



Cisco Prime Infrastructure 1.2 User Guide

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Prime Infrastructure 1.2 User Guide

© 2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **xv**

Audience **xv**

Related Documentation **xv**

Obtaining Documentation and Submitting a Service Request **xv**

xv

PART 1

Getting Started

CHAPTER 1

Introduction to Cisco Prime Infrastructure **1-1**

Prime Infrastructure Workflows **1-1**

CHAPTER 2

Setting up Prime Infrastructure **2-1**

Discovering the Network **2-1**

 Planning Discovery Runs **2-1**

 Running Discovery **2-2**

 Verifying Discovery **2-4**

 Adding Devices Manually **2-4**

 Importing Devices in Bulk **2-5**

 Adding NAM HTTP Credentials **2-5**

Setting Up Site Profiles **2-6**

 Creating Site Profiles **2-6**

 Adding Devices to Site Profiles **2-6**

Setting Up Port Monitoring **2-7**

 Port Groups **2-7**

 Monitoring Templates **2-7**

 Setting Up WAN Interface Monitoring **2-7**

Setting Up Virtual Domains **2-8**

 Creating a Site-Oriented Virtual Domain **2-9**

 Assigning Users to a Virtual Domain **2-9**

Setting Up Assurance **2-10**

 Enabling NAM Data Collection **2-10**

 Enabling NetFlow Data Collection **2-10**

Setting Up External Management Servers **2-11**

 Configuring ACS View Servers **2-11**

Configuring TFTP or FTP Servers	2-12
Next Steps	2-12

PART 2

Designing the Network

CHAPTER 3

Planning Your Network Design 3-1

Planning Guidelines	3-1
Template Workflow for Switches	3-2
Planning for Branch Deployments	3-2
Testing Templates	3-3

CHAPTER 4

Designing Device Configurations 4-1

About Configuration Templates	4-2
Deploying a Branches	4-2
Creating Configuration Templates	4-2
Default Configuration Templates	4-3
Creating CLI Configuration Templates	4-3
Creating Feature and Technology Templates	4-8
Creating Wireless Controller Templates	4-9
Creating System Templates	4-10
Creating WLAN Templates	4-17
Creating FlexConnect Templates	4-19
Creating Security Templates	4-21
Creating Wireless Protection Policies Templates	4-26
Creating Radio Templates (802.11)	4-37
Creating Radio Templates (802.11a/n)	4-39
Creating Radio Templates (802.11b/g/n)	4-45
Creating Mesh Templates	4-50
Creating Management Templates	4-51
Creating a CLI Template	4-54
Creating a Location Configuration Template	4-55
Creating IPv6 Templates	4-55
Creating Proxy Mobile IPv6 Templates	4-57
Publishing and Deploying Controller Templates	4-58
Creating Security Configuration Templates	4-59
Creating a DMVPN Templates	4-59
Creating a GET VPN Group Member Templates	4-59
Creating a GET VPN Key Server Templates	4-59

Creating ScanSafe Templates	4-60
Configuring Switch Location Configuration Templates	4-60
Creating AP Configuration Templates	4-61
Creating Lightweight Access Point Templates	4-61
Creating Autonomous Access Point Templates	4-62
Creating Autonomous Access Point Migration Templates	4-63
Configuring Autonomous AP Migration Templates	4-64
Viewing the Migration Analysis Summary	4-64
Copying a Migration Template	4-65
Deleting Migration Templates	4-66
Viewing the Current Status of Cisco IOS Access Points	4-66
Designing Controller Config Groups	4-67
Adding New Config Group	4-67
Configuring Config Groups	4-68
Applying or Scheduling Config Groups	4-69
Auditing Config Groups	4-69
Rebooting Config Groups	4-70
Reporting Config Groups	4-70
Downloading Software	4-71
Configuring wIPS Profiles	4-72
Adding a Profile	4-73
Editing a wIPS Profile	4-74
Deleting a wIPS Profile	4-76
Applying a wIPS Profile	4-76
Configuring Features on a Device	4-77
Application Visibility	4-77
Overview of NAT	4-79
Dynamic Multipoint VPN	4-85
Configuring DMVPN	4-85
GETVPN	4-89
VPN Components	4-93
Overview of Zones	4-100
Routing	4-111
Creating Composite Templates	4-114
Testing and Troubleshooting Configuration Templates	4-115

CHAPTER 5
Designing Monitoring Configurations 5-1

Creating Health Monitoring Templates	5-1
Health Monitoring Template Metrics	5-2

Defining Monitoring Thresholds	5-4
Designing Custom SNMP Monitoring Templates	5-4
Troubleshooting Monitoring Configurations	5-5

CHAPTER 6

Designing Automated Deployment Profiles 6-1

Automated Deployment	6-1
Automated Deployment Process	6-2
Automated Deployment Profile	6-2
Creating Bootstrap Configuration Templates	6-2
Creating Configuration Templates	6-4
Creating Automated Deployment Profiles	6-4
Deploying an Automated Profile	6-5
Delivering and Applying the Bootstrap	6-6
Automated Deployment Status	6-8
Configuring Controller Deployments	6-9

CHAPTER 7

Designing Sites 7-1

Updating Campuses	7-1
Importing Sites From Files	7-2
Removing Campuses or Buildings	7-2
Associating Devices With Sites	7-2
Associating Endpoints With Sites	7-3

PART 3

Deploying the Network

CHAPTER 8

Planning Template Deployments 8-1

Deployment Scenarios	8-1
----------------------	-----

CHAPTER 9

Deploying Templates 9-1

Specifying Template Deployment Options	9-1
Deploying the DMVPN Template	9-1
Deploying GETVPN Templates	9-2
Deploying ScanSafe Template	9-3
Troubleshooting Template Deployment	9-3

PART 4

Operating the Network

CHAPTER 10**Operating and Monitoring the Network 10-1**

- Monitoring Dashboards 10-1
- Configuring Monitoring Settings 10-2
- Device Work Center 10-2
- Monitoring Jobs 10-3
- Monitoring Using Reports 10-4
 - Creating Reports 10-4
- Using Packet Capture for Monitoring and Troubleshooting 10-4
- Diagnosing Site Connectivity Issues and Comparing Configurations 10-5

CHAPTER 11**Monitoring Alarms 11-1**

- What is an Event? 11-1
- What is an Alarm? 11-2
- Where to Find Alarms 11-3
- Defining Thresholds 11-4
- Getting Help for Alarms 11-5
 - Launching Cisco Support Community 11-5
 - Opening a Support Case 11-5
- Changing Alarm Status 11-6
 - When to Acknowledge Alarms 11-6
 - Including Acknowledged and Cleared Alarms in Searches 11-7
- Changing Alarm and Event Options 11-7
- Configuring Alarm Severity Levels 11-7

CHAPTER 12**Updating Device Inventory 12-1**

- Changing Discovery Settings 12-1
- Scheduling Discovery Jobs 12-3
- Monitoring the Discovery Process 12-3
- Discovery Protocols and CSV File Formats 12-4
- Updating Device Inventory Manually 12-5
- Importing Device Inventory 12-5
- Troubleshooting Unmanaged Devices 12-5
- Managing Device Groups 12-7
 - Device Accessibility in Parent-Child Device Groups 12-8
 - Creating Dynamic Device Groups 12-8
 - Assigning Devices to a Group 12-9

Synchronizing Devices 12-9

CHAPTER 13

Changing Port Groups 13-1

Creating Port Groups 13-1

Deleting a Port Group 13-2

CHAPTER 14

Working with Device Configurations 14-1

Configuration Archives 14-1

Changing Prime Infrastructure Device Configuration Settings 14-1

Comparing Current and Previous Device Configurations 14-2

Overview of Device Configurations 14-2

Changing a Single Device Configuration 14-3

Adding a Wireless LAN Controller 14-3

Changing Wireless LAN Controller Configuration Settings 14-3

Rebooting Controllers 14-4

Configuration Rollbacks 14-4

Rolling Back Device Configuration Versions 14-4

Deleting Device Configurations 14-5

Configuring Redundancy on Controllers 14-5

Prerequisites and Limitations for Redundancy 14-6

Configuring Redundancy Interfaces 14-7

Configuring Redundancy on a Primary Controller 14-7

Configuring Redundancy on a Secondary Controller 14-8

Monitoring and Troubleshooting the Redundancy States 14-9

Configuring Peer Service Port IP and Subnet Mask 14-11

Adding a Peer Network Route 14-11

Administration commands for Redundancy 14-12

Disabling Redundancy on Controllers 14-12

CHAPTER 15

Maintaining Device Configuration Inventory 15-1

Overview of Device Configuration Archive 15-1

Changing Configuration Archive Settings 15-1

Scheduling Configuration Archive Collection 15-2

Comparing Configuration Archives 15-2

Rolling Back Configuration Changes 15-2

CHAPTER 16**Maintaining Software Images 16-1**

- Setting Image Management and Distribution Preferences 16-1
- Managing Software Images 16-2
- Importing Software Images 16-2
- Changing Software Image Requirements 16-3
- Deploying Software Images to Devices 16-3
- Distributing Software Images from Cisco.com 16-4
- Viewing Recommended Software Images 16-5
- Analyzing Software Image Upgrades 16-5

CHAPTER 17**Working with Wireless Operational Tools 17-1**

- Configuring Guest User Templates 17-1
- Running Voice Audits 17-2
 - Running Voice Audits on Controllers 17-2
- Running Voice Diagnostic 17-3
 - Starting the Voice Diagnostic Test 17-3
- Configuring the Location Accuracy Tools 17-4
 - Enabling the Location Accuracy Tool 17-4
 - Using Scheduled Accuracy Testing to Verify Accuracy of Current Location 17-5
 - Using On-demand Accuracy Testing to Test Location Accuracy 17-6
- Configuring Audit Summary 17-7
- Configuring Migration Analysis 17-8
 - Upgrading Autonomous Access Points 17-9
 - Viewing a Firmware Upgrade Report 17-10
 - Viewing a Role Change Report 17-10
- Monitoring Radio Resource Management (RRM) 17-10
- Monitoring RFID Tags 17-13
 - Tag Summary 17-14
 - Searching Tags 17-14
 - Viewing RFID Tag Search Results 17-14
 - Viewing Tag List 17-15
- Configuring Chokepoints 17-16
 - Configuring New Chokepoints 17-16
 - Editing Current Chokepoints 17-18
- Monitoring Interferers 17-19
 - Monitoring AP Detected Interferers 17-19
 - Monitoring AP Detected Interferer Details 17-20

Monitoring AP Detected Interferer Details Location History	17-21
Configuring Spectrum Experts	17-22
Adding a Spectrum Expert	17-22
Spectrum Experts Details	17-23
Configuring Wi-Fi TDOA Receivers	17-23
Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting	17-23
Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps	17-24

CHAPTER 18

Tracing Application Data Paths 18-1

Setting Up Path Trace	18-1
Setting Up Path Trace on Networks With NAMs	18-1
Setting Up Path Trace on Networks Without NAMs	18-2
Configuring Routers for Medianet Performance Monitor and Mediatrace	18-3
Configuring Routers for Mediatrace and WSMA	18-4
Troubleshooting with Path Trace	18-4
Using the Path Trace Tables	18-5
Running Path Trace from Selected RTP Flows	18-6
Running Path Trace from Selected TCP Flows	18-7
Launching an Ad Hoc Path Trace From Endpoints	18-9
Troubleshooting Worst RTP Endpoints Using Dashlets	18-10
Comparing Flow Data From Multiple Sources	18-11

CHAPTER 19

Troubleshooting 19-1

Troubleshooting Users	19-1
-----------------------	------

PART 5

Assuring Network Services

CHAPTER 20

Troubleshooting Voice/Video Delivery to a Branch Office 20-1

CHAPTER 21

Troubleshooting Unjoined Access Points 21-1

CHAPTER 22

Ensuring Consistent Application Experiences 22-1

Identifying Optimization Candidates	22-1
Establishing Performance Baselines	22-2
Validating Optimization ROI	22-3
Monitoring Optimized Flows	22-4

CHAPTER 23	Troubleshooting With Multiple NAMs	23-1
CHAPTER 24	Planning Capacity Changes	24-1
CHAPTER 25	Post-Deployment Application Monitoring	25-1
PART 6	Administering the Network	
CHAPTER 26	Managing System Data	26-1
	Scaling the System	26-1
	Checking on Device and Interface Usage	26-2
	Checking on System Disk Usage	26-3
	Controlling Background Data Collection Tasks	26-3
	Controlling Report Storage and Cleanup	26-4
	Controlling Data Retention	26-4
	Handling Backups	26-7
	Running Backups On Demand	26-8
	Running Backups From the Command Line	26-8
	Scheduling Automatic Backups	26-9
	Creating Backup Repositories	26-9
	Setting Up Remote Repositories	26-10
	Restoring From Backups	26-11
	Enabling Data Deduplication	26-12
CHAPTER 27	Maintaining System Health	27-1
	Monitoring System Health	27-1
	Using System Logs	27-2
	Changing Syslog Logging Options	27-2
	Customizing Logging Options to Enhance Troubleshooting	27-3
	Working with MSE Logs	27-3
	Configuring Logging Options	27-3
	Downloading Mobility Services Engine Log Files	27-4
	High Availability	27-5
	Guidelines and Limitations for High Availability	27-5
	Failover Scenario	27-6
	Configuring High Availability	27-6
	Changing Global Prime Infrastructure Settings	27-7
	Configuring the Mail Server	27-9

Customizing Alarm Email Content	27-10
Customizing Alarm Display Settings	27-11
Checking the Status of Prime Infrastructure	27-11
Stopping Prime Infrastructure	27-11
Backing Up the Database	27-12
Scheduling Automatic Backups	27-12
Uninstalling Prime Infrastructure	27-13
Recovering the Prime Infrastructure Passwords	27-13
Downloading Device Support and Product Updates	27-14
Prime Infrastructure Licensing	27-15
Overview of Prime Infrastructure Licensing	27-16
Managing License Coverage	27-17
Verifying License Details	27-17
Adding Licenses	27-18
Deleting Licenses	27-18
Troubleshooting Licenses	27-18
MSE Licensing Overview	27-19
MSE License Structure Matrix	27-20
Sample MSE License File	27-20
Revoking and Reusing an MSE License	27-20
MSE Services Co-Existence	27-21
Managing Mobility Services Engine (MSE) Licenses	27-21

CHAPTER 28

Controlling User Access 28-1

Managing Users	28-1
Adding a User	28-2
Managing Lobby Ambassador Accounts	28-2
Creating a Lobby Ambassador Account	28-3
Logging the Lobby Ambassador Activities	28-4
Managing Guest User Accounts	28-4
Logging in to the Prime Infrastructure User Interface as a Lobby Ambassador	28-5
Adding a New Guest User Account	28-6
Scheduling a Guest User Account	28-6
Printing/Emailing User Details	28-6
Saving Guest Accounts to Device	28-7
Configuring User Preferences	28-7
Changing User Passwords	28-8
Changing User Privileges	28-8

Managing User Groups	28-8
Changing Virtual Domain Access	28-9
Changing Password Policy	28-9
Setting the AAA Mode	28-10
Changing Virtual Domains	28-10
Auditing Access	28-11
Viewing Audit Logs	28-12
Adding TACACS+ Server	28-12
Adding a RADIUS Server	28-13

CHAPTER 29**Reports 29-1**

Configuring and Managing Reports	29-2
Creating, Scheduling, and Running New Reports	29-2
Customizing Report Results	29-3
Managing Scheduled Run Results	29-4
Managing Saved Report Templates	29-4

PART 7**References****CHAPTER 30****Prime Infrastructure User Interface 30-1**

Prime Infrastructure UI Components	30-1
Global Toolbars	30-1
Filters	30-2
Data Entry Features	30-3
Common UI Tasks	30-5
Changing Your Password	30-5
Changing Your Active Domain	30-5
Monitoring Alarms	30-6
Getting Device Details Using the 360° View	30-6
Getting Help	30-6
Dashboards and Dashlets	30-7
Configuring Dashboards	30-7
Adding Dashboards	30-7
Restoring Default Dashboards	30-8
Searching for Devices or SSIDs	30-8
Performing a Quick Search	30-8
Performing an Advanced Search	30-8
Running a Saved Search	30-9

Monitoring Background Tasks 30-9

CHAPTER 31

Field Reference 31-1

- Configuration Templates Field Descriptions 31-1
 - Controller Templates Field Descriptions 31-1
 - Security Templates Field Descriptions 31-50
 - Wireless Configuration Templates Field Descriptions 31-57
- Designing Mobility Services Engine Field Description 31-68
 - Mobility Services Engine Page Field Description 31-69
 - High Availability Field Description 31-70
 - Adding Trap Destinations for a mobility services engine 31-71
 - Adding User to a mobility services engine 31-71
 - Adding User Groups 31-72
 - Provisioning MSAP service advertisement 31-72
- Wireless Operational Tools Field Descriptions 31-73
 - Guest User Controller Templates Field Descriptions 31-73
 - Voice Audit Field Descriptions 31-74
 - Voice Diagnostic Field Descriptions 31-78
 - Switch Location Configuration Templates 31-80

CHAPTER 32

Field Reference for Reports 32-1

- Field Descriptions 32-1
 - Report Launch Pad 32-1
 - Scheduled Run Results 32-5
 - Saved Report Templates 32-5

INDEX



Preface

This guide describes how to administer and use Cisco Prime Infrastructure.

Audience

This guide is for administrators who configure, monitor, and maintain networks, and who troubleshoot network problems.

Related Documentation

See the Documentation Overview for a list of all documentation for Prime Infrastructure at:

http://www.cisco.com/en/US/products/ps11687/tsd_products_support_series_home.html



Note

We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



PART 1

Getting Started

This part contains the following sections:

- [Introduction to Cisco Prime Infrastructure](#)
- [Setting up Prime Infrastructure](#)



CHAPTER 1

Introduction to Cisco Prime Infrastructure

The Cisco Prime Infrastructure is a network management tool that supports lifecycle management of all your entire network infrastructure from one graphical interface. Prime Infrastructure provides network administrators with a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

Prime Infrastructure provides two different graphical user interfaces (from which you can switch back and forth by clicking the downward arrow next to your login name):

- Lifecycle view, which is organized according to home, design, deploy, operate, report and administer menus.
- Classic view, which closely corresponds to the graphical user interface in Cisco Prime Network Control System 1.1 or Cisco Wireless Control System (WCS).

Prime Infrastructure Workflows

The Prime Infrastructure web interface is organized into a lifecycle workflow that includes the following high-level task areas described in [Table 1-1](#). This document follows the same general organization.



Note

You are strongly advised not to enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing **Tools > Internet Options** and unchecking the Enable third-party browser extensions check box on the Advanced tab.

Table 1-1 *Prime Infrastructure Task Areas*

Task Area	Description	Used By
Home	View dashboards, which give you a quick view of devices, performance information, and various incidents. See Dashboards and Dashlets for more information.	Network Engineers
Design	Design feature or device patterns, or <i>templates</i> . You create reusable design patterns, such as configuration templates, in the Design area. You may use predefined templates or create your own. Patterns and templates are used in the deployment phase of the lifecycle.	Network Engineers, Designers, and Architects

Table 1-1 **Prime Infrastructure Task Areas**

Task Area	Description	Used By
Deploy	Deploy previously defined designs, or <i>templates</i> , into your network. You specify how to deploy features, using templates created in the design phase. The deploy phase allows you to push configurations defined in your templates to one or many devices.	NOC Operators and Service Operators
Operate	Monitor your network on a daily basis and perform other day-to-day or ad hoc operations related to network device inventory and configuration management. The Operate tab contains dashboards, the Device Work Center, and the tools you need for day-to-day monitoring, troubleshooting, maintenance, and operations.	Network Engineers, NOC Operators, and Service Operators
Report	Create reports, view saved report templates, and run scheduled reports.	Network Engineers, NOC Operators, and Service Operators
Administration	Specify system configuration settings and data collection settings, and manage access control.	Network Engineers



CHAPTER 2

Setting up Prime Infrastructure

After you install Prime Infrastructure and launch the browser, read the following sections to learn how to get started using Prime Infrastructure:

- [Discovering the Network, page 2-1](#)
- [Setting Up Site Profiles, page 2-6](#)
- [Setting Up Port Monitoring, page 2-7](#)
- [Setting Up Virtual Domains, page 2-8](#)
- [Setting Up Assurance, page 2-10](#)
- [Setting Up External Management Servers, page 2-11](#)
- [Next Steps, page 2-12](#)

Discovering the Network

To view and manage the devices in your network, Prime Infrastructure must first discover the devices and, after obtaining access, collect information about them. Prime Infrastructure uses both SNMP and SSH/Telnet to connect to supported devices and collect inventory data.

The following sections describe how to discover your network:

- [Planning Discovery Runs](#)
- [Verifying Discovery](#)
- [Adding Devices Manually](#)
- [Importing Devices in Bulk](#)
- [Adding NAM HTTP Credentials](#)

Planning Discovery Runs

Prime Infrastructure uses SNMP polling to gather information about your network devices within the range of IP addresses you specify. If you have CDP enabled on your network devices, Prime Infrastructure uses the seed device you specify to discover the devices in your network.

Before you run discovery, you must do the following:

1. **Configure SNMP Credentials on Devices**—Prime Infrastructure uses SNMP polling to gather information about your network devices. You must configure SNMP credentials on all devices you want to manage using Prime Infrastructure.
2. **Set Syslog and Trap Destinations on Devices**—Specify the Prime Infrastructure server (using the Prime Infrastructure server IP address and port) as the syslog and trap destination on all devices you want to manage using Prime Infrastructure.
3. **Configure discovery email notifications**—You will then receive email notification when Prime Infrastructure has completed discovering the devices in your network. See [Configuring Discovery Email Notifications](#).

Configuring Discovery Email Notifications

By configuring mail server settings, you will receive e-mail notification when Prime Infrastructure has completed discovering the devices in your network.

Step 1 Choose **Administration > System Settings > Mail Server Configuration**.

Step 2 Enter the required information, then click **Save**.



Note

The e-mail addresses you provide for the recipient serve as the default value for other functional areas, such as alarms or reports. Any global changes you make to the recipient e-mail addresses are disregarded if you set up e-mail notifications.

Running Discovery

When you run discovery, Prime Infrastructure discovers the devices and, after access is obtained, collects device inventory data.

It is recommended that you run discovery when first getting started with Prime Infrastructure, as shown in the following steps:

Step 1 Choose **Operate > Discovery**, then click **Discovery Settings**.

Step 2 Click **New**.

Step 3 Enter the Protocol Settings as described in [Table 2-1](#).

Step 4 Do one of the following:

- Click **Save** to save your discovery settings and schedule your discovery to run at a specified time.
 - Click **Run Now** to run the discovery now.
-

Table 2-1 *Discovery Protocol Settings*

Field	Description
Protocol Settings	
Ping Sweep Module	Gets a list of IP address ranges from a specified combination of IP address and subnet mask. This module pings each IP address in the range to check the reachability of devices.
CDP Module	<p>The discovery engine reads the cdpCacheAddress and cdpCacheAddressType MIB objects in cdpCacheTable from CISCO-CDP-MIB on every newly encountered device as follows:</p> <ol style="list-style-type: none"> 1. The cdpCacheAddress MIB object is gathered from the current device. This provides a list of neighbor device addresses. 2. If the neighbor device addresses do not already exist in the global device list, they are added to the local cache.
Advanced Protocols	
Routing Table	Queries and analyzes routing tables on seed routers to discover subnets and next-hop routers.
Address Resolution Protocol	<p>The ARP Discovery Module depends on the Routing Table Discovery Module (RTDM), and is executed only when RTDM is processed. This precondition is identified based on the Discovery-module-processed flags, which are part of the DeviceObject.</p> <p>The entries coming out of the ARP Discovery Module need not necessarily pass through RTDM because (per the router Discovery algorithm) active routers are those that RTDM must process and identify.</p> <p>When the ARP table is fetched and the entries are not already discovered by RTDM, then these entries (though they may represent routers) are not active routers and need not be passed on to RTDM. This is ensured by setting the ARP Discovery Module flag to Processed and leaving the RTDM flag set to Unprocessed.</p> <p>When the RTDM comes across an entry with the RTDM flag unset and the ARP flag set, RTDM identifies the entry as a inactive router or other device and it leaves the entry as Unprocessed. The ARP Discovery Module also ignores the entry according to the algorithm, based on the Processed flag set against the ARP Discovery Module.</p> <p>When the ARP Discovery module is checked, the device MAC address needs to be updated in the device information. Applications can retrieve this information in the adapter through the DeviceInfo object. By scanning the device MAC address, the applications can distinguish between Cisco and non-Cisco devices.</p> <p>ARP cache from the device is collected using CidsARPIInfoCollector. The MAC ID of the device is retrieved from this data and set in the DeviceInfo object.</p>
Border Gateway Protocol	The BGP Discovery Module uses bgpPeerTable in the BGP4-MIB to find its BGP peer. The table contains its peers' IP addresses, which are added as clues to the local cache.
OSPF	Open Shortest Path First (OSPF) protocol is an interior gateway routing protocol. OSPF discovery uses the ospfNbrTable and ospfVirtNbrTable MIB to find neighbor IP addresses.
Filters	
System Location Filter	Filters the device based on the Sys Location string set on the device during the discovery process.
Advanced Filters	
IP Filter	Filters the device based on the IP address string set on the device during the discovery process.

Field	Description
System Object ID Filter	Filters the device based on the System Object ID string set on the device during the discovery process.
DNS Filter	Filters the device based on the DNS string set on the device during the discovery process.
Credential Settings	
SNMP V2 Credential	SNMP community string is a required parameter for discovering devices in the network. You can enter multiple rows of credentials mapped to a specific IP address, or the IP address can be a wild card; for example, *.*.*.*, 1.2.3.*.
Telnet Credential	You can specify the Telnet credentials during discovery, setting creation to collect the device data.
SSH Credential	Prime Infrastructure support SSH V1 and V2. You can configure SSH before running discovery.
SNMP V3 Credential	Prime Infrastructure supports SNMP V3 discovery for devices.

Verifying Discovery

When discovery has completed, you can verify that the process was successful by following these steps:

-
- Step 1** Choose **Operate > Discovery**.
 - Step 2** Choose the discovery job for which you want to view details.
 - Step 3** Under Discovery Job Instances, expand the arrow to view details about the devices that were discovered.
- If devices are missing:
- Change your discovery settings, then rerun the discovery. See [Table 2-1](#) for information about discovery settings.
 - Add devices manually. See [Adding Devices Manually](#) for more information.
-

Adding Devices Manually

You can add devices manually, as shown in the following steps. This is helpful if you want to add a single device. If you want to add all of the devices in your network, it is recommended that you run discovery. (See [Running Discovery](#) for more information.)

-
- Step 1** Choose **Operate > Device Work Center**, then click **Add**.
 - Step 2** Enter the parameters.
 - Step 3** Click **Add** to add the device with the settings you specified.
-

Importing Devices in Bulk

If you have another management system into which your devices are imported or if you want to import a spreadsheet that contains all of your devices and their attributes, you can import device information in bulk into Prime Infrastructure.

-
- Step 1** Choose **Operate > Device Work Center**, then click **Bulk**.
- Step 2** Click the link to download a sample file that contains all the fields and descriptions for the information that must be contained in your imported file.
- Step 3** Click **Browse** to navigate to your file, then click **Import**.
- Step 4** To view the status of the import, choose **Tools > Task Manager > Jobs Dashboard**.
- Step 5** Click the arrow to expand the job details and view the details and history for the import job.
-

Adding NAM HTTP Credentials

If you are using Cisco Network Analysis Modules (NAMs) to monitor your network, you will need to add HTTP credentials so that Prime Infrastructure can retrieve data from them. This is especially important for users who have licensed Assurance features, as most Assurance features depend on NAM data to work.

Prime Infrastructure polls NAMs directly, via HTTP (or HTTPS) to collect their data. This type of polling requires Prime Infrastructure to store each NAMs' HTTP credentials. Unlike with SNMP community strings and Telnet/SSH credentials, you cannot enter NAM HTTP credentials during the discovery process. You can only specify NAM HTTP credentials after the modules are discovered or added to inventory.

Follow the steps below to add HTTP credentials for a single NAM. You can repeat this task for all NAMs from which you want Prime Infrastructure to collect data.

-
- Step 1** Choose **Operate > Device Work Center > Device Type > Cisco Interfaces and Modules > Network Analysis Modules**.
- Step 2** Select one of the NAMs and click **Edit**.
- Step 3** In the **Edit Device** window, under **Http Parameters**:
- Protocol—Select the HTTP protocol, HTTP or HTTPS. The TCP Port will change automatically to the default port for the protocol you selected.
 - TCP Port—Enter a different TCP Port if you want to override the default.
 - Username—Enter the name of a user who can access the NAM via HTTP or HTTPS.
 - Password—Enter the password for the user name you entered.
 - Confirm Password—Re-enter the password to confirm.
- Step 4** Choose **Update**.
-

Related Topics

- [Setting Up Assurance](#)

Setting Up Site Profiles

Site profiles help you manage large campuses by associating network elements to physical locations. Site profiles have a hierarchy that includes campuses and buildings, and allows you to segment the physical structure of your network and monitor your network based on location.

There are two areas in which you can set up and change sites:

- **Design > Site Map Design**—Create a new site and change an existing site.
- **Operate > Device Work Center**—If a site has previously been created, you can add devices to a site by clicking **Add to Site** from the Device Work Center.

When you create site profiles, you need to decide how many campuses and buildings to include in your site. [Table 2-2](#) explains how to determine which elements to include in your site profiles.

Table 2-2 *Creating Elements in Site Profiles*

Create a ...	When you have ...
Campus	More than one business location
Building	More than one location within your campus

To control which users have access to the devices in the sites, you need to create virtual domains. See [Setting Up Virtual Domains](#) for more information.

For additional information about sites, see [Designing Sites](#).

Creating Site Profiles

To create a campus location, add a building to the campus:

-
- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Design > Site Map Design . |
| Step 2 | From the command menu, choose New Campus , then click Go . |
| Step 3 | Enter the necessary parameters, then click Next . |
| Step 4 | Change any settings, then click OK . |
| Step 5 | Click the campus you just created; then, from the command menu, choose New Building , and then click Go . |
| Step 6 | Enter the necessary parameters, then click Save . |
-

You can now add devices to the site profile as described in [Adding Devices to Site Profiles](#).

Adding Devices to Site Profiles

After you have created site profiles, you can assign devices to those sites. By associating devices with a campus and building, you can simplify maintenance tasks. When you need to perform maintenance tasks on devices, you can choose the site that contains the devices and apply the changes to all devices in the site.

To control which users have access to the devices in the sites, you need to create virtual domains. See [Setting Up Virtual Domains](#) for more information.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Choose the devices you want to add to a site, then click the >> icon and click **Add to Site**.
- Step 3** Choose the campus and building to which to assign the device, then click **Add**.



Note The Campus and Building fields are populated with the settings you previously entered in **Design > Site Map Design**. See [Creating Site Profiles](#) for more information.

Setting Up Port Monitoring

To monitor your device ports, you can create a port group and then display monitoring information on the Prime Infrastructure dashboard.

Port Groups

Port groups are logical groupings of interfaces that allow you to monitor device ports by the function they serve. For example, you can create a port group for the WAN ports and create another port group for the internal distribution ports on the same router.

After you create port groups, you can more efficiently configure all the devices belonging to a port group.

You need to determine which types of ports you want to monitor as a group. The following port groups are typical of most networks:

- Port Type
- User Defined
- WAN Interfaces

Monitoring Templates

Monitoring templates monitor device features, usage, health, and other factors. After you create and deploy monitoring templates, Prime Infrastructure collects and processes data from specified devices and displays the information in dashboards, dashlets, and reports. See [Setting Up WAN Interface Monitoring](#).

Setting Up WAN Interface Monitoring

You create a WAN interface port group in order to efficiently configure settings on all the WAN interfaces in a specific port group.

The following steps show you how to create a port group for the WAN interfaces for an edge router, create and deploy a WAN interface health monitoring template on those ports, and then view the results.

-
- Step 1** Choose **Design > Port Grouping**.
- Step 2** Choose device IP addresses to add to the WAN interfaces port group, then click **Add to Group**.
- Step 3** From the Select Group drop-down menu, choose **WAN Interfaces**, then click **Save**.
- Step 4** Create a WAN interface health monitoring template:
- Choose **Design > Monitoring**.
 - Choose **Features > Metrics > Interface Health**.
 - Enter the parameters for the interface health template. It is recommended that you check all parameters to be monitored for WAN interfaces.
 - Click **Save as New Template**.
- Step 5** Deploy the template:
- Choose **Deploy > Monitoring Tasks**.
 - Choose the template you created, then click **Activate**. Click **OK** to confirm.
 - Choose the template you created, then click **Deploy**.
 - Choose Port Groups, then click WAN Interfaces.
 - Click **Submit**.
- Step 6** Verify the monitoring results:
- Choose **Operate > Overview > General**.
 - Check the Top N Interfaces by WAN Utilization dashboard for the parameters you specified.
-

Related Topic

- [Changing Port Groups](#)

Setting Up Virtual Domains

Virtual domains allow you to control who has access to specific sites and devices. After you add devices to Prime Infrastructure, you can configure virtual domains. Virtual domains are logical groupings of devices and are used to control who can administer the group. By creating virtual domains, an administrator allows users to view information relevant to them specifically and restricts their access to other areas. Virtual domain filters allow users to configure devices, view alarms, and generate reports for their assigned part of the network *only*.

Virtual domains can be based on physical sites, device types, user communities, or any other designation you choose.

Before you set up virtual domains, you should determine which users should have access to which sites and devices in your network.

Creating a Site-Oriented Virtual Domain

By default, there is only one virtual domain defined (*root*) in Prime Infrastructure.

When you create a site-oriented virtual domain, you allows users to view information in a specific site and restrict their access to other areas.

The following steps explain how to choose a segment of all the devices at a particular location and make them part of the “Site 1 Routers” virtual domain.

Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the left Virtual Domain Hierarchy sidebar menu, click **New**.



Note By default, only one virtual domain (*root*) is defined in Prime Infrastructure. The selected virtual domain becomes the parent virtual domain of the newly created, subvirtual domain.

Step 3 Enter **Site 1 Routers** for the virtual domain name, then click **Submit**.

Step 4 On the Sites tab, move the sites that you want to associate with the virtual domain to the Selected Sites column, then click **Submit**.

Step 5 Click **OK** on the confirmation screens.

Assigning Users to a Virtual Domain

After you create a virtual domain, you can associate the virtual domain with specific users. This allows users to view information relevant to them specifically and restricts their access to other areas. Users assigned to a virtual domain can configure devices, view alarms, and generate reports for their assigned virtual domain *only*.

The following steps walk you through creating a user who is in charge of the Site 1 Routers virtual domain you previously created.

Step 1 Choose **Administration > Users, Roles, & AAA**.

Step 2 Click the username that you want to assign to a virtual domain.

Step 3 Click the Virtual Domains tab, then move the specific virtual domain from the Available list to the Selected list.

Step 4 Click **Submit**.



Note When using external AAA, be sure to add the custom attributes for virtual domains to the appropriate user or group configuration on the external AAA server.

Related Topic

- [Controlling User Access](#)

Setting Up Assurance

If your Prime Infrastructure implementation includes Assurance licenses, you will need to enable data collection via NAMs and NetFlow configurations. This is necessary to populate the additional dashlets, reports and other features supplied with Assurance.

Setting up Assurance-oriented data collection is covered in the following topics:

- [Enabling NAM Data Collection, page 2-10](#)
- [Enabling NetFlow Data Collection, page 2-10](#)

Enabling NAM Data Collection

To ensure that you can data from your Network Analysis Modules (NAMs), you must enable NAM data collection. You can do this for each discovered or added NAM, or for all NAMs at once.

**Note**

NAM data collection will not work unless you have first specified HTTP/HTTPS credentials for each NAM (see [Adding NAM HTTP Credentials](#)).

-
- Step 1** Choose **Administration > Data Sources > NAM Data Collector**.
- Step 2** Select all of the NAMs for which you want to enable data collection.
- Step 3** Click **Enable**.
-

Related Topics

- [Discovering the Network](#)
- [Adding Devices Manually](#)
- [Adding NAM HTTP Credentials](#)

Enabling NetFlow Data Collection

To start collecting NetFlow and Flexible NetFlow data, you need to configure your NetFlow-enabled switches, routers, and other devices to export this data to Prime Infrastructure. Prime Infrastructure provides an “out of the box” configuration template that allows you to set this up quickly. You can apply it to all or just a subset of your NetFlow enabled devices.

The following procedure is basic, and assumes that you want to configure all types of NetFlow-enabled devices in the same way. You may want to repeat this procedure with variations if, for example, you want create a separate configuration for each type of device, vary exporter or monitor names, set up multiple flow exporters or monitors on the same device type, or set up data export for multiple interfaces on a particular type of device.

-
- Step 1** Choose **Design > Configuration Templates > My Templates > OOTB > Collecting Traffic Statistics**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.

- Step 3** In the Validation Criteria section, select the Device Type dropdown, then select all of the Device Types that you want to export their NetFlow data to Prime Infrastructure.
- Step 4** In the Validation Criteria section, enter the OS Version.
- Step 5** In the Template Detail section, complete the fields as follows:
- **Flow Exporter Name**—Enter a name for the NetFlow exporter on the device types you selected. This can be any collection of characters (for example: `EXPORTER-1`).
 - **IP Address**—Enter the IP address of the Prime Infrastructure server.
 - **Flow Exporter Port**—Enter the port on which the NetFlow monitor will receive the exported data. Use the default 9991 port unless you have a special need to override it.
 - **Flow Monitor Name**—Enter an arbitrary name for the NetFlow monitor caching the data from the flow exporter (for example: `FLOW-MONITOR-1`).
 - **Int**—The name of the interface on the device whose NetFlow data you want to monitor (for example: `ethernet 0/0`).
- Step 6** Click **Save as New Template**. After you save the template, deploy it to your NetFlow-enabled devices using the procedures in [Deploying Templates](#).

Setting Up External Management Servers

This section contains the following topics:

- [Configuring ACS View Servers, page 2-11](#)
- [Configuring TFTP or FTP Servers, page 2-12](#)

Configuring ACS View Servers

To facilitate communication between Prime Infrastructure and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials.



Note

Prime Infrastructure only supports ACS View Server 5.1 or later.

To configure the ACS View Server Credentials, follow these steps:

- Step 1** Choose **Design > External Management > ACS View Servers**.
- Step 2** Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)
- Step 3** Enter the password that was established on the ACS View Server. Confirm the password.
- Step 4** Specify the time in seconds after which the authentication request times out and a retransmission is attempted by the controller.
- Step 5** Specify the number of retries to be attempted.
- Step 6** Click **Save**.

