



RUCKUS SmartZone (LT-GA) Guest Access Guide, 6.1.1

Published from

CommScope Technical Content Portal by

29 January 2025

# CommScope Legal Statements

© 2025 CommScope, Inc. All rights reserved

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

## Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

*These items are controlled by the U.S. government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.*

## Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, CommScope DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability, or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

## Limitation of Liability

IN NO EVENT SHALL CommScope, CommScope AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIES, LICENSORS, AND THIRD-PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF CommScope HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

## Trademarks

All trademarks identified by ™ or ® are trademarks or registered trademarks in the US and may be registered in other countries. All product names, trademarks, and registered trademarks are property of their respective owners.

## Patent marking notice

For applicable patents, see [www.cs-pat.com](http://www.cs-pat.com). That website is intended to give notice under 35 U.S.C. § 287(a) of articles that are patented or for use under the identified patents. That website identifies the patents associated with each of the patented articles.

# Table of Contents

## Contact Information, Resources, and Conventions

### About This Guide

New in This Document. . . . .	9
-------------------------------	---

### Guests

Working with Guest Passes. . . . .	10
Guest Pass. . . . .	11
Guest Pass Template. . . . .	25

### Working with Hotspots and Portals

Creating a Guest Access Portal. . . . .	30
Working with Hotspot (WISPr) Services. . . . .	35
Creating a Hotspot (WISPr) Portal. . . . .	36
Working with Hotspot 2.0 Services. . . . .	44
Creating a Hotspot 2.0 WLAN Profile. . . . .	45
Creating a Hotspot 2.0 Venue Profile. . . . .	61
Creating a Web Authentication Portal. . . . .	63
Creating a UA Blacklist Profile. . . . .	65
Creating a Portal Detection and Suppression Profile. . . . .	67
Creating a WeChat Portal. . . . .	71
Creating Network Segmentation Profile on the vSZ Controller. . . . .	74

Ethernet Profiles..... 86

# Contact Information, Resources, and Conventions

---

## Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckusnetworks.com> and select **Support**.

### What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

### Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

## Self-Service Resources

The RUCKUS Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://community.ruckuswireless.com>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—[https://support.ruckuswireless.com/#products\\_grid](https://support.ruckuswireless.com/#products_grid)
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at [https://support.ruckuswireless.com/case\\_management](https://support.ruckuswireless.com/case_management).

## Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at [#Ruckus-Docs@commscope.com](mailto:#Ruckus-Docs@commscope.com).

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

## RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckusnetworks.com>.

## Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). You create a CommScope account and then register for, and request access for, CommScope University.

## Document Conventions

The following table lists the text conventions that are used throughout this guide.




**Table 1.** Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	device(config)# interface ethernet 1/1/6
<b>bold</b>	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

## Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

- **Note:** A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

-  **Attention:** An ATTENTION statement indicates some information that you must read before continuing with the current action or task.
-  **CAUTION:** A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.
-  **DANGER:** A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

## Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.  Default responses to system prompts are enclosed in square brackets.
{x  y  z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

# About This Guide

---

## New in This Document

## New in This Document

**Table 1.** Key Features and Enhancements in SmartZone 6.1.1 Rev B (October 2023)

Feature	Description	Reference
Minor style guide updates	Updated all the images and tables as per the style guide.	Throughout the guide.

Parent topic: [About This Guide](#)

# Guests

---

## Working with Guest Passes

## Working with Guest Passes

Guest Passes are temporary privileges granted to guests to allow access wireless LANs.

Many options are provided for customizing Guest Passes, controlling who is allowed to issue Guest Passes, and controlling the scope of access to be granted.

With Guest Pass authentication enabled, guests are required to enter a Guest Pass code when connecting to a guest WLAN. Temporary Guest Passes can be issued for single user, multiple users, one-time login, time-limited multiple logins for a single guest user, or can be configured so that a single Guest Pass can be shared by multiple users. Additionally, they can be batch-generated, if many short-term Guest Passes must be created at once.

Guest passes can be generated in two ways:

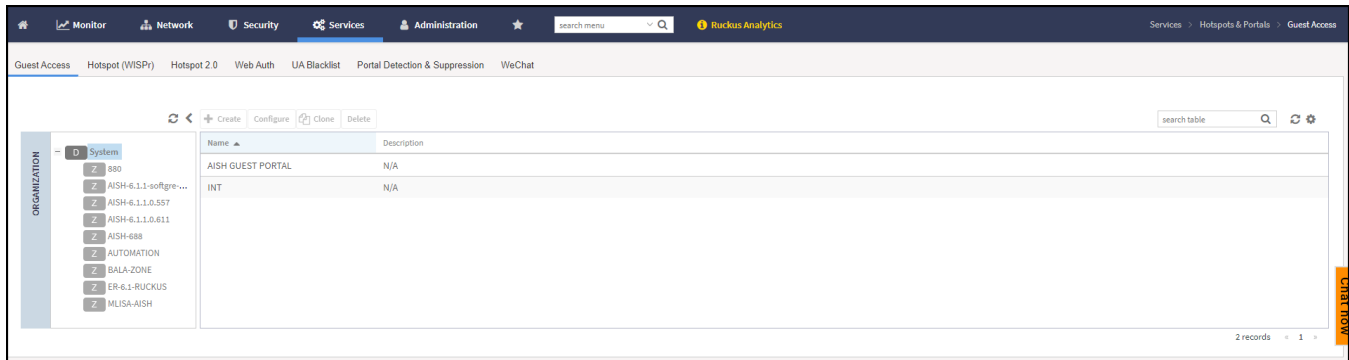
- Self-Service Generated Guest Passes
- Admin Generated Guest Passes

After generating a Guest Pass, they can be delivered in the following ways:

- Printout
- Send SMS with guest credentials
- Send email with guest credentials

- 🔗 **Note:** To enable Guest Pass delivery through email or SMS, you must first configure an email server or an SMS delivery account (Twilio or Clickatell) from the **Email** tab or the **SMS** tab (**Services > System Info**).
- 🔗 **Note:** To enable Guest Pass delivery through email or SMS, you must first configure an email server or an SMS delivery account (Twilio or Clickatell) from the **Email** tab or the **SMS** tab (**Services > System Info**).
- 🔗 **Note:** To enable Guest Pass delivery through email or SMS, you must first configure an email server or an SMS delivery account (Twilio or Clickatell) from the **Email** tab or the **SMS** tab (**Services > Hotspots & Portals > Guest Access**).

**Figure 1.** Guest Access



Parent topic: [Guests](#)

## Guest Pass

### SmartZone Guest Pass Self Registration

#### Admin Generated Guest Passes

Parent topic: [Working with Guest Passes](#)

## SmartZone Guest Pass Self Registration

Currently, Smart Zone Guest Access solution relies on assisted guest pass generation, which means IT or hotel staff needs to generate guest password to the client based on whatever credentials needed. To make the process simpler and for ZD parity, this feature is to make guest self-registration a possibility on SZ, so that steps can be configured and displayed on guest UE to guide them through a step by step process to obtain a key for the guest WLAN access.

Self-service guest pass registration only applies to guest access WLAN.

Complete the following steps to create a self registration guest pass:

1. On the menu, click **Services > Hotspots & Portals > Guest Access**. This displays the **Guest Access** window.
2. In the **Organization** tab, select the zone for which you want to create the guest access portal.
3. Click **Create** icon. This displays the **Guest Access Portal** dialog box.
4. In the **Guest Access** tab, switch on the **Self-registration** option and follow the guest pass registration process, refer to *Creating a Guest Access Portal*.

**Figure 1.** Self Registration

## Create Guest Access Portal

General Options

\* Portal Name:

Portal Description:

\* Language:

English

Redirection

Start Page:

After user is authenticated,

☒ Redirect to the URL that user intends to visit.
 ☐ Redirect to the following URL:

\*

Guest Access

Self-registration:

ON

Guest Pass SMTP Server:

OFF

\* Guest Pass SMS Gateway:

Disabled

OK

Cancel

Parent topic: [Guest Pass](#)

## Admin Generated Guest Passes

Guest passes allow temporary access to wireless LANs.

Parent topic: [Guest Pass](#)

### Step 1: Create a Guest Access Service

1. To create a guest access service in the Guest Access Portal.
2. When you finish creating a guest access service, continue to [Step 2: Create a Guest Access WLAN](#).

Parent topic: [Admin Generated Guest Passes](#)

### Step 2: Create a Guest Access WLAN

Guest passes are generated for specific WLANs only. Guest pass users will only be able to gain access to the WLANs for which the guest pass is generated.

Follow these steps to create a WLAN that will be used for guest access only.

1. On the menu, click **Network > Wireless > Wireless LANs** to display the **Wireless LANs** window.

**Figure 1. Wireless LANs**

Name	Alerts	SSID	Auth Method	Encryption Method	Clients	Traffic	VLAN	Application Recognition	Tunnelled	Status
AISH-6.1.1-802.1X	0	AISH-6.1.1-802.1X	802.1X	WPA2	0	0	76	Disabled	APBridg...	●
AISH-6.1.1-DHCP-NAT	0	AISH-6.1.1-DHCP-NAT	OPEN	NONE	0	0	76	Disabled	APBridg...	●
AISH-6.1.1-GUEST	0	AISH-6.1.1-GUEST	OPEN	NONE	0	0	76	Disabled	APBridg...	●
AISH-6.1.1-WEB	0	AISH-6.1.1-WEB	OPEN	NONE	0	0	76	Disabled	APBridg...	●
AISH-6.1.1-WISPR+802.1X	0	AISH-6.1.1-WISPR+802.1X	802.1X	WPA2	0	0	76	Disabled	APBridg...	●
AISH-6.1.1-WISPR+MAC	0	AISH-6.1.1-WISPR+MAC	MAC	NONE	0	0	76	Disabled	APBridg...	●
AISH-ALEXA	0	AISH-ALEXA	OPEN	NONE	0	0	27	Disabled	APBridg...	●
AISH-MLISA-802.1X	0	AISH-MLISA-802.1X	802.1X	WPA2	0	0	27	Disabled	APBridg...	●

2. In the **Organization** tab, select the zone from the group list for which you want to create the Wireless LANs. If you want to create a group, refer to *Creating a WLAN Group* in the *WLAN Management Guide*.
3. Click the **Create** icon to display the **Create WLAN Configuration** dialog box.

**Figure 2. Create WLAN Configuration**

**Create WLAN Configuration**

General Options

Authentication Options

Encryption Options

Data Plane Options

Accounting Service

Wireless Client Isolation

RADIUS Options

Firewall Options

Advanced Options

OK Cancel

4. In the **Authentication Options** tab, select **Guest Access** option to displays the **Guest Access Portal** tab.

**Figure 3.** Guest Access Portal

**Create WLAN Configuration**

General Options ▶

Authentication Options ▼

Authentication Type: ☐ Standard usage (For most regular wireless networks) ☐ Hotspot (WISPr) ☒ **Guest Access** ☐ Web Authentication

☐ Hotspot 2.0 Access ☐ Hotspot 2.0 Onboarding ☐ WeChat

Method: ☒ Open ☐ 802.1X EAP ☐ MAC Address ☐ 802.1X EAP & MAC

Encryption Options ▶

Data Plane Options ▶

**Guest Access Portal** ▶

Wireless Client Isolation ▶

RADIUS Options ▶

Firewall Options ▶

Advanced Options ▶

5. Complete the following fields:

**Figure 4.** Guest Access Portal: Guest and Always Accept

**Create WLAN Configuration**

Guest Access Portal ▼

Guest Authentication: ☒ Guest ☐ Always Accept ☐ Guest Access / Social Media Login ☐ Social Media Login

\* Guest Portal Service: Select a guest access ▼ + ✎

Bypass CNA: ☒ ON

Portal Detection & Suppression: System Default ▼ + ✎

Guest Accounting: ☒ OFF Use the controller as proxy

Disable ▼ + ✎

**Figure 5.** Guest Access Portal: Guest Access/Social Media Login and Social Media Login

**Guest Access Portal**

Guest Authentication: ☐ Guest ☐ Always Accept ☒ Guest Access / Social Media Login ☐ Social Media Login

\* Social Media Profile: Select a social media p


\* Guest Portal Service: INT

Bypass CNA: ☒ ON

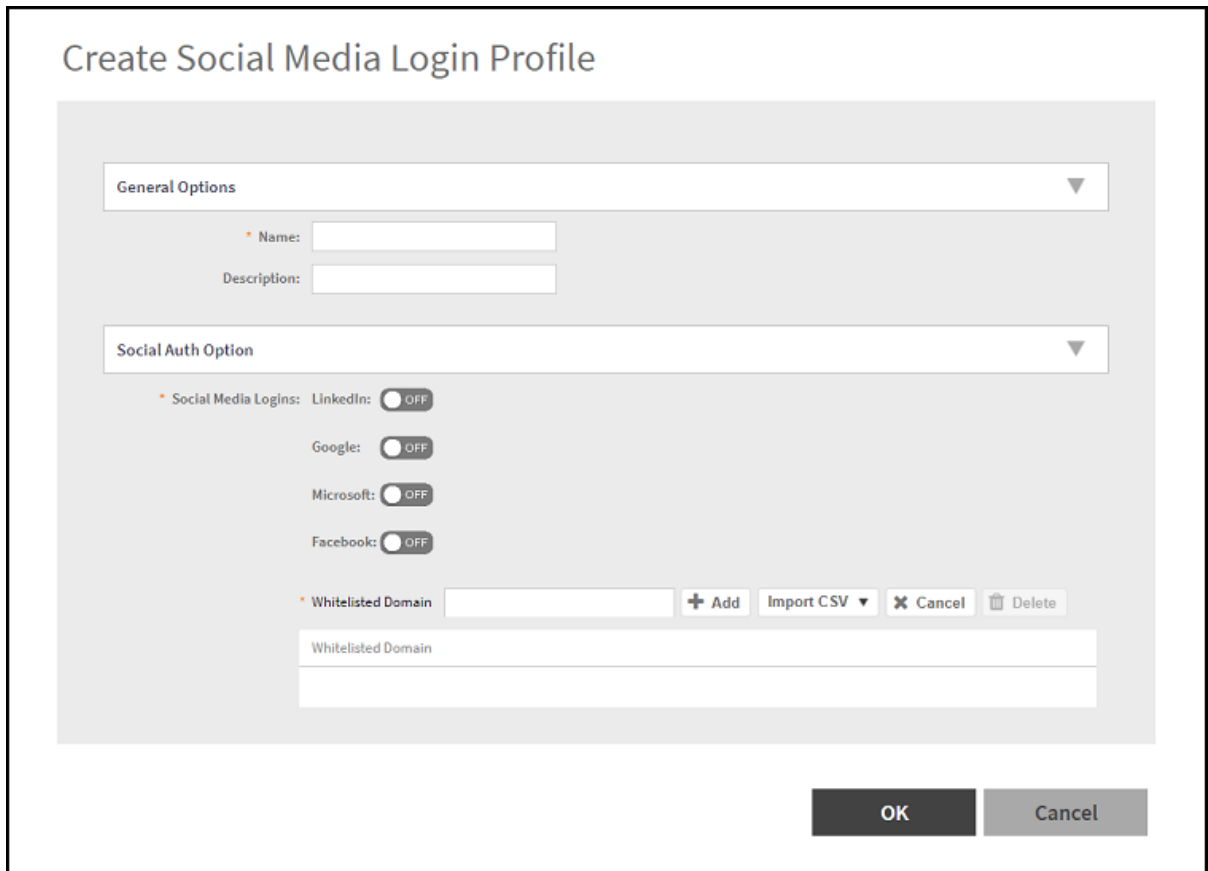
Portal Detection & Suppression: System Default

Guest Accounting: ☐ OFF Use the controller as proxy  
Disable

- **Guest Authentication:** Select from the below options.
  - **Guest:** Provides guest-level access only.
  - **Always Accept:** Allows users without guest credentials to receive authentication.
  - **Guest Access / Social Media Login:** Configures a guest-level access or social media profile.
  - **Social Media Login:** Configures social media profile for a user, use client ID and client secret options.
- **Guest Portal Service:** Select the guest access from the drop-down list or click the icon to create a new guest access portal, refer to the .
- **Note:** Click the icon to modify the selected guest portal service.
- **Bypass CNA:** By default, this option is **ON**, turn it **OFF** to disable this option.
- **Portal Detection & Suppression:** This option is available only when the **Bypass CNA** is **ON**. Choose from the drop-down list or click icon to create a new portal detection profile, refer to [Creating a Portal Detection and Suppression Profile](#).
- **Note:** Click the icon to modify the selected portal detection and suppression.
- **Guest Accounting:** By default, this option is **OFF**, turn it **ON** if you want to use the controller as proxy. Choose from the drop-down list or click the icon to create AAA server, refer to the .
- **Note:** Click the icon to modify the selected guest accounting.
- **Social Media Profile:** This option is available only when you select **Guest Access / Social Media Login** or **Social Media Login** in the **Guest Authentication**. Choose from the list or follow the below steps to create a new social media login profiles.

- a. In the **Social Media Profile** field, click the  icon to display the **Create Social Media Login Profile** dialog box.

**Figure 6.** Create Social Media Login Profile Dialog Box



The dialog box is titled "Create Social Media Login Profile". It contains two main sections: "General Options" and "Social Auth Option".

**General Options:**

- Name:** A text input field.
- Description:** A text input field.

**Social Auth Option:**

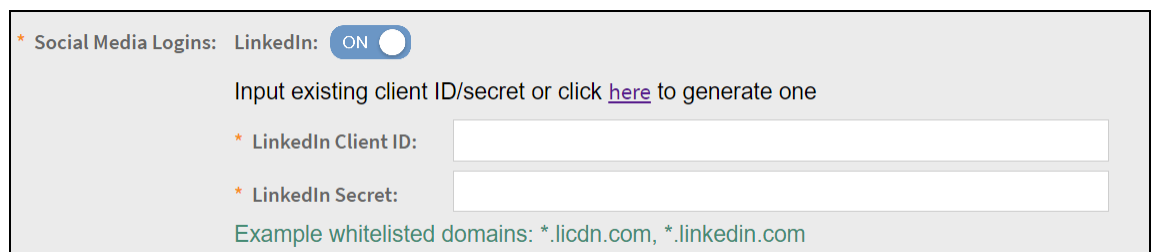
- Social Media Logins:** A list of social media platforms with toggle switches:
  - LinkedIn: OFF
  - Google: OFF
  - Microsoft: OFF
  - Facebook: OFF
- Whitelisted Domain:** A text input field with a "+ Add" button, an "Import CSV" button, a "Cancel" button, and a "Delete" button.

At the bottom right, there are "OK" and "Cancel" buttons.

- b. Complete the following fields:

- **Name:** Type a name for the social media profile that you are creating.
- **Description:** Type a short description of the social media profile.
- **Social Media Logins:** Select the required social media from the list. Switch **ON** to create a social media login.
- **LinkedIn:** Enter the **Client ID** and **Secret**.

**Figure 7.** Social Media Logins: LinkedIn



The form shows the "Social Media Logins" section with the "LinkedIn" toggle switch turned **ON**.

Below the toggle, there is a text input field for the "LinkedIn Client ID" and a text input field for the "LinkedIn Secret".

Below the input fields, there is a text input field for "Whitelisted Domain" with the example text: "Example whitelisted domains: \*.licdn.com, \*.linkedin.com".

To create a new **Client ID** and **Secret** for LinkedIn, click [here](#) or refer to <https://developer.linkedin.com/>.

- **Google:** Enter the **Client ID** and **Secret**.

**Figure 8.** Social Media Logins: Google

The screenshot shows the 'Social Media Logins' configuration interface. At the top, it says '\* Social Media Logins: LinkedIn: OFF'. Below this, 'Google:' is set to 'ON'. A text prompt reads 'Input existing client ID/secret or click [here](#) to generate one'. There are two input fields: '\* Google Client ID:' and '\* Google Secret:'. At the bottom, it lists 'Example whitelisted domains: \*.geotrust.com, \*.google.com, \*.gstatic.com'.

To create a new **Client ID** and **Secret** for Google, click [here](#) or refer to <https://console.cloud.google.com/projectselector2/apis/credentials>.

- **Microsoft:** Enter the **Client ID** and **Secret**.

**Figure 9.** Social Media Logins: Microsoft

The screenshot shows the 'Social Media Logins' configuration interface. At the top, it says '\* Social Media Logins: LinkedIn: OFF'. Below this, 'Google:' is set to 'OFF' and 'Microsoft:' is set to 'ON'. A text prompt reads 'Input existing client ID/secret or click [here](#) to generate one'. There are two input fields: '\* Microsoft Client ID:' and '\* Microsoft Secret:'. At the bottom, it lists 'Example whitelisted domains: \*.geotrust.com, \*.live.com, \*.microsoftonline.com, auth.gfx.ms, \*.msauth.net, \*.gstatic.com'.


To create a new **Client ID** and **Secret** for Microsoft, click [here](#) or refer to [https://portal.azure.com/#view/Microsoft\\_AAD\\_RegisteredApps/ApplicationsListBlade](https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade).

- **Facebook:** Enter the **Client ID** and **Secret**.

