WiNG Controller v7.9.6.0 NOVA User Guide

System Configuration and Management

9037761-06 Rev AA
April 2025

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: https://www.extremenetworks.com/about-extreme-networks/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/

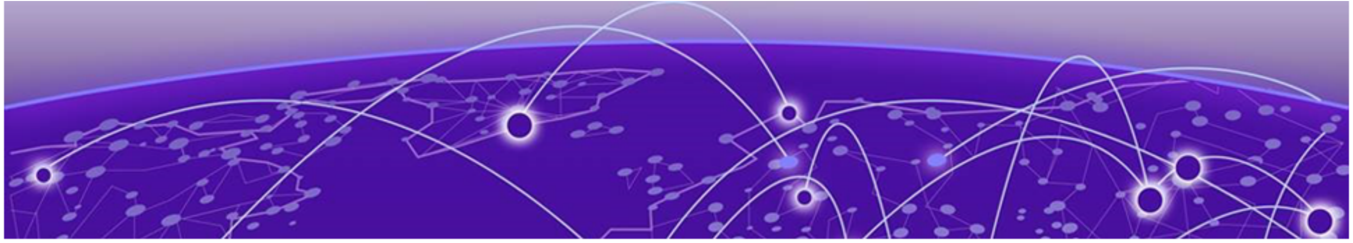
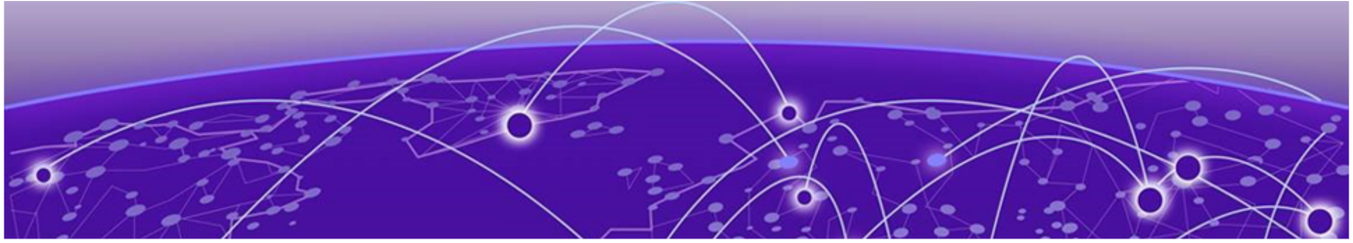
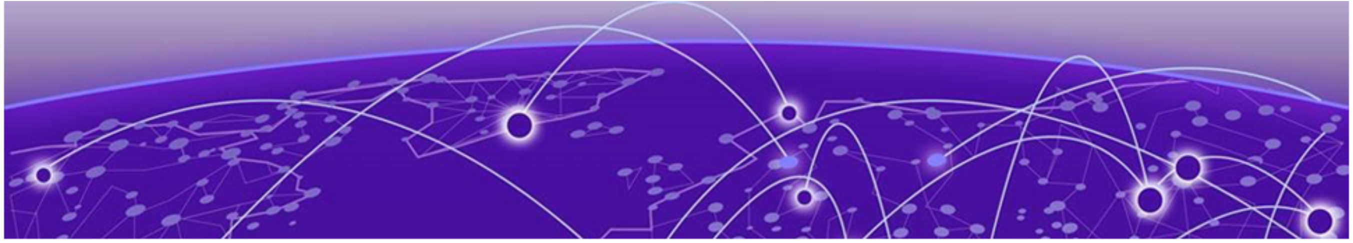


Table of Contents



Abstract

This user guide for WiNG Controller v7.9.6.0 NOVA provides comprehensive instructions for system configuration and management. It covers new features and updates across multiple releases, including enhancements in dashboard customization, site management, device configuration, and policy settings. The guide details the WiNG 7 operating system, which integrates ExtremeWireless and ExtremeWireless WiNG architectures, offering flexibility and scalability for both campus and distributed deployments. Key functionalities include advanced diagnostics, remote troubleshooting, secure guest access, application visibility and control, and self-tuning RF capabilities. The document also includes step-by-step procedures for configuring wireless LANs, profiles, mesh points, NAT, AAA policies, and various other network settings. This guide is intended for technical readers and network administrators, ensuring they can effectively deploy and manage WiNG Controller systems.



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 Extreme Networks switches or 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 *enter* and *type*	When you see the word *enter* 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 *type*.
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.
italic 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, *member*[*member*...].
\	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 articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

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 2800. 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.

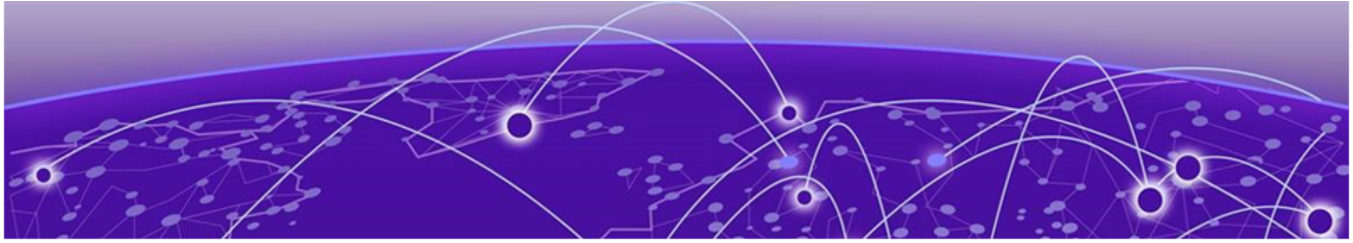
Send Feedback

The User Enablement 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.
- Broken links or usability issues.

To send feedback, email us at https://www.extremenetworks.com/documentation-feedback/ .

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

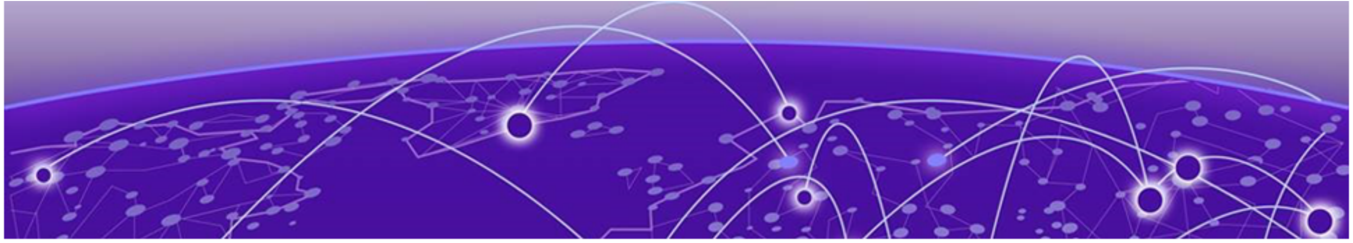


About this Guide

This guide describes how to use the *NOVA Graphical User Interface* to deploy and operate Extreme Networks service platforms and virtual platforms within a ExtremeWireless WiNG™ managed network.

The ExtremeWireless WiNG software supports the service platforms and virtual platforms described in WiNG 7 Operating System Overview on page 30.

For detailed product information about service and virtual platforms, including minimum firmware requirements, refer to the relevant product documentation and release notes: visit https://www.extremenetworks.com/support/documentation/.



New in this Guide

This chapter describes changes made to *ExtremeWireless WiNG™ Controllers NOVA User Guide* in support of the WiNG 7.9.X.X releases.

Release 7.9.6.0

The following sections describe new features and updates included in this guide in support of WiNG 7.9.6.0.

New features

Revision AA

The following table describes changes made in Revision AA of this guide in support of new features included in WiNG 7.9.6.0:

New Features	Description
Add a Custom Dashboard on page 43	Added Radio Traffic Utilization widget
Manage Sites on page 55	Added new controls to perform a reload, restore factory default settings, and upgrade all APs at a Site

The following topics have been added in Revision AA of this guide in support of new features included in WiNG 7.9.6.0:

Devices/Profiles > Interface > Virtual

VLAN IPV6 Configuration on page 128

Diagnostics

Fault Management on page 249

- Filter Events (APs only) on page 249
  - Manage Event Filters on page 250
  - Configure Event Filters on page 251
  - Disable or Enable Event Filters on page 252

Statistics

WIPS Summary on page 559

Updates

Revision AA

The following updates have been made in Revision AA of this guide:

Updates	Description
Publication title	The title of this publication has changed to *WiNG Controller Command Reference Guide*
Devices > General Configuration on page 71	Configurable parameters have changed
Smart RF Policy on page 469	Updated procedures to include 6 GHz radio details

Release 7.9.5.1

The following sections describe new features and updates included in this guide in support of WiNG 7.9.5.1.

New Features

Revision AA

The following table describes changes made in Revision AA of this guide in support of new features included in WiNG 7.9.5.1:

New Features	Description
Configure Wireless LAN Basic Settings on page 107	Added support for applying Application Management and Roaming Assist policies to a WLAN configuration.

The following topics have been added in Revision AA of this guide in support of new features included in WiNG 7.9.5.1:

Policies

Application Management Policy on page 268

- Manage Application Policies on page 269
- Configure an Application Policy on page 270

- Configure a Basic Application Management Policy on page 270
- Configure Application Policy Rules on page 273
- Apply an Application Policy to the Network on page 277

Application Group Policy on page 278

- Manage Application Group Policies on page 278
- Configure an Application Group Policy on page 279

Wireless Client Roles Policy on page 300

- Manage Wireless Client Roles Policies and Roles on page 301
- Configure a Wireless Client Role Policy on page 303
- Configure LDAP Settings on page 303
- Configure Roles and Optional Firewall Rules on page 305
- Configure Default Firewall Rules on page 311

Imagotag Policy on page 342

- Manage Imagotag Policies on page 343
- Configure an Imagotag Policy on page 344

Roaming Assist Policy on page 346

- Manage Roaming Assist Policies on page 347
- Configure a Roaming Assist Policy on page 348

Configure a BLE Data Export Policy on page 353

Profiles

NAT Configuration on page 226

- Manage NAT Resources on page 227
- Configure a NAT Pool on page 227
- Configure Static NAT Source or Destination on page 229
- Configure Dynamic NAT on page 233

Updates

Revision AA

The following updates have been made in Revision AA of this guide:

Updates	Description
Association ACL Policy on page 433	Added Deployment Guidelines.
Navigate the User Interface on page 34	Added supported policies.
Power Configuration on page 168	Updated
Configure a Passpoint Policy on page 447	Updated

Release 7.9.5.0

The following sections describe new features and updates included in this guide in support of WiNG 7.9.5.0.

New Features

Revision AB

There are no new features introduced in Revision AB of this guide.

Revision AA

The following table describes updates made in Revision AA of this guide in support of new minor features included in WiNG 7.9.5.0:

New Features	Description
Add Wireless LAN on page 107	Added option to select **MAC Inbound ACL** and **MAC Outbound ACL** firewall policies to apply to WLAN configuration.
Configure an AAA Policy Server on page 257	Added **Request Proxy Mode** Server parameter, allowing for the selection of the method of proxy that browsers use to communicate with the RADIUS authentication server.

The following topics have been added in Revision AA of this guide in support of new major features included in WiNG 7.9.5.0:

Sites

Client/Sensor Configuration on page 63

- Configure RF Domain Client Names and Sensors on page 64

Profiles - Network

Critical Resource Management Configuration on page 235

- Configure Critical Resources on page 235

Policies

URL Filtering Policy on page 285

- Manage URL Filtering Policies on page 286
- Configure a URL Filter Policy on page 287
- Configure Web Filter Rules on page 288
- Configure a URL Error Page on page 291

Association ACL Policy on page 433

- Manage Association ACL Policies and Rules on page 433
- Configure an Association ACL Policy on page 435
- Configure Association ACL Policy Rules on page 435

Configure a URL List Policy on page 483

Bulk Migration of APs to Cloud Management

Bulk Migrate APs to ExtremeCloud IQ on page 565

Updates

Revision AB

The following updates are included in Revision AB of this guide:

Updates	Description
Add a Profile on page 117	This procedure has been revised.
Configure General Profile Settings on page 118	This procedure has been revised.

The following sections have been added in Revision AB of this guide:

Devices

Back Up and Restore Configuration (Access Points Only) on page 88

Certificate Configuration on page 89

- Configure Device Trustpoints on page 89
- Manage Certificates and RSA Keys on page 92
- Import Certificates and Trustpoints on page 95
- Export Trustpoints on page 96
- Generate an RSA Key on page 97
- Import an RSA Key on page 98
- Export an RSA Key on page 98
- Create and Generate a Self-Signed Certificate on page 99
- Create and Generate a Certificate Signing Request on page 101

Wireless

Configure Wireless LAN Client Load Balancing on page 112

Statistics

Clients on page 534

- Basic on page 535
- Client Connectivity on page 536
- Client Performance Statistics on page 543

Sites on page 548

Revision AA

The following topics have been updated or added in Revision AA of this guide:

Configure Smart RF Select Shutdown Settings on page 480

Statistics on page 495

- Smart RF on page 496

- Wireless on page 503
- Devices on page 504

Release 7.9.4.0

The following sections describe new features and updates included in this guide in support of WiNG 7.9.4.0.

New Features

Revision AB

There are no new features introduced in Revision AB of this guide.

Revision AA

The following table describes updates in Revision AA of this guide in support of new minor features included in WiNG 7.9.4.0:

New Features	Description
Add a Custom Dashboard on page 43	Added new Dashboard widgets: • Added Site widget **Clients by Band** • Added Site widget **Radios by Band** • Added Site widget **Wireless Security** • Added Site widget **WLAN Utilization**
Statistics on page 495	Added description of new **Sensor** tab for Smart RF device statistics.

The following topics have been added to this guide in support of new major features included in WiNG 7.9.4.0:

Sites

Configure RF Domain Overrides on page 60

Profiles - Network

- Spanning Tree Configuration on page 188
  - Configure a Spanning Tree Profile on page 189
- Forwarding Database Configuration on page 195
  - Configure a Forwarding Database on page 195
- Alias Configuration on page 208
  - Configure a Network Basic Alias Profile on page 209
  - Configure a Network Group Alias Profile on page 212
  - Configure a Network Service Alias Profile on page 213

Policies

- MAC ACL Firewall Policy on page 330
  - Manage MAC ACL Policies and Rules on page 331
  - Configure a MAC ACL Policy on page 332
  - Configure MAC ACL Policy Rules on page 332
  - Configure EX3500 MAC ACL Policy Rules on page 335
- IPv4 ACL Policy on page 337
  - Manage IPv4 ACL Policies on page 337
  - Configure an IPv4 Policy on page 339
  - Configure IPv4 ACL Policy Rules on page 340
- Radio QoS Policies on page 418
  - Radio QoS Configuration and Deployment Considerations on page 420
  - Manage Radio QoS Policies on page 420
  - Configure a Radio QoS Policy on page 422
  - Configure Radio QoS Wireless Multimedia Policy on page 423
  - Configure Radio QoS Admission Control Policy on page 426
  - Configure Radio QoS Multimedia Optimizations Policy on page 431

Updates

Revision AB

The following updates are included in Revision AB of this guide:

Updates	Description
GRE Tunnel Configuration on page 179	Corrections made
Configure User Authentication Settings on page 368	Added AAA TACACS parameters to Management Policy Authentication configuration
Statistics on page 495	Added instructions on how to clear Smart RF configuration (Channel and Power) statistics display in the **Basics** tab

The following topics have been added in Revision AB of this guide:

Profiles

GRE Concentrator Configuration on page 182

- Configure a GRE Concentrator Profile for a ExtremeWireless WiNG Controller on page 183

CDP/LLDP Configuration on page 191

- Configure a CDP/LLDP Profile on page 191

Policies

AAA TACACS Policy on page 261

- Manage AAA TACACS Policies on page 262
- Configure an AAA TACACS Policy on page 263
- Configure AAA TACACS Server Information on page 264
- Configure AAA TACACS Settings on page 266

Revision AA

The following updates are included in Revision AA of this guide:

Updates	Description
Add a Custom Dashboard on page 43	Added new Dashboard elements: • Added Site widget **Domain Manager** • Added Site widget **Client Traffic Utilization** (RF Domain Specific) • Added Site widget **Client Quality** • Added Site widget **Radio Quality** • Added **Offline** indicator description for Device Status widget
Policies Configuration on page 79	This section has been updated.
Device Profile - Policies Configuration on page 214	This procedure has been updated.
Firewall Policies on page 313	The contents of this section have been revised.
Statistics on page 495	Added description of **History**, **Select Shutdown**, and **Sensor** tabs for Smart RF device statistics.

The following topics have been added in Revision AA of this guide:

Site

Manage Sites on page 55

Profiles - Network

- Bridge VLAN Configuration on page 197
  - Manage Bridge VLANs on page 197
  - Configure a Bridge VLAN on page 199
  - Configure Bridge VLAN General Settings on page 199
  - Bridge VLAN IGMP Snooping on page 204
  - Configure Bridge VLAN MLD Snooping on page 206

Policies

- Bonjour Gateway Policy on page 386
  - Manage Bonjour Gateway Policies on page 386
  - Configure a Bonjour Discovery Policy on page 388
  - Configure a Bonjour Forwarding Policy on page 390
- Manage Firewall Policies on page 313

Release 7.9.3.0

Revision AA

The following updates have been made in Revision AA of this guide.

Updates	Description
AP3000/X	Support added for AP3000 and AP3000X access points.
NOVA UI	The following enhancements for the NOVA UI have been introduced: • New configuration support for Bridge VLAN, Bonjour policy, GRE concentrator, and smart-rf clear. • RF domain-specific health widgets: client quality, radio quality, client traffic utilization, NTP traffic and association. • WLAN add option • Show connected clients per AP and channel/power usage per rf-domain
CX9000	Support added for Intel NIC on CX9000.

Release 7.9.2.0

Revision AA

The following updates have been made in Revision AA of this guide.

Updates	Description
CX9000	Support for CX9000, the first containerized application to run on the Extreme Networks® Universal Compute Platform (UCP). This containerized application leverages Extreme qualified 4120C hardware that can host applications based on the customer’s deployment needs. The Universal Compute Platform is a multipurpose appliance that ships with a middleware package that enables it to deploy its persona or application.

Release 7.9.1.0

The following sections describe new features and updates included in this Guide in support of WiNG 7.9.1.0.

New Features

Revision AB

There are no new features introduced in Revision AB of this Guide.

Revision AA

Note
Beginning in WiNG 7.9.1.0, to access the Flash UI on a device, users must configure it using the CLI command `(config-management-policy-default)#flash-ui`. For details, refer to *Wireless Controller, Service Platform and Access Point CLI Reference Guide* for WiNG 7.9.1.0.

The following table describes updates in Revision AA of this Guide in support of new minor features included in WiNG 7.9.1.0:

New Features	Description
Edit Site Basic Configuration on page 57	New GUI controls have been added.
Configure Wireless LAN Security Settings on page 110	New GUI controls have been added.
GRE Tunnel Configuration on page 179	Support for configuring up to 1000 GRE tunnels has been added on NX7500, NX9500, NX9600, and NX9610 platforms.
• Network Configuration • Routing Configuration on page 193	Failover invocation for static route gateways is supported with the new **Network** > **Routing** tab, which is accessible under both **Devices** and **Profiles** configuration.
Configure a Radio Profile on page 144	Client bridge support has been added with the new **Bridge** tab.
• Mesh Point Configuration on page 218 • Configure a Mesh Point Policy on page 381	Meshpoint configuration is supported on 6 GHz radio 3.
Configure Smart RF Channel and Power Settings on page 473	Smart RF channel and power configuration are supported on 6 GHz radio 3.

The following topics have been added to this Guide in support of new major features included in WiNG 7.9.1.0:

- **Devices**: Message Logging Configuration for Devices on page 86
- **Profiles**: Message Logging Configuration for Profiles on page 225
- **Diagnostics**:
  - Debug Wireless Clients on page 247
  - Event History on page 252
- Captive Portals Policy on page 391
  - Configuring a Captive Portal Policy on page 392
  - Configuring DNS Whitelist Policies on page 398
  - Captive Portal Deployment Considerations on page 400

- WLAN QoS Policies on page 400
    - Configuring a WLAN QoS Policy on page 400
    - Configure a WLAN and Wireless Client QoS Rate Limit on page 402
    - Configure Multimedia Optimizations on page 410
    - Configure a WLAN QoS WMM Policy on page 412
    - WLAN QoS Deployment Considerations on page 418
- Guest Management Policy on page 437
    - Guest Management Policy Configuration on page 437
    - Email on page 438
    - SMS on page 440
    - SMS SMTP on page 441
    - DB Export on page 443

Updates

Revision AB

The following updates are included in Revision AB of this Guide:

Updates	Description
GRE Tunnel Configuration on page 179	The devices that support GRE Tunneling and the Maximum GRE Tunnels Supported have been corrected.

Revision AA

The following updates are included in Revision AA of this Guide:

Updates	Description
Navigate the User Interface on page 34	Updated to reflect available GUI controls.
Web UI and Initial Setup on page 32	Updated to state that it is no longer necessary to include a port number in the IP address when connecting through a browser to the Web UI.
Devices on page 66	Introductory sections in this chapter have been updated to clarify instructions.
Wireless Configuration on page 104	• The "Add Wireless Network" procedure has been obsoleted. The instructions are included in the "Wireless Network Basic Configuration" procedure. • The procedure Configure Wireless LAN Basic Settings on page 107 has been updated.

Updates	Description
Configure a Radio Profile on page 144	• AP5010 6GHz radio3 support has been added. • GUI controls have been updated for the **Basic** tab. • **WLAN** > **Guard Interval** options have been updated. • MeshConnex configuration parameters have been updated under the **MCX** tab.
Power Configuration on page 168	**Power Mode** options are updated.
Authentication, Authorization, and Accounting (AAA) Policy on page 256	This section has been updated to clarify instructions.
Statistics on page 495	The "Devices" feature summary has been updated.
License Types on page 563	Added Tron Bluetooth and IOT features license support on VX9000.

Release 7.9.0.0

Following is a summary of what is included in this Guide in support of WiNG 7.9.0.0.

New Features

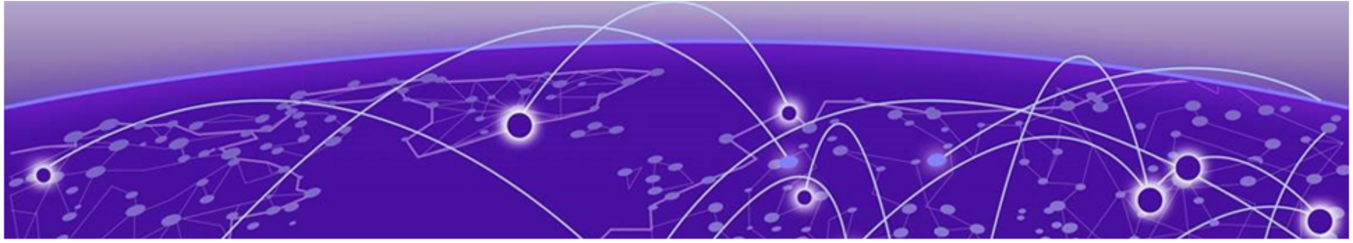
The following table describes updates in Revision AA of this Guide in support of new minor features included in WiNG 7.9.0.0.

New Features	Description
Support NOVA graphical user interface by default	The NOVA graphical user interface is the default user interface for the current release. The Flash user interface is accessible using a non-standard port. It can be manually enabled through the CLI. Port Examples: • NOVA UI `https://10.234.165.165` • Flash UI `https://10.234.165.165:10443/`
Support for the Universal Wireless AP5010	The AP5010 access point is a Wi-Fi 6E indoor access point with three radios: 2.4 GHz, 5GHz, and 6 GHz.
Device Interface Support	Configure device Interface settings from the **Devices** workbench.
Device Factory Reset	Support for device factory reset from the **Device List**.
New diagnostics tools	Support for device Ping, Traceroute, and Packet Capture from the **Diagnostics** workbench.

The following topics have been added to this Guide in support of new major features included in WiNG 7.9.0.0:

- New in this Guide on page 17
- Ping on page 244

- Traceroute on page 244
- Packet Capture on page 244
- Packet Capture Parameters on page 244
- Interface Configuration on page 74
- Interface Virtual Tab on page 74
- Interface Ethernet Tab on page 75
- Interface Radio Tab on page 76
- Interface Bluetooth Tab on page 76
- Interface PPPoE Tab on page 77
- Interface Port Channels Tab on page 78
- Licenses on page 561
- Generate Activation License Key on page 561
- Apply the License to the Controller on page 562
- License Types on page 563



WiNG 7 Operating System Overview

The WiNG 7 operating system (OS) is a solution designed for 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.

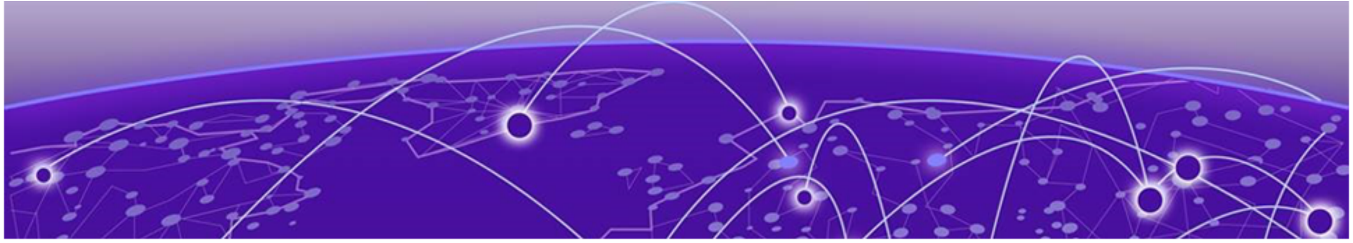
WiNG 7.X.X brings together the following key benefits of both deployment topologies under one OS:

- 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 802.11ac and 802.11ax 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 and 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. It supports the following platforms:

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

Note
NOVA UI is available only on controllers.



Web UI 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

Ensure a minimum of 1 GB of RAM is available for the UI to display and function properly. Exceptionally, the NX service platforms require 4 GB of RAM.

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

Use any of 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

Follow these steps to connect to a wireless controller or a service platform 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 supported web browser.
2. Open a browser and type https://<controller management IP> to log in to the NOVA Web GUI.

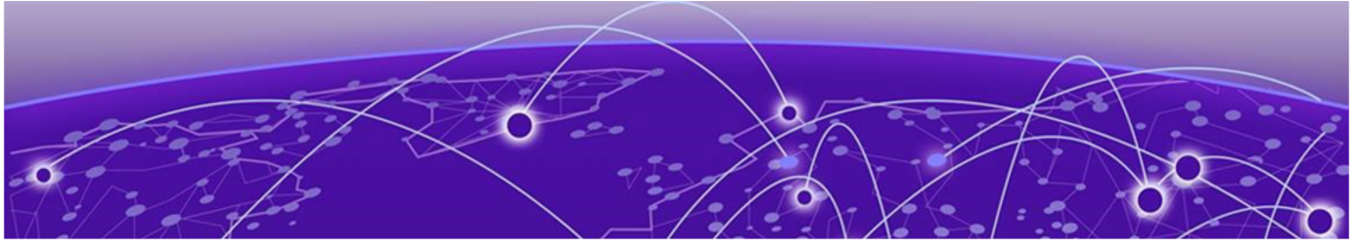
Logout

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

Related Links

Navigate the User Interface on page 34

User Roles and Preferences Settings on page 37



Navigate the User Interface

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, the default **Dashboard** screen appears. You can customize your system work space using the **Dashboard**.

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**
- **Ping**
- **Traceroute**
- **Packet Capture**
- **Debug Wireless Clients**
- **Event History**

Remote CLI

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

Policies

Configure, add, and test network policies.

- **AAA**
- **AAA TACACS**
- **Application Management**
- **Application Group**
- **Auto-Provisioning**
- **URL Filtering**
- **Device Categorization**
- **DHCPv4**
- **Wireless Client Roles**
- **Event System**
- **Wireless Firewall**
  - **Firewall Policies**
  - **MAC ACL Policy**
- **IPv4 ACL**
- **Imagotag**
- **Roaming Assist**
- **L2TPv3**
- **BLE Data Export**
- **Management**
- **Mesh**
  - **Mesh QoS Policy**
  - **Mesh Point Policy**
- **Bonjour Gateway**
  - **Bonjour Discovery Policy**
  - **Bonjour Forwarding Policy**
- **Captive Portals**
  - **Captive Portals Policy**
  - **DNS Whitelist Policy**
- **Wlan QoS**
- **Radio QoS**
- **Association ACL**
- **Guest Management**
- **NSight**
- **Passpoint**
- **RADIUS**
  - **RADiUS Group Policy**
  - **RADIUS User Pool Policy**

    - **RADIUS Server Policy**
- **SmartRF**
- **Sensor**
- **URL List**
- **WIPS**

Firmware

Firmware upload and update management.

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

Statistics

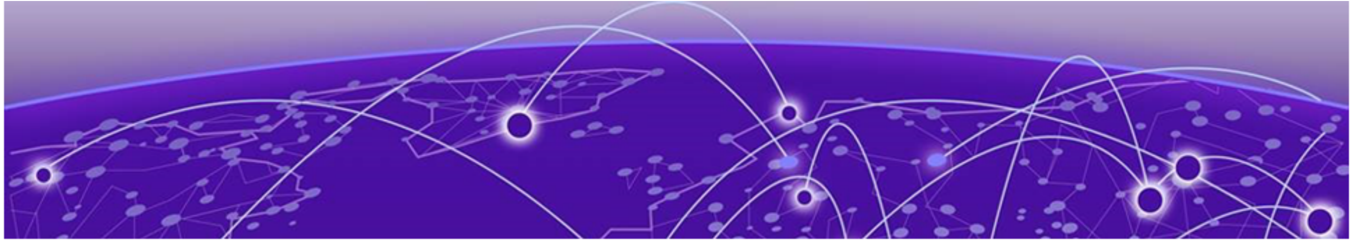
Detailed statistics for the following features in the network:

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

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

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 guest user credentials. The webuser-admin can only access the custom GUI screen and does not have access to the WiNG CLI, 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 **Save** to update and save your user preferences settings.

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.

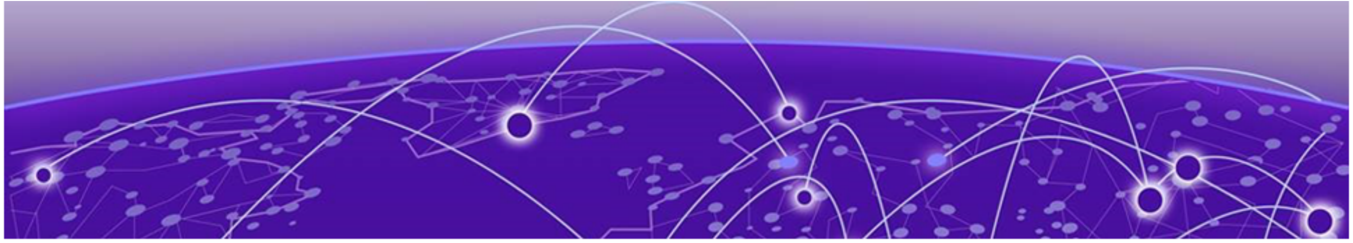
   The system displays a connection validated successfully message.
7. Select **Save** to update and save your remote server settings.
8. Select protocol to assign a remote server setting for your network.
9. Select **Save**.
10. To delete a remote server protocol, select the 🗑 icon from the action menu, and select **Save**.

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

Related Links

Tech Support on page 242

Logs on page 243



Web User GUI Access

The web user GUI is used by users with web user role for printing out Wi-Fi access vouchers for guest users and to add guest users in the RADIUS pools.

Use your web user login credentials to access the web user GUI.

Print Preview Settings

Configure print layout and font settings for a guest user.

1. Log in using your web user credentials.

   The **Guest User Configuration** screen opens.

2. Select ⚙ to configure print layout and font selection settings:

   The **Default Setting** dashboard opens.

Font family	Select a font from the drop-down list box. Options include **`Roboto`** and **`Arial`**
Font size	Select a font size from **`14`**, **`16`**, **`18`**, or **`20`**
Font weight	Select a font weight from **`normal`** or **`bold`**
Choose default layout	Select a default print layout from the available layouts

3. Select **Save** to update the print preview settings.

Guest User Configuration

Use the web user GUI to configure guest users.

1. Log in using your web user credentials.

   The **Guest User Configuration** screen opens.

2. Select **View** to see the list of local guest users or **Add** to create a new guest user access.

   The list of users with local guest access opens if you select to view existing users.

3. Select ✎ to edit guest user configuration for existing users.

   The **Configuration** dashboard opens.
4. Configure the following login settings for a guest user:

User type	Select **`Single user`** or **`Bulk users`**
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. Type a user ID or select **Generate** to create a unique user ID
Password	Assign a password for the guest user or select **Generate** to create a password
Email ID	Email address of the guest user
Contact No.	12-character minimum telephone number if the user
User Group	Select a user group from the drop-down list box to assign to the user

5. Configure the following **Time Duration** settings for the user:

Start Date	The day, month, and year the listed user can access local resources
Start Time	The time that the listed user can access local resources. The time applies only to the range defined by the start date and expiry date
Expiry Date	The day, month, and year the listed user ID can no longer access local resources
Expiry Time	The time after which the listed user loses access to local server resources. The time applies only to the range defined by the start date and expiry date

6. Select **Till Expiry** to keep the access duration same as the expiry date.

   Access duration determines the amount of time a user is allowed access when time-based access privileges are applied. The duration cannot exceed 365 days.

7. Set the data rate to be **`unlimited`** to assign no limit on the amount of data available for each guest user or **`limited`** to set a data limit for selected guest user.

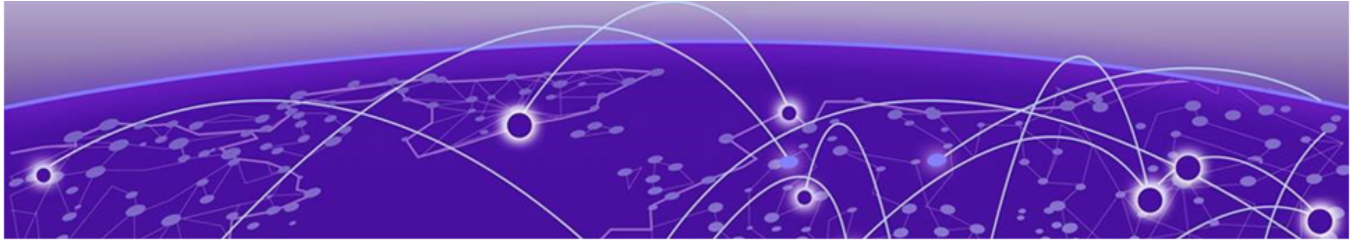
   For limited data rate, set a **`Data Limit`**.

Committed rate	• 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 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

8. Select **Add** to create a new guest user or **Update** to save guest user configuration settings.

Related Links

RADIUS User Pool on page 458



System Dashboard

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.

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

Add a Custom Dashboard

You can design a custom dashboard using a variety of widgets to help you to monitor network performance and organize network data.

To create or modify a dashboard:

1. Go to **Dashboard**, then choose from the following actions:
   - To create a new dashboard, select +. Proceed to the next step.
   - To modify a dashboard, select the target in the **Dashboard** window banner, then select ✎.
2. Optionally, type a dashboard name in the **Name** field. If you entered a name for the dashboard, select **Add**.

   If you do not assign a unique name to a dashboard, it is automatically added as **Dashboard** with a number. Example: **Dashboard 2**.

3. Design a dashboard representing the entire network or a specific site. Under **Sites**, choose from the following options:
   - Retain the default setting <system> to design a network-level dashboard.
   - Select a site from the drop-down list to design a site-level dashboard.

   > Note
   > The widgets available depend on whether you choose to design a network- or site-level dashboard.

4. Drag one widget at a time onto the dashboard area.

   Use widgets to create custom dashboard graphs. The widget graphs display a variety of information about the devices in the network or at the selected site. Dashboards allow you to assess and compare data for multiple devices at a glance. The widgets that are available for selection for system-wide and individual site graphs are described in Table 4.

Table 4: Dashboard Widgets

Widget	Description	System widget	Site widget
Clients	Displays the total number of wireless clients managed by the wireless controller or service platform. This Client table lists the top 5 RF Domains, in terms of the number of wireless clients adopted: • **Top Client Count**: Displays the client index of each listed top performing client. • **Site**: Displays the name of the client RF Domain. • **Last Update**: Displays the UTC timestamps when the client count was last reported.	Yes	No
Clients by Band	Displays a pie chart representing the radio frequency band utilization of connected RF domain member clients. Assess whether the client band utilization adequately supports the intended radio deployment objectives of the connected RF domain member access point radios. Each wedge has a label indicating its associated frequency band. You can take the following actions: • Hover over a wedge to view a pop-up showing the band and the total number of connected clients. • Toggle the interactive bands in the legend below the pie chart to include or exclude individual bands.	No	Yes

Table 4: Dashboard Widgets (continued)

Widget	Description	System widget	Site widget
Clients by Channel	Displays a pie chart of color-coded channels over which clients using 6GHz, 5GHz and 2.4GHz radios are connected. Each wedge has a label indicating its associated channel number. Note: Channels associated with 6GHz radios have an "e" appended to the channel number. You can take the following actions: • Hover over a wedge to view a pop-up showing the channel number and the total number of connected clients. • Toggle the interactive devices in the legend below the pie chart to include or exclude individual model types.	No	Yes
Client Quality	Displays a table of RF Domain connected clients requiring administration to improve performance. The table includes the following information: • Worst 5 Clients: Displays the five clients having the lowest average quality indices. • Client MAC: Displays the hard coded radio MAC of the wireless client. • Vendor: Displays the vendor name of the wireless client.	No	Yes
Client Traffic Utilization	Displays a table representing how efficiently the RF medium is utilized for connected clients. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the clients in the RF domain. The table includes the following information: • Top 5 Clients: Displays the top five performing clients with respect to overall traffic utilization. • Client MAC: Displays the hard coded radio MAC of the wireless client. • Vendor: Displays the vendor name of the wireless client.	No	Yes

Table 4: Dashboard Widgets (continued)

Widget	Description	System widget	Site widget
Device Status	Displays a color-coded donut chart representing the relative number of online versus offline devices. Each half has a label indicating its associated status. You can take the following actions: • Hover over a donut half to view a pop-up showing the number of online or offline devices and the relative percentage with respect to the total number of devices. • Toggle the interactive statuses in the legend below the donut chart to include or exclude an individual status.	Yes	Yes
Device Status Distribution	Displays a ratio of offline versus online devices within the system. The information is displayed in pie chart format to illustrate device support ratios.	Yes	Yes
Device Type	Displays an exploded pie chart representing the device types populating the RF domain. Each color-coded wedge has a label indicating its associated device model. You can take the following actions: • Hover over a wedge to view a pop-up showing the device model and the total number of them. • Toggle the interactive devices in the legend below the pie chart to include or exclude individual model types.	Yes	Yes
Device Type Distribution	Displays a numerical representation of the different controller, service platform and access point models in the current system or RF Domain. Their operational status (online and offline) device connections are also displayed.	Yes	Yes
Domain Manager	Displays the name of the RF Domain manager. The RF Domain manager is the focal point for the radio system and acts as a central registry of applications, hardware and capabilities. It also serves as a mount point for all the different pieces of the hardware system file.	No	Yes

Table 4: Dashboard Widgets (continued)

Widget	Description	System widget	Site widget
Radios	Displays top performing radios, their RF Domain memberships, and a status time stamp. RF Domain information can be selected to review RF Domain membership information in greater detail. Information in the Radio area is presented in two tables. The first lists the total number of Radios managed by this system, the second lists the top five RF Domains in terms of the number of available radios.	Yes	No
Radios by Band	Displays a pie chart representing the RF domain member device radios classified by their radio band or sensor dedication. Review this information to assess whether RF domain member radios adequately support client device traffic requirements. Each wedge has a label indicating its associated classification. You can take the following actions: • Hover over a wedge to view a pop-up showing its classification and the total number of connected radios. • Toggle the interactive classifications in the legend below the pie chart to include or exclude individual classifications.	No	Yes
Radios by Channel	Displays pie charts of the different channels utilized by RF domain member radios. These dedicated channels should be as segregated as possible from one another to avoid interference. If too many radios are utilizing a single channel, consider off-loading radios to non utilized channels to improve RF domain performance. Note: Channels associated with 6GHz radios have an "e" appended to the channel number.	No	Yes

Table 4: Dashboard Widgets (continued)

Widget	Description	System widget	Site widget
Radio Quality	Displays a table of RF quality on a per radio basis. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the transmit retry rate in both directions and the error rate. This area of the screen displays the average quality index across all the defined RF domain on the wireless controller. The table lists worst five of the RF quality values of all the radios defined on the wireless controller. The quality is measured as: • 0-20 - Very poor quality • 20-40 - Poor quality • 40-60 - Average quality • 60-100 - Good quality	No	Yes
Radio Traffic Utilization	Displays how efficiently the RF medium is used. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the RF domain. The table displays a list of the top five radios in terms of overall traffic utilization quality. It displays the radio names and radio types for each of the top five radios.	No	Yes
RF Quality	Displays RF quality per RF domain. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the connect rate in both directions, retry rate and error rate. This field displays an average quality index supporting each RF domain. The table lists the bottom five (5) RF quality values for RF domains. Listed RF domains display as individual links that can be selected to RF domain information in greater detail. Use this diagnostic information to determine what measures can be taken to improve radio performance in respect to wireless client load and the radio bands supported. The quality is measured as: • 0-20 - Very poor quality • 20-40 - Poor quality • 40-60 - Average quality • 60-100 - Good quality	Yes	No

Table 4: Dashboard Widgets (continued)

Widget	Description	System widget	Site widget
System Security	Displays RF intrusion prevention stats and their associated threat level. The greater the number of unauthorized devices, the greater the associated threat level. It also displays a list of up to five (5) RF domains in relation to the number of associated wireless clients. The RF domains appear as links that can be selected to display RF domain information in greater detail.	Yes	No
Top 5 Radios by Clients	Displays a list of radios that have the highest number of clients. This list displays the radio IDs as links that can be selected to display individual radio information in greater detail.	No	Yes
Wireless	Displays a list of WLANs utilized by RF domain member devices. The table is ordered by WLAN member device radio count and their number of connected clients. Use this information to assess whether the WLAN is overly populated by radios and clients contributing to congestion.	No	Yes

Table 4: Dashboard Widgets (continued)

Widget	Description	System widget	Site widget
Wireless Security	Wireless Security displays the overall threat index for the system. This index is based on the number of Rogue/Unsanctioned APs and Wireless Intrusion Protection System (WIPS) events detected. The index is in the range 0 - 5 where 0 indicates there are no detected threats. An index of 5 indicates a large number of intrusion detection events or rogue/unsanctioned APs detected	No	Yes
WLAN Utilization	Displays the traffic utilization index, which measures how efficiently the WLAN's traffic medium is used. WLAN Utilization is defined as the percentage of current throughput relative to maximum possible throughput for the WLAN. The table displays a list of the top five WLANs in terms of overall traffic utilization. It displays the utilization level (T-Index), WLAN name and SSIDs for each of the top five WLANs. Low indexes may require administration to assess why there's an excess of missed packets. Traffic indices are: • 0 – 20 (very low utilization) • 20 – 40 (low utilization) • 40 – 60 (moderate utilization) • 60 and above (high utilization)	No	Yes

5. Close the **Add Dashboard** pop-up window.
6. Select **Save**.

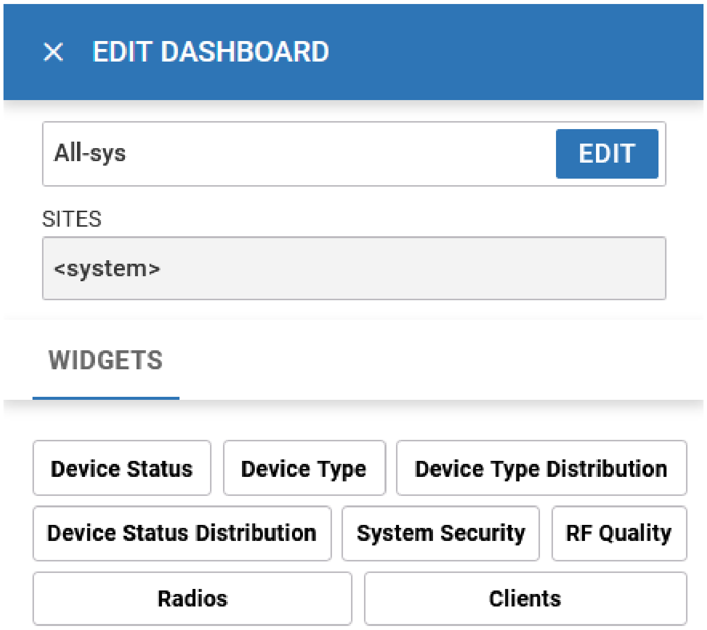
Edit or Delete a Selected Dashboard

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.

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

   Note
   You cannot edit the default dashboard.

2. Select the pencil icon to edit the dashboard.



All-sys

SITES

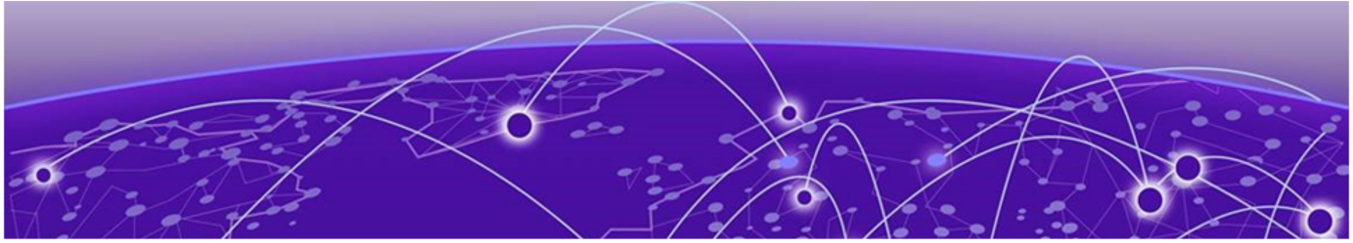
<system>

Figure 1: 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 **Dashboard** toolbar.
7. Select **Save**.

   The system displays a Dashboard Saved Successfully message.



Slide-in Device Info

To access the slide-in info panel, hover over the vertical slider at the center-right of the **Dashboard** window.

Slide-In Device Info Details Dashboard

The slide-in device info panel provides details and statistics about the controller.

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

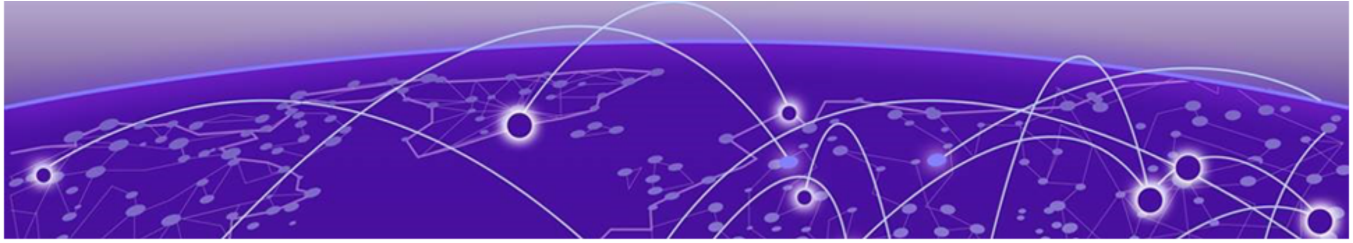
- Device: Name is determined based on the device selected in the dashboard
- Hostname: The device hostname is displayed in the following format: `device name - six digit numerical identifier`
- Version: Current firmware version running on the device
- Model: Official device model name
- MAC: Unique media access control address assigned to the controller
- Serial No: 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.

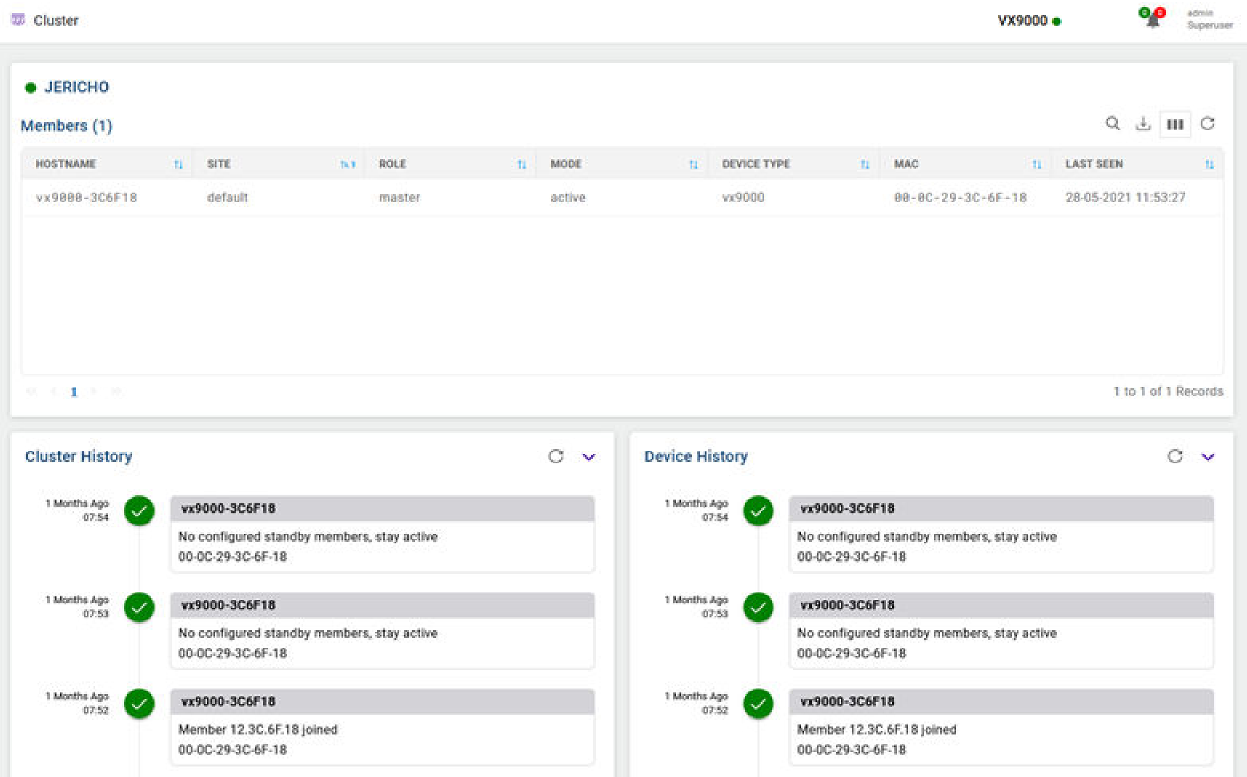
The **Adoption** panel displays the following information:

- 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 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:



JERICHO

Members (1)

HOSTNAME	SITE	ROLE	MODE	DEVICE TYPE	MAC	LAST SEEN
vx9000-3C6F18	default	master	active	vx9000	00-0C-29-3C-6F-18	28-05-2021 11:53:27

1 to 1 of 1 Records

Cluster History

1 Months Ago 07:54 — vx9000-3C6F18
No configured standby members, stay active
00-0C-29-3C-6F-18

1 Months Ago 07:53 — vx9000-3C6F18
No configured standby members, stay active
00-0C-29-3C-6F-18

1 Months Ago 07:52 — vx9000-3C6F18
Member 12.3C.6F.18 joined
00-0C-29-3C-6F-18

Device History

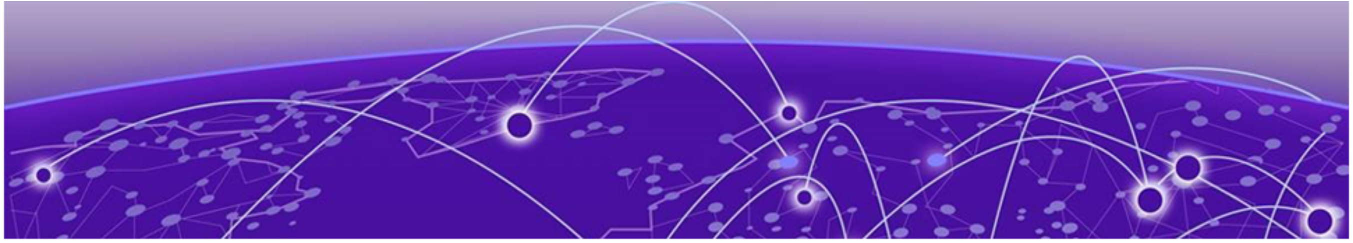
1 Months Ago 07:54 — vx9000-3C6F18
No configured standby members, stay active
00-0C-29-3C-6F-18

1 Months Ago 07:53 — vx9000-3C6F18
No configured standby members, stay active
00-0C-29-3C-6F-18

1 Months Ago 07:52 — vx9000-3C6F18
Member 12.3C.6F.18 joined
00-0C-29-3C-6F-18

Figure 2: Cluster dashboard

Members	List of cluster members within a cluster. Details include: • 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

Use **Sites** to define boundaries for fast roaming and session mobility without interruption, and to provision RF Domain-level QoS and security measures.

Manage Sites

Go to **Site**.

The **Site** window includes:

- A list of configured sites.
- Tools that allow users to manage sites.

View Configured Sites

The Sites window displays a list of all configured sites in tabular form.

Table 5 describes the type of information displayed under each column in the table.

Table 5: Sites List Column Headings

Column Heading	Description
Site Name	The name assigned to the site.
Location	The location of the site.
Contact	The site owner's contact information.
Time Zone	The time zone in which the site is situated.
Country	The country in which the site is located.
Action	See Management Tools

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select + to add and configure a new site.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a Site to modify it.
  - Select ⏻ to reload all APs at the associated Site.
  - Select ↻ to restore factory default settings on all APs at the associated Site.
  - Select ⚙ to execute a firmware upgrade on all APs at the associated Site.
  - Select 🗑 associated with a Site to delete it.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the sites entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.

Related Links

Add a Site on page 56

Add a Site

To add a site to WiNG network:

1. Select **Site** and + .

   The **Add site** window opens.

2. Configure the following site parameters:

Table 6: 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 Links

Edit Site Basic Configuration on page 57

Configure Site Policies on page 59

Delete a Site on page 60

Edit Site Basic Configuration

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

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	Name of the site
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

Field	Description
VLAN	Specify the VLAN (within a range of 1 - 4,094) used for traffic control within this site (RF Domain).
Tenant Account	Enter the ExtremeLocation Tenant's account number. At the time of registration, ExtremeLocation Tenants, receive an email containing an account number that identifies the Tenant. By configuring this account number in the RF Domain context, any RF Domain AP reports that are pushed to the ExtremeLocation server include the Tenant's account number along with the reporting AP's MAC address. Including the Tenant account number reinforces the Tenant's identity.
AD WIPS Wired Mitigation	Select this option to enable wired lockdown of wireless device connections upon acknowledgment of a threat.
AD WIPS Wireless Mitigation	Select this option to enable wireless lockdown of wireless device connections upon acknowledgment of a threat.
Enable NSight Sensor	Select this option to enable the NSight sensor module.

4. In the **Channel List**, configure channels used by RF domain member radios. These dedicated channels should be as segregated as possible from one another to avoid interference. If too many radios are utilizing a single channel, consider off-loading radios to non utilized channels to improve RF domain performance.
5. 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

6. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

   Note
   You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

Note
This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

Note
If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Add a Site on page 56
Configure Site Policies on page 59
Delete a Site on page 60

Configure Site Policies

Use this procedure to configure Site policies.

1. Go to **Site**.
2. Select a site from the **Sites** list.
3. Select the **Policies** tab.
4. Apply policies to a Site as described in

Table 7: Site Policies Parameters

Parameter	Description
SmartRF Policy	Select the SmartRF policy for the site from the drop-down menu.
NSight Policy	Select the NSight policy for the site from the drop-down menu.
WIPS Policy	Select the WIPS policy for the site from the drop-down menu.
Sensor Policy	Select the sensor policy for the site from the drop-down menu.
BLE Data Export Policy	Select the BLE Data Export policy for the site from the drop-down menu.

5. Choose from the following actions:

a. Select **Apply** to commit the configured settings.

Note
This does not save the settings you configured; it provides a preview of your applied settings. To undo the settings you applied, select **Revert**.

b. Select **Save** to commit and save the configured settings.

> Note
>
> If you do not select **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Add a Site on page 56
Edit Site Basic Configuration on page 57
Delete a Site on page 60

Delete a Site

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

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 Links

Add a Site on page 56
Edit Site Basic Configuration on page 57
Configure Site Policies on page 59

Configure RF Domain Overrides

Each WLAN provides associated wireless clients with an SSID (Service Set Identifier). This has limitations, because it requires wireless clients to associate with different SSIDs to obtain QoS and security policies. However, a ExtremeWireless WiNG managed RF Domain can have WLANs assigned and advertise a single SSID, but allow users to inherit different QoS or security policies. Use the **Override SSID** tab to assign WLANs an override SSID for the RF Domain, as needed.

Controllers and service platforms allow the mapping of a WLAN to more than one VLAN. When a wireless client associates with a WLAN, it is assigned a VLAN in such a way that users are load balanced across VLANs. The VLAN is assigned from the pool representative of the WLAN. Clients are tracked per VLAN, and assigned to the least used/loaded VLAN. Client VLAN usage is tracked on a per-WLAN basis.

Use this procedure to define an override SSID and override VLAN configuration used with an RF Domain.

1. Go to **Site** > **Overrides**.
2. Select the **Override SSID** tab, and create a new SSID override:
   a. Select **Add**.
   b. Select an existing **WLAN** to be assigned an override SSID.

      If a WLAN configuration has not been defined, see Wireless Configuration on page 104 for detailed information on the steps required to create a WLAN.

c. Enter the name of the **SSID** to use with this WLAN.

d. Proceed to the final step in this procedure or continue with configuration.

3. Select the **Override WPA2 Key** tab.

   The **Override WPA2 Key** tab enables an administrator to configure an override of a WLAN's existing WPA2 PSK at the RF Domain level (not the profile level).

   a. Select **Add** to add an override.

   b. Configure the parameters for the Override WPA2 Key as described in Table 8.

Table 8: Override WPA2 Key Parameters

Parameter	Description
WLAN	Select an existing WLAN to override its key at the RF Domain level.
WPA2 Key	Enter either an alphanumeric string of 8 to 64 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share in this new override PSK. The alphanumeric string allows character spaces. The string is converted to a numeric value. This pass phrase saves the administrator from entering the 256-bit key each time keys are generated.

   c. Proceed to the final step in this procedure or continue with configuration.

4. Select the **Override WEP128 Keys** tab.

   The **Override WEP128 Keys** screen enables an administrator to override a WLAN's existing WEP 128 Keys at the RF Domain level (not the profile level). WEP 128 uses a 104 bit key which is concatenated with a 24-bit IV *(initialization vector)* to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data on the WLAN. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

   Note
   After a WEP 128 key override is configured, it cannot be modified. It can only be deleted.

   a. Select + to add an override.

b. Configure the parameters for the WEP 128 key override as described in Table 9.

Table 9: Override WEP128 Keys Parameters

Parameter	Description
Generate Keys	Specify a 4- to 32-character RF Domain override Pass Key and select **Generate**. The pass key can be any alphanumeric string. Wireless devices and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys 1-4	Use the Key #1-4 areas to specify key numbers. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button. Selecting Show displays a key in exposed plain text.
WEP Keys	Enter 26 HEX or 13 ASCII characters representing WEP 128 Keys. Default WEP 128 keys are as follows: • Key 1 8bc9b8ea08534f3636b320afcc • Key 2 db9d5afe707faec43efc86c8e4 • Key 3 5cd34cecd69b0a3c5aac22d3cb • Key 4 697001201997e0577c49ba2793

c. Proceed to the final step in this procedure or continue with configuration.

5. Select the **Override VLAN** tab.

   a. Select + to add an override.

   b. Select an existing WLAN from the **Name** drop-down list.

   c. Set the override **VLAN** to a value in the range 1 – 4094.

   d. Define the client user limit for the VLAN. Set the **Wireless Client Limit** to a value in the range 0 – 8192.

   e. Proceed to the final step in this procedure or continue with configuration.

6. Select the **Override WLAN Shutdown** tab.

   a. Select **Add** to add an override.

   b. Select an existing WLAN from the **Name** drop-down list.

   c. Select the check box to **Enable** the override.

   d. Proceed to the final step in this procedure or continue with configuration.

7. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > Note
   > You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

   > Note
   > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
>
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Client/Sensor Configuration

Client Name Configuration

The **Client Name Configuration** pane displays clients connected to RF Domain member access points adopted by networked controllers or service platforms. Use the screen to associate administrator assigned client names to specific connected client MAC addresses for improved client management.

Sensor Configuration

The WIPS (Wireless Intrusion Protection System) protects clients and access point radio traffic from attacks and unauthorized wireless network access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities (in real time), and permits both wired and wireless device lock-downs upon threat acknowledgment.

In addition to dedicated AirDefense sensors, an access point radio can function as a sensor and upload information to an external WIPS server. Unique WIPS server configurations can be used by RF Domains to ensure a WIPS server configuration is available to support the unique data protection needs of individual RF Domains.

WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the access point radio(s) available to each managed WLAN. When an access point radio is functioning as a WIPS sensor, it is able to scan (in sensor mode) across all legal channels within the 2.4 GHz and 5 GHz radio bands. Sensor support requires an AirDefense WIPS Server on the network. Sensor functionality is not provided by the access point alone. The access point works in conjunction with a dedicated WIPS server.

The following APs can also function as an ExtremeLocation sensor: AP3000, AP3000X, AP5010, AP310i/e, AP410i/e, AP505i, AP510i/e, AP560i, AP7602, AP7612, AP7622, AP7632, AP7662, AP-8163, AP-8533

ExtremeLocation is a highly scalable indoor locationing platform that gathers location-related analytics, such as visitor trends, peak and off-peak times, dwell time, heat-maps, etc. to enable entrepreneurs deeper visibility at a venue. To enable the location tracking system, the ExtremeLocation server should be up and running and the RF Domain Sensor configuration should point to the ExtremeLocation server.

Related Links

Site on page 55

Configure RF Domain Client Names and Sensors on page 64

Configure RF Domain Client Names and Sensors

Use this procedure to configure, modify, or delete RF Domain clients and sensors.

1. Choose from the following actions:
   - If you are in the process of configuring a new Site (RF Domain), proceed to the next step.
   - If you want to edit or delete a RF Domain client or sensor, go to **Site** and select ✎ adjacent to the target Site, then follow the instructions in the steps in this procedure.
2. Select the **Client/Sensor** tab.
3. Select **Add** to create a new **ExtremeLocation Appliance**. Configure or edit the parameters as described in Table 10.

Table 10: ExtremeLocation Appliance Parameters

Parameter	Description
Server Id	Assign a Server ID for the ExtremeLocation resource. As of now only one (1) ExtremeLocation sever can be configured. Note: The ExtremeLocation sensor capabilities are supported on the following AP models: AP3000, AP3000X, AP5010, AP310i/e, AP410i/e, AP505i, AP510i/e, AP560i, AP7602, AP7612, AP7622, AP7632, AP7662, AP-8163, AP-8533
IP Address/Hostname	Provide the ExtremeLocation server's hostname. When configured, access points within the RF Domain post location-related analytics to the specified ExtremeLocation server. Note: Enter the server's hostname and not the IP address, as the IP address is likely to change periodically in order to balance load across multiple Location server instances.
Port	Specify the port for the ExtremeLocation server. This is the port on which the ExtremeLocation server is reachable. The default port is 443.
Action	Select 🗑 to delete an ExtremeLocation Appliance.

4. Select **Add** to create a new **Sensor Appliance**. Configure or edit the parameters as described in Table 11.

Table 11: Sensor Appliance Parameters

Parameter	Description
Server Id	Assign a numerical ID for up to three ADSP server resources. The server with the lowest defined ID is the first reached by the controller or service platform. The default ID is 1.
IP Address/Hostname	Provide the numerical (non DNS) IP address or hostname of each server used as a ADSP sensor server by RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore.
Port	Specify the port of each ADSP sensor server utilized by RF member devices. The default port is 443.
Action	Select 🗑 to delete a Sensor Appliance.

5. Select **Add** to create a new **Client Name**. Configure or edit the parameters as described in Table 12.

Table 12: Client Name Parameters

Parameter	Description
MAC Address	Enter the client's factory coded MAC address.
Name	Assign a name to the RF Domain member access point's connected client to make it easily recognizable.
Action	Select 🗑 to delete a Client Name.

6. After you have completed configuring the settings, choose from the following actions:
    a. Select **Revert** to restore default settings or restore the last saved settings.

        Note
        You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

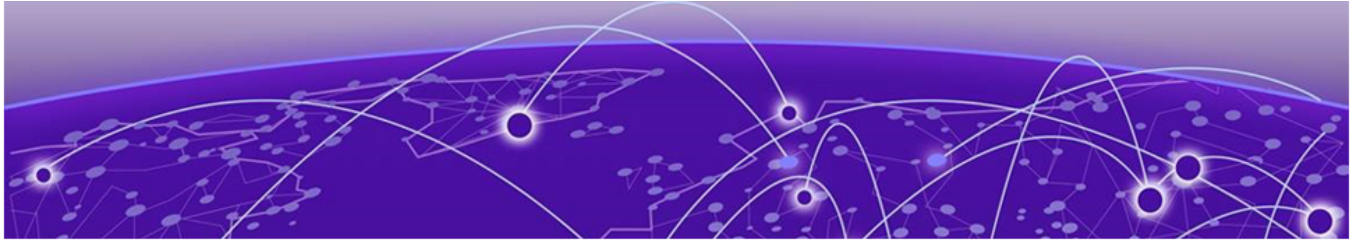
        Note
        This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

        Note
        If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Client/Sensor Configuration on page 63



Devices

This chapter describes how to manage and configure devices.

Device Management and Configuration

View, add, reload, factory reset, delete, or start a CLI session with a device:

1. Select **Devices**.

   The Devices window opens displaying the following:

   - a banner summarizing the number of configured devices in the network, the device types (access point or controller) and their status
   - **Basic Info** pane listing all the configured devices in the network

   See Device Summary and Basic Information on page 67 for details about the information provided in the Devices window.
2. You can take the following actions in the **Basic Info** pane:

   a. Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.

   b. Start a remote CLI session on a device as described in Access Remote CLI on page 68.

   c. Select the **Reload** icon ⏻ associated with a device to initiate a reload and application of configured parameters.

   d. Select the **Factory Reset** icon ⟳ associated with a device and select from the following options:

      - Delete Config and Entry
      - Delete Config
      - Reset Device

   e. Select a device in the list to open the configuration window for the device, then edit the device parameters as described in the procedures in this chapter.

f. Select the **Delete** icon 🗑 associated with a device to remove it.

g. Select the **Add** icon + to add a new device. See Add a Device on page 68 for further detail.

Device Summary and Basic Information

You can view a summary of configured devices and their status to help in performing analyses and assessments.

The **Devices** window displays a banner with the following information about configured devices in the network.

Icon	Description
●	Total number of devices
●	Number of online devices
●	Number of offline devices
●	Number of controllers
●	Number of access points (AP)

The **Basic Info** pane column heading topics provide the following information about the configured devices in the network.

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
CFG Status	Indicates the adopted Access Point configuration status
Mac Address	Device MAC address
IPv4/v6 Address	Device IPv4 or IPv6 address
Connected To	Indicates the connected controller. This column displays the cdp_lldp neighbors.
Adopted By	Indicates the controller that has adopted the device. This column displays the adopted controller MAC address.
Model	Device model number

Field	Description
Type	Device type description
Serial	Device serial number
Adoption Mode	Indicates whether the AP is connected to the controller through a VLAN or IP.
Controller	Indicates that the device is a controller
Firmware Version	WiNG firmware version running on the device
Profile Name	The name of the settings profile associated with the device

For information about actions you can take in the **Device** window, see Device Management and Configuration on page 66.

Access Remote CLI

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

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

   Note
   The remote CLI session is available only when the device status is active.

   A new remote CLI session opens.
4. Type the login credentials to access the remote CLI session.
5. Select ✕ to close the remote CLI session.

Add a Device

Add a controller or access point to the network.

Note
After modifying a device configuration profile, refresh the page before accessing device-level configuration.

1. Select **Devices**.
2. Select + to add a new device to the managed devices list.

   The **Add Device** option opens.

3. Configure the following device information:

Device Type	Select the device type from the drop-down list box
MAC Address	Provide the MAC address for the selected device
Site	Select a site from the drop-down list box to determine where the device will be located
Profile	Select a device profile

4. Select **Add** to create a new device.

   The **Basic** device configuration window opens.

Configure various device settings using the device configuration options.

Related Links

Basic Device Configuration on page 69
General Configuration on page 71
Interface Configuration on page 74
Adoption Configuration on page 73
Power Configuration (Access Points Only) on page 78
Network Configuration on page 79
Policies Configuration on page 79
Advanced Configuration on page 79
Mesh Point Configuration (Access Points Only) on page 80
Cluster Configuration (Controllers Only) on page 84
Message Logging Configuration for Devices on page 86
Back Up and Restore Configuration (Access Points Only) on page 88
Certificate Configuration on page 89
NAT Configuration on page 102
Critical Resource Management Configuration on page 103

Basic Device Configuration

Add a new device or edit an existing device basic configuration.

1. Select **Devices** > **Host Name**.

   The **Basic** configuration options open.
2. Configure the following settings:

   Note
   Device Overrides option is selected by default to ensure that device configurations receive periodic refinement automatically.

Table 13: Device Basic Configuration Options

MAC Address	Device MAC addressed assigned when adding the device. This field cannot be edited
Type	Device type selected when adding a device. This field cannot be edited
Name	Device name assigned to the selected device. Type or modify the device name using the **Name** field
Site	Device location. Use the drop-down list box to select a device site location
Profile	Assign a profile to the selected device. Profile allows admins to assign a common set of configuration parameters and policies to controllers, service platforms, and access points. Use the profile drop-down list box to assign a profile for the device

Table 14: Device Location Configuration

Area	Assign the physical area where the device is deployed. This can be a building, region, campus or other area that describes the deployment location
Floor	Assign the target device a building **Floor** name representative of the location the access point, controller, or service platform was physically deployed. The name cannot exceed 64 characters. Assigning a building floor name is helpful when grouping devices within the same general coverage area
Floor number	Assign a numerical floor designation with respect to the floor's actual location within a building. The default setting is first floor (1).

Table 14: Device Location Configuration (continued)

Latitude	Set the latitude coordinate where devices are deployed within a floor. When looking at a floor map, latitude lines specify the eastwest position of a point on the Earth's surface. The exact location of a device deployment can be ascertained by aligning the latitude and longitude points on the earth's surface
Longitude	Set the longitude coordinate where devices are deployed within a floor. When looking at a floor map, longitude lines specify the north-south position of a point on the Earth's surface. The exact location of a device deployment can be ascertained by aligning the longitude and latitude points on the earth's surface

3. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

General Configuration

Network Time Protocol (NTP) manages time and network clock synchronization within the network. NTP is a client or server implementation. Controllers, service platforms, and access points (NTP clients) periodically synchronize their clock with a main clock, which is an NTP server.

1. Select **Devices** > **Host Name** .

   The **Basic device configuration** dashboard opens.

2. Select **General** and configure the following settings:

NOC Update Interval	Specify the interval at which statistical updates are sent by the RF Domain manager to its adopting controller (the NOC controller). Enter a value in the range 5–3600 (seconds), or enter 0 to invoke auto mode where the update interval is automatically adjusted by the controller based on load information. The default value is 0.

3. Configure **NTP Server** settings.

   Select + to create a new NTP Server for the device and define NTP server resource configurations.

Server IP	Set the IP address of each server added as a potential NTP resource
Key Number	Select the number of the associated authentication peer key for the NTP resource. The key number range is between 1 to 65,534, and 1 is the default key number
Key	Type a 64 character maximum key used when the autokey setting is set to false or deactivated. Select the show option to view the character string for the key
Version	Use the spinner control to select a version between 0 to 4. The default version is 0
Minimum Polling Interval	Use the drop-down list box to select minimum polling interval. After the interval is set, the NTP resource is polled no sooner than the defined interval. Options include 64, 128, 256, 512, or 1024 seconds. The default setting is 64 seconds
Maximum Polling Interval	Use the drop-down list box to select the maximum polling interval. After the interval is set, the NTP resource is polled no later then the defined interval. Options include 1024, 2048, 4096, or 8192 seconds. The default setting is 1024 seconds
Preferred	Select **Preferred** to make the server settings the preferred setting for NTP servers
Autokey	Select **Autokey** to generate a key for the NTP server

4. Select **Add** to include the NTP server to the servers list.

5. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Adoption Configuration

Adoption is configurable and supported within a device configuration and applied to other access points supported by the host. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

1. Select **Devices** > **Host Name**.

   The **Basic device configuration** dashboard opens.
2. Select **Adoption**.
3. Within the **Controller** options, define a VLAN the access point's associating controller or service platform is reachable on.

   Use the spinner control to define a VLAN between 1 to 4,094.
4. Define a **Preferred Group** to set an optimal group for the controller's adoption.

   The preferred group name cannot exceed 64 characters.
5. Set the following host configuration:

   Select + to create a new host or ✎ to edit an existing host.

Host (IP Address)	Type a numerical IP address for the adoption resource
Host (Hostname)	Select **Host** to configure a hostname for the adoption resource. The hostname cannot exceed 64 characters
Pool	Use the spinner control to assign a pool of either 1 or 2. This is the pool the target controller belongs to

Routing Level	Use the spinner control define a routing level of either 1 or 2 for the link between adopting devices
IPSEC GW (IP Address)	Type a numerical IP address of the adopting controller resource
IPSEC GW (Hostname)	Select **IPSEC GW** to provide an admin defined hostname for the adopting controller
IPSEC Secure	Select **IPSEC Secure** to provide IPSec secure peer authentication on the connection link between the adopting devices
Remote VPN Client	Select **Remote VPN Client** to establish a secure controller link using a remote VPN client
Force	Select **Force** to create a forced link between an access point and an adopting controller

6. Select **Add** to create a new host for the adopting controller or select **Update** to make changes for an existing adopting controller.
7. Select **Save** to update adoption settings.

Interface Configuration

An access point profile can support customizable Ethernet port, virtual interface, port channel, radio and PPPoE configurations unique to each supported access point model.

1. Select **Devices** > **Host Name**.

   The Basic device configuration window opens.
2. Select **Interface**.

   A profile's interface configuration process is organized within several tabs.
3. Select each interface tab to configure settings.

Related Links

Interface Virtual Tab on page 74
Interface Ethernet Tab on page 75
Interface Radio Tab on page 76
Interface Bluetooth Tab on page 76
Interface PPPoE Tab on page 77
Interface Port Channels Tab on page 78

Interface Virtual Tab

A virtual interface is required for Layer 3 (IP) access to a controller, service platform, or virtual platform, or to provide Layer 3 service on a VLAN. The virtual interface defines which IP address is associated with each VLAN ID to which the device is connected. A virtual interface is created for the default VLAN (VLAN 1) to enable remote administration. A virtual interface is also used to map VLANs to IP address ranges. This mapping determines the destination for routing.

From the Device List, select a device, then select **Interface** > **Virtual**.

Configure the following settings for the virtual interface.

Table 15: Virtual VLAN Settings

Tab	Description
Basic	Configure admin status, limitations for maximum transmission unit (MTU), IPv6 configuration, and router advertisement settings.
IPV4	Specify the addressing protocol and the primary and secondary IP addresses and submasks with DHCP options and DHCP Relay where applicable.
Security	Configure security options such as firewall rules, a VPN crypto map, and a URL filter.
Routing	Configure routing settings for OSPF and Authentication

Interface Ethernet Tab

Configuration settings for each Ethernet Port.

Table 16: Interface Ethernet Settings

Tab	Description
Basic	Configure port settings for admin status, port channel and speed, duplex setting, and captive portal.
Switching	Configure switch port settings such as port mode, native VLAN, and allowed VLANS.
Aggregation	Configure port aggregation such as LACP port channel group and LACP port priority and specify whether the port is active or passive.
Discovery	Configure discovery settings for CDP and LLDP.
Fabric Attach	Configure VLAN ISID for fabric attach.
Security	Configure security settings for Access Control, Trust, and 802.11x Supplicant methods.
Spanning Tree	Configure settings for PortFast, MSTP, Port Cost, and Port Priority.

Interface Radio Tab

Access points can have their radio configurations modified by their management controller, service platform or peer access point. Take care not to modify an access point's configuration using its resident Web UI, CLI or SNMP interfaces when managed by a profile, or risk the access point having a configuration independent from the profile until the profile can be uploaded to the access point again from its managing device.

Configure radio settings for the selected radio.

Table 17: Interface Radio Settings

Tab	Description
Basic	Configure basic radio settings to include channel settings, RF management, client settings, channel adaptability.
WLAN	Configure WLAN radio settings to include beacon and guard intervals, probe response rate, DTIM interval, and WLAN BSS mappings.
Bridge	Configure Client Bridge settings to include roaming criteria, keep alive settings, authentication type, and channel plans.
MCX	Configure mesh network settings to include the number of mesh links, pre-shared key, preferred peer devices, and mesh mappings.
Antenna	Configure antenna settings for the device.
Aggregation	Configure aggregate-MSDU and Mpdu settings.
Scanning	Enable off-channel scanning for the selected radio.
Aeroscout	Configure the Aeroscout Real-Time Location System (RTLS) for location-based functionality.
Ekahau	Configure the Ekahau Real-Time Location System (RTLS) for location-based functionality.
Advanced	Configure preferred HT clients, braodcast/ multicast transmit rate and forwarding, fair airtime and sniffer information.

Interface Bluetooth Tab

Access Points use Bluetooth classic enabled radios to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

BLE enabled access points support Bluetooth beaconing to emit either iBeacon or Eddystone- URL beacons. The access point’s Bluetooth radio sends non-connectable, undirected low-energy (LE) advertisement packets on a periodic basis. These advertisement packets are short, and they are sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards.

Configure Internet of Things (IoT) settings.

Table 18: Interface Bluetooth Settings

Tab	Description
Basic	Configure basic BLE radio settings to include radio mode, transmit period, transmit pattern, and transmit power.
Eddystone	Configure beacon settings for Eddystone to include signal strength and transmit URL.
IBeacon	Configure beacon settings for IBeacon to include signal strength, and major, minor, and UUID values.

Interface PPPoE Tab

PPPoE connects multiple hosts on an Ethernet LAN to a remote site through a single customer device.

PPPoE is a data-link protocol for dialup connections. PPPoE allows the access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol.

PPPoE enables controllers, service platforms, and access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the access point's Wired WAN should fail.

Note
PPPoE-enabled devices continue to support VPN, NAT, PBR, and 3G failover on the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.

When PPPoE client operation is enabled, it discovers an available server and establishes a PPPoE link for traffic slow. When a wired WAN connection failure is detected, traffic flows through the WWAN interface in fail-over mode (if the WWAN network is configured and available). When the PPPoE link becomes accessible again, traffic is redirected back through the access point's wired WAN link.

When the access point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

Configure settings for the selected interface.

Table 19: Interface PPPoE Settings

Tab	Description
Basic	Configure basic PPPoE settings to include admin status, service, DSL network VLAN, client IP address, and default route priority.
Connection	Configure connections settings to include authentication credentials and type, maximum transmission unit (MTU), and idle timeout.
NAT	Configure Network Address Translation direction for network packets. Valid values are inside, outside, or none. addresses
Security	Configure broadcast-multicast control under inbound IPV4 firewall rules.

Interface Port Channels Tab

Controller, service platform and access point profiles can be applied customized port channel settings as part of their interface configuration. Configure settings for the selected port channel.

Table 20: Interface Port Channel Settings

Tab	Description
Basic	Configure port settings for admin status, speed, duplex setting, and load balance.
Switching	Configure switch port settings such as port mode, native VLAN, and allowed VLANS.
Security	Configure security settings for Access Control, firewall rules, and Trust.
Spanning Tree	Configure settings for PortFast, MSTP, Port Cost, and Port Priority.

Power Configuration (Access Points Only)

Go to **Devices** and select a target Access Point (AP), then select the **Power Config** tab.

Use device-level configuration to override profile-level settings for the selected device. Power configuration is identical for both device and profile levels. See Power Configuration on page 168 for instructions on setting **Power Config** parameters.

Network Configuration

Refer to the following topics to set up networking for a device:

- DNS Configuration on page 171
- ARP Configuration on page 172
- L2TP V3 Configuration on page 173
- GRE Tunnel Configuration on page 179
- GRE Concentrator Configuration on page 182
- IGMP and MLD Snooping Configuration on page 184
- Spanning Tree Configuration on page 188
- Routing Configuration on page 193
- Forwarding Database Configuration on page 195
- Bridge VLAN Configuration on page 197
- Alias Configuration on page 208

Policies Configuration

Assign policies to a device using the **Policies** tab. The policies available depend on the existing policies configured in the system.

Policy settings assigned to a device override any policy settings assigned to a device through an assigned device profile.

For more details about device policies configuration, see Device Profile - Policies Configuration on page 214.

Advanced Configuration

MiNT policy secures communications at the transport layer. Using MiNT, a device can be configured to communicate only with other MiNT activated devices.

Use this procedure to configure or edit MiNT Link policy.

> Note
> Use this procedure to configure a device profile, or to override profile settings for a specific device.

1. Go to **Profiles** or **Devices** and select a device from the profile or device list.
2. Select the **Advanced** tab.

