CONFIGURATION GUIDE

RUCKUS SmartZone and Cloudpath Network Segmentation Configuration Guide

Supporting SmartZone 6.1.0 and Cloudpath 5.9 R3 (5.9.5179)

Part Number: 800-73064-001 Rev A
Publication Date: December 2021

Copyright, Trademark and Proprietary Rights Information

© 2021 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, SUPPLIERS, 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

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface **5**
Contacting RUCKUS Customer Services and Support 5
What Support Do I Need? 5
Open a Case 5
Self-Service Resources 6
Document Feedback 6
RUCKUS Product Documentation Resources 6
Online Training Resources 6
Document Conventions 7
Notes, Cautions, and Safety Warnings 7
Command Syntax Conventions 7

About This Guide **9**
New In This Document 9

Prerequisites **11**

Main Configuration Steps **13**

Configuring the Integrated System in the Cloudpath UI **15**

Configuring the vSZ Controller to Prepare for Network Segmentation **17**
Configuring the DHCP/NAT License Assignment 17
Creating Profile-based DHCP 17
Configuring Global Settings 17
Configuring DHCP Pool Settings 18
Creating Profile-based NAT 19
Configuring NAT Global Settings 19
Configuring NAT Pool Setting 20
Creating an AP Group 20
Creating WLAN for Network Segmentation 22

Creating Network Segmentation Profile on the vSZ Controller **25**

Configuring a Network Segmentation Group in the Cloudpath UI **29**
Viewing the Network Segmentation Landing Page 29
Creating an eDPSK Pool for a Property 32
Creating a Property for a Network Segmentation Group 33
Adding Units to a Property of a Network Segmentation Group 36
Viewing Information of a Configured Unit 42
Using the Access Points Tab 45
Property Management Information 45
Creating a Policy to Assign to eDPSK Pools (Optional) 46
Troubleshooting 49

Preface

- Contacting RUCKUS Customer Services and Support 5
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- Document Conventions 7
- Command Syntax Conventions 7

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.commscope.com/ruckus 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://forums.ruckuswireless.com/
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—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.

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.

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.commscope.com/ruckus .

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`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* 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
bold text	Identifies command names, keywords, and command options.
italic text	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..... 9

New In This Document

TABLE 2 New/updated/deprecated sections (*December 2021*)

Feature	Description	Reference
Initial Release	Initial release.	Rev A

Prerequisites

This topic specifies the resources and systems required for configuring Network Segmentation.

System resources required:

- Minimum one Virtual SmartZone (vSZ) controller.
- Minimum one SmartZone Data Plane (vSZ-D) controller.
- Two or more Access Points (APs) which are compatible with the 6.1 controller.

Required systems:

- Cloudpath server installed.
- vSZ controller installed and the cluster is operational.
- Admin account required for Cloudpath and vSZ systems.
- vSZ-D installed and managed by vSZ.
- Operational APs installed and managed by vSZ
- Cloudpath should be able to communicate with SmartZone management interface.
- Ensure that the Cloudpath server certificate is in the controller trust store. Otherwise, the Network Segmentation feature will not work since the controller will not be able to communicate with Cloudpath.
- It is necessary that the customer has trial licenses set up for DHCP and NAT servers.

Main Configuration Steps

These are the major steps to follow - in order - to configure Network Segmentation. There are some steps that must be performed in the Cloudpath UI and some steps that must be performed on the vSZ controller. Do complete all steps by following the instructions in the following sections:

1. Configuring the Integrated System in the Cloudpath UI on page 15
2. Configuring the vSZ Controller to Prepare for Network Segmentation on page 17
3. Creating Network Segmentation Profile on the vSZ Controller on page 25
4. Configuring a Network Segmentation Group in the Cloudpath UI on page 29

Configuring the Integrated System in the Cloudpath UI

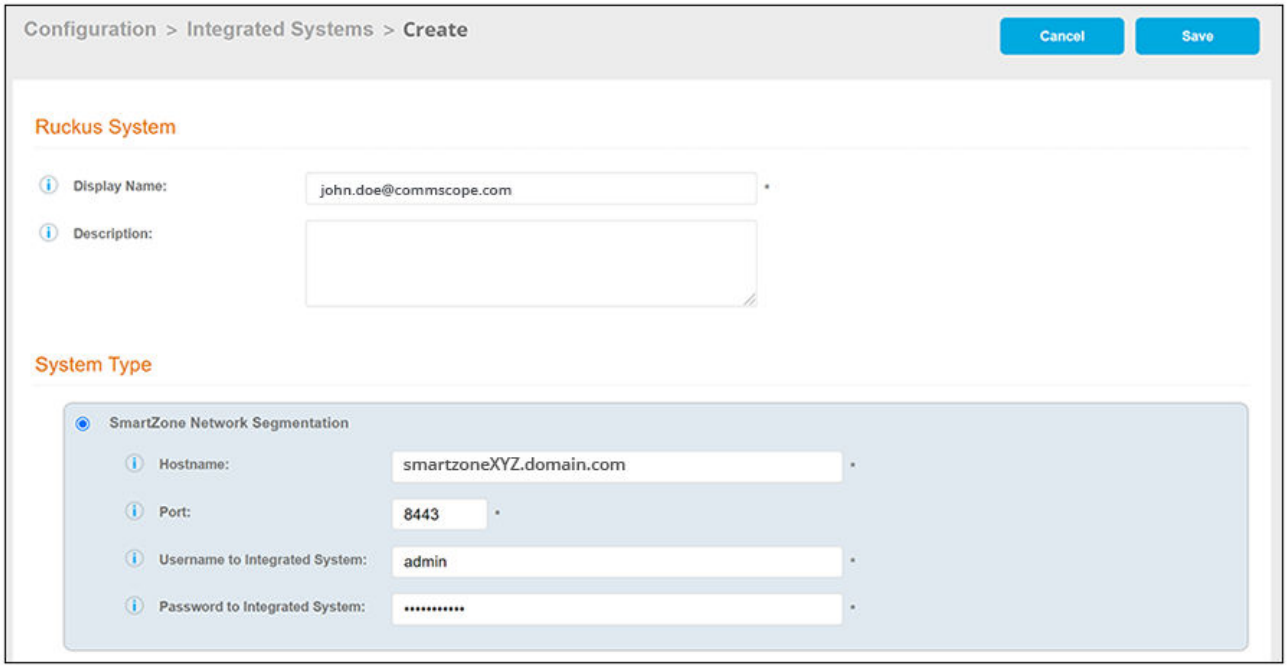
For configuring Network Segmentation, you must begin by adding your SmartZone system as an integrated system in the Cloudpath UI.

NOTE
You can configure only one integrated system. The integrated system must be a SmartZone cluster management interface.

Follow the steps below to configure SmartZone as an integrated system:

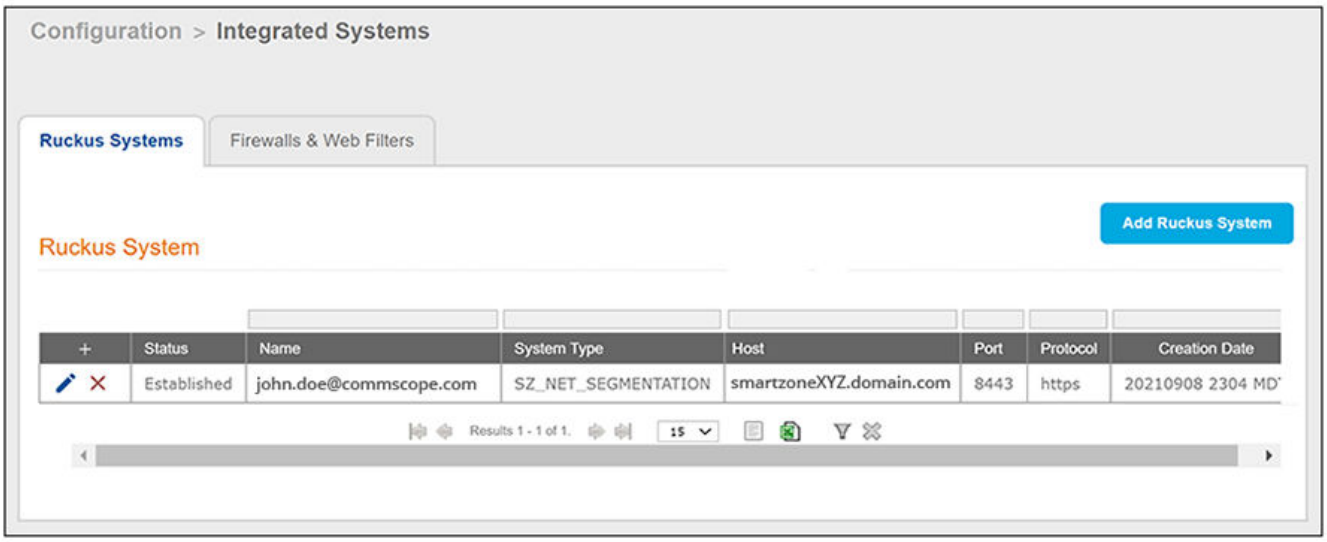
1. In the Cloudpath UI, navigate to **Configuration > Integrated Systems**, and click **Add Ruckus System**.
2. In the ensuing screen, do the following:
   a. For Display Name, enter a meaningful name for the integrated system (visible only to you, as an administrator).
   b. In the System Type section, click the **SmartZone Network Segmentation** button to expand the screen, and complete the configuration.

   FIGURE 1 Configuring the Integrated System



   - Hostname: Host name (FQDN) or IP address of the integrated system.
   - Port: Port number for connecting the integrated system.
   - Username to Integrated System: Username to access the integrated system services.
   - Password to Integrated System: Password to access the integrated system services.
3. Click **Save**. You are taken to a list view that shows the newly configured integrated system:

FIGURE 2 Newly Configured Integrated System



Configuring the vSZ Controller to Prepare for Network Segmentation

- Configuring the DHCP/NAT License Assignment....17
- Creating Profile-based DHCP....17
- Configuring Global Settings....17
- Configuring DHCP Pool Settings....18
- Creating Profile-based NAT....19
- Configuring NAT Global Settings....19
- Configuring NAT Pool Setting....20
- Creating an AP Group....20
- Creating WLAN for Network Segmentation....22

Configuring the DHCP/NAT License Assignment

License assignment specifies the capability of each Data Plane, which has the ability to assign IPs by DHCP feature and translate packets by NAT feature. Though these features already exist, starting 5.0, customers must purchase license to enable these features.

NOTE
This feature is supported only on virtual platform.

Creating Profile-based DHCP

DHCP profile can be applied to vSZ-D and the vSZ-D server can assign IP to the UE based on the profile rule. Different pools with the same subnet can be created without overlapping IP range.

NOTE
DHCP supports only access-side network.

- Configuring Global Settings on page 17
- Configuring DHCP Pool Settings on page 18

Configuring Global Settings

To configure Profile-based DHCP Global settings:

1. Go to **Services** > **DHCP & NAT** > **DHCP Profiles (DP)**.
2. Click **Create**, the Create DHCP Profile page appears.

3. Configure the following:
   - **Profile Name**: Type a name for the DHCP profile you want to create. AP supports 32 bytes.
   - **Description**: Type a description of the settings you want to create.
   - **Domain Name**: Type the domain name address.
   - **Primary DNS Server**: Type the primary domain name server address.
   - **Secondary DNS Server**: Type the secondary domain name server address.
   - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
   - **DHCP Option43 Space**: Click **Create**, the Create DHCP Option43 Space form appears. Configure the following:
     - **Space Name**: Type a name for Option43 space.
     - **Description**: Type a description for Option43 space.
     - Under **Option43 Sub Option**, click **Create** and configure the following:
       - **Sub Option Name**: Type a sub option name.
       - **Type**: Select the required option from the drop-down.
       - **Code**: Enter a code. Range: 1 through 254.
       - **ClickOK**, you have created Option43 Sub Option.
     - Click **OK**, you have created Option43 Space.
   - **Hosts**: Click **Create**, the Create Host Configuration form appears. Configure the following:
     - **General Options**
       - **Host**: Type a name for the host settings that you want to create.
       - **Description**: Type a description for the host settings that you want to create.
     - **Policy Options**
       - **Mac Address**: Type the MAC address of the DHCP host.
     - **Assigning Options**
       - **Broadcast Address**: Type the broadcast IP address.
       - **Fixed Address**: Type the fixed IP address of the host.
       - **Gateway**: Type the gateway IP address.
       - **DNS Server**: Type the IP address of the DNS server.
       - **Domain Name**: Type the domain name.
       - **Host Name**: Type the host name.
       - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
     - Click **OK**, you have created DHCP Host configuration.
4. Click **OK**.

   You have created DHCP Profile settings.

Configuring DHCP Pool Settings

To configure DHCP pool settings:

1. Go to **Services** > **DHCP & NAT** > **DHCP Profiles (DP)**.
2. Select the DHCP profile from the list for which you want to configure the pool settings.
3. Select the **Pools** tab page.

4. Click Create and configure the following:
   - **General Options**
     - **Pool Name**: Type a name for the pool configuration.
     - **Description**: Type a description for the pool configuration.
   - **Policy Options**
     - **Policy type**: Select VNI type for Network Segmentation.
   - **Assigning Options**
     - **Subnet**: Type the IP address.
     - **Subnet Mask**: Type the network address.
     - **Broadcast Address**: Type the broadcast IP address.
     - **Pool Range**: Type the address range for the pool.
     - **Exclude Pool**: Type the address range that must be excluded.
     - **Primary Gateway**: Type the primary gateway IP address.
     - **Secondary Gateway**: Type the secondary gateway IP address.
     - **Primary DNS Server**: Type the IP address of the primary DNS server.
     - **Secondary DNS Server**: Type the IP address of the secondary DNS server.
     - **Domain Name**: Type the domain name.
     - **Host Name**: Type the host name.
     - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
   - **Option43 Value**
     - Click **Create**, the Create Option43 value form appears. Configure the following:
       - Choose the **Space** Name or click **Create** to configure Option 43 Space Name.
       - Enter a **Description**.
     - Click **OK**, you have configured Option43 value.
5. Click **OK**.

   You have created DHCP pool configuration.

Creating Profile-based NAT

A NAT Profile could be applied to a vSZ-D. The NAT server settings work independently. You must configure the following settings to create a NAT profile:

NOTE
NAT does not support multiple public subnet/VLAN.

- Configuring NAT Global Settings on page 19
- Configuring NAT Pool Setting on page 20

Configuring NAT Global Settings

To create a NAT global setting:

1. Go to **Services** > **DHCP & NAT** > **NAT Profiles (DP)**.
2. Click **Create**, the Create NAT Profile page appears.

3. Configure the following:
   - **Profile Name**: Type a name for the NAT profile that you want to create. AP supports 32 bytes.
   - **Description**: Type a description for the profile that you want to create.
   - **Subnet**: Type the IP address.
   - **Policy type** : Select VNI type for Network Segmentation.
   - **Prefix**: Type a prefix value. Maximum range: 31.
   - **Gateway**: Type the gateway IP address.
4. Click **OK**.

   You have created a NAT Profile.

Configuring NAT Pool Setting

To configure NAT pool settings

1. Go to **Services** > **DHCP & NAT** > **NAT Profiles (DP)**.
2. Select the NAT profile from the list and click the **Pools** tab.
3. Click **Create**, the Create Pool Configuration page appears.
4. Configure the following:
   - **General Options**
     - **Pool Name**: Type a name for the NAT pool settings that you want to create.
     - **Description**: Type a description for the pool settings that you want to create.
   - **Policy Options**:
     - **Policy Type**: Select VNI type for Network Segmentation.
   - **Translation Options**
     - **Port Range**: Type the port range. Range: 10000 through 65534. For example: 10000-20000.
     - **Public Address Range**: Type the public address range.