**Figure 10.** Social Media Logins: Facebook

The screenshot shows the 'Social Media Logins' configuration interface. At the top, it says '\* Social Media Logins: LinkedIn: OFF'. Below this, 'Google:' is set to 'OFF', 'Microsoft:' is set to 'OFF', and 'Facebook:' is set to 'ON'. A text prompt reads 'Input existing client ID/secret or click [here](#) to generate one'. There are two input fields: '\* Facebook Client ID:' and '\* Facebook Secret:'. At the bottom, it lists 'Example whitelisted domains: \*.facebook.com, fbcdn-profile-a.akamaihd.net, fstatic-a.akamaihd.net, \*.fbcdn.net'.

To create a new **Client ID** and **Secret** for Facebook, click **here** or refer to <https://developers.facebook.com/>.

- **Whitelisted Domain:** Add the domain names and click the  **Add** icon to add the external portal domain or click **Import CSV** to import the domain name using the CSV file. The added domain names are displayed in the **Whitelisted Domain** table.

c. Click **OK**.

6. Click **OK**.

7. In the **Wireless LANs** window, select a user name from the table. Click **More** > **Enable** to enable the user or click **More** > **Disable** to disable the user.

- **Note:** You can also edit, clone, and delete a Wireless LANs by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Wireless LANs** window.

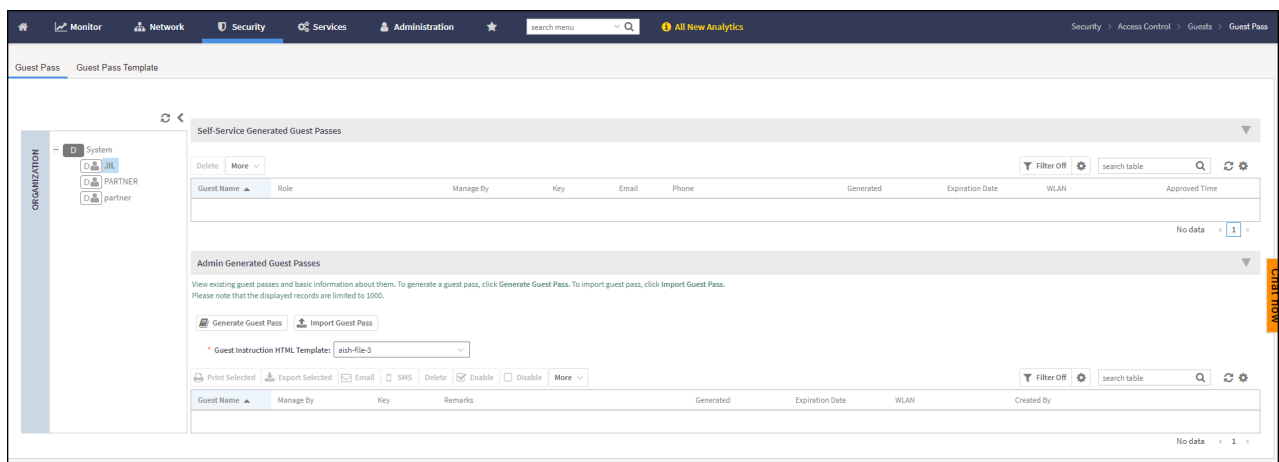
Parent topic: [Admin Generated Guest Passes](#)

### Step 3: Generate a Guest Pass

Follow these steps to generate a guest pass.

1. On the menu, click **Security** > **Access Control** > **Guests** > **Guests Pass** to displays the **Guest Pass** window.

**Figure 1.** Guest Pass



2. In the **Admin Generated Guest Passes** tab, click **Generate Guest Pass** to display the **Generate Guest Pass** dialog box.

**Figure 2.** Generating a Guest Pass

## Generate Guest Pass

\* Guest Name:

\* Guest WLAN: [ruckus] of [RUCKUS] ▼

\* Number of Passes:

\* Pass Valid For:  Days ▼

Advanced Options ▼

Pass Generation: ON ☒ Auto Generate

\* Pass Value:

Pass Effective Since: ☒ Effective from the creation time

☐ Effective from first use

\* Expire new guest pass if not used within:  days

\* Max Devices Allowed: ☒ Limited to

☐ Unlimited

Remarks:


Generate
Cancel

3. Complete the following fields:

- Guest Name: Enter guest name.
- Guest WLAN: Select the guest WLAN from the drop down menu.
- Number of Passes: Enter number of guest passes to be generated.
- Pass Valid For: Set the validity for the guest pass by entering the number and selecting the period from the drop-down menu. For example, if you want the guest pass to be valid for seven days, type 7 in the first box, and then select **Days** in the second box.

Under **Advance Options** tab complete the following fields:

- Pass Generation: The **Auto Generate** option is **ON** by default, and it generates the guest pass key automatically. If you want to generate the guest pass key manually, turn it **OFF** and enter the guest pass key in the Pass Value field.

 **Note:** If **Number of Passes** is more than one, the **Pass Generation** field will be disabled.

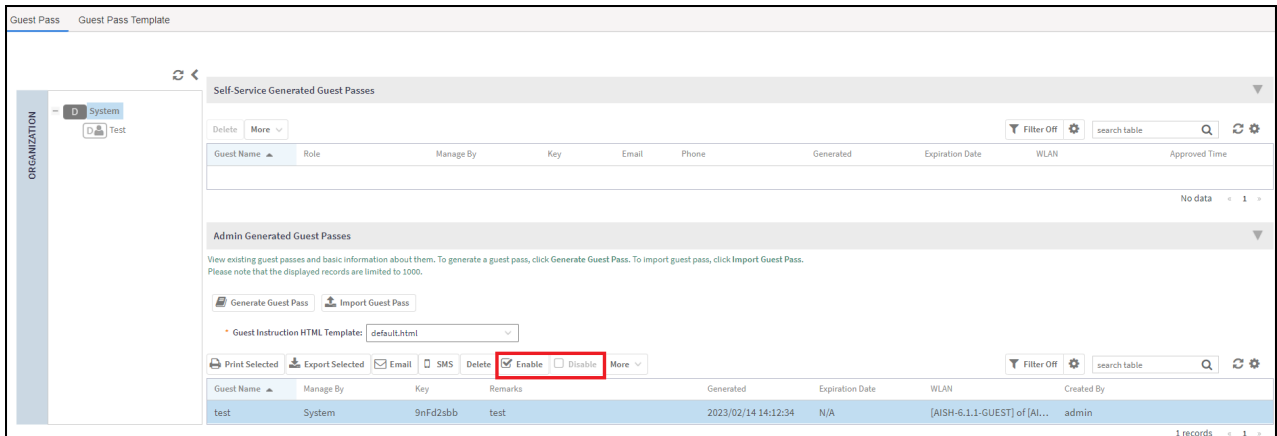
- Pass Effective Since: Set the guest pass validity period by selecting one of the following options:
  - Effective from the creation time: This type of guest pass is valid from the time it is created to the specified expiration time, even if it is not being used by any end user.
  - Effective from first use: This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (Guest Pass will expire in X days) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
  - Expire new guest pass if not used within [ ] days: If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).
- Max Devices Allowed: Set the number of users that can share this guest pass by selecting one of the following options:
  - Limited to [ ]: If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
  - Unlimited: Enable this option If you want to share the guest pass with unlimited users.
- Session Duration: This option is available only if the **Unlimited** option is enabled and the **Session Duration** option is **ON**. Enter the session time in the **Require guest re-login after [ ]** field. The session time can be set in minutes, hours, days, and weeks. This option controls the session time for users. When the session time expires, the user must log in again. This option is enabled by default. To disable it, turn it **OFF**. When this feature is disabled, connected users will not be required to log in again until the guest pass expires.
- Remarks: This is optional. Use this option to add any notes about the guest pass.


4. Click **Generate**.

The page refreshes, the guest pass generated appears in the **Admin Generated Guest Passes** table, along with other guest passes that exist on the controller.

5. To enable the guest pass for a user, select the guest pass from the **Admin Generated Guest Passes** table and click **Enable**. To disable the guest pass for a particular user, select the guest pass from the **Admin Generated Guest Passes** table and click **Disable**.

**Figure 3.** Admin Generated Guest Passes - Enable or Disable




To find the guest passes, click the  icon and apply filters or you can use the **Search Table** field.

To view the guest pass information, click on the guest pass from the **Admin Generated Guest Passes** table. A guest pass has the following information.

- **Summary:** Displays a summary of information about the user and credentials.
- **Admin Activities:** Displays information about the administrator activities.
- **Event:** Displays information about events associated with the user.

Click the  icon to apply filters. Click the  icon to export all the data into a CSV file.

To export the guest passes data into a CSV file, select the guest passes and click  icon.

- **Note:** You can generate maximum 120000 guest passes for SZ100, and 40000 guest passes for vSZ-E.
- **Note:** You can generate maximum 40000 guest passes for SZ300, and 1000000 guest passes for vSZ-H.
- **Note:** The controller GUI allows you to view only 1000 guest passes. To view the guest pass list above 1000 passes, you must use the public API's.

**Parent topic:** [Admin Generated Guest Passes](#)

## Step 4: Send Guest Passes to Guest Users

Deliver the guest passes to guest users as per the delivery options that you choose.

The page that appears after you generate a guest pass contains options for delivering the guest pass to guest users (see the following image).

**Figure 1.** Options for Delivering Guest Passes to Guest Users

Here are the generated guest passes

Guest Name ▲	Manage By	Key	Remarks	Generated	Expiration Date	WLAN
Sam	System	Wv3QSH6q	One day pass	2017/03/08 17:41:30	2017/03/09 17:41:30	[SZ-300-GUEST] of [TEST-JL...
Sen	System	sajeXkCg	N/A	2017/03/08 18:45:26	N/A	[SZ-300-GUEST] of [TEST-JL...
test2	System	DHp2u8D3	N/A	2017/01/18 14:19:18	2017/01/19 14:19:18	[SZ-300-GUEST] of [TEST-JL...

3 total records << 1 >>


Parent topic: [Admin Generated Guest Passes](#)

## Generating Guest Passes from an Imported CSV

You can also manually define the guest passes that you want to generate in a comma-separated value (CSV) file (a sample of which is available for download from the **Guest Pass** page).

Follow these steps to generate guest passes from an imported CSV file.

1. On the menu, click **Security > Access Control > Guest > Guest Pass** to display the **Guest Pass** window.

2. From the **Admin Generated Guest Passes** tab, click the  icon to display the **Import Guest Pass** dialog box.

**Figure 1.** Import Guest Pass

## Import Guest Pass

Guest List CSV File:  Browse

To download a sample guest pass, click [here](#)

**Common Guest Pass Settings**

\* Guest WLAN: [AISH-6.1.1-GUEST] of [AISH-6.1.1.0.611] ▼

\* Pass Valid For: 1 Days ▼

**Advanced Options** ▼

Pass Effective Since: ☒ Effective from the creation time  
☐ Effective from first use

\* Expire new guest pass if not used within:    days

\* Max Devices Allowed: ☒ Limited to 1  
☐ Unlimited

Import
Cancel

3. Look for the following text under Browse:

To download a sample guest pass, click **here**.

4. Click **here** to download the sample CSV file.

5. Open the CSV file with Microsoft Excel or a similar application.

6. In the CSV file, fill out the following columns:

- #Guest Name (Must): Assign a user name to the guest pass user.
- Remarks (Optional): Add some notes or comments about this guest pass.
- Key: Enter a guest pass key or leave it blank so the controller can generate the key automatically.

**Figure 2.** Sample CSV File in Excel

	A	B	C
1	#Guest Name (Must)	Remarks	Key (Empty Implies random key)
2	Batch-Guest-1	Batch generation	AAAAAAA
3	Batch-Guest-2	Batch generation	
4	Batch-Guest-3		
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

7. Save the CSV file.
8. Open **Import Guest Pass** dialog box and complete the following fields in the **Common Guest Pass Settings** tab:
  - **Guest WLAN:** Select the guest WLAN from the drop down list.
  - **Pass Valid For:** Enter the pass validity. The validity period can be set in hours, days, and weeks. For example, if you want the guest pass to be valid for seven days, type 7 in the first box, and then select **Days** in the second box.
  - In the **Advanced Options** tab complete the following fields:
    - **Pass Effective Since:** Set the guest pass validity period by selecting one of the following options:
      - **Effective from the creation time:** This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.
      - **Effective from first use:** This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (**Guest Pass will expire in X days**) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
      - **Expire guest pass if not used within [ ] days:** If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).
    - **Max Devices Allowed:** Set the number of users that can share this guest pass.

- **Limited to [ ]**: If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
- **Unlimited**: Enable this option if you want to share the guest pass with unlimited users.
- **Session Duration**: This option is available only if the **Unlimited** option is enabled. Enter the session time in the **Required guest to log on again after** field. The session time can be set in minutes, hours, days, and weeks. This option controls the session time for users. When the session time expires, the user must log in again. This option is enabled by default. To disable it, turn it OFF. When this feature is disabled, connected users will not be required to log in again until the guest pass expires.

9. In **Guest List CSV File** (at the top of the page), click **Browse**, and then select the CSV file you edited earlier. The page refreshes, and the number of guest passes that the controller has identified in the CSV file appears below the **Browse** button.

10. Click **Import**.

The page refreshes, and then the guest pass you generated appears in a table, along with other guest passes that exist on the controller.

To send the guest pass to guest users, refer to [Step 4: Send Guest Passes to Guest Users](#).

Parent topic: [Admin Generated Guest Passes](#)

## Guest Pass Template

### [Creating a Guest Instruction HTML Template](#)

### [Creating a Guest Instruction SMS Template](#)

Parent topic: [Working with Guest Passes](#)

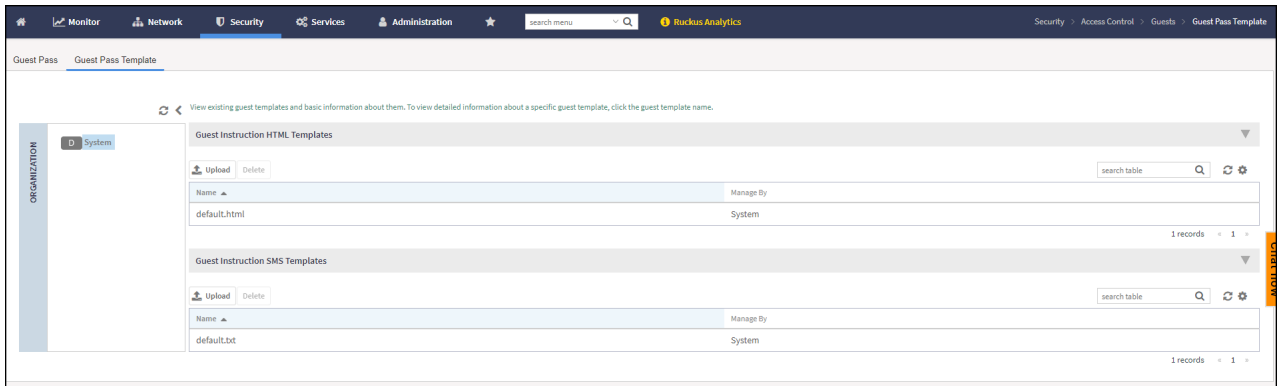
## Creating a Guest Instruction HTML Template

A guest pass template is a HTML file which contains variables for the information that guest users need to connect to the controller hotspots (for example, guest name, key, and WLAN name), and actual instructions for connecting to the guest WLAN.

A default printout template exists in the controller. If you want to create your own printout template, follow these steps.

1. On the menu, click **Security > Access Control > Guest Pass Template** to display the **Guest Pass Template** window.

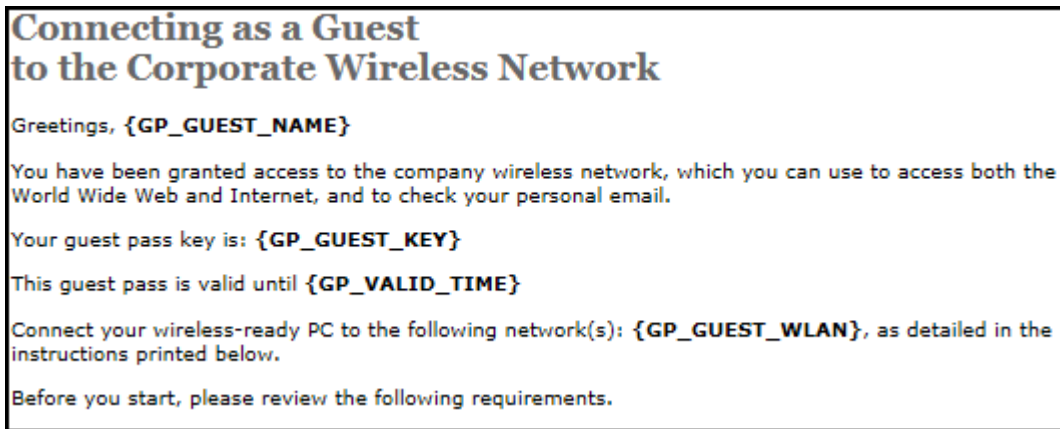
**Figure 1.** Guest Pass Template



2. In the **Guest Instruction HTML Template** tab, click `default.html`, which is the default guest pass printout template.  
The content of the default guest pass printout template appears in the Name: default.html
3. Click **Download** below the template preview area to download a copy of the template to your computer.
4. Using an HTML editor, create a new HTML file.
5. Add content to the file.

Typically, a printout template contains instructions for connecting to the controller hotspot. See the following image for the content of the default printout template.

**Figure 2.** Content of the Default Printout Template



6. Insert the following variables into the content of your template:
  - **{GP\_GUEST\_NAME}**: This is the guest pass user name.
  - **{GP\_GUEST\_KEY}**: This is the guest pass key.
  - **{GP\_VALID\_TIME}**: This is the expiration date and time of the guest pass.

- **{GP\_GUEST\_WLAN}**: This is the WLAN with which the guest user can associate using the guest name and guest key.

7. Save the file.

8. Open the **Guest Instruction HTML Template** tab, click **Upload** to display the **Upload a Template File** tab.

**Figure 3.** Upload a Template File

The screenshot shows the 'Guest Instruction HTML Templates' management interface. At the top, there are 'Upload' and 'Delete' buttons. Below them is a table with columns 'Name' and 'Manage By'. The table contains one entry: 'default.html' managed by 'System'. To the right of the table is a search bar and a refresh icon. Below the table, there is a section titled 'Upload a Template File' which contains two input fields: 'Template Name' and 'Template File', followed by a 'Browse' button. At the bottom of this section are 'Upload' and 'Cancel' buttons.

9. Complete the following fields:

- **Template Name:** Type a name for the template that you are uploading.
- **Template File:** Click **Browse**, and select the template file you created.

10. Click **Upload**.

An information message box appears and informs you that the template file has been uploaded successfully.

11. Click **OK**.

The template file you uploaded now appears in the list of templates.

**Figure 4.** Upload a Template File

This screenshot shows the same interface as Figure 3, but after the upload. The table now lists two templates: 'default.html' and 'Sha1', both managed by 'System'. The 'Upload' and 'Delete' buttons remain at the top. A 'Refresh' button has been added next to the search bar. The 'Upload a Template File' section is no longer visible, indicating the process is complete.

Parent topic: [Guest Pass Template](#)

## Creating a Guest Instruction SMS Template

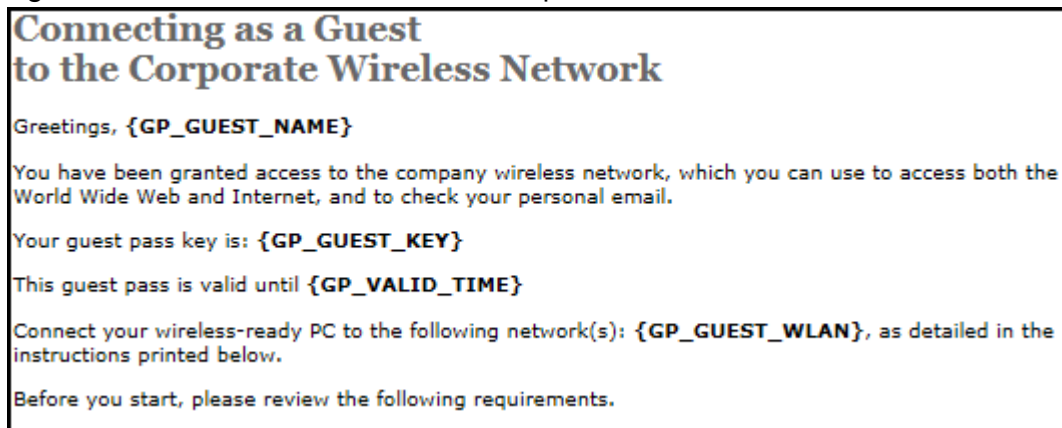
A guest SMS template is a text file which contains variables for the information that guest users need to connect to the controller hotspots (for example, guest name, key, and WLAN name), and actual instructions for connecting to the guest WLAN.

A default printout template exists in the controller. If you want to create your own printout template, follow these steps.

