



ExtremeWireless WiNG™ 7.6.3 Controllers

NOVA UI Getting Started Guide

9037026-00 Rev AA
June 2021



Copyright © 2021 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>

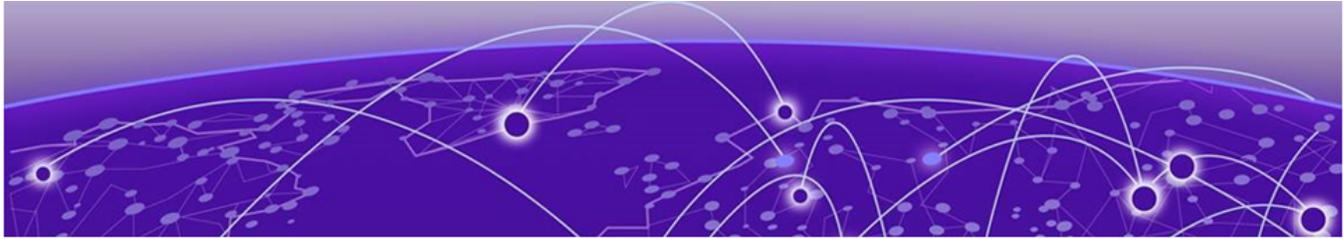
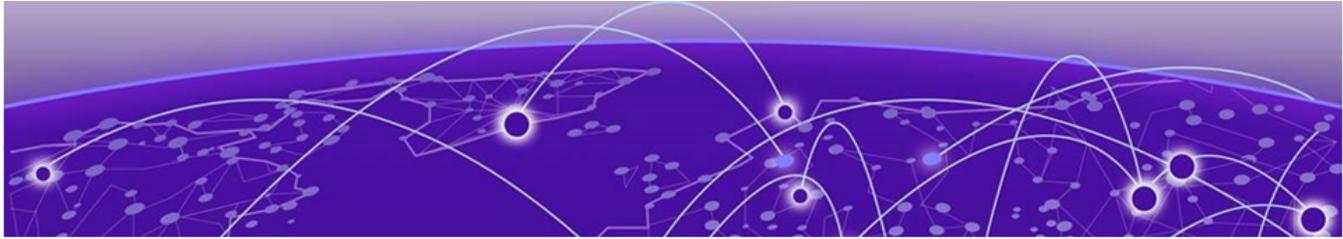


Table of Contents

Preface	6
Text Conventions.....	6
Documentation and Training.....	7
Help and Support.....	8
Subscribe to Product Announcements.....	8
Send Feedback.....	8
WiNG 7 Operating System Overview	10
Web UI and Initial Setup	12
Access the Web UI.....	12
Browser and System Requirements.....	12
Connect to the Web UI.....	12
Enable New User Interface.....	14
Navigate the User Interface	16
User Roles and Preferences Settings	18
User Roles.....	18
Per User Preferences Settings.....	18
Remote Servers Settings.....	19
System Dashboard	21
Site tree display.....	21
Add a Custom Dashboard.....	22
Edit or Delete a Selected Dashboard.....	22
Slide-in Device Info	24
Slide-In Device Info Details Dashboard.....	24
Slide-In Device Info Adoption Dashboard.....	24
Cluster	25
Site	27
Add a Site.....	28
Edit Site Basic Configuration.....	28
Edit Site Policies Configuration.....	29
Delete a Site.....	30
Devices	31
View Device Basic Info.....	31
Remote CLI from Device Configuration.....	32
Wireless Configuration	33
Add Wireless Network.....	33
Wireless Network Basic Configuration.....	34

Wireless Network Security Configuration.....	35
Profiles.....	38
Add Profile.....	39
Create Basic Profile Configuration.....	39
Network Tab Profile Configuration.....	40
Manage Profile Adoption Configuration.....	42
Set Controller Power Configuration.....	43
Profile Network Configuration.....	44
Set a Profile's DNS Configuration.....	44
Set a Profile's ARP Configuration.....	45
Set a Profile's L2TP V3 Configuration.....	46
GRE Network Configuration.....	52
IGMP and MLD Snooping Configuration.....	55
Profile Policies Configuration.....	58
Clients.....	61
Diagnostics.....	62
System Info.....	62
General System Info Diagnostics.....	62
CDP Neighbors Diagnostics.....	63
LLDP Neighbors Diagnostics.....	64
Tasks Diagnostics.....	64
Tech Support.....	64
Tech Support Session.....	64
Create a New Tech Support Session.....	65
Tech Support Server.....	65
Logs.....	65
General Logs.....	65
Advanced Logs.....	66
Remote CLI.....	67
Remote CLI Operations.....	67
Policies.....	68
Management Policy.....	68
View Management Dashboard.....	69
Add a New Management Policy.....	71
Edit or Delete a Management Policy.....	87
Authentication, Authorization, and Accounting (AAA) Policy.....	87
Add a New AAA Policy.....	88
Edit a AAA Policy.....	91
Delete a AAA Policy.....	91
NSight Policy.....	92
Add NSight Policy.....	92
Edit NSight Policy.....	93
Delete NSight Policy.....	94
RADIUS Group.....	94
Create RADIUS Group.....	95
RADIUS User Pool.....	98
RADIUS Server Policy.....	100

Configure RADIUS Server Policy.....	102
Configure RADIUS Clients.....	103
Configure RADIUS Proxy.....	104
Configure an LDAP Server.....	106
Auto-Provisioning Policy.....	108
Configure Auto-Provisioning Policy Rules.....	108
Configure Auto-Provisioning Policy Adoption Criteria.....	111
Firewall.....	112
Configure a Firewall Policy.....	112
SmartRF Policy.....	124
Sensor Policy.....	125
Configure a Sensor Policy.....	125
Configure an Event System Policy.....	126
Configure a Device Categorization Policy.....	127
WIPS Policy.....	128
Configure a WIPS Policy.....	128
Configure WIPS Events.....	130
Configure WIPS Signatures.....	132
L2TPv3 Policy.....	134
L2TPv3 Configuration.....	135
DHCPv4 Policy.....	137
Add or Edit a DHCPv4 Policy.....	137
Configure DHCPv4 Class Policy.....	138
Configure DHCPv4 Address Pools.....	139
Firmware Update and Images.....	144
Firmware Update.....	144
Firmware Images.....	144
Statistics.....	146
Index.....	147



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[]	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, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member</i> [<i>member</i> ...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and software compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other resources](#) such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

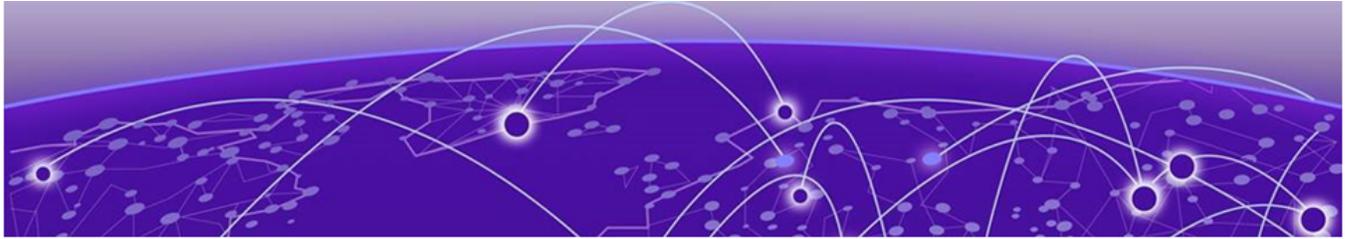
- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to send feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



WiNG 7 Operating System Overview

General information about WiNG 7 operating system.

The WiNG 7 operating system is a solution designed for 802.11n, 802.11ac and 802.11ax networking. It is a convergence of the legacy ExtremeWireless WiNG™ (5.9.X) and ExtremeWireless™ (10.X) wireless operating systems. It offers a high-level of flexibility and scalability covering both campus and distributed modes of deployment.

WiNG 7.X.X brings together the following key benefits of both deployment topologies under one fold:

- **ExtremeWireless** - The ExtremeWireless software provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11 standard. The system is intended for enterprise networks operating on multiple floors in more than one building, and is ideal for public environments, such as airports and convention centers that require multiple access points. It is an ideal solution for high-density, campus and stadium deployments. It is well suited to meet the needs of enterprises in the education, healthcare, sports and entertainment verticals. The ExtremeWireless OS key strengths are:
 - Extensive Policy Framework
 - Contextual Device and Application Control
 - Application Visibility & Control with Analytics
 - BYOD - Single SSID with Programmable Data Path
 - Voice & Video Optimized with Seamless Roaming
- **ExtremeWireless WiNG** - The WiNG architecture is a solution designed for 802.11n and 802.11ac networking. It is designed for standalone or distributed hierarchical networks. The ExtremeWireless WiNG software distributes intelligence right to the network edge, empowering every controller and access point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time. It is highly scalable and well suited to meet the needs of large, geographically distributed enterprises. It is an ideal wireless networking solution for the retail, manufacturing, transportation & logistics, and hospitality verticals. The ExtremeWireless OS key strengths are:
 - Simple Guest Access with Analytics
 - Contextual Application Control
 - Advanced Diagnostics and Remote Troubleshooting
 - Intrusion, Compliance and WiFi Forensics
 - Scale-out 1000s of APs with Rapid Rollout
 - Self-tuning RF (Smart-RF)
 - Distributed Service Intelligence

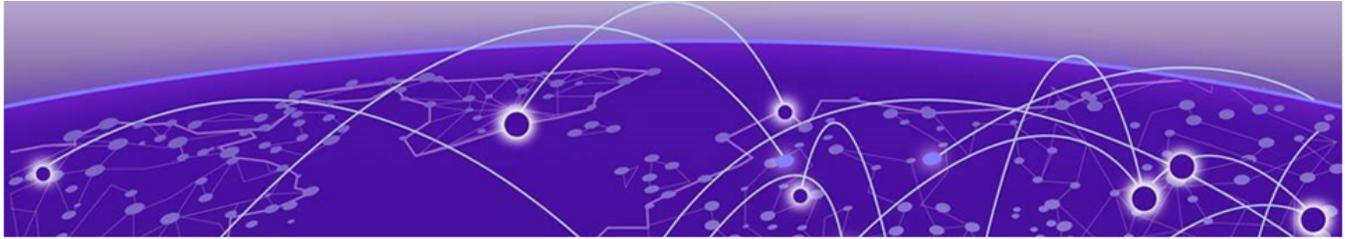
Going forward, this unified, common, wireless, infrastructure WiNG 7.X. OS will power the ExtremeWireless WiNG product family. The WiNG 7.6.3 OS supports the following platforms:

- Service Platforms — NX 5500, NX 7500, NX 9500, NX 9600, VX 9000



Note

NOVA UI is available only on controllers.



Web UI and Initial Setup

[Enable New User Interface](#) on page 14

Details about browser requirements, web UI connection, and initial setup.

As a network administrator, you can manage and view controller and service platform settings, configuration data, and status using the WiNG web UI.

Access the Web UI

Using a web browser on a client connected to the subnet in which the web UI is configured on, you can access the controllers and service platforms GUI.

Browser and System Requirements

The system used for accessing the GUI must have at least 1 GB of RAM for the UI to display and function properly, with the exception of NX service platforms, which require 4 GB of RAM.



Tip

The best practice is to use a browser with HTML5 support.

Use the following browsers to access the WiNG web UI:

- Google Chrome
- Microsoft Edge
- Safari
- Firefox

The minimum supported screen resolution is 1920 × 1024 pixels.

Connect to the Web UI

Use the following steps to connect to a wireless controller or a service platform's Web UI for the first time:

1. Connect one end of an Ethernet cable to a LAN port on the controller or service platform, and connect the other end to a computer with a working web browser.
2. Set the computer to use an IP address between **192.168.0.10** and **192.168.0.250** on the connected port.

3. Set a subnet or network mask of **255 . 255 . 255 . 0**.

- a. On windows machines, open your calculator.

To access the calculator, type **calculator** on the windows search bar.

This path varies depending on the version of Windows operating system running on your computer.

- b. With the Calculator application displayed, select **Scientific** or **Programmer** depending on the version of Windows running on your computer.
- c. Select the **Hex** radio button.
- d. Type the penultimate octet of the controller's MAC address.

In this example, the AP's MAC address is: 00:C0:23:00:F0:0A. Enter F0.

- e. Select the **Dec** radio button.

The calculator converts F0 into 240.

- f. Repeat this process for the last octet in the controller's MAC address

Type A, and select **Dec**. The calculator converts A into 10.

The controller's zero-config IP address is: 169.254.240.10

4. Open a browser, and type 10 . 234 . 165 . 165 : 10443 to access the web UI login screen.

The web UI login screen is displayed.

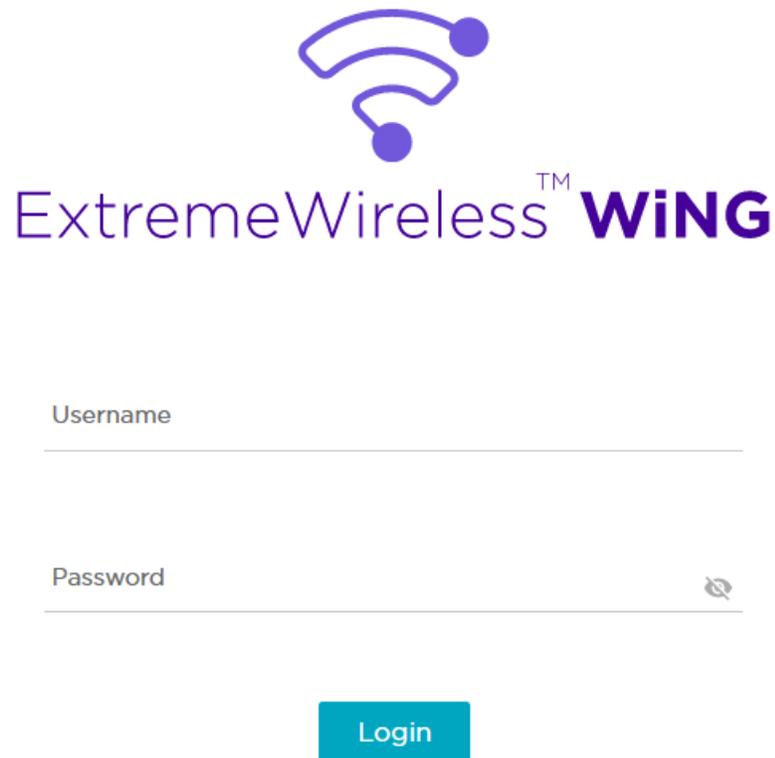


Figure 1: ExtremeWireless WiNG web UI login screen

5. Type the default username `admin` in the **Username** field.
6. Type the default password `symbol` in the **Password** field.

When logging in for the first time, you will be prompted to change the password to enhance device security. Set the new password and use it for subsequent logins.

7. Select **Login** to load the device's (wireless controller or service platform) management interface.

Logout

You can log out of the UI from the admin menu.

Related Topics

[Enable New User Interface](#) on page 14

[Navigate the User Interface](#) on page 16

[User Roles and Preferences Settings](#) on page 18

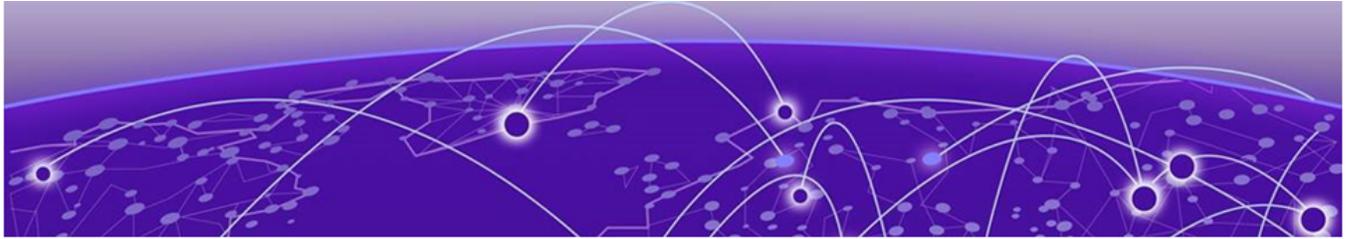
Enable New User Interface

You can enable new UI using WiNG CLI. Use the following commands to enable new UI:

```
vx9000 > enable
vx9000#
vx9000#conf
```

Type the following commands, one per line. End the command with **ctrl/Z**.

```
vx9000 (config)#management-policy default
vx9000 (config-management-policy-default)#nova
vx9000 (config-management-policy-default)#commit write memory
OK
vx9000 (config-management-policy-default)#
vx9000 (config-management-policy-default)#
```



Navigate the User Interface

Learn how to navigate the NOVA UI, use the search facility, and configure user roles and preferences.

The ExtremeWireless WiNG NOVA user interface is divided into work spaces that correspond to the network administration workflow. Monitor the controller using the **Dashboard** work space and configure network settings from the site, devices, wireless, and profiles work space.

ExtremeWireless WiNG NOVA UI offers the following work spaces:

Dashboard

When you log into the WiNG 7 UI, you are navigated to the default **Dashboard** screen. You can customize your system work space via the **Dashboard** screen.

Site

View and manage the list of sites.

Devices

View, manage, and configure devices.

Wireless

View, manage, and configure WLANs.

Profiles

View, manage, and configure device profiles.

Clients

View and monitor wireless clients.

Diagnostics

Run system diagnostics to get system information ranging from CPU usage, network usage to tech support information. Download various system logs for comparison.

- **System Info**
- **Tech Support**
- **Logs**
- **Packet Capture**
- **Traceroute**
- **Ping**

Remote CLI

Connect the current device WiNG CLI or download logs from remote CLI sessions.

Policies

Configure, add, and test network policies.

- **Management**
- **AAA**
- **NSight**
- **RADIUS Group**
- **RADIUS User Pool**
- **RADIUS Server**
- **Auto-Provisioning**
- **Firewall**
- **SmartRF**
- **Sensor**
- **Event System**
- **Device Categorization**
- **WIPS**
- **L2TPv3**
- **DHCPv4**

Firmware

Firmware upload and update management.

- **Update**
- **Images**

Statistics

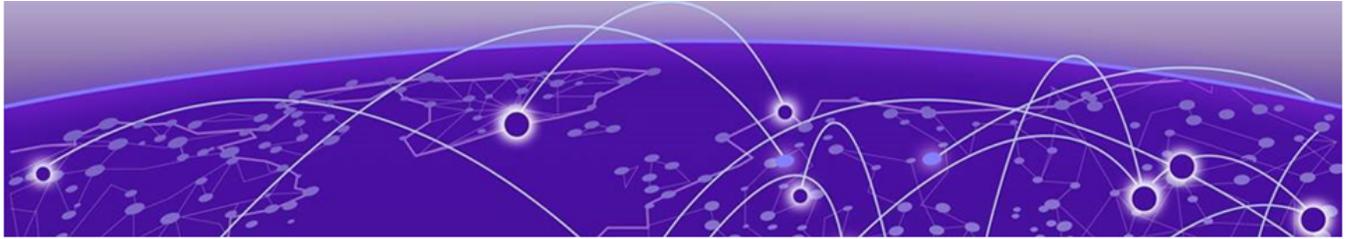
Detailed statistics for the following features in the network:

- **Smart RF**
- **Wireless**
- **Devices**
- **Clients**
- **Sites**

Notifications



Access the notifications and event logs bell icon from any work space. It is located on the top right corner of the UI. The notifications remain the same for all work spaces and provides the status of various operations.



User Roles and Preferences Settings

Details about various WiNG 7 user roles, settings, and preferences.

User Roles

WiNG operating system supports the following admin roles. Each admin user can be mapped to one of the roles mentioned in this section. Multiple admin roles can have access to an object.

admin - superuser

A superuser has complete access to all configuration aspects of the connected device, including halt and delete setup configuration.

device provisioning admin

Add, delete, or modify device configuration excluding self device and its cluster peers.

helpdesk admin

Troubleshoot tasks like clear statistics, reboot, create, and copy tech support dumps.

monitor

Read-only access to the system. Can view parts of configuration and statistics except for sensitive or protected information. Cannot view running-config.

network admin

Manage L2, L3, Wireless, Radius Server, DHCP Server, and SMART RF policies.

security admin

Can change WLAN keys.

system admin

Upgrade image, change boot partition, set time, and manage admin access.

web user - admin

Allows the front desk to create guest users and printout a voucher with their credentials. The webuser-admin can access only the custom GUI screen and does not have access to the WiNG CLI and GUI and cannot view running-config.

Per User Preferences Settings

Set user preferences from the admin menu. To access your user preference, select **admin > Settings**. The system displays the list of per user preferences.

From the **User Preferences** window, you can select **pagination**, **Auto-refresh interval (in-seconds)**, and **Logs line count**.

Pagination

Number of entries per page in the grid.

Auto-refresh interval (in-seconds)

Time for the device to refresh automatically. The minimum time is 5 seconds and the maximum time is 1 hour.

Logs line count

Number of lines displayed in diagnostic logs.

1. To change pagination date, type the number of entries in the pagination field or use the numeric up and down arrows to modify the number of entries.
2. To change the auto-refresh interval time, type the number of seconds in the auto-refresh field or use the numeric up and down arrow to adjust the time.
3. To change logs line count, type of number of line you want to see displayed in the diagnostic logs screen or use the numeric up and down arrow to adjust the logs line count.
4. Select **Apply** to commit to the user preferences settings.
5. Select **Save** to commit and save your user preferences settings.



Note

If you select only **Apply**, your settings will not be saved.

Remote Servers Settings

You can set your file transfer protocol (FTP), secure file transfer protocol (SFTP), and trivial file transfer protocol (TFTP) settings on the remote server settings menu. You can add up to 4 servers with username and password, with an option to validate the server connection. You can only set one server as the default server.

The [tech support file](#) is stored in the location selected in the remote server settings.

Protocol

Protocol settings for your network. You can select between FTP, SFTP, and TFTP

Hostname/IP

Server address.

Port

Port number assigned by default based on the protocol selected.

Username

Login credential required to access the protocol on the remote server.

Password

Security credential required to access the protocol on the remote server.

Access and configure the remote server settings from the admin menu.

1. Select **admin > Settings**. The system displays the remote servers settings.
2. Select **Add** to add a new remote server protocol and configure protocol settings. The system displays a new field for protocol settings.
3. Select **FTP, SFTP, or TFTP** from the protocol drop-down.

The port number is automatically assigned based on your protocol selection,

4. Type the host name or the IP address in the **Hostname/IP** field.
5. Assign username and password.
6. Select **validate connectivity** from action.

The system displays a connection validated successfully message.

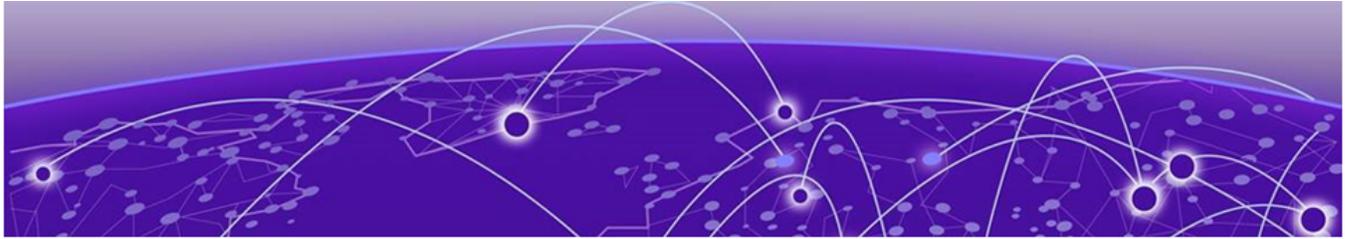
7. Select **Apply** to commit to the remote server settings.
8. Select **Save** to commit and save your remote server settings.
9. Select protocol to assign a remote server setting for your network.
10. Select **Save**.
11. To delete a remote server protocol, select the  from the action menu, and select **Save**.

The protocol is deleted and remote server protocol selection is saved.

Related Topics

[Tech Support](#) on page 64

[Logs](#) on page 65



System Dashboard

[Add a Custom Dashboard on page 22](#)

[Edit or Delete a Selected Dashboard on page 22](#)

Learn how you can use the system dashboard screen on the NOVA Graphical User Interface (GUI).

Site tree display

The **Dashboard** screen displays the **System** dashboard by default. You can monitor your network activity and performance on the system dashboard by including widgets. It can help you to proactively monitor and troubleshoot your network. The system dashboard is displayed as multiple graphical widgets. Navigate to the sites based on site location and select a particular site to view all the devices managed in that particular site.



Note

WiNG NOVA GUI comes installed with a default system dashboard. The default system dashboard is persistent after system restarts and software upgrades, and cannot be deleted or modified.

Customize the system dashboard and add additional dashboards with custom layouts using the unique set of dashboard widgets. The system supports a maximum of 16 dashboards.

The free-form dashboard can have a maximum of 6 widgets. The system dashboard widgets are classified into the type of data they access:

- Device inventory indicating the status of number of online and offline devices
- Device type distribution metrics for number of online and offline devices
- Device status distribution between the sites with their online or offline status
- Threat levels for each site based on the intensity of the threat ranging from level 1 to 5, with 1 being the lowest and 5 being the highest
- SmartRF channel distribution for the sites that have configured SmartRF policy
- Channel traffic index utilization based on the WLAN radio

Combine widgets from any of the categories to create one or more unique dashboards.