Configuring TFTP or FTP Servers

-
- Step 1** Choose **Design > External Management > TFTP/FTP Servers**.
 - Step 2** From the Select a command drop-down list, choose **Add TFTP/FTP Server**.
 - Step 3** From the Server Type drop-down list, choose **TFTP**, **FTP**, or **Both**.
 - Step 4** Enter a TFTP/FTP server name. This is a user-defined name for the server.
 - Step 5** Enter the IP address of the TFTP/FTP server.
 - Step 6** Click **Save**.
-

Next Steps

Now that you have completed the basic setup steps, you might want to do the following tasks:

Table 2-3 *Next Steps after Completing Setup Tasks*

Task	GUI Path	Documentation Reference
Set up additional users	Administration > Users, Roles & AAA , then click Users	Controlling User Access
Add additional virtual domains	Administration > Virtual Domains	Setting Up Virtual Domains
Refine your sites	Design > Site Map Design	Designing Sites
Create additional port groups and change existing port groups	Design > Port Grouping	Changing Port Groups
Start monitoring and responding to alarms	Operate > Alarms & Events	Monitoring Alarms



PART 2

Designing the Network

This part contains the following sections:

- [Planning Your Network Design](#)
- [Designing Device Configurations](#)
- [Designing Monitoring Configurations](#)
- [Designing Automated Deployment Profiles](#)
- [Designing Sites](#)



CHAPTER 3

Planning Your Network Design

Prime Infrastructure templates allow you to create reusable design patterns to simplify device configurations. When you plan your network design and then create templates based on that design, you can increase operational efficiency, reduce configuration errors, and improve compliance to standards and best practices.

It is important to plan for the following configurations when planning your configuration design:

- Feature configurations—Identify the features you want to configure on a given device. You can use a composite template that includes multiple feature templates in order to define a complete device configuration.
- Device role configurations—Identify your devices and the roles they play. For example, you'll want to design different templates for routers that function as branch routers as compared to routers that function as WAN edge routers. You want to plan for access switch configurations which differ from distribution switch configurations. You could have a number of specific devices for which you want to deploy the same configuration to all of them.
- Site configurations—Identify the various sites in your network and the configurations that are required in the different sites. Different sites could require different configurations. For example, a large-sized retail store can contain devices with configurations that differ drastically from the same devices in a small-sized warehouse.
- Monitoring configurations—At the same time that you're planning your configuration design, consider what relevant information you want to monitor. You want to ensure that the features you configured are being monitored.

Planning Guidelines

There are several factors you should consider when using the Prime Infrastructure design tools:

- What is the size of your network?
- How diverse are the devices and services that you support?
- How many network designers do you have?
- What degree of precision do you need in controlling your network?

If you have a small network with only 1-2 designers and not much variation among device configurations, you could start by copying all CLI configurations you know are “good” into a set of configuration and monitoring templates, and then create a composite template that contain these templates.

If you have a large network with many different devices, try to identify the configurations you can standardize. Create feature and technology templates as exceptions to these standards, which allows you to turn features on and off as needed.

Template Workflow for Switches

1. Create the templates for your switches, which can include:
 - Feature-level configuration templates
 - A monitoring template that monitors the important features that you configured in the configuration templates
 - A composite template that includes all the templates you want to deploy on the switches in your network
2. Create the switch deployment profile which requires that you specify:
 - The bootstrap configuration
 - The required image software on the device and the software image file location
 - The configuration template, which can be a single or composite template
3. Specify the devices on which to deploy, and create a deployment profile which includes:
 - Device profile
 - Deployment target
 - Deployment-specific configuration information

Planning for Branch Deployments

Prime Infrastructure can help you pre-provision and plan for devices in branches and sites. When you have a new branch, Prime Infrastructure will deploy the specified configuration templates and software images that you have selected for the given device type and the given branch. This simplifies and accelerates the time it takes to get a branch fully functional.

The process for planning your branch deployment is:

1. Create a bootstrap configuration that contains the minimal required information a device needs in order to be functional. (Design > Configuration Templates > CLI Template.)
2. Create an automated deployment profile for your branch under Design > Automated Deployment Profiles. This is where you specify details about the branch including the device type on which to push the configuration and the bootstrap template and software image.
3. Deploy the automated deployment template. In the deployment screen, you can specify the specific branch and device details.
4. After the bootstrap configuration is applied to the device, the Prime Infrastructure server pushes the configuration template and the software image to the device. Prime Infrastructure can then discover and manage the device.

Testing Templates

After you have created templates, you should deploy the template to a single device in order to test and troubleshoot your design. Before you roll out a template to a large number of devices, you want to make sure the templates you have designed are correct and that you don't need to make further adjustments or modifications to the template. You should plan for and schedule full deployment of a composite template.



CHAPTER 4

Designing Device Configurations

You use templates to define device parameters and settings, which you can later deploy to a specified number of devices based on device type. Templates enhance productivity when you are implementing new services or a new site. Altering configurations across a large number of devices can be tedious and time-consuming, and templates save you time by applying the necessary configurations and by ensuring consistency across devices. You can also create and deploy configuration for the selected device.

Table 4-1 describes the process for creating and deploying templates.

Table 4-1 *Process for Using Configuration Templates*

Task	Additional Information
1. Create a template.	Under the Design menu, choose which type of template to create.
2. Publish the template.	After you have created the template, click Publish to publish the template and make it available to be deployed.
3. Deploy the template.	Under the Deploy menu, choose which template to deploy. See Deploying Templates for more information.
4. Verify the status of the template deployment.	Choose Tools > Task Manager > Jobs Dashboard to verify the status of the template deployment.

This chapter contains the following sections:

- [About Configuration Templates, page 4-2](#)
- [Creating Configuration Templates, page 4-2](#)
- [Creating Wireless Controller Templates, page 4-9](#)
- [Creating Security Configuration Templates, page 4-59](#)
- [Configuring Features on a Device, page 4-77](#)
- [Creating Composite Templates, page 4-114](#)
- [Testing and Troubleshooting Configuration Templates, page 4-115](#)

About Configuration Templates

You use configuration templates to design the set of device configurations you need to set up all the devices in a branch. When you have a site, office, or branch that uses a similar set of devices and configurations, you can use configuration templates to build a generic configuration that you can apply to one more or more devices in the branch. You can also use configuration templates when you have a new branch and want to quickly and accurately set up common configurations on the devices in the branch.

Related Topic

- [Creating Configuration Templates](#)

Deploying a Branches

Deploying a branch is creating the minimum configurations for the branch router. Prime Infrastructure allows you to create a set of required features that include:

- Feature templates for the Ethernet interface
- CLI template for additional features you require

All of the templates you create can then be added to a single *composite template*, which aggregates all the individual feature templates you need for the branch router. You can then use this composite template when you perform branch deployment operations and to replicate the configurations at other branches.

When you have a set of similar devices across a branch, you can deploy a composite template that includes “golden” configurations to simplify deployment and ensure consistency across your device configurations. You can also use the composite template to compare against an existing device configuration to determine if there are mismatches.

Related Topics

- [Creating Configuration Templates](#)
- [Creating Composite Templates](#)

Creating Configuration Templates

Prime Infrastructure provides the following types of configuration templates:

- Default templates—Cisco-supplied templates that are ready for use the moment you install Prime Infrastructure. See [Default Configuration Templates](#).
- CLI templates—User-defined templates that are created based on your own parameters. CLI templates allow you to choose the elements in the configurations. Prime Infrastructure provides variables that you replace with actual values and logic statements. You can also import templates from Cisco Prime LAN Management System. See [Creating CLI Configuration Templates](#).
- Feature and technology templates—Configurations that are specific to a feature or technology in a device’s configuration. See [Creating Feature and Technology Templates](#).
- Composite templates—Two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices. See [Creating Composite Templates](#).

**Note**

All templates must be *published* before they can be deployed to devices.

You use templates to define device parameters and settings, which you can later deploy to a specified number of devices based on device type. Altering configurations across a large number of devices can be tedious and time-consuming, and templates save you time by applying the necessary configurations and ensuring consistency across devices.

Default Configuration Templates

Prime Infrastructure ships with default configuration templates that you can find under **Design > Configuration Templates > My Templates > OOTB**. These templates are described in [Table 4-2](#).

Table 4-2 Prime Infrastructure-Provided Configuration Templates


Use This Configuration Template...	To Do This...
Medianet – PerfMon	Configure performance monitoring for Medianet.
PA with WAAS	Configure Cisco Performance Agent ¹ and Wide Area Application Services (WAAS).
PA without WAAS	Configure Cisco Performance Agent without WAAS.
Collecting Traffic Statistics	Collect network traffic statistics.
Authentication Priority	Configure the level of priority you want to assign to each authentication server.
EtherChannel	Configure an EtherChannel.
Local Management Users	Configure local users, their privilege level, and password.
Logging	Configure logging, trap level, severity level, buffer size, etc.
NTP	Configure an NTP peer/server on a device.
RADIUS-AUTH	Configure a RADIUS authentication server.
RADIUS Acct. Servers	Configure a RADIUS accounting server.
SNMP	Configure SNMP V1/V2.
TACACS Server	Configure a TACACS server.
Trap Receiver	Configure a trap receiver.
STP	Configure Spanning Tree Protocol (STP).
VLAN	Configure a VLAN.

1. Cisco Performance Agent is a licensed feature of Cisco IOS Software. It offers comprehensive application performance and network usage data to help network administrators accurately assess user experience and optimize the use of network resources.

Creating CLI Configuration Templates

Before creating a CLI template, make sure you have satisfied the prerequisites as described in [Database Variables in CLI Templates](#).

-
- Step 1** Choose **Design > Configuration Templates**.
- Step 2** Expand the **CLI Template folder**, then click **CLI**.

- Step 3** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 4** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 5** In the Template Detail section, click **Manage Variables**.
This allows you to specify a variable for which you will define a value when you deploy the template.
- Step 6** Click **Add Row** and enter the parameters for a new variable, then click **Save**.
- Step 7** Enter the CLI information.
-  **Note** In the CLI field, you must enter code using Apache VTL.
- Step 8** (Optional) To change the variables, click **Form View** (a read-only view), then click **Manage Variables** and make your changes.
- Step 9** Click **Save As New Template**.

Related Topics

- [Prerequisites for Creating CLI Templates](#)
- [Database Variables in CLI Templates](#)
- [Creating CLI Configuration Templates from Copied Code](#)
- [Importing CLI Configuration Templates From Cisco Prime LMS](#)

Prerequisites for Creating CLI Templates

Creating CLI templates is an advanced function that should be done by expert users. Before you create a CLI template, you should:

- Have expert knowledge and understanding of the CLI and be able to write the CLI in Apache VTL. For more information about Apache Velocity Template Language, see <http://velocity.apache.org/engine/devel/vtl-reference-guide.html>.
- Understand to what devices the CLI you create can be applied.
- Understand the data types supported by Prime Infrastructure.
- Understand and be able to manually label configurations in the template.

Database Variables in CLI Templates

When a device is discovered and added to Prime Infrastructure, you can use the database values that were gathered during the inventory collection to create CLI templates. For example, if you want to create and deploy a CLI template to shut down all interfaces in a branch, you can create a CLI template that contains the following commands:

```
#foreach ($interfaceName in $interfaceNameList)
interface $interfaceName \n
shutdown
#end
```

where *\$interfaceNameList* is the database variable type whose value will be retrieved from the database. *\$interfaceNameList* has a default value of `Inventory::EthernetProtocolEndpoint.IntfName`.

To populate *interfaceNameList* with the value from the database, you must create a properties file to capture the query string as described below and save it in the /opt/CSColumos/conf/ifm/template/InventoryTagsInTemplate folder.

Sample Property File

Filename: interface.properties

```
# for interface name tag->Name
EthernetProtocolEndpoint.IntfName=select u.name from EthernetProtocolEndpoint u where
u.owningEntityId =
# say for other attributes of EthernetProtocolEndpoint Model, should we define tags
# any good generic way of accepting tags -attr+its mapped query ?
```

After you create the CLI template and the property file and deploy the CLI template, the following CLI is configured on the devices. This output assumes the device has two interfaces (GigabitEthernet0/1 and GigabitEthernet0/0):

```
interface GigabitEthernet0/0
shutdown
interface GigabitEthernet0/1
shutdown
```



Note

InterfaceNameList is a Prime Infrastructure default database variable.

Verify that the Enterprise JavaBeans Query Language (EJB QL) specified in the properties file returns a list of strings; or, if a single element is specified, the EJB QL should return a list containing one element.

The following are the database variables present in the CLITemplateDbVariablesQuery.properties file:

- IntfName
- UpIntfName
- DownIntfName
- AllIntf
- DeviceName
- ProductSeries
- SysObjectID
- IPAddress
- SoftwareVersion
- SerialNumber
- ModelNumber
- ImageName
- ImnageFileName
- ImageVersion
- VlanID
- VlanName
- ProductType

Related Topics

- [Creating CLI Configuration Templates](#)
- [Prerequisites for Creating CLI Templates](#)
- [Creating CLI Configuration Templates from Copied Code](#)
- [Importing CLI Configuration Templates From Cisco Prime LMS](#)

Creating CLI Configuration Templates from Copied Code

One quick way to create CLI configuration templates is to copy code from a command line configuration session, CLI script, or other stored set of configuration commands. Prime Infrastructure lets you turn all the CLI parameters in the copied CLI into template variables.

To create a CLI template variable from copied code:

-
- Step 1** Choose **Design > Configuration Templates**.
- Step 2** Expand the CLI Template directory, and then click **CLI**.
- Step 3** In the CLI template, paste the copied code into the CLI Content field.
- Step 4** Select the text that is to be the variable name.
- Step 5** Click **Manage Variable**.
- The **Manage Variable** dialog box appears with the new variable name added to the list of variables.
- Step 6** Enter the values of the following parameters:
- Name.
 - Type—Data type of the variable. Default is String.
 - Description (Optional) —Description of the variable.
 - Display Label—Display name of the variable in the template.
 - Display Label—If the variable is mandatory in the template, check this check box.
- Step 7** To set the range, validation, and default value of the variable, click the arrow next to the radio button:
- Default Value.
 - Range—If the variable is an integer, enter the range in the **From** and **To** fields.
 - Validation Expression—If the variable is a string, enter a valid regular expression to validate the user input. For example, if the string should start with “hostname,” enter `^[\S]+$` as the validation expression.
- Step 8** Click **Save**.
- Step 9** Click **Add**.
- To view the new variable, click **Form View**.
-

To edit an existing variable created from copied code:

-
- Step 1** Click **Manage Variable**.
- Step 2** Click the radio button to select a variable, and then click **Edit**.

Step 3 Continue from [Step 6](#) of the procedure for creating a variable from copied code.

Related Topics

- [Creating CLI Configuration Templates](#)
- [Prerequisites for Creating CLI Templates](#)
- [Database Variables in CLI Templates](#)
- [Importing CLI Configuration Templates From Cisco Prime LMS](#)

Importing CLI Configuration Templates From Cisco Prime LMS

In addition to creating new configuration templates, you can import configurations from Cisco Prime LAN Management Solution (LMS). If you have “golden” templates in Cisco Prime LMS, you can import those configurations into Prime Infrastructure and save them as configuration templates that you can deploy to the devices in your network.

Before you import a configuration, you must first export and save the configuration from Cisco Prime LMS.

-
- Step 1** Choose **Design > Configuration Templates**.
- Step 2** Expand the **CLI Template folder**, then choose the **CLI** template.
- Step 3** Click the **Import** icon at the top right of the CLI template page.
- Step 4** Browse to the configuration .xml file that you previously exported from Cisco Prime LMS, then click **OK**.
- Step 5** Navigation to the My Templates folder and choose the configuration you imported.
- Step 6** To view the contents of the configuration, click the **CLI Content** tab.
To view the parameters defined in the configuration, click the **Form View** tab. These values are read-only.
To change any of the variables defined in the configuration, click **Manage Variables**.
- Step 7** Click the **Publish** icon to publish the template so it can be deployed.
- Step 8** Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.
- Step 9** Click **Deploy** on the template you published.
- Step 10** Specify the deployment options as explained in [Specifying Template Deployment Options](#).
- Step 11** Click **OK**.
-

Related Topics

- [Creating CLI Configuration Templates](#)
- [Prerequisites for Creating CLI Templates](#)
- [Database Variables in CLI Templates](#)
- [Creating CLI Configuration Templates from Copied Code](#)

Creating Feature and Technology Templates

Feature and technology templates are templates that are based on device configuration. Feature and technology templates focus on specific features or technologies in a device's configuration. When you add a device to Prime Infrastructure, Prime Infrastructure gathers the device configuration for the model you added.



Note

Prime Infrastructure does not support every configurable option for all device types. If Prime Infrastructure does not have a feature and technology template for the specific feature or parameter you want configure, create a CLI template as described in [Creating CLI Configuration Templates](#).

You create feature and technology templates to simplify the deployment of configuration changes. For example, you can create an SNMP feature and technology template and then quickly deploy it to the devices you specify. You can also add one or more feature and technology templates to a composite template. If you do, when you update the SNMP template, the composite template in which the SNMP template is contained automatically has your latest changes.

-
- Step 1** Choose **Design > Configuration Templates**.
 - Step 2** Expand the **Features and Technologies** folder, choose an appropriate subfolder, then choose a template type to create.
 - Step 3** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 4** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.



Note

If you are creating a feature template that applies only to a particular device type, the Device Type field lists only the applicable device type, and you cannot change the selection.

- Step 5** In the Template Detail section, enter the CLI information.
 - Step 6** Click **Save As New Template**.
-

Creating ACL Templates

To create and deploy a template to configure access lists:

-
- Step 1** Choose **Design > Configuration Templates**.
 - Step 2** Expand the Features and Technologies folder, expand the Security subfolder, then click ACL.
 - Step 3** Enter the basic template information.
 - Step 4** In the Template Detail section, click **Add Row**, then complete the fields described in [Table 4-3](#).

Table 4-3 *ACL Template Details*

Field	Description
Name/Number	Name or number of the ACL.
Applied To	Enter the interface of the router on which to apply the ACL. It is recommended that you apply the ACL on the interface closest to the source of the traffic.
Type	Choose: Standard —Standard IP ACLs control traffic based on the source IP address. Extended —Extended IP ACLs identify traffic based on source IP address, source port, destination IP address, and destination port.
Description	Description of the ACL.

- Step 5** Click **Save As New Template**.
- Step 6** Navigate to the My Templates folder and choose the template you just saved.
- Step 7** Click the **Publish** icon to publish the template so it can be deployed.
- Step 8** Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.
- Step 9** Click **Deploy** on the template you published.
- Step 10** Specify the deployment options as explained in [Specifying Template Deployment Options](#).
- Step 11** Click **OK**.

Creating Wireless Controller Templates

Getting the wireless LAN up and running quickly and cost-effectively to meet your needs is streamlined with the broad array of Cisco Prime Infrastructure integrated configuration templates. These easy-to-use templates and deployment tools help you to provision and configure the wireless LAN to expressly deliver the services that their business requires. You use controller templates to define controller parameters and settings, which you can later deploy to a specified number of wireless LAN controllers. The controller templates enhance productivity when you are implementing new services or a new site. Altering configurations across a large number of controllers can be tedious and time-consuming, and templates save you time by applying the necessary configurations and by ensuring consistency across controllers.

See [Table 4-1](#) for information about the process for creating and deploying templates.

This section contains the following topics:

- [Creating System Templates, page 4-10](#)
- [Creating WLAN Templates, page 4-17](#)
- [Creating FlexConnect Templates, page 4-19](#)
- [Creating Security Templates, page 4-21](#)
- [Creating Wireless Protection Policies Templates, page 4-26](#)
- [Creating Radio Templates \(802.11\), page 4-37](#)
- [Creating Radio Templates \(802.11a/n\), page 4-39](#)

- [Creating Radio Templates \(802.11b/g/n\), page 4-45](#)
- [Creating Mesh Templates, page 4-50](#)
- [Creating Management Templates, page 4-51](#)
- [Creating a CLI Template, page 4-54](#)
- [Creating a Location Configuration Template, page 4-55](#)
- [Creating IPv6 Templates, page 4-55](#)
- [Creating Proxy Mobile IPv6 Templates, page 4-57](#)
- [Publishing and Deploying Controller Templates, page 4-58](#)

Creating System Templates

This section contains the following topics:

- [Creating a General Template, page 4-10](#)
- [Creating an SNMP Community Controller Template, page 4-11](#)
- [Creating an NTP Server Template, page 4-11](#)
- [Creating a QoS Templates, page 4-11](#)
- [Creating a User Roles Controller Template, page 4-12](#)
- [Creating an AP Username Password Controller Template, page 4-13](#)
- [Creating a Global CDP Configuration Template, page 4-14](#)
- [Creating an AP 802.1X Supplicant Credentials Template, page 4-13](#)
- [Creating a DHCP Template, page 4-14](#)
- [Creating an Interface Group Template, page 4-15](#)
- [Creating a Traffic Stream Metrics QoS Template, page 4-15](#)
- [Creating a Dynamic Interface Template, page 4-16](#)

Creating a General Template

To create a general template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > General**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.



Note Specifying a device type helps you to prevent a mismatch, that is, you cannot create a configuration and apply the configuration to a wrong device.

- Step 4** In the Template Detail section, complete the fields as described in [Table 31-1](#).

- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating an SNMP Community Controller Template

Create or modify a template for configuring SNMP communities on controllers. Communities can have read-only or read-write privileges using SNMP v1, v2, or v3.

To create a template with SNMP community information for a controller:

- Step 1** Choose **Design > Configuration Templates> Features and Technologies > Controller > System > SNMP Community**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, enter the SNMP Community information.



Note If the Access Mode option is configured as Read Only, then the Prime Infrastructure has only read access to the controller after applying this template.

- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating an NTP Server Template

NTP is used to synchronize computer clocks on the Internet.


To create an NTP template or make modifications to an existing NTP template:

- Step 1** Choose **Design > Configuration Templates> Features and Technologies > Controller > System > SNMP Community**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Enter the NTP server IP address.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Creating System Templates” section on page 4-10](#) for information about publishing and deploying controller templates.
-

Creating a QoS Templates

To create the quality of service (QoS) profiles:

- Step 1** Choose **Design > Configuration Templates> Features and Technologies > Controller > System > Qos Profiles**.

- Step 2** Click in the Name column for the profile you want to edit. The Edit QoS Profile Template page appears.
- Step 3** Set the following values in the Per-User Bandwidth Contracts group box. All have a default of 0 or Off.
- Average Data Rate—The average data rate for non-UDP traffic.
 - Burst Data Rate—The peak data rate for non-UDP traffic.
 - Average Real-time Rate—The average data rate for UDP traffic.
 - Burst Real-time Rate—The peak data rate for UDP traffic.
- Step 4** Set the following values in the Over-the-Air QoS group box.
- Maximum QoS RF Usage per AP - The maximum air bandwidth available to clients. The default is 100%.
 - QoS Queue Depth - The depth of queue for a class of client. The packets with a greater value are dropped at the access point.
-  **Note** The Air QoS configurations are applicable for controller Version 7.0 and earlier.
- Step 5** Set the following values in the Wired QoS Protocol group box.
- Wired QoS Protocol - Choose **802.1P** to activate 802.1P priority tags or **None** to deactivate 802.1P priority flags.
 - 802.1P Tag - Choose **802.1P priority tag** for a wired connection from 0 to 7. This tag is used for traffic and CAPWAP packets.
- Step 6** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a User Roles Controller Template

This section describes how to create or modify a template for configuring user roles. User roles determine how much bandwidth the network can use. Four QoS levels (Platinum, Bronze, Gold, and Silver) are available for the bandwidth distribution to Guest Users. Guest Users are associated with predefined roles (Contractor, Customer, Partner, Vendor, Visitor, Other) with respective bandwidth configured by the Admin. These roles can be applied when adding a new Guest User.

To create a template with User Roles information for a controller:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > User Roles**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Configure the following fields:
- Role Name
 - Average Data Rate—The average data rate for non-UDP (User Datagram Protocol) traffic.
 - Burst Data Rate—The peak data rate for non-UDP traffic.
 - Average Real-time Rate—The average data rate for UDP traffic.
 - Burst Real-time Rate—The peak data rate for UDP traffic.

- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating an AP Username Password Controller Template

Create or modify a template for setting an access point username and password. All access points inherit the password as they join the controller and these credentials are used to log into the access point via the console or Telnet/SSH.

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis.

Also, in controller software Release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To create a template with AP Username Password information for a controller:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > AP Username Password**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, enter the AP username and password information.



Note For Cisco IOS access points, you must also enter and confirm an enable password.

- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating an AP 802.1X Supplicant Credentials Template

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. All access points that are currently joined to the controller and any that join in the future are included.

To create or modify an existing AP 802.1X Supplicant Credentials template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > AP 802.1X Supplicant Credentials**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Select the **Enable** check box to enable global supplicant credentials.

- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating a Global CDP Configuration Template

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

CDP is enabled on the Ethernet and radio ports of the bridge by default.

To create a Global CDP Configuration template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > Global CDP Configuration**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-2](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.



Note

The Global Interface CDP configuration is applied only to the APs for which the CDP is enabled at AP level.

Creating a DHCP Template

To create a DHCP template or make modifications to an existing DHCP template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > DHCP**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** You can enable or disable DHCP proxy on a global basis rather than on a WLAN basis.



Note

When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the WLAN or on the WLAN itself. DHCP proxy is enabled by default.

- Step 5** Enter the DHCP Timeout in seconds, after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds.



Note

DHCP Timeout is applicable for Controller Version 7.0.114.74 and later.

- Step 6** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating an Interface Group Template

The interface group template page allows you to select list of interfaces and form a group.

To create an interface group template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > Interface Groups**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Specify the following details:
- Name—Interface Group name.
 - Description (optional)—A more detailed description of the interface group.
 - Quarantine—Indicates the type of interfaces that can be added to an interface group. If this option is enabled, you can add interfaces with quarantine VLAN ID set. If this options is disabled, you can add interfaces with quarantine VLAN ID not set.
- Step 5** Selected Controllers/Interfaces that you want to add to the group.
- Step 6** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a Traffic Stream Metrics QoS Template

Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and informs you of the QoS of the wireless LAN. These statistics are different than the end-to-end statistics provided by VoIP systems. End-to-end statistics provide information on packet loss and latency covering all the links comprising the call path. However, traffic stream metrics are statistics for only the WLAN segment of the call. Because of this, system administrators can quickly determine whether audio problems are being caused by the WLAN or by other network elements participating in a call. By observing which access points have impaired QoS, system administrators can quickly determine the physical area where the problem is occurring. This is important when lack of radio coverage or excessive interference is the root problem.

Four QoS values (packet latency, packet jitter, packet loss, and roaming time), which can affect the audio quality of voice calls, are monitored. All the wireless LAN components participate in this process. Access points and clients measure the metrics, access points collect the measurements and then send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds, and 10 minutes of data is stored at one time. The Prime Infrastructure queries the controller for the metrics and displays them in the Traffic Stream Metrics QoS Status. These metrics are compared to threshold values to determine their status level and if any of the statistics are displaying a status level of fair (yellow) or degraded (red), the administrator investigates the QoS of the wireless LAN.

For the access points to collect measurement values, traffic stream metrics must be enabled on the controller.

To create a Traffic Stream Metrics QoS template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > Traffic Stream Metrics QoS**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

The Traffic Stream Metrics QoS Controller Configuration page shows several QoS values. An administrator can monitor voice and video quality of the following:

- Upstream delay
- Upstream packet loss rate
- Roaming time
- Downstream packet loss rate
- Downstream delay

Packet Loss Rate (PLR) affects the intelligibility of voice. Packet delay can affect both the intelligibility and conversational quality of the connection. Excessive roaming time produces undesired gaps in audio.

There are three levels of measurement:

- Normal: Normal QoS (green)
- Fair: Fair QoS (yellow)
- Degraded: Degraded QoS (red)

System administrators should employ some judgement when setting the green, yellow, and red alarm levels. Some factors to consider are:

- Environmental factors including interference and radio coverage which can affect PLR.
 - End-user expectations and system administrator requirements for audio quality on mobile devices (lower audio quality can permit greater PLR).
 - Different codec types used by the phones have different tolerance for packet loss.
 - Not all calls are mobile-to-mobile; therefore, some have less stringent PLR requirements for the wireless LAN.
-

Creating a Dynamic Interface Template

To create a dynamic interface template or make modifications to an existing interface configuration:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > System > Dynamic Interface**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-3](#).

- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating WLAN Templates

This section contains the following topics:

- [Creating a WLAN Template, page 4-17](#)
- [Creating a WLAN AP Groups Template, page 4-18](#)

Creating a WLAN Template

WLAN templates allow you to define various WLAN profiles for application to different controllers. You can configure multiple WLANs with the same SSID. This feature enables you to assign different Layer 2 security policies within the same wireless LAN.

These restrictions apply when configuring multiple WLANs with the same SSID:

- WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes. These are the available Layer 2 security policies:
 - None (open WLAN)
 - Static WEP or 802.1
 - CKIP
 - WPA/WPA2
- Broadcast SSID must be enabled on the WLANs that share an SSID so that the access points can generate probe responses for these WLANs.
- FlexConnect access points do not support multiple SSIDs.

To create a WLAN template or make modifications to an existing WLAN template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > WLANs > WLAN Configuration**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Template Detail section:
- Select the General tab and complete the fields as described in [Table 31-5](#).
 - Select the Security tab and complete the fields as described in [Table 31-6](#).
 - Select the QoS tab and complete the field as described in [Table 31-7](#).
 - Select the Advanced tab and complete the fields as described in [Table 31-8](#).
 - Select the Hot Spot tab and complete the field as described in [Table 31-9](#).
- Step 4** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating Mobile Concierge (802.11u) Groups

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

To create Mobile Concierge (802.11u) Groups:

-
- | | |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Design > Configuration Templates > Features and Technologies > Controller > WLANs > WLAN Configuration . |
| Step 2 | Click the Hot Spot tab. See Table 31-9 . |
| Step 3 | Click Save As New Template . |
-

Creating a WLAN AP Groups Template

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits include more effective management of load balancing and bandwidth allocation.

To create WLAN AP Groups:

-
- | | |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Design > Configuration Templates > Features and Technologies > Controller > WLANs > AP Group VLANs . |
| Step 2 | In the Template Basic section, enter a name and a description in the appropriate fields. |
| Step 3 | In the Validation Criteria section, choose a Device Type from the list and enter the OS Version. |

This page displays a summary of the AP groups configured on your network. In this page, you can add, remove, edit, or view details of an AP group. Click in the Edit column to edit its access point(s). Select the check box in the WLAN Profile Name column, and click **Remove** to delete WLAN profiles.




Note The maximum characters that you can enter in the Description text box is 256.

Adding Access Point Groups


You can create or modify a template for dividing the WLAN profiles into AP groups.

To create a new access point group:


- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > WLANs > AP Group VLANs**.
- Step 2** If you want to add a WLAN profile, click the **WLAN Profiles** tab and configure the following fields:
- Click **Add**.




Note To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.



Note Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.



Note The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).
 - Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.
 - Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.



Note To display all available interfaces, delete the current interface from the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.
 - Select the **NAC Override** check box, if applicable. The NAC override feature is disabled by default.
 - When access points and WLAN profiles are added, click **Save**.
- Step 3** If you want to add a RF profile, click the **RF Profiles** tab, and configure the following fields:
- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
 - 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
 - When RF profiles are added, click **Save**.

Creating FlexConnect Templates

This section contains the following topics:

- [Creating a FlexConnect AP Groups Template, page 4-20](#)
- [Creating FlexConnect Users, page 4-20](#)

Creating a FlexConnect AP Groups Template

FlexConnect enables you to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of FlexConnect access points per location, but you can organize and group the access points per floor and limit them to 25 or so per building, because it is likely the branch offices share the same configuration.

To set up an FlexConnect AP group:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > FlexConnect > FlexConnect AP Groups**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section, complete the fields as described in [Table 31-10](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating FlexConnect Users



Note You can create FlexConnect users only after you save the FlexConnect AP Group.



Note Maximum 100 FlexConnect users are supported in controller version 5.2.x.x and later. If controller Version 5.2.0.0, and earlier supports only 20 FlexConnect users.

To create a FlexConnect user:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > FlexConnect > FlexConnect AP Groups**.
 - Step 2** Click the **FlexConnect Configuration** tab to enable local authentication for a FlexConnect group.
 - Step 3** Select the **FlexConnect Local Authentication** check box to enable local authentication for this FlexConnect group.
 - Step 4** Click the **Users configured in the group** link. The FlexConnect Users page appears.
 - Step 5** If you want to add a new user, choose **Add User** from the Select a command drop-down list, and click **Go**. The **Add User** page appears.
 - Step 6** In the User Name text box, enter the FlexConnect username.
 - Step 7** In the Password text box, enter the password.
 - Step 8** Reenter the password in the Confirm Password text box.
 - Step 9** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-


Creating Security Templates

This section contains the following topics:

- [Creating a General Security Controller Template, page 4-21](#)
- [Creating a Security Password Policy Template, page 4-30](#)
- [Creating a RADIUS Authentication Template, page 4-22](#)
- [Creating a RADIUS Accounting Template, page 4-22](#)
- [Creating a RADIUS Fallback Template, page 4-23](#)
- [Creating an LDAP Server Template, page 4-23](#)
- [Creating a TACACS+ Server Template, page 4-23](#)
- [Creating a Local EAP General Template, page 4-24](#)
- [Creating a Local EAP Profile Template, page 4-24](#)
- [Creating an EAP-FAST Template, page 4-25](#)
- [Creating a Network User Priority Template, page 4-25](#)
- [Creating a User Login Policies Template, page 4-31](#)
- [Creating a User Login Policies Template, page 4-31](#)
- [Creating an Access Control List Template, page 4-32](#)
- [Creating a Manually Disabled Client Template, page 4-31](#)
- [Creating an Access Control List Template, page 4-32](#)

Creating a General Security Controller Template

To create a new template with general security information for a controller:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > AAA > General**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Add or modify the following fields:
- Template Name
- 
- Note**
- Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.
- Maximum Local Database Entries (on next reboot)—Enter the maximum number of allowed database entries. This amount becomes effective on the next reboot.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a RADIUS Authentication Template

This page allows you to add a RADIUS authentication template or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

To create a RADIUS Authentication template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > AAA > RADIUS Auth Servers**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section, complete the fields as described in [Table 31-11](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a RADIUS Accounting Template

This page allows you to add a RADIUS accounting template or make modifications to an existing RADIUS accounting template.

To create a RADIUS Accounting template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > RADIUS Auth Servers**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** Use the Shared Secret Format drop-down list to choose either **ASCII** or **hexadecimal**.



Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

- Step 5** Enter the RADIUS shared secret used by your specified server.
 - Step 6** Retype the shared secret.
 - Step 7** Click if you want to establish administrative privileges for the server.
 - Step 8** Click if you want to enable the network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
 - Step 9** Specify the time in seconds after which the RADIUS authentication request times out and a retransmission by the controller occurs. You can specify a value between 2 and 30 seconds.
 - Step 10** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a RADIUS Fallback Template

This page allows you to add a RADIUS fallback template or make modifications to an existing RADIUS fallback template.

To configuring a RADIUS Fallback template:

-
- | | |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Design > Configuration Templates> Features and Technologies > Controller > Security > RADIUS Auth Servers . |
| Step 2 | In the Template Basic section, enter a name and a description in the appropriate fields. |
| Step 3 | In the Validation Criteria section, choose a Device Type from the list and enter the OS Version. |
| Step 4 | From the RADIUS Fallback Mode drop-down list, choose Off , Passive , or Active . <ul style="list-style-type: none">• Off—Disables fallback.• Passive—You must enter a time interval.• Active—You must enter a username and time interval. |
| Step 5 | Click Save as New Template . After you save the template, see the “Publishing and Deploying Controller Templates” section on page 4-58 for information about publishing and deploying controller templates. |
-

Creating an LDAP Server Template

This section explains how to configure a Lightweight Directory Access Protocol (LDAP) server as a backend database, similar to a RADIUS or local user database. An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP might use an LDAP server as its backend database to retrieve user credentials.

To create an LDAP server template or make modifications to an existing LDAP server template:

-
- | | |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Design > Configuration Templates> Features and Technologies > Controller > Security > AAA > LDAP Servers . |
| Step 2 | In the Template Basic section, enter a name and a description in the appropriate fields. |
| Step 3 | In the Validation Criteria section, choose a Device Type from the list and enter the OS Version. |
| Step 4 | In the Template Detail section, complete the fields as described in Table 31-12 . |
| Step 5 | Click Save as New Template . After you save the template, see the “Publishing and Deploying Controller Templates” section on page 4-58 for information about publishing and deploying controller templates. |
-

Creating a TACACS+ Server Template

This page allows you to add a TACACS+ server or make modifications to an existing TACACS+ server template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

To create a TACACS+ Server template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > AAA > TACACS+ Servers**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section, complete the fields as described in [Table 31-13](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating a Local EAP General Template

This page allows you to specify a timeout value for local EAP. You can then add or make changes to an existing local EAP general template.



Note

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Local EAP > General - Local EAP**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section, complete the fields as described in [Table 31-14](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating a Local EAP Profile Template

This page allows you to add a local EAP profile template or make modifications to an existing template. Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.



Note

The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Local EAP > Local EAP Profiles**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-15](#).
- Step 5** Click **Save As New Template**.
- Step 6** To enable local EAP:
- Choose **WLAN > WLAN Configuration** from the left sidebar menu.
 - Click the profile name of the desired WLAN.
 - Choose the **Security > AAA Servers** tab to access the AAA Servers page.
 - Select the **Local EAP Authentication** check box to enable local EAP for this WLAN.
- Step 7** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating an EAP-FAST Template

This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point. This page allows you to add an EAP-FAST template or make modifications to an existing EAP-FAST template.

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Local EAP > EAP-FAST Parameters**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-16](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating a Network User Priority Template

You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add or make modifications to an existing network user credential retrieval priority template.

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Local EAP > Network Users Priority**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

- Step 4** Use the left and right pointing arrows to include or exclude network user credentials in the right page.
 - Step 5** Use the up and down buttons to determine the order credentials are tried.
 - Step 6** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating Wireless Protection Policies Templates

This section contains the following topics:

- [Creating a Rogue Policies Template, page 4-26](#)
- [Creating a Rogue AP Rules Template, page 4-26](#)
- [Creating a Rogue AP Rule Groups Template, page 4-28](#)
- [Creating a Friendly Access Point Template, page 4-28](#)

Creating a Rogue Policies Template

This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

To create or modify an existing template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Wireless Protection Policies > Rogue Policies**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section, complete the fields as described in [Table 31-17](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a Rogue AP Rules Template

Rogue access point rules allow you to define rules to automatically classify rogue access points. Prime Infrastructure applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).



Note Rogue access point rules also help reduce false alarms.

**Note**

Rogue classes include the following types:

Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.

Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.

Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

To create a new classification rule template for rogue access points:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Wireless Protection Policies > Rogue AP Rules**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the General group box, configure the following fields:
 - Rule Name—Enter a name for the rule in the text box.
 - Rule Type—Choose **Malicious** or **Friendly** from the drop-down list. A rogue is considered malicious if a detected access point matches the user-defined malicious rules or has been manually moved from the Friendly AP category. A rogue is considered friendly if it is a known, acknowledged, or trusted access point or a detected access point that matches the user-defined Friendly rules.
 - Match Type—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.
- Step 5** In the Malicious Rogue Classification Rule group box of the page, configure the following fields.
 - Open Authentication—Select the check box to enable open authentication.
 - Match Managed AP SSID—Select the check box to enable the matching of a Managed AP SSID.

**Note**

Managed SSIDs are the SSIDs configured for the WLAN and known to the system.

- Match User Configured SSID—Select the check box to enable the matching of User Configured SSIDs.

**Note**

User Configured SSIDs are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

- Minimum RSSI—Select the check box to enable the Minimum RSSI threshold limit.

**Note**

Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

- Time Duration—Select the check box to enable the Time Duration limit.

**Note**

Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

- **Minimum Number Rogue Clients**—Select the check box to enable the Minimum Number Rogue Clients limit. Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

Step 6 Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating a Rogue AP Rule Groups Template

A rogue access point rule group template allows you to combine more than one rogue access point rule to controllers.

To view current rogue access point rule group templates or create a new rule group:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Wireless Protection Policies > Rogue AP Rule Groups**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Enter a name for the rule group in the General group box of the page.
- Step 5** To add a Rogue AP rule, click to highlight the rule in the left column. Click **Add** to move the rule to the right column.



Note Rogue access point rules can be added from the Rogue Access Point Rules section. See the “[Creating a Rogue AP Rules Template](#)” section on page 4-26 for more information.

- Step 6** To remove a rogue access point rule, click to highlight the rule in the right column. Click **Remove** to move the rule to the left column.
- Step 7** Use the **Move Up/Move Down** buttons to specify the order in which the rules apply. Highlight the desired rule and click **Move Up** or **Move Down** to move it higher or lower in the current list.
- Step 8** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating a Friendly Access Point Template

This template allows you to import friendly internal access points. Importing these friendly access points prevents non-lightweight access points from being falsely identified as rogues.




Note *Friendly Internal* access points were previously referred to as *Known APs*.



Note The Friendly AP page identifies the MAC address of an access point, status, any comments, and whether or not the alarm is suppressed for this access point.

To view or edit the current list of friendly access points:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Wireless Protection Policies > Friendly AP**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Friendly access points can be added by either importing the access point or manually entering the access point information:
- To import an access point using the Import feature do the following:
 - Select the **Import from File** check box.
 - Enter the file path or click **Browse** to navigate to the correct file.
- 

Note Use a line break to separate MAC addresses. For example, enter the MAC addresses as follows:

```
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46
```
-
- To manually add an access point, do the following:
 - Unselect the **Import from File** check box.
 - Enter the MAC address for the access point.
 - Choose **Internal** access point from the Status drop-down list.
 - Enter a comment regarding this access point, if necessary.
 - Select the **Suppress Alarms** check box to suppress all alarms for this access point.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating an Ignored Rogue AP Template

The Ignored Rogue AP Template page allows you to create or modify a template for importing ignored access points. Access points in the Ignored AP list are not identified as rogues.



Note

An Ignored Rogue AP template does not get applied to any controller. It suppresses the Rogue AP/Adhoc alarm if Ignored Rogue AP Template has the Rogue MAC Address when the controller reports the Rogue AP to Prime Infrastructure and this MAC address is added to the Rogue AP Ignore-List on the controller.

To create or edit the Ignored Rogue access points:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Wireless Protection Policies > Ignored Rogue AP**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

Step 4 The Ignored Rogue access points can be added by either importing the access point or manually entering the access point information:

- To import an ignored rogue access point using the Import feature:
 - Select the **Import from File** check box.
 - Enter the file path or use the **Browse** button to navigate to the correct file. The import file must be a CSV file with MAC address (one MAC Address per line).

**Note**

For example, enter the MAC addresses as follows:

00:00:11:22:33:44

00:00:11:22:33:45

00:00:11:22:33:46

- To manually add an ignored rogue access point:
 - Unselect the **Import from File** check box.

Step 5 Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a File Encryption Template

This page enables you to add a file encryption template or make modifications to an existing file encryption template.

To create a File Encryption template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > File Encryption**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Check if you want to enable file encryption.
- Step 5** Enter an encryption key text string of exactly 16 ASCII characters.
- Step 6** Retype the encryption key.
- Step 7** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a Security Password Policy Template

This page enables you to determine your security password policy.

To create or make modifications to an existing password policy template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Password Policy**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.

Step 3 In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

Step 4 Enter the template name.

Step 5 You can enable or disable the following settings:

- Password must contain characters from at least 3 different classes such as uppercase letters, lowercase letters, digits, and special characters.
- No character can be repeated more than 3 times consecutively.
- Password cannot be the default words like cisco, admin.



Note

Password cannot be “cisco”, “ocsic”, “admin”, “nimda” or any variant obtained by changing the capitalization of letters, or by substituting ‘1’ “l” or “!” for i, or substituting “0” for “o”, or substituting “\$” for “s”.

- Password cannot contain username or reverse of username.

Step 6 Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a User Login Policies Template

This page allows you to add a user login template or make modifications to an existing user login policies template. On this template you set the maximum number of concurrent logins that each single user can have.

Step 1 Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > User Login Policies**.

Step 2 In the Template Basic section, enter a name and a description in the appropriate fields.

Step 3 In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

Step 4 You can adjust the maximum number of concurrent logins each single user can have.

Step 5 Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a Manually Disabled Client Template

This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

Step 1 Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Manually Disabled Clients**.

Step 2 In the Template Basic section, enter a name and a description in the appropriate fields.

Step 3 In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

Step 4 Enter the MAC address of the client you want to disable.

Step 5 Enter a description of the client you are setting to disabled.

- Step 6** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.



Note You cannot use a MAC address in the broadcast range.

Creating an Access Control List Template

You can create or modify an ACL template for configuring the type of traffic that is allowed, by protocol, direction, and the source or destination of the traffic.

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs can be applied to data traffic to and from wireless clients or to all traffic destined for the controller Central Processing Unit (CPU) and can now support reusable grouped IP addresses and reusable protocols. After ACLs are configured in the template, they can be applied to the management interface, the AP-manager interface, or any of the dynamic interfaces for client data traffic; to the Network Processing Unit (NPU) interface for traffic to the controller CPU; or to a WAN.

This release of Prime Infrastructure provides support to IPv6 ACLs.

To create or modify an existing ACL template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Access Control Lists**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In this page, specify the following fields:

- Access Control List Name—User-defined name of the template.
- ACL Type—Choose either **IPv4** or **IPv6**.



Note IPv6 ACL is supported from controller Version 7.2.x.

- Step 5** To create reusable grouped IP addresses and protocols, choose **Access Control > IP Groups** from the left sidebar menu.
- Step 6** All the IP address groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose **Add IP Group** from the Select a command drop-down list, and click **Go**. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens.



Note For the IP address of any, an *any* group is predefined.

- Step 7** In the ACL IP Groups details page you can edit the current IP group fields.
- IP Group Name
 - IP Address

- **Netmask OR CIDR Notation**—Enter the Netmask or CIDR Notation and then click **Add**. The list of IP addresses or Netmasks appears in the List of IP Address/Netmasks text box.

CIDR notation allows you to add a large number of clients that exist in a subnet range by configuring a single client object.

Netmask allows you to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property.

- **Netmask**—A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
- **CIDR**—Classless InterDomain Routing. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks.
- **BroadCast/Network**
- **List of IP Addresses/Netmasks**—Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or Netmask.

Step 8 To define an additional protocol that is not a standard predefined one, choose **Access Control > Protocol Groups** from the left sidebar menu. The protocol groups with their source and destination port and DSCP are displayed.

Step 9 To create a new protocol group, choose **Add Protocol Group** from the Select a command drop-down list, and click **Go**. To view or modify an existing protocol group, click the URL of the group. The Protocol Groups page appears.

Step 10 The rule name is provided for the existing rules, or you can now enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the parameters of a rule, the action for this rule is exercised.

Step 11 Choose a protocol from the drop-down list:

- **Any**—All protocols
- **TCP**—Transmission Control Protocol
- **UDP**—User Datagram Protocol
- **ICMP**—Internet Control Message Protocol
- **ESP**—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP**—Internet Protocol
- **Eth Over IP**—Ethernet over Internet Protocol
- **Other Port OSPF**—Open Shortest Path First
- **Other**—Any other IANA protocol (<http://www.iana.org/>)

Step 12 Some protocol choices (such as TCP or UDP) cause additional Source Port and Dest Port GUI elements to appear.

- **Source Port**—Specify the source of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

- **Dest Port**—Specify the destination of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

Step 13 From the DSCP (Differentiated Services Code Point) drop-down list, choose **any** or **specific**. If you choose specific, enter the DSCP (range of 0 to 255).



Note DSCP is a packet header code that can be used to define the quality of service across the Internet.

Step 14 Click **Save**.

Step 15 You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear on the top of the page, and all ACL rules appear on the bottom.

Step 16 To define a new mapping, choose **Add Rule Mappings** from the Select a command drop-down list. The Add Rule Mapping page appears.

Step 17 Configure the following fields:

- **Source IP Group**—Predefined groups for IPv4 and IPv6.
- **Destination IP Group**—Predefined groups for IPv4 and IPv6.
- **Protocol Group**—Protocol group to use for the ACL.
- **Direction**—Any, Inbound (from client) or Outbound (to client).
- **Action**—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 18 Click **Add**. The new mappings populate the bottom table.

Step 19 Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Step 20 You can now automatically generate rules from the rule mappings you created. Choose the mappings for which you want to generate rules, and click **Generate**. This automatically creates the rules. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

Existing ACL templates are duplicated into a new ACL template. This duplication clones all the ACL rules and mappings defined in the source ACL template.

Creating a CPU Access Control List (ACL) Template



Note

CPU ACL configuration with IPv6 is not supported in this release because all IP addresses of controllers on interfaces use IPv4 except the virtual interface.

The existing ACLs established in the [“Creating a FlexConnect Access Control List Template” section on page 4-35](#) is used to set traffic controls between the Central Processing Unit (CPU) and Network Processing Unit (NPU).

To create or modify an existing CPU ACL template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > CPU Access Control List**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** If you select the check box to enable CPU ACL, two more fields appear. When CPU ACL is enabled and applied on the controller, Prime Infrastructure displays the details of the CPU ACL against that controller.
- Step 5** From the ACL Name drop-down list, choose a name from the list of defined names.
- Step 6** From the CPU ACL Mode drop-down list, choose which data traffic direction this CPU ACL list controls. The choices are the wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.
- Step 7** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a FlexConnect Access Control List Template

To create and apply an Access Control List template to a Controller:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > FlexConnect ACLs**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Enter a name for the new FlexConnect ACL in the **FlexConnect ACL Name** text box.
- Step 5** Click **Save**.
- A FlexConnect ACL template is created. You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All FlexConnect ACL mappings appear on the top of the page, and all FlexConnect ACL rules appear in the bottom.
- Step 6** From the Select a command drop-down list, choose **Add Rule Mappings**, and click **Go**.
- Step 7** The FlexConnect ACL IP Protocol Map page appears.
- Step 8** Configure the following fields:
- Source IP Group—Predefined groups for IPv4 and IPv6.
 - Destination IP Group—Predefined groups for IPv4 and IPv6.
 - Protocol Group—Protocol group to use for the ACL.
 - Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.
- Step 9** Click **Add**. The new mappings populate the bottom table.
- Step 10** Click **Save**.
- Step 11** You can now automatically generate rules from the rule mappings you created. Choose the mappings for which you want to generate rules, and click **Generate**. This automatically creates the rules. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

Existing FlexConnect ACL templates are duplicated into a new FlexConnect ACL template. This duplication clones all the FlexConnect ACL rules and mappings defined in the source FlexConnect ACL template.

- Step 12** From the Select a command drop-down list in the FlexConnect ACL page, choose **Apply Templates**.
The Apply to Controllers page appears.
- Step 13** Select **Save Config to Flash after apply** check box to save the configuration to Flash after applying the FlexConnect ACL to the controller.
- Step 14** Select **Reboot Controller after apply** to reboot the controller once the FlexConnect ACL is applied. This check box is available only when you select the Save Config to Flash after apply check box.
- Step 15** Select one or more controllers and click **OK** to apply the FlexConnect ACL template.
The FlexConnect ACL that you created appears in Configure > Controller Template Launch Pad > <IP Address> > Security > Access Control > FlexConnect ACLs.

Creating an ACL IP Groups Template

To create reusable grouped IP addresses:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > IP Groups**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** To define a new IP address group, choose **Add IP Group or Add IPv6 Group** from the Select a command drop-down list, and click **Go**.
- Step 5** Add or modify the fields described in [Table 31-18Controller > Security > IP Groups, page 31-29](#)
- Step 6** For IPv4 networks only: Under Broadcast Network, use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete an IP address or Netmask.
- Step 7** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on [page 4-58](#) for information about publishing and deploying controller templates.

Creating an ACL Protocol Groups Template

To define an additional protocol that is not a standard predefined one:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > Protocol Groups**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Add or modify the fields described in [Table 31-19Controller > Security > Protocol Groups, page 31-29](#)

- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating an External Web Auth Server Template

To create or modify an External Web Auth Server template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > External Web Auth Server**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
-

Creating Radio Templates (802.11)

This section contains the following topics:

- [Creating a Load Balancing Template, page 4-37](#)
- [Creating a Band Selection Template, page 4-38](#)
- [Creating a Media Parameters Controller Template \(802.11a/n\), page 4-40](#)

Creating a Load Balancing Template

To create load balancing templates:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > Load Balancing**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:
- $$\text{load-balancing page} + \text{client associations on AP with lightest load} = \text{load-balancing threshold}$$
- In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.
- Step 5** Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.
- Step 6** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a Band Selection Template

To create band selection templates:


-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > Band Select**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** Add or modify the fields described in [Table 31-20](#) **Controller > Security > 802.11 > Band Select**, page 31-30
 - Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a Preferred Call Template

This page enables you to create or modify a template for configuring Preferred Call.

To create or modify preferred call templates:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > Preferred Call**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** Add or modify the following Preferred Call parameters:
 - Template Name



Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.
 - Number Id—Enter a value to identify the preferred number. You can have a maximum of six preferred call numbers. The valid range is from 1 to 6. The default value is 1.
 - Preferred Number—Enter the preferred call number.
 - Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a Media Stream for Controller Template (802.11)

To create the media stream for a controller template for an 802.11 Radio:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > Media Stream**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.

- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Complete the fields provided in the Template Details section. See [Table 31-21](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating an RF Profiles Template

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups. To create an RF Profile for a controller template for an 802.11 Radio:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > RF Profiles**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Complete the fields provided in the Template Details section. See [Table 31-22](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating Radio Templates (802.11a/n)

This section contains the following topics:

- [Creating an 802.11a/n Parameters Template, page 4-39](#)
- [Creating a Media Parameters Controller Template \(802.11a/n\), page 4-40](#)
- [Creating an EDCA Parameters Template \(802.11a/n\), page 4-41](#)
- [Creating a Roaming Parameters Template \(802.11a/n\), page 4-41](#)
- [Creating an 802.11h Template, page 4-42](#)
- [Creating a High Throughput Template \(802.11a/n\), page 4-42](#)
- [Creating a CleanAir Controller Template \(802.11a/n\), page 4-40](#)

Creating an 802.11a/n Parameters Template

To create or modify an 802.11a/n radio template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Parameters**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Complete the fields provided in the Template Details section. See [Table 31-23](#).

- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating a CleanAir Controller Template (802.11a/n)

Create or modify a template for configuring CleanAir parameters for the 802.11a/n radio. You can configure the template to enable or disable CleanAir, reporting and alarms for the controllers. You can also configure the type of interfering devices to include for reporting and alarms.

To create a new template with 802.11a/n CleanAir information for a controller:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > CleanAir**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Select the CleanAir check box to enable CleanAir functionality on the 802.11 b/g/n network (or unselect to prevent the controller from detecting spectrum interference). If CleanAir is enabled, the Reporting Configuration and Alarm Configuration group boxes appear.
- Step 5** Complete the fields provided in the Template Detail section. See [Table 31-24](#).
- Step 6** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating a Media Parameters Controller Template (802.11a/n)

This page enables you to create or modify a template for configuring 802.11a/n voice fields such as call admission control and traffic stream metrics.

To create a new template with 802.11a/n voice fields information (such as Call Admission Control and traffic stream metrics) for a controller:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Media Parameters**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section:
- Select the Voice tab and complete the fields as described in [Table 31-25](#).
 - Select the Video tab and complete the fields as described in [Table 31-26](#).
 - Select the General tab and complete the field as described in [Table 31-27](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating an EDCA Parameters Template (802.11a/n)

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

To create 802.11a/n EDCA parameters through a controller template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > EDCA Parameters**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, choose one of the following options from the **EDCA Profile** drop-down list:
- **WMM**—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
 - **Spectralink Voice Priority**—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
 - **Voice Optimized**—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network.
 - **Voice & Video Optimized**—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.



Note Video services must be deployed with admission control (ACM). Video services without ACM are not supported.



Note You must shut down the radio interface before configuring EDCA Parameters.

- Step 5** Select the **Low Latency MAC** check box to enable this feature.



Note Enable low latency MAC only if all clients on the network are WMM compliant.

Creating a Roaming Parameters Template (802.11a/n)

To create or modify an existing roaming parameter template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Roaming Parameters**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-28](#).

**Note**

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with highest expected client speed and Roaming Hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating an 802.11h Template

802.11h informs client devices about channel changes and can limit the transmit power of the client device. Create or modify a template for configuration 802.11h parameters (such as power constraint and channel controller announcement) and applying these settings to multiple controllers.

To create or modify an 802.11h template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > 802.11h**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as follows:
- Select the **Power Constraint** check box if you want the access point to stop transmission on the current channel.
 - Select the **Channel Announcement** check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a High Throughput Template (802.11a/n)

To create or modify an 802.11a/n high throughput template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > High Throughput (802.11n)**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as follows:
- Select the **802.11n Network Status Enabled** check box to enable high throughput.

- In the MCS (Data Rate) Settings column, choose which level of data rate you want supported. Modulation coding schemes (MCS) are similar to 802.11a data rate. The defaults are, 20 MHz and short guarded interval. When you select the Supported check box next to a numbered Data Rate, the chosen numbers appear in the Selected MCS Indexes field at the bottom of the column.
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating 802.11a/n RRM Templates

This section contains the following topics:

- [Creating an RRM Threshold Template \(802.11a/n\)](#), page 4-43
- [Creating an RRM Interval Template \(802.11a/n\)](#), page 4-43
- [Creating an RRM Dynamic Channel Allocation Template \(802.11a/n\)](#), page 4-44
- [Creating an RRM Transmit Power Control Template \(802.11a/n\)](#), page 4-44

Creating an RRM Threshold Template (802.11a/n)

To create or make modifications to an 802.11a/n or 802.11b/g/n RRM threshold template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > dot11a-RRM > Thresholds**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-29](#).



Note You must disable the 802.11a/n network before applying these RRM threshold fields.

- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating an RRM Interval Template (802.11a/n)

To create or make modifications to an 802.11a/n RRM interval template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > dot11a-RRM > Intervals**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as follows:
- Neighbor Packet Frequency—Enter the interval at which you want strength measurements taken for each access point. The default is 300 seconds.

- **Channel Scan Duration**—Enter the interval at which you want noise and interference measurements taken for each access point. The default is 300 seconds.
- **Load Measurement Interval**—Enter the interval at which you want load measurements taken for each access point. The default is 300 seconds.
- **Coverage Measurement Interval** — Enter the interval at which you want coverage measurements taken for each access point. The default is 300 seconds.

Step 5 Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating an RRM Dynamic Channel Allocation Template (802.11a/n)

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.



Note Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To create 802.11 a/n RRM DCA template:


- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > dot11a-RRM > DCA**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-30](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating an RRM Transmit Power Control Template (802.11a/n)

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of the access points according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To create 802.11 a/n RRM TPC template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > dot11a-RRM > TPC**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as follows:
- Template Name—Enter the template name in the text box.
 - TPC Version—Choose TPCv1 or TPCv2.
- 

Note The TPCv2 option is applicable only for those controllers running Version 7.2.x or later.
-
- Dynamic Assignment—From the Dynamic Assignment drop-down list, choose one of three modes:
 - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
 - **On Demand**—Transmit power is updated when you click **Assign Now**.
 - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
 - Maximum Power Assignment—Indicates the maximum power assigned.
 - Range: -10 to 30 dB
 - Default: 30 dB
 - Minimum Power Assignment—Indicates the minimum power assigned.
 - Range: -10 to 30 dB
 - Default: 30 dB
 - Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
 - Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
 - Control Interval—In seconds (read-only).
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating Radio Templates (802.11b/g/n)

This section contains the following topics:

- [Creating an 802.11b/g/n Parameters Template, page 4-46](#)
- [Creating a Media Parameters Controller Template \(802.11b/g/n\), page 4-46](#)
- [Creating an EDCA Parameters Controller Template \(802.11b/g/n\), page 4-46](#)
- [Creating an Roaming Parameters Controller Template \(802.11b/g/n\), page 4-47](#)
- [Creating a High Throughput \(802.11n\) Controller Template \(802.11b/g/n\), page 4-47](#)
- [Creating a CleanAir Controller Template \(802.11 b/g/n\), page 4-48](#)
- [Creating 802.11b/g/n RRM Templates, page 4-48](#)

Creating an 802.11b/g/n Parameters Template

Create or modify a template for configuring 802.11b/g/n parameters (such as power and channel status, data rates, channel list, and CCX location measurement) and/or applying these settings to controller(s).

To create a new template with 802.11b/g/n parameters information for a controller:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Parameters**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section, complete the fields as described in [Table 31-31](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating a Media Parameters Controller Template (802.11b/g/n)

Create or modify a template for configuring 802.11b/g/n voice parameters such as Call Admission Control and traffic stream metrics.

To create a new template with 802.11b/g/n voice parameters information (such as Call Admission Control and traffic stream metrics) for a controller:


-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Media Parameters**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section:
 - Select the Voice tab and complete the fields as described in [Table 31-32](#).
 - Select the Video tab and complete the fields as described in [Table 31-33](#).
 - Select the General tab and complete the field as described in [Table 31-34](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Creating an EDCA Parameters Controller Template (802.11b/g/n)

Create or modify a template for configuring 802.11b/g/n EDCA parameters. EDCA parameters designate pre-configured profiles at the MAC layer for voice and video.

To create a new template with 802.11b/g/n EDCA parameters information for a controller:


-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > EDCA Parameters**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.

- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as follows:
- EDCA Profile—Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.
-  **Note** You must shut down radio interface before configuring EDCA Parameters.
- Streaming MAC—Only enable streaming MAC if all clients on the network are WMM compliant.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating an Roaming Parameters Controller Template (802.11b/g/n)

Create or modify a template for configuring roaming parameters for 802.11b/g/n radios.

To create a new template with 802.11b/g/n Roaming parameters information for a controller:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Roaming Parameters**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-35](#).
-  **Note** The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a High Throughput (802.11n) Controller Template (802.11b/g/n)

Create or modify a template for configuring high-throughput parameters such as MCS (data rate) settings and indexes and for applying these 802.11n settings to multiple controllers.

To create a new template with High Throughput (802.11n) information for a controller:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > High Throughput(802.11n)**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as follows:

- 802.11n Network Status—Select the check box to enable high throughput.
- MCS (Data Rate) Settings—Choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. The values 20 MHz and short guarded interval are used as defaults. When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 5 Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a CleanAir Controller Template (802.11 b/g/n)

Create or modify a template for configuring CleanAir parameters for the 802.11 b/g/n radio. You can configure the template to enable or disable CleanAir, reporting and alarms for the controllers. You can also configure the type of interfering devices to include for reporting and alarms.

To create a new template with 802.11b/g/n CleanAir information for a controller:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > CleanAir**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-36](#).
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating 802.11b/g/n RRM Templates

This section contains the following topics:

- [Creating an RRM Thresholds Controller Template \(802.11b/g/n\), page 4-48](#)
- [Creating an RRM Intervals Controller Template \(802.11b/g/n\), page 4-49](#)
- [Creating an RRM Dynamic Channel Allocation Template \(802.11b/g/n\), page 4-50](#)
- [Creating an RRM Transmit Power Control Template \(802.11b/g/n\), page 4-49](#)

Creating an RRM Thresholds Controller Template (802.11b/g/n)

Create or modify a template for setting various RRM thresholds such as load, interference, noise, and coverage.

To create a new template with 802.11b/g/n RRM thresholds information for a controller:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > Thresholds**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

- Step 4** In the Template Detail section, complete the fields as described in [Table 31-37](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating an RRM Intervals Controller Template (802.11b/g/n)

Create or modify a template for configuring RRM intervals for 802.11b/g/n radios.

To create a new template with 802.11b/g/n RRM intervals information for a controller:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > Intervals**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as follows:
- Neighbor Packet Frequency—Enter the interval at which you want strength measurements taken for each access point. The default is 300 seconds.
 - Noise Measurement Interval—Enter the interval at which you want noise and interference measurements taken for each access point. The default is 180 seconds.
 - Load Measurement Interval—Enter the interval at which you want load measurements taken for each access point. The default is 300 seconds.
 - Channel Scan Duration—Enter the interval at which you want coverage measurements taken for each access point. The default is 300 seconds.
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating an RRM Transmit Power Control Template (802.11b/g/n)

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of an access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To create 802.11b/g/n RRM TPC template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > TPC**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.

- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-38](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating an RRM Dynamic Channel Allocation Template (802.11b/g/n)

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.



Note Choosing a larger bandwidth reduces the non-overlapping channels, which could potentially reduce the overall network throughput for certain deployments.

To create 802.11b/g/n RRM DCA template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > DCA**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-39](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating Mesh Templates

Creating a Mesh Setting Template

You can configure an access point to establish a connection with the controller.

To create or modify a mesh template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Mesh > Mesh Settings**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** The Root AP to Mesh AP Range is 12,000 feet by default. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.

- Step 5** The **Client Access on Backhaul Link** check box is not selected by default. When this option is enabled, mesh access points can associate with 802.11a/n wireless clients over the 802.11a/n backhaul. This client association is in addition to the existing communication on the 802.11a/n backhaul between the root and mesh access points.



Note This feature applies only to access points with two radios.

- Step 6** The **Mesh DCA Channels** check box is not selected by default. Select this option to enable backhaul channel deselection on the Controller using the DCA channel list configured in the Controller. Any change to the channels in the Controller DCA list is pushed to the associated access points. This feature applies only to the 1524SB mesh access points. For more information on this feature, see the *Controller Configuration Guide*.
- Step 7** Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled. Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents.
- Step 8** From the Security Mode drop-down list, choose **EAP** (Extensible Authentication Protocol) or **PSK** (Pre-Shared Key).
- Step 9** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating Management Templates

This section contains the following topics:

- [Creating a Trap Receiver Template, page 4-51](#)
- [Creating a Trap Control Template, page 4-52](#)
- [Creating a Telnet SSH Template, page 4-52](#)
- [Creating a Legacy Syslog Template, page 4-52](#)
- [Creating a Multiple Syslog Template, page 4-53](#)
- [Creating a Local Management User Template, page 4-53](#)
- [Creating a User Authentication Priority Template, page 4-54](#)

Creating a Trap Receiver Template

If you have monitoring devices on your network that receive SNMP traps, you might want to add a trap receiver template.

To create or modify a trap receiver template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Management > Trap Receiver**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Enter the IP address of the server in the text box.

- Step 5** Select the **Admin Status** check box to enable the administrator status if you want SNMP traps to be sent to the receiver.
- Step 6** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a Trap Control Template

To create or modify a trap control template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Management > Trap Control**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-40](#).
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a Telnet SSH Template

To create or modify a Telnet SSH configuration template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Management > Telnet SSH**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as described in [Table 31-41](#).
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a Legacy Syslog Template

To create or modify a legacy syslog configuration template:



Note

Legacy Syslog applies to controllers Version 5.0.6.0 and earlier.

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Management > Legacy Syslog**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

- Step 4** Select the **Syslog** check box to enable syslogs. When you do, a Syslog Host IP Address text box appears.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a Multiple Syslog Template

To create or modify a multiple syslog configuration template:



Note

You can enter up to three syslog server templates.

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Management > Multiple Syslog**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Enter a template name and a syslog server IP address in the text boxes.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

Creating a Local Management User Template

To create or modify a local management user template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Management > Local Management User**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** Enter a template username.
- Step 5** Enter a password for this local management user template.
- Step 6** Reenter the password.
- Step 7** Use the Access Level drop-down list to choose either **Read Only** or **Read Write**.
- Step 8** Select the **Update Telnet Credentials** check box to update the user credentials in Prime Infrastructure for Telnet/SSH access.



Note

If the template is applied successfully and the Update Telnet Credentials option is enabled, the applied management user credentials are used in Prime Infrastructure for Telnet/SSH credentials to that applied controller.

- Step 9** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a User Authentication Priority Template

Management user authentication priority templates control the order in which authentication servers are used to authenticate the management users of a controller.

To create a user authentication priority template or make modifications to an existing template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Management > Authentication Priority**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** The local server is tried first. Choose either **RADIUS** or **TACACS+** from the drop-down list to try if local authentication fails.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a CLI Template

You can create templates containing a set of CLI commands and apply them to one or more controllers from Prime Infrastructure. These templates are meant for provisioning features in multiple controllers for which there is no SNMP support or custom Prime Infrastructure user interface. The template contents are simply a command array of strings. No support for substitution variables, conditionals, and the like exist.

The CLI sessions to the device are established based on user preferences. The default protocol is SSH.

To create or modify a CLI template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > CLI > General**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** If you are adding a new template, provide a name that you are giving to this string of commands in the text box. If you are making modifications to an existing template, the Template Name text box cannot be modified.
- Step 5** In the Commands page, enter the series of CLI commands.
- Step 6** Select the **Refresh Config after Apply** check box to perform a refresh config on the controller after the CLI template is applied successfully.
- Step 7** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.

**Note**

If the Controller Telnet credentials check fails or the Controller CLI template fails with invalid username and password even though the correct username and password are configured on the controller, check whether the controller has exceeded the number of CLI connections it can accept. If the connections have exceeded the maximum limit, then either increase the maximum allowed CLI sessions or terminate any pre-existing CLI sessions on the controller, and then retry the operation.

Creating a Location Configuration Template

To create or modify a location setting template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > Location > Location Configuration**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section:
 - Select the General tab and complete the fields as described in [Table 31-42](#).
 - Select the Advanced tab and complete the fields as described in [Table 31-43](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on [page 4-58](#) for information about publishing and deploying controller templates.
-

Creating IPv6 Templates

This section contains the following topics:

- [Creating a Neighbor Binding Timers Template, page 4-55](#)
- [Creating a RA Throttle Policy Template, page 4-56](#)
- [Creating an RA Guard Template, page 4-56](#)

Creating a Neighbor Binding Timers Template

You can create or modify a template for configuring IPv6 Router Neighbor Binding Timers such as Down Lifetime, Reachable Lifetime, State Lifetime, and corresponding intervals.

To create a Neighbor Binding Timers template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > IPv6 > Neighbor Binding Timers**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.

- Step 4** If you want to enable the down lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Down Lifetime Interval text box. This indicates the maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. The range is 0 to 86,400 seconds, and the default value is 0.
- Step 5** If you want to enable the reachable lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Reachable Lifetime Interval text box. This indicates the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is 0 to 86,400 seconds, and the default value is 0.
- Step 6** If you want to enable the stale lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Stale Lifetime Interval text box. This indicates the maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. The range is 0 to 86,400 seconds, and the default value is 0.
- Step 7** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating a RA Throttle Policy Template

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network. You can create or modify a template for configuring IPv6 Router Advertisement parameters such as RA Throttle Policy, Throttle Period, and other options.

To create a RA Throttle Policy template:

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > IPv6 > RA Throttle Policy**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** If you want to enable the down lifetime, select the **Enable** check box. If you have selected this check box, configure the following parameters:
- Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
 - Max Through—The number of RA that passes through over a period in seconds.
 - Interval Option—Indicates the behavior in case of RA with an interval option.
 - Allow At-least—Indicates the minimum number of RA not throttled per router.
 - Allow At-most—Indicates the maximum number of RA not throttled per router.
- Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating an RA Guard Template

RA Guard is a Unified Wireless solution used to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can create or modify a template for configuring IPv6 Router Advertisement parameters.

To create an RA Guard template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > IPv6 > RA Guard**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** If you want to enable the Router Advertisement Guard, select the **Enable** check box.
 - Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating Proxy Mobile IPv6 Templates

Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node and initiate the mobility signaling and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

Creating a PMIP Global Configurations Template

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > PMIP > Global Config**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section, complete the fields as described in [Table 31-44](#).
 - Step 5** Click **Save as New Template**. After you save the template, see the [“Publishing and Deploying Controller Templates” section on page 4-58](#) for information about publishing and deploying controller templates.
-

Creating an LMA Configurations Template

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > PMIP > LMA**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
 - Step 4** In the Template Detail section, complete the following fields:
 - LMA Name—Name of the LMA connected to the controller.
-

- LMA IP Address—IP address of the LMA connected to the controller.

Step 5 Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.

Creating a PMIP Profiles Template

- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Controller > PMIP > PMIP Profile**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, create a PMIP profile as follows:
- In PMIP Profile, enter the profile name.
 - Click **Add** and then complete the following fields:
 - Network Access Identifier—Name of the Network Access Identifier (NAI) associated with the profile.
 - LMA Name—Name of the LMA with which the profile is to be associated.
 - Access Point Node—Name of the access point node connected to the controller.
- Step 5** Repeat Step 4 for each additional PMIP Profile needed.
- Step 6** Click **Save as New Template**. After you save the template, see the “[Publishing and Deploying Controller Templates](#)” section on page 4-58 for information about publishing and deploying controller templates.
-

Publishing and Deploying Controller Templates

After configuring a controller template, follow these steps:

- Step 1** Navigate to the My Templates folder and choose the template you just saved.
- Step 2** Click the **Publish** icon to publish the template so it can be deployed.
- Step 3** Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.
- Step 4** Click **Deploy** on the template you published.
- Step 5** Specify the deployment options as explained in the “[Specifying Template Deployment Options](#)” section on page 9-1.
- Step 6** Click **OK**.



Note

When you deploy the WLAN Configuration templates, the controllers configured with Interface/Interface Group, selected RADIUS servers, LDAP servers, ACL name with rules, and Ingress interface appear in the Template Deployment - Prepare and Schedule page.

Creating Security Configuration Templates

The following sections explain how to create and deploy security configuration templates:

- [Creating a DMVPN Templates](#)
- [Creating a GET VPN Group Member Templates](#)
- [Creating a GET VPN Key Server Templates](#)
- [Creating ScanSafe Templates](#)

Creating a DMVPN Templates

To create a Dynamic Multipoint VPN template:

-
- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Design > Configuration Templates> Features and Technologies > Security > DMVPN . |
| Step 2 | In the Template Basic section, enter a name and a description in the appropriate fields. |
| Step 3 | In the Validation Criteria section, choose a Device Type from the list and enter the OS Version. |
| Step 4 | In the Template Detail section, complete the fields as described in Table 31-45 . |
| Step 5 | Click Save as New Template . After you save the template, see the “Deploying the DMVPN Template” section on page 9-1 for information about publishing and deploying DMVPN templates. |
-

Creating a GET VPN Group Member Templates

To create a GETVPN group member template:

-
- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Design > Configuration Templates> Features and Technologies > Security > GETVPN-GroupMember . |
| Step 2 | In the Template Basic section, enter a name and a description in the appropriate fields. |
| Step 3 | In the Validation Criteria section, choose a Device Type from the list and enter the OS Version. |
| Step 4 | In the Template Detail section, complete the fields as described in Table 31-46 . |
| Step 5 | Click Save as New Template . After you save the template, see the “Deploying GETVPN Templates” section on page 9-2 for information about publishing and deploying GETVPN Group Member templates. |
-

Creating a GET VPN Key Server Templates

To create a GETVPN Key Server template:

-
- | | |
|---------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Design > Configuration Templates> Features and Technologies > Security > GETVPN-KeyServer . |
| Step 2 | In the Template Basic section, enter a name and a description in the appropriate fields. |

- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as explained in [Table 31-47](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Deploying GETVPN Templates](#)” section on page 9-2 for information about publishing and deploying GETVPN Server templates.
-

Creating ScanSafe Templates

ScanSafe Web Security is a cloud-based SaaS (Security as a Service) that allows you to scan the content of the HTTP and HTTPS traffic. When ScanSafe Web Security is integrated with a router, selected HTTP and HTTPS traffic is redirected to the ScanSafe cloud for content scanning and malware detection.

When Cisco ISR Web Security with Cisco ScanSafe is enabled and the ISR is configured to redirect web traffic to ScanSafe, the ISR transparently redirects HTTP and HTTPS traffic to the ScanSafe proxy servers based on the IP address and port. You can configure the ISR to relay web traffic directly to the originally requested web server without being scanned by ScanSafe.

Whitelisting Traffic

You can configure the ISR so that some approved web traffic is not redirected to ScanSafe for scanning. When you bypass ScanSafe scanning, the ISR retrieves the content directly from the originally requested web server without contacting ScanSafe. When it receives the response from the web server, it sends the data to the client. This is called “whitelisting” traffic.

See

http://www.cisco.com/en/US/docs/security/web_security/ISR_SS/ISR_ScanSafe_SolutionGuide.pdf for more information on ScanSafe.

To create the ScanSafe template specify the following:

- ScanSafe server and interface information
- User information
- Whitelist information

To create a ScanSafe template:

-
- Step 1** Choose **Design > Configuration Templates > Features and Technologies > Security > ScanSafe**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, choose a Device Type from the list and enter the OS Version.
- Step 4** In the Template Detail section, complete the fields as explained in [Table 31-48](#).
- Step 5** Click **Save as New Template**. After you save the template, see the “[Deploying ScanSafe Template](#)” section on page 9-3 for information about publishing and deploying ScanSafe templates.
-

Configuring Switch Location Configuration Templates

You can configure the location template for a switch using the Switch Location Configuration template.

To configure a location template for a switch:

-
- Step 1** Choose **Design > Wireless Configuration > Switch Location Configuration**.
- Step 2** From the Select a command drop-down list, choose **Add Template**.
- Step 3** Click **Go**. The New Template page appears.
- Step 4** Complete the fields as described in [Table 31-75](#):
-

Creating AP Configuration Templates

Select the template name to view or edit parameters for current access point templates.