1. On the menu, click **Security > Access Control > Guest Pass Template** to display the **Guest Pass Template** window.
2. In the **Guest Instruction SMS Template** section, click `default.txt`, which is the default guest pass printout template.  
The content of the default guest pass printout template appears in the Name: default.txt.
3. Click **Download** below the template preview area to download a copy of the template to your computer.
4. Using an HTML editor, create a new text file.
5. Add content to the file.

Typically, a printout template contains instructions for connecting to the controller hotspot. See the following image for the content of the default printout template.

**Figure 1.** Content of the Default Printout template



6. Insert the following variables into the content of your template:
  - {GP\_GUEST\_NAME}: This is the guest pass user name.
  - {GP\_GUEST\_KEY}: This is the guest pass key.
  - {GP\_VALID\_TIME}: This is the expiration date and time of the guest pass.
  - {GP\_GUEST\_WLAN}: This is the WLAN with which the guest user can associate using the guest name and guest key.
7. Save the file.
8. In the **Guest Instruction SMS Template** tab, click **Upload** icon to display the **Upload a Template File** tab.

**Figure 2.** Upload a Template File

The screenshot shows the 'Guest Instruction SMS Templates' interface. At the top, there are 'Upload' and 'Delete' buttons. Below them is a table with columns 'Name' and 'Manage By'. The table contains one entry: 'default.txt' under 'Name' and 'System' under 'Manage By'. To the right of the table is a search bar labeled 'search table' and a refresh icon. Below the table, there is a section titled 'Upload a Template File' with two input fields: 'Template Name:' and 'Template File:'. The 'Template File:' field has a 'Browse' button next to it. At the bottom of this section are 'Upload' and 'Cancel' buttons.

9. Complete the following fields:

- **Template Name:** Type a name for the template that you are uploading.
- **Template File:** Click **Browse**, and select the template file you created.

10. Click **Upload**.

An information message box appears and informs you that the template file has been uploaded successfully.

11. Click **OK**.

The template file you uploaded now appears in the list of templates.

**Figure 3.** Upload a Template File

The screenshot shows the 'Guest Instruction SMS Templates' interface after the upload. The 'Upload' and 'Delete' buttons are still present. The table now has a 'Refresh' button to the right of the search bar. The table content remains the same: 'default.txt' under 'Name' and 'System' under 'Manage By'.

Parent topic: [Guest Pass Template](#)

# Working with Hotspots and Portals

## Creating a Guest Access Portal

## Working with Hotspot (WISPr) Services

## Working with Hotspot 2.0 Services

## Creating a Web Authentication Portal

## Creating a UA Blacklist Profile

## Creating a Portal Detection and Suppression Profile

## Creating a WeChat Portal

## Creating Network Segmentation Profile on the vSZ Controller

## Ethernet Profiles

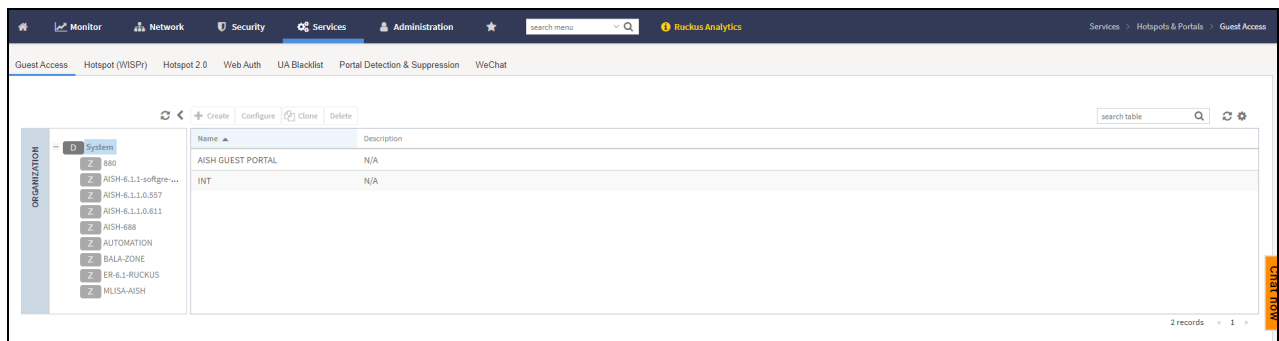
# Creating a Guest Access Portal

Using the controller's Guest Access features, you can provide visitors to your organization limited access to a guest WLAN with configurable guest policies. The following sections describe how to configure guest WLANs and access policies that control guest use of your network.

Each guest WLAN must be associated with a Guest Access service portal, which defines the behavior of the guest WLAN interface. Follow these steps to create a guest access service.

1. On the menu, click **Services > Hotspots & Portals > Guest Access** to display the **Guest Access** window.

**Figure 1.** Guest Access



2. In the **Organization** tab, select the zone for which you want to create the guest access portal.
3. Click **Create**, to display the **Create Guest Access Portal** dialog box.

**Figure 2. Creating a Guest Access Portal**

Create Guest Access Portal

General Options ▶

Redirection ▶

Guest Access ▶

User Session ▶

OK Cancel

4. Complete the following fields:

a. General Options

**Figure 3. Create Guest Access Portal - General Options**

Create Guest Access Portal

General Options ▼

\* Portal Name:

Portal Description:

\* Language:  ▼

- Portal Name: Type a name for the guest access service portal that you are creating.
- Portal Description: Type a short description of the guest access service portal.
- Language: Select the display language to use for the buttons on the guest access logon page.

b. Redirection: Select where to redirect the user after successfully completing authentication.

**Figure 4. Create Guest Access Portal - Redirection**

## Create Guest Access Portal

General Options ▶

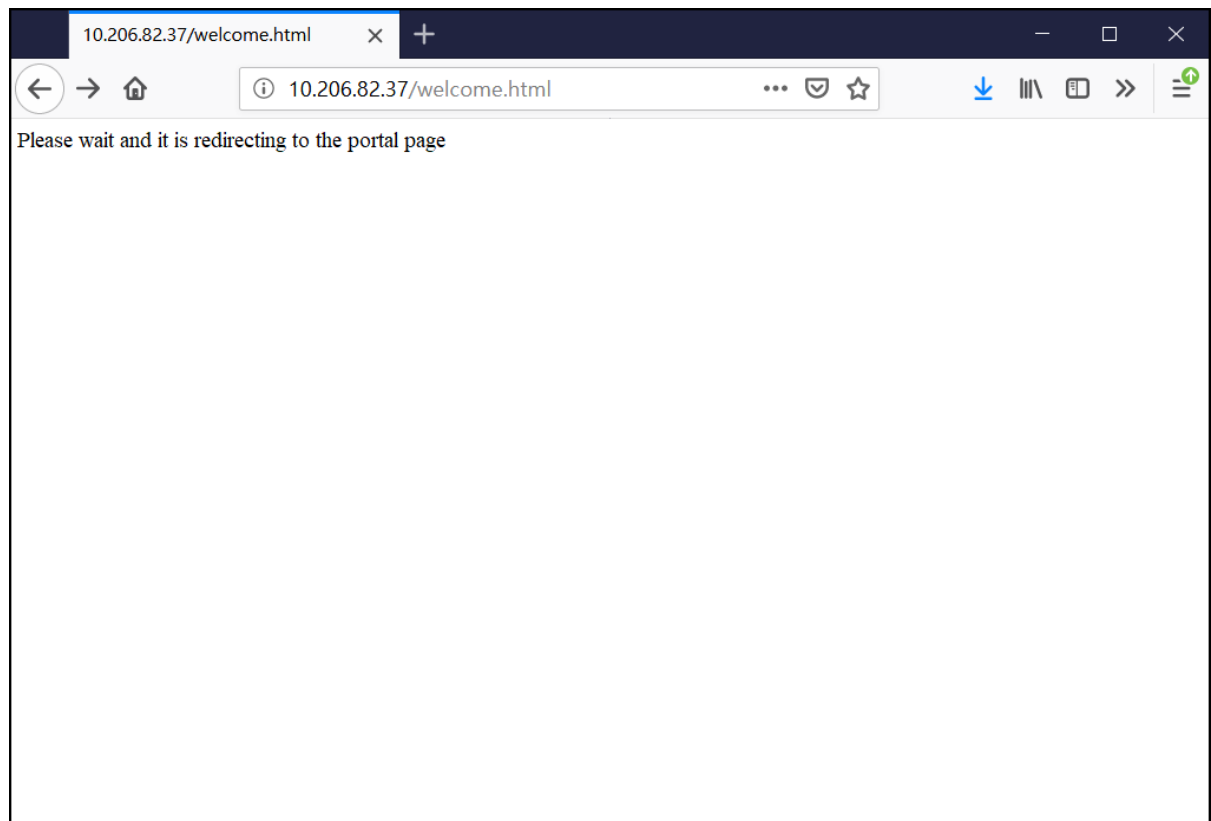
Redirection ▼

Start Page: After user is authenticated,

☒ Redirect to the URL that user intends to visit.
 ☐ Redirect to the following URL:

- Redirect to the URL that the user intends to visit: Allows the guest user to continue to their destination without redirection.
- Redirect to the following URL: Redirects to the specified domain name or IP address. If the guest access portal's guest authentication is **Always Accept** and the guest access does not enable the **Terms and Conditions**, after 3 seconds, the client or the guest is redirected to the start URL or the original URL.

**Figure 5.** Redirecting Page



c. Guest Access

**Figure 6.** Create Guest Access Portal - Guest Access

## Create Guest Access Portal

Redirection

Guest Access

Self-registration: ☒ ON

Guest Pass SMTP Server: ☐ OFF

\* Guest Pass SMS Gateway: Disabled

Terms and Conditions: ☒ ON

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.

(\*) The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.

(\*) You agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited and you are fully responsible for your use.

(\*) The wireless network is provided "as is" without warranties of any kind, either expressed or implied.

This wireless network is powered by Ruckus CommScope.

[?] Web Portal Logo:

Web Portal Title:

\* Pass Valid For:

Pass Effective Since: ☐ Effective from the creation time  
☒ Effective from first use

\* Expire new guest pass if not used within:  days

\* Max Devices Allowed: ☐ Limited to   
☒ Unlimited

Session Duration: ☒ ON \* Required guest to log on again after:

\* Notification Method:

- Self Registration: Enable the option to register for the guest pass.
- Guest Pass SMTP Server: This feature is only available if the **Self-registration** feature is enabled. Enable the option to receive the copy of guest pass by email.
- Guest Pass SMS Gateway: You can deliver the guest pass to the user using Short Message Service (SMS). But first you need to configure an SMS server. If you previously configured an SMS server, you can select it here or you can select **Disable**.
- Terms and Conditions: Users should read and accept terms and conditions prior to use, **Show Terms and Conditions** check box. This displays the default terms of use text. Edit or leave the text unchanged to use the default content.

- **Web Portal Logo:** By default, the guest hotspot logon page displays the RUCKUS logo. To use your own logo, click the **Browse** button, select your logo Web Portal Logo (recommended size is 138 x 40 pixels, maximum file size is 20KB), and then click **Open**.
- **Web Portal Title:** Type your own guest hotspot welcome text or accept the default welcome text (Welcome to the Guest Access login page).
- **Pass Valid For:** This feature is only available if the **Self-registration** feature is enabled. Set the guest pass validity. The validity time can be set in hours, days, and weeks.
- **Pass Effective Since:** This feature is only available if the **Self-registration** feature is enabled. Set the guest pass validity period by selecting one of the following options:
  - **Effective from the creation time:** This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.
  - **Effective from first use:** This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (Guest Pass will expire in X days) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
  - **Expire guest pass if not used within [ ] days:** If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).
- **Max Devices Allowed:** This feature is only available if the **Self-registration** feature is enabled. Set the number of users that can share this guest pass.
  - **Limited to [ ]:** If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
  - **Unlimited:** If you want an unlimited number of users to share this guest pass, click this option.
- **Session Duration:** This option is available only if the **Unlimited** option is enabled. Enter the session time in the **Required guest to log on again after** field. The session time can be set in minutes, hours, days, and weeks. This option controls the session time for devices. When the session time expires, the user must log in again. This option is enabled by default. To disable it, turn it OFF. When this feature is disabled, connected users will not be required to log in again until the guest pass expires.
- **Notification Method:** This feature is only available if the **Self-registration** feature is enabled. Select how the guest pass must be notified to the user. For example: E-Mail, Mobile, and Mobile and E-mail.

#### d. User Session

**Figure 7.** Create Guest Access Portal - User Session

**Create Guest Access Portal**

General Options ▶

Redirection ▶

Guest Access ▶


User Session ▼

\* Session Timeout:  Minutes (2-14400)

\* Grace Period:  Minutes (1-14399)

- Session Timeout: Specify a time limit after which users will be disconnected and required to log on again.
- Grace Period: Set the time period during which clients will not need to re-authenticate after getting disconnected from the hotspot. Enter a number (in minutes) between 1 and 14399.

5. Click **OK**.

 **Note:** You can also edit, clone and delete a guest access portal by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Guest Access** window.

Parent topic: [Working with Hotspots and Portals](#)

## Working with Hotspot (WISPr) Services

A hotspot is a venue or area that provides Internet access to devices with wireless networking capability such as notebooks and smart phones.

Hotspots are commonly available in public venues such as hotels, airports, coffee shops and shopping malls. Configure a traditional (WISPr 1.0) hotspot service to provide public access to users via its WLANs. In addition to the controller and its managed APs, you will need the following to deploy a hotspot:

**Captive Portal:** A special web page, typically a login page, to which users that have associated with your hotspot will be redirected for authentication purposes. Users will need to enter a valid user name and password before they are allowed access to the Internet through the hotspot.

**RADIUS Server:** A Remote Authentication Dial-In User Service (RADIUS) server through which users can authenticate.

For installation and configuration instructions for the captive portal and RADIUS server software, refer to the documentation that was provided with them. After completing the steps below, you will need to edit the WLAN(s) for which you want to enable Hotspot service. The controller supports up to 32 WISPr hotspot service entries, each of which can be assigned to multiple WLANs.

**Parent topic:** [Working with Hotspots and Portals](#)

## Creating a Hotspot (WISPr) Portal

To create a hotspot service, you must define the required basic settings.

SZ supports only one grace period, session timeout, UTP, VLAN and all UE session related configuration. These configurations for the first WLAN do not work when the UE joins the second WLAN. The configuration works only when the UE roams within the cluster node. The configurations do not work when the client roams from one zone to another zone or from one cluster to another cluster.

Before creating a hotspot, you need to create a user defined interface.

1. Select **Services > Hotspots & Portals > Hotspot (WISPr)**. The Hotspot (WISPr) page is displayed.

**Figure 1.** Hotspot (WISPr)

2. In the **Organization** tab, select a Zone from the system tree and click **Create**.
3. Click **Create**. The **Create Hotspot Portal** dialog box is displayed.

**Figure 2.** Creating a Hotspot (WISPr) Portal

**Create Hotspot Portal**

General Options ▶

Redirection ▶

Portal Settings ▶

User Session ▶

Location Information ▶

Walled Garden / Traffic Class Profile ▶

Advanced Options ▶

OK Cancel

4. Complete the following fields:

a. General Options

**Figure 3.** Create Hotspot Portal - General Options

**Create Hotspot Portal**

General Options ▼

\* Portal Name:

Portal Description:

- Portal Name: Type a name for the hotspot portal that you are creating.
- Portal Description: Type a short description of the hotspot portal.

b. Redirection

**Figure 4.** Create Hotspot Portal

## Create Hotspot Portal

General Options ▶

Redirection ▼

Smart Client Support: ☒ None ☐ Enable ☐ Only Smart Client Allowed

Logon URL: ☐ Internal ☒ External

Redirect unauthenticated user: \*

Primary:

Secondary:

\* Redirected MAC Format:

Start Page: After user is authenticated,

☒ Redirect to the URL that user intends to visit. ☐ Redirect to the following URL:

\*

HTTPS Redirect: ☒ ON ☐ OFF The AP will try to redirect HTTPS requests to the hotspot portal


- Smart Client Support: Select one of the following options:
    - **None:** Disables Smart Client Support on the hotspot service.
    - **Enable:** Enables Smart Client Support.
    - **Only Smart Client Allowed:** Allows only Smart Clients to connect to the hotspot service.
  - Logon URL: Select one of the following options:
    - **Internal:** Indicates the internal URL of the subscriber portal (where hotspot users can log in to the service). If you select **Internal**, you have to manually configure the following **Portal Settings**.
- Figure 5.** Create Hotspot Portal: Logon URL-Internal

- Portal Language: Select the required language from the drop down list.
- Portal Title: Enter the portal title.
- Portal Logo: Click **Browse** to upload the portal logo.
- Portal Terms & Conditions: Switch ON to accept the portal terms and conditions.
- **External**: Indicates the external URL of the subscriber portal.

Selecting **External** provides an option to reroute an unauthorized user to a primary location. You can set the primary location in **Redirect unauthenticated user**. If an unauthorized user is rerouted, the AP redirects the UE to a backup portal.

The AP subscriber portal supports ZD-style API to login and logout. A customer can use AP IP address to submit the login or logout request.

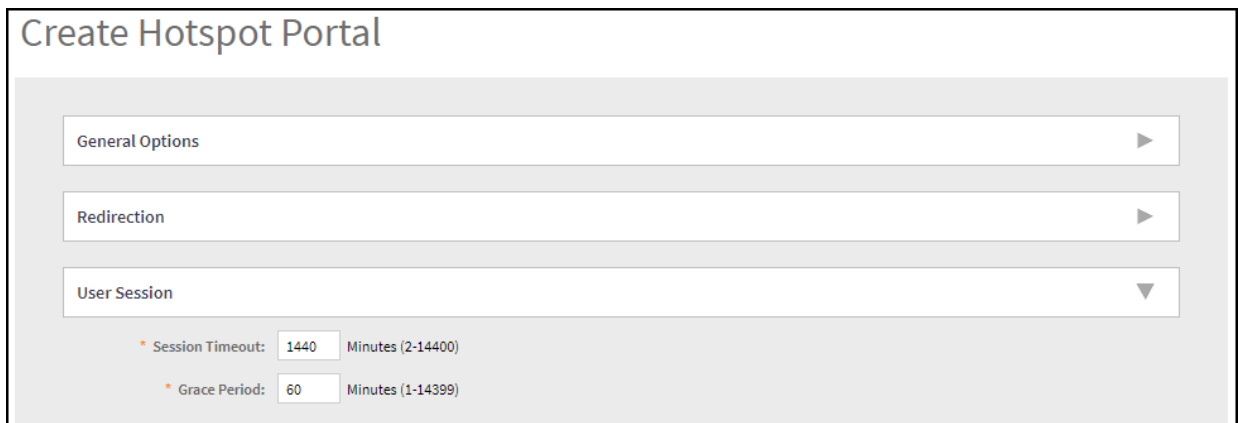
- Redirect unauthenticated user: APs can perform WISPr redirection. Native WISPr support is available on SZ-managed APs even if access to SZ is not available. It supports external portal redirection with survivability when APs cannot reach the centralized SZ. It also supports backup portal redirection if primary portal is down. The WISPr authentication load can be distributed to AP or use an AP as a WISPr authentication backup. WISPr redirection and survivability is supported only on Ruckus 11AC Wave 1 and later APs. Only ZD-style external WISPr is supported. No NBI is supported for backup.

 **Note:** The AP uses the secondary portal when the AP cannot access the primary portal.

- **Primary:** Redirects an unauthenticated user to a specified URL for authentication.
- **Secondary:** Redirects an unauthenticated user to the backup external portal if the primary URL is down. The AP periodically accesses the primary portal URL to detect and check the availability of the primary URL.
- **Redirected MAC Format:** Enter the format of the redirection MAC address.
- **Start Page:** Select one of the following options:
  - **Redirect to the URL that the user intends to visit:** Redirects users to the page that they want to visit.
  - **Redirect to the following URL:** Sets a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address to be redirected.
- **HTTPS Redirect:** Switch ON **HTTPS Redirect**, if you want the AP to redirect HTTPS requests to the hotspot portal. HTTPS requests are dropped if this option is disabled.

c. User Session

**Figure 6.** Create Hotspot Portal - User Session



The screenshot shows the 'Create Hotspot Portal' configuration interface. The 'User Session' tab is selected, showing the following settings:

- Session Timeout:** 1440 Minutes (2-14400)
- Grace Period:** 60 Minutes (1-14399)

- **Session Timeout:** Sets a time limit (in minutes) after which users will be disconnected from the hotspot service and required to log in again.
- **Grace Period:** Sets the time period (in minutes) during which disconnected users are allowed access to the hotspot service without logging in again.

d. Location Information

**Figure 7.** Create Hotspot Portal - Location Information

**Create Hotspot Portal**

General Options ▶

Redirection ▶

User Session ▶

Location Information ▼

Location ID:  (example: isocc=us,cc=1,ac=408,network=ACMEWISP\_NewarkAirport)

Location Name:  (example: ACMEWISP,Gate\_14\_Terminal\_C\_of\_Newark\_Airport)

- Location ID: enter the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The code includes the following requirements:
  - isocc (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
  - cc (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
  - ac (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.
  - network: Name of the network.