       Note: This public address must not be duplicated with the other public address in the same subnet, which includes applied NAT Profile and vSZ-D's Access and Core Interface Address.
5. Click **OK**.

   You have created a NAT pool setting.

Creating an AP Group

Creating an AP group means creating a configuration profile that defines channels, radio settings, ethernet ports and network segmentation groups and other configurable for all members of the group or for all APs of a specific model in the group.

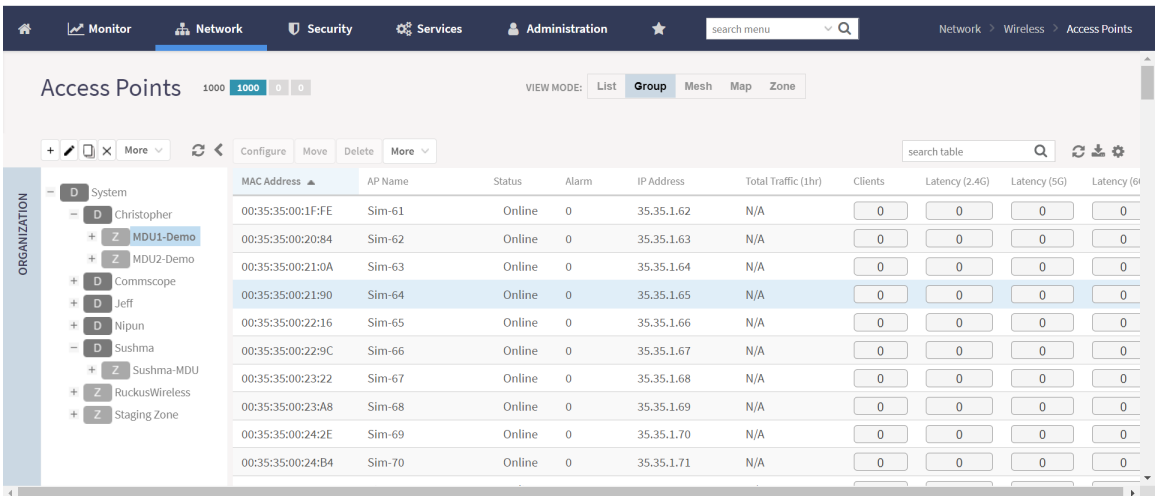
.

Follow these steps to create an AP group.

1. On the main menu, click **Network** > **Access Point**

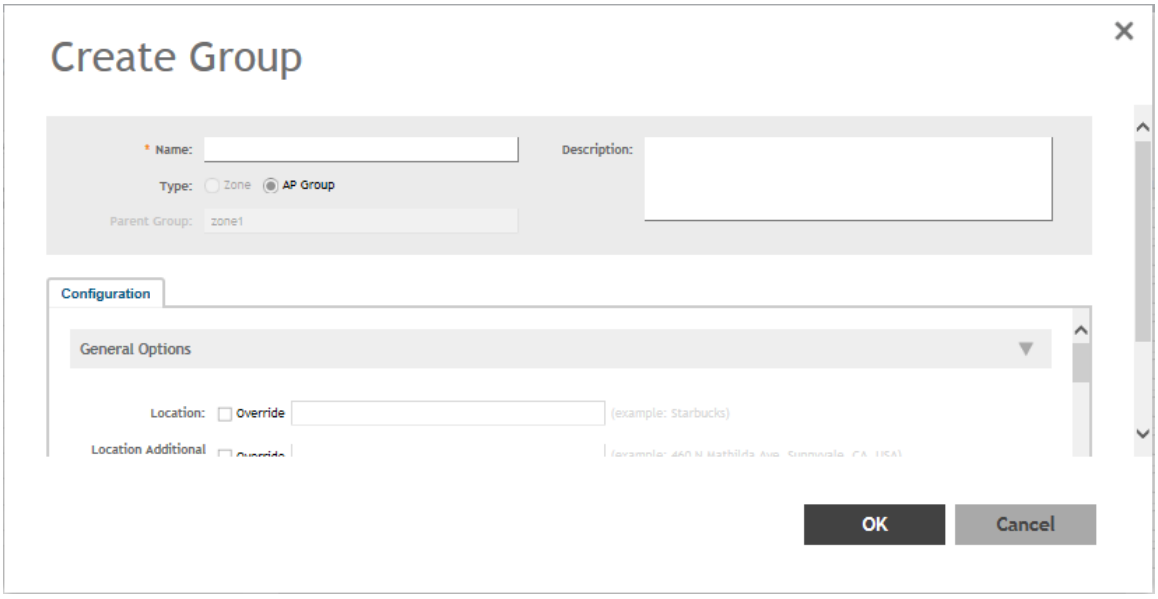
   The **Access Point** page is displayed.

FIGURE 3 Access Point



2. From the System tree hierarchy, select the location (for example: System, Domain, Zone) and click . The following figure appears.

FIGURE 4 Create Groups



3. Enter the details as explained in the following table.

   NOTE

   You can also edit the configuration of default AP group by selecting the default group and clicking the icon.

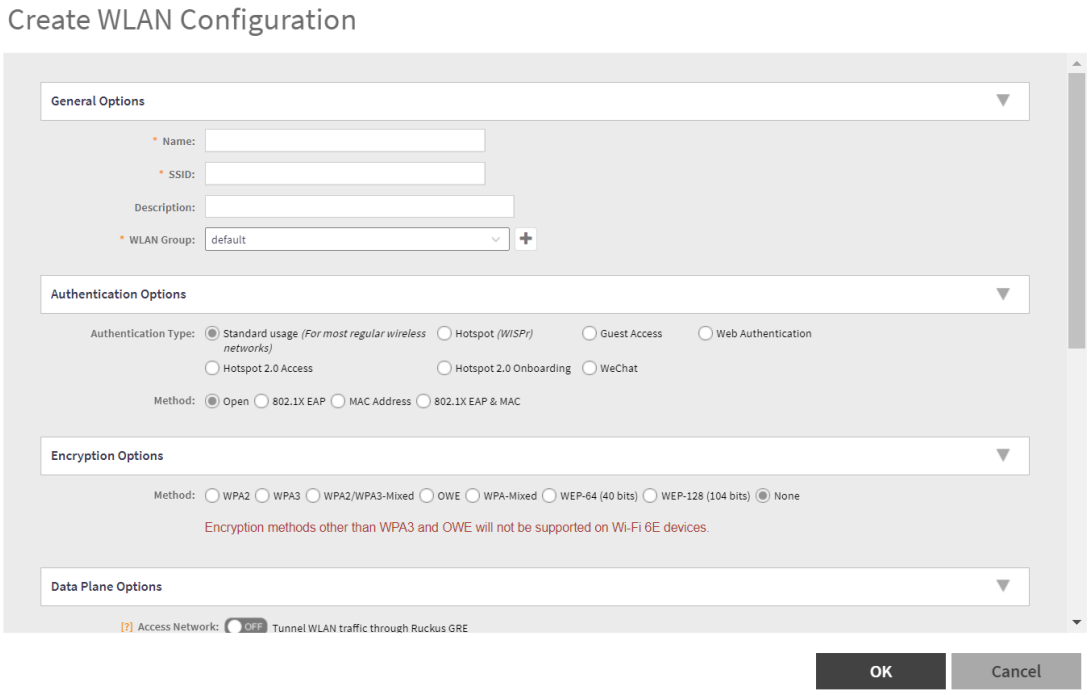
4. Click **OK**.
5. Select the AP's that will be used in the Network Segmentation and move them into the created AP Group(s).

NOTE

You can also edit, clone or delete an AP Group by selecting the options Configure , Clone or Delete respectively, from the Access Points page.

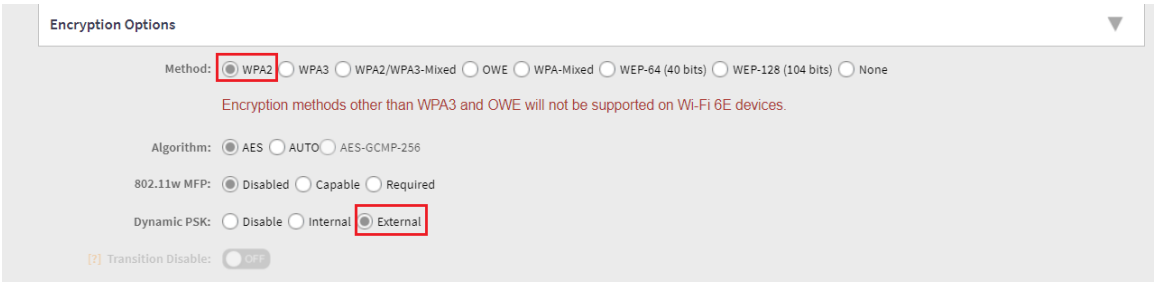
Creating WLAN for Network Segmentation

- Go to the **Network> Wireless Lans> System**.
- Click **Create .**

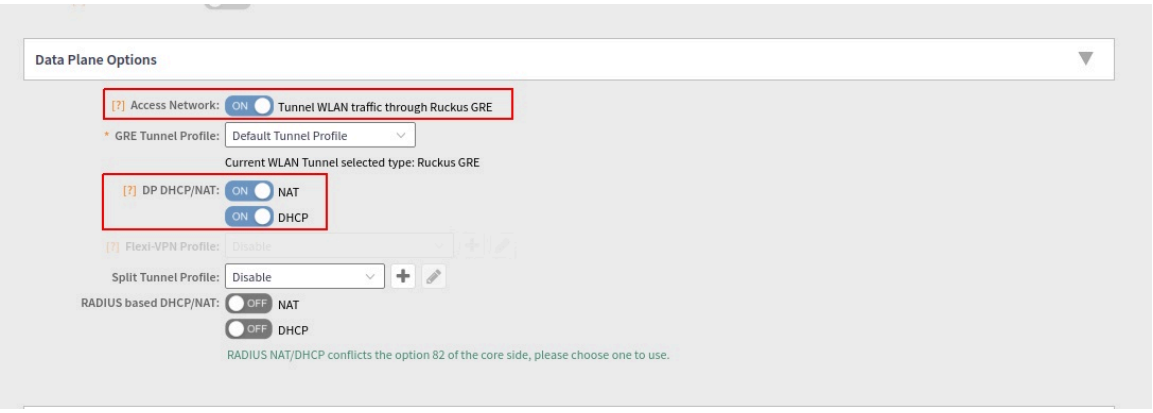


.

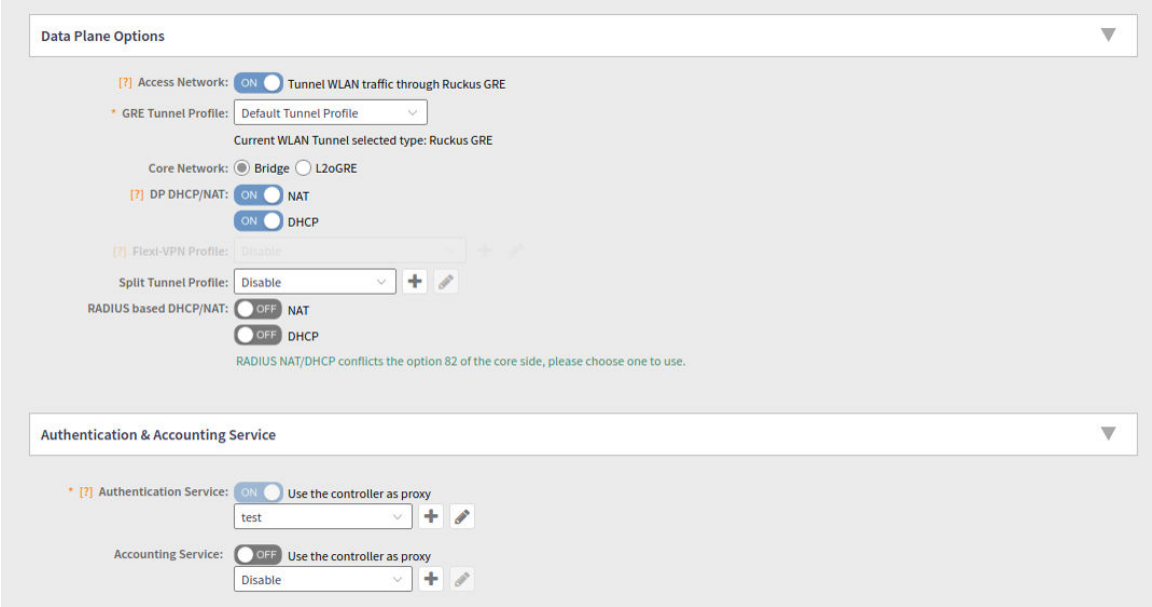
- Enter the "Name" and SSID in general options.
- Select WPA2 in encryption options.
  - Select "External" in Dynamic DPSK.



- In Data plane options, Enable "Access network".
- Enable NAT.
- Enable DHCP.
- Enter GRE tunnel profile with "Ruckus GRE" .



- Enable Authentication Service .



NOTE
WLAN will not be displayed, if any of the above conditions are not met.

For Authentication and Accounting from SmartZone.

NOTE
Refer to RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide, 6.0.0 (Part Number: 800-72580-001 Rev A) and navigate to **Services and Profiles** > **Working with Tunnels and Ports**.

Creating Network Segmentation Profile on the vSZ Controller

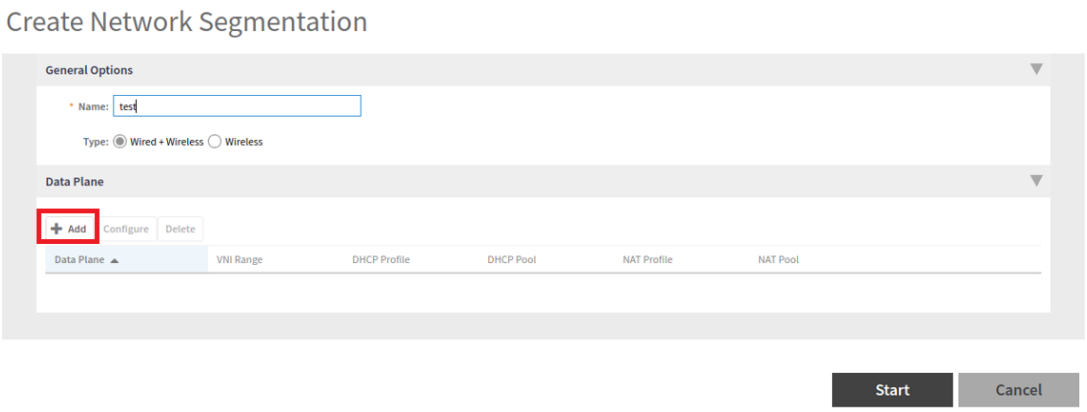
Network Segmentation was designed specifically to target Multi Dwelling Unit (MDU) deployments. Network Segmentation is currently using external Dynamic Pre shared Key (DPSK) to place a single tenant and their devices into their own individual VXLAN (iLAN).

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.