3. Configure or edit the parameters as described in Table 21.

Table 21: MiNT Link Settings

Parameter	Description
MLCP IP	Select **MLCP IP** to activate *MiNT Link Creation Protocol* using an IP address. MLCP is used to create a UDP/IP link from the device to a neighbor. The neighboring device does not need to a controller or a service platform. It can be another access point with a path to the controller or service platform
MLCP IPv6	Select **MLCP IPv6** to activate MLCP for automated MiNT UDP/IP link creation
MLCP VLAN	Select **MLCP VLAN** to activate MiNT MLCP by VLAN. MLCP is used to create one VLAN link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be another access point with a path to the controller or service platform
Tunnel MiNT Across Extended VLAN	Select **Tunnel MINT Across Extended VLAN** to tunnel MiNT protocol packets across an extended VLAN

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Mesh Point Configuration (Access Points Only)

An access point can be configured to be a part of a meshed network. A mesh network is one where nodes in the network can communicate with each where each node can maintain more than one path to its peers. Mesh networking enables users to access broadband applications anywhere, including moving vehicles, by providing robust, reliable, and redundant connectivity to all the members of the network. When one of the nodes in a mesh network becomes unavailable, the other nodes in the network can still communicate with each other directly or through intermediate nodes.

Mesh point is the name given to a device that is a part of a meshed network.

Use the mesh point settings to configure or override the parameters that set how this device behaves as a part of the mesh network.

> **Note**
> Only access points can be configured as mesh point devices.

1. Select **Devices**.
2. Select an access point from the list of devices.

   The **Basic** window opens.
3. Select **Mesh Point**.

   The **Mesh Point** dashboard opens.
4. Select + to add a new mesh policy for the selected access point.
5. Select a policy from the list of available policies and select **Add**.
   a. Select ✎ to edit an existing mesh connex policy.
   b. Select 🗑 to delete an existing mesh connex policy.
6. Select a mesh connex policy to navigate to **Settings**.
7. Configure the following **General** mesh point settings:

Is Root	Select the root behavior of this access point. **True** means that this access point is a root node for this mesh network, and **False** means that it is not a root node. A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. **None** is the default setting
Root Selection Method	Use the drop-down menu to determine whether this mesh point is the root or non-root mesh point. Select either **None** (the default setting), **auto-mint**, or **auto-proximity**

Path Method	Select the method used for path selection in a mesh network. Available options include: • **None** – No criteria are used in root path selection • **uniform** – The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths) • **mobile-snr-leaf** – The access point is mounted on a vehicle or a mobile platform. The path to the route is selected based on the Signal To Noise Ratio (SNR) with the neighbor device • **snr-leaf** – The path with the best signal to noise ratio is always selected • **bound-pair** - Select to bind one mesh point connection at a time. Once established, other mesh point connection requests are denied
Set as Cost Root	Select to set the mesh point as the cost root for mesh point root selection
Monitor Critical Resources	Select to enable critical resource monitoring for this mesh point
Monitor Primary Port Link	Select to enable monitoring of primary port link is enabled for this mesh connex policy. If the primary port link is not present and if the device is a mesh root, it is automatically changed to a non-root device. When the primary port link becomes available again, the non-root device is changed back to a root device
Wired Peer Excluded	Select to exclude wired peers when creating mesh links

8. Set the following **Root Path Preference** values:

Preferred Neighbor	Specify the MAC address of a preferred neighbor for this mesh point
Preferred Root	Specify the MAC address of a preferred mesh root for this mesh point
Preferred Interface	Select the preferred interface for this mesh point. Select **None** to set no preferences. The other interface choices are 2.4 GHz, 4.9 GHz, 5 GHz, and 6 GHz

9. Set the following **Path Method Hysteresis** values:

Minimum Threshold	Type the minimum value for SNR above which a candidate for the next hop in a dynamic mesh network is considered for selection. This value, along with **Signal Strength Delta** and **Sustained Time Period** are used to dynamically select the next hop in a dynamic mesh network. The default setting is 0 dB
Signal Strength Delta	Type a delta value in dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR value that is higher than the value configured here. This value, along with the **Minimum Threshold** and **Sustained Time Period** are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 dB
Sustained Time Period	Type the duration from 1 to 600 seconds for the amount of time a signal must sustain the constraints specified in the **Minimum Threshold** and **Signal Strength Delta** path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 second
SNR Delta Range	Select the root selection method hysteresis from 1dB to 100dB SNR delta range a candidate must sustain. The default setting is 1 dB

10. Select **Update** to save the changes made to the mesh point configuration.

Mesh Point Auto Channel Selection (Access Points Only)

Use the **Auto Channel Selection** settings to configure the parameters for the MeshConnex policy on an access point.

1. Select **Devices**.
2. Select an access point from the device list.
3. Select **Mesh Point** and a device from the **Mesh Point** policy list.
4. Select **Auto Channel Selection**.
5. Select a frequency between **2.4 GHz**, **5.0/4.9 GHz**, or **6 GHz**.

6. Configure the following **Auto Channel Selection** values:

Channel Width	Set the channel width that the mesh point automatic channel scan assigns to the selected radio. Available options include: • **Automatic** - The channel width is calculated automatically. This is the default value. • **20 MHz** - Sets the width between adjacent channels as 20 MHz • **40 MHz** - Sets the width between adjacent channels as 40 MHz • **80 MHz** - Sets the width between adjacent channels as 80 MHz • **160 MHz** - Sets the width between adjacent channels as 160 MHz
Priority Mesh point	Configure the mesh point monitored for automatic channel scans. This is the mesh point assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a mesh point is automatically selected.

   Configure the rest of the auto channel selection values.

7. Select **Update** to save the changes made to the mesh point auto channel selection configuration.

Cluster Configuration (Controllers Only)

Configuration and network monitoring are two tasks a network administrator faces as a network grows in terms of the number of managed nodes (controllers, service platforms, wireless devices etc.). Such scalability requirements lead network administrators to look for managing and monitoring each node from a single centralized management entity. NX service platforms provide centralized management solution in the form of centralized management profile that can be shared by any single controller or service platform cluster member. This eliminates dedicating a management entity to manage all cluster members and eliminates a single point of failure.

> Note
> Cluster configuration is only available on controller devices.

1. Select **Devices**.
2. Select a controller from the existing **Devices** list.
3. Select **Cluster**.

   The **Settings** dashboard opens.

4. Configure the following **Settings**:

Mode	A member can be in either an **Active** or **Standby** mode. All active member can adopt access points. Standby members only adopt access points when an active member has failed or sees an access point not adopted by a controller or service platform. The default cluster mode is Active
Name	Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters
Master Priority	Set a priority value from 1 to 255, with the higher value given higher priority. This configuration is the device's priority to become the cluster master. In a cluster environment, one device from the cluster is elected as the cluster master. The master priority setting is the device's priority to become cluster master. The active primary controller has the higher priority. The default value is 128
Force Configured State Delay	Specify a delay interval between 3 to 1800 minutes. This is the interval a standby cluster member waits before releasing adopted APs and goes back to a monitoring mode when a controller becomes active again after a failure. The default interval is 5 minutes
Force Configured State	Select to enable this cluster member to take over for an active member if it were to fail. A standby controller or service platform takes over APs adopted by the failed member. If the failed cluster member were to come available again, the active member starts a timer based on the Auto Revert Delay interval. At the expiration of the Auto Revert Delay, the standby member releases all adopted APs and goes back to a monitoring mode. The Auto Revert Delay timer is stopped and restarted if the active member goes down and comes up during the Auto Revert Delay interval
Handle STP Convergence	Select to enable Spanning Tree Protocol (STP) convergence for the controller or service platform. In general, this protocol is enabled in layer 2 networks to prevent network looping. Spanning Tree is a network layer protocol that ensures a loop-free topology in a mesh network of inter-connected layer 2 cluster members. The spanning tree protocol clears redundant connections and uses the least costly path to maintain a connection between any two controllers or service platforms in the network. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup
Radius Counter DB Sync Time	Specify a sync time from 1 to 1,440 minutes a RADIUS counter database uses as its synchronization interval with the dedicated NTP server resource. The default interval is 5 minutes

5. Within the **Member** field, select **Cluster VLAN** to designate the VLAN where cluster members are reachable. Specify a VLAN from 1 to 4094.
6. Select **Add** to include **Member IP Address** and **Routing Level** information.

   Define a routing level between 1 or 2 for the link between adopting devices. The default setting is 1.
7. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Message Logging Configuration for Devices

Configure **Message Logging** settings for a selected device:

1. Select **Device**.

   A list of configured devices appears in the **Devices** pane of the **Basic Info** window. The total number of configured devices displays in parentheses.
2. Select a device in the list.

   The device configuration window opens displaying the **Basic** configuration for the device.
3. Select the **MSG Logging** tab.

   The **Message Logging** configuration window opens.

4. Configure the following settings:

Enable Message Logging	Select this option to enable the device to log system events to a log file or a syslog server. Selecting this check box enables the rest of the parameters required to define the device's logging configuration. This option is disabled by default.
Remote Logging Host	Select **Add** to create a table to define numerical (non DNS) IP addresses and ports for up to three external resources where logged system events can be sent on behalf of the device. Select **Add** to add a new IP address. Select the delete icon 🗑 as needed to remove an IP address.
Facility to Send Log Messages	Use the drop-down menu to specify the local server (if used) for device event log transfers.
Syslog Logging Level	Select this option to enable **Syslog Logging Level**. Use the drop-down list to assign a severity level to log events based on criticality. Event severity coincides with the syslog logging level defined for the device. Severity level options are **Emergencies**, **Alerts**, **Critical**, **Errors**, **Warnings**, **Notifications**, **Informational** and **Debugging**. The default logging severity level is Warning.
Console Logging Level	Select this option to enable **Console Logging Level**. Use the drop-down list to assign a severity level to log events based on criticality. Event severity coincides with the syslog logging level defined for the device. Severity level options are **Emergencies**, **Alerts**, **Critical**, **Errors**, **Warnings**, **Notifications**, **Informational** and **Debugging**. The default logging severity level is Warning.
Buffered Logging Level	Select this option to enable **Buffered Logging Level**. Use the drop-down list to assign a severity level to log events based on criticality. Event severity coincides with the syslog logging level defined for the device. Severity level options are **Emergencies**, **Alerts**, **Critical**, **Errors**, **Warnings**, **Notifications**, **Informational** and **Debugging**. The default logging severity level is Warning.
Forward Logs to Controller	Select this option to enable **Forward Logs to Controller**. Use the drop-down list to assign a severity level for forwarding event logs to the controller. Log level options are **Emergencies**, **Alerts**, **Critical**, **Errors**, **Warnings**, **Notifications**, **Informational** and **Debugging**. The default logging severity level is Errors.
Time to Aggregate Repeated Messages	Define the increment (or interval) system events are logged on behalf of the device. The shorter the interval, the sooner the event is logged. Define an interval in seconds (0 - 60) or in minutes (0 -1). The default value is 0 seconds.

5. After you have completed configuring the settings, choose from the following actions:
    a. Select **Revert** to restore default settings or restore the last saved settings.

    > Note
    > You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

    > Note
    > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

    > Note
    > If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Back Up and Restore Configuration (Access Points Only)

Use this procedure to export (back up) an access point (AP) **Startup** or **Running** configuration to a server using FTP, or to import (restore) a Startup configuration. You can also reset the startup and running configurations to restore the AP to its factory default.

> Note
> By default, the encryption key is not stored in the startup-config file. Use the **`inline-password-encryption`** command with the CLI to move the encrypted key to the startup-config file.

1. Go to **Devices** and select a target AP.
2. Select the **Config** tab.
3. Under the **Startup** tab, choose from the following actions:
    - Enter the path to the server where you want to store the startup-config file, then select Export.
    - Enter the path to the server from where you want to import the startup-config file, then select Import
    - Select Reset to restore the AP's startup configuration to factory default.
4. Under the **Running** tab, choose from the following actions:
    - Enter the path to the server where you want to store the running-config file, then select Export.
    - Select Reset to restore the AP's running configuration to factory default.

Certificate Configuration

A certificate links identity information with a public key enclosed in the certificate. Certificates are issued by a *certificate authority* (CA).

A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain the CA certificate in its Trusted Root Library so it can trust certificates that are signed by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/ identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. *Secure Shell* (SSH) public key authentication can be used by a requesting client to access resources, if properly configured. An RSA key pair must be generated on the client. The public portion of the key pair resides with the controller or access point locally, while the private portion remains on a secure area of the client.

Related Links

Configure Device Trustpoints on page 89
Manage Certificates and RSA Keys on page 92

Configure Device Trustpoints

Before proceeding with configuring device trustpoints, review existing RSA keys and certificates for possible reuse with your application. You can use the default **default_rsa_key** and **default_trustpoint** or, if required, you can generate or import an RSA key, or generate a self-signed certificate, or generate a certificate signing request (CSR).

Use this procedure to assign trustpoints for the selected device.

1. Go to **Devices** and select a target device, then select the **Certificate** tab.

   By default, the **Trustpoint** tab displays.

2. Configure **Management Security** as described in Table 22.

Table 22: Management Security Parameters

Parameter	Description
SSH RSA Key	Assign an RSA key to the selected device for SSH authentication and encryption of connections between devices. Use the drop-down menu to invoke the use of either a **Stored** key or a **Pending** key. • **`Pending`** (default) — Enter the name (up to 32 characters) of the pending RSA key. • **`Stored`** — Use the drop-down menu to select an existing RSA key. Note: Pending RSA keys are not verified as existing on a device.

3. Configure **RADIUS Security** as described in Table 23.

Table 23: RADIUS Security Parameters

Parameter	Description
RADIUS Certificate Authority LDAPS	Assign a trustpoint to RADIUS server certificate to validate an external LDAPS server. Use the drop-down menu to invoke the use of either a **Stored** trustpoint or a **Pending** trustpoint. • **`Pending`** (default) — Enter the name (up to 32 characters) of the pending trustpoint. • **`Stored`** — Use the drop-down menu to select an existing trustpoint. Note: Pending trustpoints are not verified as existing on a device.
RADIUS Server LDAPS Trustpoint	Use the drop-down menu to select a trustpoint to validate an external LDAPS server. Options include: • **`Pending`** (default) — Enter the name (up to 32 characters) of the pending trustpoint. • **`Stored`** — Use the drop-down menu to select an existing trustpoint. Note: Pending trustpoints are not verified as existing on a device.

4. Configure **CMP Certificate** as described in Table 24.

Table 24: CMP Certificate Parameters

Parameter	Description
Authenticate Operator Certificate	Optionally, use *Certificate Management Protocol* (CMP) as an Internet protocol to obtain and manage digital certificates in a *Public Key Infrastructure* (PKI) network. A CA issues the certificates using the defined CMP. Using CMP, a device can communicate with a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating with a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire. Use the drop-down menu to invoke the use of either a **Stored** trustpoint or a **Pending** trustpoint. • **`Pending`** (default) — Enter the name (up to 32 characters) of the pending trustpoint. • **`Stored`** — Use the drop-down menu to select an existing trustpoint. Note: Pending trustpoints are not verified as existing on a device.

5. Configure **HTTPS Trustpoint Security** as described in Table 25.

Table 25: HTTPS Trustpoint Security Parameters

Parameter	Description
HTTPS Trustpoint	Assigns a trustpoint to validate HTTPS. Use the drop-down menu to invoke the use of either a **Stored** trustpoint or a **Pending** trustpoint. • **`Pending`** (default) — Enter the name (up to 32 characters) of the pending trustpoint. • **`Stored`** — Use the drop-down menu to select an existing trustpoint. Note: Pending trustpoints are not verified as existing on a device.

6. Configure **Cloud Client Certificate** as described in Table 26.

Table 26: Cloud Client Certificate Parameters

Parameter	Description
Cloud Client Certificate	Assigns a trustpoint to validate a cloud client. Use this option on cloud-enabled APs to secure the communication between the cloud AP and cloud client. The trustpoint should be existing and installed on the AP. The cloud-enabled access points are AP7502, AP7522, AP7532, and AP7562. For local-controller adopted APs, this configuration is not required. Use the drop-down menu to invoke the use of either a **Stored** trustpoint or a **Pending** trustpoint. • `Pending` (default) — Enter the name (up to 32 characters) of the pending trustpoint. • `Stored` — Use the drop-down menu to select an existing trustpoint. Note: Pending trustpoints are not verified as existing on a device.

7. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Certificate Configuration on page 89

Manage Certificates and RSA Keys on page 92

Manage Certificates and RSA Keys

Go to **Devices** and select a target device, then select the **Certificate** tab. Next, select either the **Manage Certificates** or **RSA Keys** tab.

The Manage Certificates window displays a list of existing certificates and associated details. See View Certificates and Related Details.

The RSA Keys window displays a list of existing RSA Keys and associated details. See View RSA Keys on page 94.

Both windows include tools that allow users to manage certificates and RSA keys. See Management Tools on page 95.

View Certificates and Related Details

The Certificates window displays a list of all configured certificates in tabular form. The total number of configured certificates is displayed in parentheses.

Table 27 describes the type of information displayed under each column in the table.

Table 27: Certificates Table Column Headings

Column Heading	Description
Name	Displays the name assigned to the certificate.
RSA Key	Displays the name assigned to the RSA key pair.
Valid Until	Identifies the certificate expiration date and time.

Select a certificate in the table to view its associated properties. Table 28 describes the information displayed in the **Certificate Details**, **Validity**, and **Certificate Authority (CA) Details** panes.

Table 28: Certificate Properties

Certificate Properties	Description
Certificate Details	
Subject Name	Describes the entity to which the certificate is issued.
Alternate Subject Name	Lists alternate subject information about the certificate as provided to the certificate authority.
Issuer Name	Displays the name of the organization issuing the certificate.
Serial Number	Lists the unique serial number of the certificate.
Self Signed	Indicates whether this certificate is self signed, as follows: • ✓ means the certificate is self signed. • ✗ means the certificate is not self signed.
RSA Key Used	Indicates whether the certificate includes an RSA key, as follows: • ✓ means an RSA key is included in the certificate. • ✗ means an RSA key is not included in the certificate.

Table 28: Certificate Properties (continued)

Certificate Properties	Description
RSA Key	Displays the name of the key pair generated separately (under the **RSA Keys** tab), or generated automatically when creating a certificate (under the **Create Certificate** tab). Note: This field appears only when the **RSA Key Used** checkbox indicates that an RSA key is included in the certificate.
CRL Present	Indicates whether a *certificate revocation list* (CRL) is present, as follows: • ✓ means a CRL is present. • ✗ means a CRL is not present.
Is CA	Indicates whether this certificate is an authority certificate, as follows: • ✓ means the certificate is an authority certificate. • ✗ means the certificate is not an authority certificate.
Validity	
Valid From/Until	Identifies the period of time during which the certificate is valid.
Certificate Authority (CA) Details	
Subject Name	Displays information about the entity to which the certificate is issued.
Alternate Subject Name	This section provides alternate information about the certificate as provided to the certificate authority. This field is used to provide more information that supports information provided in the Subject Name field.
Issuer Name	Displays the organization issuing the certificate.

View RSA Keys

The RSA Keys window displays a list of existing RSA keys in tabular form. The total number of existing RSA keys is displayed in parentheses.

Table 29: RSA Keys Table Column Headings

Column Heading	Description
Name	Displays the name assigned to the RSA key.
Size	Indicates the size of the RSA key (in bits).
RSA Public Key	Identifies the syntax of the public key which corresponds to the RSA key.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the certificate or RSA key entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table, select 🗑 associated with a certificate or an RSA key to delete it.

Related Links

Certificate Configuration on page 89
Import Certificates and Trustpoints on page 95
Export Trustpoints on page 96
Generate an RSA Key on page 97
Import an RSA Key on page 98
Export an RSA Key on page 98
Create and Generate a Self-Signed Certificate on page 99
Create and Generate a Certificate Signing Request on page 101

Import Certificates and Trustpoints

A certificate links identity information with a public key enclosed in the certificate. Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

Use this procedure to optionally import a certificate or trustpoint.

1. Go to **Devices** and select a device.
2. Select the **Certificate** tab.
3. Select the **Manage Certificates** tab.

4. Select Import and configure the parameters as described in Table 30.

Table 30: Import Trustpoint Parameters

Parameter	Description
Trustpoint Details	
Trustpoint Type	Select the type of trustpoint to be imported. Options include: • Import – Select to import any trustpoint. • Import CA – Select to import a Certificate Authority (CA) certificate. • Import CRL – Select to import a CRL (Certificate Revocation List). CRLs are used to identify and remove installed certificates that have been revoked or are no longer valid. A certificate can be revoked if the CA had improperly issued a certificate, or if a private key is compromised. The most common reason for revocation is that the user no longer has sole possession of the private key. • Import Signed Cert – Select to import a self-signed certificate.
Trustpoint Name	Enter the name (up to 32 characters) assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, a corporation, or an individual.
Location of Trustpoint	
Path/File	Specify the path to the trustpoint file. Enter the complete relative path to the file on the server.

5. Select **OK** to import the target trustpoint.

Related Links

Manage Certificates and RSA Keys on page 92

Export Trustpoints on page 96

Export Trustpoints

The trustpoints utilized by a controller, service platform or access point can be exported to an external resource for archive.

Once a certificate has been generated on the local authentication server, export the self-signed certificate. A digital CA certificate is different from a self-signed certificate. The CA certificate contains the public and private key pairs. The self-signed certificate only contains a public key. Export the self-signed certificate for publication on a Web server or file server for certificate deployment, or export it in to an active directory group policy for automatic root certificate deployment.

Additionally, export the key to a redundant RADIUS server so it can be imported without generating a second key. If there's more than one RADIUS authentication server, export the certificate and do not generate a second key unless you want to deploy two root certificates.

Use this procedure to export trustpoints.

1. Go to **Devices** and select a device.
2. Select the **Certificate** tab.
3. Select the **Manage Certificates** tab.
4. Select Export and configure the parameters as described in Table 31.

Table 31: Export Trustpoint Parameters

Parameter	Description
Trustpoint Details	
Trustpoint Name	Enter the name (up to 32 characters) assigned to the trustpoint. The trustpoint signing the certificate can be a certificate authority, a corporation, or an individual.
Trustpoint Location	
Path/File	Specify the path to the signed trustpoint file. Enter the complete relative path to the file on the server.

5. Select **OK** to export the defined trustpoint.

Related Links

Manage Certificates and RSA Keys on page 92

Import Certificates and Trustpoints on page 95

Generate an RSA Key

Use this procedure to generate an RSA key for the selected device.

1. Go to **Devices** and select a target device.
2. Select the **Certificate** tab.
3. Select the **RSA Keys** tab.
4. To create an RSA key, select Generate and configure the parameters as described in Table 32.

Table 32: Generate RSA Key Parameters

Parameter	Description
Key Name	Enter a name (up to 32 characters) for the RSA key.
Key Size	Set the size of the key (in bits) as either 2048 or 4096. For optimum functionality, the recommended setting is 2048.

5. Select **OK** to generate the RSA key.

Related Links

Manage Certificates and RSA Keys on page 92

Import an RSA Key on page 98

Export an RSA Key on page 98

Import an RSA Key

Controllers, service platforms and access points can import RSA keys utilized by other devices.

Use this procedure to import an RSA Key.

1. Go to **Devices** and select a target device.
2. Select the **Certificate** tab.
3. Select the **RSA Keys** tab.
4. Select Import and configure the parameters as described in Table 33.

Table 33: RSA Keys – Import Parameters

Parameter	Description
Key Name	Enter the name (up to 32 characters) of the RSA key to be imported.
Key Passphrase	Define the key used by both the controller or service platform and the server (or repository) of the target RSA key. Select 👁 to view the characters used in the passphrase. Otherwise, the passphrase displays as a series of asterisks (****).
Path/File	Specify the path to the RSA key. Enter the complete relative path to the key on the server.

5. Select **OK** to import the defined RSA key.

Related Links

Manage Certificates and RSA Keys on page 92
Generate an RSA Key on page 97
Export an RSA Key on page 98

Export an RSA Key

The keys utilized by a controller, service platform or access point can be exported to an external resource for archive and future use.

Export the key to a redundant RADIUS server to import it without generating a second key. If there is more than one RADIUS authentication server, export the certificate and do not generate a second key unless you want to deploy two root certificates.

Use this procedure to export an RSA key.

1. Go to **Devices** and select a target device.
2. Select the **Certificate** tab.
3. Select the **RSA Keys** tab.

4. Select Export and configure the parameters as described in .

Table 34: RSA Keys – Export Parameters

Parameter	Description
Key Name	Enter the name (up to 32 characters) of the RSA key to be exported.
Key Passphrase	Define the key used by both the controller or service platform and the server (or repository) of the target RSA key. Select 👁 to view the characters used in the passphrase. Otherwise, the passphrase displays as a series of asterisks (****).
Path/File	Specify the path to the RSA key. Enter the complete relative path to the key on the server.

5. Select **OK** to export the defined RSA key.

Related Links

Manage Certificates and RSA Keys on page 92

Generate an RSA Key on page 97

Import an RSA Key on page 98

Create and Generate a Self-Signed Certificate

Use this procedure to create new self-signed certificates that can be applied to managed devices. Self-signed certificates (often referred to as root certificates) do not use public or private CAs. A self-signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

1. Go to **Devices** and select the device to which you want to apply the new self-signed certificate.
2. Select the **Certificate** tab.
3. Select the **Create Certificate** tab and configure the parameters as described in Table 35.

Table 35: Create Certificate Parameters

Parameter	Description
Create Self Signed Certificate	
Certificate Name	Enter a name (up to 32-characters) to identify the trustpoint associated with the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

Table 35: Create Certificate Parameters (continued)

Parameter	Description
SSH RSA Key	Set the key used by both the controller or service platform and the server (or repository) of the target RSA key. Use the drop-down menu to select one of the following options: • Generate New — Enter a **Name** to identify the RSA key. By default, the key size is 2,048 bits. • Use Existing — Use the drop-down menu to select a RSA Key Name.
Certificate Subject Name	
Certificate Subject Name	Use the drop-down menu to select one of the following options: • User Configured — Enter the credentials of the self-signed certificate. • Auto Generate — Automatically creates the certificate's subject credentials.
Country (C)	Define the country used in the certificate. This is a required field and must not exceed 2 characters.
State (ST)	Enter the state or province name used in the certificate. This is a required field.
City (L)	Enter a city to represent the city used in the certificate. This is a required field.
Organization (O)	Define the organization represented in the certificate. This is a required field.
Organizational Unit (OU)	Enter the organization unit represented in the certificate. This is a required field.
Common Name (CN)	If there is a common name (IP address) for the organizational unit issuing the certificate, enter it here.
Additional Credentials	
Email Address	Provide an email address to be used as the contact address for issues relating to this certificate request. This is a required field.
Domain Name	Enter a *fully qualified domain name* (FQDN), which is an unambiguous domain name that absolutely specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added, for example, *somehost.example.com.*. An FQDN differs from a regular domain name by its absoluteness, as a suffix is not added. This is a required field.
IP Address	Specify the IP address used as the destination for certificate requests. Only IPv4 formatted IP addresses are permitted. IPv6 formatted addresses are not permitted. This is a required field.

4. Select **Generate Certificate** to generate the certificate.

> Note
> If you exit Create Certificate configuration without generating the certificate, configured settings will persist, but only until you log out.

Related Links

[Manage Certificates and RSA Keys](#) on page 92

Create and Generate a Certificate Signing Request

A *certificate signing request* (CSR) is a message from a requester to a certificate authority to apply for a digital certificate. The CSR is composed of a block of encrypted text generated on the server where the certificate will be used. It contains the organization name, common name (domain name), locality, and country.

An RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but it is used to digitally sign the completed request. The certificate created with a particular CSR only works with the private key generated with it. If the private key is lost, the certificate is no longer functional. The CSR can be accompanied by other identity credentials required by the certificate authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

Use this procedure to create and generate a CSR.

1. Go to **Devices** and select the device to which you want to apply the new self-signed certificate.
2. Select the **Certificate** tab.
3. Select the **Create CSR** tab and configure the parameters as described in .

Parameter	Description
Create Certificate Signing Request (CSR)	
SSH RSA Key	Set the key used by both the controller or service platform and the server (or repository) of the target RSA key. Use the drop-down menu to select one of the following options: • Generate New — Enter a **Name** to identify the RSA key. By default, the key size is 2,048 bits. • Use Existing — Use the drop-down menu to select a RSA Key Name.
Certificate Subject Name	

Parameter	Description
Certificate Subject Name	Use the drop-down menu to select one of the following options: • User Configured — Enter the credentials of the CSR. • Auto Generate — Automatically creates the CSR's subject credentials.
Country (C)	Define the country used in the CSR. This is a required field and must not exceed 2 characters.
State (ST)	Enter the state or province name used in the CSR. This is a required field.
City (L)	Enter a city to represent the city used in the CSR. This is a required field.
Organization (O)	Define the organization represented in the CSR. This is a required field.
Organizational Unit (OU)	Enter the organization unit represented in the CSR. This is a required field.
Common Name (CN)	If there is a common name (IP address) for the organizational unit issuing the certificate, enter it here.
Additional Credentials	
Email Address	Provide an email address to be used as the contact address for issues relating to this CSR request. This is a required field.
Domain Name	Enter a *fully qualified domain name* (FQDN), which is an unambiguous domain name that absolutely specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added, for example, *somehost.example.com.*. An FQDN differs from a regular domain name by its absoluteness, as a suffix is not added. This is a required field.
IP Address	Specify the IP address used as the destination for certificate requests. Only IPv4 formatted IP addresses are permitted. IPv6 formatted addresses are not permitted. This is a required field.

4. Select **Generate CSR** to generate the CSR.

Note
If you exit Create CSR configuration without generating the CSR, configured settings will persist, but only until you log out.

Related Links

Manage Certificates and RSA Keys on page 92

NAT Configuration

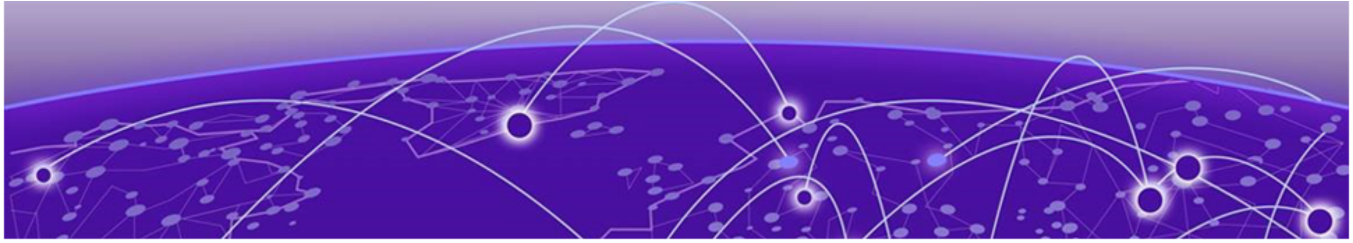
Go to **Devices** and select a target device, then select the **NAT** tab.

Use device-level configuration to override profile-level settings for the selected device. NAT configuration is identical for both device and profile levels. See NAT Configuration on page 226 for instructions on configuring NAT parameters.

Critical Resource Management Configuration

Go to **Devices** and select a target device, then select the **CRM** tab.

Use device-level configuration to override profile-level settings for the selected device. Critical Resource Management (CRM) configuration is identical for both device and profile levels. See Critical Resource Management Configuration on page 235 for instructions on configuring CRM parameters.



Wireless Configuration

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one connected access point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs can provide an abundance of services, including data communications (allowing mobile devices to access applications), E-mail, file and print services or even specialty applications (such as guest access control and asset tracking).

Each WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected access point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each connected access point. A WLAN can be advertised from a single access point radio or can span multiple access points and radios. WLAN configurations can be defined to only provided service to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

RFS 4000 model controllers support a maximum of 32 WLANs. NX 7500 model service platforms support up to 256 WLANs. An NX 95XX Series service platform supports up to 1000 WLANs. Access points can support a maximum of 16 WLANs per model.

WLAN policies can be separately selected and refined in the **Configuration → Wireless** pane located on the top left-hand side of the UI.

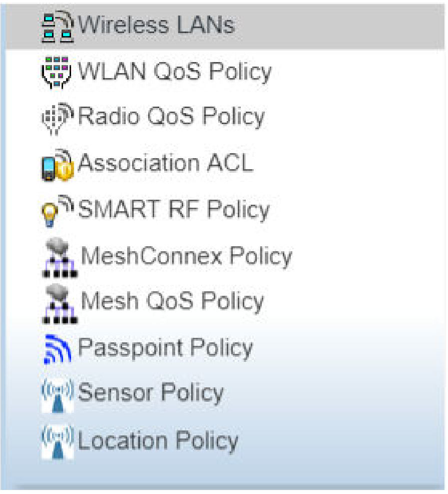


Figure 3: Configuration > Wireless Pane

Refer to the sections that follow for instructions on wireless configuration tasks.

Manage Wireless LANs

Go to **Wireless**.

The **Wireless** dashboard includes:

- A list of configured WLANs.
- Tools that allow users to manage WLANs.

View Configured WLANs

The Wireless dashboard displays a list of all configured WLANs in tabular form. The total number of WLANs is shown in parentheses.

Table 36 describes the type of information displayed under each column in the table.

Table 36: Wireless Dashboard Column Headings

Column Heading	Description
Name	Displays the name assigned to each available WLAN.
Status	Lists each WLAN's current status as follows: • ✓: enabled and available to clients on all radios where the WLAN has been mapped • ✗: disabled or shut down – if the WLAN is mapped to radios, it is not available for clients to associate either Disabled or Enabled. A green check mark defines the WLAN as available to clients on all radios where it has been mapped. A red "X" defines the WLAN as shutdown, meaning even .

Table 36: Wireless Dashboard Column Headings (continued)

Column Heading	Description
SSID	Displays the SSID assigned to the WLAN when created or last modified.
Encryption	Displays the name of the encryption type each listed WLAN is using to secure its client membership transmissions. None is listed if encryption is not used within this WLAN. Refer to the Authentication column to verify that there is some sort of data protection used with the WLAN or risk using this WLAN with no protection at all.
Authentication	Displays the name of the user authentication scheme each listed WLAN is using to secure its client membership transmissions. None is listed if authentication is not used within this WLAN. Refer to the Encryption column if no authentication is used to verify there is some sort of data protection used with the WLAN or risk no protection at all.
VLAN(s)	Lists each WLAN's current VLAN mapping. Mapping a WLAN to more than one VLAN is permitted. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. The VLAN is picked from a pool assigned to the WLAN. Keep in mind however, typical deployments only map a single VLAN to a WLAN. The use of a pool is strictly optional.
Forwarding Mode	Lists each WLAN’s current bridging mode as either: • **`Local`**: VLAN traffic is bridged locally • **`Tunnel`**: a shared tunnel is used for bridging the WLAN’s VLAN traffic The default setting is Local.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the WLAN entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.

- From under the **Actions** column in the table choose from the following actions:
    - Select ✎ associated with an entry to modify it.
    - Select 🗑 associated with an entry to delete it.
- Select + to configure a new WLAN.

Add Wireless LAN

Use this procedure to configure a new WLAN.

1. Go to **Wireless**.
2. Select + to create a new wireless network configuration.
3. Configure the Rule parameters as described in Table 37.

Table 37: Wireless Parameters

Parameter	Description
Wireless Name	Assign a name to the WLAN.
SSID	Assign a SSID (Service Set IDentifier) to the WLAN.

4. Optionally, select the **Copy From** checkbox and choose an existing WLAN from which to copy the configuration settings.
5. Select **Add**.
6. Configure WLAN parameters under the **Basic**, **Security**, and **Client Load Balancing** tabs, as necessary.

    Note
    If you exit the wireless network configuration without first adding and saving any basic or security settings, the configured WLAN persists, but only until you log out.

Related Links

Configure Wireless LAN Basic Settings on page 107
Configure Wireless LAN Security Settings on page 110

Configure Wireless LAN Basic Settings

You must be in the process of configuring a new wireless network or modifying an existing network to use this procedure.

Use this procedure to configure or modify WLAN Basic settings.

1. Choose from the following actions:
    - If you are in the process of configuring a new WLAN, proceed to the next step.
    - If you want to modify WLAN Basic settings, go to **Wireless**, then select ✎ associated with the target WLAN. Edit the Basic parameters in accordance with the steps in this procedure.

2. Configure the following **WLAN** parameters as described in Table 38.

Table 38: WLAN Parameters

Parameter	Description
Status	Enables or disables the WLAN. Status is enabled by default. Deselect the check box to disable the WLAN.
Name	Displays the Name assigned when the WLAN was created. The Name cannot be modified.
SSID	Displays the SSID (Network name) assigned when WLAN was created. The SSID can be modified.
Description	Enter a WLAN description (maximum 64 characters).
Bridging Mode	Select mode **`local`** or **`tunnel`** from the drop-down list box.
QoS Map	Select to provide a network coverage map
QoS policy	Outgoing network traffic. Default option is selected
Bonjour Gateway Discovery Policy	Select a policy from the drop-down to help users discover the wireless network
Broadcast SSID	This option is enabled by default. Deselect the checkbox to disable it.
Broadcast Probe Response	This option is enabled by default. Deselect the checkbox to disable it.
DHCP option82	Select the checkbox to enable this option. It is disabled by default.
DHCPv6 LDRA	Select the checkbox to enable this option. It is disabled by default.

3. 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
   - Fast BSS transition over DS Boolean

4. Select the **client traffic** checkbox to enable client-to-client traffic.
5. Set the max firewall sessions between 10 and 10,000.
6. Select access policies from the **Association ACL**, **Captive Portal Policy**, **Application Management Policy**, and **Roaming Assist Policy** drop-down menus.
7. Select firewall policies for **IP Inbound ACL** and **IP Outbound ACL**, and the **MAC Inbound ACL** and **MAC Outbound ACL**.

8. Select the projected management frames (PMF).

Table 39: 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

9. Use the **RRM - Radio Resource Management** checkboxes to enable or disable radio settings. These settings are enabled by default.
    a. Select **Status** to view RRM status for various managed networks.
    b. Select **Channel Report** to view this report.
    c. Select **TPC Report** to view this report.
    d. Use the **Neighbor-Report** drop-down menu to select either the **`Hybrid`** or **`Smart-RF`** option. Smart-RF is the default setting.
10. Configure the **Shutdown Criteria**.
    a. Assign a **Critical Resource Name**.
    b. Select the associated checkboxes to enable any or all of the these settings: **Unadoption**, **Wired Link Loss**, **Meshpoint Loss**, and **Critical Resource**
11. Configure the **VLAN Assignment**.
    a. Select **Single VLAN** to configure one VLAN, then type the VLAN number in the **VLAN** field.
    b. Select **VLAN Pool** to configure multiple VLANs.
        i. Type the VLAN numbers and the maximum number of wireless clients.
        ii. Select 🗑 to delete a VLAN.
12. Select the **MBO** checkbox to enable agile multi-band operation.
13. After you have completed configuring the settings, choose from the following actions:
    a. Select **Revert** to restore default settings or restore the last saved settings.

    > Note
    > You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

    > Note
    > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

    > Note
    > If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configure Wireless LAN Security Settings

Configure a wireless network's security details.

1. Select **Wireless**.
2. Select a wireless network and navigate to the **Security** tab.
3. Configure **Authentication** settings.

Setting	Description
Select Authentication	Choose an authentication method from the drop-down menu. You cannot configure **AAA policy** and **Reauthentication** if you select **PSK/None**.
AAA policy	Choose the AAA policy for the WLAN from the drop-down menu.
Reauthentication	Enter a value in the range 30 to 86400.

4. Configure encryption settings.

Table 40: Encryption details

Encryption option	Description
Select encryption	Choose an encryption type from the **Select Encryption** drop-down menu.

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

Table 41: 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. 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. 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.

Table 41: Encryption options (continued)

Encryption type	Details
Open	Open encryption. Not secured or protected
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	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. 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.
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	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. 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.

5. Choose an existing policy from the **Passpoint Policy** drop-down menu to apply it to the WLAN. If no policy exists, you can create one. See Passpoint Policy on page 446.
6. Choose an existing Wireless Network from the **OWE Companion** drop-down menu to enable *Opportunistic Wireless Encryption* (OWE) transition mode, which allows for a seamless transition from Open unencrypted WLANs to OWE WLANs.
7. Select the **SAE Hash to Element** checkbox to enable use of the SAE hash algorithms with WPA and WPA2 encryption methods.
8. Select the **Allow** checkbox to define the **EAP Types** allowed to be used for authentication on the WLAN.
9. After you have completed configuring the settings, choose from the following actions:

    a. Select **Revert** to restore default settings or restore the last saved settings.

    > Note
    > You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configure Wireless LAN Client Load Balancing

You must be in the process of configuring a new wireless network or modifying an existing network to use this procedure.

Use this procedure to configure or modify **Client Load Balancing** settings for a WLAN.

1. Choose from the following actions:
   - If you are in the process of configuring a new WLAN, proceed to the next step.
   - If you want to modify a WLAN's Client Load Balancing settings, go to **Wireless**, then select ✎ associated with the target WLAN. Edit the parameters in accordance with the steps in this procedure.
2. Select the **Client Load Balancing** tab.
3. Configure or edit the **Load Balancing Basic** parameters as described in Table 42.

   These settings apply to both the 2.4 GHz and 5.0 GHz bands.

Table 42: Load Balancing Basic Parameters

Parameter	Description
Enforce Client Load Balancing	Select this option to enforce a client load balance distribution on this WLAN's access point radios. Loads are balanced by ignoring association and probe requests. Probe and association requests are not responded to, forcing a client to associate with another access point radio. This setting is disabled by default.
Band Discovery Interval	Enter a value in the range 0 – 10,000 (seconds) to set the interval dedicated to discover a client's radio band capability before its access point radio association. The default setting is 24 seconds.
Capability Ageout Time	Enter a value in the range 0 – 10,000 (seconds) to age out a client's capabilities from the internal table. The default is 24 seconds.

4. Configure or edit the **Load Balancing (2.4GHz)** parameters as described in Table 43.

Table 43: Load Balancing (2.4GHz) Parameters

Parameter	Description
Single Band Clients	Select this option to enable association for single 2.4GHz clients, even if load balancing is available. This setting is enabled by default.
Max Probe Requests	Enter a value in the range 0 – 10,000 to set the maximum number of probe requests for clients using the 2.4GHz frequency. The default value is 60.
Probe Request Interval	Enter a value in the range 0 – 10,000 (seconds) to set an interval for client probe requests, beyond which association is allowed for clients on the 2.4 GHz frequency. The default is 10 seconds.

5. Configure or edit the **Load Balancing Settings (5GHz)** parameters as described in Table 44.

Table 44: Load Balancing Settings (5GHz) Parameters

Parameter	Description
Single Band Clients	Select this option to enable the association of single 5GHz clients, even if load balancing is available. This setting is enabled by default.
Max Probe Requests	Enter a value in the range 0 – 10,000 for the maximum number of client associations on the 5.0 GHz frequency. The default value is 60.
Probe Request Interval	Enter a value in the range 0 – 10,000 (seconds) to configure the interval for client probe requests. When exceeded, clients can associate in 5GHz. The default is 10 seconds.

6. After you have completed configuring the settings, choose from the following actions:
    a. Select **Revert** to restore default settings or restore the last saved settings.

        Note
        You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

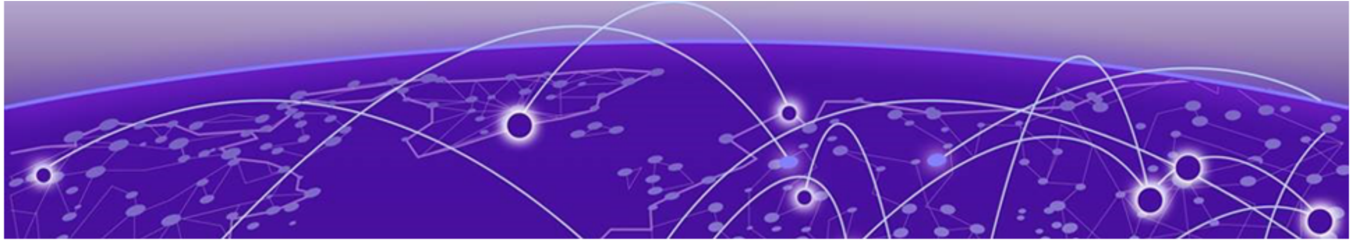
        Note
        This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

        Note
        If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Add Wireless LAN on page 107
Configure Wireless LAN Basic Settings on page 107
Configure Wireless LAN Security Settings on page 110



Profiles

You can assign common set of configuration parameters and policies to controllers, service platforms, and access points (APs). 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 APs. All AP models running WiNG OS support a single profile that is shared amongst multiple APs. The central benefit of a profile is the ability to update APs collectively without having to modify individual configurations.

A profile allows AP administration across large wireless network segments. Changes made to a profile are automatically inherited by all member APs.

➡ **Important**

You can override the profile settings at the device level (see Devices on page 66). It is important to remember that individual APs 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 AP.

After modifying a device profile and saving the settings, refresh the page before accessing device-level configuration.

Each AP model is automatically assigned a default profile. The default profile is available within the AP's configuration file. Default profiles are ideal for single-site deployments where several APs may need to share a common configuration.

➡ **Important**

Default profiles are used as pointers for an AP'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 APs using that profile.

User-defined profiles, on the other hand, are manually created for each supported service and virtual platform, wireless controller, and AP model. User-defined profiles are recommended for larger deployments using centralized controllers and service or virtual platforms when groups of devices on different floors, buildings or sites share a common configuration. These user-defined profiles can be manually, or automatically assigned to through an auto provisioning policy. An auto provisioning policy provides the means to assign profiles to access points based on model, serial number, VLAN ID, DHCP options, IP address (subnet) and MAC address. For more information, see Auto-Provisioning Policy on page 280.

View and Manage Profiles

Go to **Profiles**.

The **Profiles** window includes:

- A list of device profiles.
- Tools that allow users to manage profiles.

View Configured Profiles

The Profiles window displays a list of all profiles (default and custom) in tabular form.

Table 45 describes the type of information displayed under each column in the table.

Table 45: Profiles List Column Headings

Column Heading	Description
Profile Name	Displays the default profile name, or name assigned to the custom profile.
Device Type	Displays the device type for which the profile is designed.
Firewall Policy	Displays the Firewall Policy assigned to the profile.
Management Policy	Displays the Management Policy assigned to the profile.
Action	See Management Tools for instructions.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Profile table entries in csv format.
- Select ⦀ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a device profile to modify it.
  - Select 🗑 associated with a device profile to delete it.
- Select + to configure a new, custom device profile.

Add a Profile

Add profile information for access points (APs), controllers and service platforms.

1. Select **Profiles**.
2. Select +.

   The **Add Profile** dashboard opens.

3. Configure profile parameters as described in Table 46.

Table 46: Profile Parameters

Parameter	Description
Profile Name	Enter 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, then select an existing profile from the drop-down list to copy profile configuration information. Only profile configuration information is copied. The profile name and device type remains unique

4. Select **Add**.

   The **General** tab opens by default.

   > Note
   > You must configure and save settings in at least one of the tabs to save the profile permanently. Otherwise, the created profile persists if you move away from Profile configuration, but only until you log out.

Related Links

Profiles on page 115

Configure General Profile Settings on page 118

Adoption Configuration on page 121

Power Configuration on page 168

Configure General Profile Settings

You must be in the process of configuring a new device profile or editing an existing device profile to perform this procedure.

Use this procedure to configure or edit general device profile settings.

1. Choose from the following actions:
   - If you are in the process of configuring a new device profile, proceed to the next step.
   - If you want to edit device profile settings, go to **Profiles** and select ✎ adjacent to the profile you want to modify. Proceed to the next step.
   - If you want to override general device profile settings for a specific device, go to **Devices**, select the target device, then proceed to the next step.
2. Select the **General** tab, then configure parameters under the **Basic** and **NTP** panes. After these parameters are configured, proceed to the next step to complete this procedure.

3. After you have completed configuring the settings, choose from the following actions:
    a. Select **Revert** to restore default settings or restore the last saved settings.

        Note
        You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

        Note
        This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

        Note
        If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Basic

Configure or edit the Basic parameters as described in the following table.

Table 47: General Profile Configuration – Basic Parameters

Parameter	Description
Name	Cannot be edited. The name is set when adding a new profile
Device Type	Cannot be edited. The device type is set when adding a new profile.
Area	Specify the device location. Enter the area name (maximum 64 characters).
Floor	Enter the floor name where the target device is located (maximum 64 characters). Assigning a building floor name helps in grouping devices within the same general coverage area.
Floor No.	Optionally, set the floor number.
NOC Update Interval	Set the Network Operations Center (NOC) statistics update interval. This is the interval at which statistical updates are sent by the RF Domain manager to its adopting controller (the NOC controller). Enter a value in the range 5–3600 seconds, or enter 0 to invoke auto mode where the update interval is automatically adjusted by the controller based on load information. The default setting is 0.

NTP

NTP manages time and/or network clock synchronization within the network. NTP is a client/server implementation. Controllers, service platforms, and access points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, a controller resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Use this procedure to add new Network Time Protocol (NTP) server resources, edit existing resources, or delete existing resources.

1. Choose from the following actions:
   - Select + to add a new NTP server. Proceed to the next step.
   - Select ✎ adjacent to an existing NTP server to edit server settings.
   - Select 🗑 adjacent to an existing NTP server to delete it.
2. Configure NTP server parameters as described in the following table.

Table 48: General Profile Configuration – NTP Server Parameters

Parameter	Description
Server IP/Hostname	Specify the NTP server’s IP address, or select the check box adjacent to the field and enter the server's hostname.
Key number	Select the number of the associated authentication peer key for the NTP resource. Specify a value in the range 1–65534. The default value is 1.
Key	Enter a key (maximum 64 characters) to be used when the **Autokey** setting is disabled (default). Select 👁 to expose the actual character string comprising the key.
Version	Specify a version for the NTP server. Choose a value in the range 0–4. The value ‘0’ (default) implies that the NTP server’s version is ignored.
Minimum Polling Interval	Select a minimum polling interval. Once set, the NTP server is polled no sooner than the defined interval. The minimum polling interval options are **`64`**, **`128`**, **`256`**, **`512`**, and **`1024`** (seconds).
Maximum Polling Interval	Select a maximum polling interval. Once set, the specified NTP server is polled no later than the defined interval. The maximum polling interval options are **`1024`**, **`2048`**, **`4096`**, and **`8192`** (seconds).
Preferred	Optional. Select Preferred to designate this NTP server as a preferred NTP resource. This setting is disabled by default.
Autokey	Optional. Select **Autokey** to enable automatic configuration of the authentication key for the NTP server. This setting is disabled by default. Note: If not enabled, use the **Key** parameter to configure an authentication key for the NTP server.

3. Select **Add** to create the NTP server resource.

> Note
> This action does save the NTP server resource and settings. It is saved only when you select **Save** in the General tab.

Related Links

View and Manage Profiles on page 116

Add a Profile on page 117

Adoption Configuration

You must be in the process of configuring a new device profile or editing an existing device profile to perform this procedure.

An access point (AP), a controller, or a service platform uses the adoption process to discover available APs 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 APs supported by the profile.

At adoption, an AP solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the AP uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly among available APs, 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.

Use this procedure to configure or edit Adoption settings for a device profile.

> Note
> If you want to override Adoption settings for a specific device, go to **Devices**, select the target device, then configure or edit settings as described in this procedure..

1. Go to **Profiles**, then select the target profile.

   The device profile dashboard opens, displaying the **General** tab.
2. Select the **Adoption** tab.

3. Under the **Controller** pane, configure the WLAN's controller Adoption parameters as described in Table 49.

Table 49: Device Profile Adoption Configuration - Controller Parameters

Parameter	Description
VLAN	Select **VLAN** to include a VLAN that the AP's associating controller can reach. Use the spinner controller to set a VLAN between 1 and 4,094.
Preferred Group	Set an optimal group for the AP’s adoption. The name of the preferred group cannot exceed 64 characters.

4. The **Host** pane lists configured hosts in tabular form. Choose from the following actions:
   - Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
   - Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
   - Select ⤓ to download the Host entries in csv format.
   - Select ▥ to choose the columns displayed in the table.
   - Select ⟳ to refresh the list.
   - From under the **Actions** column in the table choose from the following actions:
     - Select ✎ associated with an entry to modify it. Proceed to the next step.
     - Select 🗑 associated with an entry to delete it.
   - Select + to configure a new host. Proceed to the next step.
5. Configure or edit Host parameters as described in Table 50.

Table 50: Device Profile Adoption Configuration - Host Parameters

Parameter	Description
Host (IP Address)	Choose from the following options: • `Host (IP Address)` (default) — Enter the numerical IP address of the host. • `Host (Hostname)` — Select the check box and enter a hostname. A hostname cannot exceed 64 characters.
Pool	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.

Table 50: Device Profile Adoption Configuration - Host Parameters (continued)

Parameter	Description
IPSec GW (IP Address)	Choose from the following options: • **`IPSec GW (IP Address)`** (default) — Select the numerical IP address of the IPSec gateway. • **`IPSec GW (IP Address)`** — Select the check box and enter the administrator-defined hostname of the adopting controller resource. A hostname cannot exceed 64 characters.
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	Select this option to establish a secure controller link using a remote VPN client.
Force	Select this setting to create a forced link between an AP and adopting controller, even when not necessarily needed. This setting is not selected by default.

6. Select **Add** to create the host entry in the table.
7. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Profiles on page 115

Add a Profile on page 117

Configure General Profile Settings on page 118

Power Configuration on page 168

Profile Interface Configuration

A profile's device interface configuration can be refined to support separate physical Ethernet configurations both unique and specific to each type of wireless controllers and service platforms. Ports vary depending on platform, but controller or service platform models do have some of the same physical interfaces.

Controllers, service platforms and access points require their Virtual Interface be configured for layer 3 (IP) access or layer 3 service on a VLAN.

A Virtual Interface defines which IP address is associated with each VLAN ID the device is connected to. If the profile is configured to support an access point radio, additional options are available unique to the radio's capabilities.

A profile's interface configuration process consists of the following procedures:

- Configure a Virtual LAN on page 126
- Configure an Ethernet Port on page 133
- Manage Radio Settings on page 144
- Manage Bluetooth Configuration on page 157
- Manage PPPoE Configuration on page 161
- Manage Port Channels Configuration on page 163

VLAN Configuration

A Virtual Interface is required for layer 3 (IP) access to access points (APs) or controllers, or to provide layer 3 service on a VLAN. The Virtual Interface defines which IP address is associated with each connected VLAN ID. A Virtual Interface is created for the default VLAN (VLAN 1) to enable remote administration. A Virtual Interface is also used to map VLANs to IP address ranges. This mapping determines the destination networks for routing.

Manage VLANs

Go to **Profiles** <*select a target device profile*> **Interface** > **Virtual**.

The **Virtual** window includes:

- A list of configured Virtual Interfaces, if any exist.
- Tools that allow users to manage Virtual Interfaces.

View Configured Virtual Interfaces

The Virtual window displays a list of all configured Virtual Interfaces in tabular form. The total number of configured Virtual Interfaces is shown in parentheses.

Table 51 describes the type of information displayed under each column in the table.

Table 51: Interface Configuration - Virtual Interface List Column Headings

Column Heading	Description
Name	Displays the name of each listed Virtual Interface assigned when it was created.
Admin Status	A green checkmark defines the listed Virtual Interface configuration as active and enabled with its supported profile. A red "X" defines the Virtual Interface as currently disabled. The interface status can be modified when a new Virtual Interface is created or an existing one is modified.
VLAN	Displays the numerical VLAN ID associated with each listed interface.
IP Address	Defines whether DHCP was used to obtain the primary IP address used by the Virtual Interface configuration.
Description	Displays the description defined for the Virtual Interface when it was either initially created or edited.
Action	See Management Tools.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Virtual Interface entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an entry to modify it.
  - Select 🗑 associated with an entry to delete it.
- Select + to configure a new Virtual Interface.

Related Links

VLAN Basic Configuration on page 126

VLAN IPV6 Configuration on page 128

VLAN IPv4 Configuration on page 129

VLAN Security Configuration on page 130

VLAN Routing Configuration on page 130

Configure a Virtual LAN

Use this procedure to create, edit, or delete a Virtual LAN (VLAN).

1. Go to **Profiles** and select a target device profile.

   The Profiles dashboard opens.
2. Select the **Interface** tab.

   The Interface dashboard opens, displaying the Virtual tab.
3. Under the Virtual tab, choose from the following actions:
   - Select + to add a new VLAN. Proceed to the next step.
   - Under the **Actions** column in the table, choose from the following actions:
     - Select ✎ associated with a VLAN to edit it. Proceed to the next step.
     - Select 🗑 associated with a VLAN to delete it.
4. Configure settings under the Basic, IPv6, IPv4, Security, and Routing tabs.
5. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > Note
   > You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

   > Note
   > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

   > Note
   > If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

VLAN Basic Configuration on page 126
VLAN IPV6 Configuration on page 128
VLAN IPv4 Configuration on page 129
VLAN Security Configuration on page 130
VLAN Routing Configuration on page 130

VLAN Basic Configuration

Configure a VLAN's basic settings:

1. Select **Profiles** > **Profile Name** > **Interface** > **Virtual** > **Basic**.

   The **Basic** tab displays by default, whether a new virtual interface is being created or an existing one is being modified.

2. Define the following basic configurations:

Index	Use the VLAN ID spinner control to define a numeric VLAN ID from 1 to 4,094. This option is valid only for new virtual interface creation
Description	Provide or edit a description (up to 64 characters) for the virtual interface that helps differentiate it from others with similar configurations
Admin Status	Select **Admin Status** to define this interface's current status within the managed network
NAT	Network Address Translation (NAT). Options include: • **inside** - The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address • **outside** - Packets passing through the NAT on the way back to the managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the switch managed network • **<none>** - No NAT activity takes place. This is the default setting
MTU	Set the MTU value between 1,280 to 1,500

3. Set the following IPv6 configuration:

   The DHCPv6 (Dynamic Host Configuration Protocol for IPv6) provides a framework for passing configuration information.

Address Autoconfiguration	Select to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits
Stateless DHCPv6	Select **Stateless DHCPv6** to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is not selected by default

Request DHCPv6 Options	Select to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than locally
ICMPv6 Redirect	Select to define whether ICMPv6 redirect messages are sent. Redirect requests data packets be sent on an alternative route
Prefix Delegation	Specify a 32-character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface. Devices use prefixes to distinguish destinations that reside on-link from those reachable using a router

4. Use the slider control to allow **Router Advertisement** and configure the following settings:

   Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

Default Router	Select **Default Router** to consider routers unavailable on this interface for default router selection
MTU	Select **MTU** to not use the existing MTU setting for router advertisements on this virtual interface. If the value is set to zero, no MTU options are sent
Hop Count	Select **Hop Count** to not use the hop count advertisement setting for router advertisements on this virtual interface

5. Select **Save** to update virtual interface basic configuration settings.

NEW! *VLAN IPV6 Configuration*

A VLAN must exist to perform this procedure.

IPv6 is the latest revision of the Internet Protocol (IP), designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. 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.

Use this procedure to configure a VLAN to use IPv6 protocol.

1. Go to **Profiles** > **Profile Name** > **Interface** > **Virtual** > **IPv6**. Select a VLAN in the **Virtual** table.

2. Select the **IPV6** tab, and configure the parameters as described in Table 52.

Table 52: VLAN IPV6 Parameters

Parameter	Description
Address Autoconfiguration	When enabled, configured prefixes are used for IPv6 address generation. The autoconfiguration option is disabled by default.
Stateless DHCPV6	Configures stateless DHCPv6 client on this interface. When enabled, the device can request configuration information from the DHCPv6 server using stateless DHCPv6. This option is disabled by default.
Request DHCPV6 Options	Requests options from DHCPv6 server on this interface. This option is disabled by default.
ICMPV6 Redirect	Requests options from DHCPv6 server on this interface. This option is disabled by default.
Prefix Delegation	Configures prefix-delegation client on this interface. Enter the IPv6 general prefix name (32 character maximum) provided by the service provider. This option is disabled by default.

VLAN IPv4 Configuration

IPv4 is a connectionless protocol. It operates on a best effort delivery model that does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP).

Use this procedure to configure the VLAN IPv4 configuration.

1. Select **Profiles** > **Profile Name** > **Interface** > **Virtual** > **IPv4**.
2. Set the following network information for the IPv4 addresses:

Primary Address	Define the IP address for the VLAN associated virtual interface. Select **`DHCP`**, **`IP Address`**, **`ZEROCONF`**, or **`<none>`**
IP Address or Subnet Mask	Select **IP Address** in the primary address option to activate the field. Type the virtual interface IP address
Secondary Zeroconf	Select **Secondary Zeroconf** to provide a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device

DHCP Options	Select **DHCP Options** to allow DHCP to provide the IP address for the virtual interface
Secondary Address	Select **Add** to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable
DHCP Relay	Use **DHCP Relay** to set the DHCP relay server configuration used with the virtual interface
Respond to DHCP Relay	Select **Respond to DHCP Relay** to allow the onboard DHCP server to respond to relayed DHCP packets on this interface
Addresses	Select **Add** to configure additional IP Address for DHCP Relay

3. Select **Save** to update virtual interface IPv4 settings.

VLAN Security Configuration

Configure virtual interface security configuration.

1. Select **Profiles** > **Profile Name** > **Interface** > **Virtual** > **Security**.
2. For information on security firewall rules, refer to Ethernet Port Security Configuration on page 139.
3. Select **Save** to update virtual interface security settings.

VLAN Routing Configuration

Configure the VLAN routing settings.

1. Select **Profiles** > **Profile Name** > **Interface** > **Virtual** > **Routing**.
2. Configure the following OSFP settings:

Priority	Select **Priority** to set the OSPF priority used to select the network designated route. Use the spinner control to set the value from 0 to 255
Cost	Assign cost to set the cost of the OSPF interface. Use the spinner control to set the value from 1 to 65,535
Bandwidth	Set the OSPF bandwidth from 1 to 10,000,000 Kbps
Authentication Type	Use the drop-down list box to select the authentication type used to validate credentials within the OSPF dynamic route The available options are **`None`**, **`null`**, **`simple-password`**, and **`message-digest`**. The default value is **`None`**

3. Select **Add** at the bottom of the **MD5 Authentication** table to add the Key ID and Password used for an MD5 validation of authenticator credentials

Key ID	Set the unique OSPF message digest authentication key ID from 1 to 255
Password	Type the OSFP password The password value is displayed either as asterisks or in plain text (select 👁 to view text)

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

Ethernet Port Configuration

The location and quantity of Ethernet ports on a ExtremeWireless WiNG controller, service platform, or access point (AP) depends on the device model. Ethernet ports that are available for a given device model appear under the **Ethernet** tab. The port parameters have default settings, and may be customized using the procedures in this section.

Related Links

Manage Ethernet Ports on page 131

Manage Ethernet Ports

Go to **Profiles** *<select a target device profile>* **Interface** > **Ethernet**.

The Ethernet window includes:

- A list of available Ethernet ports.
- Tools that allow users to manage Ethernet ports.

View Available Ethernet Ports

The Ethernet window displays a list of all available Ethernet ports in tabular form. The total number of available ports is shown in parentheses.

Table 53 describes the type of information displayed under each column in the table.

Table 53: Interface Configuration - Ethernet Port Table Column Headings

Column Heading	Description
Name	Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on controller, service platform, or access point model.
Admin Status	Indicates the current port administrative status, as follows: • ✓ (default) — Port is currently activated and available for use. • ✗ — Port is currently deactivated and unavailable for use.

Table 53: Interface Configuration - Ethernet Port Table Column Headings (continued)

Column Heading	Description
Mode	Displays the profile's current switching mode, as follows: • **`Access`** — When selected, the listed port accepts packets only from the native VLAN. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN. • **`Trunk`** — When selected, the listed port allows packets from a list of VLANs that are added to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one native VLAN, which can be tagged or untagged.
Native VLAN	Lists the numerical VLAN ID (1–4,094) set 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 over which untagged traffic is directed when using a port in Trunk mode.
Native VLAN Tagged	Indicates whether the native VLAN is tagged, as follows: • ✓ (default) — Native VLAN is tagged. • ✗ — Native VLAN is untagged. 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. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
Allowed VLANs	Displays the VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the Mode has been set to Trunk.
Description	Displays an administrator-defined description for each listed device port.
Action	See Management Tools.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.

- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Ethernet port entries in csv format.
- Select ▮▮▮ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an port to modify it.
  - Select 🗑 associated with an port to delete it.

Related Links

Ethernet Port Basic Configuration on page 134
Ethernet Port Switching Configuration on page 135
Ethernet Port Aggregation Configuration on page 136
Ethernet Port Discovery Configuration on page 137
Ethernet Port Fabric Attach Configuration on page 138
Ethernet Port Security Configuration on page 139
Ethernet Port Spanning Tree Configuration on page 141

Configure an Ethernet Port

You must be in the process of configuring a new device profile or editing an existing profile to use this procedure.
Use this procedure to configure or edit Ethernet Port settings for a device profile.

1. Go to **Profiles** and select a target device profile.

   The Profiles dashboard opens.
2. Select the **Interface** tab.

   The Interface dashboard opens, displaying the Virtual tab.
3. Select the **Ethernet** tab.

   The Ethernet window opens, displaying a list of the Ethernet Ports available for the selected device profile.
4. Select an Ethernet port in the list.
5. Configure or edit settings as described in the procedures associated with the Basic, Port Switching, Aggregation, Discovery, Fabric Attach, Security, and Spanning Tree tabs.
6. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > **Note**
   > You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Ethernet Ports on page 131
Ethernet Port Basic Configuration on page 134
Ethernet Port Switching Configuration on page 135
Ethernet Port Aggregation Configuration on page 136
Ethernet Port Discovery Configuration on page 137
Ethernet Port Fabric Attach Configuration on page 138
Ethernet Port Security Configuration on page 139
Ethernet Port Spanning Tree Configuration on page 141

Ethernet Port Basic Configuration

Define a profile's Ethernet port basic configuration.

1. Select **Profiles** > **Interface** > **Ethernet** > **Ethernet name**.

   The **Basic** screen is displayed.
2. Set the following Ethernet port properties:

Description	Type a brief description for the port (64 characters maximum). The description should reflect the port's intended function to differentiate it from others with similar configurations or perhaps just the name of the physical port
Admin Status	Select **`Enabled`** to define this port as active to the controller profile it supports. Select **`Disabled`** to deactivate this physical port in the profile
Speed	Select the speed at which the port can receive and transmit the data. Select either **`10 Mbps`**, **`100 Mbps`**, **`1000 Mbps`**, **`2500 Mbps`**, or **`5000 Mbps`**. Select either of these options to establish a 10, 100, 1000, 2500, or 5000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Auto is selected. Select **`Automatic`** to activate the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. *Automatic* is the default setting

Duplex	Select either **`half`**, **`full`** or **`automatic`** as the duplex option. Select *Half* duplex to send data over the port, then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time. Select *Full* duplex to transmit data to and from the device port at the same time. Using Full duplex, the port can send data while receiving data as well. Select *Automatic* to dynamically duplex as port performance needs dictate. Automatic is the default setting
Port Channel	Use the spinner control to set a port channel between 1 and 4. This sets the channel group for the port
Encforce Captive Portal	Select a captive portal option to apply captive portal access permission rules to data transmitted over this specific Ethernet port. Select **None** to prevent access permission rules to be enforced. Select **Authentication Failure** to apply access permission rules only when user authentication fails. Select **Always** to enforce access permissions at all times. The default value is **None**

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

Ethernet Port Switching Configuration

Define a profile's Ethernet port switching configuration.

1. Select **Profiles**.

   The profile name list opens.
2. Select a profile from the existing list.
3. Select **Interface** > **Ethernet** > **Ethernet Name** > **Switching**.
4. Set the following Ethernet port switching properties:

Mode	Select either the **`Access`** or **`Trunk`**option to set the VLAN switching mode over the port. If Access is selected, the port accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the port allows packets from a list of VLANs you add to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default mode
Native VLAN	Use the spinner control to define a numerical **Native VLAN ID** between 1 to 4,094. 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 which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1

Native VLAN Tagged	Select to tag the native VLAN. WiNG managed devices support the IEEE 802.1Q specification 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. 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 deactivated by default
Allowed VLANs	Assign the list of allowed VLANs between 1 to 4,094

5. Select **Save** to update switching settings.

Ethernet Port Aggregation Configuration

Define a profile's Ethernet port aggregation configuration.

1. Select **Profiles**.

   The profile name list opens.
2. Select a profile from the existing list of profiles.
3. Select **Interface** > **Ethernet** > **Ethernet Name** > **Aggregation**.

4. Set the following aggregation properties to activate link aggregation on the selected GE port:

Port Channel	Set a port channel between 1 and 4
Port Mode	Set the port mode as **`Active`** or **`Passive`**. If setting the port as a LAG member, specify whether the port is an active or passive member within the group. An active member initiates and participates in LACP negotiations. It is the active port that always transmits LACPDU irrespective of the remote device's port mode. The passive port only responds to LACPDU received from its corresponding active port. At least one port within a LAG, on either of the two negotiating peers, should be in the active mode. LACP negotiations are not initiated if all LAG member ports are passive. Further, the peer-to-peer LACP negotiations are always initiated by the peer with the lower system-priority value
Port Priority	Set the selected Ethernet Port's priority value, within the LAG, from 1 to 65,535. The selected port's actual priority within the LAG is determined by the port-priority value specified here along with the port's number. Higher the value, lower is the priority. Use this option to manipulate a port's priority. For example, in a LAG having five physical ports, four active and one standby, manually increasing the standby port's priority ensures that if one of the active port fails, the standby port is included in the LAG during re-negotiation

5. Select **Save** to update port aggregation settings.

Ethernet Port Discovery Configuration

Activate or deactivate the **CDP/LLDP** parameters used to configure *Cisco Discovery Protocol* and *Link Layer Discovery Protocol* for this profile's Ethernet port configuration:

1. Select **Profiles**.

   The profile name list opens.
2. Select a profile from the existing list of profiles.
3. Select **Interface** > **Ethernet** > **Ethernet Name** > **Discovery**.
4. Set the following discovery protocol parameters:

CDP Receive	Select **Receive** to allow the Cisco discovery Protocol to be received on this port. If selected, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is selected by default
CDP Transmit	Select **Transmit** to allow the Cisco discovery Protocol to be transmitted on this port. If selected, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors

LLDP Receive	Select **Receive** to allow the Link Layer Discovery Protocol to be received on this port. If selected, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is selected by default
LLDP Transmit	Select **Transmit** to allow the Link Layer Discovery Protocol to be transmitted on this port. If selected, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors

5. Select **Save** to update discovery protocol settings.

Ethernet Port Fabric Attach Configuration

Fabric Attach parameters allows ExtremeWireless WiNG devices (access points and controllers) to work as FA *(Fabric Attach)* clients.

1. Select **Profiles**.

   The profile name list opens.
2. Select a profile from the existing list.
3. Select **Interface** > **Ethernet** > **Ethernet name** > **Fabric Attach**.
4. Select **Add** to configure fabric attach parameters:

VLAN	Set the VLAN from 1 to 4,094
ISID	Use the ISID field to specify the ISID from 1 - 16,777,214. This is the *Individual Service Identifier* (ISID) associated with the VLAN interface specified above. Configuring a VLAN to ISID assignment, enables FA client operation on the selected Ethernet port. The FA Client requests acceptance of the VLAN to ISID mapping from the FAS within the *Fabric Connect* (FC) network. Once acceptance is achieved, the FC edge switch applies the ISID to the VLAN traffic from the device (AP or controller), and uses this ISID inside the Fabric. Note: A maximum of 94 pairs of ISID to VLAN mappings can be configured per Ethernet port.

   FA-enabled switches, in the FC network, send out LLDP messages with TLV extensions of Organization-specific TLV with OUI, to discover FA clients and advertise capabilities.

   The FA-enabled client associates with the *FA Server* (FAS), and obtains provisioning information (management VLAN interface details, and whether the interface is tagged or not) that allows the client to be configured with parameters that allow traffic to flow through the Fabric to the WLAN controller. Use this option to configure the ISID to VLAN mapping that the FA Client uses to negotiate with the FAS.

   You can configure FA Client capability on a device’s profile as well as device contexts.
5. Select **Save** to update fabric attach settings.

Ethernet Port Security Configuration

Edit or override the security configuration of a port.

1. Select **Profiles**.

   The profile name list opens.
2. Select a profile from the existing list.
3. Select **Interface** > **Ethernet** > **Ethernet name** > **Security**.
4. Configure the following **Access Control** settings:

Inbound IPv4 Firewall Rules	Use the IPv4 Inbound Firewall Rules drop-down list box to select the IPv4 specific firewall rules to apply to this profile's Ethernet port configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery, unlike TCP. IPv4 hosts can use link local addressing to provide local connectivity
Inbound MAC Firewall Rules	Use the MAC Inbound Firewall Rules drop-down lis box to select the firewall rules to apply to this profile's Ethernet port configuration. The firewall inspects MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances
Inbound IPv6 Firewall Rules	Use the IPv6 Inbound Firewall Rules drop-down list box to select the IPv6 specific firewall rules to apply to this profile's Ethernet port configuration. IPv6 is the latest revision of the Internet Protocol designed to replace IPv4. IPv6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons

5. Refer to the following options to configure **Trust** settings:

ARP Responses	Select **ARP Responses** to activate trust on this port. ARP packets received on this port are considered trusted, and the information from these packets is used to identify rogue devices within the network
DHCP Responses	Select **DHCP Responses** to only allow DHCP responses that are trusted and forwarded on this port. This option allows a DHCP server to connect only to a DHCP trusted port
802.1P COS	Select to activate 802.1P COS on this port

IP DSCP	Select to activate IP DSCP values on this port
ARP Header Mismatch Validation	Select **ARP Header Mismatch Validation** to activate mismatch check for the source MAC in both the ARP and Ethernet header

6. Set the following **IPv6 Trust** settings:

ND Requests	Select **ND Requests** to activate the trust of neighbor discovery requests required on an IPv6 network on this Ethernet port
DHCPv6 Responses	Select **DHCPv6 Responses** to trust all DHCPv6 responses on this Ethernet port. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, or other configuration attributes required on an IPv6 network
RA Guard	Select **RA Guard** to activate router advertisements or ICMPv6 redirects from this Ethernet port
ND Header Mismatch Validation	Select **ND Header Mismatch Validation** to activate a mismatch check for the source MAC within the ND header and Link Layer Option

7. Use the **802.1X Supplicant** slider to activate 802.1X settings. When selected, configure the following settings:

Method	Select **username** or **trustpoint**. • **username** - Authenticates supplicants using credentials they provide. Selecting this option activates the **Username** and **Password** fields • **trustpoint** - Authenticates supplicants using EAP-TLS mode of authentication. Selecting this option activates the **Trustpoint** field
Username	Specify the supplicant's username. **Note:** Username is required only if the **Method** of authentication is set to **username**

Password	Set the password associated with the sipplicant username
Trustpoint	Assign a trustpoint name when the selected **Method** of authentication is **trustpoint**. A trustpoint represents a CA or identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate Note: : Ensure that the trustpoint certificate is installed on the supplicant and the RADIUS server

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

Ethernet Port Spanning Tree Configuration

Spanning Tree Protocol (STP) (IEEE 802.1D standard) configures a meshed network for robustness by eliminating loops within the network and calculating and storing alternate paths to provide fault tolerance.

As the port comes up and STP calculation takes place, the port is set to **Blocked** state. In this state, no traffic can pass through the port. Since STP calculations take up to a minute to complete, the port is not operational thereby effecting the network behind the port. When the STP calculation is complete, the port's state is changed to **Forwarding** and traffic is allowed.

Multiple Spanning Tree Protocol (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTOP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there is only one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

An MSTP supported deployment uses multiple MST regions with multiple MST instances (MSTIs). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST). MSTP includes all of its spanning tree information in a single Bridge Protocol Data Unit (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP.

MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI message conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the access point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

To configure spanning tree settings for the selected Ethernet port:

1. Select **Profiles**.

   The profile name list opens.
2. Select a profile from the existing list.
3. Select **Interface** > **Ethernet** > **Ethernet name** > **Spanning Tree**.
4. Select the **Portfast** slider to configure portfast settings:

BPDU Filter	BPDUs are messages that are exchanged when controllers gather information about the network topology. Use the drop-down list box to invoke BPDU filter settings When activated, Portfast enabled ports do not transmit BPDU messages. When this value is set to **Default**, the BPDU Filter value is set to the bridge's BPDU filter value
BPDU Guard	Use the drop-down list box to invoke BPDU guard for this portfast enabled port. When selected, Portfast enabled ports are forced to shut down when they receive BPDU messages. When this value is set to **Default**, the Portfast BPDU Guard value is set to the bridge's BPDU guard value

5. Configure the following MSTP settings:

Link Type	Select **Point-to-Point** or **Shared** • **Point-to-Point** - Port is treated as connected to a point-to-point link An example of a **Point-to-Point** connection is a port that is connected to a controller or service platform • **Shared** - Port is shared between multiple devices An example of a **Shared** connection is a port that is connected to a hub
Cisco Interoperability	**Enable** or **Disable** interoperability with Cisco’s version of MSTP over the port. Cisco's version of MSTP is incompatible with standard MSTP

Force Protocol Version	Select **STP** to use the standard Spanning Tree Protocol Select **RSTP** to use Rapid Spanning Tree Protocol Select **MSTP** to use Multiple Spanning Tree Protocol Select **Not Supported** to deactivate spanning tree protocol for this interface **MSTP** is the default setting
Guard	Select **Root** radio to ensure that the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior BPDUs on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position Select **None** to deactivate this feature

6. Select **Add** to create a new **Port Cost** and configure the following settings:

Instance Index	Set a value between 0 to 15
Cost	This is the cost for a packet to traverse the current network segment. The cost of a path is the sum of all costs of traversal from the source to the destination. The default rule for the cost of a network segment is, the faster the media, the lower the cost Set a cost between 1 to 200000000 Note: The default path cost depends on the user-defined speed of the port. The cost helps determine the role of the port in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost

Select 🗑 to delete a port cost.

7. Select **Add** to create a new **Port Priority** and configure the following settings:

Instance Index	Set a value between 0 to 15
Priority	Set a value between 0 to 240 This is the priority for this port becoming a designated root. The default rule is, the lower this value, the higher the chance that the port is assigned as a designated root

Select 🗑 to delete a port priority.

8. Click **Save** to update the changes and overrides made to the Ethernet port's Spanning Tree configuration.

Configure a Radio Profile

Configure access point (AP) radio settings at the profile level for the selected radio. You can override the profile settings for a specific device after the radios have associated with the network.

An access point's radio profile comprises the following settings:

- Radio Settings
- Advanced Radio Settings

Manage Radio Settings

Use the **Radio** dashboard to apply QoS, ACL, operational mode, WLAN attributes and sensor configuration settings to the radio.

To edit an access point's radio settings:

1. Select **Profiles** > **Profile Name** > **Interface** > **Radio** > **radio1, radio2, or radio3**.
2. Define the following radio configuration parameters from within the **Basic** settings:

Description	Provide or edit a description (1 to 64 characters in length) for the radio that helps differentiate it from others with similar configurations.
Admin Status	Select **Enable** to define this radio as active to the profile it supports. Select **Disable** to deactivate this radio configuration within the profile. It can be activated at any future time when needed.
RF Mode	You can configure the radio to provide WLAN service for 2.4 GHz, 5 GHz, and 6 GHz enabled clients. You can also set the radio to provide sensor support, scan-ahead support, or function as a client bridge. Set the mode to either **`2.4GHz-wlan`** or **`5GHz-wlan`** or **`6GHz-wlan`**, depending on the radio's intended client support requirement. Set the mode to **`sensor`** if using the radio for rogue device detection. To set a radio as a detector, deactivate sensor mode on the other access point radio. Set the mode to **`bridge`** if the radio functions as a client bridge.
Lock RF Mode	Select **Lock RF Mode** to lock Smart RF for this radio.
LDPC	Select this option to activate low-density parity-check for the selected radio.

RIFS Mode	Set the RIFS mode for the selected radio. Options are: • Transmit Only • Receive Only (default) • Transmit and Receive • None
Radio Placement	Use the drop-down list box to specify whether the radio is located `Indoors` or `Outdoors`. The placement should depend on the country of operation and its regulatory domain requirements for radio emissions.
Channel	Use the drop-down list box to select the channel of operation for the radio. Only a trained installation professional should define the radio channel. Select `Smart` for the radio to scan non-overlapping channels listening for beacons from other access points. After channels are scanned, the radio selects the channel with the fewest access points. In the case of multiple access points on the same channel, it selects the channel with the lowest average power level. The default value is Smart. Channels with a "w" appended to them are unique to the 40 MHz band. Channels with a "ww" appended to them are 802.11ac specific, and are unique to the 80 MHz band.
Fallback Channel	Use the drop-down list box to select a fallback channel if the main channel doesn't work.
Transmit Power	Select **Smart** to automate the transmit power for the radio. Select **Transmit Power** and assign a value between 1 to 30 dBm.
Client Power	Select **Client Power** and assign a value between 1 to 20 dBm.
Max Clients	Use the spinner control or type a maximum permissible number of clients to connect with this radio. Enter a value in the range 1–512 clients. The default value is 512.
Dynamic Chain Selection	Select this option for the radio to dynamically change the number of transmit chains.
Rate Selection Method	Specify a radio selection method for the radio. The selection methods are: `Standard`: standard monotonic radio selection method is used. `Opportunistic`: sets opportunistic radio link adaptation as the radio selection method. This mode uses opportunistic data rate selection to provide the best throughput.
Radio QoS Policy	Use the drop-down list box to specify an existing QoS policy to apply to the access point radio with respect to its intended radio traffic.

Association ACL	Use the drop-down list box to specify an existing Association ACL policy to apply to the access point radio. An Association ACL is a policy-based ACL that either prevents or allows wireless clients from connecting to an access point radio. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, its compared against applied ACLs to verify the packet has the required permissions to be forwarded. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped.
Data Rates	Once the radio band is provided, the **Data Rates** drop-down list box populates with rate options depending on the 2.4, 5.0, or 6 GHz band selected. Note: If the radio band is set to Sensor or Bridge, the Data Rates drop-down list box is not activated, as the rates are fixed and not user configurable. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5 or 6 GHz is selected as the radio band, select separate 802.11a and 802.11n/ac rates then define how they are used together. When using 802.11n (in either the 2.4, 5 or 6 GHz band), set a *modulation and coding scheme* (MCS) with respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). If dedicating the radio to either 2.4, 5, or 6 GHz support, a Custom Rates option is available to set an MCS with respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). If Basic is selected within the 802.11n Rates field, the MCS0-7 option is auto selected as a Supported rate and that option is grayed out. If Basic is not selected, any combination of MCS0-7, MCS8-15 and MCS16-23 can be supported, including a case where MCS0-7 and MCS16-23 are selected and not MCS8-15. The MCS0-7 and MCS8-15 options are available to each support access point.
Adaptivity Recovery	Select this option to switch channels when an access point’s radio is in adaptivity mode. In adaptivity mode, an access point monitors interference on its set channel and stops functioning when the radio’s defined interference tolerance level is exceeded. When the defined adaptivity timeout is exceeded, the radio resumes functionality on a different channel. This option is enabled by default.
Adaptivity Timeout	Set the adaptivity timeout from 30 to 3,600 minutes. The default setting is 90 minutes.