Related Topics

[Add a Custom Dashboard on page 22](#)

[Edit or Delete a Selected Dashboard on page 22](#)

Add a Custom Dashboard

Learn how to add a custom dashboard using the dashboard widget.

About This Task

You can add a custom dashboard or create a new dashboard using the dashboard widgets to monitor your network performance and organize your network data.

Procedure

1. From the default dashboard, select the plus sign.
The system displays the **Add dashboard** tab.

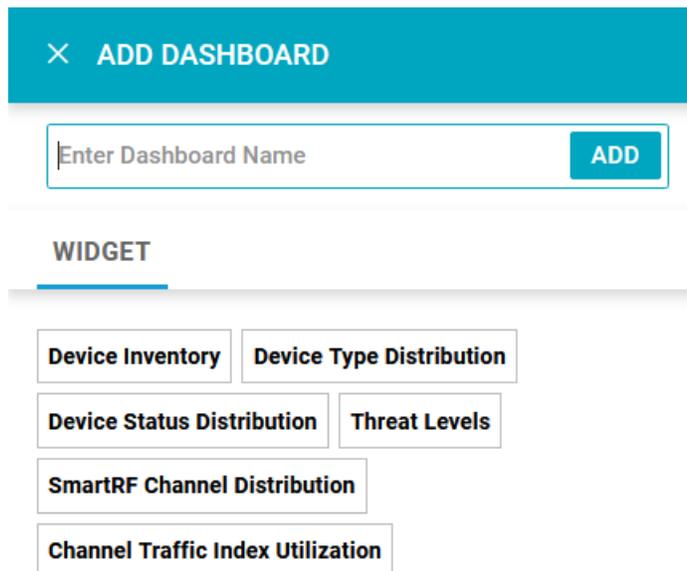


Figure 2: Add dashboard widget options

2. Type a dashboard name in the **Name** field.
3. Drag and drop a widget onto the dashboard.
4. Select **Save**.

The custom dashboard is saved.

Edit or Delete a Selected Dashboard

Details about how to edit or delete a selected dashboard.

About This Task

You can customize the default dashboard views to fit your network's analytic requirements, such as monitoring the distribution, component threat levels, and device performance.

Procedure

1. From the **Dashboard** screen, select a dashboard.



Note

You cannot edit the default dashboard.

2. Select the pencil icon to edit the selected dashboard.

× EDIT DASHBOARD

Enter Dashboard Name

WIDGET

Device Inventory Device Type Distribution

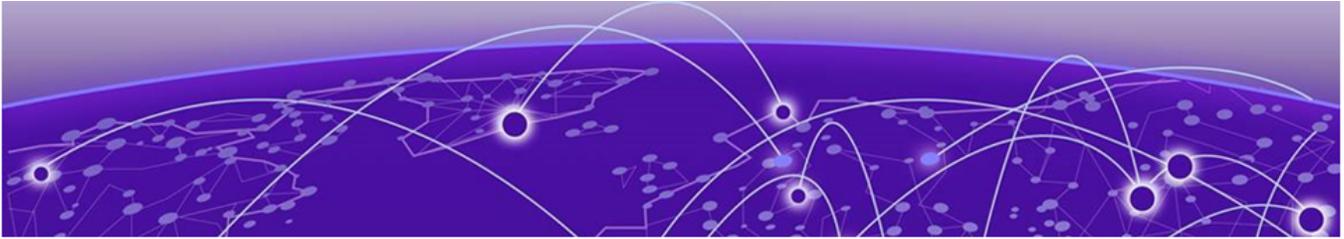
Device Status Distribution Threat Levels

SmartRF Channel Distribution

Channel Traffic Index Utilization

Figure 3: Edit dashboard widget options

3. Drag and drop the widgets onto the dashboard.
4. To delete a widget element from the dashboard, select the × icon on the dashboard widget.
5. Select **Save**.
The system displays a Dashboard Saved Successfully message.
6. To delete a custom dashboard, select the × next to the dashboard name on the main **System Dashboard** screen.
7. Select **Save**.
The system displays a Dashboard Saved Successfully message.



Slide-in Device Info

Details about the slide-in device information panel on the NOVA UI.

Slide-In Device Info Details Dashboard

The slide-in device info panel provides details and statistics about the controller. To access the slide-in info panel, hover your mouse pointer over the middle right corner on the **Dashboard** screen.

The **Details** panel displays the following information:

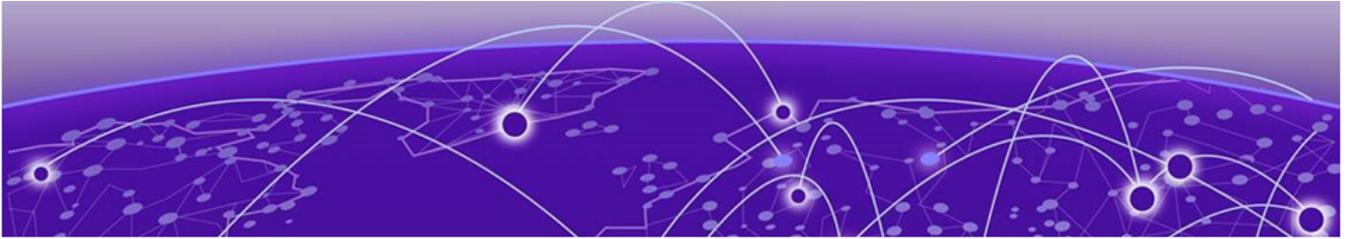
- **Device.** Name is determined based on the device selected in the dashboard
- **Hostname.** The device hostname is displayed in the following format: `device name - six digit numerical identifier`
- **Version.** Current firmware version running on the device
- **Model.** Official device model name
- **MAC.** Unique media access control address assigned to the controller
- **Serial number.** Unique identified assigned to the hardware component associated with the controller
- **Up time.** Number of days, hours, and minutes the device has been operational

Slide-In Device Info Adoption Dashboard

The slide-in device adoption dashboard provides information about controllers that are adopted by other controllers or NOC. To access the slide-in adoption panel information, hover your mouse pointer over the middle right corner on the **Dashboard** screen.

The **Adoption** panel displays the following information:

- **Type.** Controller type
- **System Name.** Controller name
- **MAC Address.** MAC address of the adopted device
- **MiNT Address.** MiNT address of the adopted device
- **Time.** Time since the device was adopted by a controller



Cluster

Details about cluster dashboard.

The cluster dashboard provides centralized management to configure all cluster members from any one member. The NOVA UI **Cluster** dashboard displays cluster feature and details about all the cluster members. The following read-only information is available in the **Cluster** dashboard:

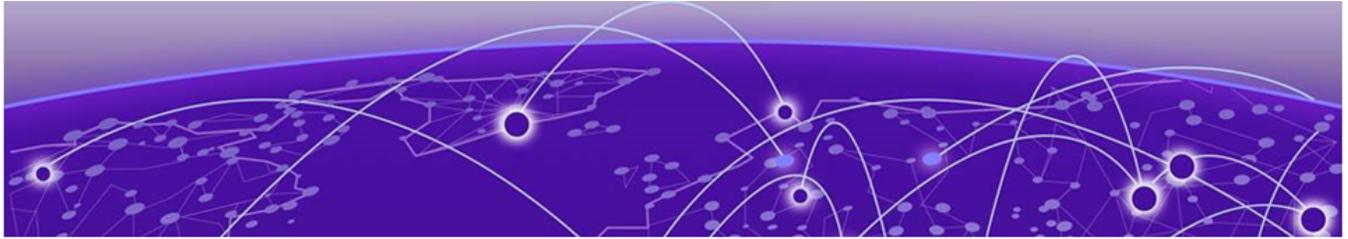
The screenshot displays the Cluster dashboard for a cluster named JERICHO. At the top, it shows the cluster name, the device type VX9000, and the user admin Superuser. Below this, the 'Members (1)' section contains a table with the following data:

HOSTNAME	SITE	ROLE	MODE	DEVICE TYPE	MAC	LAST SEEN
vx9000-3C6F18	default	master	active	vx9000	00-8C-29-3C-6F-18	28-05-2021 11:53:27

Below the members table are two history sections: 'Cluster History' and 'Device History'. Both sections show three entries for the device vx9000-3C6F18, each with a green checkmark and a timestamp of '1 Months Ago'. The first two entries indicate 'No configured standby members, stay active' with MAC address 00-0C-29-3C-6F-18. The third entry indicates 'Member 12.3C.6F.18 joined' with MAC address 00-0C-29-3C-6F-18.

Figure 4: Cluster dashboard

Members	List of cluster members within a cluster. Details include: <ul style="list-style-type: none"> • Hostname • Site • Role • Mode • Device Type • MAC • Last Seen
Cluster History	History of all devices in a cluster
Device History	History of a particular device within a cluster



Site

[Add a Site on page 28](#)

[Edit Site Basic Configuration on page 28](#)

[Edit Site Policies Configuration on page 29](#)

[Delete a Site on page 30](#)

Use sites to define boundaries for fast roaming and session mobility without interruption. Manage sites from **Site** option.

The site configuration screen lists all the available sites. You have to option to view site name, location, timezone, country, and take action on adding, editing, or deleting the site.

You can also use the main sites screen to search, download, refresh, and view other site information. The add, search, download, custom column, and refresh functionality are located on the top corner of the **Site** window.

Other Site configurations include:

Search

Type a site criteria such as site name, location, timezone, country in the search field to display all sites fulfilling the criteria.

Download

Use the  icon to download all displayed sites as a .csv file.

1. Select  > **CSV - All Rows**.
2. Select site action. You can choose to **Open with** or **Save File** to your local machine.
3. Select **OK**.

Columns

Customize the site columns displayed on the site list screen.

1. Select the  icon to select the columns.
2. Select **Select All** or select the columns individually from the options.

Refresh

Select the  icon to view the most updated version of the screen.

Related Topics

[Add a Site](#) on page 28

[Edit Site Basic Configuration](#) on page 28

[Delete a Site](#) on page 30

Add a Site

About This Task

To add a site to WiNG network:

Procedure

1. Select **Site** and  .
The **Add site** window opens.
2. Configure the following site parameters:

Table 4: Site parameter

Field	Description
Name	Determines the name of the site
Country	Define the regulatory country for the site. The regulatory domain of the AP must match the Country setting for the site. This field provides automatic search capabilities. Begin typing in the field to display the country
Copy From	Select copy site data from an existing site to copy information from an existing site. Select a site from the drop-down. Add a Site Name. The country is determined by default based on the copy site field.

3. Select **Add**.
The **Basic** screen opens.

Related Topics

[Edit Site Basic Configuration](#) on page 28

[Edit Site Policies Configuration](#) on page 29

[Delete a Site](#) on page 30

Edit Site Basic Configuration

About This Task

After a site is created, you can edit the basic configuration settings. To get started:

Procedure

1. Go to **Site**.
2. Select a site from the sites list.
The system displays the **Basic Configuration** screen.
3. Basic configuration settings:

Field	Description
Site Name	Non-editable field
Location	Physical location of the city where the site is situated
Contact	Site owner contact information
Time Zone	Drop-down to select the timezone for the site
Country	Country where the site is located
Address	Select the address picker icon to select Allow or Don't Allow on your computer's laptop settings to automatically pick the site location. Alternatively, select the address picker and manually search for the site address

4. Site tree configuration settings:

Field	Description
Country	Select the country from the drop-down list
City	Select the city from the drop-down list
Region	Select the region from the drop-down list
Campus	Select the campus from the drop-down list

5. After creating the site details, select **Apply** to commit the changes.
6. Select **Save** to commit and save the basic configuration settings.



Note

If you do not select **Save**, the basic configuration settings that you modified will not be saved when you move away from the **Basic Configuration** screen.

Related Topics

[Add a Site](#) on page 28

[Edit Site Policies Configuration](#) on page 29

[Delete a Site](#) on page 30

Edit Site Policies Configuration

About This Task

After a site is configured, you can modify site policies. To get started:

Procedure

1. Go to **Site**.
2. Select a site from the sites list.
The system displays the **Basic Configuration** screen.
3. Select the **Policies** tab.
Policies settings:

Field	Description
SmartRF Policy	Select the SmartRF policy for the site from the drop-down
NSight Policy	Select the NSight policy for the site from the drop-down
WIPS Policy	Select the WIPS policy for the site from the drop-down
Sensor Policy	Select the sensor policy for the site from the drop-down

4. Select **Apply** to commit to the changes.
5. Select **Save** to commit and save the policies changes.
The system displays a request completed successfully message.

Related Topics

- [Add a Site](#) on page 28
- [Edit Site Basic Configuration](#) on page 28
- [Delete a Site](#) on page 30

Delete a Site

About This Task

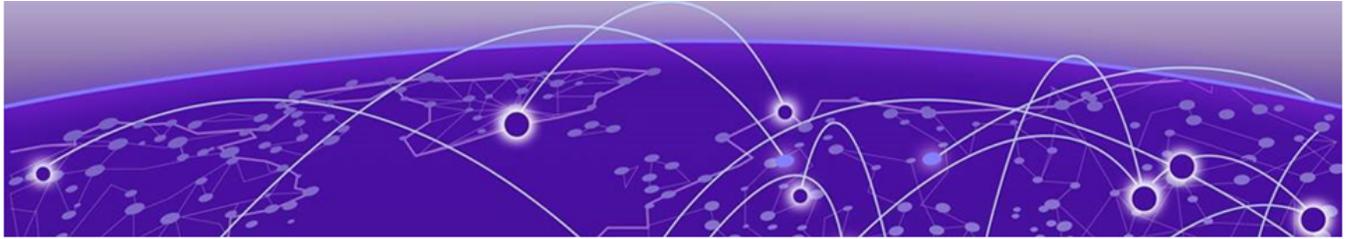
After a site is created, you can delete a site. To get started:

Procedure

1. Go to **Site**.
2. To delete a site, select the  icon from the action toolbar.
The system displays a delete confirmation message. Select **Delete**.

Related Topics

- [Add a Site](#) on page 28
- [Edit Site Basic Configuration](#) on page 28
- [Edit Site Policies Configuration](#) on page 29



Devices

[View Device Basic Info on page 31](#)

[Remote CLI from Device Configuration on page 32](#)

View the list of devices available in a site, list of online and offline devices, and device information. You can access the remote CLI for active devices.

Related Topics

[Remote CLI from Device Configuration on page 32](#)

View Device Basic Info

About This Task

You can view the device basic information on the **Devices** screen.

Procedure

1. Go to **Devices**.
2. The following information is available on the **Devices** basic info screen:

Field	Description
Host Name	Device host name
Site	Device site location
Status	Device status. An online device has a green indicator and an offline device has a red indicator
Mac Address	Device mac address
IPv4/v6 Address	Device IPv4 or IPv6 address
IP Address	Device IP address
Uptime	Amount of time for which the device has been running
Firmware Version	WiNG software version running on the device
Profile Name	Name given to the selected settings of the device

3. To go back to the **Basic Info** screen or to the main option, select the site name from the screen banner navigation.

Related Topics

[Devices](#) on page 31

[Remote CLI from Device Configuration](#) on page 32

Remote CLI from Device Configuration

About This Task

You can open remote CLI for active devices from the **Devices** configuration screen.

Procedure

1. Select **Devices**.
2. Select an online device from the device list.
3. Select the remote CLI  icon from the **Action** toolbar.



Note

The remote CLI icon is enabled only when the device status is active. A green icon against the device name indicates online status. If the device is offline, it is indicated by a circular red icon.

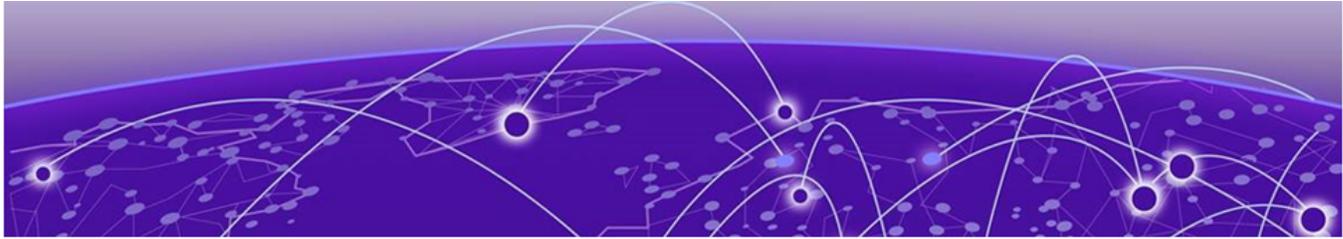
A new remote CLI session opens.

4. Type the login credentials to access the remote CLI session.
5. Select the  icon to close the remote CLI session.

Related Topics

[Devices](#) on page 31

[View Device Basic Info](#) on page 31



Wireless Configuration

[Add Wireless Network](#) on page 33

[Wireless Network Basic Configuration](#) on page 34

[Wireless Network Security Configuration](#) on page 35

You can configure all wireless LAN details using wireless configuration. View wireless LAN name, status, SSIDs, encryption type, authentication information, and number of VLANs. Manage two or more devices from your sites using the wireless LAN configuration. Access it from **Configure > Wireless**.

Access the freeform search to find wireless LANs, download configuration details as a .csv file, customize and view available columns, and take actions from the wireless configuration dashboard.

Related Topics

[Add Wireless Network](#) on page 33

[Wireless Network Basic Configuration](#) on page 34

[Wireless Network Security Configuration](#) on page 35

Add Wireless Network

About This Task

Add new wireless LAN and configure wireless LAN or copy from existing LAN configuration to manage new wireless LANs.

Procedure

1. Go to **Configure > Wireless**.
2. Select **Add**.

Type the following field details:

Field	Description
Wireless Name	Name for the wireless you need to configure and manage
SSID (Service Set Identifier)	Network's name

3. Select the **Copy From** checkbox and select from existing WLANs to copy the configuration settings.
4. Select **Add**.
5. The basic configuration dashboard opens. For more details, see [Wireless Network Basic Configuration](#) on page 34.

Related Topics

[Wireless Configuration](#) on page 33

[Wireless Network Basic Configuration](#) on page 34

[Wireless Network Security Configuration](#) on page 35

Wireless Network Basic Configuration

About This Task

Add wireless network basic configuration details or edit details for existing WLANs.

Procedure

1. Go to **Configure > Wireless**.
2. Select the pencil icon from the action menu.
The system displays the basic configuration dashboard.
3. Use the WLAN configuration slider to apply or remove the configuration settings.

Table 5: WLAN configuration options

Field	Description
Name	Name provided when you created the wireless network. This field cannot be edited
SSID	Network's name provided when adding the wireless network. This field cannot be edited
Description	WLAN description. Type up to 30 words
QoS policy	Outgoing network traffic. Default option is selected
Bridging mode	Select mode local or tunnel from the drop-down
Bonjour gateway discovery policy	Select a policy from the drop-down to help user's discover the wireless network

The broadcast SSID and broadcast probe response are selected by default. You have the option to select or remove DHCP option82 and DHCPv6 LDRA.

4. Use the fast roaming check box options to select or remove fast roaming options.
Fast roaming options include:
 - PMK caching
 - Opportunistic PMK caching
 - Pre-authentication
 - Fast BSS transition
5. Use the **client traffic** slider to power on or power off client-to-client traffic.
6. Set the max firewall sessions between 10 and 10,000.
7. Select access policies from the association ACL drop-down and the captive portal policy drop-down.
8. Set firewall policies for IP inbound ACL and outbound ACL.

9. Select the projected management frames (PMF).

Table 6: PMF parameters

Parameter	Description
Mode	Select optional or mandatory
SA query timeout	Select a number between 1 to 10
SA query attempts	Select between 100 to 1000 milliseconds

10. Use the radio resource management (RRM) slider to apply or remove settings.
 - a. Select or remove channel report and TPC report.
 - b. Use the agile multi-band operation slider to apply to remove multi-band configuration.
11. Apply shutdown criteria.

Field	Description
Critical Resource Name	Type a name for shutdown criteria

Use the slider option for applying or removing unadoption, wired link loss, meshpoint loss, critical resource configurations.

12. Configure VLAN assignment.
 - a. Select **Single VLAN** for configuring one VLAN and type the VLAN number in the **VLAN** field.
 - b. Select **VLAN Pool** to configure multiple VLANs.
 - i. Type VLAN number and the maximum number of wireless clients.
 - ii. Select  to delete a VLAN.
13. Select **Save** to commit and save wireless configuration settings.

Related Topics

[Wireless Configuration](#) on page 33

[Add Wireless Network](#) on page 33

[Wireless Network Security Configuration](#) on page 35

Wireless Network Security Configuration

About This Task

Configure a wireless network's security details.

Procedure

1. Go to **Configure > Wireless**.
2. Select a wireless network and navigate to the **Security** tab.

3. Configure authentication information.

Table 7: Authentication details

Authentication option	Description
Select authentication	Select an authentication method from the drop-down. You cannot configure AAA policy and reauthentication if you select PSK/None
AAA policy	Select the AAA policy for the site from the drop-down
Reauthentication	Type between the range 30 to 86400

4. Configure encryption settings.

Table 8: Encryption details

Encryption option	Description
Select encryption	Select from the encryption drop-down

You can select from 8 available encryption types. The encryption details are determined based on the encryption type selection.

Table 9: Encryption options

Encryption type	Details
TKIP-CCMP	Set a pre-shared key that is either 64 HEX or 8-63 ASCII characters. Select HEX or ASCII based on the pre-shared key
WEP 128	Generate keys that are 4 to 32 characters long in the Generate Keys field and select Generate . 4 keys are generated. The keys uses 26 HEX or 13 ASCII characters. <ul style="list-style-type: none"> a. Modify the key name in the field next to the key number. b. Select HEX or ASCII from the drop-down based on the number of key characters. c. Select Transmit Keys from the 4 available key choices.
WEP 64	Generate keys that are 4 to 32 characters long in the Generate Keys field and select Generate . 4 keys are generated. The key uses 10 HEX or 5 ASCII characters. <ul style="list-style-type: none"> a. Modify the key name in the field next to the key number. b. Select HEX or ASCII from the drop-down based on the number of key characters. c. Select Transmit Keys from the 4 available key choices.
Open	Open encryption. Not secured or protected

Table 9: Encryption options (continued)

Encryption type	Details
CCMP	Set a pre-shared key that is either 64 HEX or 8-63 ASCII characters. Select HEX or ASCII based on the pre-shared key
Key guard	<p>Generate keys that are 4 to 32 characters long in the Generate Keys field and select Generate. 4 keys are generated. The keys uses 26 HEX or 13 ASCII characters.</p> <ol style="list-style-type: none"> Modify the key name in the field next to the key number. Select HEX or ASCII from the drop-down based on the number of key characters. Select Transmit Keys from the 4 available key choices.
GCMP256	Set a pre-shared key that is either 64 HEX or 8-63 ASCII characters. Select HEX or ASCII based on the pre-shared key
WEP128 + Key guard	<p>Combination of WEP128 and key guard encryption settings. Generate keys that are 4 to 32 characters long in the Generate Keys field and select Generate. 4 keys are generated. The keys uses 26 HEX or 13 ASCII characters.</p> <ol style="list-style-type: none"> Modify the key name in the field next to the key number. Select HEX or ASCII from the drop-down based on the number of key characters. Select Transmit Keys from the 4 available key choices.

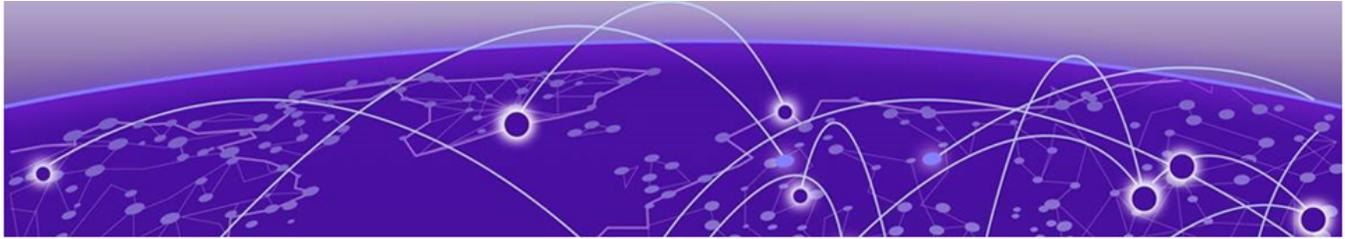
5. Select **Save** to apply wireless network security settings.

Related Topics

[Wireless Configuration](#) on page 33

[Add Wireless Network](#) on page 33

[Wireless Network Basic Configuration](#) on page 34



Profiles

[Add Profile on page 39](#)

[Create Basic Profile Configuration on page 39](#)

[Manage Profile Adoption Configuration on page 42](#)

[Set Controller Power Configuration on page 43](#)

[Profile Network Configuration on page 44](#)

[Profile Policies Configuration on page 58](#)

You can assign common set of configuration parameters and policies to controllers, service platforms, and access points. Profiles can be used to assign shared or unique network, wireless and security parameters within a large, multi-segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support.