The following example illustrates a proper location ID entry: isocc=us, cc=1, ac=408, network=Ruckus

- Location Name: Enter the name of the location of the hotspot service.

e. Walled Garden/Traffic Class Profile

**Figure 8.** Create Hotspot Portal - Walled Garden/Traffic Class Profile

## Create Hotspot Portal

General Options ▶

Redirection ▶

User Session ▶

Location Information ▶

Walled Garden / Traffic Class Profile ▼

☒ Walled Garden
 

\* Walled Garden Entry 
+ Add
Import CSV ▼
✕ Cancel
🗑 Delete

Walled Garden Entry ▲
 

Walled Garden Entry

No data « 1 »

Unauthenticated users are allowed to access the following destinations.  
Format:

- IPv4 (e.g. 10.11.12.13)
- IPv4 Range (e.g. 10.11.12.13-10.11.12.15)
- IPv4 CIDR (e.g. 10.11.12.100/28)
- IPv4 and mask (e.g. 10.11.12.13 255.255.255.0)
- IPv6 (e.g. 2607:f0d0:1002:0051:0000:0000:0000:0004)
- IPv6 with prefix (e.g. 2607:f0d0:1002:0051:0:0:0/64)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
  - \*.amazon.com
  - \*.com

☐ Traffic Class Profile
 

Select Traffic Class Profile
 +
✎
✕

- Walled Garden
  - **Walled Garden Entry Add:** Enter an IP address or a domain name and click **Add** to add a **Walled Garden Entry**.
  - **Walled Garden Entry Import:**
- Figure 9. Walled Garden Entry - Import**

Walled Garden / Traffic Class Profile ▼

☒ Walled Garden
 

\* Walled Garden Entry 
+ Add
Import CSV ▼
✕ Cancel
🗑 Delete


Walled Garden Entry ▲
 

Walled Garden Entry

No data « 1 »

Download Sample CSV

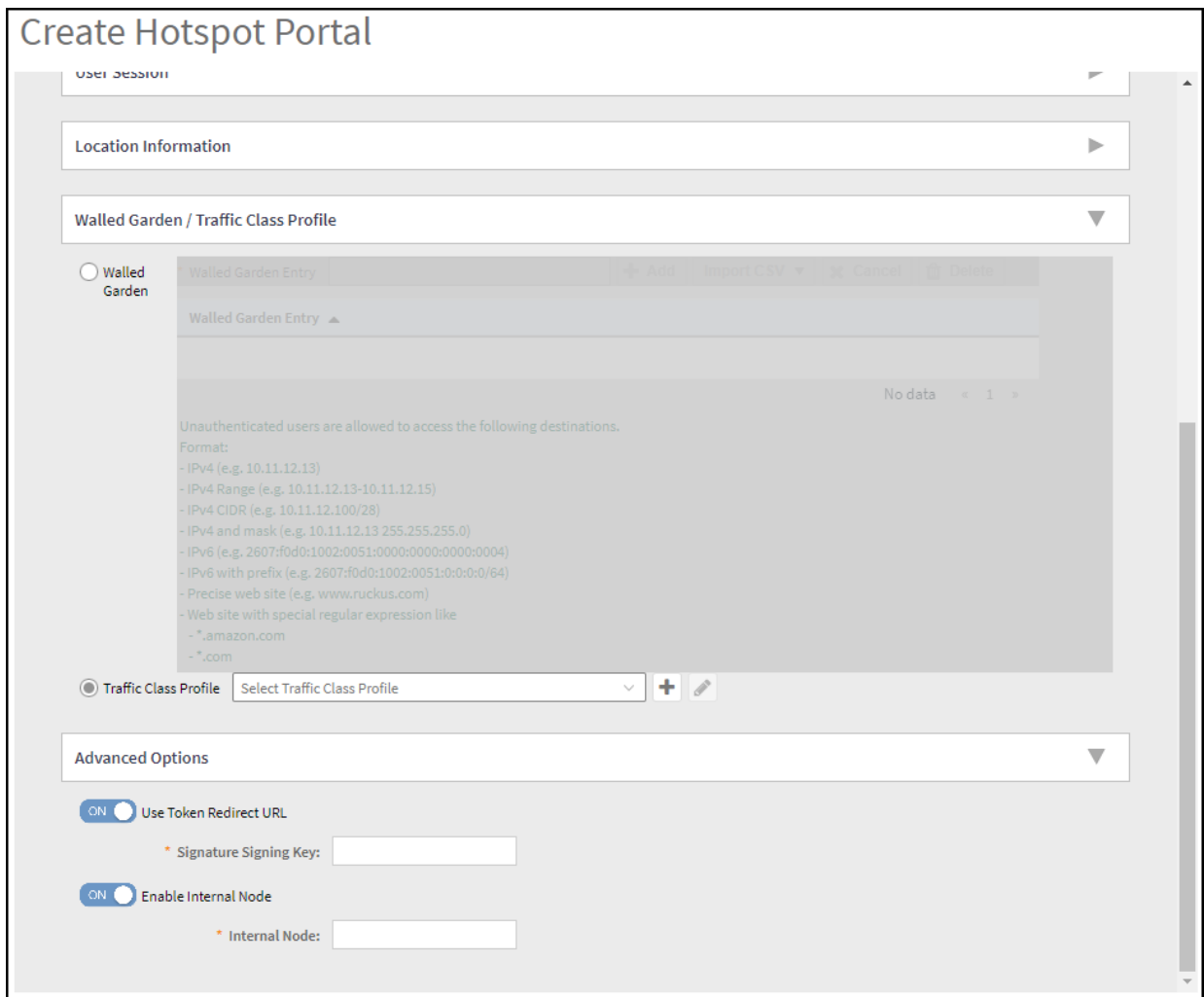
- Click drop-down arrow corresponding to the **Import CSV** and select **Download Sample CSV** and download the sample file.
- Add the user information in the download sample CSV excel file.

- Click **Import CSV** and import the sample CSV excel file.
- **Traffic Class Profile:** Select a traffic class profile from the drop down list or click the  icon to create a traffic class profile. Refer to the for more information.

f. Advanced Options

- **Note:** This option is available only if the **Traffic Class Profile** option is enabled.

**Figure 10.** Create Hotspot Portal - Advanced Options



**Create Hotspot Portal**

User Session

Location Information

Walled Garden / Traffic Class Profile

☐ Walled Garden

Walled Garden Entry

Walled Garden Entry

No data

Unauthenticated users are allowed to access the following destinations.  
Format:  
- IPv4 (e.g. 10.11.12.13)  
- IPv4 Range (e.g. 10.11.12.13-10.11.12.15)  
- IPv4 CIDR (e.g. 10.11.12.100/28)  
- IPv4 and mask (e.g. 10.11.12.13 255.255.255.0)  
- IPv6 (e.g. 2607:f0d0:1002:0051:0000:0000:0000:0004)  
- IPv6 with prefix (e.g. 2607:f0d0:1002:0051:0:0:0:0/64)  
- Precise web site (e.g. www.ruckus.com)  
- Web site with special regular expression like  
- \*.amazon.com  
- \*.com

☒ Traffic Class Profile

Select Traffic Class Profile

Advanced Options

☒ Use Token Redirect URL

\* Signature Signing Key:

☒ Enable Internal Node

\* Internal Node:

- **Use Token Redirect URL:** Switch ON **Use Token Redirect URL** and enter a signature signing key.
- **Enable Internal Node:** Switch ON **Enable Internal Node** and enter the internal node.

- **Note:**

If an **Internal node** is enabled, then only one IP is used and the IP domain name and IP ranges are not supported.

5. Click **OK**.

🔗 **Note:** If **Traffic Class Profile** or **Use Token Redirect URL** is enabled, **Smart Client Support** is set to **None**.

🔗 **Note:** You can also edit, clone, and delete a Hotspot (WISPr) portal by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Hotspot (WISPr)** window.

Parent topic: [Working with Hotspot \(WISPr\) Services](#)

## Working with Hotspot 2.0 Services

You must be aware of Hotspot 2.0 - a Wi-Fi Alliance specification that allows for automated roaming between service provider access points when both the client and access gateway support the newer protocol.

Hotspot 2.0 (also known as Passpoint™, the trademark name of the Wi-Fi Alliance certification) aims to improve the experience of mobile users when selecting and joining a Wi-Fi hotspot by providing information to the station prior to association.

This information can then be used by the client to automatically select an appropriate network based on the services provided and the conditions under which the user can access them. In this way, rather than being presented with a list of largely meaningless SSIDs to choose from, the Hotspot 2.0 client can automatically select and authenticate to an SSID based on the client's configuration and services offered, or allow the user to manually select an SSID for which the user has login credentials.

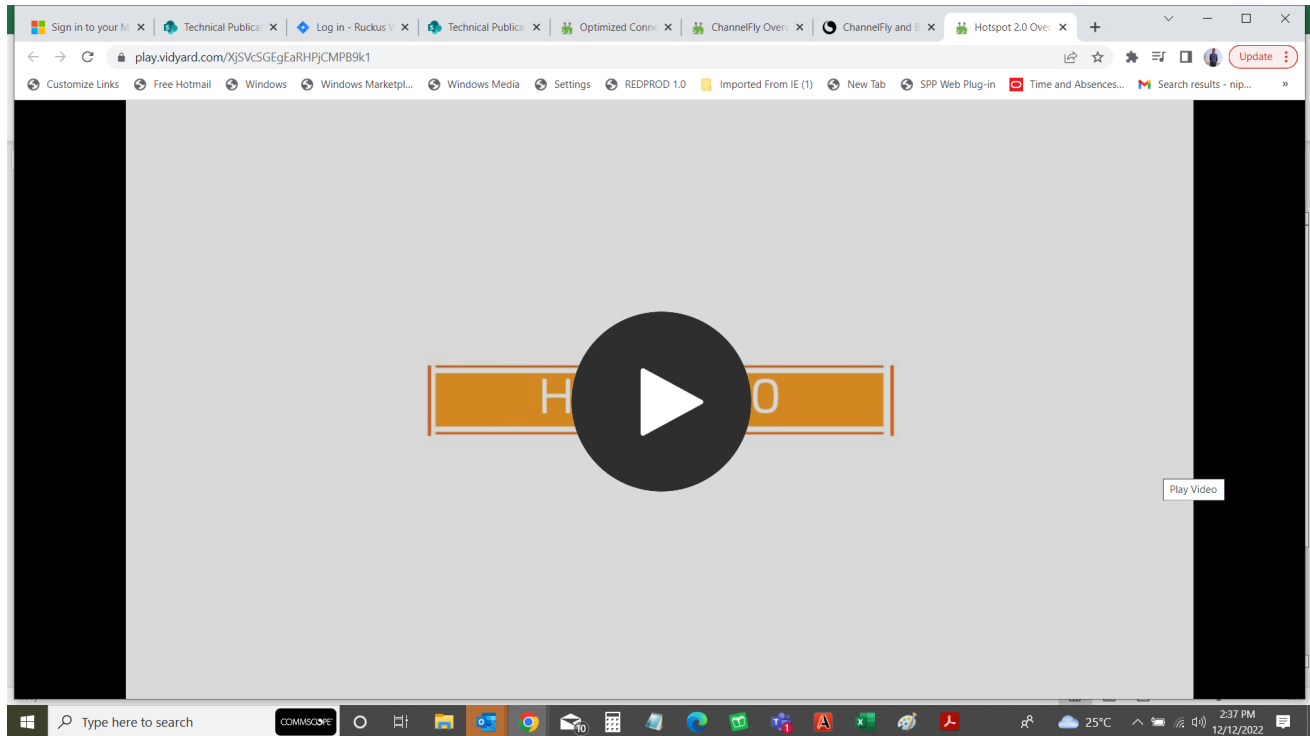
The controller's Hotspot 2.0 implementation complies with the IEEE 802.11u standard and the Wi-Fi Alliance Hotspot 2.0 Technical Specification.

See the *Hotspot 2.0 Reference Guide for SmartZone* for information on configuring Hotspot 2.0 services, including:

- Working with Hotspot 2.0 operator profiles
- Working with Hotspot 2.0 identity providers
- Creating a Hotspot 2.0 online signup portal

### Video:

**HotSpot 2.0 Overview.** This video provides a brief overview of HotSpot 2.0



Click to play video in full screen mode.

Parent topic: [Working with Hotspots and Portals](#)

Related information

Video: [HotSpot 2.0 Overview](#)

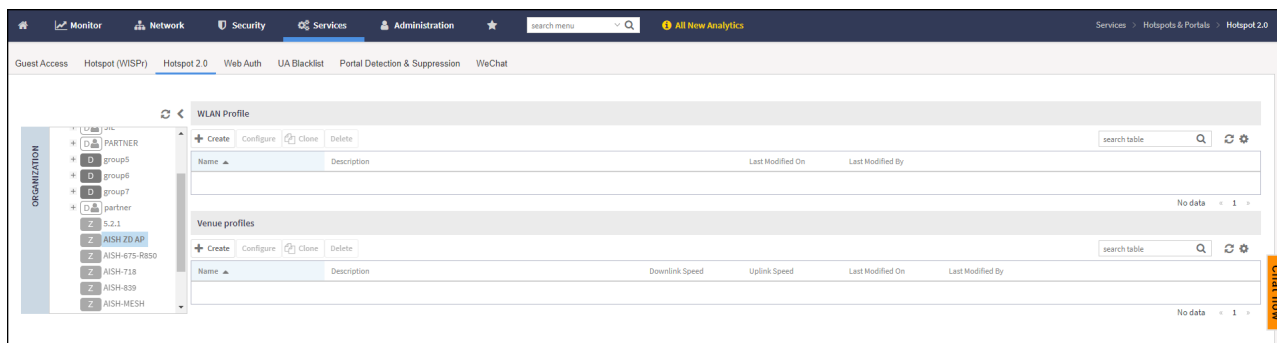
## Creating a Hotspot 2.0 WLAN Profile


You can assign and Hotspot 2.0 service to a Hotspot 2.0 WLAN, for which you must create a Hotspot 2.0 WLAN profile.

Follow these steps to create a Hotspot 2.0 WLAN profile.

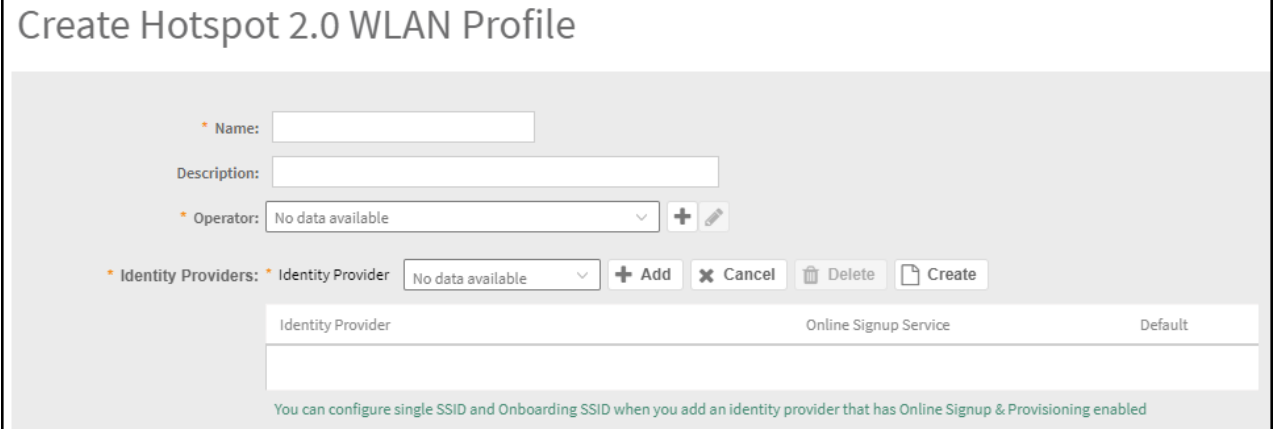
1. On the menu, click **Services > Hotspots & Portals > Hotspot 2.0** to display the **Hotspot 2.0** window.

**Figure 1.** Hotspot 2.0



2. In the **Organization** tab, select the zone for which you want to create the **Hotspot 2.0 WLAN** portal.
3. In the **WLAN Profile** tab, click the  to display the **Create Hotspot 2.0 WLAN Profile** dialog box.

**Figure 2.** Creating a Hotspot 2.0 WLAN Profile



4. Complete the following fields:

- **Name:** Enter a name for this WLAN profile. This name identifies the WLAN profile when assigning an Hotspot 2.0 service to a Hotspot 2.0 WLAN.
- **Description:** Enter a description for the WLAN profile.
- **Operator:** Select the operator profile. This name identifies the service operator when assigning an Hotspot 2.0 service to a Hotspot 2.0 WLAN.

You can also click **Create** to create a Hotspot 2.0 WiFi operator. See [Creating a Hotspot 2.0 WiFi Operator Profile](#) for more information.

- **Identity Provider:** Choose one or more identity providers. Choose the identity provider. You can configure an OSU SSID when you add an Identity Provider which enables OSU and provisioning. Since there may be more than one identity provider per Hotspot 2.0 profiles having its own authentication profile, the No Match and Unspecified mapping could be duplicated. To avoid duplication, the default identity provider is taken as the correct configuration for No Match and Unspecified mapping. OSUSSID can be OSEN or OPEN [Guest].

You can also click **Create** to create a Hotspot 2.0 identity provider. See [Creating a Hotspot 2.0 Identity Provider](#) for more information.

- **Single SSID:** Provides capability to support both OSU network and production network on the same WLAN. This option is available only when the Identity Provider has enabled Online Signup & Provisioning.
- **Onboarding SSID:** Allows the devices to connect to a Wi-Fi network automatically, where the service providers engage in roaming partnership to provide seamless access to Wi-Fi networks. Onboarding SSID is an optional configuration when Single SSID is enabled and a mandatory configuration when Single

SSID is not enabled. This option is available only when the Identity Provider has enabled Online Signup & Provisioning.

- Under **Advanced Options**, Complete the following fields:

**Figure 3.** Create Hotspot 2.0 WLAN Profile - Advanced Options

**Create Hotspot 2.0 WLAN Profile**

**Advanced Options**

Internet Option: ☒ ON ☐ Specified with connectivity to the Internet

Access Network Type:

IPv4 Address:

IPv6 Address:

Connection Capabilities:

Protocol Name	Protocol Number	Port Number	Status
ICMP	1	0	Closed
FTP	6	20	Closed
SSH	6	22	Open
HTTP	6	80	Open
Used by TLS VPN	6	443	Closed
Used by PPTP VPNs	6	1723	Closed
VoIP	6	5060	Closed
VoIP	17	5060	Closed
Used by IKEv2(IPsec VPN)	17	500	Closed
IPsec VPN	17	4500	Closed
ESP	50	0	Closed

Custom Connection Capabilities:

Protocol Name	Protocol Number	Port Number	Status
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Closed"/>

- Internet Options: Specify if this HS2.0 network provides connectivity to the Internet.
- Access Network Type: Access network type (private, free public, chargeable public, etc.), as defined in IEEE802.11u.
- IPv4 Address: Select IPv4 address type availability information, as defined in IEEE802.11u.
- IPv6 Address: Select IPv6 address type availability information, as defined in IEEE802.11u.
- Connection Capabilities: Provides information on the connection status within the hotspot of the most commonly used communications protocols and ports.

Provide the **Protocol Name**, **Protocol Number**, **Port Number** and **Status** to **Add** a new connection.

- Custom Connection Capabilities: Allows addition of custom connection capability rules. Up to 21 custom rules can be created.

Provide the **Protocol Name**, **Protocol Number**, **Port Number** and **Status** to **Add** a new connection.

5. Click **OK**.

- 🔗 **Note:** You can also edit, clone and delete a Hotspot 2.0 WLAN profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **WLAN Profile** tab in the **Hotspot 2.0** window.

Parent topic: [Working with Hotspot 2.0 Services](#)

## Creating a Hotspot 2.0 WiFi Operator Profile

An operator profile defines all the properties pertaining to an operator while a service profile defines the properties related to a service provider. If a WLAN is configured to provide Hotspot 2.0 service, it must be linked exactly like a Hotspot 2.0 operator profile.