Steps for the creation of Segmentation:

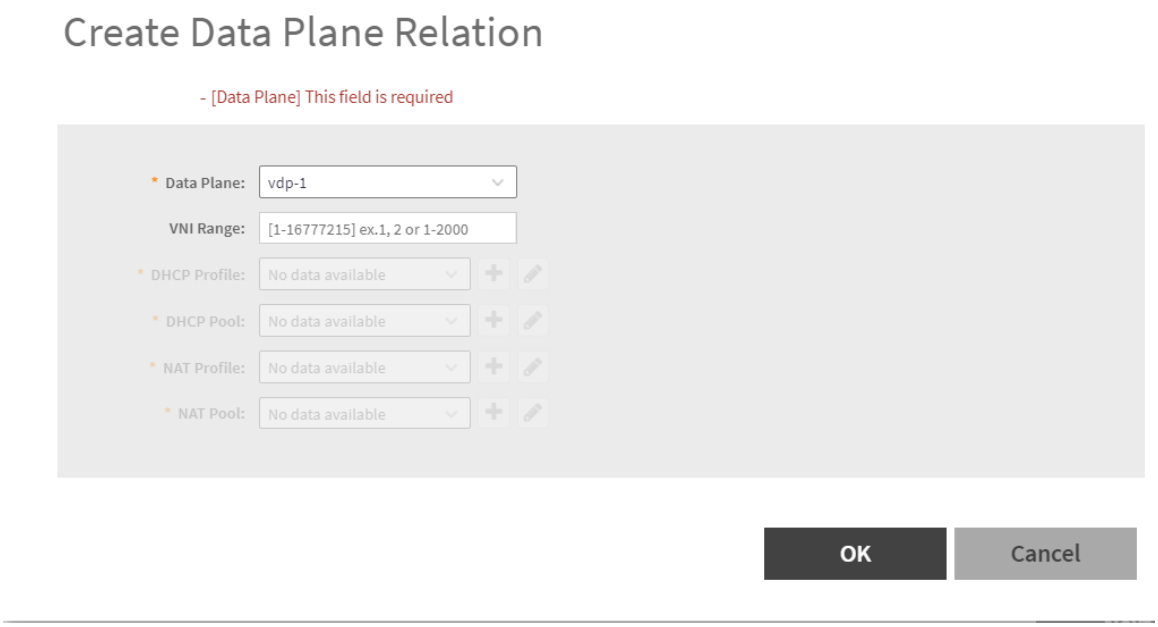
- Go to **Services> Hotspots & Portals > Network Segmentation> Network Segmentation Profiles**
- Click **Create**.

FIGURE 5 Edit Network Segmentation Groups in SmartZone User Interface



- Enter a Network Segmentation Profile name in the Name field.
- Click "Add".

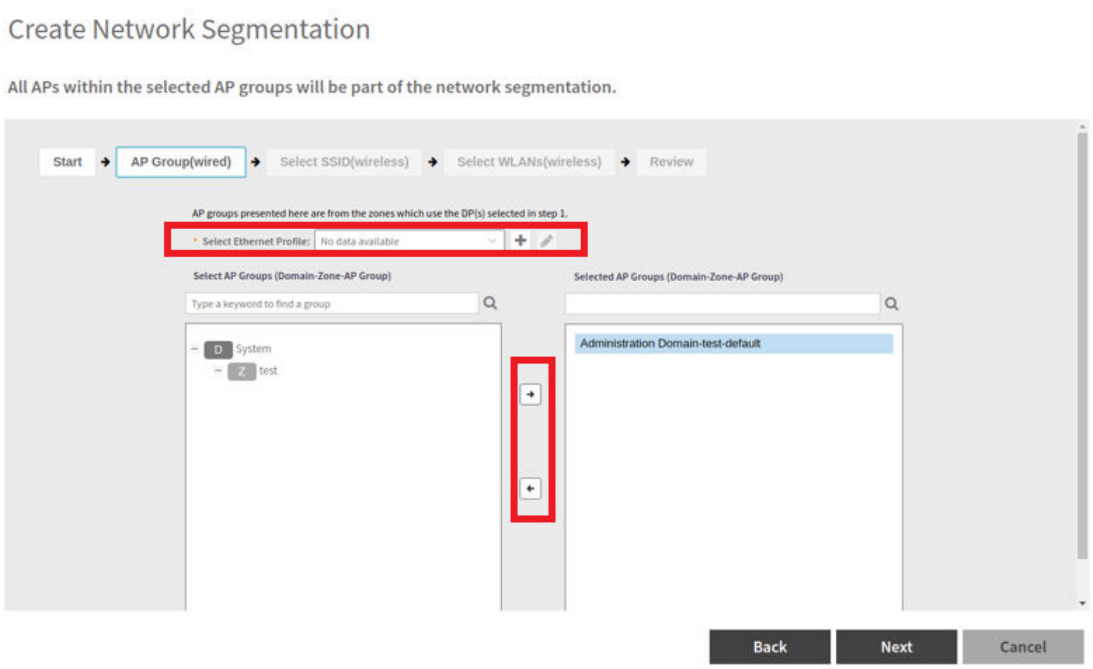
FIGURE 6 Create Data plane Relation



- Select the Data Plane details
- 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.
- Select/Create DHCP Profile and Pool.
- Select/Create NAT Profile and Pool.
- Click "OK".
- "Select AP Group(s) that will be used for Network Segmentation , refer to the figure below.

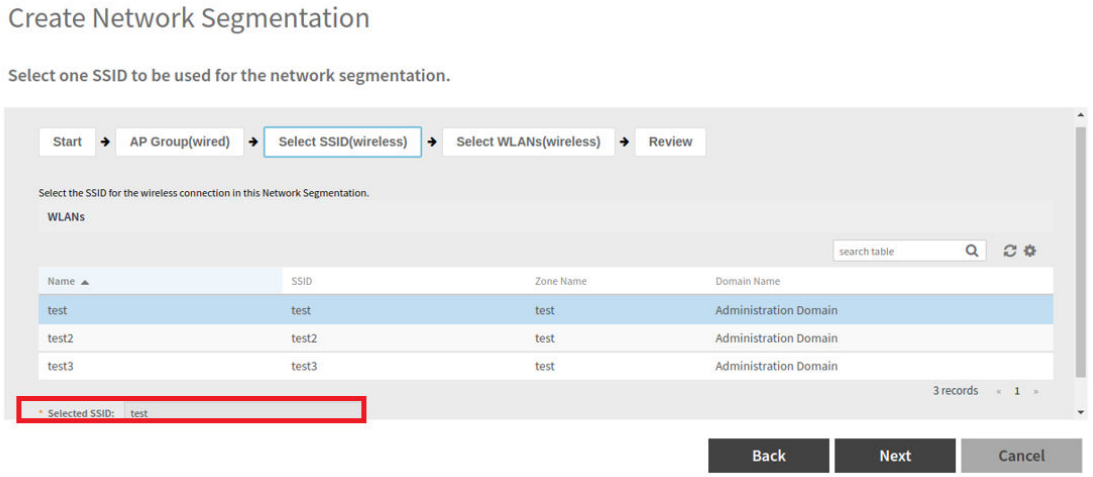
NOTE
This step is not applicable for Wireless group.

FIGURE 7 Add AP Group



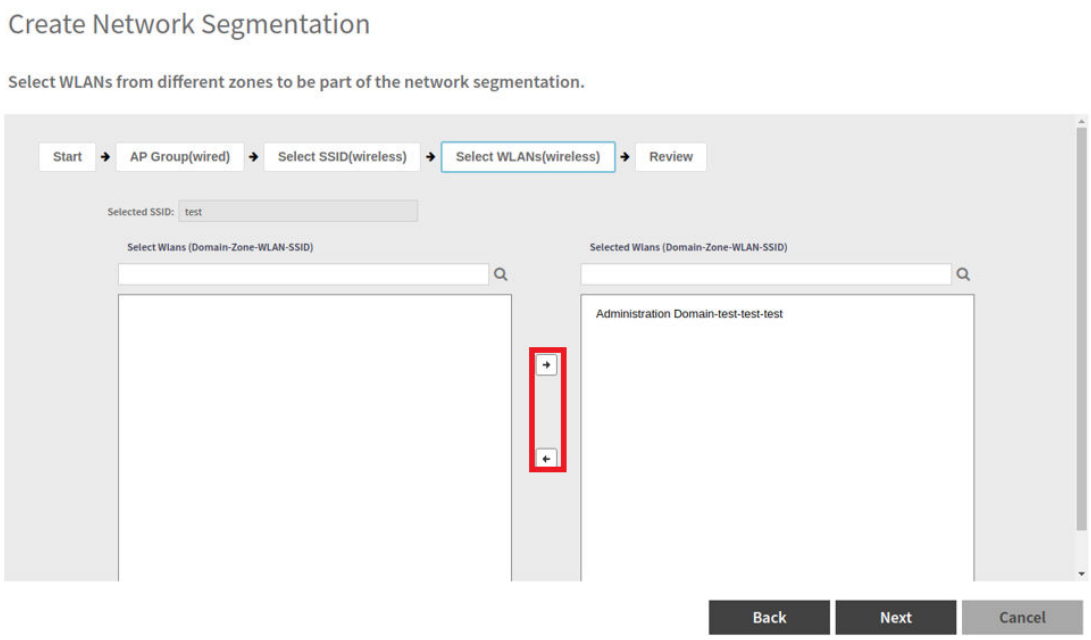
- Create/Select an ethernet profile with enabled Network Segmentation and select AP Model's port to apply.
- Click "Next".
- Select the SSID (wireless) for Network Segmentation.

FIGURE 8 Select SSID(wireless) for Network Segmentation

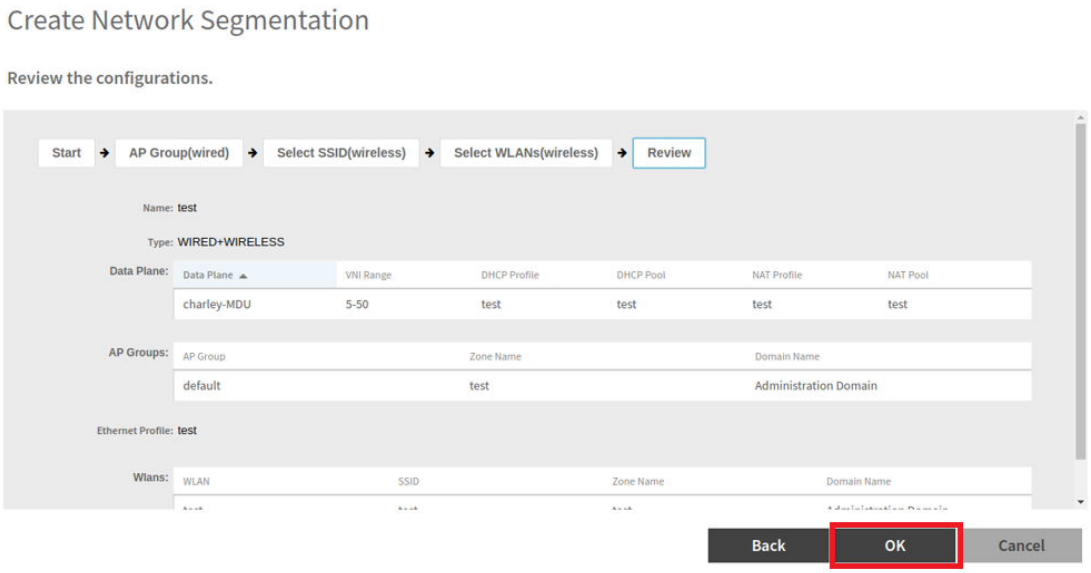


- Click "Next".
- Select WLANs (wireless) for Network Segmentation.

FIGURE 9 Select WLANs (wireless) for Network Segmentation



- Select "Next".
- Review the details entered.



- Click "OK".
- The Network Segmentation Profile is created.

Configuring a Network Segmentation Group in the Cloudpath UI

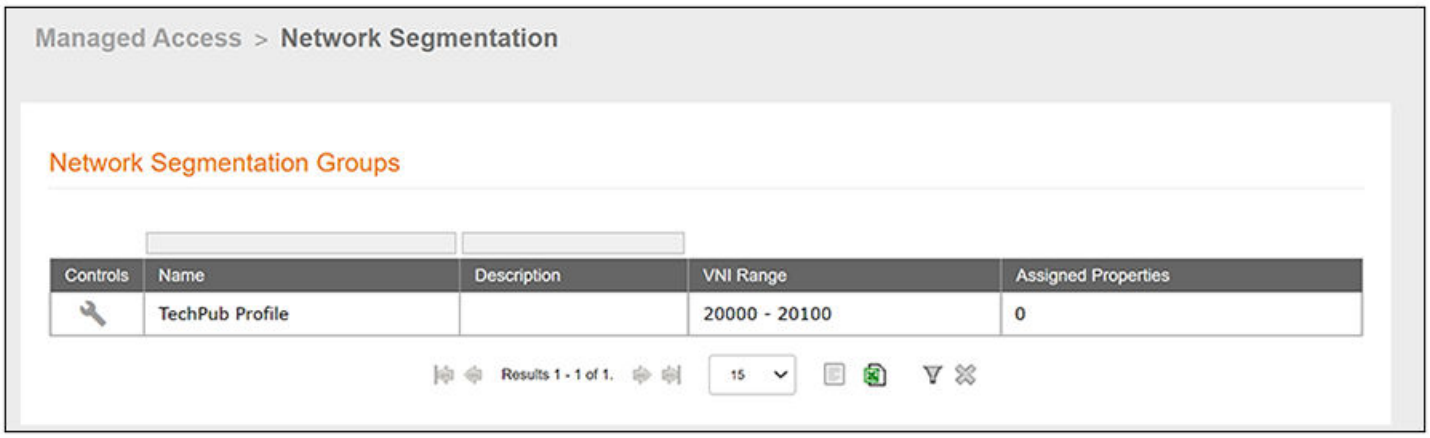
- Viewing the Network Segmentation Landing Page..... 29
- Creating an eDPSK Pool for a Property..... 32
- Creating a Property for a Network Segmentation Group..... 33
- Adding Units to a Property of a Network Segmentation Group..... 36
- Viewing Information of a Configured Unit..... 42
- Using the Access Points Tab..... 45
- Property Management Information..... 45
- Creating a Policy to Assign to eDPSK Pools (Optional)..... 46
- Troubleshooting..... 49

Viewing the Network Segmentation Landing Page

After you have configured the integrated system in the Cloudpath UI, and you have configured the Network Segmentation profile in SmartZone, a Network Segmentation group gets automatically created in Cloudpath.

To view the Network Segmentation group, go to **Managed Access > Network Segmentation**. The screen below shows the Network Segmentation group that is based on the Network Segmentation *profile* created in SmartZone. The VNI Range shown is the range that was configured in the Data Plane configuration in SmartZone for the Network Segmentation profile.