Controllers and service platforms support both default and user defined profiles implementing new features or updating existing parameters to groups of controllers or access points. All WiNG OS supported access point models support a single profile that is shared amongst multiple access points. The central benefit of a profile is the ability to update access points collectively without having to modify individual configurations.

A profile allows access point administration across large wireless network segments. Changes made to a profile are automatically inherited by all member access points. You can override the profile settings at the device level. It is important to remember that individual access points with overrides applied no longer share the profile based configuration previously deployed. These devices require careful administration, as they no longer can be tracked as profile members. Their customized configurations overwrite their profile assignments until the profile can be re-applied to the access point. Each access point model is automatically assigned a default profile. The default profile is available within the access point's configuration file. Default profiles are ideal for single-site deployments where several access points may need to share a common configuration.



Note

Default profiles are used as pointers for an access point's configuration, not just templates from which the configuration is copied. Therefore, if a change is made in one of the parameters in a profile, the change is reflected across all access points using that profile.

Related Topics

[Add Profile on page 39](#)

[Create Basic Profile Configuration on page 39](#)

[Manage Profile Adoption Configuration on page 42](#)

[Set Controller Power Configuration](#) on page 43

[Profile Network Configuration](#) on page 44

[Profile Policies Configuration](#) on page 58

Add Profile

About This Task

Add profile information for access points and controllers.

Procedure

1. Go to **Configure > Profiles > Add**.
The **Add Profile** dashboard opens.
2. Set profile name parameters:

Field	Description
Profile Name	Set a unique profile name. The profile name must not contain any spaces
Select Device Type	Select a device from the device type drop-down. A list of all available devices are displayed
Copy From	Select copy from and select an existing profile from the drop-down to copy profile configuration information. Only profile configuration information is copied. The profile name and device type remains unique

3. Select **Add**.
The system displays the **Basic** dashboard.

Related Topics

[Profiles](#) on page 38

[Create Basic Profile Configuration](#) on page 39

[Manage Profile Adoption Configuration](#) on page 42

[Set Controller Power Configuration](#) on page 43

Create Basic Profile Configuration

About This Task

Set up basic configuration for a new profile or an existing profile.

Procedure

1. For new profile basic configuration, [Add Profile](#) on page 39.
2. For editing existing profiles basic configuration, go to **Configure > Profiles > Profile Name**.

Alternatively, select  to navigate to the **Basic Configuration** dashboard.

3. Set basic configuration parameters:

Field	Description
Name	Cannot be edited. The name is set when adding a new profile
Device Type	Access point or controller
Area	Device location
Floor	Device floor identification
Floor No.	Floor number drop-down

4. Select **Save** to apply and save all basic configuration changes.
A `Profile Saved Successfully!` message is displayed.

Related Topics

- [Add Profile](#) on page 39
- [Manage Profile Adoption Configuration](#) on page 42
- [Set Controller Power Configuration](#) on page 43

Network Tab Profile Configuration

About This Task

Set network tab profile (NTP) configuration.

Procedure

1. Go to **Configure > Profiles > Profile Name**.
2. Set [Create Basic Profile Configuration](#) on page 39 parameters.
3. Add NTP parameters:
 - a. Select **Add** on **NTP Configuration** dashboard.
 - b. The **NTP** dashboard opens.

Figure 5: NTP settings dashboard

Table 10: NTP settings

Field	Description
Server IP	Type NTP server IP address
Server Hostname	For setting a server hostname, select Server IP and type a hostname
Key number	Type a number between 1 to 65534
Key	Type a password
Version	Select a version between 0 and 4
Minimum Polling Interval	Select a polling interval from the drop-down. The minimum polling intervals are 64, 128, 256, 512, and 1024
Maximum Polling Interval	Select a polling interval from the drop-down. The maximum polling intervals are 1024, 2048, 4096, and 8192
Preferred	Select Preferred to make the current NTP settings into your preferred choice
Autokey	Select Autokey to assign an automatic NTP key

- c. Select **Add**.

The status routes server is added with NTP settings.

4. Select  to edit NTP configuration settings.
5. Select **Apply** to save the configuration changes.

Related Topics

[Create Basic Profile Configuration](#) on page 39

[Add Profile](#) on page 39

[Profiles](#) on page 38

Manage Profile Adoption Configuration

About This Task

An access point, a controller, or a service platform uses the adoption process to discover available access points or peer controllers and service platforms. Adoption configurations are used to establish an association and provision the requesting device. Configure and support adoption settings within a profile and apply the settings to other access points supported by the profile.

At adoption, an access point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available access points, controllers, and service platforms. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

Procedure

1. Go to **Configure > Profiles > Profile Name**.
2. Navigate to **Adoption** tab.
3. Configure the controller settings:

Field	Description
VLAN	Type or use the number field to define a VLAN that the access point's associating controller can reach. Set VLANs between 1 and 4,094
Group	Set an optimal group for the access point's adoption. The name of the preferred group cannot exceed 64 characters

4. Add **Controller Hostnames**. Select **Add** from the controller hostnames area.

Table 11: Controller hostnames parameters

Field	Description
Host (IP Address)	Provide the numerical IP address. Select Host (IP Address) to set a hostname. Type a hostname. A hostname cannot exceed 64 characters
Pool	Use the pool field to set a pool of either 1 or 2. The target controller or service platform belongs to this pool
Routing Level	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1
IPSec GW (IP Address)	Select the numerical IP address. Select IPSec GW (IP Address) to set an administrator defined hostname of the adopting controller resource

Table 11: Controller hostnames parameters (continued)

Field	Description
IPSec Secure	Select this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is not selected by default
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client
Force	Select this setting to create a forced link between an access point and adopting controller, even when not necessarily needed. This setting is not selected by default

5. Select **Add**.
The controller hostname settings is added to the **Adoption** dashboard.
6. Select **Save** to save the controller profile adoption settings.
7. Select  or  to edit or delete an existing controller settings.

Related Topics

- [Profiles](#) on page 38
- [Add Profile](#) on page 39
- [Create Basic Profile Configuration](#) on page 39
- [Set Controller Power Configuration](#) on page 43

Set Controller Power Configuration

About This Task

Use the **Power Configuration** dashboard to set or override one of two power modes (802.3af or Automatic) for a managed controller. When Automatic is selected, the controller safely operates within available power. After the power configuration is determined, the controller configures its operating power characteristics based on its radio model and power configuration.

Procedure

1. Go to **Profiles > Profile Name**.
The **General** dashboard opens.
2. Go to **Power Configuration**.
3. Use the **Power Mode** drop-down to set or change the Power Mode Configuration on the selected controller.
When a controller is powered on for the first time, the system determines the power budget available to the controller. The Automatic setting automatically determines the best power configuration based on the available power budget. Automatic is the default setting. If you select 802.3af, the access point assumes 12.95 watts are available. If the mode is changed, reset the controller to implement the change.

Related Topics

- [Profiles](#) on page 38

[Add Profile](#) on page 39

[Create Basic Profile Configuration](#) on page 39

[Manage Profile Adoption Configuration](#) on page 42

Profile Network Configuration

Before defining a profile's network configuration, refer to the following deployment guidelines to ensure that the profile configuration is effective:

- Administrators need to route traffic between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception.
- Each time there is a change to a static route, an administrator must manually make changes to reflect the new route. If a link goes down, even if there is a second path, the router would ignore it and consider the link down.
- Static routes require extensive planning and have a high management overhead. The more routers in a network, the more routes need that to be configured. If you have N number of routers and a route between each router is needed, then you must configure $N \times N$ routes. Thus, for a network with nine routers, you'll need a minimum of 81 routes ($9 \times 9 = 81$).

Related Topics

[Set a Profile's DNS Configuration](#) on page 44

Set a Profile's DNS Configuration

About This Task

Domain Naming System (DNS) is a hierarchical naming system for resources connected to the internet or a private network. Primarily, DNS resources translate domain names into IP addresses. If one DNS server doesn't know how to translate a particular domain name, it asks another one until the correct IP address is returned. DNS enables access to resources using human friendly notations. DNS converts human friendly domain names into notations used by different networking equipment for locating resources.

Procedure

1. Go to **Configure > Profiles**.
2. Select a network from the network name list and navigate to **Network**.
3. Select **DNS**.

The system displays the DNS dashboard.

4. Configure DNS settings:

Field	Description
Domain Name	Provide the default Domain Name used to resolve DNS names. The name cannot exceed 64 characters
Domain Lookup	Select DNS Lookup to enable DNS. When selected, human friendly domain names are converted into numerical IP destination addresses. The DNS Lookup is selected by default
IPv4 Forward requests	Select this option to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by local DNS resources. This feature is not selected by default
	Add servers. Provide the default domain name used to resolve IPv4 DNS names. When an IPv4 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. A maximum of three entries are permitted. Use the Action option to delete entries
IPv6 Forward requests	Select this option to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by local DNS resources. This feature is not selected by default
	Add servers. Provide the default domain name used to resolve IPv6 DNS names. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. A maximum of three entries are permitted. Use the Action option to delete entries

5. Select **Save** to apply and save the DNS configuration changes.

Set a Profile's ARP Configuration

About This Task

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions. When an incoming packet destined for a host arrives, ARP is used to find a physical host or MAC address that matches the IP address.

ARP looks in its cache and, if it finds the address, provides it so the packet can be converted to the right packet length and format and sent to its destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format on the LAN to see if a device knows it has that IP address associated with it. A device that recognizes the IP address as its own returns a reply indicating it. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

Procedure

1. Go to **Configure > Profiles**.
2. Select a **Profile Name** from the list.
3. Select **Network > ARP**.
4. Select **Add**.
The ARP **Basic Configuration** dashboard opens.
5. Configure ARP settings:

Field	Description
Virtual interface	Select a virtual interface for an address requiring resolution with the controller, service platform or access point
IP address	Define the IP address used to fetch a MAC Address recognized on the wireless network
MAC address	Displays the target MAC address subject to resolution. This is the MAC used for mapping an IP address to a MAC address recognized on the network
Type	Specify the device type the ARP entry supports. The options are Dhcp server, host, and router

6. Select **Add** to save changes.

Set a Profile's L2TP V3 Configuration

About This Task

L2TP V3 is an Internet Engineering Task Force (IETF) standard used for transporting different types of layer 2 frames in an IP network and profile. L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables controllers, service platforms, and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WiNG managed devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. The access points support an Ethernet VLAN pseudowire type exclusively.



Note

A pseudowire is an emulation of a layer 2 point-to-point connection over a packet-switching network (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder must know the pseudowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.



Note

If connecting an Ethernet port to another Ethernet port, the pseudowire type must be Ethernet port. If connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be Ethernet VLAN.

Procedure

1. Go to **Configure > Profiles**.
2. Select a profile from the **Profile Name** list.
3. Select **Network > L2TP V3**.
The L2TP V3 **Basic Configuration** dashboard opens.
4. Configure L2TP V3 basic settings:

Field	Description
Hostname	Define a 64 character maximum hostname to specify the name of the host that sent tunnel messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP, and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host
Router ID	Set either the numeric IP address or the integer used as an identifier for tunnel AVP messages. AVP messages assist in the identification of a tunneled peer
Integer	Select IP Address from the Router ID drop-down to configure the IP address field
UDP listen port	Select this option to set the port used for listening to incoming traffic. Select a port from 1,024 to 65,535. The default port is 1701
Bridge tunnels	Select or deselect this option to enable or deactivate bridge packets between two tunnel end points. This setting is unselected by default

5. Select the **Logging** slider to configure logging settings:

Field	Description
Logging slider	Select this option to enable the logging of Ethernet frame events to and from bridge VLANs and physical ports on a defined IP address, host or router ID. This setting is grayed out by default
IP Address	Use a peer tunnel ID address to capture and log L2TP V3 events
Hostname	If not using an IP address for event logging, optionally use a peer tunnel hostname to capture and log L2TP V3 events
Router ID	If not using an IP address or a hostname for event logging, use a router ID to capture and log L2TP V3 events

6. Set **Tunnel** configuration:

Use the tunnel configuration settings to create or override a profile's L2TPv3 tunnel configuration at the device level.

- a. Select **Add** or existing L2TPv3 configuration. The **Basic Configuration** dashboard opens.

L2TPv3 tunnel basic configuration settings:

Field	Description
Name	Displays the name of each listed L2TPv3 tunnel assigned upon creation For new configuration, assign a name
Local IP Address	Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address
MTU	Displays the MTU size for each listed tunnel. The MTU is the size (in bytes) of the largest protocol data unit that the layer can pass between tunnel peers. The range is 128 to 1460
Tunnel Policy	Lists the L2TPv3 tunnel policy assigned to each listed tunnel
Router ID	Specifies the router ID sent in the tunnel establishment messages
Hostname	Lists the tunnel specific hostname used by each listed tunnel. This is the hostname advertised in tunnel establishment messages

Field	Description
Establishment Criteria	Specifies tunnel criteria between two peers
VRRP group	Select VRRP group between 1 and 255

b. Set **Peer** configuration settings:

Field	Description
ID	Set peer ID to 1 or 2 . If the peer is not specified, tunnel establishment does not occur. However, if a peer tries to establish a tunnel with this access point, it creates the tunnel if the hostname and/or Router ID matches
IP Address	Lists the IP address of the remote peer
Hostname	List the tunnel specific hostname used by the remote peer
Router ID	Specify the router ID sent in the tunnel establishment messages
Encapsulation (IP or UDP)	Select the IP option to enter the numeric IP address used as the destination peer address for tunnel establishment Select UDP encapsulation between 1,024 and 65,535. The default value is 1071
IPSec Secure/Gateway	Select this option to enable security on the connection between the access point and the Virtual Controller Specify the IP Address of the IPSec Secure Gateway
Action	Use the  option to delete an entry

c. Set the **Rate Limit** information:

Rate limit manages the maximum rate sent to or received from L2TPv3 tunnel members. Select **Add** to configure rate limit settings:

Field	Description
Session Name	Use the drop-down menu to select the tunnel session that will have the direction, burst size, and traffic rate settings applied
Direction	Select the direction for L2TPv3 tunnel traffic rate limit. Egress traffic is outbound L2TPv3 tunnel data coming to the controller, service platform or access point. Ingress traffic is inbound L2TPv3 tunnel data coming to the controller, service platform, or access point

Field	Description
Rate	Set the data rate (from 50 to 1,000,000 kbps) for egress or ingress traffic rate limit (depending on which direction is selected) for an L2TPv3 tunnel. The default setting is 5000 kbps
Max Burst Size	Set the maximum burst size for egress or ingress traffic rate limit (depending on which direction is selected) on a L2TPv3 tunnel. Set a maximum burst size between 2 to 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for L2TPv3 tunnel traffic. The default setting is 320 bytes
Background	Set the random early detection threshold in % for background traffic. Set a value from 1% to 100%. The default is 50%
Best Effort	Set the random early detection threshold in % for best effort traffic. Set a value from 1% to 100%. The default is 50%
Video	Set the random early detection threshold in % for video traffic. Set a value from 1% to 100%. The default is 25%
Voice	Set the random early detection threshold in % for voice traffic. Set a value from 1% to 100%. The default is 25%

d. Configure **Session** settings:

Field	Description
Name	Type a 31 character maximum session name. There is no idle timeout for a tunnel. A tunnel is not usable without a session and a subsequent session name. The tunnel is closed when the last session tunnel session is closed
Pseudewire ID	Define a pseudewire ID for this session from 1 to 4,294,967,295. A pseudewire is an emulation of a layer 2 point-to-point connection over a PSN. A pseudewire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network
Traffic Source Type	Select traffic type tunneled in this session (VLAN)
Traffic Source Value	Define a VLAN range to include in the tunnel session. Available VLAN ranges are from 1 to 4,094
Native VLAN	Select this option to provide a VLAN ID that will not be tagged in tunnel establishment and packet transfer

e. Select **Save** to apply **Tunnel** configuration settings.

f. Configure **Manual Session** settings. Select a manual session from the list or **Add**.

g. Configure or edit **Manual Session Basic Configuration** settings:

Field	Description
Name	Name for the manual session. You can define it or edit it
Tunnel IP address	Specify the IP address used as the tunnel source IP address. If not specified, the tunnel source IP address is selected automatically based on the tunnel peer IP address
Local session ID	Set the numeric identifier for the tunnel session between 1 to 63. This is the pseudowire ID for the session. This pseudowire ID is sent in session establishment message to the L2TP peer
Remote session ID	Define a remote session ID for this manual session from 1 to 4,294,967,295.
MTU	Define the session MTU as the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. The range is 128 to 1460.
IP address	Set the IP address of an L2TP tunnel peer. This is the peer allowed to establish the tunnel
Encapsulation	Select either IP or UDP as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes
UDP port	If UDP encapsulation is selected, use the UDP port drop-down to define the UDP encapsulation port. This is the port where the L2TP service is running. The range is 1,024 to 65,535. The default port is 1,701
Traffic source type	Select traffic type tunneled in this session (VLAN)
Traffic source value	Define the VLAN range (1 to 4,094) to include in the tunnel. Tunnel session data includes VLAN tagged frames
Native VLAN	Select Native VLAN to define the native VLAN that will not be tagged. The range is 1 to 4,094

h. Configure **Manual Session Cookie** settings. Select **Add** to configure cookie configuration:

Field	Description
Size	Set the size of the cookie field within each L2TP data packet. Options include 0, 4, and 8. The default setting is 0
Value 1	Set the cookie value's first word
Value 2	Set the cookie value's second word
End Point	Define whether the tunnel end point is local or remote

7. Select **Save** to apply all the settings and save it to the L2TP v3 configuration.

GRE Network Configuration

About This Task

GRE tunneling is configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over an IPv4 GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, access points map one or more VLANs to a tunnel. The remote endpoint is a userconfigured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. The access points can reach both the GRE peer as well as the RADIUS server using IPv4.

Procedure

1. Go to **Configure > Profiles**.
2. Select an access point from the profile name list.
3. Navigate to **Network > GRE**.
4. The GRE dashboard opens.
5. Slect **Add** to configure GRE settings:
 - a. Configure GRE **Basic Configuration** parameters:

Field	Description
Name	Define a GRE tunnel name for new configurations
Tunneled VLANs	Define the VLAN connected clients use to route GRE tunneled traffic within their respective WLANs
Native VLAN	Set a numerical VLAN ID (1 to 4,094) for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode

Field	Description
Native VLAN tagged	<p>Select this option to tag the native VLAN. The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs to. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is not available by default</p>

Field	Description
IPv4 MTU	Set an IPv4 tunnel's maximum transmission unit (MTU) from 900 to 1,476. The MTU is the largest physical packet size (in bytes) transmittable within the tunnel. Any messages larger than the MTU are divided into smaller packets before being sent. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. For IPv4, the overhead is 24 bytes (20 bytes IPv4 header + 4 bytes GRE Header), thus the default setting for an IPv4 MTU is 1,476
IPv6 MTU	Set an IPv6 tunnel's MTU from 1,236 to 1,456. The MTU is the largest physical packet size (in bytes) transmit able within the tunnel. Any messages larger than the MTU are divided into smaller packets before being sent. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. For IPv6, the overhead is 44 bytes (40 bytes IPv6 header + 4 bytes GRE header), thus the default setting for an IPv6 MTU is 1,456

- b. Configure **DSCP options**. Use the slider to enable or clear the DSCP options. Set the tunnel DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header.
- c. Configure **Peer** settings:

Field	Description
Peer Index	Assign a numeric index to each peer to help differentiate tunnel end points
Peer IP Address	Define the IP address of the added GRE peer to serve as a network address identifier

- d. Configure **Establishment Criteria** parameters:

Field	Description
Criteria	Select an establishment criteria from the criteria drop-down
VRRP group	Pick a group between 1 to 255

- e. Define **Failover** parameters. Use the **Failover** slider to configure failover settings. Select the failover option to periodically ping the primary gateway to assess its availability for failover support.

Field	Description
Ping interval	Set the duration between two successive pings to the gateway. Define this value in seconds from 1 to 250 seconds
Retries	Set the number of retry ping opportunities before the session is terminated between 1 to 10

- f. Select **Add** to save GRE basic configuration settings.
6. Select **Save** to apply GRE configuration parameters.

IGMP and MLD Snooping Configuration

About This Task

The Internet Group Management Protocol (IGMP) is used for managing IP multicast group members. Controllers and service platforms listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. On the wired side of the network, the controller or service platform floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

Procedure

1. Select **Configure > Profiles**.
2. Select an access point from the **Profile Name** list.
3. Navigate to **Network > IGMP/MLD**.
The **IGMP Snooping** dashboard opens.
4. Set the following IGMP Snooping parameters:

Field	Description
Snooping	Select this option to enable IGMP snooping. If grayed out, snooping on a per VLAN basis is also turned off. This feature is selected by default. If not selected, the settings under the bridge configuration are overridden. For example, if IGMP snooping is not selected, but the bridge VLAN is enabled, the effective setting is not enabled
Forward unknown multicast packets	Select this option to enable the forwarding of multicast packets from unregistered multicast groups. If grayed out, the unknown multicast forward feature is also not selected for individual VLANs. This setting is enabled by default

Field	Description
Fast leave	Select this option to remove a layer 2 LAN interface from IGMP snooping without initially sending IGMP group-specific queries to the interface. When receiving a group specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for all hosts on the network
Enable Querier	Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server and hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port
Version	Type the version to set the IGMP version compatibility to either version 1, 2, or 3. IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236, and IGMPv3 defined by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves over IGMPv2 by adding the ability to listen to multicast traffic originating from a set of source IP addresses exclusively. The default setting is 3
Query interval	Set the interval IGMP queries are made. This parameter is used only when the querier functionality is enabled. Define an interval value in seconds (1 to 18,000). The default setting is 60 seconds
Robustness variable	Sets the IGMP robustness variable. The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. Define a robustness variable from 1 to 7. The default robustness value is 2

Field	Description
Maximum response time	Specify the maximum interval (from 1 to 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. Only multicast packets are forwarded to radios present in the snooping table. For IGMP reports from wired ports, the controller or service platform forwards these reports to the multicast router ports. The default setting is 10 seconds
Timer expiry	Specify an interval in seconds (60 to 300) used as a timeout interval for other querier resources. The default setting is 60 seconds

5. Select **Save** to apply IGMP Snooping configuration settings.
6. Set **MLB Snooping** configuration.

MLD Snooping Configuration

About This Task

MLD (Multicast Listener Discovery) snooping enables a controller, service platform, or an access point to examine MLD packets and make forwarding decisions based on content. IPv6 devices used MLD to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform, or access point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

Procedure

1. Select **Configure > Profiles**.
2. Select an access point from the **Profile Name** list.
3. Navigate to **Network > IGMP/MLD**.

The **MLD Snooping** dashboard opens.

4. Set the following MLD Snooping parameters:

Field	Description
Snooping	Enable MLD snooping to examine MLD packets and make content forwarding for this profile. Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best effort reliability, just like IPv6 unicast. MLD snooping is not selected by default
Forward unknown multicast packets	Select this option to either enable or clear IPv6 unknown multicast forwarding. This setting is enabled by default

Field	Description
Enable Querier	Select this option to enable MLD querier on the controller, service platform, or access point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is not selected by default
Version	Define whether MLD version 1 or 2 is utilized as the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2
Query interval	Set the interval in which query messages are sent to discover device multicast group memberships. Set an interval in seconds (1 to 18,000). The default interval is 60 seconds
Robustness variable	Set a MLD IGMP robustness value (1 to 7) used by the sender of a query. The MLD robustness variable enables refinements to account for expected packet loss on a subnet. Increasing the robust count allows for more packet loss, but increases the leave latency of the subnetwork unless the value is zero. The default variable is 2
Maximum response time	Specify the maximum response time (from 1 to 25,000 seconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 10 seconds
Timer expiry	Specify an interval in seconds (60 - 300) used as a timeout interval for other querier resources. The default setting is 60 seconds

5. Select **Save** to apply all MLD Snooping configuration settings.

Profile Policies Configuration

About This Task

User defined profiles can be manually assigned or automatically assigned to access points using an AP Auto-Provisioning policy. User defined profiles should be utilized in larger deployments when groups of devices (on different floors, buildings or sites) share a common configuration. Each default and user defined profile contains policies and configuration parameters. Changes made to these parameters are automatically inherited by the devices assigned to the profile.

Configure profile policies parameters:

Procedure

1. Select **Configure > Profiles**.
2. Select an access point from the **Profile Name** list.

3. Navigate to **Policies**.

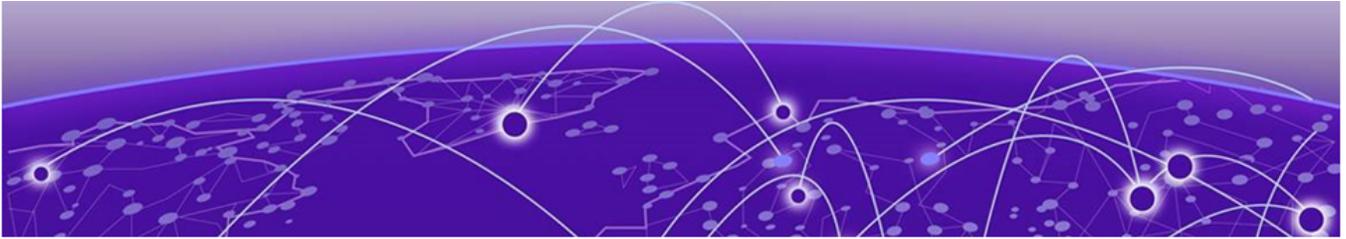
The **Policies** dashboard opens. A list of configurable policies are listed on the **Policies** screen.