DFS Revert Home	Select this option to enable a radio to return to its original channel. DFS (Dynamic Frequency Selection) prevents a radio from operating in a channel where radar signals are present. When radar signals are detected in a channel, the radio changes its channel of operation to another channel. The radio cannot use the channel it has moved from for the next 30 minutes. When DFS Revert Home is selected, the radio can return back to its original channel of operation when the 30-minute period is over. When not selected, the radio cannot return back to its original channel of operation ever after the mandatory 30-minute evacuation period is over.
DFS Duration	Set the DFS duration between 30 and 3,600 minutes. This is the duration for which the radio stays in the new channel. The default value is 90 minutes.
802.11AX	Use the slider button to enable or disable 802.11ax mode functionality for the AP. 802.11ax support is enabled by default.
BSS Color	Configures support for 802.11ax BSS coloring and assign the BSS color associated with the radio. BSS coloring is a means by which 802.11ax radios differentiate between overlapping *Basic Service Sets* (BSSs) in multi-path channels. A BSS represents a set of communicating devices consisting of one AP radio and one or more client stations. In an 802.11ax enabled wireless network, each BSS is identified by a numerical identifier (the BSS color) added to the header of the PHY frame. BSS coloring impacts channel access behavior and spatial reuse operation. Based on the BSS color detected, APs can assign new channel access behavior. Spatial reuse, is another advantage of enabling BSS color. It applies adaptive *Clear Channel Assessment* (CCA) thresholds for detected *Overlapping BSS* (OBSS) frame transmissions, enabling APs to ignore transmissions from an OBSS and transmit at the same time. BSS color support is disabled by default.
TWT	Enables 11ax *Target Wake Time* (TWT) support on the radio. The IEEE 802.11ax standard defines power saving enhancements and improved resource scheduling features, such as scheduled sleep and wake times. TWT allows devices, APs and stations, to negotiate when and how frequently they will wake up to send or receive data. TWT increases device sleep time, thereby substantially improving the client device's battery life. TWT is enabled by default.

OFDMA	Enables support for *Orthogonal frequency-division multiple access* (OFDMA) in both directions or in one direction. 802.11ax APs use OFDMA technology to partition a channel into smaller sub-channels called *resource units* (RUs) allowing multiple users, with varying bandwidth needs, to be served simultaneously. OFDMA is ideal for low bandwidth applications and results in better frequency reuse, reduced latency, and increased efficiency. When enabled, the AP mandates the RU allocation for multiple clients for *downlink* (dl) and *uplink* (ul) OFDMA. A series of trigger frames are exchanged to allow multi-user transmission in the downlink and uplink directions. **Note:** Specify a Guard Interval to avoid overlapping of OFDMA symbols. OFDMA support is enabled for both directions by default.
MU-MIMO	Select this option to enable multi-user multiple input multiple output (MU-MIMO) for the radio. When enabled, multiple users are able to simultaneously access the same channel using the spatial degrees of freedom offered by MIMO. OFDMA is disabled by default.
PSC	Select this option to enable PSC channels-only mode for the radio. PSC is disabled by default.
FILS	Select this option to enable 6 GHz Discovery Method FILS for the radio. FILS is disabled by default.
MBSSID	Select this option to enable Multiple Basic Service Set ID (MBSSID) capability for the radio. MBSSID is disabled by default.
RNR	Select this option to enable 6 GHz Discovery Methods for the radio. RNR is disabled by default.
UMUSCHEDBRCMONLY	Do not select this option. It is used only for debugging purposes.

3. Set the following profile **WLAN Properties** for the selected access point radio:

Beacon Interval	Set the interval between radio beacons in milliseconds (either 50, 100, or 200). A beacon is a packet broadcast by adopted radios to keep the network synchronized. The beacon includes the WLAN service area, radio address, broadcast destination addresses, time stamp and indicators about traffic and delivery such as a DTIM. Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default value is 100 milliseconds.
Guard Interval	Use the drop-down list box to specify **`Any`**, **`Base`**, **`Double`**, **`Long`**, or **`Quadruple`** guard interval. The guard interval is the space between the packets being transmitted. The guard interval is there to eliminate *inter-symbol interference* (ISI). ISI occurs when echoes or reflections from one transmission interfere with another. Adding time between transmissions allows echo's and reflections to settle before the next packet is transmitted. A shorter guard interval results in a shorter times which reduces overhead and increases data rates by up to 10%.The default value is Long.
RTS Threshold	Specify a *Request To Send* (RTS) threshold (between 1 to 65,536 bytes) for use by the WLAN's adopted access point radios. RTS is a transmitting station's signal that requests a *Clear To Send* (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path. Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold. Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold. A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.

Probe Response Rate	Use the drop-down list box to specify the data transmission rate used for the transmission of probe responses. Options include, **`highest-basic`**, **`lowest-basic`** and **`follow-probe-request`** (default setting).
Probe Response Retry	Select **Probe Response Retry** to retry probe responses if they are not acknowledged by the target wireless client.
Short Preamble	If using an 802.11bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink or Polycomm phones) require long preambles.
DTIM Interval BSSID	Set a DTIM Interval to specify a period for *Delivery Traffic Indication Messages* (DTIM). A DTIM is periodically included in a beacon frame transmitted from adopted radios. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates broadcast and multicast frames (buffered at the access point) are soon to arrive. These are simple data frames that require no acknowledgment, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive.
DTIM Interval - All BSSIDS	Select **Use Same DTIM Interval for All BSSIDS** to apply the same DTIM period setting to all defined BSSIDs

4. Set the following **WLAN/BSS MAPPINGS** configuration:

   Select **Add** to create a new WLAN/BSS Mapping for the selected radio.

BSSID	The BSSID is automatically assigned to the radio
Wireless	Select a WLAN from the drop-down list box

5. Set the following **Bridge** configuration:

> Note
> Set the radio's **RF Mode** to **`bridge`** before configuring these settings.

Bridge SSID	Set the infrastructure WLAN's BSSID, with which the client-bridge access point associates.
Bridge Encryption Type	Set the packet encryption mode. The encryption mode specified here should be the same as that configured on the infrastructure WLAN. The options are **`None`**, **`CCMP`**, and **`TKIP`**. The default setting is *None*. For information on WLAN encryption, see Wireless Network Security Configuration.
Channel Dwell Time	Set the channel-dwell time from 50 to 2000 milliseconds. This is the time the client-bridge radio dwells on each channel (configured in the list of channels) when scanning for an infrastructure WLAN. The default is 150 milliseconds.

Link Loss Shutdown Radio	Select this option to enable shutting down of the non-client bridge radio (this is the radio to which wireless clients associate) when the link between the client-bridge and infrastructure access points is lost. When enabled, wireless clients associated with the non-client bridge radio are pushed to search for and associate with other access points having backhaul connectivity. This option is disabled by default. If you enable this option, specify the time for which the non-client bridge radio is shut down. Use the spinner to specify a time from 1 - 1,800 seconds.
Bridge Inactivity Timeout	Set the inactivity timeout for each bridge MAC address from 0 to 864,000 seconds. This is the time for which the client-bridge access point waits before deleting a wired/ wireless client's MAC address from which a frame has not been received for more than the time specified here. For example, if the inactivity time is set at 120 seconds, and if no frames are received from a client (MAC address) for 120 seconds, it is deleted. The default value is 600 seconds.
Max Clients	Set the maximum number of client-bridge access points that can associate with the infrastructure WLAN. Specify a value from 1 to 64. The default value is 64.
Connect through Bridge	Select this option to enable the client-bridge access point radio to associate with the infrastructure WLAN through another client-bridge radio thereby forming a chain. This is referred to as daisy chaining of client-bridge radios. This option is disabled by default.
Link Up Refresh	Select this option to enable the *Switch Virtual Interface* (SVI) to refresh on re-establishing client bridge link to the infrastructure access point. If you are using a DHCP assigned IP address, this option also causes a DHCP renew. This option is enabled by default.
Protected Management Frames	Select this option to enable protected management frames between the client and its associated access point radio.
Roam Criteria Missed Beacons	Set this interval from 0 to 60 seconds. This is the time for which the client-bridge access point waits, after missing a beacon from the associated infrastructure WLAN access point, before roaming to another infrastructure access point. For example, if **Missed Beacon** is set to 30 seconds, and if more than 30 seconds have passed since the last beacon received from the infrastructure access point, the client-bridge access point resumes scanning for another infrastructure access point. The default value is 20 seconds.
Roam Criteria RSSI Threshold	Set the minimum signal-strength threshold for signals received from the infrastructure access point. Specify a value from -128 to -40 dBm. If the *Received Signal Strength Indicator* (RSSI) value of signals received from the infrastructure access point falls below the value specified here, the client-bridge access point resumes scanning for another infrastructure access point. The default is -75 dBm.

Keep Alive Type	Set the keep alive frame type exchanged between the client-bridge and infrastructure access points. This is the type of packets exchanged between the client-bridge and infrastructure access points, at specified intervals, to keep the client-bridge link up and active. The options are **null-data** and **WNMP** packets. The default value is **null-data**.
Keep Alive Interval	Set the keep alive interval from 0 to 86,400 seconds. This is the interval between two successive keep alive frames exchanged between the client-bridge and infrastructure access points. The default value is 300 seconds.
Bridge Authentication	Set the mode of authentication with the infrastructure WLAN. The authentication mode specified here should be the same as that configured on the infrastructure WLAN. The options are **None** and **EAP**. If you select **EAP**, specify the EAP authentication parameters. The default setting is *None*. For information on WLAN authentication, see Wireless Network Security Configuration.
Channels 2.4 GHz	Use the drop-down list to define a list of channels for scanning across all the channels in the 2.4 GHz radio band.
Channels 5 GHz	Use the drop-down list to define a list of channels for scanning across all the channels in the 5 GHz radio band.
Channels 6 GHz	Use the drop-down list to define a list of channels for scanning across all the channels in the 6 GHz radio band.

6. Configure the following **MCX** settings:

Mesh	Set the mesh mode for this radio – either **Client**, **Portal**, or **Disabled**. Select *Client* to scan for mesh portals, or nodes that have connection to portals, and connect through them. The *Portal* operation begins beaconing immediately and accepts connections from other mesh supported nodes. In general, the portal is connected to the wired network. The default value is Disabled.
Mesh Links	Specify the number of mesh links (1 -6) an access point radio will attempt to create. The default setting is 6 links.
Mesh PSK	Use the field to define the shared key for mesh. From the drop-down, select the type of the key: **ASCII** or **HEX**. Click the **View** icon 👁 to display the characters used in the key.
Preferred Peer Devices	Select **Add** to configure a preferred peer device for connection in a mesh network. For each peer being added, enter its MAC address and a priority from 1 - 6. Priority for mesh connection is given to the device that has the lowest number assigned.
Mesh Mappings	Select **Add** to create a mesh point mapping assignments to available BSSIDs for an existing access point deployment. The BSSID is automatically assigned when creating a new MCX mesh mapping.

7. Set the following **Antenna** configuration:

Gain	Set the antenna between 0.0 to 14.5 dBi. The access point's Power *Management Antenna Configuration File* (PMACF) automatically configures the access point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer must set the antenna gain. The default value is 0
Mode	Set the number of transmit and receive antennas on the access point. 1×1 is used for transmissions over just the single "A" antenna, 1×3 is used for transmissions over the "A" antenna and all three antennas for receiving. 2×2 is used for transmissions and receipts over two antennas for dual antenna models. 3×3×3 is used for transmissions and receipts over three antennas models. The default setting is dynamic based on the access point model deployed and its transmit power settings
Diversity	Select to activate antenna diversity on supported antennas. Antenna diversity uses two or more antennas to increase signal quality and strength

8. Set the following **Aggregation** properties:

A-MSDU Modes	Use the drop-down list box to define the A-MSDU mode supported. Options include: • **ux-rx** • **tx-rx**
A-MPDU Modes	Use the drop-down list box to define the A-MPDU mode supported. Options include **`Transmit Only`**, **`Receive Only`**, **`Transmit and Receive`** and **`None`**. The default value is Transmit and Receive. Using the default value, long frames can be both sent and received (up to 64 KB). When enabled, define either a transmit or receive limit or both

Receive A-MPDU Frame Size Limit	If the A-MPDU mode is set to *Receive Only* or *Transmit and Receive*, use this option to define an advertised maximum limit for received A-MPDU aggregated frame size. The options include: • **`8191`** - Advertises the maximum received frame size limit as 8191 bytes. • **`16383`** - Advertises the maximum received frame size limit as 16383 bytes. • **`32767`** - Advertises the maximum received frame size limit as 32767 bytes. • **`65535`** - Advertises the maximum received frame size limit as 65535 bytes. • **`128000`** - Advertises the maximum received frame size limit as 128000 bytes. • **`256000`** - Advertises the maximum received frame size limit as 256000 bytes. • **`512000`** - Advertises the maximum received frame size limit as 512000 bytes. • **`1024000`** - Advertises the maximum received frame size limit as 1024000 bytes. • **`default`** - This option auto configures the maximum received frame size based on the platform and radio type. This is the default setting.

Minimum Gap Between A-MPDU Frames	Use the drop-down list box to define, in microseconds, the minimum gap between consecutive A-MPDU frames. The options include: • `0` – Configures the minimum gap as 0 microseconds • `1` – Configures the minimum gap as 1 microseconds • `2` – Configures the minimum gap as 2 microseconds • `4` – Configures the minimum gap as 4 microseconds • `8` – Configures the minimum gap as 8 microseconds • `16` – Configures the minimum gap as 16 microseconds • `auto` – Auto configures the minimum gap depending on the platform and radio type (default setting)
Transmit A-MPDU Frame Size Limit	If the A-MPDU mode is set to *Transmit Only* or *Transmit and Receive*, use the spinner control to set limit on transmitted A-MPDU aggregated frame size. The range depends on the AP type and the radio selected. For 802.11ac capable APs, the range is as follows: • `2000 - 65,535 bytes` - For radio 1, the range is 2000 - 65,535 bytes. The default value is 65,535 bytes. Note: The WiNG *AP7662* and *AP7632* access points are an exception to the above rule. For the AP7662 and AP7632 access point models, the radio 1 range is *2000 - 1,024,000 bytes*. And the default value is 1,024,000 bytes. • `2000 - 1,024,000 bytes` - For radio 2, the range is 2000 - 1,024,000 bytes. The default value is 1,024,000 bytes.

9. Set the following **Scanning** parameters:

Enable	Select **Enable** to scan across all channels using this radio. Channel scans use access point resources and can be time consuming, so only enable when your sure the radio can afford the bandwidth be directed towards to the channel scan and does not negatively impact client support.
2.4 GHz Channels	Define a list of channels for off channel scans using the 2.4 GHz access point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 2.4 GHz radio band.
5 GHz Channels	Define a list of channels for off channel scans using the 5 GHz access point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 5 GHz radio band.
6 GHz Channels	Define a list of channels for off channel scans using the 6 GHz access point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 6 GHz radio band.

Max Multicast	Set the maximum number from 0 to 100 of multicast or broadcast messages used to perform off channel scanning. The default setting is four
Scan Interval	Set the interval from 2 to 100 dtims off channel scans occur. The default setting is 20 dtims
Sniffer Redirect Host	Specify the IP address of the host to which captured off channel scan packets are redirected.

10. Set the following **Aeroscout** and **Ekahau** parameters:

Forwarding Host	Specify the Aeroscout engine's IP address. When specified, the AP forwards Aeroscout beacons directly to the Aeroscout locationing engine without proxying through the controller or RF Domain manager
Forwarding Port	Set the port on which the Aeroscout or Ekahau engine is reachable. The range is between 0 to 65,535
MAC Address to be Forwarded	Specify the MAC address

11. Select **Save** to update the radio interface changes.

Related Links

Manage Advanced Radio Settings on page 156

Manage Advanced Radio Settings

A radio's profile configuration is customizable to define how transmit and receive data frames are processed. A radio's sniffer redirect settings can be refined to adjust how captured packets are directed. Additionally, channel scanning settings can refined in respect to channel scanning requirements on either the 2.4, 5, or 6 GHz radio bands.

To set or edit the selected radio's advanced settings:

1. Select **Profiles** > **Profile Name** > **Interface** > **Radio** > **radio 1, radio 2, or radio 3** > **Advanced**.
2. Configure the following **Advanced** settings:

Prefer HT Clients	Select **Prefer HT Clients** option to prioritize clients with higher throughput (802.11n clients) over clients with slower throughput (802.11 a/ b/g) clients. Use the spinner control to set a weight between 1 and 10 for the higher throughput clients
Broadcast/Multicast Transmit Rate	Use the drop-down list box to define the data rate broadcast and multicast frames are transmitted. Seven different rates are available if the not using the same rate for each BSSID, each with a separate menu

Broadcast/Multicast Forwarding	Define whether client broadcast and multicast packets should always follow DTIM, or only follow DTIM when using Power Save Aware mode. The default setting is **follow-dtim**
Fair Airtime	Select **Fair Airtime** to provide equal client access to radio resources

3. Define the radio's captured packet **Sniffer** configuration:

Host for Redirected Packets	If packets are re-directed from a connected access point radio, define an IP address resource (additional host system) to capture the re-directed packets. This address is the numerical (non DNS) address of the host used to capture re-directed packets.
Channel	Use the drop-down list box to specify the specific channel used to capture re-directed packets. The default value is channel 1.

4. Select **Save** to update the advanced radio settings changes.

Manage Bluetooth Configuration

Create and define a profile's bluetooth configuration. The access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. Both *Bluetooth classic* and *Bluetooth low energy* (BLE) technology are supported.

WiNG model access points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The access point’s Bluetooth radio periodically sends non-connectable, undirected low-energy (LE) advertisement packets. These advertisement packets are short and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. However, portions of the advertising packet are customizable via the Bluetooth radio interface configuration context.

To define a Bluetooth radio interface configuration:

1. Select **Profiles** > **Profile Name** > **Interface** > **Bluetooth**.

   The **Bluetooth** dashboard displays the list of managed devices.
2. Select a bluetooth from the existing list and configure the following basic settings:

Description	Define a 64 character maximum description for the access point’s Bluetooth radio to differentiate this radio interface from other Bluetooth supported radio’s that might be members of the same RF Domain
Admin Status	Select **Enabled** or **Disabled** to activate or deactivate support for Bluetooth beacon transmission on the selected access point

Radio Mode	Use the drop-down list box to configure the access point's Bluetooth radio functional mode. The options include: • **bt-sensor** - Select this option to activate the radio as a bt-sensor. BT sensors are Bluetooth classic sensors providing robust wireless connections for legacy devices. Typically, these connections are not ideally suited for the newer BLE (Bluetooth low energy) technology supported devices. This is the default setting • **le-beacon** - Select this option to provide Bluetooth support for newer BLE technology supported devices. Le-beacons are newer Bluetooth low energy beacons ideal for applications requiring intermittent or periodic transfers of small amounts of data. Le-beacons are not designed as replacements for classic beacon sensors • **le-sensor** - Select this option to provide Bluetooth support for LE (low energy) asset tracking. When enabled, it uses the AP’s Bluetooth radio to detect BLE ‘asset tags’ within the managed network. This information is reported to a backend server. The interval at which the AP scans for asset tags is determined by the Sensor policy applied on the AP's self or in the AP's RF domain context • **le-dual** - Select this option to enable the AP to beacon and scan concurrently. As of now, WiNG APs can either perform beaconing or scanning operation. Starting with WiNG 7.3.1, APs can be configured to perform both operations concurrently. When not beaconing, the AP will switch to scanning In the le-dual mode, by default, APs beacon once in every 60 seconds and scan the rest of the time. When performing scanning, the radio senses other BLE devices and sends the information to a backend server. The backend server configuration is set in the AP's RF Domain context

Transmit Period	Use the spinner control to set the Bluetooth radio’s beacon transmission period from 100 to 10,000 milliseconds. As the defined period increases, so does the CPU processing time and the number packets incrementally transmitted (typically one per minute)
Transmit Pattern	Use the drop-down list box to set the beacon’s transmission pattern. The options include: • **eddystone-url1** or **eddystone-url2** - An eddystoneURL frame broadcasts a URL using a compressed encoding scheme to better fit within a limited advertisement packet. Once decoded, the URL can be used by a client for internet access • **ibeacon** - - iBeacon was created by Apple for use in iOS devices (beginning with iOS version 7.0). Apple has made three data fields available to iOS applications: a UUID for device identification, a major value for device class, and a minor value for more refined information like product category
Transmit Power	Use the spinner control to set the Bluetooth radio's le-beacon transmit power. This determines how far a beacon can transmit data. Set a value between -15 to 31 dBM.
Antenna	Select between **internal** or **external** antenna options

3. Set the following **eddystone** configuration:

Calibration Signal Strength	Set the Eddystone Beacon measured calibration signal strength, from -127 dBm to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters. The default setting is -19 dBm
Transmit URL1	Type a 64-character maximum Eddystone-URL1. The URL must be 17 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a web server
Transmit URL2	Type a 64-character maximum Eddystone-URL2. The URL must be 17 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a web server

4. Define the following iBeacon settings:

Calibration Signal Strength	Set the iBeacon measured calibration signal strength, from -127 dBm to 127 dBm, at 1 meter. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 1 meter. The default setting is -60 dBm
Major Number	Set the iBeacon major value from 0 to 65,535. Major values identify and distinguish groups. For example, each beacon on a specific floor in a building could be assigned a unique major value. The default value is 1,111

Minor Number	Set the iBeacon minor value from 0 to 65, 535. Minor values identify and distinguish individual beacons. Minor values help identify individual beacons within a group of beacons assigned a major value. The default setting is 2,222
UUID	Define a 32 hex character maximum Universally Unique IDentifier (UUID). The UUID classification contains 32 hexadecimal digits, split into 5 groups, separated by dashes – for example, `f2468da6-5fa8-2e84-1134-bc5b71e0893e`. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration

5. Select **Save** to update the Bluetooth configuration settings.

Manage PPPoE Configuration

PPP over Ethernet (PPPoE) is a data-link protocol for dialup connections. PPPoE allows an access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers are currently supporting (or deploying) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables controllers, service platforms and access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide a point-to-point connection, each PPPoE session determines the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the Wired WAN were to fail.

Note

Devices with PPPoE enabled continue to support VPN, NAT, PBR and 3G failover over the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.

When PPPoE client operation is enabled, a requesting client discovers an available server and establishes a PPPoE link for its traffic flow. When a wired WAN connection failure is detected, traffic flows through the WWAN interface in fail-over mode (if the WWAN network is configured and available). When the PPPoE link becomes accessible again, client traffic is redirected back through the access point's wired WAN link.

When the access point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

1. Select **Profiles**.

   The profile name list opens.
2. Select a profile from the existing list.
3. Select **Interface** > **PPPOE** > **PPPoE**.
4. Use the **Basic** settings to configure PPPoE client:

Admin Status	Select **Enabled** to support a high speed client mode point-to-point connection using the PPPoE protocol
Service	Type the 128 character maximum PPPoE client service name provided by the service provider
DSL Network VLAN	Use the spinner control to set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem. The available range is 1 to 4,094. The default VLAN is VLAN1
Client IP Address	Select this option to provide Client IP Address Provide the numerical (non hostname) IP address of the PPPoE client
Default Route Priority	Use the spinner control to set the default route priority between 1 and 8000

5. Define the following **Authentication** parameters for PPPoE client interoperation:

Username	Provide the 64 character maximum username used for authentication support by the PPPoE client
Password	Provide the 64 character maximum password used for authentication by the PPPoE client
Type	Use the drop-down list box to specify authentication type used by the PPPoE client, and whose credentials must be shared by its peer access point. Supported authentication options include *None, PAP, CHAP, MSCHAP*, and *MSCHAP-v2*

6. Define the following **Connection** settings for the PPPoE point-to-point connection with the PPPoE client:

Maximum Transmission Unit (MTU)	Set the PPPoE client maximum transmission unit (MTU) from 500 to 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492
Client Idle Timeout	Set a timeout in either between 1 and 65,535 seconds. The access point uses the defined timeout so it does not sit idle waiting for input from the PPPoE client and server that may never come. The default setting is 600 seconds
Keep Alive	Select **Keep Alive** option to ensure that the point-to-point connection to the PPPoE client is continuously maintained and not timed out

7. Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

   NAT converts an IP address in one network to a different IP address or set of IP addresses in another network. The access point maps its local (inside) network addresses to WAN (outside) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. The default setting is **None** (neither inside or outside).
8. Define the following **Security Settings** for the PPPoE configuration:

   Use the **Inbound IPv4 Firewall Rules** drop-down list box to define the security settings for the selected PPPoE.
9. Select **Save** to update PPPoE settings.

Manage Port Channels Configuration

Controller, service platform, and access point profiles can be applied customized port channel settings as part of their interface configuration.

1. Select **Profiles**.

   The profile name list opens.
2. Select a profile from the existing list.
3. Select **Interface** > **Port Channels**.

4. If there is a port channel already configured, review the existing settings and current status:

Name	Displays the port channel's numerical identifier assigned to it when it was created. The numerical name cannot be modified as part of the edit process
Type	Displays whether the type is port channel
Description	Lists a short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations
Admin Status	A green checkmark defines the listed port channel as active and currently activated with the profile. A red "X" defines the port channel as currently deactivated and not available for use. The interface status can be modified with the port channel configuration as required

Related Links

Port Channels Basic Configuration on page 164

Port Channels Switching Configuration on page 165

Port Channels Security Configuration on page 167

Port Channels Spanning Tree Configuration on page 167

Port Channels Basic Configuration

You can add a new port channel configuration or edit an existing configuration.

1. Select **Profiles** > **Profile Name** > **Interface** > **Port Channels**.
2. Select + to add a new port channel.

   The **Basic** dashboard opens.
3. Set the following port channel properties:

Index	Set an index value between 1 and 8
Admin Status	Use the drop-down list box to activate or deactivate the admin status for the selected port channel. Select **Enable** to define this port channel as active to the profile it supports. Select **Disable** to deactivate this port channel configuration within the profile. It can be activated at any future time when needed. The default setting is enabled
Description	Type a brief description for the port channel (64 characters maximum). The description should reflect the port channel's intended function

Speed	Select the speed at which the port channel can receive and transmit the data. Select either **10 Mbps**, **100 Mbps**, **1000 Mbps**, **2500 Mbps**, **5000 Mbps**, or **auto**. Select either of these options to establish a respective speed data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if **auto** is selected. Select **auto** to activate the port channel to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis
Duplex	Use the drop-down list box to select **Automatic**, **Half**, or **Full** as the duplex option. Select Half duplex to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted. Like a Full duplex transmission, a Half duplex transmission can carry data in both directions, just not at the same time. Select Full duplex to transmit data to and from the port channel at the same time. Using Full duplex, the port channel can send data while receiving data as well. Select Automatic to dynamically duplex as port channel performance needs dictate
Load Balance	Use the **Load Balance** drop-down list box to define whether port channel load balancing is conducted using a Source/ Destination IP (**src-dst-ip**) or a Source/ Destination MAC (**src-dst-mac**)

4. Select **Save** to update port channel basic settings.

Port Channels Switching Configuration

Define a port channel's switching configuration.

1. Select **Profiles** > **Profile Name** > **Interface** > **Port Channels** > **Switching**.

2. Define the following **Switching** parameters to apply to port channel configurations:

Mode	Use the **Mode** drop-down list box to select **Access** or **Trunk** mode to set the VLAN switching mode over the port channel • **Access** - The port channel accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN • **Trunk** - The port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged **Access** mode is the default setting
Native VLAN	Use the spinner control to define a numerical ID between 1 to 4,094. 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 which untagged traffic will be directed over when using trunk mode. The default value is 1

Native VLAN Tagged	Select **Native VLAN Tagged** to tag the native VLAN. WiNG managed devices support the IEEE 802.1Q specification 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. 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
Allows VLANs	Selecting **Trunk** as the mode activates the **Allows VLANs** parameter. Set VLANs between 1 and 4,094

3. Select **Save** to update port channel switching configuration.

Port Channels Security Configuration

Define a port channel's security configuration.

1. Select **Profiles** > **Profile Name** > **Interface** > **Port Channels** > **Security**.
2. Configure the **Access Control**, **Trust**, and **IPv6 Trust** settings.

   For more information on security settings, see Ethernet Port Security Configuration on page 139.
3. Select **Save** to update port channel security configuration.

Port Channels Spanning Tree Configuration

Define a port channel's spanning tree configuration.

1. Select **Profiles** > **Profile Name** > **Interface** > **Port Channels** > **Spanning Tree**.
2. Configure **Portfast**, **MSTP**, **Port Cost**, and **Port Priority** settings.

   For more information on spanning tree settings, see Ethernet Port Spanning Tree Configuration on page 141.
3. Select **Save** to update port channel spanning tree configuration.

Power Configuration

Note
This procedure applies to AP3000/X, AP5010, AP310i/e, AP410i/e, AP505i, AP510i, AP510e, AP560i, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8533.

An access point (AP) uses a complex programmable logic device (CPLD) to manage power. The CPLD determines proper supply sequencing, the maximum power available and other status information. One of the primary functions of the CPLD is to determine the maximum power budget. When an AP is powered on (or performing a cold reset), the CPLD determines the maximum power provided by the POE device and the budget available to the AP. The CPLD also determines the AP hardware SKU (model) and the number of radios.

If the access point’s POE resource cannot provide sufficient power to run the access point (with all intended interfaces enabled), some of the following interfaces could be disabled or modified:

- The access point’s transmit and receive algorithms could be negatively impacted.
- The access point’s transmit power could be reduced due to insufficient power.
- The access point’s WAN port configuration could be changed (either enabled or disabled).

APs that support IEEE 802.3af, 802.3at, or 802.3bt standards can be powered up with POE or through an external power source. If connected to a POE BT power source (51W) or external power source, the APs operate in high power mode with full performance. If connected to a POE AT power source (25.5W) or external power source, the APs operate in normal power mode with full performance. If connected to a POE AF power source (15.4 W), the APs operate in low power mode with limited performance.

Use this procedure to configure the transmit output power of access point (AP) radios.

1. Go to **Profiles** and select the target AP profile.
2. Select the **Power Config** tab.

3. Configure the Power Mode parameters as described in Table 54.

Table 54: Power Mode Parameters

Parameter	Description
Power Mode	The power mode options are: • **`Automatic`** — Using the Automatic setting, the access point automatically determines the best power configuration based on the available power budget. Automatic is the default setting. • **`8.02.3af`** — Low power mode. This allows the access point to assume 12.95 watts. • **`8.02.3at`** — Normal power mode • **`802.3bt`** — High power mode If you change the mode, you must reset the AP to implement the change.
802.3AF	Note: This setting is available only for ANYAP device profiles. Set the 802.3af power mode. Options include: • **`Throughput`** (default) — This mode provides lower power but has more transmission (tx) chains. Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/ multicast transmission performance. • **`Range`** — This mode provides higher power but fewer tx chains. Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates.

Table 54: Power Mode Parameters (continued)

Parameter	Description
802.3AT	Note: This setting is available only for ANYAP device profiles. Set the 802.3at power mode. Options include: • **`Throughput`** (default) — This mode provides lower power but has more tx chains. Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance. • **`Range`** — This mode provides higher power but fewer tx chains. Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates.
802.3BT	Note: This setting is available only for ANYAP device profiles. Set the 802.3bt power mode. Options include: • **`Throughput`** (default) — This mode provides lower power but has more tx chains. Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance. • **`Range`** — This mode provides higher power but fewer tx chains. Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates.

4. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Profiles on page 115
Add a Profile on page 117
Configure General Profile Settings on page 118
Adoption Configuration on page 121

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. Bridge 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 bridge VLAN 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 x N routes. Thus, for a network with nine routers, you'll need a minimum of 81 routes (9 x 9 = 81).

Related Links

DNS Configuration on page 171
ARP Configuration on page 172
L2TP V3 Configuration on page 173
GRE Tunnel Configuration on page 179
IGMP and MLD Snooping Configuration on page 184
Spanning Tree Configuration on page 188
Routing Configuration on page 193
Forwarding Database Configuration on page 195
Bridge VLAN Configuration on page 197
Alias Configuration on page 208

DNS Configuration

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.

1. Select a network from the network name list and navigate to **Network**.
2. Select **DNS**.

   The system displays the DNS dashboard.
3. 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

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

ARP Configuration

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.

1. Select a profile or device from the list.
2. Select **Network** > **ARP**.
3. Select **Add**.

   The ARP **Basic Configuration** dashboard opens.
4. 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

5. Select **Add** to save changes.

L2TP V3 Configuration

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.

1. Select a profile or device from the list.
2. Select **Network** > **L2TP V3**.

   The L2TP V3 **Basic Configuration** dashboard opens.
3. 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

Field	Description
Integer	Select **IP Address** from the **Router ID** drop-down to configure the IP address filed
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

4. 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

5. 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

Field	Description
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
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
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 kbytes
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
Psuedowire ID	Define a psuedowire ID for this session from 1 to 4,294,967,295. A pseudowire is an emulation of a layer 2 point-to-point connection over a PSN. A pseudowire 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.

Field	Description
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

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

GRE Tunnel Configuration

Generic Routing Encapsulation (GRE) offers direct, point-to-point communication between network nodes with support for one to three termination points. 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 (APs) map one or more VLANs to a tunnel. The remote endpoint is a user configured 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 APs can reach both the GRE peer as well as the RADIUS server using IPv4.

Note
You can override GRE profile settings for an individual device. Go to **Devices** <*select a device*> **Network** > **GRE**, and configure the parameters as described in this procedure.

Use this procedure to create, edit, or delete GRE tunnels for a device profile.

1. Go to **Profiles** <*select a device profile*> **Network** > **GRE**.
2. Choose from the following actions:
   - To add a new GRE tunnel, select +.
   - To edit an existing GRE tunnel, select ✎ associated with the target tunnel.
   - To delete a GRE tunnel, select 🗑 associated with the target tunnel.
3. Configure the GRE tunnel parameters as described in Table 55.

Table 55: GRE Tunnel Parameters

Parameter	Description
Basic	
Name	Enter a GRE tunnel name. The name cannot be edited.
Native VLAN	Set a numerical VLAN ID in the range 1–4,094 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
Tunneled VLANs	Identify the VLAN(s) that connected clients use to route GRE tunneled traffic within their respective WLANs. Enter a VLAN ID, then select **Add**. Select 🗑 associated with a configured VLAN ID to remove it from the list of Tunneled VLANs.
IPv4 MTU	Set an IPv4 tunnel’s maximum transmission unit (MTU) in the range 900 – 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

Table 55: GRE Tunnel Parameters (continued)

Parameter	Description
IPv6 MTU	Set an IPv6 tunnel's MTU in the range 1,236 – 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
Native VLAN Tagged	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. 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
DSCP Options	
DSCP Options	Use the slider to enable or disable Differentiated Services Code Point (DSCP) options. Select **Reflect**, or select the spinner control field and set the tunnel DSCP/802.1q priority value (1–63) from encapsulated packets to the outer packet IPv4 header.
Peer	
Add	Select **Add** to identify a new GRE peer. Select 🗑 associated with an existing GRE peer to remove it.
Peer Index	Assign a numeric index to each peer to help differentiate tunnel end points.
Peer IP Address	Identify the IP address of the added GRE peer to serve as a network address identifier.
Establishment Criteria	

Table 55: GRE Tunnel Parameters (continued)

Parameter	Description
Criteria	Select an establishment criteria from the criteria drop-down
VRRP Group	Virtual Router Redundancy Protocol (VRRP) provides IP abstraction to key functionality in support of load balancing and high-availability functions. Pick a group in the range 1–255.
Failover	
Failover (enable/ disable)	Use the slider to enable or disable the failover option to periodically ping the primary gateway to assess its availability for failover support.
Ping interval	Set the duration between two successive pings to the gateway. Define this value in seconds in the range 1–250 seconds.
Retries	Set the number of retry ping opportunities before the session is terminated in the range 1–10.

4. Select **Add** to add the GRE profile settings.
5. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

GRE Concentrator Configuration

The GRE Concentrator feature supports GRE tunneling between APs and ExtremeWireless WiNG controllers.

With this feature, an AP acts as GRE initiator and creates wireless client tunnels to an ExtremeWireless WiNG controller that is operating as a GRE concentrator tunnel terminator.

The maximum limits on GRE tunnel configuration for each platform are as follows:

Platform	Maximum GRE Tunnels Supported
NX5500	512
NX7500	1000
NX9610	1024
CX9000	Not suppported
VX9000	1024

To enable the GRE Concentrator feature, complete the following procedures in the order given:

1. Configure an ExtremeWireless WiNG controller to operate as a GRE Concentrator tunnel terminator. See Configure a GRE Concentrator Profile for a ExtremeWireless WiNG Controller on page 183.
2. Configure VLANs for an AP. See Interface Virtual Tab on page 74.

   Note
   GRE Concentrator can terminate GRE tunnels mapped to more than one VLAN. You must configure one Native VLAN that is capable of transmitting untagged (default) or tagged traffic. All other VLANs will transmit tagged traffic. Select the Native VLAN when you configure the GRE tunnel profile in the next step.

3. Configure the GRE peer-to-peer settings on the AP and try to reach the concentrator using the ping command. See GRE Tunnel Configuration on page 179.

You can view the GRE Concentrator connection information on the ExtremeWireless WiNG controller using the following CLI command:

```
show gre concentrator-tunnels
```

Configure a GRE Concentrator Profile for a ExtremeWireless WiNG Controller

Use this procedure to configure a network GRE Concentrator profile to apply to ExtremeWireless WiNG controllers.

Note
You can override the GRE Concentrator profile settings for individual controllers. Go to **Devices** <*select a controller*> **Network** > **GRE Concentrator**, and configure the parameters as described in this procedure.

1. Go to **Profiles** <*select a controller device profile*> **Network** > **GRE Concentrator**.

2. Configure the parameters as described in Table 56.

Table 56: GRE Concentrator Parameters

Parameter	Description
Name	Enter a name (up to 32 characters) for the GRE Concentrator.
Idle Timeout	Enter an Idle Timeout value in the range 120 – 3600.
Allowed VLANs	Enter the VLAN ID(s) of the VLAN(s) allowed to connect to the GRE Concentrator on this controller. One or more VLANs can be entered. Use a hyphen to enter a range of VLANs and comma delimeters to enter multiple individual VLANs (97-98,102,107). Note: One VLAN must be capable of transmitting tagged or untagged (default) packets.

3. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Next, configure VLANs. See Interface Virtual Tab on page 74.

Finally, configure GRE tunnels on APs. See GRE Tunnel Configuration on page 179.

IGMP and MLD Snooping Configuration

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.

1. Select an access point from the profile or device list.
2. Navigate to **Network** > **IGMP/MLD**.

   The **IGMP Snooping** dashboard opens.

3. 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
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 learned on it and only if present, then it is forwarded on that port

Field	Description
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
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

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

MLD Snooping Configuration

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.

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
Snopping	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
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

Field	Description
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.

Spanning Tree Configuration

Spanning Tree Protocol (STP) (IEEE 802.1D standard) configures a meshed network for robustness by eliminating loops within the network and calculating and storing alternate paths to provide fault tolerance.

As the port comes up and STP calculation takes place, the port is set to **`Blocked`** state. In this state, no traffic can pass through the port. Since STP calculations take up to a minute to complete, the port is not operational thereby effecting the network behind the port. When the STP calculation is complete, the port's state is changed to **`Forwarding`** and traffic is allowed.

Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w standard) is an evolution over the standard STP. The primary aim is to reduce the time taken to respond to topology changes while being backward compatible with STP. PortFast allows the port to bypass the listening and learning states, thereby rapidly changing the state of a port from Blocked to Forwarding. The port allows traffic while the STP calculation is in progress.

Multiple Spanning Tree Protocol (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTOP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there is only one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

An MSTP supported deployment uses multiple MST regions with multiple MST instances (MSTIs). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST). MSTP includes all of its spanning tree information in a single Bridge Protocol Data Unit (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP.

MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI message conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the access point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

Related Links

Configure a Spanning Tree Profile on page 189

Configure a Spanning Tree Profile

To add or edit a spanning tree profile:

1. Go to **Profiles** <*select a device profile*> **Network** > **Spanning Tree**.
2. Configure or modify the Spanning Tree profile parameters as described in Table 57.

Table 57: Spanning Tree Profile Parameters

Parameter	Description
MSTP	
MSTP Enable	Select to enable Multiple Spanning Tree Protocol.
Max Hop Count	Define the maximum number of hops for which the BPDU is valid. Set a value in the range 7 – 127. The default value is 20.
MSTP Config Name	Enter a name using 1 – 64 characters to represent the MST region.
MST Revision Level	Define a revision level value in the range 0 – 255 for configuration information purposes. The default value is 0.
Cisco MSTP Interoperability	Set to **Enable** to enforce interoperability with Cisco’s version of MSTP over the port. Cisco's version of MSTP is incompatible with standard MSTP. The default value is **Disable**.
Hello Time	Set a BPDU interval value in the range 1 – 10 (seconds). The default value is 2.
Forward Delay	Set the forwarding delay time to a value in the range 4 – 30 (seconds). The default value is 15.
Maximum Age	Set the maximum amount of time to listen for root bridge using a value in the range 6 – 40 (seconds). The default value is 20.
Portfast	
PortFast BPDU Filter	Select to enable a BPDU filter. MSTP BPDUs are messages that are exchanged when controllers gather information about the network topology. When enabled, PortFast enabled ports do not transmit BPDU messages. The default setting is disabled.

Table 57: Spanning Tree Profile Parameters (continued)

Parameter	Description
PortFast BPDU Guard	Select to enable BPDU guard. MSTP BPDUs are messages that are exchanged when controllers gather information about the network topology. When enabled, PortFast enabled ports are forced to shut down when they receive BPDU messages. The default setting is disabled.
Error Disable	
Enable Recovery	Select to enable error disable timeout due to BPDU guard.
Recovery Interval	Set the interval after which the port is to be enabled using a value in the range 10 – 1000000 (seconds). The default value is 300.
Spanning Tree Instance	
Instance	Set an instance index using a value in the range 0 – 15. The default value is 1.
Priority	Set a Bridge Priority in increments of 4096, using a value in the range 0 – 61440. This is the priority for this port becoming a designated root. The default rule is, the lower this value, the higher the chance that the port is assigned as a designated root. The default value is 32768.
Spanning Tree Instance VLANs	
Instance	Set an instance index using a value in the range 0 – 15. The default value is 1.
VLANs	Identify the VLANs to be associated with this instance. Valid values are in the range 0 – 4094. Enter multiple VLANs using comma delimiters.

3. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Profile Network Configuration on page 171

CDP/LLDP Configuration

Cisco Discovery Protocol

CDP (Cisco Discovery Protocol) is a proprietary Data Link Layer protocol implemented in Cisco networking equipment. It is primarily used to obtain IP addresses of neighboring devices and discover their platform information. CDP is also used to obtain information about the interfaces the access point uses. CDP runs only over the data link layer enabling two systems that support different network-layer protocols to learn about each other.

Link Layer Discovery Protocol

LLDP (Link Layer Discovery Protocol) provides a standard way for a controller or access point to advertise information about themselves to networked neighbors and store information they discover from their peers.

LLDP is neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about them to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management and connection endpoint information from adjacent devices.

Using LLDP, an access point is able to advertise its own identification, capabilities and media-specific configuration information and learn the same information from connected peer devices.

LLDP information is sent in an Ethernet frame at a fixed interval. Each frame contains one m LLDP PDU (Link Layer Discovery Protocol Data Unit). A single LLDP PDU is transmitted in a single 802.3 Ethernet frame.

Related Links

Configure a CDP/LLDP Profile on page 191

Configure a CDP/LLDP Profile

Use this procedure to configure Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) profile settings to be applied to the selected profile device type.

> **Note**
> You can override these settings for individual devices. Go to **Devices** <*select a device*> **Network** > **CDP/LLDP** and configure the parameters as described in this procedure.

To configure or modify CDP or LLDP parameter settings:

1. Go to **Profiles** <*select a device profile*> **Network** > **CDP/LLDP**.

2. Under the **Cisco Discovery Protocol (CDP)** pane, configure the parameters as described in Table 58.

Table 58: CDP Profile Parameters

Parameter	Description
Enable CDP	Select this option to enable CDP and allow for network address discovery of Cisco supported devices and operating system version. This option is enabled by default.
Hold Time	Set a hold time (in seconds) for the transmission of CDP packets. Set a value in the range 10 – 1,800. Note: The default setting is 1,800 seconds.
Timer	Set the interval for CDP packet transmissions in the range 5 – 900 seconds. Note: The default setting is 60 seconds.

3. Under the **Link Layer Discovery Protocol (LLDP)** pane, configure the parameters as described in Table 59.

Table 59: LLDP Parameters

Parameter	Description
Enable LLDP	Select this option to enable LLDP on the access point. When enabled, an access point advertises its identity, capabilities and configuration information to connected peers and learns the same from them. This option is enabled by default.
Hold Time	Use the spinner control to set the hold time (in seconds) for transmitted LLDP PDUs. Set a value in the range 10 – 1,800. The default hold time is 180 seconds.
Timer	Set the interval used to transmit LLDP PDUs. Define an interval in the range 5 – 900 seconds. The default setting is 60 seconds.
Inventory Management Discovery	Select this option to include LLPD-MED inventory management discovery TLV in LLDP PDUs. This setting is enabled by default.
Extended Power via MDI Discovery	Select this option to include LLPD-MED extended power via MDI discovery TLV in LLDP PDUs. This setting is enabled by default.

4. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

CDP/LLDP Configuration on page 191

Routing Configuration

Routing configuration establishes the IP paths over which network traffic is routed. Use the **Routing** tab to set destination IP and gateway addresses, enabling assignment of static IP addresses for requesting clients. Priority assignments for static routes determines the default gateway. If connectivity fails or the default gateway becomes unusable, failover to the next highest priority, active static route occurs.

To add or delete static route for a device:

1. Select either **Profiles** or **Devices**.

   The window displays a list controllers and access points within the managed network.
2. Select a profile or device in the list to open its configuration window.
3. Select the **Network** > **Routing** tabs.

   The network routing configuration window opens. If any static routes have been configured, they appear in a list in the **Static Routes** pane. The **Total** number of existing static routes is shown in parentheses. The currently active default gateway is identified with a green checkmark under the **Default Gateway** column.
4. In the **Static Routes** pane, choose from the following actions:

   a. Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.

   b. Select the **Edit** icon ✎ associated with a static route to modify the **Network Address** and **Gateway** settings, as described in the table below. To edit priority settings for configured gateways, proceed to step 7.

c. Select the **Delete** icon 🗑 to delete an existing static route.

d. Select the **Add** icon + to configure a static route. Set the following parameters, then proceed to step 5 to assign a priority to this route.

Network Address	Add network IP addresses and network masks.
Gateway	Enter the Gateway IP address. This is the gateway used to route traffic to the specified network.

5. In the **Default Route Priority** pane, set the following parameters to assign priorities to the static route gateway added in the previous step:

Static Default Route Priority	Use the spinner control to set the priority value (1 - 8,000) for the default static route. This is weight assigned to this route versus others that have been defined. The default setting is 100.
DHCP Client Default Route Priority	Use the spinner control to set the priority value (1 - 8,000) for the default route learned from the DHCP client. The default setting is 1000.
Enable Routing Failure	When selected, all configured gateways are monitored for activity. The system invokes failover to a live gateway if the current default gateway becomes unusable. This feature is enabled by default.

6. After you have completed configuring the settings, choose from the following actions:

a. Select **Revert** to restore default settings or restore the last saved settings.

> Note
> You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

7. To view or edit the static route and DHCP client priority settings for the configured gateways, go to **Remote CLI** and select the **Add** icon + to start a CLI session. Log in, and choose from the following actions:

a. To view the assigned priorities for configured gateways, use the CLI command: **`<DEVICE>(config-device-<MAC>|config-profile-<PROFILE-NAME>)#show ip default-gateways`**

b. To edit the assigned priorities for configured gateways, use the CLI command: **`<DEVICE>(config-device-<MAC>|config-profile-<PROFILE-NAME>)#ip default-gateway [<IP>|<HOST-ALIAS-NAME>|failover|priority [dhcpclient <1-8000>|static-route <1-8000>]]`**

Example:

```
vx9000-3C6F18(config-profile-default-profile)#ip default-gateway priority dhcp-client
<1-8000>
```

Forwarding Database Configuration

A Forwarding Database is used to forward or filter packets on behalf of a controller, service platform, or access point. The packet's destination MAC address is read and the controller, service platform, or access point decides to either forward the packet or drop (filter) it. If it is determined that the destination MAC is on a different network segment, the device forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). As nodes transmit packets through the bridge, the bridge updates its forwarding database with known MAC addresses and their locations on the network. This information is then used to filter or forward the packet.

Related Links

Configure a Forwarding Database on page 195

Configure a Forwarding Database

Use this procedure to configure a Forwarding Database profile for a device.

1. Go to **Profiles** *<select a device profile>* **Network** > **Forwarding Database**.
2. Configure **Aging Time** parameters as described in Table 60.

Table 60: Aging Time Parameters

Parameter	Description
Bridge Aging Time	The aging time defines the length of time an entry remains in the a bridge's forwarding table before being deleted due to inactivity. Define a **Bridge Aging Time**. Enter a value in the range 10 – 1000000 seconds. The default value is 300 seconds.
L3e Lite Entry Aging Time	The L3e Lite table stores information about destinations and their location within a specific IPSec tunnel. This allows for quicker packet transmissions. The table is updated as nodes transmit packets. Define a **L3e Lite Entry Aging Time** to stipulate the amount of time a learned L3e entry (IP, VLAN) is to remain in the L3e Lite table before deletion due to lack of activity. Enter a value in the range 10 – 1000000 seconds. The default value is 300 seconds.

3. Configure and manage the **Static Forwarding Table**.

   The Static Forwarding Table lists configured forwarding destinations in tabular form.

   Choose from the following actions:

   - Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ⇅1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.

- Select 🔍 and enter a keyword in the search field to narrow the list of forwarding destination entries in the table.
- Select ⤓ to download the forwarding destination entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an entry to modify the forwarding destination details.
  - Select 🗑 associated with an entry to delete it.
- Select + to add a new forwarding destination. Configure the **Static Forwarding Table** parameters as described in Table 61.

Table 61: Static Forwarding Table Parameters

Parameter	Description
MAC Address	Set a destination **MAC Address** address. The bridge reads the packet's destination MAC address and decides to forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered).
VLAN ID	Define the target **VLAN ID** if the destination MAC is on a different network segment.
Interface Name	Enter an **Interface Name** used as the target destination interface for the target MAC address.

4. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   Note
   You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

   Note
   This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

   Note
   If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Forwarding Database Configuration on page 195

Bridge VLAN Configuration

A Virtual LAN (VLAN) is a separately administrated virtual network within the same physical network. VLANs are broadcast domains defined within switches to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.

Administrators often need to route traffic to interoperate between different VLANs. Bridge VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which untags it. When a data frame is received on a port, the bridge VLAN determines the associated VLAN based on the port of reception. Using forwarding database information, the bridge VLAN forwards the data frame on the appropriate port(s).

Related Links

Manage Bridge VLANs on page 197
Configure a Bridge VLAN on page 199
Configure Bridge VLAN General Settings on page 199
Bridge VLAN IGMP Snooping on page 204
Configure Bridge VLAN MLD Snooping on page 206

Manage Bridge VLANs

Go to **Profiles** <*select a device profile*> **Network** > **Bridge VLAN**.

Note
You can override configured Bridge VLAN profile settings for a specific device. Go to **Devices** <*select a device*> **Network** > **Bridge VLAN**.

The **Bridge VLAN** window includes:

- A list of configured Bridge VLANs.
- Tools that allow users to manage Bridge VLANs.

View Configured Bridge VLANs

The Bridge VLAN window displays a list of all configured Bridge VLANs in tabular form.

Table 62 describes the type of information displayed under each column.

Table 62: Bridge VLAN List Column Headings

Column Heading	Description
VLAN	Displays the numerical identifier defined for the Bridge VLAN when initially created.
Description	Displays the description of the VLAN assigned when it was created or modified.
Edge VLAN Mode	Identifies whether the VLAN is currently in edge VLAN mode, as follows: • ✓ indicates Yes. • ✗ indicates No.

Table 62: Bridge VLAN List Column Headings (continued)

Column Heading	Description
Trust ARP Responses	Identifies whether **Trust ARP Responses** is enabled, as follows: • ✓ indicates Yes. • ✗ indicates No.
Trust DHCP Responses	Identifies whether **Trust DHCP Responses** is enabled, as follows: • ✓ indicates Yes. • ✗ indicates No.
IPv6 Firewall	Identifies whether **IPv6 Firewall** is enabled, as follows: • ✓ indicates Yes. • ✗ indicates No.
DHCPv6 Trust	Identifies whether **DHCPv6 Trust** is enabled, as follows: • ✓ indicates Yes. • ✗ indicates No.
RA Guard	Identifies whether **RA Guard** is enabled, as follows: • ✓ indicates Yes. • ✗ indicates No.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download a list of the Bridge VLAN entries in the table in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a Bridge VLAN entry to modify it.
  - Select 🗑 associated with a Bridge VLAN entry to delete it.
- Select + to configure a new Bridge VLAN.

Related Links

Configure a Bridge VLAN on page 199

Configure a Bridge VLAN

Use this procedure to configure, edit, or delete a Bridge VLAN profile.

1. Choose from the following actions:
   - If you are in the process of configuring a new Profile, go to **Network** > **Bridge VLAN** then proceed to the next step.
   - If you want to edit or delete a Bridge VLAN profile, go to **Profiles** <*select a device profile*> **Network** > **Bridge VLAN**.

     Choose from the following actions:
     - To edit a Bridge VLAN profile, select ✎ adjacent to the target profile. Modify the profile in accordance with the steps in this procedure.
     - To delete a Bridge VLAN profile, select 🗑 adjacent to the target profile.
2. Select + to create a new Bridge VLAN profile.
3. Enter a numerical value (1 - 4094) in the **VLAN** field, then select **Add**.
4. Configure the parameters in the **General**, **IGMP Snooping**, and **MLD Snooping** tabs.
5. Select **Add** to create the new Bridge VLAN profile.
6. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure Bridge VLAN General Settings on page 199

Bridge VLAN IGMP Snooping on page 204

Configure Bridge VLAN MLD Snooping on page 206

Configure Bridge VLAN General Settings

Use this procedure to configure or modify Bridge VLAN profile parameters under the **General** tab.

1. Choose from the following actions:
   - If you are in the process of configuring a new Bridge VLAN profile, proceed to the next step.

- If you want to modify an existing Bridge VLAN profile, go to **Profiles** <*select a device profile*> **Network** > **Bridge VLAN**. Select ✎ associated with the target Bridge VLAN entry to modify it. Modify the settings in accordance with the steps in this procedure.

2. Select the **General** tab and configure the parameters as described in Table 63.

Table 63: General Tab Parameters

Parameter	Description
Basic	
Name	Enter a **Name**, not exceeding 32 characters, for the Bride VLAN.
Description	Enter a **Description** (up to 64 characters) unique to the specific configuration of the VLAN to help differentiate it from other VLANs with similar configurations.
Per VLAN Firewall	Select **Per VLAN Firewall** to enable an IPv4 firewall on this interface. Firewalls, generally, are configured for all interfaces on a device. When configured, firewalls generate flow tables that store information on the traffic allowed to traverse through the firewall. These flow tables occupy a large portion of the limited memory that could be used for other critical purposes. With the per VLAN firewall feature enabled on an interface, flow tables are only generated for that interface. Flow tables are not generated for those interfaces where this feature is not enabled. This frees up memory which can be used for other purposes. Firewalls can be switched off for those interfaces which are known to carry trusted traffic and only enabled on the interfaces that can provide a vector for an attack on the network. This parameter is disabled by default.
URL Filter	
URL Filter	Select a **URL Filter**. URL filters are used to control the access to resources on the Internet.
Application Policy	
Application Policy	Select the appropriate **Application Policy** to use with this Bridge VLAN configuration. An application policy defines the rules or actions executed on recognized HTTP (Facebook), enterprise (Webex) and peer-to-peer (gaming) applications or application-categories.
Extended VLAN Tunnel	

Table 63: General Tab Parameters (continued)

Parameter	Description
Bridging Mode	Select a **Bridging Mode** for the VLAN. Options are: • Automatic: Select automatic to let the controller, service platform or access point determine the best bridging mode for the VLAN. • Local: Select Local to use local bridging mode for bridging traffic on the VLAN. • Tunnel: Select Tunnel to use a shared tunnel for bridging traffic on the VLAN. • isolated-tunnel: Select isolated-tunnel to use a dedicated tunnel for bridging VLAN traffic.
IP Outbound Tunnel ACL	Select an appropriate **IP Outbound Tunnel ACL** for outbound traffic.
IPv6 Outbound Tunnel ACL	Select an appropriate **IPv6 Outbound Tunnel ACL** for outbound traffic.
MAC Outbound Tunnel ACL	Select an appropriate **MAC Outbound Tunnel ACL** for outbound traffic.
Tunnel Over Level 2	Select **Tunnel Over Level 2** to allow VLAN traffic to be tunneled over Level 2 links. This parameter is disabled by default.
Extended VLAN Tunnel Authentication	
MAC Authentication	Select **MAC Authentication** to enable source MAC authentication for extended VLAN and tunneled traffic (MiNT and L2TPv3) on this bridge VLAN. When enabled, it provides fast path authentications of clients, whose captive portal session has expired. This parameter is disabled by default.
Captive Portal Enforcement	Select the authentication mode to be used for extended VLAN and tunneled traffic on this Bridge VLAN. Options are: • None: No Authentication mode used. • Authentication Failure: Configures MAC Authentication as the primary and Captive-Portal Authentication as the fallback authentication mode. • Always: Configures Captive-Portal Authentication as the only mode of Authentication.
Tunnel Rate Limit	
Add	Select **Add** to display and configure **Tunnel Rate Limit** parameters. Select 🗑 to delete and hide the parameters.
Mint Link Level	Select the **MINT Link Level**.

Table 63: General Tab Parameters (continued)

Parameter	Description
Rate	Define a transmit **Rate** limit in the range 50 – 1000000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the Bridge VLAN. Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.
Max Burst Size	Set a **Max Burst Size** in the range 2 – 1024 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion. The default burst size is 320 kbytes.
Background	Set the random early detection threshold in % for background traffic. Set a value from 0 - 100%. The default is 50%.
Best Effort	Set the random early detection threshold in % for best-effort traffic. Set a value in the range 0 - 100%. The default is 50%.
Video	Set the random early detection threshold in % for video traffic. Set a value in the range 1 - 100%. The default is 25%.
Voice	Set the random early detection threshold in % for voice traffic. Set a value in the range 1 - 100%. The default is 0%.
Layer 2 Firewall	
Trust ARP Response	Select this option to use trusted ARP packets to update the DHCP Snoop Table to prevent IP spoof and arp-cache poisoning attacks. This feature is disabled by default.
Trust DHCP Responses	Select this option to use DHCP packets from a DHCP server as trusted and permissible within the managed network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. This feature is disabled by default.
Edge VLAN Mode	Select this option to enable edge VLAN mode. When selected, the edge controller's IP address in the VLAN is not used, and is now designated to isolate devices and prevent connectivity. This feature is enabled by default.
IPv6 Settings	
IPv6 Firewall	Select this option to enable IPv6 on this Bridge VLAN. This setting is enabled by default.

Table 63: General Tab Parameters (continued)

Parameter	Description
DHCPv6 Trust	Select this option to enable the trust all DHCPv6 responses on this Bridge VLAN. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is enabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects on this Bridge VLAN. This setting is enabled by default.
Registration	
Name	Enter the RADIUS group name in which registered users are placed. When left blank, users are not associated with a RADIUS group.
Type	Select the self-registration type used for this Bridge VLAN. Options are as follows: • None • Local • Tunnel • Isolated Tunnel
Expiry Time	Set the amount of time (in the range 1 - 43,800 hours) before registration addresses expire and must be re-entered.
Registration External	
Enable	Specifies that the wired client registration is handled by an external resource. Registration requests are forwarded to the external registration server by the captive portal gateway controller.
Follow AAA	Select to enable the use of an AAA policy to point to the guest registration, authentication, and accounting server. When enabled, guest registration is handled by the RADIUS server specified in the AAA policy. This is the AAA policy used in the captive-portal applied on the bridge vlan interface. In case of EGuest deployment, in the AAA policy, the RADIUS authentication and accounting server configuration should point to the EGuest server. The use of option is recommended in EGuest replica-set deployments.
Send Mode	Specifies the protocol used to forward registration requests to the external AAA policy server.
Captive Portal	

Table 63: General Tab Parameters (continued)

Parameter	Description
Captive Portal Name	Select an existing captive portal configuration to apply access restrictions to the Bridge VLAN configuration. If an existing captive portal does not suit the Bridge VLAN configuration, see Captive Portals Policy on page 391 for information on configuring a captive portal policy.
Captive Portal Snoop Subnet	For wired captive portal clients with static IP, to learn IPV4 to MAC snooping, select **Add** and enter the corresponding subnet and excluded IP.
Captive Portal Snoop IPv6 Subnet	For wired captive portal clients with static IP, to learn IPV6 to MAC snooping, select **Add** and enter the corresponding subnet and excluded IP.

3. If Bridge VLAN configuration is complete, select **Add**. Otherwise, select the **IGMP Snooping** or **MLD Snooping** tabs and continue with configuration.

Related Links

Configure a Bridge VLAN on page 199

Bridge VLAN IGMP Snooping on page 204

Configure Bridge VLAN MLD Snooping on page 206

Bridge VLAN IGMP Snooping

IGMP Snooping is used to keep host memberships alive. It is primarily used in a network where there is a multicast streaming server, 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 packets are not flooded on the wired port. IGMP membership is also learned on it and only if present, then it is forwarded on that port.

Use this procedure to configure or modify IGMP Snooping parameters for the Bridge VLAN profile.

1. Choose from the following actions:
   - If you are in the process of configuring a new Bridge VLAN profile, proceed to the next step.
   - If you want to modify an existing Bridge VLAN profile, go to **Profiles** <*select a device profile*> **Network** > **Bridge VLAN**. Select ✎ associated with a Bridge VLAN profile entry to modify it. Modify the settings in accordance with the steps in this procedure.

2. Select the **IGMP Snooping** tab and configure the parameters as described in Table 64.

Table 64: IGMP Snooping Tab Parameters

Parameter	Description
General	
Enable IGMP Snooping	**Enable IGMP Snooping** is enabled by default. If disabled, snooping on this Bridge VLAN is disabled, and the settings under bridge configuration are overridden.
Forward Unknown Unicast Packets	**Forward Unknown Unicast Packets** enables multicast forwarding of packets from unregistered multicast groups. If disabled, unknown multicast forwarding is also disabled for this Bridge VLAN. Forwarding of unknown packets is enabled by default.
Enable Fast Leave Processing	Select **Enable Fast Leave Processing** to remove a Layer 2 LAN interface from the IGMP snooping forwarding table entry 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. This parameter is disabled by default.
Last Member Query Count	Specify the number (1–7) of group-specific queries sent before removing an IGMP snooping entry. The default setting is 2.
Multicast Router	
Interface Names	Select the interface used for IGMP snooping over a multicast router. Multiple interfaces can be selected.
Multicast Router Learn Mode	Select **`static`** or **`pim-dvmrp`** as the mode used to determine client multicast traffic levels on specific routes.
IGMP Querier	
Enable IGMP Querier	**Enable IGMP Querier** is selected by default.
Source IP Address	Define an IP address applied as the **Source IP Address** in the IGMP query packet. This address is used as the default VLAN querier IP address.
IGMP Version	Set the **IGMP Version** compatibility to either version 1, 2, or 3. The default setting is 3.

Table 64: IGMP Snooping Tab Parameters (continued)

Parameter	Description
Maximum Response Time	Specify the **Maximum Response Time** (1 – 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. For IGMP reports from wired ports, reports are only forwarded to the multicast router ports. The default setting is 10 seconds.
Other Querier Timer Expiry	Specify an interval (60 – 300 seconds) to be used as a timeout interval for other querier resources. The default setting is 60 seconds.

3. If Bridge VLAN configuration is complete, select **Add**. Otherwise, select the **General** or **MLD Snooping** tabs and continue with configuration.

Related Links

Configure a Bridge VLAN on page 199

Configure Bridge VLAN General Settings on page 199

Configure Bridge VLAN MLD Snooping on page 206

Configure Bridge VLAN MLD Snooping

Multicast Listener Discovery (MLD) Snooping enables a controller, service platform or access point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices 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.

Use this procedure to configure or modify MLD Snooping parameters for the Bridge VLAN profile.

1. Choose from the following actions:
   - If you are in the process of configuring a new Bridge VLAN profile, proceed to the next step.
   - If you want to modify an existing Bridge VLAN profile, go to **Profiles** <*select a device profile*> **Network** > **Bridge VLAN**. Select ✎ associated with a Bridge VLAN profile entry to modify it. Modify the settings in accordance with the steps in this procedure.

2. Select the **MLD Snooping** tab and configure the parameters as described in Table 65.

Table 65: MLD Snooping Tab Parameters

Parameter	Description
General	
Enable MLD Snooping	The **Enable MLD Snooping** function examines MLD packets and supports content forwarding on this Bridge VLAN. Packets delivered are identified by a single multicast group address. Multicast packets are delivered using best-effort reliability, just like IPv6 unicast. MLD Snooping is enabled by default.
Forward Unknown Packets	**Forward Unknown Packets** enables multicast forwarding of unknown IPv6 packets. Forwarding of unknown packets is enabled by default.
Multicast Router	
Interface Names	Select the **Interface Names** to be used for MLD snooping.
Multicast Router Learn Mode	Set **Multicast Routing Learn Mode** to either `Pim-dvmrp` or `Static`. DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths. Pim-dvmrp is the default setting.
MLD Querier	
Enable MLD Querier	Select **Enable MLD Querier** 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. Enable MLD Querier is enabled by default.
MLD Version	Select **MLD Version** to enable it. Select either version 1 or 2 to define which version is to be used with 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 setting is version 2.

Table 65: MLD Snooping Tab Parameters (continued)

Parameter	Description
Maximum Response Time	Specify the **Maximum Response Time** (1 – 25000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 1 millisecond.
Other Querier Timer Expiry	Specify an interval (60 – 300 seconds) to be used as a timeout interval for other querier resources. The default setting is 60 seconds.

3. If Bridge VLAN configuration is complete, select **Add**. Otherwise, select the **General** or **IGMP Snooping** tabs and continue with configuration.

Related Links

Configure a Bridge VLAN on page 199

Configure Bridge VLAN General Settings on page 199

Bridge VLAN IGMP Snooping on page 204

Alias Configuration

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if a network alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias works with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

For more information, refer to the following:

- Configure a Network Basic Alias Profile on page 209
- Configure a Network Group Alias Profile on page 212
- Configure a Network Service Alias Profile on page 213

Configure a Network Basic Alias Profile

A **Basic Alias** consists of VLAN, Host, Address Range, Network, and String alias configurations. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

1. Go to **Profiles** <*select a device profile*> **Network** > **Alias** > **Basic Alias**.
2. Select **Add** and configure **VLAN Alias** parameters as described in Table 66.

   Use the **VLAN Alias** to create unique aliases for VLANs that can be utilized at different deployments. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias. At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.

Table 66: VLAN Alias Parameters

Parameter	Description
Name	Assign a distinguishing name of up to 32 characters. The alias name always starts with a dollar sign ($).
VLAN	Set the VLAN ID to a value in the range 1 – 4094.

Note
A VLAN alias is used to replace VLANs in the following locations:

- Bridge VLAN
- IP Firewall Rules
- L2TPv3
- Switchport
- Wireless LANs

3. Select **Add** and configure **Host Alias** parameters as described in Table 67.

   Use the **Host Alias** to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

Table 67: Host Alias Parameters

Parameters	Description
Name	Assign a distinguishing name of up to 32 characters. The alias name always starts with a dollar sign ($).
Host	Set the numeric IP address set for the host.

Note

A host alias can be used to replace host names in the following locations:

- IP Firewall Rules
- DHCP

4. Select **Add** and configure **Address Range Alias** parameters as described in Table 68.

   Use the **Address Range Alias** to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110, the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

Table 68: Address Range Alias Parameters

Parameter	Description
Name	Assign a distinguishing name of up to 32 characters. The alias name always starts with a dollar sign ($).
Start IP	Set a starting IP address used with a range of addresses utilized with the address range alias.
End IP	Set an ending IP address used with a range of addresses utilized with the address range alias.

5. Select **Add** and configure **Network Alias** parameters as described in Table 69.

   Use the **Network Alias** to configure aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new

ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

Table 69: Network Alias

Parameter	Description
Name	Assign a distinguishing name of up to 32 characters. The alias name always starts with a dollar sign ($).
Network	Provide a network address in the form of host/mask.

Note
A network alias can be used to replace network declarations in the following locations:

- IP Firewall Rules
- DHCP

6. Select **Add** and configure **String Alias** parameters as described in Table 70.

   Use **String Alias** to create aliases for strings that can be utilized at different deployment locations. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

Table 70: String Alias Parameters

Parameter	Description
Name	Assign a distinguishing name of up to 32 characters. The alias name always starts with a dollar sign ($).
Value	Provide a string value to use in the alias.

Note
A string alias can be used to replace domain name strings in DHCP.

7. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   Note
   You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

   Note
   This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
>
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure a Network Group Alias Profile on page 212

Configure a Network Service Alias Profile on page 213

Configure a Network Group Alias Profile

A **Network Group Alias** consists of Host and Network configurations.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight host entries, eight network entries and eight IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

1. Go to **Profiles** <*select a device profile*> **Network** > **Alias** > **Network Group Alias**.
2. Select + to add a Network Group alias.
3. Assign a **Name** for the alias in the range 1 – 32 characters.

   > Note
   >
   > The Network Group Alias name always starts with a dollar sign ($).

4. Select **Add** to configure **Host** alias settings. Specify the Host IP address for up to eight IP addresses supporting network aliasing. Enter a single IP address using the form 192.168.10.23.
5. Select **Add** to configure **Network** alias settings. Specify the netmask for up to eight (8) IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Enter an IP address representing complete networks in the form of 192.168.10.0/24, or enter an IP address range as described in the next step.
6. Select **Add** to configure a **Range** of IP addresses for use with Network alias configurations. Enter an IP address range using the **Start IP** and **End IP** fields.
7. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > Note
   >
   > You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

   > Note
   >
   > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
>
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure a Network Basic Alias Profile on page 209
Configure a Network Service Alias Profile on page 213

Configure a Network Service Alias Profile

A **Network Service Alias** consists of protocol and port mapping configurations. Both source and destination ports are configurable. For each protocol, up to two (2) source port ranges and up to two (2) destination port ranges can be configured. A maximum of four (4) protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

1. Go to **Profiles** <*select a device profile*> **Network** > **Alias** > **Network Service Alias**.
2. Select + to add a Network Service alias.
3. Assign a **Name** for the alias in the range 1 – 32 characters.

   > Note
   >
   > The Network Group Alias name always starts with a dollar sign ($).

4. Select **Add** to add an **Entry** and configure the parameters as described in Table 71.

Table 71: Network Service Alias

Parameter	Description
Protocol	Specify the protocol for which the alias is created. Use the drop down to select the protocol from **`eigrp`**, **`gre`**, **`icmp`**, **`igmp`**, **`ip`**, **`vrrp`**, **`igp`**, **`ospf`**, **`tcp`** and **`udp`**. Select **`other`** if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
Service Port	This field is relevant only if the protocol is *tcp* or *udp*. Specify the service ports for this protocol entry. Up to eight (8) service ports can be specified.
Destination Port	This field is relevant only if the protocol is *tcp* or *udp*. Specify the destination ports for this protocol entry. Up to eight (8) service ports can be specified.

5. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure a Network Basic Alias Profile on page 209
Configure a Network Group Alias Profile on page 212

Device Profile - Policies Configuration

User defined profiles can be customized and 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.

Note
You can override the policy settings assigned to a device profile by configuring the same settings at the device level. Go to **Devices** <*select a device*> **Policies**.

Configure policies parameters for a device profile:

1. Go to **Profiles** <*select a device profile*> **Policies**.

   Configure the device profile Policies parameters as described in Table 72.

Table 72: Device Profile - Policy Parameters

Parameter	Description
Management Policy	Select a Management Policy to assign to the device profile. The default setting is **`default`**. 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	Select a Firewall Policy to assign to the device profile. The default setting is **`default`**
RADIUS Server Policy	Select a RADIUS Server Policy to assign to the device profile. The default setting is **`none`**. A RADIUS Server policy provides customized, profile specific, management of authentication data such as username and password.
Event System Policy	Select an Event System Policy to assign to the device profile. The default setting is **`none`**. An Event System Policy allows the profile to capture system events and append them to a log file.
DHCPv4 Policy	Select a DHCPv4 Policy to assign to the device profile. The default setting is **`none`**.
Captive Portal Policy	Select a Captive Portal Policy to assign to the device profile. There is no default setting. If no policy is selected, no captive portal policy is assigned to the profile.
Bonjour Gateway Forwarding Policy	Select a Bonjour Gateway Forwarding Policy to assign to the device profile. The default setting is **`none`**.

2. Configure **Auto-Provisioning Policy** parameters as described in Table 73.

Table 73: Device Profile - Auto-Provisioning Policy Parameters

Parameter	Description
Auto-Provisioning Policy	Select an Auto-Provisioning Policy to assign to the device profile. The default setting is `none`. 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.
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. Options are `No`, `Yes`, and `Always`. The default setting is No.
Learn and Save Network Configuration	Select this option to allow the controller or service platform to maintain local configuration records of devices requesting adoption and provisioning. This feature is enabled by default

3. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Advanced Configuration

MiNT policy secures communications at the transport layer. Using MiNT, a device can be configured to communicate only with other MiNT activated devices.

Use this procedure to configure or edit MiNT Link policy.

Note
Use this procedure to configure a device profile, or to override profile settings for a specific device.

1. Go to **Profiles** or **Devices** and select a device from the profile or device list.
2. Select the **Advanced** tab.
3. Configure or edit the parameters as described in Table 74.

Table 74: MiNT Link Settings

Parameter	Description
MLCP IP	Select **MLCP IP** to activate *MiNT Link Creation Protocol* using an IP address. MLCP is used to create a UDP/IP link from the device to a neighbor. The neighboring device does not need to a controller or a service platform. It can be another access point with a path to the controller or service platform
MLCP IPv6	Select **MLCP IPv6** to activate MLCP for automated MiNT UDP/IP link creation
MLCP VLAN	Select **MLCP VLAN** to activate MiNT MLCP by VLAN. MLCP is used to create one VLAN link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be another access point with a path to the controller or service platform
Tunnel MiNT Across Extended VLAN	Select **Tunnel MINT Across Extended VLAN** to tunnel MiNT protocol packets across an extended VLAN

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

Note

If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Mesh Point Configuration

Mesh networking provides users wireless access to broadband applications anywhere, including a moving vehicle. Initially developed for secure and reliable military battlefield communications, mesh technology supports public safety, public access, and public works. Mesh technology reduces the expense of wide-scale networks, by leveraging Wi-Fi enabled devices already deployed.

Mesh points are access points dedicated to mesh network support. Mesh points capture and disseminate their own data and serve as a relay for other nodes.

1. Select **Profiles**.
2. Select an existing target profile.

   The general menu opens.
3. Select **Mesh Point**.

   The mesh connex policy configuration associated with the profile opens.
4. Review existing mesh point configurations to determine whether a new configuration needs to be created or an existing configuration needs to be modified.

Mesh Point Connex Policy	Lists the administrator assigned name for the MeshConnex Policy, defined upon its creation. The name cannot be edited later with other parameters.
Is Root	Indicates whether the mesh point is the root node in the mesh network. **`True`** defines the mesh point as a root, **`False`** indicates that the mesh point is not a root, and **`None`** means the mesh point root has not been assigned yet
Preferred Root	Lists the MAC address of a preferred root device
Root Selection Method	Displays the method used for selecting a root node. Options inclue: • **`auto-mint`** • **`auto-proximity`**
Preferred Neighbor	Lists the MAC address of the preferred neighbor within the mesh point's mesh topology
Preferred Interface	Displays either **`2.4GHz`**, **`4.9GHz`**, **`5GHz`** or **`6GHz`** as the preferred band of operation for the mesh point.

Monitor Critical Resources	When activated, you allow the dynamic conversion of a mesh point from root to non-root when there is a critical resource failure. This option is not selected by default.
Monitor Primary Port Link	When activated, you allow the dynamic conversion of a mesh point from root to non-root during a link down event. This option is not selected by default.
Path Method	Lists the root path selection method used in the mesh network. Available options include: • **`None`** - Indicates no criteria used in root path selection • **`uniform`** - The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths) • **`mobile-snr-leaf`** - The access point is mounted on a vehicle or a mobile platform. The path to the route is selected based on the *Signal To Noise Ratio* (SNR) with the neighbor device • **`snr-leaf`** - The path with the best signal to noise ratio is always selected • **`bound-pair`** - Binds one mesh point connection at a time. Once established, other mesh point connection requests are denied

5. If there is no existing mesh point connex policy configuration, select + to create a new policy.

   The **Add** dashboard opens.
6. Select a policy from the drop-down list box.
7. Select **Add** to include a new policy.
8. Select **Save** to include the policy to an existing profile.

Configure mesh point device basic settings and auto channel selection.

Configure Mesh Point Device Basic Settings

Configure basic settings for a new mesh point configuration or modify the device settings on an existing mesh point configuration.

1. Select **Profiles** > **Profile Name** > **Mesh Point** > **Mesh Point Connex Policy**.

   The **Settings** dashboard opens.

2. Set the following **General** parameters:

Is Root	Select the root behavior of this mesh point. Select **True** to indicate this mesh point is a root node for this mesh network. Select **False** to indicate this mesh point is not a root node for this mesh network
Root Selection Method	Use the drop-down list box to determine whether this meshpoint is the root or non-root meshpoint
Path Method	Select the root path selection method used in the mesh network. For available path methods, see Mesh Point Configuration on page 218
Set as Cost Root	Select to set the mesh point as the cost root for meshpoint root selection
Monitor Critical Resources	Select to allow dynamic conversion of a mesh point from root to non-root when there is a critical resource failure
Monitor Primary Port Link	Select to allow dynamic conversion of a mesh point from root to non-root during a link down event
Wired Peer Excluded	Select to exclude a mesh from forming a link with another mesh device that's a wired peer

Note
When using 4.9 GHz, the root preferences selection for the radio's preferred interface still displays as 5 GHz.

3. Set the following **Root Path Preferences**:

Preferred Neighbor	Specify the MAC address of a preferred neighbor within the mesh topology
Preferred Root	Specify the MAC address of a preferred root device
Preferred Interface	Use the drop-down list box to set the preferred mesh point interface to either **2.4 GHz**, **4.9 GHz**, **5 GHz**, or **6 GHz**

4. Set the following **Path Method Hysteresis**:

Minimum Threshold	Type or use the spinner control to set the minimum value for SNR (between -100 to 0 dB) above which a candidate for the next hop in a dynamic mesh network is considered for selection. This field along with **`Signal Strength Delta`** and **`Sustained Time Period`** are used to dynamically select the next hop in a dynamic mesh network
Signal Strength Delta	Type a delta value or use the spinner control to set the signal strength between 1 to 100 dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR value that is higher than the value configured here. This field along with the **`Minimum Threshold`** and **`Sustained Time Period`** are used to dynamically select the next hop in a dynamic mesh network
Sustained Time Period	Type the duration or use the spinner control to set the time period in seconds for the duration a signal must sustain the constraints specified in the **`Minimum Threshold`** and **`Signal Strength Delta`** path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network
SNR Delta Range	Type or use the spinner control to set the delta range between 1 to 100 dB. The device must sustain a signal strength within the delta range to be considered a candidate

5. Select **Update** to apply mesh point basic settings.

Configure Mesh Point Auto Channel Selection

The Auto Channel Selection settings is used to define the Dynamic Root Selection for 2.4 GHz, 4.9 GHz, 5.0 GHz, and 6GHz interfaces.

1. Select **Profiles** > **Profile Name** > **Mesh Point** > **Mesh Point Connex Policy**.

   The **Settings** dashboard opens.
2. Select **Auto Channel Selection**.
3. Configure the following values, which are common to 2.4 GHz, 5.0/4.9 GHz, and 6 GHz channels. Use the auto channel selection settings to refine channel scans, set

the scan duration, enable off-channel scanning, specify the scan sample size, and channel hold time, etc.