This section contains the following topics:

- [Creating Lightweight Access Point Templates, page 4-61](#)
- [Creating Autonomous Access Point Templates, page 4-62](#)

Creating Lightweight Access Point Templates

To create a Lightweight Access Point template:

-
- Step 1** Choose **Design > Wireless Configuration > Lightweight AP Configuration Templates**.
- Step 2** From the Select a command drop-down list, choose **Add Template**.
- Step 3** Click **Go**.
- Step 4** Enter a template name in the text box.
- Step 5** Enter a template description in the text box.
- Step 6** Click **Save**. If you are updating an already existing template, click the applicable template in the Template Name column. The Lightweight AP Template Detail page appears.
- Step 7** Select each of the following tabs and complete the fields as described in [Lightweight AP Configuration Templates, page 31-58](#):
- [Lightweight AP Configuration Templates> AP Parameters](#)
 - [Lightweight AP Configuration Templates> Mesh](#)
 - [Lightweight AP Configuration Templates> 802.11a/n](#)
 - [Lightweight AP Configuration Templates > 802.11a SubBand](#)
 - [Lightweight AP Configuration Templates > 802.11b/g/n](#)
 - [Lightweight AP Configuration Templates > CDP](#)
 - [Lightweight AP Configuration Templates > FlexConnect](#)
 - [Lightweight AP Configuration Templates > Select APs](#)
 - [Lightweight AP Configuration Templates > Report](#)
-

Creating Autonomous Access Point Templates

The Autonomous AP Configuration Templates page allows you to configure CLI templates for autonomous access points.

This section contains the following topics:

- [Creating an Autonomous Access Point Template, page 4-62](#)
- [Applying an AP Configuration Template to an Autonomous Access Point, page 4-62](#)
- [Configuring Autonomous AP Migration Templates, page 4-64](#)

Creating an Autonomous Access Point Template

To create a new Autonomous Access Point template:

-
- Step 1** Choose **Design > Wireless Configuration > Autonomous AP Configuration Templates**.
 - Step 2** From the Select a command drop-down list, choose **Add Template**.
 - Step 3** Click **Go**. If you are updating an already existing template, click the applicable template in the Template Name column.
 - Step 4** Enter a Template Name.
 - Step 5** Enter the applicable CLI commands.



Note Do not include any show commands in the CLI commands text box. The show commands are not supported.

- Step 6** Click **Save**.
-

Applying an AP Configuration Template to an Autonomous Access Point

To apply an AP Configuration template to an autonomous access point:

-
- Step 1** Choose **Design > Wireless Configuration > Autonomous AP Configuration Templates**.
 - Step 2** Click the template name link to select a template and apply it to the an autonomous access point. The Autonomous AP Configuration Template page appears.
 - Step 3** Click **Apply to Autonomous Access Points**. The Apply to Autonomous Access Points page appears.
 - Step 4** Select the desired autonomous access point.
 - Step 5** Click **OK**.

**Note**

Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the Autonomous AP. If this check box is not selected, any errors encountered while applying a command in the template to a Autonomous AP causes the rest of the commands to be not applied.

Viewing Template Results

To view the results when you apply an Autonomous AP Configuration template to an access point:

- Step 1** Choose **Design > Wireless Configuration > Autonomous AP Configuration Templates**.
- Step 2** Click the template name link to select a template and apply it to the an autonomous access point. The Autonomous AP Configuration template page appears.
- Step 3** Click **Apply to Autonomous Access Points**. The Apply to Autonomous Access Points page appears.
- Step 4** Select the desired autonomous access point.
- Step 5** Click **OK**. The Template Results page appears.

Creating Autonomous Access Point Migration Templates

To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to lightweight access points. The migration utility is available in the Autonomous AP Migration Templates page (Design > Wireless Configuration > Autonomous AP Migration Template) where existing templates are listed.

The Autonomous AP Migration Templates list page displays the following information:

- Name.
- Description.
- AP Count.
- Schedule Run.
- Status—Indicates one of the following task statuses:
 - Not initiated—The template is yet to start the migration and starts at the scheduled time.
 - Disabled—The template is disabled and does not run at the scheduled time. This is the default state for a template when it is created without selecting any autonomous access points.
 - Expired—The template did not run at the scheduled time (this might be due to the Prime Infrastructure server being down).
 - Enabled—The template is yet to start the migration and starts at the scheduled time.
 - In progress—The template is currently converting the selected autonomous access points to CAPWAP.
 - Success—The template has completed the migration of autonomous access point to CAPWAP successfully.

- Failure—The template failed to migrate all the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.
- Partial Success—The template failed to migrate a subset of the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.

**Note**

In any of these states, you can edit the template by clicking the **Name** link.

**Note**

Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.

Related Topics

- [Configuring Autonomous AP Migration Templates](#)
- [Viewing the Migration Analysis Summary](#)
- [Copying a Migration Template](#)
- [Deleting Migration Templates](#)
- [Viewing the Current Status of Cisco IOS Access Points](#)

Configuring Autonomous AP Migration Templates

To create a migration template:

- Step 1** Choose **Design > Wireless Configuration > Autonomous AP Migration Templates**.
- Step 2** From the Select a command drop-down list, choose **Add Template**.
- Step 3** Click **Go**. If you are updating an already existing template, click the applicable template in the Template Name column.
- Step 4** Configure the necessary parameters as described in [Autonomous AP Migration Templates, page 31-68](#).
- Step 5** Click **Save**.

Related Topics

- [Creating Autonomous Access Point Migration Templates](#)
- [Viewing the Migration Analysis Summary](#)
- [Copying a Migration Template](#)
- [Deleting Migration Templates](#)
- [Viewing the Current Status of Cisco IOS Access Points](#)

Viewing the Migration Analysis Summary

To view the Migration Analysis Summary:

**Note**

You can also view the migration analysis summary by choosing **Operate > Wireless > Migration Analysis**.

Step 1 Choose **Design > Wireless Configuration > Autonomous AP Migration Templates**.

Step 2 Choose **View Migration Analysis Summary** from the Select a command drop-down list, and click **Go**. The Migration Analysis Summary page appears.

The autonomous access points are eligible for migration only if all the criteria have a pass status. A red X designates ineligibility, and a green check mark designates eligibility. These columns represent the following:

- **Privilege 15 Criteria**—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- **Software Version Criteria**—Conversion is supported only in Cisco IOS Release 12.3(7)JA excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- **Role Criteria**—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
 - root
 - root access point
 - root fallback repeater
 - root fallback shutdown
 - root access point only
- **Radio Criteria**—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

Related Topics

- [Creating Autonomous Access Point Migration Templates](#)
- [Configuring Autonomous AP Migration Templates](#)
- [Copying a Migration Template](#)
- [Deleting Migration Templates](#)
- [Viewing the Current Status of Cisco IOS Access Points](#)

Copying a Migration Template

To copy a migration template:

Step 1 Choose **Design > Wireless Configuration > Autonomous AP Migration Templates**.

Step 2 Select the check box of the template you want to copy, and then choose **Copy Template** from the Select a command drop-down list.

Step 3 Click **Go**.

- Step 4** Enter the name for the new template to which you want to copy the current template.
-

Related Topics

- [Creating Autonomous Access Point Migration Templates](#)
- [Configuring Autonomous AP Migration Templates](#)
- [Viewing the Migration Analysis Summary](#)
- [Deleting Migration Templates](#)
- [Viewing the Current Status of Cisco IOS Access Points](#)

Deleting Migration Templates

To delete migration templates:

-
- Step 1** Choose **Design > Wireless Configuration > Autonomous AP Migration Templates**.
- Step 2** Select the check boxes of the templates you want to delete, and then choose **Delete Templates** from the Select a command drop-down list.
- Step 3** Click **Go**.
- Step 4** Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.
-

Related Topics

- [Creating Autonomous Access Point Migration Templates](#)
- [Configuring Autonomous AP Migration Templates](#)
- [Viewing the Migration Analysis Summary](#)
- [Copying a Migration Template](#)
- [Viewing the Current Status of Cisco IOS Access Points](#)

Viewing the Current Status of Cisco IOS Access Points

-
- Step 1** Choose **Design > Wireless Configuration > Autonomous AP Migration Templates**.
- Step 2** Select **View Current Status** from the Select a command drop-down list.
- Step 3** Click **Go**.

The following information is displayed:

- IP Address—IP address of the access point.
 - Status—Current status of the migration.
 - Progress—Summary of the migration progress.
-

Related Topics

- [Creating Autonomous Access Point Migration Templates](#)
- [Configuring Autonomous AP Migration Templates](#)
- [Viewing the Migration Analysis Summary](#)
- [Copying a Migration Template](#)
- [Deleting Migration Templates](#)

Designing Controller Config Groups

By creating a config group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all the controllers in a group. You can add, delete, or remove config groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected config groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected config groups.

**Note**

A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

This section contains the following topics:

- [Adding New Config Group, page 4-67](#)
- [Configuring Config Groups, page 4-68](#)
- [Applying or Scheduling Config Groups, page 4-69](#)
- [Auditing Config Groups, page 4-69](#)
- [Rebooting Config Groups, page 4-70](#)
- [Reporting Config Groups, page 4-70](#)
- [Downloading Software, page 4-71](#)

Adding New Config Group

- Step 1** Choose **Design > Wireless Configuration > Controller Config Groups**.
- Step 2** From the Select a command drop-down list, choose **Add Config Group**, and click **Go**. The Add New Group page appears.
- Step 3** Enter the new config group name. It must be unique across all groups. If Enable Background Audit is selected, the network and controller audits occur for this config group. If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.

**Note**

If the Enable Background Audit option is chosen, the network and controller audit is performed on this config group.

- Step 4** Other templates created in Prime Infrastructure can be assigned to a config group. The same WLAN template can be assigned to more than one config group. Choose from the following:

- Select and add later: Click to add a template at a later time.
- Copy templates from a controller: Click to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new config group. Only the templates are copied.

**Note**

The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.

Step 5 Click **Save**.

Configuring Config Groups

Step 1 Choose **Design > Wireless Configuration > Controller Config Groups**.

Step 2 Click a group name in the Group Name column. The Config Group page appears.

Step 3 Click the **General** tab. The following options for the config group appear:

- Group Name: Name of the config group
 - Enable Background Audit—If selected, all the templates that are part of this group are audited against the controller during network and controller audits.
 - Enable Enforcement—If selected, the templates are automatically applied during the audit if any discrepancies are found.

**Note**

The audit and enforcement of the config group template happens when the selected audit mode is *Template based audit*.

- Enable Mobility Group—If selected, the mobility group name is pushed to all controllers in the group.
- Mobility Group Name: Mobility Group Name that is pushed to all controllers in the group. The Mobility Group Name can also be modified here.

**Note**

A controller can be part of multiple config groups.

- Last Modified On: Date and time config group was last modified.
- Last Applied On: Date and time last changes were applied.

Step 4 You must click the **Apply/Schedule** tab to distribute the specified mobility group name to the group controllers and to create mobility group members on each of the group controllers.

Step 5 Click **Save**.

Applying or Scheduling Config Groups

The scheduling function allows you to schedule a start day and time for provisioning.

To apply the mobility groups, mobility members, and templates to all the controllers in a config group:

-
- Step 1** Choose **Design > Wireless Configuration > Controller Config Groups**.
 - Step 2** Click a group name in the Group Name column.
 - Step 3** Click the **Apply/Schedule** tab to access this page.
 - Step 4** Click **Apply** to start the provisioning of mobility groups, mobility members, and templates to all the controllers in the config group. After you apply, you can leave this page or log out of Prime Infrastructure. The process continues, and you can return later to this page to view a report.



Note Do not perform any other config group functions during the apply provisioning.

A report is generated and appears in the Recent Apply Report page. It shows which mobility group, mobility member, or template were successfully applied to each of the controllers.



Note If you want to print the report as shown on the page, you must choose landscape page orientation.

- Step 5** Enter a starting date in the text box or use the calendar icon to choose a start date.
 - Step 6** Choose the starting time using the hours and minutes drop-down lists.
 - Step 7** Click **Schedule** to start the provisioning at the scheduled time.
-

Auditing Config Groups

The Config Groups Audit page allows you to verify if the configuration complies of the controller with the group templates and mobility group. During the audit, you can leave this screen or log out of Prime Infrastructure. The process continues, and you can return to this page later to view a report.



Note Do not perform any other config group functions during the audit verification.

To perform a config group audit:

-
- Step 1** Choose **Design > Wireless Configuration > Controller Config Groups**.
 - Step 2** Click a group name in the Group Name column.
 - Step 3** Click the **Audit** tab to access this page.
 - Step 4** Click to highlight a controller from the Controllers tab, choose >> (**Add**), and **Save Selection**.
 - Step 5** Click to highlight a template from the Templates tab, choose >> (**Add**), and **Save Selection**.
 - Step 6** Click **Audit** to begin the auditing process.

A report is generated and the current configuration on each controller is compared with that in the config group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.



Note This audit does not enforce Prime Infrastructure configuration to the device. It only identifies the discrepancies.

- Step 7** Click **Details** to view the Controller Audit Report details.
- Step 8** Double-click a line item to open the Attribute Differences page. This page displays the attribute, its value in Prime Infrastructure, and its value in the controller.



Note Click **Retain Prime Infrastructure Value** to push all attributes in the Attribute Differences page to the device.

- Step 9** Click **Close** to return to the Controller Audit Report page.

Rebooting Config Groups

- Step 1** Choose **Design > Wireless Configuration > Controller Config Groups**.
- Step 2** Click a group name in the Group Name column.
- Step 3** Click the **Reboot** tab.
- Step 4** Select the **Cascade Reboot** check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.
- Step 5** Click **Reboot** to reboot all controllers in the config group at the same time. During the reboot, you can leave this page or logout of Prime Infrastructure. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report page shows when each controller was rebooted and what the controller status is after the reboot. If Prime Infrastructure is unable to reboot the controller, a failure is shown.



Note If you want to print the report as shown on the page, you must choose landscape page orientation.

Reporting Config Groups

To display all recently applied reports under a specified group name:

- Step 1** Choose **Design > Wireless Configuration > Controller Config Groups**.
- Step 2** Click a group name in the Group Name column.

- Step 3** Click the **Report** tab. The Recent Apply Report page displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:
- **Apply Status**—Indicates success, partial success, failure, or not initiated.
 - **Successful Templates**—Indicates the number of successful templates associated with the applicable IP address.
 - **Failures**—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
 - **Details**—Click **Details** to view the individual failures and associated error messages.
- Step 4** If you want to view the scheduled task reports, click the **click here** link at the bottom of the page. You are then redirected to the Configure > Scheduled Configuration Tasks > Config Group menu where you can view reports of the scheduled config groups.
-

Downloading Software

To download software to all controllers in the selected groups after you have a config group established:

-
- Step 1** Choose **Design > Wireless Configuration > Controller Config Groups**.
- Step 2** Select the check box to choose one or more config groups names on the Config Groups page.
- Step 3** Choose **Download Software** from the Select a command drop-down list, and click **Go**.
- Step 4** The Download Software to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On field.
- Step 5** Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.
- Step 6** Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.
- Step 7** The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. The controller uses this local filename as a base name and then adds _custom.sgi as a suffix.
- If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.
- Step 8** Click **OK**.
-

Downloading IDS Signatures

-
- Step 1** Choose **Design > Wireless Configuration > Controller Config Groups**.
- Step 2** Select the check box to choose one or more config groups on the Config Groups page.
- Step 3** Choose **Download IDS Signatures** from the Select a command drop-down list, and click **Go**.
- Step 4** The Download IDS Signatures to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On field.

- Step 5** Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.
- Step 6** Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.
- Step 7** The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it. The controller uses this local filename as a base name and then adds _custom.sgi as a suffix.
- If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.
- Step 8** Click **OK**.
-

Downloading Customized WebAuth

-
- Step 1** Choose **Design > Wireless Configuration > Controller Config Groups**.
- Step 2** Select the check box to choose one or more config groups on the Config Groups page.
- Step 3** Choose **Download Customized WebAuth** from the Select a command drop-down list, and click **Go**.
- Step 4** The Download Customized Web Auth Bundle to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed.
- Step 5** Choose **local machine** from the File is Located On field.
-

Configuring wIPS Profiles

Prime Infrastructure provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile 'as is' or customize it to better meet your needs.

Pre-defined profiles include the following:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

To access the wIPS Profile page, choose **Design > Wireless Configuration > wIPS Profiles**.

The wIPS Profiles > Profile List page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles.

The Profile List provides the following information for each profile:

- **Profile Name**—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.



Note When you hover your mouse cursor over the profile name, the Profile ID and version appear.

- **MSE(s) Applied To**—Indicates the number of mobility services engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- **Controller(s) Applied To**—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

This section contains the following topics:

- [Adding a Profile, page 4-73](#)
- [Deleting a wIPS Profile, page 4-76](#)
- [Applying a wIPS Profile, page 4-76](#)

The profile editor allows you to create new or modify current profiles. See the [“Editing a wIPS Profile” section on page 4-74](#) for more information.

Adding a Profile

A new wIPS profile can be created using the default or a pre-configured profile.

To add a wIPS profile:

-
- Step 1** Select **Design > Wireless Configuration > wIPS Profiles**. The wIPS Profiles page appears.
 - Step 2** From the Select a command drop-down list, choose **Add Profile**.
 - Step 3** Click **Go**.
 - Step 4** Type a profile name in the Profile Name text box of the Profile Parameters page.
 - Step 5** Select the applicable pre-defined profile, or choose **Default** from the drop-down list.
 - Step 6** Select one of the following:
 - **Save**—Saves the profiles to the Prime Infrastructure database with no changes and no mobility services engine or controller assignments. The profile appears in the profile list.
 - **Save and Edit**—Saves the profile and allows you to edit the profile.
-

Related Topics

- [Configuring wIPS Profiles](#)
- [Editing a wIPS Profile](#)
- [Deleting a wIPS Profile](#)
- [Applying a wIPS Profile](#)

Editing a wIPS Profile

The profile editor allows you to configure profile details including the following:

- SSID groups—Add, edit, or delete SSID groups.
- Policy inclusion—Determine which policies are included in the profile.
- Policy level settings—Configure settings for each policy such as threshold, severity, notification type, and ACL/SSID groups.
- MSE/controller applications—Select the mobility services engine(s) or controller(s) to which you want to apply the profile.

To create profile details:

-
- Step 1** Access the profile editor. This can be done in two ways:
- When creating a new profile, click **Save and Edit** in the Profile Parameters page.
 - Click the profile name from the Profile List page.
- Step 2** From the SSID Groups page, you can edit and delete current groups or add a new group.
- Step 3** When SSID groups have been added or edited as needed, select one of the following:
- Save—Saves the changes made to the SSID groups.
 - Cancel—Returns to the profile list with no changes made.
 - Next—Proceeds to the Profile Configuration page.
- Step 4** From the Profile Configuration page, you can determine which policies are included in the current profile. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. You can enable or disable an entire branch or an individual policy as needed by selecting the check box for the applicable branch or policy.



Note By default, all policies are selected.

- Step 5** In the Profile Configuration page, click an individual policy to display the policy description and to view or modify current policy rule settings.

The following options are available for each policy:

- Add—Click **Add** to access the Policy Rule Configuration page to create a new rule for this policy.
- Edit—Select the check box of the applicable rule, and click **Edit** to access the Policy Rule Configuration page to edit the settings for this rule.
- Delete—Select the check box of the rule you want to delete, and click **Delete**. Click **OK** to confirm the deletion.



Note There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

- Move Up—Select the check box of the rule you want to move up in the list. Click **Move Up**.
- Move Down—Select the check box of the rule you want to move down in the list. Click **Move Down**.

The following settings can be configured at the policy level:

- **Threshold** (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.



Note Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues.



Note Threshold options vary based on the selected policy.



Note Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page. Choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.

- **Severity**—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.
- **Notification**—Indicates the type of notification associated with the threshold.
- **ACL/SSID Group**—Indicates the ACL or SSID Group(s) to which this threshold is be applied.



Note Only selected groups trigger the policy.

Step 6 When the profile configuration is complete, select one of the following:

- **Save**—Saves the changes made to the current profile.
- **Cancel**—Returns to the profile list with no changes made.
- **Back**—Returns to the SSID Groups page.
- **Next**—Proceeds to the MSE/Controller(s) page.

Step 7 In the Apply Profile page, select the check box(es) of the mobility services engine and controller(s) to which you want to apply the current profile.

Step 8 When the applicable mobility services engine(s) and controller(s) are selected, choose one of the following:

- **Apply**—Applies the current profile to the selected mobility services engine/controller(s).
- **Cancel**—Returns to the profile list with no changes made.



Note A created profile can also be applied directly from the profile list. From the Profile List page, select the check box of the profile you want to apply and click **Apply Profile** from the Select a command drop-down list. Click **Go** to access the Apply Profile page.

Related Topics

- [Configuring wIPS Profiles](#)
- [Adding a Profile](#)

- [Deleting a wIPS Profile](#)
- [Applying a wIPS Profile](#)

Deleting a wIPS Profile

To delete a wIPS profile:

-
- Step 1** Choose **Design > Wireless Configuration > wIPS Profiles**. The wIPS Profiles page appears.
 - Step 2** Select the check box of the wIPS profiles you want to delete.
 - Step 3** From the Select a command drop-down list, choose **Delete Profile**.
 - Step 4** Click **Go**.
 - Step 5** Click **OK** to confirm the deletion.



Note If the profile is already applied to a controller, it cannot be deleted.

Related Topics

- [Configuring wIPS Profiles](#)
- [Adding a Profile](#)
- [Editing a wIPS Profile](#)
- [Applying a wIPS Profile](#)

Applying a wIPS Profile

To apply a wIPS profile:

-
- Step 1** Choose **Design > Wireless Configuration > wIPS Profiles**. The wIPS Profiles page appears.
 - Step 2** Select the check box of the wIPS profiles you want to apply.
 - Step 3** From the Select a command drop-down list, choose **Apply Profile**.
 - Step 4** Click **Go**.
 - Step 5** Select the mobility services engines and controllers to which the profile is applied.



Note If the new assignment is different than the current assignment, you are prompted to save the profile with a different name

- Step 6** When the applicable mobility services engines and controllers are selected, click **Apply**.
-

Related Topics

- [Configuring wIPS Profiles](#)

- [Adding a Profile](#)
- [Editing a wIPS Profile](#)
- [Deleting a wIPS Profile](#)

Configuring Features on a Device

You can create or change the feature configuration for the selected device. The following topics provide more information:

- [Application Visibility, page 4-77](#)
- [Overview of NAT, page 4-79](#)
- [Dynamic Multipoint VPN, page 4-85](#)
- [GETVPN, page 4-89](#)
- [VPN Components, page 4-93](#)
- [Overview of Zones, page 4-100](#)
- [Routing, page 4-111](#)

Application Visibility

The Application Visibility (AV) feature helps in monitoring the traffic sent towards the internet. To configure AV, you need to perform the following:

- Create / Update AV Configuration
- Assign AV policies on interfaces
- Change AV Advanced options



Note

The Application Visibility feature is supported on ASR devices from the IOS version 3.5 or later. This feature is not supported on ISR devices. The CLI changes that starts with “EMS_” is not supported and may cause unexpected behavior.

Configuring AV

The Application Visibility Configuration feature creates the required elements in the device to send the NetFlow messages for Transaction Records and Usage Records. To configure AV, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Choose the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Application Visibility folder**, and then choose the **Configuration**. The AV Configuration page appears.
 - Step 5** From the AV Configuration page, set the Primary CM IP Address and port, Secondary CM IP Address and port, VPN Routing and Forwarding (VRF), and Source IP address and Export protocol.

**Note**

For Source IP address, specify the IP address for an interface, which will be used as the source for sending FNF messages towards the CM.

**Note**

The Export Protocol is supported from IOS version 3.7 or later. For the IOS version 3.7 or later, IPfix is the default value. For older versions, netflow-v9 is set as the default value.

- Step 6** Set the advanced AV parameters. For more information on the Advanced AV parameters, see [Changing AV Advanced Options, page 4-79](#).
- Step 7** Click **Save / Apply** to save the changes in the server.

Editing AV Policy

To edit the existing AV policy, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Choose the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Application Visibility** folder, and then choose the **Interfaces**.
- Step 5** In the Interface page, select one or more interfaces and click **Edit**.
- Step 6** To monitor the bandwidth usage and the traffic at transactions level, select the usage/transaction records in the input reports or output reports section.

**Note**

Application Visibility configuration supports all the interfaces that are supported on the ASR device.

- Step 7** Select the IPv4 or IPV6 or IPv4+IPv6 from the drop-down list.
- a. Usage Records (UR)—Usage Records are records of the different type of applications that run on a specific interface. The operator can use the Usage Records to monitor the bandwidth usage of different applications. The Usage Records can show the application usage over a specific time period, the peak and average usages, and usage for a specific application type. Usage Records perform periodic aggregation of the category information for the interface. (For example, export information for peer-to-peer traffic or email usage).
 - b. Transaction Records (TR)—A transaction is a set of logical exchanges between endpoints. There is normally one transaction within a flow. The Transaction Record monitors the traffic at transaction levels. These records provide a detailed analysis of the traffic flows. Transaction Records are bound to the input and output directions of the network side interfaces. These Transaction Records allow the system to capture each unidirectional flow once.
- Step 8** Click **OK** to deploy the changes to the device.

Changing AV Advanced Options

To change the Application Visibility Advanced options, follow these steps.

-
- | | |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Operate > Device Work Center . |
| Step 2 | Select the device from the list or click Add to create a new device, then configure the device. |
| Step 3 | After selecting the device, click Configuration . The Feature Configuration panel appears. |
| Step 4 | Expand the Application Visibility folder , and then click Configuration . |
| Step 5 | In the AV Configuration page, set the new values for the AV configuration. |
| Step 6 | Specify the Differentiated Services Codepoint (DSCP) value to set the exporter DSCP service code point value. |
| Step 7 | Specify the Time-to-Live (TTL) value to set the exporter TTL or hop limit. |
| Step 8 | Click on the title area to view the to view the FNF Advanced Options, FNF Record Advanced Options, and NBAR Advanced options. |
| Step 9 | To customize the value, check the specific attribute check box and set the new value. To use the system default value, uncheck the check box of the specific attribute. |
| Step 10 | In the FNF Advanced Options, set the timeout value in seconds. |
| Step 11 | In the FNF Record Advanced Options, set the maximum flow entries in the flow cache and specify the active/inactive flow timeout in seconds. Disable Unresolved Traffic Reporting check box to disable the total usage records. |
| Step 12 | In the IPv4/IPv6 NetFlow Sampled Transaction Records section, set the maximum flow entries in the flow cache and define the sampling rate. |
| Step 13 | In the NBAR Advanced Options section, define the maximum allowed sessions in multiples of 50000. |
| Step 14 | Click Save / Deploy to save the changes in the device. |
| Step 15 | Click Reset to Default to reset the parameter values to their default values. |
-

Overview of NAT

The Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The NAT helps to limit the number of public IP addresses used by an organization or company, for both economy and security purposes.

The NAT feature allows organizations to resolve the problem of IP address depletion when they have existing networks and need to access the Internet. The NAT allows the IP network of an organization to use different IP address space for the outside network. Thus, NAT allows an organization that does not have globally routable addresses to connect to the Internet by translating those addresses into globally routable address space. The NAT also allows a more graceful renumbering strategy for organizations that are changing service providers or voluntarily renumbering into Classless Inter Domain Routing (CIDR) blocks. The NAT is described in RFC 1631.

A router configured with the NAT will have at least one interface to the inside network and one to the outside network. In a typical environment, the NAT is configured at the exit router between a sub domain and a backbone. When a packet leaves the domain, the NAT translates the locally significant source address into a globally unique address. When a packet enters the domain, the NAT translates the globally

unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. If the NAT cannot allocate an address because it has run out of addresses, it drops the packet and sends an Internet Control Message Protocol (ICMP) host unreachable packet.

For more information on NAT, see

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/xr-3s/iadnat-addr-consv.html.

Types of NAT

The NAT operates on a router—Generally connecting only two networks together—and translates your private (inside local) addresses within the internal network, into public (inside global) addresses before any packets are forwarded to another network. This functionality gives you the option to configure the NAT so that it will advertise only a single address for your entire network to the outside world. Doing this effectively hides the internal network from the world, giving you some additional security.

NAT types include:

- Static Address Translation (SAT) —Allows one-to-one mapping between local and global addresses.
- Dynamic Address Translation—Maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.
- Overloading—A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as Port Address Translation (PAT). By using PAT (NAT Overload), thousands of users can be connected to the Internet using only one real global IP address.

How to Configure NAT for IP Address Conservation

To configure NAT, perform the following steps:

1. Create the NAT pool (required for Dynamic NAT)
2. Configure the ACL
3. Create the NAT44 rules
4. Assign rules on the interfaces
5. Set up the NAT maximum translation (Optional)



Note

The NAT feature is supported on the ASR platform from the IOS version 3.5 or later. The NAT feature is supported on the ISR platform from the IOS version 12.4(24)T or later. The CLI changes that starts with “EMS_” is not supported and may cause unexpected behavior.

IP Pools

The IP Pool is a device object that represents IP ranges to be used on the Dynamic NAT. The NAT IP Pools feature allows you to create a new pool that can be used in the Dynamic NAT, change the existing pool, and delete the pool from the device.

Creating, Editing, and Deleting IP Pools

To create, edit, and delete the IP Pools, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security**, expand the **NAT** subfolder, and then click **IP Pools**. The NAT Pools page appears.
- Step 5** Click the **Add IP Pool > IP+Prefix** or **IP Range + Prefix** button, and enter the Name, IP Address/Range, Prefix Length, and Description. You cannot change the name of the pool after creating the pool.



Note A valid IPv4 address consists of 4 octets separated by a period (.).

- Step 6** Click **OK** to save the configurations.
- Step 7** Click the **Apply** button to deploy the pool to the server database.
- Step 8** To edit the existing IP Pool, in the NAT IP Pools page do the following:
- Click on the selected IP Pools parameters row, and edit the parameters. or
 - Select the IP Pools, and click the **Edit** button. The selected IP Pools opens for editing. You can edit all the parameters except the pool name.
- Step 9** Click **Save / Apply** to save the changes in the server.
- Step 10** To delete the existing IP Pools, select the IP Pool, and then click the **Delete** button.
- Step 11** Click **OK** on the warning message to delete the IP Pool. The selected IP Pool will be deleted.
-

NAT44

The NAT44 feature allows the user to create, delete, and change the NAT44 rules.

Creating, Editing, and Deleting NAT44 Rule

This section describes how to create the NAT44 rules.

There are three types of NAT rules:

- Static
- Dynamic
- Dynamic PAT

To create the NAT44 rule, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security**, expand the **NAT** subfolder, and then click **NAT44**.
- Step 5** From the NAT 44 Rule page, click the down arrow icon on the **Add NAT Rule** button.
- Click Static to create Static Rule. For elements on this page, see [Table 4-4](#).

- Click Dynamic to create Dynamic NAT Rule. For elements on this page, see [Table 4-5](#).
- Click Dynamic PAT to create Dynamic PAT Rule. For elements on this page, see [Table 4-6](#).

[Table 4-4](#) lists the elements on the Static Rule page.

Table 4-4 **Static Rule Page**

Element	Description
Direction	Displays the directions. This release supports only the Inbound to Outbound direction.
VRF	Displays the VRF on which the NAT translation process happens.
Source A	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period (.). <ul style="list-style-type: none"> • If the Source A is defined, then the Source B must also be defined. • If the Source A is defined, then the Destination A will be Any by default.
Destination A	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period (.). <ul style="list-style-type: none"> • If the Destination A is defined, then the Destination B must also be defined. • If the Destination A is defined, then the Source A will be Any by default.
Translation	Displays the static translation type.
Source B	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period (.). You can also select an interface from the list of interfaces. <ul style="list-style-type: none"> • If the Source B is defined, then the Source A must also be defined. • If the Source B is defined, then the Destination B will be Any by default.
Destination B	Enter a valid IPv4 address. A valid IPv4 address consists of 4 octets separated by a period (.). <ul style="list-style-type: none"> • If the Destination B is defined, then the Destination A must also be defined. • If the Destination B is defined, then the Source A and B will be Any by default.
Options	Displays the advance options for the Static type. Configure the following: <ul style="list-style-type: none"> • To ignore the embedded IP addresses (no-Payload), check the Ignore Embedded IP address check box. • To enable port translation, check the Enable Port Translation check box, and then define the following: <ul style="list-style-type: none"> – TCP or UDP – Original Port – Port Translation

[Table 4-5](#) lists the elements on the Dynamic NAT page.

Table 4-5 **Dynamic NAT Page**

Element	Description
Direction	Displays the directions. This release supports only the Inbound to Outbound direction.
VRF	Displays the VRF on which the NAT translation process happens.

Table 4-5 **Dynamic NAT Page (continued)**

Element	Description
Source A	Select the ACL name from the list. <ul style="list-style-type: none"> • If the Source A is defined, then the Source B must also be defined. • If the Source A is defined, then the Destination A will be Any by default.
Destination A	Select the ACL name from the list. <ul style="list-style-type: none"> • If the Destination A is defined, then the Destination B must also be defined. • If the Destination A is defined, then the Source A will be Any by default.
Translation	Displays the Dynamic NAT translation type.
Source B	Choose the NAT pool from the drop-down list. You can also select an interface from the list of interfaces. <ul style="list-style-type: none"> • If the Source B is defined, then the Source A must be defined. • If the Source B is defined, then the Destination B will be Any by default.
Destination B	Choose the NAT pool from the drop-down list. <ul style="list-style-type: none"> • If the Destination B is defined, then the Destination A must also be defined. • If the Destination B is defined, then the Source A and B will be Any by default.
Options	Displays the advance options for the Dynamic type. <ul style="list-style-type: none"> • To ignore the embedded IP addresses (no-Payload), check the Ignore Embedded IP address check box. • To enable port translation, check the Enable Port Translation check box, and then define the following: <ul style="list-style-type: none"> – TCP or UDP – Original Port – Port Translation <p>Note This option is supported only on the ISR devices.</p>

Table 4-6 lists the elements on the Dynamic PAT page.

Table 4-6 **Dynamic PAT Page**

Element	Description
Direction	Displays the directions. This release support the Inbound to Outbound directions.
VRF	Displays the VRF on which the NAT translation process happens.
Source A	Select the ACL name from the list.
Destination A	Not defined.
Translation	Displays the Dynamic PAT translation type.
Source B	Select the IP Pool Name from the list. You can also select an interface from the list of interfaces.
Destination B	Not defined.

Table 4-6 **Dynamic PAT Page**

Element	Description
Options	Displays the advance options for the Dynamic PAT. Select the Ignores embedded IP Addresses (no-Payload) option. The options are: Yes or No . Note This option is supported only on the ISR devices.

- Step 6** Click:
- **Save** to save and deploy the changes to the device.
 - **Cancel** to exit without saving.
- Step 7** To edit the existing NAT44 rule in the NAT44 page, do one of the following:
- Click on the selected NAT44 rules parameters row, and edit the parameters.
 - Select the NAT44 rule, and click the **Edit** button. The selected NAT44 rule opens for editing. You can edit all the parameters except the pool Name.
- Step 8** You can change the Source and Destination according to the creation rules. You can also change the Options selection according to the creation rules.
- Step 9** Click **Save/ Apply** to save the changes in the server.
- Step 10** To delete the existing NAT44 rules, select the rules, and then click the **Delete** button.
- Step 11** Click **OK** on the warning message to delete the rules. The selected NAT44 rules will be deleted.

Managing Interfaces

A virtual interface is a logical interface configured with generic configuration information for a specific purpose or for configuration common to specific users, plus router-dependent information.

Configuring Interfaces

To assign the interfaces to a specific association, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security**, expand the **NAT** subfolder, and then click **Interfaces**.

In the Interface page, select the interface you want to change and select the association from the drop-down list. The options are: Inside, Outside, and None.
- Step 5** Click:
- **Save/ Apply** to save the changes in the server.
 - **Cancel** to exit without saving.

Managing NAT MAX Translation

The Rate Limiting NAT Translation feature provides the ability to limit the maximum number of concurrent NAT operations on a router. In addition, the NAT MAX feature gives users additional control to use the NAT addresses. The Rate Limiting NAT Translation feature can be used to limit the effects of viruses, worms, and denial-of-service attacks.

The NAT Maximum Translations feature allows you to reset the global translation attribute values.

Setting NAT MAX Translation

To set the MAX Translation, follow these steps.

-
- | | |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Operate > Device Work Center . |
| Step 2 | Select the device from the list or click Add to create a new device, then configure the device. |
| Step 3 | After selecting the device, click Configuration . The Feature Configuration panel appears. |
| Step 4 | Expand the Security , expand the NAT subfolder, and then click Max. Translation . |
| Step 5 | Reset the parameter values. Configure the maximum number of NAT entries that are allowed for all the parameters. A typical range for a NAT rate limit is from 100 to 300 entries. |
| Step 6 | Click: <ul style="list-style-type: none">• Save / Apply to save the changes in the server.• Cancel to exit without saving. |
-

Dynamic Multipoint VPN

The DMVPN feature allows users to scale large and small IP Security (IPsec) VPNs by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).

A typical VPN connection is a point-to-point IPsec tunnel connecting two routers. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes using a GRE over IPsec tunnel. IPsec traffic is routed through the hub to the spokes in the network.

See [Dynamic Multipoint IPsec VPNs \(Using Multipoint GRE/NHRP to Scale IPsec VPNs\)](#) for more information about DMVPN (requires a CCO login ID).

Configuring DMVPN

Cisco Network Control System allows you to configure your router as a DMVPN hub or DMVPN spoke. You can configure the router in the following ways:

Hub

- [Configuring Hub and Spoke Topology, page 4-87](#)

Spoke




- [Configuring Fully Mesh Topology, page 4-87](#)

Creating DMVPN Tunnel

You should configure the following parameters to create the DMVPN tunnel:

- Device role and topology type
- Multipoint GRE interface information
- NHRP and tunnel parameters
- Next Hub Server (NHS) Server (Optional)

To create the DMVPN tunnel, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then click **DMVPN**. Click the **Add** button to create the DMVPN.
- Step 5** In the Device Role and Topology Type section, select the topology and the device role. The options are: Spoke, Hub, and Dynamic Connection between Spokes.
- Step 6** In the Multipoint GRE Interface Information section, select the WAN interface that connects to the Internet from the drop-down list.
- Step 7** Enter the IP address of the Tunnel Interface, and Subnet Mask.
- Step 8** In the NHRP and Tunnel Parameters section, complete the fields on this section.
-
-  **Note** The Network ID is a unique 32-bit network identifier from a Non Broadcast Multiaccess (NBMA) network. The tunnel key is used to enable a key ID for a particular tunnel interface. The MTU size of IP packets that are sent on a particular interface.
-
-  **Note** The default MTU value for Ethernet and the serial interface is 1500. The default value varies depending upon the media type. The Tunnel throughput delay is used to set the delay value for a particular interface.
-
- Step 9** In the Encryption policy field, click the anchored plus button (+) to add the Transform Set Profile.
- Step 10** In the Transform Set Profile dialog box, enter the Name and choose the acceptable combination of security protocols and algorithm from the drop-down list to configure the transform set.
- Step 11** Enable the IP Compression check box to enable the IP compression for the transform set.
- Step 12** Choose the mode for the transform set. The options are: Tunnel mode or Transport mode.
- Step 13** In the NHS Server Information section, enter the IP address for the physical interface of the hub and tunnel and the Fallback Time. If the device supports the cluster then add the next hop server information, such as Cluster ID, Max Connection, Hub IP address, and Priority.
-
-  **Note** The NHS server information is required only for spoke configuration. If you check the Use Cluster for NHS check box, add the information, such as Cluster ID, Max Connection, and Next Hub Server. The template with the NHS cluster configuration will be applied only to the device running Cisco IOS Software version 15.1(2)T or later.
-

- Step 14** In the Routing Information section, choose the routing information. The options are: EIGR, RIPv2, and Other.