Field	Description
Management Policy	Lists the name of Management policies applied to each listed profile. A management policy is a mechanism to allow or deny management access for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled or turned off as required for each policy
Firewall Policy	Displays an existing firewall policy, if any, assigned to each listed profile. Firewall policies can be assigned when creating or editing a profile
RADIUS Server Policy	Displays the name of the RADIUS Server policy applied to each listed profile. A RADIUS Server policy provides customized, profile specific, management of authentication data such as username and password. This setting is not selected by default
Event System Policy	Displays the name of the Event System policy applied to each listed profile. A Event System Policy allows the profile to capture system events and append them to a log file. This option is not selected by default
DHCPv4 Policy	Lists the name of the DHCPv4 Policy used with each listed profile. This option is not selected by default

4. Configure **Auto-Provisioning Policy** settings:

Field	Description
Auto-Provisioning Policy	Displays the Auto-Provisioning policy applied to this profile. At adoption, an AP solicits and receives multiple adoption responses. These adoption responses contain preference and loading policy information the AP uses to select the optimum controller or access point for adoption. By default, an Auto-Provisioning policy generally distributes AP adoption evenly amongst available adopters. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of this particular profile
Use NOC Auto-Provisioning Policy	Select this option to use the NOC's auto provisioning policy instead of the policy local to the controller or service platform. The NOC is an elected controller or service platform capable of provisioning all of its peer controllers, service platforms and adopted devices. The options are No, Yes, and Always. The default selection is No
Learn and Save Network Configuration	Select this option to enable allow the controller or service platform to maintain a local configuration records of devices requesting adoption and provisioning. This feature is enabled by default

5. Select **Save** to apply policies changes and configuration to the selected profile.

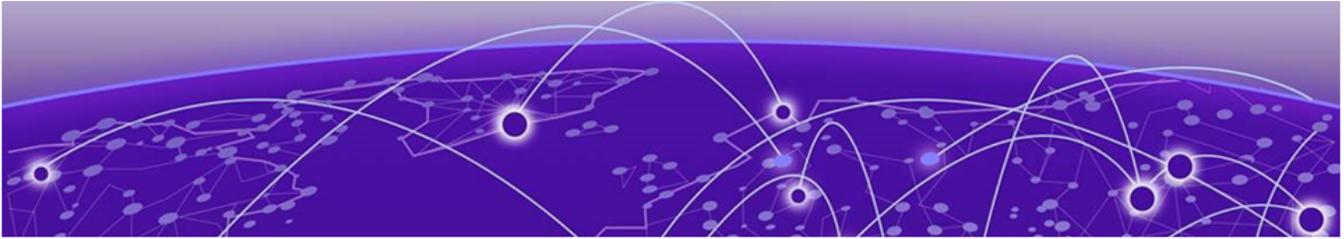


Clients

Details about clients screen.

The **Clients** screen display the list of all the sites managed by the device. The clients summary bar shows clients operating in 2.4 GHz, 5 GHz, 6 GHz and radios in the 2.4 GHz, 5 GHz, and 6 GHz frequency.

Use the **Clients** screen to manage all sites, client information for each site, add, edit, search, and download client site information.



Diagnostics

[System Info](#) on page 62

[Tech Support](#) on page 64

[Logs](#) on page 65

Details about sites and system diagnostics.

Diagnostic capabilities enable administrators to understand how devices are performing and troubleshoot issues impacting device performance. Performance and diagnostic information is collected and measured on controllers, service platforms, and access points for any anomalies potentially causing a key processes to fail.

Numerous tools are available within the **Diagnostics** menu. Some allow event filtering, some enable log views and some allow you to manage files generated when hardware or software issues are detected.

Diagnostic capabilities include:

- [System info](#)
- [Tech support](#)
- [Logs](#)

System Info

General System Info Diagnostics

The general system information diagnostics provides graphical representation of the system health, including, central processing unit (CPU) usage, memory usage, disk usage, temperature, fan speed, and RAID status.

CPU Usage

Real-time representation of CPU usage through a red line graph. Hover over the graph to view the CPU usage percentage.

Memory Usage

Real-time representation of memory usage through red line graph. Hover over the graph to view the memory usage percentage.

Disk Usage

Real-time representation of memory usage through red line graph. Hover over the graph to view the disk usage percentage.

Network Activity

Graphical representation of network activity for Tx, Rx, and dropped information. Select each option to apply or remove the information from the network activity graph.

Temperature

Line graph of device temperature.

Fan Speed

Line graph of fan speed for a device.

RAID Status

Status of physical drives.

- Red means device is offline
- Green means device is online
- Alarm
- Last checkin - time when device was last checked in
- Size - device drive size
- Type - device type
- State - device state

PSU Status

Read only information showing device location, status, and device type.

CDP Neighbors Diagnostics

CDP neighbors provides read-only information about device CDP diagnostics. Use the CDP device columns to view the following information:

- Device ID
- Platform
- Local interface
- Port ID
- Duplex
- Capabilities
- Advertised version
- IP address
- Native VLAN
- Version
- TTL

LLDP Neighbors Diagnostics

LLDP neighbors diagnostic provides read-only device LLDP information. Use the device LLDP column option to view the following information:

- Chassis ID
- Device ID
- Platform
- Capabilities
- Enabled capabilities
- Local interface
- Port ID
- Port description
- Management addresses
- TTL

Tasks Diagnostics

The task diagnostics is a read-only grid providing the following information:

- Name
- CPU %
- Memory %
- PID/PPID
- RSS size
- Status

View the per task graphs for CPU usage and memory usage as a line graph.

Tech Support

Create a tech support information collection session.

Tech Support Session

The tech support session read-only dashboard provides the following information:

Field	Description
Status	Running or completed
Session name	Name provided when starting the tech support session
Started by	User details
Type	Tech support type
Hosts	Controller or access point information
Message	Success information or error message

Create a New Tech Support Session

You can create a new tech support information collection session.

1. Select **Diagnostics > Tech Support**. The system displays the session dashboard.
2. Select **New** to start a new tech support diagnostics.
3. Select refresh in the **Session** tab.
4. When the session is complete, the tech support shows **Completed** status.

The system displays a session success message or an error message in the message tab.



Note

Do not navigate to a different screen until your tech support diagnostics session is completed.

The tech support file is stored in the server and location set by the user in user preferences setup. For more details, see Remote Servers Settings in [User Roles and Preferences Settings](#) on page 18.

Tech Support Server

Configure and view tech support remote server information.

1. Go to **Diagnostics > Tech Support > Server**.
2. View the tech support file name, size, timestamp, and action information.
3. From action, select  to view or save the tech support file to a local machine.

Logs

General Logs

You can view the most recent system logs diagnostics. The general logs is a read-only screen providing the following information:

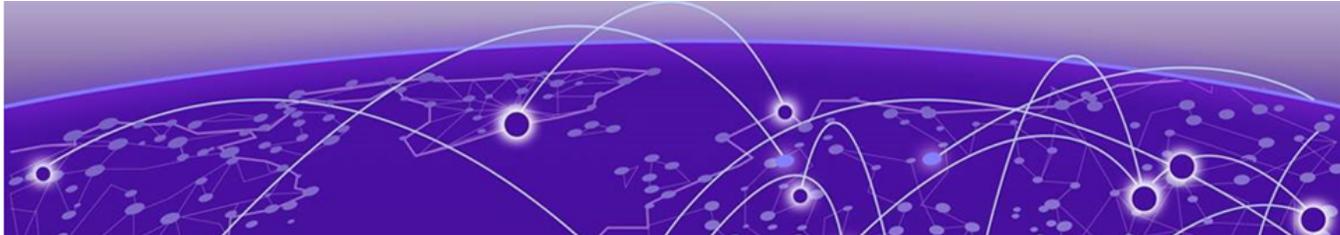
- Timestamp
- Device
- Module
- Event
- User
- Message

Use the logs column to select or remove logs information from the dashboard.

You can view up to 100 recent logs sorted by timestamp and use the free form search to look up a log. Change the log preference in settings. See per user preference settings in [User Roles and Preferences Settings](#) on page 18.

Advanced Logs

To view advanced logs information, go to **Diagnostics > Logs > Advanced**. Select  to download a log file to your local machine.



Remote CLI

Remote CLI Operations on page 67

Learn how to use the remote command line interface (CLI).

Use **Remote CLI** to add a new remote CLI session for the device, download all console logs as a .txt file from the active remote CLI tab, or download all console logs as a .txt file from all remote CLI tabs as a zip file.



Note

Telnet access must be provided for individual users to access Remote CLI. For more information, see [Set Access Control Configuration](#) on page 76.

Remote CLI Operations

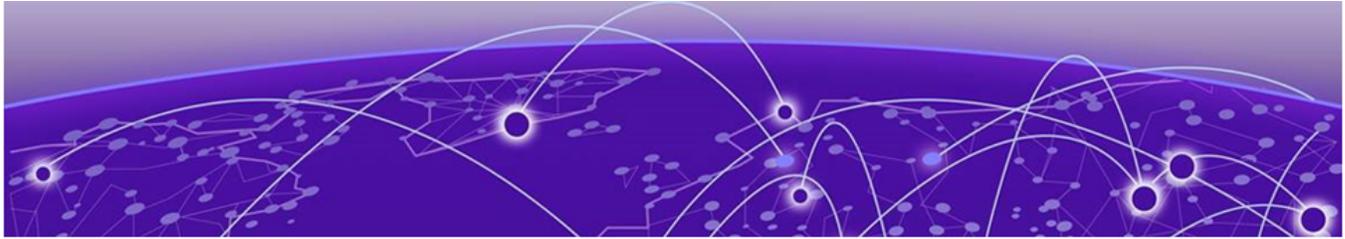
Details about how to create and close a remote CLI session.

About This Task

Create upto eight new remote CLI session for current device using the **Remote CLI** dashboard. Add, download, or download all remote CLI sessions from the **Remote CLI** dashboard.

Procedure

1. Select **Remote CLI** to open the remote CLI session dashboard.
2. Select  to begin a new remote CLI session for the managed device.
Log in to the remote CLI using your login credentials. The login session will time out after 90 seconds.
3. Select  and select **download** to download all console logs as a .txt file from the active remote CLI tab.
4. Select  and select **download all** to download all console logs as a .txt file from all remote CLI tabs as a zipped file.
5. To close out a remote CLI session, navigate to a different screen or select  next to the remote CLI device name.



Policies

[Management Policy on page 68](#)

[Authentication, Authorization, and Accounting \(AAA\) Policy on page 87](#)

[NSight Policy on page 92](#)

[RADIUS Group on page 94](#)

[RADIUS User Pool on page 98](#)

[RADIUS Server Policy on page 100](#)

[Auto-Provisioning Policy on page 108](#)

[Firewall on page 112](#)

[SmartRF Policy on page 124](#)

[Sensor Policy on page 125](#)

[Configure an Event System Policy on page 126](#)

[Configure a Device Categorization Policy on page 127](#)

[WIPS Policy on page 128](#)

[L2TPv3 Policy on page 134](#)

[DHCPv4 Policy on page 137](#)

Configure various policies for your controller and access point systems using the policies dashboard. Policies help determine user access, authentication, access control, and locations for various systems.

Related Topics

[Authentication, Authorization, and Accounting \(AAA\) Policy on page 87](#)

[NSight Policy on page 92](#)

[RADIUS Group on page 94](#)

Management Policy

Controllers and service platforms have mechanisms to allow or deny device access for separate interfaces and protocols such as HTTP, HTTPS, Telnet, SSH, or SNMP. Management access can be enabled or turned off as required for unique policies. The **Management** functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IP addresses to access specific interfaces.

Controllers and service platforms can be managed using multiple interfaces (SNMP, CLI, and Web UI). By default, management access is unrestricted, allowing management access to any enabled IP interface from any host using any enabled management service.

To enhance security, administrators can apply various restrictions such as:

- Restrict SNMP, CLI, and Web UI access to specific hosts or subnets
- Clear unused and insecure interfaces as required within managed access profiles. Deactivating unused management services can reduce an attack footprint and free resources on managed devices
- Provide authentication for management users
- Apply access restrictions and permissions to management users

Management restrictions can be applied to meet specific policies or industry requirements requiring only certain devices or users to be granted access to critical infrastructure devices. Management restrictions can also be applied to reduce the attack footprint of the device when guest services are deployed.



Note

Access points utilize a single Management access policy. Ensure that all the intended administrative roles, permissions, authentication, and SNMP settings are correctly set. If an access point is functioning as a Virtual Controller, these are the access settings used by adopted access points of the same model as the Virtual Controller.



Note

Users must be given Telnet permission at the user-level within a management policy for successful Remote CLI access and login. For more information, see [Set Access Control Configuration](#) on page 76.

Related Topics

[View Management Dashboard](#) on page 69

[Add a New Management Policy](#) on page 71

[Edit or Delete a Management Policy](#) on page 87

View Management Dashboard

About This Task

Existing policies can be updated as management permissions change, or new policies can be added as needed.

To view and modify existing Management policies:

Procedure

1. Go to **Policies > Management**.

The management dashboard opens by default. The dashboard lists all the management policies created and managed thus far and their unique protocol support configurations.

2. Refer to the following management policy configurations to determine whether the existing policies can be used as is, require modification, or require a new policy creation.

A green '✓' check mark indicates that the controller or service platform is allowed to use the listed protocol. A red 'x' mark indicates device access is denied from using the listed protocol.

Name	Displays the name of the Management policy assigned when the policy is initially created. The name must be unique and cannot be updated when modifying a policy
Telnet	Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication
SSHV2	Secure Shell (SSH) version 2, like Telnet, provides a command line interface to a remote host. However, all SSH transmissions are encrypted, increasing their security
HTTP	Hypertext Transfer Protocol (HTTP) provides access to the device's UI using a Web browser. This protocol is not very secure
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) provides fairly secure access to the device's GUI using a Web browser. Unlike HTTP, HTTPS uses encryption for transmission, and is therefore more secure
SNMPV1	Simple Network Management Protocol (SNMP) exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified. SNMP is generally used to monitor a system's performance and other parameters. SNMP v1 is easy to set up, and only requires a plain text. It does not support 64 bit counters, only 32 bit counters, and that provides little security
SNMPV2	SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk
SNMPV3	SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended
FTP	File Transfer Protocol (FTP) is a standard protocol for files transfers over a TCP/IP network
Action	Edit or delete a policy from the list

Related Topics

[Management Policy](#) on page 68

[Add a New Management Policy](#) on page 71

[Edit or Delete a Management Policy](#) on page 87

Add a New Management Policy

About This Task

Create a new management policy.

Procedure

1. Go to **Policies > Management**.
The system displays the **Management** dashboard.
2. Select **Add**.
The **Add Policy** dashboard opens.
3. Type the policy name and select **Add** to enable users configuration.
4. Select **Add** to enable the users, locations, access control, authentication, SNMP, and SNMP traps tabs and the policy configuration.

What to Do Next

Set up user account to configure other management policy settings.

Related Topics

[Management Policy](#) on page 68

[View Management Dashboard](#) on page 69

[Edit or Delete a Management Policy](#) on page 87

Configure Management User Account

About This Task

Management services (Telnet, SSHv2, HTTP, HTTPS, and FTP) require administrators to enter a valid username and password which is authenticated locally or centrally on a RADIUS server. SNMPv3 also requires a valid username and password which is authenticated by the SNMPv3 module. For CLI and Web UI users, the controller or service platform also requires user role information to know what permissions to assign.

- If local authentication is used, associated role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied RADIUS using vendor specific return attributes. If no role information is supplied by RADIUS, the controller or service platform applies default read-only permissions.

Administrators can limit users to specific management interfaces. During authentication, the controller or service platform looks at the user's access assignment to determine if the user has permissions to access an interface:

- If local authentication is used, role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied by RADIUS using vendor specific return attributes.

The controller or service platform also supports multiple RADIUS server definitions as well as fallback to provide authentication in the event of failure. If the primary RADIUS server is unavailable, the controller or service platform authenticates with the next RADIUS sever, as defined in the AAA policy. If a RADIUS server is not reachable, the controller or service platform can fall back to the local database for authentication. If both RADIUS and local authentication services are unavailable, read-only access can be optionally provided.

The controller or service platform authenticates users using the integrated local database. When user credentials are presented the controller or service platform validates the username and password against the local database and assigns permissions based on the associated roles assigned. The controller or service platform can also deny the authentication request if the user is attempting to access a management interface not specified in the account's access mode list.

Use the **Management** tab to review existing administrators, their access medium type, and administrative role within the controller, service platform or access point managed network. New administrators can be added, and existing administrative user configurations modified or deleted as required.



Note

The management policy administrator role requires to have at least one **Superuser**.

Procedure

1. [Add a new user to a management policy.](#)
2. Configure the following user settings for existing administrators:

Setting	Description
Username	The field displays the default name assigned to the administrators upon creation of their account. The name field cannot be modified
Password	Password associated with the username
Confirm Password	Re-type the password to confirm associated password
Access type	Lists the console, SSH, telnet, and web UI access type assigned to each listed administrator. A single administrator can have any one or all of these roles assigned at the same time Options include: <ul style="list-style-type: none"> • Console - select this option to enable access to the device's console • SSH - select this option to enable access to the device using SSH • Telnet - select this option to enable access to the device using Telnet • Web UI - select this option to enable access to the device's Web User Interface

Setting	Description
Administrator role	<p>Lists the role assigned to each listed administrator. An administrator can only be assigned one role at a time</p> <p>Options include:</p> <ul style="list-style-type: none"> • Device Provisioning admin - Assigns the device provisioning administrator role to the new user. This role has privileges to update provision device configuration files or firmware. However, such updates run the risk of overwriting and loss of existing device configurations unless properly archived. <p>Note: You can restrict a device-provisioning-admin user's access to devices within a specific location or locations by applying the Locations tag. When applied, this user will only have access to devices within the locations (sites/ tree-node paths) associated with the locations tag</p> <p>For more information, see set locations configuration</p> <ul style="list-style-type: none"> • Help Desk - Assign this role to the person who troubleshoots and debugs problems reported by the customer. The Help Desk manager typically runs troubleshooting utilities, runs service commands, views, and retrieves logs. Help Desk personnel are <i>not</i> allowed to conduct controller or service platform reloads • Monitor - Assigns the System Monitor role to the new user. This role has read only access to the system. The user can only view configuration and statistics. The user cannot view protected information and passwords. Select Monitor to assign permissions without any administrative rights • Network Admin - The Network administrator role provides full access to configure all wired and wireless parameters like IP configuration, VLANs, L2/L3 security, WLANs, radios, and captive portal • Rest API User - Assigns the REST API user role. This user role provides read-only permission for the user to use APIs to retrieve statistics, etc. The user will not have permission to change or write configurations • Security Admin - Select Security administrator to set the administrative rights for a security administrator allowing configuration of all security parameters • Superuser - Select this option to assign complete administrative rights to the user. This entails all the roles listed for all the other administrative roles

Setting	Description
	<ul style="list-style-type: none"> • System Admin - The System administrator role provides permissions to configure general settings like NTP, boot parameters, licenses, perform image upgrades, auto install, manager redundancy or clustering and control access • Vendor Admin - Configures this user's role as vendor-admin. Once created, the vendor-admin can access the online device-registration portal to add devices to the RADIUS vendor group to which the admin belongs. Vendor-admins only have web access to the device registration portal. <p>The WiNG software allows multiple vendors to securely on-board their devices through a single SSID. Each vendor has a 'vendoradmin' user who is assigned a unique username and password credential for RADIUS server validation. Successfully validated vendor-admins can on-board their devices, which are, on completion of the on-boarding process, immediately placed on the vendor-allowed VLAN.</p> <p>If assigning the vendor-admin role, provide the vendor's group name for RADIUS authentication. The vendor's group takes precedence over the statically configured group for device registration.</p> <p>Note: The Allowed Location option is not applicable to this role</p> <ul style="list-style-type: none"> • Web User admin - Assigns the Web User administrator role to the new user. This role allows the user to create guest users and credentials. The Web user admin can access only the custom GUI screen and does not have access to the normal CLI and GUI

Setting	Description
Allowed Location	Use the allowed location field to specify the allowed-locations tag. Each allowed-location tag is mapped to one or multiple locations (RF Domains/sites/tree-node paths). By specifying an allowed location tag, you are restricting the user's access to the locations mapped to the tag. However, in WiNG, this option is only applicable to the Device Provisioning admin user role Note: Ensure that the allowed location tag is existing and configured. Use the locations tab on the Management dashboard to create a tag and map it to locations (RF Domains, sites, tree-node paths, etc.) within your managed network. For more information, see Set Location Configuration
Group	Specify the group to which the user belongs

Set Location Configuration

About This Task

The **Locations** option is a means to control a user's access to locations (RF Domains, sites, or tree-node paths) within the managed network. Use this option to configure locations tag and associate one or more locations with the tag. After creating locations tag, use the **Users** dashboard to apply these tags to users.



Note

The locations tag is only applicable to the WiNG Device Provisioning admin user. The device provisioning admins will only be able to provision devices that they manage.

To set locations configuration:

Procedure

1. Select the **Locations** tab.
2. Review the existing locations configuration.
3. Select the + icon to add a new location.

The location setting dashboard opens.

4. Set or modify the following allowed location parameters:

Field	Description
Name	If adding a new Locations configuration, provide a name that is less than 32 characters without any space. Provide a name that identifies the associated locations (RF Domain)
Locations	<p>Specify the RF Domain name in the Locations field and select Add to add the location. You can associate a single RF Domain or multiple RF Domains with a Locations tag. The location can also be specified as a treenode path or multiple tree-node paths.</p> <p>Select Add to add location to the locations list</p> <p>To edit a location, select the  icon from the action option</p> <p>To delete a location, select the  icon from the action option</p>

5. Select **Save** to apply the location settings.

Set Access Control Configuration

About This Task

Restricting remote access to a controller or service platform ensures only trusted hosts can communicate with enabled management services. This ensures only trusted hosts can perform management tasks and provide protection from brute force attacks from hosts attempting to break into the controller or service platform managed network.

Administrators can permit management connections to be established on any IP interface on the controller or service platform (including IP interfaces used to provide captive portal guest access).

Administrators can restrict management access by limiting access to a specific host (IP address), subnet, or ACL on the controller or service platform.

Refer to the **Access Control** dashboard to allow or deny management access to the network using strategically selected protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Access options can be either activated or deactivated as required. Consider deactivating unused interfaces to close unnecessary security holes. The Access Control tab is not meant to function as an ACL (in routers or other firewalls), where you can specify and customize specific IPs to access specific interfaces.

- Source hosts - Management access can be restricted to one or more hosts by specifying their IP addresses
- Source subnets - Management access can be restricted to one or more subnets
- IP ACL - Management access can be based on the policies defined in an IP based ACL

In the following example, a controller has two IP interfaces defined with VLAN10 hosting management and network services and VLAN70 providing guest services. For security, the guest network is separated from all trusted VLANs by a firewall.

Interface	Description	IP Address	Management
VLAN10	Services	Yes	Yes
VLAN70	Guest	Yes	No

By default, management services are accessible on both VLAN10 and VLAN70. By restricting access to VLAN10, the controller only accepts management sessions on VLAN10. Management access on VLAN70 is longer available.

Administrators can secure access to a controller or service platform by disabling less secure interfaces. By default, the CLI, SNMP and FTP disable interfaces that do not support encryption or authentication. However, Web management using HTTP is enabled. Insecure management interfaces such as Telnet, HTTP and SNMP should be disabled, and only secure management interfaces, like SSH and HTTPS should be used to access the controller or service platform managed network.