Channel Width	Set the channel width that the meshpoint automatic channel scan assigns to the selected radio. The available options are: • **`auto`** - Defines the channel width is calculated automatically. This is the default value • **`20 MHz`** - Sets the width between two adjacent channels as 20 MHz • **`40 MHz`** - Sets the width between two adjacent channels as 40 MHz • **`80 MHz`** - Sets the width between two adjacent channels as 80 MHz • **`160 MHz`** - Sets the width between two adjacent channels as 160 MHz
Priority Mesh Point	Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected
Off-Channel Duration	Set the duration between 20 to 250 milliseconds. The scan dwells on each channel when performing an off channel scan. The default value is 50 milliseconds
Off-Channel Scan Frequency	Set the duration between 1 to 60 seconds between two consecutive off channel scans. The default value is 6 seconds
Sample Count	Set the number of scan samples between 1 and 10. The scans are performed for data collection before a mesh channel is selected. The default value is 5
Channel Hold Time	Set the duration between 0 to 86,400 seconds to remain on a channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring. The default value is 1800 seconds
SNR Delta	Type or use the spinner control to set the delta range between 1 to 100 dB. When path selection occurs, the defined value is utilized for selecting the optimal path. A better candidate, on a different channel, must have a signal strength that exceeds this delta value when compared to the signal strength of the next hop in the mesh network. The default value is 5 dB

Signal Threshold	Type or use the spinner control to set the minimum value for signal threshold between -100 to 0 dB. If the signal strength of the next mesh hop falls below this set value, a scan is triggered to select a better next hop. The default value is -65 dB
Path Minimum	Set the minimum path metric between 100 to 20,000 for mesh connection establishment. The default value is 1,000
Path Metric Threshold	Set a minimum threshold between 800 to 65,535 for triggering an automatic channel selection for mesh point selection. The default value is 1500
Tolerance Period	Set a duration (between 10 to 600 seconds) to wait before triggering an automatic channel selection for the next mesh hop. The default value is 60 seconds
Channel Switch Delta	Set the delta (between 5 to 35 dBm) that triggers a mesh point root automatic channel selection when exceeded. The default value is 10 dBm

4. Select **Update** to apply mesh point auto channel selection settings.

Cluster Configuration (Controllers Only)

A cluster (or redundancy group) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the cluster, members discover and establish connections to other members and provide wireless network self-healing support in the event of member's failure.

A cluster's load balance is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members join and exit the cluster.

1. Select **Profiles**.
2. Select a controller from the list of device profile.
3. Select **Cluster**.
4. Configure the following **Settings**:

Mode	A member can be in either an **Active** or **Standby** mode. All active member can adopt access points. Standby members only adopt access points when an active member has failed or sees an access point not adopted by a controller or service platform. The default cluster mode is Active
Name	Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters

Master Priority	Set a priority value from 1 to 255, with the higher value given higher priority. This configuration is the device's priority to become the cluster master. In a cluster environment, one device from the cluster is elected as the cluster master. The master priority setting is the device's priority to become cluster master. The active primary controller has the higher priority. The default value is 128
Force Configured State Delay	Specify a delay interval between 3 to 1800 minutes. This is the interval a standby cluster member waits before releasing adopted APs and goes back to a monitoring mode when a controller becomes active again after a failure. The default interval is 5 minutes
Force Configured State	Select to enable this cluster member to take over for an active member if it were to fail. A standby controller or service platform takes over APs adopted by the failed member. If the failed cluster member were to come available again, the active member starts a timer based on the Auto Revert Delay interval. At the expiration of the Auto Revert Delay, the standby member releases all adopted APs and goes back to a monitoring mode. The Auto Revert Delay timer is stopped and restarted if the active member goes down and comes up during the Auto Revert Delay interval
Handle STP Convergence	Select to enable Spanning Tree Protocol (STP) convergence for the controller or service platform. In general, this protocol is enabled in layer 2 networks to prevent network looping. Spanning Tree is a network layer protocol that ensures a loop-free topology in a mesh network of inter-connected layer 2 cluster members. The spanning tree protocol clears redundant connections and uses the least costly path to maintain a connection between any two controllers or service platforms in the network. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup
Radius Counter DB Sync Time	Specify a sync time from 1 to 1,440 minutes a RADIUS counter database uses as its synchronization interval with the dedicated NTP server resource. The default interval is 5 minutes

5. Within the **Member** field, select **Cluster VLAN** to designate the VLAN where cluster members are reachable. Specify a VLAN from 1 to 4094.
6. Select **Add** to include **Member IP Address** and **Routing Level** information.

   Define a routing level between 1 or 2 for the link between adopting devices. The default setting is 1.
7. Select **Save** to update cluster configuration settings.

Controller Cluster Profile Configuration and Deployment Considerations

Before defining a profile cluster configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- A cluster member cannot adopt more APs than its hardware capacity and license provisions allow. This is important when the number of pooled AP and AAP licenses exceeds the aggregated AP and AAP capacity available after a cluster member has failed. A cluster supported profile should be designed to ensure adequate AP and AAP capacity exists to address failure scenarios involving both APs and AAPs.
- When cluster is enabled for a profile and a failure occurs amongst one of the cluster members, AP and AAP licenses are persistent in the cluster even during reboots or power outages. If a cluster member failure were to occur, cluster settings must remain enabled on all remaining cluster members or the pooled member licenses will be deprecated.

Message Logging Configuration for Profiles

Follow these steps to configure **Message Logging** parameters for the selected profile:

1. Select **Profile**.

   A list of profiles appears in the **Profile** window.
2. Select a profile in the list.

   The profile configuration window opens displaying the **General** configuration for the device profile.
3. Select the **MSG Logging** tab.

   The **Message Logging** configuration window opens.
4. Configure the Message Logging settings as follows:

Enable Message Logging	Select this option to enable the profile to log system events to a log file or a syslog server. Selecting this check box enables the rest of the parameters required to define the profile's logging configuration. This option is disabled by default.
Remote Logging Host	Select **Add** to create a table to define numerical (non DNS) IP addresses and ports for up to three external resources where logged system events can be sent on behalf of the profile. Select **Add** to add a new IP address. Select the delete icon 🗑 as needed to remove an IP address.
Facility to Send Log Messages	Use the drop-down menu to specify the local server (if used) for profile event log transfers.
Syslog Logging Level	Select this option to enable **Syslog Logging Level**. Use the drop-down list to assign a severity level to log events based on criticality. Event severity coincides with the syslog logging level defined for the profile. Severity level options are **`Emergencies`**, **`Alerts`**, **`Critical`**, **`Errors`**, **`Warnings`**, **`Notifications`**, **`Informational`** and **`Debugging`**. The default logging severity level is Warning.

Console Logging Level	Select this option to enable **Console Logging Level**. Use the drop-down list to assign a severity level to log events based on criticality. Event severity coincides with the syslog logging level defined for the profile. Severity level options are `Emergencies`, `Alerts`, `Critical`, `Errors`, `Warnings`, `Notifications`, `Informational` and `Debugging`. The default logging severity level is Warning.
Buffered Logging Level	Select this option to enable **Buffered Logging Level**. Use the drop-down list to assign a severity level to log events based on criticality. Event severity coincides with the syslog logging level defined for the profile. Severity level options are `Emergencies`, `Alerts`, `Critical`, `Errors`, `Warnings`, `Notifications`, `Informational` and `Debugging`. The default logging severity level is Warning.
Forward Logs to Controller	Select this option to enable **Forward Logs to Controller**. Use the drop-down list to assign a severity level for forwarding event logs to the controller. Log level options are `Emergencies`, `Alerts`, `Critical`, `Errors`, `Warnings`, `Notifications`, `Informational` and `Debugging`. The default logging severity level is Errors.
Time to Aggregate Repeated Messages	Define the increment (or interval) system events are logged on behalf of the profile. The shorter the interval, the sooner the event is logged. Define an interval in seconds (0 - 60) or in minutes (0 -1). The default value is 0 seconds.

5. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

NAT Configuration

Network Address Translation (NAT) is a technique that is used to modify network address information within IP packet headers during transit across a traffic routing device. This enables mapping one IP address to another to protect network address credentials. In typical deployment models, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

NAT can provide a profile outbound Internet access to wired and wireless hosts connected to a controller, service platform or access point (AP). Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows a controller, service platform or AP to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

> **Note**
> NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

Manage NAT Resources

Configuring Network Address Translation (NAT) comprises the following tasks:

- Defining network pools
- Setting Static NAT Source and Destination parameters
- Setting Dynamic NAT parameters

The user interfaces involved in NAT configuration are arranged under tabs. When you select any given tab, configured items display as list entries in tabular form. Each of the tabs provides a common set of tools that allow users to manage the table entries.

Management tools are used as follows:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the table entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an entry to modify it.
  - Select 🗑 associated with an entry to delete it.
- Select + to configure a new table entry.

Configure a NAT Pool

Use this procedure to configure or edit Network Address Translation (NAT) Pool settings for a device profile, or to override NAT Pool device profile settings for a specific device.

Define a range of IP addresses hidden from the public Internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device.

> **Note**
> NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

1. Choose from the following actions:
   - If you are in the process of configuring a new device profile, proceed to the next step.
   - If you want to configure or edit NAT Pool settings for an existing device profile, go to **Profiles**, select the target profile, then proceed to the next step.
   - If you want to override NAT Pool device profile settings for a specific device, go to **Devices**, select the target device, then proceed to the next step.
2. Select the **NAT** tab.

   The **NAT Pool** tab displays by default. The NAT Pool window lists the configured NAT Pools, if any exist. The total number of configured NAT Pools appears in parentheses.
3. Choose from the following actions:
   - Select + to add a new NAT Pool.
   - Select ✎ adjacent to an existing NAT Pool, then edit the settings in accordance with the steps in this procedure.
   - Select 🗑 adjacent to an existing NAT Pool to remove it.
4. If you are creating a new NAT Pool, assign a **Name** to it that will distinguish it from others with similar configurations. The name cannot exceed 64 characters.

   > **Note**
   > You cannot edit the name of an existing NAT Pool.
5. Under the **IP Address Range** pane, choose from the following actions:
   - Select **Add** to define a new IP Address Range. Repeat this action to define up to 128 entries.
   - Edit an IP Address Range.
   - Select 🗑 adjacent to an existing IP Address Range entry to remove it.
6. Select **Add** to create the new NAT Pool, or select **Update** to apply changed settings for an existing NAT Pool.
7. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > **Note**
   > You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configure Static NAT Source or Destination

Static NAT Source configurations create permanent, one-to-one mappings between addresses on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

Static NAT Destination configurations ensure packets passing through the NAT back to the managed LAN are searched against the records kept by the NAT engine. The destination IP address is changed back to the specific internal private class IP address to reach the LAN over the network.

Use this procedure to perform any of the following tasks:

- Configure, edit, or delete Static NAT settings for a device profile.
- Override Static NAT device profile settings for a specific device.

Configuring Static NAT comprises setting Source and Destination parameters.

Configure Static NAT

1. Choose from the following actions:
   - If you are in the process of configuring a new profile, proceed to the next step.
   - If you want to configure, edit, or delete Static NAT settings for an existing profile, go to **Profiles**, select the target device profile, then proceed to the next step.
   - If you want to override Static NAT device profile settings for a specific device, go to **Devices**, select the target device, then proceed to the next step.
2. Select the **NAT** tab.
3. Select the **Static NAT Source** tab or the **Static NAT Destination** tab.

   Depending on your selection, a list of source or destination configurations displays, if any exist. The total number of source or destination configurations appears in parentheses.
4. See the *Configure Static NAT Source* and *Configure Static NAT Destination* procedures below for instructions on setting parameters.

Configure Static NAT Source

1. Choose from the following actions:
   - Select + to add a new Static NAT Source. Proceed to the next step.
   - From under the **Action** column:
     - Select ✏ associated with a Static NAT Source, then modify it in accordance with the steps in this procedure.
     - Select 🗑 associated with a Static NAT Source to delete it.
2. In the **Add NAT Source** pop-up window, configure or edit the parameters as described in the following table, then select **Add** to create the NAT Source.

Table 75: Static NAT Source Parameters

Parameter	Description
Source IP	Enter the local address used at the origination of the static NAT configuration. This address (once translated) is not exposed to the outside world when the translation address is used to interact with the remote destination.
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either source or destination based on the direction specified.
Network	Select **`Inside`** or **`Outside`** as the network direction. Select Inside to create a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. Inside is the default setting.

3. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > Note
   > You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

   > Note
   > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

   > Note
   > If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configure Static NAT Destination

1. Choose from the following actions:
   - Select + to add a new Static NAT Destination. Proceed to the next step.

- From under the **Action** column:
  - Select ✏ associated with a Static NAT Destination, then modify it in accordance with the steps in this procedure.
  - Select 🗑 associated with a Static NAT Destination to delete it.

2. In the **Add NAT Destination** pop-up window, configure or edit the parameters as described in the following table, then select **Add** to create the NAT Destination.

Table 76: Static NAT Destination Parameters

Parameter	Description
Protocol	Select the protocol for use with static translation. Options include: • `TCP` — TCP is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. • `UDP` — The *User Datagram Protocol* (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. • `Any` — This is the default setting.
Destination IP	Enter the local address used at the (source) end of the static NAT configuration. This address (once translated) is not be exposed to the outside world when the translation address is used to interact with the remote destination.
Destination Port	The Destination Port and Destination Protocol parameters work together to identify the local port and protocol used at the (source) end of the static NAT configuration. The NAT engine uses these settings as match criteria for packets passing through the NAT back to the managed LAN. Set the Destination Port number in the range 1–65535. The default port is 1, which corresponds to no specific Destination Protocol. Note: This field is automatically datafilled according to the selected Destination Protocol.

Table 76: Static NAT Destination Parameters (continued)

Parameter	Description
Destination Protocol	Specify the protocol port to be used by the NAT engine as match criteria for packets passing through the NAT back to the managed LAN. Options include: • **`Other`** (default) — No designated protocol port (1) • **`ftp`** — Configures the default File Transfer Protocol (FTP) control services port (21) • **`ftpdata`** — Configures the default FTP data services port (20) • **`gopher`** — Configures the default GOPHER services port (70) • **`https`** — Configures the default HTTPS services port (443) • **`idap`** — Configures the default Lightweight Directory Access Protocol (LDAP) services port (389) • **`nntp`** — Configures the default Network News Transfer Protocol (NNTP) protocol port (119) • **`ntp`** — Configures the default Network Time Protocol (NTP) services port (123)
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either *source* or *destination* based on the direction specified.
NAT Port	Set the port number of the matching packet to the specified value. This option is valid only if the direction specified is destination.
NAT Protocol	Identify a specific destination or protocol port to match Select the NAT protocol to match. Options include: • **`Other`** • **`ftp`** • **`ftpdata`** • **`gopher`** • **`https`** • **`idap`** • **`nntp`** • **`ntp`**
Network	Select **`Inside`** (default) or **`Outside`** NAT as the network direction.

3. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configure Dynamic NAT

Dynamic NAT translates the IP address of packets from one interface to another interface based on configured conditions. Dynamic NAT requires packets be switched through a NAT router to generate translations in the translation table.

Use this procedure to perform any of the following tasks:

- Configure, edit, or delete Dynamic NAT settings for a device profile
- Override Dynamic NAT device profile settings for a specific device

1. Choose from the following actions:
   - If you are in the process of configuring a new profile, proceed to the next step.
   - If you want to configure, edit, or delete Dynamic NAT settings for an existing profile, go to **Profiles**, select the target profile, then proceed to the next step.
   - If you want to override Dynamic NAT device profile settings for a specific device, go to **Devices**, select the target device, then proceed to the next step.
2. Select the **NAT** tab.
3. Select the **Dynamic NAT** tab.

   A list of Dynamic NAT configurations displays in tabular format, if any exist. The total number of Dynamic NAT configurations appears in parentheses. A summary of configuration characteristics—represented by column headings—is provided for each table entry.

4. See Table 77 for instructions on setting parameters.

Table 77: Dynamic NAT Parameters

Parameter	Description
Source List ACL	Select an access control list (ACL) policy to define the packet selection criteria for NAT. NAT is applied only on packets that match a rule defined in the ACL. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with the remote destination. If no policy exists, see IPv4 ACL Policy on page 337 to create one.
Network	Select **Inside** or **Outside** NAT as the network direction for the dynamic NAT configuration.
ACL Precedence	Set a priority value in the range 1–5000 for applying the source list ACL. The lower the value, the higher the priority assigned to the ACL rule.
Interface	Select the interface used as the communication medium between the source and destination points within the NAT configuration. Options are: • **VLAN** — Selects a VLAN interface. Select a **VLAN ID** in the range 1–4094. Note: Ensure that the VLAN selected adequately supports the intended network traffic within the NAT supported configuration. • **WWAN** — Selects Wireless WAN interface • **PPPoE1** — Selects PPP over Ethernet interface
Overload Type	Define the overload type used when several internal addresses are NATed to only one or a few external addresses. Options are: • **NAT Pool** • **One Global Address** • **Interface IP Address**
NAT Pool	Select the an existing NAT pool for use with the dynamic NAT configuration. Note: This option is enabled only if the **Overload Type** is set to **NAT Pool**.
Overload IP	If **One Global IP Address** is selected as the **Overload Type**, define an IP address to use as a filter address for the IP ACL rule.

5. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Critical Resource Management Configuration

Critical resources are device IP addresses or interface destinations on the network that are deemed critical to the health of the network. The critical resource feature allows for the continuous monitoring of these addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, a AAA server, a WAN interface, or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly by the access point. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. By default, no critical resource policy is enabled, and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they are discovered. For example, a critical resource on the same subnet as the access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to be monitored on that VLAN.

You can configure critical resources for access points and wireless controllers using their respective profiles.

Related Links

Configure Critical Resources on page 235

Configure Critical Resources

To use this procedure, you must be in the process of configuring a new profile, modifying an existing profile, or overriding a profile's Critical Resource settings for an individual device.

Use this procedure to define, modify, or delete **Critical Resources** for the selected profile or device.

1. Choose from the following actions:
   - If you are in the process of configuring a new profile, proceed to the next step.
   - If you want to edit or delete Critical Resource settings, go to **Profiles** or **Devices**, select the target profile or device in the list, then proceed to the next step.
2. Select the **CRM** tab and configure or edit the parameters in the **General** pane as described in the following table, then continue to the next step.

Table 78: Critical Resources General Parameters

Parameter	Description
Monitor Interval	Set the period between two successive pings to the critical resource. Enter a value in the range 5 – 86,400 seconds. The default value is 30 seconds.
Source IP for Port-Limited Monitoring	Enter the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface. Generally, the source address 0.0.0.0 is used in the APR packets used to detect critical resources. However, some devices do not support the above IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for Port-Limited Monitoring must be different from the IP address configured on the device.
Monitor Retry Count	Enter the number of retry connection attempts (1 – 10) permitted before this device connection is defined as down (offline). The default setting is 3 connection attempts.

3. If any Critical Resources are configured, they appear in tabular form in the **List Of Critical Resources** pane. The total number of configured Critical Resources is displayed in parentheses. Choose from the following actions:
   a. Select + to add a new Critical Resource. Proceed to the next step.
   b. Select ⇅ adjacent to sort the list of Critical Resources. By default, the resources are sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the list in descending order ↓1.
   c. Select 🔍 and enter a keyword in the search field to narrow the list of resources in the table.
   d. Select ⤓ to download the resource entries in the table in csv format.
   e. Select ▥ to choose the columns displayed in the table.
   f. Select ⟳ to refresh the list.
   g. Under the **Actions** column in the table, choose from the following actions:
      - Select ✎ and modify the Critical Resource Monitoring settings as described in the steps in this procedure. Select **Update** to apply the changes.
      - Select 🗑 to delete a Critical Resource.

4. Configure or edit the **Critical Resources Monitoring** parameters as described in the following tab Table 79.

Table 79: Critical Resources Monitoring Parameters

Parameter	Description
Critical Resource Name	Assign a name (up to 32 characters) that uniquely identifies the Critical Resource.
Use Flows	Select **Use Flows** to enable monitoring of the critical resources using firewall flows for DHCP or DNS instead of ICMP or ARP packets. This reduces the amount of traffic on the network. This parameter is disabled by default.
Sync Adoptees	Select **Sync Adoptees** to sync adopted devices to state changes with a resource-state change message. This parameter is disabled by default.
Offline Resource Detection	Use the **Offline Resource Detection** drop-down menu to define how critical resource event messages are generated. Options include: • **`Any`**: If you select this option, an event is generated when the state of any single critical resource changes. • **`All`**: If you select this option, an event is generated when the state of all monitored critical resources change.
Monitor Criteria	This parameter is active only when the **`Use Flows`** option is enabled. Use the **Monitor Criteria** drop-down menu to select one of the following options: • **`rf-domain-manager`**: If you select rf-domain-manager, the current rf-domain manager performs resource monitoring, and the rest of the devices do not. The RF-domain-manager updates any state changes to the rest of the devices in the RF Domain. • **`cluster-master`**: With the cluster-master option, the cluster master performs resource monitoring and updates the cluster members with state changes. • **`All`**: With a controller-managed RF Domain, set Monitor Criteria to All because the controller might not know the VLAN bridged locally by the devices in the RF Domain monitoring DHCP.
Monitor Via	Use the drop-down menu to choose the means by which the critical resource is to be monitored. Options include: • **`None`**: This is the default setting. • **`IP`**: Select this option to monitor a critical resource directly (within the same subnet) and enter the IP address to be used as a network identifier. • **Interface**: Select this option to monitor a critical resource using the critical resource's **`VLAN`**, **`WWAN1`** or **`PPPoE1`** interface. If you select **`VLAN`**, use the spinner control to define the destination VLAN ID used as the interface for the critical resource.

5. In the **Critical Resource Monitoring** window, under the **Resources** pane, choose from the following actions:

   a. Select **Add** to configure a new resource as described in Table 80.

b. Select 🗑 adjacent to a resource to delete a it. You cannot modify Resources.

Table 80: Resources Parameters

Parameter	Description
Mode	Sets the ping mode used when the availability of a critical resource is validated. Select from: • `Not Set` (default) – No mode specified. • **`arp-only`** – Use only the *Address Resolution Protocol* (ARP) for pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known. • **`arp-and-ping`** – Use both ARP and Internet Control Message Protocol (ICMP) for pinging the critical resource and sending control messages (for example, device not reachable or requested service not available).
VLAN	Using the spinner control, define the VLAN on which the critical resource is available.
IP/Alias/Network	Provide the IP address, alias, or network address of the critical resource. This is the address used by the access point to ensure the critical resource is available.
Port	Define the interface on which to monitor critical resource. This field lists the available hardware interfaces. This option is available only when the selected mode is **`arp-only`**.

6. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

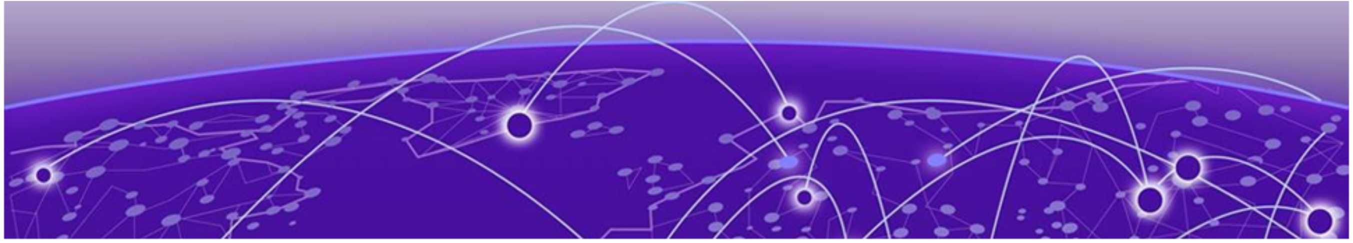
      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

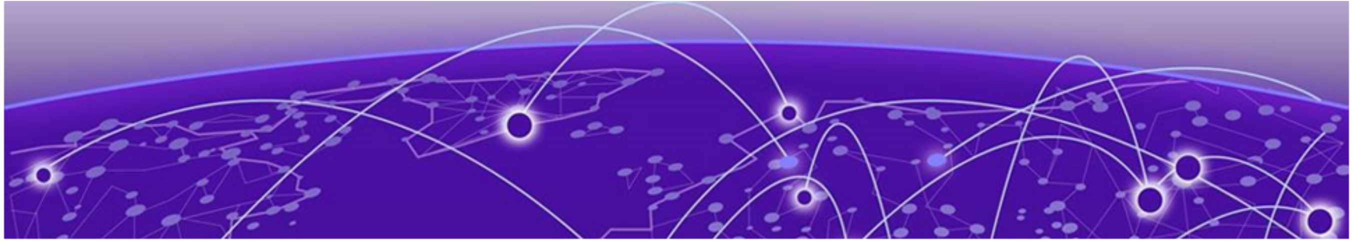
Critical Resource Management Configuration on page 235



Clients

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

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.

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.

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 is automatically generated 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 37.

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 37.

Advanced Logs

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

Ping

Ping is a command that determines the reachability of a device on the network. Initiate Ping from a specific device to a specified destination. Specify the site, device, and IP address or DNS name destination to determine reachability.

To access Ping:

1. Go to **Diagnostics** > **Ping**.
2. Select a site.
3. Select a device.
4. Enter the IP address or DNS name of the selected destination.
5. Select **Start**.

Traceroute

Initiate the Traceroute command, which traces the path of a packet from ExtremeCloud IQ to the IP address or FQDN that you specify. It lists the routers it passes until it reaches its destination, or fails to. It also indicates the length of each hop.

To access Traceroute:

1. Go to **Diagnostics** > **Traceroute**.
2. Select a site.
3. Select a device.
4. Enter the IP address or DNS name of the selected destination.
5. Select **Start**.

Packet Capture

Use Packet Capture to identify network inconsistencies by intercepting packets from the APs. Packets are captured based on the parameter configurations that you specify.

Capture packets from an individual AP or from a site. Go to **Diagnostics** > **Packet Capture**.

Packet Capture Parameters

To access packet capture, go to **Diagnostics** > **Packet Capture** and configure the following settings:

Table 81: Packet Capture Parameters

Field Name	Description
In the **Basic** pane, configure the following settings:	
Site	Network Site
Device	Origin device of packet capture

Table 81: Packet Capture Parameters (continued)

Field Name	Description
Maximum Packet Count	Specify the maximum number of packets captured and logged to the PACP file. The default value is 200. Possible range is 1 - 1000000. Packet capture stops once the threshold specified here is reached, unless manually stopped beforehand. Note: The default maximum packet capture data limit is 1 GB. Therefore, regardless of the Maximum Packet Capture Count specified, packet capture stops once the PCAP file size reaches 1 GB.
Send Packet To	Select File to send the packets to a PCAP file.
Path/File	Specify the path to the PCAP file.
In the **Capture Locations** pane, configure the following settings:	
Bridge	Select this option to capture packets to and from the appliance. When capturing appliance data ports, you must configure at least one filter. From the **Filters** pane, select either IP address or MAC address for the appliance. Only one capture task can apply to the Appliance Data Ports at a time. If more than one capture task is started using the Appliance Data Ports, the last requested task will be started.
Dropped	Select this option to capture dropped packets to and from the appliance.

Table 81: Packet Capture Parameters (continued)

Field Name	Description
Wired	Enables wired-packet capture on the selected AP and selected wired port. Select the port type and number. Valid values for port type are: • ge • up • port-channel • pppoe • vlan • vmif • wwan • xge Filter packets on the basis of the direction of packet flow: • **Inbound** — Capture packets received by the AP. • **Outbound** — Capture packets transmitted by the AP. • **Any** — Capture packets transmitted and received by the AP. This is the default value. Select **Includes Wired Clients** to include wired-packets received and transmitted to and from wired clients associated with the selected AP. This option is disabled by default.
Wireless	Enables wireless-packet capture on the selected AP. Specify the radio interface on which to enable wireless-packet capture. • **Radio 1** — Enable packet capture on the Radio 1 interface. • **Radio 2** — Enable packet capture on the Radio 2 interface. • **Radio 3** — Enable packet capture on the Radio 3 interface. • **All Radios** — Enable packet capture on all radio interfaces for the selected AP. This option is selected by default. Filter packets on the basis of the direction of packet flow: • **Inbound** — Capture packets received by the AP. • **Outbound** — Capture packets transmitted by the AP. • **Any** — Capture packets transmitted and received by the AP. This is the default value.

Table 81: Packet Capture Parameters (continued)

Field Name	Description
In the **Filter** pane, filter packets by **MAC address**, **IP address**, **IP Protocol**, or **Port**. The filters are mutually exclusive and are applied in the order in which they are listed. Enter at least one MAC address or IP address. Note: Excessive packet capture degrades network performance. If you are going to enable packet capture on all APs, specify at least one MAC address filter and one IP address filter to avoid performance degradation.	
MAC address	When a MAC address is specified, only packets that move to and from the specified MAC addresses are captured.
IP address	When an IP address is specified, only packets that move to and from the specified IP address are captured. Both IPv4 and IPv6 address formats are supported.
IP Protocol	Valid protocol filters: • TCP • UDP • TCP/UDP • ICMP • IGMP • DHCP • DNS
Port	Specify a TCP or UDP port number. Packets with the matching port number are captured. Use **Port** as an additional filter.

Debug Wireless Clients

An administrator can select an RF domain and capture connected client debug messages at a specified interval and from a selected location. Client debug information can either be collected historically or in real time.

To troubleshoot issues with wireless client connectivity within a controller, service platform, virtual platform or access point managed RF domain:

1. Select **Diagnostics** > **Debug Wireless Clients**.

2. Configure the **Basic**, **Debug Messages**, **Wireless Clients**, and **Settings** parameters:

Site	Use the **Select a site** drop-down menu to identify a site (RF domain) used for wireless client debugging. RF domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building, or site.
Device	Use the **Select a device** drop-down menu to select one or more devices assigned to the site (RF domain) from which debug messages are to be collected.
Send Data To	Use the **Send Data To** drop-down menu to select where wireless client debug messages are collected. If **`Screen`** is selected, the wireless client debug information is sent to the **Event Logs** window at the bottom of the dialog window. If **`File`** is selected, the file location must be specified in the **Path/File** field for the **Settings** parameters to transfer the logs to the server. The default setting is **`File`**.
Debug Messages	Select the **All** radio button to capture all debug messages for wireless clients associated with the selected devices in the selected RF domain. Choose **Selected** to specify which types of debug messages to capture. If you choose **Selected**, you can capture any combination of the following debug messages: • Management • RADIUS • EAP • System • Migration • WPA/WPA2
Wireless Clients	Select the **All** radio button to capture debug information from all wireless clients associated with the selected devices in the selected RF domain. Choose **Selected** to capture information from up to three specified wireless clients. Specify the MAC address for the wireless clients. The information captured and displayed on-screen or logged to a file contains only information from the specified wireless clients.
Duration of Message Capture	Use the spinner controls to select how long to capture wireless client debug information. This can range between 1 second and 24 hours. The default value is 60 seconds.
Maximum Events Per Wireless Client	Use the spinner controls to select the maximum number of debug messages to capture per wireless client. Set the limit from between 1 to 9999 events. The default value is 50 events.

Path/File	If the **Send Data To** field is set to **File**, you must specify the path to the file in the **Path/File** field.
Event Logs	When the **Send Data To** field is set to **Screen**, this pane displays live debug information captured for wireless clients associated with the selected device in the selected RF domain.

3. When all configuration fields are complete, select **Start** to start the wireless client debug message capture.

   If information is being sent to the screen, it displays in the **Event Logs** pane. If the data is being sent to a file, that file populates with debug information. If you have set a long message capture duration and want to end the capture early, select **Stop**.

   The Event Logs pane displays the following information.

Field	Description
Status	Running or completed
Session name	Name is automatically generated when starting the remote debug wireless session
Started by	User details
Type	Network type
Hosts	Controller or access point information
Message	Success information or error message

NEW! Fault Management

Fault management allows users who are administering multiple sites to assess how individual devices are performing and review issues impacting the network, and take remedial actions if necessary. Use the Fault Management screens to troubleshoot errors generated by a controller, service platform, access point or wireless client.

Related Links

Filter Events (APs only) on page 249

Event History on page 252

NEW! Filter Events (APs only)

Use Filter Events to diagnose faults on access points (APs). Administrators can configure filters to track—all or specific—devices, event types, and severities, or a combination of these.

Related Links

Manage Event Filters on page 250

Configure Event Filters on page 251

Configure an Event System Policy on page 312

NEW!Manage Event Filters

Go to **Diagnostics** > **Fault Management** > **Events Filter**.

The **Event Filters** window includes:

- A list of configured Event Filters, if any exist.
- Tools that allow users to manage filters.

View Configured Event Filters

The **Event Filters** window displays a list of all configured filters in tabular form. The total number of configured filters is shown in parentheses.

Table 82 describes the type of information displayed under each column in the table.

Table 82: Event Filters Table Column Headings

Column Heading	Description
Severity	Displays the severity assigned to the associated event filter.
Module Name	Displays the module(s) used to track the event.
Source	Displays the MAC address of the source device tracked by the selected module(s).
Message	Displays the message assigned to the event filter, which aims to provide meaningful and relevant information to administrators for troubleshooting.
Filter Status	Indicates the status of the event filter, as follows: • ✓ — indicates that the filter is active • ✗ — indicates that the filter is inactive
Action	SeeManagement Tools

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table. Select it again to clear the search field and revert to the default list view.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- Under the **Actions** column, choose from the following:
  - Select the ⏻ toggle to disable or enable the associated filter.

    - Select 🗑 to delete the associated filter.
- Use « ‹ 1 2 › » to navigate pages if multiple pages exist.

Related Links

Configure Event Filters on page 251

Disable or Enable Event Filters on page 252

NEW!

Configure Event Filters

Use this procedure to create filters to help diagnose faults on an access point (AP). Newly created filters are active by default. Administrators must deactivate filters as necessary.

1. Go to **Diagnostics** > **Fault Management** > **Filter Events**.
2. Set the parameters for the new Event Filter you want to create as described in Table 83.

Table 83: Event Filters Parameters

Parameter	Description
Severity	Set the filtering severity. Select from the following: **`All Severities`** – All events are displayed, irrespective of their severity **`Critical`** – Only critical events are displayed **`Error`** – Only errors and higher severity events are displayed **`Warning`** – Only warnings and higher severity events are displayed **`Notice`** – Only notices and higher severity events events are displayed
Event Module	Select the event module for which events are tracked. When an event module is selected, events from other modules are not tracked. Remember this when interested in events generated by a particular module. Individual modules can be selected (such as **`test`** or **`pm`**) or all modules can be tracked by selecting **`All Modules`**.
Source	Set the MAC address of the source device to be tracked. Retaining the default MAC address of FF-FF-FF-FF-FF-FF allows all devices to be tracked.
Message Substring	Optionally append a text message (substring) to the Event Filter to assist the administrator in distinguishing this filter from others with similar attributes.

Note
Retain the Source field default value of FF-FF-FF-FF-FF-FF to track all MAC addresses.

3. Select Add to active filters to create the new filter and add it to the **Active Event Filters** table.

Related Links

Manage Event Filters on page 250

Disable or Enable Event Filters on page 252

NEW! *Disable or Enable Event Filters*

When initially created, event filters are enabled by default. Use this procedure to disable or enable event filters.

1. Go to **Diagnostics** > **Fault ManagementFilter Events**.
2. Choose from the following actions:
   a. To deactivate all the event filters in the **Active Events Filters** table, select **Disable All Events**.
   b. To activate all the event filters in the **Active Events Filters** table, select **Enable All Events**.
   c. To disable or enable one or more individual event filters, under the **Action** column in the **Active Event Filters** table, select the ⏻ adjacent to the target filter.

Related Links

Configure Event Filters on page 251

Event History

The Event History screen displays historical events for both wireless controllers and access points.

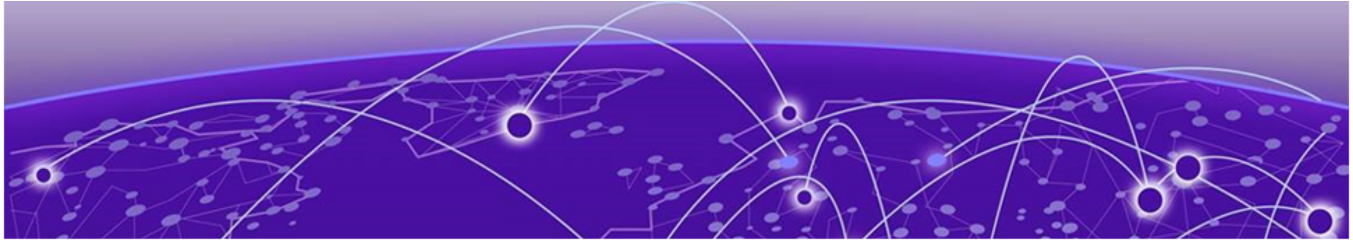
Use this procedure to view a list of historical events for a specified device at a specified site (RF Domain).

1. Go to **Diagnostics** > **Event History**.
2. Select a **Site**.
3. Select a **Device** assigned to the site for which you want to view historical events.
4. Select **Fetch Historical Events** to generate and display the events data.
5. Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
6. Select **Clear** to remove the data displayed in the **Event History** pane.

The **Event History** pane displays a list of historical events for the specified device at the specified site (RF Domain).

The following event data is fetched and displayed:

Timestamp	Displays the timestamp (time zone specific) when each listed event occurred.
Module	Displays the module tracking the listed event. Events detected by other modules are not tracked.
Message	Displays error or status messages for each event.
Severity	Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include: *All Severities* – All events are displayed irrespective of their severity. *Critical* – Only critical events are displayed. *Error* – Only errors and higher severity events are displayed. *Warning* – Only warnings and higher severity events are displayed. *Informational* – Only informational and higher severity events are displayed.
RF Domain	Displays the Site selected for which the event history logs are captured.
Source	Displays the MAC address of the device tracked by the selected module.
Mnemonic	Displays the shorthand definition of a message action in a single word.



Remote 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.

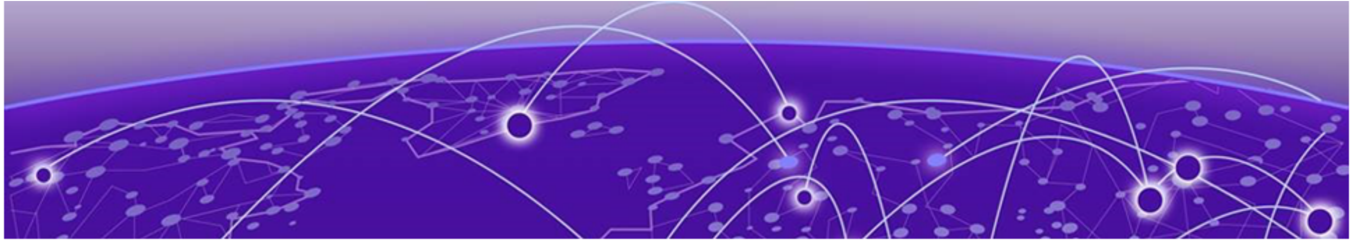
Note
Telnet access must be provided for individual users to access Remote CLI. For more information, see Set Access Control Configuration on page 363.

Remote CLI Operations

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

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

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.

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.

AAA Policy Configuration

To view, edit, delete, or add an AAA policy:

1. Select **Policies** > **AAA**.

   The **AAA** window displays. If any AAA policies are configured, they appear in tabular form in the AAA pane. The total number of AAA policies is shown in parentheses.

   Table 84 describes the column headings in the AAA policies table.

Table 84: AAA Policies Table Column Headings

Column Heading	Description
Policy Name	Lists the names of configured AAA policies.
Accounting Packet Type	Displays the accounting type set for the AAA policy. These include: • Start/Stop • Start/Interim/Stop
Wireless Client Attempts	Displays the number of attempts by the wireless client

2. Choose from the following actions:
   a. Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ⇅1. Toggle the icon to sort the column data in descending order ⇅1. The "1" indicates by which column heading topic the data is currently sorted.

   b. Select the **Edit** icon ✎ associated with an AAA policy to modify it.

      When you select **Edit**, the configuration window appears for the selected policy. Edit the parameters in accordance with the instructions in the procedures in this section. You cannot edit the **Policy Name**.

   c. Select the **Delete** icon 🗑 associated with an AAA policy to remove it.

   d. Select the **Add** icon + to create a new AAA policy.

      When you select **Add**, the **Add Policy** window appears.

      i. Assign a policy **Name**. The name cannot exceed 32 characters.
      ii. Select **Add** to save the policy.
      iii. Configure the settings in the General and RADUIS tabs.

Configure an AAA Policy Server

A AAA policy must exist. See AAA Policy Configuration on page 257.

Configure or edit general information for an AAA policy server:

1. Choose from the following actions:
   a. To continue configuring settings for a new AAA policy, skip to step 2 .
   b. To edit AAA policy server settings, select **Policy > AAA**, then select an existing policy from the list in the **AAA** pane to open the configuration window.

2. In the **General** tab, choose from the following actions:
    a. Select the **Add** icon + to configure a new AAA policy server.
    b. Select an existing AAA policy server in the list and edit the settings as described in the table below.
3. Configure or edit or the following **Server** settings:

Server parameter	Description
Sever ID	Set the numerical server index (1-12) for the accounting server when added to the list available to the access point.
Server Type	Select the AAA policy server type. Options are: • **Authentication** • **Accounting**
Port	Set the port on which the RADIUS server listens to traffic within the access point managed network. The port range is 1 - 65,535. For an Authentication server, the default port is `1812`. For an Accounting server, the default port is `1813`.
Server Host	Select the server host type. Options are: • **IP/Host** • **Onboard** • **Controller** • **Centralized** If the server host selected is **IP/Host**, use the drop-down menu to select either **Hostname** or **IP Address** and, accordingly, type the host name or IP address in the associated field. Enter the password in the **Secret** field.
Request Proxy Mode	Specify the method of proxy that browsers use to communicate with the RADIUS authentication server. Options are: • None • Through Controller • Through Centralized Controller • Through RF Domain Manager • Through MINT Host
Request Attempts	Set 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	Set 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.

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configure AAA Policy Server RADIUS Settings

An AAA policy must exist. See AAA Policy Configuration on page 257.

Configure or edit RADIUS server settings:

1. Choose from the following actions:
   a. To continue configuring settings for a new AAA policy, skip to step 2.
   b. To edit RADIUS server settings, select **Policy > AAA**, then select an existing policy from the list in the **AAA** pane to open the configuration window.

2. Configure or edit the following RADIUS server **Settings**:

Radius settings	Description
Accounting type	Select the accounting type to specify the frequency of event notifications. Options include: • **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 a process is running, and a stop notice at the end of a process. • **Stop Only** — Sends only a stop notice at the end of a process. The default option is **Start/Stop**
Address format	Specify the format in which the MAC address must be filled in the Radius-Request frames. Options include: • **No Delimiter (AABBCCDDEEFF)** • **Colon Delimiter (AA:BB:CC:DD:EE:FF)** • **Hyphen Delimiter (AA-BB-CC-DD-EE-FF)** • **Space Delimiter (AA BB CC DD EE FF)** • **Dot Delimiter per Four (AABB.CCDD.EEFF)** • **Middle Hyphen Delimiter (AABBCC-DDEEFF)** The default option is **Hyphen Delimiter (AA-BB-CC-DD-EE-FF)**
Case	Specify the **Case** of the MAC address that must be filled in Radius-Request frames: • **Upper** • **Lower** The default option is **Upper**.
Attributes	Specify the RADIUS attributes to which the MAC address format is applicable: • **All** — Applies to all attributes with MAC addresses such as username, password, calling-station-id, and called-station-id • **Username-Password** — Applies only to the username and password fields. The default option is **Username-Password**.

Radius settings	Description
Server pooling	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. Selecting the **Load-Balance** option results in all available servers transmitting requests in round robin mode. The default option is **Fail Over**.
Authentication Protocol	Options include: • PAP • CHAP • MS-CHAP • MS-CHAPv2 The default protocol option is **PAP**

3. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

AAA TACACS Policy

Terminal Access Controller Access - Control System+ (TACACS) is a protocol created by CISCO Systems which provides access control to network devices (routers, network access servers and other networked computing devices) using one or more centralized servers. TACACS provides separate authentication, authorization, and accounting services running on different servers.

TACACS controls user access to devices and network resources while providing separate accounting, authentication, and authorization services. Some of the services provided by TACACS include the following:

- Authorizing each command with the TACACS server before execution
- Accounting each session's log in and log out event
- Authenticating each user with the TACACS server before enabling access to network

Related Links

Manage AAA TACACS Policies on page 262

Manage AAA TACACS Policies

Go to **Policies** > **AAA TACACS**.

The **Authentication, Authorization, and Accounting (AAA) TACACS** window includes:

- A list of configured policies.
- Tools that allow users to manage policies.

View Configured Policies

The Authentication, Authorization, and Accounting (AAA) TACACS window displays a list of all configured policies in tabular form.

Table 85 describes the type of information displayed under each column in the table.

Table 85: AAA TACACS Policy List Column Headings

Column Heading	Description
Policy Name	Displays the name assigned to the AAA TACACS policy when it was initially created. The name cannot be modified.
Accounting Access Method	Displays the connection method used to access the AAA TACACS accounting server. Possible values on display include: • All • Console • Telnet • SSH
Authentication Access Method	Displays the method used to access the AAA TACACS authentication server. Possible values on display include: • All • Console • Telnet • SSH • Web
Authorization Access Method	Displays the method used to access the AAA TACACS authorization server. Possible values on display include: • All • Console • Telnet • SSH

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the AAA TACACS policy entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a policy to modify it.
  - Select 🗑 associated with a policy to delete it.
- Select + to configure a new AAA TACACS policy.

Related Links

Configure an AAA TACACS Policy on page 263

Configure an AAA TACACS Policy

To create, modify, or delete an AAA TACACS policy:

1. Go to **Policies** > **AAA TACACS**.
2. Choose from the following actions:
   - Select + to configure a new AAA TACACS policy. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy to modify it.
     - Select 🗑 associated with a policy to delete it.
3. Enter a **Name** for the policy. The name can be up to 32 characters in length.
4. Select **Add** to create the policy.

   The **Server Info** tab displays by default.
5. Configure AAA TACACS policy parameters under the **Server Info** and **Settings** tabs.

   > **Note**
   > If you exit the AAA TACACS policy configuration without first saving any settings in the tabs, the new policy you created persists, but only until you log out.

Related Links

Manage AAA TACACS Policies on page 262

Configure AAA TACACS Server Information on page 264

Configure AAA TACACS Settings on page 266

Configure AAA TACACS Server Information

You must be in the process of configuring a new AAA TACACS policy or modifying an existing policy to use this procedure.

Use this procedure to configure or modify server information for an AAA TACACS policy.

1. Choose from the following actions:
   - If you are in the process of configuring a new AAA TACACS policy, proceed to the next step.
   - If you want to edit server information settings for an AAA TACACS policy, go to **Policies** > **AAA TACACS**.

     Select ✎ adjacent to the target AAA TACACS policy. Modify the settings in the Server Info tab in accordance with the steps in this procedure.
2. Select the **Server Info** tab.
3. In the **Authentication** pane, select **Add** to assign an authentication server. Configure the server parameters as described in Table 86 on page 265.
4. In the **Authorization** pane, select the server which is to receive authorization requests. Options include:
   - <None>
   - authenticated-server-host (default)
   - authenticated-server-number

   If you choose **`<None>`** or **`authenticated-server-number`**, select **Add** to assign an authorization server. Configure the server parameters as described in Table 86 on page 265.
5. In the **Accounting** pane, select the server which is to receive accounting requests. Options include:
   - <None>
   - authenticated-server-host (default)
   - authenticated-server-number
   - authorized-server-host
   - authorized-server-number

   If you choose **`<None>`**, **`authenticated-server-number`**, or **`authorized-server-number`**, select **Add** to assign an accounting server. Configure the server parameters as described in Table 86 on page 265.
6. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > Note
   > You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Use the information provided in the following table to complete steps 3 through 5 of this procedure.

Table 86: AAA TACACS Policy - Authentication, Authorization, and Accounting Server Parameters

Parameter	Description
Server Id	Set numerical server index (1 – 2) for the authentication server when added to the list of available TACACS authentication server resources.
Host	Specify the IP address or hostname of the AAA TACACS server.
Port	Define or edit the port on which the AAA TACACS server listens to traffic. The port range is 1 – 65,535. The default port is 49.
Secret	Specify (and confirm) the secret (password) used for authentication between the selected AAA TACACS server and the controller, service platform or access point. By default the secret is displayed as asterisks. To see the secret being entered, or to view it later, select 👁.
Request Timeout	Specify the time for the re-transmission of request packets after an unsuccessful attempt. The default is 3 seconds. If the set time is exceeded, the authentication session is terminated.
Request Attempts	Set the number of connection request attempts to the TACACS server before it times out of the authentication session. The available range is 1 – 10. The default is 3.
Retry Timeout Factor	Set the scaling of retransmission attempts in the range 50 – 200 seconds. The timeout at each attempt is the function of the retry timeout factor and the attempt number. The default value (100) implies a constant timeout on each retry. Smaller values indicate more aggressive (shorter) timeouts. Larger numbers define more conservative (larger) timeouts on each successive attempt. The default is 100.

Related Links

Configure an AAA TACACS Policy on page 263

Configure AAA TACACS Settings on page 266

Configure AAA TACACS Settings

You must be in the process of configuring a new AAA TACACS policy or modifying an existing policy to use this procedure.

Use this procedure to configure or modify settings for an AAA TACACS policy.

1. Choose from the following actions:
    - If you are in the process of configuring a new AAA TACACS policy, proceed to the next step.
    - If you want to edit settings for an AAA TACACS policy, go to **Policies** > **AAA TACACS**.

      Select ✏ adjacent to the target AAA TACACS policy. Modify the settings in the Settings tab in accordance with the steps in this procedure.
2. Select the **Settings** tab.
3. In the **Authentication** pane, configure the parameters as described in Table 87.

Table 87: AAA TACACS Policy Authentication Parameters

Parameter	Description
Authentication Access Method	Specify the connection method(s) for authentication requests. • All – Authentication is performed for all types of access without prioritization. • Console – Authentication is performed only for console access. • Telnet – Authentication is performed only for access through Telnet. • SSH – Authentication is performed only for access through SSH. • Web – Authentication is performed only for access through the Web interface.
Directed Request	Select this option to enable the AAA TACACS authentication server to be used with the '@<server name>' nomenclature. The specified server must be present in the list of defined Authentication servers. This option is disabled by default.

4. In the **Authorization** pane, configure the parameters as described in Table 88.

Table 88: AAA TACACS Policy Authorization Parameters

Parameter	Description
Authorization Access Method	Specify the connection method(s) for authorization requests. • All – Authorization is performed for all types of access without prioritization. • Console – Authorization is performed only for console access. • Telnet – Authorization is performed only for access through Telnet. • SSH – Authorization is performed only for access through SSH.
Allow Privileged Commands	Select this option to enable privileged commands executed without command authorization. Privileged commands are commands that can alter/ change the authorization server configuration. This Option is disabled by default.

5. In the **Accounting** pane, configure the parameters as described in Table 89.

Table 89: AAA TACACS Policy Accounting Parameters

Parameter	Description
Accounting Access Method	Specify the connection method(s) for accounting requests. • All – Accounting is performed for all types of access without prioritization. • Console – Accounting is performed only for console access. • Telnet – Accounting is performed only for access through Telnet. • SSH – Accounting is performed only for access through SSH.
Authentication Failure	Select this option to enable accounting upon authentication failures. This option is disabled by default.
CLI Commands	Select this option to enable accounting for CLI commands. This option is disabled by default.
Session	Select this option to enable accounting for session start and session stop events. This option is disabled by default.

6. In the **Service Protocol Settings** pane, select **Add**, then configure the parameters as described in Table 90.

Note
A maximum or 5 entries can be made in the **Service Protocol Settings** table.

Table 90: AAA TACACS Policy Service Protocol Parameters

Parameter	Description
Service Name	Provide a 30 character maximum shell service for user authorization.
Service Protocol	Enter a protocol for user authentication using the service.

7. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure an AAA TACACS Policy on page 263

Configure AAA TACACS Server Information on page 264

Application Management Policy

When an application is recognized and classified by the ExtremeWireless WiNG application recognition engine, administrator-defined actions can be applied to that specific application. An Application Management policy defines the rules or actions executed on recognized applications (for example, Facebook) or application-categories (for example, social networking). The following are rules that can be applied and actions that can be taken in an Application Management policy:

- Allow - Allow packets from a specific application or application category, or both.
- Deny - Deny packets from a specific application or application category, or both.
- Mark - Mark packets with DSCP/8021p value from a specific application or application category, or both.
- Rate-limit - Rate limit packets from a specific application or application category, or both.

For each rule defined, a precedence is assigned to resolve conflicting rules for applications and application categories. A deny rule is exclusive, as no other action can be combined with a deny. An allow rule is redundant with other actions, since the default action is allow. An allow rule is useful when you want to deny packets for an application category, but allow a few applications in the same category to proceed. In such a cases, add an allow rule for applications with a higher precedence than a deny rule for that category.

Mark actions will mark packets for a recognized application and category with DSCP/8021p values used for QoS. Rate limits create a rate-limiter applied to packets recognized for an application and category. Inbound and outbound rates can be specified for the rate-limiter, but both are not required. Mark and rate-limit are the only two actions that can be combined for an application and category. All other combinations are invalid.

Related Links

Manage Application Policies on page 269

Manage Application Policies

Go to **Policies** > **Application Management**.

The **Application Policy** window includes:

- A list of configured policies.
- Tools that allow users to manage policies.

View Configured Application Policies

The Application Policy window displays a list of all configured policies in tabular form. The total number of configured policies appears in parentheses.

Table 91 describes the type of information displayed under each column in the table.

Table 91: Application Policy List Column Headings

Column Heading	Description
Name	Displays the name assigned to each listed Application Management policy.
Description	Displays the description assigned to each listed Application Management policy.
Action	See Management Tools.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Application policy list entries in csv format.

- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a policy to modify it.
  - Select 🗑 associated with a policy to delete it.
- Select + to configure a new policy.

Related Links

Application Management Policy on page 268

Configure an Application Policy on page 270

Configure an Application Policy

Use this procedure to create, modify, or delete an Application policy.

1. Go to **Policies** > **Application**.
   If any policies exist, they appear in tabular form in the Application window. The total number of configured policies is shown in parentheses.
2. Choose from the following actions:
   - Select + to create a new Application policy.
     a. Assign a **Name** to the policy (up to 32 characters) to distinguish this Application policy from others with similar attributes.
     b. Select **Add** to create the new policy.
     c. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ adjacent to a policy to modify it. Proceed to the next step.
     - Select 🗑 adjacent to a policy to delete it.
3. Configure the **Basic** parameters and **Application Policy Rules**, then follow the instructions in Apply an Application Policy.

   Note
   If you exit the Application policy configuration without first applying or saving basic settings and rules, the configured policy persists, but only until you log out.

Related Links

Manage Application Policies on page 269

Configure an Application Policy on page 270

Configure a Basic Application Management Policy on page 270

Configure Application Policy Rules on page 273

Apply an Application Policy to the Network on page 277

Configure a Basic Application Management Policy

You must be in the process of configuring a new Application Management policy or modifying an existing policy to use this procedure.

Use this procedure to configure or modify basic settings for an Application Management policy.

1. Choose from the following actions:
   - If you are in the process of configuring a new Application Management policy, proceed to the next step.
   - If you want to edit basic settings for an Application Management policy, go to **Policies** > **Application Management**. Select ✎ adjacent to the target policy. Modify the settings in accordance with the steps in this procedure.
2. Select the **Basic** tab.
3. Enter an **Application Policy Description** in the range 1–80 characters. Highlight the application and category filters to differentiate this policy from other policies with similar settings.
4. Choose from the **Application Logging** options to enable and filter logging for application-specific packet flows. Set the parameters as described in Table 92.

Table 92: Application Logging Parameters

Parameter	Description
Enable Logging	Select this option to enable DPI application recognition logging. This feature is by disabled by default. DPI is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When enabled, DPI inspects packets of all flows to identify applications (such as, Netflix, Twitter, Facebook) and extract metadata (such as, host name, server name, TCP-RTT) for further use by the ExtremeWireless WiNG firewall.
Enable Logging Level	This option invokes logging of application events by severity, and is enabled by default when **Enable Logging** is enabled. Select a severity level for this Application Management policy. Options include: • **`Notifications`** (default) • **`Emergency`** • **`Alert`** • **`Critical`** • **`Error`** • **`Warning`** • **`Information`** • **`Debug`**

5. Use the **Application Policy Enforcement Time** table to configure an enforcement time period for this Application Management policy. The enforcement time is applicable only to those rules, within the Application Management policy, that do

not have an associated Schedule policy. By default, an Application Management policy is enforced on all days.

Note
Schedule policies are a means of enforcing allow/deny/mark/rate-limit rules at different time periods. If no Schedule policy is applied, all rules within an Application Management policy are enforced at the time specified using this enforcement time command. To configure a Schedule policy for use with this Application Management policy, use the CLI command **`schedule-policy`**, then select the policy while performing the procedure Configure Application Policy Rules on page 273

Select **Add** to populate the table with an enforcement time configuration to activate an Application Management policy based on the current local time. The option to configure an activation period is applicable for a single policy. Configure the time period when the policy is enforced as described in Table 93. If no time enforcement configuration is set, the policy is continually in effect without restriction.

Table 93: Application Policy Enforcement Time Parameters

Parameter	Description
Days	Select the day(s) on which this Application Management policy is to be enforced. Options include: • **`All`** (default) — Enforces the policy continuously. • **`Weekends`** — Enforces the policy only on weekends, between the hours and minutes specified. • **`Weekdays`** — Enforces the policy only on weekdays, between the hours and minutes specified. • **`Monday`** — Enforces the policy only on Monday, between the hours and minutes specified. • **`Tuesday`** — Enforces the policy only on Tuesday, between the hours and minutes specified. • **`Wednesday`** — Enforces the policy only on Wednesday, between the hours and minutes specified. • **`Thursday`** — Enforces the policy only on Thursday, between the hours and minutes specified. • **`Friday`** — Enforces the policy only on Friday, between the hours and minutes specified. • **`Sarurday`** — Enforces the policy only on Sarurday, between the hours and minutes specified.
Start Time	Specify the time of day at which this policy enforcement is to begin. Use the spinner control to set the time using the 24 hr format, where **00.00** represents 24:00 hrs.
End Time	Specify the time of day at which this policy enforcement is to end. Use the spinner control to set the time using the 24 hr format, where **00.00** represents 24:00 hrs.

6. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links
Configure an Application Policy on page 270
Configure Application Policy Rules on page 273

Configure Application Policy Rules

You must be in the process of configuring a new Application policy or modifying an existing policy to use this procedure.

Use this procedure to configure or modify **Application Policy Rules**.

1. Choose from the following actions:
   - If you are in the process of configuring a new Application policy, proceed to the next step.
   - If you want to edit rules settings for an Application policy, go to **Policies** > **Application**. Select ✎ adjacent to the target Application policy. Modify the settings in accordance with the steps in this procedure.
2. Select the **Application Policy Rules** tab.

   A list of configured **Rules** appear in tabular format, if any exist. The total number of configured rules is shown in parentheses.
3. Choose from the following actions:
   - Select + to create a new rule. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a rule to modify it. Edit the parameters in accordance with the steps in this procedure.
     - Select 🗑 associated with a rule to delete it.

4. Configure the parameters as described in Table 94. These parameters apply to all **Action** types: Allow, Mark, Deny, and Rate-Limit.

Table 94: Application Policy Rules Parameters – All Actions

Parameter	Description
Rule Precedence	Set a priority value in the range 1–256 for the application policy rule. The lower the value, the higher the priority assigned to this rule's enforcement action and the category and application assigned. A precedence also helps resolve conflicting rules for applications and categories.
Action	Set the action to be executed on the specified application category and application. Options are: • **`Allow`** (default) — Select to create an Allow rule and configure the match criteria. • **`Mark`** — Select to create a Mark rule and configure the match criteria. Configure Mark specific parameters as described in Table 95 on page 276. • **`Deny`** — Select to create a Deny rule and configure the match criteria. • **`Rate-Limit`** — Select to create a Rate-Limit rule and configure the match criteria. Configure Rate-Limit specific parameters as described in Table 96 on page 276.
Schedule Policy	Associates a schedule policy with the rule. When associated, the rule is enforced only on the days and time configured in the schedule policy. Without the association of a schedule policy, all rules within an application policy are enforced concurrently (defined by the Application Policy Enforcement Time setting under the Basic tab). If scheduling a rule, ensure that the time configured in the schedule policy is a subset of the application policy's enforcement time. In other words, the application policy should be active when the rule is being enforced. For example, if the application policy is enforced on Mondays from 10:00 to 22:00 hours and the schedule policy time-rule is set for Fridays, then this rule will never be hit. When enforcing rules at different times the best practice would be to keep the application policy active at all time (that is, ensure the Application Policy Enforcement Time has not been set, since by default enforcement is continuos). Use the Schedule Policy drop-down menu to select an existing schedule policy to strategically enforce application filter policy rules for specific intervals. This provides stricter, time- and schedule-based access or restriction to specific applications and their parent categories. If no Schedule policy exists or an existing policy does not meet requirements, use the CLI command **`schedule-policy`** to configure one. Otherwise, retain the default value **`<none>`** to use no schedule-based filtering.
App-Category	Specify the application category as the match criteria. Each packet's app-category is matched with the value specified here. In case of a match, the system forwards, drops, marks, or rate-limits the packet, depending on the Action specified. Options are:

Table 94: Application Policy Rules Parameters – All Actions (continued)

Parameter	Description
	• **`All`** (default) — The system forwards all packets regardless of the application category. • **`business`** • **`conference`** • **`custom`** • **`database`** • **`ecommerce`** • **`filetransfer`** • **`gaming`** • **`generic`** • **`im`** • **`industrial`** • **`mail`** • **`mobile`** • **`network management`** • **`other`** • **`p2p`** • **`remote_control`** • **`sharehosting`** • **`social networking`** • **`streaming`** • **`tunnel`** • **`voip`** • **`web`**
Application	Specify the application name. Each packet's application is matched with the application name specified here. In case of a match, the system forwards, drops, marks, or rate-limits the packet, depending on the Action specified. Note: The WiNG system provides approximately 309 canned applications. In addition to these, the database also includes custom-made applications. These are application definitions you can create using the CLI **`application`** command.

If you set the **Action** parameter to **`Mark`**, configure related parameters as described in Table 95.

Table 95: Application Policy Rules Parameters – Mark Action

Parameter	Description
Mark Type	Select the Mark type. Packets that meet the criteria specified in the **Schedule Policy**, **App-Category**, and **Application** fields are marked according to the setting in this field. Options are: • **`8021p`** (default) — Marks packets matching the specified criteria with the 802.1p priority value specified in the **Mark Value** field. The IEEE 802.1p signaling standard enables marking of Layer 2 network traffic. Layer 2 network devices (such as switches), using 802.1p standards, group traffic into classes based on their 802.1p priority value, which is appended to the packet's MAC header. In case of traffic congestion, packets with higher priority get precedence over lower priority packets and are forwarded first. • **`dscp`** — Marks packets matching the specified criteria with DSCP ToS code specified in the **Mark Value** field. The DSCP protocol marks Layer 3 network traffic. Layer 3 network devices (such as routers) using DSCP, mark each Layer 3 packet with a six-bit DSCP code, which is appended to the packet's IP header. Each DSCP code is assigned a corresponding level of service, enabling packet prioritization.
Mark Value	Enter a value representing packet prioritization defined by the **Mark Type** specified, as follows: • If **`8021p`** is specified as Mark Type, enter a value in the range 0–7. • If **`dscp`** is specified as Mark Type, enter a value in the range 0–63.

If you set the **Action** parameter to **`Rate-Limit`**, configure related parameters as described in Table 96.

Table 96: Application Policy Rules Parameters – Rate-Limit Action

Parameter	Description
Enable Outbound Rating	Select this option to enable rate limit action for outbound traffic.
Outbound Max Burst Size	Set the maximum burst size value in the range 2–1024 (Kbytes) for outgoing packets.
Outbound Traffic Rate	Set the rate limit value in the range 50–1000000 (Kbps) for outgoing packets.
Enable Inbound Rating	Select this option to enable rate limit action for inbound traffic.

Table 96: Application Policy Rules Parameters – Rate-Limit Action (continued)

Parameter	Description
Inbound Max Burst Size	Set the maximum burst size value in the range 2–1024 (Kbytes) for incoming packets.
Inbound Traffic Rate	Set the rate limit value in the range 50–1000000 (Kbps) for incoming packets.

5. Select **Add** to create the rule.
6. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure an Application Policy on page 270

Configure a Basic Application Management Policy on page 270

Apply an Application Policy to the Network

Once created and configured, apply the Application policy at the following levels within the network to enforce application assurance:

- RADIUS change of authorization (CoA) usage — From CLI, in device/profile configuration mode, use the `application-policy radius <APP-POLICY-NAME>` command to apply the policy to every user successfully authenticated by the RADIUS server.
- User role — See Configure Roles and Optional Firewall Rules on page 305 for instructions on how to apply the Application policy to all users assigned to the role.
- WLAN — See Configure Wireless LAN Basic Settings on page 107 for instructions on how to apply the Application policy to all users accessing the WLAN.
- Bridge VLAN — See Configure Bridge VLAN General Settings on page 199 to apply the Application policy for the traffic corresponding to the bridged VLAN.

Application Group Policy

An application group policy is a user-defined diverse collection of system-provided and/or user-defined applications and application categories. It consists of multiple applications grouped together to form a collection.

Creating an application group allows you to collectively deny or allow access to a set of applications within a specific application category.

Related Links

Manage Application Group Policies on page 278

Manage Application Group Policies

Go to **Policies** > **Application Group**.

The **Application Group** window includes:

- A list of configured policies.
- Tools that allow users to manage policies.

View Configured Policies

The Application Group window displays a list of all configured policies in tabular form.

Table 97 describes the type of information displayed under each column in the table.

Table 97: Application Group Policy List Column Headings

Column Heading	Description
Name	Displays the name of each user-defined application group.
Description	Displays the description assigned to each listed user-defined application group.
Action	See Management Tools.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Application Group policy entries in csv format.
- Select ⦀ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.

- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an entry to modify it.
  - Select 🗑 associated with an entry to delete it.
- Select + to configure a new policy.

Related Links

Application Group Policy on page 278

Configure an Application Group Policy on page 279

Configure an Application Group Policy

Use this procedure to create, edit, or delete an Application Group policy.

1. Go to **Policies** > **Application Group**.
2. Choose from the following actions:
   - Select + to create a new Application Group policy.
     a. Enter a **Name** (up to 32 characters) for the policy. Ensure that the name uniquely differentiates this policy from existing Application Group policies.
     b. Select **Add** to create the policy.
     c. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy and modify it in accordance with the steps in this procedure.
     - Select 🗑 associated with a policy to delete it.
3. Configure the parameters under the **Details** tab as described in Table 98.

Table 98: Application Group Policy Parameters

Parameter	Description
Description	Enter a description (up to 80 characters) for the policy.
Applications	This field lists all available applications, including those that are system-provided and user-defined. The WiNG software has over 300 built-in applications. You can configure custom applications using the CLI command **`application`**. You can add up to 8 applications to a policy. Select applications using either of the following methods: • Scroll through the list and select the check box adjacent to individual applications to add them to the policy. • Enter an application name in the search field to narrow the list. For example, enter *amazon* to narrow the list to strictly amazon related applications. Then, scroll through the list and select individual applications, or select the checkbox adjacent to the search field to select all the applications.

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Application Group Policies on page 278

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 Links

Configure Auto-Provisioning Policy Rules on page 281

Configure Auto-Provisioning Policy Adoption Criteria on page 285

Configure Auto-Provisioning Policy Rules

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:

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 autoprovisioning policy rule configuration.
Operation	Lists the operation taken upon receiving an adoption request from an access point: The following operations are available: • allow • deny • redirect • upgrade

Setting	Description
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: • 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: • 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: • 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

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

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.

URL Filtering Policy

A URL filter is a Web content filter that is comprised of several filter rules. To construct a filter rule, either Allow or Deny a filter level, category type, category or a custom category. An Allow list bans all sites except those in the categories and URL lists defined in the Allow list. A Deny list allows all sites except the categories and URL lists defined in the Deny list.

URL filtering allows you to enable URL filtering on the device, create and apply a URL filter defining the banned and/or allowed URLs. When enabled, the URL filter is applied to all user-initiated URL requests to determine if the requested URL is banned or allowed. Only if allowed is the user’s request (in the form of a HTTP request packet) forwarded to the Web server.

URL filters can be applied at any of the following points: the user’s application (browser/email reader), the network’s gateway, at the Internet service provider (ISP) end, and also on a Web portal.

For wireless clients, the WLAN infrastructure is the best place to implement these filters. A URL filter is a set of whitelist and/or blacklist rules. The whitelist allows access only to those Websites and URLs specified in it. All other Websites and URLs, apart from those specified in the whitelist, are banned. On the other hand, the blacklist bans all Websites and URLs specified in it. All other Websites and URLs, apart from those specified in the blacklist, are allowed.

To simplify URL filter configuration, Websites have been classified into pre-defined category-types and categories. The system provides 14 category-types and 62 categories. To further simplify configuration, these 14 category-types have been grouped into five (5) pre-defined levels. The actual classification of URLs (on the basis of the pre-defined factors mentioned above) is done by the classification server. A local database also helps by caching URL records for a user-defined time period. The classification server host is specified in the Web filter policy. The Web filter policy also defines the URL database parameters. Use the CLI command **`web-filter-policy`** to configure a Web Filter policy.

The WiNG software also allows you to create URL lists. Each URL list contains a list of user-defined URLs. Use the URL list in a URL filter (whitelist or blacklist rule) to identify the URLs to ban or allow. For example, a URL list named SocialNetworking is created listing the following three sites: Facebook, Twitter, and LinkedIn. When applied to a URL filter’s blacklist these three sites are banned. Whereas, when applied to a whitelist only these three sites are allowed. For more information on configuring a URL list, Configure a URL List Policy on page 483.

Manage URL Filtering Policies

Go to **Policies** > **URL Filtering**.

Configuring a URL Filter policy consists of creating a policy and assigning it a name, then configuring policy rules. The user interfaces used to perform these configuration tasks include:

- A list of configured URL Filter policies or Web Filter Rules.
- Tools that allow users to manage the policies and rules.

View Configured Policies and Rules

Table 99 and Table 100 on page 286 describe the type of information displayed under each column in user interfaces used to perform URL Filter policy configuration tasks.

Table 99: URL Filter Table Column Headings

Column Heading	Description
Policy Name	The name assigned to the URL Filter policy when it was created.
Action	See Management Tools on page 287 for details about the controls under this column.

Table 100: Web Filter Rules Table Column Headings

Column Heading	Description
Precedence	Displays the priority of the rule.
Method	Indicates whether the rule is exclusive (whitelist) or inclusive (blacklist) of all sites except those in the defined Categories and URL Lists.
Filter Type	Displays the filter type in use for the policy. Possible filter types include: • category • category_type • level • url_list
Category	If the Filter Type is set to **`category`**, this column displays the configured category. There are 62 possible categories. Categories are based on an external database, and cannot be modified or removed. Custom categories can be created with the URL List and added to the database.
Category Type	If the Filter Type is set to **`category_type`**, this column displays the configured category type. There are 14 possible category types.

Table 100: Web Filter Rules Table Column Headings (continued)

Column Heading	Description
Level	If the Filter Type is set to `level`, this column displays the configured level. There are 6 possible levels.
URL List	If the Filter Type is set to `url_list`, this column displays the selected URL List which is defined in the URL List policy.
Description	Provides a description of the Web filter rule to help differentiate it from others with similar categories.
Action	See Management Tools for details about the controls under this column.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ⇅1. Toggle the icon to sort the column data in descending order ⇵1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the URL Filter policy entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a policy to modify it.
  - Select 🗑 associated with a policy to delete it.
- Select + to configure a new policy.

Related Links

Configure a URL Filter Policy on page 287
Configure Web Filter Rules on page 288
Configure a URL Error Page on page 291

Configure a URL Filter Policy

Use this procedure to create, modify, or delete a URL Filter policy.

1. Go to **Policies** > **URL Filtering**.
2. Choose from the following actions:
   - Select + to create a new URL Filter policy.
     a. Assign a **Name** to the policy (up to 32 characters) to distinguish this URL Filter from others with similar attributes.

    b. Select **Add** to create the new policy.
    c. Proceed to the next step.

  - From under the **Actions** column:
    - Select ✎ adjacent to a policy to modify it. Proceed to the next step.
    - Select 🗑 adjacent to a policy to delete it.

3. Configure or modify the parameters under the **Web Filter Rules** and **URL Error Page** tabs.

   > **Note**
   > If you exit the URL Filter policy configuration without first saving any settings in the tabs, the configured policy persists, but only until you log out.

Related Links

Manage URL Filtering Policies on page 286
Configure Web Filter Rules on page 288
Configure a URL Error Page on page 291

Configure Web Filter Rules

You must be in the process of configuring a new URL Filter policy or modifying an existing policy to use this procedure.

Use this procedure to configure, modify, or delete **Web Filter Rules** for a URL Filter policy.

1. Choose from the following actions:
   - If you are in the process of configuring a new URL Filter policy, proceed to the next step.
   - If you want to modify or delete Web Filter rules, go to **Policies** > **URL Filtering**. Select ✎ associated with the target URL Filter policy.

     Choose from the following actions:
     - To edit a Web Filter Rule, select ✎ associated with the rule you want to modify. Modify the rule in accordance with the steps in this procedure.
     - To delete a Web Filter Rule, select 🗑 associated with the target rule.

2. Configure the Web Filter Rule parameters as described in Table 101.

Table 101: Web Filter Rule Parameters

Parameter	Description
Precedence	Set a precedence (priority) for the filter rule's in the context of other Web filter rules. Set a value in the range 1 – 500, where 1 is the highest priority and 500 is the lowest priority.
Method	Select either Whitelist or Blacklist to specify whether the rule is for inclusion or exclusion. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.
Filter Type	Use the drop down menu to select from a list of predefined filters to align with the whitelist or blacklist Method designation and the precedence assigned. When you select a given filter type, the drop-down menu associated with that filter type becomes active, and drop-down menus for the other types remain or become inactive. Possible filter types include: • **`category`**: A category is a predefined URL list included in the ExtremeWireless WiNG software. • **`category_type`**: A category type is a set of logically-grouped, predefined categories. • **`level`**: A level is a set of logically-grouped, predefined category types. • **`url_list`**: A URL List is a policy you can configure to customize URL filtering. You can neither change the categories in the category types used for these pre-configured filter levels nor add, modify, or remove the category types mapped to the filter types.
Category	If the Filter Type is **`category`**, use the Category drop-down menu to select a predefined URL category. There are 62 categories available.
Category Type	If the Filter Type is **`category_type`**, use the Category Type drop-down menu to select a predefined category type (adult-content, security-risk, etc.) and either blacklist or whitelist the URLs in that category type. There are 14 category types available.

Table 101: Web Filter Rule Parameters (continued)

Parameter	Description
Level	If the Filter Type is `level`, use the Level drop-down menu to select a predefined level. Options are: · `basic` · `custom` · `high` · `low` · `medium` · `medium-high` Each level is pre-configured to use a set of category types. However, you can create a custom filter level by configuring a URL List policy. When you select `custom`, filtering is based on all the configured URL List policies.
URL List	URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories.
Description	Enter a 80 character maximum description for this Web filter rule to help differentiate it from others with similar category include or exclude rule configurations.

3. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage URL Filtering Policies on page 286
Configure a URL Filter Policy on page 287
Configure a URL Error Page on page 291

Configure a URL Error Page

You must be in the process of configuring a new URL Filter policy or modifying an existing policy to use this procedure.

Use this procedure to define the configuration and layout of a URL error page to be launched when a Web filter rule is invoked and an error page needs to be displayed to a user instead of their expected Web page.

1. Choose from the following actions:
   - If you are in the process of configuring a new URL Filter policy, proceed to the next step.
   - If you want to modify a URL Error Page, go to **Policies** > **URL Filtering**.

     Select ✏ associated with the target URL Filter policy. Edit the URL Error Page settings in accordance with the steps in this procedure.
2. Select the **URL Error Page** tab.
3. Configure the URL Error Page parameters as described in Table 102.

Table 102: URL Error Page Parameters

Parameter	Description
Name	Enter a name (maximum 32 characters) for the title of the blocking page. The name should help convey that this page is launched to prevent the client’s requested page from displaying.
Description	Provide a description (maximum 80 characters) of the page to help differentiate it from other pages with similar page restriction properties.
Page Path	Set the path to the page that is to be sent to the client browser explaining the reason for blocking the client-requested URL. Options are: • **`Internal`** (default): the system generates and sends the page as required, displaying a standard response. • **`External`**: the system sends the page stored on external Web server at the specified URL. This option allows administrators to utilize a customized page. If you choose Internal, review the default standard response settings in the **Internal Page Configuration** pane of the URL Error Page tab. You can modify the standard response settings if necessary. If you choose External, you must provide a link to the external blocking page in the **External Page Location** pane.
External Page URL	If you select External as the Page Path, enter an External Page URL (maximum 511 characters) to be used as the Web link designation of the externally hosted blocking page.
Internal Page Title	Either enter a title (maximum 255 characters) for the URL blocking page or use the default text: *This URL may have been filtered.*

Table 102: URL Error Page Parameters (continued)

Parameter	Description
Internal Page Header	Either enter a header (maximum 255 characters) to be displayed at the top of the URL blocking page or use the default text: *The requested URL could not be retrieved.*
Internal Page Content	Either enter a message (maximum 255 characters) to be displayed in the body (middle portion) of the blocking page or use the default message: *The site you have attempted to reach may be considered inappropriate for access.*
Internal Page Footer	Either enter a footer (maximum 255 characters) to be displayed at the bottom of the URL blocking page or use the default text: *If you have any questions please contact your IT department.*
Internal Page Org Name	Enter the organization name (maximum 255 characters) that is responsible for the URL blocking page. The default name—Your Organizational Name—is not practical, and is included as guideline for customization.
Internal Page Org Signature	Enter a signature (maximum 255 characters) for the organization responsible for the URL blocking page. The default signature—Your Organizational Name, All Rights Reserved—is not practical, and is included as guideline for customization.
Internal Page Logo 1	Provide the location and filename (maximum 255 characters) of a small graphic image to be displayed in the blocking page.
Internal Page Logo 2	Provide the location and filename (maximum 255 characters) of a main graphic image displayed in the blocking page.

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage URL Filtering Policies on page 286

Configure a URL Filter Policy on page 287

Configure Web Filter Rules on page 288

Configure a Device Categorization Policy

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.

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.

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 Links

Add or Edit a DHCPv4 Policy on page 294
Configure DHCPv4 Class Policy on page 295
Configure DHCPv4 Address Pools on page 296

Add or Edit a DHCPv4 Policy

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

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: • 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 Links

DHCPv4 Policy on page 293

Configure DHCPv4 Class Policy on page 295

Configure DHCPv4 Address Pools on page 296

Configure DHCPv4 Class Policy

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.

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 Links

DHCPv4 Policy on page 293

Add or Edit a DHCPv4 Policy on page 294

Configure DHCPv4 Address Pools on page 296

Configure DHCPv4 Address Pools

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.

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: • 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.
   a. Select **Add** to configure the IP address.
   b. 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.
   c. 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 Links

DHCPv4 Policy on page 293

Add or Edit a DHCPv4 Policy on page 294

Configure DHCPv4 Class Policy on page 295

Wireless Client Roles Policy

Define wireless client roles to filter clients' network access based on matching policies. Matching policies (much like ACLs) are sequential collections of *permit* and *deny* conditions that apply to packets received from connected clients. When a packet is received from a client, the controller, service platform or access point compares the packet fields against applied matching policy rules to verify whether the packet has the required permissions to be forwarded. If a packet does not meet the specified criteria, the packet is dropped.

Additionally, wireless client connections are managed by granting or restricting access by specifying a range of IP or MAC addresses to include or exclude from connectivity. These MAC or IP access control mechanisms are configured as Firewall Rules to further refine client filter and matching criteria.

A Wireless Client Roles policy also enables LDAP service, allowing controllers and access points to retrieve user information from the LDAP server. This information is matched with the user-defined role filters to determine if a client matches the role or not, and should be allowed or denied access to the controller managed network.

Related Links

Manage Wireless Client Roles Policies and Roles on page 301

Manage Wireless Client Roles Policies and Roles

Go to **Policies** > **Wireless Client Roles** to view and manage role policies, then select the **Roles** tab to view and manage roles.

The Wireless Client Roles policy and Roles tab windows include:

- A list of configured Wireless Client Roles policies and Roles, if any exist
- Tools that allow users to manage policies

View Configured Policies and Roles

The **Wireless Client Roles** and **Roles** windows display configured policies and roles in tabular form. The total number of configured policies and roles is shown in parentheses.

Table 103 and Table 104 on page 302 describe the type of information displayed under the table column headings.

Table 103: Wireless Client Roles Policy Table Column Headings

Column Heading	Description
Policy Name	Displays the name assigned to the policy when it was initially created.
Action	See Management Tools on page 302 for details.

Table 104: Roles Table Column Headings

Column Heading	Description
Role Name	Displays the name assigned to the client role policy when it was initially created.
Precedence	Displays the precedence number associated with each role. Precedence numbers determine the order in which a role is applied. Roles with lower numbers are applied before those with higher numbers. Precedence numbers are assigned when a role is created or modified. Two or more roles can share the same precedence.
Action	See Management Tools for details.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Wireless Client Roles policy or Roles entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- Under the **Actions** column in the table, choose from the following actions:
  - Select ✎ associated with a policy or role to modify it.
  - Select 🗑 associated with a policy or role to delete it.
- Select + to configure a new policy.

Related Links

Configure a Wireless Client Role Policy on page 303

Configure Roles and Optional Firewall Rules on page 305

Configure a Wireless Client Role Policy

Use this procedure to create, modify, or delete a Wireless Client Roles policy.

1. Go to **Policies** > **Wireless Client Roles**.
2. Choose from the following actions:
   - Select + to create a new Wireless Client Role policy.
     a. Assign a **Name** to the policy (up to 32 characters) to distinguish it from other policies with similar attributes.
     b. Select **Add** to create the new policy.
     c. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy to modify it. Proceed to the next step.

       Note
       You cannot modify the policy name.

     - Select 🗑 associated with a policy to delete it.
3. Configure the parameters under the **LDAP Settings**, **Roles**, and **Default Firewall Rules** tabs, as necessary.

   Note
   If you exit the Wireless Client Role policy user interface without first applying or saving any LDAP Settings, Roles, or Default Firewall Rules, the configured policy persists, but only until you log out.

Related Links

Manage Wireless Client Roles Policies and Roles on page 301
Configure LDAP Settings on page 303
Configure Roles and Optional Firewall Rules on page 305
Configure Default Firewall Rules on page 311

Configure LDAP Settings

Use this procedure to configure LDAP settings for a Wireless Client Roles policy.

1. Choose from the following actions:
   - If you are in the process of configuring a new Wireless Client Roles policy, proceed to the next step.
   - If you want to edit LDAP Settings for an existing policy, go to **Policies** > **Wireless Client Roles**, then select ✎ adjacent to the target policy. Proceed to the next step.