Note The routing information is required only for hub configuration.

- Step 15** Choose the existing EIGRP number from the drop-down list or enter an EIGRP number. Use the Other option to configure the other protocols.
- Step 16** Click **Save** to save the single NHS server entry details and the priority of the server, save the entire group of server, and save the NHS cluster information. When you save the NHS cluster information, the NHS server will be populated in the non-editable field.
- Step 17** Click **OK** to save the configuration to the device.
- Step 18** Click **Cancel** to cancel all the changes you have made without sending them to the router.

Configuring Hub and Spoke Topology

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then click **DMVPN**. Click the **Add** button to create the DMVPN tunnel.
- Step 5** In the Device Type and Topology section, choose Hub and Spoke as the topology, and select either Hub or Spoke as a device role.
- Step 6** Select the WAN interface from the drop-down list, and then configure the Multipoint GRE IP Address and the subnet mask for the tunnel interface.
- Step 7** Configure the NHRP and the Tunnel Interface parameters, such as the IP address, NHRP parameters and map, MTU value, Source of the Tunnel, Tunnel Mode, and Tunnel Key.
- Step 8** Create the transform-set for protecting the data flow between the devices. You can specify up to four transforms: One Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IPSec security protocols and the algorithms.
- Step 9** Configure the routing protocol to be used.
- Step 10** Click **Save** to save the configuration to the device.
- Step 11** Click **Cancel** to close the Create DMVPN Tunnel page without applying the changes to the device.

Configuring Fully Mesh Topology


The dynamic spoke-to-spoke option allows you to configure the DMVPN fully meshed topology. In this topology, you can configure the router as a spoke, capable of establishing a direct IPSec tunnel to other spokes in the network.

To configure the hub and spoke topology, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Security folder**, and then click **DMVPN**. Click the **Add** button to create the DMVPN tunnel with fully meshed topology.
 - Step 5** From the Create DMVPN Tunnel configuration page, select the **Full Mesh** radio button to configure the network type as full mesh topology.
 - Step 6** Repeat [Step 6](#) through [Step 8](#) from the [Configuring Hub and Spoke Topology](#) section.
 - Step 7** For Fully Mesh spoke topology, in the NHS Server Information section, add the next hub server information, such as the IP Address of Hub's physical interface and the IP address of Hub's tunnel interface.
 - Step 8** Click **Save** to save the configuration to the device.
 - Step 9** Click **Cancel** to close the Create DMVPN Tunnel page without applying the changes to the device.
-

Cluster Configuration

To configure the cluster, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Security folder**, and then click **DMVPN**. Click the **Add** button to create the DMVPN tunnel.
 - Step 5** From the Create DMVPN Tunnel configuration page, select the **Spoke** radio button to configure the device role as a spoke.
 - Step 6** Repeat [Step 6](#) through [Step 8](#) from the [Configuring Hub and Spoke Topology](#) section.
-
-  **Note** The device must be running IOS version of 15.1(2)T or later.
-
- Step 7** Click the **Add Row** button to configure the cluster related information, and add the Cluster-ID and Maximum Connection values.
 - Step 8** Click the **Expand Row** button (next to the radio button) and click the **Add Row** button to add the NHS server information.
 - Step 9** Enter the NHS server, the GRE Tunnel IP addresses, and the Priority of this NHS server. Click the **Save** button to save the NHS server entry configuration.
 - Step 10** Click the **Save** button to save the NHS server group information.
 - Step 11** Click the **Save** button again to save the NHS group information with the cluster configuration. This will automatically populate the NHS server IP address in the table.
-

Edit DMVPN

To edit the existing DMVPN tunnel, follow these steps.

-
- | | |
|---------------|-----------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Operate > Device Work Center . |
| Step 2 | Select the device from the list or click Add to create a new device, then configure the device. |
| Step 3 | After selecting the device, click Configuration . The Feature Configuration panel appears. |
| Step 4 | Expand the Security folder , and then click DMVPN . The available tunnel is displayed. |
| Step 5 | Select the tunnel, and click the Edit button. The Edit DMVPN Tunnel page opens. |
| Step 6 | From the Edit DMVPN Tunnel page, you can edit the DMVPN parameters. |
| Step 7 | Click OK to send the edited DMVPN tunnel configuration to the device. |
| Step 8 | Click Cancel to close the Edit DMVPN Tunnel page without applying the configuration to the device. |
-

Delete DMVPN

To delete the existing DMVPN tunnel, follow these steps.

-
- | | |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Operate > Device Work Center . |
| Step 2 | Select the device from the list to delete the DMVPN tunnel. If the device is not added, click the Add button to add the device. |
| Step 3 | After selecting the device, click Configuration . The Feature Configuration panel appears. |
| Step 4 | Expand the Security folder , and then click DMVPN . The available tunnel is displayed. |
| Step 5 | Select the tunnel, and click the Delete button. |
| Step 6 | Click Yes on the warning message to delete the selected tunnel. |
| Step 7 | Click No on the warning message if you do not want to delete the selected tunnel. |
| Step 8 | Click Cancel to cancel all the changes you have made without sending them to the router. |
-

GETVPN

A Group Encrypted Transport VPN (GETVPN) deployment has primarily three components: Key Server (KS), Group Member (GM), and Group Domain of Interpretation (GDOI) protocol. GMs encrypt/decrypt the traffic and KS distributes the encryption key to all the group members. The KS decides on one single data encryption key for a given life time. Because all GMs use the same key, any GM can decrypt the traffic encrypted by any other GM. GDOI protocol is used between the GM and KS for group key and group Security Association (SA) management. Minimum one KS is required for a GETVPN deployment.

Unlike traditional IPSec encryption solutions, GETVPN uses the concept of group SA. All members in the GETVPN group can communicate with each other using a common encryption policy and a shared SA. Therefore, there is no need to negotiate IPSec between GMs on a peer-to-peer basis; thereby reducing the resource load on the GM routers.

Group Member

The GM registers with the KS to get the IPsec SA that is necessary to encrypt data traffic within the group. The GM provides the group identification number to the KS to get the respective policy and keys for this group. These keys are refreshed periodically by the KS, before the current IPsec SAs expire, so that there is no traffic loss.

Key Server

The KS is responsible for maintaining security policies, authenticating the GMs and providing the session key for encrypting traffic. KS authenticates the individual GMs at the time of registration. Only after successful registration can the GMs participate in group SA.

A GM can register at any time and receive the most current policy and keys. When a GM registers with the KS, the KS verifies the group identification number of the GM. If this identification number is valid, and the GM has provided valid Internet Key Exchange (IKE) credentials, the KS sends the SA policy and the Keys to the group member.

There are two types of keys that the GM will receive from the KS: the Key Encryption Key (KEK) and the Traffic Encryption Key (TEK). The TEK becomes part of the IPsec SA with which the group members within the same group encrypt the data. KEK is used to secure rekey messages between the KS and the GMs.

The KS sends out rekey messages either because of an impending IPsec SA expiration or because the security policy has changed on the KS. Keys can be distributed during re-key using either multicast or unicast transport. Multicast method is more scalable as keys need not be transmitted to each group member individually. Unlike in unicast, KS will not receive acknowledgement from GM about the success of the rekey reception in multicast rekey method. In unicast rekey method, KS will delete a GM from its database if three consecutive rekeys are not acknowledged by that particular GM.

GDOI protocol is used for Group key and group SA management. GDOI uses Internet Security Association Key Management Protocol (ISAKMP) for authenticating the GMs and KSs. All the standard ISAKMP authentication schemes like RSA Signature (certificates) and Pre-shared key can be used for GETVPN.

For more information on GETVPN, See

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/deployment_guide_c07_554713.html.

Configuring GETVPN

The Cisco Network Control System allows you to configure the GETVPN. To configure the GETVPN, you should configure the following:

- Group member
- Key server

Creating GETVPN Group Member

Use the Add GroupMember configuration page to configure the GETVPN group member.

To create the GETVPN group member, follow these steps.

Step 1 Choose **Operate > Device Work Center**.

- Step 2** Select the device from the list or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security** folder, and then click **GETVPN-GroupMember**. Click the **Add** button to create the GET VPN group member.
- Step 5** In the Add GroupMember dialog box, select the General tab, and enter the Group Name and Group Identity. Choose the Registration Interface from the drop-down list.
- Step 6** Enter the Primary Key Server and Secondary Key Server IP addresses. Click the **Add Row** or **Delete** button to add or delete the secondary key server IP addresses.

**Note**

The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizes with the secondary key servers. The server with the highest priority is elected as a primary key server.

- Step 7** Click on the **row** or **field** to edit the secondary key server IP address.
- Step 8** Click:
- **Save** to save the configuration.
 - **Cancel** to exit without saving your changes.
- Step 9** In the Add Group Member dialog box, select the Advanced tab, and choose the Local Exception ACL and Fail Close ACL from the drop-down list.

**Note**

If the Fail Close feature is configured, all the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.

- Step 10** Select the Migration tab, and check the Enable Passive SA check box to enable passive SA. Use this option to turn on the Passive SA mode on this group member.
- Step 11** Click:
- **OK** to add the Group member in the table. To display the commands, click **CLI** preview. After the scheduled deploy is completed, the configuration is applied on the device.
 - **Cancel** to cancel all the changes you have made without sending them to the router.
 - **Close** to close the page.

Creating GETVPN Key Server

Use the Add KeyServer configuration page to configure the GETVPN key server.

To create the GETVPN key server, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.

- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then click **GETVPN-KeyServer**. Click the **Add** button to create the GETVPN key server.
- Step 5** In the Add Key Server dialog box, select the General tab, and enter the Group Name, Group Identity, WAN IP address, and Priority of this key server.
- Step 6** Enter the Co-operative Key Servers IP address. Click the **Add Row** or **Delete** button to add or delete the Co-operative key server IP address. Click on the **row** or **field**, and edit the IP address.
- Step 7** In the Add KeyServer dialog box, select the Rekey tab, and choose the Distribution method from the drop-down list.

**Note**

The distribution method is used to send the rekey information from key server to group members. When you choose the distribution method as multicast, specify the multicast address to which the rekey needs to be transmitted.

- Step 8** In the Add KeyServer dialog box, select the GETVPN Traffic tab, and enter the Traffic to be encrypted, Encryption Policy, and Anti Replay.

**Note**

The access list defines the traffic to be encrypted. Only the traffic which matches the “permit” lines will be encrypted. Be sure not to encrypt certain traffic that should always be permitted even if the crypto sessions are not up

- Step 9** Click:
- **OK** to add the Group member in the table. To display the commands, click **CLI** preview. After the scheduled deployment is completed, the configuration is applied on the device.
 - **Cancel** to cancel all the changes you have made without sending them to the router.
- Step 10** Click **Close** to close the page.

Editing GET VPN Group Member or Key Server

To edit the existing GETVPN group member or the GETVPN key server, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then click **GETVPN-Group Member** or **GETVPN-KeyServer**. The GETVPN-GroupMember or GETVPN-KeyServer summary page opens.
- Step 5** From the GETVPN summary page, select the group name and click **Edit**. The Edit GETVPN-GroupMember or GETVPN-Keyserver page appears.
- Step 6** From the Edit GETVPN-GroupMember or GETVPN-KeyServer page, you can edit the GETVPN parameters.
- Step 7** Click:

- **OK** to save the configurations.
- **Cancel** to cancel all the changes you have made without sending them to the router.

Step 8 Click **Close** to close the page.

Deleting GETVPN Group Member or Key Server

To delete the existing GETVPN group member or the GETVPN key server, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then click **GETVPN-Group Member** or **GETVPN-KeyServer**. The GETVPN-GroupMember or GETVPN-KeyServer summary page opens.
- Step 5** From the GETVPN summary page, select the group name and click **Delete**.
- Step 6** Click:
- **OK** to save the configurations.
 - **Cancel** to cancel all the changes you have made without sending them to the router.
- Step 7** Click **Close** to close the page.
-

VPN Components

The VPN components primarily include the following:

- [IKE Policies, page 4-93](#)
- [IKE Settings, page 4-96](#)
- [IPsec Profile, page 4-97](#)
- [Pre-shared Keys, page 4-98](#)
- [RSA Keys, page 4-98](#)
- [Transform Sets, page 4-100](#)

IKE Policies

The Internet Key Exchange (IKE) is a standard method for arranging secure and authenticated communications. The IKE establishes session keys (and associated cryptographic and networking configuration) between two hosts across the network. The IKE policies will protect the identities of peers during authentication.

The IKE negotiations must be protected; therefore, each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states the security parameters that will be used to protect subsequent IKE negotiations. After the two peers agree on a policy, the security parameters of the policy are identified by a security association established at each peer. These security associations are applied to all the subsequent IKE traffic during the negotiation.

When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both the peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies. The remote peer checks each of its policies in the order of its priority (highest first) until a match is found. A match is made when both the policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman (D-H) parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. If the lifetimes are not identical, the shorter lifetime is used from the remote peer's policy.

Creating, Editing, and Deleting IKE Policies

The IKE Policies feature allows you to create, edit, and delete the IKE policies.

To create, edit, or delete the IKE policies, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select a device or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Security folder**, and then choose **VPN Components > IKE Policies**.
 - Step 5** Click the **Add Row** button to create the IKE policies.
 - Step 6** In the IKE Policies page, enter the Priority, Authentication, D-H Group, Encryption, Hash, and Lifetime.
 - Step 7** To edit the IKE policies parameters, click on the **Field** and edit the parameter of that IKE policy.
 - Step 8** To delete the IKE policies, select the IKE policies from the list, and click the **Delete** button.

[Table 4-7](#) lists the elements on the IKE Policies page.

Table 4-7 IKE Policies Page

Element	Description
IKE Policies	
Priority	<p>Enter the priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.</p> <p>The range is from 1 to 10000. The lower the number, the higher the priority.</p>
Authentication	<p>Choose the Pre-shared keys or RSA Signatures from the drop-down list.</p> <ul style="list-style-type: none"> Pre-SHARE—Authentication will be performed using pre-shared keys. RSA_SIG— Authentication will be performed using digital signatures.

Table 4-7 **IKE Policies Page (continued)**

Element	Description
Encryption	<p>Choose the encryption algorithm from the drop-down list.</p> <ul style="list-style-type: none"> • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Diffie-Hellman Group	<p>Choose the D-H group algorithm from the drop-down list.</p> <p>The Diffie-Hellman group is used for driving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are:</p> <ul style="list-style-type: none"> • 1—Diffie-Hellman Group 1 (768-bit modulus). • 2—Diffie-Hellman Group 2 (1024-bit modulus). • 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys).
Hash	<p>Choose the hash algorithm used in the IKE proposal from the drop-down list. The hash algorithm creates a message digest, which is used to ensure message integrity. The options are:</p> <ul style="list-style-type: none"> • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.
Lifetime	<p>The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.</p> <p>The range is from 60 to 86400 seconds. The default value is 86400.</p>

Step 9 Click:

- **Save** to save the configuration.
- **Cancel** to exit without saving your changes.
- **Save** again to generate the CLI commands.

IKE Settings

The IKE Settings feature allows you to globally enable the IKE for your peer router.

Creating IKE Settings

To enable the IKE policies and set the aggressive mode for the IKE, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select a device or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then choose **VPN Components > IKE Settings**.
- Step 5** Check the Enable IKE and Enable Aggressive Mode check box to enable the IKE policies and the aggressive mode.
- Step 6** Choose the IKE Identity from the drop-down list.
- Step 7** Enter the Dead Peer Detection Keepalive and Dead Peer Detection Retry time in seconds.

[Table 4-8](#) lists the elements on the IKE Settings page.

Table 4-8 *IKE Settings Page*

Element	Description
IKE Settings	
Enable IKE	<p>Check the Enable IKE check box to globally enable the IKE. By default, the IKE is enabled. You do not have to enable IKE for individual interfaces, but it can be enabled globally for all the interfaces at the router.</p> <p>If you do not want to use the IKE for your IP Security (IPSec) implementation, you can disable the IKE for all your IPSec peers. If you disable the IKE for one peer, you must disable it for all the IPSec peers.</p>
Enable Aggressive Mode	<p>Check the Enable Aggressive Mode check box to enable the Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode. If you disable the aggressive mode, all aggressive mode requests to the device and all aggressive mode requests made by the device will be blocked.</p>
IKE Identity	<p>Choose the ISAKMP identity from the drop-down list. The options are: IP address, Distinguished Name and HostName. An ISAKMP identity is set whenever you specify pre-shared keys or RSA signature authentication. As a general rule, you should set all peers' identities in the same way, either by IP address or by host name.</p> <ul style="list-style-type: none"> IP Address—Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during the IKE negotiations. Distinguished Name—Sets the ISAKMP identity to the distinguished name (DN) of the router certificate. Host Name—Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com).

Table 4-8 **IKE Settings Page (continued)**

Element	Description
Dead Peer Detection Keepalive	Enable the gateway to send the DPD messages to the peer. DPD is a keepalive scheme that allows the router to query the liveliness of its Internet Key Exchange (IKE) peer. Specify the number of seconds between DPD messages in the DPD Keepalive field. The range is from 10 to 3600 seconds.
Dead Peer Detection Retry	Specify the number of seconds between retries if the DPD messages fail in the DPD Retry. The range is from 2 to 60 seconds.

Step 8 Click:

- **Save** to save the configuration.
- **Refresh** to refresh the page.

IPsec Profile

The IPsec profiles, also called ISAKMP profiles, enable you to define a set of IKE parameters that you can associate with one or more IPsec tunnels. An IPsec profile applies parameters to an incoming IPsec connection identified uniquely through its concept of match identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, Fully Qualified Domain Name (FQDN), and group (the Virtual Private Network (VPN) remote client grouping).

Creating, Editing, and Deleting IPsec Profile

The IKE Profile feature allows you to create, edit, and delete the IPsec Profile.

To create, edit, or delete the IPsec Profile, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select a device or click **Add** to add a new device, and then configure the device. The device details appear on the lower part of the screen.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then choose **VPN Components > IPsec Profile**.
- Step 5** Click the **Add Row** button to create the IPsec profile.
- Step 6** In the IPsec Profile page, enter the information such as Name, Description, and Transform Set, and the IPsec SA Lifetime.

**Note**

When you edit a profile, you cannot edit the name of the IPsec profile. A transform set represents a certain combination of security protocols and algorithms. During the IPsec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform describes a particular security protocol with its corresponding algorithms

- Step 7** Enter the IPsec SA Lifetime in seconds to establish a new SA after the set period of time elapses.
- Step 8** To edit the IPsec profile parameters, click on the **Field** and edit the parameter of that IPsec profile.

Step 9 To delete the IPsec profile, select the IPsec Profile from the list, and click the **Delete** button.

Step 10 Click:

- **Save** to save the configuration.
 - **Cancel** to exit without saving your changes.
 - **Save** again to generate the CLI commands.
-

Pre-shared Keys

The Pre-shared Keys feature allows you to share a secret key between two peers and will be used by the IKE during the authentication phase.

Creating, Editing, and Deleting Pre-shared Keys

To create, edit, or delete the pre-shared keys, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select a device or click **Add** to add a new device, and then configure the device. The device details appear on the lower part of the screen.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Security** folder, and then choose **VPN Components > Pre-Shared Keys**.
 - Step 5** Click the **Add Row** button to create the pre-shared key.
 - Step 6** In the Pre-Shared Keys page, enter the IP Address, Host Name, Subnet Mask, and Pre-Shared Keys.
 - Step 7** To edit the pre-shared key parameters, click on the **Field** and edit the parameter of that pre-shared key.
 - Step 8** To delete the pre-shared key, select the pre-shared key from the list, and click the **Delete** button.
 - Step 9** Click:
 - **Save** to save the configuration.
 - **Cancel** to exit without saving your changes.
 - **Save** again to save the configuration and generate the CLI commands.
-


RSA Keys

An RSA key pair consists of a public key and a private key. When setting up your Public Key Infrastructure (PKI), you must include the public key in the certificate enrollment request. After the certificate is granted, the public key will be included in the certificate so that the peers can use it to encrypt the data that is sent to the router. The private key is kept on the router and used for both to decrypt the data sent by the peers and to digitally sign transactions when negotiating with the peers.

The RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

Creating, Importing, Exporting, and Deleting RSA Keys

To create, export, import, or delete the RSA keys, follow these steps.


-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select a device or click **Add** to add a new device, and then configure the device. The device details appear on the lower part of the screen.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then choose **VPN Components > RSAKeys**.
- Step 5** Click the **Add Row** button to create the RSA Keys.
- Step 6** The Add RSA Keys dialog box appears.
- Step 7** In the Add RSA Keys dialog box, enter the Label, Modulus, and Type.
-
-  **Note** For a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer. The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with a large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.
-
- Step 8** Check the Make the Key exportable check box to generate the RSA as a exportable key.
- Step 9** Click:
- **OK** to save the configuration.
 - **Cancel** to exit without saving your changes.
- Step 10** To import the RSA key, click the **Import** button. The Import RSA Key dialog box appears.
- Step 11** In the Import RSA Key dialog box, enter the label of the RSA key, Key type, and password to decrypt the key. If the key type is general-keys, signature or encryption, copy and paste the public and private key data that was saved.
- Step 12** To import usage-key, enter the public and private key data of both the signature and encryption keys.
- Step 13** Click:
- **Import** to import the RSA key.
 - **Close** to exit without saving your changes.
- Step 14** To export the RSA key, select the RSA key from the list and click the **Export** button. The Export RSA Key Pair dialog box appears.
- Step 15** In the Export RSA Key Pair dialog box, enter the password to encrypt the RSA key and choose the encryption algorithm from the drop-down list.
- Step 16** Click:
- **OK** to display the exported keys.
 - **Cancel** to exit without saving your changes.
- Step 17** To delete the RSA key, select the RSA key from the list, and click the **Delete** button.
-

Transform Sets

A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to Upset protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Creating, Editing, and Deleting Transform Sets

To create, edit, or delete the transform sets, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select a device or click **Add** to add a new device, then configure the device. The device details appear on the lower part of the screen.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Security folder**, and then choose **VPN Components > Transform Sets**.
- Step 5** Click the **Add Row** button to create the transform sets.
- Step 6** In the Transform Sets page, enter the Name and select the acceptable combination of security protocols and algorithm to configure the transform set.
-
-  **Note** The ESP encryption algorithm is used to encrypt the payload and the integrity algorithm is used to check the integrity of the payload.
-
- Step 7** Specify the mode for a transform set. The options are: Tunnel mode or Transport mode.
- Transport—Encrypt data only. Transport mode is used when both endpoints support IPsec. Transport mode places the authentication header or encapsulated security payload after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets.
 - Tunnel—Encrypt data and IP header. Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as a router to act as an IPsec proxy for multiple VPN users; tunnel mode should be used in those configurations.
- Step 8** To edit the Transform sets parameters, click on the **Field** and edit the parameter of that transform sets.
- Step 9** To delete the transform set, select the transform set from the list, and click the **Delete** button.
- Step 10** Click:
- **Save** to save the configuration.
 - **Cancel** to exit without saving your changes.
 - **Save** again to save the configuration changes.
-

Overview of Zones

The Zone Based Firewall (ZBFW) feature allows users to easily manage Cisco IOS unidirectional firewall policy between groups of interfaces known as zones.

A zone is a group of interfaces that have similar functions or features. For example, on a router, Gigabit Ethernet interface 0/0/0 and Gigabit Ethernet interface 0/0/1 may be connected to the local LAN. These two interfaces are similar because they represent the internal network, so they can be grouped into a zone for firewall configurations.

By default, the traffic between interfaces in the same zone is not subjected to any policy. The traffic passes freely. Firewall zones are used for security features.

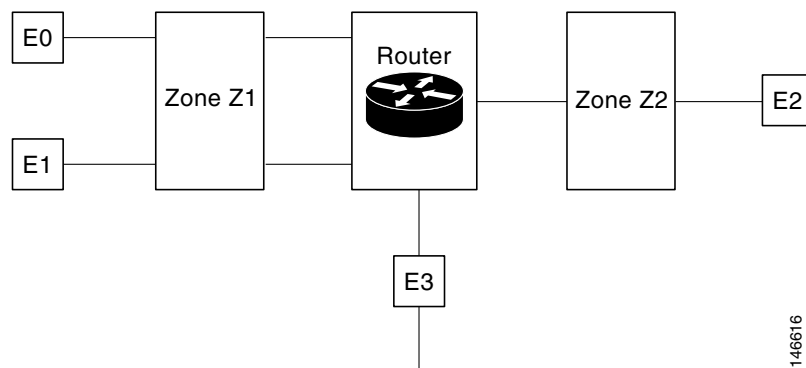
Security Zones

A security zone is a group of interfaces to which a policy can be applied. Grouping interfaces into zones involves the following two procedures:

- Creating a zone so that the interfaces can be attached to it.
- Configuring an interface as a member of a given zone.

By default, the traffic flows among the interfaces that are members of the same zone. When an interface is a member of a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped. To permit the traffic to and from a zone-member interface, you must make that zone part of a zone pair, and then apply a policy to that zone pair. If the policy permits the traffic (through inspect or pass actions), traffic can flow through the interface.

Figure 4-1 Security Zone Diagram



- Interfaces E0 and E1 are members of the security zone Z1.
- Interface E2 is a member of the security zone Z2.
- Interface E3 is not a member of any of the security zone.

In this scenario, the following situations exist:

- Traffic flows freely between the interfaces E0 and E1 because they are members of the same security zone (Z1).
- If no policies are configured, traffic will not flow between interfaces (for example, E0 and E2, E1 and E2, E3 and E1, and E3 and E2).
- Traffic can flow between E0 or E1 and E2 interfaces only when an explicit policy is configured to permit the traffic between the zone Z1 and zone Z2.
- Traffic can never flow between E3 and E0/E1/E2 interfaces because E3 is not a part of any security zone.

The following topics provide more information:

- [Managing Applications, page 4-102](#)
- [Managing Default Parameters, page 4-110](#)
- [Managing Interfaces, page 4-110](#)
- [Managing Policy Rules, page 4-104](#)
- [Creating Security Zone, page 4-108](#)
- [Creating Security Zone, page 4-108](#)

Managing Applications

This feature allows you to assign or un-assign the Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) ports to an application.



Note

When you click the **Save** or **Delete** button, the changes are deployed on the device. You cannot review the requested operation and also, you cannot remove the operation request from the pending changes queue. The CLI changes that starts with “EMS_” is not supported and may cause unexpected behavior.

Editing Port Application Mapping

To assign or un-assign the TCP/UDP ports to an application, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Zone Based Firewall** folder, expand the **Common Building Block** subfolder, and then click **Port Applications Mapping**. The Port Application Mapping page appears.



Note

Displays the application name that is driven from the device.

-
- Step 5** To assign or unassign the TCP/UDP ports to an application, click on the application and update its TCP/UDP ports value. The TCP/UD Port values are assigned to the specific application.
 - a. Assign port(s) by defining one or more ports separated by comma (For example: 1234, 2222 and so on).
 - b. Assign port(s) by defining the port range (For example: 1111-1118). You can also assign a group of ports or port range.
 - c. Unassign port(s) by deleting the existing port values.
 - Step 6** Click **Save** to save the configurations.
-

Managing Services

This feature allows you to create, update or delete the service element.

Creating Services

To create the services, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Zone Based Firewall** folder, expand the **Common Building Block** subfolder, and then click **Services**. The Service page appears.
 - Step 5** In the Service page, click the **Add Service** button to create a new service.
 - Step 6** In the Service page, enter the Service Name. You cannot change the name after creating the service. Also, you cannot create a service without an application.
 - Step 7** To assign Applications, click the down arrow icon. The Applications Object Selector dialog box appears.
 - a. In the Applications dialog box, check the Applications check box to select the applications from the list (can be multiple selection).
 - b. Click **OK** to accept the changes or **Cancel** to cancel the changes.
 - Step 8** Click **Save** to apply your changes to the device.
-

Editing Service

To edit the existing service, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Zone Based Firewall** folder, expand the **Common Building Block** subfolder, and then click **Services**.
 - Step 5** In the Service page:
 - a. Click on the Service parameters row and edit the parameters. or
 - b. Select the service, and click the **Edit** button. The selected Service entity opens for editing. You can add new applications or remove an already selected application.
 - c. To remove an application from the selected list, rest your cursor on the application name, and click the **X** icon.
 - Step 6** Click **Save** to save the configuration.
-

Deleting the Service

To delete the existing service, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.

- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Zone Based Firewall** folder, expand the **Common Building Block** subfolder, and then click **Services**.
 - Step 5** From the Service page, select the service, and then click the **Delete** button.
 - Step 6** Click **OK** on the warning message to delete the service. The selected service is deleted.
-

Managing Policy Rules

The policy rule section allows you to create a new firewall policy rule, change the existing policy rule, delete the policy rule, and change the policy rule order. When you create the firewall policy rule, it is up to you to define the location in the policy table.

Creating Policy Rules

To create the policy rules, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Zone Based Firewall** folder, expand the **Security** subfolder, and then click **Policy Rules**. The Firewall Rules page appears.
 - Step 5** From the Firewall Rules page, click the **Add Rule** button and complete the fields. The source zone and the destination zone must be different.
 - Step 6** To move the rules, click on the down arrow icon on the **Add Rule** button. You can place the selected rule at the top of the list or bottom of the list or move the selected rule after or before a rule in the table.



Note

The name field is optional. If you do not provide the name for the firewall rule, the system generates a name for the firewall rule. You cannot use these formats *rule_<number>* or *EMS_rule_<number>* to create the firewall rule name (For example, *rule_1*). These are system reserved formats.

-
- Step 7** To add the source and the destination IP address, click the **add** icon. The Source/Destination IP address dialog box appears.
 - a. From the Source/Destination IP address dialog box, check the **Any** check box to set the value to any.
 - a. Enter the source/ destination IP addresses.
 - b. Click the **Add** button to add the new IP address and the subnet.
 - c. Click **Delete** to delete the existing value.
 - d. Click **OK** to save the configurations.
 - e. Click **Cancel** to cancel all the changes you have made without sending them to the router.
 - Step 8** Set the Service values. To add or remove the Application, click the down arrow icon. The Firewall Service dialog box appears.
 - a. In the Firewall Service dialog box, check the Application check box to select the application to inspect.

- b. To select an ACL Based Application, select either the TCP or UDP or ICMP application.
 - c. To select an interface,
 - d. Use the navigation arrow buttons to navigate forward and backward.
 - e. Click **OK** to save the configurations.
- Step 9** Select the appropriate action. The options are: **Drop**, **Drop and Log**, **Inspect**, **Pass**, and **Pass and Log**.
- Step 10** If you select the action to inspect, click the **Configure** button in the Advance options column. The Advanced Parameters Configuration dialog box appears.
- Step 11** In the Advanced Parameters Configuration dialog box, do the following:
- a. To customize the device default value, check the Parameter box and set the new value.
 - b. To apply the device default value, uncheck the Parameter box.
 - c. To view the firewall rule default parameters, see [“Managing Default Parameters” section on page 4-110](#).
 - d. When you rest your cursor on the Advanced Options icon, the configured parameters will be displayed in the quick view window.

[Table 4-9](#) lists the elements on the policy rule page.

Table 4-9 Policy Rule Page

Element	Description
Name	(Optional) Enter a name for the policy rule.
Source Zone	Enter the name of the source zone. The source zone specifies the name of the zone from which the traffic is originating.
Destination Zone	Enter the name of the destination zone. The destination zone specifies the name of the router to which the traffic is bound to.
Source	Enter the source IP address of the inspected data. The valid parameters are: <ul style="list-style-type: none"> Any IP Address Subnet
Destination	Enter the destination IP address of the inspected data. The valid parameters are: <ul style="list-style-type: none"> Any IP Address Subnet
Service	The service of the inspected data. The valid parameters are: <ul style="list-style-type: none"> L3/4 Applications, see “Managing Applications” section on page 4-102 Services “Creating Security Zone” section on page 4-108 ACL Based application: TCP, UDP, ICMP

Table 4-9 Policy Rule Page (continued)

Element	Description
Action	<p>Choose the action to perform on the traffic when there is a match on Rule condition. The rule matches when:</p> <ul style="list-style-type: none"> • The traffic Source IP matches the Source Rule condition. • The traffic Destination IP matches the Destination Rule condition and the traffic inspected Service matches the Service Rule condition. <p>The action options are:</p> <ul style="list-style-type: none"> • Drop • Drop and Log • Inspect • Pass • Pass and Log
Advance Options	Specify the configuration parameters to set the Firewall Rule Parameter-Map behavior when the Action option is set to Inspect.

Step 12 Click **Save** to apply the rule to the device.

Monitoring Policy Rules

To monitor Policy Rules, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Zone Based Firewall** folder, expand the **Security** subfolder, and then click **Policy Rules**. The Firewall Rules page appears.
- Step 5** In the Firewall Rules page, click **Hit Counters** and use the options to analyze the sessions and packets of the selected rules.
- Step 6** Click the **Show all** option to view the packets and sessions counters. The packets and sessions counters are displayed in two separate columns. The packet counters are used to analyze the pass/drop rules and sessions counters are used for the inspect rules.



Note

When you select the **Show all** option, the system will display a warning message stating that it may take more time to complete this operation.

- Step 7** To know the time of the last update for the rules, hover the mouse over the column names or click the **Last Update Time** option in the Hit Counters. You can refresh the Hit counters for a specific rule or for all the selected rules. This option is enabled when you select the “Show for selected rules” option.
- Step 8** Use the pre-defined filters options to display the rules at the top or bottom based on the packets/sessions counts.

- Step 9** Click the **Reset All Counters** to discard all the rules counters. The application will display a warning message before resetting the rules counters.
-

Editing Policy Rule

To edit the existing Policy Rule, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Zone Based Firewall folder**, expand the **Security** subfolder, and then click **Policy Rules**.
- Step 5** In the Firewall Rules page, choose one of the following options:
- Click on the Rules parameters row and edit the parameters.
 - Check the check box to select the rule, and then click the **Edit** button. The selected Rule opens for edit. You cannot edit the name of the policy rule.
- Step 6** Click **Save** to apply the changes in the device.
-

Deleting the Policy Rule

To delete the existing Policy Rule, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Zone Based Firewall folder**, expand the **Security** subfolder, and then click **Policy Rules**.
- Step 5** In the Firewall Rules page, check the check box to select the rules, and then click the **Delete** button.
- Step 6** Click **OK** on the warning message to delete the policy rule. The selected policy rule is deleted from the device.
-

Changing the Firewall Rule Order

The class-default rules always appear at the bottom of the list and their location is fixed. The regular rules cannot be moved beneath the class-default rules.

To change the Policy Rule order, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Zone Based Firewall folder**, expand the **Security** subfolder, and then click **Policy Rules**.

- Step 5** In the Firewall Rules page, to move the rule to a specific row, drag and drop the rule to the new location.
-

Creating Security Zone

To create the security zone, follow these steps,



Note

The Zone Based Firewall feature is supported on ASR platform from the IOS version 3.5 or later. The Zone Based Firewall feature is supported on ISR platform from the IOS release 12.4(24)T or later.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Zone Based Firewall** folder, expand the **Security** subfolder, and then click **Zones**.
- Step 5** Click the **Add Zone** button to create the security zone.
- Step 6** In the security zone page, enter the Zone Name.
- Step 7** Select the VRF of the zone.
- VRF selection will affect the interface that can be assigned to the security zone.
 - If the user selects the default VRF option, then the security zone can be assigned only to the interfaces that are not related to any other VRF.
- Step 8** To assign the interfaces to the security zone, click the down arrow icon. The Interface Object Selector dialog box appears.
- In the Interface selector dialog box, check the Interface check box to select the interface from the list (can be multiple selection).
 - Click **OK** to save the configuration.
 - Click **Cancel** to cancel all the changes you have made without sending them to the router.
- Step 9** In the Advance options column, click the **Configure** button. The Advanced Parameters Configuration dialog box appears.
- Step 10** In the Advanced Parameters Configuration dialog box, do the following:
- Check the Alert check box and click the **On** radio button to set the alert.
 - Check the Maximum Detection check box to set the maximum detection.
 - Check the TCP SYN-Flood Rate per Destination check box to set the TCP flood rate.
 - Check the Basic Threat Detection Parameters check box and click the **On** radio button to configure the FW drop threat detection rate, FW inspect threat detection rate, and FW SYN attack threat detection rate.
- Step 11** Click:
- OK** to save configuration.
 - Cancel** to exit without saving.
- Step 12** To edit the existing security zone parameters, select the zone, and click the **Configure** button on the Advance options column. The Advanced Parameters Configuration dialog box appears.

- Step 13** In the Advanced Parameters Configuration dialog box, edit the values and click **Save** to save the changes. When you rest your cursor on the Advanced Options icon, the configured parameters will be displayed in the quick view window.



Note By default, the Advanced configurations parameters are disabled.

- Step 14** Enter the description for the zone.

- Step 15** Click:

- **Save** to save the changes.
- **Cancel** to exit without saving.

Editing Security Zone

To edit the existing security zone, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Zone Based Firewall folder**, expand the **Security** subfolder, and then click **Zones**.
- Step 5** In the Security Zone page, choose one of the following options:
- a. Click on the Zone parameters row, and edit the parameters. or
 - b. Select the zone, and click the **Edit** button. The selected Zone entity opens for editing.
- Step 6** Click the **add** icon to assign the interface to the zone or to un-assign the existing interfaces from the zone. You can also change the Description of the zone.
- Step 7** Click **Save** to save the configuration.

Deleting the Security Zone

To delete the existing security zone, follow these steps.

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Zone Based Firewall folder**, expand the **Security** subfolder, and then click **Zones**.
- Step 5** In the Security Zone page, select the security zone, and then click the **Delete** button.
- Step 6** Click **OK** on the warning message to delete the security zone. The selected zone is deleted.

Configuring Default-Zone

To configure the default zone, follow these steps.