The following table provides interfaces security comparison information:

Access type	Encryption	Authentication	Default state
Telnet	No	Yes	Deactivated
SNMPv2	No	No	Activated
SNMPv3	Yes	Yes	Activated
HTTP	No	Yes	Deactivated
HTTPS	Yes	Yes	Deactivated
FTP	No	Yes	Deactivated
SSHv2	Yes	Yes	Deactivated

To set an access control configuration for the Management Access policy:

Procedure

1. Select the **Access control** tab.

2. Set the following parameters required for Telnet access:

Setting	Description
Activate Telnet	Select the toggle button to activate Telnet device access. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is not selected by default. Select telnet for a user to activate Remote CLI login
Telnet port	Set the port on which Telnet connections are made (1 - 65,535). The default port is 23. Change this value using the spinner control next to this field or by entering the port number in the field

3. Set the following parameters for SSH access:

Setting	Description
Activate SSHv2	Select the toggle button to activate SSH device access. SSH (Secure Shell) version 2, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is not selected by default
SSHv2 port	Set the port on which SSH connections are made. The default port is 22. Change this value using the spinner control next to this field or by entering the port number in the field

4. Set the following HTTP and HTTPS parameters:

Setting	Description
Enable HTTP	Select Enable HTTP to activate HTTP device access. HTTP provides limited authentication and no encryption
Enable HTTPS	Select Enable HTTPS to activate HTTPS device access. HTTPS (Hypertext Transfer Protocol Secure) is more secure than plain HTTP. HTTPS provides both authentication and data encryption



Note

If the a RADIUS server is not reachable, HTTPS or SSH management access to the controller or service platform may be denied

5. Set the following General parameters:

Setting	Description
Idle Session Timeout	Specify an inactivity timeout for management connects (in seconds) between 1 - 4,320. The default setting is 30
Message of the Day	Type a message no longer than 255 characters to be displayed at login for clients connecting via Telnet or SSH

6. Select **Enable Rest Server** option to facilitate device on-boarding.

When selected, the REST server allows vendor-specific users access to the online device registration portal. All requests and responses to and from the on-boarding portal are handled by the REST server through restful Application Programming Interface (API) transactions. The REST server serves the Web pages used to associate a device's MAC address with a specific vendor group. This option is selected by default.

7. Select **Enable NOVA** option to facilitate NOVA access.
 8. Set the following parameters required for FTP access:

Setting	Descriptio
Activate FTP	Select the toggle button to activate FTP (File Transfer Protocol) device access. FTP is the standard protocol for transferring files over a TCP or IP network. FTP requires administrators enter a valid username and password authenticated locally on the controller. FTP access is not activated by default
Username	Specify a username required when logging in to the FTP server. The username cannot exceed 32 characters
Password	Specify a password required when logging in to the FTP server. Reconfirm the password in the field provided to ensure it has been entered correctly. The password cannot exceed 63 characters
Root Directory	Provide the complete path to the root directory in the root directory field. The default setting has the root directory set to flash:/

9. Set the following access restrictions parameters:

Setting	Description
Filter Type	Select a filter type for access restriction. Options include IP access list, Source Address, or None. To restrict management access to specific hosts, select Source Address as the filter type and provide the allowed addresses within the Source Hosts field
IP Access List	If the selected filter type is IP access list, select an access list from the drop-down list box. IP based firewalls function like Access Control Lists (ACLs) to filter or mark packets based on the IP from which they arrive, as opposed to filtering packets on layer 2 ports. IP firewalls implement uniquely defined access control policies, so if you do not have an idea of what kind of access to allow or deny, a firewall is of little value, and could provide a false sense of network security
Source Hosts	If the selected filter type is Source Address, type an IP Address or IP Addresses for the source hosts. To restrict management access to specific hosts, select Source Address as the filter type and provide the allowed addresses within the Source Hosts field
Source Subnets	If the selected filter type is Source Address, type a source subnet or subnets for the source hosts. To restrict management access to specific subnets, select Source Address as the filter type and provide the allowed addresses within the Source Subnets field
Logging Policy	If the selected filter is Source Address, select a logging policy for administrative access. Options includes None, Denied Only, or All

10. Set the User Lockout Settings. Select **Add** to configure the following role-based user-account lockout and unlock criteria:

Setting	Description
Role	<p>Select a user role to set account lockout. The options are:</p> <ul style="list-style-type: none"> • Device Provisioning admin • Help Desk • Monitor • Network Admin • Rest API User • Security Admin • Superuser • System Admin • Vendor Admin • Web User admin <p>Note: You can set account lockout for multiple roles. After specifying the role, set the Lockout Time and Number of Password Attempts.</p> <p>User-account lockout is individually applied to each account within the specified role. For example, consider the 'monitor' role having two users: 'user1' and 'user2'. The Number of Password Attempts and Lockout Time is set at '5' attempts and '10' minutes respectively. In this scenario, user2 makes 5 consecutive, failed login attempts, and the user2 account is locked out for 10 minutes. However, during this lockout time the user1 account remains active</p>
Lockout Time	Specify the maximum time for which an account remains locked. Specify a value from 0 to 600 minutes. The value '0' indicates that the account is permanently locked
Number of Password Attempts	Specify the maximum number of consecutive, failed attempts allowed before an account is locked. Specify a value from 1 to 100
Action	Use the action option to delete a user lockout setting

11. Select **Apply** or **Save** to set the user access control settings.

Configure User Authentication Settings

About This Task

Refer to the **Authentication** tab to define how user credential validation is conducted on behalf of a Management Access policy. Setting up an authentication scheme by policy allows for policy member credential validation collectively, as opposed to authenticating users individually.

Procedure

1. Go to **Policies > Management**.
2. Select a management policy from the list.
3. Navigate to **Authentication**.

4. Define the following settings to authenticate management access requests:

Setting	Description
Local	<p>Use this option to enable or clear local authentication mode. Local authentication uses the local username and password database to authenticate a user. When not selected, an external authentication resource is used to validate user access requests. The external authentication resource could be a dedicated RADIUS server</p> <p>Note: The local authentication mode is enabled by default. Not selecting the local authentication enables the RADIUS and AAA Policy parameters.</p>
RADIUS	<p>If authentication is to be handled by an external RADIUS server, select one of the following options:</p> <ul style="list-style-type: none"> • External - Select this option to forward client authentication requests to an external RADIUS server. This option enables external RADIUS server as the preferred authentication mode. However, this option does not provide fallback to local database authentication in case the server is unreachable or if the server rejects the request • Fallback - Select this option to revert to local database authentication in case the external RADIUS server is unreachable. <p>When this option is enabled, RADIUS authentication is attempted first. However, if the external RADIUS server is unreachable the local database is used to authenticate the user</p> <ul style="list-style-type: none"> • Fallthrough - Select this option to revert to local database authentication in the following scenarios: <ul style="list-style-type: none"> ◦ If the external RADIUS server is unreachable ◦ If the external RADIUS server rejects the user authentication request <p>When this option is selected, RADIUS authentication is attempted first. However, if the external RADIUS server is unreachable or rejects the authentication request the local database is used to authenticate the user</p>
AAA Policy	<p>If external RADIUS server authentication option is selected, select the AAA policy to use with the external RADIUS resource. Controllers and service platforms that are not using their local RADIUS resource will need to inter-operate with a RADIUS and LDAP Server (AAA Servers) to provide user database information and user authentication</p>

Setting	Description
	data. The AAA policy points to this external RADIUS server resource Select a policy from the AAA Policy drop-down list

5. Select **Save** to apply user authentication settings.

Set SNMP Configuration

About This Task

Use the Simple Network Management Protocol (SNMP) to communicate with controllers and service platforms within the wireless network. SNMP is an application layer protocol that facilitates the exchange of management information to and from a managed device. SNMP enabled devices listen on port 162 (by default) for SNMP packets from the management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string is used to gather statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to set device parameters. SNMP is used to monitor a system's performance and other parameters.

SNMP version	Encryption	Authentication	Default state
SNMPV1	No	No	Deactivated
SNMPV2	No	No	Activated
SNMPV3	Yes	Yes	Activated

To configure SNMP management access:

Procedure

1. Select the **SNMP** tab.

2. Activate or deactivate SNMPV1, SNMPV2, or SNMPV3.

Setting	Description
Enable SNMPV1	SNMP V1 exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified as text strings, with version 1 being the original implementation. SNMPV1 is activated by default.
Enable SNMPV2	Select the checkbox to activate SNMPV2 support. SNMPV2 provides device management using a hierarchical set of variables. SNMPv2 uses Get, GetNext, and Set operations for data management. SNMPV2 is activated by default
Enable SNMPV3	Select the checkbox to activate SNMPV3 support. SNMPV3 adds security and remote configuration capabilities to previous versions. The SNMPV3 architecture introduces the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. The architecture supports the concurrent use of different security, access control, and message processing techniques. SNMPV3 is activated by default

3. Set the SNMP V1/V2C Community String configuration.

Select **Add** to include additional SNMP V1/V2C community strings. Select the  icon to remove the SNMP community string.

Field	Description
Community	Define a public or private community designation. By default, SNMPV2 community strings on most devices are set to public for the read-only community string, and private for the read-write community string
Access Control	Set the access permission for each community string used by devices to retrieve or modify information. The available options are: <ul style="list-style-type: none"> • Read Only - Allows a remote device to retrieve information • Read-Write - Allows a remote device to modify settings
IP SNMP ACL	Set the IP SNMP ACL used along with community string. Use the drop-down list box to select an existing ACL

- Set the SNMPV3 Users configuration.

Select **Add** to include additional SNMPV3 user configurations. Select the  icon to remove the user configuration.

Setting	Description
User Name	Use the drop-down list box to define a user name. Options include snmpmanager, snmpoperator, or snmptrap
Authentication	Displays the authentication scheme used with the listed SNMPV3 user. The listed authentication scheme ensures only trusted and authorized users and devices can access the network
Encryption	Select to activate encryption
Password	Provide the user's password in the field provided. Select the  icon to display the character string used in the password

- Select **Save** to update SNMP configuration.

Set SNMP Traps Configuration

About This Task

Controller or service platform managed networks use SNMP trap receivers for fault notifications. SNMP traps are unsolicited notifications triggered by thresholds or actions, and are an important fault management tool. A SNMP trap receiver is the defined destination for SNMP messages. A trap is generated when a device consolidates event information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community etc. SNMP trap notifications exist for most operations, but not all are necessary for day-to-day operations.

To define a SNMP trap configuration for receiving events at a remote destination:

Procedure

- Select the **SNMP Traps** tab.
- Select **Enable** Trap Generation to activate trap generation using the trap receiver configuration defined. This feature is not selected by default.
- Select **Add** to include User Lockout Settings for the SNMP trap.

Configure the user lockout settings parameters:

Setting	Description
IP Address	Type the IP address of an external server resource dedicated to receive SNMP traps on behalf of the controller or service platform
Port	Set the virtual port of the server resource dedicated to receiving SNMP traps. The default port is port 162

Setting	Description
Version	Select the SNMP version to send SNMP traps. SNMPv2c is the default version
Trap Community	Provide a 32 character maximum trap community string. The community string functions like a user id or password allowing access to controller or access point resources. If the community string is correct, the controller provides with the requested information. If the community string is incorrect, the device controller discards the request and does not respond

4. Select **Save** to update SNMP trap configuration settings.

Edit or Delete a Management Policy

About This Task

Use the **Management** tab to review existing administrators, their access medium type, and administrative role within the controller, service platform or access point managed network. New administrators can be added, and existing administrative user configurations modified or deleted as required.

Procedure

1. Go to **Policies > Management**.
2. To delete a management policy, select the  icon.
The system displays a **Delete this Management?** message.
 - a. Select **Cancel** to retain the management policy.
 - b. Select **Delete** to remove the management policy.
3. To edit a management policy, select the name of an existing policy or the pencil icon on the **Action** column.
The system displays the users dashboard.
4. Navigate to the protocol that you need to edit.
5. Select **Save** to apply the changes.

Related Topics

[Management Policy](#) on page 68

[View Management Dashboard](#) on page 69

[Add a New Management Policy](#) on page 71

Authentication, Authorization, and Accounting (AAA) Policy

Authentication, authorization, and accounting (AAA) is a framework for controlling access to the network, enforcing user authorization policies, and auditing and tracking usage. The AAA policy helps determine the networks and resources a user can access and helps keep track of user activity over the network. These combined processes are central for securing wireless client resources and wireless network data flows.

A controller, service platform, or access point can interoperate with external RADIUS and LDAP Servers (AAA servers) to provide an additional user database and authentication resource. Each WLAN can maintain its own unique AAA configuration.

Authentication — Authentication provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before being allowed to access the network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

Authorization — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or can be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating attribute-value (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces.

Accounting — Accounting is the method for collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on the access control server. The data can be analyzed for network management, client billing, and auditing. Accounting methods must be defined through AAA. When AAA accounting is activated, it's applied equally to all interfaces on the access servers.

Related Topics

[Add a New AAA Policy](#) on page 88

[Edit a AAA Policy](#) on page 91

[Delete a AAA Policy](#) on page 91

Add a New AAA Policy

About This Task

Configure a new AAA policy to determine access to a network and how to control user authorization.

Procedure

1. Go to **Policies > AAA**.
2. Select **Add** to configure a new AAA policy.
The system displays the **Add Policy** dashboard.
3. Type a AAA policy name on the **AAA** field.
The policy name must be unique and cannot be the same as an existing AAA policy name.

4. Select **Add**.

The **General** policy dashboard opens.

a. Select **Add** to add general AAA policy settings. The **Server** dashboard opens.

b. Set AAA policy server parameters:

Server parameter	Description
Sever ID	Displays the numerical server index (1-12) for the accounting server when added to the list available to the access point
Server Type	Displays the type of AAA server in use as either Authentication or Accounting
Port	Displays the port on which the RADIUS server listens to traffic within the access point managed network. The port range is 1 - 65,535. The default port is 1812
Server Host	Displays the IP address or hostname of the RADIUS authentication server. The options are IP/Host , Onboard , Controller , or Centralized IP/Host server host option configuration: Select IP/Host to display the IP address or hostname of the RADIUS authentication server and set the hostname or IP address and password in the Secret field
Request Attempts	Displays the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3
Request Timeout	Displays the time (from 1 - 3600) seconds for the re-transmission of request packets. The default is 5 seconds. If this time is exceeded, the authentication session is terminated

c. Select **Add** and **Save** to apply the AAA policy general server settings.

5. Navigate to **Radius** dashboard to configure the following AAA policy settings:

Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data; such as captive portal start and stop times, executed commands (such as

PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track captive portal services that users are using.

Radius settings	Description
Accounting type	<p>Displays the accounting type set for the AAA policy. Options include:</p> <ul style="list-style-type: none"> • Start/Stop — Sends a start accounting notice at the beginning of a process and a stop notice at the end of a process. The start accounting record is sent in the background. The requested process begins regardless of whether the start accounting notice is received by the accounting server • Start/Interim/Stop— Sends a start accounting notice at the beginning of a process, multiple regular notices while the process is running, and a stop notice at the end of a process <p>The default option is Start/Stop</p>
Address format	<p>Options include:</p> <ul style="list-style-type: none"> • No Delimiter • Colon Delimiter • Dash Delimiter • Pair Hyphen • Pair Space • Dot Delimited per Four • Middle Dash Delimiter <p>The default option is Pair Hyphen</p>
Server pooling	<p>The server pooling mode controls how requests are transmitted across RADIUS servers. Selecting Fail Over results in working down the list of servers if a server is unresponsive and unavailable. The Load-Balance option uses all available servers transmitting requests in round robin</p>
Authentication Protocol	<p>Options include:</p> <ul style="list-style-type: none"> • PAP • CHAP • MS-CHAP • MS-CHAPv2 <p>The default protocol option is PAP</p>

6. Select **Save** to apply RADIUS settings changes to the AAA policy.

Related Topics

[Authentication, Authorization, and Accounting \(AAA\) Policy](#) on page 87

[Edit a AAA Policy](#) on page 91

[Delete a AAA Policy](#) on page 91

Edit a AAA Policy

About This Task

Edit a AAA policy from existing AAA policies.

Procedure

1. Go to **Policies > AAA**.

The **AAA** policy dashboard is displayed with the following information for existing AAA policy:

AAA policy parameter	Description
Policy Name	Displays the name assigned to the AAA policy when it was initially created. The name cannot be edited within a listed profile
Accounting Packet Type	Displays the accounting type set for the AAA policy. Options include: <ul style="list-style-type: none"> • Start/Stop • Start/Interim/Stop
Wireless Client Attempts	Displays the number of attempts by the wireless client
Action	Options include: <ul style="list-style-type: none"> • Edit— Select the  option to edit an existing AAA policy. • Delete— Select the  option to delete a AAA policy.

2. Select  to delete an existing AAA policy.
3. Select  action to edit an existing AAA policy.
4. Edit the general settings or the RADIUS settings.
5. Select **Save** to apply general and RADIUS settings.

Related Topics

[Authentication, Authorization, and Accounting \(AAA\) Policy](#) on page 87

[Add a New AAA Policy](#) on page 88

[Delete a AAA Policy](#) on page 91

Delete a AAA Policy

About This Task

Delete an existing AAA policies.

Procedure

1. Go to **Policies > AAA**.

2. Select  to delete an existing policy from the policy list.
3. The system displays a 'delete this AAA policy' message.
4. Select **Cancel** to exit and keep the AAA policy.
5. Select **Delete** to erase the AAA policy from the system.
6. The request to delete is completed and the AAA policy is deleted. All settings associated with the AAA policy is also deleted from the system.

Related Topics

[Authentication, Authorization, and Accounting \(AAA\) Policy](#) on page 87

[Add a New AAA Policy](#) on page 88

[Edit a AAA Policy](#) on page 91

NSight Policy

NSight is an advanced network visibility, service assurance, and analytics platform that is responsive and easy to use. It is designed for day-to-day network monitoring and troubleshooting with the capability of providing essential macro trending analytics for network planning, usage modeling, and SLA management. NSight provides real-time monitoring, historical trend analytics, and troubleshooting capabilities for WLAN deployment management.

Configure NSight policies for the WiNG controllers and applications.

The main **NSight** policy screen displays the following information:

Element	Description
Policy Name	The name assigned to the NSight policy. The assigned policy name cannot be modified
Server Host	Server host type when the server is added for an NSight policy
Action	Options include edit and delete for existing NSight policies

Related Topics

[Add NSight Policy](#) on page 92

[Edit NSight Policy](#) on page 93

[Delete NSight Policy](#) on page 94

Add NSight Policy

About This Task

Configure and add an NSight policy for the network.

Procedure

1. Go to **Policies > NSight**.
The NSight policy list dashboard opens.

2. Select **Add**.
The system displays the **Add Policy** dashboard.
3. Type a NSight policy name in the **Name** field.
4. Select **Add**.
The NSight policy is added to the list and the **General** settings dashboard opens.
5. Configure general NSight server parameters:
The server grid allows a maximum of three entries.

NSight server option	Description
Host Type	Type of security for the host URL. Options include <ul style="list-style-type: none"> • Https • Http The default option is Https
Host URL	Host website address. Type the host URL in the following format: [http or https://<IP or hostname>[:port]]
Enforce SSL verification	Option available only when you select Https host type. Use the slider to select or clear SSL verification for the host URL
Poll	Use the slider to enable or clear poll option for the host URL

6. Use the **Status** slider on the general dashboard to view or stop viewing the server status.
7. Select **Add** to add the host server to the NSight policy.
8. Select **Save** to apply all configured changes.

Related Topics

- [NSight Policy](#) on page 92
- [Edit NSight Policy](#) on page 93
- [Delete NSight Policy](#) on page 94

Edit NSight Policy

Before You Begin

Only existing NSight policies can be edited.

About This Task

Edit available NSight policies from the NSight policy list dashboard.

Procedure

1. Go to **Policies > NSight**.
The list of available NSight policies are displayed in the NSight policy dashboard.
2. Select  or select the Nsight policy to edit an existing NSight policy.

3. Edit the server information such as host URL, SSL verification, status, or polling option.
4. Select **Save** to apply the configuration changes.

Related Topics

- [NSight Policy](#) on page 92
- [Add NSight Policy](#) on page 92
- [Delete NSight Policy](#) on page 94

Delete NSight Policy

About This Task

Delete an existing NSight policy.

Procedure

1. Go to **Policies > NSight**.
The list of available NSight policies are displayed in the NSight policy dashboard.
2. Select  to remove an existing NSight policy from the list.

Related Topics

- [Add NSight Policy](#) on page 92
- [Edit NSight Policy](#) on page 93
- [NSight Policy](#) on page 92

RADIUS Group

Remote Authentication Dial-In User Service (RADIUS) is a client or server protocol and software. It enables remote access servers to authenticate users and authorize their access. RADIUS is a distributed client or server system that secures networks against unauthorized access.

RADIUS clients send authentication requests to the controller or service platform's local RADIUS server containing user authentication and network service access information. RADIUS enables centralized management of authentication data (usernames and passwords). When a client attempts to associate to the controller or service platform, authentication requests are sent to the RADIUS server. Authentication and encryption takes place through the use of a shared secret password that is not transmitted over the network.

The controller's local RADIUS server stores the user database locally, and can optionally use a remote user database. It ensures higher accounting performance. It allows the configuration of multiple users, and assign policies for group authorization.

Controllers and service platforms have full internal RADIUS resource capability. Additionally, all controllers maintain a local RADIUS resource. The local enforcement of user-based policies is configurable.

User policies include dynamic VLAN assignment and access restrictions based on time of day. A certificate is required for EAP TTLS, PEAP, and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after authentication with the RADIUS server. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

Related Topics

[Create RADIUS Group](#) on page 95

Create RADIUS Group

About This Task

The RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in a local database. The user ID in the received access request is mapped to the specified group for authentication. RADIUS groups allows to create and apply the following policies managing user access.

- Assign a VLAN to the user upon successful authentication
- Define a start and end of time in (HH:MM) when the user is allowed to authenticate
- Define the list of SSIDs to which a user belonging to this group is allowed to associate
- Define the days of the week the user is allowed to login
- Rate limit traffic



Note

A RADIUS group can only be assigned either a guest group or a management group.

Procedure

1. Go to **Policies > RADIUS Group**.
2. Select a group from RADIUS dashboard to view the following read-only information for existing groups:

Setting	Description
RADIUS Group Policy	Displays the group name or identifier assigned to each listed group when it was created. The name cannot exceed 32 characters or be modified as part of the group edit process
Guest Group	Specifies whether a user group only has guest access and temporary permissions to the local RADIUS server. The conditions of the guest access can be set uniquely for each group. A red "X" designates the group as having no access to the local RADIUS server and a green checkmark designates permanent access to the local RADIUS server. Guest user groups cannot be made management groups with unique access and role permissions
Management Group	A red "X" designates the management group having no access. A green checkmark designates this RADIUS user group as a management group. Management groups can be assigned unique access and role permissions

Setting	Description
Role	If a group is listed as a management group, it may also have a unique role assigned. Available roles include: <ul style="list-style-type: none"> • monitor - Read-only access • helpdesk - Helpdesk/support access • network-admin - Wired and wireless access • security-admin - Full read or write access • system-admin - System administrator access
VLAN	Displays the group's VLAN ID. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the network (once authenticated by the local RADIUS server)
Start Time	Specifies the time users within each listed group can access local RADIUS resources
Stop Time	Specifies the time users within each listed group lose access to local RADIUS resources
Action	Use the action option to edit or delete a RADIUS group policy

3. Select **Add**.

The **RADIUS Group** policy dashboard opens.

4. Assign a policy name and select **Add**.

The general settings dashboard opens.

5. Define the following settings to define the user group configuration general settings:

Setting	Description
RADIUS Group Policy	If you are creating a new RADIUS group, assign it a name to help differentiate it from others with similar configurations. The name cannot exceed 32 characters or be modified as part of a RADIUS group edit process
Guest User Group	Select this option to assign only guest access and temporary permissions to the local RADIUS server. Guest user groups cannot be made management groups with unique access and role permissions
VLAN	Select this option to assign a specific VLAN to this RADIUS user group. Ensure Dynamic VLAN assignment (single VLAN) is enabled for the WLAN in order for the VLAN assignment to work properly
WLAN SSID	Assign a list of SSIDs users within this RADIUS group are allowed to associate with. An SSID cannot exceed 32 characters. Assign WLAN SSIDs representative of the configurations a guest user will need to access. The parameter is not available if this RADIUS group is a management group

Setting	Description
Rate Limit from Air	Select the checkbox to set the rate limit for clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 kbps. Setting a value of 0 stops rate limiting
Rate Limit to Air	Select the checkbox to set the rate limit from clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 kbps. Setting a value of 0 disables rate limiting
Session Time	Select the option to activate session timeout. Use the drop-down box to set a client session time in minutes (5 - 144,000). This is the session time a client is granted upon successful authentication. When this time expires, the RADIUS session is stopped
Inactivity Timeout	Select the option to activate inactivity timeout. Use the drop-down box to specify an interval in seconds (60 - 86,400). If no frame is received for this duration, the session is timed out
Management Group	Select this option to designate a RADIUS group as a management group. If set as management group, assign member roles using the role drop-down list box. This feature is not selected by default
Access	If a group is listed as a management group, assign how the devices can be accessed. Available access types are: <ul style="list-style-type: none"> • Web - Web access through browser is permitted • SSH - SSH access through command line is permitted • Telnet - Telnet access through command line is permitted • Console - Console access to the device is permitted
Role	Select a role if a group is listed as a management group. Available roles include: <ul style="list-style-type: none"> • monitor - Read-only access • helpdesk - Helpdesk and support access • network-admin - Wired and wireless access • security-admin - Full read and write access • system-admin - System administrator access • super user - • web user admin - • device provisioning admin - • REST API user -

6. Set the schedule to configure access times and days.

Setting	Description
Restrict Access by Day	Select the days on which RADIUS group members can access RADIUS resources. This is an additional means of refining the access permissions of RADIUS group members
Restrict Access by Time	<ul style="list-style-type: none"> Start Time - Use the spinner control to set the time (in HH:MM format) RADIUS group members are allowed access the RADIUS server resources Stop Time - Use the spinner control to set the time (in HH:MM format) RADIUS group members are denied access to RADIUS server resources

7. Select **Save** to update set configurations.

RADIUS User Pool

About This Task

A user pool defines policies for individual user access to local controller or service platform RADIUS resources. User pools are a convenient means of providing RADIUS resources based on the pool's unique permissions (temporary or permanent). A pool can contain a single user or group of users.