FIGURE 10 Network Segmentation Groups in Cloudpath UI



You can click on the wrench icon to invoke a three-tab view:

FIGURE 11 Details-Tab-View of the Network Segmentation Group

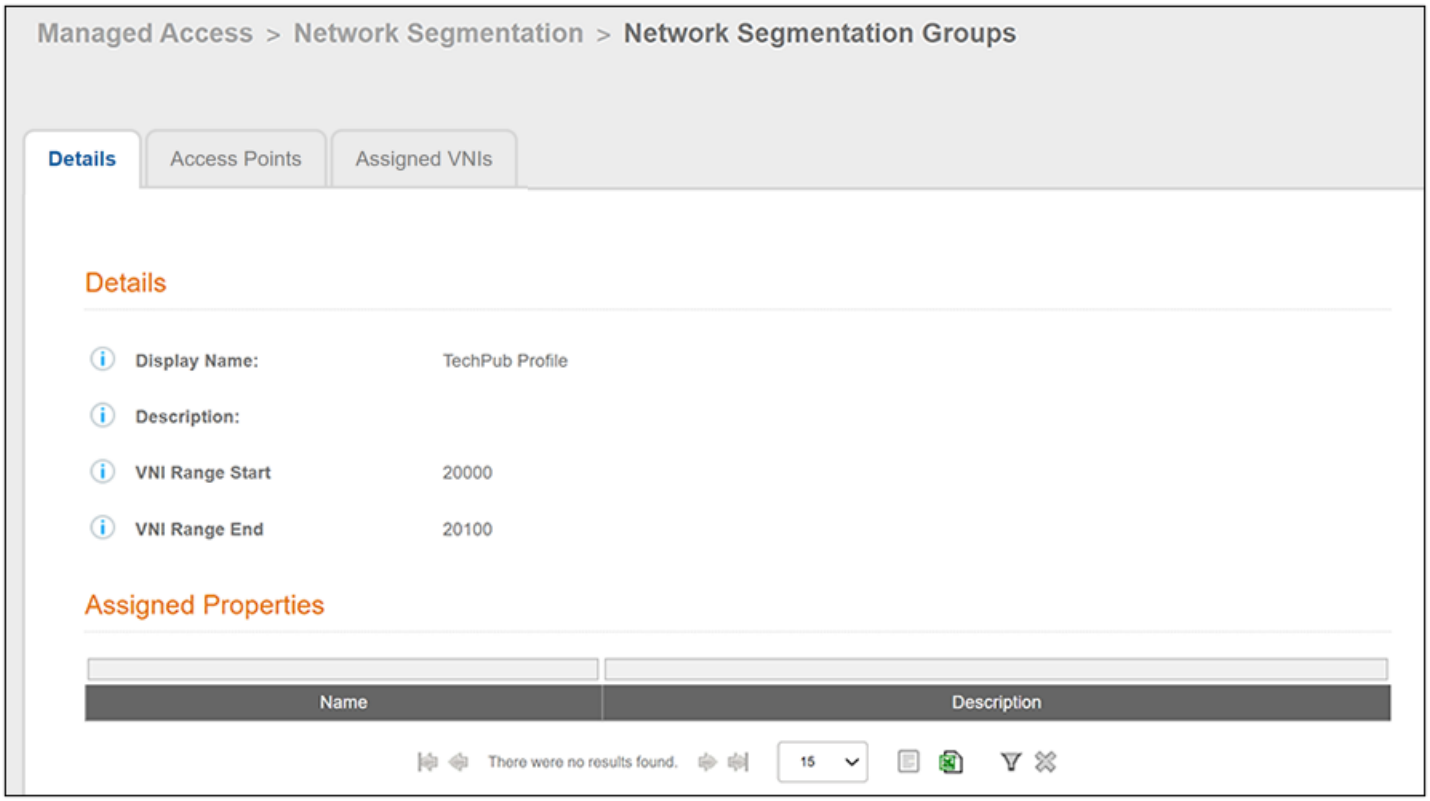
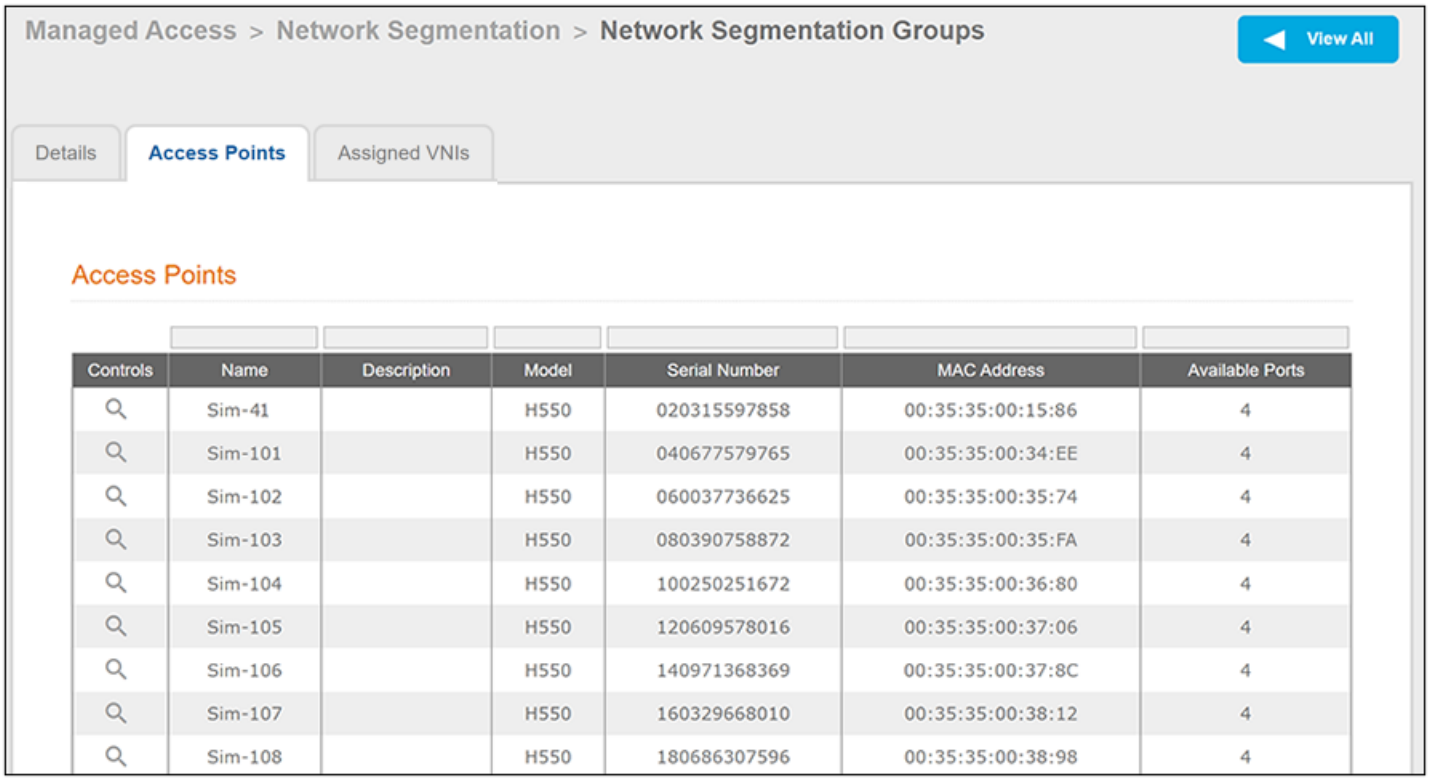


FIGURE 12 Access-Points-Tab View of the Network Segmentation Group

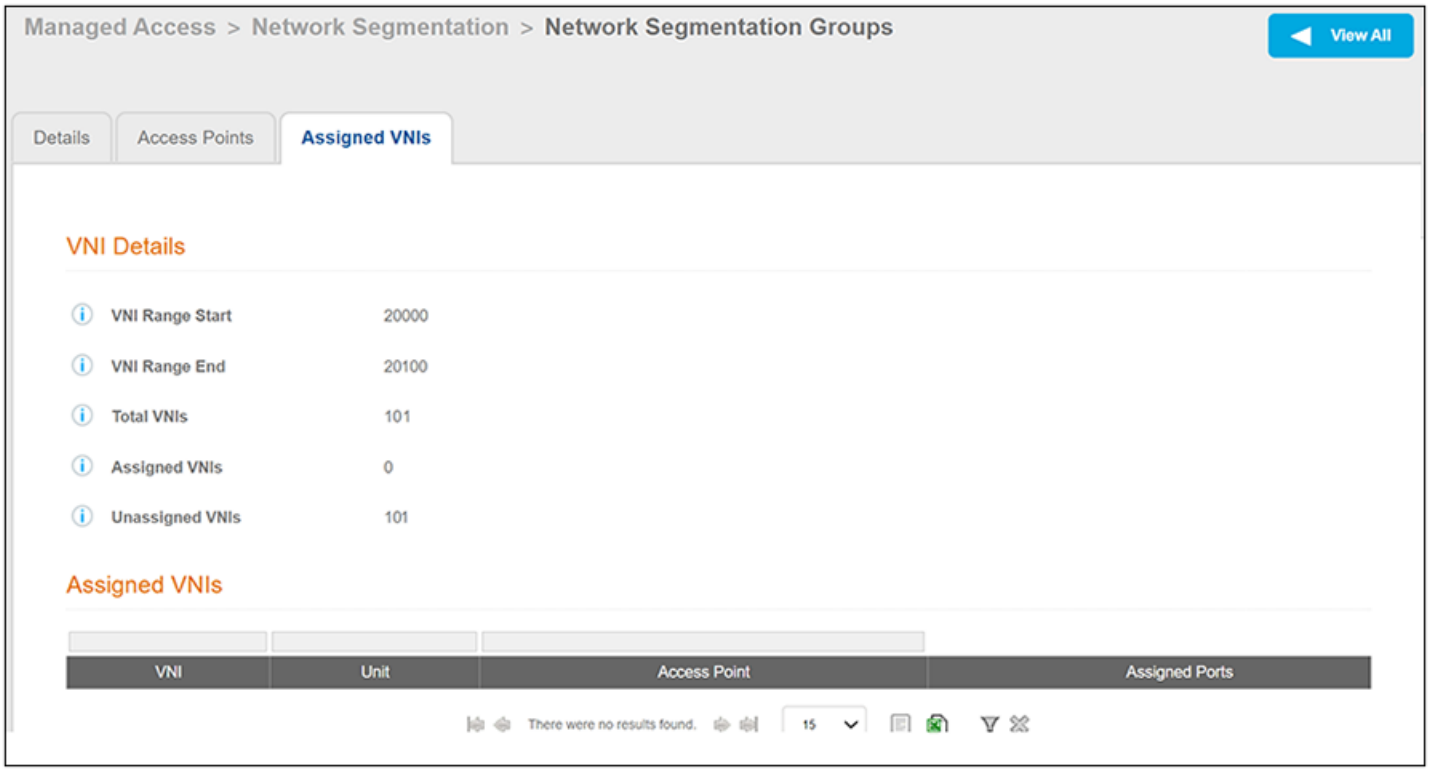


Controls	Name	Description	Model	Serial Number	MAC Address	Available Ports
	Sim-41		H550	020315597858	00:35:35:00:15:86	4
	Sim-101		H550	040677579765	00:35:35:00:34:EE	4
	Sim-102		H550	060037736625	00:35:35:00:35:74	4
	Sim-103		H550	080390758872	00:35:35:00:35:FA	4
	Sim-104		H550	100250251672	00:35:35:00:36:80	4
	Sim-105		H550	120609578016	00:35:35:00:37:06	4
	Sim-106		H550	140971368369	00:35:35:00:37:8C	4
	Sim-107		H550	160329668010	00:35:35:00:38:12	4
	Sim-108		H550	180686307596	00:35:35:00:38:98	4

NOTE

For more information, see Using the Access Points Tab on page 45.

FIGURE 13 Assigned-VNIs-Tab View of the Network Segmentation Group



NOTE
For an example of the Assigned VNIs tab after VNIs have been assigned, refer to Figure 25 on page 42.

Next Steps:

Before you can create (and then assign) properties to a Network Segmentation group, you need to create an eDPSK pool for each property. Once you create one or more properties, you assign units to the properties. You can assign multiple properties to a network segmentation group. Therefore, the remaining sequence to complete the Cloudpath portion of the Network Segmentation configuration is:

1. Creating an eDPSK Pool for a Property on page 32
2. Creating a Property for a Network Segmentation Group on page 33
3. Adding Units to a Property of a Network Segmentation Group on page 36
4. Creating a Policy to Assign to eDPSK Pools (Optional) on page 46

Creating an eDPSK Pool for a Property

Before you can create a property to add to your Network Segmentation group, you need to create an eDPSK pool. One (and only one) eDPSK pool must be assigned to a property.

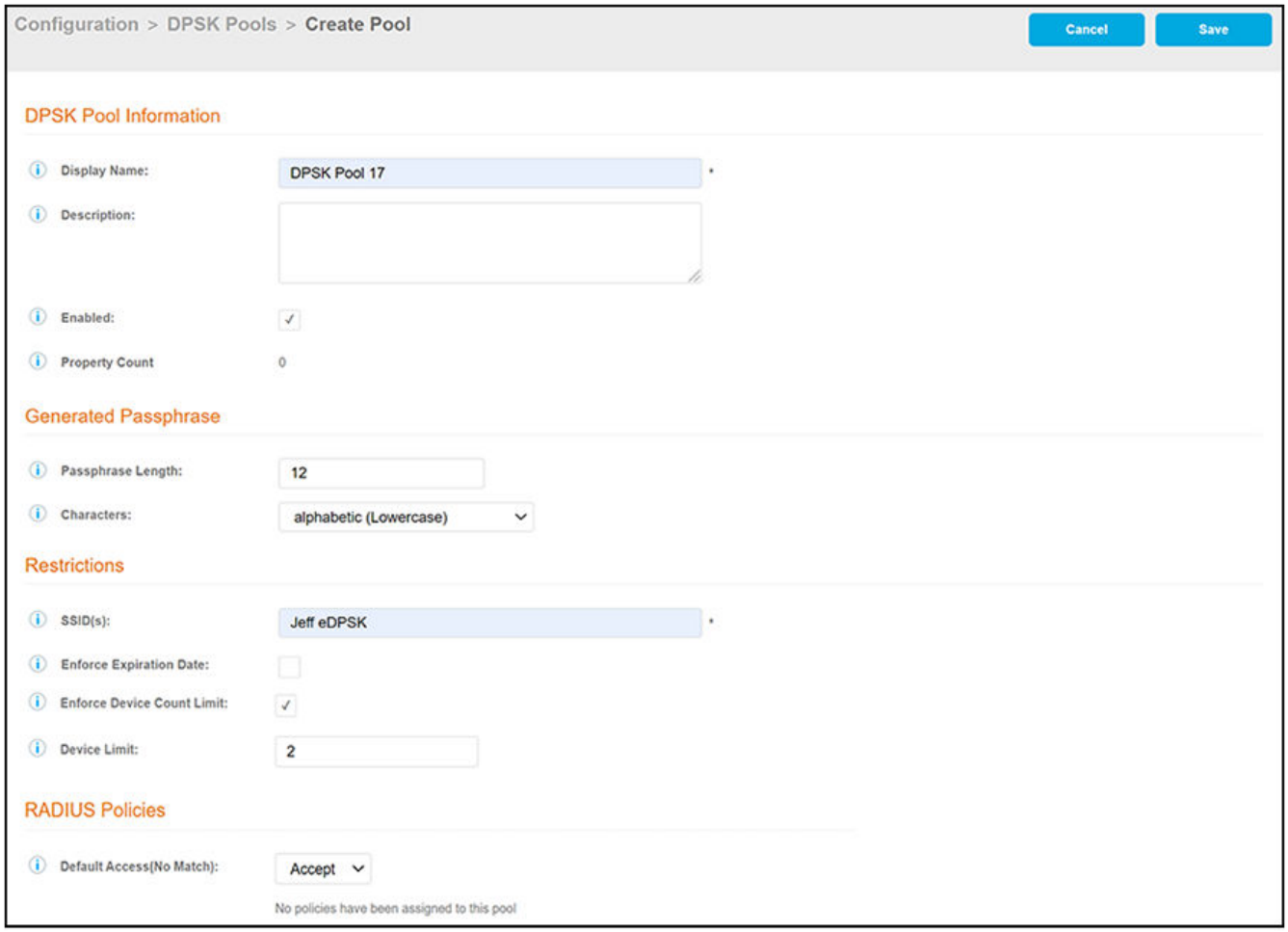
To create a new eDPSK pool, follow these steps:

1. In the Cloudpath UI, go to **Configuration > DPSK Pools**.
2. Click **Create DPSK Pool**.

3. In the ensuing Create Pool screen, enter the information to create the pool, then click **Save**. The following screen shows an example. For detailed steps, see the *Cloudpath Enrollment System External Dynamic Pre-Shared Key (eDPSK) Configuration Guide*.

   NOTE
   The SSID field value *must* match the SSID that you created in SmartZone. Also, if you assign more than one SSID to the pool, the tenant portal will not include a button that displays the QRCode for either the wi-fi passphrase or the guest wi-fi passphrase. (For more information about how the tenant portal is used, refer to the *Cloudpath Enrollment System Property Management Adminitration Guide*.)