2. Under the **General** pane, configure the LDAP parameters as described in Table 105.

Table 105: General LDAP Parameters

Parameter	Description
LDAP Query	Select to enable LDAP Query service for this Wireless Client Roles policy, then use the drop-down menu to select an LDAP query mode. Options include: • `Internal (Self)` ▯ Select Internal (Self) to use local LDAP server resources configured under the LDAP Server Options pane. • `Through Wireless Controller` ▯ If this option is selected, the AP queries the LDAP server for user information through the controller. Use this option when the AP is Layer 2 adopted to the controller.
Dead Period	Select the Dead Period in the range 60–300 seconds. The LDAP dead period is the interval between two consecutive attempts to bind with the LDAP server.
Timeout	Select a Timeout value in the range 1–5 seconds to specify the allowable delay between a request sent to and response from the LDAP server before LDAP bind and queries will be timed out.

3. Under the **LDAP Server Options** pane, you can modify settings of an existing LDAP server, or select **Add** to add a maximum of two LDAP servers to the list.

   Configure the parameters as described in Table 106.

Table 106: LDAP Server Options Parameters

Parameter	Description
Server ID	Enter the LDAP server ID as either 1 or 2.
Host	Enter the LDAP server's fully qualified domain name or IP address in the **Host** field.
Bind DN	Enter the LDAP server's bind distinguished name.
Base DN	Enter the LDAP server's base distinguished name.
Bind Password	Enter the password for bind. Select 👁 to display the password.
Port	Enter the LDAP server port number. Select a port number in the range 1–65535.
Action	Select 🗑 to delete an LDAP server entry.

4. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > Note
   > You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
>
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
>
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure a Wireless Client Role Policy on page 303

Configure Roles and Optional Firewall Rules on page 305

Configure Default Firewall Rules on page 311

Configure Roles and Optional Firewall Rules

Use this procedure to create, modify, or delete Roles for a Wireless Client Roles policy. This procedure also provides instructions on how to configure firewall rules that apply specifically to a Role. Otherwise, you can configure default firewall rules that apply to all Roles.

1. Choose from the following actions:
    - If you are in the process of configuring a new Wireless Client Roles policy, proceed to the next step.
    - If you want to modify Role Settings or delete a Role associated with a Wireless Client Roles policy, go to **Policies** > **Wireless Client Roles** and select ✎ adjacent to the target policy. Proceed to the next step.
2. Select the **Roles** tab.
3. Choose from the following actions:
    - Select + to create a new Role. Proceed to the next step.
    - From under the **Actions** column:
        - Select ✎ associated with a Role to modify it. Edit the parameters in accordance with the steps in this procedure.
        - Select 🗑 associated with a Role to delete it.
4. Configure the **General** parameters.
5. After the Role and General parameters have been configured and added, optionally select ✎ associated with newly created Role to configure the parameters under the **Firewall Rules** tab.

General

1. If you are creating a new Role, assign it a **Role Name** that differentiates it from others that have similar properties.

    The Role Name cannot exceed 32 characters. The Role Name cannot be modified as part of the edit process.

2. In the **Role Precedence** field, set a numerical precedence value in the range 1–10000.

   Precedence determines the order a role is applied. Roles with lower numbers are applied before those with higher numbers. There is no default precedence for a role, and two or more roles can share the same precedence.

3. Use the **Discovery Policy** drop-down menu to specify the **Bonjour Gateway**.

   Bonjour provides a method to discover services on a LAN. Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

4. In the **Client Identity** field, select the client type to be used as matching criteria within the Wireless Client Roles policy.

   The ExtremeWireless WiNG software provides a set of built-in device fingerprints that load by default and identify client device types. You can create new client identity types or edit existing ones as required, using the CLI command **`client-identity`**.

5. Use the **Match Expressions** parameters to create filter rules based on AP locations, SSIDs and RADIUS group memberships.

Table 107: Match Expressions Parameters

Parameter	Description
AP Location	Use the drop-down menu to specify the location of an access point (AP) matched in a Site (RF domain) configuration or the access point's resident configuration. Select one of the following filter options: • **`Any`** — The role is applied to any AP location. This is the default setting. • **`Exact`** — The role is applied only to APs with the exact location string specified here. • **`Contains`** — The role is applied only to APs whose location contains the location string specified here. • **`Does Not Contain`** — The role is applied only to APs whose location does not contain the location string specified here.
SSID Configuration	Use the drop-down menu to define a wireless client filter option based on how the SSID is specified in a WLAN. Select one of the following options: • **`Any`** — The role is applied to any SSID Location. This is the default setting. • **`Exact`** — The role is applied only when the exact SSID string is specified here. • **`Contains`** — The role is applied only when the SSID contains the string specified here. • **`Does Not Contain`** — The role is applied when the SSID does not contain the string specified here.

Table 107: Match Expressions Parameters (continued)

Parameter	Description
Group Configuration	Use the drop-down menu to define a wireless client filter option based on how the RADIUS group name matches the provided expression. Select one of the following options: • **`Any`** — The role is applied to any RADIUS Group Name. This is the default setting. • **`Exact`** — The role is applied only when the exact RADIUS Group Name string is specified here. • **`Contains`** — The role is applied when the RADIUS Group Name contains the string specified here. • **`Does Not Contain`** — The role is applied when the RADIUS Group Name does not contain the string specified here.
RADIUS User	Use the drop-down menu to define a filter option based on how the RADIUS user name (1-255 characters in length) matches the provided expression. Select one of the following options: • **`Any`** — The role is applied to any RADIUS user name. This is the default setting. • **`Exact`** — The role is applied only when the exact RADIUS user string is specified here. • **`Contains`** — The role is applied when the RADIUS user contains the string specified here. • **`Does Not Contain`** — The role is applied when the RADIUS user does not contain the string specified here. • **`Starts With`** — The role is applied when the RADIUS user starts with the string specified here. • **`Ends With`** — The role is applied when the RADIUS user ends with the string specified here.

6. Use the **Wireless Client Filter** parameter to define a wireless client MAC address filter to be applied to this Role.

   The default value **Any** allows any MAC or MAC Mask address. Disable this parameter to specify a MAC or MAC Mask address.

7. Set the **Captive Portal Connection** parameter to define when wireless clients are authenticated when making a captive portal authentication request.

   Secure guest access is referred to as a captive portal. A captive portal is a guest access policy for providing temporary and restrictive access to the wireless network. Existing captive portal policies can be applied to a WLAN to provide secure guest access.

   Use the drop-down menu to select from the following options:

   - Select **Any** (default) to specify no distinction on whether authentication is conducted before or after the client has logged in.
   - Select **Pre-Login** to conduct captive portal client authentication before the client is logged in.
   - Select **Post-Login** to have the client share authentication credentials after it has logged into the network.
8. Use the **Authentication / Encryption** field to set the authentication and encryption filters applied to this wireless client role.

   The options for both Authentication and Encryption are as follows:

   - **Any** (default) — Select to specify that this Role allows any authentication or encryption type.
   - **Equals** — Select to specify that this Role is applied only when the authentication and encryption types match the exact method(s) specified by your selections. Options include:
     - Authentication
       - **None**
       - **EAP**
       - **MAC**
       - **Kerberos**
     - Encryption
       - **None**
       - **CCMP**
       - **TKIP**
       - **WEB128**
       - **WEB64**
       - **Keyguard**
   - **Not Equals** — Select to specify that this Role is applied only when the authentication and encryption type does not match the exact method(s) specified by your selections. Options are as described above.
9. Select > adjacent to **LDAP Attributes** to expand the display and configure related parameters.

   The following filter criteria apply to each LDAP attribute:

   Any

   Select to specify that this Role is to be applied to any LDAP attribute. This is the default setting.

   Exact

Select to specify that this Role is to be applied only when the LDAP attribute matches the exact string specified here.

Contains

Select to specify that this Role is to be applied only when the LDAP attribute contains the string specified here.

Does Not Contain

Select to specify that this Role is to be applied only when the LDAP attribute does not contain the string specified here.

If you select Exact, Contains, or Does Not Contain criteria, follow the guidelines in the table below to specify LDAP attributes. This Role is applied if the LDAP attributes match your specifications.

Table 108: LDAP Attributes for Role Filtering

Attribute	Description
City	Enter the name (2–31 characters) of the city.
Company	Enter the name (2–31 characters) of the organizational company.
Country	Enter the name (2–31 characters) of the country.
Department	Enter the name (2–31 characters) of the organizational department.
Email	Enter the Email address (2–31 characters).
Employee Id	Enter the employee ID (2–31 characters).
State	Enter the name of the state (2–31 characters).
Title	Enter the name of the job or organizational title (2–31 characters).
Member Of	Enter a description of the group membership (up to 64 characters).

10. Select **Add** to save settings for new configurations, or select **Update** to save modified settings for existing configurations.

Firewall Rules

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic based on inbound and outbound IP and MAC rules.

IP-based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, administrators can filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny, or mark designation to packet traffic.

Use this procedure to configure Firewall Rules to apply specifically to this Role.

> Note
> To configure rules that apply to all Roles, see Configure Default Firewall Rules on page 311.

1. Select the **Firewall Rules** tab to set Inbound and Outbound IP and MAC Firewall rules.
2. Set the **VLAN ID** to a value in the range 1–4094 representing the VLAN used by clients matching the IP or MAC inbound and outbound rules of this policy.
3. Select the appropriate **Application Policy** to use with this firewall rule.

   An application policy defines the rules or actions executed on recognized HTTP (Facebook), enterprise (Webex), and peer-to-peer (gaming) applications or application-categories.
4. Under the **IP Inbound** or **IP Outbound** panes:
   a. Select **Add**.
   b. Choose an **IP Firewall Rules Name** using the drop-down menu.
   c. Assign the rule **Precedence** using the spinner control.

      Rules with lower precedence are always applied first to packets.

   Select 🗑 to remove IP firewall rules.

   If no IP Inbound or Outbound firewall ACL exists, follow the instructions in IPv4 ACL Policy on page 337 to create one.
5. Under the **IPv6 Inbound** or **IPv6 Outbound** panes:
   a. Select **Add**.
   b. Choose an **IP Firewall Rules Name** using the drop-down menu.
   c. Assign the rule **Precedence** using the spinner control.

      Rules with lower precedence are always applied first to packets.

   Select 🗑 to remove IP firewall rules.

   If no IPv6 Inbound or Outbound firewall ACL exists, follow the instructions in latest version of the WiNG Controller Command Reference Guide to create one.
6. Under the **MAC Inbound** or **MAC Outbound** panes:
   a. Select **Add**.
   b. Choose a **MAC Firewall Rules Name** using the drop-down menu.
   c. Assign the rule **Precedence** using the spinner control.

      Rules with lower precedence are always applied first to packets.

   Select 🗑 to remove MAC firewall rules.

   If no MAC Inbound or Outbound firewall ACL exists, follow the instructions in MAC ACL Firewall Policy on page 330 to create one.

7. After you have completed configuring the settings, choose from the following actions:
    a. Select **Revert** to restore default settings or restore the last saved settings.

        Note
        You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

        Note
        This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

        Note
        If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Wireless Client Roles Policies and Roles on page 301
Configure a Wireless Client Role Policy on page 303
Configure LDAP Settings on page 303
Configure Default Firewall Rules on page 311

Configure Default Firewall Rules

Before you begin, configure IP and MAC firewall policies using instructions provided in Wireless Firewall on page 313 and IPv4 ACL Policy on page 337. These are required to complete this procedure.

Use this procedure to define default firewall rules. These firewall rules are applied if no Role-specific firewall rules have been specified.

1. Choose from the following actions:
    - If you are in the process of configuring a new Wireless Client Roles policy, proceed to the next step.
    - If you want to edit Default Firewall Rules settings go to **Policies** > **Wireless Client Roles** and select ✎ adjacent to the target policy, then follow the instructions in the steps in this procedure.
2. Select the **Default Firewall Rules** tab.
3. Configure **IP Inbound**, **IP Outbound**, **MAC Inbound**, or **MAC Outbound** firewall rules, as follows:
    a. Select **Add** to add a rule, or select 🗑 to delete a rule.
    b. Use the drop-down menu to select a pre-configured rule for the Inbound and Outbound **IP Firewall Rules Name** or **MAC Firewall Rules Name** fields.
    c. Use the spinner control to assign the rule **Precedence**.

        Rules with the lowest-numbered precedence are always applied first to packets.

4. After you have completed configuring the settings, choose from the following actions:
    a. Select **Revert** to restore default settings or restore the last saved settings.

        Note
        You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

        Note
        This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

        Note
        If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure a Wireless Client Role Policy on page 303
Configure LDAP Settings on page 303
Configure Roles and Optional Firewall Rules on page 305

Configure an Event System Policy

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

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.

Wireless 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.

Firewall Policies

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

Related Links

Configure a Firewall Policy on page 314
Configure a Basic Firewall Policy on page 315
Configure Firewall Denial of Service (DoS) Policy on page 320
Configure Firewall Storm Control Policy on page 327
Configure Firewall IPv6 Policy on page 329

Manage Firewall Policies

Go to **Policy** > **Wireless Firewall** > **Firewall**.

The **Firewall** window includes:

- A list of configured Firewall policies.
- Tools that allow users to manage Firewall policies.

View Configured Firewall Policies

The Firewall window displays a list of all configured policies in tabular form.

Table 109 describes the type of information displayed under each column in the table.

Table 109: Firewall Policy List Column Headings

Column Heading	Description
Firewall Policy	Displays the name assigned to the policy when created. The name cannot be modified after the policy is created.
Status	Indicates the policy activation status, as follows: • ✓ means the policy is active. • ✗ means the policy is inactive.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Firewall policy entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a policy to modify it.
  - Select 🗑 associated with a policy to delete it.
- Select + to configure a new Firewall policy.

Related Links

Firewall Policies on page 313

Configure a Firewall Policy on page 314

Configure a Firewall Policy

To configure, modify, or delete a Firewall policy:

1. Select **Policies** > **Wireless Firewall** > **Firewall Policy**.
2. Choose from the following actions:
   - Select + to create a new Firewall policy. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy to modify it.
     - Select 🗑 associated with a policy to delete it.
3. Enter a **Name** for the policy.
4. Select **Add** to create the policy.
5. Configure Firewall policy parameters under the **Basic**, **DoS**, **Storm Control**, and **IPv6** tabs, as necessary.

> **Note**
> If you exit the Firewall policy configuration without first saving any policy settings in a tab, the configured policy persists, but only until you log out.

Related Links

Manage Firewall Policies on page 313

Configure a Basic Firewall Policy on page 315

Configure Firewall Denial of Service (DoS) Policy on page 320

Configure Firewall Storm Control Policy on page 327

Configure Firewall IPv6 Policy on page 329

Configure a Basic Firewall Policy

To configure or modify basic Firewall policy settings:

1. Choose from the following actions:
   - If you are in the process of configuring a new Firewall policy, proceed to the next step.
   - If you want to modify basic policy settings, go to **Policy** > **Wireless Firewall** > **Firewall Policy**, then select ✎ adjacent to the policy you want to modify. Proceed to the next step, and modify the basic settings in accordance with the steps in this procedure.
2. Select **Basic** tab.
3. Under the **Firewall Status** pane, configure or modify parameters as described in Table 110.

   The **Firewall Status** feature is enabled by default. Select the toggle to deactivate the firewall status feature.

Table 110: Firewall Status Parameters

Parameter	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.

Table 110: Firewall Status Parameters (continued)

Parameter	Description
IPMAC Conflict Action	Use the drop-down list to select 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 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 in the range 472 – 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 – 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 in the range 1 – 60 seconds applicable to both IPv4 and IPv6 packets. The default value is 1.

Table 110: Firewall Status Parameters (continued)

Parameter	Description
Max Defragmentations/Datagram	Set a value in the range 2 – 8,129 to stipulate the maximum number of defragentations allowed in a datagram before it is dropped. The default value is 140.
Max Fragments/Host	Set a value in the range 1 – 16,384 to stipulate the maximum number of fragments allowed per host before it is dropped. The default value is 8.
Min Length Required	Select **Min Length Required** to set a minimum length in the range 8 – 1,500 bytes to enforce a minimum packet size before being subject to fragment based attack prevention.

4. Under the **Firewall Enhanced Logging** pane, configure or modify the parameters as described in Table 111.

Table 111: Firewall Enhanced Logging Parameters

Parameter	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. Under the **Application Layer Gateway** pane, configure or modify the parameters as described in Table 112 .

Table 112: Firewall Application Layer Gateway Parameters

Parameter	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. Under the **Flow Timeout** pane, configure or modify the parameters as described in Table 113.

   These parameters define flow timeout intervals for the flow types impacting the firewall.

Table 113: Firewall Flow Timeout Parameters

Parameters	Description
TCP Close Wait	Define a flow timeout value in seconds (1 – 32,400). The default setting is 10 seconds.
TCP Established	Define a flow timeout value in seconds (1 – 32,400). The default setting is 5,400 seconds.

Table 113: Firewall Flow Timeout Parameters (continued)

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

7. Under the **TCP Protocol Checks** pane, configure or modify the parameters as described in Table 114.

   All of the TCP Protocol Checks are enabled by default.

Table 114: Firewall TCP Protocol Checks Parameters

Parameter	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. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Firewall Policies on page 313
Configure a Firewall Policy on page 314
Configure Firewall Storm Control Policy on page 327
Configure Firewall IPv6 Policy on page 329

Configure Firewall Denial of Service (DoS) Policy

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 configure or modify a Firewall DoS policy:

1. Choose from the following actions:
   - If you are in the process of configuring a new Firewall policy, proceed to the next step.
   - If you want to modify DoS settings, go to **Policy** > **Wireless Firewall** > **Firewall Policy**, then select ✎ adjacent to the policy you want to modify. Proceed to the next step, and modify the DoS settings in accordance with the steps in this procedure.
2. Select the **DoS** tab.

3. Under the **Settings** pane, configure the DoS event parameters for the wireless controller's firewall, as described in Table 115.

Table 115: Firewall DoS Event Policy Parameters

Parameter	Description
Event	Lists the name of each DoS attack type. See Firewall DoS Event Descriptions on page 322 for a detailed description of each attack type.
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 • 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

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Firewall Policies on page 313

Configure a Firewall Policy on page 314
Configure a Basic Firewall Policy on page 315
Configure Firewall Storm Control Policy on page 327
Configure Firewall IPv6 Policy on page 329

Firewall DoS Event Descriptions

Table 116 provides a summary of each Denial of Service event the firewall can filter.

Table 116: DoS Events for Firewall Filter

DoS Event	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
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

Table 116: DoS Events for Firewall Filter (continued)

DoS Event	Description
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

Table 116: DoS Events for Firewall Filter (continued)

DoS Event	Description
Router Solicit	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). 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
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	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

Table 116: DoS Events for Firewall Filter (continued)

DoS Event	Description
TCP Intercept	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. 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.

Table 116: DoS Events for Firewall Filter (continued)

DoS Event	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

Configure Firewall Storm Control Policy

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 configure or modify Storm Control parameters for a Firewall policy:

1. Choose from the following actions:
   - If you are in the process of configuring a new Firewall policy, proceed to the next step.
   - If you want to modify Storm Control settings, go to **Policy** > **Wireless Firewall** > **Firewall Policy**, then select ✎ adjacent to the policy you want to modify. Proceed to the next step, and modify the Storm Control settings in accordance with the steps in this procedure.
2. Select the **Storm Control** tab.
3. Under the **Settings** pane, choose from the following actions:
   - Select **Add** to configure a new Storm Control policy, as described in Table 117.
   - Select 🗑 associated with an existing policy to delete it.

Note
Storm Control policy settings cannot be modified.

Table 117: Storm Control Policy Parameters

Parameter	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

4. Select **Add** to apply Storm Control policy settings.

5. Under the **Logging** pane, choose from the following actions:
   - Select **Add** to configure a new Storm Control Logging policy, as described in Table 118.
   - Select 🗑 associated with an existing policy to delete it.

     Note
     Storm Control Logging policy settings cannot be modified.

Table 118: Storm Control Logging Policy Parameters

Parameter	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

6. Select **Add** to apply Storm Control Logging policy settings.
7. Optionally, repeat the steps in this procedure to create more Storm Control policies and Storm Control Logging policies.
8. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Firewall Policies on page 313
Configure a Firewall Policy on page 314
Configure a Basic Firewall Policy on page 315
Configure Firewall IPv6 Policy on page 329

Configure Firewall IPv6 Policy

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 configure or modify Firewall policy IPv6 settings:

1. Choose from the following actions:
   - If you are in the process of configuring a new Firewall policy, proceed to the next step.
   - If you want to modify Firewall IPv6 settings, go to **Policy** > **Wireless Firewall** > **Firewall Policy**, then select ✎ adjacent to the policy you want to modify. Proceed to the next step, and modify the IPv6 settings in accordance with the steps in this procedure.
2. Select the **IPv6** tab.

   The IPv6 firewall provides support to IPv6 packet streams. The **IPv6 Firewall** 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. Under the **Settings** pane, configure **Event** parameters to activate individual IPv6 unique events, as described in Table 119.

Table 119: IPv6 Event Parameters

Parameter	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

Table 119: IPv6 Event Parameters (continued)

Parameter	Description
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 • 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. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Firewall Policies on page 313
Configure a Firewall Policy on page 314
Configure a Basic Firewall Policy on page 315
Configure Firewall Storm Control Policy on page 327

MAC ACL Firewall Policy

Access points can use MAC based firewalls like Access Control Lists (ACLs) to filter and mark packets based on the IP from which they arrive, as opposed to filtering packets on Layer 2 ports.

Optionally, filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.

Note
Once defined, a set of MAC firewall rules must be applied to an interface to be a functional filtering tool.

Manage MAC ACL Policies and Rules

Go to **Policies** > **Wireless Firewall** > **MAC ACL**.

Configuring a **MAC ACL** policy consists of creating a policy and assigning it a name, then configuring policy rules under the **ACL Settings** and **EX3500 MAC ACL** tabs. The user interfaces used to perform these configuration tasks include:

- A list of configured policies or rules in tabular form.
- Tools that allow users to manage the policies or rules.

View Configured Policies and Rules

Table 120 and Table 121 on page 331 describe the type of information displayed under each column in the user interfaces used to perform MAC ACL policy configuration tasks.

Table 120: MAC ACL Policy List Column Headings

Column Heading	Description
Policy Name	Displays the name assigned to the policy.

Table 121: ACL Settings Rules and EX3500 MAC ACL Rules List Column Headings

Column Heading	Description
Precedence	Displays the assigned precedence value. Rules assigned with lower values are applied first.
Rules	Displays a summary of the rule settings. • ✗ means that a packet matching the rule settings is to be denied. • ✓ means that a packet matching the rule settings is to be allowed.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.

- Select ⤓ to download the table entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- Under the **Actions** column, choose from the following actions:
  - Select ✎ associated with a list entry to modify it.
  - Select 🗑 associated with a list entry to delete it.
- Select + to configure a new policy or rule.

Related Links

Configure a MAC ACL Policy on page 332
Configure MAC ACL Policy Rules on page 332
Configure EX3500 MAC ACL Policy Rules on page 335

Configure a MAC ACL Policy

Use this procedure to configure, edit, or delete a MAC ACL policy.

1. Go to **Policies** > **Wireless Firewall** > **MAC ACL**.
2. Choose from the following actions:
   - Select + to create a new MAC ACL policy.
     a. Assign a **Name** to the policy (up to 32 characters) to distinguish this MAC ACL policy from others with similar attributes.
     b. Select **Add** to create the new policy.
     c. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy to modify it. Edit the parameters in accordance with the steps in this procedure.
     - Select 🗑 associated with a policy to delete it.
3. Configure the policy rules under the **ACL Settings** or **EX3500 MAC ACL** tabs, as necessary.

   > Note
   > If you exit the MAC ACL policy configuration without first adding and saving any policy rules, the configured policy persists, but only until you log out.

Related Links

Manage MAC ACL Policies and Rules on page 331
Configure MAC ACL Policy Rules on page 332
Configure EX3500 MAC ACL Policy Rules on page 335

Configure MAC ACL Policy Rules

Use this procedure to configure, edit, or delete MAC ACL policy rules.

1. Choose from the following actions:
   - If you are in the process of configuring a new MAC ACL policy, select the **ACL Settings** tab and proceed to the next step.

- If you want to add, edit, or delete a rule for an existing MAC ACL policy, go to **Policies** > **Wireless Firewall** > **MAC ACL**.

  Select ✎ adjacent to the target MAC ACL policy, then select the **ACL Settings** tab. Choose from the following actions:

  - To edit a MAC ACL policy rule, select ✎ adjacent to the rule you want to modify. Modify the rule in accordance with the steps in this procedure.
  - To delete a policy rule, select 🗑 adjacent to the target rule.
  - To create a new rule for the policy, proceed to the next step.

2. Select + to create a new rule.
3. Configure the **Rule** parameters as described in Table 122.

Table 122: ACL Settings Rule Parameters

Parameter	Description
Allow	Every MAC ACL firewall rule is made up of matching criteria rules. The **Allow** action defines what to do with the packet if it matches the specified criteria. The following actions are supported: • **Deny**: Instructs the firewall to prevent a packet from proceeding to its destination. • **Permit**: Instructs the firewall to allow a packet to proceed to its destination.
VLAN ID	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). The VLAN ID can be from 1 – 4094.
Match 802.1P	Configures IP DSCP to 802.1p priority mapping for untagged frames. Set a value in the range 0 – 7.
Source and Destination MAC	Enter both **Source MAC** and **Destination MAC** addresses. Access points use the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.
Actions	The following actions are supported: • **Log**: Events are logged for archive and analysis. • **Mark**: Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. ◦ VLAN 802.1p priority. ◦ DSCP bits in the IP header. • Mark, Log - Conducts both mark and log functions.
Attribute to Mark	This parameter appears if **Mark** is selected for the **Actions** parameter. Select **8021p** or **dscp**.

Table 122: ACL Settings Rule Parameters (continued)

Parameter	Description
Traffic Class	Select this parameter to enable filtering using traffic class. Specify a **Traffic Class** value in the range 1 – 10.
Precedence	Specify a **Precedence** for this MAC firewall rule between 1 – 1500. Rules with lower precedence are always applied first to packets.
Ether Type	An Ether type is a two octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame. Specify an **Ether Type**. Options are: • Other • ipv4 • arp • rarp • appletalk • aarp • mint • wisp • ipx • 802.1q • ipv6
Ether Value	This parameter appears if **Other** is selected for the **Ether Type** parameter. Enter an **Ether Value** in the range 1 – 5,535
Description	Provide a **Description** (up to 64 characters) for the rule to help differentiate it from others with similar configurations.

4. Select **Add** to add the rule.
5. Optionally, repeat the steps in this procedure to add more policy rules.
6. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
>
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage MAC ACL Policies and Rules on page 331
Configure a MAC ACL Policy on page 332
Configure EX3500 MAC ACL Policy Rules on page 335

Configure EX3500 MAC ACL Policy Rules

Use this task to configure, edit, or delete EX3500 MAC ACL policy rules.

1. Choose from the following actions:
   - If you are in the process of configuring a new MAC ACL policy, select the **EX3500 MAC ACL** tab and proceed to the next step.
   - If you want to add, edit, or delete a rule for an existing EX3500 MAC ACL policy, go to **Policies** > **Wireless Firewall** > **MAC ACL**.

     Select ✎ adjacent to the target MAC ACL policy, then select the **EX3500 MAC ACL** tab. Choose from the following actions:
     - To edit an EX3500 MAC ACL policy rule, select ✎ adjacent to the rule you want to modify. Modify the rule in accordance with the steps in this procedure.
     - To delete a policy rule, select 🗑 adjacent to the target rule.
     - To create a new rule for the policy, proceed to the next step.
2. Select + to create a new rule.
3. Configure the **Rule** parameters as described in Table 123.

Table 123: EX3500 MAC ACL Rule Parameters

Parameter	Description
Allow	Every EX3500 MAC ACL firewall rule is made up of matching criteria rules. The **Allow** action defines what to do with the packet if it matches the specified criteria. The following actions are supported: • **Deny**: Instructs the firewall to prevent a packet from proceeding to its destination. • **Permit**: Instructs the firewall to allow a packet to proceed to its destination.
VLAN ID	Enter a **VLAN ID** (1 – 4094) that is representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server).
VLAN Mask	Enter a VLAN ID bit mask value.

Table 123: EX3500 MAC ACL Rule Parameters (continued)

Parameter	Description
Source and Destination MAC	Enter both **Source MAC** and **Destination MAC** addresses. Access points use the source MAC address and destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.
Ether Type	Specify an **Ether Type**. An Ether Type is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame. Select a value in the range 0 – 65535. This parameter is enabled by default. The default value is 1.
Ether Mask	Specify the **Ether Mask**. Select a value in the range 0 – 65535. This field is enabled by default. The default value is 1.
Packet Type	Identify the Packet Type. Options are: • All • Tagged-Eth2 • Untagged-Eth2
Time Range	Select a **Time Range** during which this ACL is to be enabled. The time range must be predefined through CLI using the command `ex3500 time-range <TIMERANGE-NAME>`.
Precedence	Specify a **Precedence** for this MAC firewall rule. Enter a value in the range 1 – 5000. Rules with lower precedence values are always applied first to packets.

4. Select **Add** to add the rule.
5. Optionally, repeat the steps in this procedure to add more policy rules.
6. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage MAC ACL Policies and Rules on page 331
Configure a MAC ACL Policy on page 332
Configure MAC ACL Policy Rules on page 332

IPv4 ACL Policy

IP-based firewalls function like Access Control Lists (ACLs) to filter or mark packets, as opposed to filtering packets on Layer 2 ports.

IP-based Firewall rules are specific to source and destination IP addresses and the unique rules and precedence definitions assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying an IP ACL. Firewall rules are processed by a firewall supported device from first to last. When a rule matches the network traffic a controller or service platform is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

> Note
> Once defined, a set of IP firewall rules must be applied to an interface to be a functional filtering tool.

There are separate policy creation mechanisms for IPv4 traffic. With IPv4, if you intend to deny specific types of packets, best practice is to create access rules for traffic entering a controller, service platform, or access point interface before the controller, service platform, or access point spends time processing them. This is because access rules are processed before other types of firewall rules.

Manage IPv4 ACL Policies

Go to **Policies** > **IPv4 ACL**.

Configuring an IPv4 ACL policy consists of creating a policy and assigning it a name, then configuring policy rules. The user interfaces used to perform these configuration tasks include:

- A list of configured policies or rules in tabular form.
- Tools that allow users to manage the policies or rules.

View Configured Policies and Rules

Table 124 and Table 125 on page 338 describe the type of information displayed under each table column in the user interfaces used to perform IPv4 ACL policy configuration tasks.

Table 124: IPv4 ACL Policy Table Column Headings

Column Heading	Description
Policy Name	Displays the name assigned to the policy.
Action	See Management Tools on page 339 for details.

Table 125: IPv4 ACL Policy Rules Table Column Headings

Column Heading	Description
Precedence	Displays the assigned precedence value. Rules assigned with lower values are applied first.
Allow	Identifies whether packets that meet the criteria stipulated in the rule are to be allowed or denied. • ✓ indicates Allow • ✗ indicates Deny
DNS Name	Displays the assigned **DNS Name**.
DNS Match Type	Identifies the assigned DNS match criteria. Possible entries are **exact**, **suffix**, or **contains**. If no DNS Name is specified, the entry in this column is **Not Set**.
Source	Displays the source IP address used as basic matching criteria for this IP ACL rule.
Destination	Identifies the characteristics of the filtered packet destinations for this IP firewall rule. Possible entries are **any**, **alias**, **host**, or **network**.
Protocol	Displays the configured Protocol. Possible
Source Port	Applies only when TCP or UDP Protocol is configured. Identifies whether the source port for incoming IP ACL rule application is **any**, **equals**, or an administrator defined range. If you are not using tcp or udp, this setting displays as N/A.
Destination Port	Applies only when TCP or UDP Protocol is configured. Identifies whether the destination port for outgoing IP ACL rule application is **any**, **equals**, or an administrator defined range. If you are not using tcp or udp, this setting displays as N/A.
ICMP Type	Applies only when ICMP Protocol is configured. Displays the assigned ICMP Type value.
ICMP Code	Applies only when ICMP Protocol is configured. Displays the assigned ICMP Code value.
Start VLAN	Displays the beginning numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
End VLAN	Displays the end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.

Table 125: IPv4 ACL Policy Rules Table Column Headings (continued)

Column Heading	Description
Log	Indicates whether event logging for this rule's usage is enabled. • ✓ indicates Enabled • ✗ indicates Disabled
Enable	Indicates whether the policy rule is enabled. • ✓ indicates Enabled • ✗ indicates Disabled
Description	Lists the administrator assigned description applied to the IP ACL rule.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the IPv4 ACL policy entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an entry to modify it.
  - Select 🗑 associated with an entry to delete it.
- Select + to configure a new policy or rule.

Related Links

IPv4 ACL Policy on page 337

Configure an IPv4 Policy on page 339

Configure IPv4 ACL Policy Rules on page 340

Configure an IPv4 Policy

Use this procedure to configure, edit, or delete an IPv4 ACL policy.

1. Go to **Policies** > **IPv4 ACL**.
2. Choose from the following actions:
   - Select + to create a new IPv4 ACL policy. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy to modify it.

- Select 🗑 associated with a policy to delete it.

3. Enter a **Name** for the policy.
4. Select **Add** to save the policy.
5. Configure IPv4 policy rules under the **General** window.

> Note
> If you exit the IPv4 ACL policy configuration without first adding and saving any policy rules, the configured policy persists, but only until you log out.

Related Links

Manage IPv4 ACL Policies on page 337
Configure IPv4 ACL Policy Rules on page 340

Configure IPv4 ACL Policy Rules

Use this procedure to configure, edit, or delete IPv4 ACL policy rules.

1. Choose from the following actions:
   - If you are in the process of configuring a new IPv4 ACL policy, proceed to the next step.
   - If you want to add, edit, or delete a rule for an existing IPv4 ACL policy rule, go to **Policies** > **IPv4 ACL**.

     Select ✎ adjacent to the target IPv4 ACL policy. Choose from the following actions:
     - To edit an IPv4 ACL policy rule, select ✎ adjacent to the rule you want to modify. Modify the rule in accordance with the steps in this procedure.
     - To delete a policy rule, select 🗑 adjacent to the target rule.
     - To create a new rule for the policy, proceed to the next step.
2. Select + to create a new rule.
3. Configure the **Rule** parameters as described in Table 126.

Table 126: IPv4 ACL Policy Rule Parameters

Parameter	Description
Precedence	Assign a **Precedence** value for this IP policy in the range 1 – 5000. Rules with lower precedence are always applied to packets first. If you are modifying a precedence to apply a higher integer—and assuming the rule table is sorted with highest precedence first—the rule will move down the table to reflect its lower priority.
Allow	Every IPv4 ACL rule consists of matching criteria rules. The **Allow** parameter defines the packet's disposition if it matches the specified criteria. The following actions are supported: • Deny: Instructs the firewall to restrict a packet from proceeding to its destination. • Allow: Instructs the firewall to allow a packet to proceed to its destination.

Table 126: IPv4 ACL Policy Rule Parameters (continued)

Parameter	Description
Source	Select the source IP address used as basic matching criteria for this IP ACL rule.
Destination	Determine the characteristics of the filtered packet destinations for this IP firewall rule. Select the corresponding **Destination** setting, as follows: • If the destinations do not require any classification, select **any**. • If the destinations are designated as a set of configurations consisting of protocol and port mappings, select **alias**. Note: Selecting alias requires that a destination network group alias be available or created. • If the destinations are set as a numeric IP address, select **host**. • If the destinations are defined as network IP and mask, select **network**.
Network Service Alias	The Network Service Alias is a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $) and include the protocol as relevant.
Protocol	Set a service alias as a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $) and include the protocol as relevant. Selecting either **`tcp`** or **`udp`** displays an additional set of specific TCP/UDP source and destination port options.
Source Port	If you are using either **`tcp`** or **`udp`** as the protocol, define whether the source port for incoming IP ACL rule application is **`any`**, **`equals`**, or an administrator defined range. This is the data local origination port designated by the administrator. Selecting **`equals`** invokes a drop-down list for selecting a protocol type. Selecting **`range`** invokes spinner controls to set low and high numeric range settings. A source port cannot be a destination port.
Destination Port	If you are using either **`tcp`** or **`udp`** as the protocol, define whether the destination port for outgoing IP ACL rule application is **`any`**, **`equals`**, or an administrator defined range. This is the data destination virtual port designated by the administrator. Selecting **`equals`** invokes a drop-down list for selecting a protocol type. Selecting **`range`** invokes spinner controls to set low and high numeric range settings. A source port cannot be a destination port.
ICMP Type	Selecting **`ICMP`** as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. The *Internet Control Message Protocol* (ICMP) uses messages identified by numeric type. ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10.

Table 126: IPv4 ACL Policy Rule Parameters (continued)

Parameter	Description
ICMP Code	Selecting `ICMP` as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding code, helpful for troubleshooting network issues, for example *0 - Net Unreachable*, *1 - Host Unreachable*, and *2 - Protocol Unreachable*.
Description	Lists the administrator assigned description applied to the IP ACL rule.
Start VLAN	Select **Start VLAN** to set a start VLAN range for this IP ACL filter. The Start VLAN represents the virtual LAN beginning numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
End VLAN	Select **End VLAN** to set (apply) an end VLAN range for this IP ACL filter. The End VLAN represents the virtual LAN end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
Log	Select **Log** to enable or disable event logging for this rule’s usage.
Enable	Select **Enable** to include this rule with the IP firewall policy.

4. Select **Add** to add the rule.
5. Optionally, repeat the steps in this procedure to add more policy rules.
6. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage IPv4 ACL Policies on page 337

Configure an IPv4 Policy on page 339

Imagotag Policy

SES-imagotag’s ESL *(Electronic Shelf Label)* tags are small, battery-powered devices used by retail businesses to display information, such as product code and pricing.

These tags are activated, configured, and managed through an SES-Imagotag provided server. The tags and server communicate through an ESL communicator (a USB dongle), connected to the USB port on a ExtremeWireless WiNG AP. This communication is over the 2.4 GHz band using a proprietary RF protocol. The ESL communicator acts as a bridge between the tags and the server, using a ExtremeWireless WiNG AP as an infrastructure device.

Use this policy to enable support for SES-imagotag's ESL tags on ExtremeWireless WiNG APs with USB interfaces. An Imagotag-enabled AP recognizes the ESL communicator, and facilitates communication between communicator and tags.

Note
This feature is supported only on the AP-8432 model access point.

Related Links

Manage Imagotag Policies on page 343

Manage Imagotag Policies

Go to **Policies** > **Imagotag**.

The **Imagotag** window includes:

- A list of configured policies.
- Tools that allow users to manage policies.

View Configured Policies

The Imagotag window displays a list of all configured policies in tabular form, if any exist. The total number of configured policies displays in parentheses.

Table 127 describes the type of information displayed under each column in the table.

Table 127: Imagotag Policy Table Column Headings

Column Heading	Description
Imagotag Name	Displays the Imagotag policy name.
Enable	Displays the status of the policy as follows: • ✓ — indicates that the policy is enabled • ✗ — indicates that the policy is disabled
Channel	Displays the channel assigned for ESL communicator to tag communication in the 2.4 GHz band.
Window Size	Displays the transmission window size for messages exchanged between ESL communicator and tags.
Payload Size	Displays the maximum payload size in packets exchanged between ESL communicator and tags.
Output Power	Displays the maximum output power set for the ESL communicator.

Table 127: Imagotag Policy Table Column Headings (continued)

Column Heading	Description
SSL	Indicates whether Secure Socket Layer (SSL) encryption mode of communication is enabled, as follows: • ✓ — indicates that SSL encryption is enabled • ✗ — indicates that SSL encryption is disabled
FCC-Mode	Indicates whether the FCC compatibility mode is enabled on the ESL communicator, as follows: • ✓ — indicates that FCC compatibility mode is enabled • ✗ — indicates that FCC compatibility mode is disabled

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Imagotag policy entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a policy to modify it.
  - Select 🗑 associated with a policy to delete it.
- Select + to configure a new policy.

Related Links

Imagotag Policy on page 342

Configure an Imagotag Policy on page 344

Configure an Imagotag Policy

Use this procedure to configure, edit, or delete an Imagotag policy.

1. Go to **Policies** > **Imagotag**.
2. Choose from the following actions:
   - Select + to create a new Imagotag policy.
     a. Assign a **Name** to the policy (up to 32 characters) to distinguish this Imagotag policy from others with similar attributes.
     b. Select **Add** to create the new policy.
     c. Proceed to the next step.

- From under the **Actions** column:
  - Select ✏ associated with a policy to modify it. Edit the parameters in accordance with the steps in this procedure.
  - Select 🗑 associated with a policy to delete it.

3. Configure or edit the Imagotag policy settings as described in Table 128.

Table 128: Imagotag Policy Parameters

Parameter	Description
Enable	Select to enable the policy.
Channel	Assign a channel for the ESL communicator to tag communication in the 2.4 GHz band. Options are: • **`ACS`** (default) — Enables Auto-Channel Selection mode. • **`0-10`** — Sets the RF channel of operation in the range 0-10.
Window Size	Set the transmission window size for messages exchanged between ESL communicator and tags. Set a value in the range 1–14 bytes. The default value is 14 bytes. Note: SES-Imagotag recommends that you DO NOT change the default setting.
Payload Size	Set the maximum size of the payload in packets exchanged between ESL communicator and tags. Set a value in the range 1–32 bytes. The default setting is 32 bytes Note: SES-Imagotag recommends that you DO NOT change the default setting.
Output Power	Use the spinner control to configure the maximum output power for the ESL communicator. The options are: • **`Level-A`** (default) — Sets the output power to –1 dBm • **`Level-B`** — Sets the output power to –4 dBm • **`Level-C`** — Sets the output power to –6 dBm • **`Level-D`** — Sets the output power to –12 dBm • **`Level-E`** — Sets the output power to 0 dBm • **`Level-F`** — Sets the output power to –2 dBm • **`Level-G`** — Sets the output power to –8 dBm • **`Level-H`** — Sets the output power to –10 dBm Note: SES-Imagotag recommends that you DO NOT change the default setting, which conforms to various country/region specific RF regulations.
SSL	Select to enable secure, encrypted communication over the Secure Socket Layer (SSL) between the AP and SES-imagotag server. This option is disabled by default.
FCC-Mode	Select to enable the Federal Communications Commission (FCC) compatibility mode on the ESL communicator. This option is disabled by default.

Table 128: Imagotag Policy Parameters (continued)

Parameter	Description
IP/Hostname	Specify the Imagotag server's IP address or hostname. The AP initiates communication with the ESL Imagotag server. The AP sends a connection request to the ESL server specified here.
Port	Identify the port on which the Imagotag server is reachable. Enter a port number in the range 0–65535. The default value is 7353.

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Imagotag Policies on page 343

Roaming Assist Policy

A Roaming Assist policy enables a group of access points (APs) to constantly monitor a given client's packets and received signal strength indicator (RSSI) to determine which among them is the optimal AP for the client to use for roaming. The system then forces the client to connect to the optimal AP.

Specify a roaming aggressiveness value for wireless clients. Configuring this value increases the client’s roaming capabilities in scenarios where the client’s location is likely to change drastically and suddenly. For example, when a client hops on to a train that speeds up quickly. In such a scenario, the AP receives a maximum of 2 (two) messages from the client that have a relatively low RSSI values. This results in a decaying-average, which is above the specified handover-threshold value. Consequently, the client is unable to roam.

Related Links

Manage Roaming Assist Policies on page 347

Manage Roaming Assist Policies

Go to **Policies** > **Roaming Assist**.

The **Roaming Assist** window includes:

- A list of configured Roaming Assist policies.
- Tools that allow users to manage policies.

View Configured Roaming Assist Policies

The Roaming Assist window displays a list of all configured policies in tabular form. The total number of policies is shown in parentheses.

Table 129 describes the type of information displayed under each column in the table.

Table 129: Roaming Assist Policy Table Column Headings

Column Heading	Description
Policy Name	Displays the name of configured Roaming Assist policies. This is the name assigned to each listed policy when it was created. A policy name cannot be modified after the policy is saved.
Action	See Management Tools.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of policies in the table.
- Select ⤓ to download the policy entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with a policy to modify it.
  - Select 🗑 associated with a policy to delete it.
- Select + to configure a new policy.

Related Links

Roaming Assist Policy on page 346

Configure a Roaming Assist Policy on page 348

Configure a Roaming Assist Policy

Use this procedure to create, modify, or delete a Roaming Assist policy.

1. Go to **Policies** > **Roaming Assist**.

   If any policies exist, they appear in tabular form in the Roaming Assist window. The total number of configured policies is shown in parentheses.
2. Choose from the following actions:
   - Select + to create a new Roaming Assist policy.
     a. Assign a **Name** to the policy (up to 32 characters) to distinguish this Roaming Assist policy from others with similar attributes.
     b. Select **Add** to create the new policy.
     c. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ adjacent to a policy to modify it. Proceed to the next step.
     - Select 🗑 adjacent to a policy to delete it.

3. Configure the **Basic** parameters as described in Table 130.

Table 130: Roaming Assist Policy Parameters

Parameter	Description
Action	Specify the action to be invoked on the client once it reaches the specified threshold value. The threshold values are configured based on the client load. Options are: • **`assisted-roam`** — Provides 802.11v assisted roaming facility to the client • **`deauth`** (default) — De-authenticates the client. • **`log`** — Generates a log Note: In all three cases an event is generated. However, the message generated differs and is based on the action specified.
Aggresiveness	Set a roaming aggressiveness value for wireless clients. Options are: • **`Highest`** — De-authenticates the client in case of any degradation in the client's link quality. When selected, the access point considers only the RSSI value of the last message received from the client. • **`Lowest`** (default) — De-authenticates the client only in case of significant degradation in the client's link quality. With this option, the access point uses a weighted average [80% of decaying average + 20% of last seen RSSI] as the final reported RSSI value. • **`Medium`** — This is an intermediate setting between not roaming and performance. • **`Medium-High`** — Allows roaming even if performance degrades. With this option, the AP calculates the client's signal strength based on average received signal as well as last received signal level, weighted towards the last received value. • **`Medium-Low`** — Allows roaming even if performance becomes average. With this option, the AP calculates the client's signal strength based on average received signal as well as last received signal level, weighted towards the average value.
Detection Threshold	Assign a detection threshold RSSI value determining when a client is monitored. Clients with poor RSSI values are monitored more frequently. Set an RSSI value in the range –100 dBm to –40 dBm. The default is –75 dBm.
Disassociation Time	Specify the interval after which a disassociation message is to be sent. Set a value in the range 1–10 seconds. The default value is 5 seconds.
Handoff Count	Specify the number of times a client can exceed the configured **Handoff Threshold** value before an action is invoked. Enter a value in the range 1–10. The default value is 3.

Table 130: Roaming Assist Policy Parameters (continued)

Parameter	Description
Handoff Threshold	Assign a threshold RSSI value determining when client handoff action is to be taken. When a client's detected RSSI exceeds the value set here and meets the value set in **Handoff Count**, an action is invoked. Set an RSSI value in the range –100 dBm to –40 dBm. The default value is -80 dBm. Note: If the client’s RSSI increases beyond the set handoff-threshold, it is removed from the queue for monitoring and action invocation.
Monitoring Interval	Specify the interval (duration) during which clients are monitored to determine whether their RSSI is below the specified **Handoff Threshold**. Set the interval in the range 1–60 seconds. The default value is 5 seconds.
Sampling Interval	Specify the interval between two successive client samplings to determine their RSSI value. Set a sampling interval in the range 5–60 seconds. The default value is 15 seconds. Note: Higher RSSI values, indicate stronger signals.

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Roaming Assist Policies on page 347

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 psuedowire 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 Links

L2TPv3 Configuration on page 351

L2TPv3 Configuration

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:

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

Setting	Description
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.

Configure a BLE Data Export Policy

Before enabling BLE data export:

1. Ensure that the AP's Bluetooth radio is active and the mode is set to `le-sensor`.

   For more information on configuring the Bluetooth settings for an AP's profile, see Manage Bluetooth Configuration on page 157.
2. Perform the procedure Configure a Sensor Policy on page 482 to define the interval at which RSSI data is forwarded from the BLE sensor to the external, third-party server. Next, apply the policy to an RF Domain. See Configure Site Policies on page 59 for instructions.

A BLE Data Export policy enables forwarding of Bluetooth Low Energy (BLE) data to an external, third-party server.

The BLE data export policy provides the external, third-party server's REST URL. After configuring the policy, you must apply it to a Site (RF Domain). Once applied, BLE-enabled WiNG APs within the domain are able to sense BLE iBeacon and Eddystone beacons from other BLE-enabled devices, and forward device data to the specified third-party server. This data is forwarded in JSON format.

1. Go to **Policies** > **BLE Data Export**.

   The BLE Data Export window opens and displays a list of configured policies, if any exist. The total number of configured policies is shown in parentheses.
2. Choose from the following actions:

   a. Select the sort icon ⇅ adjacent to the Policy Name column heading to sort the data. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading the data is currently sorted.

   b. Select ✎ associated with a BLE Data Export policy to modify it.

      Edit the BLE Data Export policy in accordance with the instructions in the steps in this procedure. You cannot edit the **Policy Name**.

c. Select 🗑 associated with a BLE Data Export policy to remove it.

d. Select + to create a new BLE Data Export policy.

   The **Add Policy** pop-up window opens.

   i. Assign a policy **Name**. The name cannot exceed 32 characters.

   ii. Select **Add** to save the policy.

   The **Basic** window opens.

   iii. Configure the BLE Data Export policy in accordance with the instructions in the steps in this procedure.

3. In the **REST** field, enter the URL of the external, third-party server to which you want to send the RSSI feed.
4. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > Note
   > You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

   > Note
   > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

   > Note
   > If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Next, apply the policy to the Site (RF Domain). See Configure Site Policies on page 59 for instructions.

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 363.

Related Links

View Management Dashboard on page 355
Add a New Management Policy on page 357
Edit or Delete a Management Policy on page 374

View Management Dashboard

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

To view and modify existing Management policies:

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 '×' 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 Links

Management Policy on page 354

Add a New Management Policy on page 357

Edit or Delete a Management Policy on page 374

Add a New Management Policy

Create a new management policy.

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.

Set up user account to configure other management policy settings.

Related Links

Management Policy on page 354

View Management Dashboard on page 355

Edit or Delete a Management Policy on page 374

Configure Management User Account

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**.

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

Setting	Description
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: • 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	Lists the role assigned to each listed administrator. An administrator can only be assigned one role at a time Options include: • 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. 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 For more information, see set locations configuration • 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 *not* 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

Setting	Description
	• 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 • 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. 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. 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. Note: The Allowed Location option is not applicable to this role • 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

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:

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	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. Select **Add** to add location to the locations list To edit a location, select the ✏ icon from the action option To delete a location, select the 🗑 icon from the action option

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

Set Access Control Configuration

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:

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
Enable SSH	Select the toggle button to activate SSH device access. The Weak MAC Algo (Algorithm) option is enabled by default.
Activate SSHv2	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	Description
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	Select a user role to set account lockout. The options are: • Device Provisioning admin • Help Desk • Monitor • Network Admin • Rest API User • Security Admin • Superuser • System Admin • Vendor Admin • Web User admin Note: You can set account lockout for multiple roles. After specifying the role, set the Lockout Time and Number of Password Attempts. 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
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

Use this procedure 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.

To configure or edit Management policy Authentication settings:

1. Choose from the following actions:
   - If you are in the process of configuring a new Management policy, proceed to the next step.
   - If you want to edit a Management policy's Authentication settings, go to **Policies** > **Management**. Select ✎ adjacent to the target Management policy. Proceed to the next step.
2. Select the **Authentication** tab.
3. To authenticate management access requests, configure the parameters as described in Table 131.

Table 131: Management Policy Authentication Parameters

Parameter	Description
Local	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 Note: The local authentication mode is enabled by default. Not selecting the local authentication enables the RADIUS and AAA Policy parameters.
RADIUS	If authentication is to be handled by an external RADIUS server, select one of the following options: • 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. 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 • Fallthrough - Select this option to revert to local database authentication in the following scenarios: ◦ If the external RADIUS server is unreachable ◦ If the external RADIUS server rejects the user authentication request 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

Table 131: Management Policy Authentication Parameters (continued)

Parameter	Description
AAA Policy	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 data. The AAA policy points to this external RADIUS server resource Select a policy from the AAA Policy drop-down list
TACACS	If local authentication is disabled, and authentication is to be handled by an external TACACS server, select one of the following options: • **`Authentication`** - Select to enable TACACS authentication on login. • **`Fallback`** - Select this option to revert to local database authentication in case the TACACS server is unreachable. When this option is enabled, TACACS authentication is attempted first. However, if the external TACACS server is unreachable the local database is used to authenticate the user. • **`Fallthrough`** - Select this option to revert to local database authentication in the following scenarios: ◦ If the external TACACS server is unreachable. ◦ If the external TACACS server rejects the user authentication request. When this option is enabled, TACACS authentication is attempted first. However, if the TACACS server is unreachable *or* rejects the authentication request the local database is used to authenticate the user. • **`Accounting`** - Select to enable TACACS accounting on login. • **`Authorization`** - Select to enable TACACS authorization on login. ◦ **`Authorization Fallback`** - Select to enable fallback on TACACS authorization failure. This option is only available when Authorization is selected.
AAA TACACS Policy	If enabling external TACACS server authentication, select the TACACS policy to use. The AAA TACACS policy points to this external TACACS server resource. Select an existing AAA TACACS policy. Otherwise, perform the procedure Manage AAA TACACS Policies on page 262 to create a new policy that you can then select here.

4. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Set SNMP Configuration

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:

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: • 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

4. 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

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

Set SNMP Traps Configuration

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:

1. Select the **SNMP Traps** tab.
2. Select **Enable** Trap Generation to activate trap generation using the trap receiver configuration defined. This feature is not selected by default.
3. 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

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.

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 Links

Management Policy on page 354
View Management Dashboard on page 355
Add a New Management Policy on page 357

Mesh Policy

Mesh Quality of Service (QoS) provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications, then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

Mesh QoS ensures that each mesh point on the mesh network receives a fair share of the overall bandwidth, either equally or per the proportion configured. Packets directed to clients are classified into data types (video, voice, data, and so forth). Packets within each category are processed based on the weight (prioritization) set for each mesh point.

The **Quality of Service** screen displays a list of mesh QoS policies available to mesh points. Each mesh QoS policy can be selected to edit its properties. If none of the exiting Mesh QoS policies supports an ideal QoS configuration for the intended data traffic of this mesh point, select + to create a new policy. Select an existing mesh QoS policy and select ✎ to change the properties of the mesh QoS policy.

Related Links

Configure a Mesh QoS Policy on page 375
Configure a Mesh Point Policy on page 381

Configure a Mesh QoS Policy

Define a mesh QoS policy.

Excessive traffic can cause performance issues or bring down the network. Excessive traffic can be caused by network loops, faulty devices, or malicious software like a worm or virus that has infected one or more devices at the branch. By activating rate limiting, you can limit the maximum rate sent to or received from the wireless network (and mesh point) per neighbor. It prevents any single user from overwhelming the wireless network. It also provides differential service for service providers. You can set separate QoS rate limit configurations for data transmitted from the network and from a mesh point's neighbor back to their associated access point radios and managing controller or service platform.

Before you define rate limit thresholds for mesh point transmit and receive traffic, define the normal number of ARP, broadcast, multicast, and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) is dropped, resulting in intermittent outages and performance problems.

A connected neighbor can also have QoS rate limit settings defined in both the transmit and receive direction.

1. Select **Policies** > **Mesh** > **Mesh QoS**.
2. Select + to create a new mesh QoS policy or ✎ to edit an existing policy.

   The **Rate Limit** dashboard opens.

3. Configure the following parameters for the **From Air Upstream Rate Limit**, or traffic from the controller to associated access point radios and their associated neighbor:

Mesh Tx Rate Limit	Select to activate rate limiting for all data received from any mesh point in the mesh
Rate	Define a receive rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received over the mesh point from all access categories. Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5,000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 and 1,024K bytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the mesh point’s client destinations. By trending the typical number of ARP, broadcast, multicast, and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320K bytes.

4. Set the following **From Air Upstream Random Early Detection Threshold** settings, for each access category:

   An early random drop occurs when a traffic stream falls below the set threshold.

Background Traffic	Set a percentage value for background traffic in the transmit direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator using a time trend analysis. The default threshold is 50%
Best Effort Traffic	Set a percentage value for best effort traffic in the transmit direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator using a time trend analysis. The default threshold is 50%.

Video Traffic	Set a percentage value for video traffic in the transmit direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator using a time trend analysis. The default threshold is 25%
Voice Traffic	Set a percentage value for voice traffic in the transmit direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator using a time trend analysis. The default threshold is 0%

5. Configure the following parameters for the **To Air Downstream Rate Limit**, or traffic from neighbors to associated access point radios and the controller or service platform:

Mesh Rx Rate Limit	Select to activate rate limiting for all data transmitted by the device to any mesh point in the mesh
Rate	Define a transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received over the mesh point (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5,000 kbps
Maximum Burst Size	Set a maximum burst size between 2 and 1,024K bytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the mesh point’s wireless client destinations. By trending the typical number of ARP, broadcast, multicast, and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320K bytes

6. Set the following **To Air Downstream Random Early Detection Threshold** settings, for each access category.

   An early random drop occurs when the number of tokens for a traffic stream falls below the set threshold.

Background Traffic	Set a percentage value for background traffic in the receive direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator using a time trend analysis. The default threshold is 50%
Best Effort Traffic	Set a percentage value for best effort traffic in the receive direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator using a time trend analysis. The default threshold is 50%
Video Traffic	Set a percentage value for video traffic in the receive direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator using a time trend analysis. The default threshold is 25%
Voice Traffic	Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator using a time trend analysis. The default threshold is 0%

7. Configure the following settings for **From Air Upstream Rate Limit** in the **Neighbor Settings** field:

Neighbor Rx Rate Limit	Select to activate rate limiting for data transmitted from the client to its associated access point radio and connected controller or service platform. Enabling this option does not invoke client rate limiting for data traffic in the receive direction
Rate	Define a transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received from all access categories. Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 1,000 kbps
Maximum Burst Size	Set a maximum burst size between 2 and 1,024K bytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 320K bytes

8. Configure the following settings for **From Air Upstream Random Early Detection Threshold** in the **Neighbor Settings** field:

Background Traffic	Set a percentage value for background traffic in the transmit direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50%
Best Effort Traffic	Set a percentage value for best effort traffic in the transmit direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50%
Video Traffic	Set a percentage value for video traffic in the transmit direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 25%
Voice Traffic	Set a percentage value for voice traffic in the transmit direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 0%, which implies that no early random drops will occur

9. Configure the following settings for **To Air Downstream Rate Limit**, or traffic from a controller or service platform to associated access point radios and the wireless client:

Neighbor Tx Rate Limit	Select to activate rate limiting for data transmitted from connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the transmit direction
Rate	Define a transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 1,000 kbps
Maximum Burst Size	Set a maximum burst size between 2 and 1,024K bytes. The smaller the burst, the less likely the receive packet transmission will result in congestion for the wireless client. The default burst size is 320K bytes

10. Set the following **To Air Downstream Random Early Detection Threshold** settings for each access category:

Background Traffic	Set a percentage value for background traffic in the receive direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50%
Best Effort Traffic	Set a percentage value for best effort traffic in the receive direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 50%
Video Traffic	Set a percentage value for video traffic in the receive direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 25%
Voice Traffic	Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold is 0%, which implies that no early random drops will occur

11. Select **Save** to update this mesh QoS rate limit settings.
12. Select **Multimedia Optimizations**.

13. Set the following **Accelerated Multicast** settings:

Disable Multicast Streaming	Select to deactivate all multicast streaming on the mesh point.
Automatically Detect Multicast Streams	Select to have bridged multicast packets converted to unicast to provide better overall airtime utilization and performance. The administrator can either have the system automatically detect multicast streams and convert all detected multicast streams to unicast, or specify which multicast streams are to be converted to unicast. When the stream is converted and being queued up for transmission, a number of classification mechanisms can be applied to the stream. The administrator can choose from the following classification types: **`Trust`**, **`Voice`**, **`Video`**, **`Best Effort`**, and **`Background`**.
Manually Configure Multicast Addresses	Select and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches. Select **Add** and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches

14. Select **Save** to update the Mesh Multimedia Optimizations settings.

Configure a Mesh Point Policy

In MeshConnex systems, a mesh point (MP) is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 MPs can be created and 2 can be created per radio. MPs can be configured to use one or both radios in the device. If the MP is configured to use both radios, the path selection protocols will continually select the best radio to reach each destination. Each MP participates in a single Mesh Network, defined by the MeshID, that is typically a descriptive network name, similar to the SSID of a WLAN. All MPs configured to use the same MeshID attempt to form a mesh and inter-operate. The MeshID allows overlapping mesh networks to discriminate and disregard MPs belonging to different networks.

To configure a mesh point policy:

1. Select **Policies** > **Mesh** > **Mesh Point**.

   The list of existing mesh point policies dashboard opens.

2. Select + to create a new policy, ✎ to edit an existing policy, or 🗑 to delete an existing policy.

   For new policies, the **Add Policy** screen opens.

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

   The **Configuration** dashboard opens.

3. Set the following configuration data:

Mesh ID	The IDs (mesh identifiers) assigned to mesh points
Mesh Point Status	The status of each configured mesh point, either **`Enabled`** or **`Disabled`**
Mesh QoS Policy	The mesh Quality of Service (QoS) policy associated with each configured mesh point
Beacon Format	Specify the format in which beacons from the mesh point are sent. To use access point style beacons, select **`access-point`** from the drop-down list box. To use mesh point style beacons, select **`mesh-point`**. The default value is **`mesh-point`**.
Is Root	Select to define the mesh point as a root in the mesh topology
Control VLAN	Enter the VLAN designated as the dedicated control VLAN for this meshpoint. Specify the VLAN ID (1–4094) for the control VLAN on each of the configured mesh points If VLAN 1 is configured as the control VLAN, ensure that the VLAN is configured in the wired port of all access points belonging to same meshpoint. Note: The designated Control VLAN need not necessarily be added in the **Allowed VLANs** list.
Allowed VLANs	Enter the list of VLANs allowed on each configured mesh point. Specify the VLAN ID (1–4094) or the range of IDs to be managed. When entering a range of IDs, use a hyphen to separate sequential IDs and use a comma to separate non-sequential entries (example: 4-53,59,77,94). Mesh management traffic can be sent over a dedicated VLAN. This dedicated VLAN is known as the control VLAN, and should be configured in the backhaul port of all the access points configured as meshpoint roots. Once configured, the control VLAN carries the mesh point's control traffic.
Neighbor Inactivity Timeout	Specify the amount of time allowed between frames received from a neighbor before their client privileges are revoked. Specify the timeout value between 1 to 86,400 seconds
Description	Descriptive text provided by the administrator for each configured mesh point. Type a 64-character description for the mesh point configuration

4. Select **Save** to update the MeshConnex configuration settings for this policy.
5. Select **Security**.

6. Refer to the **Select Authentication** field to define an authentication method for the mesh policy.

Security Mode	Select a security authentication mode for the mesh point. Select **None** to have no authentication for the mesh point. Select **EAP** to use a secured credential exchange, dynamic keying and strong encryption. If selecting **EAP**, refer to the **EAP PEAP** Authentication field at the bottom of the screen and define the credentials of an EAP user and trustpoint. Select **PSK** to set a pre-shared key as the authentication for the mesh-point. If **PSK** is selected, enter a pre-shared key in the **Key Settings** field

7. Set the following **Key Settings** for the mesh point.

Pre-Shared Key	When the security mode is set as **PSK**, type a 64 character HEX or an 8-63 ASCII character passphrase used for authentication on the mesh point.

8. Set the following **Key Rotation** settings for the mesh point.

Unicast Rotation Interval	Define an interval for unicast key transmission between 30 to 86,400 seconds
Broadcast Rotation Interval	When activated, the key indices used for encrypting or decrypting broadcast traffic is alternatively rotated based on the defined interval. Define an interval for broadcast key transmission in seconds, between 30 to 86,400. Key rotation enhances the broadcast traffic security on the WLAN

9. If you are using EAP to secure the mesh point, set the following **EAP PEAP Authentication** settings:

User ID	Create a 32-character maximum user name for a *peap-mschapv2* authentication credential exchange
Password	Define a 32-character maximum password for the EAP PEAP user ID
Trust Point	Provide the 64 character maximum name of the trustpoint used for installing the CA certificate and validating the server certificate
EAP TLS	Provide the 64 character maximum name of the trustpoint used for installing the client certificate, client private key and CA certificate
Type	Configure the EAP authentication method used by the supplicant. The default EAP type is **HEX**

EAP Identity	Type the 32-character maximum identity string used during phase 1 authentication. This string does not need to represent the identity of the user, rather an anonymous identity string
AAA Policy	Select an existing AAA Policy from the drop-down list box to apply to this user’s mesh point EAP configuration. *Authentication, authorization, and accounting* (AAA) is a framework for intelligently controlling access to the network, enforcing user authorization policies, and auditing and tracking usage. These combined processes are central for securing wireless client resources and wireless network data flows

10. Select **Save** to update the changes made to the configuration.
11. Select **Radio Rates**.

12. Set the following **Radio Rates** for the 2.4 GHz, 5 GHz, and 6 GHz radio bands:

2.4 GHz Mesh Point	Use the drop-down menu to select radio rates for the 2.4 GHz band. Define both minimum `Basic` and optimal `Supported` rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band. These are the rates wireless client traffic is supported within this mesh point. If you are supporting 802.11n, select a Supported MCS index. Set an MCS (*modulation and coding scheme*) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only
5.0 GHz Mesh Point	Use the drop-down menu to select radio rates for the 5.0 GHz band. Define both minimum and optimal rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 5.0 GHz radio band. These are the rates at which wireless client traffic is supported within this mesh point. If you are supporting 802.11n, select a Supported MCS index. Set an MCS (*modulation and coding scheme*) with respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only
6.0 GHz Mesh Point	Use the drop-down menu to select radio rates for the 6.0 GHz band. Define both minimum and optimal rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 6.0 GHz radio band. These are the rates at which wireless client traffic is supported within this mesh point. If you are supporting 802.11n, select a Supported MCS index. Set an MCS (*modulation and coding scheme*) with respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight data rates, bonded channels, multiple spatial streams, different guard intervals, and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only

13. Select **Save** to update the changes made to the configuration.

Bonjour Gateway Policy

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates the devices (printers, computers etc.) and services these computers provide over a local network.

Bonjour provides a method to discover services on a local area network (LAN). Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

Note
Up to eight Bonjour discovery policies can be configured.

Related Links

Manage Bonjour Gateway Policies on page 386

Manage Bonjour Gateway Policies

Go to **Policies** > **Bonjour Gateway**. Select either **Discovery Policy** or **Forwarding Policy**.

Configuring Bonjour Gateway policy consists of configuring discovery policies, forwarding policies, and rules. The user interfaces used to perform these configuration tasks include:

- A list of configured policies or rules.
- Tools that allow users to manage policies or rules.

View Configured Policies and Rules

Table 132, Table 133 on page 386, and Table 134 on page 387 describe the type of information displayed under each column in the user interfaces used to perform Bonjour Gateway policy configuration tasks.

Table 132: Discovery and Forwarding Policy List Column Headings

Column Heading	Description
Policy Name	Displays the name assigned to the policy.

Table 133: Discovery Rules List Column Headings

Column Heading	Description
Service	Displays the service that can be discovered by the Bonjour Gateway.
VLAN Type	Identifies whether the configured **Service VLANs** are either `local` or `tunneled`.

Table 133: Discovery Rules List Column Headings (continued)

Column Heading	Description
Service VLANs	Identifies the VLAN(s) on which the selected service is discoverable.
Instance Name	Displays the instance name (if configured) that the Bonjour service uses in its query of services to be dicovered.

Table 134: Forwarding Rules List Column Headings

Column Heading	Description
From VLANs	Displays the VLAN(s) or VLAN alias where the Apple services are available.
To VLANS	Displays the VLAN(s) or VLAN alias where clients for the services are available.
Rule Id	Identifies the unique ID assigned to the rule.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the policy entries in csv format.
- Select ▮▮▮ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an entry to modify it.
  - Select 🗑 associated with an entry to delete it.
- Select + to configure a new policy or rule.

Related Links

Configure a Bonjour Discovery Policy on page 388

Configure a Bonjour Forwarding Policy on page 390

Configure a Bonjour Discovery Policy

The Bonjour Discovery policy determines how Bonjour services are located. It identifies the VLANs on which the Bonjour services can be found. You can configure a maximum of eight Discovery policies.

1. Go to **Policies** > **Bonjour Gateway** > **Discovery Policy**.

   The **Bonjour Discovery** window opens. If any Discovery policies are configured, they appear in a list in the **Discovery** pane. The total number of configured Discovery policies is shown in parentheses.
2. Choose from the following actions:
   - Select + to create a new Discovery policy. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy to modify it. Modify the parameters in accordance with the steps in this procedure.
     - Select 🗑 associated with a policy to delete it.
3. Enter a **Name** for the policy.
4. Select **Add** to create the policy.

   Note
   If you exit the Discovery policy configuration without first adding and saving any policy rules, the configured policy persists, but only until you log out.
5. Select + to add a new policy rule.
6. Configure the policy rule parameters as described in Table 135.

Table 135: Discovery Policy Rule Parameters

Parameter	Description
Service Name	Define the service that can be discovered by the Bonjour gateway. • Predefined – Use the drop-down menu to select from a list of predefined Apple services (Scanner, Printer, HomeSharing etc.). • Alias – Use an existing alias to define a service that is not available in the predefined list.
VLAN Type	Use the drop-down menu to select the VLAN type. • `local` – The VLAN(s) defined in the **Service VLAN** field use a local bridging mode. • `tunneled` – The VLAN(s) defined in the **Service VLAN** field are shared tunnel VLANs.

Table 135: Discovery Policy Rule Parameters (continued)

Parameter	Description
Service VLANs	Enter a VLAN or a list of VLANs on which the selected service is discoverable. Specify a VLAN ID (1–4094). When specified, Bonjour discovery queries are delivered to all clients on the specified VLANs. Applicable only if enabling Bonjour Services discovery on local VLANs.
Instance Name	Optionally, specify the selected Bonjour service's instance name. When specified, the Bonjour service discovery queries contain the instance name. of the service to be discovered. You can either directly specify the string value to be used as a match criteria, or use a string alias (for example, $BONJOURSTRING) to identify the string to match. If using a string alias, ensure that it is existing and configured. For information on configuring a string alias, see Configure a Network Basic Alias Profile on page 209. This option is useful especially in large distributed, enterprise networks. Use it to create different instances of a Bonjour service for the different organizations or departments (VLANS) within your network. Creating instances allows you to advertise specific service instances for a specific set of VLANs, instead of advertising top-level Bonjour Services to various allocated VLAN(s).

7. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Bonjour Gateway Policy on page 386

Manage Bonjour Gateway Policies on page 386

Configure a Bonjour Forwarding Policy on page 390

Configure a Bonjour Forwarding Policy

A Bonjour forwarding policy enables the discovery of services on VLANs not visible to the device running the Bonjour Gateway. Bonjour forwarding enables the forwarding of Bonjour advertisements across VLANs to enable the Bonjour gateway to build a list of services and VLANs where services are available.

Note
Only one Bonjour forwarding policy is configurable for APs, and two policies are configurable for controllers.

Note
There must be Layer 2 connectivity between devices for forwarding to work.

1. Go to **Policies** > **Bonjour Gateway** > **Forwarding Policy**.

   The **Bonjour Forwarding** window opens. If any Forwarding policies are configured, they appear in a list in the **Forwarding** pane. The total number of Forwarding policies is shown in parentheses.
2. Choose from the following actions:
   - Select + to create a new Forwarding policy. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy to modify it. Modify the parameters in accordance with the steps in this procedure.
     - Select 🗑 associated with a policy to delete it.
3. Enter a **Name** for the policy.
4. Select **Add** to create the policy.

   Note
   If you exit the Forwarding policy configuration without first adding and saving any policy rules, the configured policy persists, but only until you log out.
5. Select + to add a new policy rule.
6. Configure the policy rule parameters as described in Table 136.

   Advertisements from VLANs that contain services are forwarded to VLANs containing clients.

Table 136: Forwarding Policy Rule Parameters

Parameter	Description
From VLANs	**From VLANs** are virtual interfaces where the Apple services are available. Enter a VLAN ID or a range of VLANs. Aliases can also be used.
To VLANs	**To VLANs** are virtual interfaces where clients for the services are available. Enter a VLAN ID or a range of VLANs. Aliases can also be used.
Rule ID	Specify a unique ID in the range 1 – 16 for this rule. This acts as numerical differentiator from other rules.

7. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Bonjour Gateway Policy on page 386
Manage Bonjour Gateway Policies on page 386
Configure a Bonjour Discovery Policy on page 388

Captive Portals Policy

A *captive portal* is an access policy for providing guests temporary and restrictive access to the controller or service platform managed network.

A captive portals policy provides secure authenticated controller or service platform access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional Terms and Agreement, Welcome, Fail and No Service pages provide the administrator with a number of options on captive portal screen flow and user appearance.

Captive portal authentication is used primarily for guest or visitor access, but is increasingly used to provide authenticated access to private network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

Authentication for captive portal access requests is performed using a username and password pair, authenticated by an integrated RADIUS server. Authentication for private network access is conducted either locally on the requesting wireless client, or centrally at a datacenter.

Captive portal uses a Web provisioning tool to create guest user accounts directly on the controller or service platform. The connection medium defined for the Web connection is either HTTP or HTTPS. Both HTTP and HTTPS use a request and response procedure clients follow to disseminate information to and from requesting wireless clients.

Configuring a Captive Portal Policy

> **Note**
> You must configure the policy's security, access, and whitelist basic parameters before actual HTML pages can be defined for guest user access requests.

1. Select **Policies** > **Captive Portals**.

   The **Captive Portal** window opens. If any captive portal policies are configured, they appear in a list in the Captive Portal pane. The total number of captive portal policies is shown in parentheses. You can choose from the following actions:

   a. Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.

   b. Select the **Edit** icon ✏ associated with a captive portal policy to modify it.

      When you select **Edit**, the **Basic Configuration** screen appears. Edit the captive portal policy parameters in accordance with the instructions in the steps in this procedure. You cannot edit the **Policy Name**.

   c. Select the **Delete** icon 🗑 associated with a captive portal policy to remove it.

   d. Select the **Add** icon + to create a new captive portal policy.

      When you select **Add**, the **Add Policy** window appears.

      i. Assign a policy **Name** representative of its access permissions, location or intended wireless client user base. The name cannot exceed 32 characters.

      ii. Select **Add** to save the policy.

         The **Basic Configuration** screen opens.

      iii. Configure the captive portal policy parameters in accordance with the instructions in the steps in this procedure.

2. Configure the following captive portal policy **Settings**:

Captive Portal Server Mode	Set the server mode. Options are: as either • `Internal (Self)` — Select this option to maintain the captive portal configuration (Web pages) internally. • `Centralized` — Select this option if the captive portal is supported on an external server. • `Centralized Controller` — Select this option if the captive portal is supported on a centralized controller or service platform. The default value is `Internal (Self)`.
Hosting VLAN Interface	When `Centralized Controller` is selected as the **Captive Portal Server Mode**, specify the VLAN (between 0 and 4096) for client communication. Select 0 to use the default client VLAN. 0 is the default setting.
Captive Portal IPv6 Server	Set a numeric IP address (non DNS hostname) for the server validating guest user permissions for the captive portal policy. This option is available only if you are hosting the captive portal on an external (`Centralized`) server resource. When using `Centralized` mode, select this option to define an IPv6 formatted address of the controller, service platform, virtual platform or access point resource hosting the captive portal.
Captive Portal Server Host	When `Centralized` is selected as the **Captive Portal Server Mode**, set a numeric IP address (or DNS hostname) for the server validating guest user permissions for the captive portal policy. When `Centralized Controller` is selected, use this field to provide the hostname of the controller or controllers acting as the captive portal server host.
Simultaneous Access	Select this check box and use the spinner control to set from 1-8192 users (client MAC addresses) allowed simultaneous access to the captive portal and its resources.
Connection Mode	Select either `HTTP` or `HTTPS` to define the connection medium to the Web server. We recommend the use of HTTPS because it affords some additional data protection HTTP cannot provide. The default value, however, is HTTP.

3. To define the **Security** settings, use the **AAA Policy** drop-down menu to select the policy used to validate user credentials and provide captive portal access to the network.

   If no AAA policies exist, you must create one. See Authentication, Authorization, and Accounting (AAA) Policy on page 256 for details.

4. Set the following **Access** parameters to define captive portal access, RADIUS lookup information, and whether the Login pages contain agreement terms that must be

accepted before access is granted to controller, service platform or virtual plarform resources using the captive portal:

Access Type	Select the authentication scheme applied to clients requesting captive portal guest access to the WiNG network. Options are: • **No authentication required** - Requesting clients are redirected to the captive portal Welcome page without authentication. • **RADIUS Authentication** - A requesting client's user credentials require authentication before access to the captive portal is permitted. This is the default setting. • **Registration** - A requesting client's user credentials require authentication through social media credential exchange. • **Email Access** - Clients use E-mail username and passwords for authenticating their captive portal session. Optionally set whether E-mail access requests are RADIUS validated. • **Mobile Access** - Mobile clients use their device's access permissions for authenticating their captive portal session. Optionally set whether mobile access requests are RADIUS validated. • **Other** - Requesting guest clients use a different means of captive portal session access (aside from E-mail or mobile device permissions). Optionally set whether these other access requests are RADIUS validated.
Terms and Conditions page	Select this option (with any access type) to include terms that must be adhered to for clients requesting captive portal access. These terms are included in the Terms and Conditions page when `No authentication required` is selected as the access type, otherwise the terms appear in the Login page. The default setting is disabled.
Frictionless Onboarding	Select this option to enable wireless clients, associated with guest WLANs, to self-register with the *Extreme Guest* server. In other words, this feature enables frictionless on-boarding of guest users to the ExtremeGuest server. It also provides an integration API, as a means of on-boarding guest users through a loyalty application. In the captive portal, set **Access Type** to `Registration`, enable **Frictionless Onboarding**, and provide the Localization URL to trigger a one-time redirect on demand. The defined URL is triggered from a mobile application to derive location information from the wireless network so an application can be localized to a particular store or region.

	Note: If enabling this option, in the WLAN (using this captive-portal) configure the settings as follows: • Set authentication-type as 'MAC'. • Set registration-mode as 'device'. • Enable the 'External Controller' and 'Follow AAA' options. • Use the AAA Policy drop-down menu to specify the AAA policy. • In the AAA policy, ensure that the authentication server configuration points to the ExtremeGuest server.

5. Set the following **Social Media Authentication** parameters to utilize a requesting client's social media profile for captive portal registration:

Facebook	Select this option to register the requesting client's guest user Facebook social media profile (collected from the social media server) on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication. This option is disabled by default.
Google	Select this option to register the requesting client's guest user Google social media profile (collected from the social media server) on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication. This option is disabled by default.

6. Select the checkbox to enable **Bypass Captive Portal Detection** capabilities.

   If enabled, captive portal detection requests are bypassed. This feature is disabled by default.

7. Configure the following **Client Settings** to define client VLAN assignments, how long clients are allowed captive portal access, and when clients are timed out due to inactivity:

RADIUS VLAN Assignment	Select this option to enable the RADIUS server to assign a VLAN post authentication. Once a captive portal user is authenticated, the user is assigned the VLAN as configured in the **Post Authentication VLAN ID** field. Select this option to enable client VLAN assignments using the RADIUS server. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS access-accept packet, and this feature is enabled, all client traffic is forwarded on the post authentication VLAN. If disabled, the RADIUS server's VLAN assignment is ignored and the VLAN configuration defined within the WLAN configuration is used instead. This feature is disabled by default.
Post Authentication VLAN ID	When this option is selected, a specific VLAN is assigned to the client upon successful authentication. The available range is from 1 - 4,096.

Client Access Time	Use the spinner control to define the duration wireless clients are allowed access to using the captive portal policy when there is no session time value defined for the RADIUS response. Set an interval from 10 - 10,800 minutes. The default interval is 1,440 minutes.
Inactivity Timeout	Use the drop-down menu to specify an interval in seconds (60 - 86,400) that, when exceeded, times out the session. The default is 10 minutes.

8. Configure the following **Loyalty App** settings to allow administrators to detect and report a captive portal client's usage of a selected (preferred) loyalty application:

Enable	Select this option to report a captive portal client's loyalty application presence and store this information in the captive portal's user database. The client's loyalty application detection occurs on the access point to which the client is associated and allows a retail administrator to assess whether a captive portal client is using specific retail (loyalty) applications in their captive portal. This setting is enabled by default.
App Name	Use the drop-down menu to select an existing application to track for loyalty utilization by captive portal clients. This enables an administrator to assess whether patrons are accessing an application as expected in specific retail environments.

9. To effectively host captive portal pages on an external web server, configure a set of allowed destination IP addresses for the captive portal. These allowed DNS destination IP addresses are called a *whitelist*.

   Each supported access point model can support up to 32 whitelists.

   a. Select **DNS Whitelist** checkbox to enable the **Select DNS Whitelist** field.
   b. Use the **Select DNS Whitelist** drop-down menu to view a list of existing DNS Whitelist policy entries, and to select a policy to be applied to the current captive portal policy.

      If no DNS Whitelist policy entries exist, you must create one. See Configuring DNS Whitelist Policies on page 398.

10. Set the following **Accounting** parameters to define how accounting is conducted for clients entering and exiting the captive portal.

    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 users are consuming.

