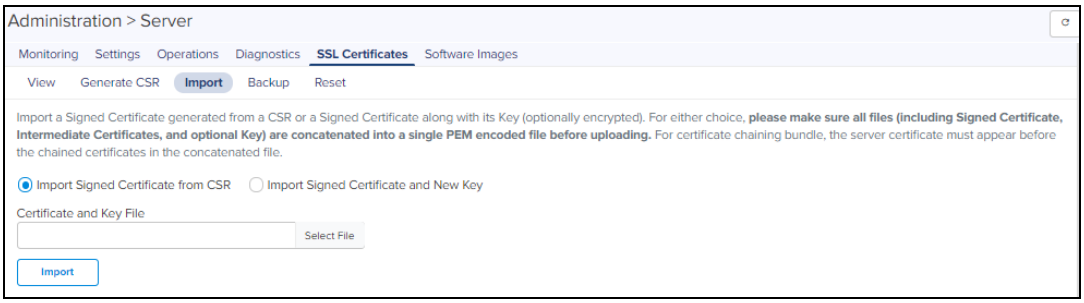
4. Click **Generate CSR**., the user is prompted to save a cnMaestro .csr file to their hard drive. The CSR can then be sent to a Certificate Authority and signed.

Import a Certificate

Once the CSR has been transferred to the Certificate Authority to create a certificate, it can be imported back into cnMaestro. cnMaestro will validate the certificate maps correctly to the stored Private Key, and disallow the import if incorrect. Alternatively, the user can append the Private Key to the Certificate file in PEM format and upload both if certificate and key is generated outside cnMaestro. User can also provide password optionally if key is generated with the password. This will replace both the Certificate and Key on cnMaestro.

To import a certificate:

1. Click **Import** tab.



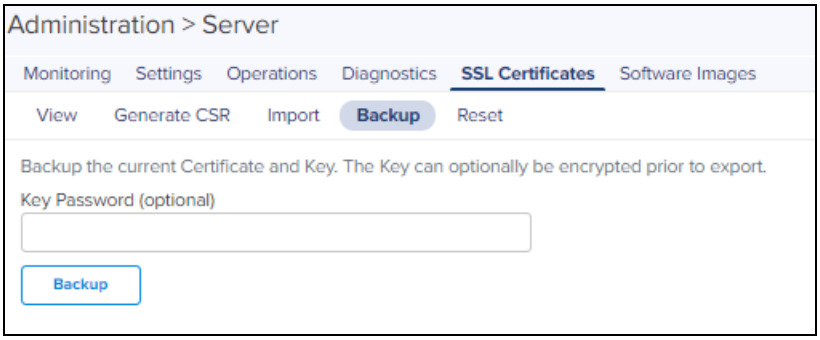
2. Select any one of the below options:
   a. Import signed Certificate from CSR
   b. Import signed Certificate and new Key
3. Browse and upload the Certificate and Key file.
4. Click **Import**.

	The Certificate, and any optional intermediate certificates should be appended and stored in a single PEM-encoded file prior to submission. The signed Certificate should be positioned at the top of the file, followed by any intermediate certificates.
	When importing a Certificate and Key, a single PEM-encoded file should be submitted with entries in the following order: Certificate, intermediate certificates, and Key. If the Key is encrypted, a password should be provided in the textbox on the UI at the time of import.

Backup Management

cnMaestro generates a 4096-bit Private Key when it boots up. This section allows the customer export this Key and current Certificate for backup. These will be exported as a single file, and the Key can optionally be encrypted with a password. To backup the certificate and the key:

1. Click **Backup** tab.



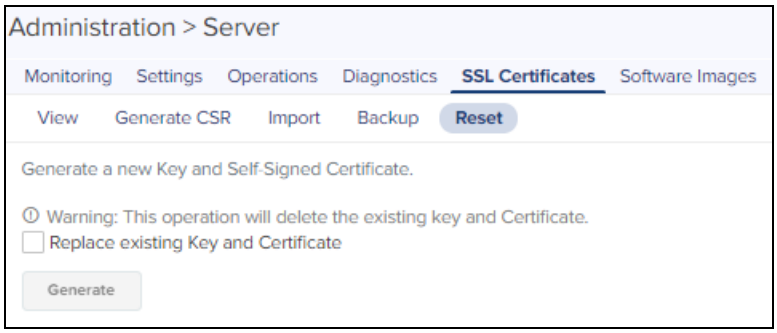
2. Enter the password for the key in the Key **Password** texbox.
3. Click **Backup**.

Reset

It replaces the current Private Key and Certificate and recreates them from scratch. The Certificate is self-signed, and it can be replaced using the Certificate import mechanism detailed above.

To generate a new private key:

1. Click **Reset** tab.



2. Select the **Replace the existing Key and Certificate** checkbox.
3. Click **Generate**.

Manage Software Images

This section provides the following details:

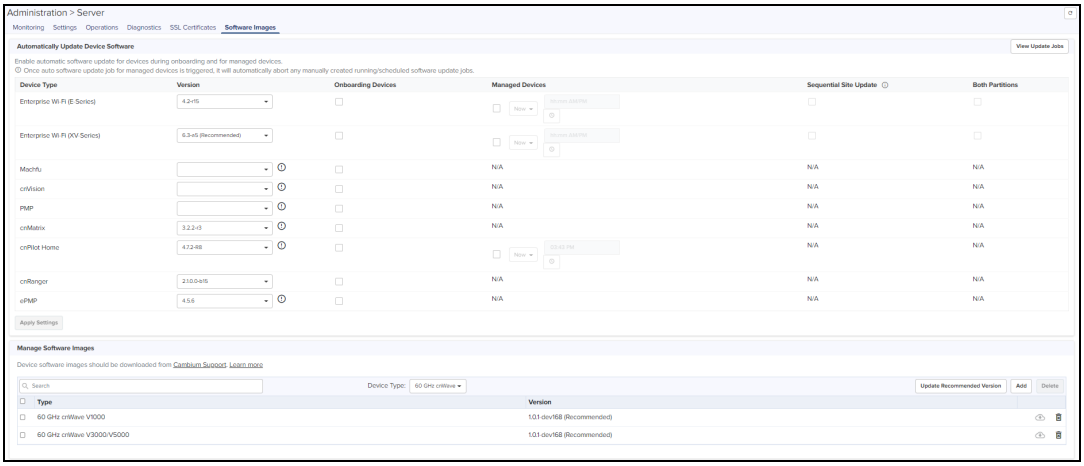
- Overview
- Automatically Update Device Software

Overview

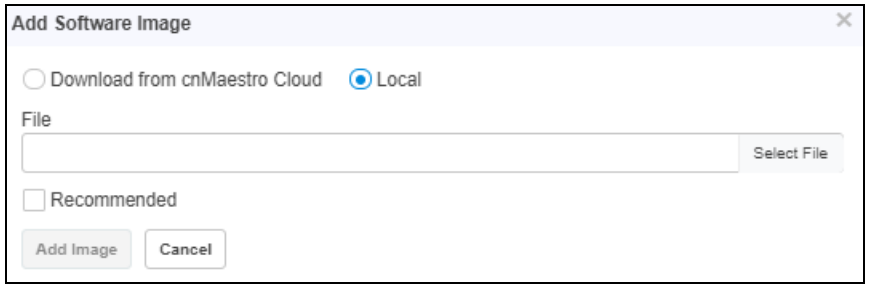
cnMaestro On-Premises allows one to add new device software images as they are released by the device teams. Adding new device software is a manual process: one needs to first download the images from the Cambium Support Center and then upload them into cnMaestro.

The steps are shown below for local upload:

1. Navigate to https://support.cambiumnetworks.com/files and download the device image to your laptop.
2. In the cnMaestro On-Premises UI, navigate to **Administration** > **Server** > **Software Images** tab.



3. Select the image file and then click **Add** button.
4. Add Software Image window pops-up



5. Once file is successfully uploaded to the server, it will appear in the grid.

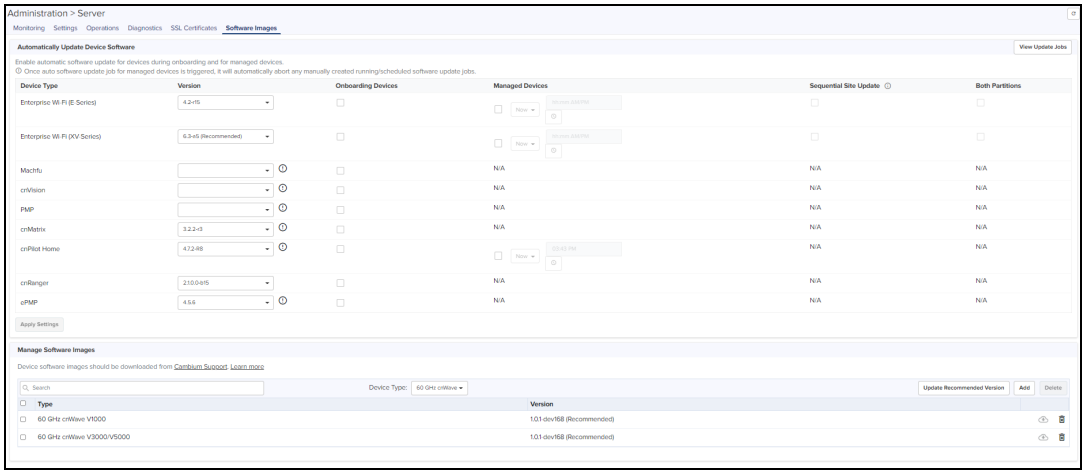
> **NOTE**
>
> cnMaestro uses the name of the uploaded file to determine the version and device type. Please do not change the file name during the upload or download process.
>
> All the check box will be disabled by default.

Add Images

Once the On-Premises server is synced with the cloud, the user can upload the software images from cloud directly to the On-Premises.

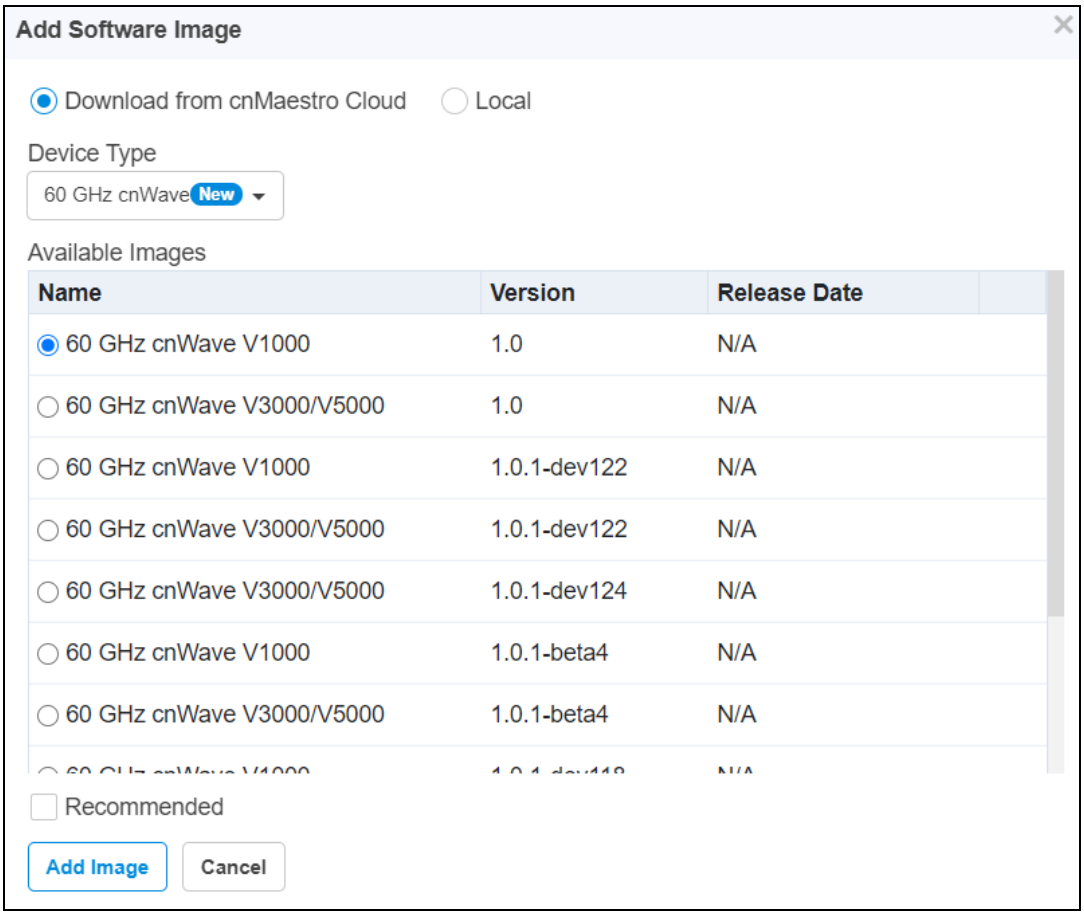
To upload Software Image perform as follows:

1. Navigate to **Administration > Server > Software Images.**



2. Click **Add Image.**
3. **Add Software image** window appears.

- If the On-Premises account has onboarded to any anchor account in cloud.
  a. Click **Download from cnMaestro Cloud,**
  b. Select **Device Type**.



c. Select the Version and

d. Click **Add Image.**

- If the On-Premises account is not onboarded to any anchor account in cloud.

a. Click **Local**.



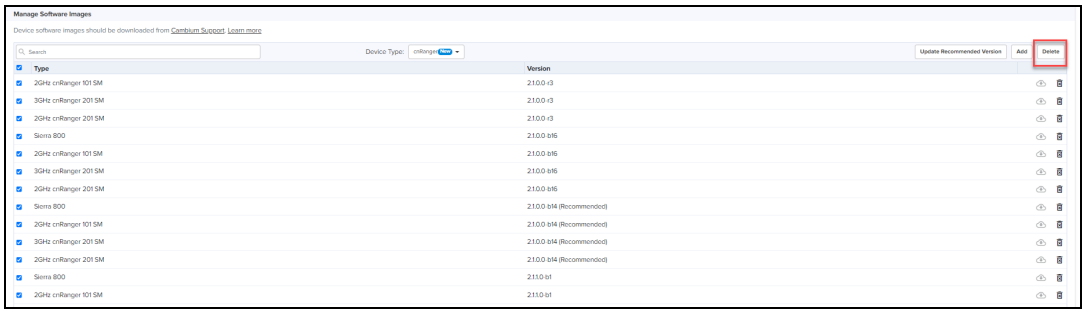
b. **Select File** from the local desktop.

c. Click **Add Images**.

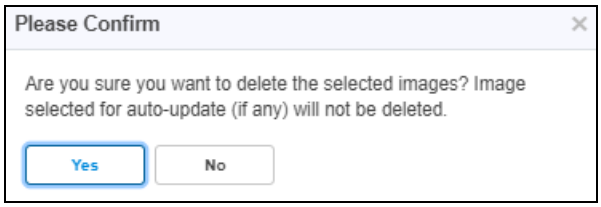
Delete Images

To delete Software Image perform as follows:

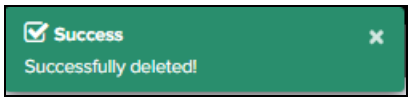
1. Navigate to **Administration > Server > Software Images.**



2. Select the images to be deleted and Click **Delete.**
3. Click **Yes** in Please confirm window to delete the images.



4. It will display the Success message as shown below:

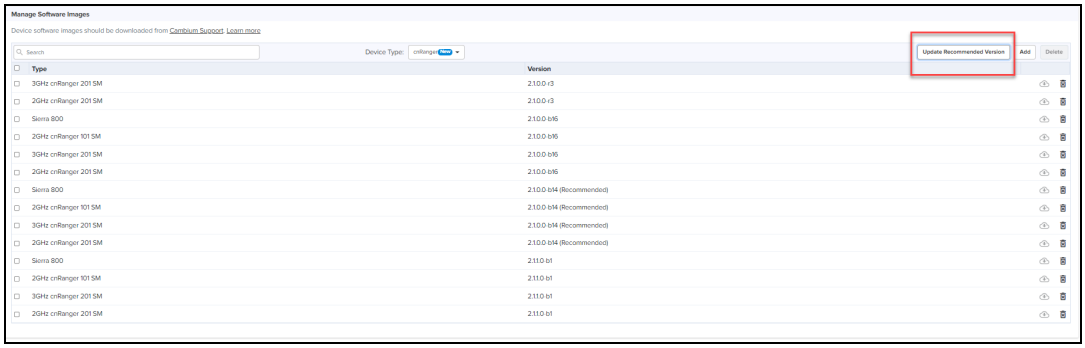


Update Recommended Version

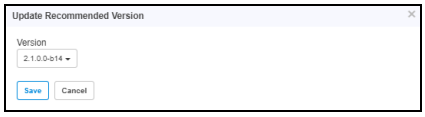
Update recommended version allows the user to update the Version with the recommended version available from the drop-down.

To update recommended version perform as follows:

1. Navigate to **Administration > Server > Software Images.**



2. Click **Update Recommended Version** and window pops-up**.**



3. Select the **Version** from the drop-down and click **Save.**

Automatically Update Device Software

cnMaestro Cloud allows one to update the device software during onboarding and for managed devices.

Adding update device software is a manual process as follows:

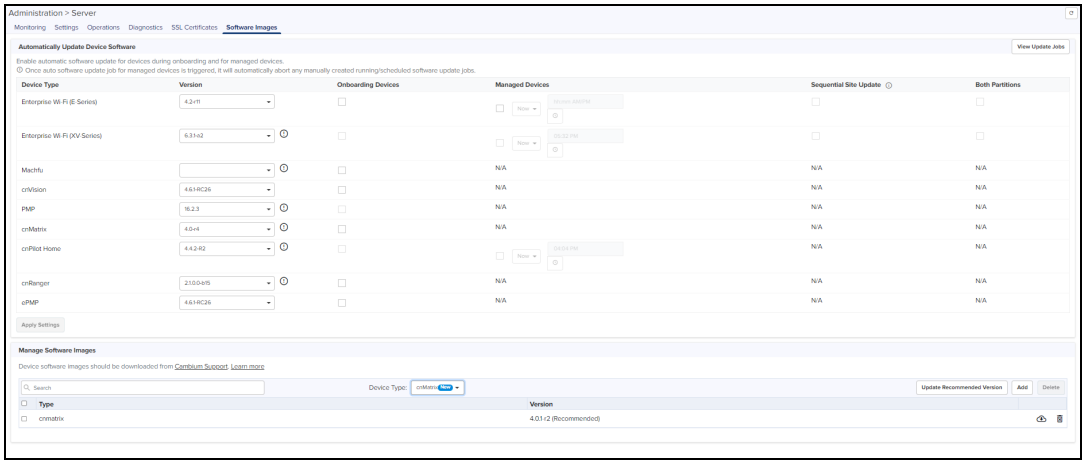
1. Navigate to **Administration > Server > Software Images > Automatically Update Device Software** tab.
2. Select the version file and then click **onboarding/Managed Devices**.

	NOTE: Enable the onboarding check box, to avoid the failure of onboarding devices with minimum supported version rather than the recommended version.

3. Enable the checkbox as follows:
   - Enable **Managed Devices** flag only for Wi-Fi devices (E series and R series).
   - Enable **Sequential Site Update** and **Both Partitions** flag only for only E-Series and XV-Series devices.
4. Click **Apply Settings.**

	NOTE: • Once auto software update job for managed devices is triggered, it will automatically abort any manually created running/scheduled software update jobs. • To avoid failures in onboarding devices having minimum supported version other than recommended version enable the onboarding checkbox.

Figure 177 Automatically Update Device Software



Webhooks

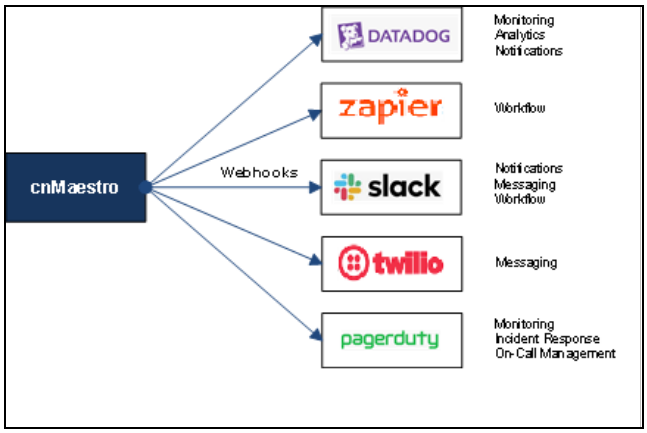
cnMaestro Webhooks provides real-time streaming for alarms using a push notification model. Webhooks data is HTTPS posted to an external Web service. They enable the following benefits:

Benefit	Details
Cloud Friendly	Webhooks are a standard mechanism for Cloud alerts and inter-service asynchronous communication.
Firewall Friendly	HTTPS is generally amenable for outgoing and incoming firewall connections.
Real-Time	Alarms to be sent to third-party services in real-time.
Security	All communication is over HTTPS, and the target domain is validated. Optional security parameters are available for client authentication.
TCP	Webhooks use TCP instead of UDP, so they can alert when the external system is down, or the event was not received.
Third-Party Support	Many Cloud and On-Premises services support Webhooks.

Integrations

Webhooks enable integration with external Cloud services, such as Slack, Twilio, Zapier, Datadog, PagerDuty, etc. They can also be supported using a local HTTPS server and custom applications. Once configured, cnMaestro streams alarms to these services over HTTPS to the configured URL. Some example services are provided below:

Figure 178 Webhook Integration with External Cloud Services



The Webhooks payload is sent in a JSON or a URL-encoded format, and the parameters are comparable to the alarm details present in the RESTful API and email notifications. In addition, cnMaestro also provides default and custom Webhooks templates, so the data format can be tailored to specific services.

Limits

Webhooks are limited to 2 entries per account. In a managed services environment, each managed account can have two Webhooks.

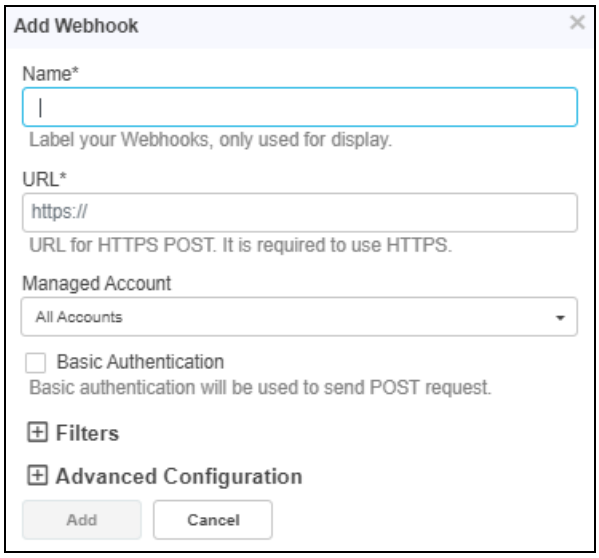
cnMaestro Webhooks Configuration

1. Navigate to **Administration > Settings > Webhook**.



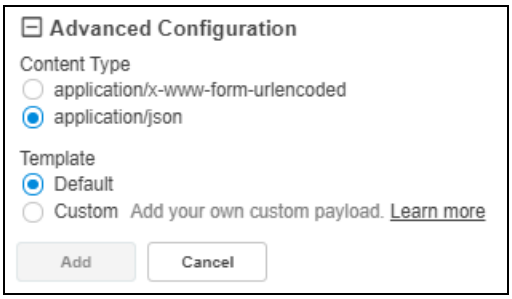
2. Click **Add Webhook**. The following window appears:

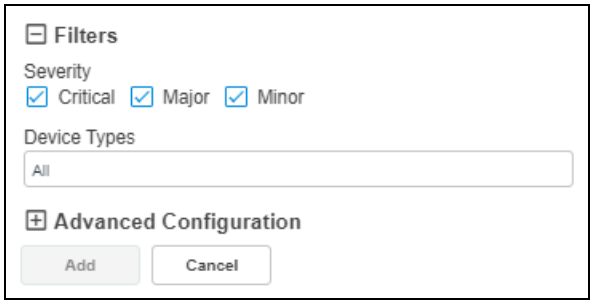
Figure 179 Configure: Add Webhook parameters Page



3. Enter the parameters as shown in the below table.

Table 61: Add Webhook parameters

Parameter	Description
Advanced Configuration - Content type and Template	You can choose content-type as JSON or URL-Encoded Form. cnMaestro supports default and custom templates for the payload. Custom templates allow specialized payload formats. Enable the Custom checkbox and upload your own custom payload JSON. Details on templates are presented later. The Webhooks JSON payload follows the same format as the cnMaestro RESTful API, with a few additional Webhook-specific variables/keys. 
Basic Authentication	Optionally add HTTPS Basic Authentication to the Webhook POST request. By enabling Basic Authentication, you can configure the username and password associated with your endpoint. The Basic Authentication parameters are Base64 encoded and included in the header of HTTP request. Note 1: The username and password for Basic Authentication are different from cnMaestro user credentials. These credentials are used at your endpoint, few external integrations like Slack only require Webhooks URL, for integrations where Basic Authentication is not required. Note 2: Basic Authentication is an HTTP standard which that adds an “Authorization: Basic <credentials>” header to the HTTPS POST request. Credentials are Base64 encoded username and password, encoded the following way: Base64(username:password)
Filters	You can filter the alarms based on severity such as Minor, Major, or Critical. You can also select multiple severities. Device type allows to select the particular device from the drop-down.

Parameter	Description
	
Managed Account	If cnMaestro is configured for MSP (Managed Service Provider), you can map the Webhooks to a Managed Account. Note A maximum of two Webhooks can be configured per Managed Account.
Name and URL	Webhooks label for display and filtering purposes. This will also be included in the default payload as Webhook_name. The URL defines the endpoint for the HTTPS POST request. Only HTTPS is supported.
Type	Type of cnMaestro notification to configure Webhook. Note cnMaestro release 2.4.0 supports only alarms as the type for Webhooks configuration.

For example, Configuration Sync Alarm from e500 Device default payload is as shown below:


```
{
  "ip": "10.110.212.130",
  "network": "FR",
  "message": "Failed to push configuration to device",
  "name": "Configuration Sync",
  "severity": "minor",
  "source_type": "wifi-enterprise",
  "Device Model": "cnPilot e500",
  "status": "active",
  "time_raised": "2019-07-29T11:36:35+00:00",
  "site": "lehavre",
  "tower": "",
  "duration": "0",
  "id": "5d3eda434e222e0a28d14372",
  "code": "CONFIG_SYNC",
  "mac": "00:04:56:BB:14:4E",
  "acknowledged_by": "",
  "source": "E500-BB144E-Test-LAB-A",
  "managed_account": "",
  "webhook_retry_count": "0",
  "webhook_timestamp": "2019-07-29T11:36:35+00:00",
  "webhook_name": "cnmaestro_webhook"
}
```

Types of Variables

The following variables can be used to specify your own payload within a custom template. The variables will be replaced with actual values before sending to Webhooks endpoint.

Table 62: Types of Variables

Variable	Description
$ACKNOWLEDGED_BY	Alert acknowledged by
$ALARM_DURATION	Alarm duration (seconds)
$ALARM_ID	Alarm ID (e.g. 9bd4Gc313a4d1e8fie2482df7b77628)
$ALARM_MSG	Alarm message (e.g.: “GPS Sync state changed to Synchronized”)
$ALARM_NAME	Alarm name (e.g.: Configuration Sync)
$ALARM_SEVERITY	Alarm severity (e.g. critical, major, minor)
$ALARM_STATUS	Alarm status (e.g. active)
$ALARM_TIME_RAISED	Alarm raised time (ISO 8601 Date format: 'YYYY-MM-DDTHH:mm:ssZ')
$ALERT_CODE	Alert code (e.g. STATUS)
$DEVICE_MAC	Device MAC address (e.g: AA:BB:CC:DD:EE:FF)
$DEVICE_MODEL	Device Model (e.g: ePMP 1000, cnPilot r201)
$DEVICE_NAME	Device name
$DEVICE_IP	Device IP Address (e.g. 192.168.0.1)
$DEVICE_TYPE	Device type (e.g.Wi-Fi-enterprise)
$MANAGED_ACCOUNT	Managed account name (absent if not mapped to an account)
$NETWORK_NAME	Network name
$SITE_NAME	Site name (note: value will be blank if the device is not under a Site)
$TOWER_NAME	Tower name (note: 'value will be blank if the device is not under a Tower')
$WEBHOOK_NAME	Webhook name
$WEBHOOK_RETRY_COUNT	Retry count (note: only present if Webhook is retried; default is 0)
$WEBHOOK_TIMESTAMP	Webhook sent time (ISO 8601 Date format: 'YYYY-MM-DDTHH:mm:ssZ')

Error and Retransmission

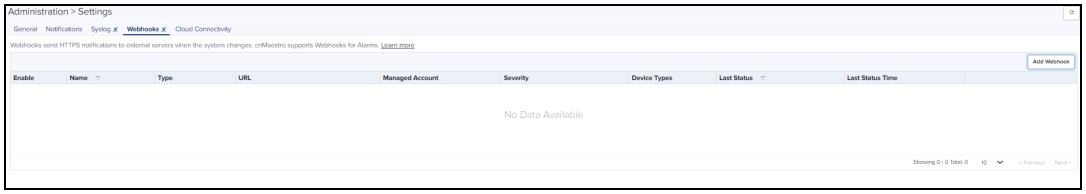
cnMaestro expects an HTTP status code 2XX reply from the Webhooks URL to confirm the alarm notification sent via HTTPS POST that is successfully delivered. For any request, if status code 5XX is received, cnMaestro will keep retrying the same payload at the interval of 1, 2, 5, 10 and every 15 minutes thereafter until the request succeeds. 3XX or 4XX response will not be retried.