Note

The Default-Zone feature is supported only on ASR platform.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Zone Based Firewall folder**, expand the **Security** subfolder, and then click **Zones**.
 - Step 5** In the Security Zone page, click the **Default Zone** button to enable or disable the default security zone in the device. The device will host all the interfaces that are not related to any zone.
 - Step 6** Click **OK** to save the configuration.
-

Managing Default Parameters

To change the Default Parameters Map, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Zone Based Firewall folder**, expand the **Security** subfolder, and then click **Default Parameters Map**.
 - Step 5** From the Default Parameters Map page, change the parameters map value.



Note

You can change the default parameters only on ISR devices.

-
- Step 6** Click **Save** to save the configuration.
-

Managing Interfaces

A virtual interface is a logical interface configured with generic configuration information for a specific purpose or configured for a common to specific users. The zone member information is acquired from a RADIUS server, and then the dynamically created interface is made as a member of that zone.

Configuring Interfaces

To assign the interfaces to the zone and un-assign the interface from a specific zone, follow these steps.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add** to create a new device, then configure the device.

- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Zone Based Firewall folder**, expand the **Security** subfolder, and then click **Interfaces**.
- Step 5** In the Interface page, select the interface you want to change and click the down arrow icon. The Zone dialog box appears.
- Step 6** In the Zone dialog box, select the new security zone for the interface. If the selected interface is already assigned to a zone, you will get a warning message.
- Step 7** Click **Yes** on the warning message if you want to change the assignment of that interface.
- Step 8** To un-assign the interface from the specific zone, select the interface and delete the zone information.
- Step 9** Click:
- **Save** to save and apply your changes.
 - **Cancel** to exit without saving.
-

Routing

A Routing protocol specifies how routers communicate with each other in a network, select their routing paths between two nodes on a computer network to transmit data, and how network information can be shared with each other.

Prime Infrastructure supports the following routing protocols:

- [“Static Routing” section on page 4-111](#)
- [“RIP Routing” section on page 4-112](#)
- [“EIGRP Routing” section on page 4-113](#)
- [“OSPF Routing” section on page 4-114](#)

Static Routing

Static routing is the simplest form of routing, where the network administrator manually enters the routes into the routing table of the router. The route does not change until the network administrator changes it. Static routing is normally used when there are very few devices to be configured and the administrator is very sure that the routes do not change. The main drawback of static routing is that a change in the network topology or a failure in the external network cannot be handled as the routes that are configured manually must be updated to fix any lost connectivity.

To create a static route, do the following:

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add Device** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Routing** folder, and then click **Static**. The Static Routing page appears with options to configure IPv4 and IPv6 static routes.
- Step 5** To configure an IPv4 static route, do the following:
- a. From the **IPv4 Static Routes** page, click **Add Row**, and then complete the fields.
For Permanent Route, choose:

- **True** to specify that the route will not be removed from the routing table, even if the next-hop interface shuts down or the next-hop IP address is not reachable.
- **False** to specify that the route will be removed from the routing table, even if the next-hop interface shuts down or the next-hop IP address is not reachable.

b. Click **Save**.

c. Click **Save** to save the configuration.

Step 6 To configure an IPv6 static route, do the following:

- a. From the **IPv6 Static Routes** page, click **Add Row**, and then complete the fields.



Note Effective from 1.2 release, only Unicast is supported for IPv6 static routes.

b. Click **Save**.

c. Click **Save** to save the configuration.

RIP Routing

Routing Information Protocol (RIP) is a distance-vector routing protocol, which uses the hop count as a routing metric. RIP implements a limit on the hop count (a maximum of 15 hop counts) allowed in a path from the source to a destination to prevent routing loops. This hop limit also limits the size of the networks that RIP can support. RIP sends its routing table every 30 seconds.

The most popular variants of RIP are RIP version 1 (described in RFC1058) and RIP version 2 (described in RFC2453). RIP uses the split horizon, route poisoning, and holddown mechanisms to prevent incorrect routing information from being propagated.

To create a RIP route, do the following:

Step 1 Choose **Operate > Device Work Center**.

Step 2 Select the device from the list or click **Add Device** to create a new device, then configure the device.

Step 3 After selecting the device, click **Configuration**. The Feature Configuration panel appears.

Step 4 Expand the **Routing** folder, and then click **RIP**. The RIP Routing page appears with options to configure IPv4 and IPv6 RIP routes.

Step 5 To configure an IPv4 RIP route, do the following:

- From the **IPv4 RIP Routes** page, select the RIP version.
- Click **Add Row**, and then complete the fields.
- Click **Save**.
- Click **Passive Interface** to select the passive interface you want to add.
- Click **Save** to save the configuration.

- Step 6** To configure an IPv6 RIP route, do the following:
- From the **IPv6 RIP Routes** page, click **Add Row**, and then complete the fields.
 - Click **Save**.
 - Choose **Add/Remove Interfaces** to add or remove an interface from your routing domain (AS number).
 - Click **Save** to save the configuration.
-

EIGRP Routing

EIGRP is an enhancement of the Interior Gateway Routing Protocol (IGRP). In EIGRP, when an entry in the routing table changes in any of the routers, it notifies its neighbors only of the change rather than sending the entire routing table. Every router in the network sends a “hello” packet periodically so that all routers on the network understand the state of its neighbors. If a “hello” packet is not received from a router during a certain period of time, it is assumed that the router is inoperative.

EIGRP uses the Diffusing Update Algorithm (DUAL) to determine the most efficient route to a destination and provides a mechanism for fast convergence. Routers using EIGRP and IGRP can interoperate because the routing metric used with one protocol can be easily translated into the routing metric of the other protocol.

To create an EIGRP route, do the following:

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Select the device from the list or click **Add Device** to create a new device, then configure the device.
- Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
- Step 4** Expand the **Routing** folder, and then click **EIGRP**. The EIGRP Routing page appears with options to configure IPv4 and IPv6 EIGRP routes.
- Step 5** To configure an IPv4 EIGRP route, do the following:
- From the **IPv4 EIGRP Routes** page, click **Add Row**, and then complete the fields.
 - Click **Save**.
 - Click **Add Interface** to select the passive interface you want to associate to the Autonomous System (AS) number created.
 - Click **Save** to save the configuration.
- Step 6** To configure an IPv6 EIGRP route, do the following:
- From the **IPv6 EIGRP Routes** page, click **Add Row**, and then complete the fields.
 - Click **Save**.
 - Choose **Add/Remove Interfaces** to add or remove an interface associated with the AS number you created.
 - Click **Save** to save the configuration.
-

OSPF Routing

Open Shortest Path First (OSPF) is a standards-based routing protocol that uses the Shortest Path First (SPF) algorithm to determine the best route to its destination. OSPF sends Link State Advertisements (LSAs) to all other routers within the same area. OSPF only sends routing updates for the changes, and does not send the entire routing table.


To create an OSPF route, do the following:

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device from the list or click **Add Device** to create a new device, then configure the device.
 - Step 3** After selecting the device, click **Configuration**. The Feature Configuration panel appears.
 - Step 4** Expand the **Routing** folder, and then click **OSPF**. The OSPF Processes page appears with options to configure IPv4 and IPv6 OSPF processes.
 - Step 5** To configure an IPv4 OSPF process, do the following:
 - a. From the **IPv4 OSPF Processes** page, click **Add Row**, and then complete the fields.
 - b. Click **Save**.
 - c. Click **Passive Interfaces** to select the passive interface you want to associate to the process created.
 - d. Click **Advanced**. The Advanced OSPF IPv4 Configuration dialog box appears.
 - e. Click **Networks > Add Row**, and then complete the fields.
 - f. Click **Route Summarization > Add Row**, and then complete the fields.
 - g. Click **OK**.
 - h. Click **Save** to save the configuration.
 - Step 6** To configure an IPv6 OSPF process, do the following:
 - a. From the **IPv6 OSPF Processes** page, click **Configure**.
 - b. Click **Add Row**, and then complete the fields.
 - c. Click **Save**.
 - d. Click **Advanced**. The Route Summarization dialog box appears.
 - e. Click **Add Row**, and then complete the fields.
 - f. Click **OK**.
 - g. Click **Enable**, and then complete the fields.
 - h. Click **Save** to save the configuration.
-

Creating Composite Templates

You create a composite template if you have a collection of existing feature or CLI templates that you want to apply collectively to devices. You specify the order in which the templates contained in the composite template are applied to devices.

If you have multiple similar devices replicated across a branch, you can create and deploy a “master” composite template to all the devices in the branch. This master composite template can also be used later when you create new branches.

-
- Step 1** Choose **Design > Templates > Configuration**, then click **Composite Template**.
- Step 2** Enter parameters for the composite template.
- Step 3** From the Validation Criteria drop-down list, choose the devices to which all of the templates contained in the composite template apply. For example, if in your composite template you have a template that applies to Cisco 7200 Series routers and another that applies to all routers, choose the Cisco 7200 Series routers in the Device Type drop-down menu.
-  **Note** If a device type is grayed out, the template cannot be applied on that device type.
-
- Step 4** Under Template Details, choose the templates to include in the composite template.
- Step 5** Using the arrows, put the templates in the composite into the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the interface template.
- Step 6** Click **Save as New Template**.
- Step 7** Navigate to the My Templates folder and choose the template you just saved.
- Step 8** Click **Publish** to publish the template so it can be deployed.
- Step 9** Click **Deploy** on the template you published.
- Step 10** Specify the deployment options as explained in [Creating Wireless Controller Templates](#).
- Step 11** Click **OK**.
- Step 12** Choose **Administration > Jobs Dashboard** to verify the status of a template deployment.
-

Testing and Troubleshooting Configuration Templates

The most common reasons that a template might not be deployed are:

- One or more devices are unreachable—Verify that the device credentials are correct; ping the device to verify that it is reachable. (See [Getting Device Details Using the 360° View](#) for more information.)
- A device CLI returned an error because the CLI was incorrect—Verify that the CLI commands contained in the template are correct by running the commands on a test device.

After you create a new template, you should deploy it to one device only to verify that it works as designed. After you test that your configuration template is working on a single device, you can deploy it to multiple devices as necessary.



CHAPTER 5

Designing Monitoring Configurations

You use monitoring templates to enable Prime Infrastructure to monitor router and switch metrics such as CPU and memory utilization statistics and alert you of changing conditions before any issues can impact operation.

[Table 5-1](#) describes the process for creating and deploying monitoring templates.

Table 5-1 Steps for Using Monitoring Templates

Task	Additional Information
1. Create a template.	Under the Design menu, choose which type of template to create.
2. Deploy the template.	Under the Deploy menu, choose which template to deploy. See Designing Monitoring Configurations for more information.
3. Verify the status of the template deployment.	Choose Administration > Jobs Dashboard to verify the status of the template deployment.

Prime Infrastructure provides the following types of monitoring templates:

- Device Health—See [Creating Health Monitoring Templates, page 5-1](#).
- Interface Health—See [Creating Health Monitoring Templates, page 5-1](#).
- Threshold—See [Defining Thresholds, page 11-4](#).
- SNMP Polling—See [Designing Custom SNMP Monitoring Templates, page 5-4](#)

Creating Health Monitoring Templates

You use health monitoring templates to enable Prime Infrastructure to monitor network device metrics such as CPU and memory utilization statistics and alert you of changing conditions before the issues impact their operation.

To create a template to monitor overall device health:

- Step 1** Choose **Design > Monitoring Configuration**.
- Step 2** Expand **Features**, then **Metrics**, then click **Device Health** or **Interface Health**.
- Step 3** Enter the basic template information.
- Step 4** Under Template Content, choose the parameters to monitor. To change a parameter, click the parameter name, description, or polling frequency value and change the field.

- Step 5** Click **Save**.
- Step 6** Click **Save As New Template**.
- Step 7** You can now deploy the template under **Deploy > Monitoring Deployment**. See [Deploying Templates](#) for more information.

Health Monitoring Template Metrics

For the following health monitoring templates under **Design > Monitoring Configuration > Features > Metrics**, Prime Infrastructure polls SNMP objects in order to gather monitoring information:

- Device Health—[Table 5-2](#) describes the device health parameters polled.
- Interface Health—[Table 5-3](#) describes the interface parameters polled.
- Class Based Quality of Service—[Table 5-4](#) describes the QoS parameters. polled.

For the following monitoring templates that provide assurance information, data is collected through NetFlow or NAMs:

- Application
- NAM Health
- Traffic Analysis
- Voice Video Data
- Voice video Signaling

Table 5-2 *Device Health Monitoring Metrics*

Metric	Devices Polled	MIB	MIB Objects Included
Device Availability	All SNMP devices	SNMPv2-MIB	sysUpTime
CPU Utilization	IOS devices, Nexus 7k	CISCO-PROCESS-MIB	cpmCPUTotalPhysicalIndex cpmCPUTotal1minRev
Memory Pool Utilization	IOS devices	CISCO-MEMORY-POOL-MIB ciscoMemoryPoolUsed / (ciscoMemoryPoolUsed + ciscoMemoryPoolFree)) * 100	CiscomemoryPooltype CiscomemoryPoolName ciscoMemoryPoolUsed CiscomemoryPoolFree
	Nexus 7K	CISCO-MEMORY-POOL-MIB (cempMemPoolUsed / (cempMemPoolUsed + cempMemPoolFree)) * 100	
Env Temp	ASR, Nexus 7k	CISCO-ENVMON-MIB	entSensorValue
	Cat2k,3k,4k,6k,ISR	CISCO-ENVMON-MIB	ciscoEnvMonTemperatureStatusValue

Table 5-2 *Device Health Monitoring Metrics*

Metric	Devices Polled	MIB	MIB Objects Included
Largest Free Buffer Percentage	IOS devices	CISCO-MEMORY-POOL-MIB	ciscoMemoryPoolLargestFree ciscoMemoryPoolFree
Total Number of Buffer Misses	IOS devices	OLD-CISCO-MEMORY-MIG	bufferSmHit, bufferMdHit, bufferBgHit, bufferLgHit, bufferHgHit, bufferSmMiss, bufferMdMiss, bufferBgMiss, bufferLgMiss, bufferHgMiss

Table 5-3 *Interface Health Monitoring Metrics*

Metric	Devices Polled	MIB	MIB Objects Included
Interface Availability	IOS devices, Nexus 7K	IF-MIB	ifOperStatus ifOutOctets ifHighSpeed ifInOctets if InErrors ifOutErrors ifInDiscards ifOutDiscards
Input Broadcast Packet Percentage	IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifInErrors, ifInDiscards, ifInUnknownProtos ifHCInBroadcastPkts, ifHCInMulticastPkts
Input Queue Drop Percentage	IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifHCInUcastPkts, ifInDiscards, ifInUnknownProtos, locIfInputQueueDrops
Output Queue Drop Percentage	IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCOutBroadcastPkts, ifHCOutMulticastPkts, ifHCOutUcastPkts, ifOutDiscards, ifOutUnknownProtos, locIfOutputQueueDrops

Table 5-4 *Class Based Quality of Service Health Monitoring Metrics*


Metric	Devices Polled	MIB	MIB Objects Included
QOS calculation		CISCO-CLASS-BASED-QOS-MIB	cbQosCMDropByte64 cbQosCMPostPolicyByte64 cbQosCMPrePolicyByte64

Defining Monitoring Thresholds

You use monitoring templates to define thresholds. When the thresholds you specify are reached, Prime Infrastructure issues an alarm.

You must first create an Interface Health Monitoring template under **Design > Monitoring Configuration > Features > Metrics** before you can define threshold values related to health monitoring.

To define thresholds:

-
- Step 1** Choose **Design > Monitoring Configuration**.
 - Step 2** Under Features, choose **Threshold**.
 - Step 3** Complete the basic template fields.
 - Step 4** Under Feature Category, choose one of the following metrics:
 - Device Health—Allows you to change threshold values for CPU utilization, memory pool utilization, and environment temperature.
 - Interface Health—Allows you to change threshold values for the number of outbound packets that are discarded.
 - Step 5** From the Template Instance menu, select a default template or a previously created template.
- 

Note If there is no default template for the Feature Category you selected, you must first create the necessary template under **Design > Monitoring Configuration > Features > Metrics** before you can define threshold values.
-
- Step 6** Under Metric Parameters, select the parameter for whose threshold you want to change, then click **Edit Threshold Setting**. The list of parameters displayed corresponds to the parameters that were included when the monitoring template was created, or if you are using a default template, all available parameters are displayed.
 - Step 7** Enter a new value and choose the alarm severity for the threshold.
 - Step 8** Click **Done**.
 - Step 9** Click **Save as New Template**.
 - Step 10** You can now deploy the template under **Deploy > Monitoring Deployment**. See [Deploying Templates](#) for more information.
-

Designing Custom SNMP Monitoring Templates

Prime Infrastructure allows you to design custom SNMP polling templates to monitor third-party devices and device groups. You can also use these templates for Cisco devices and device groups. You can upload the SNMP MIB for the device type, then choose devices and attributes to poll and the polling frequency. You can upload one MIB, or a package of MIBs in a ZIP file. You deploy the custom SNMP polling template the same way as other monitoring templates, and you can display the results in the form of a line chart or a table. This feature enables you to easily repeat polling for the same devices and attributes, and can be used to customize the way Cisco devices are polled using SNMP.

To create a custom SNMP polling template:

-
- Step 1** Choose **Tools > Custom SNMP Template**.
- Step 2** On the Basic tab, make entries for the following:
- Name—Name of the custom SNMP template.
 - MIBs—Select a MIB from the list. If you want to use a new MIB, click **UploadMIB** to browse for the MIB file you want to use. You can upload a single MIB file, or a group of MIBs with their dependencies as a zip file. Specify a filename extension only if you are uploading a zip file.
 - Tables—Choose the table you want to poll from the list of tables supported in the MIB you selected. A list of attributes is displayed, based on the table type you selected. Choose the parameters that you want for your template.
- Step 3** If you want to edit the generated configuration file, click the **Advanced** tab and make your changes. It is usually useful to change the Display name and Description for the attributes. Be aware that the configuration file must remain a valid XML file after your changes.
- Step 4** Click **Save**.
- Step 5** On the Monitoring Template page, choose **Features > Custom SNMP** and select your new custom SNMP template.
- Step 6** Under Template Basics, make entries for the following:
- Name—Name of the design instance of your custom SNMP template.
 - Description.
 - Author Contact.
- Step 7** Under Template Content, select a polling frequency from the **Select Polling Frequency** drop-down menu.
- Step 8** Click **Save As New Template**.
-

Related Topic

- [Designing Custom SNMP Monitoring Templates](#)

Troubleshooting Monitoring Configurations

The most common reasons that a template might not be deployed are:

- One or more devices are unreachable.
- A device CLI returned an error because the CLI was incorrect.



CHAPTER 6

Designing Automated Deployment Profiles

Prime Infrastructure helps automate the deployment of new devices on the network. Prime Infrastructure obtains and applies the necessary software image and configuration on a new network device. By using the features such as Cisco Network Services (CNS) “call-home” and Cisco IOS “auto-install” (which uses Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP)), Prime Infrastructure reduces the time a new device takes to join the network and become functional.

Automated Deployment

The Automated Deployment feature of Prime Infrastructure allows you to create templates to define features and configurations that can be reused and applied to new devices. You can streamline new device deployment by creating templates, which define necessary initial configuration, to communicate with the Prime Infrastructure. You can specify (and *pre-deploy*) software images and configurations for the devices that will be added to the network in future.



Note

Before using the Prime Infrastructure Automated Deployment feature based on CNS, you should set up the Cisco Prime Plug and Play (PnP) gateway. For detailed information about setting up the Cisco Prime PnP gateway, see the “Setting Up the Plug and Play Gateway” section of the *Cisco Prime Infrastructure 1.2 Quick Start Guide*.



Note

Do not execute the **cns config retrieve** and **cns image retrieve** commands on a device that is added using the Automated Deployment feature.

For automated deployment, you must pre-provision software images and configurations using an automated deployment profile. There are two types of pre-provisioning:

- Device ID—Specify the hardware serial-ID or the unique device-ID (UDI) of the device on which the configurations need to be deployed.
- Device Type—Specify the type of device on which the configurations need to be deployed. This device type of pre-provisioning can be used for bulk provisioning of new devices.

Automated Deployment Process

For automated deployment, you must first create an automated remote deployment profile. Next, based on the automated deployment method, add a new device that have CNS capabilities to the network and apply a bootstrap configuration to activate the CNS agent on the device. This can be achieved by using any of the bootstrap delivery methods supported by the Prime Infrastructure, or by using your own mechanism. When you apply the bootstrap configuration, the device will use the “call-home” agent capabilities to connect to the Prime Infrastructure server and the automated deployment is initiated.

After the automated deployment is initiated, Prime Infrastructure server checks the serial number or device ID specified in the automated deployment profile of that device. If the serial number in the automated deployment profile matches one on the device, Prime Infrastructure adds the device to its inventory. Prime Infrastructure applies the software image and the configuration specified in the automated deployment profile on the device, and uses Prime Infrastructure features to manage the device.

To define the profiles for your devices, see [Automated Deployment Profile](#).

Automated Deployment Profile

Prime Infrastructure Automated Deployment feature allows you to perform an initial provisioning of a software image, and configuration on a new device.

Before creating an automated deployment profile, perform these tasks:

- [Creating Bootstrap Configuration Templates](#) using a CLI template
- (Optional) [Downloading Software Images](#)
- [Creating Configuration Templates](#)

Creating Bootstrap Configuration Templates

The bootstrap configuration template should have the minimum required CLI configurations, to enable the new device to communicate with the Prime infrastructure PnP gateway server.

To create a bootstrap configuration template for the CNS devices, perform these steps:

Step 1 Choose **Design > Configuration Templates**.

Step 2 Expand the **CLI Template folder**, then click **CLI**. For more information, see [Chapter 4, “Creating CLI Configuration Templates.”](#)

The CLI template should have these configurations for the device “call-home” agent to connect to the Prime Infrastructure PnP gateway server:

- IP reachability to the Prime Infrastructure PnP gateway server (if required).
- CNS configurations

The CNS configurations for the CNS-based deployment are:

- a. Device ID-based deployment

The device ID-based deployment configuration example is:

```
ip host <PnP Gateway server fully qualified host name> <IP address>
ip host <PnP Gateway server short hostname> <PnP Gateway IP address>
```

```

cns trusted-server all-agents <PnP Gateway server fully qualified host name>
cns trusted-server all-agents <PnP Gateway server short host name>
cns trusted-server all-agents <PnP Gateway IP address>
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns config partial <PnP Gateway server fully qualified host name> 80
cns event <PnP Gateway server fully qualified host name> keepalive 120 2
reconnect-time 60
cns config initial <PnP Gateway server fully qualified host name> 80
cns exec 80
cns image server http://<PnP Gateway server fully qualified host
name>/cns/HttpMsgDispatcher status http://<PnP Gateway server fully qualified host
name>/cns/HttpMsgDispatcher

```

b. Device Type-based deployment

The device type-based deployment configuration example is:

```

ip host <PnP Gateway server fully qualified host name> <PnP Gateway IP address>
ip host <PnP Gateway server short hostname> <PnP Gateway IP address>
cns trusted-server all-agents <PnP Gateway server fully qualified host name>
cns trusted-server all-agents <PnP Gateway server short host name>
cns trusted-server all-agents <PnP Gateway IP address>
cns id udi
cns id udi
cns id udi image
cns config partial <PnP Gateway server fully qualified host name> 80
cns event <PnP Gateway server fully qualified host name> keepalive 120 2
reconnect-time 60
cns config initial <PnP Gateway server fully qualified host name> 80
cns exec 80
cns image server http://<PnP Gateway server fully qualified host
name>/cns/HttpMsgDispatcher status http://<PnP Gateway server fully qualified host
name>/cns/HttpMsgDispatcher

```



Note

The **CNS ID udi** and **CNS config initial inventory** commands are supported from IOS release 12.3, or later.

If the device does not have CNS capabilities, automated deployment can be performed, based on the IP address. The automated deployment can be performed only if the device is directly reachable to the Prime Infrastructure server. Note that bulk provisioning (device type-based deployment) is not supported in this case. The bootstrap configuration required for this device is:

```

snmp-server enable traps config
snmp-server host <Prime Infrastructure IP> public snmp
snmp-server host <Prime Infrastructure IP> public udp-port 162

```



Note

The default Prime Infrastructure trap receiver port is 162.

Downloading Software Images

To download the images, perform these steps:

-
- Step 1** Choose **Operate > Software Image Management**.
 - Step 2** Click **Import**.
 - Step 3** Specify the source from where the software image is to be imported.
 - Step 4** Specify Collection Options and when to import the image file. You can run the job immediately or schedule it to run at a later time.



Note The image import job is non-repetitive.

- Step 5** Click **Submit**.
 - Step 6** To view the details of image management job, choose **Tools > Task Manager > Jobs Dashboard**.
-

Creating Configuration Templates

You can use one of these templates as the configuration template:

- CLI template (for more information, see [Chapter 4, “Creating CLI Configuration Templates.”](#))
- Composite template that has multiple CLI templates (for more information, see [Chapter 4, “Creating Composite Templates.”](#))

Creating Automated Deployment Profiles

Before creating automated deployment profiles, ensure you have satisfied the prerequisites sub-section of the [Automated Deployment Profile](#) section.

To create an automated deployment profile on new devices, perform these steps:

-
- Step 1** Select **Design > Automated Deployment Profiles**.
 - Step 2** Hover the mouse over PnP Profile Quick View icon, and click **New**.
 - Step 3** Select the Device Type of the new devices that can use this profile.



Note In bulk deployments, the devices use the same deployment profile with the same set of images and configurations. To use the deployment profile for specific device IDs, do not select the Device Type.

- Step 4** (Optional) Associate the bootstrap CLI template.
- Step 5** (Optional) Associate a software image and specify the flash location on the device where the image needs to be distributed.
- Step 6** (Optional) Associate the configuration template.
- Step 7** Click **Save as New PnP Profile**.

Step 8 Click:

- **Publish** to publish your profile and make it available for future deployment.
 - **Deploy** to create the pre-provisioning definition for the incoming devices. You can create multiple pre-provisioning definitions for one profile.
-

Deploying an Automated Profile

There are two types of deployment profiles:

- [Device ID-Based Deployment](#)
- [Device Type-Based Deployment](#)

Device ID-Based Deployment

To deploy the profile based on the device ID, perform these steps:

Step 1 Choose **Deploy > Automated Deployment Profiles**.

Step 2 From the PnP Profiles page, select the profile, and click **Deploy**.

Step 3 From the Device Provisioning Profiles page, click **Add** to deploy a new device.

**Note**

One profile may have multiple provisioning definitions that can be applied for different devices.

Step 4 Specify the hardware serial-ID or the UDI of the device.

Step 5 Specify these profile parameters:

- Bootstrap template properties
- Image properties:
 - Image location—By default, the location specified during the design phase is shown as the target location. If required, you can change this location.
 - Continue on Image Failure—Allows you to continue with the configuration deployment, even if the image is not successfully deployed.
 - Erase Flash—Allows you to erase the flash memory before distributing the image (This will erase the entire content of the flash).
 - Activate Image—Allows you to activate the new image on the device.
- Configuration template properties

Step 6 Specify these device management parameters:

- IP address— In CNS based deployment(s), if the IP address is not specified, the IP address that is given by the Prime Infrastructure PnP gateway is used for adding the device to the Prime infrastructure device inventory.
- SNMP
- SSH/Telnet

**Note**

When the network is secured by firewalls and NAT, the IP address given by the Prime Infrastructure PnP gatewayserver may not be the actual IP address of the device.

**Note**

Cisco Prime Infrastructure does not deliver any device management parameters onto the device. The device management parameters are used by Prime Infrastructure inventory to manage the device after the image and CLI configurations are applied. All configurations are performed only through the configuration templates in the profile.

Step 7 Click **OK**.

Step 8 Click **Close** to close the Device Provisioning Profiles page.

Device Type-Based Deployment

For a device type-based deployment, you do not have to associate the device ID with the deployment profile. Matching profiles are identified by the device type (PID) of the incoming device that is specified in the profile during the design phase.

The device type is matched hierarchically. The Prime Infrastructure searches for a profile with the same device type as that of the incoming device. If the profile does not match the device type, the Prime Infrastructure searches for a profile that is defined for a higher level of the device type in the hierarchy.

For example, if the 'switch_profile' in Prime Infrastructure is defined for 'Switches and Hubs', and the incoming device is of type Switches and Hubs > Cisco Catalyst 2928 Series Switches > Cisco Catalyst 2928-24TC-C switch, and if there is no profile defined specifically for this switch (Catalyst 2928-24TC-C s or Cisco Catalyst 2928 Series Switches), the 'switch_profile' is considered for deployment.

**Note**

Device Type-based deployment is useful primarily for switches that uses the same set of images and configurations.

Delivering and Applying the Bootstrap

You can deliver the bootstrap configuration in these ways:

- [Exporting](#)
- [Delivering through Trivial File Transfer Protocol](#)
- [E-mailing](#)
- [E-mailing the Pin](#)

Exporting

To export the bootstrap configuration, perform these steps:

Step 1 Choose **Deploy > Automated Deployment Profile**.

- Step 2** From the PnP Profiles page, click **Deploy**.
- Step 3** From the Device Provisioning Profiles page, select the device profile from the list, and then click **Export Bootstrap**.
- Step 4** Click **OK**.

The operator can manually apply the bootstrap on the device. After the bootstrap configuration is applied, the automated deployment is initiated and the administrator can view the configuration status on Prime Infrastructure.

Delivering through Trivial File Transfer Protocol

To deliver the bootstrap configuration through TFTP, perform these steps:

- Step 1** Choose **Deploy > Automated Deployment Profile**.
- Step 2** From the PnP Profiles page, click **Deploy**.
- Step 3** In the Device Provisioning Profiles page, select the Device Profile from the list, and then click **TFTP**.
- Step 4** Click **OK**.



Note

The TFTP can be used to deliver the bootstrap configuration to the Prime Infrastructure TFTP server. You can specify the file name that should be created on the TFTP server. This file is used by the auto-install enabled devices to get the IP address and TFTP server details through the DHCP. In the DHCP server, the TFTP server must be configured in the same manner as the Prime Infrastructure TFTP server.

E-mailing

To e-mail the bootstrap configuration to the operator, perform these steps:

- Step 1** Choose **Deploy > Automated Deployment Profile**.
- Step 2** From the PnP Profiles page, click **Deploy**.
- Step 3** From the Device Provisioning Profiles page, select the Device Profile from the list, and click **Email Bootstrap**.
- Step 4** Enter the e-mail address to which the bootstrap configuration is be sent.



Note

To e-mail the bootstrap configuration, ensure that you have set e-mail settings under **Administration > System Settings > Mail Server Configuration**.

- Step 5** Click **OK**.

The operator can manually apply the bootstrap on the device. After the bootstrap configuration is applied, the automated deployment is initiated. The administrator can view the configuration status on Prime Infrastructure.

E-mailing the Pin

To deliver the pin for the bootstrap configuration, perform these steps.

-
- Step 1** Choose **Deploy > Automated Deployment Profile**.
 - Step 2** From the PnP Profiles page, click **Deploy**.
 - Step 3** From the Device Provisioning Profiles page, select the device profile from the list, and then click **Email PIN**.
 - Step 4** Enter your e-mail address and click **OK**.
 - Step 5** If you are manually applying the bootstrap configuration using the pin, then:
 - a. Use the pin to download the bootstrap configuration from the Prime Infrastructure PnP gateway <https://<pnp-gateway-server>/cns/PnpBootstrap.html>.
 - b. Apply the bootstrap configuration on the device manually.
 - Step 6** If you are applying the bootstrap configuration using the deployment application, then the Prime Infrastructure PnP deployment application communicates to the Prime Infrastructure and applies the bootstrap configuration on the device.

The operator can manually apply the bootstrap on the device. After the bootstrap configuration is applied, the automated deployment is initiated. The administrator can view the configuration status on Prime Infrastructure.

Automated Deployment Status

To view the automated deployment status, perform these steps:

-
- Step 1** To view information about all incoming devices, choose **Operate > Automated Deployment Status**.
 - Step 2** To view the status of a selected device, for a selected profile, choose **Deploy > History**.
 - Step 3** To view the history of deployment, hover over the Quick View icon at the top right corner of the page.
-

Related Topic

- [Automated Deployment](#)

Configuring Controller Deployments

To view and manage the devices in your network, Prime Infrastructure must first discover the devices and, after obtaining access, collect information about them. For details, see the [“Discovering the Network” section on page 2-1](#).

Cisco Prime Infrastructure simplifies WLAN deployments with support for auto-provisioning. Auto provisioning allows Prime Infrastructure to automatically configure a new or replace a current wireless LAN controller (WLC). Prime Infrastructure auto provisioning feature can simplify deployments for customers with a large number of controllers.

**Note**

For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status. To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration > AAA > User Groups > *group name* > List of Tasks Permitted in Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

**Note**

A controller radio and b/g networks are initially disabled by Prime Infrastructure downloaded startup configuration file. If desired, you might turn on those radio networks by using a template, which should be included as one of the automated templates.

**Note**

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

This section contains the following topics:

- [Using the Auto Provisioning Filter List, page 6-9](#)
- [Adding an Auto Provisioning Filter, page 6-10](#)
- [Auto Provisioning Primary Search Key Settings, page 6-10](#)

Using the Auto Provisioning Filter List

The Auto Provision Filters page allows you to create and edit auto provisioning filters which define the list of allowable devices to be auto provisioned or auto monitored by Prime Infrastructure.

Filter parameters include the following:

- Filter Name—Identifies the name of the filter.
- Filter Enable—Indicates whether or not the filter is enabled.

**Note**

Only enabled filters can participate in the Auto Provisioning process.

- Monitor Only—If selected, the WLC defined in this filter is managed by Prime Infrastructure but not configured by Prime Infrastructure if the WLC contacts Prime Infrastructure during the auto provisioning process.

- **Filter Mode**—Indicates the search mode for this filter (Host Name, MAC Address, or Serial Number).
- **Config Group Name**—Indicates the Configuration Group name.



Note All Config-Groups used by auto provision filters should not have any controller defined in them.

Adding an Auto Provisioning Filter

To add an Auto Provisioning Filter, follow these steps:

-
- Step 1** Choose **Deploy > Controller Deployment**. The Auto Provisioning Filters page appears
 - Step 2** From the Select a command drop-down list, choose **Add Filter**.
 - Step 3** Click **Go**. The Add Filter page appears.
 - Step 4** Enter the required parameters.
 - Step 5** Click **Save**.



Note You can specify the Dynamic Interface configuration and Device Specific configuration details only when you input a CSV file. These two configurations cannot be performed using the graphical user interface.

Auto Provisioning Primary Search Key Settings

The Primary Search Key Setting enables you to set the matching criteria search order.

To indicate the Search Key Order, follow these steps:

-
- Step 1** Choose **Deploy > Controller Deployment**. The Auto Provisioning Filters page appears
 - Step 2** From the left sidebar menu, choose **Setting**.
 - Step 3** Click to highlight the applicable search key.
 - Step 4** Use the **Move Up** or **Move Down** buttons to move the search key to a higher or lower priority.
 - Step 5** Click **Save** to confirm the changes.
-



CHAPTER 7

Designing Sites

Prime Infrastructure Sites help you manage your network by associating network elements with your organization's physical locations. They allow you to segment the physical structure of your network, and to monitor and troubleshoot your network based on location information.

Sites have a hierarchy. At the top are campuses, which can contain buildings and outdoor areas. You may create as many campuses as your organization needs. Buildings within a campus can contain floors. You can specify the number of floors in a building, the size and height of any floor, and associate images (including photographs and drawings) of these areas with your specifications. You can make the site structure as simple or as complex as you need.

As your organization grows and changes, you need to change your site structure. The areas where you set up and change sites include:

- **Design > Site Map Design**—Create a new site or update an existing site.
- **Operate > Device Work Center**—If a site has previously been created, you can add devices to a site by clicking **Add to Site** from the Device Work Center.
- You can also associate network endpoints

Updating Campuses

The following steps explain how to edit your campuses. Editing a campus allows you to change the campus name, contact, and any associated image file.

Step 1 Choose **Design > Site Map Design**.

Step 2 Choose the campus you want to change. then select the appropriate command from the Go menu:

To do this:	Select this command and click Go
Add a new building to the currently selected campus	New Building
Add a new outdoor area to the currently selected campus	New Outdoor Area
Edit the campus name, contact, associated image file, latitude and longitude, address, and dimensions in feet.	Edit Campus
Delete the currently selected campus and all of its contained buildings and outdoor areas.	Delete Campus

Importing Sites From Files

Prime Infrastructure supports direct import of site map information stored in the following formats:

- XML—A TAR GZIP or ZIP file containing definitions of all Prime Infrastructure map data, including images and calibration data.
- AP/Wifi TDOA Received/Chokepoint Placement files—A CSV file exportable from Cisco WCS 7.0.
- WLSE Map and AP Location Data—An encrypted XML file exportable by Cisco Wireless LAN Solution Engine (WLSE).

-
- Step 1** Choose **Design > Site Map Design** or **Operate > Maps**.
- Step 2** In the Go menu, select **Import Maps**, then click **Go**.
- Step 3** Select the import file format and click **Next**
- Step 4** Click **Browse** to browse for the file, then click **Import**.
-

Removing Campuses or Buildings

Deleting a campus deletes all buildings assigned to the campus. Deleting a campus does not remove the inventory assigned to the campus.

To delete a campus or building:

-
- Step 1** Choose **Operate > Maps**.
- Step 2** Choose the campus or building you want to remove.
- Step 3** From the command menu, choose **Delete**, and then click **Go**.
-

Associating Devices With Sites

After you have created site profiles, you can assign devices to those sites. By associating devices with a campus or buildings, you can simplify maintenance tasks. When you need to perform maintenance tasks on devices, you can choose the site that contains the devices and apply the changes to all the devices in the site.

To control which users have access to the devices in the sites, you need to create virtual domains. See [Setting Up Virtual Domains](#) for more information.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Choose the devices you want to add to a site
- Step 3** Choose **Groups & Sites > Add To Group**.
- Step 4** In the Select Group list, choose the campus, building, outdoor site, or floor to which to assign the devices, then click **Save**.

**Note**

The Campus and Building fields are populated with the settings you previously entered in **Operate > Maps**. See [Setting Up Site Profiles](#) for more information.

Associating Endpoints With Sites

Endpoint-Site association rules allow you to associate all the devices on particular subnets to a Site profile, and (optionally) to specify the VLAN location and monitoring data source for the devices on that subnet. This allows you to associate the logical structure of your network with your organizational locations, enabling troubleshooting using Prime Infrastructure's multi-segment analysis features.

Note the you can specify multiple rules for the same subnet, allowing you to (for example) specify multiple monitoring data sources or VLANs.