FIGURE 14 Create eDPSK Pool Configuration Screen



Creating a Property for a Network Segmentation Group

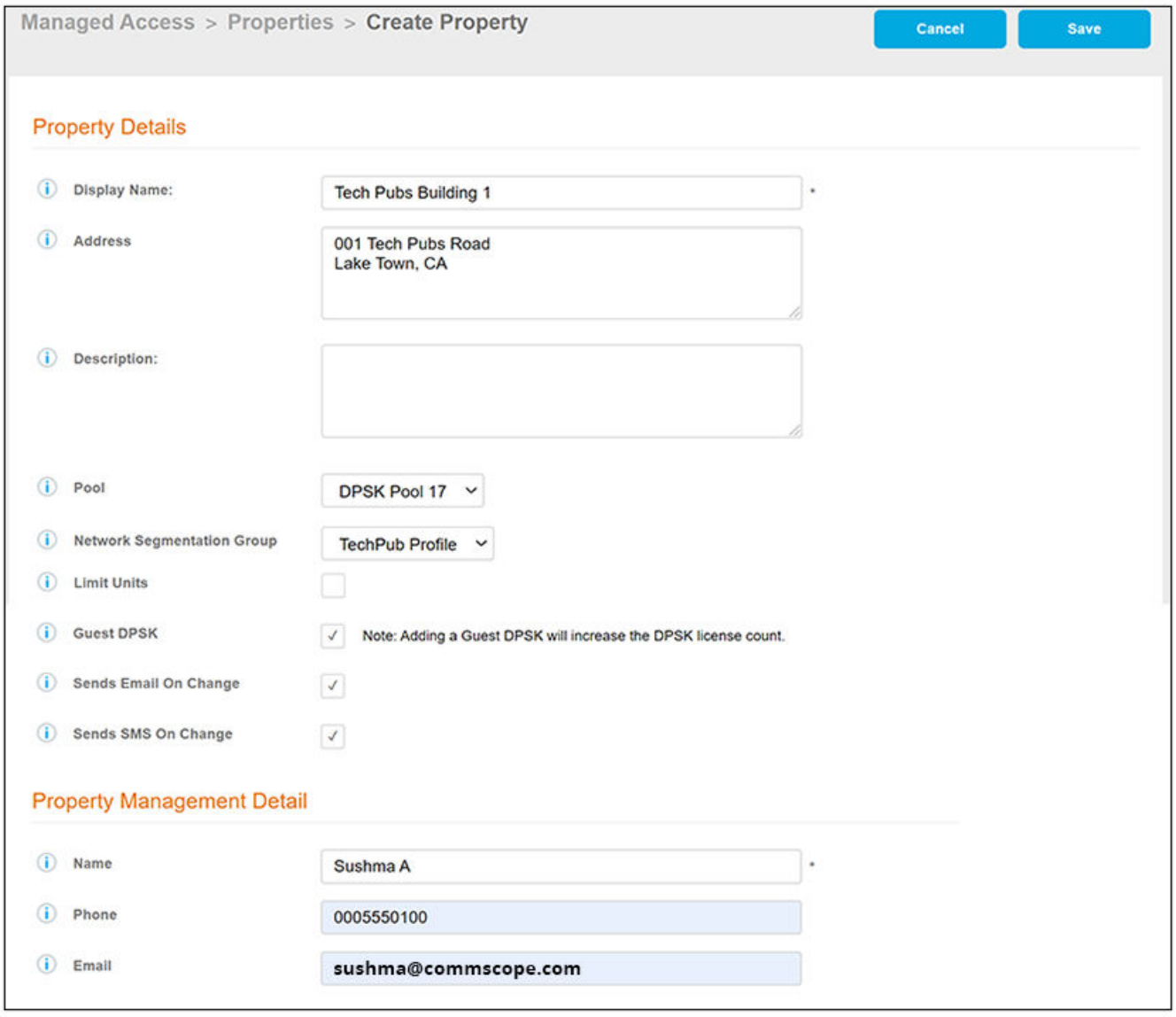
Once you have created an eDPSK pool, you can create a property that uses that pool, and you can assign the property to a Network Segmentation group.

Follow the steps below to configure a property and assign it to a Network Segmentation group:

NOTE
For more information about configuring properties, refer to the *Cloudpath Enrollment System Property Management Administration Guide*.

1. In the Cloudpath UI, go to **Managed Access > Properties**.
2. Click **Add Property**.
3. Configure the property, as shown and described in the following example.

FIGURE 15 Creating a Property to Assign to Network Segmentation Group



- Display Name: A meaningful name for the property (visible to you, as an administrator, and visible on the tenant portal).
- Address: Address of the property.
- Description (optional): Description of the property (visible only to you, as an administrator).

- Pool: The eDPSK pool assigned to this property (selected from the drop-down list).
- Network Segmentation Group: The name of the Network Segmentation group to assign to this property (selected from the drop-down list). All access points and VNI assignments on units (how to add units is described later) are derived from this Network Segmentation group. Once a unit has been assigned to the property, the group cannot be changed.
- Limit Units: You can check this box if you want to limit the number of units that can be assigned to this property. If you check the box, a "Max Units" pop-up field appears where you can enter the desired number.
- Guest DPSK: Checking this box assigns a guest DPSK to every unit that you add to the property. This field cannot be set on individual units, nor can this selection be changed once units have been assigned to the property.
- Sends Email On Change: Checking this box means that the contact person for a unit gets notified by email whenever the DPSK of the unit or the unit's guest DPSK (if guest DPSKs are being used) changes, or if the access token to the tenant portal is changed.

  NOTE
  If this box is checked, the contact person of the unit also gets notified by email as soon as you have added that unit to the property and saved the configuration.

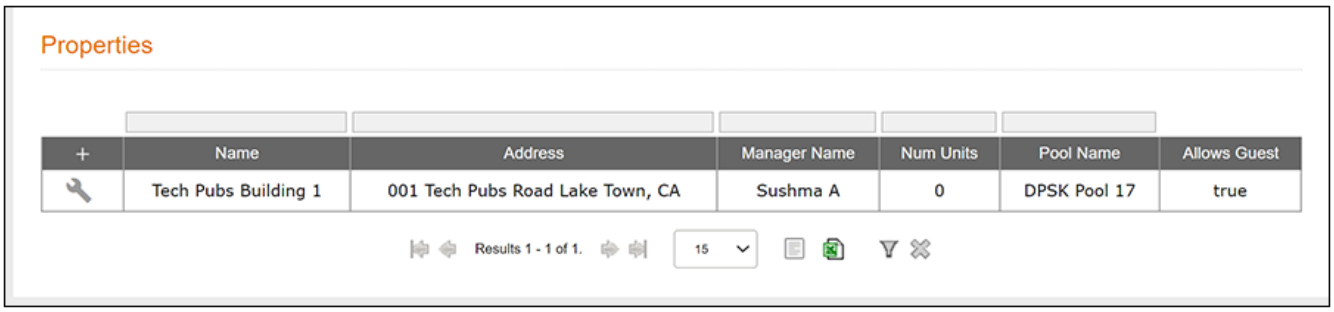
- Sends SMS On Change: Checking this box means that the contact person for a unit gets notified by text whenever the DPSK of the unit or the unit's guest DPSK (if guest DPSKs are being used) changes, or if the access token to the tenant portal is changed.

  NOTE
  If this box is checked, the contact person of the unit also gets notified by text as soon as you have added that unit to the property and saved the configuration.

- Management Info section: As the property manager, this should be your contact information that you want displayed in all communications with your tenants.

4. Click **Save**. You are returned to the main Properties screen where your newly configured property is now displayed, as shown in the example below:

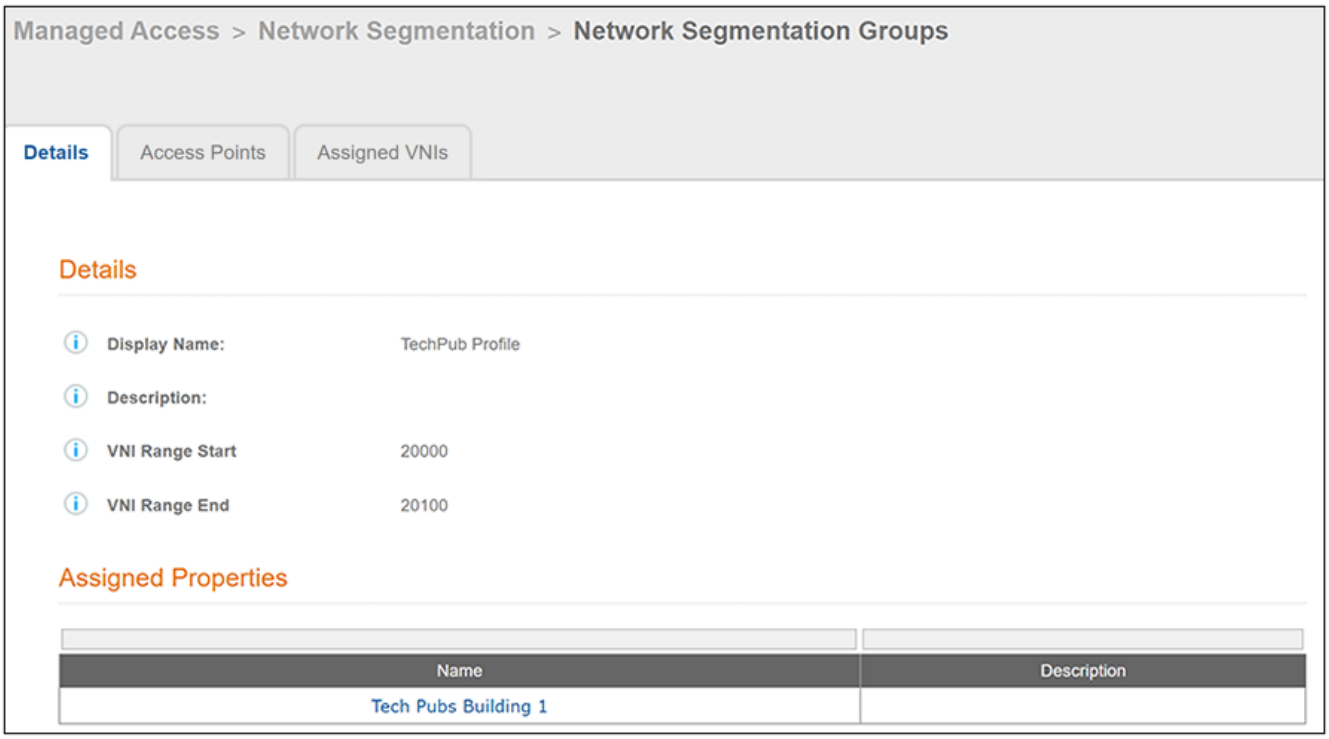
FIGURE 16 Main Properties Screen With Newly Configured Property



From the grid view of the property (see screen above), you can click the wrench icon to invoke four tabs that allow you to perform various action on the property.

NOTE
If you return to the **Managed Access > Network Segmentation** portion of the UI, then click the wrench icon of the Network Segmentation group, the ensuing screen displays live links to any properties you have assigned to the group, as shown in the following example:

FIGURE 17 Network Segmentation Groups Screen Showing Assigned Properties



For information about adding units to a property that is part of a Network Segmentation group, proceed to Adding Units to a Property of a Network Segmentation Group on page 36.

Adding Units to a Property of a Network Segmentation Group

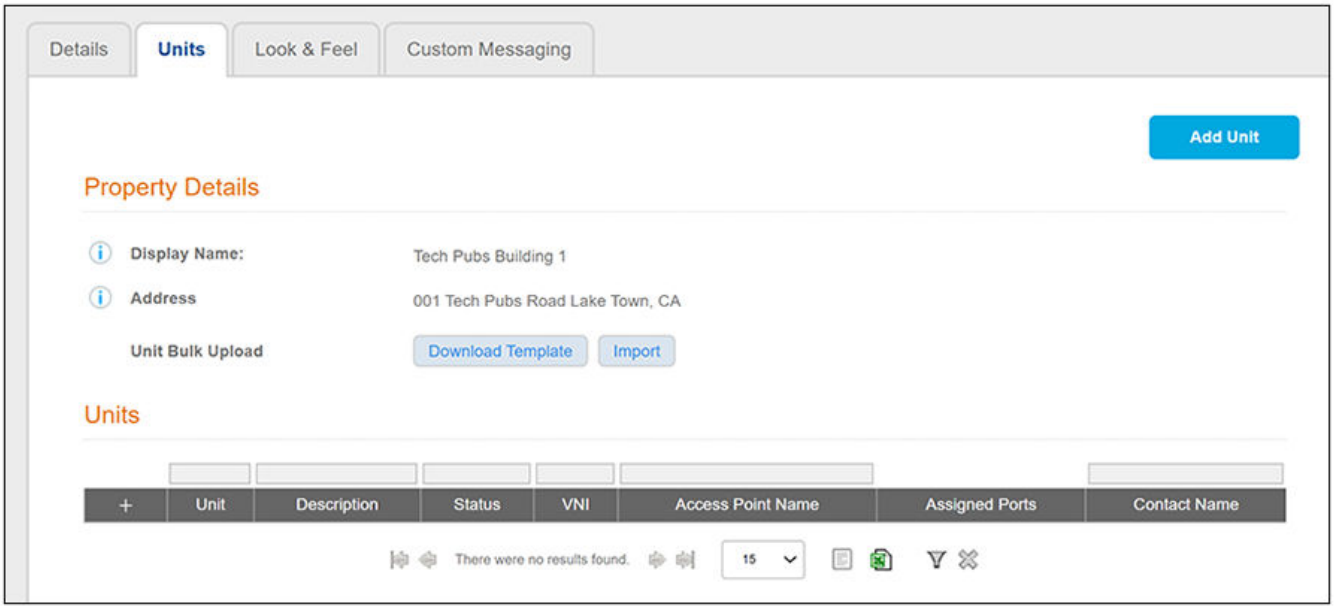
Once you have added a property to a Network Segmentation group, you can then add units to the property.

Follow the steps below to add units to the property:

NOTE
For information about how DPSKs get assigned, refer to the *Cloudpath Enrollment System Property Management Administration Guide*.