To configure a RADIUS user pool and unique user IDs:

Procedure

- Go to **Policies > RADIUS User Pool**.
The RADIUS User Pool list opens and displays the existing user pool.
- Select an existing user pool to edit an user.
- Select  icon to delete a user pool.
- Select  icon to add a new RADIUS user pool.
The **Add Policy** dashboard opens.
- Assign a policy name up to 32 characters and select **Add**.
The **General** user pool section opens.

6. Select  to add configure user settings.

The user settings define when specific user IDs have access to RADIUS resources.

Setting	Description
User ID	The unique string identifying this user. This is the ID assigned to the user when created and cannot be modified with the rest of the configuration
Password	The password cannot exceed 32 characters. Select the show icon to view the password's character string
Group	Select a group from existing group list
Guest User	Use the toggle to assign guest user access. This determines if a user has temporary permissions to the local RADIUS server. Selecting the guest user access option will open guest user settings
Email ID	The Email address (in 64 characters or less) of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool
Telephone	The 12-character maximum telephone number of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool
Guest User Settings	
Start Date	The month, day, and year the listed user ID can access local RADIUS server resources
Start Time	The time the listed user ID can access local RADIUS server resources. The time applies only to the range defined by the start and expiry date
Expiry Date	The month, day, and year the listed user ID can no longer access local RADIUS server resources
Expiry Time	The time the listed user loses access to RADIUS server resources. The time applies only to the range defined by the start and expiry date

Setting	Description
Access Duration	The amount of time a user is allowed access when time-based access privileges are applied. The duration cannot exceed 365 days. Select Till Expiry to keep the access duration the same as the expiry date
Data	<p>The total amount of bandwidth available for each guest user. Options include:</p> <ul style="list-style-type: none"> • Unlimited - no limit on the amount of data available for each guest user • Limited - Set data limit for each guest user <ul style="list-style-type: none"> ◦ Data Limit (MB or GB) - The total amount of bandwidth consumable by each guest user ◦ Committed Downlink Rate (kbps or mbps) - The download speed allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to Reduced Downlink Rate ◦ Committed Uplink Rate (kbps or mbps) - The upload speed allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to Reduced Uplink Rate ◦ Reduced Downlink Rate (kbps or mbps) - The reduced speed the guest utilizes when exceeding their specified data limit ◦ Reduced Uplink Rate (kbps or mbps) - The reduced speed the guest utilizes when exceeding their specified data limit

7. Select **Add** or **Update** to include user settings to the RADIUS user.
8. Select **Save** to update user configurations.

RADIUS Server Policy

A RADIUS server policy is a unique authentication and authorization configuration for client connection requests, authenticating users, and returning the configuration information necessary to deliver service to the requesting client and user. The client is the entity with authentication information requiring validation. The controller or service platform local RADIUS server has a database of authentication information used to validate the client's authentication request.

The **RADIUS Server** dashboard displays the following read-only configuration information:

Setting	Description
RADIUS Server	Lists the administrator assigned policy name defined upon creation of the server policy
RADIUS User Pools	Lists the user pools assigned to the server policy. These are the client users who an administrator has assigned to each listed group. The users must adhere to the network access requirements before receiving access to controller or service platform resources
Default Source	Displays the RADIUS resource designated for user authentication requests. Options include local (resident controller or service platform RADIUS server resources) or LDAP (designated remote LDAP resource)
Default Fallback	States whether a fallback is enabled providing a option to revert to local RADIUS resources if the designated external LDAP resource were to fail or become unavailable. Fallback options include true or false. The default option is false for local source
Authentication Type	Lists the local EAP authentication scheme used with this policy. The following EAP authentication types are supported by the local RADIUS and remote LDAP servers: <ul style="list-style-type: none"> • All - Enables both TTLS and PEAP • PEAP and GTC - The EAP type is PEAP with default authentication using GTC • PEAP and MSCHAPv2 - The EAP type is PEAP with default authentication using MSCHAPv2 • TLS - Uses TLS as the EAP type • TTLS and MD5 - The EAP type is TTLS with default authentication using MD5 • TTLS and MSCHAPv2 - The EAP type is TTLS with default authentication using MSCHAPv2 • TTLS and PAP - The EAP type is TTLS with default authentication using PAP
CRL Validation	Specifies whether a Certificate Revocation List (CRL) check is made. Options include true for CRL validation and false for CRL is deactivation

Related Topics

[Configure RADIUS Server Policy](#) on page 102

[Configure RADIUS Clients](#) on page 103

[RADIUS Server Policy](#) on page 100

[Configure an LDAP Server](#) on page 106

Configure RADIUS Server Policy

About This Task

The RADIUS server ensures that the information is correct using an authentication scheme like PAP, CHAP, or EAP. The user's proof of identification is verified along with other information. A RADIUS server policy can also use an external LDAP resource to verify user credentials.

Procedure

1. Select **Policies > RADIUS Server**.

The **RADIUS Server** dashboard opens.

2. Select  to add a new policy or  to edit an existing policy.
3. Configure the following server policy settings:

Setting	Description
RADIUS User Pools	Select one or multiple RADIUS user pool from the available list
RADIUS Groups	Select one or multiple RADIUS user groups
LDAP Server Dead Period	Type or use the spinner to assign LDAP server inactive period in seconds. The range is 0 through 600 seconds, and the default is 300 seconds
LDAP Group Verification	Select this option to add verification to an LDAP group. This option is selected by default
LDAP Chase Referral	This option is not selected by default
Local Realm	Type a local realm name and add it to the RADIUS server

4. Configure the following authentication settings:

Setting	Description
Default Source	Select the RADIUS source designated for user authentication requests. The default selection is Local
Default Fallback	Select the option to activate a fallback option to revert to local RADIUS resources if the designated external LDAP resource were to fail or become unavailable. This option is not selected by default
Sources	Select Add to create a new authentication data source settings. Settings include: <ul style="list-style-type: none"> • Precedence - Set a precedence between 1 and 5000 • SSID - Assign a SSID • Source - Select a local or LDAP source • Fallback - Select this option to provide fallback for the source

Setting	Description
Authentication Type	Select an authentication type from the list of available authentication options. The default selection is ALL
Do Not Verify Username	Select this option to not verify a username during user authentication
Enable EAP Termination	Extensible Authentication Protocol (EAP) is used to provide secured authentication access to WLANs. When using an external RADIUS server, EAP requests are forwarded. Select this option to cancel EAP authentication
Enable CRL Validation	Select this option to validate CRL check
Bypass CRL Check	Select this option to skip CRL check. This option is selected by default
Allow Expired CRL	Select this option to permit CRL check past the date. This option is selected by default
LDAP Agent	Select Add to create a new LDAP agent. Configure the following LDAP Agent settings: <ul style="list-style-type: none"> • Username - Type a unique username for the LDAP agent • Password - Type a password to use with the LDAP agent username • Confirm Password - Retype the password • Redundancy - Select primary or secondary redundancy. The default option is primary • Domain Name - Provide a domain name for the LDAP Agent Select Add to save the LDAP Agent settings

5. Configure session resumption or fast reauthentication settings:

Setting	Description
Enable Session Resumption	Select this option to force an EAP supported clients to reauthenticate
Cached Entry Lifetime	Assign cached entry lifetime between 1 and 24 hours. The default option is 1 hour
Maximum Cache Entries	Assign maximum cache entries between 1 and 1,024. The default option is 128 entries

6. Select **Save** to update server policy configuration.

Configure RADIUS Clients

About This Task

A RADIUS client is a mechanism to communicate with a central server to authenticate users and authorize access to the controller, service platform or access point managed network.

The client and server share a secret (a password). That shared password followed by the request authenticator is put through a MD5 hash algorithm to create a 16 octet value which is XORed with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS access request packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified access accept packet, and if the username and password are correct, then the user is authenticated. If the client receives a verified access reject message, the user is not authenticated.

To define a RADIUS client configuration:

Procedure

1. Go to **Policies > RADIUS Server**.
2. Select a RADIUS Server from the list and navigate to the **Client** dashboard.
3. Select **Add** to create a new client IP address, mask, and a shared secret.
The **RADIUS Clients** dashboard opens.
4. Configure RADIUS clients settings:

Setting	Description
IP Address/Mask	Specify the IP Address and mask of the RADIUS client authenticating with the RADIUS server
Shared Secret	Specify a Shared Secret for authenticating the RADIUS client Shared secrets verify RADIUS messages with a RADIUS enabled-device configured with the same shared secret

5. Select **Add** to create include the RADIUS clients settings.
6. Select **Save** to update the RADIUS clients configuration.

Configure RADIUS Proxy

About This Task

A user's access request is sent to a proxy server if it cannot be authenticated by a controller or service platform local RADIUS resources. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to the NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the RADIUS server receives a request for a user name containing a realm, the server references a table of configured realms. If the realm is known, the server proxies the request to the RADIUS server. The behavior of the proxying server is configuration-dependent on most servers. In addition, the proxying server can be configured to add, remove, or rewrite requests when they are proxied.

To define a proxy configuration:

Procedure

1. Go to **Policies > RADIUS Server**.
2. Select a radius server and navigate to the **Proxy** dashboard.
3. Configure the proxy settings:

Setting	Description
Proxy Retries	<ul style="list-style-type: none"> • Proxy Retry Delay - Type the Proxy server retry delay time in the Proxy Retry Delay field. Enter a value from 5 -10 seconds. This is the interval the RADIUS server waits before making an additional connection attempt. The default delay interval is 5 seconds • Proxy Retry Count - Type the Proxy server retry count value in the Proxy Retry Count field. Set the number of retries from 3 - 6 sent to proxy server before giving up the request. The default retry count is 3 attempts
Realms	<p>Select Add to create a RADIUS server policy realm and network address.</p> <p>Select  icon to delete an existing RADIUS service policy.</p> <p>Configure the following realms settings:</p> <ul style="list-style-type: none"> • Realm Name - Assign a realm name in the Realm Name field. The realm name cannot exceed 50 characters. When the RADIUS server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server • IP Address - Provide the Proxy server IP address in the IP Address field. This is the address of server checking the information in the user access request and either accepting or rejecting the request on behalf of the local RADIUS server • Port Number - Type the TCP/IP port number for the server used as a data source for the proxy server. Use the spinner to select a value from 1024 and 65535. The default port is 1812 • Shared Secret - Provide the RADIUS client shared secret password in the Shared Secret field. This password is for authenticating the RADIUS proxy <p>Select the  icon to reveal the shared secret's character string</p> <p>Select Add to include the realm in the proxy server.</p>

4. Select **Save** to update the changes.

Configure an LDAP Server

About This Task

Administrators have the option of using RADIUS server resources to authenticate users against an external LDAP server resource. Using an external LDAP user database allows the centralization of user information and reduces administrative overhead, making the RADIUS authorization process more secure and efficient.

RADIUS is a protocol for asking questions to a user database like LDAP. LDAP however is just a database of user credentials that can be used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location. Local controller or service platform RADIUS resources provide the tools to perform user authentication and authorize users based on complex checks and logic.

To configure an LDAP server configuration for use with the RADIUS server:

Procedure

1. Go to **Policies > RADIUS Server**.
2. Select a policy from the **RADIUS Server** list and navigate to the **LDAP** dashboard.
3. Select **Add** to configure LDAP Server settings:

Setting	Description
Redundancy	<p>Define whether this LDAP server is a primary or secondary server resource. Primary servers are always queried for connection first.</p> <p>Tip: The best practice is to designate at least one secondary server is a good practice to ensure RADIUS user information is available if a primary server is unavailable</p> <p>Primary option is selected by default</p>
Network	<ul style="list-style-type: none"> • IP Address - Set the 128-character maximum IP address or FQDN of the external LDAP server acting as the data source for the RADIUS server • Login - Define a unique login name used for accessing the remote LDAP server resource. Consider using a unique login name for each LDAP server provided to increase the security of the connection to the remote LDAP server • Port Number - Use the spinner control to set the physical port number used by the RADIUS server to secure a connection with the remote LDAP server. The default option is 389 • Timeout - Set an interval from 1 - 10 seconds the local RADIUS server uses as a wait period for a response from the primary or secondary LDAP server. The default setting is 10 seconds

Setting	Description
Access	<ul style="list-style-type: none"> • Secure Mode - Specify the security mode when connecting to an external LDAP server. Use start-tls or tls-mode to connect. The start-tls mode provides a way to upgrade a plain text connection to an encrypted connection using TLS. The default port value for start-tls is 389. The default port value for stls-mode is 636 • Bind DN - Specify the distinguished name to bind with the LDAP server. The distinguished name (DN) is the name that uniquely identifies an entry in the LDAP directory. A DN is made up of attribute value pairs, separated by commas • Base DN - Specify a DN that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. LDAP DNs begin with the most specific attribute (usually some sort of name), and continue with progressively broader attributes, often ending with a country attribute. The first component of the DN is referred to as the Relative Distinguished Name (RDN). It identifies an entry distinctly from any other entries that have the same parent • Bind Password - Type a valid password for the LDAP server. The password cannot exceed 32 characters • Password Attribute - Type the LDAP server password attribute. The password cannot exceed 64 characters
Attribute	<ul style="list-style-type: none"> • Group Attribute - LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group, an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password, or group membership name • Group Filter - The group filters used by the LDAP server. This filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service • Group Membership Attribute - The group member attribute sent to the LDAP server when authenticating users

4. Select **Add** to update LDAP server settings.
5. Select **Save** to change LDAP settings.

Auto-Provisioning Policy

Wireless devices can adopt and manage other wireless devices. For example, a wireless controller can adopt any number of access points. When a device is adopted, the device configuration is provisioned by the adopting device. Since multiple configuration policies are supported, an adopting device needs to define which configuration policies are used for a given adoptee. Auto-provisioning policies determine which configuration policies are applied to an adoptee based its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CDP snoop strings, etc.

Once created an auto-provisioning policy can be used in profiles or device configuration objects. An Auto-Provisioning policy contains a set of ordered by precedence rules that either deny or allow adoption based on potential adoptee properties and a catch-all variable that determines if the adoption should be allowed when none of the rules is matched. All rules (both deny and allow) are evaluated sequentially starting with the rule with the lowest precedence. The evaluation stops as soon as a rule has been matched, no attempt is made to find a better match further down in the set.

The **Auto-Provisioning** dashboard displays the following read-only information:

Setting	Description
Auto-Provisioning Policy	Lists the name of each policy when it was created. It cannot be modified as part of the Auto-provisioning policy's edit process
Adopt if no Rules Match	Displays whether this policy will adopt devices if no adoption rules apply. The result is displayed as a green checkmark. This feature is not activated by default
Rerun Policy Rules Every Time AP Adopts	Displays whether this policy will be run every time an AP is adopted. The result is displayed as a green checkmark. This feature is not activated by default
Action	Edit or delete an existing auto-provisioning policy

Related Topics

[Configure Auto-Provisioning Policy Rules](#) on page 108

[Configure Auto-Provisioning Policy Adoption Criteria](#) on page 111

Configure Auto-Provisioning Policy Rules

About This Task

Auto-provisioning policies are created or modified as unique deployment requirements to deploy changes in the number of access point radios within a specific radio coverage area.

Add a new auto-provisioning policy or edit an existing policy configuration:

Procedure

1. For modifying an existing policy, select a policy from the **Auto-Provisioning** policy dashboard.
2. The **Rules** dashboard opens.

3. Review the following data to determine whether a rule can be used as is, requires an edit, or whether new rules need to be defined:

Setting	Description
Rule Precedence	Displays the precedence (sequence) the adoption policies rules are applied. Rules with the lowest precedence receive the highest priority. This value is set from 1 to 10,000 when adding a new auto-provisioning policy rule configuration.
Operation	Lists the operation taken upon receiving an adoption request from an access point: The following operations are available: <ul style="list-style-type: none"> • allow • deny • redirect • upgrade
Device Type	Sets the access point or controller model for which this policy applies. Adoption rules are specific to the selected model
Match Type	Lists the matching criteria used in the policy. This is a filter and further refines the APs that can be adopted. The options are: <ul style="list-style-type: none"> • Any • CDP • DHCP Option • FQDN • IP • IPv6 • LLDP • MAC Address • Model Number • Serial Number • VLAN
Argument 1	The number of arguments vary on the Match Type. This column lists the first argument value. This value is not set as part of the rule creation or edit process
Argument 2	The number of arguments vary on the Match Type. This column lists the second argument value. This value is not set as part of the rule creation or edit process
Site/Alias	Lists the site name where the policy is applied
Profile Name	Defines the name of the profile used when the auto-provisioning policy is applied to a device
Action	Select  icon to edit an existing policy or  icon to delete an existing policy

4. Select **+** to create a new policy rule.
The **Add Policy** dashboard opens.
5. Provide a name and select **Add**. The name must not exceed 32 characters.
The **Rules** dashboard opens.
6. Select **+** to add new rules settings and configure the following parameters:

Setting	Description
Rule Precedence	Assign a priority from 1 - 10,000 for the application of the autoprovisioning policy rule. Rules with the lowest value have priority and the default value is 1
Operation	Define the operation taken upon receiving an adoption request from an access point. The options are: <ul style="list-style-type: none"> • allow - Allows the normal provisioning of connected access points upon request • deny - Prohibits the provisioning of connected access point upon request • redirect - When selected, an access point seeks a steering controller (upon adoption request), that will forward the network credentials of a designated controller resource that initiates the provisioning process • upgrade - Conducts the provisioning of requesting access points from this controller resource
Device Type	Sets the access point model for which this policy applies. Adoption rules are specific to the selected model, as radio configurations are often unique to specific models
Site/Alias	Use the site to which the device is adopted automatically. Use the drop-down list box to select the desired site or alias
Profile Name	Define the profile used when an auto-provisioning policy is applied to a device

Setting	Description
Match Type	Lists the matching criteria used in the policy. This is a filter and further refines the APs that can be adopted. The options are: <ul style="list-style-type: none"> • MAC Address – The filter type is a MAC Address of the selected access point model • IP Address – The filter type is the IP address of the selected access point model • VLAN – The filter type is a VLAN • Serial Number – The filter type is the serial number of the selected access point model • Model Number – The filter type is the access point model number • DHCP Option – The filter type is the DHCP option value of the selected access point model
Area	Type a 64 character maximum deployment area name assigned to this policy
Floor	Type a 32 character maximum deployment floor name assigned to this policy
Controller 1	If you have set Operation to redirect , provide a 1st choice steering controller Hostname or IP Address and pool to forward network credentials for a controller resource to initiate the provisioning process. The pool options are 1 or 2
Controller 2	If you have set Operation to redirect , provide a 2nd choice steering controller Hostname or IP Address and pool to forward network credentials for a controller resource to initiate the provisioning process. The pool options are 1 or 2
Routing Level	If you have set Operation to redirect , specify the routing level as 1 or 2.
Upgrade	Select the upgrade option to advance the policy

7. Select **Update** to configure rules settings.
8. Select **Save** to update the auto-provisioning policy rule.

Configure Auto-Provisioning Policy Adoption Criteria

About This Task

Configure the auto-provisioning policy's default to match adoption configuration.

Procedure

1. Select **Policies > Auto-Provisioning > Auto-Provisioning Policy > Default**.
The **Default** dashboard opens.
2. Select **Adopt if No Rules Match** to adopt when no matching filter rules apply.
3. Select **Rerun Policy Rules Every Time AP Adopts** to run this policy and apply its rule set every time an access point is adopted.

4. Select **Save** to update default auto-provisioning policy rule information.

Firewall

A Firewall is a first line of defense in protecting proprietary information within the access-point managed network. Firewall helps blocking and permitting data traffic in the network.

With WiNG access points, firewalls are configured to protect against unauthenticated logins from outside the network. This helps prevent hackers from accessing managed wireless clients. Well designed firewalls block traffic from outside the network while permitting authorized users to communicate freely outside the network.

All traffic entering or leaving a controller or service platform passes through the firewall, which examines each message and blocks the ones that do not meet the predefined security rules.

Related Topics

- [Configure a Firewall Policy](#) on page 112
- [Firewall Policy Denial of Service \(DoS\)](#) on page 116
- [Configure Firewall Policy Storm Control](#) on page 121
- [Configure Firewall Policy IPv6 Settings](#) on page 122

Configure a Firewall Policy

About This Task

Firewall configurations can be defined as separate policies available to the administrator for specific controller or service platform.

Procedure

1. Select **Policies > Firewall** to view existing firewall policies.
2. Refer to the following configuration data for existing wireless firewall policies:

Setting	Description
Firewall Policy	Displays the name assigned to the policy when created. The name cannot be modified as part of the edit process
Status	Displays a green check mark if the policy has been activated
Action	Edit or delete an existing firewall policy

3. Select  to create a new firewall policy.
The **Add Policy** dashboard opens.
4. Provide a name for the policy not exceeding 64 characters.
5. Select **Add** to create a new firewall policy.
The **Basic** firewall settings dashboard opens.

6. Configure the basic firewall policy settings.

The firewall policy configuration is divided into the following dashboards:

- [Firewall policy basic settings](#)
- [Firewall policy denial of service \(DOS\) settings](#)
- [Firewall policy storm control settings](#)
- [Firewall policy IPv6 settings](#)

Basic Firewall Policy Settings

About This Task

Use the basic settings to define the common firewall policy settings.

Procedure

1. Select **Basic** tab.
2. Configure or modify **Firewall Status** settings.

The **Firewall Status** is selected by default. Toggle to turn off firewall status.
3. Configure the following settings for new or existing firewall status:

Setting	Description
Enable Proxy ARP	Select Enable Proxy ARP to allow the Firewall Policy to use Proxy ARP responses for this policy on behalf of another device. Proxy ARP allows the firewall to handle ARP routing requests for devices behind the firewall. This feature is selected by default
DHCP Broadcast to Unicast	Select DHCP Broadcast to Unicast for the conversion of broadcast DHCP offers to unicast. Converting DHCP broadcast traffic to unicast traffic can help reduce network traffic loads. This feature is not selected by default
L2 Stateful Packet Inspection	Select L2 Stateful Packet Inspection for stateful packet inspection for RF Domain manager routed interfaces within the Layer 2 firewall. This feature is not activated by default
TCP MSS Clamping	Select TCP MSS Clamping for TCP MSS Clamping. TCP MSS Clamping allows for the configuration of the maximum segment size of packets at a global level
IPMAC Conflict Enable	When multiple devices on the network have the same IP or MAC address this can create routing issues for traffic being passed through the firewall. To avoid these issues, select IPMAC Conflict Enable for IP and MAC conflict detection. This feature is selected by default
IPMAC Conflict Action	Use the drop-down list box to set the action taken when an attack is detected. Options include Log Only, Drop Only, or Log and Drop. The default setting is Log and Drop

Setting	Description
IPMAC Conflict Logging	Select IPMAC Conflict Logging for logging for IP and MAC address conflict detection. The default selection is Warnings
IP TCP Adjust MSS	Select IP TCP Adjust MSS and adjust the value for the maximum segment size (MSS) for TCP segments on the router. Set a value between 472 bytes and 1,460 bytes to adjust the MSS segment size. The default value is 0
IPMAC Routing Conflict Enable	Select IPMAC Routing Conflict Enable for IPMAC Routing Conflict detection. This is also known as a Hole-196 attack in the network. This feature helps to detect if the client is sending routed packets to the correct router-mac-address
IPMAC Routing Conflict Action	Use the drop-down list box to set the action taken when an attack is detected. Options include Log Only, Drop Only, or Log and Drop. The default setting is Log and Drop
IPMAC Routing Conflict Logging	Select IPMAC Routing Conflict Logging for conflict detection
DNS Snoop Entry Timeout	Set a timeout in seconds for DNS Snoop Entry. DNS Snoop Entry stores information such as Client to IP Address and Client to Default Gateways and uses this information to detect if the client is sending routed packets to a wrong MAC address. The range is 30 through 86,400 seconds, and the default value is 1,800 seconds
Virtual Defragmentation	Select Virtual Defragmentation for IPv4 and IPv6 virtual defragmentation to help prevent fragment based attacks, such as tiny fragments or large number of fragments
Virtual Defragmentation Timeout	Set a virtual defragmentation timeout from 1 to 60 seconds applicable to both IPv4 and IPv6 packets. The default value is 1
Max Defragmentations/Datagram	Set a value for the maximum number of defragments between 2 and 8,129 allowed in a datagram before it is dropped. The default value is 140
Max Fragments/Host	Set a value for the maximum number of fragments, between 1 and 16,384 allowed per host before it is dropped. The default value is 8
Min Length Required	Select Min Length Required to set a minimum length between 8 bytes and 1,500 bytes to enforce a minimum packet size before being subject to fragment based attack prevention

4. Configure the following settings for new or existing firewall enhanced logging:

Setting	Description
Log Dropped ICMP Packets	Use the drop-down list box to define how dropped ICMP packets are logged. Logging can be rate limited for one log instance every 20 seconds. Options include Rate Limited, All, or <none>. The default setting is <none>
Log Dropped Malformed Packets	Use the drop-down list box to define how dropped malformed packets are logged. Logging can be rate limited for one log instance every 20 seconds. Options include Rate Limited, All, or <none>. The default setting is <none>
Enable Verbose Logging	Toggle to activate verbose logging mode for the firewall
Enable Stateful DHCP Checks	Toggle to activate stateful DHCP checks for the firewall

5. Configure the following settings for new or existing firewall application layer gateway:

Setting	Description
FTP ALG	Select FTP ALG to allow FTP traffic through the firewall using its default ports. This feature is selected by default
TFTP ALG	Select TFTP ALG to allow TFTP traffic through the firewall using its default ports. This feature is selected by default
PPTP ALG	Select PPTP ALG to allow PPTP traffic through the firewall using its default ports. The Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to an enterprise server by creating a VPN across TCP/IP-based data networks. PPTP encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. This feature is selected by default
SIP ALG	Select SIP ALG to allow SIP traffic through the firewall using its default ports. This feature is not selected by default
SCCP ALG	Select SCCP ALG to allow SCCP traffic through the firewall using its default ports. This feature is not selected by default
Facetime ALG	Select Facetime ALG to allow Facetime traffic through the firewall using its default ports. This feature is not selected by default
DNS ALG	Select DNS ALG to allow DNS traffic through the firewall using its default ports. This feature is selected by default

6. Define flow timeout intervals for the following flow types impacting the firewall:

Setting	Description
TCP Close Wait	Define a flow timeout value in seconds (1 to 32,400). The default setting is 10 seconds
TCP Established	Define a flow timeout value in seconds (1 to 32,400). The default setting is 5,400 seconds
TCP Reset	Define a flow timeout value in seconds (1 to 32,400). The default setting is 10 seconds
TCP Setup	Define a flow timeout value in seconds (1 to 32,400). The default setting is 10 seconds
Stateless TCP Flow	Define a flow timeout value in seconds (1 to 32,400). The default setting is 90 seconds
Stateless FIN/RESET Flow	Define a flow timeout value in seconds (1 to 32,400). The default setting is 10 seconds.
ICMP	Define a flow timeout value in seconds (1 to 32,400). The default setting is 30 seconds
UDP	Define a flow timeout value in seconds (15 to 32,400). The default setting is 30 seconds
Any Other Flow	Define a flow timeout value in seconds (1 to 32,400). The default setting is 30 seconds

7. Configure the TCP Protocol Checks to set the following parameters:

The TCP Protocol Check are selected by default

Setting	Description
Check TCP states where a SYN packet tears down the flow	This option allows a SYN packet to delete an old flow in TCP_FIN_FIN_STATE and TCP_CLOSED_STATE and creates a new flow
Check unnecessary resends of TCP packets	This option allows the checking of unnecessary resends of TCP packets
Check sequence number in ICMP Unreachable error packets	This option allows sequence number checks in ICMP unreachable error packets when an established TCP flow is stopped
Check acknowledgment number in RST packets	This option allows the checking of the acknowledgment number in RST packets which stops a TCP flow in the SYN state
Check sequence number in RST packets	This option checks the sequence number in RST packets which stops an established TCP flow

8. Select **Save** to update the firewall basic settings.

Firewall Policy Denial of Service (DoS)

About This Task

A Denial of Service (DoS) attack is an attempt to make a computer or network resource unavailable to its intended users. Although the means to carry out a DoS attack will vary, it generally consists of a

concerted effort of one or more persons attempting to prevent a device, site or service from functioning temporarily or indefinitely.