-
- Step 1** Choose **Design > Endpoint-Site Association**.
- Step 2** Click Add Row to add an Endpoint-Site association rule
- Step 3** Complete the fields as follows:
- Site—Select the campus you want to associate with this subnet. You must have already created the campus.
 - Subnet—Enter the routing prefix of the subnetwork to be associated with this Site (and optional Data Source and VLAN). The entry must be in Classless Inter-Domain Routing notation.
 - Data Source—Select the edge router or NAM monitoring traffic to and from the devices in the specified subnetwork.
 - VLAN—Enter the VLAN ID of the subnetwork.
- Step 4** Click **Save**.
-



PART 3

Deploying the Network

This part contains the following sections:

- [Planning Template Deployments](#)
- [Deploying Templates](#)



CHAPTER 8

Planning Template Deployments

After you design your network, you go to the Deploy menu to reuse and deploy the designs you've created. You can deploy feature templates, composite templates, profiles, etc. You need to determine answers to the following questions before deploying objects:

1. What are you deploying? Determine whether you are deploying a configuration template, automated deployment profile, etc.
2. Where is being deployed? Determine which devices should be included in the deployment.
3. When is it being deployed? Determine when the deployment should happen.

Deployment Scenarios

You can plan your template deployments based on the following device conditions:

- Existing devices—You can deploy a configuration or monitoring template to a device that is already in your network.
- New devices that are known—You can deploy a configuration or monitoring template based on the device type and function. For example, if a new WAN edge router is discovered, you can deploy a configuration template that configures the necessary features for the WAN edge router. (pre-provisioning)
- New devices that are unknown or generic—You can deploy a generic configuration to a device that will provide a minimum set of configurations.



CHAPTER 9

Deploying Templates

There are two steps to deploying configuration or monitoring templates:

1. Chose the template you want to deploy.
2. Specify the scope. After you have chosen the template to deploy, you need to determine which devices should be included in the deployment.

Specifying Template Deployment Options

After you publish a template and want to deploy it to one or many devices, you can specify devices, values, and scheduling information to tailor your deployment. [Table 9-1](#) explains the deployment options.

Table 9-1 *Deploy > Configuration Task Options*

Option	Description
Device Selection	Displays the list of devices to which you want to deploy the template.
Value Assignment	<p>Allows you to specify a variable other than what was previously defined in the configuration template. Click a name, and the previously defined variables are displayed. To change any of the values, click the variable you want to change, enter a new value, and click Apply.</p> <p>Note The changes you make apply only to the specific configuration you are deploying. To change the configuration template for <i>all</i> future deployments, choose Design > Configuration Templates and change the template.</p>
Schedule	Allows you to create a meaningful deployment job name, then specify whether to run the job now or in the future.
Summary	Summarizes your deployment option selections.

Deploying the DMVPN Template

To deploy the DMVPN template:



Note

You must publish the specified template before it can be deployed to devices.

- Step 1** Choose **Deploy > Configuration Tasks > My Templates**.

- Step 2** On the My Templates page, select the DMVPN template, and click the **Tasked View** button.
- Step 3** From the Deploy Task pad, click **Deploy**.
- Step 4** On the Template Deployment page, enter the required information; if you change any of the default values, click **Apply**.
- Step 5** Under Summary, verify your entries and click OK.
- Step 6** For DMVPN, you can change the values for GRE IP Address, Subnet Mask, and Tunnel Throughput Delay.
- Step 7** If you have changed the values, click **Apply**.
- Step 8** In the Schedule section, enter the Job Name, then click one of the following radio buttons:
- **Run**—To run the job immediately.
 - **Run at Schedule Time**—To specify a time to run the job.
- Step 9** Under Summary, verify your entries, then click **OK**.
-

Deploying GETVPN Templates

This task enables you to deploy the GETVPN group member and key server template.



Note

Before you can deploy your template to devices, you must publish the template.

To deploy the GETVPN template:

- Step 1** Choose **Deploy > Configuration Tasks > My Templates**.
- Step 2** On the My Templates page, select the **GETVPN-GroupMember** or **KeyServer** template, and click the **Tasked View** button.
- Step 3** From the Deploy Task Pad, click **Deploy**.
- Step 4** On the Template Deployment page, enter the required information; if you change any of the default values, click **Apply**.
- Step 5** Under Summary, verify your entries and click OK.
- Step 6** For GETVPN-GroupMember, you can change the values for Registration Interface, Enable Passive SA, Local Exception Policy ACL, and Fail Close ACL.
- Step 7** For GETVPN Key Server, you can change the values for Keyserver, WAN IP Address, ACL, Priority, and Cooperative servers.
- Step 8** If you have changed the values, click **Apply**.
- Step 9** Click the Schedule section, enter the Job Name, then click one of the following radio buttons:
- **Run**—To run the job immediately.
 - **Run at Schedule Time**—To specify a time to run the job.
- Step 10** Under Summary, verify your entries, then click **OK**.
-

Deploying ScanSafe Template

To deploy the ScanSafe template:

**Note**

You must publish the specified template before it can be deployed to devices.

-
- Step 1** Choose **Deploy > Configuration Tasks > My Templates**.
- Step 2** On the My Templates page, select the **ScanSafe** template, and click the **Tasked View** button.
- Step 3** From the Deploy Task pad, click **Deploy**.
- Step 4** On the Template Deployment page, enter the required information; if you change any of the default values, click **Apply**.
- Step 5** Under Summary, verify your entries and click OK.
- Step 6** For ScanSafe, you can change the interfaces.
- Step 7** If you have changed the values, click **Apply**.
- Step 8** In the Schedule section, enter the Job Name, then click one of the following radio buttons:
- **Run**—To run the job immediately.
 - **Run at Schedule Time**—To specify a time to run the job.
- Step 9** Under Summary, verify your entries, then click **OK**.
-

Troubleshooting Template Deployment

The most common reasons that a template might not be deployed are:

- One or more devices are unreachable—Verify that the device credentials are correct; ping the device to verify that it is reachable. (See [Getting Device Details Using the 360° View](#) for more information.)
- A device CLI returned an error because the CLI was incorrect—Verify that the CLI commands contained in the template are correct by running the commands on a test device.



PART 4

Operating the Network

This part contains the following sections:

- [Operating and Monitoring the Network](#)
- [Monitoring Alarms](#)
- [Updating Device Inventory](#)
- [Changing Port Groups](#)
- [Working with Device Configurations](#)
- [Maintaining Device Configuration Inventory](#)
- [Maintaining Software Images](#)
- [Working with Wireless Operational Tools](#)
- [Tracing Application Data Paths](#)
- [Troubleshooting](#)



CHAPTER 10

Operating and Monitoring the Network

Under the Operate tab, Prime Infrastructure provides tools to help you monitor your network on a daily basis, as well as perform other day-to-day or ad hoc operations relating to network device inventory and configuration management. The Operate tab contains dashboards, the Device Work Center, and the tools you need for day-to-day monitoring, troubleshooting, maintenance, and operations.

Monitoring Dashboards

Prime Infrastructure automatically displays monitoring data in dashboards and dashlets. You can choose one of the following dashboards under **Operate > Monitoring Dashboard** to view summary information:

- **Overview**—Displays overview information about your network such as device counts, and the top 5 devices by CPU and memory utilization. From the overview dashboard, you can click on device or interface alarms counts to view detailed dashboards and alarms and events in order to help troubleshoot and isolate issues.
- **Incidents**—Displays a summary of alarms and events for your entire network, for a particular site, or for a particular device. By clicking on an item in the dashboard, you can view details about the alarm or event and troubleshoot the problem.
- **Performance**—Displays CPU and memory utilization information.
- **Detail Dashboards**—Displays network health summaries for sites, devices, or interfaces. The detailed dashboards allow you to see congestion in your network and gather detailed site, device, and interface information. For example, you can view detailed dashboards for a particular site to determine which devices have the most alarms, device reachability status for the site, etc.

You can change the information displayed in the dashboards as explained in [Dashboards and Dashlets](#). [Table 10-1](#) describes where to find monitoring information in the Prime Infrastructure dashboards.

Table 10-1 Finding Monitoring Data

To View this Monitoring Data	Choose this Dashboard
Alarm information	Operate > Monitoring Dashboard > Incidents
CPU utilization	Operate > Monitoring Dashboard > Performance
Detailed device information	Operate > Monitoring Dashboard > Detail Dashboards
Detailed interface information	Operate > Monitoring Dashboard > Detail Dashboards
Device reachability status	Operate > Monitoring Dashboard > Overview

Table 10-1 *Finding Monitoring Data*

To View this Monitoring Data	Choose this Dashboard
Event information	Operate > Monitoring Dashboard > Incidents
Interface status, availability, and utilization information	Operate > Monitoring Dashboard > Performance
Licensing information	Operate > Monitoring Dashboard > Overview
Memory utilization	Operate > Monitoring Dashboard > Performance
Site information	Operate > Monitoring Dashboard > Detail Dashboards
Syslog sender information	Operate > Monitoring Dashboard > Incidents
Utilization statistics	Operate > Monitoring Dashboard > Overview

Configuring Monitoring Settings

You can define how Prime Infrastructure monitors the devices and interfaces in your network.

By enabling the Auto Monitoring option, you can have Prime Infrastructure monitor the availability, CPU, memory and temperature of all your network devices automatically. By default, Prime NCS (WAN) polls all devices in your network every 15 minutes for device-health data. Most users will want to enable Auto Monitoring.

You may want to avoid enabling Auto Monitoring if you have a very large network or Prime Infrastructure deployment, to avoid excessive polling traffic. In this case, you can leave Auto Monitoring disabled, and create one or more device groups containing your business-critical devices only. You may also want to create a version of the default device health monitoring template with a polling frequency appropriate for these devices. When you deploy the default or custom device health monitoring template, you can select to apply it to your business-critical device group only.

You can also enable deduplication, if applicable, for Cisco IOS Netflow and Cisco Prime Assurance. If you have multiple routers and switches that send netflow to the Cisco Prime Assurance server and multiple NAMs that Cisco Prime Assurance retrieves data from, Cisco Prime Assurance could receive the same traffic statistic more than once. You can enable deduplication so that Cisco Prime Assurance doesn't count the same metrics more than once.

Step 1 Choose **Administration > System Settings**, then select **Monitoring Settings**.

Step 2 Check the following options:

- **Auto monitoring** to have Prime Infrastructure monitor all devices and interfaces automatically.
 - **Enable deduplication** to have Prime Infrastructure eliminate redundant data.
-

Device Work Center

From **Operate > Device Work Center**, you can view the device inventory and device configuration information. The Device Work Center contains general administrative functions at the top and configuration functions at the bottom as described in [Table 10-2](#).

Table 10-2 **Device Work Center Tasks**

Task	Description	Location in Operate > Device Work Center
Manage devices	Add, edit, bulk import, and delete devices, and force data collection from devices.	Buttons located at the top of the Device Work Center.
View basic device information and collection status	View basic device information such as reachability status, IP address, device type, and collection status information.	Displayed in the top portion of the Device Work Center. Rest your cursor on the Collection Status cell and click on the icon to view errors related to the inventory collection.
Manage device groups	By default, Prime Infrastructure creates dynamic device groups and assigns devices to the appropriate Device Type folder. You can create new device groups that appear under the User Defined folder.	Displayed on the left pane of the Device Work Center. See Managing Device Groups for more information about creating and using device groups.
Add devices to sites	After you set up a site profile, you can add devices to the site. Note A device can belong to one site only.	Add to Site button located at the top of the Device Work Center. See Creating Site Profiles for more information about adding devices to sites.
View device details	View device details such as memory, port, environment, and interface information.	Choose a device in the Device Work Center, then click the Device Details tab at the bottom of the screen.
	View device information, status, and associated modules, alarms, neighbors, and interfaces. See Getting Device Details Using the 360° View for more information.	Rest your cursor on a device IP address and click the icon that appears.
Create and deploy configuration templates	You can create and deploy configuration templates for the selected device. You can also preview the CLI that will be deployed to the device.	Click the Configuration tab at the bottom of the Device Work Center. See Configuring Features on a Device for more information about configuring features on a device.
View device configurations	View archived configurations, schedule configuration rollbacks, and schedule archive collections.	Click the Configuration Archive tab at the bottom of the Device Work Center.
View software images	View details about the image on the selected device, the recommended software image for the device, and the latest software image operations for a device.	Click the Image tab at the bottom of the Device Work Center.

Monitoring Jobs

Choose **Administration > Jobs Dashboard** to view the status of jobs and to:

- View all running and completed jobs and corresponding job details
- Filter jobs to view the specific jobs for which you are interested

- View details of the most recently submitted job
- View job execution results
- Modify jobs including deleting, editing, running, canceling, pausing, and resuming jobs

**Note**

Internally scheduled jobs are not displayed in the Jobs Dashboard.

If a job fails, you can get troubleshooting information from the Jobs Dashboard. When you expand a job to view its details, click the History tab, and rest your cursor over the Status field. The results window displays troubleshooting information that can help you determine why the job failed.

Monitoring Using Reports

Prime Infrastructure reporting helps you monitor the system and network health as well as troubleshoot problems. Reports can be run immediately or scheduled to run at a time you specify. Once defined, the reports can be saved for future diagnostic use or scheduled to run and report on a regular basis.

Reports are saved in either CSV or PDF format and are either saved to a file on Prime Infrastructure for later download or e-mailed to a specific e-mail address.

Choose **Report > Report Launch Pad** to view the list of available reports.

**Tip**

Rest your cursor on the information icon next to the report type to view report details.

Creating Reports

-
- Step 1** Choose **Report > Report Launch Pad**.
- Step 2** Click **New** next to the report you want to create.
- Step 3** Enter report details, then click a save option.
-

Using Packet Capture for Monitoring and Troubleshooting

Prime Infrastructure allows you to run capture traffic in your network to help monitor network usage, gather network statistics, and analyze network problems.

-
- Step 1** Choose **Operate > Packet Capture**, then click **Create**.
- Step 2** Specify the required capture session parameters, then click **Create**.
-

Diagnosing Site Connectivity Issues and Comparing Configurations

You can use the Prime Infrastructure dashboards to monitor your network and locate problematic devices in your network, and then use the Device Workcenter to change the device configuration.

-
- Step 1** Choose **Operate > Detailed Dashboards**, choose the site for which you are experiencing connectivity issues, then click **Go**.
 - Step 2** Check the data reported under Device Reachability Status and Top *N* Devices with Most Alarms to determine the source of the issue.
 - Step 3** Click on the name of the device for which you see the most alarms.
 - Step 4** From the 360-degree view of the device, click the Alarm Browser icon to view the alarms for that device. Expand the alarm to view details for the alarm.
 - Step 5** To compare the configuration on the device to a previously known good configuration, choose **Operate > Device Work Center**, then select the device whose configuration you want to change.
 - Step 6** Click the Configuration Archive tab, expand the arrow to view additional options, then select the configuration type and a configuration against which to compare.
 - Step 7** Change or rollback the configuration. See [Rolling Back Device Configuration Versions](#) for more information.
-



CHAPTER 11

Monitoring Alarms

An *alarm* is a Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the resulting condition no longer occurs.

What is an Event?

An *event* is an occurrence or detection of some condition in and around the network. An event is a distinct incident that occurs at a specific point in time. Examples of events include:

- Port status change
- Device reset
- Device becomes unreachable by the management station

An event can also be a:

- Possible symptom of a fault that is an error, failure, or exceptional condition in the network. For example, when a device becomes unreachable, an unreachable event is triggered.
- Possible symptom of a fault clearing. For example, when a device state changes from unreachable to reachable, a reachable event is triggered.

One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. You can view the list of events using the Event Browser.

Choose **Operate > Alarms & Events**, then click Events to access the Events Browser page.

Event Creation

Prime Infrastructure maintains an event catalog and decides how and when an event is created and whether to associate an alarm with the event. Multiple events can be associated to the same alarm.

Prime Infrastructure discovers events in the following ways:

- By receiving notification events and analyzing them; for example, syslog and traps.
- By automatically polling devices and discovering changes; for example, device unreachable.
- By receiving events when a significant change occurs in the Prime Infrastructure server; for example, rebooting the server.
- By receiving events when the status of the alarm is changed; for example when the user acknowledges or clears an alarm.

Incoming event notifications (traps and syslogs) are identified by matching the event data to predefined patterns. A trap or syslog is considered supported by Prime Infrastructure if it has matching patterns and can be properly identified. If the event data does not match with predefined patterns, the event is considered as unsupported and it is dropped.

Faults are discovered by Prime Infrastructure through polling, traps, or syslog messages. Prime Infrastructure maintains the context of all faults and ensures that duplicate events or alarms are not maintained in the Prime Infrastructure database.

The following table provides examples of when Prime Infrastructure creates an event.

Time	Event	Prime Infrastructure Behavior
10:00AM PDT December 1, 2011	Device A becomes unreachable.	Creates a new unreachable event on device A.
10:30AM PDT December 1, 2011	Device A continues to be unreachable.	No change in the event status.
10:45AM PDT December 1, 2011	Device A becomes reachable.	Creates a new reachable event on device A.
11:00AM PDT December 1, 2011	Device A stays reachable.	No change in the event status.
12:00AM PDT December 1, 2011	Device A becomes unreachable.	Creates a new unreachable event on device A.

What is an Alarm?

An *alarm* is a Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the resulting condition no longer occurs.

One or more events can result in a single alarm being raised. An alarm is created in the following sequence:

1. A notification is triggered when a fault occurs in the network.
2. An event is created, based on the notification.
3. An alarm is created after checking if there is no active alarm corresponding to this event.

An alarm is associated with two types of events:

- Active events: Events that have not been cleared. An alarm remains in this state until the fault is resolved in a network.
- Historical events: Events that have been cleared. An event changes its state to an historical event when the fault is resolved in a network.

After an alarm is cleared, it indicates the end of an alarm life cycle. A cleared alarm can be revived if the same fault reoccurs within a preset period of time. The present period is set to 5 minutes in Prime Infrastructure.

Event and Alarm Association

Prime Infrastructure maintains a catalog of events and alarms. The catalog contains the list of events managed by Prime Infrastructure, and the relationship among the events and alarms. Events of different types can be attached to the same alarm type.

When a notification is received:

1. Prime Infrastructure compares an incoming notification against the event and alarm catalog.
2. Prime Infrastructure decides whether an event has to be raised.

3. If an event is raised, Prime Infrastructure decides whether the event triggers a new alarm or associates it to an existing alarm.

A new event is associated with an existing alarm, if the new event triggered is of the same type and occurs on the same source.

For example, an active interface error alarm. The interface error events that occur at the same interface, are all associated to the same alarm.

Alarm Status

Table 11-1 describes the alarm statuses.

Table 11-1 Alarm Status Descriptions

Alarm Status	Description
New	When an event triggers a new alarm or an event is associated with an existing alarm.
Acknowledged	When you acknowledge an alarm, the status changes from New to Acknowledged.
Cleared	<p>An alarm can be in these statuses:</p> <ul style="list-style-type: none">• Auto-clear from the device—The fault is resolved on the device and an event is triggered for the same. For example, a device-reachable event clears the device-unreachable event. This in-turn, clears the device-unreachable alarm.• Manual-clear from Prime Infrastructure users: You can manually clear an active alarm without resolving the fault in the network. A clearing event is triggered and this event clears the alarm.• If the fault continues to exist in the network, a new event and alarm are created subsequently based on the event notification (traps/syslogs).

Event and Alarm Severity

Each event has an assigned severity. Events fall broadly into the following severity categories, each with their associated color in Prime Infrastructure:

- Flagging—Indicates a fault: Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- Informational—Info (blue). Some of the Informational events clear the flagging events.

For example, a Link Down event might be assigned a Critical severity, while its corresponding Link Up event will be an Informational severity.

In a sequence of events, the event with the highest severity determines the severity of the alarm.

Where to Find Alarms

Table 11-2 lists the places where you can find alarms.

Table 11-2 *Where to Find Alarms*

Location in GUI	Description
Operate > Alarms & Events	Displays a new page listing all alarms with details such as severity, status, source, timestamp. You can change the status of alarms, assign, annotate, delete, and specify email notifications from this page.
Rest your cursor on Alarm Summary	Displays a table listing the critical, major, and minor alarms currently detected by Prime Infrastructure.
Alarm Browser	Opens a window that displays the same information as in the Operate > Alarms & Events but does not take you to a new page.
From device 360° view	Click the Alarms tab to view alarms on the device, their status and category, or click the Alarm Browser icon to launch the Alarm Browser.
Operate > Monitoring Dashboard > Incidents	Displays dashlets that contain alarm summary information, top sites with the most alarms, top alarm types, top events, and top interfaces with issues.

Defining Thresholds

You use monitoring templates to define thresholds. When the thresholds you specify are reached, Prime Infrastructure issues an alarm.

To define thresholds:

-
- Step 1** Choose **Design > Monitoring Templates**.
 - Step 2** Under Features, choose **Threshold**.
 - Step 3** Complete the basic template fields.
 - Step 4** Under Feature Category, choose one of the following metrics:
 - Device Health—allows you to change threshold values for CPU utilization, memory pool utilization, and environment temperature
 - Interface Health—allows you to change threshold values for the number of outbound units that are discarded, inbound and outbound utilization, and other health parameters.
 - Step 5** Under Metric Parameters, choose the threshold setting you want to change, then click **Edit Threshold Setting**.
 - Step 6** Enter a new value and choose the alarm severity when the threshold is met or exceeded.
 - Step 7** Click **Done**.
 - Step 8** Click **Save as New Template**.
 - Step 9** Under the My Templates folder, navigate to the template you created and select it.
 - Step 10** Click **Go to Deployment**.
 - Step 11** Choose the template you created, then click **Deploy**.
-

Getting Help for Alarms

Prime Infrastructure provides helpful tools for network operators to connect to Cisco experts to diagnose and resolve problems. If you receive an alarm for which you need help troubleshooting, Prime Infrastructure allows you to:

- Connect with the Cisco Support Community to view and participate in discussion forums. See [Launching Cisco Support Community](#).
- Open a support case Cisco Technical Support. See [Opening a Support Case](#).

Launching Cisco Support Community

If you receive an alarm in **Operate > Alarms & Events**, you can use Prime Infrastructure to view discussion forums on the Cisco Support Community. By viewing and participating in the Cisco Support Community forums, you can find information that can help you diagnose and resolve problems. You must enter your Cisco.com username and password to view and participate in the Cisco Support Community forums.

-
- Step 1** Chose **Operate > Alarms & Events**, then rest your mouse over the IP address of the device on which the alarm occurred.
- Step 2** From the device 360° view, click the **Support Community** icon.
- Step 3** On the Cisco Support Community Forum page, enter additional search parameters to refine the discussions that are displayed.

Opening a Support Case

If you receive an alarm in **Operate > Alarms & Events** for which you cannot find a resolution in the Cisco Support Community (see [Launching Cisco Support Community](#)), you can use Prime Infrastructure to open a support request and to help you gather critical information to be attached to the support case. You must enter your Cisco.com username and password to open a support case.

**Note**

You must have a direct internet connection on the Prime Infrastructure server in order to access the Cisco Support Community and to open a support case.

-
- Step 1** To open a support case, click **TAC Service Requests** in the lower right corner of the Prime Infrastructure window.
- Step 2** Enter your Cisco.com username and password.
- Step 3** Click Create New Case.
- Prime Infrastructure gathers information about the device and populates the fields for which it can retrieve information. You can enter a Tracking Number that corresponds to your own organization's trouble ticket system.
- Step 4** Click **Next** to enter a description of the problem.

By default, Prime Infrastructure enters information that it can retrieve from the device. Prime Infrastructure automatically generates the necessary supporting documents such as the technical information for the device, configuration changes, and all device events over the last 24 hours. You can also upload files from your local machine.

Step 5 Click **Create Service Request**.

Changing Alarm Status

You can remove an alarm from the list of alarms by changing its status to acknowledged or cleared. No e-mails will be generated for these alarms.

-
- Step 1** Choose **Operate > Alarms & Events**.
- Step 2** Click the expand icon next to an alarm.
- Step 3** Choose **Change Status > Acknowledge** or **Clear**.
-

When to Acknowledge Alarms

You may want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain device, you may want to stop that device from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the device in the Alarms list, select the check box, and choose **Acknowledge** from the Select a command drop-down list.

Now if the device generates a new violation on the same interface, Prime Infrastructure will not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, a new alarm is created.

By default, acknowledged alarms are not displayed in either the Alarm Summary page or any alarm list page. Also, no emails are generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, go to the **Administration > System Settings > Alarms and Events** page and disable the **Hide Acknowledged Alarms** preference.

When you acknowledge an alarm, the following warning appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled.



Note

When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Use the **Administration > User Preferences** page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. Prime Infrastructure automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which Prime Infrastructure has already generated an alarm.

Including Acknowledged and Cleared Alarms in Searches

By default, acknowledged and cleared alarms are not included for any search criteria. To change this default, choose **Administration > System > Alarms and Events** and disable the Hide Acknowledged Alarms or Hide Cleared Alarms preference.

Cleared alarms remain in the Prime Infrastructure database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

Changing Alarm and Event Options

To change alarm and event options such as when alarms are deleted, which alarm severities are displayed, and alarm email options:

-
- Step 1** Choose **Administration > System Settings > Alarms and Events**.
 - Step 2** Change the necessary settings for the alarms.
 - Step 3** Click **Save**.
-

Configuring Alarm Severity Levels

To configure the severity level for newly generated alarms:

-
- Step 1** Choose **Administration > System Settings**.
 - Step 2** From the left sidebar menu, choose **Severity Configuration**.
 - Step 3** Select the check box of the alarm condition whose severity level you want to change.
 - Step 4** From the Configure Severity Level drop-down list, choose a severity level, then click **Go**.
 - Step 5** Click **OK** to confirm the changes.
-



CHAPTER 12

Updating Device Inventory

Prime Infrastructure provides two ways to discover the devices in your network:

- **Quick**—Allows you to quickly discover the devices in your network based on the SNMP community string, seed IP address, and subnet mask you specify. Choose **Operate > Discovery**, then click **Quick Discovery**.
- **Regular**—Allows you to specify protocol, credential and filter settings for discovery and to schedule when to run the discovery job. See [Changing Discovery Settings](#).

Changing Discovery Settings

- Step 1** Choose **Operate > Discovery**, then click **Discovery Settings**.
- Step 2** Click **New**. Enter the settings as described in [Table 12-1](#).
- Step 3** Click:
- **Save** to save the settings
 - **Run Now** to save the settings and immediately start the discovery job.

Table 12-1 **Discovery Settings**

Field	Description
Protocol Settings	
Ping Sweep Module	Gets a list of IP Address ranges from a specified combination of IP address and subnet mask. This module pings each IP Address in the range to check the reachability of devices.
CDP Module	<p>The discovery engine reads the cdpCacheAddress and cdpCacheAddressType MIB objects in cdpCacheTable from CISCO-CDP-MIB on every newly encountered device.</p> <ol style="list-style-type: none"> 1. Fetch cdpCacheAddress MIB object from the current device. This provides a list of neighbor device addresses. 2. If the neighbor device addresses do not already exist in the global device list, add them to the local cache.
Advanced Protocols	
Routing Table	Queries and analyzes routing tables on seed routers to discover subnets and next-hop routers.
Address Resolution Protocol	<p>The ARP Discovery Module depends on the Routing Table Discovery Module (RTDM), and is executed only when RTDM is processed. This precondition is identified based on the Discovery-module-processed flags, which are part of the DeviceObject.</p> <p>The entries coming out of the ARP Discovery Module need not necessarily pass through RTDM because (per the router Discovery algorithm) active routers are those that RTDM must process and identify.</p> <p>When the ARP table is fetched and the entries are not already discovered by RTDM, then these entries (though they may represent routers) are not active routers and need not be passed on to RTDM. This is ensured by setting the ARP Discovery Module flag to Processed and leaving the RTDM flag set to Unprocessed.</p> <p>When the RTDM comes across an entry with the RTDM flag unset and the ARP flag set, RTDM identifies the entry as a inactive router or other device and it leaves the entry as Unprocessed. The ARP Discovery Module also ignores the entry according to the algorithm, based on the Processed flag set against the ARP Discovery Module.</p> <p>When the ARP Discovery module is selected, the device MAC address needs to be updated in the device information. Applications can retrieve this information in the adapter through the DeviceInfo object. By scanning the device MAC address, the applications can distinguish between Cisco and non-Cisco devices.</p> <p>ARP cache from the device is collected using CidsARPInfoCollector. The MAC ID of the device is retrieved from this data and set in the DeviceInfo object.</p>
Border Gateway Protocol	The BGP Discovery Module uses bgpPeerTable in the BGP4-MIB to find its BGP peer. The table contains its peers' IP addresses, which are added as clues to the local cache.
OSPF	Open Shortest Path First (OSPF) protocol is an interior gateway routing protocol. OSPF discovery uses the ospfNbrTable and ospfVirtNbrTable MIB to find neighbor IP addresses.
Filters	
System Location Filter	Filters the device based on the Sys Location string set on the device during discovery process.
Advanced Filters	
IP Filter	Filters the device based on the IP address string set on the device during discovery process.
System Object ID Filter	Filters the device based on the System Object ID string set on the device during discovery process.

Table 12-1 *Discovery Settings (continued)*

Field	Description
DNS Filter	Filters the device based on the DNS string set on the device during discovery process.
Credential Settings	
SNMP V2 Credential	SNMP community string is a required parameter to discover devices in the network. You can enter multiple rows of credentials mapped to a specific IP address, or the IP address can be a wild card e.g *.*.*.*, 1.2.3.*.
Telnet Credential	You can specify the telnet credentials during discovery setting creation to collect the device data.
SSH Credential	Prime Infrastructure support SSH V1 and V2. You can configure SSH before running discovery.
SNMP V3 Credential	Prime Infrastructure supports SNMP V3 discovery for devices.
Preferred Management	
IP Method	<ul style="list-style-type: none">• Use Loopback• Use SysName• Use DNSReverseLookup

Scheduling Discovery Jobs

To create a discovery job to run at a future time you specify:

- Step 1** Choose **Operate > Discovery**, then click **Discovery Settings**.
- Step 2** Click **New**.
- Step 3** Enter the settings as described in [Table 12-1](#), then click **Save**.
- Step 4** In the Discovery Settings window, select the discovery job you just created, then click **Schedule**.
- Step 5** Enter the schedule information, then click **Save**.

Monitoring the Discovery Process

To monitor the discovery process:

- Step 1** Choose **Operate > Discovery**.
- Step 2** Select the discovery job for which you want to see details.

Discovery Protocols and CSV File Formats

Prime Infrastructure uses six protocols to discover devices:

- Ping Sweep
- Cisco Discovery Protocol (CDP)
- Routing Table
- Address Resolution Protocol (ARP)
- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)

You can import a CSV file to add data for the protocols. [Table 12-2](#) describes the CSV file format for each of the protocols.


Note

You can import a CSV file if you are using a supported version of Mozilla Firefox only.

Table 12-2 **Discovery Protocols and CSV File Formats**

Protocol	CSV File Format
Ping sweep	Any valid IP address and subnet mask, separated by a comma. You can specify multiple networks in a single discovery by adding additional rows, for example: 1.1.1.1,255.255.240.0 2.1.1.1,255.255.255.0
Cisco Discovery Protocol (CDP)	Any valid IP address and the hop count, separated by a comma, for example: 1.1.1.1,3 2.2.2.2,5
Routing table	Any valid IP address and the hop count, separated by a comma, for example: 1.1.1.1,3 2.2.2.2,5
Address Resolution Protocol (ARP)	Any valid IP address and the hop count, separated by a comma, for example: 1.1.1.1,3 2.2.2.2,5
Border Gateway Protocol (BGP)	Seed device IP address for any device that is BGP enabled, for example: 1.1.1.1 2.2.2.2 3.3.3.3
Open Shortest Path First (OSPF)	Seed device IP address for any device that is OSPF enabled, for example: 1.1.1.1 2.2.2.2 3.3.3.3

Updating Device Inventory Manually

It is recommended that you run discovery to update your device inventory. However, you can also add devices manually.

To update the device inventory manually:

-
- | | |
|---------------|-------------------------------------------------------------------------|
| Step 1 | Choose Operate > Device Work Center , then click Add . |
| Step 2 | Enter the required parameters. |
| Step 3 | Click Add to add the device with the settings you specified. |
-

Importing Device Inventory

If you have another management system in which your devices are imported or if you want to import a spreadsheet that contains all your devices and their attributes, you can import device information in bulk into Prime Infrastructure.

To import device inventory:

-
- | | |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Operate > Device Work Center , then click Bulk . |
| Step 2 | Click the link to download a sample file that contains all the fields and descriptions for the information that must be contained in your imported file. |
| Step 3 | Click Browse to navigate to your file, then click Import and wait for the import to complete. (To check the status of the import, choose Administration > Jobs Dashboard). |
-

Troubleshooting Unmanaged Devices

[Table 12-3](#) describes the possible reasons a device is unmanageable by Prime Infrastructure:

Table 12-3 **Reasons for Unmanageable Device**

Possible Cause	Actions
Prime Infrastructure cannot reach the device because the device is down or because any device along the path from the Prime Infrastructure server to the device is down.	<ul style="list-style-type: none"> • Use the ping and traceroute tools to verify that the Prime Infrastructure can reach the device. See Getting Device Details Using the 360° View for more information. • If the device is reachable, verify that the retry and timeout values set for the device are sufficient. (Chose Operate > Device Work Center, select the device, then click Edit.) • Verify that SNMP is configured and enabled on the device: <ul style="list-style-type: none"> – If using SNMPv2, verify that the <i>read-write</i> community string configured on the device is the same as that entered in Prime Infrastructure. <p>Note The read-write community string is required.</p> <ul style="list-style-type: none"> – If using SMNPv3, verify that the following parameters are configured on the device, and that the configured parameters on the device match those entered in Prime Infrastructure: Username AuthPriv mode (noAuthNoPriv, authNoPriv, authPriv) Authentication algorithm (for example, MD5, SHA, etc.) and the authentication password Privacy algorithm (for example, AES, DES, etc.) and the privacy password • Verify that the SNMP credentials configured on the device match the SNMP credentials configured in Prime Infrastructure. • Re-enter the SNMP credentials in Prime Infrastructure, then resync the device. (Chose Operate > Device Work Center, select the device, then click Sync.) See Synchronizing Devices for more information.
Prime Infrastructure cannot gather information from the device because Telnet or SSH is not configured on the device.	<ul style="list-style-type: none"> • Verify that Telnet or SSH is configured and enabled on the device, and that the same protocol is configured on Prime Infrastructure. (Chose Operate > Device Work Center, select the device, then click Edit.) <p>Note If the device type requires HTTP, verify that the Prime Infrastructure HTTP parameters match those configured on the device.</p> <ul style="list-style-type: none"> • Verify that the username, Telnet or SSH passwords, and the enable mode password for Cisco IOS devices are configured correctly on the device and that the parameters entered in Prime Infrastructure match those configured on the device. If you did not configure a username on the device for authentication, you can leave this field empty in Prime Infrastructure. • Verify that the authorization level configured for the Telnet/SSH user is not limited to lower enable privilege levels.

Table 12-3 *Reasons for Unmanageable Device (continued)*

Possible Cause	Actions
Restrictions were placed for SNMP through SNMP views or access lists.	Remove any restrictions for SNMP through SNMP views or access lists.
TACACS+ “per-command authorization” is configured on the devices,	If TACACS+ is configured, verify the permissions for the Telnet/SSH user for the permitted CLI commands. It is recommended that you allow all CLI commands for the Prime Infrastructure user account; or alternatively, exclude only commands that need to be absolutely restricted.

For more information about configuring SNMP, Telnet, and SSH on Cisco IOS devices, see:

- [Cisco IOS Software Releases 12.0 T SNMPv3](#)
- [Configuring Secure Shell on Routers and Switches Running Cisco IOS](#)

Managing Device Groups

By default, Prime Infrastructure creates rule-based device groups and assigns devices to the appropriate Device Type folder. You cannot edit these device groups. You can view the rules for the device group by resting your cursor on the device group folder.

Device groups are logical groupings of devices. You create device groups to help you more efficiently update and manage your devices. For example, you can create a device group that includes devices that have a particular module. If you later want to configure a feature related specifically to that module, you use the device group you created to push the configuration change to all the devices contained in the group.

You can create a new group which can be one of two types:

- **Static**—You create and name a new device group to which you can add devices using the **Add to Group** button from **Operate > Device Work Center**.
- **Dynamic**—You create and name a new device group and specify the rules to which devices must comply in order to be added to this device group. See [Creating Dynamic Device Groups](#) for more information.

When you create a device group, you are distinguishing that group of devices from others in your network. For example, if you have devices that reside in different time zones, you can create device groups based on geographic regions so that the devices in one group can have a different time zone setting from the devices in another group.

In smaller deployments where all devices can be configured with the same settings, you may only need to create one general device group. This setup allows you to configure settings for the group, and then apply those settings consistently across all your devices.

Groups not only save you time when configuring multiple devices, but they also ensure that configuration settings are applied consistently across your network.



Note

You cannot control which users have access to which device groups. All users can see all device groups. For role-based access control (RBAC), you need to create sites and virtual domains.

Creating device groups is a two-part process:

1. Create a new device group. See [Creating Dynamic Device Groups](#).

2. Assign devices to the device group. See [Assigning Devices to a Group](#).

Related Topic

- [Device Accessibility in Parent-Child Device Groups](#)

Device Accessibility in Parent-Child Device Groups

When you create a child group under a parent device group, the devices accessible to the child group depend on the device group you create:

- If the parent and child group are *both dynamic* device groups, the child group can access the devices available in the parent group only.
- If the parent group is *static* device group and the child group is a dynamic group, the child group is not limited to the devices available in the parent group.

In dynamic device groups only, the child group “inherits” its devices from the parent device group.

Related Topics

- [Creating Dynamic Device Groups](#)
- [Assigning Devices to a Group](#)

Creating Dynamic Device Groups

Before you create a dynamic device group, make sure you understand the unique properties that you want the group to contain. For example, you may want to set up two device groups that have different authentication settings or different time zone settings.



Note While there is no limit on the number of rules you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

To create a dynamic device group:

-
- | | |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Operate > Device Work Center . |
| Step 2 | In the Groups menu on the left, click the Settings icon, then click Create Group . |
| Step 3 | Enter the group name, group description, and select the parent group if applicable. |
| Step 4 | Uncheck Save as a Static Group so you can specify rules to which all devices must comply to be added to the group. You can click Save as a Static Group if you want to manually add the devices to the group and not have the group be rule-based. |
| Step 5 | Specify the rules for the devices must match. |
| Step 6 | Click Save to add the device group with the settings you specified. The device group you created appears under the User Defined groups. |
-

Assigning Devices to a Group

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device you want to assign to a group, then click **Add To Group**.
 - Step 3** Select the group, then click **Save**.
-

Synchronizing Devices

You can force an inventory collection in order to sync the Prime Infrastructure database with the configuration currently running on a device.

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Select the device whose configuration you want synced with the configuration stored in Prime Infrastructure database.
 - Step 3** Click **Sync**.
-



CHAPTER 13

Changing Port Groups

As you add and remove devices and modules, you will need to create new port groups and change existing port groups.