1. On the menu, click **Services > Hotspots & Portals > Hotspot 2.0** to display the **Hotspot 2.0** window.

**Figure 1.** Hotspot 2.0: Wi-Fi Operator


The screenshot displays the 'Hotspot 2.0: Wi-Fi Operator' configuration page. The interface includes a top navigation bar with tabs for Monitor, Network, Security, Services, and Administration. The 'Services' tab is active, showing a breadcrumb trail: Services > Hotspots & Portals > Hotspot 2.0. The main content area is divided into two sections: 'Wi-Fi Operator' and 'Identity Provider'. The 'Wi-Fi Operator' section features a table with the following data:

Name	Manage By	Description	Last Modified On	Last Modified By
1205	System	N/A	2021/01/28 17:02:41	admin
407-R2-OP	System	N/A	2021/01/27 17:00:58	admin
HS2.0-S.1.1-GA	System	N/A	2019/04/18 13:27:59	admin
HS2.0-OP	System	N/A	2018/07/26 16:29:21	admin
HS2.0-OP-R2	System	N/A	2018/09/05 10:08:23	admin
Operator	System	Operator	2019/01/30 12:12:30	admin

The 'Identity Provider' section also contains a table with similar columns. The 'Details' panel at the bottom shows the configuration for the selected '1205' operator profile:

- Name: 1205
- Manage By: System
- Description: N/A
- Domain Names: wi-fi.org
- Signup Security: Yes
- Friendly Names: angSP Real Test Only(, korSP 발당 테스트 전용)
- Last Modified By: admin
- Last Modified On: 2021/01/28 17:02:41

2. In the **Organization** tab, select the zone for which you want to create the **Hotspot 2.0** portal.

3. From **Wi-Fi Operator** tab, click  icon to display the **Create Hotspot 2.0 Wi-Fi Operator Profile** dialog box.

**Figure 2.** Creating a hotspot 2.0 Wi-Fi operator profile

## Create Hotspot 2.0 Wi-Fi Operator Profile

\* Name:

Description:

\* Domain Names: \* Domain Name  + Add ✕ Cancel 🗑 Delete

Domain Name
<input type="text"/>

Signup Security: ☐ OFF ☐ Support Anonymous Authentication (OSEN)

\* [?] Certificate:  + ✎

\* Friendly Names: \* Language \* Name

+ Add ✕ Cancel 🗑 Delete

Language	Name
<input type="text"/>	<input type="text"/>

Advice of Charge: + Create Configure Delete

Type	NAI Realm	Plan Information
<input type="text"/>	<input type="text"/>	<input type="text"/>

Operator Icon: \* Language \* Icon

Browse Clear + Add ✕ Cancel 🗑 Delete

Language	Icon	File Name
<input type="text"/>	<input type="text"/>	<input type="text"/>

Terms Conditions: File Name:

Time Stamp:

OK Cancel

#### 4. Complete the following fields:

- Name: Enter a name for this Wi-Fi operator profile.
- Description: Enter a description for the venue profile.
- Domain Names: HS2.0 operator's domain name is a mandatory field, which specifies the operator's domain name. Hotspot 2.0 AP broadcasts the domain name to indicate the home Wi-Fi providers.
- Signup Security: This is an optional field and is disabled by default. Enabling would mean that operator supports secure onboarding (OSEN).


- **Certificate:** Select the certificate for the operator - AAA. This can be the same certificate as the one used with OSU service.
- **Friendly Names:** HS2.0 operator's friendly name is a mandatory field. Operator's friendly name is displayed on mobile client's screen. It is also used for operator verification during secure onboarding (OSEN). Select the display language from the drop down list.
- **Advice of Charge:** The advice of charge may be issued for the first time or every time a user connects to a Wi-Fi service. The advice of charge must be acknowledged before accessing the network. Click **Create** to display the **Create Advice of Charge** dialog box.

Complete the following fields:

- **Type:** Select one of the following plan type.
  - Time-Based
  - Data-Volume-Based
  - Time-and-Data-Volume-Based
  - Unlimited
- **NAI Realm:** Select one of the following encoding option.
  - Encoding
  - Name
- **Plan Information:** The plan information is provided on a per NAI-realm basis. Each authentication realm can advertise the charges associated with obtaining the network access. Click **Create**, the **Create Plan Information** form is displayed. Update the following plan information.
  - Language
  - Currency
  - XML content
- Click **OK**.
- **Operator Icon:** A maximum of two icons can be uploaded for an operator profile. The maximum size of an icon can be upto 64 KB. Select the **Language**, click **Browse** to select an icon, and click **Add**.
- **Terms Conditions:** Allows to communicate the terms and conditions of the Wi-Fi services. Updated terms and conditions can also be communicated to existing service users. Update the following information.

- File Name
- Time Stamp

5. Click **OK**.

 **Note:** You can also edit, clone, and delete a Hotspot 2.0 WLAN profile by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Wi-Fi Operator** tab in the **Hotspot 2.0** window.

Parent topic: [Creating a Hotspot 2.0 WLAN Profile](#)

## Creating a Hotspot 2.0 Identity Provider

The Hotspot 2.0 identity provides the authentication, accounting and online sign-up service. There can be one or more identity providers per Hotspot 2.0 access WLAN.

To configure the Hotspot 2.0 Identity Provider, go to **Services > Hotspot & Portals > Hotspot 2.0 > Identity Provider** and click **Create**. The **Create Hotspot 2.0 Identity Provider** page is displayed. Configure the following details to create a Hotspot 2.0 Identity Provider:

1. Network Identifier
2. Online Signup and Provisioning
3. Authentication
4. Accounting
5. Review

Parent topic: [Creating a Hotspot 2.0 WLAN Profile](#)

## Configure the Hotspot 2.0 Identity Provider

1. On the menu, click **Services > Hotspot & Portals > Hotspot 2.0 > Identity Provider** to display the **Identity Provider** window.  
**Figure 1.** Hotspot 2.0: Identity Provider

The screenshot displays the Ruckus SmartZone (LT-GA) Guest Access Guide interface. The top navigation bar includes tabs for Monitor, Network, Security, Services, Administration, and a search bar. The main content area is divided into two sections: Wi-Fi Operator and Identity Provider.

**Wi-Fi Operator**

Name	Manage By	Description	Last Modified On	Last Modified By
1205	System	N/A	2021/01/28 17:02:41	admin
407-R2-OP	System	N/A	2021/01/27 17:00:58	admin
HSD-0-S-1-GA	System	N/A	2019/04/18 13:27:59	admin
HSD-0-OP	System	N/A	2018/07/26 16:29:21	admin
HSD-0-CP-R2	System	N/A	2018/09/05 10:08:23	admin
Operator	Operator		2019/01/30 12:12:30	admin

8 records

**Identity Provider**


Name	Manage By	Online Signup Service	Description	Last Modified On	Last Modified By
1205	System	https://osu-server/2/testbed-aru-wi-fi.org/944...	N/A	2021/01/28 17:01:55	admin
1315	System	https://osu-server/2/testbed-aru-wi-fi.org/944...	N/A	2021/03/17 12:48:59	admin
407-R2	System	https://osu-server/2/testbed-aru-wi-fi.org/44...	N/A	2022/05/23 15:44:15	API
HSD-0-GA-S-11	System	https://osu-server/2/testbed-aru-wi-fi.org/44...	N/A	2019/04/18 13:26:49	admin
HSD-0-IP	System	https://osu-server/2/testbed-aru-wi-fi.org/44...	N/A	2018/07/27 16:00:29	admin
HSD-0-R2-ID-392	System	https://osu-server/2/testbed-aru-wi-fi.org/44...	N/A	2018/08/13 11:15:09	admin
HSD-0-R2-IP	System	https://osu-server/2/testbed-aru-wi-fi.org/44...	N/A	2019/01/07 16:29:29	admin
HSD-Pretest	System	https://osu-server/2/testbed-aru-wi-fi.org/44...	HSD-Pretest	2019/01/30 12:23:24	admin

8 records

**DETAILS**

Name: 1205  
 Manage By: System  
 Description: N/A  
 Domain Names: wi-fi.org  
 Signup Security: Yes  
 Friendly Names: ang/SP But Test Only, kor/SP 테스트 (외국인 전용)  
 Last Modified By: admin  
 Last Modified On: 2021/01/28 17:02:41

2. In the **Organization** tab, select the zone for which you want to create the **Identity Provider** portal.

3. In the **Identity Provider** tab, click the  icon to display the **Create Hotspot 2.0 Identity Provider** dialog box.

**Figure 2.** Creating a Hotspot 2.0 Identity Provider

### Create Hotspot 2.0 Identity Provider

[Network Identifier](#) → [Online Signup & Provisioning](#) → [Authentication](#) → [Accounting](#) → [Review](#)

\* Name:  ⓘ

Description:

PLMNs: \* MCC  \* MNC  [+ Add](#) [X Cancel](#) [Delete](#)

MCC	MNC
<input type="text"/>	<input type="text"/>

\* Realms:

\* Name:  [+ Add](#) [X Cancel](#) [Delete](#)

\* Encoding: RFC-4282

EAP Methods:

#1	#2	#3	#4
EAP Method: <input type="text" value="N/A"/>			

Name	Encoding	EAP Methods
<input type="text"/>	<input type="text"/>	<input type="text"/>

Home OIs: \* Name  \* Length  \* Organization ID  [+ Add](#) [X Cancel](#) [Delete](#)

Name	Length	Organization ID
<input type="text"/>	<input type="text"/>	<input type="text"/>

[Next](#) [Cancel](#)

4. Configure the following sections to create a **Hotspot 2.0 Identity Provider**:

- Network Identifier
- Online Signup and Provisioning
- Authentication
- Accounting
- Review

## Network Identifier

- Complete the following fields:

**Figure 3.** Create Hotspot 2.0 Identity Provider - Network Identifier

## Create Hotspot 2.0 Identity Provider

Network Identifier → Online Signup & Provisioning → Authentication → Accounting → Review

\* Name:  ⓘ

Description:

PLMNs: \* MCC  \* MNC  + Add ✕ Cancel 🗑 Delete

MCC ▲	MNC
<input type="text"/>	<input type="text"/>

\* Realms:

\* Name:  + Add ✕ Cancel 🗑 Delete

\* Encoding:

EAP Methods:

#1	#2	#3	#4
EAP Method: <input type="text" value="N/A"/>			

Name ▲	Encoding	EAP Methods
<input type="text"/>		

Home OIs: \* Name  \* Length  \* Organization ID  + Add ✕ Cancel 🗑 Delete

Name ▲	Length	Organization ID
<input type="text"/>	<input type="text"/>	<input type="text"/>


Next
Cancel

- Name: Enter a name or this network identifier profile.
- Description: Enter a description for the network identifier profile.
- PLMNs: Each record contains MCC and MNC.


Complete the following fields and click the + Add icon to add the PLMNs. The configured information will be displayed in a table below the **PLMNs** field.

- MCC: Set the correct country code for the geographical location. This is required when the controller sends MAP authentication information. Type the mobile country code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.
- MNC: Set the mobile network code based on the geographical location. This is required when controller sends MAP authentication information. Type the mobile network code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.

- **Realms:** List of NAI realms corresponding to service providers or other entities whose networks or services are accessible via this AP. Up to 16 NAI realm entries can be created. Each NAI realm entry can contain up to four EAP methods.

Complete the following fields and click  icon to add the Realms. The configured information will be displayed in a table below the **Realms** field.

- **Name:** Enter a name.
- **Encoding:** Choose between RFC-4282 and UTF-8.
- **EAP Methods:** Choose the **EAP Methods** from the drop down list. You can select four **EAP Methods**, click **#1**, **#2**, **#3**, or **#4** to configure the **EAP Methods** for each choice.
- **Home OIs:** Organization Identifier (OI) is a unique value assigned to the organization. User can configure a maximum of 12 OI values and can adjust the order since the AP takes only 3 OIs in the beacon.

Complete the following fields and click  icon to add the Home OIs. The configured information will be displayed in a table below the **Home OIs** field.

- **Name:** Enter a name.
- **Length:** Choose between 3 Hexadecimal or 5 Hexadecimal.
- **Organization ID:** Enter organization ID in the XX-XX-XX format for 3 Hexadecimal or XX-XX-XX-XX-XX format for 5 Hexadecimal.

2. Click **Next**.

## Online Signup and Provisioning

1. Complete the following fields:

**Figure 4.** Create Hotspot 2.0 Identity Provider - Online Signup and Provisioning

## Create Hotspot 2.0 Identity Provider

Network Identifier → Online Signup & Provisioning → Authentication → Accounting → Review

☒ Enable Online Signup & Provisioning

- [External Service URL] This field is required
- [OSU NAI Realm] This field is required
- [OSU Service Description] is required

**Provisioning Options**

Provisioning Service: \* External Service URL:  ⓘ

Provisioning Protocol: ☐ OFF OMA-DM ☒ ON SOAP-XML

**Online Signup Options**

OSU NAI Realm:  ⓘ

Single SSID NAI:

Common Language Icon:  Browse

OSU Service Description:

Language	Friendly Name	Description	Icon	
English				<span>Browse</span> <span>+ Add</span> <span>✕ Cancel</span> <span>🗑 Delete</span>
Language ▲	Friendly Name	Description	Icon	Format Width Height

Whitelisted Domains: \* Domain Name  + Add ✕ Cancel 🗑 Delete

Domain Name ▲

Back
Next
Cancel

- Provisioning Options tab, complete the following fields:

- Provisioning Service.

External Service URL: Enter the external OSU server URL.

The provisioning service is responsible for any subscription provisioning process in which messages are communicated between the UE and the SZ resulting in a PPS-MO provisioned into the UE. The provisioning supports both SOAP-XML and OMA-DM as communication protocols for the process based on the initial request coming from the UE. The provisioning service supports sign-up; remediation and policy update flows where the UE is provisioned with a full PPS -MO or only with internal node/s of the PPS-MO. Administrator can only set External Internal Provisioning Services, where the administrator is required to fill the external OSU server URL.

- Provisioning Protocol: Switch ON communication protocols OMA-DM or SOAP-XML.
- Online Signup Options tab, complete the following fields:
- OSU NAI Realm: Select from the drop down list.

This configuration is only for External Provision Service. In case of Internal Provisioning Service, the NAI realm should be configured per authentication service, which is available during on-boarding.

- Single SSID NAI: Enter the SSID.

This configuration is for enabling single SSID for WLAN profile, The NAI length can have a maximum of 255 characters.

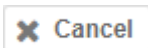

- Common Language Icon: Click **Browse** to upload the language icon.


This is the default icon presented in the device for this identity provider in case the device does not find any match for other icons per language in the table.

- OSU Service Description: This configures the friendly name, description and icon per language. This information is presented on the device when it receives ANQP message which includes OSU providers. Friendly names, which are required to be part of the OSU certificate is automatically populated in this table. In case description is also included in the OSU certificate it is automatically populated into the table. Administrators are required to set the matched icon per language as included in the OSU certificate.

Complete the following fields and click the  icon to add the OSU Service Description. The configured information will be displayed in a table below the **OSU Service Description** field.

- Language: Select the language from the drop down list.
- Friendly Name: Enter the name.
- Description: Enter the description.
- Icon: Click **Browse** to upload the icon.

Click the  icon to exit from the creating OSU Service Description. To delete the OSU Service Description, select the Friendly Name and click the  icon.

- Whitelisted Domain: Add the domain names and click the  icon to add the External Portal domain.

2. Click **Next**.

## Authentication

1. Complete the following fields:

**Figure 5.** Create Hotspot 2.0 Identity Provider - Authentication

## Create Hotspot 2.0 Identity Provider

[Network Identifier](#) → [Online Signup & Provisioning](#) → **Authentication** → [Accounting](#) → [Review](#)

Authentication Services for Access WLAN ▼

[+ Create](#) [Configure](#) [Delete](#)

Realm	Protocol	Auth Service	Dynamic VLAN ID
No Match	NA	NA-Disabled	N/A
Unspecified	NA	NA-Disabled	N/A

Note: If device onboarding was done with credential type 'remote', then map your 'realm' value to its respective authentication service PLUS define 'Unspecified' realm & map it to corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.

[Back](#) [Next](#) [Cancel](#)

Click the  icon to display the **Create Realm Based Authentication Service** dialog box.

**Figure 6.** Create Realm Based Authentication Service

## Create Realm Based Authentication Service

\* Realm:


\* Service:  [+](#) [✎](#)


Dynamic VLAN ID:

[OK](#) [Cancel](#)

Complete the following fields:

- **Realm:** Enter the realm information to configure the realm mapping to the authentication service.
- **Service:** Select the service from the drop down list to map the realm to an external RADIUS server which should be pre-configured.

To create a realm service, click  icon to display the **Create Authentication Service** dialog box. Create an authentication service, refer to *Creating Realm Based Authentication Profile* from the *Security Guide*.

Click the  Icon to edit the selected realm service.

- Dynamic VLAN ID: Enter the VLAN ID.

To modify the realm, select the realm from the table and click **Configure** icon.

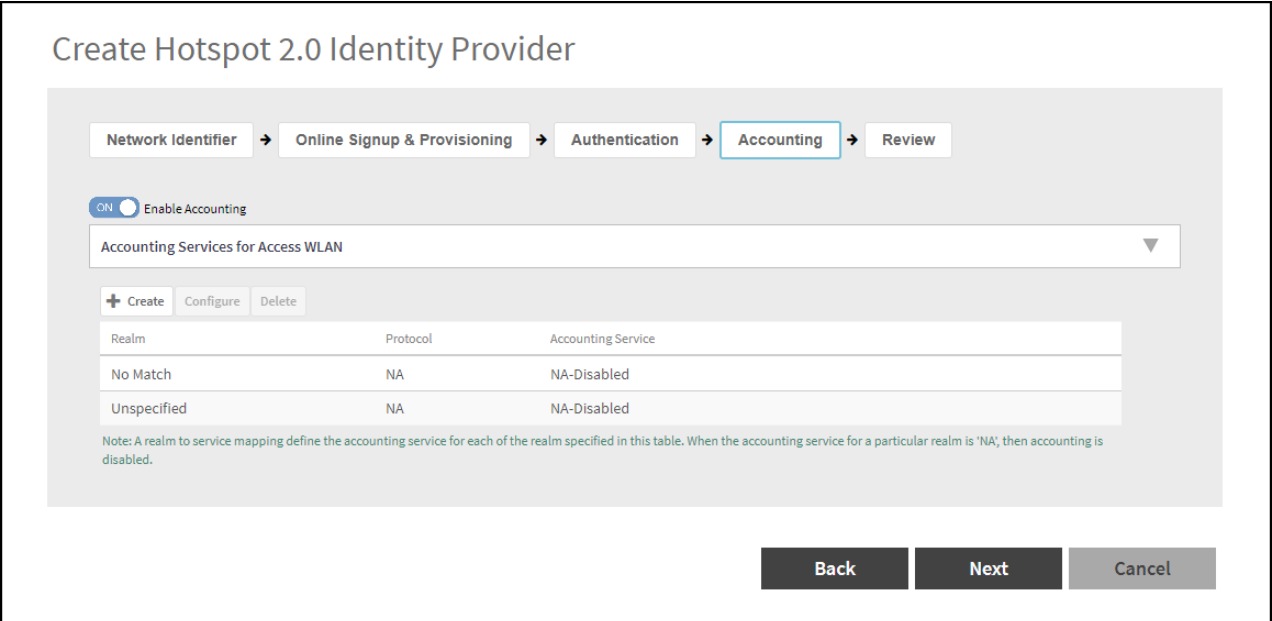
To delete the realm, select the realm from the table and click **Delete** icon.

2. Click **Next**.

## Accounting

1. This feature is OFF by default, turn it ON to enable accounting and to display the table.

**Figure 7.** Create Hotspot 2.0 Identity Provider - Accounting



Create Hotspot 2.0 Identity Provider

Network Identifier → Online Signup & Provisioning → Authentication → **Accounting** → Review

☒ ON Enable Accounting

Accounting Services for Access WLAN ▼

**+ Create** Configure Delete

Realm	Protocol	Accounting Service
No Match	NA	NA-Disabled
Unspecified	NA	NA-Disabled

Note: A realm to service mapping define the accounting service for each of the realm specified in this table. When the accounting service for a particular realm is 'NA', then accounting is disabled.

Back Next Cancel

Click the  **Create** icon to display the **Create Realm Based Accounting Service** dialog box.

**Figure 8.** Create Realm Based Accounting Service

**Create Realm Based Accounting Service**

\* Realm:

\* Service: No data available +

**OK** **Cancel**

Complete the following fields:

- Realm: Enter the realm information.

If the authentication's realm is set as remote credential type, administrator should set this realm here to the customer's external accounting server.

- Service: Select the service from the drop down list.

To create a realm service, click the icon to display the **Create Accounting Service** dialog box. Create an authentication service, refer to *Creating Proxy Accounting AAA Servers* from the *Security Guide*.

Click the icon to edit the selected realm service.

To modify the realm, select the realm from the table and click **Configure** icon.

To delete the realm, select the realm from the table and click **Delete** icon.

2. Click **Next**.

## Review

Review the configuration on the page before committing the changes to the server. Click **OK** to create the Hotspot 2.0 identity provider.