1. From the main Properties screen, click the wrench icon for the specific property.
2. On the ensuing screen, click the **Units** tab to invoke the following screen:

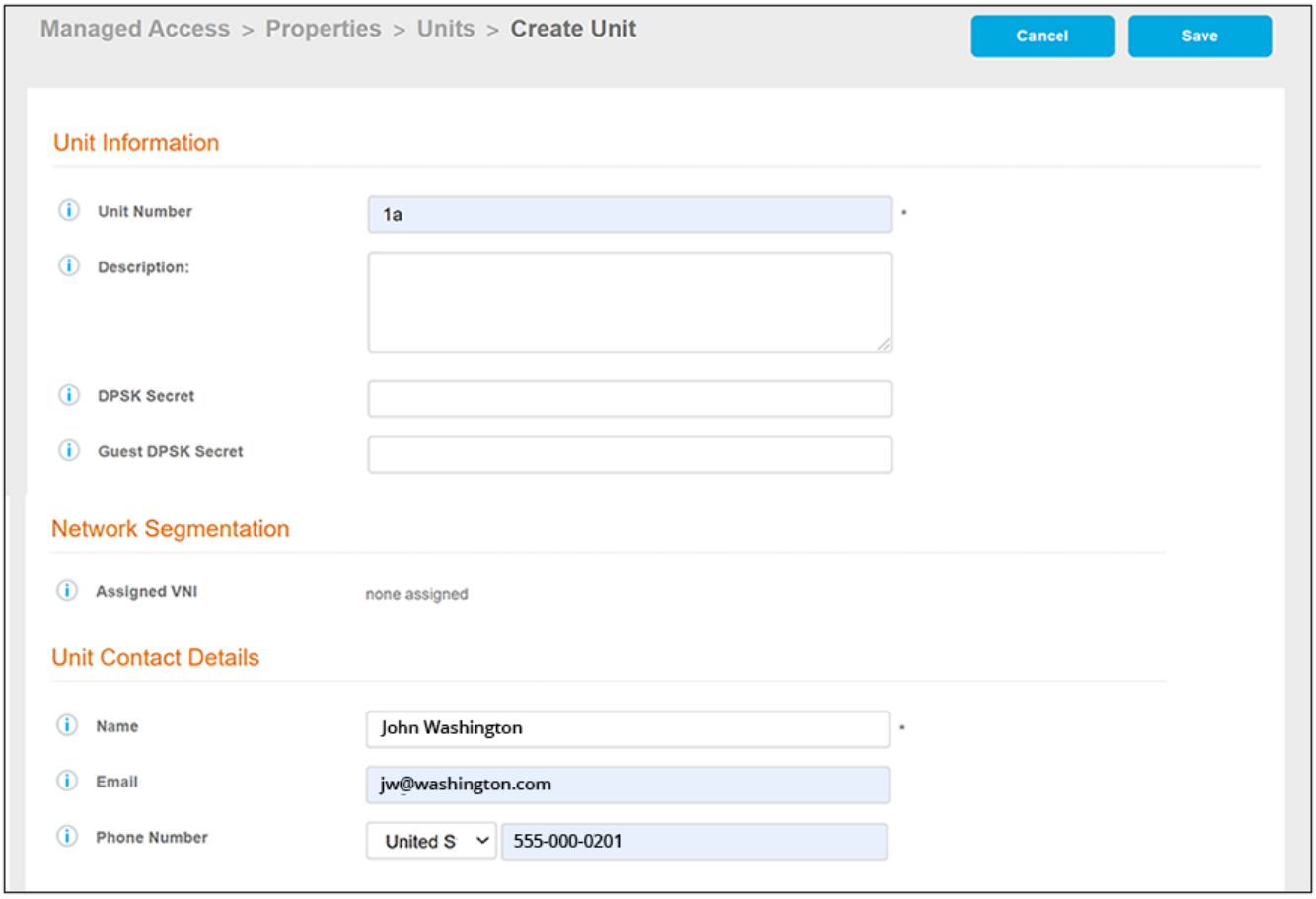
FIGURE 18 Adding Units By Bulk Upload or Individually



NOTE
If you have a lot of units to add, you can use the **Download Template** and **Import** buttons to add units by bulk (field descriptions are provided in the following steps). For more information about bulk uploads, refer to the "Bulk Upload Considerations" section of the *Cloudpath Enrollment System Property Management Administration Guide*. To add units individually, proceed to the next step.

3. Click **Add Unit** to add the first unit to your property, as shown and described in the following example:

FIGURE 19 Adding a Unit to Your Property



- Unit Number: Number or name of the unit you are adding.
- Description (optional): Description of the unit.
- DPSK Secret (optional): This is the secret that all devices connecting to this unit will need for wi-fi access. On the tenant portal, this secret is called the "Wi-Fi Passphrase." In the Cloudpath UI, you do not need to enter a value here because the secret is automatically generated. However, you can enter a value if you wish, and you can also change the unit secret at a later time.

  NOTE
  If, when you created the property, you checked the "Guest DPSK" box, a separate "Guest DPSK Secret" gets generated that all guest devices connecting to this unit will need for wi-fi access.

- Guest DPSK Secret (optional): This field is present in unit configuration only if you checked the "Guest DPSK" box when you configured the property. This is the secret that all *guest* devices connecting to this unit need for wi-fi access. On the tenant portal, this secret is called the "Guest Passphrase." In the Cloudpath UI, you do not need to enter a value here because the secret is automatically generated. However, you can enter a value if you wish, and you can also change the guest secret at a later time.
- Assigned VNI: The VNI number assigned to this unit on the Network Segmentation group associated with this property. By default, all units that belong to a property with a Network Segmentation group will have an assigned VNI, but this VNI can be removed by the administrator if desired.

NOTE
The VNI is assigned once you save the configuation. For example, you can see the VNIs assigned to two configured units in Figure 20. If no VNIs are available when the unit is created, no VNI is assigned. However, as soon as a VNI becomes free (for example, if the range of VNIs is increased or if a unit is deleted), a newly available VNI is auto-assigned to the new unit.

- Unit Contact Details: Enter the contact information for the tenant of this unit. The email and mobile phone information that you enter will be used to notify the tenant about how to access the tenant portal and what the pass phrases are for unit and guest wi-fi access.

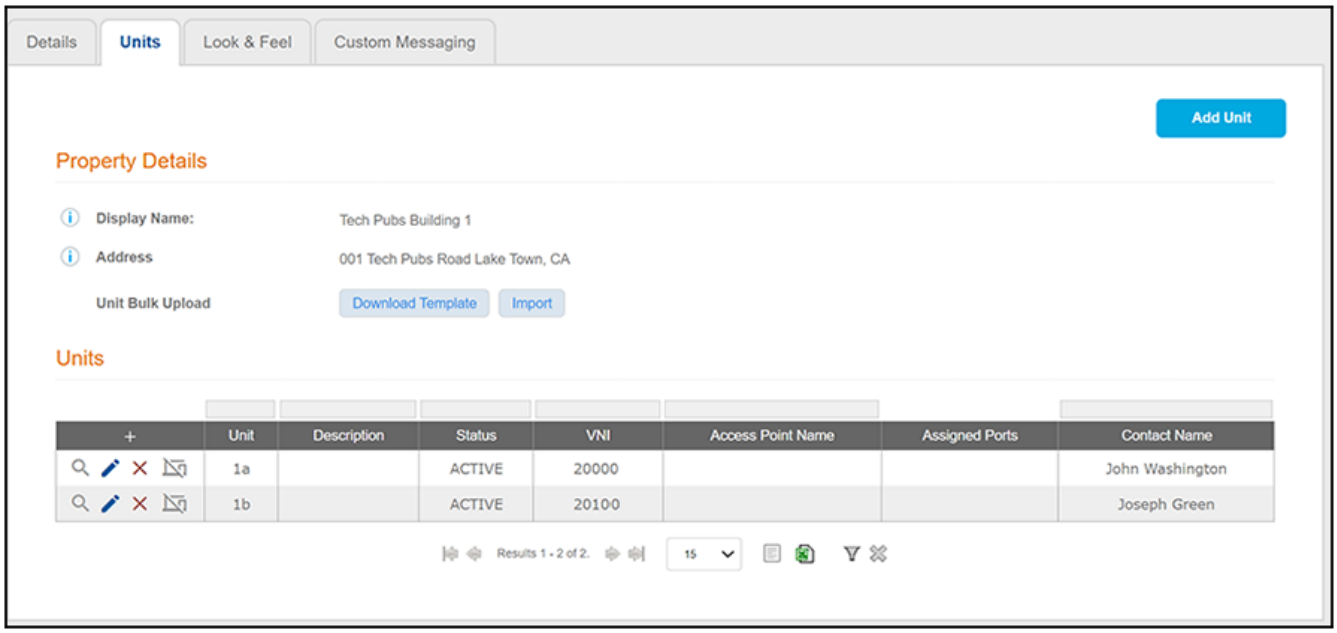
  NOTE
  The name you enter here will appear near the top of the home page on this person's tenant portal.

4. Click **Save**.

   NOTE
   Once you save the configuration of a new unit, you have the option of resending the assignment SMS/Email to the phone number and/or email defined for this unit, provided that sending SMS/Email has been enabled in the configuration of the applicable property. To resend this information (for example, if you have changed a wi-fi passphrase), you can enter edit mode for the unit, and enable the "Resend SMS/Email" check box in the "Unit Contact Details" section of the screen, then click **Save**. Another method of resending this information is to click the magnifying glass for the unit (in the grid view of all configured units), then click the **Resend Unit Assignment SMS/Email** button in the "Unit Contact Details" section of the screen (refer to Figure 27 on page 44).

5. Using the **Add Unit** button (or the **+** button above the Units grid), continue to add as many units to the property as you want. The following screen shows two units have been added to the property:

   FIGURE 20 Property Details Example After Adding Two Units



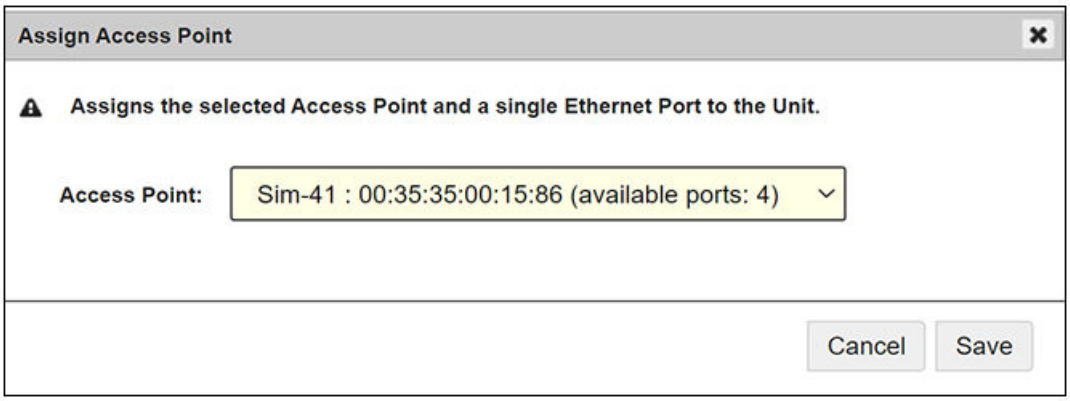
6. To add access points and assign ports, click the magnifying glass for a unit such as unit 1a in the example above.

7. In the "Network Segmentation Information" section of the ensuing screen, click **Assign Access Point**.

FIGURE 21 Using the Assign Access Point Button

8. From the Access Point drop-down (see screen below), select the AP and a single ethernet port to assign to the Unit, then click **Save**.

FIGURE 22 Access Point Selection



9. After your selection is saved, the Network Segmentation Information on the screen reflects the selection, as shown in the following screen:

FIGURE 23 Network Segmentation Information For a Unit After Access Point Is Selected

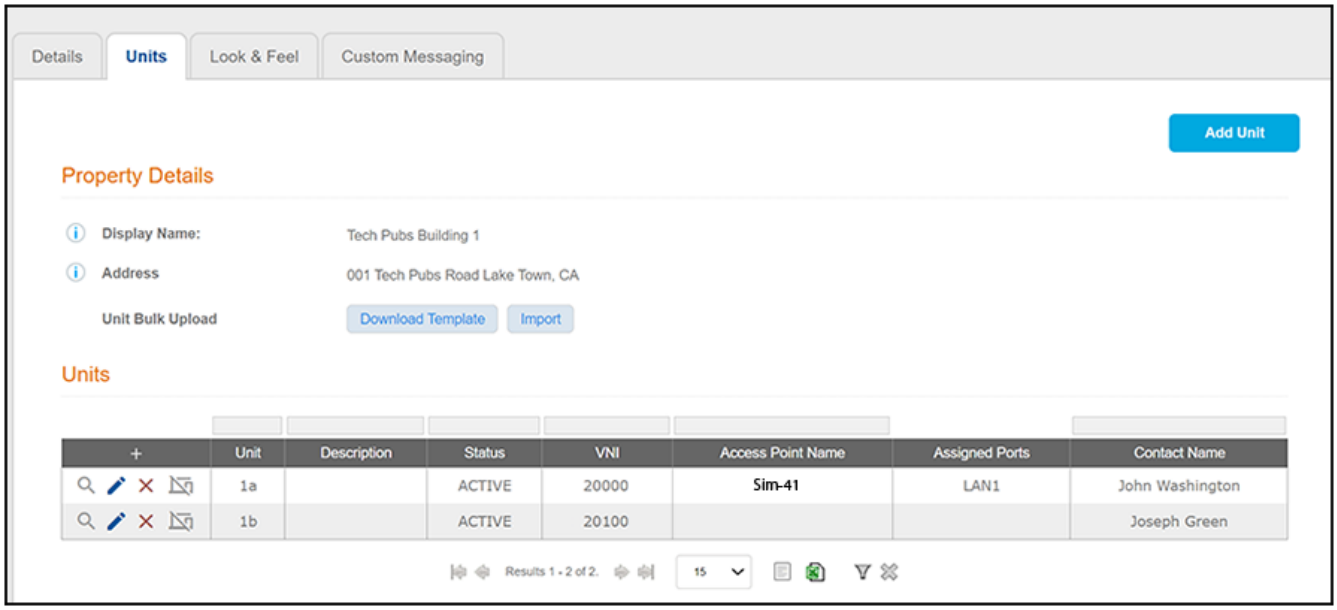
You can use the buttons shown as follows:

- Change Access Point: This button allows you to change your selection from the Access Point drop-down list.

- Remove Assignment: This button removes the access point and ethernet port assignments from the unit.
- Assign Ports: This button invokes a popup screen that shows available ethernet ports you can select.

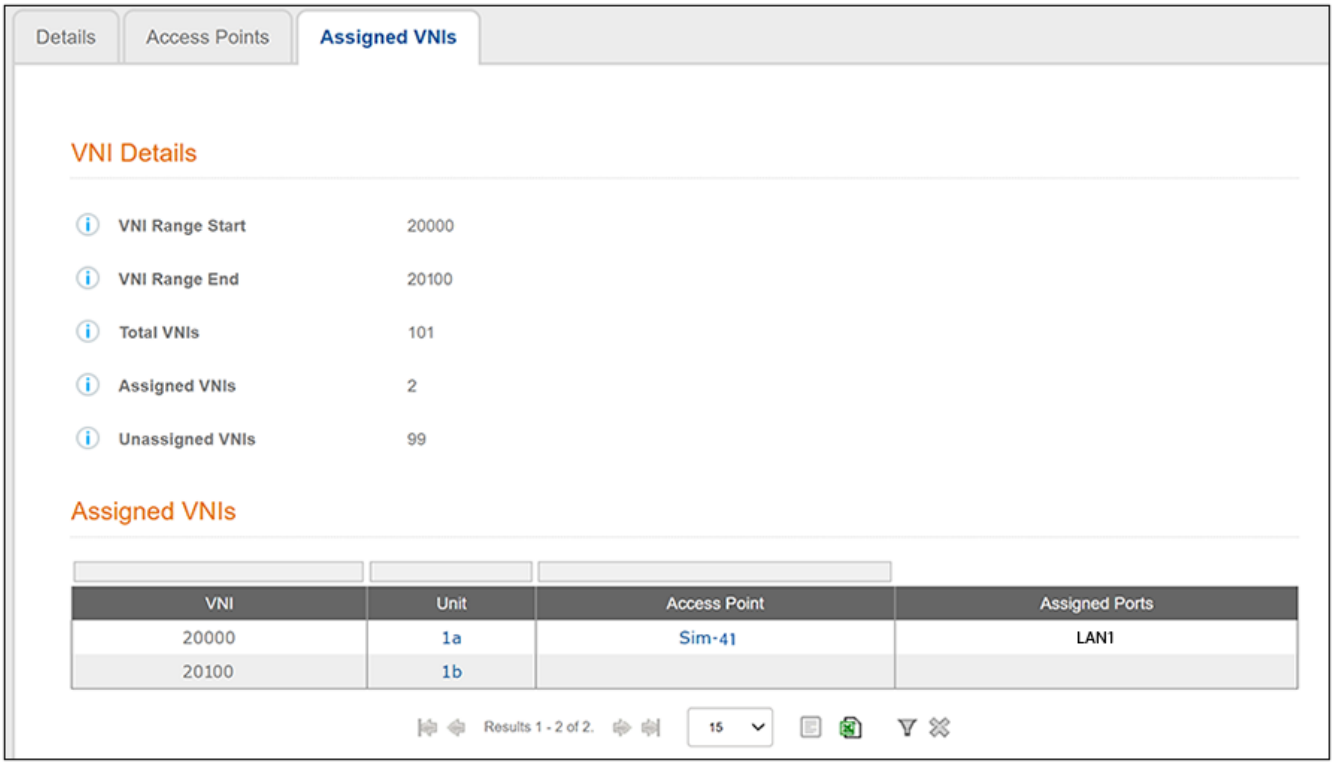
If you return to the **Units** tab view of the property, the access point and port selection you just made now appear:

FIGURE 24 Units Tab View of Property With AP and Ports Assigned to a Unit



You can also return to the Assigned VNIs tab of the Network Segmentation Group to view the updated list of assigned VNIs, as shown in the following example screen:

FIGURE 25 Assigned VNIs Tab Example After Two VNIs Have Been Assigned

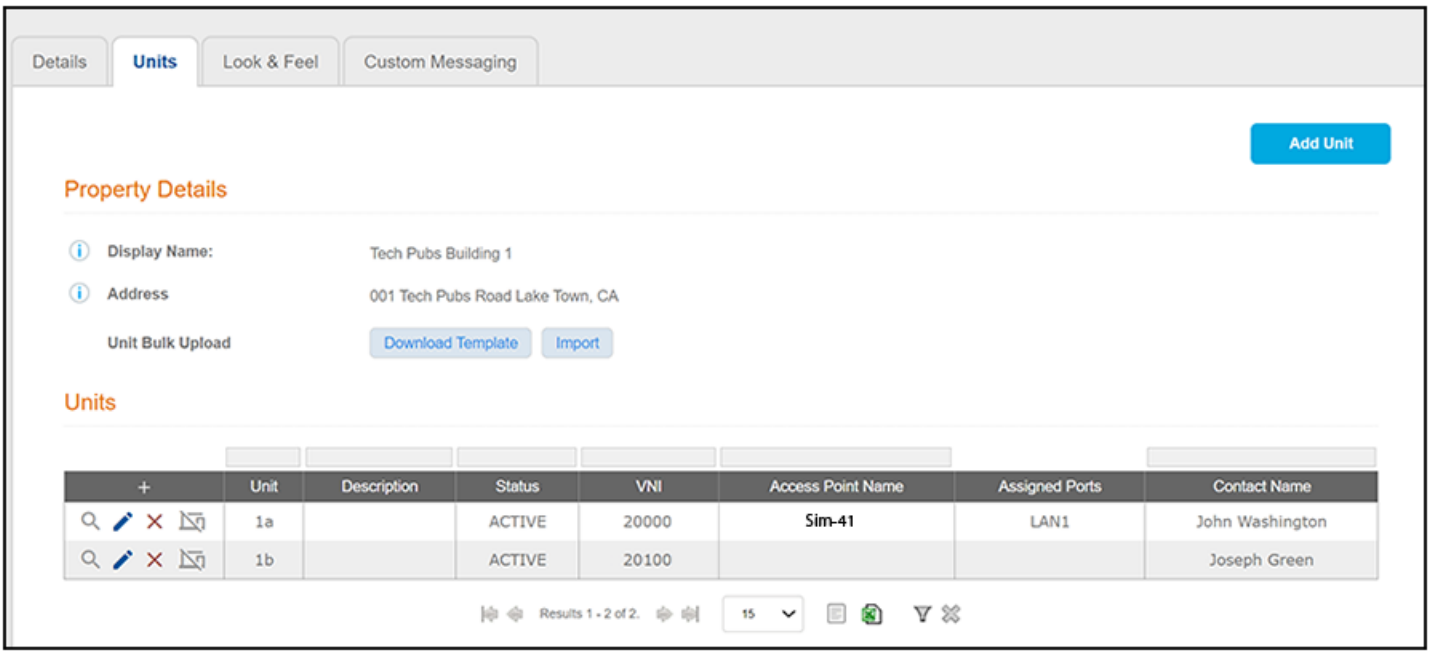


Viewing Information of a Configured Unit

Once you have configured a unit, there is a lot of information about the unit that you can find useful.

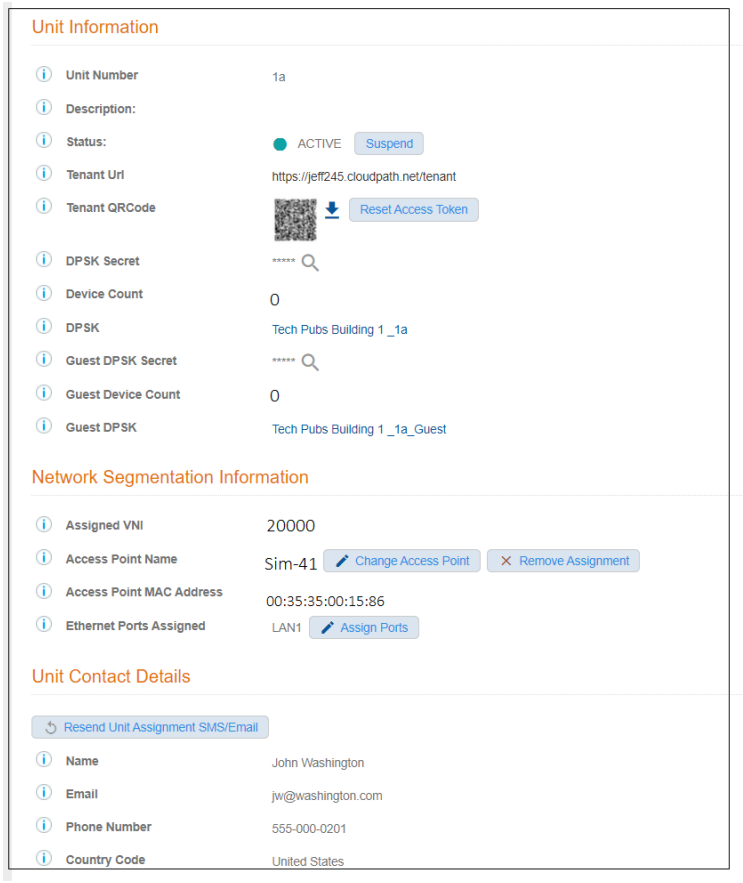
If you go to the main Properties page (**Managed Access > Properties**) in the Cloudpath UI, click the wrench icon for the desired property, then click the **Units** tab, you get a view such as the one below:

FIGURE 26 View of All Units Within a Property



Then, you can click the magnifying glass icon to view all the settings of one of the units. The example below shows the information for the unit called 1a:

FIGURE 27 Unit-Specific Information



Some fields of interest include:

- Status: If for any reason you want to suspend this unit, you can do so from this field. This would revoke its associated DPSKs and prevent it from accessing the tenant portal and wi-fi network. You can re-activate the unit at anytime.
- Tenant URL: This is a live link that will take you directly to the tenant portal for this unit. For more information of using tenant portals, refer to the *Cloudpath Enrollment System Property Management Administration Guide*.
- Tenant QRCode: You can download the code and give it to the tenant as another option to provide them with access to the portal if they have QRCode-compatible devices. You can also reset the access token for any reason if you want to prevent the original code from working. Once you reset the code, the tenant receives a notification with the new access information.

  NOTE
  The tenant also has the ability to reset the access code from the tenant portal profile page if he or she thinks the code has been compromised. For more information, refer to *Cloudpath Enrollment System Property Management Administration Guide*. In this case too, the tenant receives a notification with the new access information as soon as the code has been reset.

- DPSK Secret: You can view the secret from here by clicking the magnifying glass. You can also change the secret from the UI by editing the unit configuration. This is described in more detail later.
- DPSK: The name of the DPSK is formed as: ***name of the property_name of the unit***
- Guest DPSK Secret: You can view the secret from here by clicking the magnifying glass. You can also change the secret from the UI by editing the unit configuration. This is described in more detail later.

- Guest DPSK: The name of the Guest DPSK is formed as: ***name of the property_name of the unit_Guest***
- Network Segmentation area: You can use the buttons to make changes to APs and ports, as desired.
- Resend Unit Assignment SMS/Email: Clicking this button resends the assignment SMS/Email to the phone number and/or email defined for this unit, provided that sending SMS/Email has been enabled in the configuration of the applicable property.

Using the Access Points Tab

You can use the **Access Points** tab of the **Managed Access > Network Segmentation** portion of the Cloudpath UI to view assigned APs and ethernet ports, and to make any changes to these assignments.

Navigate to **Managed Access > Network Segmentation**, click the wrench icon for the Network Segmentation group, and go to the **Access Points** tab. A view like the one shown in Figure 12 on page 31 is displayed.

You can then click the magnifying glass of an AP of interest. The screen below shows an AP that is already in use. Because it is in use, it contains a button you can use if you wish to remove the AP assignment. You can also remove any assigned ethernet ports by clicking the **X** next to the desired port.

FIGURE 28 Details of an Access Point Already Being Used

Property Management Information

Properties and units that belong to a network configuration group can be used in conjunction with the property management features that are described in the *Cloudpath Enrollment System Property Management Administration Guide*.

Refer to the following topics in the *Cloudpath Enrollment System Property Management Administration Guide* for additional information:

- "Generating an API Key"

- "Setting up the Look and Feel of the Tenant Portal"
- "Connecting to the Tenant Portal"
- "Connecting to the Wi-Fi Network"
- "Using the Tenant Portal"
- "Creating a Management Portal" and its subsections
- **NOTE**
  There are some differences in configuration and unit information displayed on the management portal between properties and units that belong to a network segmentation group and those that do not. The main differences are that network segmentation group units do not use VLAN, but instead use VNIs, AP names, AP MAC addresses, and Ethernet port assignments.

Creating a Policy to Assign to eDPSK Pools (Optional)

Before you create a DPSK pool for a property, you can configure policies that can be applied to eDPSK pools. Policies allow for mapping incoming successful RADIUS authentication requests to a set of RADIUS response attributes based on dynamic conditions of the request.

NOTE
When you create a DPSK pool, you can set the default behavior of whether to accept or reject a user who does not match the acceptance criteria of any policies. If you choose to use the “Accept” setting, a user is always accepted, and you do not need to configure a policy. However, if you use "Reject” as the default policy behavior, you need to configure at least one policy that is a match for each VNI (VXLAN) in the Network Segmentation group.

Each policy has an associated RADIUS attribute group which defines the RADIUS response attributes (such as filter ID, and class). Each authentication is matched against an assigned list of candidate policies in sequential order. Criteria of a policy can include dynamic conditions such as a user's physical location, username, or the time of day.

NOTE
"VLAN ID" is not applicable to network segmentation. Instead, a VXLAN is assigned to a unit that is part of the network segment. This VLXAN is the virtual network identifier (VNI); for an example refer to Figure 20 on page 39.

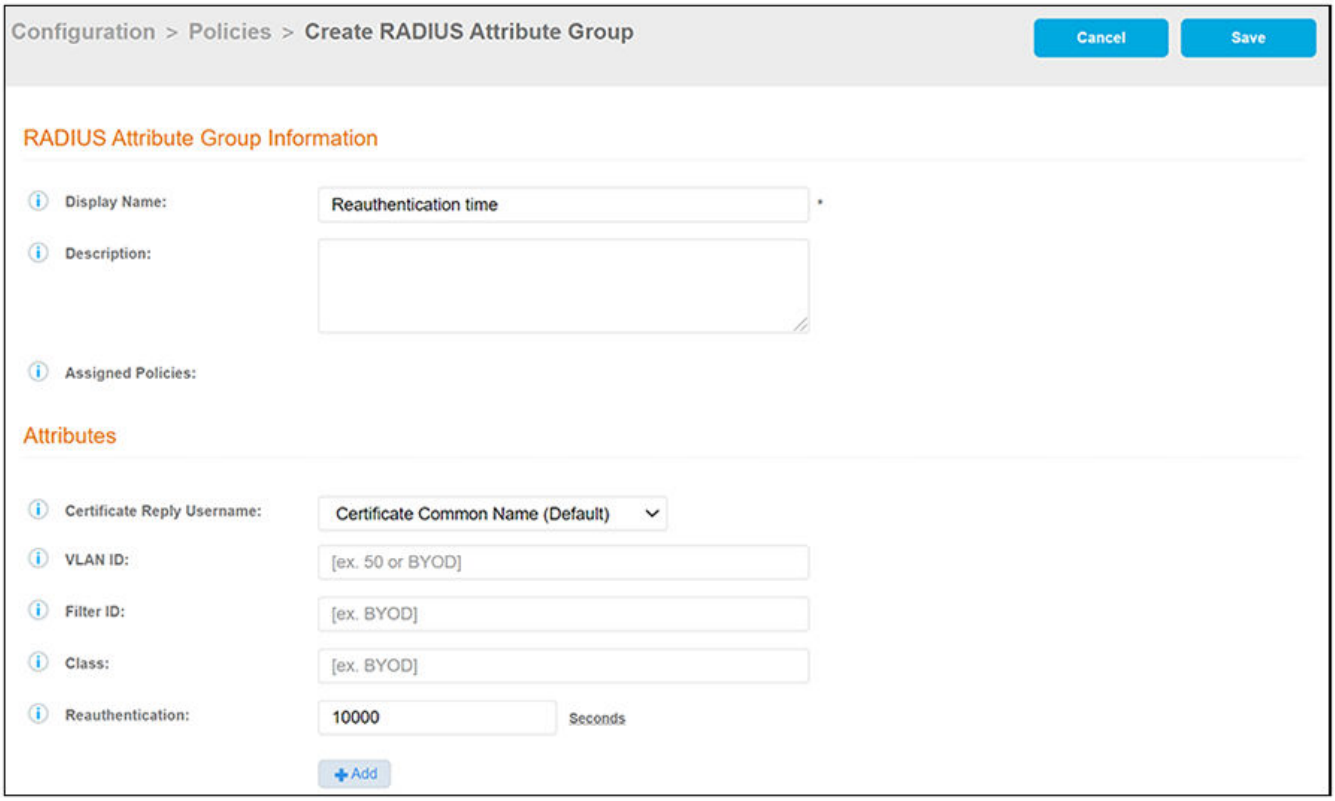
The following procedure guides you first through creating RADIUS attribute groups for your policies, then creating the policies themselves. You must create at least one RADIUS attribute group before you can configure a policy because a policy needs to have at least one RADIUS attribute group available for selection.

1. In the Cloudpath UI, go to **Configuration > Policies**.
2. Select the **RADIUS Attribute Groups** tab, then click the **Add RADIUS Attribute Group** button.
3. In the ensuing Create Radius Attribute Group screen, enter the information to create the group, then click **Save**.

   NOTE
   You can configure as many RADIUS Attribute groups as you want. One RADIUS Attribute group will later be assigned to each policy you create.

   An example screen is shown below. For detailed steps, refer to the "Configuring Policies" section of the *Cloudpath Enrollment System External Dynamic Pre-Shared Key (eDPSK) Configuration Guide*.