Enable RADIUS Accounting	Select this option to use an external RADIUS resource for AAA accounting. When selected, a AAA Policy field displays. This setting is disabled by default.
Enable Syslog Accounting	Select this option to log information about the use of remote access services by users using an external syslog resource. This information is of great assistance in partitioning local versus remote users. Remote user information can be archived to an external location for periodic network and user administration. This feature is disabled by default.
Syslog Host	When syslog accounting is enabled, use the drop-down menu to determine whether an IP address or Hostname is used as a syslog host. The IP address or hostname of an external server resource is required to route captive portal syslog events to that destination external resource destination. A hostname cannot contain an underscore.
Syslog Port	When syslog accounting is enabled, define the numerical syslog port the used to route traffic with the external syslog server. The default port is 514.

11. Set the following **Data Limit** parameters values to define a data limit for clients accessing the network using the restrictions of a captive portal:

Limit	Select this option to enable data limits for captive portal clients. Specify the maximum amount of data, in megabytes, allowed for each captive portal client. When a user reaches this threshold, from 1 and 102,400 megabytes, it triggers the specified action.
Action	When a captive portal client reaches its data usage limit, a specified log action is executed. Choose from one of the following: • **`Log Only`** — Logs the event • **`log-and-disconnect`** — Logs the event and disconnects the user When **`Log Only`** is selected, an entry is added to the log file whenever a captive portal client exceeds the data limit. When **`log-and-disconnect`** is selected, an entry is added to the log file when the data limit is exceeded and the client is disconnected from the captive portal.

12. Set the **Logout FQDN** as the *fully qualified domain name* (FQDN) of the domain where the user is to be redirected after logging out of the captive portal.

    Example: `logout.guest.com`

13. Configure the following **Localization** parameters to add a URL to trigger a one-time redirect on demand.

    The defined URL is triggered from a mobile application to derive location information from the wireless network so an application can be localized to a particular store or region.

FQDN	Provide the FQDN address (for example, `local.guestaccess.com`) used to obtain localization parameters for a client.
Response	Enter a response message (512-character maximum) directed back to the client for localization HTTP requests.

14. Configure the **Redirection PortsDestination Port** field) by entering destination ports or consideration when re-directing client connections. Separate the defined ports by using a comma or a dash to indicate a range.

    Standard ports 80 and 443 are always considered for client connections regardless of what is entered by the administrator.

15. After you have completed configuring the settings, choose from the following actions:

    a. Select **Revert** to restore default settings or restore the last saved settings.

    > Note
    > You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

    > Note
    > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

    > Note
    > If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configuring DNS Whitelist Policies

A DNS approved list policy is used in conjunction with a captive portal to provide access services to wireless clients. Use the policy to create a set of destination IP addresses that are permitted within the captive portal. To effectively host hotspot pages on an external Web server, the IP address of the destination Web server(s) must be in the approved list.

To configure the list:

1. Go to **Policies** > **Captive Portals** > **DNS Whitelist**.

   The **DNS Whitelist** window opens. If any policies are configured, they appear in a list in the DNS Whitelist pane. The total number of configured policies is shown in parentheses. You can choose from the following actions:

   a. Select the sort icon ↑↓ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.

   b. Select the **Edit** icon ✎ associated with an existing policy in the list to modify it. See step 2 for details.

   c. Select the **Delete** icon 🗑 associated with an existing policy in the list to remove it.

   d. Select the **Add** icon + to create a new policy.

      When you select **Add**, the **Add Policy** window opens.

      i. Enter a **Name** for the policy that is to be applied to the captive portal policy. Enter a policy name containing up to 32 characters.

      ii. Select **Add** to save the new policy, then proceed to step 2.

2. Edit or configure the **Whitelist Entries** parameters in the **Details** window as follows:

   a. Enter a numerical IP address or Hostname within the **DNS Entry** field.

   b. Use the **Match Suffix** drop-down menu to choose `Yes` to match any hostname or domain name as a suffix. The default setting is **No**.

   c. Select **Add** to add a new entry.

   d. If necessary, you can select the **Delete** icon 🗑 associated with an existing entry to remove the entry from the list.

3. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Captive Portal Deployment Considerations

Consider the following before deploying a captive portal:

- Take into account the number of wireless clients allowed, services provided, and deployment requirements when considering the benefits and disadvantages of various topologies in the network architecture design.
- Captive portal authentication uses secure HTTPS to protect user credentials, but does not typically provide encryption for user data once the user has been authenticated. For private access applications, enable WPA2 (with a strong passphrase) to provide strong encryption.
- Assign guest user traffic to a dedicated VLAN, separate from other internal networks.
- Include firewall policies in guest access configurations. This ensures that logical separation is provided between guest and internal networks, preventing internal networks and hosts from being reachable through guest devices.
- Define guest access services in such a way that end-user traffic does not cause network congestion.
- Issue and install a valid certificate on all devices providing captive portal access to the WLAN and wireless network. Ensure the certificate is issued from a public certificate authority, allowing guests to access the captive portal without browser errors.

WLAN QoS Policies

Quality of service (QoS) provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

QoS helps ensure each WLAN receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories, for example Video, Voice, and Data. Packets within each category are processed based on the weights defined for each WLAN.

Each access point model supports up to 32 WLAN QoS policies.

Note
WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radios themselves, independent from the wireless clients the access point radios supported.

Configuring a WLAN QoS Policy

This procedure describes how to create a new policy, or edit or delete an existing policy.

1. Select **Policies** > **WLAN QoS**.

   The **WLAN QoS** window opens. If any WLAN QoS policies are configured, they appear in a list in the **Wlan QoS** pane. The total number of policies is shown in parentheses.

   The **Wlan QoS** pane column heading topic definitions are as follows:

Policy Name	The name assigned to this WLAN QoS policy. The assigned policy name cannot be modified.
Wireless Client Classification	Each policy's Wireless Client Classification as defined for this WLAN's intended traffic. The Classification Categories are the different WLAN-WMM options available to a radio. Classification types include: • `WMM` – Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). WMM classification is required to support the high throughput data rates required of 802.11n device support. • `Voice`– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. • `Video` – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. • `Normal` – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. • `Low` – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio. • `Non-Unicast` – Optimized for non-Unicast traffic. Implies all traffic on this WLAN is designed for broadcast or multicast.
SVP Prioritization	A green check mark defines the policy as having *Spectralink Voice Prioritization* (SVP) enabled to allow the wireless controller to identify and prioritize traffic from Spectralink/Polycomm phones using the SVP protocol. Phones using regular WMM and SIP are not impacted by SVP prioritization. A red "X" defines the QoS policy as not supporting SVP prioritization.
WMM Power Save	Enables support for the WMM based power-save mechanism, also known as *Unscheduled Automatic Power Save Delivery* (U-APSD). This is primarily used by voice devices that are WMM capable. The default setting is enabled.

Multicast Mask Primary	The primary multicast mask defined for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.
Multicast Mask Secondary	The secondary multicast mask defined for each listed QoS policy.

2. Choose from the following actions:

   a. Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.

   b. Select an existing policy in the list, or select the **Edit** icon ✎ to the right of the policy you want to modify.

      The **Rate Limit** configuration window appears for the selected policy. You can open the **Multimedia Optimizations** and **WMM** configuration screens by selecting the appropriate tabs. Edit the policy parameters in accordance with the instructions in the steps of the relevant procedure. You cannot edit the **Policy Name**.

   c. Select the **Delete** icon 🗑 to the right of the policy you want to remove.

   d. Select the **Add** icon + to create a new policy.

      When you select **Add**, the **Add Policy** window appears.

      i. Assign a policy **Name** representative of its access permissions, location or intended wireless client user base. The name cannot exceed 32 characters.

      ii. Select **Add** to save the policy.

          The **Rate Limit** configuration screen opens by default. You can open the **Multimedia Optimizations** and **WMM** configuration screens by selecting the appropriate tabs.

3. Continue with the WLAN QoS policy configuration as described in the following procedures:

   - Configure a WLAN and Wireless Client QoS Rate Limit on page 402
   - Configure Multimedia Optimizations on page 410
   - Configure a WLAN QoS WMM Policy on page 412

Configure a WLAN and Wireless Client QoS Rate Limit

A WLAN QoS policy must exist. See Configuring a WLAN QoS Policy on page 400.

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices, or malicious software such as a worm or virus that has infected one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. An administrator can set separate QoS rate limit configurations for data transmitted from the access point (upstream) and data transmitted from a WLAN's wireless clients back to their associated access point radios (downstream).

Before defining rate limit thresholds for WLAN upstream and downstream traffic, define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) will be dropped resulting in intermittent outages and performance problems.

Connected wireless clients can also have QoS rate limit settings defined in both the *upstream* and *downstream* direction.

To configure a QoS rate limit configuration for a WLAN and its connected clients:

To configure or edit a QoS rate limit for a WLAN:

1. Select **Policies** > **Wlan QoS**, then select a policy in the list to open the configuration window.
2. In the **Wireless LAN** pane, select the **Upstream Rate Limit** checkbox to enable rate limiting for data transmitted from the controller to associated access point radios and connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default. Select the **Upstream Rate Limit** checkbox to enable rate limiting for data transmitted from access point radios to associated clients on this WLAN. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default.

3. Configure the following WLAN **From Air Upstream Rate Limit** parameters. These values apply to traffic from the controller to associated access point radios and connected wireless clients.

Rate	Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely an upstream packet transmission will result in congestion for the WLAN's client traffic. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes.

4. Configure the following WLAN **From Air Upstream Random Early Detection Threshold** parameters for each access category. An early random drop is done when a traffic stream falls below the set threshold.

Background Traffic	Set a percentage value for background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.

Video Traffic	Set a percentage value for video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the upstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.

5. In the **Wireless LAN** pane, select the **Downstream Rate Limit** checkbox to enable rate limiting for data transmitted from access point radios to associated wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.to enable rate limiting for data transmitted from the controller or service platform to its associated access point radios and connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.
6. Configure the following WLAN **To Air Downstream Rate Limit** settings.

   These values apply to traffic from wireless clients to associated access point radios.

   These values apply to traffic from wireless clients to associated access point radios and the controller or service platform.

Rate	Define a downstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes.

7. Configure the following WLAN **To Air Downstream Random Early Detection Threshold** parameters for each access category. An early random drop is done when the amount of tokens for a traffic stream falls below the set threshold.

Background Traffic	Set a percentage value for background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Video Traffic	Set a percentage value for video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early random drops will occur.

8. In the **Wireless Client** pane, select the **Upstream Rate Limit** checkbox to enable rate limiting for data transmitted from access point radios to associated clients. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default.to enable rate limiting for data transmitted from the client to its associated access point radio and connected wireless controller. Enabling this option does not invoke client rate limiting for data traffic in the downstream direction. This feature is disabled by default.

9. Configure the following Wireless Client **From Air Upstream Rate Limit** parameters:

Rate	Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the wireless client. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 64 kbytes.

10. Set the following Wireless Client **From Air Upstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for wireless client traffic.

Background Traffic	Set a percentage value for background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value, once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.

Video Traffic	Set a percentage value for video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.0% implies no early random drops will occur.

11. In the **Wireless Client** pane, select the **Downstream Rate Limit** checkbox to enable rate limiting for data transmitted from connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.
12. Configure the following Wireless Client **To Air Downstream Rate Limit** parameters:

    These values apply to wireless client traffic.

    These values apply to traffic from a controller or service platform to associated access point radios and the wireless client.

Rate	Define a downstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default rate is 1,000 kbytes.
Maximum Burst Size	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for wireless client traffic. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 64 kbytes. Set a maximum burst size between 2 - 64 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

13. Configure the following **To Air Downstream Random Early Detection Threshold** parameters.

    These settings apply to each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for wireless client traffic.

Background Traffic	Set a percentage value for background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default is 50%.
Video Traffic	Set a percentage value for video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general downstream rate is known by the network administrator (using a time trend analysis). The default is 25%.
Voice Traffic	Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.0% means no early random drops will occur.

14. After you have completed configuring the settings, choose from the following actions:

    a. Select **Revert** to restore default settings or restore the last saved settings.

    > Note
    > You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configure Multimedia Optimizations

A WLAN QoS policy must exist. See Configuring a WLAN QoS Policy on page 400.

Multimedia optimizations customize the size and speed of multimedia content (voice, video, and so forth.) to deliver WLAN traffic strategically to the WLAN's managed clients and their defined QoS requirements.

To configure a QoS rate limit configuration for a WLAN:

To configure or edit a QoS rate limit configuration for a controller, service platform, virtual platform or access point managed WLAN:

1. Select **Policies** > **Wlan QoS**, then select a policy in the list to open the configuration window.
2. Select the **Multimedia Optimizations** tab.

3. Configure the **Multicast Mask** settings as follows:

Multicast Primary	Configure the primary multicast mask defined for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.
Multicast Secondary	Set a secondary multicast mask for the WLAN QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling. Set a secondary multicast mask for the WLAN QoS policy in case the primary becomes unavailable.

4. Use the **Accelerated Multicast** drop-down list to choose one of the following settings:

Disable Multicast Streaming	Select this option to disable all accelerated multicast streaming on the WLAN.
Automatically Detect Multicast Streams	Select this option to have multicast packets converted to unicast to provide better overall airtime utilization and performance. The administrator can either have the system automatically detect multicast streams and convert all detected multicast streams to unicast, or specify which multicast streams are converted to unicast. When the stream is converted and queued for transmission, a number of classification mechanisms can be applied to the stream, and the administrator can select the desired classification type.
Forwarding QoS Classification	This option appears if you select **`Automatically Detect Multicast Streams`** . Use the drop-down menu to select the classification to use. Options are: **`Trust`**, **`Voice`**, **`Video`**, **`Best Effort`**, **`Background`**.
Manually Configure Multicast Addresses	Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

5. If you selected **`Manually Configure Multicast Addresses`** in the previous step, configure a list of addresses as follows:

   a. Select **Add** to add a new entry to the list.

b. Configure the settings as follows:

Multicast IP Address	Enter the multicast IP address.
Classification	Use the **Classification** drop-down list to select the classification to use. Options are: `Trust`, `Voice`, `Video`, `Best Effort`, `Background`.

c. If necessary, you can delete a multicast IP address by selecting the 🗑 icon at the right side of the list entry.

6. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   > Note
   > You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

   > Note
   > This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

   > Note
   > If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Configure a WLAN QoS WMM Policy

A WLAN QoS policy must exist. See Configuring a WLAN QoS Policy on page 400.

Using *Wi-Fi Multimedia* (WMM), end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for both home networks and enterprises to decide which data streams are most important and assign them a higher traffic priority.

WMM's prioritization capabilities are based on the four access categories. The higher the access category, the higher the probability to transmit this kind of traffic over a controller, service platform or access point managed WLAN. Access categories were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms. WMM enabled controllers, service platforms and access points can coexist with legacy devices (not WMM-enabled).

Packets not assigned to a specific access category are categorized by default as having best effort priority. Applications assign each data packet to a given access category; packets are then added to one of four independent transmit queues (one per access category - voice, video, best effort or background) in the client. The client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

The same mechanism deals with external collision, to determine which client(s) should be granted the TXOP *(opportunity to transmit)*. The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category.

- The minimum interframe space, or *Arbitrary Inter-Frame Space Number* (AIFSN)
- The contention window, sometimes referred to as the random backoff wait

Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the access category. As frames with the highest access category tend to have the lowest backoff values, they are more likely to get a TXOP.

After each collision the contention window is doubled until a maximum value (also dependent on the access category) is reached. After successful transmission, the contention window is reset to its initial, access-category dependent value. The access category with the lowest backoff value gets the TXOP.

To configure a WMM configuration for a WLAN:

1. Select **Policies** > **Wlan QoS**, then select a policy in the list to open the configuration window.
2. Select the **WMM** tab.

3. Configure the following **Settings** with respect to the WLAN's intended WMM radio traffic and user requirements:

Wireless Client Classification	Use the drop-down menu to select the Wireless Client Classification for this WLAN's intended traffic type. The classification categories are the different WLAN-WMM options available to the radio. Classification types include: • **`WMM`** – Implies Wi-Fi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). WMM classification is required to support the high throughput data rates required of 802.11n device support. This is the default setting. • **`Voice`**– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. • **`Video`** – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. • **`Normal`** – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. • **`Low`** – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.
Non-Unicast Classification	Use this drop-down menu to define how traffic matching multicast masks is classified relative to prioritization on the radio. Options include **`Video`**, **`Voice`**, **`Normal`**, **`Low`**, and **`Default`**. The default setting is **`Default`**. Use the drop-down menu to select the Non-Unicast Classification for this WLAN's intended traffic. Non-unicast classification types include: • **`Default`** • **`Voice`**– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. • **`Video`** – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. • **`Normal`** – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. • **`Low`** – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.

Configure Non WMM Client Traffic	Use the drop-down menu to specify how non-WMM client traffic is classified on this access point WLAN if the Wireless Client Classification is set to WMM. Options include **`Video`**, **`Voice`**, **`Normal`**, and **`Low`**. The default setting is **`Normal`**. Use the drop-down menu to select the Non-WMM client traffic Classification. Non-WMM classification types include: • **`Voice`**– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. • **`Video`** – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. • **`Normal`** – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. • **`Low`** – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.
Enable Voice Prioritization	Select this option if Voice traffic is prioritized on the WLAN. This gives priority to voice and voice management packets supported only on certain legacy VOIP phones. This feature is disabled by default.
Enable SVP Prioritization	Enabling *Spectralink Voice Prioritization* (SVP) allows the identification and prioritization of traffic from Spectralink/Polycomm phones. This gives priority to voice on certain legacy VOIP phones. If the wireless client classification is WMM, non WMM devices recognized as voice devices have their traffic transmitted at voice priority. Devices are classified as voice when they emit SIP, SCCP, or H323 traffic. Thus, selecting this option has no effect on devices supporting WMM. This feature is disabled by default.
Enable WMM Power Save	Enables support for the WMM based power-save mechanism, also known as *Unscheduled Automatic Power Save Delivery* (U-APSD). This is primarily used by voice devices that are WMM capable. This feature is enabled by default.
Enable QBSS Load IE	Check this option to enable a QBSS *(QoS Basis Service Set)* IE *(information element)* in beacons and probe response packets advertised by access point radios. This feature is enabled by default.

4. Configure the following **Voice Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 47.
AIFSN	Set the current AIFSN (Arbitrary Inter-Frame Space Number) between 2 and 15. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2.

ECW Min	The **`ECW Min`** is combined with the **`ECW Max`** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 2.
ECW Max	The **`ECW Max`** is combined with the **`ECW Min`** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3.

5. Configure the following **Normal (Best Effort) Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 0.
AIFSN	Set the current AIFSN between 2 and 15. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access. The default value is 3.
ECW Min	The **`ECW Min`** is combined with the **`ECW Max`** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 4.
ECW Max	The **`ECW Max`** is combined with the **`ECW Min`** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 10.

6. Configure the following **Video Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default values is 94.
AIFSN	Set the current AIFSN between 2 and 15. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2.

ECW Min	The **`ECW Min`** is combined with the **`ECW Max`** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 3.
ECW Max	The **`ECW Max`** is combined with the **`ECW Min`** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 4.

7. Configure the following **Low (Background) Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 0.
AIFSN	Set the current AIFSN between 2 and 15. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access. The default value is 7.
ECW Min	The **`ECW Min`** is combined with the **`ECW Max`** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 4.
ECW Max	The **`ECW Max`** is combined with the **`ECW Min`** to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 10.

8. Set the following **Other Settings** for the WLAN's QoS policy:

Trust IP DSCP	Select this option to trust (utilize) IP DSCP values for WLANs. The default value is enabled.
Trust 802.11 WMM QoS	Select this option to trust (utilize) 802.11 WMM QoS values for WLANs. The default value enabled.

9. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   Note
   You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

Note
This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

Note
If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

WLAN QoS Deployment Considerations

Before defining a QoS configuration on a controller, service platform or access point managed WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WLAN QoS configurations differ significantly from QoS policies configured for associated radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients the radios support.
- Enabling WMM support on a WLAN only advertises WMM capability to wireless clients. The wireless clients must also support WMM and use the parameters correctly while accessing the wireless network to truly benefit.
- Rate limiting is disabled by default on WLANs. To enable rate limiting, a threshold must be defined for WLAN.
- Before enabling rate limiting on a WLAN, a baseline for each traffic type should be performed. Once a baseline has been determined, a minimum 10% margin should be added to allow for traffic bursts.
- The bandwidth required for real-time applications such as voice and video are very fairly easy to calculate because the bandwidth requirements are consistent and can be realistically trended over time. Applications such as web, database, and email are harder to estimate because bandwidth usage varies depending on how the applications are used.

Radio QoS Policies

Without a dedicated Quality of Service (QoS) policy, any wireless network operates on a best-effort delivery basis, meaning all traffic has equal priority and equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped!

When configuring a QoS policy for a radio, select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide deployment customizations best suited to each QoS policy's intended wireless client base.

WiNG managed controllers and their associated access point radios and wireless clients support several QoS techniques enabling real-time applications (such as voice and video) to coexist with lower priority background applications (such as web, email, and file transfers). A well designed QoS policy should:

- Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.
- Minimize the network delay and jitter for latency sensitive traffic.
- Ensure higher priority traffic has a better likelihood of delivery in the event of network congestion.
- Prevent the ineffective utilization of access points degrading session quality by configuring admission control mechanisms within each radio QoS policy.

In a wireless network, wireless clients supporting low and high priority traffic contend with one another for access and data resources. The IEEE 802.11e amendment has defined *Enhanced Distributed Channel Access* (EDCA) mechanisms stating high priority traffic can access the network sooner then lower priority traffic. The EDCA defines four traffic classes (or access categories): voice (highest), video (next highest), best effort, and background (lowest). The EDCA has defined a time interval for each traffic class, known as the *Transmit Opportunity* (TXOP). The TXOP prevents traffic of a higher priority from completely dominating the wireless medium, thus ensuring lower priority traffic is still supported by the controller or service platform, their associated access points and connected radios.

IEEE 802.11e includes an advanced power saving technique called *Unscheduled Automatic Power Save Delivery* (U-APSD) that provides a mechanism for wireless clients to retrieve packets buffered by an access point. U-APSD reduces the amount of signaling frames sent from a client to retrieve buffered data from an access point. U-APSD also allows access points to deliver buffered data frames as *bursts*, without backing-off between data frames. These improvements are useful for voice clients, as they provide improved battery life and call quality.

The Wi-Fi alliance has created *Wireless Multimedia* (WMM) and *WMM Power Save* (WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. A WiNG wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.

Enabling WMM support on a WLAN just advertises the WLAN's WMM capability and radio configuration to wireless clients. The wireless clients must be also able to support WMM and use the values correctly while accessing the WLAN.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters apply to both connected access point radios and their wireless clients. Parameters that affect access point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN's WMM settings.

WiNG managed controllers, service platforms and access points include Session Initiation Protocol (SIP), Skinny Call Control Protocol (SCCP), and Application Layer

Gateways (ALGs) that enable devices to identify voice streams and dynamically set voice call bandwidth. Controllers use the data to provide prioritization and admission control to these devices without requiring TSPEC or WMM client support.

WiNG managed controllers, service platforms, and access points support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. When enabled on a WLAN, traffic forwarded to a client is prioritized and forwarded based on the WLAN's WMM access control setting.

Note
Statically setting a WLAN WMM access category value prioritizes traffic to the client, but does not prioritize traffic from the client.

Rate limits can be applied to WLANs using groups defined locally or externally from a RADIUS server using *Vendor Specific Attributes* (VSAs). Rate limits can be applied to authenticating users using 802.1X, captive portal authentication and MAC authentication.

Related Links

Radio QoS Configuration and Deployment Considerations on page 420
Manage Radio QoS Policies on page 420

Radio QoS Configuration and Deployment Considerations

Before defining a radio QoS policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- To support QoS, each multimedia application, wireless client and WLAN is required to support WMM.
- WMM enabled clients can coexist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a best effort access category.
- Use default WMM values for all deployments. Changing these values can lead to unexpected traffic blockages, and these blockages might be difficult to diagnose.
- Overloading an access point radio with too much high priority traffic (especially voice) degrades overall service quality for all of its users.
- TSPEC admission control is available only with newer voice over WLAN phones. Many legacy voice devices do not support TPSEC or even support WMM traffic prioritization.

Manage Radio QoS Policies

Go to **Policies** > **Radio QoS**.

The **Radio Quality of Service (QoS)** window includes:

- A list of configured Radio QoS policies.
- Tools that allow users to manage policies.

View Configured Radio QoS Policies

The Radio QoS window displays a list of all configured policies in tabular form.

Table 137 describes the type of information displayed under each column in the table.

Table 137: Radio QoS Policy List Column Headings

Column Heading	Description
Radio QoS Policy	Displays the name of configured radio QoS policies. This is the name set for each listed policy when it was created. Policy names cannot be modified after the policy is saved.
Firewall detection traffic Enable (e.g., SIP)	A ✓ defines the policy as applying radio QoS settings to traffic detected by the Firewall. A ✗ defines the policy as having Firewall detection disabled. When enabled, the Firewall simulates the reception of frames for voice traffic when the voice traffic was originated via SIP or SCCP control traffic. If a client exceeds configured values, the call is stopped and/or received voice frames are forwarded at the next non admission controlled traffic class priority. This applies to clients that do not send TPSEC frames only.
Implicit TPSEC	A ✓ indicates that the policy requires wireless clients to send their traffic specifications before they can transmit or receive data. If enabled, this setting applies to just this radio's QoS policy. When enabled, the Access Point simulates the reception of frames for any traffic class by looking at the amount of traffic the client is receiving and sending. If the client sends more traffic than has been configured for an admission controlled traffic class, the traffic is forwarded at the priority of the next non admission controlled traffic class. This applies to clients that do not send TPSEC frames only.
Voice	A ✓ indicates that Voice prioritization QoS is enabled on the radio. A ✗ indicates that **`Voice`** prioritization QoS is disabled on the radio.
Best Effort	A ✓ indicates that Best Effort QoS is enabled on the radio. A ✗ indicates that **`Best Effort`** QoS is disabled on the radio.
Video	A ✓ indicates that Video prioritization QoS is enabled on the radio. A ✗ indicates that **`Video`** prioritization QoS is disabled on the radio.
Background	A ✓ indicates that Background prioritization QoS is enabled on the radio. A ✗ indicates that **`Background`** prioritization QoS is disabled on the radio.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the Radio QoS policy entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ↻ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an entry to modify it.
  - Select 🗑 associated with an entry to delete it.
- Select + to configure a new policy.

Related Links

Configure a Radio QoS Policy on page 422

Configure a Radio QoS Policy

Use this procedure to configure, edit, or delete a Radio QoS policy.

1. Go to **Policies** > **Radio QoS**.
2. Choose from the following actions:
   - Select + to create a new Radio QoS policy. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ associated with a policy to edit it. Modify the parameters as described in the relevant procedures listed under Related Topics.
     - Select 🗑 associated with a policy to delete it.
3. Enter a **Name** for the policy.
4. Select **Add** to create the policy.

   The **Radio QoS Policy** screen displays the WMM tab by default.
5. Configure Radio QoS policy rules under the **WMM**, **Admission Control**, and **Multimedia Optimizations** tabs.

   Note

   If you exit the Radio QoS policy configuration without first saving any policy rules in the tabs, the configured policy persists, but only until you log out.

Related Links

Radio QoS Configuration and Deployment Considerations on page 420

Manage Radio QoS Policies on page 420

Configure Radio QoS Wireless Multimedia Policy on page 423

Configure Radio QoS Admission Control Policy on page 426
Configure Radio QoS Multimedia Optimizations Policy on page 431

Configure Radio QoS Wireless Multimedia Policy

Use the WMM tab to define the access category configuration (CWMin, CWMax, AIFSN and TXOP values) with respect to the type of wireless data planned for this radio QoS policy.

1. Go to **Policies** > **Radio QoS** > **WMM**.
2. Configure or modify **Voice Access** parameters for the radio QoS policy as described in Table 138.

Table 138: Voice Access Parameters

Parameters	Description
Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. When resources are shared between a Voice over IP (VoIP) call and a low priority file transfer, bandwidth is normally exploited by the file transfer, thus reducing call quality or even causing the call to disconnect. With voice QoS, a VoIP call (a real-time session), receives priority, maintaining a high level of voice quality. For higher-priority traffic categories (like voice), the **`Transmit Ops`** value should be set to a low number. The default value is 47.
AIFSN	Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 1.
ECW Min	The **`ECW Min`** is combined with the **`ECW Max`** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 2.
ECW Max	The **`ECW Max`** is combined with the **`ECW Min`** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3.

3. Configure or modify **Normal (Best Effort) Access** parameters for the radio QoS policy as described in Table 139.

Table 139: Normal (Best Effort) Access Parameters

Parameter	Description
Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
AIFSN	Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 3.
ECW Min	The **`ECW Min`** is combined with the **`ECW Max`** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 4.
ECW Max	The **`ECW Max`** is combined with the **`ECW Min`** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 6.

4. Configure or modify **Video Access** parameters for the radio QoS policy as described in Table 140.

Table 140: Video Access Parameters

Parameter	Description
Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 94.
AIFSN	Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 1.

Table 140: Video Access Parameters (continued)

Parameter	Description
ECW Min	The **ECW Min** is combined with the **ECW Max** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3.
ECW Max	The **ECW Max** is combined with the **ECW Min** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 4.

5. Configure or modify **Low (Background) Access** parameters for the radio QoS policy as described in Table 141.

Table 141: Low (Background) Access Parameters

Parameter	Description
Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
AIFSN	Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 7.
ECW Min	The **ECW Min** is combined with the **ECW Max** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 4.
ECW Max	The **ECW Max** is combined with the **ECW Min** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 10.

6. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   Note
   You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure a Radio QoS Policy on page 422
Configure Radio QoS Admission Control Policy on page 426
Configure Radio QoS Multimedia Optimizations Policy on page 431

Configure Radio QoS Admission Control Policy

You must be in the process of configuring a new Radio QoS policy or modifying an existing policy to use this procedure.

Admission control requires that clients send their traffic specifications (TSPEC) to a controller or service platform managed Access Point before they can transmit or receive data.

To configure or modify **Admission Control** parameters for this Radio QoS policy:

1. Go to **Policies** > **Radio QoS** > **Admission Control**.
2. Select **Firewall All Detection Traffic Enable** to enforce admission control for traffic whose access category is detected by the firewall (ALG.

   This feature is enabled by default.
3. Select **Implicit TSPEC** to require wireless clients to send their traffic specifications to a controller or service platform managed access point before they can transmit or receive data.

   If enabled, this setting applies to the QoS policy for this radio only. This feature is enabled by default.

4. Configure or modify **Voice Access** admission control parameters for this radio QoS policy as described in Table 142.

Table 142: Voice Access Parameters

Parameter	Description
Enable Voice	Select to enable admission control for this policy's voice traffic. Only voice traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured).
Maximum Airtime	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value ensures the radio's bandwidth is available for high bandwidth voice traffic (if anticipated on the wireless medium) or other access category traffic if voice support is not prioritized. Voice traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support voice. The default value is 75%.
Maximum Wireless Clients	Set the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. Consider setting this value proportionally to the number of other QoS policies supporting the voice access category, as wireless clients supporting voice use a greater proportion of resources than lower bandwidth traffic (like low and best effort categories). The default value is 100 clients.
Maximum Roamed Wireless Clients	Set the number of voice supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%.

5. Configure or modify **Video Access** admission control parameters for this radio QoS policy as described in Table 143.

Table 143: Video Access Parameters

Parameter	Description
Enable Video	Select to enable admission control for this policy's video traffic. Only video traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). This feature is disabled by default.
Maximum Airtime	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for high bandwidth video traffic (if anticipated on the wireless medium) or other access category traffic if video support is not prioritized. Video traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support video. The default value is 75%.
Maximum Wireless Clients	Set the number of wireless clients supporting video traffic allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients.
Maximum Roamed Wireless Clients	Set the number of video supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%.

6. Configure or modify **Normal (Best Effort) Access** admission control parameters for this radio QoS policy as described in Table 144.

Table 144: Normal (Best Effort) Access Parameters

Parameter	Description
Enable Best Effort	Select to enable admission control for this policy's normal traffic. Only normal traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured).
Maximum Airtime	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal best effort client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for lower bandwidth normal traffic (if anticipated to proliferate the wireless medium). Normal background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for best effort data support. The default value is 75%.
Maximum Wireless Clients	Set the number of wireless clients supporting best effort traffic allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients.
Maximum Roamed Wireless Clients	Set the number of normal best effort supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal best effort supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%.

7. Configure or modify **Low (Background) Access** admission control parameters for this radio QoS policy as described in Table 145.

Table 145: Low (Background) Access Parameters

Parameter	Description
Enable Background	Select to enable admission control for this policy's lower priority background traffic. Only low background traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured).
Maximum Airtime	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for low background client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for lower bandwidth normal traffic (if anticipated to proliferate the wireless medium). Background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for background data support. The default value is 75%.
Maximum Wireless Clients	Set the number of low and background supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients.
Maximum Roamed Wireless Clients	Set the number of low and best effort supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal background supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%.

8. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

Note

If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure a Radio QoS Policy on page 422
Configure Radio QoS Wireless Multimedia Policy on page 423
Configure Radio QoS Multimedia Optimizations Policy on page 431

Configure Radio QoS Multimedia Optimizations Policy

You must be in the process of configuring a new Radio QoS policy or modifying an existing policy to use this procedure.

Use the Multimedia Optimizations tab to configure advanced multimedia QoS and Smart Aggregation parameters for the radio QoS policy.

1. Go to **Policies** > **Radio QoS** > **Multimedia Optimizations**.
2. Configure the **Accelerated Multicast** parameters for this radio QoS policy as described in Table 146.

Table 146: Accelerated Multicast Parameters

Parameter	Description
Maximum multicast streams allowed	Specify the maximum number of multicast streams (between 0 and 256) permitted to use accelerated multicast. The default value is 25.
When wireless client count exceeds the above limit	When the wireless client count using accelerated multicast exceeds the maximum number, set the radio to either `Reject` new wireless clients or `Revert` existing clients to a non-accelerated state.
Maximum multicast streams per client	Specify the maximum number of multicast streams (between 1 and 4) wireless clients can use. The default value is 2.
Packets per second for multicast flow for it to be accelerated	Specify the threshold of multicast packets per second (between 1 and 500) that triggers acceleration for wireless clients. The default value is 25.
Timeout for wireless clients	Specify a timeout value in seconds (between 5 and 6,000) for wireless clients to revert to a non-accelerated state. The default value is 60.

3. Configure **Smart Aggregation** parameters as described in Table 147.

   Smart Aggregation enhances frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In a frame's typical aggregation, an aggregated frame is sent when it meets one of these conditions:

   - A predefined number of aggregated frames is reached
   - An administrator defined interval has elapsed since the first frame (of a set of frames to be aggregated) was received

- An administrator defined interval has elapsed since the last frame (not necessarily the final frame) of a set of frames to be aggregated was received

With this enhancement, an aggregation delay is set uniquely for each traffic class. For example, voice traffic is not aggregated but is sent immediately, while background data traffic is sent only after frames have been aggregated.

Table 147: Smart Aggregation Parameters

Parameters	Description
Smart Aggregation	Select to enable smart aggregation and dynamically define when an aggregated frame is transmitted. Smart aggregation is disabled by default.
Max Delay for Best Effort	Set the maximum time (in milliseconds) to delay best effort traffic. The default setting is 150 milliseconds.
Max Delay for Background	Set the maximum time (in milliseconds) to delay background traffic. The default setting is 250 milliseconds.
Max Delay for Streaming Video	Set the maximum time (in milliseconds) to delay streaming video traffic. The default setting is 150 milliseconds.
Max Delay for Video Conferencing	Set the maximum time (in milliseconds) to delay video conferencing traffic. The default setting is 40 milliseconds.
Max Delay for Voice	Set the maximum time (in milliseconds) to delay voice traffic. The default setting is 0 milliseconds.
Minimum frames per Aggregate limit	Set the minimum number of frames to aggregate in a frame before it is transmitted. The default setting is 8 frames.
Max Mesh Links	Set the maximum number of mesh hops for smart aggregation. The default setting is 3.

4. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Configure a Radio QoS Policy on page 422
Configure Radio QoS Wireless Multimedia Policy on page 423
Configure Radio QoS Admission Control Policy on page 426

Association ACL Policy

An association ACL is a policy-based ACL that either allows or denies clients from connecting to a controller, service platform or access point managed WLAN. An association ACL affords a system administrator the ability to restrict access by specifying a client MAC address or range of addresses to either include or exclude from WLAN connectivity.

Association ACLs are applied to WLANs as an additional access control mechanism. They can be applied to WLANs through WLAN Basic configuration. For more information on applying an existing association ACL to a WLAN, see Configure Wireless LAN Basic Settings on page 107.

Deployment Guidelines

Before configuring an Association ACL policy and applying it to a controller, service platform or access point managed WLAN, consider the following deployment guidelines to ensure the configuration is optimally effective:

- Strategically name and configure ACL policies to meet the requirements of the particular WLANs to which they apply. Be careful, however, not to name ACLs after specific WLANs, because individual ACL policies can be used by more than one WLAN.
- You cannot apply more than one MAC based ACL to a Layer 2 interface. If a MAC ACL is already configured on a Layer 2 interface, and a new MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

Related Links

Manage Association ACL Policies and Rules on page 433

Manage Association ACL Policies and Rules

Go to **Policies** > **Association ACL**.

Configuring an Association ACL policy consists of creating a policy and assigning it a name, then configuring policy rules and URL Error Page settings. The user interfaces used to configure the policies and rules include:

- A list of configured policies or rules in tabular form.
- Tools that allow users to manage the policies and rules.

View Configured Policies and Rules

Table 148 and Table 149 on page 434 describe the type of information displayed under each table column in the user interfaces used to configure the policies and rules.

Table 148: Association ACL Policy Table Column Headings

Column Heading	Description
Policy Name	The name assigned policy.
Action	See Management Tools on page 434 for details.

Table 149: Association ACL Policy Rules Table Column Headings

Column Heading	Description
Precedence	Displays the precedence (priority) assigned to a particular rule.
Starting MAC Address	Displays the starting MAC address for clients requesting association.
Ending MAC Address	Displays the ending MAC address for clients requesting association.
Allow/Deny	Indicates whether clients whose MAC address falls within the defined starting and ending MAC address range are to be allowed or denied access.
Action	See Management Tools for details.

Management Tools

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table.
- Select ⤓ to download the MAC ACL policy entries in csv format.
- Select ▮▮▮ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- From under the **Actions** column in the table choose from the following actions:
  - Select ✎ associated with an entry to modify it.
  - Select 🗑 associated with an entry to delete it.
- Select + to configure a new policy.

Related Links

Association ACL Policy on page 433

Configure an Association ACL Policy on page 435

Configure Association ACL Policy Rules on page 435

Configure an Association ACL Policy

Use this procedure to create, modify, or delete an Association ACL policy.

1. Go to **Policies** > **Association ACL**.

   If any policies exist, they appear in tabular form in the Association ACL window. The total number of configured policies is shown in parentheses.
2. Choose from the following actions:
   - Select + to create a new Association ACL policy.
     a. Assign a **Name** to the policy (up to 32 characters) to distinguish this Access Control List (ACL) policy from others with similar attributes.
     b. Select **Add** to create the new policy.
     c. Proceed to the next step.
   - From under the **Actions** column:
     - Select ✎ adjacent to a policy to modify it. Proceed to the next step.
     - Select 🗑 adjacent to a policy to delete it.
3. Configure the Association ACL policy **Rules**.

   > Note
   > If you exit the Association ACL policy configuration without first adding any rules, the configured policy persists, but only until you log out.

Related Links

Manage Association ACL Policies and Rules on page 433

Configure Association ACL Policy Rules on page 435

Configure Association ACL Policy Rules

You must be in the process of configuring a new Association ACL policy or modifying and existing policy to use this procedure.

Use this procedure to create, modify, or delete Association ACL policy **Rules**.

1. Choose from the following actions:
   - If you are in the process of configuring a new ACL policy, select + to create a new rule. Proceed to the next step.
   - If you want to edit or delete an Association ACL policy rule, go to **Policies** > **Association ACL**.

     Select ✎ adjacent to the target Association ACL policy to open the **Rules** window. Choose from the following actions:
     - To edit an Association ACL policy rule, select ✎ adjacent to the rule you want to modify. Modify the rule in accordance with the steps in this procedure.
     - To delete a policy rule, select 🗑 adjacent to the target rule.

2. Configure the **Rule** parameters as described in Table 150.

Table 150: Association ACL Policy Rule Parameters

Parameter	Description
Association ACL	If you are creating an new Association ACL, provide a name specific to its function. Avoid naming it after the WLAN it supports. The name cannot exceed 32 characters.
Precedence	The rules within a WLAN's ACL are applied to packets based on precedence. Every rule has a unique sequential precedence value you define. You cannot add two rules with the same precedence. The default precedence increments sequentially (starting at 1) with each new rule added, and can be modified. If, for example, you modify the default precedence value 3 to 6, and then add a new rule, the default precedence for the new rule will increment to 4, not 7. Therefore it is necessary to be vigilent when prioritizing ACLs as they are added.
Starting MAC Address	Enter a starting MAC address for clients requesting association.
Ending MAC Address	Enter an ending MAC address for clients requesting association.
Allow/Deny	Use the drop-down menu to specify whether to `Allow` or `Deny` client access if a MAC address matches this rule.

3. Optionally, repeat the steps in this procedure to add more policy rules.
4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

Manage Association ACL Policies and Rules on page 433

Configure an Association ACL Policy on page 435

Guest Management Policy

A guest management policy redirects guest users to a registration portal upon association with the captive portal SSID. The guest users are redirected to a registration page (registration.html)—hosted internally or externally—where the guest user can complete the registration process if the user has not previously registered. The internal captive portal adds a new registration page that is customizable based on business requirements.

A guest management policy configuration sets the E-mail host and SMS gateway related commands along with the credentials required for sending a passcode to a guest through email and SMS. Configure up to 32 different guest management policies. Each guest management policy allows an administrator to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents, and E-mail message body. There can be only one guest management policy active for each device.

Guest registration is supported on NX9000 series service platforms and the CX9000 and VX9000 virtual platforms as an adopting controller with up to 2 million user identity entries. Guest registration is supported on NX 7500 series service platforms as an adopting controller with up to 1 million user identity entries.

Note
An option to backup the guest registration configuration is not available in the user interface. To backup the guest user database, a guest-databasebackup command must be invoked using the CLI. For more information, refer to the *WiNG Controller Command Reference Guide*.

Guest Management Policy Configuration

To view, edit, delete, or add a guest management policy:

1. Select **Policies** > **Guest Management**.

   The **Guest Management** window displays. If any guest management policies are configured, they appear in a list in the Guest Management pane. The total number of guest management policies is shown in parentheses.

   Following is a description of the column headings in the Guest Management window:

Policy Name	Lists the names of configured guest user policies.
Email Enable	A green check mark defines Email as enabled for guest management, a red X defines Email as disabled. Guest users can register themselves with their E-mail credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered email/mobile/member id and the received pass code for further login to the captive portal.

SMS Enable	A green check mark defines SMS as enabled for guest management, a red X defines SMS as disabled. SMS enables guest users to registers themselves with their E-mail or mobile device ID as the primary key for authentication. The captive portal provides the passcode for registration, and the guest users utilizes use their registered E-mail or mobile device ID and received passcode for login to the captive portal.
SMS SMTP Enable	A green check mark defines SMS SMTP as enabled for guest management, a red X defines SMS SMTP as disabled. Optionally configure an E-mail host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway E-mail address to which the message is E-mailed. The gateway server converts the E-mail into SMS and sends the message to the guest user's mobile device.
DB Export Enable	A green check mark indicates that exporting the guest user database is enabled for this device. When enabled, the list of guest users on the captive portal can be periodically exported to an external server.

2. Choose from the following actions:

   a. Select the sort icon adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon . Toggle the icon to sort the column data in descending order . The "1" indicates by which column heading topic the data is currently sorted.

   b. Select the **Edit** icon associated with a guest management policy to modify it.

      When you select **Edit**, the **Guest Management** window appears for the selected policy. Edit the parameters in accordance with the instructions in the procedures in this section. You cannot edit the **Policy Name**.

   c. Select the **Delete** icon associated with a guest management policy to remove it.

   d. Select the **Add** icon to create a new guest management policy.

      When you select **Add**, the **Add Policy** window appears.

      i. Assign a policy **Name**. The name cannot exceed 32 characters.

      ii. Select **Add** to save the policy.

         The **Guest Management** window appears.

      iii. Configure the parameters in the Email, SMS, or SMS SMTP tab, depending on which authentication methods are to be extended to guest users.

3. Optionally, configure DB Export to export the guest user database to an external server for analysis and database backup.

Email

Guest users can register themselves with their email credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered email/mobile/ member id and the received pass code for further login to the captive portal.

To define a guest management configuration using email as the primary key for authentication:

1. Select **Policies** > **Guest Management**.
2. Select the **Email** tab.
3. Set the following email guest user network address and message content information required for notifying a guest with a passcode using email:

Enable	Enable this option so guest users can register themselves with their email credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered Email/ mobile/member id and the received pass code for further login to the captive portal. This setting is disabled by default and must be enabled to define the required settings.
Host	Define a hostname or IPv4 formatted IP address of the SMTP server resource used for guest management email traffic, guest user credential validation and passcode reception. Optionally create an alias to define the host once and use the alias across different configuration items.
Sender	Provide a 100 character maximum sender name for the guest user receiving the passcode required for registering their guest email credentials.
Security	Use the drop-down menu to select ssl or starttls as the email host server user authentication validation scheme for this particular username and password combination. Optionally select None to apply to no additional user authentication beyond the required username and password combination.
Username	Provide a unique 100 character maximum username unique to this guest management configuration. This username will require its own password and must be correctly provided to receive the required passcode for registering guest email credentials.
Password	Define a 63 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest email credentials.
Subject	Enter the 100 character maximum email subject for the email message sent to the guest user along with the required passcode. You can use the tag ‘GM_NAME’ in the subject which is replaced by the guest user’s name.
Message	Create the 1024 character maximum message content for the email sent to the guest user along with the passcode. You can use the following tags in the message body. • GM_NAME – indicates the guest user’s name in the message. This tag is replaced by the guest user’s name when the email is created. • GM_PASSCODE - indicates the password assigned to the user. The tag is replaced by the actual password when the email is created. • CR-NL - indicates a line break. When used, the word next to this tag starts on a new line when the email is created.

4. After you have completed configuring the settings, choose from the following actions:
    a. Select **Revert** to restore default settings or restore the last saved settings.

        Note
        You cannot restore default settings after applying or saving changes.

    b. Select **Apply** to commit the configured settings.

        Note
        This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

    c. Select **Save** to commit and save the configured settings.

        Note
        If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

SMS

SMS enables guest users to registers themselves with their email or mobile device ID as the primary key for authentication. The captive portal provides the passcode for registration, and the guest users utilizes use their registered email or mobile device ID and received passcode for login to the captive portal.

Note
When utilizing SMS, the WLAN's authentication type should be None and the registration type should be enabled as user registration. Captive portal authentication must always enforce guest registration.

SMS is similar to MAC address based self registration, but in addition a captive portal sends a SMS message to the user on the mobile phone number provided at registration containing an access code. The user then inputs the access code on the user screen. The captive portal verifies the code, returns the Welcome page and provides access. This allows the administrator to verify the phone number provided and can be traced back to a specific individual should the need arise.

The default gateway used with SMS is Clickatell. A passcode can be sent with SMS to the guest user directly using Clickatell, or the passcode can be sent via email to the SMS Clickatell gateway server, and Clickatell sends the passcode SMS to the guest user.

To define a guest management configuration using SMS:

1. Select **Policies** > **Guest Management**.
2. Select the **SMS** tab.

3. Set the following SMS guest user network address and message content information required for notifying a guest with a passcode:

Enable	Select this option to enable guest users to registers themselves with their email or mobile device ID as the primary key for authentication. This setting is disabled by default and must be enabled to define the required settings.
Host	By default, *clickatell* is the only host SMS gateway server resource. Upon receiving the passcode email, the SMS gateway sends the actual notification passcode SMS to the guest user.
Username	Provide a unique 32 character maximum username unique to this SMS guest management configuration. This username will require its own password and must be correctly provided to receive the required passcode for registering guest user credentials with SMS.
Password	Define a 63 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest user credentials with SMS.
API Id	Set a 32 character maximum API Id for the configuration of the clickatell api_id (http/smtp api_id).
User Agent	Select the user agent for configuring the clickatell SMS gateway server and its related credentials for sending the passcode to guests.
Source Number	Set a 32 character maximum source-address from the number associated with clickatell. It can be a large integer or short code. The source number is only applicable to certain countries (like the United States).
Message	Create the 1024 character maximum message content for the SMS based request sent to the guest user along with the passcode.

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

SMS SMTP

Optionally configure an email host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway email address to which the message is emailed. The gateway server converts the email into SMS and sends the message to the guest user's mobile device.

When sending an email, the email client interacts with a SMTP server to handle the content transmission. The SMTP server on the host may have conversations with other SMTP servers to deliver the Email.

To define a guest management configuration using SMS SMTP:

1. Select **Policies** > **Guest Management**.
2. Select the **SMS SMTP** tab.
3. Set the following SMS SMTP guest user network and message content information required for notifying a guest with a passcode:

Enable	Enable this setting to configure an email host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway Email address to which the message is emailed. This setting is disabled by default and must be enabled to define the required settings.
Host	Define a hostname or IPv4 formatted IP address of the SMS gateway server resource used for guest management email traffic, guest user credential validation and passcode reception. Consider providing the host as an alias. An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the alias across different configuration items.
Sender	Provide a 100 character maximum sender name for the guest user receiving the passcode required for registering their guest email credentials using SMTP.
Security	Use the drop-down menu to select `ssl` or `starttls` as the SMTP server user authentication validation scheme for this particular username and password combination. Optionally select None to apply to no additional user authentication beyond the required username and password combination. The default value is `ssl`.
Username	Provide a unique 64 character maximum username unique to this SMTP guest management configuration. This username requires its own password and must be correctly provided to receive the required passcode for registering guest user credentials.
Password	Define a 64 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest user credentials with SMTP.
Email of Recipient	Enter a 64 character maximum email address for the recipient of guest management email traffic.
Subject	Enter a 100 character maximum email subject for the email message sent to the guest user along with the required passcode.
Message	Enter a 1024 character maximum email message per the message format required by the gateway server. The sms-over-smtp message format is the required format from clickatell while sending email to the SMS gateway server.

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

DB Export

Optionally configure the guest user database export parameters. The guest user database can be periodically exported to an external server for backup and analysis.

To define the database export parameters:

1. Select **Policies** > **Guest Management**.
2. Select the **DB Export** tab.
3. Set the following DB Export parameters:

Enable	Enable this setting to configure the guest user database to an external server for backup and analysis. This setting is disabled by default and must be enabled to define the required settings.
Start Time	Define the start time when the first database backup occurs. The first run of the guest user database backup is always the current day. Use the spinner controls to set the start hour and minute. Use the AM/PM options to configure the exact hour. The default value is 12:00 AM.
Frequency	Define the backup frequency. This is the time interval between two consecutive backups. Use the spinner control to set the value between 1 hour and 168 hours. The default frequency is 4 hours.
Format	The guest user database can be exported in the following formats: • CSV • JSON Select the appropriate export format. The default export format is CSV.

Last Visit Within	Use this field to filter or restrict the amount of data that is exported. Use the spinner to set a value in the range 1–168 hours. If for example, the last visit within value is set at 2 hours, then only the last 2 hours of guest user collections—since the last database backup—will be exported. The default value is 4 hours.
URL Directory	Use the field to provide the URL to which the guest user database is exported. Select the Advanced link to expose fields for setting the remote server's URL.

4. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

      Note
      You cannot restore default settings after applying or saving changes.

   b. Select **Apply** to commit the configured settings.

      Note
      This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

   c. Select **Save** to commit and save the configured settings.

      Note
      If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

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 Links

Add NSight Policy on page 445
Edit NSight Policy on page 445
Delete NSight Policy on page 446

Add NSight Policy

Configure and add an NSight policy for the network.

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 • 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 Links

NSight Policy on page 444
Edit NSight Policy on page 445
Delete NSight Policy on page 446

Edit NSight Policy

Only existing NSight policies can be edited.

Edit available NSight policies from the NSight policy list dashboard.

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 Links

NSight Policy on page 444
Add NSight Policy on page 445
Delete NSight Policy on page 446

Delete NSight Policy

Delete an existing NSight policy.

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 Links

Add NSight Policy on page 445
Edit NSight Policy on page 445
NSight Policy on page 444

Passpoint Policy

A passpoint policy provides an interoperable platform for streamlining Wi-Fi access to access points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices.

Passpoint makes connecting to Wi-Fi networks easier by authenticating the user with an account based on an existing relationship, such as the user's mobile carrier or broadband ISP.

The **Passpoint Policy** screen displays a list of passpoint polices for network hotspots. Each passpoint policy can be selected to edit its properties. If no exiting passpoint policies supports the required deployment, select Add to create a new policy.

To administrate and manage existing passpoint policies:

1. Select **Policies** > **Passpoint**.

2. Refer to the following configuration data for existing passpoint policies:

Policy Name	Displays the administrator assigned name of each passpoint policy.
Access Network Type	Displays the network access permissions the administrator has set for the passpoint policy
Operator Name	Displays the unique name assigned to the administrator or operator responsible for the configuration and operation of the hotspot
Venue Name	Displays the administrator assigned name of the venue or physical location of the deployed hotspot

3. Select + to define a new passpoint policy, or ✎ to edit an existing policy configuration.

4. Select 🗑 to delete an existing policy.

Related Links

Configure a Passpoint Policy on page 447
Configure Passpoint Policy NAI Realm on page 450
Configure Passpoint Policy OSU Provider on page 452

Configure a Passpoint Policy

Create or manage a passpoint policy.

1. Select **Policies** > **Passpoint**.

2. Select an existing policy or + to create a new passpoint policy.

   Type a unique policy name and select **Add** to define a new policy.

   The **Configuration** dashboard opens.

3. Configure the following **Settings** to define an internet connection medium for the passpoint policy:

HESSID	Select to apply a homogenous ESS ID. Leaving this option blank applies the BSSID instead
Internet	Select to activate Internet access to users of the passpoint hotspot
OSU SSID	Define a 32 character maximum sign-on ID that must be correctly provided to access the passpoint policy's hotspot resources

Domain Name	Add a 255-character maximum domain name to the pool available to the passpoint policy
Roam Consortium	Enter a list of RC (Roaming Consortium) OIs (Organization Identifiers) supported on this hotspot. Specify the Roaming Consortium OI in hexadecimal format (up to 128 characters). The beacons and probe responses communicate this Roaming Consortium list to devices. This information enables a device to identify the networks available through this AP. Each OI identifies a either a group of SSPs (Subscription Service Providers) or a single SSP.
IPv4 Address Type	Select the IPv4 formatted address type for this passpoint policy. IPv4 is a connectionless protocol operating on a best effort delivery model. IPv4 does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP). Options include **not-available**, **available**, and **unknown**
IPv6 Address Type	Select the IPv6 formatted address type for this passpoint policy. IPv6 is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. Options include **not-available**, **available**, and **unknown**

4. Set the following **Basic Configuration**:

Access Network Type	Select the network access method for this passpoint policy. Access network types include: • **`private`** - General access to a private network hotspot (default setting) • **`private-guest`** - Access to a private network hotspot with guest services • **`chargeable-public`** - Access to a public hotspot with billable services • **`personal-device`** - Access to a hotspot for personal devices such as wireless routers • **`emergency services`** - Dedicated network hotspot access for emergency services only
Venue Group	Passpoint is supported across a wide range of wireless network deployment scenarios and client devices. Select the group type best suited to the majority of hotspot requesters utilizing the passpoint policy's unique configuration
Venue Name Lang	Select **Add** and provide a venue name language code and name • **`Code`** - Type the two- or three-character ISO-14962-1997 encoded string that defines the language used • **`Name`** - Type the name of the venue. The name cannot exceed 252 characters
Venue Type	Select the venue type value between 0 and 255 best suited to where the actual location passpoint requesters are located
Venue Name	The administrator assigned name of the venue or physical location of the deployed access point hotspot

5. Set the **WAN Metrics** parameters:

Up Speed	Select to activate this option and estimate the maximum upstream bandwidth from 0 to 4,294,967,295 Kbps
Down Speed	Select to activate this option and estimate the maximum downstream bandwidth from 0 to 4,294,967,295 Kbps

6. Set the following **Connection Capability** for the passpoint policy's FTP, HTTP, ICMP, IPSec VPN, PPTP VPN, SIP, SSH, and TLS VPN interfaces:

   Use the drop-down list boxes to define these interfaces as **`open`**, **`closed`**, or **`unknown`** for this passpoint policy configuration.

   Tip
   The best practice is to deactivate unused interfaces to close unnecessary security holes.

7. Select **Add** to set a **Connection Capability Variable** to make specific virtual ports **`open`**, **`closed`**, or **`unknown`** for Wi-Fi connection attempts and to set rules for how the user can connect with routing preference using this passpoint policy.
8. Select **Add** to set a **Network Authentication Type** to select how Wi-Fi connection attempts are authenticated and validated using a dedicated redirection URL resource.
9. Set the following **Operator Network Parameters**:

Operator Name	Provide the unique name of the administrator or operator responsible for the configuration and management or the hotspot. The name cannot exceed 64 characters
Operator Name Lang	Operator names can be listed in multiple languages. Select **Add** to create operator name languages. Type the two- or three-character ISO-14962-1997 encoded string that defines the language used in the Code field. Type the name of the operator in the Name field. The name cannot exceed 252 characters
PLMNID	Operators providing mobile and Wi-Fi hotspot services have a unique Public Land Mobile Network (PLMN) ID. Select **Add** to create PLMN information for operators responsible for the configuration and operation of the hotspot. Provide a description for the PLMN, not exceeding 64 characters. Type a three-digit Mobile Country Code (MCC) and two-digit Mobile Network Code (MNC) for the PLMN ID. The MCC identifies the region and country where the hotspot is deployed. The MNC identifies the operator responsible for the configuration and management of the hotspot by PLMN ID and country. Both the MCC and MNC fields are mandatory

10. Select **Save** to update passpoint policy settings.

Configure Passpoint Policy NAI Realm

The Network Access Identifier (NAI) is the user identity submitted by the hotspot requesting client during authentication. The standard syntax is `user@realm`. NAI is frequently used when roaming, to identify the user and assist in routing an authentication request to the user's authentication server. The realm name is often the domain name of the service provider.

1. Select **Policies** > **Passpoint** > **Policy Name** > **NAI Realm**.
2. Select + to create a new NAI realm configuration for passpoint hotspot utilization, ✎ to modify the attributes of an existing configuration, or 🗑 to remove a selected configuration from the existing policies.

   Provide a realm name.
3. Set the following **EAP Method** attributes to secure the NAI realm used by the passpoint policy:

Index	Select an EAP instance index from 1 to 10 to apply to this hotspot’s EAP credential exchange and verification session. NAIs are often user identifiers in the EAP authentication protocol
Method	Set an EAP method for the NAI realm. Options include **`identity`**, **`otp`**, **`gtc`**, **`rsa-public-key`**, **`tls`**, **`sim`**, **`ttls`**, **`peap`**, **`ms-auth`**, **`ms-authv2`**, **`fast`**, **`psk`**, and **`ikev2`**
Authentication Type	Specify the EAP method authentication type. Options include **`expanded-eap`**, **`non-eap-inner`**, **`inner-eap`**, **`expanded-inner-eap`**, **`credential`**, **`tunn-eap-credential`**, and **`vendor`**
Authentication Value	If you are setting the authentication type to either **`non-eap-inner`**, **`inner-eap`**, **`credential`**, or **`tunnel-eap-credential`**, define an authentication value that must be shared with the EAP credential validation server resource. Options include **`chap`**, **`mschap`**, **`mschapv2`**, and **`pap`**
Authentication Vendor ID	If the authentication type is set to either **`expanded-eap`** or **`expanded-inner-eap`**, set a six-character authentication vendor ID. This ID must match the ID utilized by the EAP server resource
Authentication Vendor Specific	If required, add 2 to 510 character vendor-specific authentication data required for the selected authentication type. Type the value in an a- FA -F0-9 format
Authentication Vendor Type	Set an eight-character authentication vendor type used exclusively for the **`expanded-eap`** or **`expanded-inner-eap`** authentication types

4. Select **Add** to save the NAI realm updates.

Configure Passpoint Policy OSU Provider

WiNG managed clients can use *Online Sign-Up* (OSU) for registration and credential provisioning to obtain hotspot network access. Service providers have an OSU AAA server and certificate authority (CA). For a client and hotspot to trust one another, the OSU server holds a certificate signed by a CA whose root certificate is issued by a CA authorized by the Wi-Fi Alliance, and CA certificates are installed on the client device. A CA performs the following functions:

- Issues certificates (creates and signs)
- Maintains certificate status information and issues certificate revocation lists (CRLs)
- Publishes current (non-expired) certificates and CRLs
- Maintains status archives for the expired or revoked certificates it has issued

Passpoint certificates are governed by the Hotspot 2.0 OSU Certificate Policy Specification. An OSU server certificate should be obtained from any of the CAs authorized by the Wi-Fi Alliance. Once an OSU provider is selected, the client connects to the OSU WLAN. It then triggers an HTTPS connection to the OSU server, which was received with the OSU providers list. The client validates the server certificate to ensure it's a trusted OSU server. The client is prompted to complete an online registration through their browser. When the client has a valid credential for the hotspot 2.0 WLAN, it disassociates from the OSU WLAN and connects to the hotspot 2.0 WLAN.

1. Select + to create a new OSU provider configuration for passpoint hotspot utilization, ✎ to edit or modify the existing configuration attributes, or 🗑 to delete a selected configuration.
2. If you are creating a new OSU provider configuration, provide a 32-character maximum OSU ID that will serve as an online sign up identifier.
3. Set the following attributes to secure the *Network Access Identifier* (NAI) submitted by the hotspot during OSU authentication:

Server URL	Provide a 255 character maximum sign up server URL for the OSU provide
NAI	Type a 255 character maximum NAI to identify the user and assist in routing an authentication request to the authentication server. The realm name is often the domain name of the service provider

Method OMA DM Priority	Select to provide *Open Mobile Alliance* (OMA) device management priority. OMA is a standards body developing open standards for mobile clients. OMA is relevant to service providers working across countries (with different languages), operators and mobile terminals. Adherence to OMA is strictly voluntary. Use the drop-down list box to specify the priority as 1 or 2
Method Soap XML SPP Priority	Select to apply a SOAP-XML subscription provisioning protocol priority of either 1 or 2. The *Simple Object Access Protocol* (SOAP) is a protocol for exchanging structured information in web services. SOAP uses XML as its message format and relies on other application layer protocols, like HTTP or SMTP, for message negotiation and transmission

4. Refer to the **Name** field to set a 252-character English language sign up name, then provide a 3-character maximum ISO-639 language code to apply the sign up name in a language other than English.

   Apply a 252-character maximum hexadecimal online sign up name to encode in the ISO-639 language code applied to the sign up name.

5. Refer to the **OSU Provider Description** field to set an online sign up description in a language other than English.

   Select **Add** and provide a 3-character maximum ISO-639 language code to apply the sign up name in a language other than English.

   Apply a 252-character maximum hexadecimal online sign up description to encode in the ISO-639 language code applied to the sign up name.

6. Select **Add** and provide an **OSU Provider Icon**.

   Apply the following configuration attributes to the icon.

Code	Type a 3-character maximum ISO-639 language Code to define the language used in the OSU provider icon
File Name	Provide a 255-character maximum icon name and directory path location for the icon file
Height	Provide the icon's height in pixels from 0 to 65,535. The default setting is 0
Mime Type	Set the icon's MIME file type from 0 to 64. The MIME associates the file name extensions with a MIME type. A MIME allows a fallback on an extension and are frequently used by web servers
Width	Provide the icon's width in pixels from 0 to 65,535. The default setting is 0

7. Select **Add** to save OSU provider settings updates.

RADIUS Policy

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.

Create RADIUS Group

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.

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
Role	If a group is listed as a management group, it may also have a unique role assigned. Available roles include: • 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
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

Setting	Description
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: • 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: • 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	• 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

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:

1. Go to **Policies** > **RADIUS User Pool**.

   The RADIUS User Pool list opens and displays the existing user pool.
2. Select an existing user pool to edit an user.
3. Select 🗑 icon to delete a user pool.
4. Select + icon to add a new RADIUS user pool.

   The **Add Policy** dashboard opens.
5. 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

Setting	Description
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	The total amount of bandwidth available for each guest user. Options include: • Unlimited - no limit on the amount of data available for each guest user • Limited - Set data limit for each guest user ◦ 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: • 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 Links

- Configure RADIUS Server Policy on page 462
- Configure RADIUS Clients on page 464
- RADIUS Server Policy on page 460
- Configure an LDAP Server on page 467

Configure RADIUS Server Policy

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.

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

Setting	Description
Sources	Select **Add** to create a new authentication data source settings. Settings include: • 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
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: • 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

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:

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

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:

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	• 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	Select **Add** to create a RADIUS server policy realm and network address. Select 🗑 icon to delete an existing RADIUS service policy. Configure the following realms settings: • 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 Select the 👁 icon to reveal the shared secret's character string Select **Add** to include the realm in the proxy server.

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

Configure an LDAP Server

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:

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	Define whether this LDAP server is a primary or secondary server resource. Primary servers are always queried for connection first. 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 Primary option is selected by default
Network	• 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	• 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	• 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

Setting	Description
	• 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.

Smart RF 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 no `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.

Related Links

Configure Smart RF Basic Settings on page 470
Configure Smart RF Channel and Power Settings on page 473
Configure Smart RF Scanning Configuration on page 475
Configure Smart RF Recovery Settings on page 477
Configure Smart RF Select Shutdown Settings on page 480

Configure Smart RF Basic Settings

1. Select **Policies** > **Smart RF**.

   A list of existing Smart RF policies opens. Review existing Smart RF policies:

Policy	Displays the name assigned to the Smart RF policy when it was initially created. The name cannot be modified as part of the edit process
Status	A green check mark indicates that Smart RF has been activated for the listed policy. A red “X” designates the policy as being deactivated
Interference Recovery	A green check mark indicates that interference recovery has been activated for the listed policy. A red “X” designates the policy as being deactivated
Coverage Hole Recovery	A green check mark indicates that coverage hole recovery has been activated for the listed policy. A red “X” designates the policy as being deactivated
Neighbor Recovery	A green check mark indicates that neighbor recovery has been activated for the listed policy. A red “X” designates the policy as being deactivated

2. Select + to add a new Smart RF policy or ✎ to edit an existing Smart RF policy.

   The **Add Policy** window opens for new policy. The **Basic Settings** dashboard opens to edit basic configuration setting.
3. Assign a unique policy name and select **Add**.

   A new Smart RF policy is added and the **Basic Settings** dashboard opens.

4. Define the following basic settings:

Sensitivity	Select an option from the drop-down list box to configure Smart RF sensitivity. The options include: • Custom • High • Low • Medium The **Custom** option allows an administrator to adjust the parameters and thresholds for **Interference Recovery**, **Coverage Hole Recovery**, and **Neighbor Recovery**. Using the Low, Medium (recommended), and High settings allows these features to be utilized
Policy Enable	Select **Policy Enable** to enable Smart RF for immediate inclusion within an RF Domain. Smart RF is selected by default
Interference Recovery	Select **Interface Recovery** to enable compensations from neighboring radios when radio interference is detected. When interference is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client (as seen by the access point radio). If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. This option is selected by default
Coverage Hole Recovery	Select **Coverage Hole Recovery** to enable coverage compensation from neighboring radios when a radio coverage hole is detected within the Smart RF supported radio coverage area. When a coverage hole is detected, Smart RF first determines the power increase needed based on the signal-to-noise ratio for a client as seen by the access point radio. If a client's signal-to-noise value is above the threshold, the transmit power is increased until the signal-to-noise rate falls below the threshold. This option is selected by default
Neighbor Recovery	Select **Neighbor Recovery** to enable Neighbor Recovery when a failed radio is detected within the Smart RF supported radio coverage area. Smart RF can provide automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. Neighbor Recovery is selected by default when the sensitivity setting is **Medium**

5. Configure **Calibration Assignment** per area by selecting **Enable per Area** or **Enable per Floor**.

6. Configure **Smart Sensor** parameters to activate auto-provisioning of access points as sensors.

   It is important to get the right balance between the number of APs functioning as sensors and APs providing WLAN service in a larger deployment. Smart sensor automates provisioning of APs as sensors without compromising network security.

Enable Smart Sensor	Select **Enable Smart Sensor** to activate auto-provisioning of access points as sensors. Select this option to automatically turn on the sensor radios on 1/3rd of the deployed access points Note: By default, Smart RF selects and provisions only tri-radio APs as sensors. To enable Smart RF to select dual-radio APs, configure the Smart RF policy through the CLI and run the `no > smart-sensor > tri-radio-only` command
Auto Trigger	Select **Auto Trigger** to enable smart-sensor settings automatically Note: The smart-sensor calibration is auto-triggered when smart-sensor is enabled for the first time. In case a re-calibration is required, manually issue the `trigger-smartsensor` on command through the CLI to activate the algorithm. Re-calibration maybe needed if you change the number of APs deployed or the AP deployment pattern within the RF Domain
Algorithm Cell Size	Select **Algorithm Cell Size** to enable the use of an algorithmic function to identify the sensor APs. The WiNG Smart-sensor feature uses an algorithm to provision APs as sensor within a site (RF Domain). The algorithm creates a cluster of cells based on inputs from the Smart-RF neighbor table. Each cell in the cluster represents an AP and adjacent cells are the AP's neighbor. The algorithm then identifies APs with best coverage area and provisions them as sensors. However, the algorithmic calculations vary depending on the cell size. The current implementation provides two algorithms based on the cell size (dense, none, or sparse). Select the algorithm best suited for your deployment: • dense - Selects the algorithm best suited for dense deployments. In dense deployments, the cell-size is small, with APs deployed close to each other • none - No cell size is selected • sparse - Selects the algorithm best suited for sparse deployments. In sparse deployments, the cell-size is large, with APs deployed far apart from each other
Smart Band	Select the radio band frequency to work with smart sensor
Tri-Radio	Select to enable smart senor only on tri-radio access points

7. Select **Save** to configure and update Smart RF basic settings for this policy.

Configure Smart RF Channel and Power Settings

Use the **Channel and Power** dashboard to refine Smart RF power settings over 6 GHz, 5 GHz, and 2.4 GHz radios and select channel settings with respect to the device channel usage.

Note
The **Channel and Power Settings** parameters are activated only when **Custom** or **Medium** is selected as the **Sensitivity** setting from the Smart RF **Basic** dashboard.

1. Select **Policies** > **Smart RF**.

   A set of existing Smart RF policy list opens.
2. Select a Smart RF policy.
3. Select **Channel and Power**.
4. Refer to the **Power Settings** field to define Smart RF recovery settings for the selected 6 GHz (802.11ax), 5 GHz (802.11a) or 2.4 GHz (802.11bg) radio.

2.4 GHz Minimum Power	Use the spinner control to select a 1 dBm to 20 dBm minimum power level for Smart RF to assign to a radio in the 2.4 GHz band. The default setting is 4 dBm.
2.4 GHz Maximum Power	Use the spinner control to select a 1 dBm to 20 dBm maximum power level for Smart RF to assign to a radio in the 2.4 GHz band. The default setting is 17 dBm.
5 GHz Minimum Power	Use the spinner control to select a 1 dBm to 20 dBm minimum power level for Smart RF to assign to a radio in the 5 GHz band. The default setting is 4 dBm.
5 GHz Maximum Power	Use the spinner control to select a 1 dBm to 20 dBm maximum power level for Smart RF to assign to a radio in the 5 GHz band. The default setting is 17 dBm.
6 GHz Minimum Power	Use the spinner control to select a 1 dBm to 20 dBm minimum power level for Smart RF to assign to a radio in the 6 GHz band. The default setting is 4 dBm.
6 GHz Maximum Power	Use the spinner control to select a 1 dBm to 20 dBm maximum power level for Smart RF to assign to a radio in the 6 GHz band. The default setting is 17 dBm.

5. Set the following **Channel Settings** for the 6 GHz, 5 GHz, and 2.4 GHz radios.

2.4 GHz Channels	Use the drop-down list box to define the 2.4 GHz channels used for Smart RF assignments.
2.4 GHz Channel Width	20 MHz and 40 MHz channel widths are supported by the 802.11a radio. 20 MHz is the default setting for 2.4 GHz radios. 20 MHz or 40 MHz operation (the default setting for the 5 GHz radio) allows the access point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 Ghz and 5 GHz radios. If an 11n user selects two channels (a primary and secondary channel), the system is configured for dynamic 20 MHz or 40 MHz operation. When 20 MHz or 40 Mhz is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select **Automatic** to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. **Automatic** is the default setting.
5 GHz Channels	Use the drop-down list box to define the 5 GHz channels used for Smart RF assignments
5 GHz Channel Width	20 MHz, 40 MHz, and 80 MHz channel widths are supported by the 802.11a radio. 40 MHz is the default setting setting for 5 GHz radios. 20 MHz, 40 MHz, or 80 MHz operation allows the access point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a primary and secondary channel), the system is configured for dynamic 20/40 operation. When 20, 40, 80 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select **Automatic** to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. **Automatic** is the default setting. 80 MHz channel is used for 802.11ac access points

6 GHz Channels	Use the drop-down list box to define the 6 GHz channels used for Smart RF assignments.
6 GHz Channel Width	20 MHz, 40 MHz, 80 MHz, and 160 MHz channel widths are supported by the 802.11ax radio. 40 MHz is the default setting for the 6 GHz radio. 20 MHz, 40 MHz, 80 MHz, and 160 MHz operation allows the access point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a primary and secondary channel), the system is configured for dynamic 20/40 operation. When 20, 40, 80 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select **Automatic** to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. **Automatic** is the default setting. 80 MHz channel is used for 802.11ac access points

6. Select **Add** to create new area based channel settings.

   The **Settings** window opens.

7. Configure the following Area Based Channel Settings for the Smart RF policy:

Name	Specify the deployment area assigned to the listed policy when deployed as a means of identifying the device's physical locations.
Band	Select the radio band, either **2.4 GHz** , **5 GHz**, or **6 GHz** for the Smart RF policy assigned to the specified area.
Channel List	Select the channels associated with the Smart RF policy for the specified area and band.

8. Select **Add** to update area based channel settings.
9. Select 🗑 to delete an existing area based channel setting.
10. Select **Save** to update channel and power settings for this Smart RF policy.

Configure Smart RF Scanning Configuration

Set Smart RF policy smart monitoring and OCS monitoring using the Smart RF scanning configuration settings.

> **Note**
> The monitoring and scanning parameters in the **Scanning Configuration** screen are activated only when **Custom** is selected as the Sensitivity setting from the **Basic** dashboard.

1. Select **Policies** > **Smart RF**.

   A set of existing Smart RF policy list opens.

2. Select a Smart RF policy from the list.
3. Select **Scanning Configuration**.
4. Select or clear **Smart Monitoring Enable**.

   The feature is selected by default. When it is selected, detector radios monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.
5. Select **Add** and set **OCS Monitoring Awareness Settings** for the Smart RF policy.

Threshold	Select **Threshold** and specify a threshold from 10 to 10,000. When the threshold is reached, awareness settings are overridden with the values specified in the table
Index	Select an Index value from 1 to 3 for awareness overrides. The overrides are run based on index, with the lowest index being run first
Band	Use the drop-down list box to select a day of the week to apply the override. Selecting **All** will apply the policy every day. Selecting individual days of the week will apply the policy only on the selected days
Start Time	Set the starting time of day when the overrides will be activated. Use the spinner controls to select the hour and minute, in 24 hour time format
End Time	Set the ending time of day when the overrides will be deactivated. Use the spinner controls to select the hour and minute, in 24 hour time format

6. Set the following **Scanning Configuration for 5.0 GHz and 2.4 GHz** radio bands:

Duration	Set a channel scan duration (from 20 to 150 milliseconds) that access point radios use to monitor devices within the network and, if necessary, perform self healing, and neighbor recovery to compensate for coverage area losses within an RF Domain. The default setting is 50 milliseconds for 6.0 GHz, 5.0 GHz, and 2.4 GHz bands
Frequency	Use the spinner control to set a scan frequency between 1 to 120 seconds. The default setting is 6 seconds for 6.0 GHz, 5.0 GHz, and 2.4 GHz bands
Extended Scan Frequency	Use the spinner control to set an extended scan frequency between 0 to 50. This is the frequency in which radios scan channels on other than their peer radios. The default setting is 5 for 6.0 GHz, 5.0 GHz, and 2.4 GHz bands

Sample Count	Use the spinner control to set a sample scan count value between 1 to 15. This is the number of RF readings a radio gathers before it sends the data to the Smart RF manager. The default setting is 5 for 6.0 GHz, 5.0 GHz, and 2.4 GHz bands
Client Aware Scanning	Select **Client Aware Scanning** to set client awareness count between 1 to 255 during off channel scans for either 6.0 GHz, 5.0 GHz, or 2.4 GHz bands
Power Save Aware Scanning	Select **Dynamic**, **Strict**, or **Disable** to define how power save scanning is set for Smart RF. Strict turns off smart monitoring as long as a power save capable client is associated to a radio. Dynamic turns off smart monitoring as long as there is data buffered for a power save client at the radio. The default setting is Dynamic for 6.0 GHz, 5.0 GHz, and 2.4 GHz bands
Voice Aware Scanning	Select **Dynamic**, **Strict**, or **Disable** to define how voice aware recognition is set for Smart RF. Strict turns off smart monitoring as long as a power save capable client is associated to a radio. Dynamic turns off smart monitoring as long as there is data buffered for a voice client at the radio. The default setting is Dynamic for 6.0 GHz, 5.0 GHz, and 2.4 GHz bands
Transmit Load Aware Scanning	Select **Transmit Load Aware Scanning** to set a transmit load percentage from 1 to 100 serving as a threshold before scanning is avoided for an access point’s 6.0 GHz, 5.0 GHz, or 2.4 GHz radio

7. Select **Save** to update scanning configuration for this Smart RF policy.

Configure Smart RF Recovery Settings

Set the Smart RF recovery settings using the **Recovery** configuration options.

Note

The recovery parameters within the Neighbor Recovery, Interference, and Coverage Hole Recovery tabs are enabled only when **Custom** is selected as the **Sensitivity** setting from the Smart RF **Basic** screen.

The Neighbor Recovery tab displays by default. Use the Neighbor, Interference, and Coverage Hole recovery tabs to define how 6.0 GHz, 5.0 GHz, and 2.4 GHz radios compensate for failed neighbor radios, interference that affects the Smart RF supported network, and detected coverage holes that require intervention by neighbor radios.

1. Select **Policies** > **Smart RF**.

   A set of existing Smart RF policy list opens.
2. Select a Smart RF policy from the list.
3. Select **Recovery**.
4. Use the **Power Hold Time** field to define the minimum time between two radio power changes during neighbor recovery.

   Set the time between 0 to 3600 seconds.
5. Set the following **Neighbor Recovery** parameters:

6 GHz Neighbor Power Threshold	Set the maximum power increase threshold from -85 dBm to -55 dBm that the 6.0 GHz radio uses if it is required to increase its output power to compensate for a failed radio within its wireless radio coverage area. The default value is -70 dBm
5 GHz Neighbor Power Threshold	Set the maximum power increase threshold from -85 dBm to -55 dBm that the 5.0 GHz radio uses if it is required to increase its output power to compensate for a failed radio within its wireless radio coverage area. The default value is -70 dBm
2.4 GHz Neighbor Power Threshold	Set the maximum power increase threshold from -85 dBm to -55 dBm that the 2.4 GHz radio uses if it is required to increase its output power to compensate for a failed radio within its wireless radio coverage area. The default value is -70 dBm

6. Set the following **Dynamic Sample Recovery** parameters:

Dynamic Sample Enabled	Select **Dynamic Sample Enabled** to activate dynamic sampling. Dynamic sampling allows an administrator to define how Smart RF adjustments are triggered by locking retry and threshold values. This option is not activated by default
Dynamic Sample Retries	Set the number of retries (from 1 to 10) attempted before a power level adjustment is implemented to compensate for a potential coverage hole. The default setting is 3
Dynamic Sample Threshold	Set the minimum number of sample reports (from 1 to 30) used before a Smart RF power compensation requires dynamic sampling. The default setting is 5

7. Configure Smart RF **Interference Recovery** settings:

Interference	Select **Interference** to allow the Smart RF policy to scan for excess interference from supported radio devices. WLANs are susceptible to sources of interference, such as neighboring radios, cordless phones, microwave ovens, and Bluetooth devices. When interference for WiFi sources is detected, Smart RF supported devices can change the channel and move to a clearer channel. This feature is activated by default
Noise	Select **Noise** to allow the Smart RF policy to scan for excess noise from WiFi devices. When detected, Smart RF supported devices can change their channel and move to a clearer channel. This feature is activated by default
Noise Factor	Set the level of network interference detected taken into consideration by Smart RF during interference recovery calculations. The default setting is 1.5
Channel Hold Time	Define the minimum time between channel changes during neighbor recovery. Set the time between 0 to 86,400 seconds. The default setting is 1400 seconds
Client Threshold	Set a client threshold for the Smart RF policy between 1 to 255. If the set threshold number of clients are connected to a radio, the radio does not change its channel, even though required, based on the interference recovery determination made by the Smart RF admin. The default setting is 50
6 GHz Channel Switch Delta	Set a channel switch delta (interference delta), from 5 dBm to 35 dBm, for the 6.0 GHz radio. This parameter is the difference between noise levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm

5 GHz Channel Switch Delta	Set a channel switch delta (interference delta), from 5 dBm to 35 dBm, for the 5.0 GHz radio. This parameter is the difference between noise levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm
2.4 GHz Channel Switch Delta	Set a channel switch delta (interference delta), from 5 dBm to 35 dBm, for the 2.4 GHz radio. This parameter is the difference between noise levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm

8. Configure Smart RF **Coverage Hole Recovery for 6 GHz, 5 GHz and 2.4 GHz** radios:

Client Threshold	Use the spinner to set a client threshold for the Smart RF policy between 1 to 255. This is the minimum number of clients a radio should have associated in order for coverage hole recovery to start. The default setting is 1
SNR Threshold	Set a signal-to-noise (SNR) threshold , between 1 to 75 dB. This is the signal-to-noise threshold for an associated client as seen by its associated access point radio. When exceeded, the radio increases its transmit power in order to increase coverage for the associated client. The default value is 20 dB for 2.4 GHz, 5.0 GHz, and 6.0 GHz radios
Coverage Interval	Define the length of time (between 1 to 120 seconds) after which coverage hole recovery should be initiated when a coverage hole is detected. The default is 10 seconds for 2.4 GHz, 5.0 GHz, and 6.0 GHz radios
Interval	Define the length of time (between 1 to 120 seconds) coverage hole recovery should be conducted before a coverage hole is detected. The default is 30 seconds for 2.4 GHz, 5.0 GHz, and 6.0 GHz radios

9. Select **Save** to update the Smart RF recovery settings for this policy.

Configure Smart RF Select Shutdown Settings

Configuring auto-shutdown of select 2.4 GHz radios—in dual-band networks—maintains CCI levels within specified limits. When **Select Shutdown** is enabled, Smart RF monitors CCI levels to ensure that the deployment average CCI remains within specified minimum and maximum limits. If the deployment average CCI is found to exceed the maximum threshold, 2.4 GHz radios causing neighbor interference are shut down one-by-one until the deployment average CCI falls below the specified maximum threshold. The reverse process occurs when the deployment average CCI falls below the minimum threshold. In this scenario, previously deactivated radios are activated until the deployment average CCI reaches acceptable levels.