**Figure 9.** Create Hotspot 2.0 Identity Provider - Review

## Create Hotspot 2.0 Identity Provider

[Network Identifier](#) → [Online Signup & Provisioning](#) → [Authentication](#) → [Accounting](#) → [Review](#)

\* Name:

Description:

PLMNs:

MCC	MNC
123	133

\* Realms:

Name	Encoding	EAP Methods
test	RFC-4282	#1: N/A #2: N/A #3: N/A #4: N/A

Home OIs:

Name	Length	Organization ID
tst	5 Hex	0x00 0x00 0x00 0x00 0x00

☒ Enable Online Signup & Provisioning

Provisioning Options

Provisioning Service: \* External Service URL:

\* Provisioning Protocol: ☒ OMA-DM ☐ SOAP/XML

Online Signup Options

\* OSU NAI Realm:

Single SSID NAI:

\* Common Language Icon:

\* OSU Service Description:

Language	Friendly Name	Description	Icon	Format	Width	Height
English	test	1212222			N/A	N/A

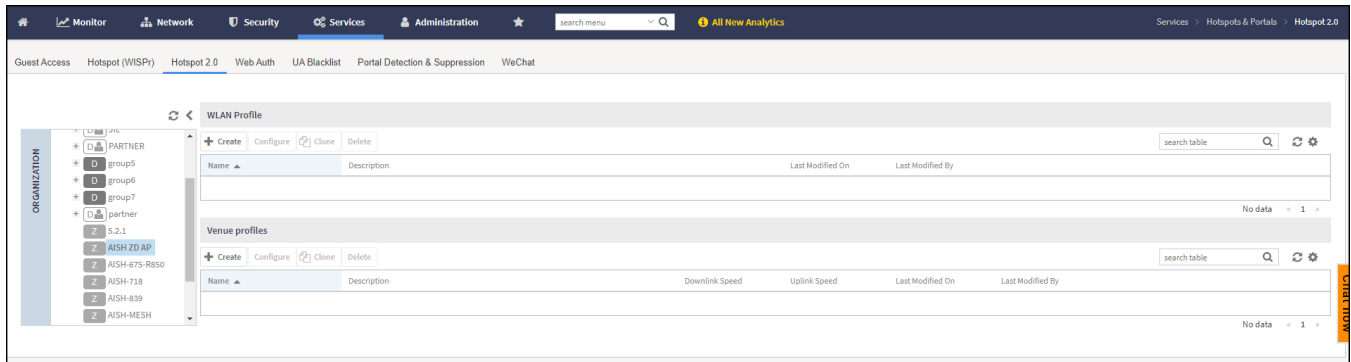
**Note:** You can also edit, clone and delete a Hotspot 2.0 WLAN profile by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Identity Provider** tab in the **Hotspot 2.0** window.

## Creating a Hotspot 2.0 Venue Profile


The hotspot 2.0 technology allows users to seamlessly roam between the provider's home Wi-Fi network and the visited Wi-Fi network in a different location. A Wi-Fi provider can partner with several roaming partners to provide Wi-Fi access to partner's subscribers. Public venues such as institutions, restaurants, and stadiums are considered roaming partners.

1. On the menu, click **Services > Hotspots & Portals > Hotspot 2.0** to display the **Hotspot 2.0** window.

**Figure 1.** Hotspot 2.0 - Venue Profiles

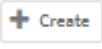


2. In the **Organization** tab, select the zone for which you want to create the **Hotspot 2.0 Venue Profiles**.

3. In the **Venue profiles**, click the  icon to display the **Hotspot 2.0 Venue Profiles** dialog box.

**Figure 2.** Creating a Hotspot 2.0 Venue Profile

4. Complete the following fields:

- **Name:** Enter a name for this venue profile. This name identifies the venue profile when assigning an HS2.0 service to a HS2.0 venue.
- **Description:** Enter a description for the venue profile.
- **Venue Names:** Select the venue from the table or to create a new venue, click the  icon to display the **Create Venue Names** dialog box.
  - **Venue Names:** Select the language from the drop down list.

- **Name:** Enter a name for the new venue.
- **URL:** Enter additional URLs to the venue name and click **Add**. The URL can have a maximum of 254 characters. A maximum of four venue URLs can be mapped to a venue name.
- Click **OK**.
- **Venue Category:** Select venue group from the drop down list and venue type as defined in IEEE802.11u, Table 7.25m/n.
- **WAN Metrics:** Enter information about the WAN link connecting an IEEE 802.11 access network and the Internet; includes uplink/downlink speed estimates.

Select the operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.

5. Click **OK**.

- 🔗 **Note:** You can also edit, clone and delete a Hotspot 2.0 venue profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Venue Profile** tab in the **Hotspot 2.0** window.

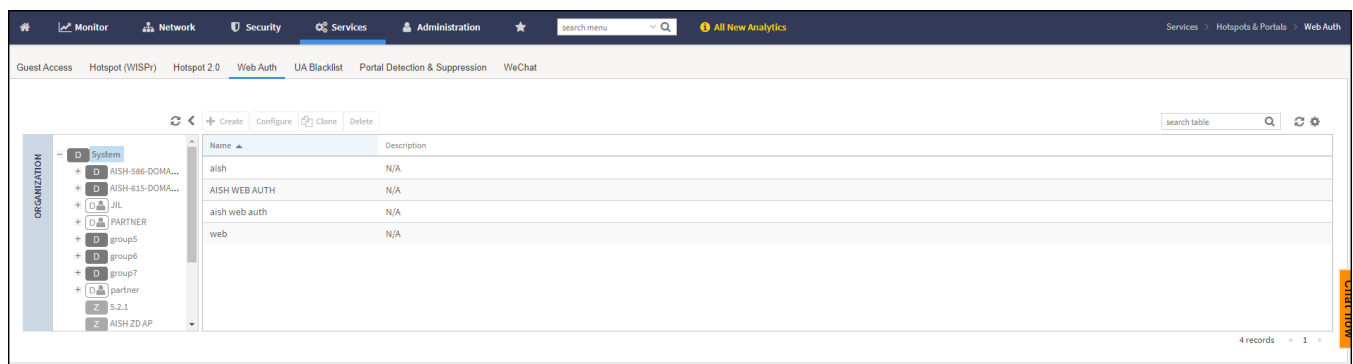
Parent topic: [Working with Hotspot 2.0 Services](#)

## Creating a Web Authentication Portal

Web Authentication (also known as a “captive portal”) redirects users to a login web page the first time they connect to this WLAN, and requires them to log in before granting access to use the WLAN.

1. On the menu, click **Services > Hotspots & Portals > Web Auth** to display the **Web Auth** window.

**Figure 1. Web Auth**



2. In the **Organization** tab, select the zone for which you want to create the **Web Auth**.
3. Click **Create** to display the **Create Web Authentication Portal** dialog box.

Figure 2. Creating a Web Authentication Portal

**Create Web Authentication Portal**

**General Options**

\* Portal Name:

Portal Description:

\* Language:

**Redirection**

Start Page: After user is authenticated,

☒ Redirect to the URL that user intends to visit. ☐ Redirect to the following URL:

\*

**Web Authentication**

[?] Web Portal Logo:

Web Portal Title:

**User Session**

\* Session Timeout:  Minutes (2-14400)

\* Grace Period:  Minutes (1-14399)

4. Complete the following fields:


- General Options
  - Portal Name: Type a name for the hotspot service portal that you are creating.
  - Portal Description: Type a short description of the hotspot service portal.
  - Language: Select the display language that you want to use on the web authentication portal.
- Redirection (Select where to redirect the user after successfully completing authentication.)

- Redirect to the URL that user intends to visit: Allows the guest user to continue to destination URL without redirection.
- Redirect to the following URL: Redirect the user to a specified web page (entered into the text box) prior to forwarding to the destination URL. When a guest user lands on this page, the guest pass expiration time is displayed.

Enter a domain name or IP address to which to be redirected.

- Web Authentication
  - Web Portal Logo: By default, the web portal page displays the Ruckus logo. To use your own logo, click the **Browse** button, select your web portal logo (recommended size is 138 x 40 pixels, maximum file size is 20 KB), and then click **Open**.
  - Web Portal Title: Type your own web portal title text or accept the default portal title text (Welcome to the Web Authentication login page).
- User Session
  - Session Timeout: Set a time limit (in minutes) after which users will be disconnected from the hotspot service and will be required to log in again.
  - Grace Period: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot service without having to log in again.

5. Click **OK**.

 **Note:** You can also edit, clone, or delete a Web Authentication by selecting the options **Configure**, **Clone**, and **Delete**, respectively, from the **Web Auth** window.

Parent topic: [Working with Hotspots and Portals](#)

## Creating a UA Blacklist Profile

The controller automatically blocks certain user agents (or software used by a user) from accessing hotspots provided by controller-managed APs. When the controller blocks any of these user agents, an error message appears on the user device. You can add to or remove user agents from this blacklist.

Following are some of the blocked user agents:

- ZoneAlarm
- VCSOAPClient
- XTier NetIdentity

- DivX Player
- Symantec LiveUpdate
- Windows Live Messenger
- StubInstaller
- windows-update-agent
- Windows Live Essentials
- Microsoft Dr. Watson for Windows (MSDW)
- Avast Antivirus Syncer
- Microsoft Background Intelligent Transfer Service (BITS)
- Google Update
- TrendMicro client
- Skype WISPr

To blacklist a user agent profile:

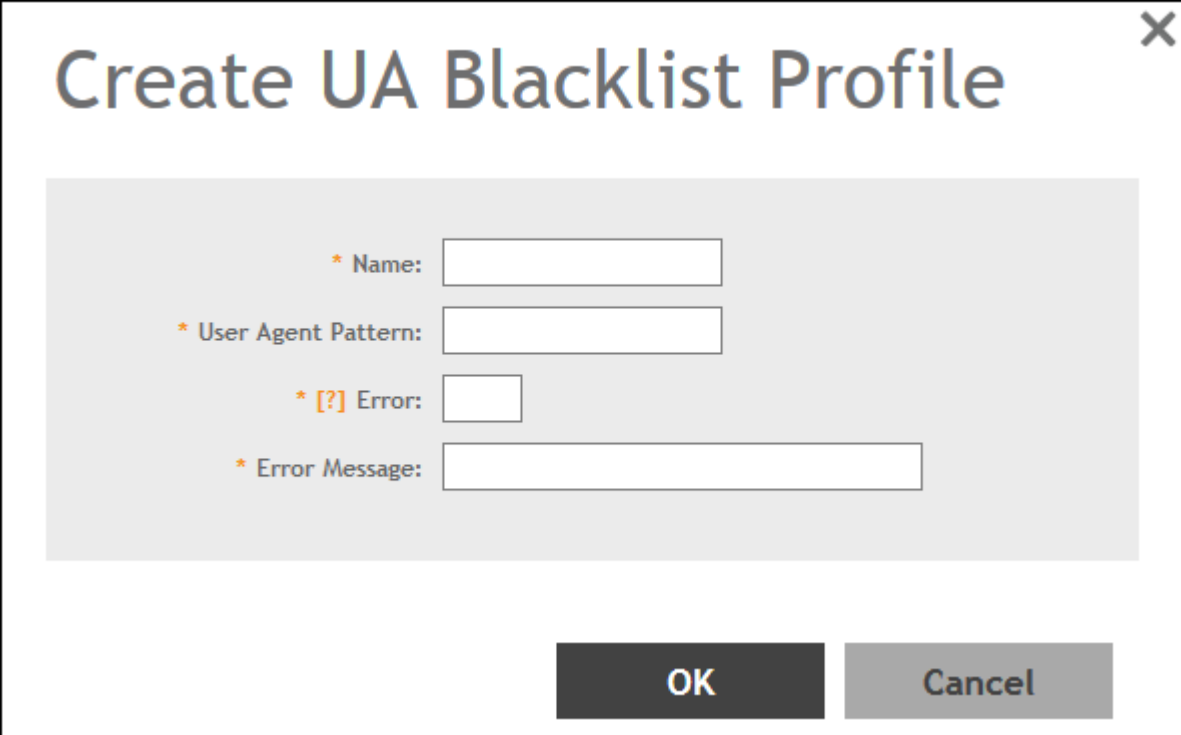
1. On the menu, click **Services > Hotspots & Portals > UA Blacklist** to display the **UA Blacklist** window.

**Figure 1. UA Blacklist**

Name	User Agent Pattern	Error	Error Message
DivX Player	*DivX Player*	503	Un-authorized protocol detected - DivX Player
Google Update	*Google Update.*	503	Un-authorized protocol detected - Google Update
Microsoft BITS	*Microsoft BITS.*	503	Un-authorized protocol detected - Microsoft BITS
MSDW	*MSDW.*	503	Un-authorized protocol detected - MSDW
Skype WISPr	*[sS]kype.*	503	Un-authorized protocol detected - Skype WISPr
StubInstaller	*StubInstaller.*	503	Un-authorized protocol detected - StubInstaller
Symantec LiveUpdate	*Symantec LiveUpdate.*	503	Un-authorized protocol detected - Symantec LiveUpdate
Syncer	*Syncer.*	503	Un-authorized protocol detected - Syncer AVAST AV
TrendMicro client	*TMUFE.*	503	Un-authorized protocol detected - TrendMicro client TMUFE
VCSOAPClient	*VCSOAPClient.*	503	Un-authorized protocol detected - VCSOAPClient
Windows Live Essentials	*[Ww]indows [Ll]ive [Ee]ssentials.*	503	Un-authorized protocol detected - Windows Live Essentials
Windows Live Messenger	*Windows Live Messenger.*	503	Un-authorized protocol detected - Windows Live Messenger
windows-update-agent	*[wW]indows-[uU]pdate-[aA]gent.*	503	Un-authorized protocol detected - windows-update-agent
XTier NetIdentity	*XTier NetIdentity.*	503	Un-authorized protocol detected - XTier NetIdentity
ZoneAlarm	*ZoneAlarm.*	503	Un-authorized protocol detected - ZoneAlarm

2. Click the  icon to display the **Create UA Blacklist Profile** dialog box.

**Figure 2. Creating a UA Blacklist Profile**



**Create UA Blacklist Profile**

\* Name:

\* User Agent Pattern:

\* [?] Error:


\* Error Message:

OK Cancel

3. Complete the following fields:

- Name: Enter the name of the user agent.
- User Agent Pattern: Type the agent pattern.
- Error: Specify the error message number.
- Error Message: Specify the error message.

4. Click **OK**.

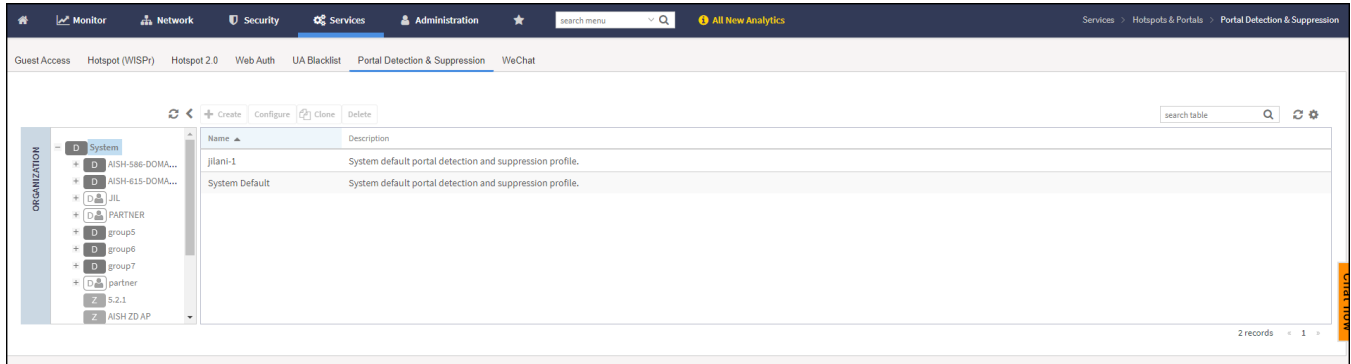
 **Note:** You can also edit, clone, and delete a UA blacklist profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **UA Blacklist** window.

Parent topic: [Working with Hotspots and Portals](#)

## Creating a Portal Detection and Suppression Profile

To restrict an unauthorized user in a walled garden, a service operator must set defined policy rules by creating a portal detection and suppression profile.

1. On the menu, click **Services > Hotspots & Portals > Portal Detection & Suppression** to display the **Portal Detection & Suppression** window.

**Figure 1. Portal Detection & Suppression**

2. In the **Organization** tab, select the zone for which you want to create the **Portal Detection**.

3. Click the  **Create** icon to display the **Portal Detection & Suppression** dialog box.

**Figure 2. Creating Portal Detection Profile**

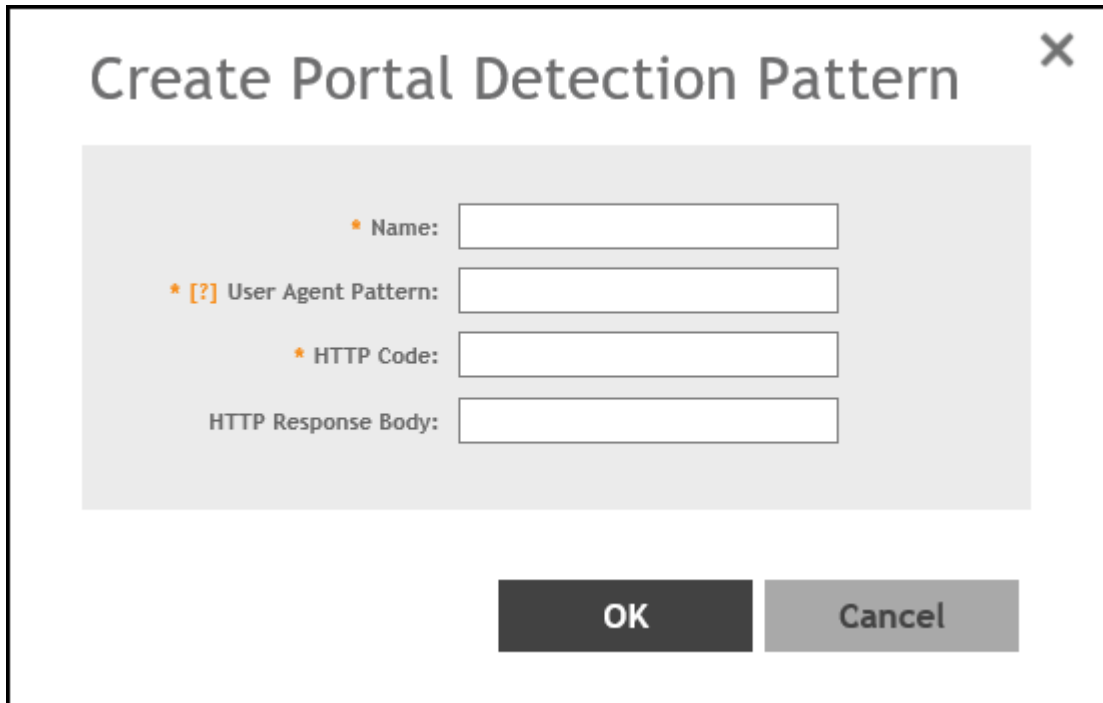
4. Complete the following fields:

- General Options
  - Name: Enter a policy list name.
  - Description: Enter description for the policy list.

- Portal Detection Patterns: Select the portal detection patterns from the table or create a portal detection pattern as show below.



- Click the  icon to display the **Create Portal Detection Pattern** dialog box.

**Figure 3.** Creating Portal Detection Pattern



The dialog box titled "Create Portal Detection Pattern" features a close button (X) in the top right corner. It contains four input fields, each preceded by an asterisk (\*) indicating they are required. The fields are: "Name:", "\* [?] User Agent Pattern:", "\* HTTP Code:", and "HTTP Response Body:". Below these fields are two buttons: "OK" and "Cancel".

- Complete the following fields:

- Name: Enter the name of the portal detection pattern.
- User Agent Pattern: Enter the user agent pattern.
  -  **Note:** The user agent pattern must follow a regular expression format, starting and ending with . \* (for example, . \* Android-WiFi. \*). The default captive portal detection may not support all the Android devices and the new Microsoft phone if different user agent patterns are used. In this case, new rules must be created to cover such patterns. Using an improper user agent pattern may impact browser behaviors.
- HTTP Code: Enter the code.
  -  **Note:** The HTTP code range must be from 100 through 599.
- HTTP Response Body: Enter the HTML string.

c. Click **OK**.