	Note If there are multiple Webhooks configured, a retry/error on the one Webhook will not affect the other. For example, if you have Zapier and Twilio, a retry/error on the Twilio will not affect the Zapier, any new alarm notification on Twilio will be discarded and a retry will happen only with the cached payload.

Viewing Configured Webhooks

To view the status of configured Webhooks, navigate to **Administration > Settings** page.

Figure 180 Viewing Configured Webhooks



cnMaestro Webhooks Configuration provide details on the parameters displayed:

Table 63: Webhook parameters

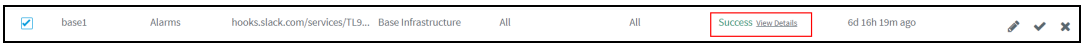
Parameter	Description
Device Type	The Device Type filter on Webhook.
Enable	Select Enable checkbox to enable the Webhook.
Last Status	Last status of Webhook
Last Status Time	Last Webhook send time.
Managed Account	If the MSP Service is enabled, this is the type of account (E.g. All Accounts, Base Infrastructure, or Managed Account Name).
Name	Label to identify the Webhook.
Severity	Alarm Severity filter on Webhook.
Type	Type of notification. (e.g. Alarm).
URL	The URL where HTTPS POST requests will be sent.

Parameter	Description
	Edit the Webhook.
	Send a test message. It can be used to test Webhook's reachability.
	Delete a Webhook.

Status Check

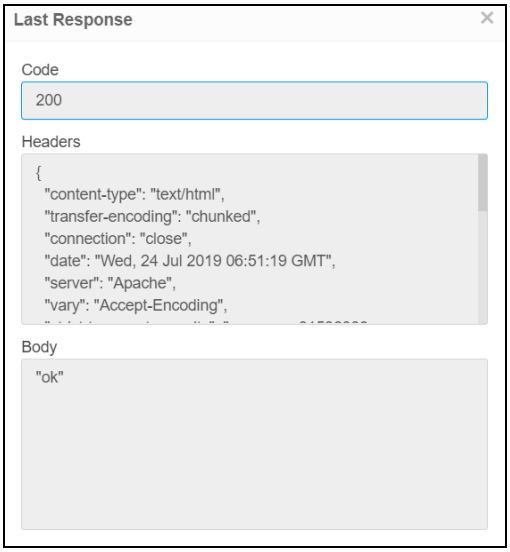
Click **View Details** to check the status of message sent last.

Figure 181 Status check view



View Details displays the response Code, Headers and Body of Webhooks endpoint.

Figure 182 Last response code



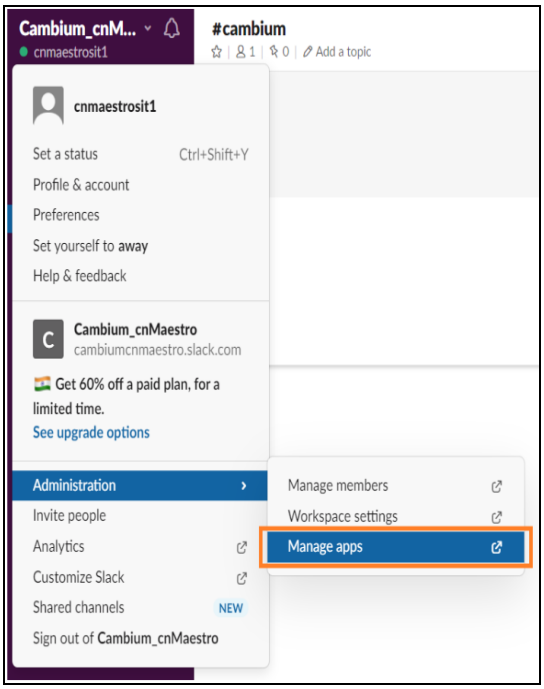
Custom Template Examples

Slack Configuration

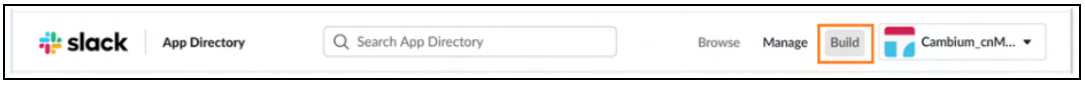
Slack is a platform for team communication, offering instant messaging, document sharing, and knowledge search.

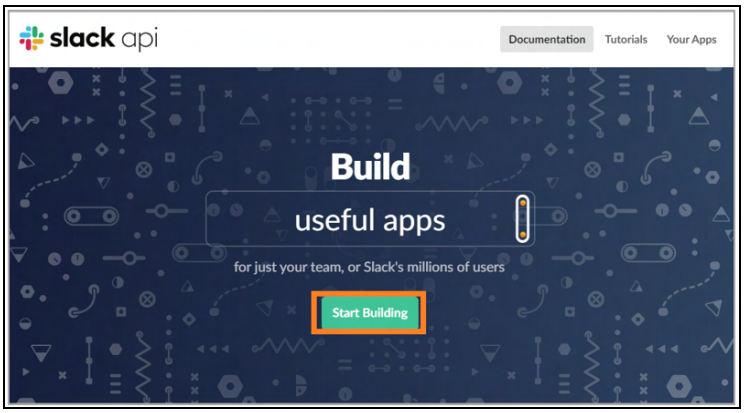
Following is a simple example of configuring Slack integration with cnMaestro Webhooks using a custom Template.

1. On your Slack Screen, click on your workspace name at the top of the left-hand menu and open **Administration** > **Manage** apps.

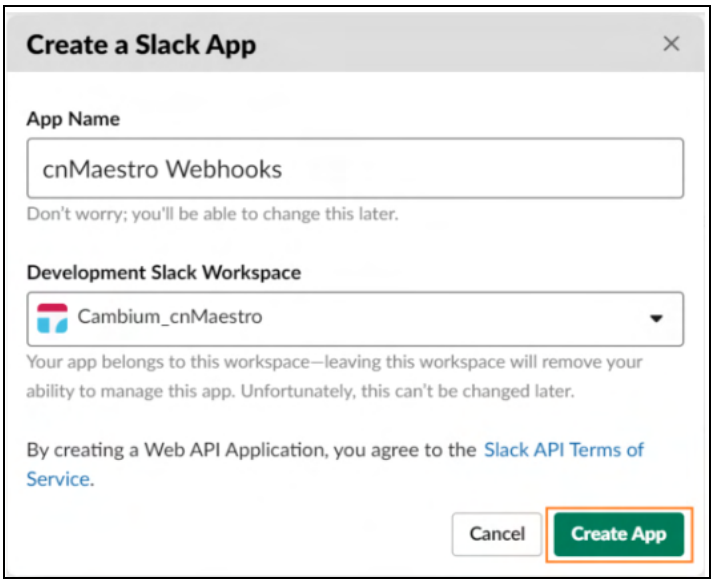


2. In the apps screen, click the Build and then the **Start Building**.

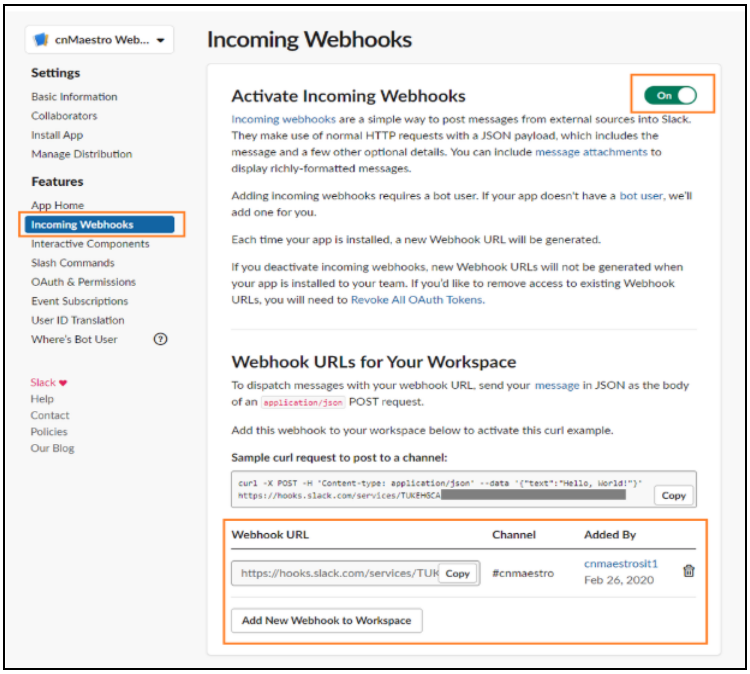




3. In the **Create Slack App** screen, enter an app name of your choice and select your Slack Workspace in the drop-down. Click **Create App**.



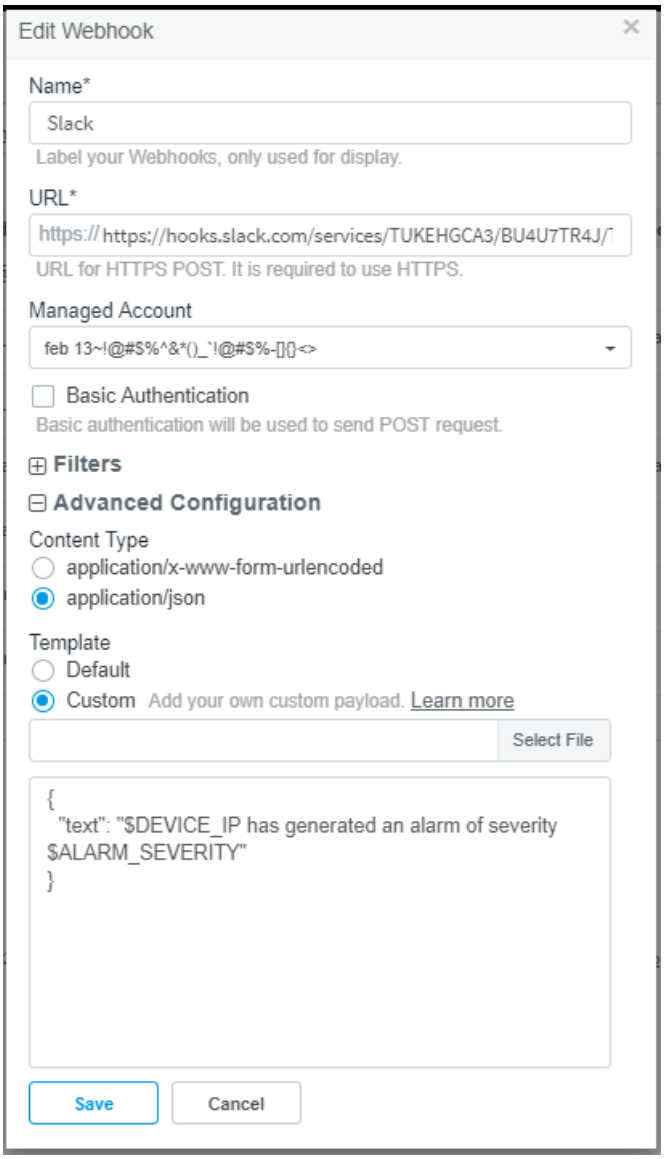
4. In the **Basic Information** tab, select **Incoming Webhooks** from the left menu and create a webhook, providing all the permission and targeted Slack Channel details.



5. From the above screen copy the **Webhook URLs**, which needs to be used as URL in cnMaestro Webhooks in the next steps.

	NOTE Learn more about Slack Webhook and expected JSON format at https://api.slack.com/incoming-webhooks

6. Login to cnMaestro and navigate to **Administration** > **Settings** > **Webhook**.
7. Click **Add Webhook**. Paste the URL from Slack and Expand **Advanced Configuration**.



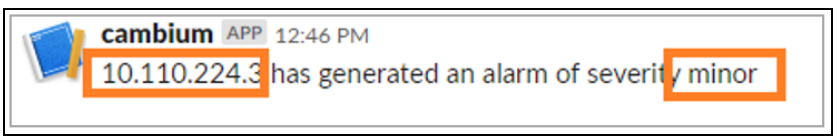
Slack expects a custom JSON payload (https://api.slack.com/incoming-webhooks), The simple one is as follows:

```
{
  "text" : "<message>"
 }
```

For this example, we are using the following custom template with variables $DEVICE_IP and $ALARM_SEVERITY in the formatted message.

```
{
  "text" : "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY"
}
```

8. Once an alarm occurs, the following message appears in the configured Slack channel. Notice the variables have been replaced with actual values.



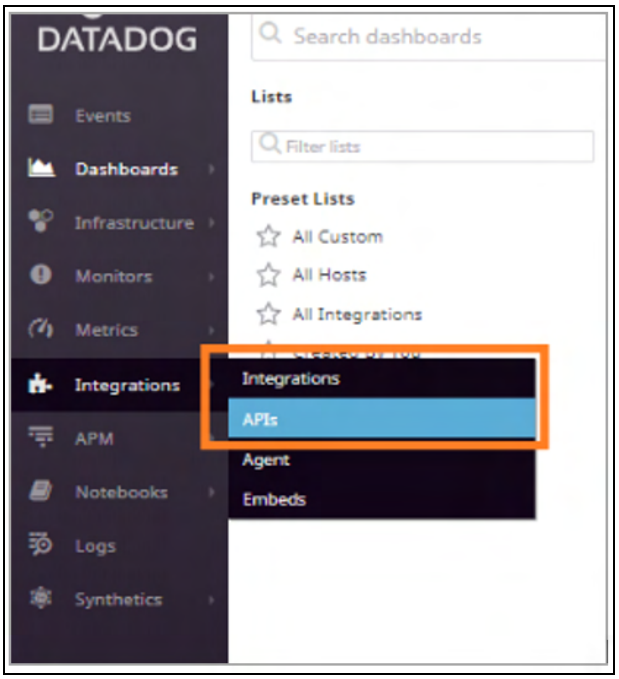
Datadog Configuration

Datadog is a service for IT, Operations and Development teams who write and run applications at scale.

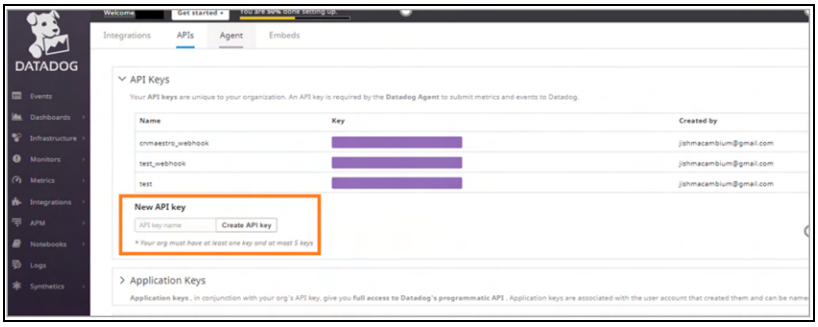
Following is an example of how to create Datadog events using cnMaestro Webhooks and custom templates.

Sign up to https://app.datadoghq.com/signup and set up your Datadog agent. The agent can also be set up outside the cnMaestro UI device.

1. On your Datadog dashboard, navigates to **Integrations** and open **APIs > API keys.**



2. In the API keys, create a new API key and enter a name for the API key created.



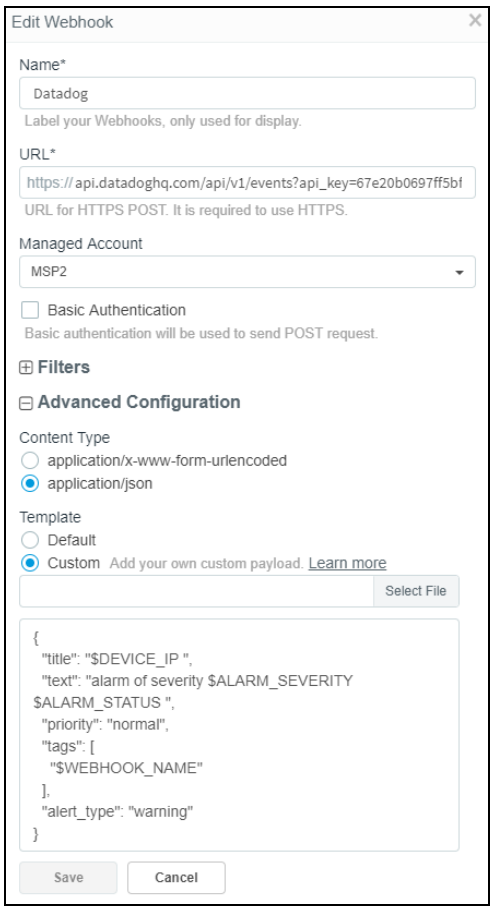
Add the API key to https://api.datadoghq.com/api/v1/events?api_key=<YOUR_API_KEY> , this URL is used as cnMaestro Webhook URL.

3. Datadog expects a custom JSON payload, following is a simple Datadog specific payload format using cnMaestro Webhook variables.

```
{
  "title": "$DEVICE IP",
  "text": "Alarm of severity $ALARM_SEVERITY $ALARM_STATUS",
  "priority": "normal",
  "tags": ["$WEBHOOK_NAME"],
  "alert_type": "warning"
}
```

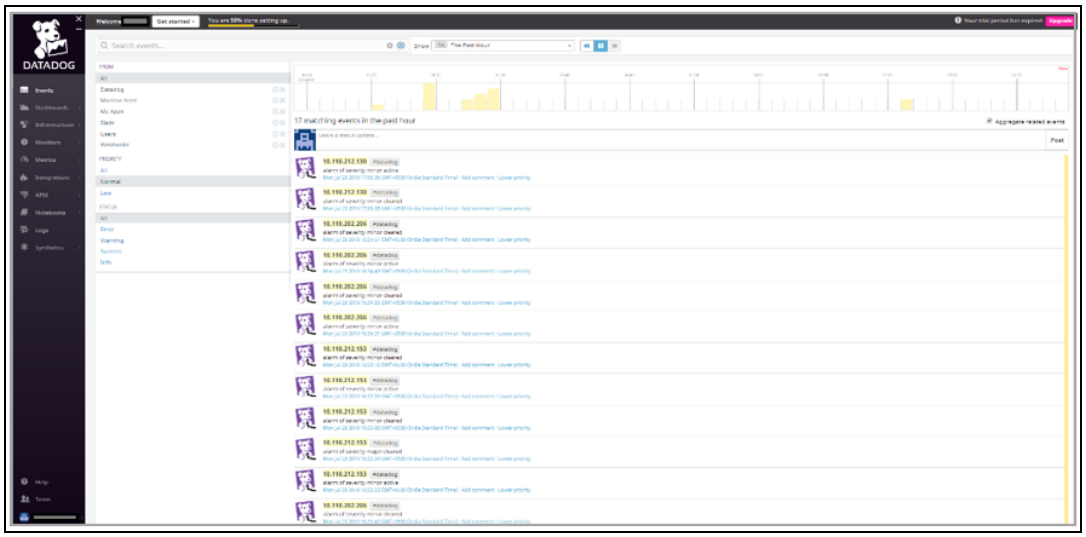
	Note Learn more about Datadog Events and expected JSON format at https://docs.datadoghq.com/api/?lang=bash#events.

4. Login to cnMaestro and navigate to **Administration > Settings > Webhook**.
5. Click **Add Webhook**. Paste the URL from Datadog and expand **Advanced Configuration**.



6. Once an Alarm occurs, the following message appears to configure Datadog events. This can be checked in Datadog dashboard at **Events** > **My Apps**.





PagerDuty configuration

PagerDuty is an incident management platform that provides reliable notifications, automatic escalations, on-call scheduling, and other functionality to help teams detect and fix infrastructure problems quickly.

Following is a simple example of configuring PagerDuty integration with cnMaestro Webhooks. We can use both default or custom templates in JSON and x-www-form-urlencoded content types.

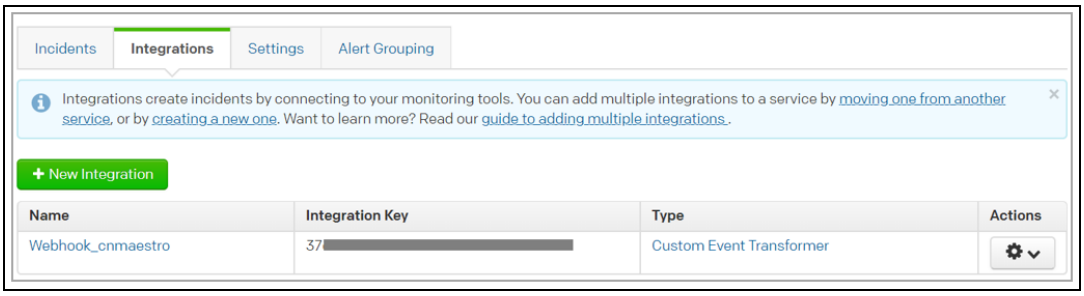
To begin, login to PagerDuty or create a new account.

https://app.pagerduty.com/

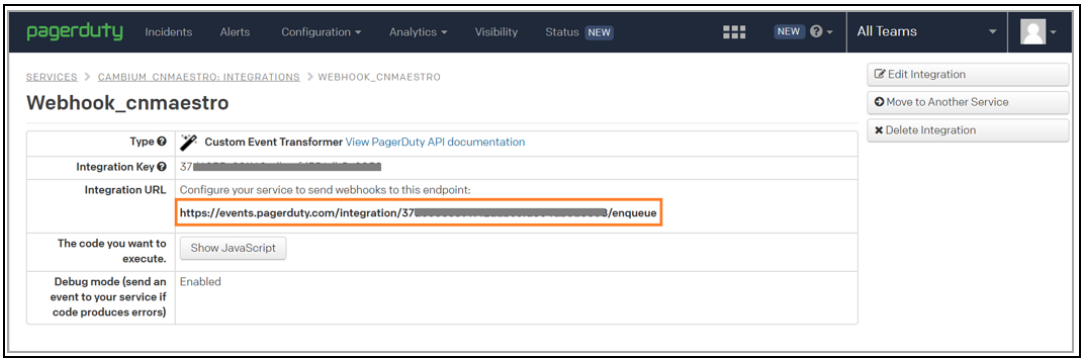
To capture the cnMaestro alarms you need to add a new integration into PagerDuty using a Transformer tool.

After login to your PagerDuty account, to add an integration:

1. Navigate to **Configuration > Services**.
2. If you are creating a new service for your integration, click **Add New Service**. If you are adding your integration to an existing service, click the Name of the service you want to add the integration, navigate to the **Integrations** tab, then click **New Integration**.
3. Select the Integration **Type** as **Custom Event Transformer**. Complete the remaining incident settings as desired and save by clicking the **Add Service/Integration** at the bottom.



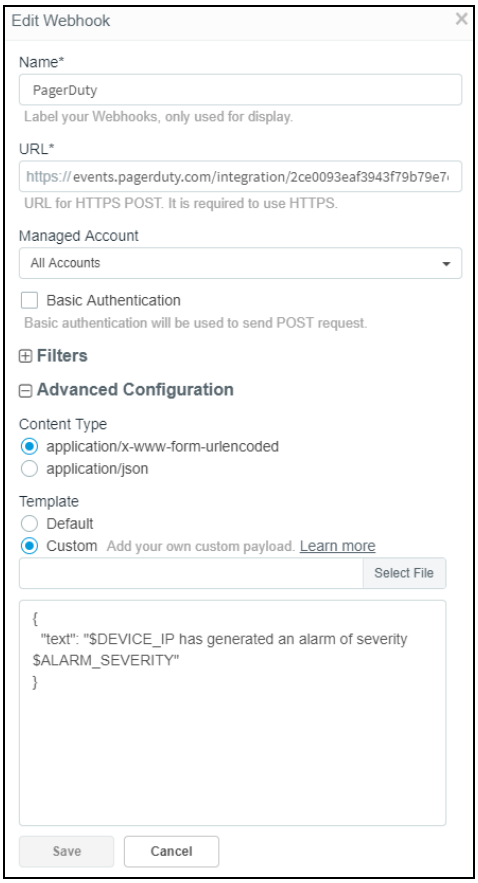
4. Click on the Name of your new integration to view the details.



Integration URL is used in configuration of cnMaestro Webhooks.

https://events.pagerduty.com/integration/<integartion_key>/enqueue

5. Login to cnMaestro and navigate to **Administration > Settings > Webhook**.
6. Click **Add Webhook**. copy and paste the integration URL from PagerDuty and expand **Advanced Configuration**.



You can use the custom payload or default option in cnMaestro. For this example, we are using the following custom template with variables $DEVICE_IP and $ALARM_SEVERITY in the formatted message.

```
{
  "text" : "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY"
}
```

Note

Learn more about PagerDuty and different integrations at https://support.pagerduty.com/docs/webhooks.

7. Once an Alarm occurs, the following message appears in configured service's incidents. Notice the variables have been replaced with actual values.



Twilio Configuration

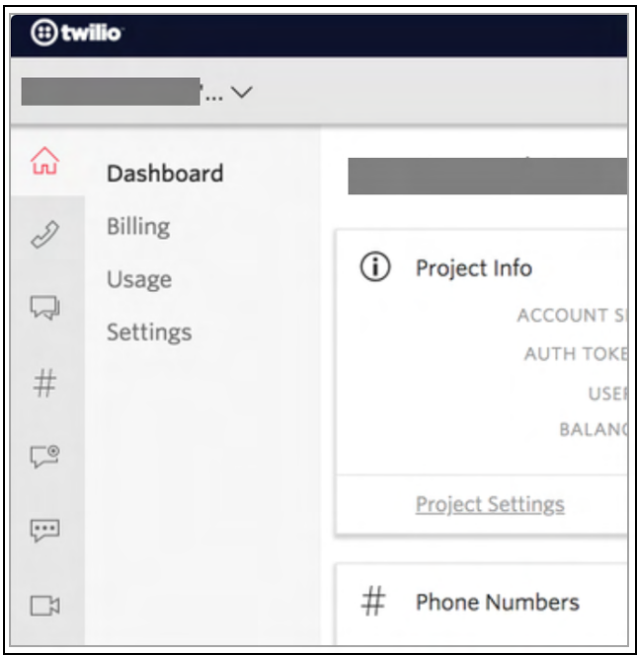
Twilio is a developer platform for communications. Software teams use the Twilio API to add capabilities like voice, video, and messaging to their applications. Twilio is mainly used as an SMS service provider for websites and apps.

Twilio supports HTTP Basic Authentication. This allows you to protect the URLs on your web server so only you and Twilio can access them.

Following is an example of integrating Twilio with cnMaestro Webhooks using an application/x-www-form-urlencoded custom template.

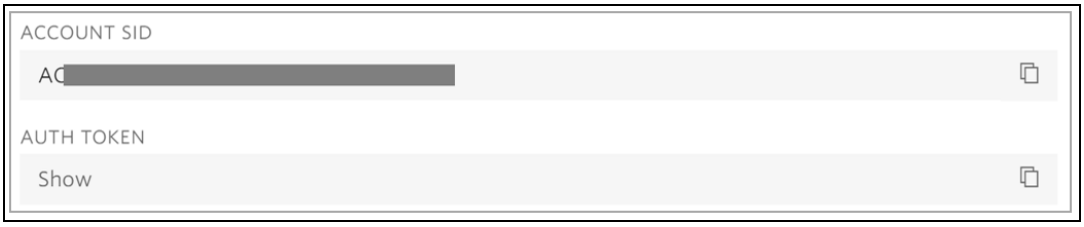
To send a cnMaestro alarm as an SMS directly to a phone, we are going to use the Twilio's API to programmatically send text messages.