Use this procedure to activate auto-shutdown of 2.4 GHz access point radios causing interference within the Smart RF monitored network.

1. Go to **Policies** > **Smart RF** <*select a Smart RF policy*> **Select Shutdown**.
2. Toggle the **Select Shutdown** slider to enable auto-shutdown.
3. Configure auto-shutdown parameters as described in Table 151.

Table 151: Select Shutdown Parameters

Parameter	Description
CCI High Threshold	Specify the maximum CCI threshold from -85 dBm to -55 dBm. If the threshold is not specified, the system uses the default value as the upper limit for the deployment average CCI range. The default value is -80 dBm.
CCI Low Threshold	Specify the minimum CCI threshold from -100 dBm to -55 dBm. If the threshold is not specified, the system uses the default value as the lower limit for the deployment average CCI range. The default value is -100 dBm.
Frequency	Set the interval, in minutes, at which 2.4 GHz radios are selected for shutdown. When the deployment average CCI exceeds the specified maximum threshold, Smart RF shuts down 2.4 GHz radios until the CCI reaches acceptable levels. Use this option to configure the interval between successive radio shutdown events. Specify a Frequency in the range 0 – 3600 minutes. The default is 60 minutes.
Frequency Limiter	Configure the minimum multiple of Interference Recovery frequency that the select-shutdown frequency can be set to. Specify a value from 1 to 1000. The default value is 10.

4. After you have completed configuring the settings, choose from the following actions:

   a. Select **Revert** to restore default settings or restore the last saved settings.

   Note
   You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

Note
This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

Note
If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Sensor Policy

The ExtremeLocation system for Wi-Fi locationing 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 Links

Configure a Sensor Policy on page 482

Configure a Sensor Policy

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

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	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 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 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
Channel Width	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) 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 With **Channel-Lock** selected: You cannot adjust the width between adjacent channels, because only one channel is locked
Scan Weight	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. With **Custom-Scan** selected: Each selected channel can have its weight prioritized with respect to the amount of time a scan is permitted within the defined RSSI scan interval With **Channel-Lock** selected: With one channel locked for an RSSI scan, you cannot adjust scan weights for other, unlocked channels

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

Configure a URL List Policy

A **URL List** policy is used in conjunction with a **URL Filtering** policy. After a URL List policy is configured, it becomes selectable when configuring a URL Filtering policy if you choose the **Filter Method** option **`url_list`**.

URL lists are used to select highly utilized URLs for smart caching. The selected URLs are monitored and routed according to existing cache content policies.

Use this procedure to configure, modify, or delete a URL List policy:

1. Go to **Policies** > **URL List**.

   If any policies are configured, they appear in the URL List window in tabular form. The total number of configured URL List policies is shown in parentheses.
2. Choose from the following actions:
   - Select + to create a new URL List policy.
     a. Enter a **Name** for the policy. The name cannot exceed 32 characters.
     b. Select **Add** to create the policy.
     c. Proceed to configuring URL Entries in the next step.

     Note
     If you exit the URL List policy configuration without first adding and saving any URL Entries, the configured URL List policy persists, but only until you log out.
   - Under the **Actions** column, choose from the following:
     - Select ✎ associated with a policy to modify it. Edit the URL entries in accordance with the steps in this procedure. The URL List policy Name cannot be edited.
     - Select 🗑 associated with a policy to delete it.
3. In the **URL Entries** window, choose from the following actions:
   - Select **Add** to add a new URL. Proceed to the next step.
   - Select 🗑 associated with a URL entry to delete it.
4. Configure the URL Entries parameters as described in Table 152.

Table 152: URL Entries Parameters

Parameter	Description
URL	Enter the requested URL that is to be monitored and routed according to existing cache content policies. This value is mandatory.
Depth	Select the number of levels to be cached. Because Web sites have different parameters to uniquely identify specific content, the same content may be stored on multiple origin servers. Smart caching uses subsets of these parameters to recognize that the content is the same and serves it from cache. Enter a value in the range 1 – 10. This value is mandatory.

5. After you have completed configuring the settings, choose from the following actions:
   a. Select **Revert** to restore default settings or restore the last saved settings.

   Note
   You cannot restore default settings after applying or saving changes.

b. Select **Apply** to commit the configured settings.

> Note
> This does not permanently save the settings you configured. If you perform a Reload (warm reboot), applied settings will be lost.

c. Select **Save** to commit and save the configured settings.

> Note
> If you do not select **Apply** or **Save**, the settings that you configured are not saved when you move away from the configuration window.

Related Links

URL Filtering Policy on page 285

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 Links

Configure a WIPS Policy on page 485
Configure WIPS Events on page 487
Configure WIPS Signatures on page 489

Configure a WIPS Policy

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.

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

Setting	Description
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
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 Links

WIPS Policy on page 485

Configure WIPS Events on page 487

Configure WIPS Signatures on page 489

Configure WIPS Events

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

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
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 Links

WIPS Policy on page 485

Configure a WIPS Policy on page 485

Configure WIPS Signatures on page 489

Configure WIPS Signatures

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
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.

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

Setting	Description
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
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

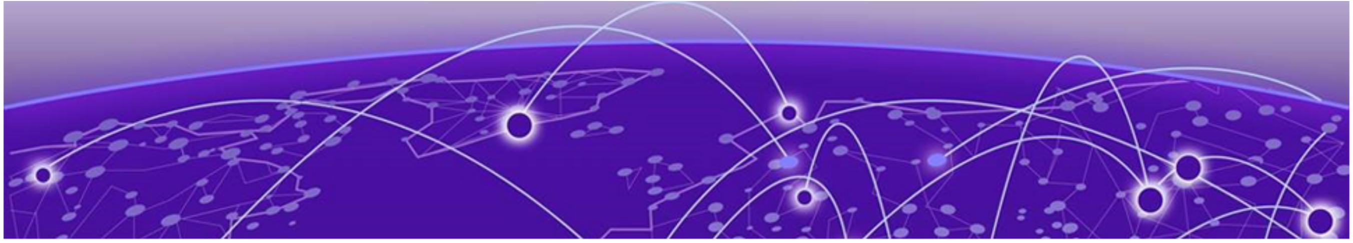
7. Select **Update** to save the WIPS signature configuration.

Related Links

WIPS Policy on page 485

Configure a WIPS Policy on page 485

Configure WIPS Events on page 487



Firmware Update and 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:

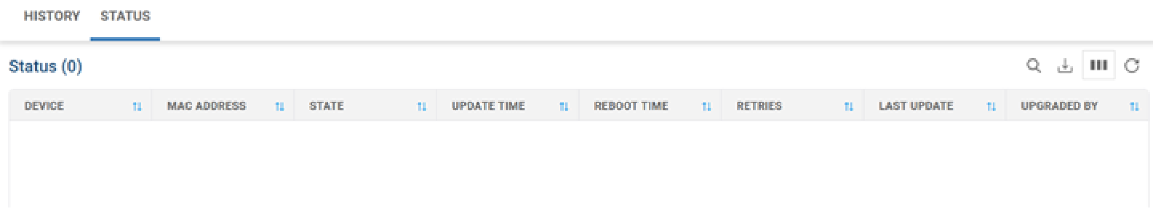
Device Type	Select a device type from the drop-down list box
Path/File	Provide an image path
Site	Select a site from the list of available sites
Device	Select a device from the site

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

Firmware Update Status

Once an update operation has been started or scheduled, an administrator can assess whether the firmware update was successful, the number of times the operation was attempted before completed, and the updated device's current status.

1. Select **Firmware** > **Update** > **Status**.
2. Use the **Status** dashboard to search, download, view, and refresh device update status.



Status (0)

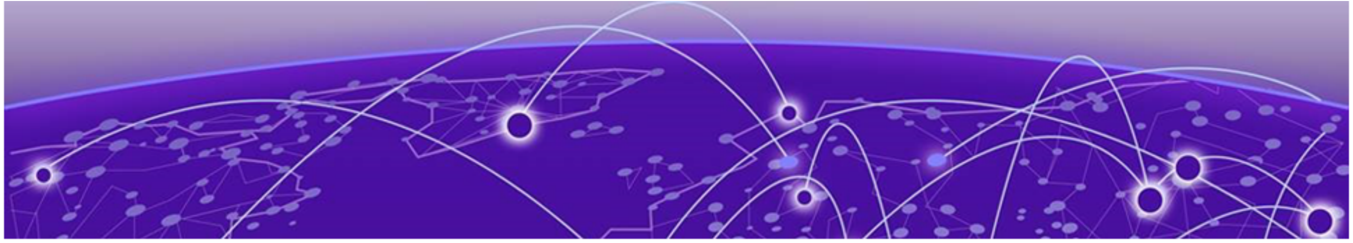
DEVICE	MAC ADDRESS	STATE	UPDATE TIME	REBOOT TIME	RETRIES	LAST UPDATE	UPGRADED BY

Figure 4: Device update status dashboard

Device	Displays the model number of devices pending an update. Each listed device is provisioned an image file unique to that model
MAC Address	Lists the factory encoded MAC address of a device either currently updating or in the queue of scheduled updates
State	Displays the state of the disk during the update process

Update Time	Displays whether an update is immediate or set by an administrator for a specific time. Staggering update is helpful to ensure a sufficient number of devices remain in service at any given time while others are updating
Reboot Time	Displays whether a reboot is immediate or time set by an administrator for a specific time. Reboots render the device offline, so planning reboots carefully is central to ensuring a sufficient number of devices remain in service
Progress	Lists the number of specific device types currently updating
Retries	Displays the number of retries, if any, needed for an in-progress firmware update operation
Last Update	Lists the last reported update and reboot status of each listed in progress or planned update operation
Upgraded By	Lists the model of the controller, service platform or access point RF Domain manager that’s provisioning an image to a listed device

3. Select ⤓ download the update status as a CSV file.



Statistics

Statistics display detailed information about how device policies configured by the user for various managed devices work in the ExtremeWireless WiNG environment. Through Statistics views, 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.

View and Manage Statistics

Statistics are compiled for devices within an ExtremeWireless WiNG controller-manged **Site** (RF Domain).

View Statistics

Go to **Statistics** and select the type of statistics you want to view. Choices are:

- Smart RF
- Wireless
- Devices
- Clients
- Sites
- Mesh Point

When you select any Statistics type, the **Sites** window opens. At a minimum, this window includes:

- A list of Sites managed by the controller
- Tools that allow you to manage the information displayed

> Note
> Any information displayed in the Sites window that is unique to a Statisics type is described in the relevant section of this chapter.

Select a Site under the **Site Name** column to view statistics for the RF Domain or RF Domain member devices.

Manage Statistics Views

Most Statistics windows display information in tabular form and provide a common set of tools you can use to manage the information displayed.

Choose from the following actions:

- Select the sort icon ⇅ adjacent to a column heading to sort the data by the heading topic. By default, the data is sorted in ascending order, as indicated by the direction of the arrow in the icon ↑1. Toggle the icon to sort the column data in descending order ↓1. The "1" indicates by which column heading topic the data is currently sorted.
- Select 🔍 and enter a keyword in the search field to narrow the list of entries in the table. Select ✕ to revert to the default list view.
- Select ⤓ to download table entries in csv format.
- Select ▥ to choose the columns displayed in the table.
- Select ⟳ to refresh the list.
- Use « ‹ 1 2 › » to navigate pages if multiple pages exist.

> Note
> Any tool that is unique to a Statisics type is described in the relevant section of this chapter.

Smart RF

When invoked by an administrator, Smart RF *(Self-Monitoring At Run Time)* instructs Access Point (AP) radios to change to a specific channel and begin beaconing using the maximum available transmit power. Within a well-planned deployment, any RF Domain member AP radio should be reachable by at least one other radio. Smart RF records signals received from its neighbors as well as signals from external, unmanaged radios. AP-to-AP distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

By examining Smart RF statistics, administrators are able to assess the efficiency of RF Domains and take action where necessary.

Go to **Statistics** > **Smart RF**.

The Smart RF window displays a list of **Sites** managed by the controller. If a Smart RF policy is assigned to a site, the **Policy Name** is identified.

To view Smart RF statistics for an RF domain, select a site under the **Site Name** column that has an associated Smart RF policy. The Smart RF statistics are arranged under the following tabs:

- Basic on page 497
- Activity on page 498
- Neighbors on page 498
- Interference on page 499
- Channel Distribution on page 500
- Energy on page 500
- History on page 502
- Select Shutdown on page 502
- Sensor on page 503

Related Links

View and Manage Statistics on page 495

Basic

The **Basic** tab displays a list of RF domain members and related details in tabular form. Table 153 describes the type of information displayed under each column in the table.

Table 153: Smart RF Statistics – Basic Table Column Headings

Column Heading	Description
Hostname	Displays the administrator defined hostname assigned to RF domain member AP.
MAC Address	Displays the AP factory-encoded hardware MAC address.
Radio MAC	Displays the factory-encoded hardware MAC address of the AP radio.
Radio ID	Lists each radio’s designation (radio 1, radio 2 or radio 3).
Type	Identifies the 802.11 radio type.
State	Indicates the current operational state of a AP. Possible states are: • normal • offline • sensor
Channel	Identifies on which channel the device is detected.
Power	Displays the configured transmit output power of device radios.

Related Links

Smart RF on page 496

View and Manage Statistics on page 495

Activity

Use the statistics displayed under the **Activity** tab to assess the significance of any Smart RF initiated compensations within the RF Domain.

The **Activity** tab displays Smart RF activity details of RF Domain member radios in tabular form. Table 154 describes the type of information displayed under each column in the Activity table.

Table 154: Smart RF Statistics – Activity Table Column Headings

Column Heading	Description
Hostname	Displays the administrator assigned hostname assigned to a RF Domain member AP.
MAC Address	Displays the AP factory-encoded hardware MAC address.
Type	Identifies the 802.11 radio type.
Channel	Displays the number of Smart RF initiated channel changes reported for the RF Domain member radio.
Coverage	Displays the number of Smart RF initiated coverage changes reported for this RF Domain member radio.
Power	Displays the number of Smart RF initiated power level changes reported for the RF Domain member radio.
Shutdowns	Displays the number of Smart RF initiated shutdowns reported for the RF Domain member radio.
Total	Displays the total number of Smart RF initiated compensations reported for the RF Domain member radio.

Related Links

Smart RF on page 496

View and Manage Statistics on page 495

Neighbors

Refer to the **Neighbors** tab to review the attributes of neighbor radio resources that are available for Smart RF radio compensations for other RF Domain member radios.

The Neighbors tab displays a list of RF Domain member radios and related details in tabular form. You can expand the view to see the attributes of any neighbor radios.

Table 155 describes the type of information displayed under each column in the Neighbors table.

Table 155: Smart RF Statistics – Neighbors Table Column Headings

Column Heading	Description
Hostname	Displays the administrator defined hostname assigned to RF domain member AP.
Radio ID	Indicates each radio's designation (radio 1, radio 2 or radio 3).
MAC Address	Displays the radio's MAC address.
Channel	Identifies the radio's current operating channel.
Neighbors	Select + to view the same type of information described in this table, as it pertains to a neighbor radio. Also displayed are **Neighbor Power** (current operating power in dBm) and **Neighbor Attenuation** (measure of the reduction of signal strength during transmission in dB). Note: Attenuation is the opposite of amplification, and is normal when a signal is sent from one point to another. If the signal attenuates too much, it becomes unintelligible. Attenuation is measured in decibels.

Related Links

Smart RF on page 496

View and Manage Statistics on page 495

Interference

Review the information in the **Interference** tab to assess RF Domain member radios whose level of interference exceeds the threshold set for acceptable performance.

The Interference tab displays details about RF Domain radio performance based on received signal strength indication (RSSI). Table 156 describes the type of information displayed under each column in the Interference table.

Table 156: Smart RF Statistics – Interference Table Column Headings

Column Heading	Description
Interferer	Lists the administrator defined name of the interfering RF Domain device.
Radio MAC	Displays the factory encoded hardware MAC address assigned to the RF Domain device radio.
Vendor	Displays the vendor name (manufacturer) of the interfering RF Domain device radio.
Radio	Displays the model and numerical value assigned to the radio as its unique identifier.

Table 156: Smart RF Statistics – Interference Table Column Headings (continued)

Column Heading	Description
Channel	Displays the channel on which interference was detected for RF Domain device radios. Numerous interfering devices on the same channel could signal the need for better channel segregation to reduce the levels of detected interference.
RSSI	Lists a RSSI (in dBm) for those RF Domain devices falling into the poorest performing 10 devices based on the administrator defined threshold value.

Related Links

Smart RF on page 496

View and Manage Statistics on page 495

Channel Distribution

Use the data provided in the **Channel Distribution** tab to determine how RF domain member devices are utilizing different channels to optimally support connected devices and avoid congestion and interference with neighboring devices. Use this data to assess whether the channel spectrum is being effectively utilized and whether channel changes are warranted to improve RF domain member device performance.

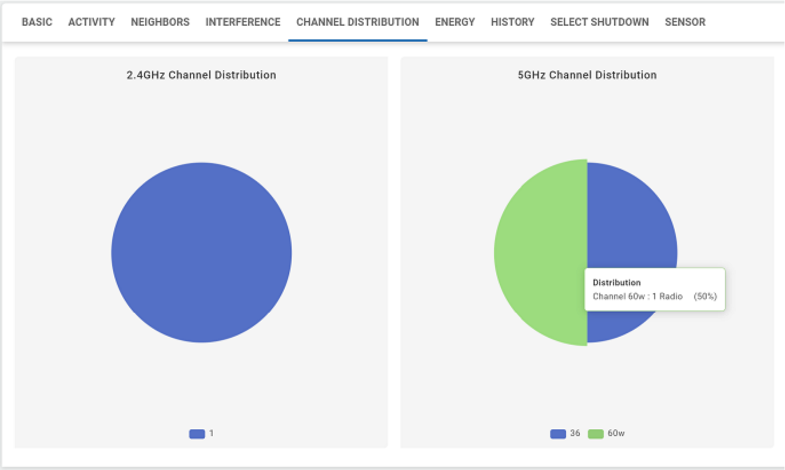


Figure 5: Channel Distribution Chart

Related Links

Smart RF on page 496

Energy

The **Energy** tab displays a list of RF Domain member radios and related details in tabular form.

Table 157 describes the type of information displayed under each column in the Energy table.

Table 157: Smart RF Statistics – Energy Table Column Headings

Column Heading	Description
Hostname	Displays the administrator defined hostname assigned to the RF domain member AP.
MAC Address	Displays the AP MAC address.
Radio MAC	Displays the factory encoded hardware MAC address of the AP radio. You can select an AP's corresponding **Radio MAC** address to open an **Energy** graph depicting .
Radio ID	Indicates each radio’s designation (radio 1, radio 2 or radio 3).
Radio Type	Identifies the 802.11 radio type.
Channel	Identifies the radio's current operating channel.

If a RF Domain member radio's operational state is normal (use `show smart-rf ap` command on CLI), you can select the radio's MAC Address to open an **Energy** graph, as shown in Figure 6. The Smart RF Energy graph displays the selected radio's operating channels, noise level and neighbor count. Use this information to assess whether Smart RF neighbor recovery is needed with respect to poorly performing radios.

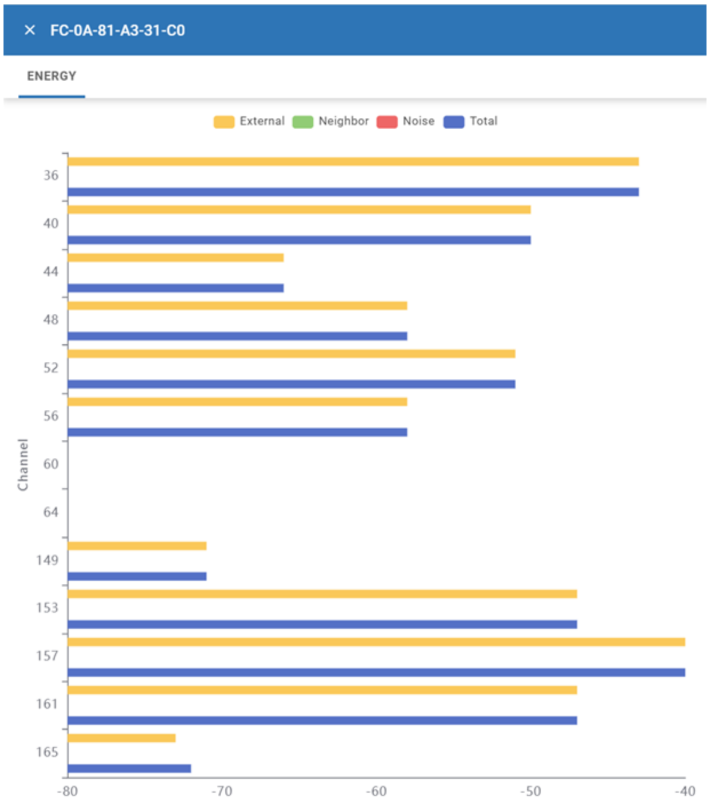


Figure 6: Smart RF Statistics - Example Energy Display

Related Links

Smart RF on page 496

View and Manage Statistics on page 495

History

Select the **History** tab to review Smart RF events impacting RF Domain members. Table 158 describes the type of information displayed under each column in the History table.

Table 158: Smart RF Statistics – History Table Column Headings

Column Heading	Description
Timestamp	Displays the time stamp when Smart RF status was updated to record a Smart RF adjustment within the selected RF Domain.
Event	Provides a high-level description of the Smart RF activity initiated for a RF Domain member.
Description	Provides a more detailed description of the Smart RF event with respect to the actual Smart RF calibration or adjustment made to compensate for detected coverage holes and interference.

Related Links

Smart RF on page 496

View and Manage Statistics on page 495

Select Shutdown

The **Select Shutdown** tab displays the 2.4 GHz APs that have been shut down to maintain CCI levels.

Note

This information is displayed only if Select Shutdown is enabled in a deployed Smart RF policy. For more information, see Configure Smart RF Select Shutdown Settings on page 480.

Details about the RF Domain member radios that have been automatically shut down are presented in tabular form. Table 159 describes the type of information displayed under each column in the table.

Table 159: Smart RF Statistics – Select Shutdown Table Column Headings

Column Heading	Description
AP Hostname	Displays the hostname of an AP that was shut down by Smart RF as part of the Select Shutdown feature process.
AP MAC	Displays the MAC address of an AP.
Radio	Identifies a radio that was shutdown.

Table 159: Smart RF Statistics – Select Shutdown Table Column Headings (continued)

Column Heading	Description
Radio MAC	Displays the MAC address of a radio.
Radio Status	Indicates the current status of a radio.

Related Links

Smart RF on page 496

View and Manage Statistics on page 495

Sensor

Select the **Sensor** tab to review which RF Domain member APs have dedicated sensors and determine whether there is adequate coverage for the RF Domain.

Table 160 describes the type of information displayed under each column in the Sensor table.

Table 160: Smart RF Statistics – Sensor Table Column Headings

Column Heading	Description
Hostname	Displays the administrator defined hostname assigned to RF domain member AP.
MAC	Displays the AP factory-encoded hardware MAC address.
Status	Displays the radio sensor status. Possible status displays are On or Off.

Related Links

Smart RF on page 496

View and Manage Statistics on page 495

Wireless

Use **Wireless** statistics to monitor radio performance of RF Domain Wireless LAN (WLAN) members.

Go to **Statistics** > **Wireless**. The Wireless window displays a list of **Sites** managed by the controller.

To view RF Domain WLAN statistics, select a site under the **Site Name** column to open the **Basic** window. See Basic on page 503 for details on information displayed in the Basic window.

Basic

Go to **Statistics** > **Wireless**, then select a Site in the list.

The **Basic** pane displays Wireless statistics for the selected Site, in tabular form. Table 161 describes the type of information displayed under each column in the table.

Table 161: Wireless Statistics - Basic List Column Headings

Column Heading	Description
Name	The administrator assigned SSID for the WLAN.
User Traffic	Displays the rate (in kbps) user data is transmitted and received by each WLAN member AP radio. This rate only applies to user data and does not include any management overhead.
Management Packets	Displays the total number of management packets transmitted and received by each WLAN member AP radio within the WLAN.
Throughput	Displays the data throughput (in bps) within the WLAN.
Radio Count	Displays the number of WLAN member AP radios currently in use.
Dropped Count	Displays the total number of packets dropped by each WLAN member AP radio during transmission. This includes user data as well as management overhead packets.
Error Count	Displays the total number of packets containing errors, received by each WLAN member AP radio. The higher the error rate, the less reliable the connection or data transfer.

Related Links

Wireless on page 503

View and Manage Statistics on page 495

Devices

Use the **Devices** statistics to monitor RF Domain member performance and make adjustments as required.

In addition to basic device information (model, serial number, MAC address, status, firmware, power management), you can view the following data:

- Resource (CPU, Disk, RAM) usage
- Interface characteristics and operations
- NTP status and statistics of an associated NTP Server of an AP
- Adoption, upgrade, and reboot history

To view RF Domain member device statistics:

1. Go to **Statistics** > **Devices**. The Devices window displays a list of **Sites** managed by the controller.
2. Select a site under the **Site Name** column to open the **Basic** window.
3. Select a device under the **Hostname** column.

See Basic on page 505 for details on information displayed in the Basic window.

Basic

Go to **Statistics** > **Devices**, then select a Site in the list. The **Basic** pane opens, displaying all the RF Domain member devices and related details in tabular form.

You can select a device under the **Hostname** column to view a graphical presentation of the device's statistics. The controller and access point statistics differ.

Table 162 describes the type of information displayed under each column in the Basic table.

Table 162: Devices Statistics - Basic Table Column Headings

Column Heading	Description
Hostname	Displays the administrator-assigned host name of the RF Domain member device.
MAC	Displays the MAC address of the device.
Type	Identifies the device type, for example AP410C-1.
Model	Identifies the device model, for example AP410C-1-WR.
Controller	Indicates whether a device is a controller, as follows: • ✗ – is not a controller • ✓ – is a controller
Adopted By	Identifies the MAC address of the controller which has adopted the device.
Profile	Displays the name of the Profile assigned to the device.
Version	Displays the current device firmware version.
IP	Displays the device's primary IP address.
Last Adoption	Indicates the time at which the device was last adopted by the controller within the past 24 hrs.

Related Links

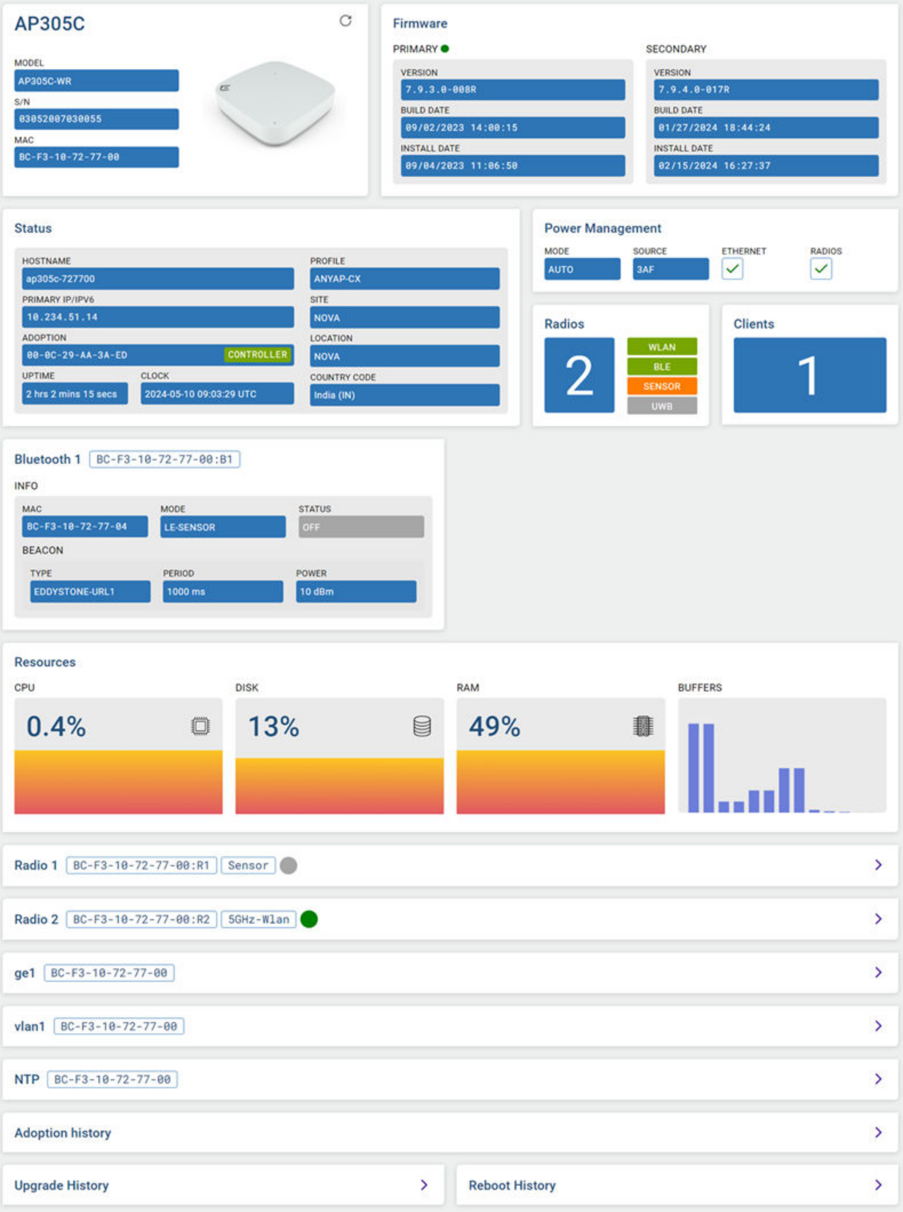
View and Manage Statistics on page 495

Access Point Statistics on page 505

Controller Statistics on page 522

Access Point Statistics

Figure 7 shows an example of a device statistics display for APs.



AP305C

MODEL: AP305C-WR

S/N: 03052007030055

MAC: BC-F3-10-72-77-00

Firmware

PRIMARY ●

VERSION: 7.9.3.0-008R

BUILD DATE: 09/02/2023 14:00:15

INSTALL DATE: 09/04/2023 11:06:50

SECONDARY

VERSION: 7.9.4.0-017R

BUILD DATE: 01/27/2024 18:44:24

INSTALL DATE: 02/15/2024 16:27:37

Status

HOSTNAME: ap305c-727700

PROFILE: ANYAP-CX

PRIMARY IP/IPV6: 10.234.51.14

SITE: NOVA

ADOPTION: 00-0C-29-AA-3A-ED CONTROLLER

LOCATION: NOVA

UPTIME: 2 hrs 2 mins 15 secs

CLOCK: 2024-05-10 09:03:29 UTC

COUNTRY CODE: India (IN)

Power Management

MODE: AUTO

SOURCE: 3AF

ETHERNET: ☑

RADIOS: ☑

Radios: 2 (WLAN, BLE, SENSOR, UWB)

Clients: 1

Bluetooth 1 BC-F3-10-72-77-00:B1

INFO

MAC: BC-F3-10-72-77-04

MODE: LE-SENSOR

STATUS: OFF

BEACON

TYPE: EDDYSTONE-URL1

PERIOD: 1000 ms

POWER: 10 dBm

Resources

CPU: 0.4%

DISK: 13%

RAM: 49%

Radio 1 BC-F3-10-72-77-00:R1 Sensor ●

Radio 2 BC-F3-10-72-77-00:R2 5GHz-Wlan ●

ge1 BC-F3-10-72-77-00

vlan1 BC-F3-10-72-77-00

NTP BC-F3-10-72-77-00

Figure 7: Example of Device Statistics Display for APs

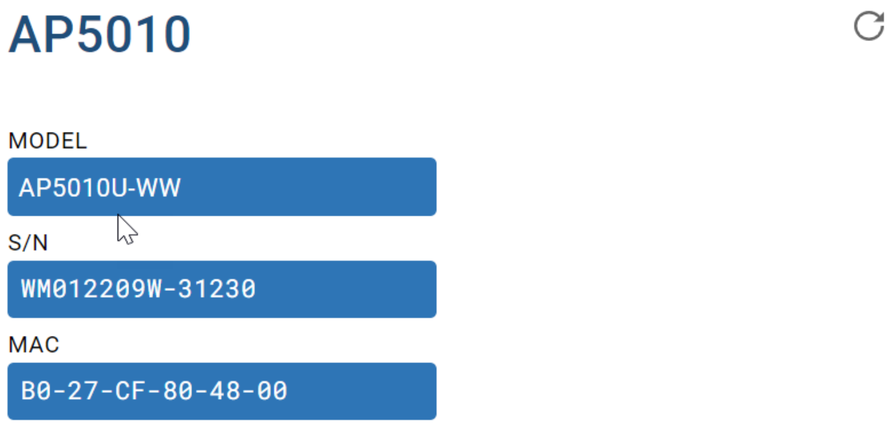
Access Point (AP) statistics are arranged under the following panes (left-to-right, top-to-bottom):

- Device Information on page 507
- Firmware on page 507
- Status on page 508
- Power Management on page 509
- Radios and Clients on page 510
- Bluetooth on page 511
- Resources on page 512
- Radios on page 513

- GbE Ports on page 514
- VLANs on page 519
- NTP on page 520
- Adoption History on page 520
- Upgrade History on page 521
- Reboot History on page 521

Device Information

Figure 8 shows an example of device information displayed for APs in the RF Domain.



AP5010

MODEL

AP5010U-WW

S/N

WM012209W-31230

MAC

B0-27-CF-80-48-00

Figure 8: AP Statistics – Example Device Information Display

Select ↻ to refresh the display.

Table 163 describes the information displayed.

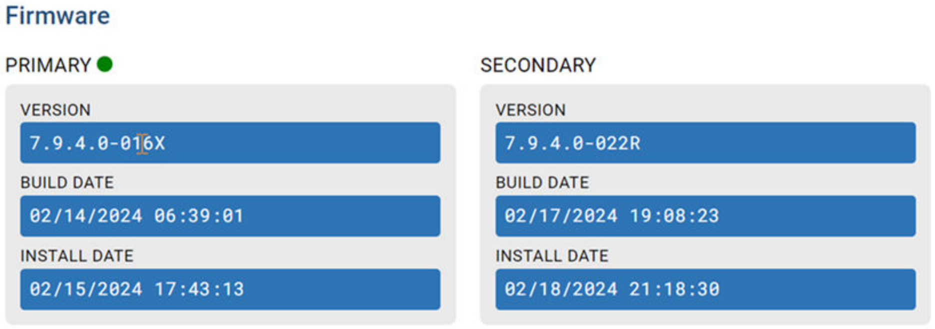
Table 163: AP Statistics – Device Information Description

Field	Description
Type	The AP type is displayed in the upper–left position of the pane.
Model	Displays the model of the selected AP to distinguish its exact SKU and country of operation.
S/N	Displays the serial number of the AP.
MAC	Displays the MAC address of the AP. This is factory assigned and cannot be changed.

Firmware

Figure 9 shows an example of device firmware information displayed for APs in the RF Domain.

You can store both a **Primary** and **Secondary** firmware version in memory. An automatic fallback mechanism exists, which loads the Secondary version if the Primary version fails. A ● appears adjacent to either Primary or Secondary, indicating which firmware is currently in use.



Firmware

PRIMARY ●

VERSION: 7.9.4.0-016X

BUILD DATE: 02/14/2024 06:39:01

INSTALL DATE: 02/15/2024 17:43:13

SECONDARY

VERSION: 7.9.4.0-022R

BUILD DATE: 02/17/2024 19:08:23

INSTALL DATE: 02/18/2024 21:18:30

Figure 9: AP Statistics – Example Firmware Information Display

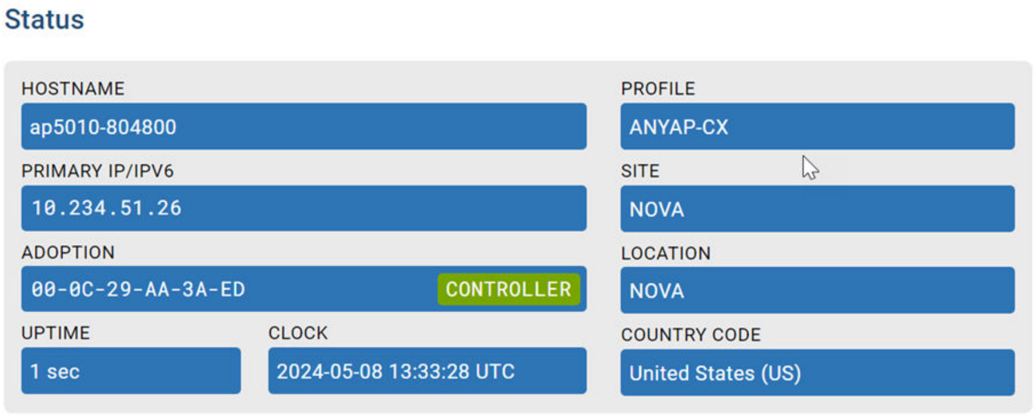
Table 164 describes the information displayed.

Table 164: AP Statistics – Firmware Information Description

Field	Description
Version	Displays the software (firmware) version on the AP. Use this information to assess whether a firmware upgrade would enhance the AP's support capability.
Build Date	Displays the date on which the firmware version build was created.
Install Date	Displays the date on which the firmware was installed on the AP.

Status

Figure 10 shows an example of device status information displayed for APs in the RF Domain.



Status

HOSTNAME: ap5010-804800

PROFILE: ANYAP-CX

PRIMARY IP/IPV6: 10.234.51.26

SITE: NOVA

ADOPTION: 00-0C-29-AA-3A-ED CONTROLLER

LOCATION: NOVA

UPTIME: 1 sec

CLOCK: 2024-05-08 13:33:28 UTC

COUNTRY CODE: United States (US)

Figure 10: AP Statistics – Example Device Status Display

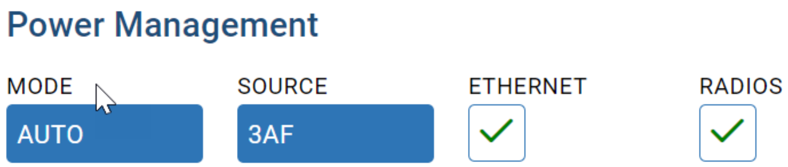
Table 165 describes the information displayed.

Table 165: AP statistics – Device Status Information Description

Field	Description
Hostname	Displays the unique administrator-assigned name of the AP.
Profile	Identifies the Profile that has been assigned to the AP.
Primary IP/IPv6	Displays the IPv4 or IPv6 address assigned to the AP either through DHCP or through static IP assignment.
Site	Displays the RF Domain name of which the AP is a member. Unlike a controller or service platform, an AP can belong to one RF Domain only, based on its model.
Adoption	Identifies the MAC address of the controller to which the AP has been adopted.
Location	Displays the geographical location of the Site (RF Domain), if it is configured. If this parameter is not configured, the Site name appears in this field by default.
Uptime	Displays the cumulative time since the AP was last rebooted or lost power.
Clock	Displays the date, time, and time zone of system clock.
Country Code	Displays the country code assigned to the AP.

Power Management

Figure 11 shows an example of power management information displayed for APs in the RF Domain.



Power Management

MODE: AUTO

SOURCE: 3AF

ETHERNET: ✓

RADIOS: ✓

Figure 11: AP Statistics – Example Power Management Display

Table 166 describes the statistics displayed.

Table 166: AP Statistics – Power Management Statistics Description

Field/Check box	Description
Mode	Displays the configured Power Management mode. Possible modes include: • Automatic • 802.3af • 802.3at • 802.3bt See Power Configuration on page 168 for a description of these modes and their function.
Source	Displays the power mode currently invoked by the selected AP.
Ethernet	Displays the AP's Ethernet port status, as follows: • ✓: enabled • ✗: disabled
Radios	Displays the AP's radio power status, as follows: • ✓: enabled • ✗: disabled Each AP radio is capable of having a unique, administrator-defined power transmission setting.

Radios and Clients

Figure 12 shows an example of radio and client statistics displayed for APs in the RF Domain.

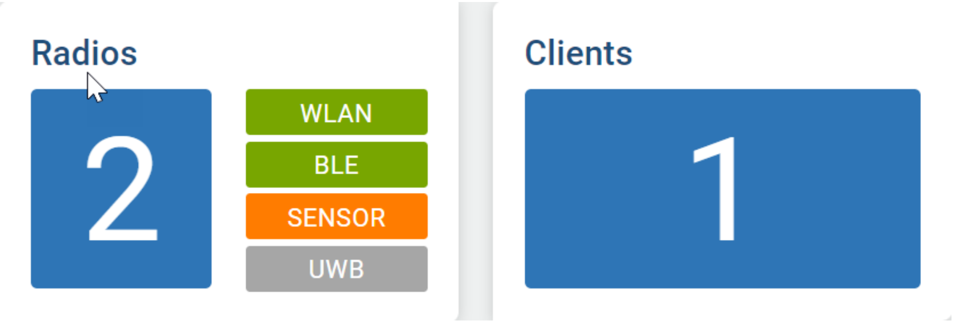


Figure 12: AP Statistics – Example Radios and Clients Displays

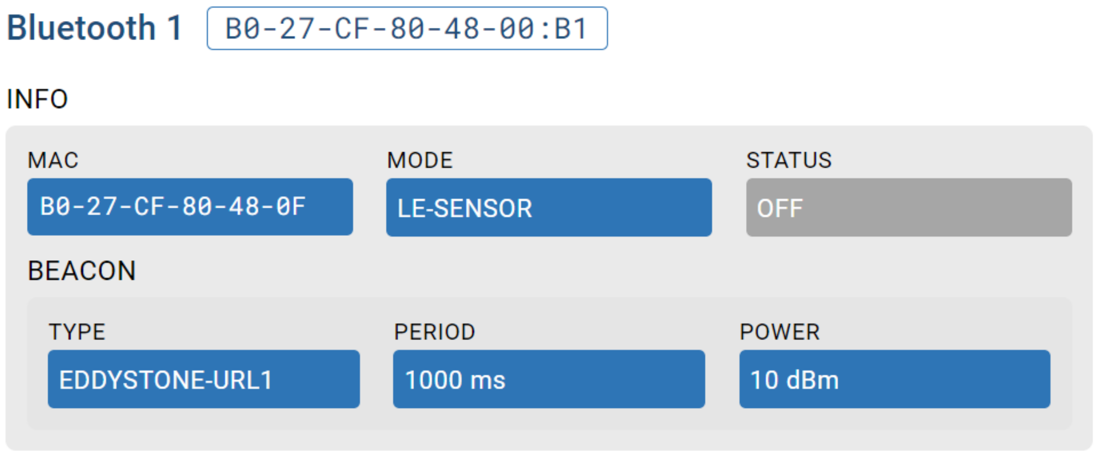
Table 167 describes the information displayed.

Table 167: AP Statistics – Radios and Clients Statistics Description

Element	Description
Radios	Displays the total number of radios configured on the AP and their assignments: WLAN, BLE, Sensor, or UWB.
Clients	Displays the total number of clients connected to the AP.

Bluetooth

Figure 13 shows an example of Bluetooth radio information displayed for APs in the RF Domain.



Bluetooth 1 B0-27-CF-80-48-00:B1

INFO

MAC: B0-27-CF-80-48-0F
MODE: LE-SENSOR
STATUS: OFF

BEACON

TYPE: EDDYSTONE-URL1
PERIOD: 1000 ms
POWER: 10 dBm

Figure 13: AP Statistics – Example Bluetooth Radio Display

Table 168 describes the information displayed.

Table 168: AP Statistics – Bluetooth Radio Information Description

Field	Description
Bluetooth 1	Displays the system-assigned Bluetooth radio name, consisting of the AP's MAC address and the radio number.
MAC	Displays the factory-set, hard-coded MAC address for the AP's Bluetooth radio.

Table 168: AP Statistics – Bluetooth Radio Information Description (continued)

Field	Description
Mode	Indicates the current Radio Mode setting for the Bluetooth radio. Possible modes displayed are: • bt-sensor • le-beacon • le-sensor • le-dual See Manage Bluetooth Configuration on page 157 for details about these mode types and their function.
Status	Displays the current operational status of the Bluetooth radio: either **On** or **Off**.
Type	Identifies the transmission pattern currently configured for the Bluetooth radio beacon. Possible pattern types include: • eddystone-url1 • eddystone-url2 • ibeacon See Manage Bluetooth Configuration on page 157 for details about these pattern types and their function.
Period	Displays the configured Bluetooth radio's beacon transmission period (100 – 10,000 milliseconds).
Power	Displays the current power level the radio is using for transmissions.

Resources

Figure 14 shows an example of Resources information displayed for APs in the RF Domain.

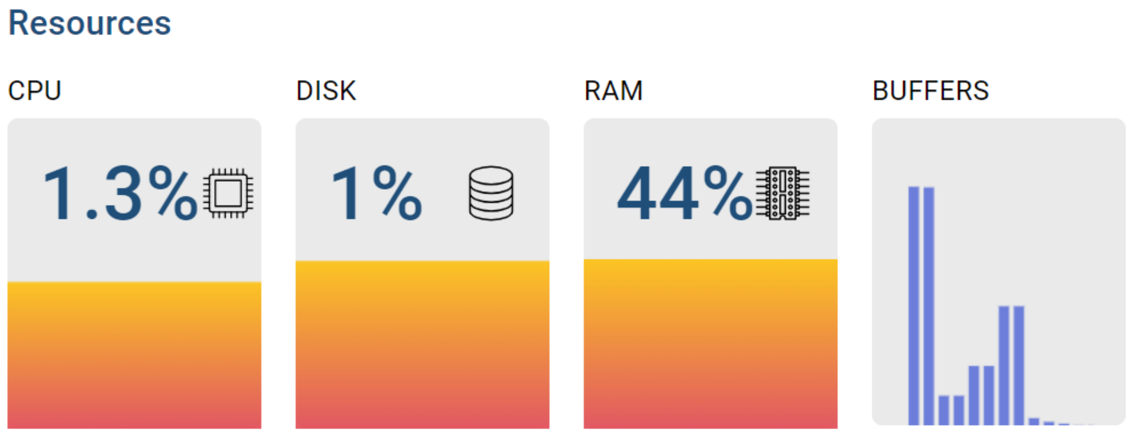


Figure 14: AP Statistics – Example Resources Display

Table 169 describes the information displayed.

Table 169: AP Statistics – Resources Information Description

Resource	Description
CPU	Displays the percentage of total available CPU currently in use.
Disk	Displays the percentage of total available disk space currently in use. Hover over the colored area to view a pop-up detailing current disk usage in megabytes (MB).
RAM	Displays the percentage of total available RAM currently in use. Hover over the colored area to view a pop-up detailing current memory usage in megabytes (MB).
Buffers	Displays the current buffers available to the AP. Hover over the bar graph lines to view a pop-up detailing buffer size, current utilization, and buffer limit.

Radios

Figure 15 and Figure 16 on page 514 show examples of Radio information displayed for APs in the RF Domain.

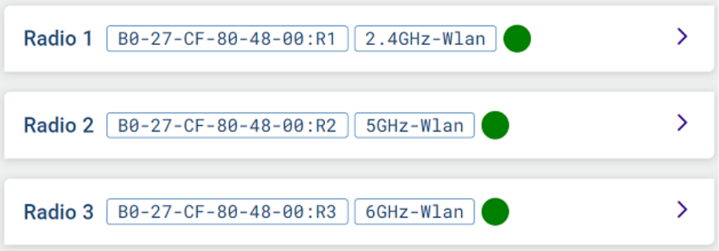
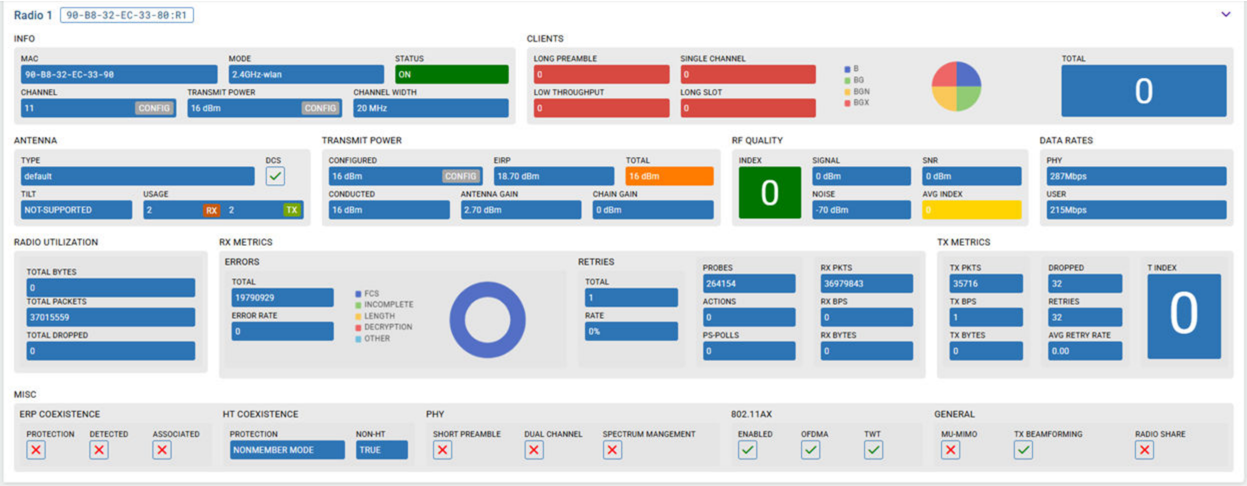


Figure 15: AP Statistics - Radios Information Display

Select > associated with a radio to view further detail.



Radio 1 90-B8-32-EC-33-80:R1

INFO

- MAC: 90-B8-32-EC-33-90
- MODE: 2.4GHz-wlan
- STATUS: ON
- CHANNEL: 11 CONFIG
- TRANSMIT POWER: 16 dBm CONFIG
- CHANNEL WIDTH: 20 MHz

CLIENTS

- LONG PREAMBLE: 0
- SINGLE CHANNEL: 0
- LOW THROUGHPUT: 0
- LONG SLOT: 0
- TOTAL: 0

ANTENNA

- TYPE: default
- DCS: ☑
- TILT: NOT-SUPPORTED
- USAGE: 2 RX 2 TX

TRANSMIT POWER

- CONFIGURED: 16 dBm CONFIG
- EIRP: 18.70 dBm
- TOTAL: 16 dBm
- CONDUCTED: 16 dBm
- ANTENNA GAIN: 2.70 dBm
- CHAIN GAIN: 0 dBm

RF QUALITY

- INDEX: 0
- SIGNAL: 0 dBm
- SNR: 0 dBm
- NOISE: -70 dBm
- AVG INDEX: 0

DATA RATES

- PHY: 287Mbps
- USER: 215Mbps

RADIO UTILIZATION

- TOTAL BYTES: 0
- TOTAL PACKETS: 37015559
- TOTAL DROPPED: 0

RX METRICS

ERRORS

- TOTAL: 19790929
- ERROR RATE: 0

RETRIES

- TOTAL: 1
- RATE: 0%

- PROBES: 264154
- ACTIONS: 0
- PS-POLLS: 0
- RX PKTS: 36979843
- RX BPS: 0
- RX BYTES: 0

TX METRICS

- TX PKTS: 35716
- TX BPS: 1
- TX BYTES: 0
- DROPPED: 32
- RETRIES: 32
- AVG RETRY RATE: 0.00
- T INDEX: 0

MISC

ERP COEXISTENCE

- PROTECTION: ☒
- DETECTED: ☒
- ASSOCIATED: ☒

HT COEXISTENCE

- PROTECTION: NONMEMBER MODE
- NON-HT: TRUE

PHY

- SHORT PREAMBLE: ☒
- DUAL CHANNEL: ☒
- SPECTRUM MANGEMENT: ☒

802.11AX

- ENABLED: ☑
- OFDMA: ☑
- TWT: ☑

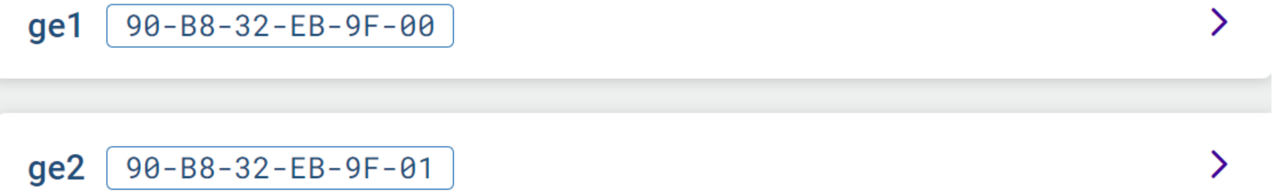
GENERAL

- MU-MIMO: ☒
- TX BEAMFORMING: ☑
- RADIO SHARE: ☒

Figure 16: AP Statistics - Radios Detailed Display

GbE Ports

Figure 17 and Figure 18 on page 515 show an example of Gigabit Ethernet port information displayed for APs in the RF Domain.

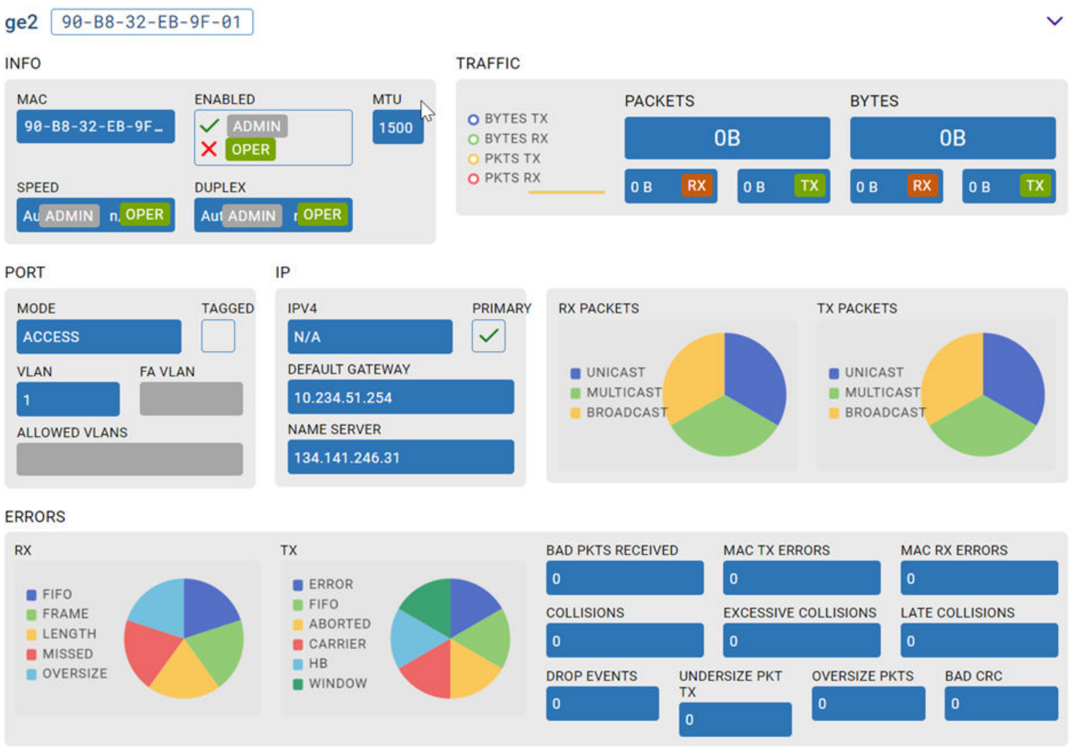


ge1 90-B8-32-EB-9F-00 >

ge2 90-B8-32-EB-9F-01 >

Figure 17: AP Statistics – Example GbE Port Information Display

Select > associated with a GbE port to view further detail.



ge2 90-B8-32-EB-9F-01

INFO

MAC: 90-B8-32-EB-9F…

ENABLED: ✓ ADMIN ✗ OPER

MTU: 1500

SPEED: Au ADMIN n OPER

DUPLEX: Aut ADMIN r OPER

TRAFFIC

PACKETS: 0B

BYTES: 0B

0 B RX 0 B TX 0 B RX 0 B TX

PORT

MODE: ACCESS

TAGGED: □

VLAN: 1

FA VLAN:

ALLOWED VLANS:

IP

IPV4: N/A

PRIMARY: ☑

DEFAULT GATEWAY: 10.234.51.254

NAME SERVER: 134.141.246.31

ERRORS

BAD PKTS RECEIVED: 0

MAC TX ERRORS: 0

MAC RX ERRORS: 0

COLLISIONS: 0

EXCESSIVE COLLISIONS: 0

LATE COLLISIONS: 0

DROP EVENTS: 0

UNDERSIZE PKT TX: 0

OVERSIZE PKTS: 0

BAD CRC: 0

Figure 18: AP Statistics – Example GbE Port Details Display

Table 170 describes the information displayed in the preceding figures.

Table 170: AP Statistics – GbE Port Information Description

Element	Description
GbE Port	Displays the Gigabit Ethernet port name (ge*X*) and interface MAC address.
Info	
MAC	Displays the interface MAC address.
Enabled	Indicates the interface status, as follows: • ✓ ◦ interface **ADMIN**istrative status = Enabled ◦ interface **OPER**ational status = Up • ✗ ◦ interface **ADMIN**istrative status = Disabled ◦ interface **OPER**ational status is Down
MTU	Identifies the largest IPv6-formatted packet size that can be sent over this interface.

Table 170: AP Statistics – GbE Port Information Description (continued)

Element	Description
Speed	Displays the configured interface speed and the actual operating speed, as follows: • **Admin**: Displays the configured maximum speed (in Mbps) at which the port can transmit or receive. This value can be either **`10`**, **`100`**, **`1000`** or **`Auto`**. Auto indicates the speed is negotiated between connected devices. • **Oper**: Displays the current speed of the data transmitted and received over the interface.
Duplex	Displays the configured duplex setting and the actual duplex setting in use, as follows: • **Admin**: Displays the configured Duplex setting for the interface. This value can be either **`Auto`**, **`H`** (half duplex), or **`F`** (full). Auto indicates the duplex mode is negotiated between connected devices. • **Oper**: Displays the current operating Duplex mode of interface as either **`H`** (half duplex) or **`F`** (full duplex).
Traffic	
Packets	RX PKTS: Displays the number of good packets received. TX PKTS: Displays the number of good packets transmitted.
Bytes	RX Bytes: Displays the number of octets (bytes) with no errors received by the interface. TX Bytes: Displays the number of octets (bytes) with no errors sent by the interface.
Port	
Mode	The Mode can be either of the following: • Access: This Ethernet interface accepts packets only from the native VLANs. • Trunk: This Ethernet interface allows packets from a list of VLANs you can add to the trunk.
Tagged	Indicates whether the VLAN is tagged, as follows: • ✓: means the native VLAN is tagged. • ✗: means the native VLAN is untagged.
VLAN	Displays the tag assigned to the native VLAN (if mode is Trunk) or the access VLAN (if mode is Access).
FA VLAN	Displays the tag assigned to the Fabric Attach (FA) client VLAN (if mode is Access).
Allowed VLANs	Displays the VLANs that exclusively send packets over the port (if mode is Trunk).

Table 170: AP Statistics – GbE Port Information Description (continued)

Element	Description
IP	
IPv4	Displays the IP address of the interface.
Primary	The presence of a check mark indicates that the IP address is assigned to this interface either through DHCP or through static IP assignment.
Default Gateway	Displays the Default Gateway's IP address. This is the gateway used to route traffic to the specified network.
Name Server	Displays the names of the servers designated to provide DNS resources to this access point.
RX Packets	Displays the number of multicast/unicast/ broadcast packets received through the selected GbE interface in a pie chart.
TX Packets	Displays the number of multicast/unicast/ broadcast packets sent through the selected GbE interface in a pie chart
Errors	
RX	Displays RX Errors in a pie chart, as follows: • FIFO Errors: Displays the number of FIFO errors received at the interface. First-In First-Out queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally. • Frame Errors: Displays the number of frame errors received at the interface. A frame error occurs when a byte of data is received, but not in the format expected. • Length Errors: Displays the number of length errors received at the interface. Length errors are generated when the received frame length was less than (or exceeded) the Ethernet standard. • Missed Errors: Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store the incoming packet. • Oversize Errors: Displays the number of overflow errors. An overflow occurs when packet size exceeds the allocated buffer size.

Table 170: AP Statistics – GbE Port Information Description (continued)

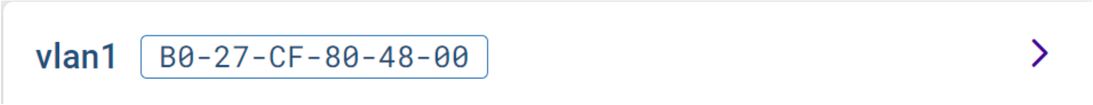
Element	Description
TX	Displays TX Errors in a pie chart, as follows: • Error: Displays the number of packets with errors transmitted on the interface. • FIFO: Displays the number of FIFO errors received at the interface. Firstin-First-Out queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally. • Aborted: Displays the number of packets aborted on the interface because a clear-to-send request was not detected. • Carrier: Displays the number of carrier errors on the interface. This generally indicates bad Ethernet hardware or cabling. • Heart Beat: Displays the number of heartbeat errors. This generally indicates a software crash or packets stuck in an endless loop. • Window Errors: Displays the number of window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) in the receive window field the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment from the receiving host, it constitutes a window error.
Bad Pkts Received	Displays the number of bad packets received through the interface.
MAC TX Errors	Displays the number of transmits that failed because of an internal MAC sublayer error that is not a late collision, excessive collision count, or a carrier sense error.
MAC RX Errors	Displays the number of received packets failed because of an internal MAC sublayer that is not a late collision, excessive collision count, or a carrier sense error.
Collisions	Displays the number of collisions on the interface.
Excessive Collisions	Displays the number of excessive collisions. Excessive collisions occur when the traffic load increases to the point that a single Ethernet network cannot handle it efficiently.

Table 170: AP Statistics – GbE Port Information Description (continued)

Element	Description
Late Collisions	A late collision is any collision that occurs after the first 64 octets of data have been sent by the sending client. Late collisions are not normal, and are usually the result of out-of-specification cabling or a malfunctioning device.
Drop Events	Displays the number of dropped packets transmitted or received through the interface.
TX Undersize Pkts	Displays the number of undersized packets transmitted through the interface.
Oversize Pkts	Displays the number of oversized packets transmitted through the interface.
Bad CRC	Displays the CRC error. The Cyclical Redundancy Check (CRC) is the 4-byte field at the end of every frame. The receiving station uses it to interpret whether the frame is valid. If the CRC value computed by the interface does not match the value at the end of the frame, it is considered a bad CRC.

VLANs

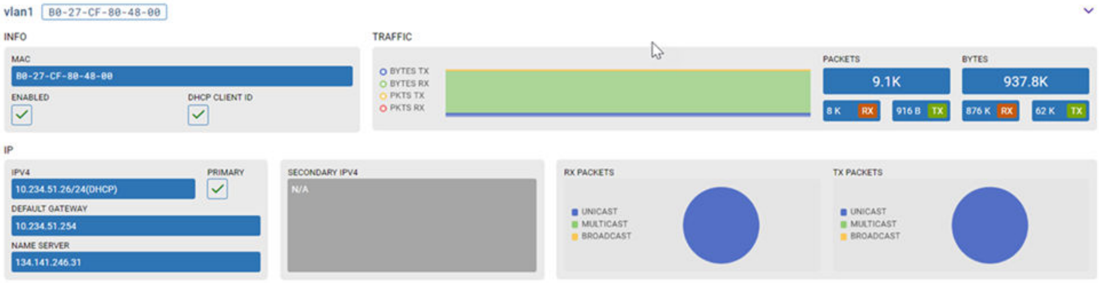
Figure 19 and Figure 20 on page 519 show an example of VLAN information displayed for APs in the RF Domain.



vlan1 B0-27-CF-80-48-00

Figure 19: AP Statistics - VLAN Information Display

Select > associated with a VLAN to view further detail.



vlan1 B0-27-CF-80-48-00

INFO

MAC: B0-27-CF-80-48-00

ENABLED ☑ DHCP CLIENT ID ☑

TRAFFIC

PACKETS: 9.1K (8 K RX, 916 B TX)

BYTES: 937.8K (876 K RX, 62 K TX)

IP

IPV4: 10.234.51.26/24(DHCP) PRIMARY ☑

DEFAULT GATEWAY: 10.234.51.254

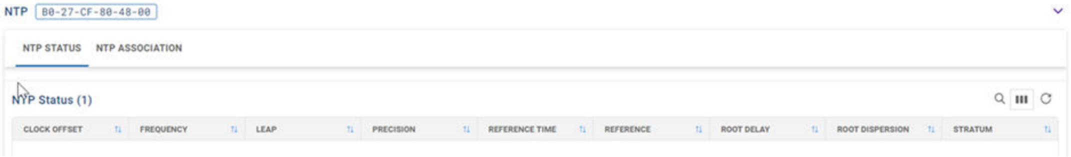
NAME SERVER: 134.141.246.31

SECONDARY IPV4: N/A

Figure 20: AP Statistics – VLAN Details Display

NTP

Figure 21 shows an example of Network Time Protocol (NTP) information displayed for APs in the RF Domain. This information is presented in tabular form.



NTP B0-27-CF-80-48-00

NTP Status (1)

CLOCK OFFSET	FREQUENCY	LEAP	PRECISION	REFERENCE TIME	REFERENCE	ROOT DELAY	ROOT DISPERSION	STRATUM

Figure 21: AP Statistics – NTP Status Information Display

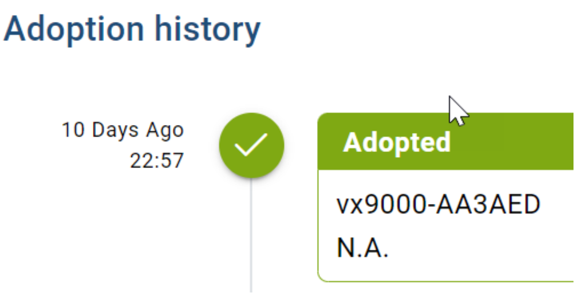
Table 171 describes the type of information displayed under each column in the table.

Table 171: AP Statistics - NTP Information Description

Column Heading	Description
Clock Offset	Displays the time differential between the AP's time and its NTP resource's time.
Frequency	Indicates the SNTP server clock's skew (difference) for the AP.
Leap	Indicates if a second is added or subtracted to SNTP packet transmissions, or if transmissions are synchronized.
Precision	Displays the precision of the time clock (in Hz). The values that normally appear in this field range from -6 (for mains-frequency clocks) to -20 (for microsecond clocks).
Reference Time	Displays a time stamp indicating when the AP's clock was last synchronized or corrected.
Reference	Displays the address of the time source with which the AP is synchronized.
Root Delay	Displays the total round-trip delay in seconds. This variable can take on both positive and negative values, depending on relative time and frequency offsets. The values that normally appear in this field range from negative values (a few milliseconds) to positive values (several hundred milliseconds).
Root Dispersion	Displays the difference between the time on the root NTP server and its reference clock. The reference clock is the clock used by the NTP server to set its own clock.
Stratum	Displays how many hops the AP is from its current NTP time resource.

Adoption History

Figure 22 shows an example of Adoption History information displayed for APs in the RF Domain.



Adoption history

10 Days Ago
22:57

Adopted

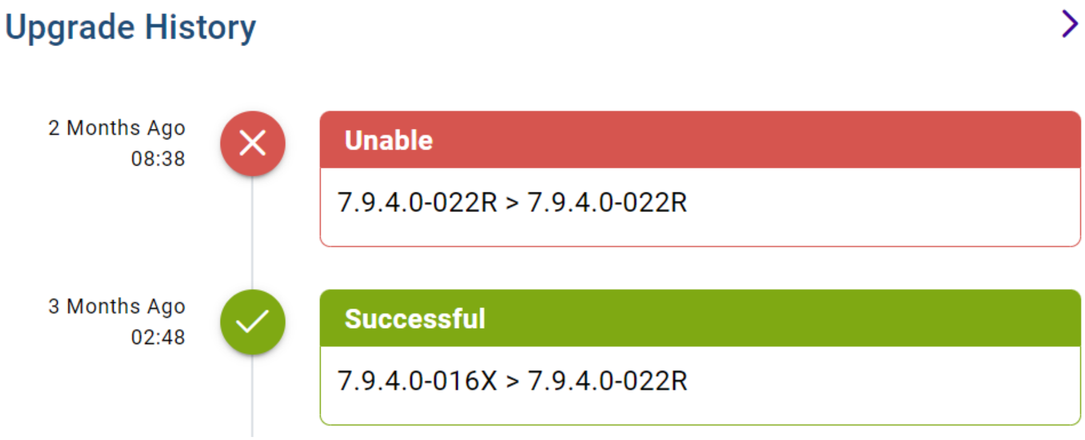
vx9000-AA3AED
N.A.

Figure 22: AP Statistics – Example Adoption History Display

Note
If adoption is unsuccessful, "N.A." is replaced with a reason message (for example, auto-provisioning policy issue, licensing issue, or device is unreachable).

Upgrade History

Figure 23 shows an example of Upgrade History information displayed for APs in the RF Domain.



Upgrade History

2 Months Ago
08:38

Unable

7.9.4.0-022R > 7.9.4.0-022R

3 Months Ago
02:48

Successful

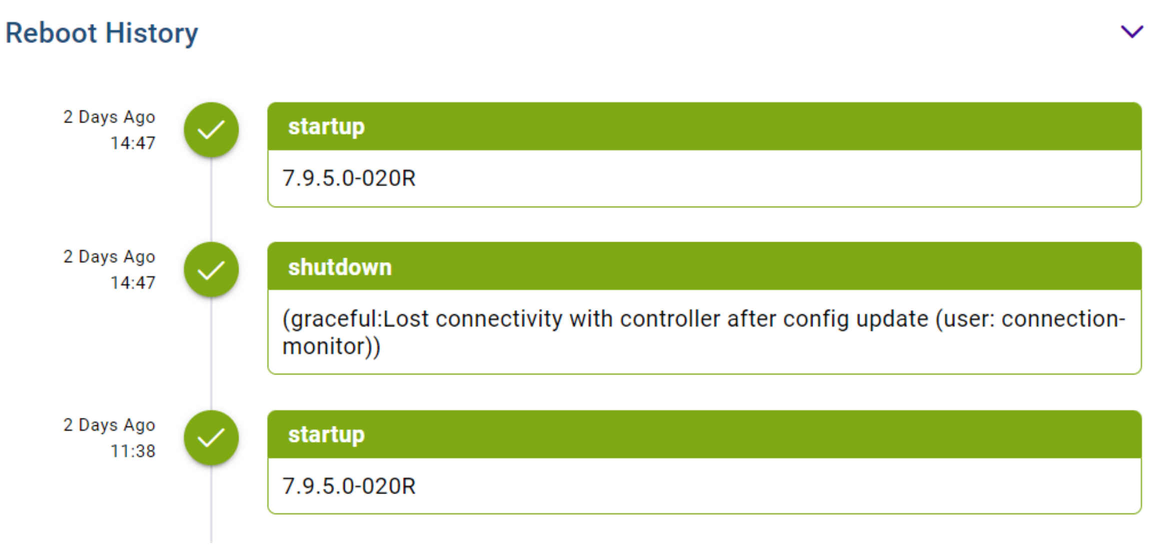
7.9.4.0-016X > 7.9.4.0-022R

Figure 23: AP Statistics – Example Upgrade History Display

Reboot History

Check the Reboot History statistics to assess performance of the selected AP. If the AP reboots frequently, you can go to **Diagnostics** > **Event History** and consult the data recorded for the selected AP to help determine the cause.

Figure 24 shows an example of Reboot information displayed for APs in the RF Domain.



Reboot History

2 Days Ago 14:47 — startup

7.9.5.0-020R

2 Days Ago 14:47 — shutdown

(graceful:Lost connectivity with controller after config update (user: connection-monitor))

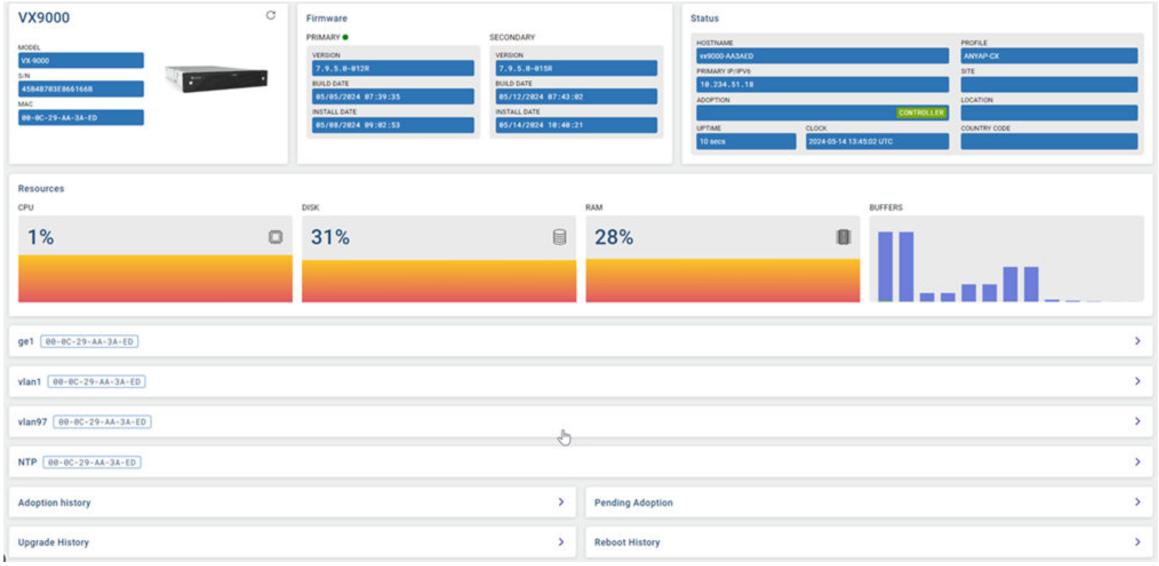
2 Days Ago 11:38 — startup

7.9.5.0-020R

Figure 24: Access Point Statistics - Example Reboot History Display

Controller Statistics

Controller Statistics on page 522 shows an example of a device statistics display for controllers.



VX9000

MODEL: VX-9000

S/N: 45848703E8661668

MAC: 00-0C-29-AA-3A-ED

Firmware

PRIMARY ●

VERSION: 7.9.5.0-012R

BUILD DATE: 05/05/2024 07:39:35

INSTALL DATE: 05/08/2024 09:02:53

SECONDARY

VERSION: 7.9.5.0-015R

BUILD DATE: 05/12/2024 07:43:02

INSTALL DATE: 05/14/2024 10:40:21

Status

HOSTNAME: vx9000-AA3AED

PROFILE: ANYAP-CX

PRIMARY IP/IPV6: 10.234.51.18

SITE:

ADOPTION: CONTROLLER

LOCATION:

UPTIME: 10 secs

CLOCK: 2024-05-14 13:45:02 UTC

COUNTRY CODE:

Resources

CPU: 1%

DISK: 31%

RAM: 28%

BUFFERS

ge1 00-0C-29-AA-3A-ED

vlan1 00-0C-29-AA-3A-ED

vlan97 00-0C-29-AA-3A-ED

NTP 00-0C-29-AA-3A-ED

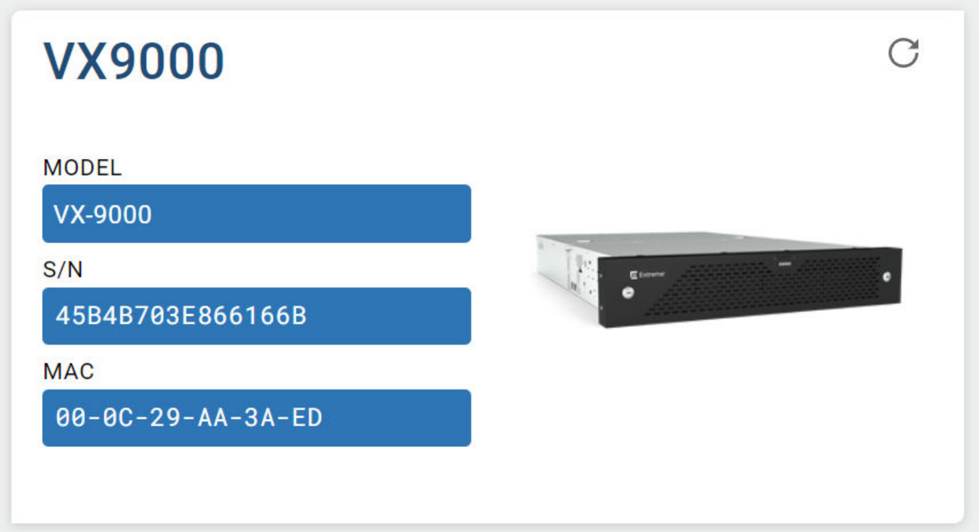
Figure 25: Controller Statistics

Controller statistics are arranged under the following panes (left-to-right, top-to-bottom):

- Device Information on page 523
- Firmware on page 524
- Status on page 524

Device Information

Figure 26 shows an example of device information displayed for controllers in the RF Domain.



VX9000

MODEL
VX-9000

S/N
45B4B703E866166B

MAC
00-0C-29-AA-3A-ED

Figure 26: Controller Statistics – Example Device Information Display

Select ↻ to refresh the display.

Table 172 describes the information displayed.

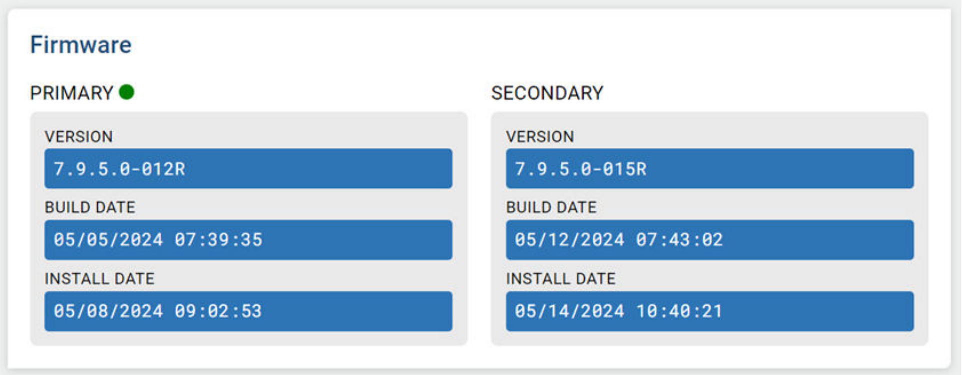
Table 172: Controller Statistics – Device Information Description

Field	Description
Type	The controller type is displayed in the upper–left position of the pane.
Model	Displays the model number for the selected controller.
S/N	Displays the serial number factory encoded on the controller at the factory.
MAC	Displays the MAC address of the controller. This is factory assigned and cannot be changed.

Firmware

Figure 27 shows an example of device firmware information displayed for controllers in the RF Domain.

You can store both a **Primary** and **Secondary** firmware version in memory. An automatic fallback mechanism exists, which loads the Secondary version if the Primary version fails. A ● appears adjacent to either Primary or Secondary, indicating which firmware is currently in use.



Firmware

PRIMARY ●

VERSION
7.9.5.0-012R

BUILD DATE
05/05/2024 07:39:35

INSTALL DATE
05/08/2024 09:02:53

SECONDARY

VERSION
7.9.5.0-015R

BUILD DATE
05/12/2024 07:43:02

INSTALL DATE
05/14/2024 10:40:21

Figure 27: Controller Statistics - Example Firmware Display

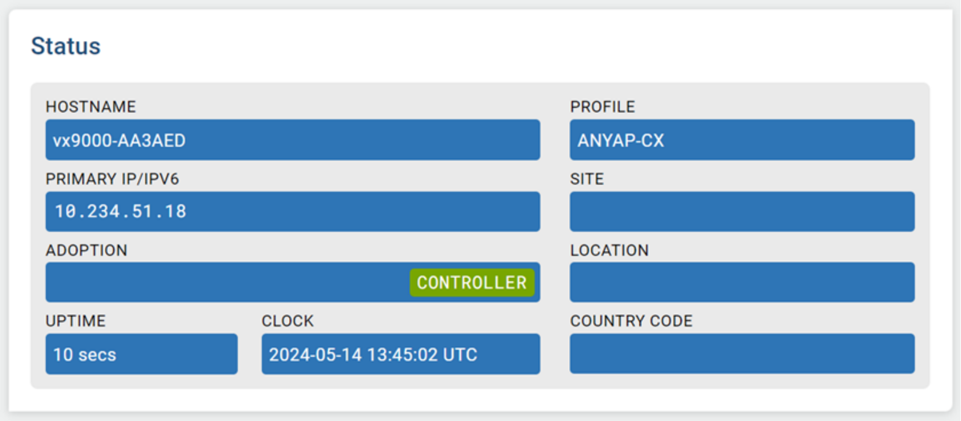
Table 173 describes the information displayed.