FIGURE 29 Create RADIUS Attribute Screen

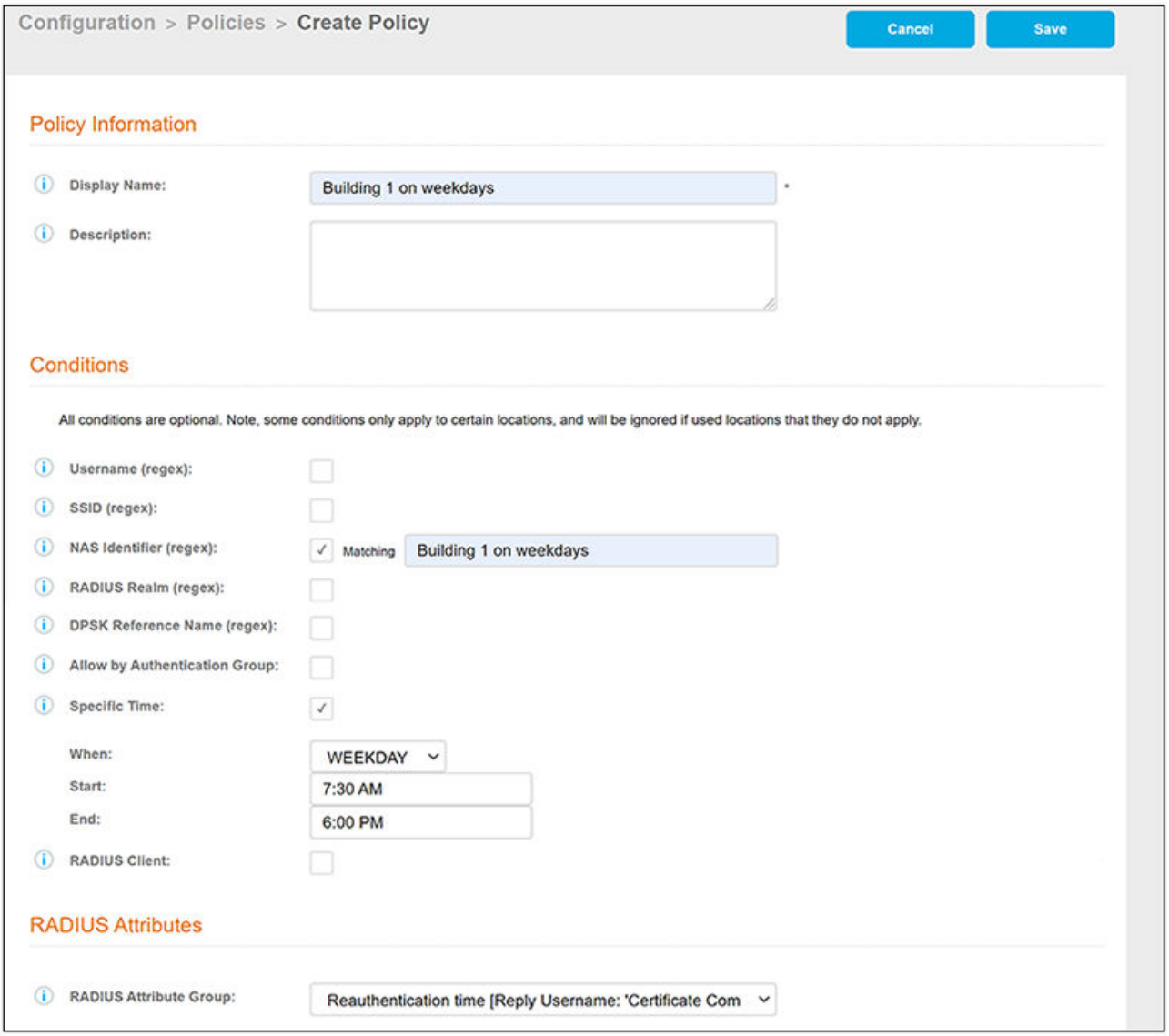


4. Configure your policies:
   a. In the **Configuration > Policies** area of the UI, select the **Policies** tab, then click **Add Policies**.
   b. In the ensuing Create Policy screen, enter the information to create the policy, then click **Save**.

      NOTE
      You can configure as many policies as you want.

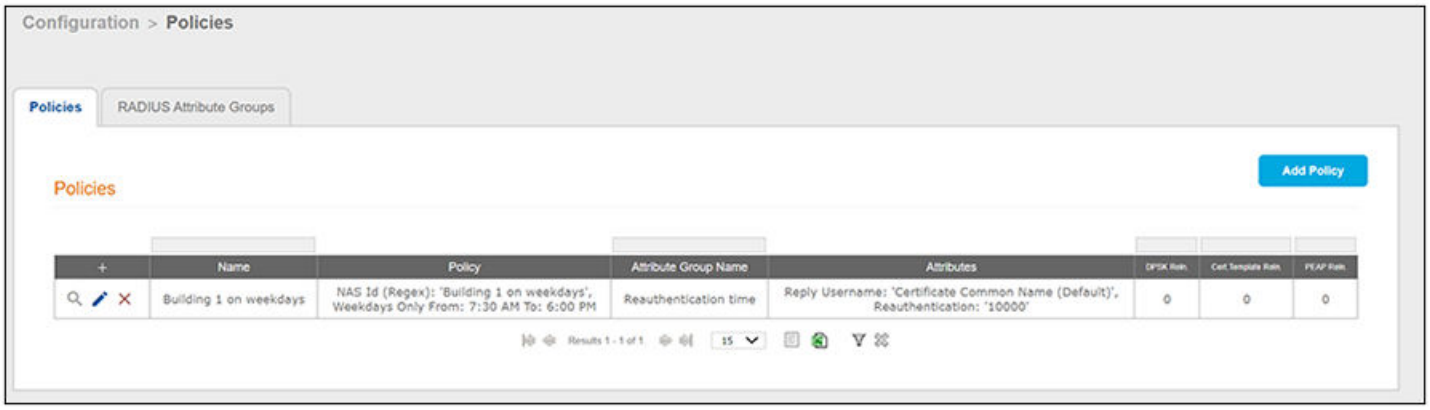
      An example screen follows. For detailed steps, refer to the "Configuring Policies" section of the *Cloudpath Enrollment System External Dynamic Pre-Shared Key (eDPSK) Configuration Guide*.

FIGURE 30 Create Policy Screen



The following illustration shows the Policies tab after one policy has been added. The information shown in the table represents the policy configuration shown in the example in the Create Policy Screen. The attribute group name and its attributes come from the attribute group name selected in the Create Policy Screen drop-down list. (The "Certificate Reply Username" applies only to certificate-based authentications, and is therefore described in the Cloudpath documentation of certificate templates.) The RADIUS attribute information shown below comes from the example in the Create RADIUS Attribute Screen.

FIGURE 31 Policies Table Example After One Policy Is Configured



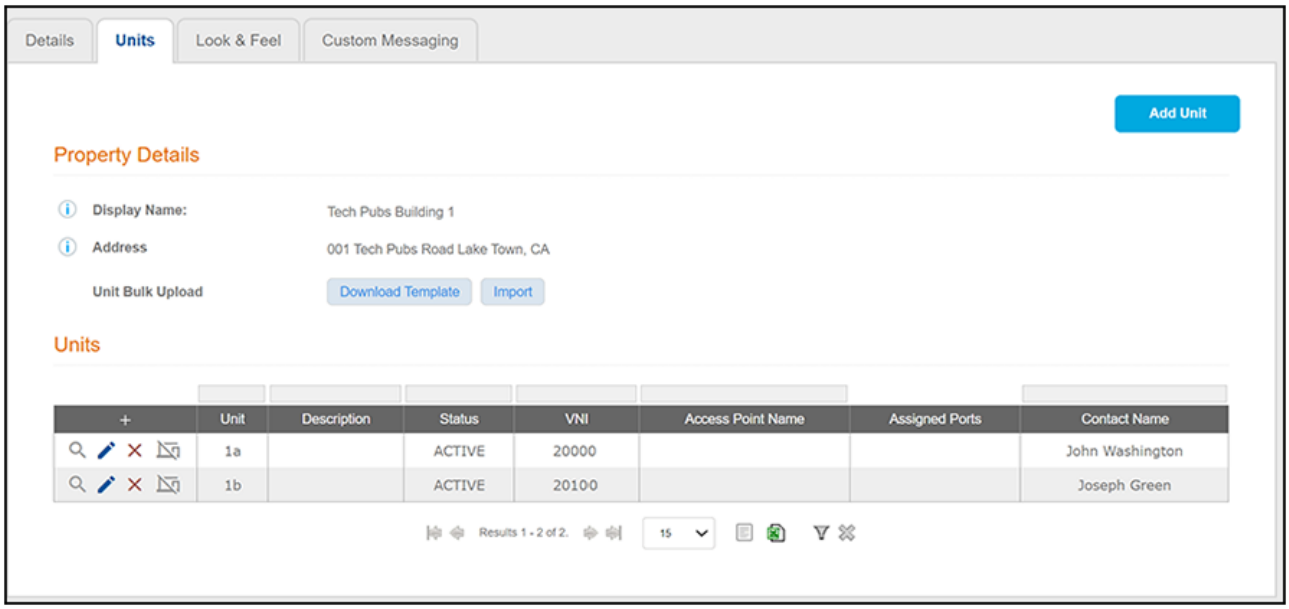
Troubleshooting

There are some basic troubleshooting steps you can try if the tenant of a unit that belongs to a network segmentation group is having difficulty connecting to the network.

Here are some steps to follow:

1. Make sure that the tenant's unit still exists in the Cloudpath UI property configuration (for illustrative purposes, the tenant is named John Washington and lives in unit 1a):
    a. In the Cloudpath UI, go to **Managed Access > Network Segmentation**.
    b. Click the wrench icon for the network segmentation group in which the unit belongs.
    c. Under "Assigned Properties," click on the name of the property in which the unit belongs.
    d. On the ensuing screen, click the **Units** tab to display all units that belong to this property, as shown in the screen below:

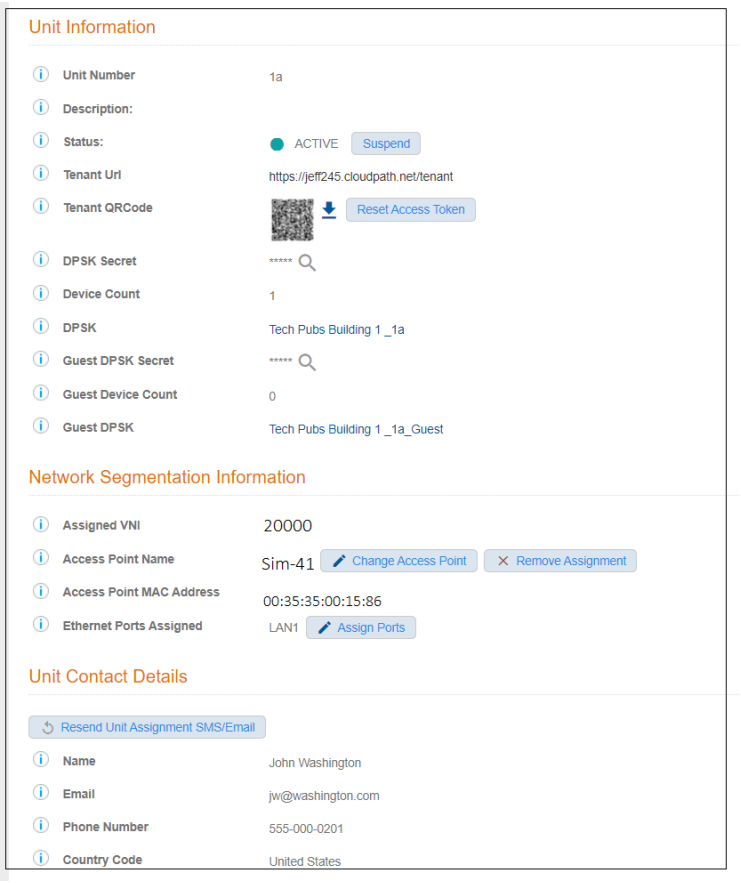
FIGURE 32 Units Tab View of Property in Network Segmentation Group



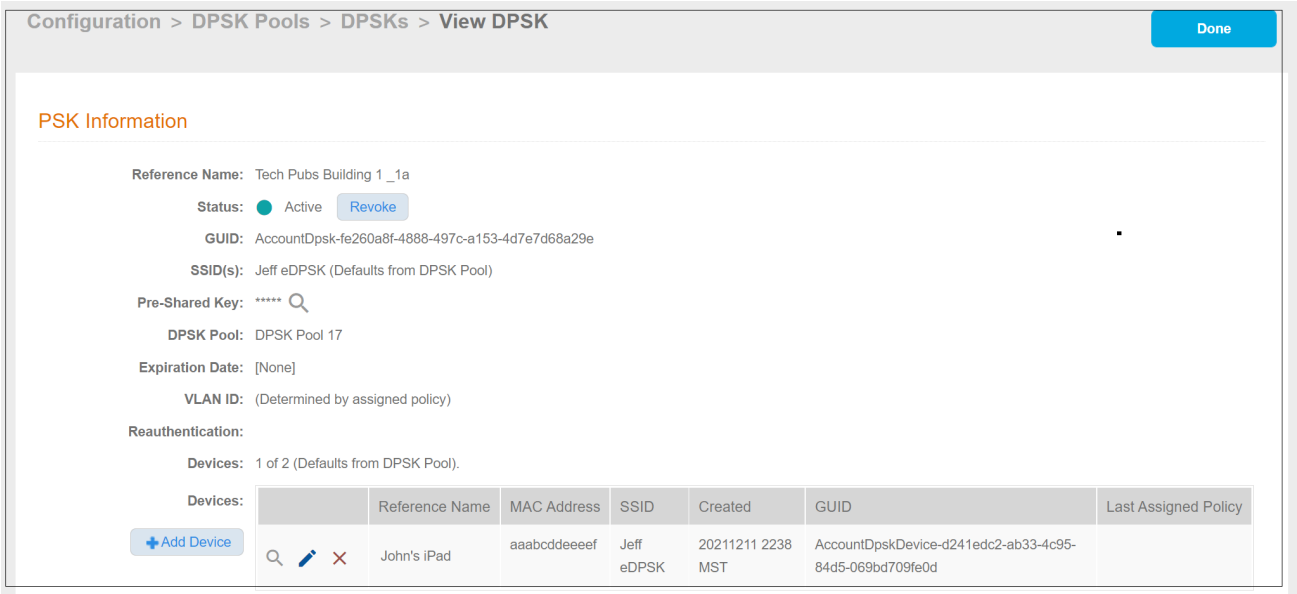
e. The tenant in question and his unit are shown in the above screen, as expected.

2. Check the wireless configuration. Click on the magnifying glass for the unit to invoke the following screen:

FIGURE 33 Unit-Specific Information



- Check that the "Status" field is ACTIVE.
- Click the "DPSK Secret" magnifying glass to view the secret, then confirm with the tenant that the proper secret was entered. You could also change the secret or resend it by clicking the **Resend Unit Assignment SMS/Email** button in the Unit Contact Details section of the screen.
- Make sure there is a VNI assigned to the unit (Network Segmentation Information section of the screen).
- Click on the link of the currently assigned DPSK (**Tech Pubs Building 1 _1a** in the screen example above). This invokes the PSK Information screen:



In the PSK information, you can check to see if any devices have connected to the network. In the example above, the device called "John's iPad" has successfully connected.

3. Check the wired configuration. Return to the unit-specific information screen for unit 1a and scroll down to the Network Segmentation Information area.
   a. Check that the correct AP has been assigned to the unit.
   b. Make sure that the correct ethernet port(s) are being used in the unit. (Verify that the Cloudpath and vSmartZone systems that compose the network segmentation group have the same ethernet port(s) activated.
4. Check RADIUS logs and AUTH Logs. In the Cloudpath UI, go to **Configuration > RADIUS Server** > Status tab, scroll down to the RADIUS Logs section, and set the Log Level to **Debug**. When you check the log files, check for items such as the following:
   - Any policies that might be assigned to the eDPSK pool being used by the property that might not be allowing access to the user/unit in question.
   - VNI information
   - PSK information
5. If none of the preceding steps uncover the connection issue, the next steps would be for the vSmartZone administrator to perform troubleshooting steps on the vSmartZone controller that is being used in this network segmentation group.

COMMSCOPE®
RUCKUS®

© 2021 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com