1. Login to Twilio or create a new account. https://www.twilio.com/
2. After login to your Twilio account, navigate to your console **Dashboard**.

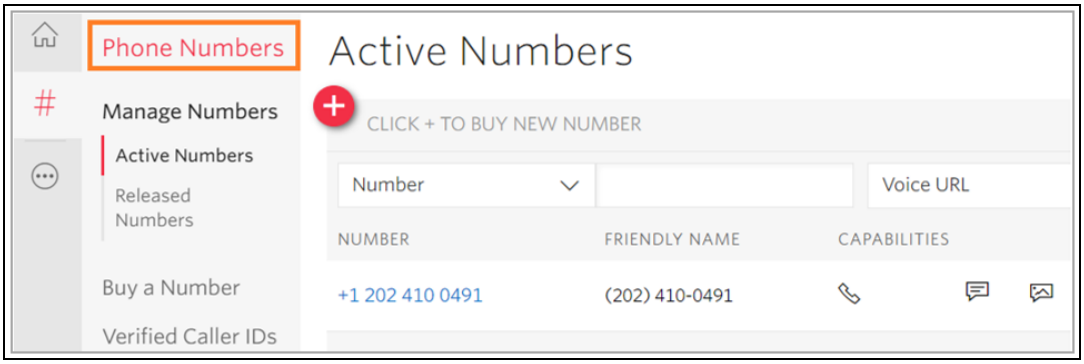


Make a note of the Account SID, Auth Token values on the main twilio.com/user/accountpage – you need it when you configure the cnMaestro Webhooks with Basic Authentication username and password.

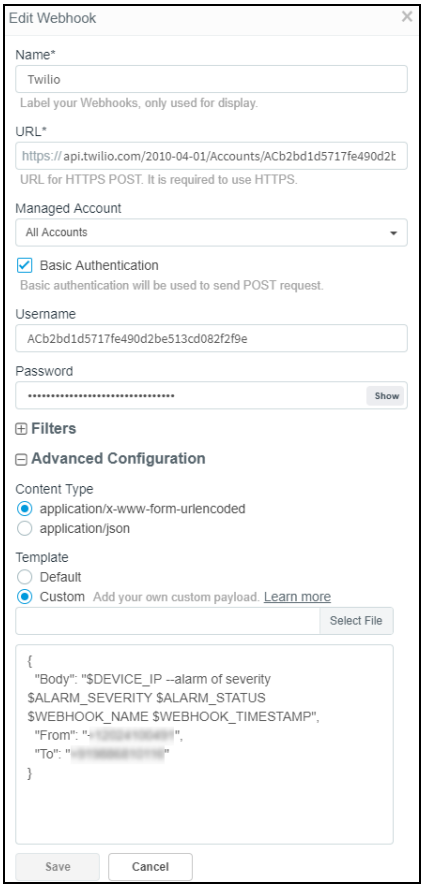
3. Add the **Account SID** to Add the Account SID to https://api.twilio.com/2010-04-01/Accounts/ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/Messages.json, this URL will be used as cnMaestro Webhook URL.



4. Go to **Phone Numbers** under All Products and Services in the console to get the phone number or click on the red plus (+) icon to add a new number and note down the assigned number.



5. Login to cnMaestro and navigate to **Administration > Settings > Webhook**.
6. Click **Add Webhook**. Fill the Account SID and Auth Token from Twilio for URL and Basic Authentication and expand **Advanced Configuration**.



Using the custom payload option in cnMaestro, specify a custom payload adapted to Twilio's format.

```
{
  "Body": "<message>",
  "From": "+<country_code><Twilio_number>",
  "To": "+<country_code><destination_number>"
}
```

For this example, we are using the following custom template with variables $DEVICE_IP and $ALARM_SEVERITY in the formatted message.

```
{
  "Body": "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY",
  "From": "+12024100491",
  "To": "+91**********"
}
```

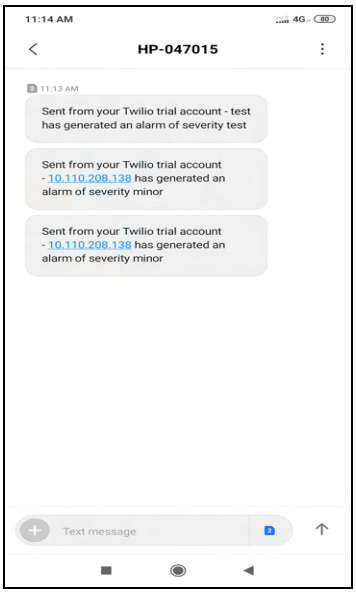


NOTE

To configure Twilio to cnMaestro Webhooks you should use application/x-www-form-urlencoded as content type.

Learn more about Twilio and expected JSON format at https://www.twilio.com/docs/usage/api

7. Once an Alarm occurs in cnMaestro, the following message will be sent to the destination number from the Twilio number. Notice the variables have been replaced with actual values.



Zapier Configuration

Zapier is an online platform that aims to connect various apps together to automate workflows.

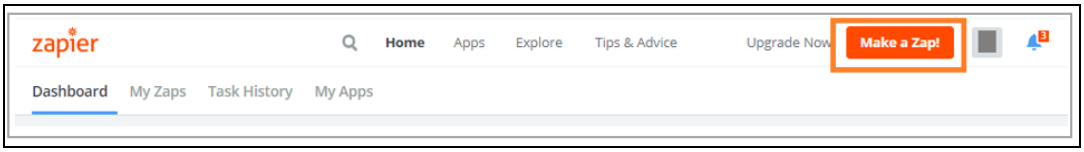
With Zapier you can build Zaps that perform your automation for you. These automations are achieved by mixing a Trigger with actions available on your favourite apps. Zapier supports hundreds of apps. You can mix and match triggers and actions to automate.

Following is an example of configuring Zapier integration with cnMaestro Webhooks. For example, you could make a Zap that would automatically save alarms from cnMaestro Webhooks to a new row on a Microsoft Excel. Zapier can catch a Webhook POST from cnMaestro, automatically adding the information to a new row in Excel.

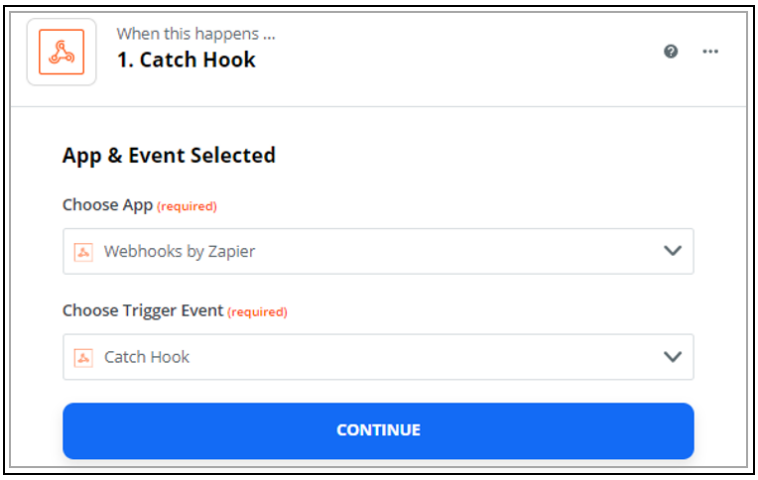
First, Login to Zapier or create a new account.

/https://zapier.com/

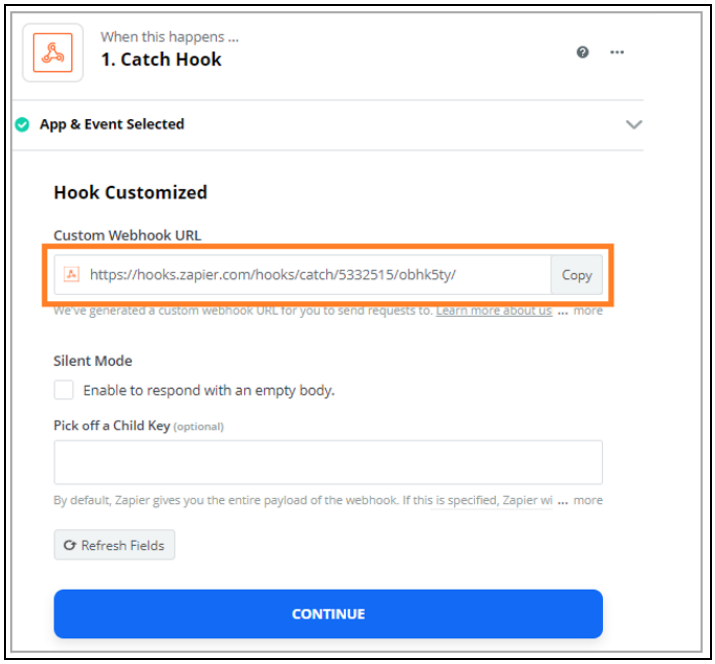
1. After login to your Zapier account, navigate to dashboard.
2. On your Zapier dashboard, click on **Make a Zap** at the top right-hand side.



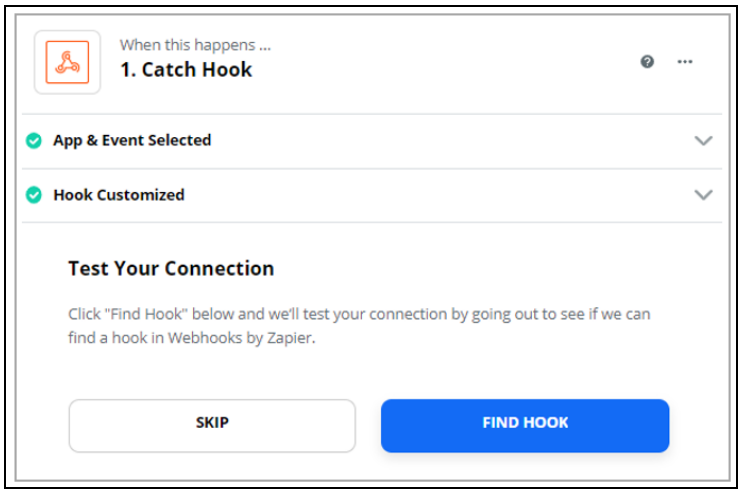
3. Choose **Webhooks by Zapier** and **Catch Hook** as the trigger app and trigger event.



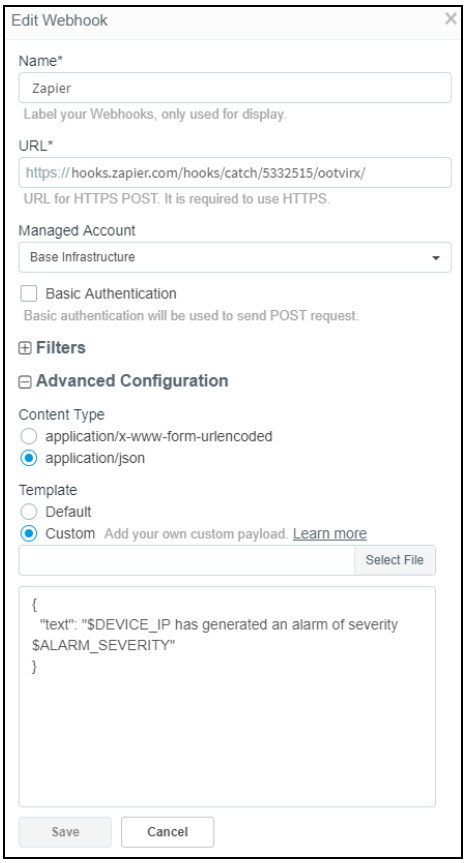
4. To customize your webhook trigger, copy the given URL and configure it in your cnMaestro Webhook.



5. Click continue redirects to **Test your connection** page.



6. To test the connection, open cnMaestro Webhooks and configure the given custom URL from Zapier then can customize and fill the **Advanced Configuration**.



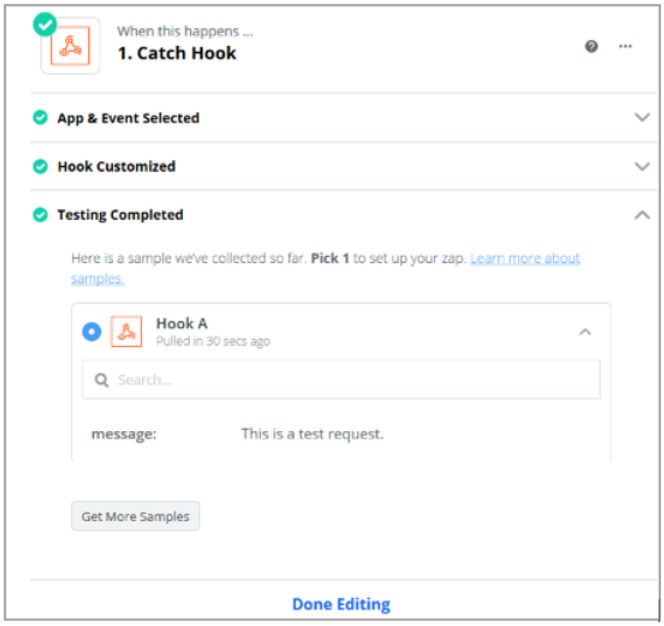
You can use the custom payload or default option in cnMaestro. For this example, we are using the following custom template with variables $DEVICE_IP and $ALARM_SEVERITY in the formatted message.

```
{
  "text" : "$DEVICE_IP has generated an alarm of severity $ALARM_SEVERITY"
}
```

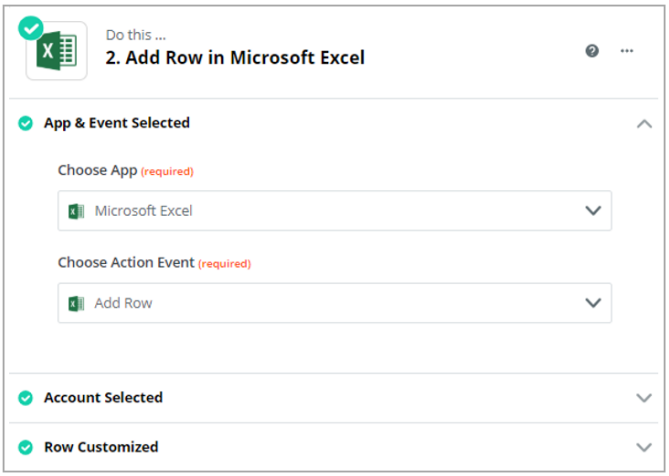
7. Send a test webhook by clicking on the test icon on the right-hand side of the webhook table.



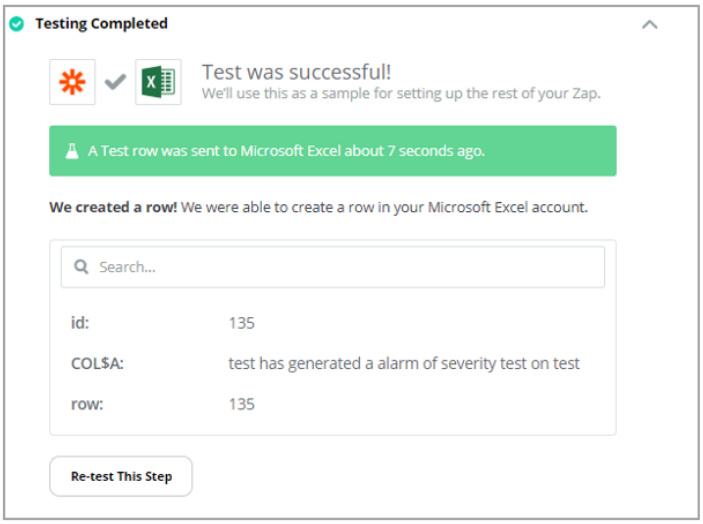
8. Now go back to Zapier and click **Find Hook** to complete the testing.



9. Set up Microsoft Excel as the action for your Zap, action event, connect your excel account and customize.



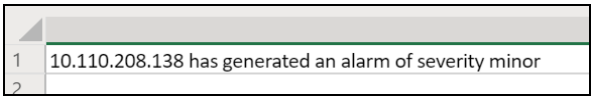
10. To check if your action works as expected. Click **Send Test** to run the action step. The next screen shows whether Zapier has been able to successfully perform the action step or not.



Note

Learn more about how Zapier supports different apps at https://zapier.com/help/.

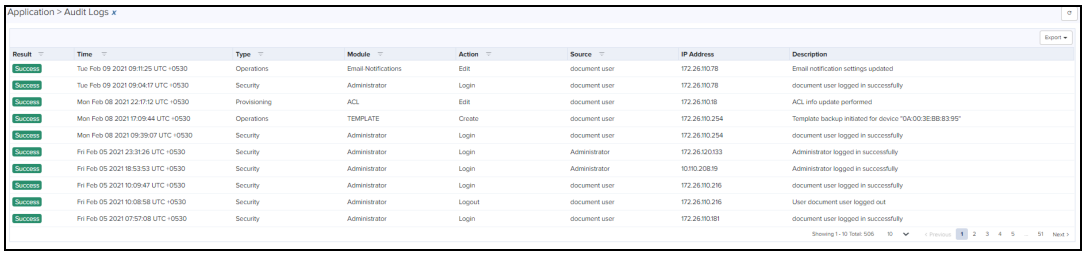
11. Once an Alarm occurs, the following message appears in the configured excel sheet. Notice the variables replaces with actual values.



Audit Logs

Audit Logs record administration activities through both the Web UI and the RESTful API. Audit Log entries usually include destination and source addresses, a timestamp and user login information. User can access Audit Logs in the **Administartion** > **Audit Logs** page.

Figure 183 Audit Logs



The following table describes the Audit Logs parameters and their descriptions.

Table 64: Audit Log Parameters

Parameter	Description
Action	Displays the action performed by the user (create, delete, download, etc.).
Description	Textual description of the task.
Export	Enable export as CSV or PDF.
IP Address	IP address of the Web browser or API application.
Module	Module generating entry (AAA, administrator, alarm).
Result	The result of the audit log as **Success** or **Failed**.
Source	Administrator or API client name.
Source Type	Entity making the update: administrator or API client.
Type	Type of the log entry (configuration, operation, onboarding, security).
Time	The time when the action was performed.

Log Action

An action log contains a set of transactions. Each transaction contains one or more Actions. Each Action has a name and input parameters. Some Actions have output parameters.

The following Actions will be supported for individual Audit Log entries. Each activity performed in the server is detailed in this table.

Table 65: Log Action Parameters

Parameter	Description
Claim	Claim a device in the network operator.
Cloud-Connect	Provides the status of the On-Premises to Cloud account connection.
Create	Create an object in the network device.
Delete	Delete an object in the network device.
Download	Download a file.
Edit	Edit an existing device detail.
Link Test	Perform a Link Test.
Login	Login to a device.
Logout	Logout from a device.
Mail	Mail ID of a device.
Move	Move a device from the server.
Reboot	Reboot a device.
Reset	To reset a device
Upload	Upload a file on the server.

Audit Modules

Auditing activity is mapped to individual modules within cnMaestro. A breakdown of the available modules is listed below.

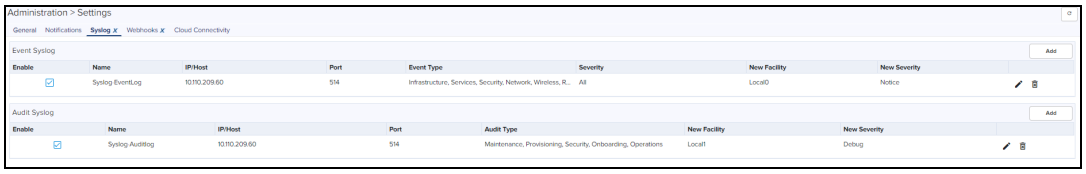
Module	Type (s)	Description
ACL	provisioning	Adding Editing Removing the ACL Entries
Administrator	provisioning operations security	User Management: Login, Users, Roles, Email, etc.
Alarm	provisioning	Alarms and Alarm History.
API	provisioning	API Management: API Clients and Webhooks
Auditing	provisioning	Auditing Infrastructure
Auto-Provision	provisioning	Auto-Provisioning

Module	Type (s)	Description
CBRS	Services	CBRS
Data-tunnel	provisioning	Data Tunneling
Device	provisioning operations	Device management
Guest-Portal	provisioning	Guest Portal
Infrastructure	provisioning	Site, Network, Tower Management
Jobs	provisioning operations	Jobs Infrastructure
License	licensing	Update license details
MSP	operations	Operations covering Managed Services and Managed Account
Onboard	provisioning operations	Onboarding Queue
Report	provisioning operations	Data Reports
Software-Upgrade	provisioning operations	Software Upgrade: device image import/export, upgrade device
SIM	provisioning	SIM claim and delete
System	provisioning operations security	System Services: VM management, change log level, system upgrade, system monitoring, software images, system settings
Template	provisioning	Template-Based Configuration
Tools	provisioning operations	Technical support dump, networking operations, etc.
Webhooks	provisioning	Webhooks configuration and management
Wi-Fi	provisioning operations security	AP Groups, WLANs: edit W-Fi configuration objects

Syslog

cnMaestro supports Notification Syslog (Event Log) and Audit Syslog. The generated Event Logs and Audit Logs are sent to the syslog server configured under **Administartion > Settings** page. Every syslog has a Facility and a Severity level. Maximum of five entries can be added in Notification syslog and Audit syslog.

Figure 184 Syslog



The following table describes the parameters in Syslog server:

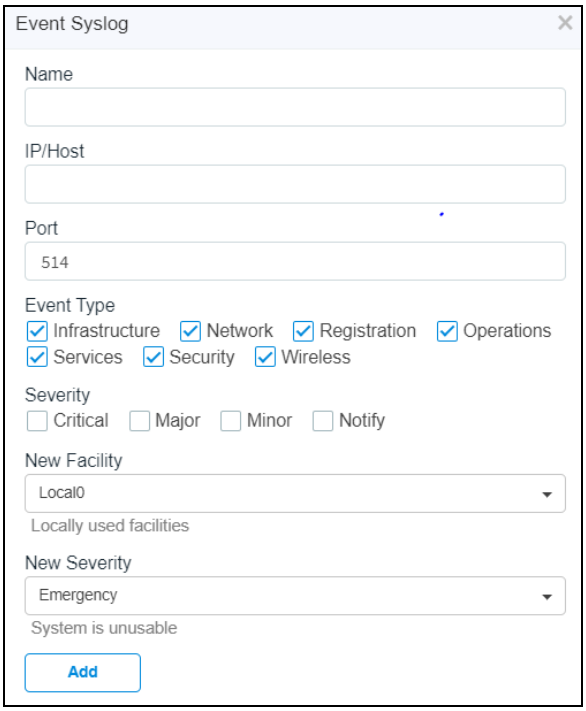
Table 66: Syslog Server Parameters

Field	Description
☑	Enable the notification syslog or audit syslog.
Event Type	The type of event (Infrastructure, Network, Operation, Security and Wireless). You can select one or multiple events.
IP/Host	The IP address provided to the server.
Name	The username provided to the server.
New Facility	The type of program logging the message. The allowed facilities are local 0 to local 7.
New Severity	The severity of the system log message.
Port	IP address or hostname provided to the server.
Severity	The initial severity of the generated syslog messages (i.e. Critical, Major, Minor or Notify).

Event Syslog

Notification messages are filtered based upon Type (which may be slightly different between Events and Alarms) and Severity.

Click **Add** to add a new Event Syslog window pops-up.



NOTE:

At least one Event Type or Severity must be selected.

1. Enter **Name**.
2. Enter the **IP/Host** address.
3. Enter the **Port** number. Port 514 is the default for syslog
4. Select **Event Type**.
5. Select **Severity Type**.
6. Select the **New Facility** from the drop-down list.

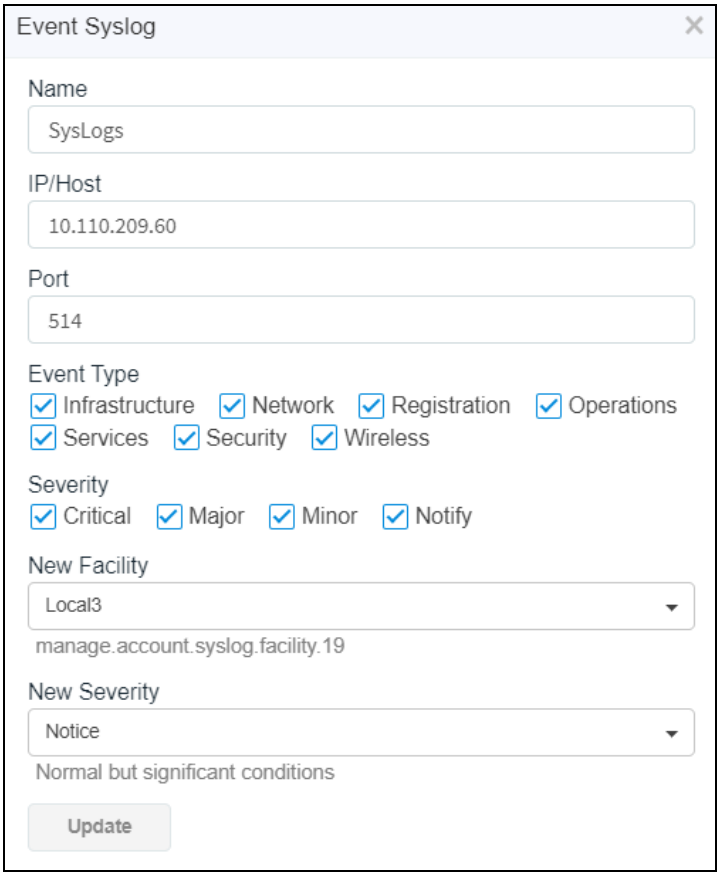
Facility	Description
Local 0-Local 7	It is the locally used facilities.

7. In the **New Severity** drop-down, select the type of Severity. Please refer to the below Severity table:

Value	Severity	Description
0	Emergency	System is unusable.
1	Alert	Action must be taken immediately.
2	Critical	Critical conditions of hard device errors.
3	Error	Error conditions

Value	Severity	Description
4	Warning	Warning conditions.
5	Notice	Normal but significant conditions. Conditions that are not error conditions but may require special handling.
6	Informational	Informational messages.
7	Debug	Debug-level-messages.

8. Click ◪ to edit the Event Syslog. The dialog box appears:

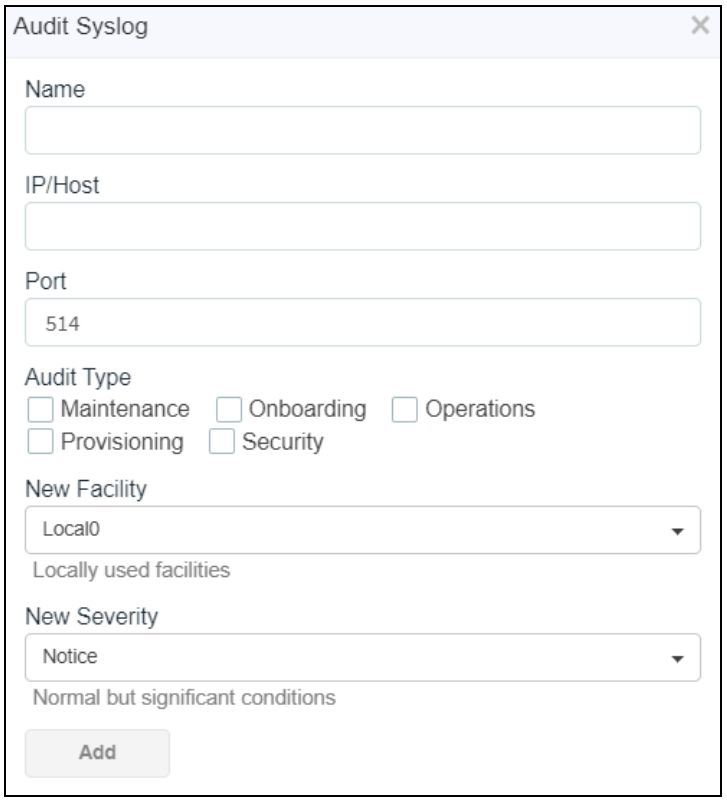


9. Repeat the above steps to update an existing Notification Syslog.

Audit Syslog

The Audit Syslog separates messages based upon Audit Type.