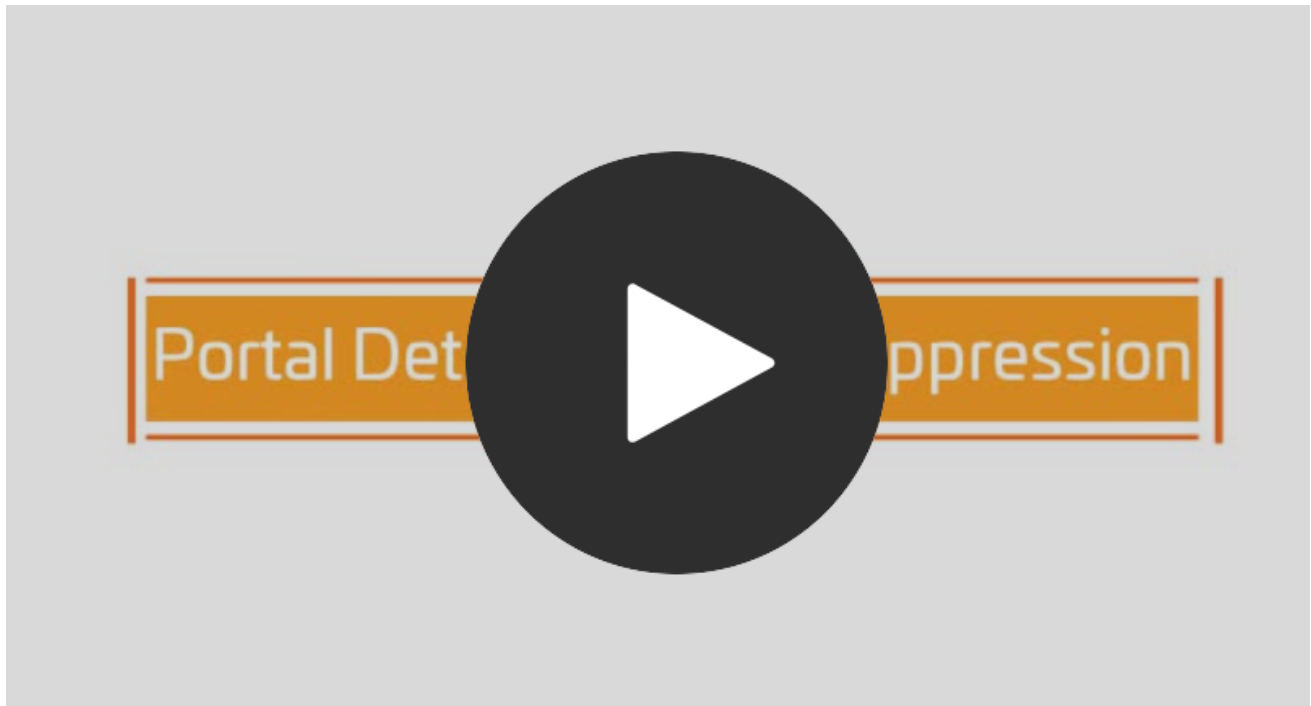
- **Note:** You can also edit, clone, and delete a Portal Detection Patterns by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Portal Detection Patterns** tab.

5. Click **OK**.

- **Note:** To select a **Portal Detection Pattern** profile, **Bypass CNA** must be enabled in the WLAN configuration page. Use **Bypass CNA** to enable or disable portal detection service for **HotSpot**, **Web Authentication**, and **Guest Access WLAN**.
- **Note:** You can also edit, clone, or delete a portal detection and suppression by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Portal Detection & Suppression** window.

#### Video:

**Portal Detection and Suppression Overview.** This video provides a brief overview of portal detection and suppression.



[Click to play video in full screen mode.](#)

**Parent topic:** [Working with Hotspots and Portals](#)

#### Related information

[Video: Portal Detection and Suppression Overview](#)

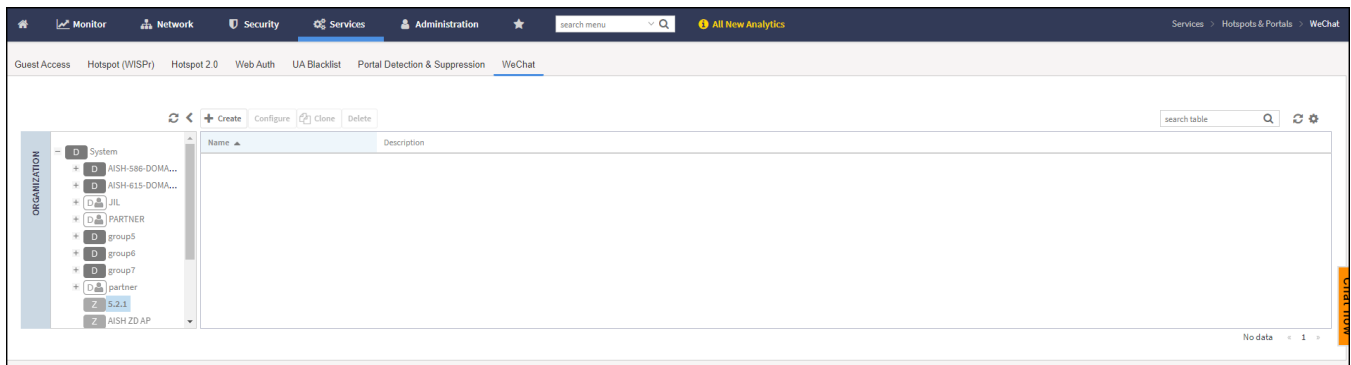
# Creating a WeChat Portal


WeChat is a mobile app from Tenecent that enables its users to call and send text messages to one another. If you have WeChat users on the network and you want your WLANs to support WeChat services, you can create a WeChat portal that WeChat users can use.

A WeChat portal defines the third party authentication server, also known as the equipment service provider (ESP) server, to which the controller will forward all WeChat authentication requests from wireless devices that are associated with controller-managed APs. In turn, the third party authentication server will forward these authentication requests to the WeChat server.

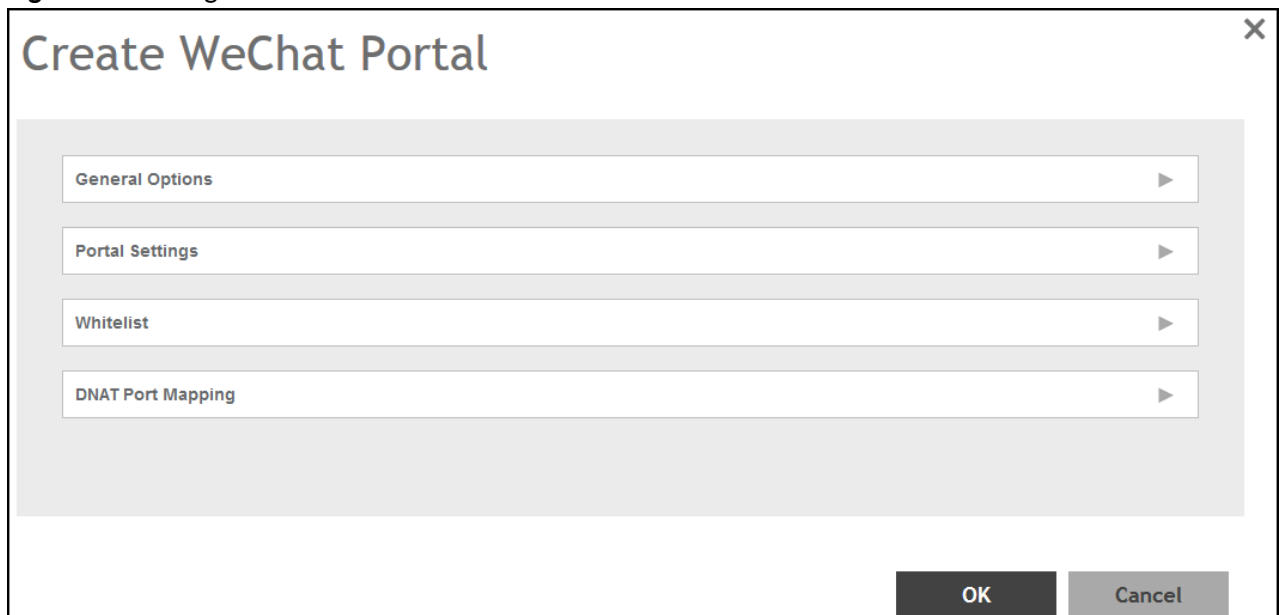
1. On the menu, click **Services > Hotspots & Portals > WeChat** to display the **WeChat** window.

**Figure 1.** WeChat



2. In the **Organization** tab, select the zone for which you want to create the **WeChat** portal.
3. Click the  **Create** icon to display the **Create WeChat Portal** dialog box.

**Figure 2.** Creating a WeChat Portal



#### 4. Complete the following fields:

- General Options

**Figure 3.** Create WeChat Portal - General Options

Create WeChat Portal

General Options

\* Name:

Description:

- Name: Type a name for the portal that you are creating.
- Description: Type a short description of the portal.

- Portal Settings

**Figure 4.** Create WeChat Portal - Portal Settings

Create WeChat Portal

General Options

Portal Settings

\* Authentication URL:

\* DNAT Destination:

Grace Period:  Minutes (1-14399)

\* Blacklist:

- Authentication URL: Enter the authentication interface URL on the third party authentication server. When a managed AP receives a WeChat logon request from a client device, it will send the request to this authentication URL and get the authorization result.
- DNAT Destination: Enter the DNAT destination server address to which the controller will forward HTTP requests from unauthenticated client devices. The DNAT destination server and the authentication server (above) may or may not be the same server.
- Grace Period: Enter the number of minutes during which disconnected users who were recently connected will be allowed to reconnect to the portal without needing to re-authenticate. The default grace period is 60 minutes (range is between 1 and 14399 minutes).
- Blacklist: Enter the network destinations that the controller will automatically block associated wireless clients from accessing. Use a comma to separate multiple entries.

- Whitelist

**Figure 5.** Create WeChat Portal - Whitelist

**Create WeChat Portal**

General Options ▶

Portal Settings ▶

Whitelist ▼

Whitelist: \* Walled Garden Entry  **+ Add** **Import CSV** **✕ Cancel** **🗑 Delete**

Walled Garden Entry ▲

No data « 1 »

Unauthenticated users are allowed to access the following destinations.  
Format:

- IPv4 (e.g. 10.11.12.13)
- IPv4 Range (e.g. 10.11.12.13-10.11.12.15)
- IPv4 CIDR (e.g. 10.11.12.100/28)
- IPv4 and mask (e.g. 10.11.12.13 255.255.255.0)
- IPv6 (e.g. 2607:f0d0:1002:0051:0000:0000:0000:0004)
- IPv6 with prefix (e.g. 2607:f0d0:1002:0051:0:0:0:0/64)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
- \*.amazon.com
- \*.com

- Walled Garden Entry: Enter the network destinations that the controller will automatically allow associated wireless clients to access. You can add a single entry or multiple entries.

To add a single entry, enter the entry in **Wall Garden Entry** field, and then click the **+** icon. The entry you added appears in the table below. To add multiple entries, in a comma-separated value (CSV) file, type all the network destinations that you want to add to the whitelist, and then save the CSV file. In the Whitelist section, click **Import CSV**, and then select the CSV file you created. Click **Open**. The entries in the CSV file are added to the whitelist.

- DNAT Port Mapping

**Figure 6.** Create WeChat Portal - DNAT Port Mapping

**Create WeChat Portal**

General Options ▶

Portal Settings ▶

Whitelist ▶

DNAT Port Mapping ▼

DNAT Port Mapping: Source Port Dest Port + Add x Cancel Delete

Source Port ▲	Dest Port
80	80

Specify at least one pair of source-to-destination port mapping. To add a port mapping, enter the source and destination ports in the fields Source Port and Dest Port, and then click the **+** icon. The AP will use this information to drop or forward HTTP requests from associated clients to specified ports on the DNAT server. For example, if an HTTP request from a wireless client does not originate from the specified source (from) port, the AP will discard the HTTP request. By default, a port mapping of 80-80 (source-destination) exists.

5. Click **OK**.

- 🔗 **Note:** You can also edit, clone and delete a WeChat service portal by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **WeChat** window.

Parent topic: [Working with Hotspots and Portals](#)

## Creating Network Segmentation Profile on the vSZ Controller

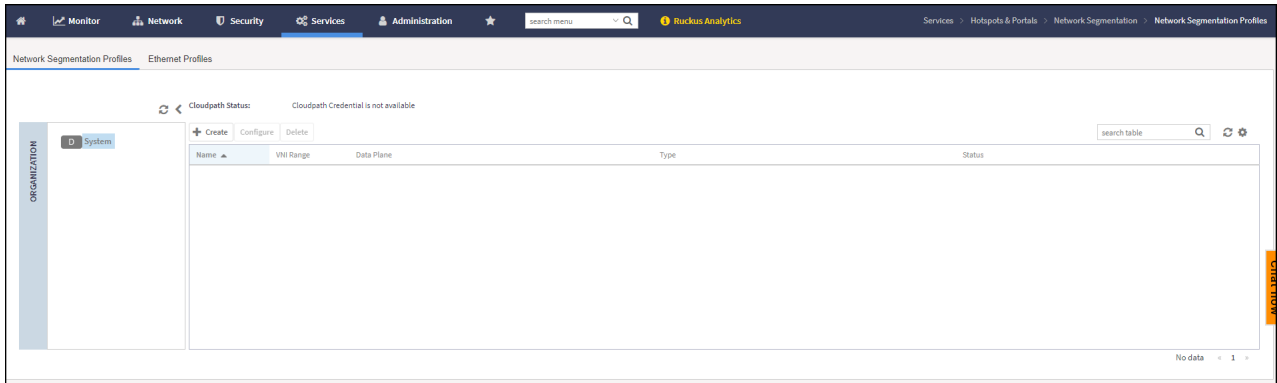
Network Segmentation was designed specifically to target Multi Dwelling Unit (MDU) deployments. Network Segmentation is currently using external Dynamic Pre-shared Key (DPSK) to place a single tenant and their devices into their own individual VXLAN (iLAN).

- 🔗 **Note:** For 6.1.1.5 Smartzone Release, Network Segmentation supports Rodan/ FastIron release 10.0.10 ICX.

Data Plane (DP) will play the role of Home DP or Partner DP. Each DP plays the home DP role and has its own VXLAN Network Identifier (VNI) range. Home DP facilitates MDU UE, connect with each other based on the same VNI number.

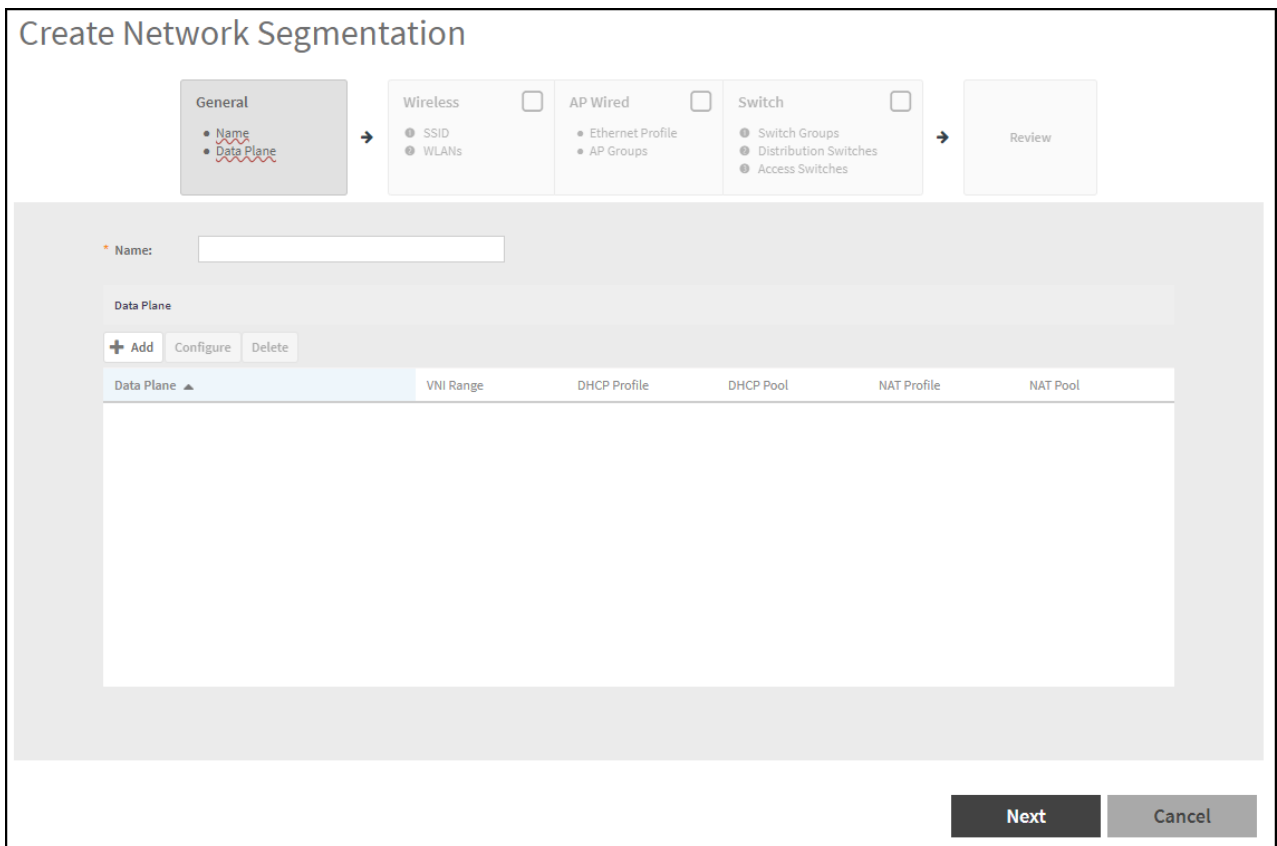
1. On the menu, click **Services > Hotspots & Portals > Network Segmentation > Network Segmentation Profiles** to display the **Network Segmentation Profiles**.

**Figure 1. Network Segmentation Profiles**




2. Click the **Create** icon to display the **Create Network Segmentation** dialog box.

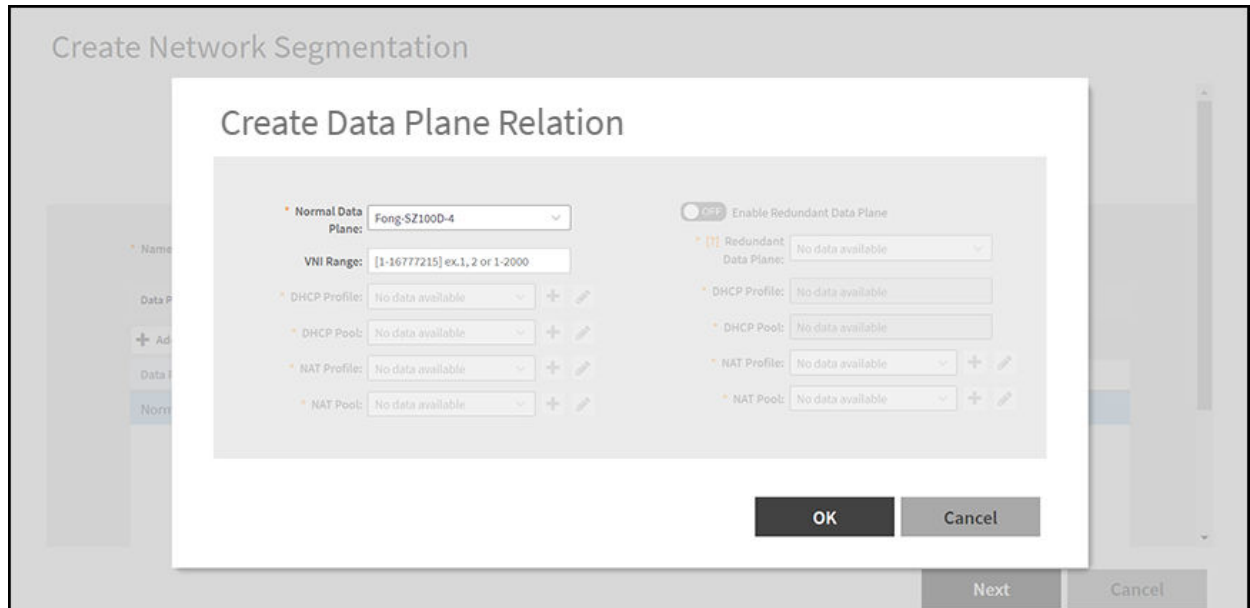
**Figure 2. Editing Network Segmentation Groups in SmartZone User Interface**







3. Complete the following fields under the **General** dialog box:

- **Name:** Enter a network segmentation profile name.
- **Data Plane:** Select the data plane from the table or create a data plane by clicking the  icon to display the **Create Data Plane Relation** dialog box.

**Figure 3.** Creating Data Plane Relation



Complete the following fields:

- **Normal Data Plane:** Select the data plane from the list.
- **VNI Range:** Enter the VNI range; ensure your VNI range is large enough to accommodate all units in the property. Each unit gets its own unique VNI.
- 🔗 **Note:** The VNI value can be mapped from the client data in *Troubleshooting* from the *Management Guide*, if user is having issues in selecting the VNI range.
- **DHCP Profile:** Select the DHCP profile from the drop down list or click the  to create a DHCP Profile. refer to *Creating Profile-based DHCP* from the RUCKUS Traffic Management Guide.
- **DHCP Pool:** Select the DHCP pool from the drop down list or click the  to create a DHCP pool. Refer to *Creating Profile-based DHCP* from the RUCKUS Traffic Management Guide.
- **NAT Profile:** Select the NAT profile from the drop down list or click the  to create a NAT profile. Refer to *Creating Profile-based NAT* from the RUCKUS Traffic Management Guide.
- **NAT Pool:** Select the NAT pool from the drop down list or click the  to create a NAT pool. Refer to *Creating Profile-based NAT* from the RUCKUS Traffic Management Guide.

**Note:** By default, the **Redundant Data Plane** is switched off. Switch it on to enable the **Redundant Data Plane**.

**Note:** You can also edit and delete a data plane by selecting the options **Configure** and **Delete** respectively, from the **Data Plane** tab.

4. Click **Next**.

5. Complete the following fields under the **Wireless** dialog box:

By default, the **Wireless** option is disabled. Switch on to enable the **Wireless** option.