Most DoS attacks involve saturating the target device with external communications requests so it cannot respond to legitimate traffic or respond so slowly the device becomes unavailable in respect to its defined data rate. DoS attacks are implemented by either forcing targeted devices to reset or consuming the device's resources so it can no longer provide service.

To define a denial of service configuration for a Firewall policy:

Procedure

1. Go to **Policies > Firewall > Firewall Policy > DoS**
2. The **Settings** dashboard contains a list of all of the DoS attacks for which the wireless controller's firewall has filters.

Each DoS filter contains the following items:

Setting	Description
Event	Lists the name of each DoS attack
Enable	Select Enable to set the firewall policy to filter the associated DoS attack based on the selection in the Action column
Action	If a DoS filter is selected, chose an action from the drop-down list box to determine how the firewall policy treats the associated DoS attack <ul style="list-style-type: none"> • Log and Drop - An entry for the associated DoS attack is added to the log and then the packets are dropped • Log Only - An entry for the associated DoS attack is added to the log. No further action is taken • Drop Only - The DoS packets are dropped. No further action is taken
Log Level	Select to enable logging to the system log. Then select a standard Syslog level from the Log Level drop-down list box
Info	Additional information about the DoS firewall setting

3. Refer to the following for a summary of each Denial of Service attack the firewall can filter.

Setting	Description
Ascend	Series of attacks that target known vulnerabilities in various versions of Ascend routers
Broadcast/Multicast ICMP	A series of attacks that take advantage of ICMP behavior in response to echo replies. These usually involve spoofing the source address of the target and sending ICMP broadcast or multicast echo requests to the rest of the network and in the process flooding the target machine with replies

Setting	Description
Chargen	Establishes a Telnet connection to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services
Fraggle	Uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic
FTP Bounce	Uses a vulnerability in the FTP "PORT" command as a way to scan ports on a target machine by using another machine in the middle
Invalid Protocol	Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, called hijacking, or a DoS attack
IP TTL Zero	Sends spoofed multicast packets onto the network which have a Time To Live (TTL) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload
IP Spoof	A category of DoS attack that sends IP packets with forged source addresses. This can hide the identity of the attacker
LAND	Sends spoofed packets containing the SYN flag to the target destination using the target port and IP address as both the source and destination. This will either crash the target system or result in high resource utilization slowing down all other processes
Option Route	Enables the IP Option Route denial of service check in the firewall
Router Advertisement	In this attack, the attacker uses ICMP to redirect the network router function to some other host. If that host can not provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the 'false' router). By providing router services from a compromised host, the attacker can also place themselves in a man-in-the-middle situation and take control of any open channel at will. This is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions

Setting	Description
Router Solicit	<p>The ICMP Router Solicitation scan is used to actively find routers on a network. Of course, a hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network. ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122).</p> <p>By sending ICMP router solicitation packets (ICMP type 9) on the network and listening for ICMP router discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests</p>
Smurf	Sends ICMP echo requests to a list of broadcast addresses in a row, and then repeats the requests, thus flooding the network
Snork	Uses UDP packet broadcasts to consume network and system resources
TCP Bad Sequence	Enables a TCP Bad Sequence denial of service check in the firewall
TCP FIN Scan	<p>Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the Finish (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply</p>

Setting	Description
TCP Intercept	<p>A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing email, using FTP service, and so on. The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.</p> <p>When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.</p>

Setting	Description
TCP Null Scan	Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. This type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply
TCP Post SYN	A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an Intrusion Detection System (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS
TCP Packet Sequence Past Window	An attempt to predict the sequence number used to identify packets in a TCP connection, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number used by the sending host. If successful, they can send counterfeit packets to the receiving host which will seem to originate from the sending host, even though the counterfeit packets may originate from some third host controlled by the attacker
TCP XMAS Scan	The TCP XMAS Scan floods the target system with TCP packets including the FIN, URG, and PUSH flags. This is used to determine details about the target system and can crash a system
TCP Header Fragment	Enables the TCP Header Fragment denial of service check in the firewall
Twinge	Sends ICMP packets and cycles through using all ICMP types and codes. This can crash some Windows systems
UDP Short Header	Enables the UDP Short Header denial of service check in the firewall
WINNUKE	Sends a large amount of data to UDP port 137 to crash the NETBIOS service on windows and can also result on high CPU utilization on the target machine

4. Select events individually to enable or deactivate event settings.
5. Select **Save** to update the DoS settings.

Configure Firewall Policy Storm Control

About This Task

The firewall maintains a facility to control packet storms. Storms are packet bombardments that exceed the high threshold value configured for an interface. During a storm, packets are throttled until the rate

falls below the configured rate, severely impacting performance for the site manager interface. Thresholds are configured in terms of packets per second.

To define a storm control configuration for a Firewall policy:

Procedure

1. Go to **Policies > Firewall > Firewall Policy > Storm Control**.
2. Select **Add** to create new storm control policy settings.

Setting	Description
Traffic Type	Use the drop-down list box to define the traffic type for which the Storm Control configuration applies. Options include ARP, Broadcast, Multicast, and Unicast
Interface Type	Use the drop-down list box to define the interface for which the Storm Control configuration is applied. Only the specified interface uses the defined filtering criteria. Options include Ethernet, WLAN, and Port Channel
Interface Name	Use the drop-down list box to refine the interface selection to a specific WLAN or physical port. This helps with threshold configuration for potentially impacted interfaces
Packets per Second	Type or use the spinner tool to select the packet per second between 1 to 1,000,0000

3. Select **Add** to save storm control settings.
4. Select **Add** to create new storm control logging settings.

Setting	Description
Traffic Type	Use the drop-down list box to define the traffic type for which the Storm Control logging configuration applies. Options include ARP, Broadcast, Multicast, and Unicast
Logging	Select a logging setting used for specifying the standard log level used if a Storm Control attack is detected

5. Select  to delete existing settings.
6. Select **Add** to create more storm control settings and logging settings.
7. Select **Save** to update storm control configuration.

Configure Firewall Policy IPv6 Settings

About This Task

IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery (ND) protocol via ICMPv6 router discovery messages. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. When first connected to a network, a host sends a link-local

router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.

To define a firewall policy IPv6 settings:

Procedure

1. Select **Firewall > Policy > Firewall Policy > IPv6**.
2. Toggle to activate or deactivate **IPv6 Firewall**.

The IPv6 firewall provides support to IPv6 packet streams. This setting is selected by default. Deactivating IPv6 firewall support also deactivates proxy neighbor discovery.

3. Select **IPv6 Rewrite Flow** to provide flow label rewrites for each IPv6 packet.

A flow is a sequence of packets from a particular source to a particular (unicast or multicast) destination. The flow label helps keep packet streams from looking like one massive flow. Flow label rewrites are not selected by default.

Flow label re-writes enable the re-classification of packets belonging to a specific flow. The flow label does nothing to eliminate the need for packet filtering.

4. Select **Enable Proxy ND** to generate neighbor discovery responses on behalf of another controller or service platform.

When selected, any IPv6 packet received on an interface is parsed to see whether it is known to be a neighbor solicitation. This setting is selected by default.

5. Configure **Event Settings** to activate individual IPv6 unique events.

Setting	Description
Event	Lists the name of each IPv6 specific event subject to logging
Enable	Select Enable to set the firewall policy to filter the associated IPv6 event based on the selection in the Action column
Action	If a filter is selected, chose an action from the drop-down list box to determine how the firewall treats the associated IPv6 event <ul style="list-style-type: none"> • Log and Drop - An entry for the associated IPv6 event is added to the log and then the packets are dropped • Log Only - An entry for the associated IPv6 event is added to the log. No further action is taken • Drop Only - The packet is dropped. No further action is taken
Log Level	Select Log Level and then select a standard log level from the Log Level drop-down list box
Info	Additional information about IPv6 settings

6. Select **Save** to update IPv6 firewall policy settings.

SmartRF Policy

Self Monitoring At Run Time RF Management (Smart RF) is an innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization radio performance improvements.

A Smart RF policy can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power for each radio. Smart RF policies can be added to specific RF Domains to apply site specific deployment configurations and self-healing values to device groups.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using data obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs by constantly monitoring the network for external WiFi interference, neighbor WiFi interference, non-WiFi interference and client connectivity. Smart RF then intelligently applies various algorithms to arrive at the optimal channel and power selection for all access points in the network and constantly reacts to changes in the RF environment.

Smart RF also provides self-healing functions by monitoring the network in real-time and provides automatic mitigation from potentially problematic events such as radio interference, non-WiFi interference (noise), external WiFi interference, coverage holes and radio failures. Smart RF employs self-healing to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual reconfiguration to resolve.

Smart RF is supported on any RF Domain manager. In standalone environments, an individual controller, service platform or access point manages the calibration and monitoring phases. In clustered environments, a single device is elected a Smart RF master and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart RF master co-ordinates the calibration and configuration and during the monitoring phase receives information from the Smart RF clients.

If a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is activated, the radio picks a channel defined in the Smart RF policy
- If Smart RF is deactivated, but a Smart RF policy is mapped, the radio picks a channel specified in the Smart RF policy
- If no Smart RF policy is mapped, the radio selects a random channel

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access points detects radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired. Change this behavior using a `dfs-rehome` command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.



Note

RF planning must be performed to ensure overlapping coverage exists at a deployment site for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it.

Sensor Policy

The ExtremeLocation system for Wi-Fi locating includes WiNG controllers functioning as sensors. Within the ExtremeLocation architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated ExtremeLocation server resource, as opposed to an ADSP server. The ExtremeLocation server collects the RSSI data from WiNG sensor devices, and calculates the location of Wi-Fi devices.

Related Topics

[Configure a Sensor Policy](#) on page 125

Configure a Sensor Policy

About This Task

Use the sensor policy to collect RSSI data from WiNG sensor devices. Edit an existing policy or create a new sensor policy for controllers.

Procedure

1. Select **Policies > Sensor Policy**.

The **Sensor** dashboard opens.

2. Select  to create a new sensor policy or select  to edit an existing policy.

The **Details** dashboard opens.

3. Provide a unique policy name.



Note

Sensor policy name cannot exceed 32 characters and cannot contain spaces. Define a name unique to the policy's channel and scan mode configuration to help differentiate it from other policies.

4. Select **Add** to create a new policy.
5. Configure the following sensor policy details:

The **Sensor Policy Details** dashboard displays with the Scan Mode set to Default-Scan. The user configurable parameters on this dashboard differ, depending on which Scan Mode is selected.

6. Use the RSSI Scan Interval drop-down list box to set a scan interval from 1 - 60 seconds.

This is the scan period used by dedicated sensors for RSSI (signal strength) assessments. Once the sensor obtains the RSSI data, the sensor sends the data to a specified ExtremeLocation server resource for calculating Wi-Fi device locations. The default is 10 seconds.

7. The following Scan Mode values are available:

The values depend on whether you have selected **Default-Scan**, **Custom-Scan**, or **Channel-Lock** as the mode for scan operation.

Setting	Description
Channel	<p>With Default-Scan selected: The list of available scan channels is fixed and defaulted in a spread pattern of channels 1, 6, 11, 36, 40, 44, and 48. You cannot change this channel pattern</p> <p>With Custom-Scan selected: A list of unique channels in the 2.4, 4.9, 5, and 6 GHz band can be collectively or individually enabled for customized channel scans and RSSI reporting</p> <p>With Channel-Lock selected: The Channel, Channel Width, and Scan Weight fields are replaced by a Lock Frequency drop-down menu. Use this menu to lock the RSSI scan to one specific channel</p>
Channel Width	<p>With Default-Scan selected: Each channel's width is fixed and defaulted to either 40MHz-Upper (Ch 1), 40MHz-Lower (Ch 6 and CH 11) or 80MHz (CH 36, CH 40, CH 44 and CH 48)</p> <p>With Custom-Scan selected: You can define the width for each selected channel. Note that many channels have their width fixed at 20MHz. 802.11a radios support 20 MHz and 40 MHz channel widths</p> <p>With Channel-Lock selected: You cannot adjust the width between adjacent channels, because only one channel is locked</p>
Scan Weight	<p>With Default-Scan selected: Each default channel's scan is of equal duration (1000) within the defined RSSI scan interval. No one channel receives scan priority within the defined RSSI scan interval.</p> <p>With Custom-Scan selected: Each selected channel can have its weight prioritized in respect to the amount of time a scan is permitted within the defined RSSI scan interval</p> <p>With Channel-Lock selected: With one channel locked for an RSSI scan, you cannot adjust scan weights for other, unlocked channels</p>

8. Select **Save** to update the sensor policy.

Configure an Event System Policy

About This Task

Use Event System Policy to define or override how controller or service platform system messages are logged and forwarded on behalf of the profile

Procedure

1. Select **Policies > Event System**.

The **Event System** list opens.

2. Select an **Event System Policy** from the list to edit it.

If a policy does not exist, select  to configure a new policy.

3. Provide a unique policy name and select **Add**.

The **Details** dashboard opens.

4. Configure event module details.

- a. Choose an event from the **Select Event Module** drop-down list box to track the occurrence of each list event.

The list of events change according to the selected event module.

- b. Review each event and select or clear the **Forward to Controller**, **Email**, **SNMP**, and **Syslog** options as required for the event.
- c. Select **Save** to update event system details configuration.

Configure a Device Categorization Policy

About This Task

Having devices properly classified can help suppress unnecessary unsanctioned alarms. It allows an administrator to focus on the alarms and devices that are causing issues. An intruder with a device erroneously authorized could potentially perform activities that can harm your organization while appearing to be legitimate. Device categorization policy enables devices to be categorized as access points or wireless clients, then defined as sanctioned or unsanctioned within the network.

Sanctioned access points and wireless clients conform with the organization's security policies. Unsanctioned devices interoperate within the managed network, but are not approved. These devices should be filtered to avoid jeopardizing data.

Procedure

1. Select **Policies > Device Categorization**.

The **Device Categorization** list displays the authorization policies defined thus far.

2. Select  to create a new policy or  to edit an existing policy.

3. For new policy, provide a unique policy name not exceeding 64 characters.

4. Select **Add**.

The **Marked Devices Details** dashboard opens.

5. Select **Add** to configure marked devices settings:

Setting	Description
Index	Use the spinner controls to set the Index number for each Device Categorization Name. The default setting is 1
Classification	Use the drop-down list box to designate the target device as either sanctioned (True) or neighboring (False)
Device Type	Use the drop-down list box to designate the target device as either an access point or wireless client
MAC Address	Type the factory coded MAC address of the target device. This address is hard coded by the device manufacturer and cannot be modified. The MAC address will be defined as sanctioned or unsanctioned as part of the device categorization process
SSID	Type the SSID of the target device requiring categorization. The SSID cannot exceed 32 characters

6. Select **Add** to update **Marked Devices** settings.

WIPS Policy

The WIPS (Wireless Intrusion Protection System) provides continuous protection against wireless threats and acts as an additional layer of security complementing wireless VPNs and existing encryption and authentication policies. Controllers and service platforms support WIPS through the use of dedicated sensor devices, designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block devices using manual termination, air lock down, or port suppression.

Related Topics

[Configure a WIPS Policy](#) on page 128

[Configure WIPS Events](#) on page 130

[Configure WIPS Signatures](#) on page 132

Configure a WIPS Policy

About This Task

Unauthorized device detection needs to be activated for each WIPS policy. Whether currently activated or deactivated, a WIPS policy can have specific categorization policies defined and specific events activated for detection. Once defined, a WIPS policy is available for use with a controller or a service platform device profile.

Procedure

1. Select **Policies > WIPS**.
The **WIPS** dashboard opens.

2. The **WIPS** dashboard displays the following read-only information:

Setting	Description
Name	Displays the name assigned to the WIPS policy when it was initially created. The name cannot be modified as part of the edit process
Status	Displays a green check mark if the listed WIPS policy is activated and ready for use with a profile. A red "X" designates the listed WIPS policy as deactivated
Duplicate Detection Interval	Displays the duration when event duplicates or redundant events are not stored in event history

3. Select  to create a new WIPS policy,  to modify the attributes of a selected policy, or  to remove obsolete policies from the list of available policies.

If you are adding or editing an existing WIPS policy, the **WIPS** dashboard displays the **Basic** tab by default.

4. For new policies, assign a unique name not exceeding 64 characters.
5. Select **Add** to create a new policy.
The **Basic** configuration dashboard opens.
6. Configure the following WIPS policy basic settings:
 - a. Toggle to deactivate **WIPS Status**. The WIPS Status is activated by default.
 - b. Type an interval between 30 to 86,400 seconds in the **Duplicate Event Detection Interval** field. The default value is 120 seconds.
7. Refer to the **Rogue AP Detection** settings to define the following detection settings for a WIPS policy:

Setting	Description
Enable	Select Enable to activate the detection of unauthorized devices for this WIPS policy. The default setting is not selected
Wait Time to Determine AP Status	Define a wait time in 10 through 600 seconds before a detected AP is interpreted as a rogue device, and potentially removed. The default interval is 60 seconds
Ageout for AP Entries	Set the interval the WIPS policy uses to age out rogue devices. Set the policy in 30 to 86,400 seconds. The default setting is 1,800 seconds
Interference Threshold	Specify an RSSI threshold from -100 to -10 dBm after which a detected access point is classified as a rogue device. The default value is -75 dBm
Recurring Event	Set an interval between 0 to 10,000 seconds. When the interval is exceeded, the policy duplicates a rogue AP event if the rogue device is still active in the network. The default setting is 300 seconds

Setting	Description
Air Termination	Select Air Termination to activate the cancellation of detected rogue AP devices. Air termination lets you cancel the connection between your wireless LAN and any access point or client associated with it. If the device is a client, its connection with the access point is canceled. This setting is not selected by default
Air Termination Channel Switch	Select Air Termination Channel Switch to allow neighboring access points to switch channels for rogue AP cancellation. This setting is not selected by default
Air Termination Mode	If Air Termination is selected, use the drop-down list box to specify the cancellation mode used on detected rogue devices. The options are auto and manual, and the default setting is manual

8. Select **Save** to update the settings.

Related Topics

[WIPS Policy](#) on page 128

[Configure WIPS Events](#) on page 130

[Configure WIPS Signatures](#) on page 132

Configure WIPS Events

About This Task

Use WIPS Events to configure events, filters, and threshold values for a WIPS policy.

Procedure

1. Select **Policies > WIPS**.
2. Select an existing policy from the WIPS policy list.
The **Basic** dashboard opens.
3. Select **Events**.

The **Excessive** tab lists a series of events that can impact the performance of the network. An administrator can activate or deactivate the filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action.

An Excessive Action Event is an event where an action is performed repetitively and continuously. DoS attacks come under this category. Use the **Excessive Action Events** table to select and configure the action taken when events are triggered.

AP events can be globally activated and deactivated as required using the **Status** option.

4. Set the configurations for the following **Excessive Action Events**:

Setting	Description
Name	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted
Status	Displays whether tracking is activated for each Excessive Action Event. Use the Status option to activate or cancel events as required
Filter Expiration	Set the duration between 0 to 86,400 seconds to filter the anomaly causing client. This creates a special ACL entry and frames coming from the client are silently dropped. The default setting is 0 seconds. If a station is detected performing an attack and is filtered by one of the APs, the information is passed to the domain controller or service platform
Client Threshold	Set the client threshold between 0 to 65,535 seconds after which the filter is triggered and an event generated
Radio Threshold	Set the radio threshold between 0 to 65,535 seconds after which an event is recorded to the events history

5. Select **Save** to update excessive actions configuration used by the WIPS policy.
 6. Select **MU Anomaly**.

The **MU Anomaly Events** list opens.

7. Configure **MU Anomaly Events**.

MU anomaly events are suspicious events by wireless clients that can compromise the security and stability of the network. Use the **MU Anomaly Events** dashboard to configure the intervals clients can be filtered upon the generation of each defined event.

MU events can be globally activated and deactivated as required using the **Status** option.

MU Anomaly Events configurations:

Setting	Description
Name	Displays the name of the MU anomaly event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted
Status	Displays the status of the event and whether tracking is activated for each event. Each event is not selected by default. MU events can be globally activated and deactivated as required using the Status option

8. Select **Save** to update MU Anomaly Events configuration.

9. Select **AP Anomaly** to configure AP Anomaly Events.

AP anomaly events are suspicious frames sent by a neighboring access points. Use the **AP Anomaly** dashboard to determine whether an event is activated for tracking. AP events can be globally activated or deactivated as required using the **Status** option.

AP Anomaly configurations:

Setting	Description
Name	
Status	Displays the status of the event and whether tracking is activated for each AP anomaly event. Each event is not selected by default. AP events can be globally activated and deactivated as required using the Status option
Filter Expiration	Use the spinner to set filter expiration duration for the activated AP anomaly event between 0 to 86,400 seconds

10. Select **Save** to update AP Anomaly Events configuration.

Related Topics

[WIPS Policy](#) on page 128

[Configure a WIPS Policy](#) on page 128

[Configure WIPS Signatures](#) on page 132

Configure WIPS Signatures

About This Task

A WIPS signature is the set or parameters, or pattern, used by WIPS to identify and categorize particular sets of attack behaviors in order to classify them.

The **WIPS Signatures** dashboard displays the following read-only data:

Setting	Description
Name	Lists the name assigned to each signature when it was created. A signature name cannot be modified as part of the edit process
Status	Displays whether the signature is activated. A green check mark defines the signature as activated. A red "X" defines the signature as deactivated. Each signature is deactivated by default
BSSID MAC	Displays each BSS ID MAC address used for matching purposes and potential device exclusion
Source MAC	Displays each source MAC address of the packet examined for matching purposes and potential device exclusion

Setting	Description
Destination MAC	Displays each destination MAC address of the packet examined for matching purposes and potential device exclusion
Matching Frame	Lists the frame types specified for matching with the WIPS signature
Matching SSID	Lists each SSID used for matching purposes

Use the **Action** option to edit or delete a WIPS signature.