Click Add a new Audit Syslog window pops-up.



NOTE:

At least one Audit Type must be selected.

1. Enter **Name**.
2. Enter the **IP/Host** address.
3. Enter the **Port** number. The port number 514 is the standard syslog port.
4. Filter by **Audit Type**.
5. Select **New Facility** from the drop-down list.

Facility	Description
Local 0-Local 7	Available facilities.

6. Select the type of **Severity**.
7. Click **Add**.

Cloud Connectivity

Overview

Cloud Anchor accounts exist alongside Cloud NMS accounts, which enable device management through cloud.cambiumnetworks.com. Anchor accounts are attached to cnMaestro On-Premises installations and have their own Cambium ID. All new cnMaestro On-Premises 3.1.0 deployments must connect to an Anchor account at installation, and all existing cnMaestro instances will need to connect to an Anchor account before updating to cnMaestro 3.2.0.

The Anchor account collects statistics and automatically pushes announcements of new device firmware and cnMaestro software images. cnMaestro On-Premises reports the following details to the Anchor account:

Type	Details
System	Uptime, Processor, RAM, Disk, Virtualization Vendor
Devices	Count, Type
Application	Software Version, User Types and Count, Account View, Country
Features	MSP, CBRS, Wi-Fi Performance, Auto-Provisioning, SNMP, etc.

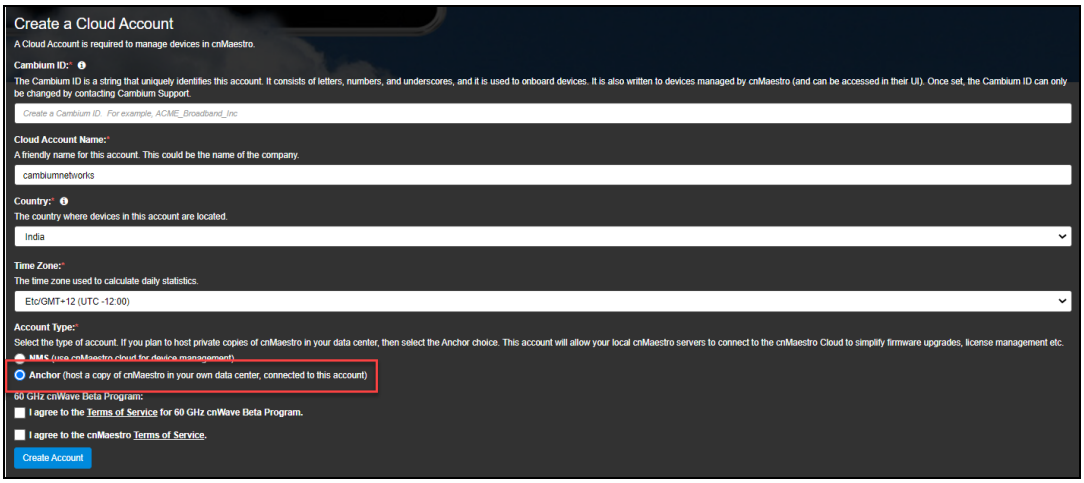
Anchor accounts also simplify CBRS provisioning and billing by aggregating multiple On-Premises instances. In future, Anchor accounts will be used to manage On-Premises cnMaestro X subscriptions.

You must create an Anchor account before connecting the On-Premises instance, as shown below:

1. Navigate to https://cloud.cambiumnetworks.com.
2. Click **Create Account**.



3. In account type, select **Anchor**.

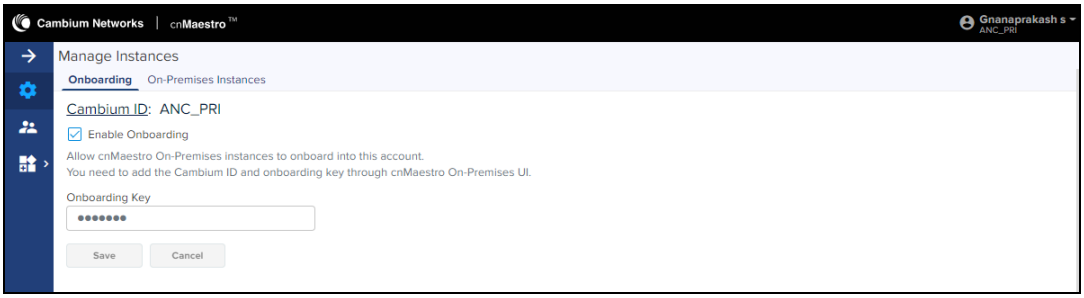


4. Click **Create Account**.

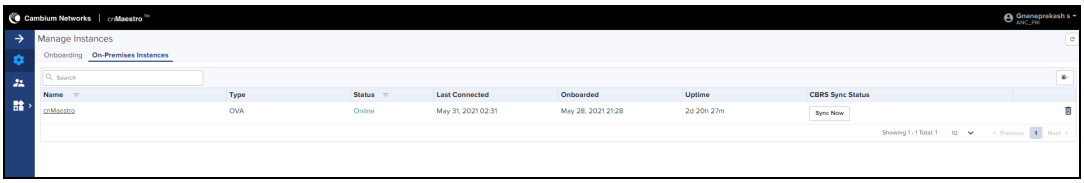
Onboarding Key

Once the Anchor Account is created, an Onboarding Key needs to be set, to allow On-Premises instances to connect.

1. Navigate to the **Manage Instances** page and edit the **Onboarding Key**. This key will be entered into the cnMaestro On-Premises UI to connect to the Anchor Account.



2. Once the On-Premises server onboards, the On-Premises Instances page lists all servers in the account.



Click the instance host name, to view the collected information specific to the On-Premises server.

Connecting cnMaestro On-Premises to Anchor Account

Perform the following steps to connect the cnMaestro On-Premises server with the Cloud Anchor Account:

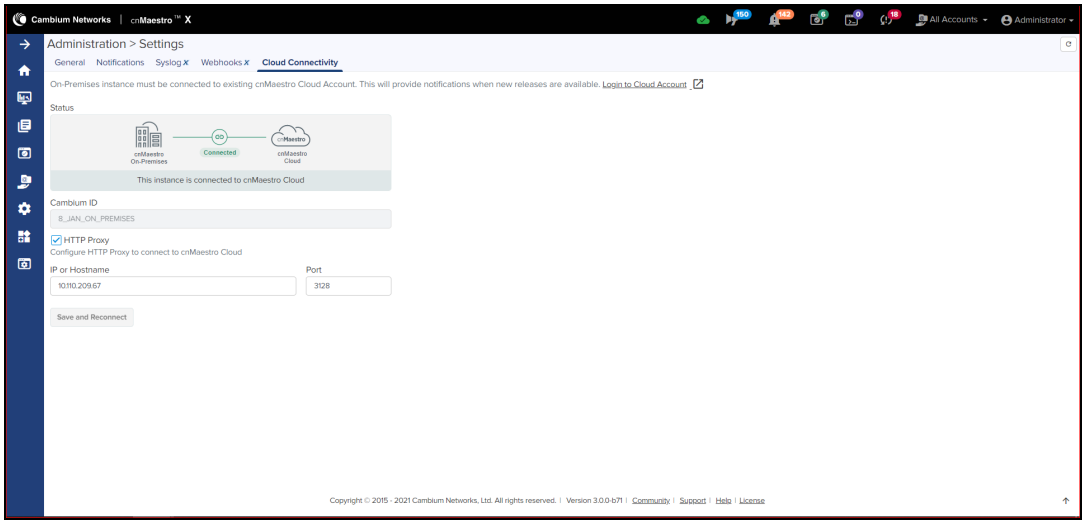
1. Navigate to the **Administration > Settings > Cloud Connectivity** in the cnMaestro On-Premises UI.
2. Enter the **Cambium ID** for the Cloud Anchor Account.
3. Enter the **On-boarding Key** created in the section above.
4. Enable **HTTP Proxy** if required by setting the IP address or Host Name.



NOTE:

Enable **HTTP Proxy** only when On-Premises server needs to connect with public network through proxy.

5. Click **Save and Connect**.



NOTE:

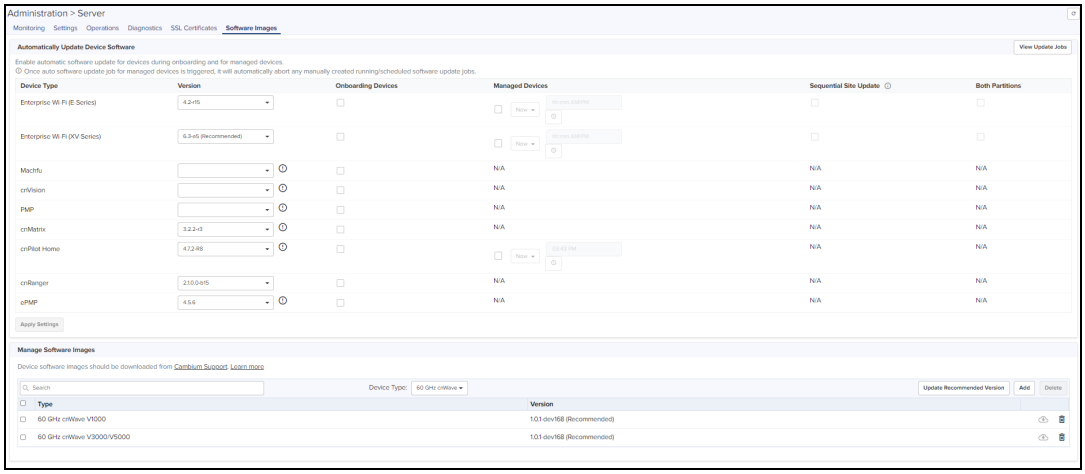
- During the retry time it will take 15 minutes to connect the On-Premises with Anchor Cloud account.
- For every 1 hour it updates the periodic inventory status of On-Premises to Cloud.

Software Images

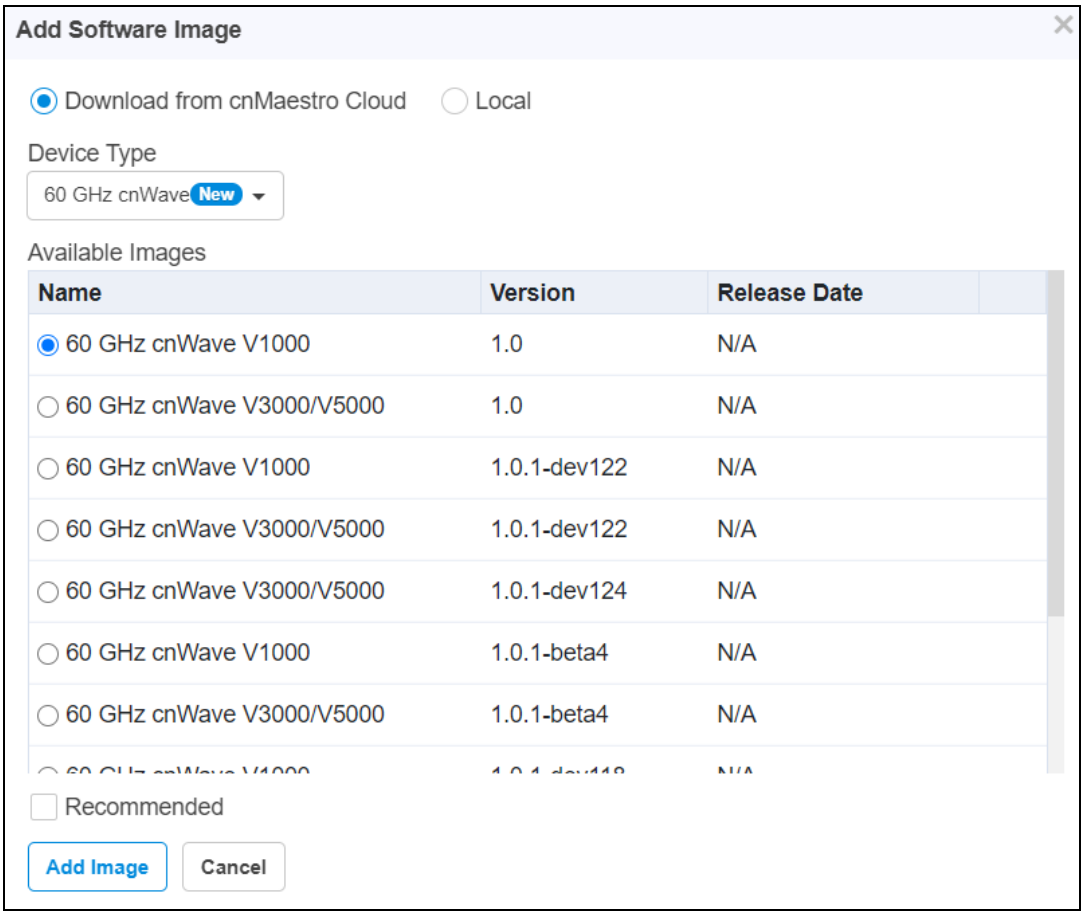
Once the On-Premises server is synced with the cloud, the user can upload the software images from cloud directly to the On-Premises.

To upload Software Image perform as follows:

1. Navigate to **Administration > Server > Software Images.**



2. Click **Add Image.**
3. Click **Download from cnMaestro Cloud** and select **Device Type**.



4. Select the Version and click **Add Image.**

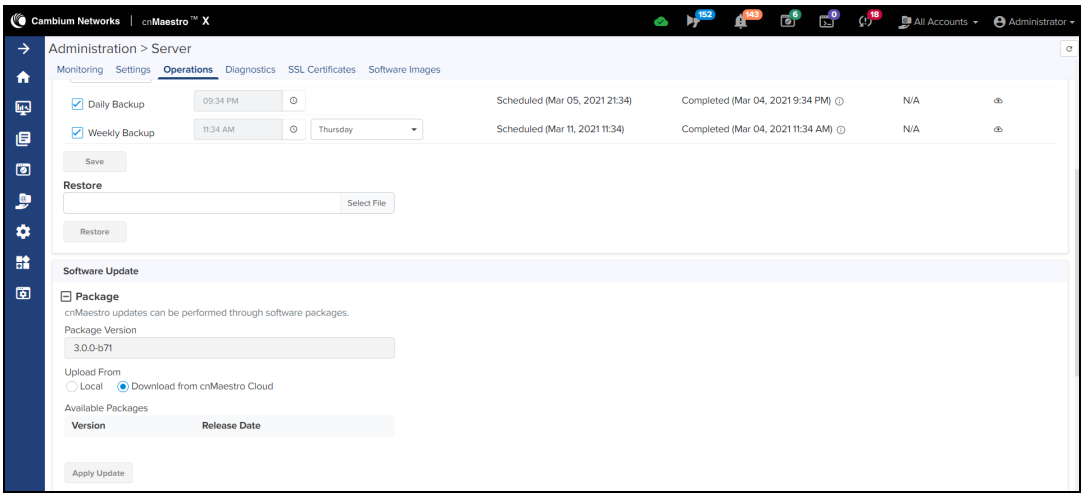
cnMaestro System Update

Package

Once the Cloud is synced with the On-Premises, user can upload the package from Cloud to On-Premises.

To upload a Package, perform the following:

1. Navigate to **Administration > Operations > Package.**
2. Select option **Download from cnMaestro Cloud** under **Upload From.**
3. Click **Apply Update**.

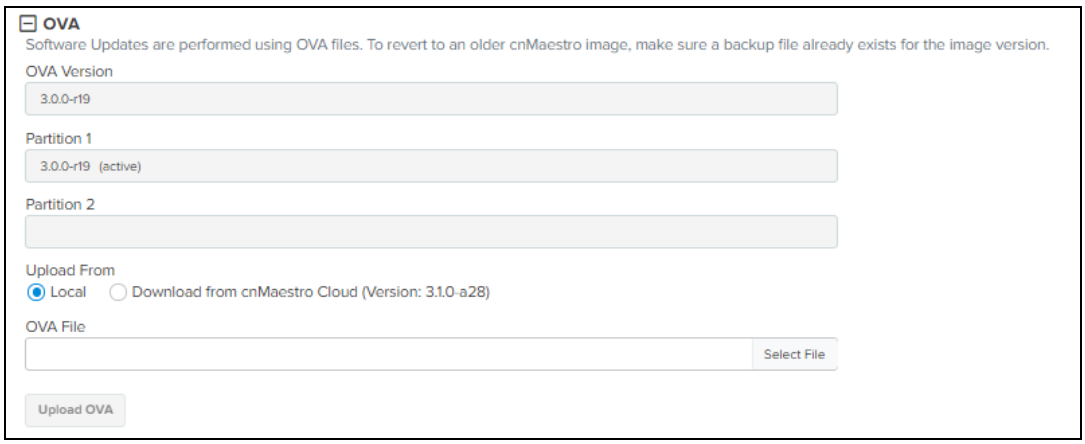


OVA

Once the Cloud is synced with the On-Premises user can upload the software package from Cloud to On-Premises.

To upload an OVA Image, perform the following:

1. Navigate to **Administration > Server > Operations > OVA.**
2. Select option **Download from cnMaestro Cloud.**
3. Select OVA listed in the table.
4. Click **Upload OVA**.



Appendix

This section includes the following topics:

- Maintenance
- Deployments
- Windows DHCP
- Network Port Requirements
- Contacting Cambium Networks

Maintenance

This section provides the following details:

- Command Line Alternatives
- SSH Access
- Data Backup
- Extending the Data Disk
- Account Recovery
- Application Account Recovery
- Configure Network Time Protocol (NTP)

Command Line Alternatives

Cambium Networks highly recommends using the cnMaestro UI for all application operations; however, in case the cnMaestro system is not executing correctly, a number of command-line alternatives exist. You can access these by logging into the cnMaestro CLI (through the VM Console) and selecting the “Shell” option to launch a Unix shell.

Export cnMaestro Data

Navigate to **Manage > Server > Operations > System Backup** to the UI version of this command. From the command line the data can be exported using the following:

```
sudo cnmaestro-export
```

The location of the exported data file is printed when the command completes. It can then be copied to an external directory using SCP or FTP. From there it can be imported into a different cnMaestro instance.

Import cnMaestro Data

Navigate to **Manage > Server > Operations > System Backup** to the UI version of this command. From the command line the data can be imported using the following:

```
sudo cnmaestro-import <data file>
```

The data file needs to be copied to the cnMaestro instance prior to executing this command. This can be done using either SCP or FTP.

Technical Support Dump

The UI version of this command is located at: **Manage > Server > Diagnostics > Technical Support Dump**. From the command line the technical support dump can be exported using the following:

sudo cnmaestro-techdump

The location of the file will be printed when the command completes. It can then be copied to an external directory using SCP or FTP and then sent to Cambium support personnel.

Apply OVA Upgrade

This section describes a failsafe mechanism to apply an OVA Upgrade using the Command Line. First make the image accessible to the operating system either by downloading it through SCP (and storing in /srv/storage/tmp/) or mounting a shared folder. Then execute the following commands:

- Extract and stage the image into the unused partition

  ```
  sudo /srv/bin/cnmaestro-image stage <OVA Filename>
  ```

- View status of the extraction (wait until it completes/hits 100% -- about 10 minutes)

  ```
  watch -n2 sudo /srv/bin/cnmaestro-image status
  ```

- Boot into the new image. Use the inactive partition from the status command

  ```
  sudo /srv/bin/cnmaestro-image upgrade <os2 or os1>
  ```



NOTE:

Above mentioned steps are only a failsafe if the UI upgrade is unavailable. They should not be used for downgrades, which are unsupported.

Apply Package Update

Navigate to **Manage > Server > Operations > Apply cnMaestro Package** to the UI version of this command. From the command line an update package can be applied using the following:

sudo /srv/bin/cnmaestro-image patch <package-file>

The upgrade file needs to be copied to the cnMaestro instance prior to executing this command. This can be done using either SCP or FTP. The update file itself is downloaded from Cambium Networks and only updates the cnMaestro application.

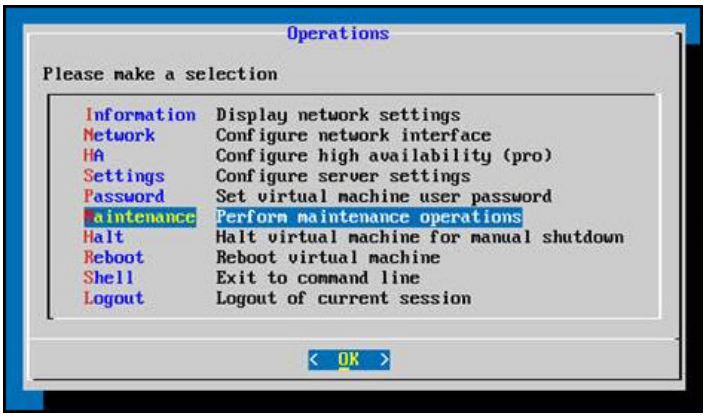
SSH Access

cnMaestro supports SSH access using the 'cambium' user account and password. Enabling this feature is not recommended, due to the password security, but it is available if needed.

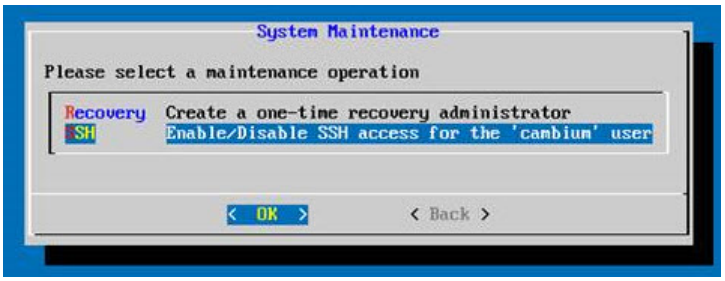
Enabling SSH Access

Follow the below steps to enable SSH access:

1. From the **Operations** page, select **Maintenance**.



2. Select **SSH** for the SSH Server page.



3. Select **Enable SSH** option.



A screen pops-up if SSH is enabled successfully.



You can then log into the cnMaestro system using the same 'cambium' account used to log in through the Console.

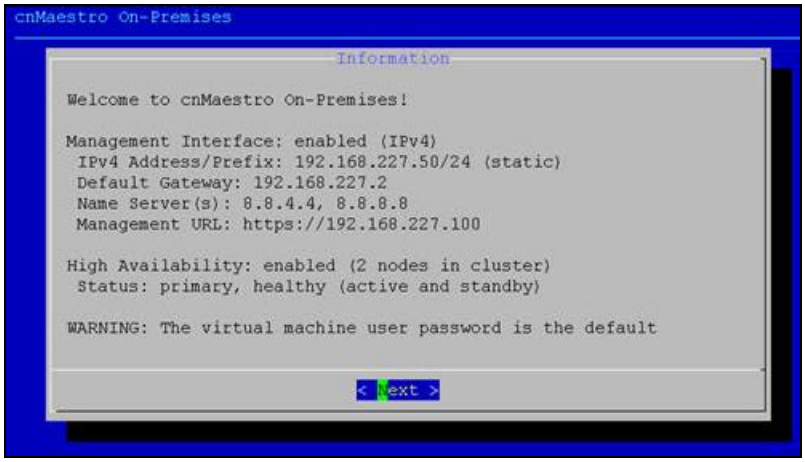
```
# ssh cambium@192.168.127.51
```



NOTE:

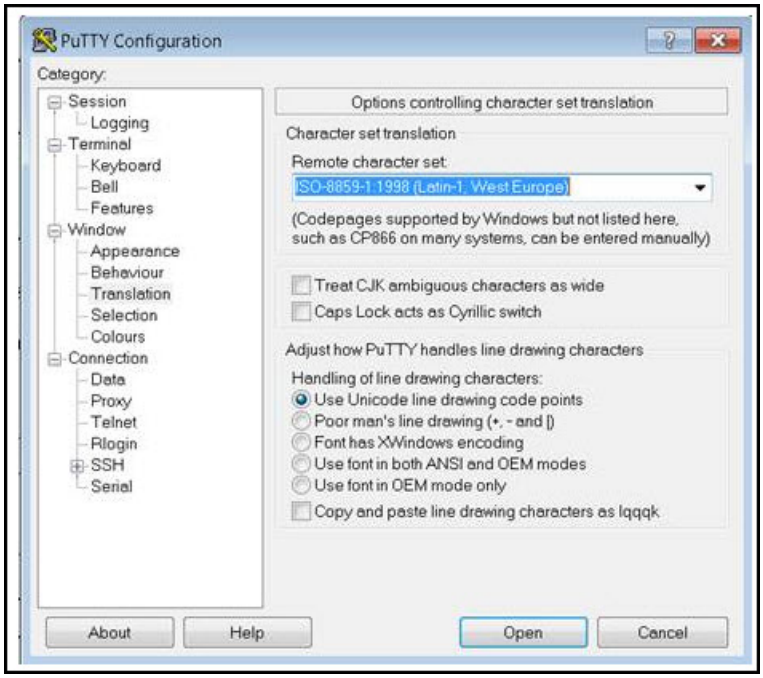
The 'cambium' user has sudo access, so if using SSH, be sure to change the default password of this user before enabling the feature.

The Windows application putty, by default, will not print the dialog correctly, and the customer needs to set the Translation accordingly.

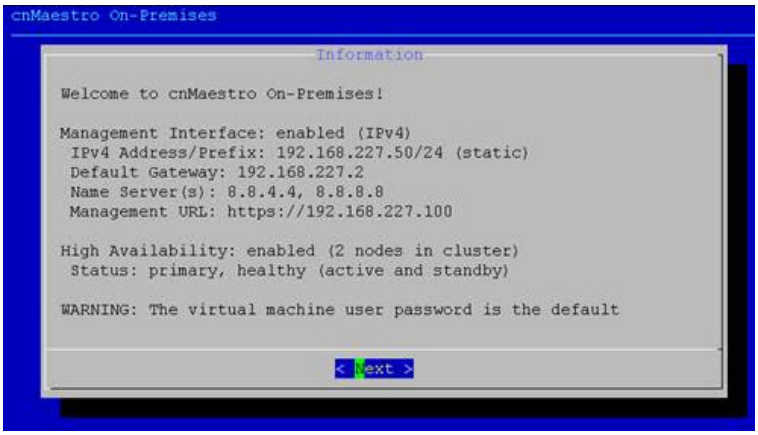


NOTE:

When accessing the CLI from putty on Windows, you may need to change the Remote Character Set (Window > Translation in the putty Configuration dialog) to "ISO-8859-1 1998 (Latin-1, West Europe)" to correctly display the menu.



After setting the configuration properly, the window appears as below:



Data Backup

Overview

> **NOTE:**
>
> cnMaestro backups taken from version 3.0.0 and later will only include statistics for the last month (in addition to configuration). To backup all statistics in a cnMaestro X account (up to 2 years), one needs to periodically copy the data disk outside of cnMaestro.

cnMaestro On-Premises stores its configuration and statistics on a virtual "data" disk. This disk could be tens of gigabytes in size. Backing up the disk requires snapshotting and copying it using the virtualization infrastructure.

cnMaestro configuration backups should normally be made using the standard cnMaestro backup mechanism available through the UI. When full historical data is required, a snapshot-based disk backup mechanism should be used.

cnMaestro backups

Standard cnMaestro backups are done through the cnMaestro UI. They are fast: ideal for pre-change checkpointing or upgrades. They can be executed on-demand or on a schedule, and they are a quick way to restore cnMaestro configuration. Standard backups also restore the last week of device statistics, but they do not save any Wi-Fi Client statistics.

> **NOTE:**
>
> Standard cnMaestro backups are performed using the cnMaestro UI.

Full Backups

Full backups copy all cnMaestro data, including configuration and long-term statistics. They can be taken from a running system, but they can only be restored when the system is shut down, because they require the data disk to be swapped.

The method of creating snapshot backups varies per virtualization technology, but the basics are the same: a point in time snapshot of the data disk is created, and the snapshot is used as the source for the backup.

If snapshot backups are taken of a running instance, the backup will be "crash consistent". This means the instance will be restored to a state similar to the instant before a power loss or reset. While small amounts of uncommitted

data may be lost, this is generally safe, because the cnMaestro data is stored transactionally. If you prefer to have a fully consistent backup, power down the instance before taking the snapshot backup. In the case of the HA cluster, always take data backup of the Primary Server only.



NOTE:

It is recommended to only use snapshot backup methods, as data is constantly being written, and backups otherwise are likely to be inconsistent or unusable.