**Figure 4.** Selecting SSID (wireless) for Network Segmentation

**Edit Network Segmentation**

General → **Wireless** (checked) → AP Wired (checked) → Switch (unchecked) → Review

• Name  
• Data Plane

• SSID  
• WLANs

• Ethernet Profile  
• AP Groups

• Switch Groups  
• Distribution Switches  
• Access Switches

ON Enable

1 Select one SSID to be used for the network segmentation.

search table

WLAN Name	SSID	Zone Name	Domain Name
MDU	MDU@NIPUN	Nipun-MDU	Nipun

1 records 1

\* Selected SSID: MDU@NIPUN

2 Select WLANs from different zones to be part of the network segmentation.

Select WLANs (Domain-Zone-WLAN-SSID)

Select WLANs (Domain-Zone-WLAN-SSID)

Nipun-Nipun-MDU-MDU-MDU@NIPUN

Back Next Cancel

- **SSID:** Select the **SSID** for Network Segmentation from the drop down list.

The selected **SSID** will be displayed in the **Selected SSID** field.

- **WLAN:** Select WLANs (wireless) for **Network Segmentation**.

6. Click **Next**.

7. Complete the following fields under the **AP Wired** dialog box:

By default, the **AP Wired** option is disabled. Switch on to enable the **AP Wired** option.

**Figure 5.** AP Wired Ethernet Profile

**Edit Network Segmentation**

General → Wireless → **AP Wired** → Switch → Review

☒ Enable

AP groups presented here are from the zones which use the DP(s) selected in step 1.

Select Ethernet Profile: MDU-Profile1

Select AP Groups (Domain-Zone-AP Group)

Type a keyword to find a group

Nipun  
Nipun-MDU

Selected AP Groups (Domain-Zone-AP Group)

Nipun-Nipun-MDU-RealAP  
Nipun-Nipun-MDU-default

Back Next Cancel

- Select the Ethernet profile: Select the ethernet profile from the drop down list or click the icon to create an ethernet profile.

The selected SSID will be displayed in the **Selected SSID** field.

- Select the AP group: Select the AP group from the table.

8. Click **Next**.

9. Complete the following fields under the **Switch** dialog box:

By default, the **Switch** option is disabled. Switch on to enable the **Switch** option.

**Figure 6.** Selecting Switch Groups

### Edit Network Segmentation

General

Wireless ☒

AP Wired ☒

Switch ☒

Review

• Name

• Data Plane

• SSID

• WLANs

• Ethernet Profile

• AP Groups

• Switch Groups

• Distribution Switches

• Access Switches

ON ☐ Enable

1 Select Switch Groups

Available Switch Groups

Type a keyword to find a group

- D System

+ D Christopher

+ D Commscope

+ D Jeff

+ D Nipun

+ D Sushma

→

Selected Switch Groups

NetworkSegP2

Back

Next

Cancel

- Select the Switch Groups: From the table, select the switch group which is to be added to the Network Segmentation group.

**Note:** To select the participated Switch Group for the segment profile, administrator can utilize the search function to filter out the groups.

- Select Distribution Switches: Select the distribution switch from the drop down list which is to be added to the Network Segmentation group.

**Figure 7.** Select Distribution Switches

### Edit Network Segmentation

General

Wireless ☒

AP Wired ☒

Switch ☒

Review

• Name

• Data Plane

• SSID

• WLANs

• Ethernet Profile

• AP Groups

• Switch Groups

• Distribution Switches

• Access Switches

2 Setup Distribution Switches

NET41XX-CORE-DIS [8C:7A:15:3C:DC:FA]

[?] Select Distribution Switches

No data available

Configure

search table

Distribution Switches	Dispatch Status	Data Plane	Access Switches	VLAN List	Loopbar	Loopback Interface IP	Keep alive
NET41XX-CORE-DIS [8C:7A:15:3C:DC:FA]	[SUCCESS]	vDP-7-113-Two	NET41XX-M...	300-399	41	10.10.41.1/255.255.255.0	5

Back

Next

Cancel

- **Note:** VXLAN is supported only on higher end switches such as ICX 7850, 7650 and 7550 model with router image, so distribution switch should use the above mentioned ICX models.

To configure the distribution switches, select the switch from the table and click **Configure** Icon to display the **Edit Distribution Switch** dialog box.

**Figure 8.** Configure Distribution Switch

Complete the following fields:

- **Data Plane:** Select the data plane.
- **VLAN List:** Enter the VLAN List.
- **Loopback Interface ID:** Enter the Loopback Interface ID.
- **Loopback Interface IP:** Enter the Loopback Interface IP.
- **Loopback Interface Subnet Mask:** Enter the Loopback Interface Subnet Mask.
- **Keep alive:** Enter the keep alive time interval to enable data plane monitor status. This option is enabled, if the **Data Plane Redundancy** is switched on.

Keep alive value is restricted between the range of 1 - 20 seconds to check Data plane status by ICMP Ping.

- **Retry times:** Enter the retry time interval to enable data plane monitor status. This option is enabled, if the **Data Plane Redundancy** is switched on.

Retry times is restricted between the range of 1 - 5 to check Data plane status retry times if no response.

- **Available Access Switches:** The available access switches are displayed in the table.
  - **Selected Access Switches:** Select the access switch from the interface.
- Figure 9.** Selected Access Switches

**Edit Distribution Switch: NET41XX-CORE-DIS**

\* Data Plane: vDP-7-113-Two

\* [?] VLAN List:

\* Loopback Interface ID:

\* Loopback Interface IP:

\* Loopback Interface Subnet Mask:

\* [?] Keep alive: 5

\* [?] Retry times: 3

[?] Data Plane Redundancy: OFF

+ Create Delete Up Down

Priority	Redundant Data Plane

[?] Available Access Switches

NET41XX-MDU1 [D4:C1:9E:10:A1:00]
NET41XX-MDU-2 [C0:C5:20:B0:C4:F5]

[?] Selected Access Switches

OK Cancel

- **Data Plane Redundancy:** Administrator can disable/enable site redundancy.

**Note:** The maximum size of redundancy server is seven.

- Distribution Switch and Data Plane communicate client VNI information via VxLAN Tunnel as follows:
  - a. Switch Client connect to Access Switch.
  - b. Access Switch connect to the Distribution Switch.
  - c. Distribution Switch establish VxLAN tunnel to the Data Plane.

Switch Client management:

- a. Distribution Switch use loopback interface connect to Data Plane interface.

**Figure 10.** Loopback Interface Connect to Data Plane Interface

**Edit Distribution Switch: ICX7850-48C Router**

\* Data Plane: 2392-6110140-1

\* [?] VLAN List: 3001,3002

\* Loopback Interface ID: 1

\* Loopback Interface IP: 111.111.111.113

\* Loopback Interface Subnet Mask: 255.255.255.0

\* [?] Keep alive: 10

\* [?] Retry times: 3

[?] ON Data Plane Redundancy

+ Create Delete Up Down

Priority	Redundant Data Plane
1	2392-6110140-a

[?] Available Access Switches

[?] Selected Access Switches

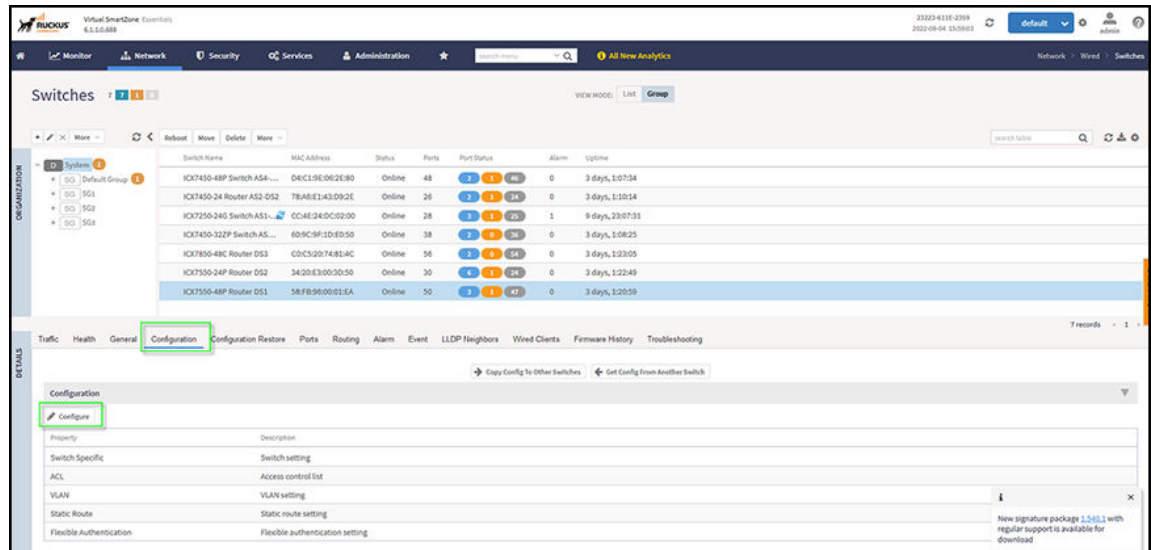
ICX7450-48P Switch [D4:C1:9E:06:2E:80]

- b. Network Routing will be carried out between Distribution Switch loopback interface and Data Plane data interface.
- c. Switch Client belonging to Access Switch should authenticate VLAN network.
- d. Browser will re-direct to Web Authentication page.
- e. After the Switch Client pass web authentication, the Distribution Switch forward the client traffic to Data Plane.

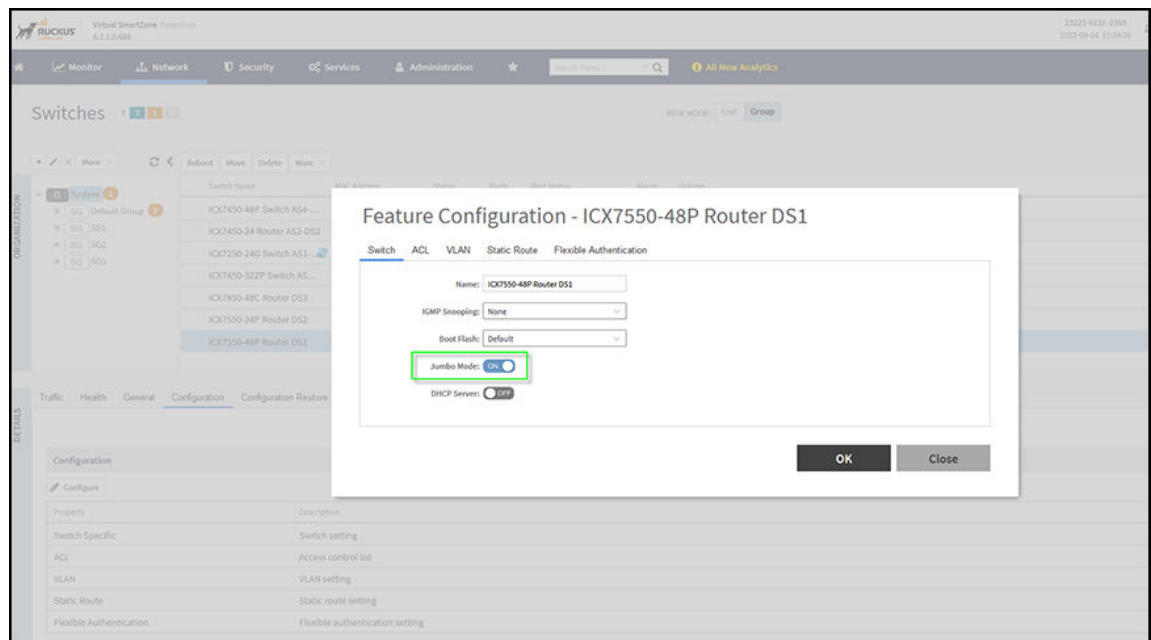
For the Network Segmentation function of Switch part, all devices between Distribution Switch and Data Plane must enable the Jumbo mode. This includes the Distribution Switch itself and vSZ-D Data interface which belongs to the vSwitch on ESXi. Otherwise, switch client will not be able to access the internet connection.

To enable the Jumbo mode, do the following:

- On the menu, click **Network > Wired > Switches** to display the **Switches** window.
- Figure 11.** Switches



- Click **Configuration > Configure** to display **Feature Configuration** dialog box.
  - Switch ON to enable the Jumbo mode.
- Figure 12. Feature Configuration**



- Click **OK**.
- f. The data plane detects the VxLAN.
- g. Data Plane provide the DHCP/NAT service according to Switch Client VNI information.
- Setup Access Switches: Select the access switch and apply the setting.
- Figure 13. Setup Access Switches**

**Setup Access Switches**

Uplink Port:  VLAN ID:

**Web Auth Page Settings**

Header:

Title:  Password Label:  Button Text:

Footer:

search table

Access Switches	Model	Dispatch Status	Distribution Switches	Uplink Port	VLAN ID	Web Auth Page Settings	Port Rate Limiting
ICX7150-48 Switch [90:3A...	ICX7150-48	[SUCCESS]	ICX7550-24ZP Router [34...	1/1/1	10	Header: N/A Title: N/A Password Label: N/A Button Text: N/A Footer: N/A	

Complete the following fields:

- You can choose multiple switches as access switches, administrator can unify the **Web Auth Page** settings by clicking the **Apply to all**. The access switch will share the same configurations instead of configuring each switch manually.

10. Click **Next**.

11. Verify the data in the **Review Page**.

**Figure 14.** Review Page

### Edit Network Segmentation

General

- Name
- Data Plane

Wireless

- SSID
- WLANs

AP Wired

- Ethernet Profile
- AP Groups

Switch

- Switch Groups
- Distribution Switches
- Access Switches

Review

Name: Shared-Profile

Type: Wireless + AP Wired

Data Plane: Data Plane

VNI Range	DHCP Profile	DHCP Pool	NAT Profile	NAT Pool
Normal : vDP-7-113-Two	MDU-Pool1	MDU-DHCP-Pool1	NET3500-NAT-Pr...	NET3500-...

Ethernet Profile: MDU-Profile1

AP Groups:

Name	Zone Name	Domain Name
RealAP	Nipun-MDU	Nipun
default	Nipun-MDU	Nipun

2 records

Wlans:

Name	SSID	Zone Name	Domain Name
MDU	MDU@NIPUN	Nipun-MDU	Nipun

1 records

Switch Groups: NetworkSegP2

Distribution Switches:

Distribution Switches	Dispatch Status	Data Plane	Access Switches	VLAN List	Loopbar	Loopback Interface IP
NET41XX-CORE-DIS [8C:7...	N/A	vDP-7-113-Two	NET41XX-M...	2	1	102.168.60.5/255.255.255.0

Access Switches:

Access Switches	Model	Dispatch Status	Distribution Switches	Uplink Port	VLAN ID	ID Label	Passwor
NET41XX-MDU-2 [C0:C5:2...	ICX7150-C08P	N/A	NET41XX-CORE-DIS [8C:7...	1/1/1	10	N/A	N/A

Back
OK
Cancel

12. Click **OK**.

From the table, select the network segmentation profile to view the profile settings details.

**Figure 15.** Network Segmentation Profile Settings


Name	66-2								
Type	Wireless + Switch								
Status	Completed								
Operation Result	N/A								
Data Plane									
Data Plane ▲	VNI Range	DHCP Profile	DHCP Pool	NAT Profile	NAT Pool				
Normal : 2392-6110140-1 Redundant : 2392-6110140-a	16777210-16777215	DHCP1 DHCP1	DHCP1-VNI-102 DHCP1-VNI-102	NAT1 NATa	NAT1-VNI-102 NATa-VNI-202				
Normal : 2392-6110140-2	N/A								
Normal : 2392-6110140-b	N/A								
WLANs									
Name	SSID	Zone Name	Domain Name						
QA-Bin.Hua_MDU_H2	QA-Bin.Hua_MDU_H2	381_Z4	Administration Domain						
QA-Bin.Hua_MDU_H2	QA-Bin.Hua_MDU_H2	Z4	Administration Domain						
Distribution Switches									
Distribution Switches	Dispatch Status	Data Plane	Access Switches	VLAN List	Loopba	Loopback Interface IP	Keep alive	Retry times	Data Plane Redundancy
ICX7850-48C Router [C0:...	[SUCCESS]	2392-6110140-1	ICX7450-48P Switch [D4:C1:9E:06:2E:80]	3001,3002	1	111.111.111.113/255.255.255.0	10	3	2392-6110140-a
Access Switches									
Access Switches	Model	Dispatch Status	Distribution Switches	Uplink Port	VLAN ID	ID Label	Password Label	Port Rate Limiting	
ICX7450-48P Switch [D4:...	ICX7450-48P	[SUCCESS]	ICX7850-48C Router [C0:C5:20:74:81:4C]	1/1/1	121	N/A	N/A		


Functions of switches are as follows:

- Access Switch provide Web Authentication Service and handles VLAN service.
- Distribution Switch handles VNI/VLAN mapping and forward the traffic to Data Plane.

The data plane handles VNI and DHCP/NAT services.

When Switch Client access the internet by browser, most packets come back from gateway to the Data Plane. The Data Plane must add VxLAN header and then forward to the Distribution Switch.

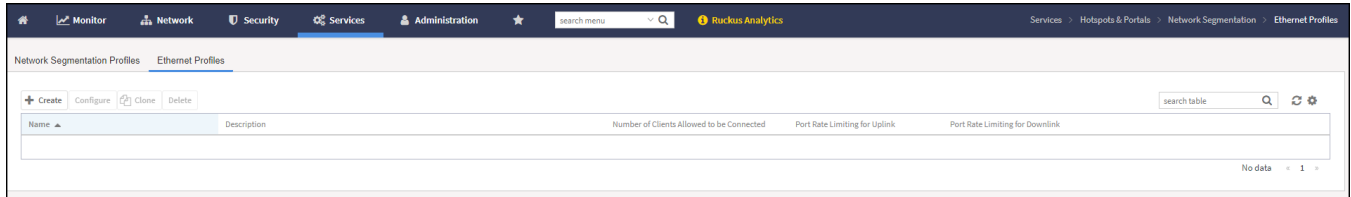
 **Note:** The maximum packet length between Distribution Switch and Data Plane is 1564 (1514 general +50 VxLAN header)


 **Note:** You can also edit and delete Network Segmentation Profiles by selecting the options **Configure** and **Delete** respectively, from the **Network Segmentation Profiles** window.

Parent topic: [Working with Hotspots and Portals](#)

## Ethernet Profiles

1. On the menu, click **Services > Hotspots & Portals > Network Segmentation > Ethernet Profiles** to display the **Ethernet Profiles** window.

**Figure 1. Ethernet Profiles**

2. Select the ethernet profile from the table or create a ethernet profile, click the  icon to display the **Create Network Segmentation Ethernet Port** dialog box.

**Figure 2. Create Network Segmentation Ethernet Port**

The screenshot shows the 'Create Network Segmentation Ethernet Port' dialog box. It has two main sections: 'General Options' and 'Ethernet Port Usage'.  
 In the 'General Options' section, there are fields for 'Name', 'Description', and a 'Type' dropdown menu set to 'Access Port'.  
 In the 'Ethernet Port Usage' section, there are radio buttons for 'Access Networks' (Default WAN, Local Subnet(LAN), Tunnel Ethernet Port traffic) and a 'User Side Port' section with a toggle switch set to 'ON' and a text input field for 'Number of clients allowed to be connected' with the value '8'.  
 Below the 'User Side Port' section, there is a 'Port Rate Limiting' section with 'Uplink' and 'Downlink' toggle switches, both set to 'OFF', and input fields for 'mbps (1~1000)'. A red warning message states: 'Only User port Rate Limit is supported for the wired clients. Firewall Profile Rate Limit and Device policy Rate Limit features are not supported for the wired clients.'  
 At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Complete the following fields:

- General Options
  - Name: Enter the ethernet port name.
  - Description: Enter a short description of the ethernet port.
  - Type: Select from the drop down list.
- Ethernet Port Usage

- Access Network: Select from **Default WAN**, **Local Subnet (LAN)**, or **Tunnel Ethernet Port Traffic**.
- User Side Port: By default, this option is switched ON. Switch OFF to disable this option.
- Number of clients allow to be connected: Enter the number of clients allowed to be connected.
- Port Rate Limiting: Only User port Rate Limit is supported for the wired clients. Firewall Profile Rate Limit and Device policy Rate Limit features are not supported for the wired clients.

Uplink: By default, this option is switched OFF. Switch ON to enable uplink limit. You can enter the limit between 1-1000 mbps.

Downlink: By default, this option is switched OFF. Switch ON to enable downlink limit. You can enter the limit between 1-1000 mbps.

4. Click **OK**.

- 🔗 **Note:** You can also edit, clone, or delete a Ethernet Profiles by selecting the options **Configure**, **Clone**, and **Delete**, respectively, from the **Ethernet Profiles** window.

**Parent topic:** [Working with Hotspots and Portals](#)



**Corporate Headquarters**

**CommScope • Hickory • North Carolina • 28602 • USA**

T: 1-828-324-2200

[www.commscope.com](http://www.commscope.com)