Procedure

1. Select  to create a new WIPS signature.
The **Basic** dashboard opens.
2. Assign a unique WIPS signature name not exceeding 64 characters.
3. Select **Add** to create the new WIPS signature.
The **WIPS Signature** basic settings dashboard opens.
4. Configure the following network address information for a new or modified WIPS Signature:

Setting	Description
Enable Signature	Clear the checkbox to deactivate the WIPS signature for use with the profile. The signature is activated by default
BSSID MAC	Select BSSID MAC to define a BSS ID MAC address used for matching and filtering with the signature
Source MAC	Define a source MAC address for packets examined for matching, filtering, and potential device exclusion using the signature
Destination MAC	Set a destination MAC address for the packet examined for matching, filtering, and potential device exclusion with the signature
Matching Frame	Use the drop-down list box to select a frame type for matching and filtering with the WIPS signature
Matching SSID	Set the SSID used for matching and filtering with the signature. Ensure that it is specified properly, or the SSID will not be properly filtered
SSID Length	Set the character length of the SSID used for matching and filtering with this signature. The maximum length is 32 characters
Wireless Client Threshold	Specify the threshold limit per client that, when exceeded, signals the event. The configurable range is from 1 to 65,535

Setting	Description
Radio Threshold	Specify the threshold limit per radio that, when exceeded, signals the event. The configurable range is from 1 to 65,535
Filter Expiration Time	Set a Filter Expiration from 1 through 86,400 seconds that specifies the duration a client is excluded from RF Domain manager radio association when responsible for triggering a WIPS event

5. Select **Add** to create a new payload.
6. Configure the following **Payload** settings:

Setting	Description
Index	Set the index between 1 and 3
Pattern	Assign a pattern for the payload
Offset	Set a offset between 0 and 255
Action	Select  to delete a payload option

7. Select **Update** to save the WIPS signature configuration.

Related Topics

[WIPS Policy](#) on page 128

[Configure a WIPS Policy](#) on page 128

[Configure WIPS Events](#) on page 130

L2TPv3 Policy

L2TPv3 is an IETF standard used for transporting different types of layer 2 frames in an IP network. L2TPv3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Multiple pseudowires can be created within an L2TPv3 tunnel. WiNG managed access points support an Ethernet VLAN pseudowire type exclusively.



Note

A pseudowire is an emulation of a layer 2 point-to-point connection over a PSN (packet switching network). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP v3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (a L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TPv3 session originator and responder need to know the pseudowire type and identifier. These two parameters are communicated during L2TPv3 session establishment. An L2TPv3 session created within an L2TPv3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TPv3 session. If a L2TPv3 session is down, the pseudowire associated with it must be shut down. The L2TPv3 control connection keepalive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

**Note**

If connecting an Ethernet port to another Ethernet port, the pseudowire type must be Ethernet port, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be Ethernet VLAN.

Related Topics

[L2TPv3 Configuration](#) on page 135

L2TPv3 Configuration

About This Task

Use L2TP v3 to create tunnels for transporting layer 2 frames. L2TP v3 enables WiNG supported controllers to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP v3 tunnels can be defined between WiNG managed devices and other vendor devices supporting the L2TP v3 protocol.

To define an L2TPv3 tunnel configuration:

Procedure

1. Select **Policies > L2TPv3**.
The L2TPv3 dashboard open and lists the existing policy configurations.
2. Select a policy from the list to edit the policy.
The basic settings dashboard opens.
3. Select  icon to add a new policy.
The **Add Policy** dashboard opens.
4. Set a policy name that is less than 31 characters and select **Add**.
The basic settings dashboard opens.

5. Configure the following L2TPv3 policy settings based on new policy creation or modification:

Setting	Description
Cookie Size	Displays the size of each policy's cookie field within each L2TP V3 data packet. L2TP V3 data packets contain a session cookie which identifies the session (pseudowire) corresponding to it. If using the CLI, the cookie size can't be configured per session, and are the same size for all sessions with in a tunnel. Use the drop-down list box to select a cookie size. The options include 0B, 4B, and 8B
Hello Interval	Displays each policy's interval between L2TPv3 hello messages exchanged within the L2TPv3 connection. Set the time limit between 1 to 3,600 seconds. The default option is 60 seconds
Reconnect Attempts	Lists each policy's maximum number of re-connection attempts to reestablish a tunnel between peers. The range is between 0 and 8
Reconnect Interval	Displays the duration set for each listed policy between two successive reconnection attempts. The range is 1 to 3,600 seconds. The default option is 120 seconds
Retry Attempts	Lists the number of retransmission attempts set for each listed policy before a target tunnel peer is defined as not reachable. The range is 0 through 10, and the default is 5
Retry Interval	Lists the interval the interval (in seconds) set for each listed policy before the retransmission of a L2TPv3 signaling message. The range is 1 through 350 seconds, and the default is 5 seconds
RX Window Size	Displays the number of packets that can be received without sending an acknowledgment. The range 0 through 15, and the default is 10
TX Window Size	Displays the number of packets that can be transmitted without receiving an acknowledgment. The range is 0 through 15, and the default is 10
Failover Delay	Lists the time in seconds for establishing a tunnel after a failover (VRRP, RF Domain, or Cluster). The range is 5 to 60 seconds, and the default is 5 seconds
L2 Path Recovery	Lists whether force L2 path recovery is activated or deactivated. Once a tunnel is established, enabling this setting forces server and gateway learning behind the L2TPv3 tunnel

6. Select **Save** to configure all the updates to the L2TPv3 policy.

DHCPv4 Policy

Controllers and service platforms contain an internal DHCP (Dynamic Host Configuration Protocol) server. DHCP can provide IP addresses automatically to requesting devices. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters (IP address, network mask gateway, etc.) from a DHCP server to a host.

The **DHCPv4** dashboard displays the following read-only information for existing policies:

Name	Name assigned when creating a DHCPv4 policy
Address Pool	General DHCPv4 policy address information
Network	The network on which the policy is configured
Action	Edit or delete a DHCPv4 policy

Related Topics

[Add or Edit a DHCPv4 Policy](#) on page 137

[Configure DHCPv4 Class Policy](#) on page 138

[Configure DHCPv4 Address Pools](#) on page 139

Add or Edit a DHCPv4 Policy

About This Task

Assign new DHCP policy or edit an existing policy to configure automatic IP address assignment.

Procedure

1. Select **Policies > DHCPv4**.
The **DHCPv4** dashboard opens.
2. Select  to add a new policy.
The **Add Policy** window opens.
3. Provide a unique policy name.
4. Select **Add**.
The new policy is added to the dashboard and the **Basic** configuration dashboard opens.

5. Configure the following basic DHCPv4 policy information:

Setting	Description
Ignore BOOTP Requests	Select Ignore BOOTP Requests to cancel requests to boot remote systems within the controller or service platform managed network. BOOTP messages are encapsulated inside UDP messages and are forwarded by the controller or service platform
Ping Timeout	Set the interval from 1 to 10 seconds for a DHCP server ping timeout. The timeout is used to intermittently ping and discover whether a client requested IP address is already in use
Activation Criteria	Set an activation criteria for the policy to work. Options include: <ul style="list-style-type: none"> • None • vrrp-master • cluster-master • rf-domain-manager

6. Select **Add** to create new global DHCP server options.

7. Configure **Global DHCP Server Options** settings:

Setting	Description
Name	Assign a name for the server
Type	Select a server type
Code	Assign a code between 0 to 254

8. Select **Save** to update DHCPv4 basic configuration settings.

Related Topics

[DHCPv4 Policy](#) on page 137

[Configure DHCPv4 Class Policy](#) on page 138

[Configure DHCPv4 Address Pools](#) on page 139

Configure DHCPv4 Class Policy

About This Task

A controller or service platform's local DHCP server assigns IP addresses to requesting DHCP clients based on user class option names. The DHCP server can assign IP addresses from as many IP address ranges as defined by an administrator. The DHCP user class associates a particular range of IP addresses to a device in such a way that all devices of that type are assigned IP addresses from the defined range.

Refer to the **DHCP Class Policy** screen to review existing DHCP class names and their current multiple user class designations. Multiple user class options enable a user class to transmit option values to DHCP servers supporting multiple user class options. Either add a new class policy, edit the configuration of an existing policy or permanently delete a policy as required.

Procedure

1. Select **Policies > DHCPv4**.
2. Select a DHCPv4 policy from the list.
3. Select **Class Policy**.
4. Select  to create a new class policy.
The **Class Policy** basic dashboard opens.
5. Configure the following basic class policy settings:

Setting	Description
Name	assign a name representative of the device class supported not exceeding 32 characters
User Class Option	Select a row within the Value column to type a 32-character maximum value string
Multiple User Class Support	Select Multiple User Class Support to activate multiple option values for the user class. This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options

6. Select **Add** to create a new user class policy.

Related Topics

[DHCPv4 Policy](#) on page 137

[Add or Edit a DHCPv4 Policy](#) on page 137

[Configure DHCPv4 Address Pools](#) on page 139

Configure DHCPv4 Address Pools

About This Task

A pool or range of IP network addresses and DHCP options can be created for each IP interface configured. This range of addresses can be made available to DHCP enabled wireless devices on either a permanent or leased basis. DHCP options are provided to each DHCP client with a DHCP response and provide DHCP clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters or octets with a meaning specified by the vendor of the DHCP client.

Procedure

1. Select **Policies > DHCPv4**.
The **Address Pools** dashboard opens.
2. Select **Address Pools**.
3. Select  to add a new address pool or  to edit an existing address pool option.
The **General** tab opens.

4. Configure the following **General** settings:

An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values.

Setting	Description
Name	If adding a new pool, a name is required. The pool is the range of IP addresses defined for DHCP assignment or lease. The name assigned cannot be modified as part of the edit process. However, if the network pool configuration is obsolete it can be deleted. The name cannot exceed 32 characters
Subnet	Define the IP address, Subnet Mask, or IP alias used for DHCP discovery and requests between the local DHCP server and clients. The IP address and subnet mask (or its alias) are required to match the addresses of the layer 3 interface for the addresses to be supported through that interface. If you are setting a subnet IP alias, ensure that it begins with a dollar sign (\$) and does not exceed 32 characters. A numeric IP address is the default setting, not an alias
Unicast	Select true or false
Boot File	Define a boot file name
BOOTP Next Server	Select BOOTP Next Server and define server name
Lease Time	DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address within the defined time, that IP address can be re-assigned to another DHCP supported client. Select this option to assign a lease in seconds (1 - 31,622,399). The default setting is 86,400 seconds

5. Configure **Network** settings:

Domain Name	Provide the domain name or domain alias used with this pool. Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A fully qualified domain name (FQDN) consists of a host name plus a domain name. For example, computername.domain.com. If you are setting a domain name alias, ensure that it begins with a dollar sign (\$) and does not exceed 32 characters. A numeric IP address is the default setting, not an alias
DNS Server	Define one (or a group) of Domain Name Servers (DNS) to translate domain names to IP addresses. An alias can alternatively be applied for a DNS server IP address. Up to 8 IP addresses can be supported. If you are setting a DNS IP alias, ensure that it begins with a dollar sign (\$) and does not exceed 32 characters. An actual DNS IP address is the default setting, not an alias
Default Router	After a DHCP client has booted, the client begins sending packets to its default router. Set the IP address or IP alias for one or more routers used to map host names into IP addresses for clients. Up to eight default router IP addresses are supported. If setting a default router IP alias, ensure it begins with a dollar sign (\$) and does not exceed 32 characters. An actual router IP address is the default setting, not an alias. If you are setting a default router IP alias, ensure that it begins with a dollar sign (\$) and does not exceed 32 characters. An actual router IP address is the default setting, not an alias

6. Configure **NetBIOS** settings:

Node Type	Select a node type used with this particular pool. The following options are available: <ul style="list-style-type: none"> • Broadcast - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name • Peer-to-Peer - Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine • Mixed - A mixed node using broadcast queries to find a node, and failing that, queries a known p-node name server for the address • Hybrid - A combination of two or more nodes • None - No node type is applied
Servers	Specify a numerical IP address of a single NetBIOS WINS server or a group of servers available to requesting clients. A maximum of eight server IP addresses can be assigned. The IP option is selected by default. Optionally select Alias to provide a NetBIOS server IP alias beginning with a dollar sign (\$) and not exceeding 32 characters

7. Define **Static Routes** settings:

Destination	Define a address pool destination
Gateway	Provide a gateway for the address pool

8. Define the range of included (starting and ending IP addresses) addresses for this particular pool. Use the **Address Range** fields for this operation.

- Select **Add** to configure the IP address.
- Type a viable range of IP addresses in the IP Start and IP End columns. This is the range of addresses available for assignment to requesting clients.
- Select a DHCP Class policy for the IP address range.

9. Select **Add** to create an excluded address range.

Add ranges of IP address to exclude from lease to requesting clients.

**Tip**

The best practice is to have ranges of unavailable addresses to ensure IP address resources are in reserve.

10. Select **Add** to configure general address pool settings.

11. Select **Advanced** tab to configure DHCPv4 pool's advanced settings.

Domain Name	Provide a domain name for DDNS updates representing the forward zone in the DNS server. For example, test.net. The Name option is selected by default. Optionally select Alias to provide a DDNS domain name alias beginning with a dollar sign (\$) and not exceeding 32 characters
TTL	Set a TTL (Time to Live) to specify the validity of DDNS records. The maximum value configurable is 864,000 seconds
Multi User Class	Select Multi User Class to associate the user class option names with a multiple user class. This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options
Update DNS	Set if DNS is updated from a client or a server. Select either Client Update, No Update, or Server Update. The default setting is Do Not Update, implying that no DNS updates occur at all
Server	Specify a numerical IP address of one or two DDNS servers. Dynamic DNS (DDNS) prompts a computer or network to obtain a new IP address lease and dynamically associate a hostname with that address, without having to manually enter the change every time. Since there are situations where an IP address can change, it helps to have a way of automatically updating hostnames that point to the new address every time. The IP option is selected by default. Optionally select Alias to provide a DDNS server IP alias beginning with a dollar sign (\$) and not exceeding 32 characters

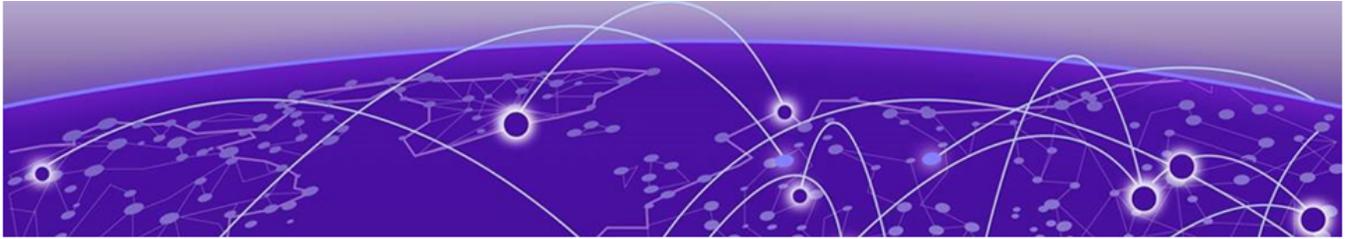
12. Select **Add** to update address pool advanced settings.

Related Topics

[DHCPv4 Policy](#) on page 137

[Add or Edit a DHCPv4 Policy](#) on page 137

[Configure DHCPv4 Class Policy](#) on page 138



Firmware Update and Images

Learn how to update device firmware and use the firmware images.

Use the **Firmware** dashboard to update your device firmware version, obtain an image and its configuration.

Firmware Update

Go to **Firmware > Update** to view update details. You can add a new firmware update and view any past updates. Obtain device firmware update information such as timestamp, mac address, hostname, upgraded by mac address or hostname, upgrade result, number of retries, and upgrade error information.

1. Select **Update** to configure firmware update schedule.
2. Configure the following information:
 - Update - Select **Self** and provide FTP address path or file name. Use self update to periodically update the firmware automatically. This option is not selected by default.



Note

Reload the system to activate self update.

- Select **All** to update firmware on devices and sites.
 - Select **Device Type** to update the firmware for a specific device.
 - Select **Site** to update firmware for a site.
3. Select **Force** to force update a firmware.
 4. Select **Immediate** to update the firmware at the current time. For future update, clear **Immediate** schedule selection and select a date and time.
 5. Configure reboot schedule:
 - Automatic - this option reboots the system immediately.
 - Staggered - select this option to reboot the system at a future time.
 6. Select **Update** to save firmware update schedule.

Firmware Images

Go to **Firmware > Images** to obtain firmware image details. Customize dashboard view using controller mac address or hostname, device type, and version columns.

For image details, select **Load Image** and select device type from the device drop-down.

To add a new firmware image:

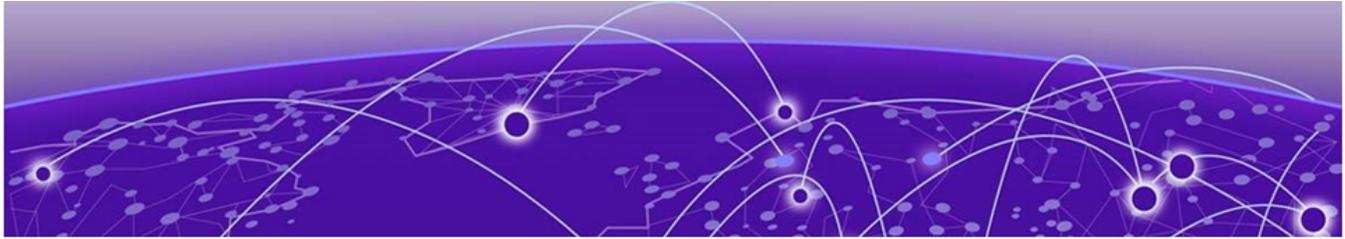
1. Select  .

The **Add Firmware Image** dashboard opens.

2. Configure the following settings:

Device Type	Select a device type from the drop-down list box
Path/File	Provide an image path
Site	Select a site from the list of available sites
Device	Select a device from the site

3. Select **Add** to update firmware image settings.



Statistics

Details about statistics displayed on the graphical user interface (GUI). Statistics are available for controllers or service platforms and their managed devices.

Statistics display detailed information about how device policies configured by the user for various managed devices work in the WiNG environment. Through the statistics option, you can monitor device inventories, wireless clients associations, adopted access point information, rogue access points and WLANs.

You can use the statistics data to assess if configuration changes are required to improve network performance.

Smart RF

A Smart RF statistical history is available to assess adjustments made to device configurations to compensate for detected coverage holes or device failures. Smart RF statistics can be exclusively customized to monitor basic information, device activity, device neighbors, radio interference, channel distribution, and various device history events.

Wireless

Wireless statistics are available for an overview of client health. Wireless client statistics includes user traffic received and transmitted, and management packets received and transmitted by a device.

Devices

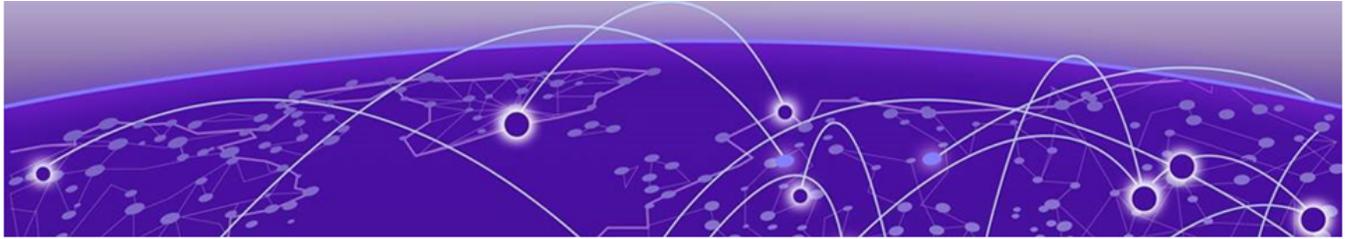
Device statistics is available for the list of devices managed in a site. Select a site name to view the list of devices and it's hostname, mac address, device type, device status, channel, and power information.

Client

Client statistics provides details about your rf-domain manager for each site. Select a site name to access device details, hostname, ingress, egress, total traffic, SNR (dB), and noise floor (dBm).

Sites

Sites statistics provides a summary of all the sites. It includes site name, site manager details, number of managed devices on each site, number of radios on each site, number of clients, and sensors on the site.



Index

A

- AAA policy
 - general 87
 - radius 87
- access control configuration 76
- add a new management policy 71
- add a site 28
- add AAA policy 88
- add an NSight policy 92
- add profile
 - copy from profile 39
 - device type 39
 - profile name 39
- add wireless LAN configuration 33
- adoption profile configuration 42
- announcements 8
- auto-provisioning adoption 111
- auto-provisioning policy 108

B

- basic firewall settings 113
- basic profile configuration
 - add basic configuration 39

C

- cluster
 - cluster history 25
 - device history 25
 - members 25
- configure devices 31
- configure profiles
 - add profile 38
 - adoption configuration 38
 - basic configuration 38
 - interface configuration 38
 - network configuration 38
 - policies configuration 38
 - power configuration 38
- configure site 27
- configure WIPS events 130
- configure WIPS policy 128
- conventions
 - notice icons 6
 - text 6

D

- dashboard
 - system dashboard
 - add custom dashboard 21
 - delete custom dashboard 21
 - edit custom dashboard 21
- default auto-provisioning 111
- delete a AAA policy 91
- delete a management policy 87
- delete NSight policy 94
- delete site 30
- device basic info 31
- device categorization
 - configure device categorization 127
 - device categorization policy 127
- device info 31
- devices basic info 31
- DHCPv4 address pools 139
- DHCPv4 class policy 138
- DHCPv4 class policy configuration 138
- DHCPv4 policy
 - add a DHCPv4 policy 137
 - edit a DHCPv4 policy 137
- diagnostics
 - logs 62
 - system info 62
 - tech support 62
- documentation
 - feedback 8
 - location 7
- DoS firewall 116

E

- edit a AAA policy 91
- edit a management policy 87
- edit a site 28
- edit NSight policy 93
- edit wireless network basic configuration 34
- enable new UI
 - CLI UI for controllers 14
- event system
 - event system configuration 126
 - event system policy 126

F

- feedback 8
- firewall 112

- firewall configuration 112
- firewall policy 112
- firewall policy IPv6 settings 122
- firmware
 - images 144
 - update 144

G

- GRE network configuration
 - basic configuration 52
 - establishment criteria 52
 - failover 52
 - peer configuration 52

I

- IGMP snooping configuration 55

L

- L2TPv3 configuration 135
- L2TPv3 policy 134
- LDAP server configuration 106
- locations configuration 75
- logs
 - advanced 65, 66
 - general 65, 66

M

- management dashboard 69
- management policy 68
- management user authentication 81
- management users 71
- MLP snooping configuration 55

N

- notices 6
- NSight policy 92
- NTP configuration
 - add NTP server 40
 - NTP server settings 40

P

- policies 68
- policies configuration
 - auto-provisioning policy 58
 - DHCPv4 policy 58
 - event system policy 58
 - firewall policy 58
 - management policy 58
 - RADIUS server policy 58
- policy rules
 - auto-provisioning policy 108
- power configuration
 - 802.3af 43

- power configuration (*continued*)
 - automatic 43
- product announcements 8
- profile ARP configuration 45
- profile DNS configuration 44
- profile L2TPv3 configuration 46
- profile network configuration
 - ARP 44
 - DNS 44
 - GRE 44
 - IGMP/MLD 44
 - L2TPV3 44

R

- RADIUS clients 103
- RADIUS group
 - add RADIUS group 95
- RADIUS proxy 104
- RADIUS server 100
- RADIUS server policy configuration 102
- RADIUS user pool 98
- remote CLI
 - add 67
 - download 67
 - download all 67
- remote CLI operations 67
- remote server settings 18, 19

S

- sensor policy 125
- sensor policy configuration 125
- site configuration 28
- site policies 29
- site policies configuration 29
- slide-in device info 24
- SmartRF policy 124
- SNMP configuration 84
- SNMP traps configuration 86
- statistics
 - clients 146
 - devices 146
 - sites 146
 - smart RF 146
 - wireless 146
- storm control 121
- support, *see* technical support
- system info diagnostics
 - CDP neighbors 62–64
 - general 62–64
 - LLDP neighbors 62–64
 - tasks 62–64

T

- tech support diagnostics
 - server 64, 65
 - session 64, 65

technical support
 contacting 8

U

UI navigation
 search 16
 system admin settings 16
 user preference 16
 user role 16
user roles
 admin
 settings 18, 19
 user preferences 18, 19
 superuser 18, 19

W

warnings 6
Web UI
 access the web UI 12
 browser and system requirements 12
 connect to web UI 12
WiNG 7
 overview 10
WIPS events 130
WIPS policy 128
WIPS signature 132
WIPS signature configuration 132
wireless configuration 33
wireless network security configuration 35