NOTE:

Recommended HA data restore procedure is as follows:

1. Power OFF the existing Secondary Server, so that the Primary Server will be in Peer-Down state.
2. Replicate or attach the disk of the backed-up Primary Server to the newly created server.
3. After backup replication is done, Power OFF the existing Primary (cnMaestro Active) Server and Power ON the newly created server. The new server will become Primary (cnMaestro Active) in Peer-Down state.
4. Power ON the Secondary Server. HA replication will occur.

Virtualization System specific Backup Methods

VMware

Dedicated backup software for either VMware or your datastore device is recommended. A basic disk clone backup without additional backup software can be performed through the following:

- Delete all existing snapshots
- Create a new snapshot of the disk
- Clone the disk using vmkfstools
- Delete the snapshot

Disk clone backup using additional backup software can be performed using this alternatives Veeam Backup & Replication or Vinchin Backup.

Standard snapshot-based backups work with existing VMware-supported backup tools, and are likely to work with your existing backup solution. It is not recommended attempting to backup snapshot or disk files directly from storage.



NOTE:

The backup process will consume resources and may impact performance of all VMs, henceforth plan backup accordingly. Initial full backups are likely to take a long time depending on disk size and type.

Hyper-V

It is recommended to use dedicated backup software for Hyper-V, a basic crash-consistent disk backup can be made using either Hyper-V manager or (Export-VM). There are a number of backup solutions available, if snapshot backup is supported it will successfully backup cnMaestro data disks. Test your backup solution before starting backup process. If you do not have an existing backup solution for your VMs, disk backup using additional software using the alternatives such as Veeam Backup & Replication or Vinchin Backup.

Citrix Hypervisor (XenServer)

To backup Citrix Hypervisor refer Back up and restore hosts and VMs. There are a number of backup solutions available, if snapshot backup is supported it will successfully backup cnMaestro data disks. Test your backup solution before starting backup process. If you do not have an existing backup solution for your VMs, disk backup using additional software using the alternative such as Vinchin Backup.

Extending the Data Disk

cnMaestro has two virtual disks, one for the operating system, and the second for data. If the data disk becomes overloaded, it can be extended. This is done by increasing the disk size through the virtual machine, and then following the command line instructions in this guide.

The process will have two phases:

- Phase 1: Expand the virtual disk (using the virtual machine infrastructure).
- Phase 2: Extend the cnMaestro partition and file system (using the command line instructions listed below).

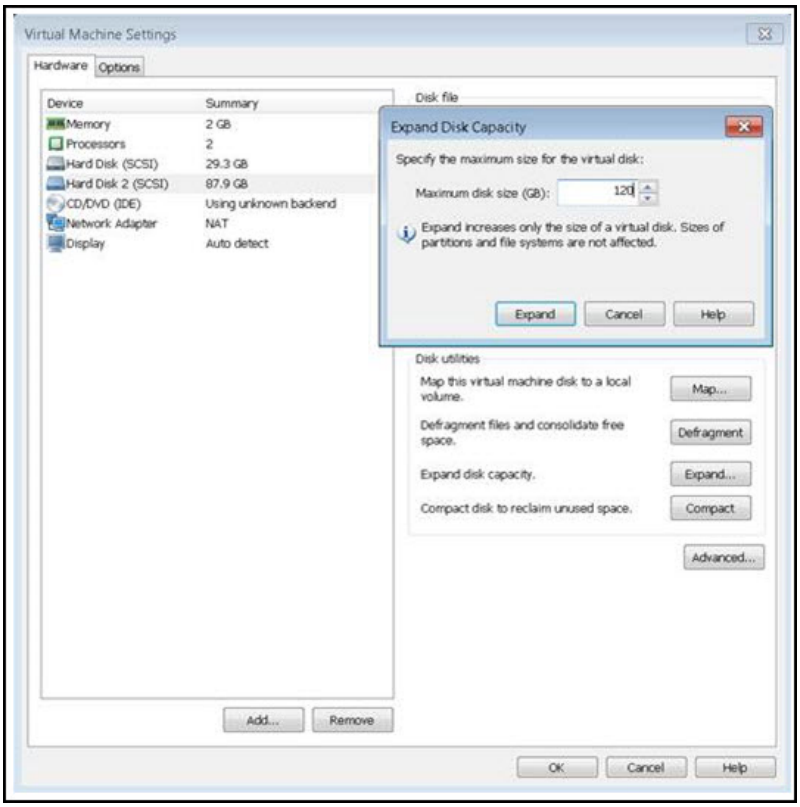


NOTE:

Please take a backup copy of your virtual machine before performing any operations below.

VMware Workstation Disk Expansion

To expand the virtual disk in VMware Workstation, make sure the virtual machine has no VMware snapshots and is currently turned off. You can then select Hard Disk 2 and click **Expand** to select a new disk size. Only expansion is allowed (the data disk can grow but not shrink). An Expand Disk Capacity window launches to update the size. Once a new disk size is chosen, restart cnMaestro. A similar mechanism is used for ESXi.



VirtualBox Disk Expansion

VirtualBox requires command line expansion of the virtual disk. One also needs to convert the disk format from VMDK to VDI before the transformation, and then back again when finished. The commands below are for the Windows installation of VirtualBox. The steps are to convert to VDI; then resize the VDI disk; then convert back to VMDK.

Once the resized.vmdk is created, replace the current Disk 2 in the VirtualBox UI with the resized vmdk and restart the virtual machine.

```
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" clonehd source.vmdk clone.vdi --format vdi
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" modifyhd clone.vdi --resize 120000
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" clonehd clone.vdi resized.vmdk --format vmdk
```

Once the resized.vmdk is created, replace the current Disk 2 in the VirtualBox UI with the resized vmdk and restart the virtual machine.

Partition and File System Updates

cnMaestro will not recognize the additional disk space until the partition is extended. So after the reboot, launch the cnMaestro CLI and select **Shell** to exit to the command line. There type the following commands to grow the partition and file system disk; then convert back to VMDK.

```
$ sudo growpart /dev/sdb 1
$ sudo resize2fs /dev/sdb1
```

You can validate the command completed successfully by typing df -k and reviewing the size of /dev/sdb1 (/mnt/data).

```
cambium@cnmaestro:~$ df -k
Filesystem                     1K-blocks    Used Available Use% Mounted on
udev                             1003608       0   1003608   0% /dev
tmpfs                             204800   10272    194528   6% /run
/dev/mapper/cnmaestro--vg-root  28377236 3622112  23290600  14% /
tmpfs                            1023992       4   1023988   1% /dev/shm
tmpfs                               5120       0      5120   0% /run/lock
tmpfs                            1023992       0   1023992   0% /sys/fs/cgroup
/dev/sda1                         736752  106512    592816  16% /boot
/dev/sdb1                      125783080  429028 125354052   1% /mnt/data
tmpfs                             204800       0    204800   0% /run/user/1000
```

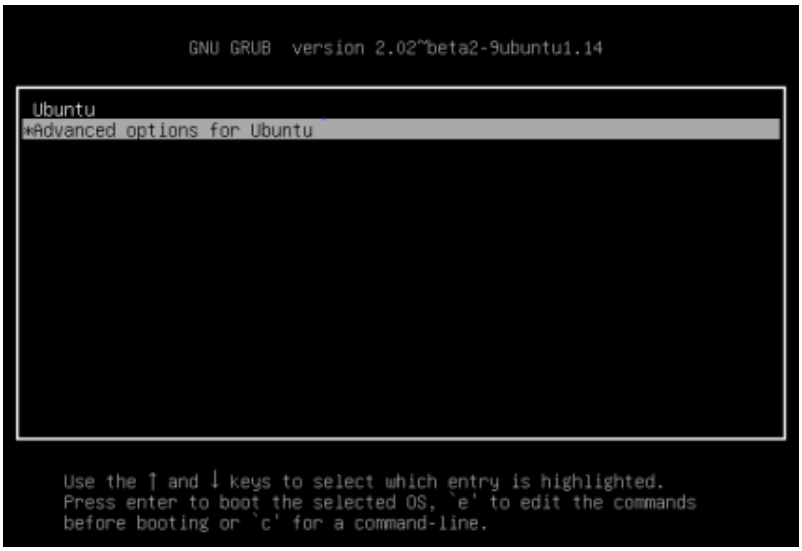
Account Recovery

cnMaestro has two types of accounts: the Virtual Machine (Console) account and the cnMaestro Application account. Both of these can be recovered if the administrator password is lost.

Virtual Machine (Console) Account Recovery

cnMaestro is installed on Ubuntu Server and can leverage the Ubuntu Recovery Mode process to reset the "Cambium Networks" Console login password. The steps are the following:

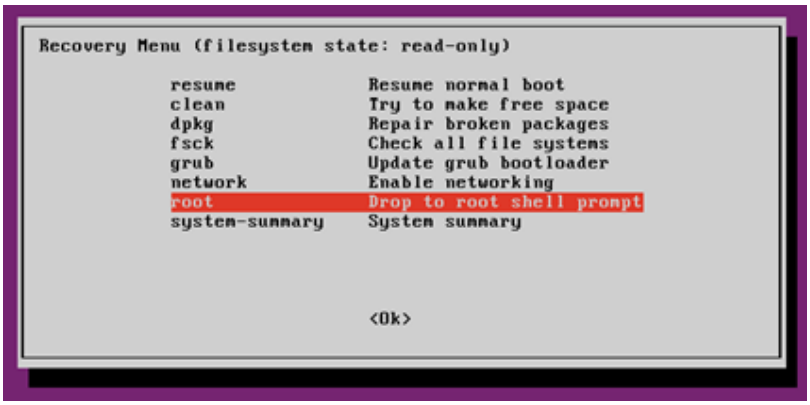
1. When booting up cnMaestro in the VM Console after a full shutdown, quickly press and hold the Shift key after the BIOS has finished loading. This will launch the GNU GRUB menu.



2. Select Advanced Options and then Ubuntu Recovery Mode

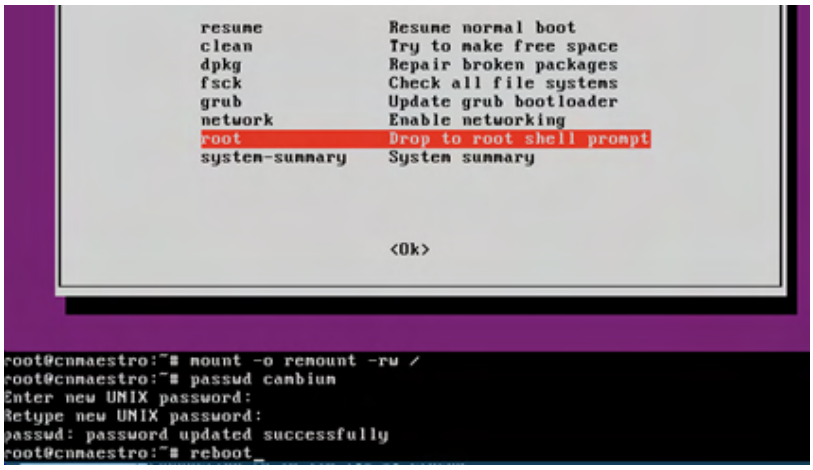


3. Once in the Recovery Menu, select the **root** option to enter a root shell

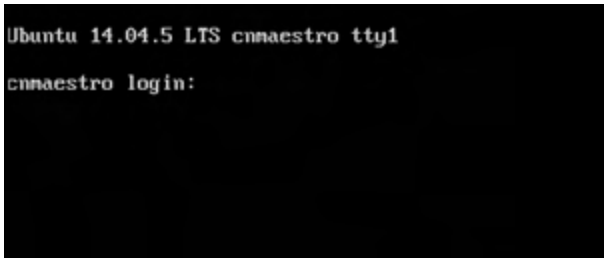


4. The shell will display a command parser along the bottom of the screen. Type the following (without the '#')to reset the password of the **cambium** user.

```
# mount -o remount -rw /
# passwd cambium
# reboot
```



5. You should now be able to login to the console using the new password.



cnMaestro Application Account Recovery

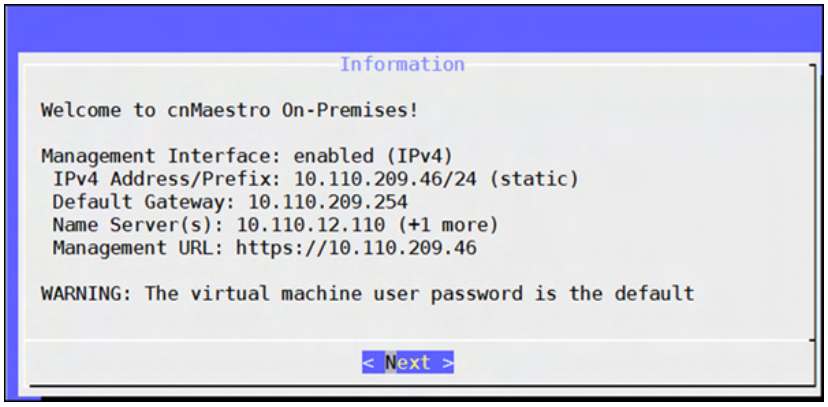
Application Account recovery is useful if you are unable to log in to the cnMaestro UI. It allows you to create a one-time password through the command line, so you can access the UI as a Super Administrator and update current authentication settings.

Application Account Recovery

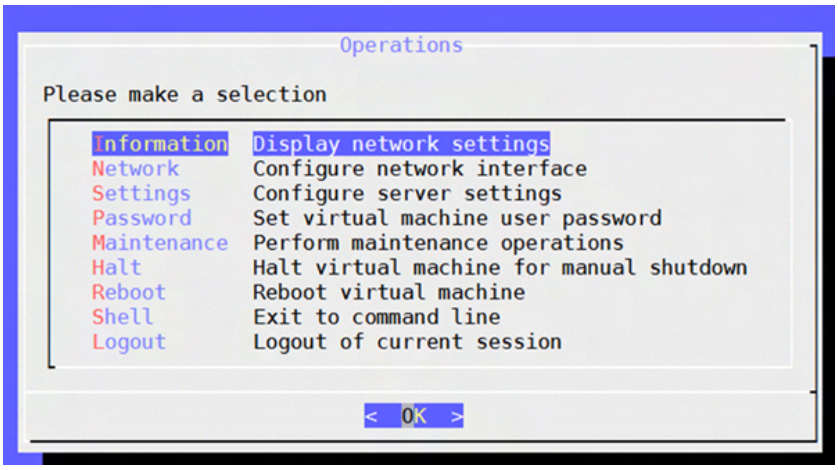
Console administrators can create a one-time password providing Super Administrator access to the cnMaestro UI for a single session (the password will expire in one hour or after a single use). This is a fail safe mechanism that allows cnMaestro access to update current authentication settings.

To create a one-time password:

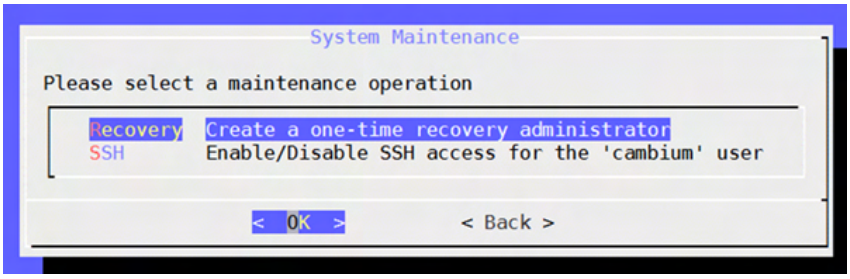
1. Log into the cnMaestro Console and following window pops-up:



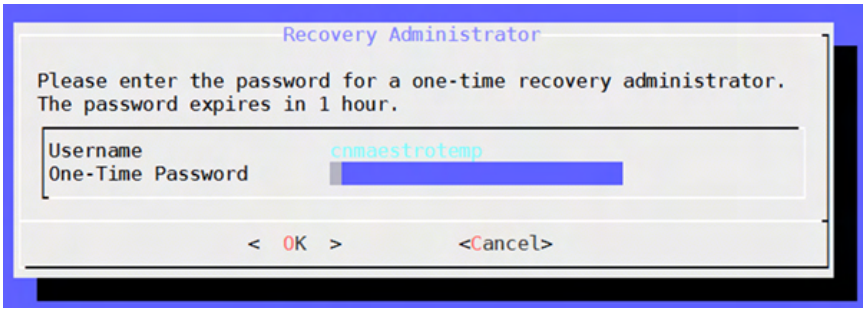
2. Click **Next**.
3. Select **Information** and click **Ok**.



4. Select **Recovery** tab and click **Ok**.



5. Enter the password in the **OneTime Password** text box.

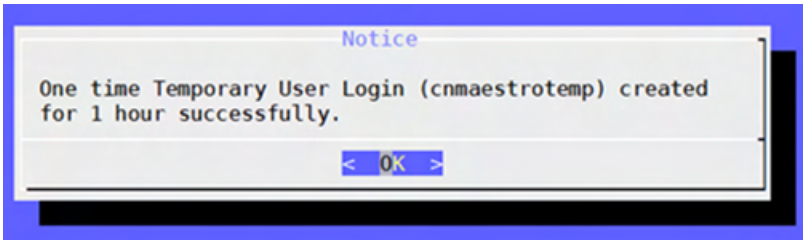




NOTE:

The username for temporary user login is **cnmaestrotemp**. It cannot be changed.

6. Click **OK**. The following window is displayed:



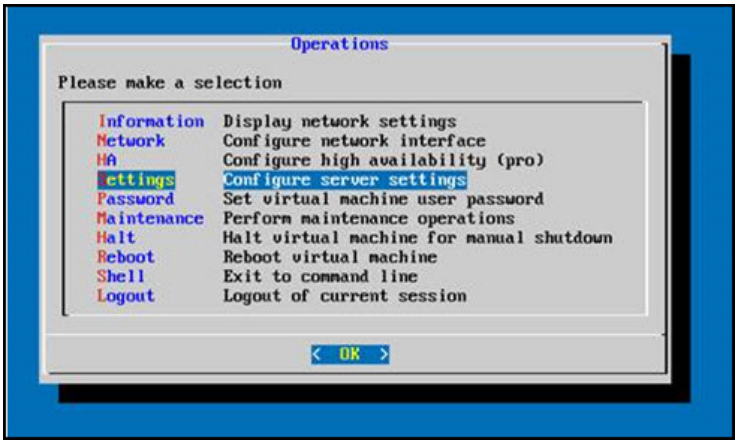
Configure Network Time Protocol (NTP)

cnMaestro uses NTP for time synchronization. This is particularly important for HA environments. By default, NTP is configured to use Google NTP services. NTP can be disabled, if one wants to leverage the NTP feature of VMware, or changed to enable a customized group of NTP servers.

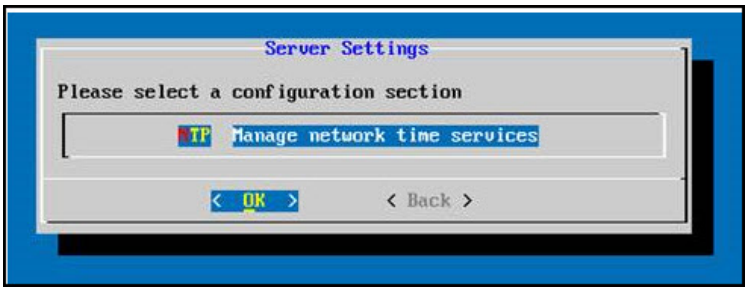
Disabling NTP Support

Follow the below steps to disable NTP Support:

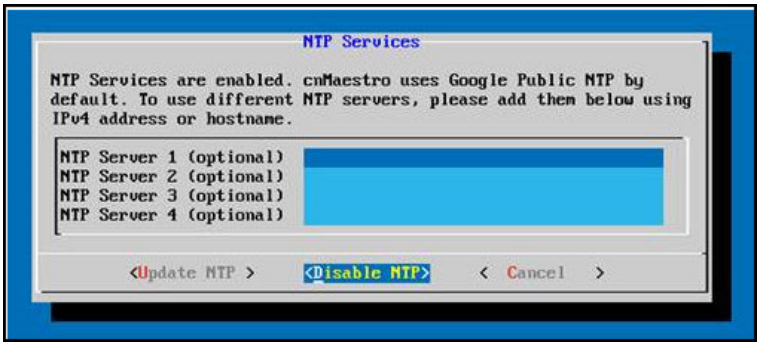
1. From the **Operations** page, select **Settings**.



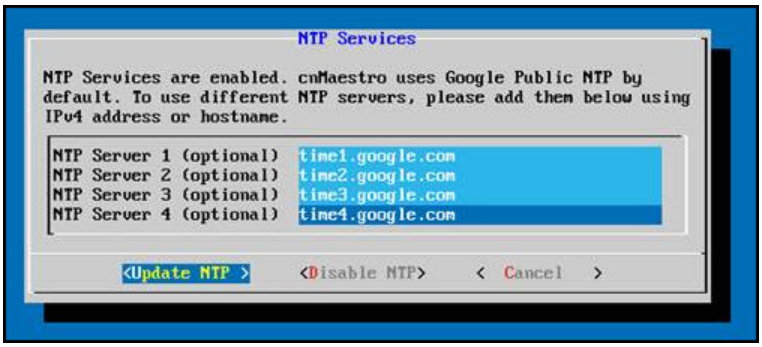
2. Select NTP to **Manage Network Time Services.**



3. To disable NTP, select the **Disable NTP** Option.



4. Set custom NTP servers and Update NTP.



Statistics API Response (v1 Format)

API v1 is replaced by v2 in cnMaestro 3.0.0 release. It will be supported from cnMaestro 3.2.0 release and no longer be supported.

This section provides the Statistics API response v1 Format for the following devices:

- cnMatrix
- cnReach
- Fixed Wireless
- PTP
- Wi-Fi

cnMatrix

General

Name	Details
cpu	CPU utilization
config_version	Configuration version
last_sync	Last synchronization (UTC Unix time milliseconds)
mac	MAC address
managed_account	Managed account name
mode	Device mode
name	Device name
network	Network
site	Site name
site_id	Site unique identifier
status	Status [online, offline, claimed, waiting, onboarding]

Name	Details
status_time	Uptime/downtime interval (seconds)
tower	Tower name
type	Device type

Networks

Name	Details
ip	IP address

cnReach

General

Name	Details	Mode
config_version	Configuration version	All
connected_sms	Connected SM count	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
tower	Tower name	All
type	Device type	All

Networks

Name	Details	Mode
ip	IP address	All
ip_wan	WAN IP	All

Radios

Name	Details	Mode
radio.radio1.device_id	Device ID	Radios
radio.radio1.linked_with	Linked with	Radios
radio.radio1.mac	Radio MAC	Radios
radio.radio1.margin	Margin	Radios
radio.radio1.mode	Radio mode [ap, ep, rep]	Radios
radio.radio1.neighbors	Radio neighbors	Radios
radio.radio1.network_address	Network address	Radios
radio.radio1.noise	Average noise (dB)	Radios
radio.radio1.power	Transmit power	Radios
radio.radio1.rssi	RSSI value (dB)	Radios
radio.radio1.rx_bytes	Receive bytes	Radios
radio.radio1.software_version	Current software version.	Radios
radio.radio1.temperature	Radio temperature	Radios
radio.radio1.tx_bytes	Transmit bytes	Radios
radio.radio1.type	Radio type [ptp, ptmp]	Radios
radio.radio2.device_id	Device ID	Radios
radio.radio2.linked_with	Linked with	Radios
radio.radio2.mac	Radio MAC	Radios
radio.radio2.margin	Margin	Radios
radio.radio2.mode	Radio mode [ap, ep, rep]	Radios
radio.radio2.neighbors	Radio neighbors	Radios
radio.radio2.network_address	Network address	Radios
radio.radio2.noise	Average noise	Radios
radio.radio2.power	Transmit power	Radios

Name	Details	Mode
radio.radio2.rssi	RSSI value (dB)	Radios
radio.radio2.rx_bytes	Receive bytes	Radios
radio.radio2.software_version	Radio current software version.	Radios
radio.radio2.temperature	Radio temperature	Radios
radio.radio2.tx_bytes	Transmit bytes	Radios
radio.radio2.type	Radio type [ptp, ptmp]	Radios

Fixed Wireless

General

Name	Details	ePMP	PMP
ap_mac	AP MAC	SM	SM
config_version	Configuration version	AP/SM	AP/SM
connected_sms	Connected SM count	AP	AP
distance	SM distance (KM)	SM	SM
gain	Antenna gain (dBi)	AP/SM	AP/SM
gps_sync_state	GPS synchronization state	AP/SM	
last_sync	Last synchronization (UTC Unix time milliseconds)	AP/SM	AP/SM
mac	MAC address	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM
network	Network	AP/SM	AP/SM
reboots	Reboot count	AP/SM	
status	Status [online, offline, claimed, waiting, onboarding]	AP/SM	AP/SM
status_time	Uptime/downtime interval (seconds)	AP/SM	AP/SM

Name	Details	ePMP	PMP
temperature	Temperature		AP/SM
tower	Tower name	AP	AP
vlan	VLAN		AP/SM

Networks

Name	Details	ePMP	PMP
default_gateway	Default gateway	AP/SM	AP/SM
ip	IP address	AP/SM	AP/SM
ipv6	IPv6 address	AP/SM	
ip_dns	DNS	AP/SM	AP/SM
ip_dns_secondary	Secondary DNS		AP/SM
ip_wan	WAN IP	AP/SM	
lan_mode_status	LAN mode status [no-data, half, full]	AP/SM	
lan_mtu	MTU size	SM	
lan_speed_status	LAN speed status	AP/SM	
lan_status	LAN status [down, up]	AP/SM	AP/SM
netmask	Network mask	AP/SM	AP/SM

Radios

Name	Details	ePMP	PMP
radio.auth_mode	Authentication mode	SM	
radio.auth_type	Authentication type ePMP [open, wpa1, eap- ttls] PMP [disabled, enabled]	AP/SM	AP/SM
radio.channel_width	Channel width ePMP [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP [...]	AP/SM	AP/SM
radio.color_code	Color code		AP/SM
radio.dfs_status	DFS status ePMP:	AP/SM	AP/SM

Name	Details	ePMP	PMP
	[not-applicable, channel- availability-check, in-service, radar- signal-detected, alternate-channel- monitoring, not-in- service] PMP: [Status String]		
radio.dl_err_drop_pkts	Downlink error drop packets	SM	
radio.dl_err_drop_pkts_ percentage	Downlink error drop packets percentage	SM	
radio.frequency	RF frequency	AP/SM	AP/SM
radio.frame_period	Frame period		AP
radio.dl_frame_utilization	Downlink frame utilization		AP
radio.dl_lqi	Downlink Link Quality Indicator		SM
radio.dl_mcs	Downlink MCS	SM	
radio.dl_modulation	Downlink Modulation		SM
radio.dl_pkts	Downlink packet count	AP/SM	AP/SM
radio.dl_pkts_loss	Downlink packet loss		AP/SM
radio.dl_retransmits	Downlink Retransmission	AP/SM	
radio.dl_retransmits_pct	Downlink Retransmission percentage	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance		AP
radio.dl_snr	Downlink SNR (dB)	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal		SM
radio.dl_snr_v	Downlink SNR (dB) vertical		SM
radio.dl_throughput	Downlink throughput	AP/SM	AP/SM
radio.mac	Wireless MAC	AP/SM	
radio.mode	Radio mode [eptp-master, eptp- slave, tdd, tdd-ptp, ap/sm]	AP/SM	
radio.sessions_dropped	Session drops	AP	AP/SM

Name	Details	ePMP	PMP
radio.software_key_throughput	Software key – max throughput		SM
radio.ssid	SSID	AP/SM	
radio.sync_source	Synchronization source		AP
radio.sync_state	Synchronization state		AP
radio.tdd_ratio	TDD ratio ePMP [75/25, 50/50, 30/70, flexible] PMP [...]	AP	AP
radio.tx_capacity	SM transmit capacity	SM	
radio.tx_power	Radio transmit power	AP/SM	AP/SM
radio.tx_quality	SM transmit quality	SM	
radio.ul_err_drop_pkts	Uplink error drop packets	SM	
radio.ul_err_drop_pkts_ percentage	Uplink error drop packets percentage	SM	
radio.ul_frame_utilization	Uplink frame utilization		AP
radio.ul_mcs	Uplink MCS	AP/SM	
radio.ul_modulation	Uplink Modulation example [2X MIMO-B)]		SM
radio.ul_lqi	Uplink Link Quality Indicator		SM
radio.ul_pkts	Uplink packet count	AP/SM	AP/SM
radio.ul_pkts_loss	Uplink packet loss		AP/SM
radio.ul_retransmits	Uplink Retransmission	SM	
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM
radio.ul_snr	Uplink SNR (dB)	SM	
radio.ul_snr_h	Uplink SNR (dB) horizontal		SM
radio.ul_snr_v	Uplink SNR (dB) vertical		SM
radio.ul_throughput	Uplink throughput	AP/SM	AP/SM
radio.wlan_status	WLAN status [down, up]	AP/SM	

PTP

General

Name	Details	Mode
config_version	Configuration version	All
connected_sms	Connected SM count	Master
gain	Antenna gain (dBi)	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
temperature	Temperature	All
tower	Tower name	All
type	Device type	All
vlan	VLAN	All

Networks

Name	Details	Mode
default_gateway	Default gateway	All
ip	IP address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
lan_status	LAN status [down, up]	All
netmask	Network mask	All

Radios

Name	Details	Mode
ethernet.aux_ interface.rx_frames	Aux Rx Frames Oversize	All
ethernet.aux_ interface.tx_util	Aux Tx Bandwidth Utiliization	All
ethernet.aux_ interface.rx_util	Aux Rx Bandwidth Utiliization	All
ethernet.aux_ interface.speed	Aux speed and duplex	All
ethernet.main_psu_ interface.rx_frames	Main PSU Rx Frames Oversize	All
ethernet.main_psu_ interface.rx_util	Main PSU Rx Bandwidth Utiliization	All
ethernet.main_psu_ interface.speed	Main PSU speed and duplex	All
ethernet.main_psu_ interface.tx_util	Main PSU Tx Bandwidth Utiliization	All
ethernet.sfp_interface.rx_ frames	SFP Rx Frames Oversize	All
ethernet.sfp_interface.rx_ util	SFP Rx Bandwidth Utiliization	All
ethernet.sfp_ interface.speed	SFP speed and duplex	All
ethernet.sfp_interface.tx_ util	SFP Tx Bandwidth Utiliization	All
radio.byte_error_ratio	Byte Error Ratio	All
radio.channel_width	Channel width ePMP: [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP: [...]	All
radio.color_code	Color code	All

Name	Details	Mode
radio.rx_frequency	Receive frequency	All
radio.tx_frequency	Transmit frequency	All
radio.tx_power	Radio transmit power	All

Wi-Fi



NOTE:

Mode is Enterprise, Home, or All.