Table 173: Controller Statistics – Firmware Information Description

Field	Description
Version	Displays the unique alphanumeric firmware version name for the controller firmware.
Build Date	Displays the date on which the firmware version build was created.
Install Date	Displays the date on which the firmware was installed on the controller.

Status

Figure 28 shows an example of device status information displayed for controllers in the RF Domain.



Status

HOSTNAME: vx9000-AA3AED

PROFILE: ANYAP-CX

PRIMARY IP/IPV6: 10.234.51.18

SITE:

ADOPTION: CONTROLLER

LOCATION:

UPTIME: 10 secs

CLOCK: 2024-05-14 13:45:02 UTC

COUNTRY CODE:

Figure 28: Controller Statistics - Example Status Display

Table 174 describes the information displayed.

Table 174: Controller Statistics – Device Status Information Description

Field	Description
Hostname	Displays the unique administrator-assigned name of the controller.
Profile	Identifies the Profile that has been assigned to the controller.
Primary IP/IPv6	Displays the IPv4 or IPv6 address assigned to the controller either through DHCP or through static IP assignment.
Site	Displays the RF Domain name of which the controller is a member. Unlike a controller or service platform, a AP can belong to one RF Domain only, based on its model.
Adoption	Indicates that this device is the adopting Controller.
Location	Displays the geographical location of the Site (RF Domain), if it is configured. If this parameter is not configured, the Site name appears in this field by default.
Uptime	Displays the cumulative time since the controller was last rebooted or lost power.
Clock	Displays the date, time, and time zone of system clock.
Country Code	Displays the country code assigned to the controller.

Resources

Figure 29 shows an example of Resources information displayed for controllers in the RF Domain.

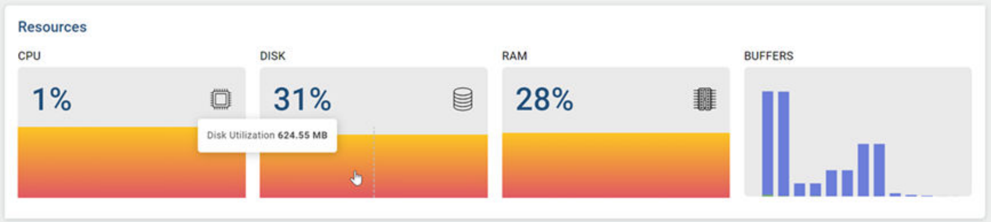


Figure 29: Controller Statistics - Example Resources Display

Table 175 describes the information displayed.

Table 175: Controller Statistics – Resources Information Description

Resource	Description
CPU	Displays the percentage of total available CPU currently in use.
Disk	Displays the percentage of total available disk space currently in use. Hover over the colored area to view a pop-up detailing current disk usage in megabytes (MB).
RAM	Displays the percentage of total available RAM currently in use. Hover over the colored area to view a pop-up detailing current memory usage in megabytes (MB).
Buffers	Displays the current buffers available to the controller. Hover over the bar graph lines to view a pop-up detailing buffer size, current utilization, and buffer limit.

GbE Port

Figure 30 and Figure 31 on page 527 show an example of Gigabit Ethernet port information displayed for controllers in the RF Domain.

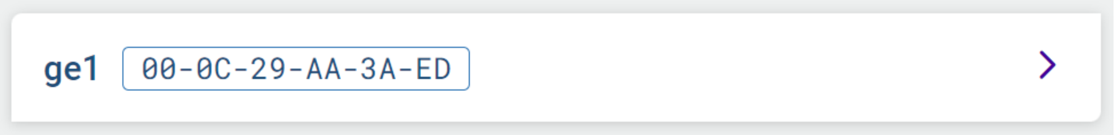
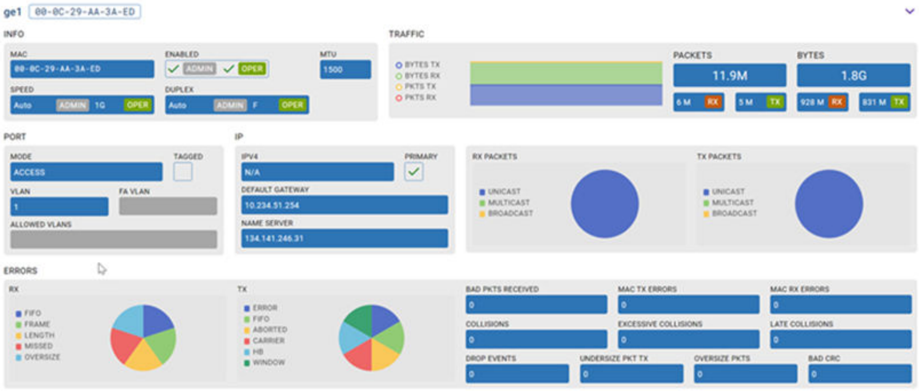


Figure 30: Controller Statistics - Example GbE Port Information Display

Select > associated with a GbE port to view further detail.



ge1 00-0C-29-AA-3A-ED

INFO

MAC: 00-0C-29-AA-3A-ED

ENABLED: ✓ ADMIN ✓ OPER

MTU: 1500

SPEED: Auto ADMIN 1G OPER

DUPLEX: Auto ADMIN F OPER

TRAFFIC

PACKETS: 11.9M — 6 M RX, 5 M TX

BYTES: 1.8G — 928 M RX, 831 M TX

PORT

MODE: ACCESS

TAGGED: □

VLAN: 1

FA VLAN:

ALLOWED VLANS:

IP

IPV4: N/A

PRIMARY: ☑

DEFAULT GATEWAY: 10.234.51.254

NAME SERVER: 134.141.246.31

ERRORS

BAD PKTS RECEIVED: 0

MAC TX ERRORS: 0

MAC RX ERRORS: 0

COLLISIONS: 0

EXCESSIVE COLLISIONS: 0

LATE COLLISIONS: 0

DROP EVENTS: 0

UNDERSIZE PKT TX: 0

OVERSIZE PKTS: 0

BAD CRC: 0

Figure 31: Controller Statistics - Example GbE Port Details Display

Table 176 describes the information displayed in the preceding figures.

Table 176: Controller Statistics – GbE Port Information Description

Element	Description
GbE Port	Displays the Gigabit Ethernet port name (ge*X*) and interface MAC address.
Info	
MAC	Displays the interface MAC address.
Enabled	Indicates the interface status, as follows: • ✓ ◦ interface **ADMIN**istrative status = Enabled ◦ interface **OPER**ational status = Up • ✗ ◦ interface **ADMIN**istrative status = Disabled ◦ interface **OPER**ational status is Down
MTU	Identifies the largest IPv6-formatted packet size that can be sent over this interface.
Speed	Displays the configured interface speed and the actual operating speed, as follows: • **Admin**: Displays the configured maximum speed (in Mbps) at which the port can transmit or receive. This value can be either `10`, `100`, `1000` or `Auto`. Auto indicates the speed is negotiated between connected devices. • **Oper**: Displays the current speed of the data transmitted and received over the interface.

Table 176: Controller Statistics – GbE Port Information Description (continued)

Element	Description
Duplex	Displays the configured duplex setting and the actual duplex setting in use, as follows: • **Admin**: Displays the configured Duplex setting for the interface. This value can be either **`Auto`**, **`H`** (half duplex), or **`F`** (full). Auto indicates the duplex mode is negotiated between connected devices. • **Oper**: Displays the current operating Duplex mode of interface as either **`H`** (half duplex) or **`F`** (full duplex).
Traffic	
Packets	RX PKTS: Displays the number of good packets received. TX PKTS: Displays the number of good packets transmitted.
Bytes	RX Bytes: Displays the number of octets (bytes) with no errors received by the interface. TX Bytes: Displays the number of octets (bytes) with no errors sent by the interface.
Port	
Mode	The Mode can be either of the following: • Access: This Ethernet interface accepts packets only from the native VLANs. • Trunk: This Ethernet interface allows packets from a list of VLANs you can add to the trunk.
Tagged	Indicates whether the VLAN is tagged, as follows: • ✓: means the native VLAN is tagged. • ✗: means the native VLAN is untagged.
VLAN	Displays the tag assigned to the native VLAN (if mode is Trunk) or the access VLAN (if mode is Access).
FA VLAN	Displays the tag assigned to the Fabric Attach (FA) client VLAN (if mode is Access).
Allowed VLANs	Displays the VLANs that exclusively send packets over the port (if mode is Trunk).
IP	
IPv4	Displays the IP address of the interface.
Primary	The presence of a check mark indicates that the IP address is assigned to this interface either through DHCP or through static IP assignment.
Default Gateway	Displays the Default Gateway's IP address. This is the gateway used to route traffic to the specified network.
Name Server	Displays the names of the servers designated to provide DNS resources to this access point.
RX Packets	Displays the number of multicast/unicast/broadcast packets received through the selected GbE interface in a pie chart.

Table 176: Controller Statistics – GbE Port Information Description (continued)

Element	Description
TX Packets	Displays the number of multicast/unicast/broadcast packets sent through the selected GbE interface in a pie chart
Errors	
RX	Displays RX Errors in a pie chart, as follows: • FIFO Errors: Displays the number of FIFO errors received at the interface. First-In First-Out queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally. • Frame Errors: Displays the number of frame errors received at the interface. A frame error occurs when a byte of data is received, but not in the format expected. • Length Errors: Displays the number of length errors received at the interface. Length errors are generated when the received frame length was less than (or exceeded) the Ethernet standard. • Missed Errors: Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store the incoming packet. • Oversize Errors: Displays the number of overflow errors. An overflow occurs when packet size exceeds the allocated buffer size.

Table 176: Controller Statistics – GbE Port Information Description (continued)

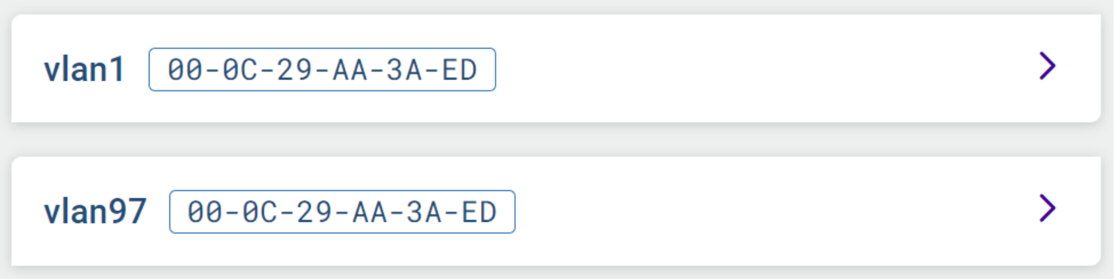
Element	Description
TX	Displays TX Errors in a pie chart, as follows: • Error: Displays the number of packets with errors transmitted on the interface. • FIFO: Displays the number of FIFO errors received at the interface. Firstin-First-Out queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally. • Aborted: Displays the number of packets aborted on the interface because a clear-to-send request was not detected. • Carrier: Displays the number of carrier errors on the interface. This generally indicates bad Ethernet hardware or cabling. • Heart Beat: Displays the number of heartbeat errors. This generally indicates a software crash or packets stuck in an endless loop. • Window Errors: Displays the number of window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) in the receive window field the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment from the receiving host, it constitutes a window error.
Bad Pkts Received	Displays the number of bad packets received through the interface.
MAC TX Errors	Displays the number of transmits that failed because of an internal MAC sublayer error that is not a late collision, excessive collision count, or a carrier sense error.
MAC RX Errors	Displays the number of received packets failed because of an internal MAC sublayer that is not a late collision, excessive collision count, or a carrier sense error.
Collisions	Displays the number of collisions on the interface.
Excessive Collisions	Displays the number of excessive collisions. Excessive collisions occur when the traffic load increases to the point that a single Ethernet network cannot handle it efficiently.
Late Collisions	A late collision is any collision that occurs after the first 64 octets of data have been sent by the sending client. Late collisions are not normal, and are usually the result of out-of-specification cabling or a malfunctioning device.
Drop Events	Displays the number of dropped packets transmitted or received through the interface.
TX Undersize Pkts	Displays the number of undersized packets transmitted through the interface.

Table 176: Controller Statistics – GbE Port Information Description (continued)

Element	Description
Oversize Pkts	Displays the number of oversized packets transmitted through the interface.
Bad CRC	Displays the CRC error. The Cyclical Redundancy Check (CRC) is the 4-byte field at the end of every frame. The receiving station uses it to interpret whether the frame is valid. If the CRC value computed by the interface does not match the value at the end of the frame, it is considered a bad CRC.

VLAN

Figure 32 and Figure 33 on page 531 show an example of VLAN information displayed for controllers in the RF Domain.

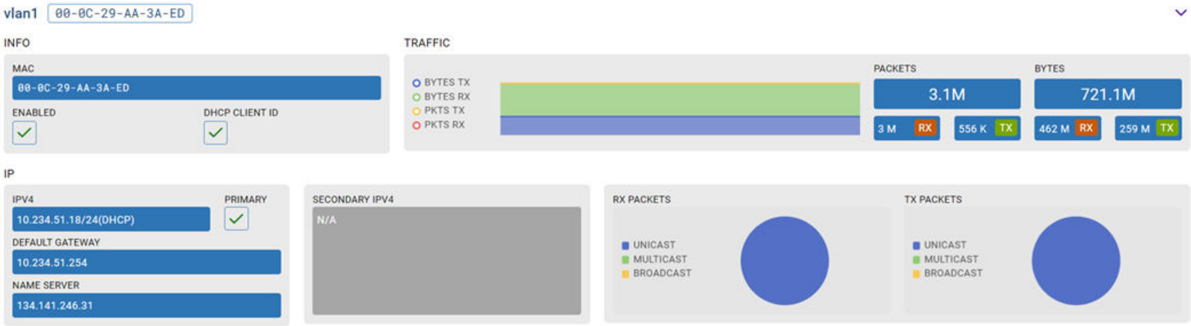


vlan1 00-0C-29-AA-3A-ED

vlan97 00-0C-29-AA-3A-ED

Figure 32: Controller Statistics - Example VLAN Information Display

Select > associated with a VLAN to view further detail.



vlan1 00-0C-29-AA-3A-ED

INFO

MAC: 00-0C-29-AA-3A-ED

ENABLED: ✓ DHCP CLIENT ID: ✓

TRAFFIC

PACKETS: 3.1M (3 M RX, 556 K TX)

BYTES: 721.1M (462 M RX, 259 M TX)

IP

IPV4: 10.234.51.18/24(DHCP) PRIMARY: ✓

DEFAULT GATEWAY: 10.234.51.254

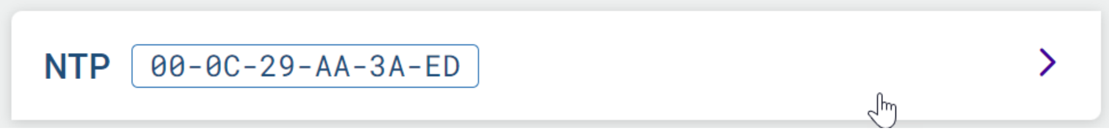
NAME SERVER: 134.141.246.31

SECONDARY IPV4: N/A

Figure 33: Controller Statistics – VLAN Details Display

NTP

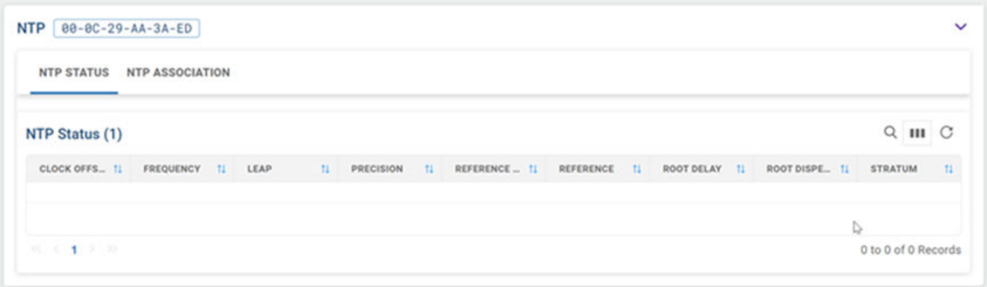
Figure 34 and Figure 35 on page 532 show examples of Network Time Protocol (NTP) information displayed for controllers in the RF Domain. This information is presented in tabular form.



NTP 00-0C-29-AA-3A-ED

Figure 34: Controller Statistics - Example NTP Information Display

Select > associated with NTP to view further detail.



NTP 00-0C-29-AA-3A-ED

NTP Status (1)

CLOCK OFFS...	FREQUENCY	LEAP	PRECISION	REFERENCE ...	REFERENCE	ROOT DELAY	ROOT DISPE...	STRATUM

0 to 0 of 0 Records

Figure 35: Controller Statistics – NTP Status Details Display

Table 177 describes the type of information displayed under each column in the table.

Table 177: Controller Statistics - NTP Information Description

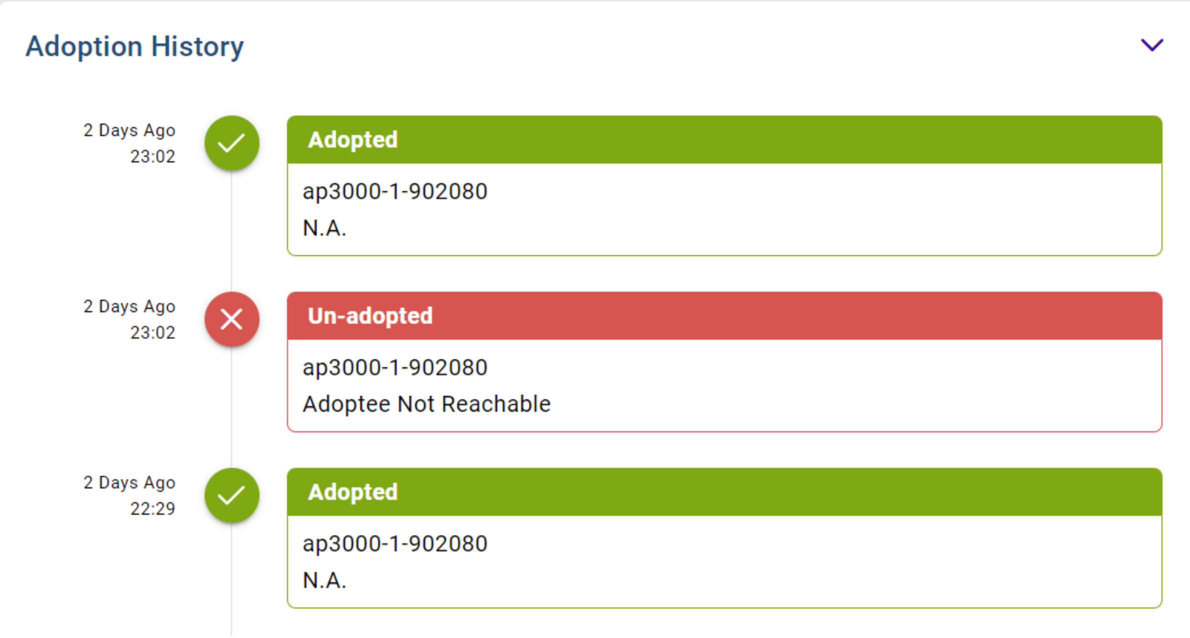
Column Heading	Description
Clock Offset	Displays the time differential between the controller's time and its NTP resource’s time.
Frequency	Indicates the SNTP server clock’s skew (difference) for the controller.
Leap	Indicates if a second is added or subtracted to SNTP packet transmissions, or if transmissions are synchronized.
Precision	Displays the precision of the time clock (in Hz). The values that normally appear in this field range from -6 (for mains-frequency clocks) to -20 (for microsecond clocks).
Reference Time	Displays a time stamp indicating when the controller’s clock was last synchronized or corrected.
Reference	Displays the address of the time source with which the controller is synchronized.
Root Delay	Displays the total round-trip delay in seconds. This variable can take on both positive and negative values, depending on relative time and frequency offsets. The values that normally appear in this field range from negative values (a few milliseconds) to positive values (several hundred milliseconds).

Table 177: Controller Statistics - NTP Information Description (continued)

Column Heading	Description
Root Dispersion	Displays the difference between the time on the root NTP server and its reference clock. The reference clock is the clock used by the NTP server to set its own clock.
Stratum	Displays how many hops the controller is from its current NTP time resource.

Adoption History

Figure 36 shows an example of Adoption History information displayed for controllers in the RF Domain.



Adoption History

2 Days Ago 23:02 ✓ Adopted
ap3000-1-902080
N.A.

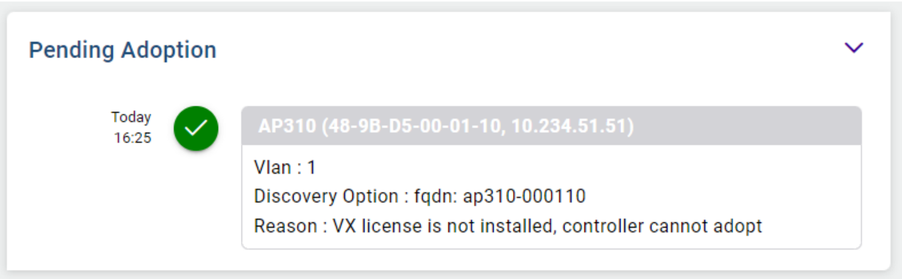
2 Days Ago 23:02 ✕ Un-adopted
ap3000-1-902080
Adoptee Not Reachable

2 Days Ago 22:29 ✓ Adopted
ap3000-1-902080
N.A.

Figure 36: Controller Statistics - Example Adoption History Display

Pending Adoption

Figure 37 shows an example of Pending Adoption information displayed for controllers in the RF Domain.



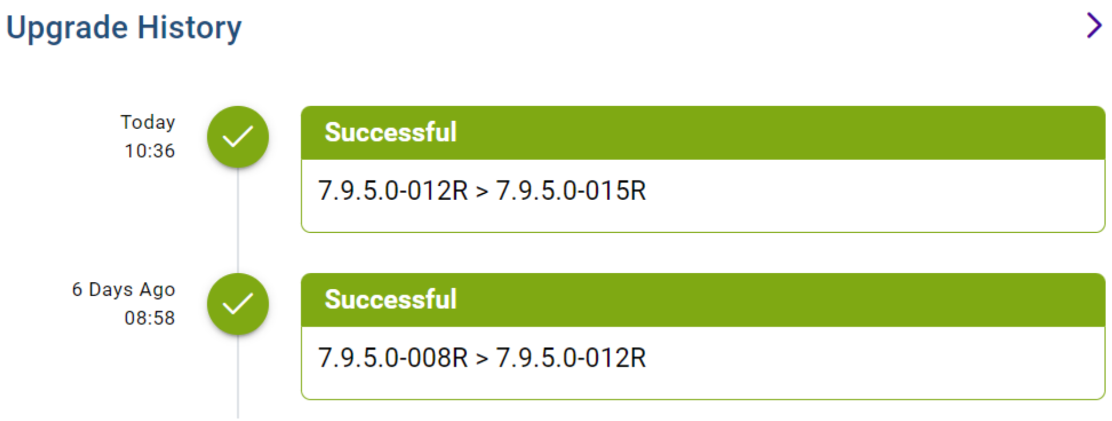
Pending Adoption

Today 16:25 ✓ AP310 (48-9B-D5-00-01-10, 10.234.51.51)
Vlan : 1
Discovery Option : fqdn: ap310-000110
Reason : VX license is not installed, controller cannot adopt

Figure 37: Controller Statistics - Example Pending Adoption Display

Upgrade History

Figure 38 shows an example of Upgrade History information displayed for controllers in the RF Domain.



Upgrade History

Today 10:36

Successful

7.9.5.0-012R > 7.9.5.0-015R

6 Days Ago 08:58

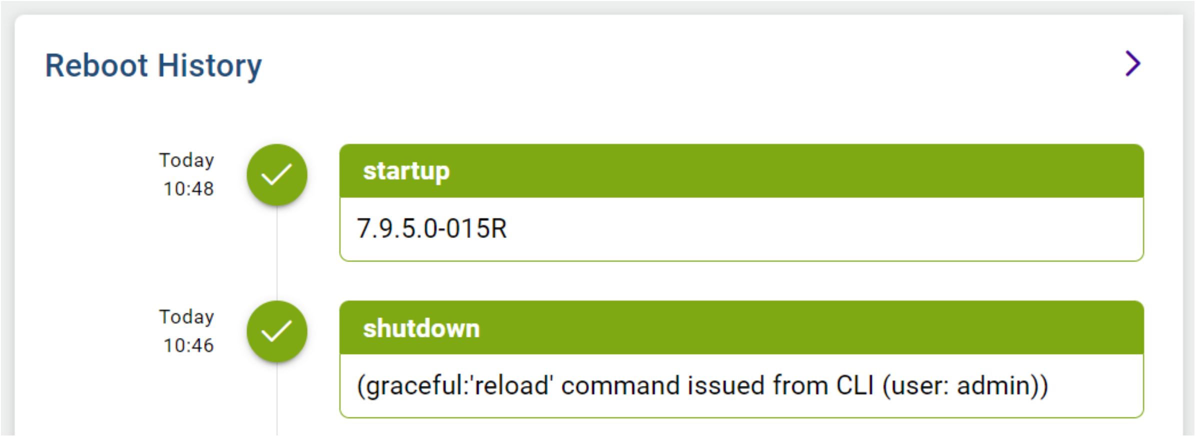
Successful

7.9.5.0-008R > 7.9.5.0-012R

Figure 38: Controller Statistics - Example Upgrade History Display

Reboot History

Figure 39 shows an example of Reboot information displayed for controllers in the RF Domain.



Reboot History

Today 10:48

startup

7.9.5.0-015R

Today 10:46

shutdown

(graceful:'reload' command issued from CLI (user: admin))

Figure 39: Controller Statistics - Example Reboot History Display

Clients

Client statistics allows you to examine the following data for the selected client:

- Connectivity information related to the client itself, and the connected AP, WLAN, and radio
- Performance metrics

To view client connectivity and performance data:

1. Go to **Statistics** > **Clients**. The Clients window displays a list of **Sites** managed by the controller.
2. Select a site under the **Site Name** column to open the **Basic** window. The Basic window displays all clients connected to devices at the selected site. Each listed client has an associated performance summary.

   See Basic on page 535 for details on information displayed in the Basic window and actions you can take.
3. Under the (interactive) **MAC Address** column, select the address associated with a target client to view a graphical presentation of client connectivity data and performance metrics.

Related Links

Basic on page 535
Client Connectivity on page 536
Client Performance Statistics on page 543

Basic

Go to **Statistics** > **Clients**, then select a **Site** in the list.

The **Basic** window opens, displaying all the connected clients for the selected site, in tabular form. Each client listed in the table is identified by its **MAC Address** and includes a summary of performance data.

Table 178 describes the type of information displayed under each column in the table.

Table 178: Clients Statistics - Basic Table Column Headings

Column Heading	Description
MAC Address	Host (MAC address) of each listed wireless client. This address is hard-coded at the factory and can not be modified. Note: The entries under this column are interactive and can be selected to view details about client connectivity and performance.
Username	Wireless client's username displays only when the authentication type is EAP, EAP-MAC, EAP-PSK, or MAC.
Hostname	Wireless client's hostname
Ingress	Total RX bytes processed by the wireless client
Egress	Total TX bytes processed by the wireless client
Total Traffic	Total bytes processed by the wireless client
SNR	SNR (*signal-to-noise ratio*) of the wireless client (in –dB)
Noise Floor	Level of disturbing influences on the signal by interference of signals (in –dBm)

Table 178: Clients Statistics - Basic Table Column Headings (continued)

Column Heading	Description
RSSI	Client-connected radio's *received signal strength indication* (RSSI) threshold level (in dBm). This threshold determines the RSSI level at which the radio acknowledges the SOP (Start of Packet) frames received from the client, and begins to demodulate and decode the packets.
TX Rate	Average data rate for the listed client for packets transmitted on the selected RF Domain member WLAN
RX Rate	Average data rate for the listed client for packets received on the selected RF Domain member WLAN

You can select a client's MAC Address to open and view a graphical display of client connectivity data and performance metrics.

Related Links

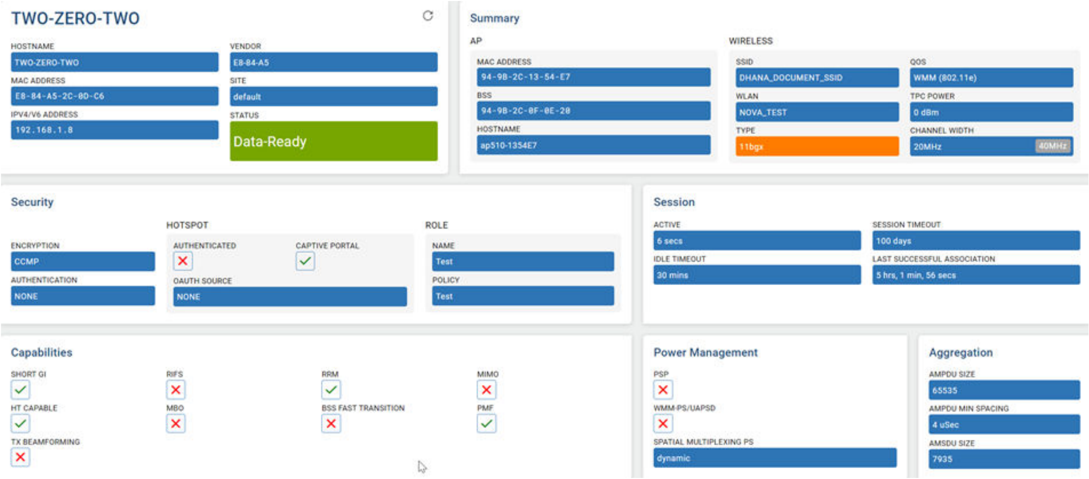
View and Manage Statistics on page 495

Client Connectivity on page 536

Client Performance Statistics on page 543

Client Connectivity

Figure 40 shows an example of a client connectivity information display.



TWO-ZERO-TWO

HOSTNAME: TWO-ZERO-TWO
VENDOR: E8-84-A5
MAC ADDRESS: E8-84-A5-2C-0D-C6
SITE: default
IPV4/V6 ADDRESS: 192.168.1.8
STATUS: Data-Ready

Summary

AP
MAC ADDRESS: 94-9B-2C-13-54-E7
BSS: 94-9B-2C-0F-0E-28
HOSTNAME: ap510-1354E7

WIRELESS
SSID: DHANA_DOCUMENT_SSID
QOS: WMM (802.11e)
WLAN: NOVA_TEST
TPC POWER: 0 dBm
TYPE: 11bgx
CHANNEL WIDTH: 20MHz 40MHz

Security

ENCRYPTION: CCMP
AUTHENTICATION: NONE

HOTSPOT
AUTHENTICATED: ☒
CAPTIVE PORTAL: ✓
OAUTH SOURCE: NONE

ROLE
NAME: Test
POLICY: Test

Session

ACTIVE: 6 secs
SESSION TIMEOUT: 100 days
IDLE TIMEOUT: 30 mins
LAST SUCCESSFUL ASSOCIATION: 5 hrs, 1 min, 56 secs

Capabilities

SHORT GI: ✓
RIFS: ☒
RRM: ✓
MIMO: ☒
HT CAPABLE: ✓
MBO: ☒
BSS FAST TRANSITION: ☒
PMF: ✓
TX BEAMFORMING: ☒

Power Management

PSP: ☒
WMM-PS/UAPSD: ☒
SPATIAL MULTIPLEXING PS: dynamic

Aggregation

AMPDU SIZE: 65535
AMPDU MIN SPACING: 4 uSec
AMSDU SIZE: 7935

Figure 40: Example of Client Connectivity Information Display

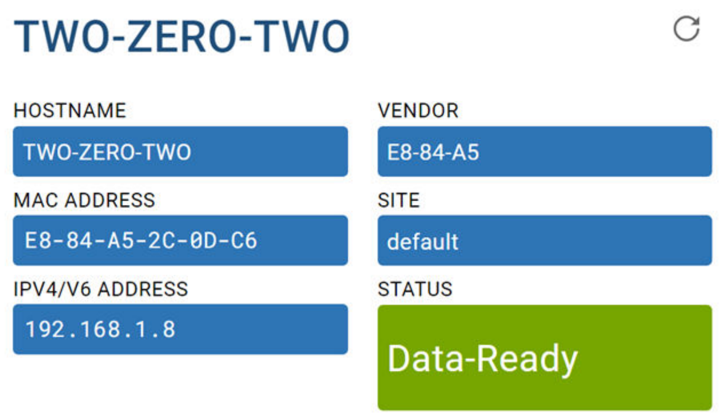
Client connectivity information is arranged under the following panes (left-to-right, top-to-bottom):

- Client Information on page 537
- Summary on page 538
- Security on page 539
- Session on page 540

- Capabilities on page 540
- Power Management on page 541
- Aggregation on page 542

Client Information

Figure 41 shows an example of client information collected and displayed.



TWO-ZERO-TWO

HOSTNAME: TWO-ZERO-TWO

VENDOR: E8-84-A5

MAC ADDRESS: E8-84-A5-2C-0D-C6

SITE: default

IPV4/V6 ADDRESS: 192.168.1.8

STATUS: Data-Ready

Figure 41: Client Connectivity – Example of Client Information Display

Select ⟳ to refresh the display.

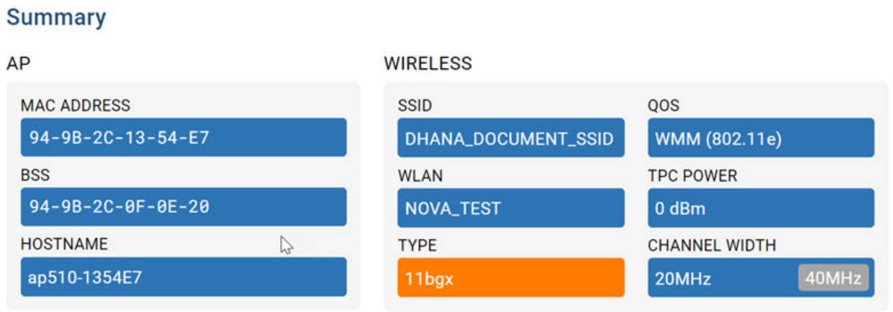
Table 179 describes the information displayed.

Table 179: Client Connectivity – Client Information Description

Field	Description
Hostname	Displays the hostname of the selected wireless client.
Vendor	Displays the vendor name (manufacturer) of the wireless client.
MAC Address	Displays the factory encoded MAC address of the selected wireless client.
Site	Displays the site (RF Domain) at which the client has a connection.
IPv4/IPv6 Address	Displays the IPv4 or IPv6 address the selected wireless client is currently utilizing as a network identifier.
Status	Displays the current operational status of the wireless client. The possible client status values include: • Data Ready • Not Data Ready • Roaming • Not Roaming

Summary

Figure 42 shows an example of information displayed for a client-connected access point (AP) and the Wireless LAN (WLAN) with which it is associated.



Summary

AP

MAC ADDRESS
94-9B-2C-13-54-E7

BSS
94-9B-2C-0F-0E-20

HOSTNAME
ap510-1354E7

WIRELESS

SSID
DHANA_DOCUMENT_SSID

QOS
WMM (802.11e)

WLAN
NOVA_TEST

TPC POWER
0 dBm

TYPE
11bgx

CHANNEL WIDTH
20MHz 40MHz

Figure 42: Client Connectivity – Example Summary Display

Table 180 describes the information displayed.

Table 180: Client Connectivity – Summary Display Description

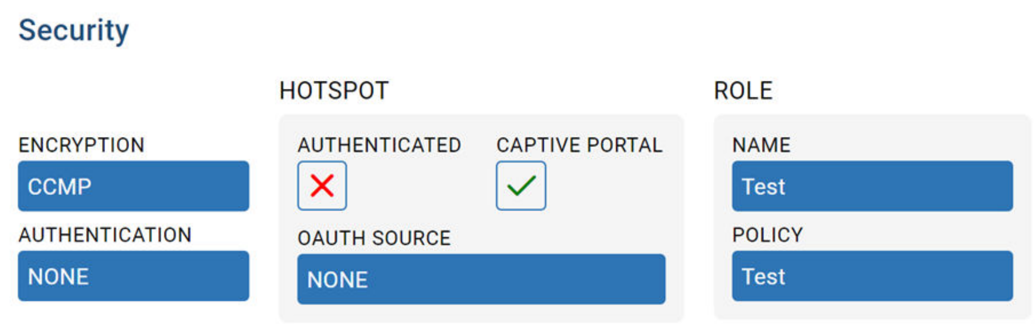
Field	Description
AP	
MAC Address	Displays the MAC address of the wireless client's connected AP.
BSS	Displays the MAC address of the *Basic Service Set* (BSS) to which the AP belongs. A BSS is a set of stations that can communicate with one another.
Hostname	Displays administrator-assigned hostname of the AP reporting client stats to RF Domain member devices.
Wireless	
SSID	Displays the SSID assigned to the WLAN.
QoS	Identifies the WLAN QoS policy setting.
WLAN	Displays the name assigned to the WLAN when it was created.
TPC Power	Displays the *transmit power control* (TPC) mitigation value (in dBm), if it is configured. Transmit power is configured for radio interface. A value of 0 (zero) in this field indicates that Smart RF manages the power.

Table 180: Client Connectivity – Summary Display Description (continued)

Field	Description
Type	Displays the radio type. The possible radio type values include: • 802.11b • 802.11bg • 802.11bgn • 802.11a • 802.11an
Channel Width	Displays the current channel width versus the maximum possible channel width (shaded in gray).

Security

Figure 43 shows an example display of Security information for the selected wireless client.



Security

ENCRYPTION: CCMP

AUTHENTICATION: NONE

HOTSPOT

AUTHENTICATED: ☒

CAPTIVE PORTAL: ✓

OAUTH SOURCE: NONE

ROLE

NAME: Test

POLICY: Test

Figure 43: Client Connectivity – Example of Security Display

Table 181 describes the information displayed.

Table 181: Client Connectivity – Security Display Description

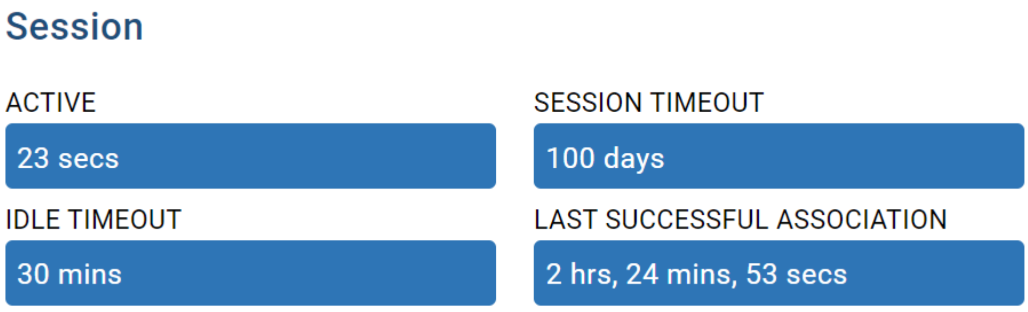
Field	Description
Encryption	Identifies the encryption scheme, as defined in WLAN **Security** settings.
Authentication	Identifies the authentication scheme, as defined in WLAN **Security** settings.
Hotspot	
Authenticated	Indicates whether the client successfully authenticated by guest access
Captive Portal	Indicates whether a Captive Portals policy is enforced on the WLAN connected to an AP that is deployed as a public hotspot.

Table 181: Client Connectivity – Security Display Description (continued)

Field	Description
Oauth Source	Identifies the source of how the user is oauthed using social media login. Possible sources include Facebook, Google, Twitter, Linkedin, or None.
Role	
Name	Displays the assigned user **Role Name** in a Role policy that is applied to the AP.
Policy	Displays the name of the Role policy that is applied to the AP.

Session

Figure 44 shows an example display of Session information for the selected wireless client.



Session

ACTIVE

23 secs

SESSION TIMEOUT

100 days

IDLE TIMEOUT

30 mins

LAST SUCCESSFUL ASSOCIATION

2 hrs, 24 mins, 53 secs

Figure 44: Client Connectivity – Example Session Display

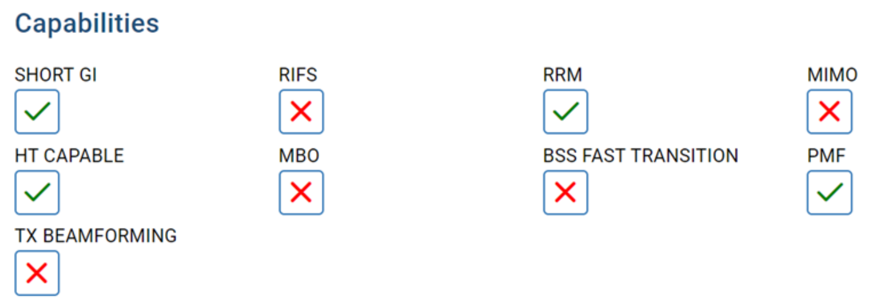
Table 182 describes the information displayed.

Table 182: Client Connectivity – Session Display Description

Field	Description
Active	Displays the duration (in seconds) of the last active session between the wireless client and its connected AP.
Session Timeout	Displays the duration for which a session can be maintained by the wireless client without it being disassociated from its connected AP radio.
Idle Timeout	Displays the **Inactivity Timeout** setting of the Captive Portal policy applied to the AP.
Last Successful Association	Displays the duration the wireless client was in association with its connected AP.

Capabilities

Figure 45 shows an example Capabilities display for the selected client.



Capabilities

SHORT GI ☑

RIFS ☒

RRM ☑

MIMO ☒

HT CAPABLE ☑

MBO ☒

BSS FAST TRANSITION ☒

PMF ☑

TX BEAMFORMING ☒

Figure 45: Client Connectivity – Example Capabilities Display

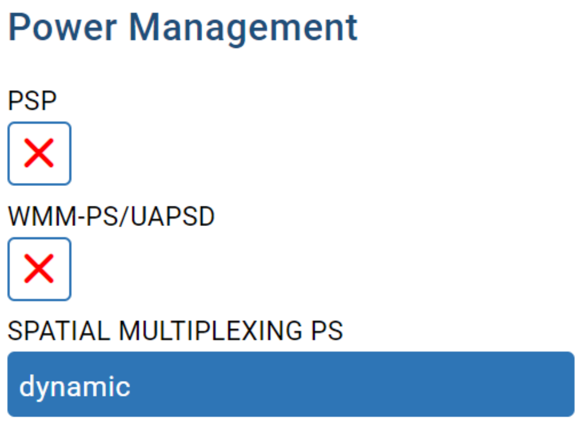
Table 183 describes the information displayed.

Table 183: Client Connectivity – Capabilities Display Description

Field	Description
Short GI	Indicates whether Short Guard Interval is enabled for the radio.
RIFS	Indicates whether RIFS (Reduced Interframe Spacing) parameters are configured for the radio.
RRM	Indicates whether RRM (Radio Resource Management) settings are configured for the WLAN.
MIMO	Indicates whether MU-MIMO (multi-user multiple input multiple output) is configured for the radio. MU-MIMO is disabled by default.
HT Capable	Indicates whether clients with higher throughput (802.11n clients) are prioritized over clients with slower throughput (802.11 a/ b/g) clients. **Prefer HT Clients** is disabled by default under **Advanced** settings for the radio.
MBO	Indicates whether Multi Band Operation is enabled or disabled (default) for the WLAN.
BSS Fast Transition	Indicates whether Fast BSS Transition is enabled or disabled (default) for the WLAN.
PMF	Indicates whether Protected-management-frames (PMF) enforcement is enabled for the WLAN.
TX Beamforming	Indicates whether transmit beamforming is enabled for the radio. Note: This feature is enabled on the radio interface using CLI command `transmit-beamforming`.

Power Management

Figure 46 shows an example Power Management display for the selected client.



Power Management

PSP

✗

WMM-PS/UAPSD

✗

SPATIAL MULTIPLEXING PS

dynamic

Figure 46: Client Connectivity – Example Power Management Display

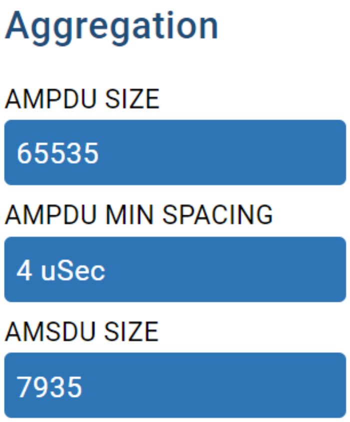
Table 184 describes the information displayed.

Table 184: Client Connectivity – Power Management Display Description

Field	Description
PSP	Indicates whether PSP (Power Save Poll) mode is enabled or disabled. • ✓ means PSP is enabled. • ✗ means PSP is disabled. Power Save Poll is a protocol that helps to reduce the amount of time a radio needs to be powered. PSP allows the WiFi adapter to notify the AP when the radio is powered down. The AP holds any network packet to be sent to this radio.
WMM-PS/UAPSD	Indicates whether WMM-PS (WMM Power Save)/U-APSD (Unscheduled Automatic Power Save Delivery) is enabled or disabled. The **WMM Power Save** mechanism (enabled by default) is applied through a Radio QoS policy. See Radio QoS Policies on page 418 for details.
Spatial Multiplexing PS	Displays whether this feature is enabled on the wireless client. The SM (spatial multiplexing) power save mode allows an 802.11n client to power down all but one of its radios. This power save mode has two sub modes of operation: static operation and dynamic operation.

Aggregation

Figure 47 shows an example of an Aggregation display.



Aggregation

AMPDU SIZE

65535

AMPDU MIN SPACING

4 uSec

AMSDU SIZE

7935

Figure 47: Client Connectivity – Aggregation

Table 185 describes the information displayed.

Table 185: Client Connectivity – Aggregation Display Description

Field	Description
AMPDU Size	Displays the maximum size of AMPDU (in bytes). AMPDU is a set of Ethernet frames addressed to the same destination wrapped in an 802.11n MAC header. AMPDUs are used in noisy environments to provide reliable packet transmission.
AMPDU Min Spacing	Displays the time interval between two consecutive Ethernet frames (in uSec).
AMSDU Size	Displays the maximum size of AMSDU frame size (in bytes). AMSDU is a set of Ethernet frames addressed to the same destination that are wrapped in a 802.11n frame.

Client Performance Statistics

To view Client Statistics:

1. Go to **Statistics** > **Clients** and select a target **Site**.
2. Select a target **Client**.
3. Scroll to the bottom of the display and select > adjacent to **Statistics** to expand the display and view client performance statistics.

Figure 48 shows an example of a client statistics display.

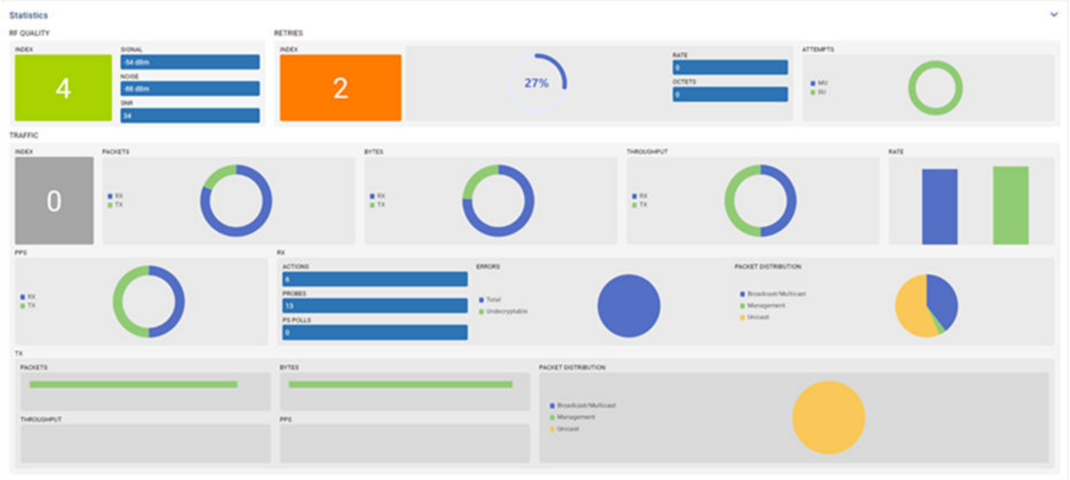


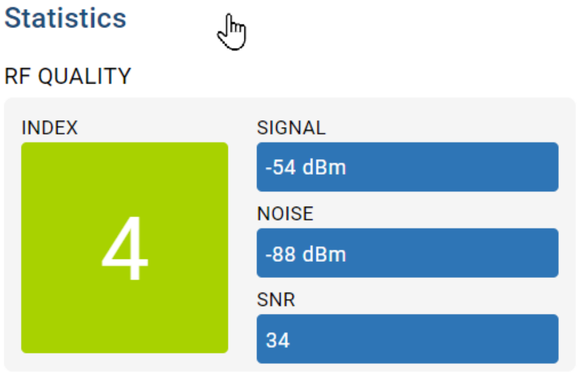
Figure 48: Example of Client Statistics Display

Client performance statistics are arranged under the following panes (left-to-right, top-to-bottom):

- RF Quality
- Retries on page 545
- Traffic on page 546

RF Quality

Figure 49 shows an example RF Quality display for a client.



Statistics

RF QUALITY

INDEX

4

SIGNAL

-54 dBm

NOISE

-88 dBm

SNR

34

Figure 49: Client Performance Statistics – Example RF Quality Display

Table 186 describes the information displayed.

Table 186: Client Performance Statistics – RF Quality Description

Widget/Field	Description
Index	Displays an integer indicating the overall RF performance for the selected client. The RF quality indices are: • 0 – 50 (Poor) • 50 – 75 (Acceptable) • 75 – 100 (Good)
Signal	Displays the power of the radio signals (in –dBm) for the selected client.
SNR	Displays the selected client's signal-to-noise ratio (SNR). A high SNR could warrant a different AP connection to improve performance.
Noise	Displays the level of noise (in –dbm) in the client-connected radio signal.

Retries

Figure 50 shows an example of a Retries display for a client.

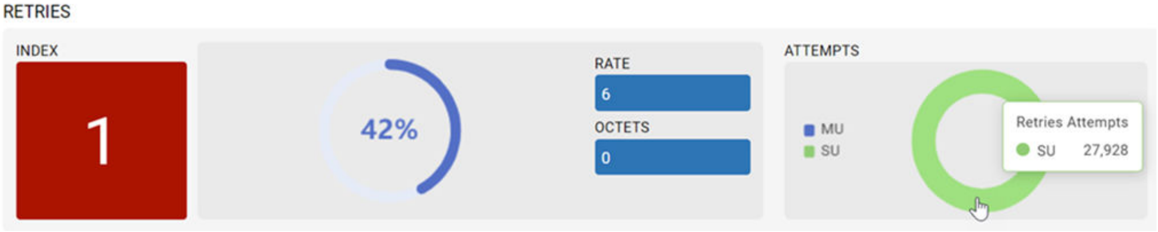


Figure 50: Client Performance Statistics – Example Retries Display

Table 187 describes the information displayed.

Table 187: Client Performance Statistics – Retries Description

Widget/Field	Description
Index	Displays the average number of retries per packet (and a performance indicator). A high Index number indicates possible network or hardware problems. Assess the error rate with respect to potentially high signal and SNR values to determine whether the error rate coincides with a noisy signal.
Rate	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.

Table 187: Client Performance Statistics – Retries Description (continued)

Widget/Field	Description
Octets	Displays the total number of transmitted retried octets (bytes) with no errors.
Attempts	Displays the number of retry connection attempts for multi-user multiple input, multiple output (MU-MIMO) and Single-user multiple input, multiple output (SU-MIMO) transmissions between the selected client and its associated AP.

Traffic

Traffic widgets display statistics on the traffic generated and received by the selected client. Hover over widgets to view detailed statistics.

Figure 51 shows an example of a Traffic display.

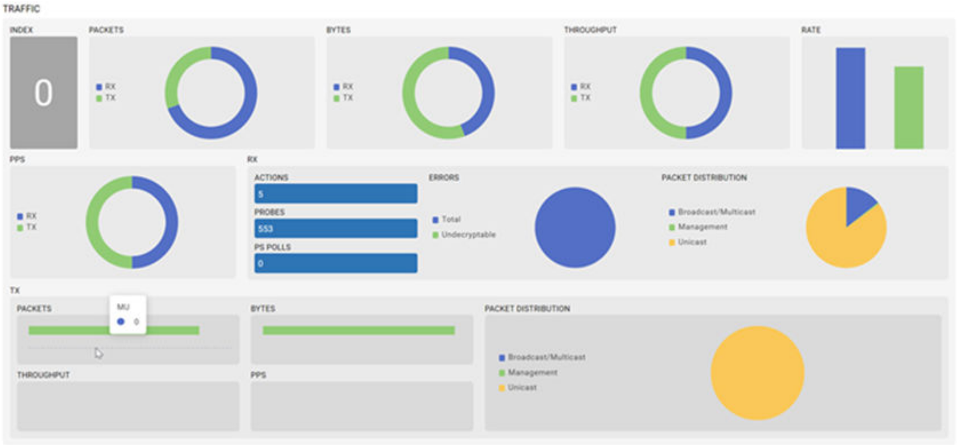


Figure 51: Client Performance Statistics – Example Traffic Display

Table 188 describes the information displayed.

Table 188: Client Performance Statistics – Traffic Description

Widget/Field	Description
Index	The traffic Index measures how efficiently the traffic medium is utilized. It is defined as the percentage of current throughput relative to the maximum possible throughput. Traffic indices are: • 0 – 20 (Very low utilization) • 20 – 40 (Low utilization) • 40 – 60 (Moderate utilization) • 60 and above (High utilization)
Packets	Displays the total number of packets transmitted and received by the selected client.

Table 188: Client Performance Statistics – Traffic Description (continued)

Widget/Field	Description
Bytes	Displays the total TX and RX bytes processed by the selected client.
Throughput	Displays the total amount user data transmitted and received by the selected client (in bytes).
Rate	Displays the average user data rate in both directions.
PPS	Displays the average packet rate at the physical layer in both directions.
RX	The following performance statistics are displayed: • The number of receive Actions during data transmission with the client's connected AP. • The number of Probes received. A probe is a program or other device inserted at a key juncture in a network for the purpose of monitoring or collecting data about network activity. • The number of power save events using the PSP (Power Save Poll) mode. Power Save Poll is a protocol that helps to reduce the amount of time a radio needs to be powered. PSP allows the WiFi adapter to notify the AP when the radio is powered down. The AP holds back any network packet to be sent to this radio. • The number of Errors encountered during data transmission. The higher the error rate, the less reliable the connection or data transfer between the client and connected AP. • Displays the distribution of Broadcast/Multicast, Management, and Unicast packets received by the client.
TX	The following performance statistics are displayed: • The total number of SU-MIMO and MU-MIMO Packets transmitted to the client by its connected AP. • The total number of SU-MIMO and MU-MIMO Bytes transmitted to and processed by the client. • The total amount user data sent by the selected client during SU-MIMO and MU-MIMO transmissions (in bytes). • The number of power save events during SU-MIMO and MU-MIMO transmissions using the PSP (Power Save Poll) mode. Power Save Poll is a protocol that helps to reduce the amount of time a radio needs to be powered. PSP allows the WiFi adapter to notify the AP when the radio is powered down. The AP holds back any network packet to be sent to this radio. • Displays the distribution of Broadcast/Multicast, Management, and Unicast packets transmitted by the selected client.

Sites

Go to **Statistics** > **Sites**.

The Sites window displays all the RF Domains managed by the controller or service platform, as well as a summary of site-related statistics, in tabular form.

Table 189 describes the type of statistical information displayed under each column in the table.

Table 189: Sites Statistics Description

Column Heading	Description
Site Name	Identifies the name assigned to the site (RF Domain).
Manager	Displays the RF Domain Manager.
Devices	Indicates the number of online APs within the RF Domain
Radios	Displays the number of radios within the RF Domain
Clients	Indicates the number of connected clients within the RF Domain
Sensors	Indicates the number of radios configured as sensors within the RF domain
Rate	Displays the average user data rate within the RF Domain.
Traffic	Displays the total bytes of data transmitted and received within the RF Domain.
Pkts	Displays the total number of data packets transmitted and received within the RF Domain.
PPS	Displays the transmit and receive transmission rates in packets-per-second.
Management	Displays the total number of management packets processed within the RF Domain.
Rx errors	Displays the number of errors encountered during data transmission within the RF Domain. The higher the error rate, the less reliable the connection or data transfer.
Tx dropped	Displays the total number of dropped data packets within the RF Domain.

Mesh Point

Mesh networking provides users wireless access to broadband applications anywhere, even in a moving vehicle. Initially developed for secure and reliable military battlefield communications, mesh technology supports public safety, public access, and public works. Mesh technology reduces the expense of wide-scale networks, by leveraging Wi-Fi enabled devices that are already deployed.

Mesh points are APs dedicated to mesh network support. Mesh points capture and disseminate their own data and serve as a relay for other nodes.

The **Statistics** > **Mesh Point** option has the following sub-dashboards:

- Details
- Statistics
- Config
- Logical View
- Geographical View

1. Select **Statistics** > **Mesh Point**.

   The list of available sites opens.
2. Select a site to view statistical details about the mesh point configurations on the site.

   The **Details** window opens.

Details

View mesh point statistics for member APs and their connected clients.

1. Select **Statistics** > **Mesh Point** > **Details**.
2. View the following details:

Hostname	Displays the administrator assigned hostname for each configured mesh point in the mesh network
MAC Address	Displays the MAC Address of each configured mesh point in the mesh network
Mesh Point Name	Displays the name of each configured mesh point in the mesh network
Root	A root mesh point is defined as a mesh point connected to the WAN and provides a wired backhaul to the network

3. Select + from the `Root` option to view additional device details.

   The root information provides the list of devices not connected to a root within a mesh network.
4. Select a device from **Device Type** to view the following details:
   - General
   - Path
   - Root
   - Multicast Path
   - Neighbors
   - Security
   - Proxy

5. Refer to the **General** tab for the following information:

Name	Unique name of each configured mesh point in the mesh network
MAC	MAC Address of each configured mesh point in the mesh network
Hostname	Administrator assigned hostname for each configured mesh point in the mesh network
Configured as Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network
Is Root	Indicates whether the current mesh point is a root mesh point
Destination Address	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID
Root MP ID	Lists the interface ID of the interface on which the next hop for the mesh network can be found
Interface ID	Uniquely identifies an interface associated with the ID. Each mesh point on a device can be associated with one or more interfaces
Next Hop IFID	Identifies the ID of the interface on which the next hop for the mesh network can be found
Root Bound Time	Displays the duration this mesh point has been connected to the mesh root
IFID Count	Displays the number of IFIDs associated with all the configured mesh points in the network
Next Hops Use Time	Lists the time when the next hop in the mesh network topology was last utilized
Root Hops	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out
Radio Interface	Lists the radio interface on which the mesh point operates

6. Refer to the **Path** tab for the following information:

Name	Displays the name of each configured mesh point in the RF Domain
Destination Address	The destination is the endpoint of mesh path. It can be a MAC address or a mesh point ID

Destination	The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh
Is Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network
MiNT ID	Displays the MiNT Protocol ID for the global mint area identifier. This area identifier separates two overlapping MiNT networks and need only be configured if the administrator has two MiNT networks that share the same packet broadcast domain
Next Hop IFID	The Interface ID of the mesh point that traffic is being directed to
Hops	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out
Mobility	Displays whether the mesh point is a mobile or static node. Displays **`True`** when the device is mobile and **`False`** when the device is not mobile
Metric	A measure of the quality of the path. A lower value indicates a better path
State	Indicates whether the path is currently **`Valid`** or **`Invalid`**
Binding	Indicates whether the path is **`bound`** or **`unbound`**
Timeout	The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is **`Init`** or **`In Progress`**, the timeout duration has no significance. If the state is **`Enabled`**, the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is **`Failed`**, the timeout duration is the amount of time after which the system will retry
Sequence	The sequence number also known as the destination sequence number. It is updated whenever a mesh point receives new information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination

7. Refer to the **Root** tab for the following information:

Name	Displays the name of each configured mesh point in the RF Domain
Recommended	Displays the root that is recommended by the mesh routing layer
Root MP ID	The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration
Next Hop IFID	The IFID of the next hop. The IFID is the MAC Address on the destination device
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor
Bound	Indicates whether the root is **bound** or **unbound**
Metric	Displays the computed path metric between the neighbor and their root mesh point
Interface Bias	This field lists any bias applied because of the Preferred Root Interface Index
Neighbor Bias	This field lists any bias applied because of the Preferred Root Next-Hop Neighbor IFID
Root Bias	This field lists any bias applied because of the Preferred Root MPID (mesh point ID)

8. Refer to the **Multicast Path** tab for the following information:

Name	Displays the name of each configured mesh point in the RF Domain
Subscriber Name	Lists the subscriber name is used to distinguish between other mesh point neighbors both on the same device and on other devices
Subscriber MP ID	Lists the subscriber ID to distinguish between other mesh point neighbors both on the same device and on other devices

Group Address	Displays the MAC address used for the Group in the mesh point
Timeout	The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is `Init` or `In Progress`, the timeout duration has no significance. If the state is `Enabled`, the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is `Failed`, the timeout duration is the amount of time after which the system will retry

9. Refer to the **Neighbors** tab for the following information:

Name	Displays the name of each configured mesh point in the RF Domain
Destination Address	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID
Neighbor MP ID	The MAC Address that the device uses to define the mesh point in the device that the neighbor is a part of. It is used to distinguish the device that is the neighbor
Neighbor IFID	The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh
Root MP ID	The mesh point ID of the neighbor's root mesh point
Is Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. `Yes` if the mesh point that is the neighbor is a root mesh point or `No` if the Mesh Point that is the neighbor is not a root
Mobility	Displays whether the mesh point is a mobile or static node. Displays `True` when the device is mobile and `False` when the device is not mobile
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor

Mesh Root Hops	The number of devices between the neighbor and its root mesh point. If the neighbor is a root mesh point, this value will be **0**. If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be **1**. Each mesh point between the neighbor and its root mesh point is counted as 1 hop
Resourced	Displays whether the mesh point has been resourced or not. The Mesh Connex neighbor table can contain more neighbors than the AP supports. If the neighbor is resourced, it will take away a one of the resources for a wireless client device to be used for meshing. Displays **True** when the device is resourced and **False** when the device is not
Link Quality	An abstract value depicting the quality of the mesh link between the device and the neighbor. The range is from 0 (weakest) to 100 (strongest)
Link Metric	This value shows the computed path metric from the device to the neighbor mesh point using this interface. The lower the number the better the possibility that the neighbor will be chosen as the path to the root mesh point
Root Metric	The computed path metric between the neighbor and their root mesh point

Rank	The rank is the level of importance and is used for automatic resource management • **8** – The current next hop to the recommended root • **7** – Any secondary next hop to the recommended root to has a good potential route metric • **6** – A next hop to an alternate root node • **5** – A downstream node currently hopping through to get to the root • **4** – A downstream node that could hop through to get to the root, but is currently not hopping through any node (look at authentication, as this might be an issue) • **3** – A downstream node that is currently hopping through a different node to get to the root, but could potentially have a better route metric if it hopped through this node • **2** – Reserved for active peer to peer routes and is not currently used • **1** - A neighbor bound to the same recommended root but does not have a potential route metric as good as the neighbors ranked 8 and 7 • **0** – A neighbor bound to a different root node • **–1** – Not a member of the mesh as it has a different mesh ID All client devices hold a rank of 3 and can replace any mesh devices lower than that rank
Age	Displays the number of milliseconds since the mesh point last heard from this neighbor

10. Refer to the **Security** tab for the following information:

Name	Unique name of each configured mesh point in the network
Destination Address	Endpoint of a mesh path. It can be a MAC address or a mesh point ID
Radio Interface	Indicates the interface that is used by the device to communicate with this neighbor
Interface ID	The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces

State	Displays the link state for each mesh point: • **`Init`** - indicates the link has not been established or has expired • **`Enabled`** - indicates the link is available for communication • **`Failed`** - indicates the attempt to establish the link failed and cannot be retried yet • **`In Progress`** - indicates the link is being established but is not yet available
Timeout	Displays the maximum value in seconds that the link is allowed to stay in the **`In Progress`** state before timing out
Keep Alive	Indicates whether the local mesh point will act as a source to authenticate the link and not let it expire

11. Refer to the **Proxy** tab for the following information:

Name	Displays the name of each configured mesh point in the RF Domain
Destination Address	The destination is the endpoint of mesh path. It may be a MAC address or a MPID (mesh point ID)
Proxy Address	Displays the MAC Address of the proxy used in the mesh point
Age	Displays the age of the proxy connection for each of the mesh points in the RF Domain
Proxy Owner	The owner (MPID) is used to distinguish the device that is the neighbor
VLAN	The VLAN ID used as a virtual interface with this proxy. A value of 4095 indicates that there is no VLAN ID

Statistics

View the mesh point statistical data.

1. Select **Statistics** > **Mesh Point** > **Statistics**.
2. Select a mesh point from the list of available mesh points.
3. View the following mesh point data for transmit and receive statistics:

Indicators: Index	Displays information to indicate whether or not a traffic index is present
Indicators: Max User Rate	Displays the maximum user throughput rate for mesh points in a mesh network

Indicators: Neighbor Count	Displays the total number of neighbors known to the mesh points in a mesh network
Indicators: Radio Count	Displays the total number of neighbor radios known to the mesh points in a mesh network
Data Bytes	Displays the total amount of data, in Bytes, transmitted and received by mesh points in a mesh network
Data Rates	Displays the average data rate, in kbps, for all data transmitted and received by mesh points in a mesh network
Packets Rate	Displays the average data packet rate, in packets per second, for all data transmitted and received by mesh points in a mesh network
Packets	Displays the total amount of data, in packets, transmitted and received by mesh points in a mesh network
Broadcast	Displays the total number of broadcast and multicast packets transmitted and received from mesh points in a mesh network
Management	Displays the total number of management packets that were transmitted and received through the mesh points in a mesh network

Config

View the configuration details of Mesh Points configured.

1. Select **Statistics** > **Mesh Point** > **Config**.

   All the configured Mesh Points within a system are displayed in the **Config** dashboard.
2. Review the following configuration details for each Mesh Point:

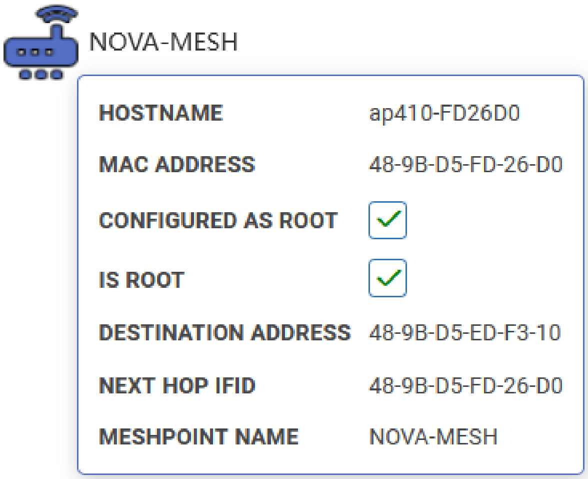
Name	The unique name of configured mesh point
Status	The status of each configured mesh point, either selected or crossed
Mesh ID	The ID (mesh identifier) assigned to mesh point
Radio Count	Displays the number of managed radios by a mesh point

Logical View

View the logical representation of mesh point statistics.

1. Select **Statistics** > **Mesh Point** > **Logical View**.
2. Select a **Mesh Point** from the list of available mesh points.

   The graphical representation of the selected mesh point opens.
3. Hover over the mesh point graphics to display the mesh point details, as shown in Figure 52.



NOVA-MESH

HOSTNAME	ap410-FD26D0
MAC ADDRESS	48-9B-D5-FD-26-D0
CONFIGURED AS ROOT	☑
IS ROOT	☑
DESTINATION ADDRESS	48-9B-D5-ED-F3-10
NEXT HOP IFID	48-9B-D5-FD-26-D0
MESHPOINT NAME	NOVA-MESH

Figure 52: Mesh Point statistical logical view data

Geographical View

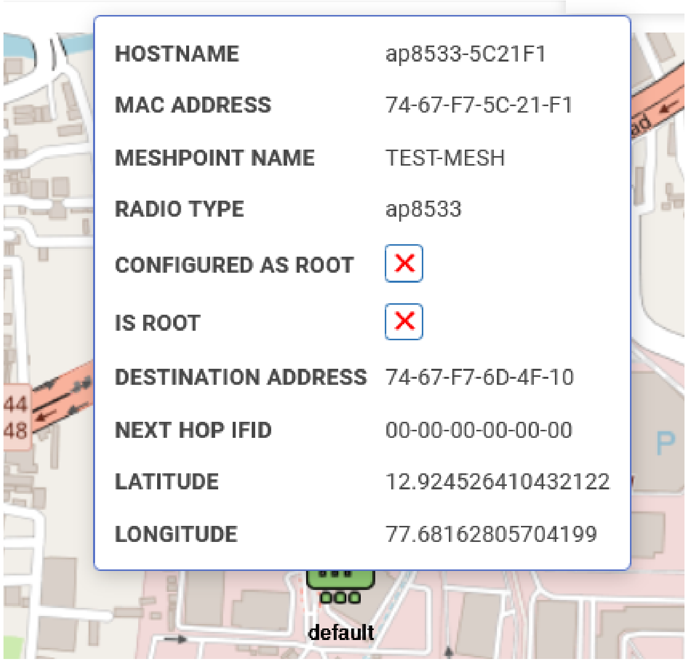
View a map where icons of each device in the mesh point are overlaid. The devices within a mesh point are assigned latitude and longitude values. This provides a geographical overview of the location of each member device.

Devices that do not have any assigned latitude or longitude values within a mesh are displayed in the **Unplaced Devices** window.

1. Select **Statistics** > **Mesh Point** > **Geographical View**.
2. Select a **Mesh Point**.

   The devices that are part of that network open in the map.
3. Use the + or - icons to zoom in and out of the map.

4. Select the device graphics to view various device details, including latitude and longitude information.



HOSTNAME	ap8533-5C21F1
MAC ADDRESS	74-67-F7-5C-21-F1
MESHPOINT NAME	TEST-MESH
RADIO TYPE	ap8533
CONFIGURED AS ROOT	☒
IS ROOT	☒
DESTINATION ADDRESS	74-67-F7-6D-4F-10
NEXT HOP IFID	00-00-00-00-00-00
LATITUDE	12.924526410432122
LONGITUDE	77.68162805704199

Figure 53: Mesh point geographical details

5. Use the **Unplaced Devices** window to review the list of devices that are not placed in any of the geographical locations within the mesh network.

NEW!

WIPS Summary

The WIPS (Wireless Intrusion Protection System) provides continuous protection against wireless threats and acts as an additional layer of security complimentary 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.

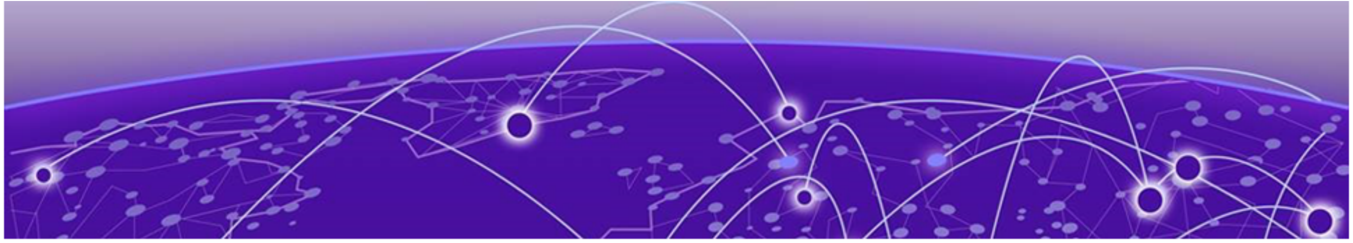
The WIPS Summary window lists existing RF Domains (Sites) in the system and reports the number of unauthorized and interfering devices contributing to the potential poor performance of the RF Domain's network traffic. Additionally, the number of WIPS events reported by each RF Domain is also listed to help an administrator better mitigate risks to the network.

Go to **Statistics** > **DevicesWIPS Summary**. The **Sites** pane opens, displaying all the RF Domain member devices and related details in tabular form.

Table 190 describes the type of information displayed under each column in the Sites table.

Table 190: WIPS Summary Statistics - Sites Table Column Headings

Column Heading	Description
Site Name	Lists the RF Domain within the system reporting rogue and interfering AP event counts. Use this information to assess whether a particular RF Domain is reporting an excessive number of events or a large number of potentially invasive rogue APs versus the other RF Domains within the controller, service platform or AP managed system.
Number of Rogue APs	Displays the number of unsanctioned devices in each listed RF Domain. Unsanctioned devices are those devices detected within the listed RF Domain, but have not been deployed by a administrator as a known and approved controller, service platform or AP managed device.
Number of Interfering APs	Displays the number of devices exceeding the interference threshold in each listed RF Domain. Each RF Domain utilizes a WIPS policy with a set interference threshold (from -100 to -10 dBm). When a device exceeds this noise value, it is defined as an interfering AP capable of disrupting the signal quality of other sanctioned devices operating below an approved RSSI maximum value.
Number of WIPS Events	Lists the number of devices triggering a WIPS event within each listed RF Domain. Each RF Domain utilizes a WIPS policy where excessive, MU and AP events can have their individual values set for event generation. An administrator can enable or disable the filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action.



Licenses

Licenses are required for the number of allowable adoptions per access point, controller, service platform, or managed cluster.

> Note
> The **Licenses** screen is available only to controllers and service platforms capable of sustaining device connections, and thus requires license support to set the maximum number of device connections permitted.

Managing infrastructure devices requires a license key to enable software functionality or define the number of adoptable devices allowable. Apply new **Licenses** to the controller to increase the number of device adoptions permitted, or to allow the use of the advanced security features.

Each controller and service platform family has multiple models to choose from that range from zero licenses to the maximum number that can be loaded for that specific SKU.

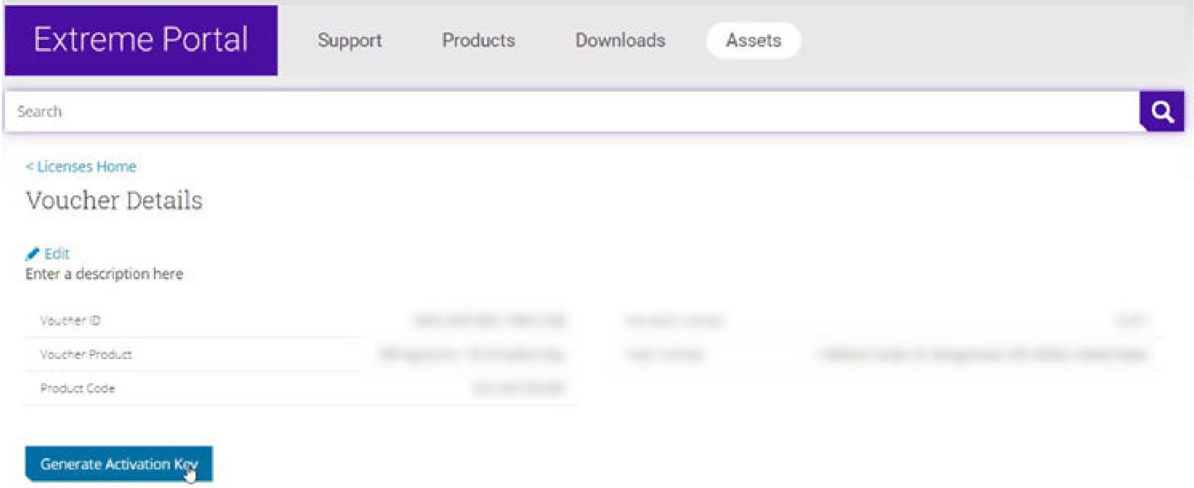
Generate the license on the Extreme Networks Support Portal and apply the license on the controller.

Generate Activation License Key

All customers must generate and install an Activation License Key for ExtremeCloud IQ. Regardless of whether you obtain a new license or upgrade to ExtremeCloud IQ, follow these steps to generate and install the Activation License Key:

1. To obtain the controller Serial Number:
    a. Log in to ExtremeCloud IQ.
    b. Go to the **Device List** > **Serial** column for the controller.
2. Log into the Extreme Networks Support Portal.
3. Go to **Assets** > **Licenses Home** and select the ExtremeCloud IQ Voucher ID line item from the list.

4. On the **Voucher Details** page, select **Generate Activation Key**.



Voucher ID [redacted] [redacted]

Voucher Product [redacted] [redacted]

Product Code [redacted]

Figure 54: Generate Activation Key

5. Provide the Serial Number for the ExtremeCloud IQ to be activated.
6. Check the box to accept **Terms and Conditions** and select **Submit**.
7. The Activation License Key is generated.
8. Copy the Activation Key from the Extreme Networks Portal.
9. On the ExtremeCloud IQ, go to **License** and paste the Activation Key string in the appropriate String field.

   The number of supported devices is populated in the Value field.

Apply the License to the Controller

After you have generated the license on the Extreme Networks Portal, apply the license to the controller. There are different types of licenses available that provide special features.

1. Go to **License** and enter the license string and value for the AP or AAP (Adaptive AP Licenses).
2. To add a feature license, select the plus sign.
3. From the License Type field, select a feature license and provide the license key.

   Feature license types:

   - AP
   - AAP (Adaptive AP Licenses)
   - Advanced Security
   - Hotspot Analytics
   - Web Filtering
   - VX

Related Links

License Types on page 563

License Types

ExtremeCloud IQ offers feature licenses that you apply directly on the controller. To add feature licenses, from the **License** page, select the plus sign and add the license key for the selected feature.

AP License	The number of APs available for adoption under the restrictions of the license. This number applies to dependent mode adaptive APs only, and not independent mode APs. The **Cluster** pane lists the number of APs available for adoption by cluster members under the restrictions of the licenses, as pooled amongst the cluster members.
AAP License (Adaptive AP Licenses)	The number of AAPs available for adoption under the restrictions of the license. This number applies to dependent mode adaptive AAPs only, and not independent mode AAPs. The **Cluster** pane lists the number of AAPs available for adoption by cluster members under the restrictions of the licenses, as pooled amongst the cluster members.
Advanced Security	The Role-Based Firewall feature with increased IPSec VPN tunnels. The number of IPSec tunnels varies by platform.
Hot Spot Analytics	The Analytics tool (an enhanced statistical management tool) for NX9500 and NX9600 series service platforms. An analytics tool used with Passpoint. A passpoint policy provides an interoperable platform for streamlining Wi-Fi access to access points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices.
Web Filtering	Use Web Filtering to restrict access to specific resources on the internet. With Web Filtering, you can manage records and URL caching time. You can also filter access to cached URLs when a server is unreachable or is unable to classify request types.
VX	License for a virtual platform.

Related Links

Cluster License Details on page 564

Cluster License Details

AP Cluster Details

The **Cluster** pane displays further details about AP licensing.

Table 191: AP Cluster Details

AP Installed Licenses	Number of installed licenses.
AP Borrowed Licenses	Borrowed licenses are the total number of AP licenses borrowed by the site controller from the NOC controller (NOC controllers if a NOC controller is in a cluster). AP borrowed licenses are always zero in the NOC controller. AP borrowed licenses can be non-zero only on site controllers.
AP Licenses Used	Total number of used licenses.
AP Licenses Remaining	Total number of not used licenses.
AP Total Licenses	The cumulative number of both **Device** and **Cluster** AP licenses supported by the listed controller or service platform.

AAP Cluster Details

The **Cluster** pane displays further details about AAP licensing.

Table 192: AAP Cluster Details

AAP Installed Licenses	Number of installed licenses.
AAP Borrowed Licenses	Borrowed licenses are the total number of AAP licenses borrowed by the site controller from the NOC controller (NOC controllers if a NOC controller is in a cluster). AAP borrowed licenses are always zero in the NOC controller. AAP borrowed licenses can be non-zero only on site controllers.
AAP Licenses Used	Total number of used licenses.
AAP Licenses Remaining	Total number of not used licenses.
AAP Total Licenses	Lists the cumulative number of both **Device** and **Cluster** AAP licenses supported by the listed controller or service platform.

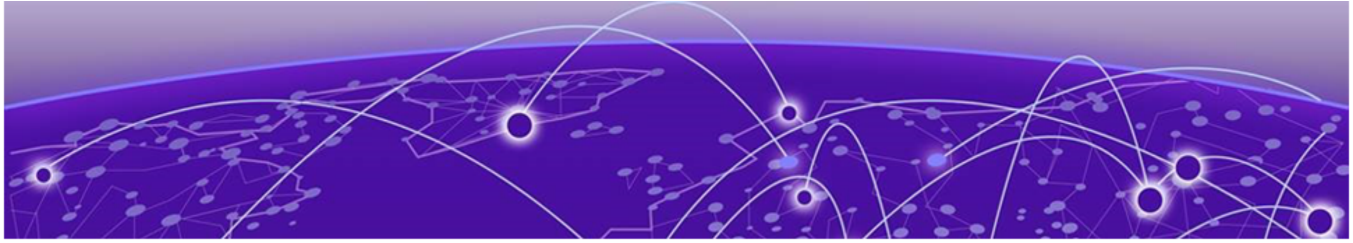
Bulk Migrate APs to ExtremeCloud IQ

ExtremeWireless WiNG release 7.9.5 introduces the ability to carry out bulk migration of ExtremeWireless WiNG Universal APs from local-management to cloud-management by ExtremeCloud IQ. This is achieved by resetting the operational mode of eligible ExtremeWireless WiNG locally-managed Universal APs to factory settings.

From the factory, Universal APs are configured to discover ExtremeCloud IQ by default.

Implement bulk migration from ExtremeWireless WiNG CLI using the new **`device-upgrade operational-mode xiq-cloud`** command and related configurable parameters.

Consult the *WiNG Controller Command Reference Guide* for details.



Index