General

Name	Details	Mode
config_version	Configuration version	All
cpu	CPU utilization	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode [AP, SM]	All
memory	Available memory	All
name	Device name	All
network	Network	All
parent_mac	Parent MAC	All
site	Site name	All
site_id	Site unique identifier	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
type	Device type	All

Network

Name	Details	Mode
ip	IP address	All
ipv6	IPv6 address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
ip_wan	WAN IP	All
lan_mode_status	LAN mode status [no-data, half, full]	Enterprise
lan_speed_status	LAN speed status	All
lan_status	LAN status [down, up]	Home
netmask	Network mask	All

Radios

Name	Details	Mode
radio.24ghz.airtime	Airtime	All
radio.24ghz.bssid	Radio mac	Enterprise
radio.24ghz.channel	Channel	All
radio.24ghz.multicast_rate	Multicast rate	All
radio.24ghz.noise_floor	Noise floor	All
radio.24ghz.num_clients	Number of clients	All
radio.24ghz.num_wlans	Number of WLANs	Enterprise
radio.24ghz.power	Transmit power	All
radio.24ghz.quality	RF Quality description	Enterprise
radio.24ghz.radio_state	Radio state	Enterprise
radio.24ghz.rx_bps	Receive bits/second	Enterprise
radio.24ghz.rx_bytes	Receive bytes	All

Name	Details	Mode
radio.24ghz.tx_bps	Transmit bits/second	Enterprise
radio.24ghz.tx_bytes	Transmit bytes	All
radio.24ghz.unicast_rates	Unicast rates	All
radio.24ghz.utilization	Radio utilization	Enterprise
radio.5ghz.airtime	Airtime	All
radio.5ghz.bssid	Radio mac	Enterprise
radio.5ghz.channel	Channel	Enterprise
radio.5ghz.multicast_rate	Multicast rate	All
radio.5ghz.noise_floor	Noise floor	All
radio.5ghz.num_clients	Number of clients	Enterprise
radio.5ghz.num_wlans	Number of WLANs	Enterprise
radio.5ghz.power	Transmit power	All
radio.5ghz.quality	RF quality description	Enterprise
radio.5ghz.radio_state	Radio state	Enterprise
radio.5ghz.rx_bps	Receive bits/second	Enterprise
radio.5ghz.rx_bytes	Receive bytes	All
radio.5ghz.tx_bps	Transmit bits/second	Enterprise
radio.5ghz.tx_bytes	Transmit bytes	All
radio.5ghz.unicast_rates	Unicast rates	All
radio.5ghz.utilization	Radio utilization	Enterprise

Performance API Response (v1 Format)

This section provides the performance API response v1 Format for the following devices:

- cnMatrix
- cnReach
- Fixed Wireless
- PTP
- Wi-Fi

cnMatrix

General

Name	Details
mac	MAC address
managed_account	Managed account name
mode	Device mode
name	Device name
network	Network
site	Site
timestamp	Timestamp
tower	Tower
type	Device type

Switch

Name	Details
switch.rx.broadcast_pkts	Receive broadcast packets
switch.dl_kbits	Downlink usage (in kbits on hour or minute basis)
switch.dl_throughput	Downlink throughput (Kbps)
switch.ul_kbits	Uplink (in Kbits on hour or minute basis)
switch.rx.multicast_pkts	Receive multicast packets
switch.ul_throughput	Uplink throughput (Kbps)
switch.rx.pkts_err	Receive Packet error
switch.rx.unicast_pkts	Receive unicast packets
switch.tx.broadcast_pkts	Transmit broadcast packets
switch.tx.multicast_pkts	Transmit multicast packets
switch.tx.pkts_err	Transmit packet error
switch.tx.unicast_pkts	Transmit unicast packets

cnReach

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
site	Site	All
sm_count	Connected SM count	All
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios

Name	Details	Mode
radio.radio1.neighbors	Radio neighbors	Radios
radio.radio1.noise	Average noise	Radios
radio.radio1.power	Transmit power	Radios
radio.radio1.rssi	RSSI value	Radios
radio.radio1.rx_bytes	Receive bytes	Radios
radio.radio1.throughput	Total throughput	Radios
radio.radio1.tx_bytes	Transmit bytes	Radios
radio.radio2.neighbors	Radio neighbors	Radios
radio.radio2.noise	Average noise	Radios

Name	Details	Mode
radio.radio2.power	Transmit power	Radios
radio.radio2.rssi	RSSI value	Radios
radio.radio2.rx_bytes	Receive bytes	Radios
radio.radio2.throughput	Total throughput	Radios
radio.radio2.tx_bytes	Transmit bytes	Radios

Fixed Wireless

General

Name	Details	ePMP	PMP
mac	MAC address	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM
network	Network	AP/SM	AP/SM
online_duration	Duration of device connection with server (seconds)	AP/SM	AP/SM
sm_count	Connected SM count	AP	AP
sm_drops	Session drops	AP/SM	AP
timestamp	Timestamp	AP/SM	AP/SM
tower	Tower	AP/SM	AP/SM
type	Device type	AP/SM	AP/SM
uptime	Device online time (seconds)	AP/SM	AP/SM

Radios

Name	Details	ePMP	PMP
radio.dl_frame_utilization	Downlink frame utilization		AP
radio.dl_kbits	Downlink usage (in Kbits on hour or minute basis)	AP/SM	
radio.dl_mcs	Downlink MCS	SM	

Name	Details	ePMP	PMP
radio.dl_modulation	Downlink modulation		SM
radio.dl_pkts	Downlink packet count	AP/SM	
radio.dl_pkts_loss	Downlink packet loss		AP/SM
radio.dl_retransmits_pct	Downlink retransmission percentage	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance		SM
radio.dl_snr	Downlink SNR	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal		SM
radio.dl_snr_v	Downlink SNR (dB) vertical		SM
radio.dl_throughput	Downlink Throughput (Kbps)	AP/SM	AP/SM
radio.ul_frame_utilization	Uplink frame utilization		AP
radio.ul.kbits	Uplink usage (in Kbits on hour or minute basis)	AP/SM	
radio.ul_mcs	Uplink MCS	SM	
radio.ul_modulation	Uplink modulation		SM
radio.ul_pkts	Uplink packet count	AP/SM	
radio.ul_pkts_loss	Uplink packet loss		AP/SM
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM
radio.ul_snr	Uplink SNR	SM	
radio.ul_snr_h	Uplink SNR (dB) horizontal		SM
radio.ul_snr_v	Uplink SNR (dB) vertical		SM
radio.ul_throughput	Uplink Throughput (Kbps)	AP/SM	AP/SM

PTP

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
sm_count	Connected SM count	Master
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All

Ethernet

Name	Details	Mode
ethernet.aux_ interface.max_rx	AUX maximum receive bytes	All
ethernet.aux_ interface.max_tx	AUX maximum transmit bytes	All
ethernet.aux_ interface.min_rx	AUX minimum receive bytes	All
ethernet.aux_ interface.min_tx	AUX minimum transmit bytes	All
ethernet.aux_ interface.pkt_error	AUX packet error	All
ethernet.aux_interface.rx	AUX receive bytes	All
ethernet.aux_interface.tx	AUX transmit bytes	All
ethernet.link_loss	Link loss	All
ethernet.main_psu_ interface.max_rx	Main PSU maximum receive bytes	All

Name	Details	Mode
ethernet.main_psu_ interface.max_tx	Main PSU maximum transmit bytes	All
ethernet.main_psu_ interface.min_rx	Main PSU minimum receive bytes	All
ethernet.main_psu_ interface.min_tx	Main PSU minimum transmit bytes	All
ethernet.main_psu_ interface.pkt_error	Main PSU packet error	All
ethernet.main_psu_ interface.rx	Main PSU receive bytes	All
ethernet.main_psu_ interface.tx	Main PSU transmit bytes	All
ethernet.pcb_ temperature	PCB temperature	All
ethernet.rx_channel_util	Receive channel utilization	All
ethernet.rx_capacity	Receive capacity	All
ethernet.ssr	Signal strength ratio	All
ethernet.rx_power	Receive power	All
ethernet.rx_throughput	Receive throughput	All
ethernet.sfp_ interface.max_rx	SFP maximum receive bytes	All
ethernet.sfp_ interface.max_tx	SFP maximum transmit bytes	All
ethernet.sfp_ interface.min_rx	SFP minimum receive bytes	All
ethernet.sfp_ interface.min_tx	SFP minimum transmit bytes	All
ethernet.sfp_ interface.pkt_error	SFP packet error	All
ethernet.sfp_interface.rx	SFP receive bytes	All

Name	Details	Mode
ethernet.sfp_interface.tx	SFP transmit bytes	All
ethernet.tx_channel_util	Transmit channel utilization	All
ethernet.tx_capacity	Transmit capacity	All
ethernet.tx_power	Transmit power	All
ethernet.tx_throughput	Transmit throughput	All
ethernet.vector_error	Vector error	All

Wi-Fi

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
site	Site	All
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios

Name	Details	Mode
radio.24ghz.clients	Number of clients	All
radio.24ghz.rx_bps	Receive bits/second	Enterprise
radio.24ghz.throughput	Total throughput	All
radio.24ghz.tx_bps	Transmit bits/second	Enterprise

Name	Details	Mode
radio.5ghz.clients	Number of clients	All
radio.5ghz.rx_bps	Receive bits/second	Enterprise
radio.5ghz.throughput	Total throughput	All
radio.5ghz.tx_bps	Transmit bits/second	Enterprise

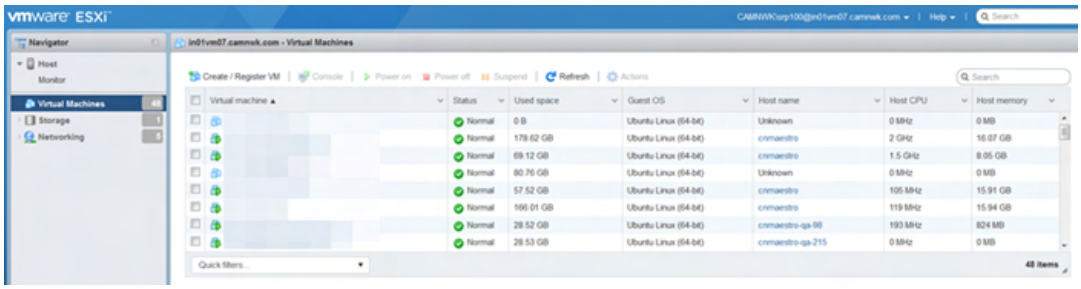
Deployments

VMware ESXi Installation

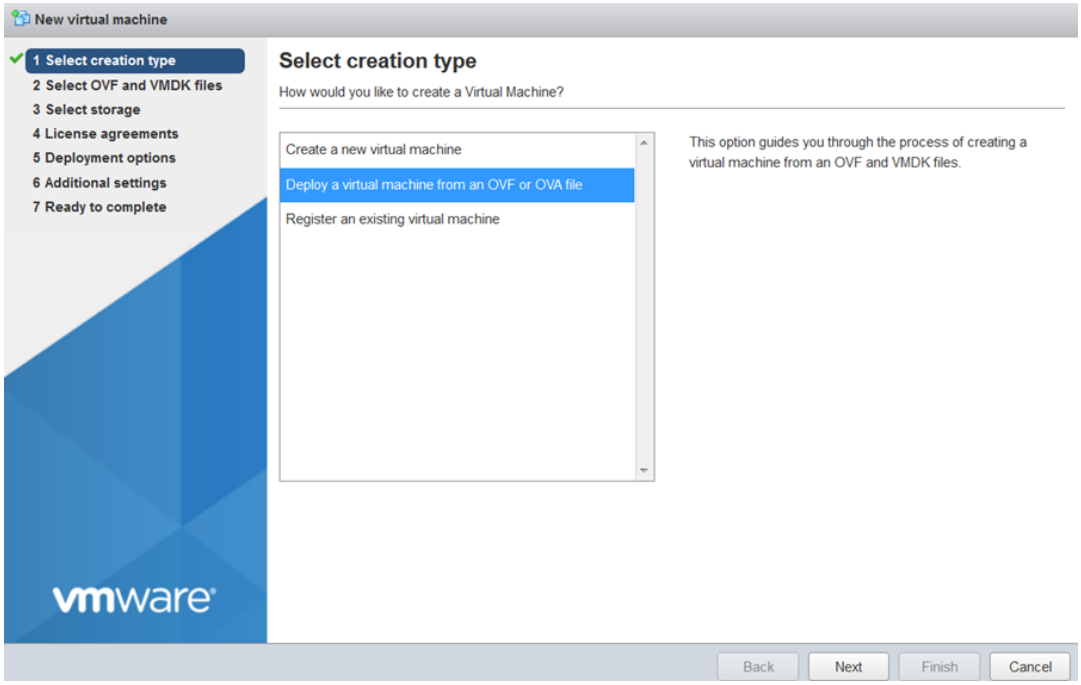
> **NOTE:**
>
> Deploying ESXi is an involved process. The steps below assume you have VMware ESXi version 6.0.0 Update 3 (Build 7967664) or higher already installed on hardware. If you don't have an ESXi hypervisor available, you can download it from VMware website. VMware provides directions for installing the ESXi ISO on a server.

cnMaestro VM Deployment

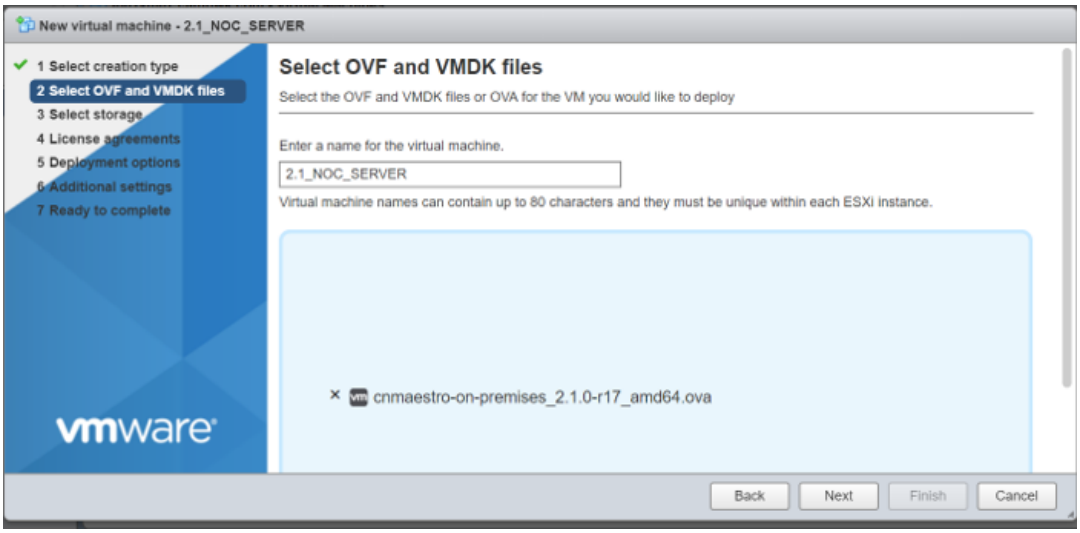
1. Login into ESXi host.
2. Click **Virtual Machines**.



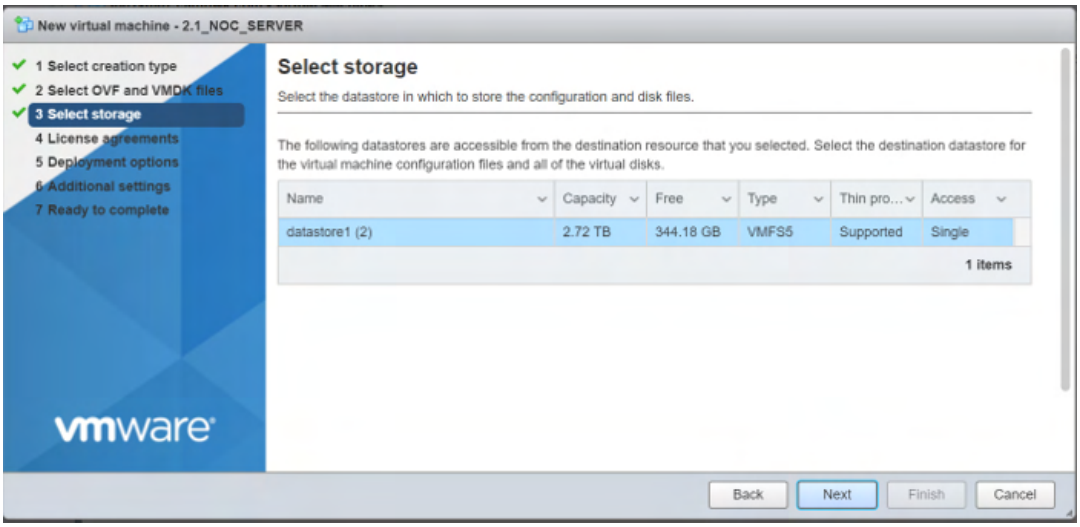
3. Click **Create/Register VM.**



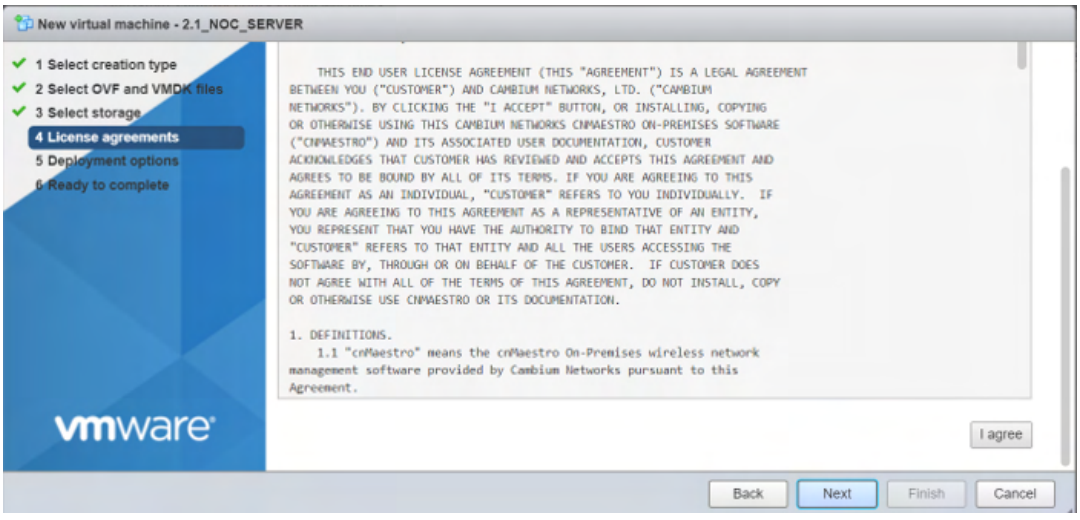
4. Click **Next**.



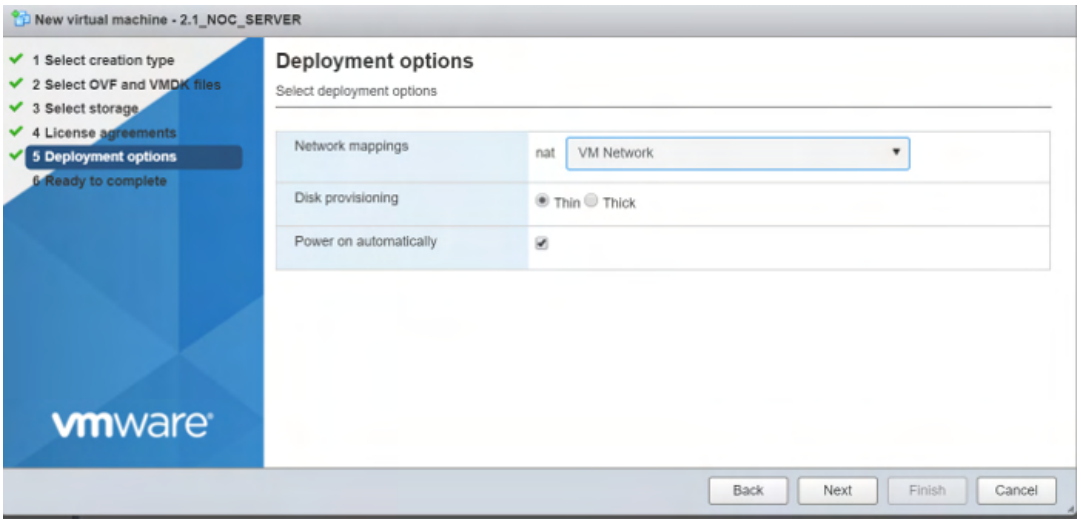
4. Select datastore which has more space



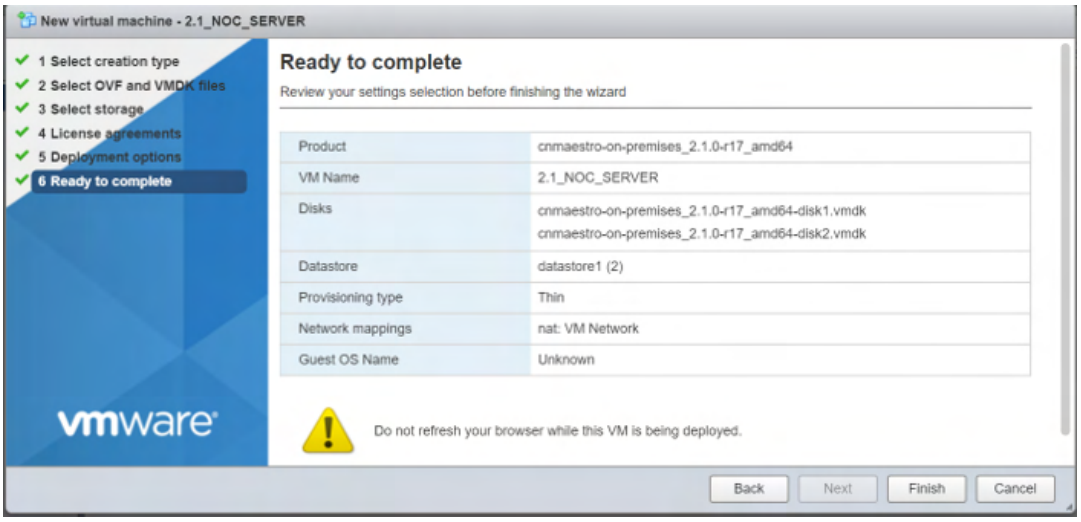
5. Click **Next**.



6. Click **I Agree** the license agreements and click **Next**.

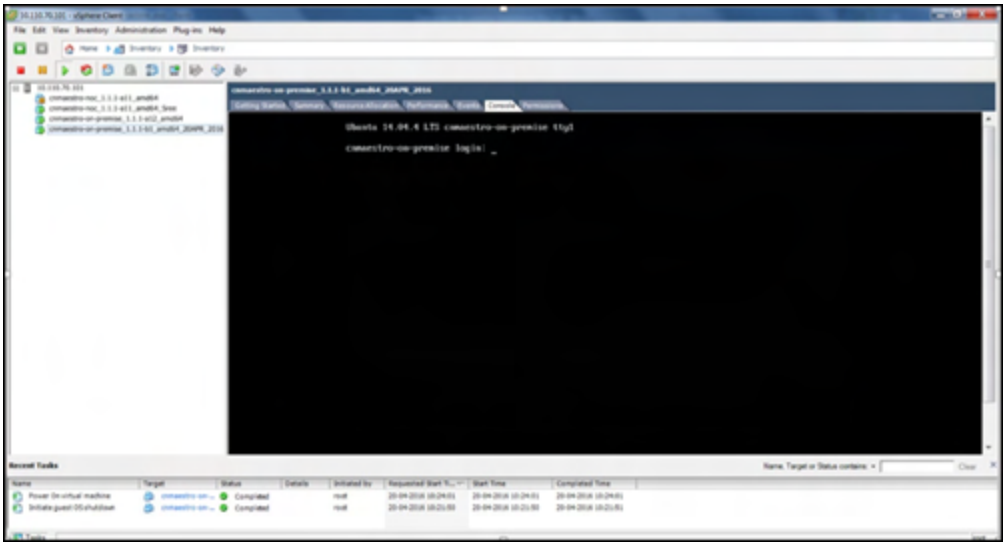


7. Select the network and click **Next.**



8. Verify the details and click **Finish** to complete deployment.

9. When the loading is complete, a virtual machine with the name chosen will appear. Choose the VM and click **power on** button.



10. Enter the default credentials (cambium/cnmaestro) in the console tab.

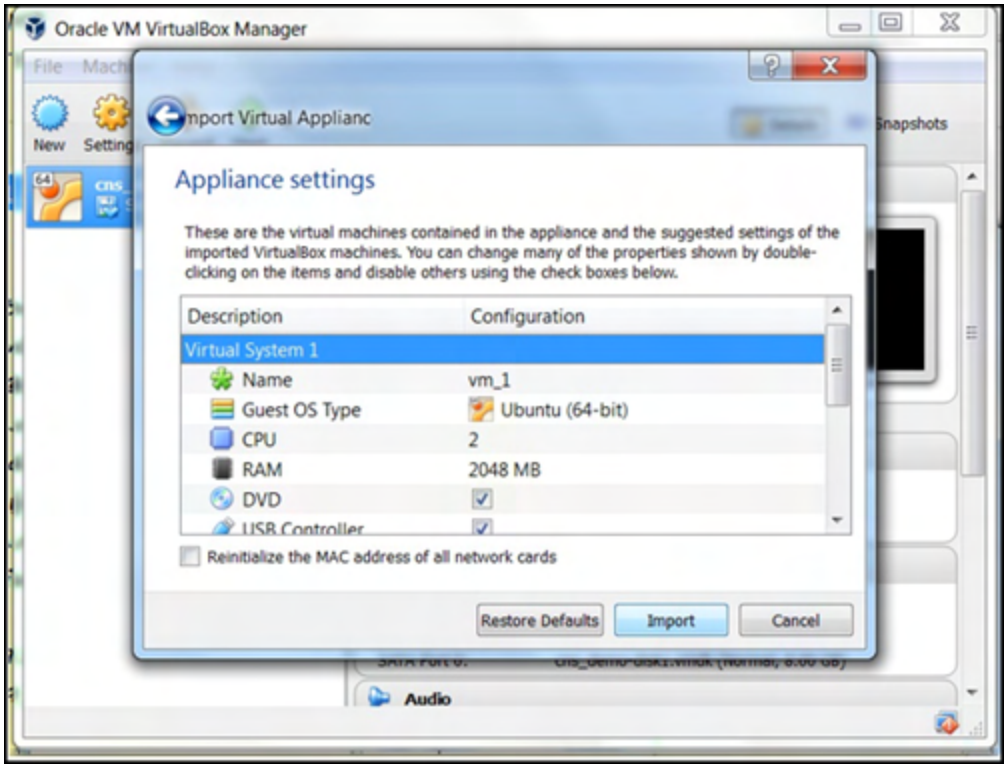
Oracle VirtualBox 5 Installation

Deployment

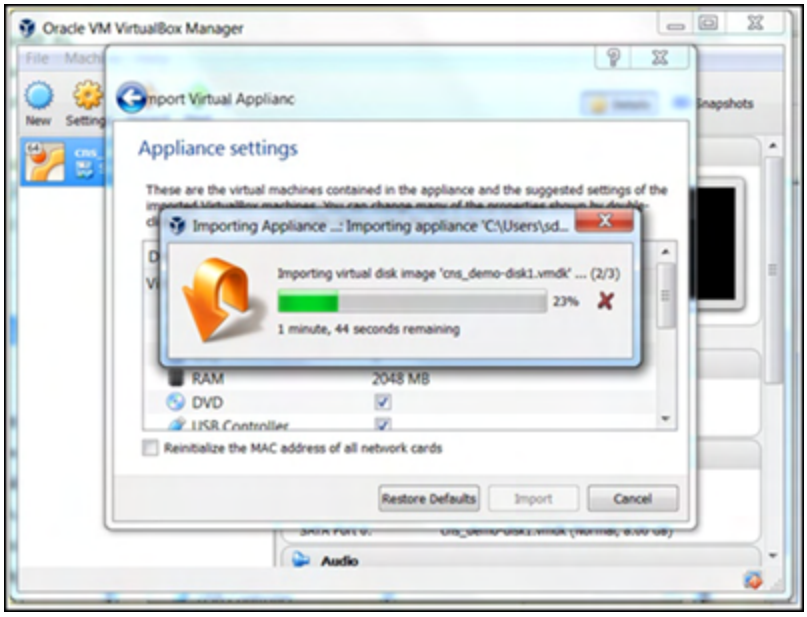
The steps to import cnMaestro On-Premises into Oracle VirtualBox are below. VirtualBox is not recommended for a production environment.

1. Open Oracle VirtualBox Manager, and select **File** > **Import Appliance**.
2. Browse and select CnMaestro On-Premises release OVA file and click **Next** to continue.

3. Configure the resources required for the VM.

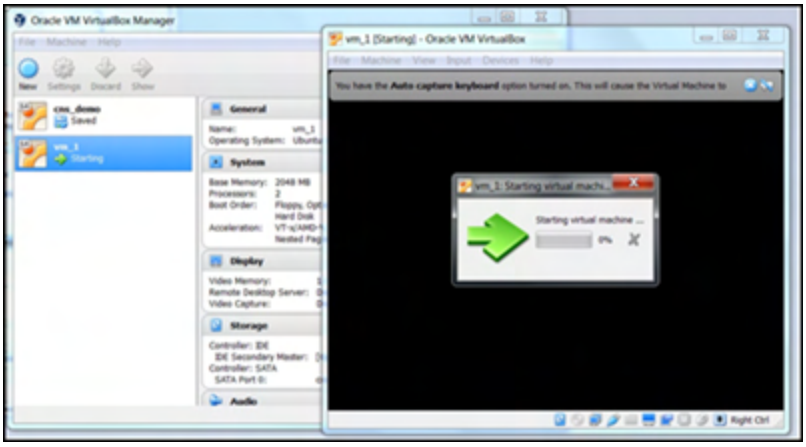


4. Click **Import**.



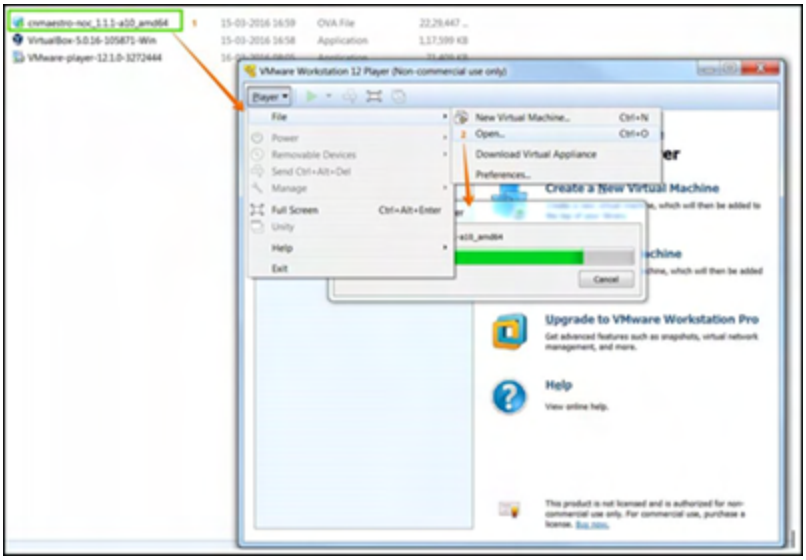
5. The new VM will appear on the left panel. Select the VM and click **start VM** and navigates to the configuration screen.

The new virtual machine appears in the left panel. After the VM is started, customer gets the login screen, and continue to configure cnMaestro and access the UI.

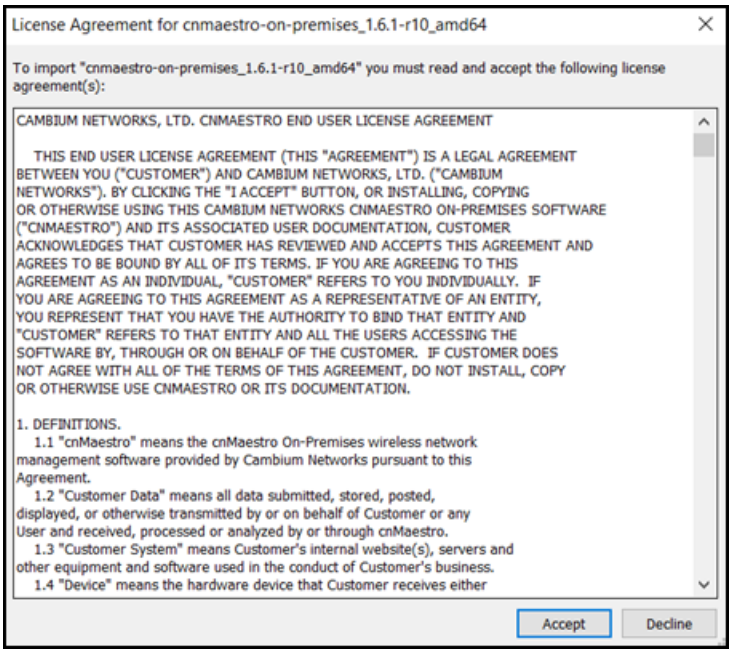


VMWare Workstation

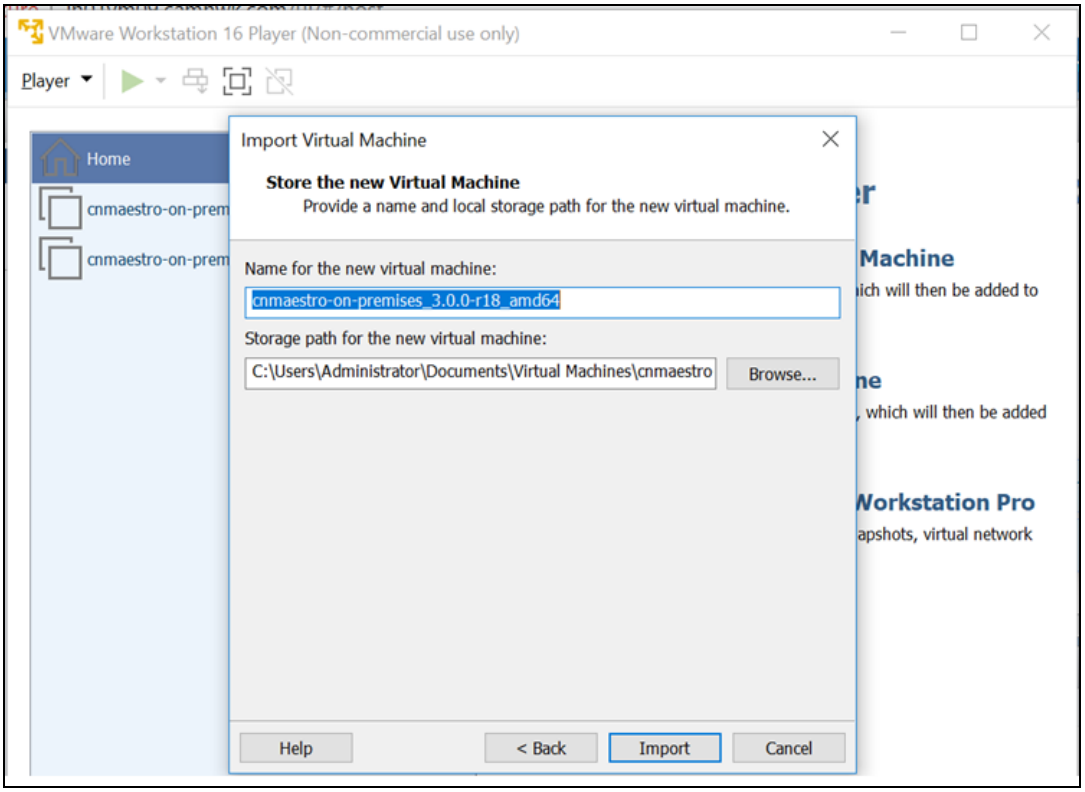
1. Open VMware workstation player. Navigate to **Player > File > Open Menu** and select CnMaestro On-Premises release OVA file.



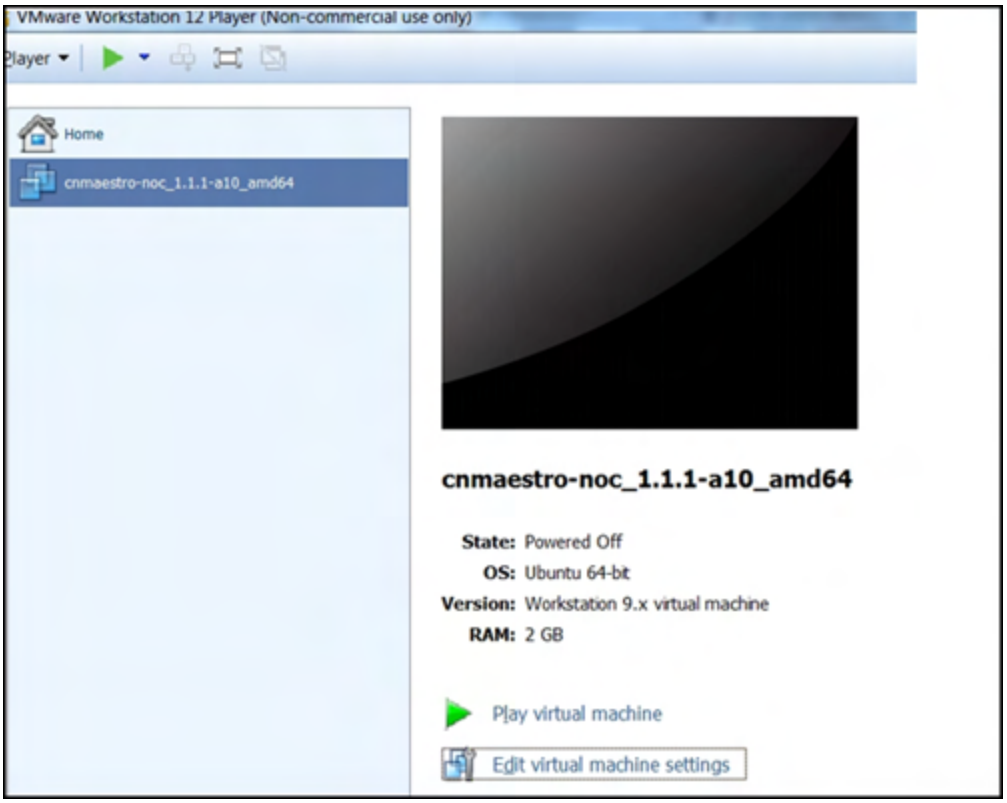
2. Accept the cnMaestro EULA, once the EULA is accepted, cnMaestro will be imported into the VM environment and it could take a couple minutes.



3. Click **Import** to start the deployment.



4. Once the file is loaded, click **Play** and wait for the configuration screen.



KVM Installation

	NOTE: KVM is not officially recommended for cnMaestro deployment. The directions below are for customers who want to evaluate the system in a KVM 0.9.5 or later environment.

Deployment

After installing KVM on the hardware, follow the below steps to import cnMaestro On-Premises into KVM:

1. **Extract cnMaestro On-Premise OVA**

$ tar xvf cnmaestro-on-premises_1.2.1-b19_amd64.ova

cnmaestro-on-premises_1.2.1-b19_amd64.ovf

cnmaestro-on-premises_1.2.1-b19_amd64.mf

cnmaestro-on-premises_1.2.1-b19_amd64-disk1.vmd

2. **Convert vmdk image to qcow2**

$ qemu-img convert -O qcow2 cnmaestro-on-premises_1.2.1-b19_amd64-disk1.vmdk cnmaestro-on-premises_1.2.1-b19_amd64.qcow

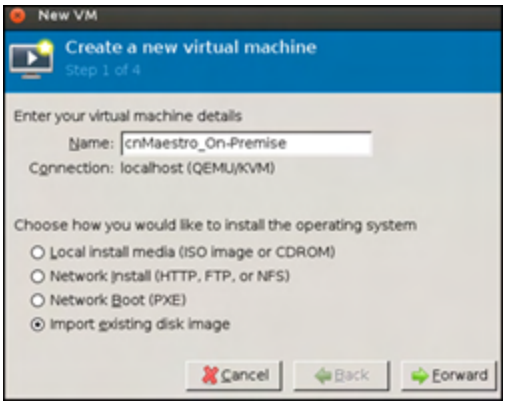
3. **Create New VM**

a. Launch Virtual Machine manager.

b. Create new VM.

c. Choose **import existing disk image**.

d. Click **Forward.**

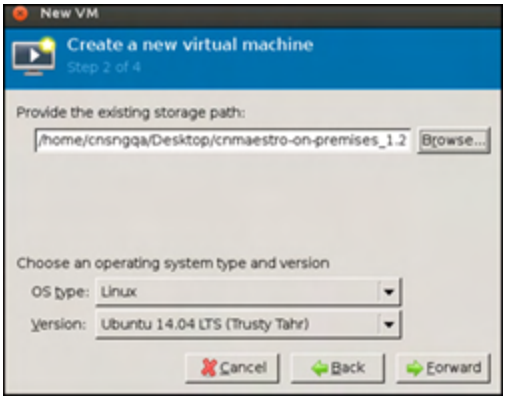


4. Select disk image file

a. Choose **qcow2** image that is created in earlier steps.

b. Select OS type as **Linux**

c. Click **Forward.**



5. Configure Memory and CPU

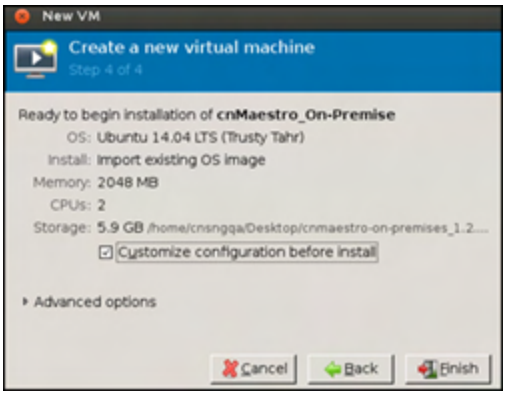
Configure Memory and CPU settings as per the requirements.



6. Customize other VM Configuration

a. Select **Customize Configuration before install** check box

b. Click **Finish**.



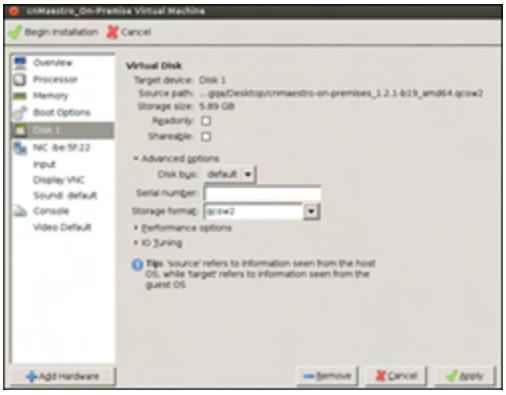
7. **Set Disk format to qcow2**

   a. Select **Disk** from the options on the left side.

   b. Expand **Advance options** section.

   c. Choose Storage format: as “qcow2”.

   d. Click **Apply**.



8. **Configure Network Adapter**

   a. Select NIC from the left pane.

   b. Select the appropriate source device. Default: NAT.

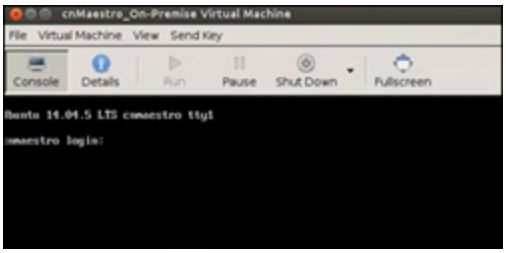
   c. Click **Apply**.



9. **Begin Installation**

   a. Click **Begin installation** on the top left. It would take few minutes to complete.

   b. After installation console may show blank for some time. Wait for 10-15 minutes. Restart VM if **cnmaestro login**: prompt is not shown.


cnMaestro_On-Premise Virtual Machine
File Virtual Machine View Send Key
Console
Details
Run
Pause
Shut Down
Fullscreen
Ubuntu 14.04.5 LTS cnmaestro tty1
cnmaestro login:

Windows DHCP

This section details how to configure a Microsoft Windows-based DHCP server to send DHCP Options to Cambium Networks devices such as ePMP, ePMP 1000 Hotspot, and cnPilot Enterprises and Home devices.

Following settings has to be configured:

- Configuring Option 60
- Configuring Option 43
- Configuring Option 15
- Configuring Vendor Class Identifiers
- Defining DHCP Policies

DHCP servers are a popular way to configure clients with basic networking information such as an IP address, default gateway, network mask, and DNS server. Most DHCP servers have the ability to also send a variety of optional information, including the Vendor-Specific Option Code Option 43. When a Cambium device requests Option 43 Vendor Specific Information, the DHCP server responds with values configured by the DHCP administrator.

Configuring Option 60

This section describes how to configure the Vendor Class Identifier Code (option 60) on a Microsoft Windows-based DHCP server. As mentioned in the overview section, option 60 identifies and associates a DHCP client with a particular vendor. Since option 60 is not a predefined option on a Windows DHCP server, you must add it to the option list.

Windows DHCP Server Configuration

1. On the DHCP server, open the DHCP server administration tool by clicking **Start > Administrative Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Select **Set Predefined Options**.
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information and click **OK** to save.

Field	Information
Name	CambiumOption60
Code	60
Data Type	String (select the Array check box also)
Description	Cambium AP vendor class identifier

5. In the Predefined Options and Values dialog box, make sure **060 CambiumOption60** is selected from the Option Name drop-down list.
6. In the Value field, enter the following information: String: Cambium, Cambium-WiFi-AP, Cambium-cnPilot r200P, Cambium-cnPilot R201P
7. Click **OK** to save this information.

8. Under the server, select the scope you want to configure and expand it. Select **Scope Options**, then select **Configure Options**.
9. In the Scope Options dialog box, scroll down and select **060 CambiumOption60**. Confirm the value is set as mentioned in point 7 above and click **OK**.



NOTE:

The Data type should be string. If only one device type is to be onboarded to the cnMaestro server, then there is no need to select the Array option. If multiple device types need to be onboarded, then please select the Array option, so the value can contain multiple option 60 entries.

Configuring Option 43

Option 43 returns the cnMaestro URL to the Cambium Devices.

Windows DHCP Server Configuration

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Select Set Predefined options
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information:

Field	Information
Name	CambiumOption43
Code	43
Data Type	String
Description	Cambium AP Option 43

5. Click **OK** to save this information.
6. In the Predefined Options and Values dialog box, make sure **043 CambiumOption43** is selected from the Option Name drop-down list.
7. In the Value field, enter the following information: String: https://<NOC Server Hostname/IP>
8. Click **OK** to save this information.



NOTE:

If Option 43 is already in predefined options with the data type as Binary, then it cannot be changed to string. If this is the case, while defining the policies, specify the values in the ASCII column in the Actions tab of the policy after selecting Option 43. This will be detailed in the Policies section later in the document.

Configuring Option 15

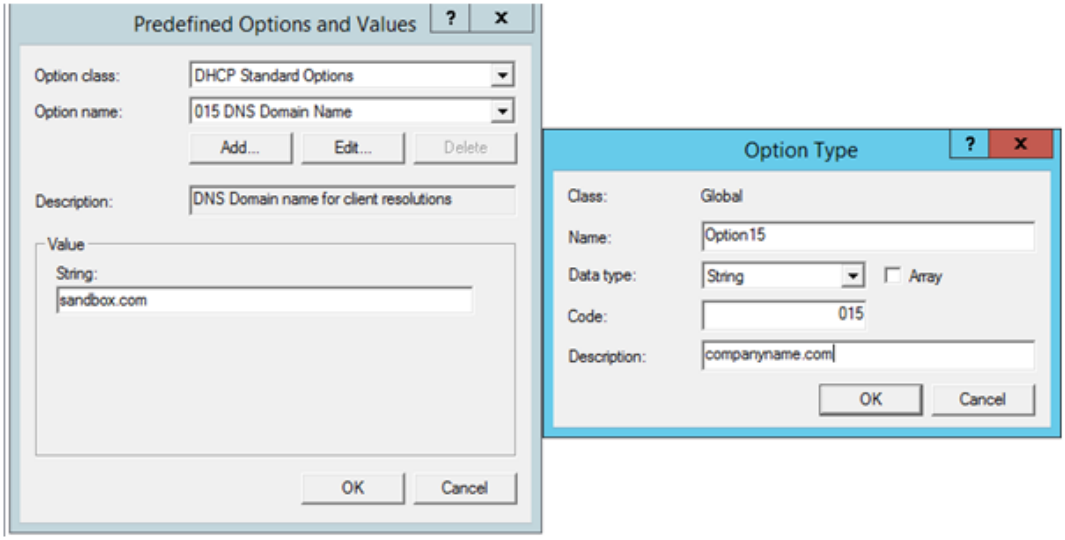
Option 15 returns the domain name to the Cambium Devices.

Windows DHCP Server Configuration

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Click on Set Predefined Options
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information:

Field	Information
Name	CambiumOption15
Code	15
Data Type	String
Description	Cambium AP Option 15

5. Click **OK** to save this information.
6. In the Predefined Options and Values dialog box, make sure **015 CambiumOption15** is selected from the Option Name drop-down list.
7. In the Value field, enter the following information: String: <companyname.com>
8. Click **OK** to save this information.



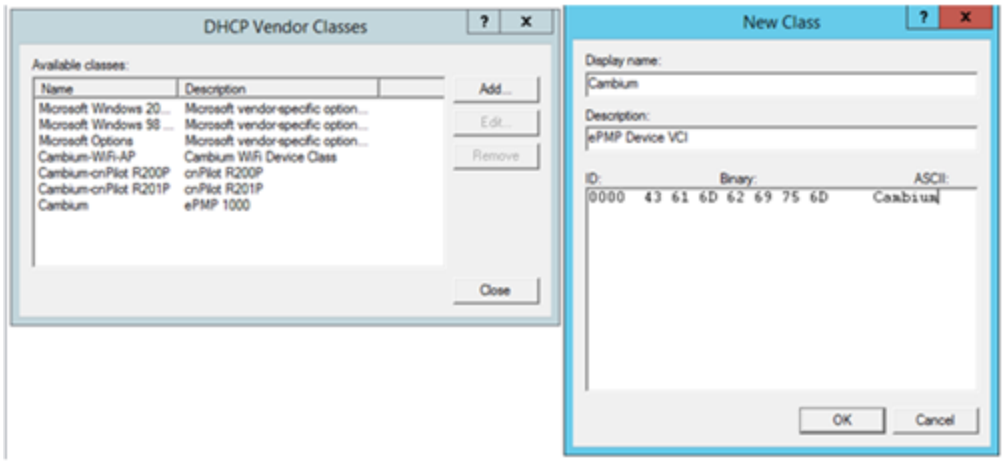
NOTE:

In the DNS Server, the user needs to map the cnMaestro hostname to the IP address of the cnMaestro On-Premises server.

Configuring Vendor Class Identifiers

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.

2. Find your server and right-click on the scope to be configured under the server name. Click on the **Define Vendor Classes** and click the **Add** button in the dialog box that appears.
3. Provide the Display name, Description and then click in the ASCII column and enter the value as Cambium as shown in the below figure, and then click **OK**.



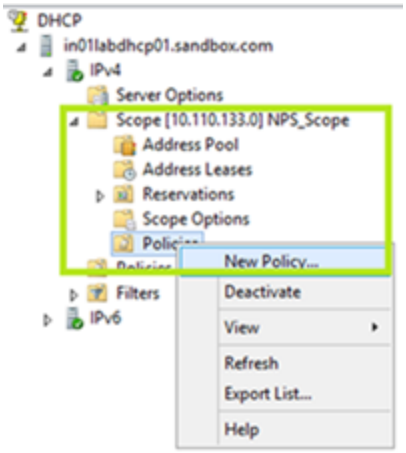
The above example is for an ePMP device. In order to create the VCI for other device types, please follow the same steps, and in the ASCII column provide the following values:

Product	VCI (DHCP Option 60)
cnPilot R200P	Cambium-cnPilot r200P
cnPilot R201P	Cambium-cnPilot R201P
cnPilot R190	Cambium-cnPilot R190
cnPilot Enterprise	Cambium-WiFi-AP
ePMP	Cambium
ePMP 1000 hotspot	Cambium-WiFi-AP

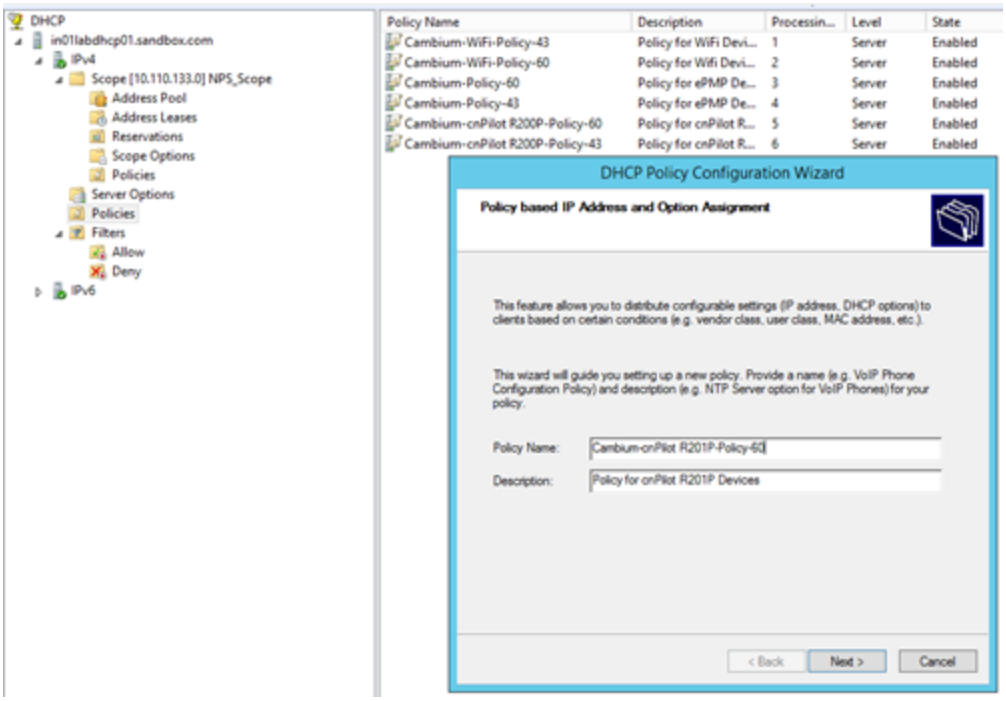
Configuring the Policies at the SCOPE Level

Once Options 43, 60, 15, and Vendor Classes are created, one needs to create policies at scope level. This allows the DHCP server to send the Option 43 and 60 to the Cambium Devices -- based on their VCI for that device. The policy will make sure these options are only sent if the VCI matches that provided by the device.

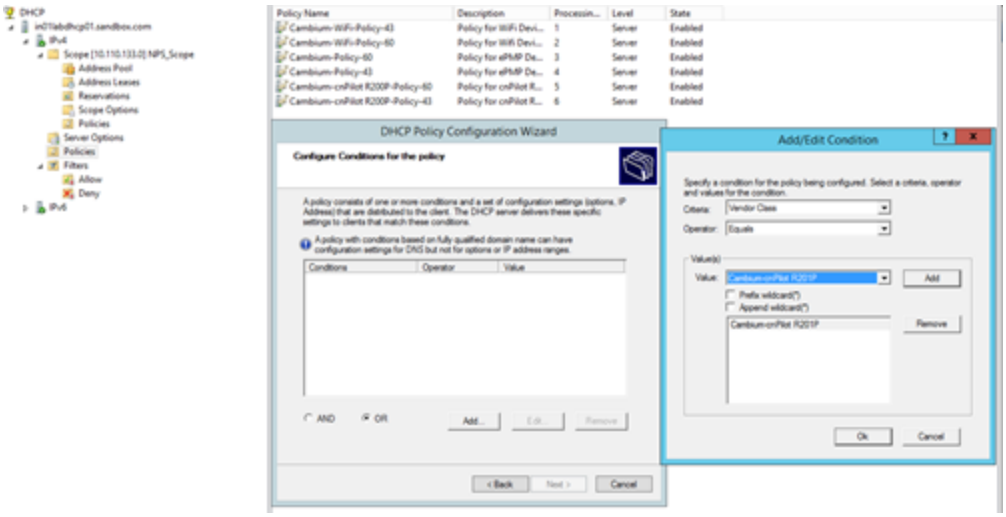
1. Select the scope in which you want to create the policy, and then right click on the Policies option. Select New Policy.



2. In the pop-up, enter the Policy Name and Description and click **Next** button.



3. The Policy consists of Matching conditions based on Vendor Class, user class, MAC Address, Client Identifiers, FQDN and Relay Agent Information. For Cambium Devices we need Vendor Class based match conditions only.
   a. In the dialog, click on the **Add** button and in the pops-up select the Criteria as **Vendor Class**, the Operator as **Equals**, and the Value as the VCI created for the Cambium Device type.
   b. For example, for cnPilot R201P device the Vendor Class selection is “Cambium-cnPilot R201P”.
   c. Click **Add** and then **OK** in the pop-up. Click **Next** in the Policy Configuration Wizard.

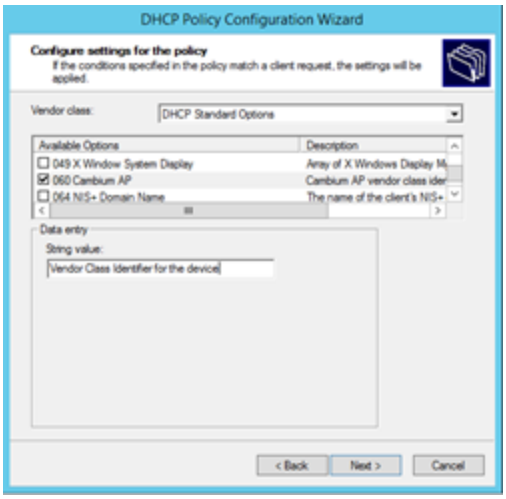


4. In the policy configuration settings wizard, select the option **No** and click **Next**.

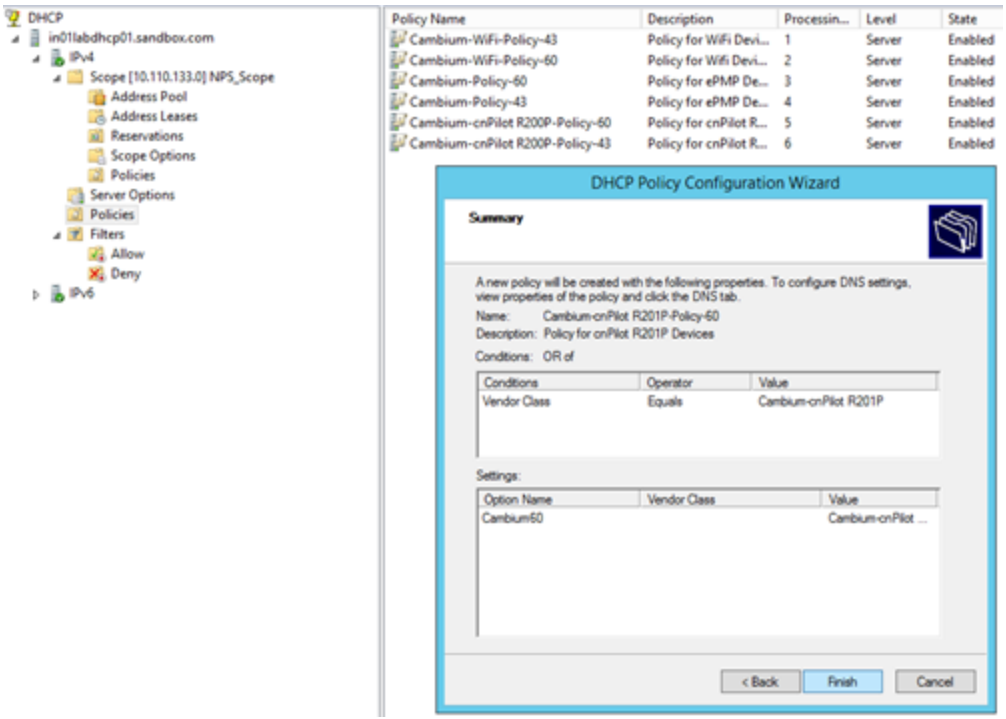


Then select the vendor class as DHCP standard options and Select the options 43 and 60 from the available options and specify the values that need to be sent to the device. Click **Next** once the options are selected and values are specified.





5. Click Finish in the final settings page. The policy is displayed in the RHS pane.



The above Policy is a generic one. For all the device types, the policies should be created in a similar way --, with the match conditions and action as follows:

Also the Policies can be created at the Scope level or Server level. If separate scope is defined for Cambium devices, it is better to define scope level policies; otherwise the policies can be defined at the Server level in the similar way.

Device Type	Match Condition	Actions
cnPilot E-Series	Vendor Class for E400/E410/E425H/E500/E501S/E502S/E505/E600	Cambium option 43 and 60 selected and values specified
cnPilot Home	Vendor Class for cnPilot R190/R195/R200/R201	Cambium option 43 and 60 selected and values specified
ePMP	Vendor Class for ePMP	Cambium option 43 and 60 selected and values specified
ePMP 1000 Hotspot	Vendor Class for Hotspot	Cambium option 43 and 60 selected and values specified

Citrix Hypervisor Installation

Overview

cnMaestro can be installed on Citrix Hypervisor (formerly known as XenServer). The OVA image can be downloaded from the Cambium Support Center https://support.cambiumnetworks.com/.

Resources

The following resources are required for deployment.



Note:

1. If NBI APIs or Performance Data Reports are extensively used, vCPUs and RAM should be increased by 50%.
2. SSD disks are recommended to improve performance.

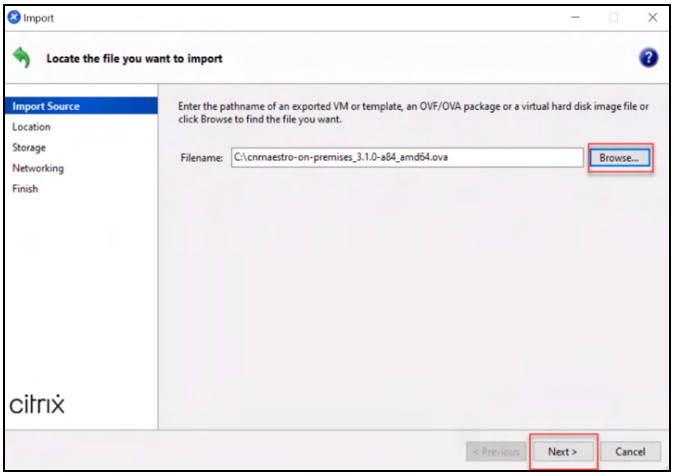
Table 67: Supported devices

Number of Devices	Wireless Clients	Number of vCPUs	RAM Size (GB)	Hard Disk (GB)
1 - 100	Up to 1500	2	4	120
101 – 1,000	Up to 15,000	4	4	120
1,001 - 4,000	Up to 60,000	4	8	150
4,001 - 10,000	Up to 150,000	8	16	250

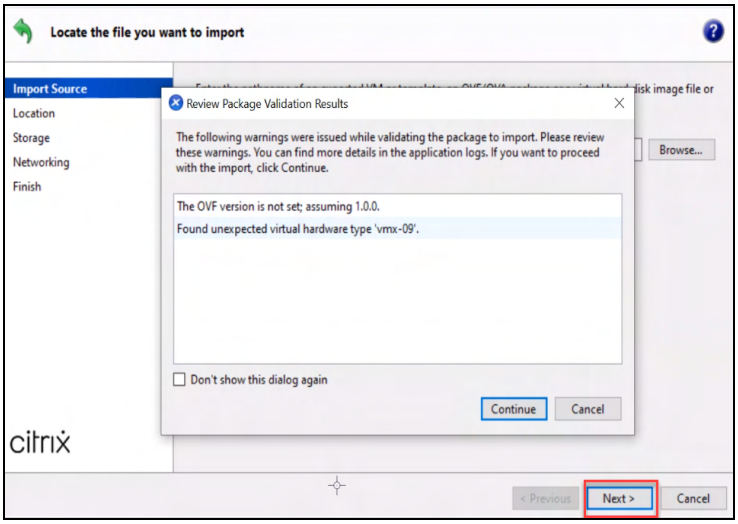
Import using Citrix Hypervisor

Perform the following steps to install the Citrix Hypervisor:

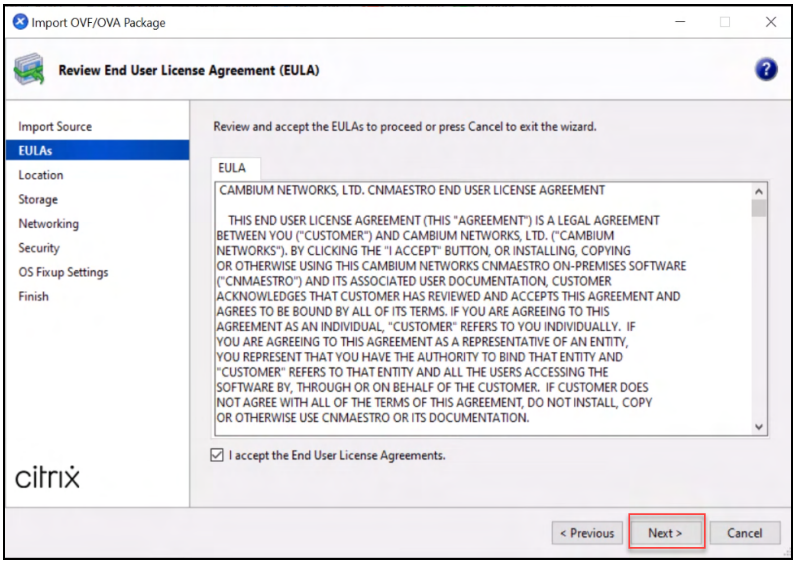
1. Navigate to **XenCenter** and right-click **citrix hypervisor.**
2. Click **Import**.
3. Click **Next** on the import wizard, browse to the downloaded OVA and click **Next.**



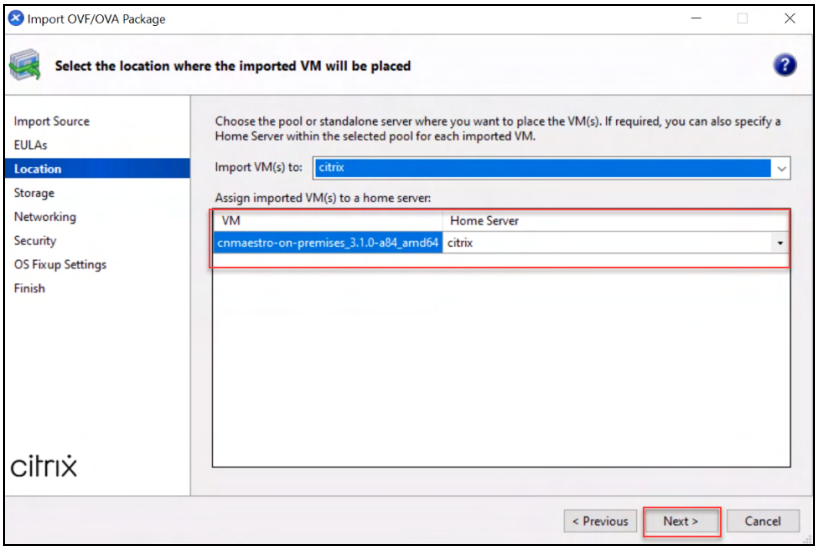
4. Review the Package Validation results and click **Next**.



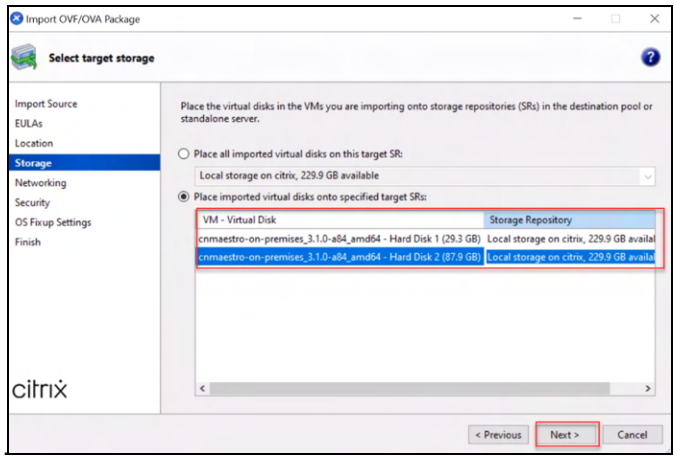
5. Accept the EULA.



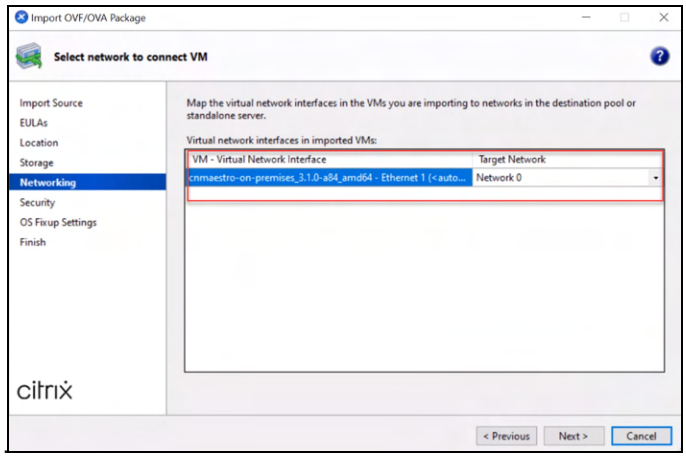
6. Select the location where the imported VM will be placed.



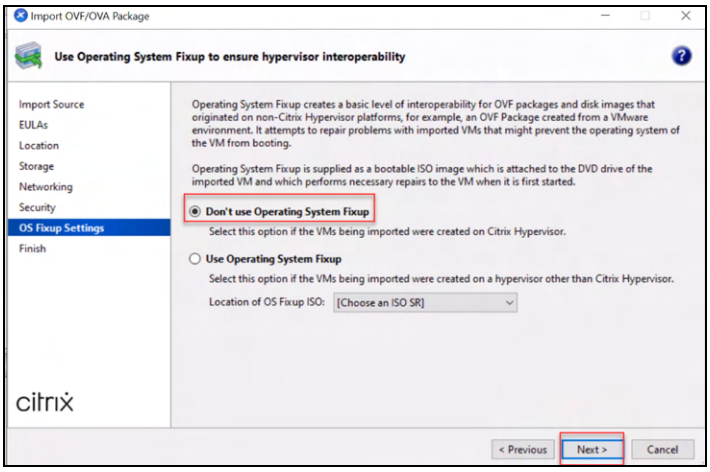
7. Select a storage repository for the second/data disk.



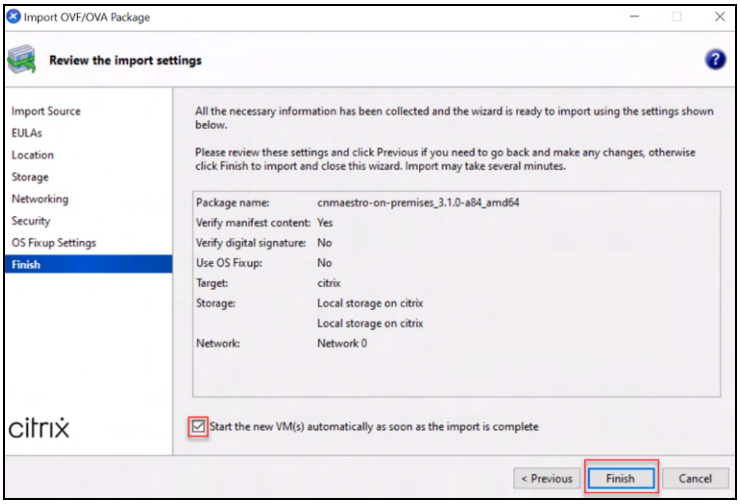
8. Select a network.



9. Verify the included manifest to ensure the OVA is not damaged. Select **Don't use Operating System Fixup**.

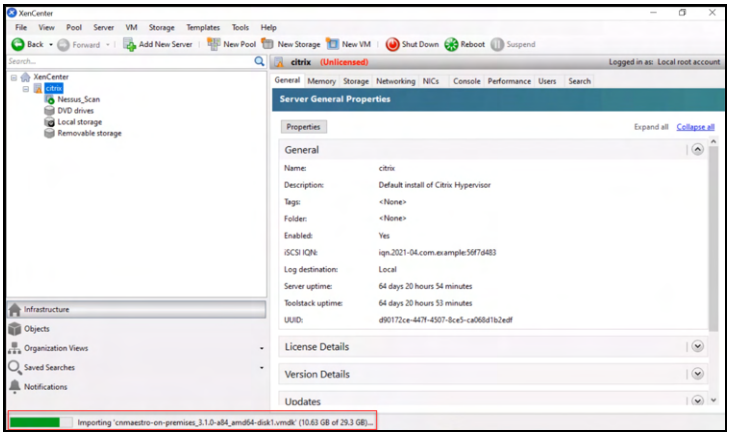


10. Enable the check box to start a new VM when the import completes.

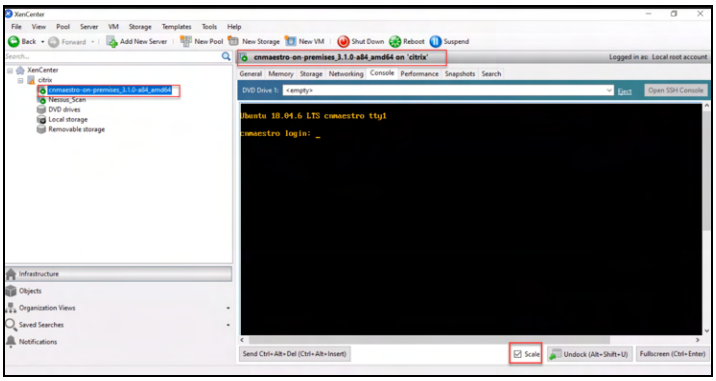


11. Click **Finish**.

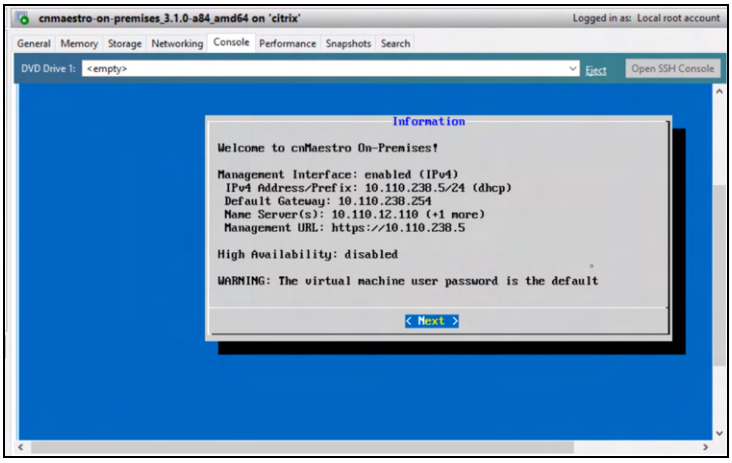
The Import might take few minutes depending on the network, number of hard disks, and the Storage Repository speed. Once the Import completes, start the VM. The Import status can be viewed in the status bar as shown in the figure below.



12. The new VM will appear on the left panel. Select the VM and click **Start VM** and navigate to the configuration screen.



13. Open the **Console** tab and login with user name **cambium** and default password **cnmaestro**.
14. If needed, the **Scale** option may make the console easier to view.
15. The console provides status as well as a basic settings interface for the appliance.



Access cnMaestro

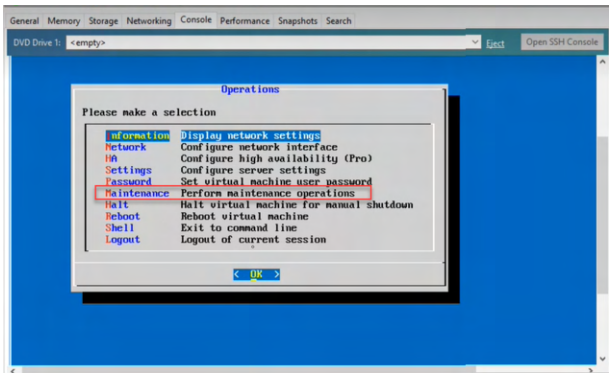
SSH Access

	Note: • The TUI warns if you have not changed the default password. • Uncheck **Scale** option to view console.

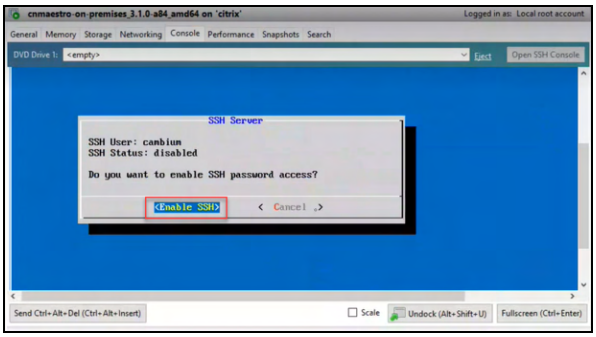
SSH access is disabled by default.

To enable SSH

1. Navigate to **Maintenance > SSH** in the menu.



2. Select **Enable SSH**.



Once enabled, you can access cnMaestro over SSH. You must change the default password before enabling SSH.

HTTPS Access

You can launch the web UI over HTTPS by entering the cnMaestro IP address in the browser. The default SSL certificate is self-signed and will generate a self-signed certificate error. After logging in, you can upload a custom certificate by navigating to **Administration > Server > SSL Certificates** in the web UI.

Advanced Options

Expand the Data Disk

	**Warning:** Always take a snapshot of the data volume before expanding it.

The data volume can be expanded at any time as the number of devices in the account increases. The process consists of two parts:

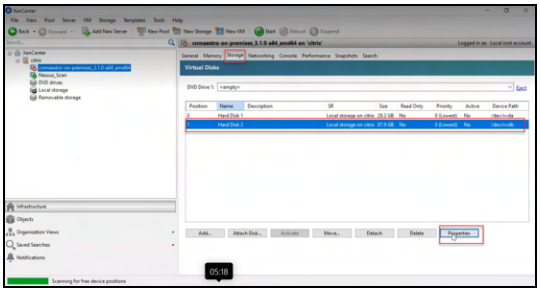
- Expand the volume through Citrix Hypervisor
- Expand the file system within cnMaestro

Expand the volume through Citrix Hypervisor

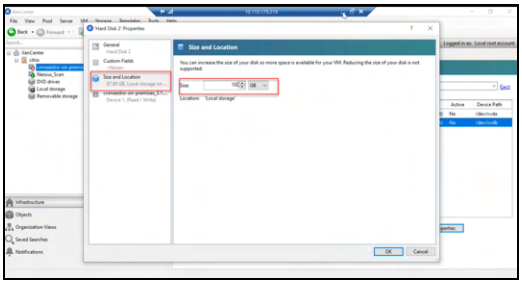
Expand the volume using the Citrix Hypervisor:

	**Note:** Shutdown the VM before increasing the hard disk size.

1. Open the VM **Storage** tab.



2. Right-click on the data disk (by default **Hard Disk 2** is selected).
3. Click **Properties**.
4. In the **Size and Location** tab, increase size of hard disk selected and click **OK**.



5. Restart the VM.

Expand the file system within cnMaestro

If the file system is not automatically expanded, you may need to do this manually. You can do this by using the cnMaestro Console or SSH.

1. Login to cnMaestro through SSH and exit to the command line.
2. Run `lsblk` command to determine the disk that maps to the data store.

- The name might be different, depending on the type of image originally selected for the instance.

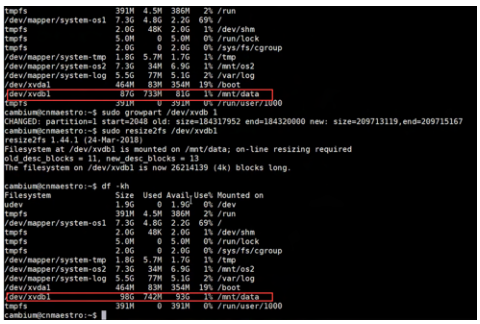
3. Grow the partition to use the full disk.

For example, expand partition 1 of the /dev/xvdb device:

```
sudo growpart /dev/xvdb 1
```

4. Grow the file system mapping to /mnt/data. For the above example, execute the below command:

```
sudo resize2fs /dev/xvdb1
```



Network Requirements

Inbound Ports

The following table provides information about network port requirements for inbound:

Table 68: Inbound Port Details

Serial Number	Port Number	Port Type	Purpose
1	443	TCP	HTTPs Web Access and device communication
2	18301	TCP/UDP	Wi-Fi Performance Test
3	161	UDP	SNMP Communication
4	22	TCP	Data Replication (High Availability)
5	8300	TCP	Distribution Synchronization (High Availability)
6	8301	TCP/UDP	Distribution Synchronization (High Availability)
7	3799	UDP	RADIUS CoA for RADIUS Proxy feature

Outbound Ports

The following table provides information about network port requirements for outbound:

Table 69: Outbound Port Details

Serial Number	Port Number	Port Type	Purpose
1	18301	TCP/UDP	Wi-Fi Performance Test
2	162	UDP	SNMP Trap Receiver
3	465 and 587	TCP	SMTP Server communication
4	20 and 21	TCP	FTP and SFTP communication
5	49	TCP/UDP	TACAC Server communication
6	1812	UDP	Free Radius Server Authentication communication
7	1813	UDP	RADIUS Server Accounting communication
8	389 and 636	TCP/UDP	LDAP or Active Directory (AD) server communication
9	514	UDP	Syslog server

Custom Network Scripts

If your network requirements are more complex than cnMaestro configuration, you can script custom networking commands, so they are executed after cnMaestro initializes networking. The commands are added to the file **/srv/files/etc/cnmaestro-network.override**, which also contains directions and a sample static route.

Contact Cambium Networks

Support Website	http://www.cambiumnetworks.com/support
Main Website	http://www.cambiumnetworks.com
cambium Community	http://community.cambiumnetworks.com
Sales Enquiries	solutions@cambiumnetworks.com
Support Enquiries	https://www.cambiumnetworks.com/support/contact-support/
Telephone Number List	http://www.cambiumnetworks.com/support/contact-support
Address	Cambium Networks Limited, 3800 Golf Road, Suite 360, Rolling Meadows, IL 60008 USA.