By default, Prime Infrastructure creates rule-based port groups and assigns ports or interfaces to the appropriate Port Group folder. You cannot edit these port groups. You can view the rules for the port group by resting your cursor on the port group folder.

You can create a new port group which can be one of two types:

- **Static**—You create and name a new port group to which you can add devices using the **Add to Group** button from **Design > Port Grouping**.
- **Dynamic**—You create and name a new port group and specify the rules to which ports or interfaces must comply in order to be added to this port group.



Note While there is no limit on the number of rules you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

Related Topic

- [Creating Port Groups](#)

Creating Port Groups

To create a new dynamic port group:

-
- Step 1** Choose **Design > Port Grouping**.
 - Step 2** In the Port Groups menu on the left, click the Settings icon, then click **Create Group**.
 - Step 3** Enter the name, description, and parent group if applicable.
 - Step 4** Uncheck **Save as a Static Group** so you can specify rules to which all ports or interfaces must comply to be added to the group. You can click **Save as a static group** if you want to manually add the ports or interfaces to the group and not have the group be rule-based.
 - Step 5** If you are creating a dynamic port group, enter the required information, then click **Save**.
The port group you created appears under the User Defined folder.
-

Deleting a Port Group

To delete a port group:

Step 1 Choose **Design > Port Grouping**.



Note

If you are deleting a static port group, make sure the static port group does not contain any subgroups or members.

If you are deleting a dynamic port group, make sure the dynamic port group does not contain any subgroups; however, the dynamic group can be associated with members.

Step 2 Rest your cursor on the name of the name of the port group you want to delete, then click **Delete Group**.



CHAPTER 14

Working with Device Configurations

Prime Infrastructure provides information such as the date of last configuration change, status of the configuration jobs, etc.

Configuration Archives

Prime Infrastructure attempts to collect and archive the following device configuration files:

- Startup configuration
- Running configuration
- VLAN configuration, if configured

You can specify how Prime Infrastructure archives the configurations:

- On demand—You can have Prime Infrastructure collect the configurations of selected devices by selecting **Operate > Configuration Archives**.
- Scheduled—You can schedule when Prime Infrastructure collects the configurations of selected devices and specify recurring collections by selecting **Operate > Configuration Archives**, then clicking **Schedule Archive**.
- During inventory—You can have Prime Infrastructure collect device configurations during the inventory collection process. See [Changing Prime Infrastructure Device Configuration Settings](#) for more information.
- Based on Syslogs—If device is configured to send syslogs, when there is any device configuration change, Prime Infrastructure collects and stores the configuration.

Changing Prime Infrastructure Device Configuration Settings

By default, Prime Infrastructure has the following configuration settings:

- Does not backup the running configuration before pushing configuration changes to a device.
- Does not have Prime Infrastructure attempt to roll back to the previously saved configuration in the archive if the configuration deployment fails
- When pushing CLI to a device, uses 5 thread pools.

To change the default configuration settings:

-
- Step 1** Choose **Administration > System Settings**, then click **Configuration**.
- Select **Backup Running Configuration** to have Prime Infrastructure backup the running configuration before pushing configuration changes to a device.
 - Select **Rollback Configuration** to have Prime Infrastructure attempt to roll back to the previously saved configuration in the archive if the configuration deployment fails.
- Step 2** Click **Save**.
-

Comparing Current and Previous Device Configurations

To compare a current device configuration with a previous version:

-
- Step 1** Choose **Operate > Configuration Archives**.
- Step 2** Click the expand icon for the device whose configuration you want to view. Then click the expand icon again to view the specific configuration version you want to compare.
- Step 3** Under the Compare With column, choose the configuration for which you want to compare the configuration you selected in the previous step:
- **Previous**—Compares the selected version with the previously archived configuration.
 - **StartUp**—Compares the selected version with the start up configuration.
 - **Other Version**—Allows you to select with which version to compare the selected version.
 - **Other Device**—Allows you to compare the selected configuration with the configuration from another device.

The color key at the bottom of the report shows the differences between the configurations.

Overview of Device Configurations

You can change a device's configuration in two ways:

- **Operate > Device Work Center**—Use the Device Work Center to change the configuration of a single device. See [Changing a Single Device Configuration](#).
- **Design > Configuration Template**—To change the configuration of more than one device and apply a common set of changes, use a configuration template to make the changes.

Prime Infrastructure provides the following default configuration templates:

- **CLI templates**—CLI templates are user-defined and created based on your own parameters. CLI templates allow you to select the elements in the configurations. Prime Infrastructure provides variables which you replace with actual values and logic statements. You can also import templates from Cisco Prime LAN Management System. See [Creating CLI Configuration Templates](#).
- **Feature and technology templates**—Feature templates are configurations that are specific to a feature or technology in a device's configuration. See [Creating Feature and Technology Templates](#).

- Composite templates—Composite templates are two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices. See [Creating Composite Templates](#).

Changing a Single Device Configuration

-
- Step 1** Choose **Operate > Device Work Center**, then click on a device name.
The device details appear on the lower part of the screen.
- Step 2** Click the Configuration tab.
The Feature Selector displays the values, organized into features, for the device you selected.
- Step 3** Select the feature you want to change, then make the necessary changes.
- Step 4** Click **Save** to save your configuration changes in the Prime Infrastructure database. (To view the status of the configuration change, click **Administration > Jobs Dashboard**.)
You can also click any of the following icons:
- The Configuration Updates CLI Preview icon to view the CLI that was generated for the change you specified.
 - The Cancel Pending Deployment CLI icon to undo the change you made.
 - The Schedule Deploy icon to push the change to the device immediately or schedule when to deploy the change. You can also specify the job name.
-

Adding a Wireless LAN Controller

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Click **Add**. The Add Device page appears.
- Step 3** In the Add Device page, enter the necessary parameters.
- Step 4** Click **Add**.
-

Changing Wireless LAN Controller Configuration Settings

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Expand Device Type, and then click **Wireless Controller**.
- Step 3** Select the controller you want to change. The Device Work Center contains configuration functions at the bottom of the page. For details, see the [Device Work Center](#).
- Step 4** Click the **Configure** tab, then make the necessary changes.
- Step 5** Click **Save**.
-

Rebooting Controllers

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Expand Device Type, and then click **Wireless Controller**.
- Step 3** Select the check box(es) of the applicable controller(s).
- Step 4** From the Reboot drop-down list, choose **Reboot Controllers**.



Note Save the current controller configuration prior to rebooting.

- Step 5** Select the Reboot Controller options that must be applied.
- Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
 - Reboot APs—Select the check box to enable a reboot of the access point after making any other updates.
 - Swap AP Image—Indicates whether or not to reboot controllers and APs by swapping AP images. This could be either Yes or No.



Note Options are disabled unless the Reboot APs check box is selected.

- Step 6** Click **OK** to reboot the controller with the optional configuration selected.
-

Configuration Rollbacks

You can change the configuration on a device with a configuration stored in Prime Infrastructure. You can select multiple archived versions or a single archived version to which you want to “rollback.”

During the configuration rollback process, the configuration is converted into a set of commands which are then executed sequentially on the device.

When rolling back a configuration file you can specify the following options:

- The type of configuration file to which to rollback, for example running or startup configuration
- Whether to sync the running and startup configurations after rolling back the running configuration
- If rolling back a startup configuration only, specify to reboot the device so that startup configuration becomes the running configuration
- Before rolling back the configuration, specify whether to create new archived versions

Rolling Back Device Configuration Versions

You can use Prime Infrastructure to rollback a device’s configuration to a previous version of the configuration.

To roll back a configuration change.

-
- Step 1** Choose **Operate > Configuration Archives**.
 - Step 2** Click the expand icon for the device whose configuration you want to roll back.
 - Step 3** Click the specific configuration version you want to roll back, then click **Schedule Rollback**.
 - Step 4** Specify the rollback options.
 - Step 5** Specify the scheduling options.
 - Step 6** Click **Submit**.
-

Deleting Device Configurations

By default, Prime Infrastructure archives up to five device configuration versions for each device for seven days after:

- Every inventory collection
- Prime Infrastructure receives a configuration change event

You cannot delete configuration versions, but older configuration versions are replaced by newer configuration versions.

To change the number of configurations that Prime Infrastructure retains:

-
- Step 1** Choose **Administration > System Settings**, then click **Configuration Archive**.
 - Step 2** Enter a new value in the Number of Versions field. To archive an unlimited number of configuration versions, uncheck **Number of version to retain** and **Number of days to retain**.
 - Step 3** Click **Save**.
-

Configuring Redundancy on Controllers

The term Redundancy in the Prime Infrastructure refers to the High Availability (HA) framework in Controllers. Redundancy in wireless networks allows you to reduce the downtime of the networks. In a redundancy architecture, one controller is in the Active state and a second controller is in the Standby state, which continuously monitors the health of the controller in the Active state through a redundant port. Both controllers share the same configurations including the IP address of the management interface.

The Standby or Active state of a controller is based on the redundancy stock keeping unit (SKU), which is a manufacturing ordered unique device identification (UDI). A controller with redundancy SKU UDI is in the Standby state for the first time when it boots and pairs with a controller that runs a permanent count license. For controllers that have permanent count licenses, you can manually configure whether the controller is in the Active state or the Standby state.

In this release, a stateful switchover of access points (AP SSO) is supported. An AP SSO ensures that the AP sessions are intact even after a switchover.

**Note**

The stateful switchover of clients is not supported, which means that all clients, with the exception of clients on locally switched WLANs on access points in FlexConnect mode, are deauthenticated and forced to reassociate with the new controller in the Active state.

This section contains the following topics:

- [Prerequisites and Limitations for Redundancy, page 14-6](#)
- [Configuring Redundancy Interfaces, page 14-7](#)
- [Configuring Redundancy on a Primary Controller, page 14-7](#)
- [Configuring Redundancy on a Secondary Controller, page 14-8](#)
- [Monitoring and Troubleshooting the Redundancy States, page 14-9](#)
- [Configuring Peer Service Port IP and Subnet Mask, page 14-11](#)
- [Adding a Peer Network Route, page 14-11](#)
- [Administration commands for Redundancy, page 14-12](#)
- [Disabling Redundancy on Controllers, page 14-12](#)

Prerequisites and Limitations for Redundancy

Before configuring Redundancy, you must consider the following prerequisites and limitations:

- The Redundancy is supported only on the 5500, 7500, 8500, and Wism2 controllers.
- The primary and secondary controllers must be of the same hardware model.
- The primary and secondary controllers must be running the same Controller software release.
- The IP addresses of the Management, Redundancy Management, and Peer Redundancy Management interfaces must be in the same subnet.
- The service port IP address and route information is maintained for each device.
- If the Redundancy is enabled on a controller, the Prime Infrastructure or any other device cannot manage the standby controller.
- You cannot enable the Redundancy on a controller, if the controller is added to the Prime Infrastructure through the service port. You must delete the controller and add it through the management interface to enable the Redundancy on that controller.
- When there is an audit mismatch between a controller and the Prime Infrastructure, you must not restore the Redundancy parameters from the Prime Infrastructure on to the controller. However, you can refresh the Redundancy Parameters in the Prime Infrastructure.
- Before you enable the Redundancy, you must download the certificates for each device.
- Configuration is downloaded from the network to the active controller, and then the details are transferred to the standby controller through the Redundancy interface.
- When an old active controller pairs up with the new active controller, the control is not transferred back to the old active controller and it becomes the standby controller for the new active controller.

Configuring Redundancy Interfaces

There are two Redundancy interfaces—redundancy-management interface and redundancy-port interface. The redundancy-management interface is a local physical management interface that shares the subnet mask, gateway, and VLAN ID from the management interface. You must configure only the IP address for the redundancy management interface to enable Redundancy on the primary and secondary controllers. The IP address for the redundancy-port interface is auto-generated and it is used internally.

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the controller that you have chosen as the primary controller. The details of the device appear on the lower part of the page.
- Step 4** Click the **Configuration** tab.
- Step 5** From the left sidebar menu, choose **System > Interfaces**. The Interfaces list page appears.
- Step 6** Click the **redundancy-management** interface. The redundancy-management interface details page appears.
- Step 7** In the IP Address field, enter an IP address that belongs to the management interface subnet.
- Step 8** Click Save.
-

**Note**

You can also configure the IP address of the Redundancy Management in the Global Configuration details page. Choose **Operate > Device Work Center > Device Type > Wireless Controller > Controller > Configuration > Redundancy > Global Configuration** to access the Global Configuration details page.

Configuring Redundancy on a Primary Controller

To configure redundancy on a primary or active controller:

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the primary controller for which you have configured the redundancy-management interface IP address. The details of the controller appear on the lower part of the page.
- Step 4** Click the **Configuration** tab.
- Step 5** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.
- Step 6** You must configure the following parameters before you enable the Redundancy Mode for the primary controller:
- Redundancy-Management IP—The IP address of the local physical management interface, which you had configured in the redundancy-management interface details page is displayed. You can also modify the IP address.

- Peer Redundancy-Management IP—Enter the IP address of the peer redundancy management interface.
- Redundant Unit—Choose **Primary**.
- Mobility MAC Address—Enter the virtual MAC address for the Redundancy pair. Ensure that the mobility MAC address that you enter is the same for both primary and secondary controllers.

Step 7 Click **Save**. The Enabled check box for the Redundancy Mode becomes available for editing.

Step 8 Select the **Enabled** check box for the Redundancy Mode to enable the Redundancy on the primary controller.

**Note**

After you enable the Redundancy, you cannot modify the Redundancy-Management IP, Peer Redundancy-Management IP, Redundant Unit, and Mobility MAC Address.

**Note**

You cannot configure this controller during the Redundancy pair-up process.

Step 9 Click **Save**. The configuration is saved and the system reboots.

Configuring Redundancy on a Secondary Controller

To configure Redundancy on a secondary or standby controller:

Step 1 Choose **Operate > Device Work Center**.

Step 2 Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the controller that you have chosen as a secondary controller. The details of the controller appear on the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration Details page appears.

Step 6 You must configure the following parameters before you enable the Redundancy Mode for the secondary controller:

- Redundancy-Management IP—Enter the IP address of the local physical management interface. This IP address must be the same as the IP address of the peer redundancy management interface of the primary controller.
- Peer Redundancy-Management IP—Enter the IP address of the peer physical management interface. This IP address must be the same as the IP address of the local physical management interface of the primary controller.
- Redundant Unit—Choose **Secondary**.
- Mobility MAC Address—Enter the virtual MAC address of the Redundancy pair. Ensure that the mobility MAC address that you enter is the same for both primary and secondary controllers.

Step 7 Click **Save**. The Enabled check box for the Redundancy Mode becomes available for editing.

Step 8 Select the **Enabled** check box for the Redundancy Mode to enable the Redundancy on the secondary controller.

**Note**

After you enable the Redundancy, you cannot modify the Redundancy-Management IP, Peer Redundancy-Management IP, Redundant Unit, and Mobility MAC Address.

**Note**

You cannot configure the primary controller during the Redundancy pair-up process.

Step 9 Click **Save**. The configuration is saved and the system reboots.

Monitoring and Troubleshooting the Redundancy States

After the Redundancy mode is enabled on the primary and secondary controllers, the system reboots. The Redundancy state for both the controllers becomes Enabled in the Wireless Controller Members list page. The following traps are triggered:

- **RF_SWITCHOVER_ACTIVITY**—This trap is triggered when the standby controller becomes the new active controller. For more information about this trap, see the [“RF_SWITCHOVER_ACTIVITY” section on page 14-9](#).
- **RF_PROGRESSION_NOTIFY**—This trap is triggered by the primary or active controller when the peer state changes from 'Disabled' to 'StandbyCold', and then to 'StandbyHot'. For more information about this trap, see the [“RF_PROGRESSION_NOTIFY” section on page 14-10](#)
- **RF_HA_SUP_FAILURE_EVENT**—This trap is triggered when the redundancy fails because of a discrepancy between the active and the standby controllers. For more information about this trap, see the [“RF_HA_SUP_FAILURE_EVENT” section on page 14-10](#)

You can view the Redundancy state details such as the local and peer state, unit, IP addresses of the redundancy management, peer redundancy management, redundancy port, peer redundancy port, and peer service port of the paired controller. Choose **Operate > Device Work Center > Device Type > Wireless Controller > Controller > Device Details > Redundancy > Redundancy States** to view these details.

RF_SWITCHOVER_ACTIVITY

MIB Name	ciscoRFSwactNoti
Alarm Condition	Switch over activity triggered.
NCS Message	Switch Over Activity triggered. Controller <i>IP addr</i>
Symptoms	This notification is sent by the active controller when the switch over activity is triggered.
Severity	Critical
Category	Controller
Probable Causes	When the primary controller crashes or reboots, the switch over occurs and the secondary controller becomes active.
Recommended Actions	None.

RF_PROGRESSION_NOTIFY

MIB Name	ciscoRFProgressionNotif
Alarm Condition	Peer state of the active controller change.
NCS Message	<ol style="list-style-type: none"> 1. Redundancy notification trap triggered by controller <i>IP addr</i> having Redundancy-Management IP <i>IP addr</i>, Local state is 'Active' and Peer Redundancy-Management IP <i>IP addr</i> and peer state 'Disabled'. 2. Redundancy notification trap triggered by controller <i>IP addr</i> having Redundancy-Management IP <i>IP addr</i>, Local state is 'Active' and Peer Redundancy-Management IP <i>IP addr</i> and peer state 'StandbyCold'. 3. Redundancy notification trap triggered by controller <i>IP addr</i> having Redundancy-Management IP <i>IP addr</i>, Local state is 'Active' and Peer Redundancy-Management IP <i>IP addr</i> and peer state 'StandbyHot'.
Symptoms	This notification is sent by the active controller when the peer state changes from 'Disabled' to 'StandbyCold', and then to 'StandbyHot'.
Severity	Critical
Category	Controller
Probable Causes	<ol style="list-style-type: none"> 1. 'Disabled'—The Redundancy is enabled on the primary controller and it is disabled in the secondary controller. 2. 'StandbyCold'—The Redundancy is enabled on the secondary controller and the configuration synchronization is in progress between the primary and the secondary controllers. 3. 'StandbyHot'—The Redundancy pair up process is completed.
Recommended Actions	None.

RF_HA_SUP_FAILURE_EVENT

MIB Name	ciscoRFSupHAFailureEvent
Alarm Condition	Triggered when the Redundancy fails.
NCS Message	Redundancy Failure Event trap triggered by controller <i>IP addr</i> for the reason '{1}'.
Symptoms	This notification is sent when the Redundancy fails due to the discrepancy between the active and the standby controllers.
Severity	Major.
Category	Controller
Probable Causes	None.
Recommended Actions	None.

Running Redundancy Status Background Tasks

Sometimes, when the peer state changes from 'StandbyCold' to 'StandbyHot', the Redundancy traps are missed by the Prime Infrastructure. As a result, the Redundancy pair-up process cannot be completed. To fix this issue, you must run the Redundancy Status background task manually.

To run the Redundancy Status background task:

-
- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Under the Other Background Tasks section, select the **Redundancy Status** background task.
- Step 3** From the Select a command drop-down list, select **Execute Now**.
- Step 4** Click **Go**.
-

When traps are missed by the Prime Infrastructure, you must run this background task to complete the following:

- Remove the standby controller from the Prime Infrastructure.
- Swap the network route table entries with the peer network route table entries.
- Update the Redundancy state information and system inventory information.

Once the Redundancy pair-up process is completed, the Redundancy state for the active controller becomes Paired and the standby controller is removed from the Prime Infrastructure.

Configuring Peer Service Port IP and Subnet Mask

You can configure a peer service port IP address and a subnet mask only when the state of the peer controller is in 'StandbyHot'. Ensure that DHCP is disabled on local service port before you configure the peer service port IP address.

To configure the peer service port IP and subnet mask:

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the primary or active controller. The details of the controller appear on the lower part of the page.
- Step 4** Click the **Configuration** tab.
- Step 5** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.
- Step 6** In the Peer Service Port IP field, enter the IP address of the peer service port.
- Step 7** In the Peer Service Netmask IP field, enter the IP address of the peer service subnet mask.
- Step 8** Click **Save**.
-

Adding a Peer Network Route

You can add a peer network route on an active controller only when the state of the peer controller is in 'StandbyHot'. A new network route table is maintained. When the standby controller becomes active, the entries of the network route table swaps with the entries of the peer network route table.

To add a peer network route:

-
- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.

- Step 3** Select the primary controller for which you have configured the redundancy-management interface IP address. The details of the controller appear on the lower part of the page.
 - Step 4** Click the **Configuration** tab.
 - Step 5** From the left sidebar menu, choose **Redundancy > Peer Network Route**.
 - Step 6** From the Select a command drop down list, choose **Add Peer Network Route**.
 - Step 7** Click **Go**. The Peer Network Route Details page appears.
 - Step 8** Configure the required fields.
 - Step 9** Click **Save**. The peer network route is added.
-

Administration commands for Redundancy

When the standby controller is in the 'StandbyHot' state and the Redundancy pair-up process is completed, you can reset the standby controller using the **Reset Standby** command. Also, you can upload files from the standby controller to the active controller using the **Upload File from Standby Controller** command. Choose **Operate > Device Work Center > Device Type > Wireless Controller > Controller > Device Details > Redundancy > Redundancy Commands** to access these commands.

Disabling Redundancy on Controllers

To disable redundancy on a controller:

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
 - Step 3** Select the controller for which you want to disable the redundancy. The details of the controller appear on the lower part of the page.
 - Step 4** Click the **Configuration** tab.
 - Step 5** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.
 - Step 6** Deselect the **Enabled** check box for the Redundancy Mode to disable the Redundancy on the selected controller.
 - Step 7** Click **Save**. The configuration is saved and the system reboots.
-

When you disable redundancy on the controller, both active and standby controllers reboot. You must refresh the configuration from the device to remove any audit mismatches in the Redundancy parameters. The active controller becomes a standalone controller and the standby controller reboots with all the ports disabled.



CHAPTER 15

Maintaining Device Configuration Inventory

Overview of Device Configuration Archive

When Prime Infrastructure discovers the devices in your network, it retrieves and stores the device configurations in its archives. When you make a change to a device configuration, Prime Infrastructure stores the previous version as well as the current version. Prime Infrastructure stores all device configuration versions.

You can perform configuration archive tasks in two places:

- **Operate > Configuration Archives**—Lists all configuration archives by device type, site group, or user-defined group. You can schedule archive collections, rollbacks, and view details of configurations.
- **Operate > Device Work Center**—View a specific device's archived configurations, compare its configurations, schedule a configuration rollback, and schedule archive collections for that device.

Changing Configuration Archive Settings

By default, Prime Infrastructure archives up to five device configuration versions for each device for seven days after:

- Every inventory collection
- Prime Infrastructure receives notification of a configuration change event

To change when Prime Infrastructure archives configurations:

-
- | | |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Administration > System Settings > Configuration Archive . |
| Step 2 | Change the necessary settings. To archive an unlimited number of configuration versions, uncheck Number of version to retain and Number of days to retain . |
| Step 3 | To have Prime Infrastructure ignore commands for a particular device type, click the Advanced tab, choose the device type, and enter the commands to be ignored.

If the device you specify has a change in its configuration and Prime Infrastructure detects that the change is in one of the commands in the exclude list, Prime Infrastructure does not create an archived version of the configuration with this change. |
| Step 4 | Click Save . |
-

Scheduling Configuration Archive Collection

To specify when to archive configurations:

-
- Step 1** Choose **Operate > Configuration Archives**.
 - Step 2** Choose the device(s) whose configuration you want to archive, then click **Schedule Archive**.
 - Step 3** In the Configuration Archive Schedule window, enter schedule parameters for the archive collection.
 - Step 4** Click **Save**.
 - Step 5** To view the progress of the configuration archive job, choose **Administration > Jobs Dashboard**.
-

Comparing Configuration Archives

You can compare any two archived running or startup configurations to find changes made to a device. If you decide to cancel a configuration change, you can roll back to any earlier archived configuration (see [Rolling Back Configuration Changes, page 15-2](#)).

To compare archived configurations:

-
- Step 1** Choose **Operate > Device Work Center**.
 - Step 2** Choose the device whose configurations you want to compare, then click **Configuration Archive**. The list of archived configurations for the selected device appears.
 - Step 3** Click the expand icon for the archived configuration you want to compare with others.
 - Step 4** Click the appropriate link in the **Compare With** column:
 - a. To compare the running and startup configurations, click **Startup**.
 - b. To compare the archived configuration with another archived version, click **Other Version**. Then select the other archived version and click **Compare**.
 - c. To compare the archived configuration with an archived configuration on a different device, click **Other Device**. Then select the other device and click **Compare**.
 - Step 5** To see only the differences between the two configuration archives you are comparing:
 - a. Click **Raw Configuration**.
 - b. From the **Select Type** drop-down menu, choose **Difference only**.
The differences are highlighted in red.
-

Rolling Back Configuration Changes

You can use Prime Infrastructure to rollback a device's configuration to a previous version of the configuration. See [Rolling Back Device Configuration Versions](#) for more information.



CHAPTER 16

Maintaining Software Images

Manually upgrading your devices to the latest software version can be error prone and time consuming. Prime Infrastructure simplifies the version management and routine deployment of software updates to your devices by helping you plan, schedule, download, and monitoring software image updates. You can also view software image details, view recommended software images, and delete software images.

Prime Infrastructure stores all the software images for the devices in your network. The images are stored according to the image type and version.

Before you can upgrade software images, your devices must be configured with SNMP read-write community strings that match the community strings entered when the device was added to Prime Infrastructure.

Related Topics

- [Setting Image Management and Distribution Preferences](#)
- [Managing Software Images](#)
- [Importing Software Images](#)
- [Changing Software Image Requirements](#)
- [Deploying Software Images to Devices](#)
- [Distributing Software Images from Cisco.com](#)
- [Viewing Recommended Software Images](#)
- [Analyzing Software Image Upgrades](#)

Setting Image Management and Distribution Preferences

You can specify image management preferences such as whether to reboot devices after successfully upgrading a software image, and whether images on Cisco.com should be included during image recommendation of the device.

Because collecting software images can slow the data collection process, by default, Prime Infrastructure does not collect and store device software images when it gathers inventory data from devices.

To change the default behavior and to specify additional image management preferences:

-
- Step 1** Choose **Administration > System Settings > Image Management**.
- Step 2** Enter your Cisco.com user name and password so you can access software images from the cisco.com web site.

- Step 3** To have Prime Infrastructure automatically retrieve and store device images when it collects device inventory data, check **Collect images along with inventory collection**.
 - Step 4** Select other options as necessary. Rest your cursor on the information icon to view details about the options.
 - Step 5** Click **Save**.
 - Step 6** Choose **Operate > Image Dashboard** to view all the software images retrieved by Prime Infrastructure. The images are organized by image type and stored in the corresponding software image group folder.
-

Managing Software Images

The software image dashboard displays the top software images used in your network and allows you to change image requirements, see the devices on which an image is running, and distribute images.

-
- Step 1** Choose **Operate > Image Dashboard**.
 - Step 2** Click on a software image name to display details about the image.
 - Step 3** You can perform the following actions:
 - Change image requirements. See [Changing Software Image Requirements](#).
 - View the devices on which the software image is running.
 - Distribute the image. See [Deploying Software Images to Devices](#).
-

Importing Software Images

It can be helpful to have a baseline of your network images by importing images from the devices in your network. You can also import software images from Cisco.com and store them in the image repository.

By default, Prime Infrastructure does not automatically retrieve and store device images when it collects device inventory data. (You can change this preference as described in [Setting Image Management and Distribution Preferences](#).)



Note

For wireless LAN controllers, you can import software images from Cisco.com, file, or a URL, but not from a device.

To import a software image:

-
- Step 1** Choose **Operate > Software Image Management**.
 - Step 2** Click **Import**.
 - Step 3** Specify the source from where to import the software image.
 - Step 4** Specify Collection Options and when to import the image file. You can run the job immediately or schedule it to run at a later time.



Note The image import job is non-repetitive.

Step 5 Click **Submit**.

Step 6 Choose **Tools > Task Manager > Jobs Dashboard** to view details for the image management job.

Related Topics

- [Deploying Software Images to Devices](#)
- [Distributing Software Images from Cisco.com](#)

Changing Software Image Requirements

To change the RAM, Flash, and boot ROM requirements that a device must meet in order for a software image to be distributed to the device:

Step 1 Choose **Operate > Software Image Management**.

Step 2 Navigate to and select the software image for which you want to change requirements, then click **Image Details**.

Step 3 Modify the necessary fields, then click **Save**. Your changes are saved in the software version in which you made the change.

Deploying Software Images to Devices

You can distribute a software image to a device or set of similar devices in a single deployment. Prime Infrastructure verifies that the device and software image are compatible.

Step 1 Choose **Deploy > Software Deployment**.

Step 2 Select the software image(s) you want to distribute, then click **Distribute**.

By default, the devices for which the selected image is applicable are shown.

Step 3 Check **Show All Devices** to see all the devices available in Prime Infrastructure, or from the Device Groups list, select the device(s) which are running the image you selected.



Note If you check **Show All Devices**, all devices are displayed even if the software image you selected is not applicable for all the devices.

Step 4 Click the image name in Distribute Image Name field to change your selection and pick a new image, then click **Save**.

Step 5 To change the location on the device in which to store the software image, click the value displayed in Distribute Location field, select a new location, then click **Save**.

The Status and Status Message fields display the validity of the selections you made. For example, if the status is green, there is adequate space available to store the image on the specified location on the device.

Step 6 Specify Distribution Options. You can change the default options in **Administration > System > Image Management**.

Step 7 Specify schedule options, then click **Submit**.



Note The distribute image job is non-repetitive.

Step 8 Choose **Administration > Jobs Dashboard** to view details for the image management job.

Distributing Software Images from Cisco.com

Step 1 Choose **Operate > Software Image Management**.

Step 2 Navigate to and select the software image for which you want to change requirements, then click **Image Details**.

Step 3 Expand Device Details, select a device or devices on which to distribute the image, then click **Distribute**.



Note Only the devices that are running the specific software image you modified are displayed as selection choices.

Step 4 Choose one of the following image sources:

- **Recommend Image from Cisco.com** to select an image available on Cisco.com. Specify options, then click **Start Recommendation**, then skip to Step 6.



Note For wireless LAN controllers, you cannot recommend software images because the flash requirement is not available. Whereas, you can upgrade/distribute software images.

- **Select Image from Local Repository** to select an image stored locally. Then, under Local Repository:
 - Select **Show All Images** to display all images available in the Prime Infrastructure repository.
 - Uncheck **Show All Images** to display the software images applicable to the selected device.

Step 5 Select the image to distribute, then click **Apply**.

Step 6 Click the image name in Distribute Image Name field to change your selection and pick a new image, then click **Save**.

Step 7 To change the location on the device in which to store the software image, click the value displayed in Distribute Location field, select a new location, then click **Save**.

The Status and Status Message fields display the validity of the selections you made. For example, if the status is green, there is adequate space available to store the image on the specified location on the device.

- Step 8** Specify Distribution Options. You can change the default options in **Administration > System > Image Management**.
- Step 9** Specify schedule options, then click **Submit**.
-

Viewing Recommended Software Images

You can view the recommended software image for a single device, and then import or distribute that image. If you want to distribute a software image to multiple devices, see [Deploying Software Images to Devices](#).

- Step 1** Choose **Operate > Device Work Center**, then select a device for which you want to view the recommended software image.
- Step 2** Click the **Image** tab.
- Step 3** Scroll down to Recommended Images to view the recommended image for the device you selected. Prime Infrastructure gathers the recommended images from both Cisco.com and from the local repository.
- Step 4** You can import the recommended image (see [Importing Software Images](#)) or distribute (see [Deploying Software Images to Devices](#)) the recommended image.
-

Analyzing Software Image Upgrades

Prime Infrastructure can generate an Upgrade Analysis report to help you determine prerequisites for a new software image deployment. These reports analyze the software images to determine the hardware upgrades (boot ROM, Flash memory, RAM, and boot Flash, if applicable) required before you can perform the software upgrade.

The Upgrade Analysis report answers the following questions:

- Does the device have sufficient RAM to hold the new software?
- Is the device's Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device?



Note

For wireless LAN controllers, you cannot generate the Upgrade Analysis report because there is no minimum requirement for RAM or ROM. The newly upgraded image replaces the existing image after an upgrade.

To run the Upgrade Analysis report:

- Step 1** Choose **Operate > Software Image Management**.
- Step 2** Click **Upgrade Analysis**.
- Step 3** Choose the source of the software image you want to analyze.
- Step 4** Select the devices on which to analyze the software image.

Step 5 Select the image(s) to analyze for the selected devices.

Step 6 Click **Run Report**.



CHAPTER 17

Working with Wireless Operational Tools

The Wireless Operational Tools menu provides access to the Guest User Controller Templates, Voice Audit, Voice Diagnostic, Location Accuracy Tool, Configuration Audit Summary, Migration Analysis, Radio Resource Management (RRM), RFID Tags, Chokepoints, Interferers, Spectrum Experts, and WiFi TDOA Receivers features of the Cisco Prime Infrastructure. This chapter contains the following sections:

- [Configuring Guest User Templates, page 17-1](#)
- [Running Voice Audits, page 17-2](#)
- [Running Voice Diagnostic, page 17-3](#)
- [Configuring the Location Accuracy Tools, page 17-4](#)
- [Configuring Audit Summary, page 17-7](#)
- [Configuring Migration Analysis, page 17-8](#)
- [Monitoring Radio Resource Management \(RRM\), page 17-10](#)
- [Monitoring RFID Tags, page 17-13](#)
- [Configuring Chokepoints, page 17-16](#)
- [Monitoring Interferers, page 17-19](#)
- [Configuring Spectrum Experts, page 17-22](#)
- [Configuring Wi-Fi TDOA Receivers, page 17-23](#)

Configuring Guest User Templates

This page allows you to add a guest user template or make modifications to an existing guest user template. The purpose of a guest user account is to provide a user account for a limited amount of time. A Lobby Ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires. See the [Managing Guest User Accounts, page 28-4](#) for further information on guest access.

-
- Step 1** Choose **Operate > Operational Tools > Wireless > Guest User**. The Guest Users Controller Templates page appears.

**Note**

To reduce clutter, Prime Infrastructure does not show expired templates by default. You can specify which guest users to filter based on their status (active, scheduled, expired, not active, or none). Use the Select a Status Filter drop-down list to determine the filter criteria.

- Step 2** If you want to add a new template, choose **Add Guest User** from the Select a command drop-down list, and click **Go**. The New Controller Template page appears.

**Note**

You can also modify an existing template by clicking the template name link.

- Step 3** In the New Controller Template page, complete the fields as described in [Table 31-68](#) and [Table 31-69](#).

- Step 4** Click **Save**.

Running Voice Audits

Prime Infrastructure provides voice auditing mechanism to check the controller configuration and to ensure that any deviations from the deployment guidelines are highlighted as an Audit Violation.

To access the Voice Audit feature, choose **Operate > Operational Tools > Wireless > Voice Audit**. The Voice Audit Report page appears. For information about the tabs and fields on this page, see [Table 31-70](#).

This section contains the following topic:

- [Running Voice Audits on Controllers, page 17-2](#)

Running Voice Audits on Controllers

To run the voice audit, you must first choose the controller(s) on which to run the voice audit, and then indicate the applicable VoWLAN SSID and the applicable rules for this voice audit.

The Controllers tab allows you to choose the controller(s) on which to run the voice audit and the Rules tab allows you to indicate the applicable rules for the voice audit.

**Note**

You can run the voice audit on a maximum of 50 controllers in a single operation.

To run the voice audit:

- Step 1** Choose **Operate > Operational Tools > Wireless > Voice Audit**.
- Step 2** Click the **Controllers** tab, and complete the fields as described in
- Step 3** Click the **Rules** tab to determine the rules for this voice audit.
- Step 4** In the VoWLAN SSID field, type the applicable VoWLAN SSID. For information about the Rules and Rule Details, see [Table 31-71](#).

**Note**

The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.

- Step 5** When the rules are configured for this voice audit, click **Save** to save the current configuration or **Save and Run** to save the configuration and run the report.
- Step 6** Click the **Report** tab to view the Report results. See [Table 31-72](#) for more information.

Running Voice Diagnostic

The Voice diagnostic tool is an interactive tool to diagnose the voice calls in real time. This tool reports call control related errors, roaming history of the clients and the total active calls accepted and rejected by an associated AP. This tool enables you to start or stop the voice diagnostic.

The Voice diagnostic test is provisioned for multiple controllers, that is if the AP is associated to more than one controller during roaming, the Voice diagnostics tests all the associated controllers. Prime Infrastructure supports testing on controllers whose APs are placed on +/- 3 floors. For example, Prime Infrastructure map has floors 1 to 4 and all APs are associated to controllers (wlc1, wlc2, wlc3, wlc4) and are placed on the Prime Infrastructure map, if a client is associated on any AP with WLC1 on first floor and if voice diagnostic test is started for this client, test will also be provisioned on wlc2 to wlc3 also). This is done for roaming reason.

The Voice diagnostic page lists the prior test runs, if any. For information about the fields on this page, see [Table 31-73](#).

You can either start a new test or view the existing test results or delete a test from the Select a command from the drop-down list.



Note


To support roaming, the tool figures out controllers in the same building as of client's associated AP building and adds to all controller's watchlist. The tool looks for controllers in +/-5 floors from client's current association A's location to configure on controllers. Configuration on controller's watchlist is done for 10 minutes. After 10 minutes controller will remove the entry from the watchlist.

This section contains the following topic:

- [Starting the Voice Diagnostic Test, page 17-3](#)

Starting the Voice Diagnostic Test

To start a Voice Diagnostic test:

- Step 1** Click **Operate > Operational Tools > Wireless > Voice Diagnostics**.
- Step 2** From the Select a command drop-down list, click the New test and click Go. It takes you to the configuration page.
-  **Note** On this page, you can configure maximum of two clients for voice call diagnosis. Both clients can be on the same call or can be in a different call.
- Step 3** Enter the Test name and the time duration to monitor the voice call. You can do a voice diagnosis test for 10, 20, 30, 40, 50 or 60 minutes. 10 minutes is the default duration selected by Prime Infrastructure.
- Step 4** Enter the MAC address of the device for which you want to do the voice diagnostic test.

- Step 5** Select the device type. It could be either a cisco based phone or custom phones. If it is a custom phone you have to enter the RSSI range for the custom phone. For Cisco phones the RSSI range is preselected.
- Step 6** Click StartTest to start the test or if the test is completed you can restart the test.



Note If the test is not completed the state is Running and if test is completed then the state is Completed. To stop the test in between, you can use the Stop button, the state is then stopped.

For information about the details displayed on the Voice Diagnostic Test Report page, see [Table 31-74](#).

Configuring the Location Accuracy Tools

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy Tools.

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

The Location Accuracy Tools enable you to run either of the following tests:

There are two ways to test location accuracy:

- **Scheduled Accuracy Testing**—Employed when clients, tags, and interferers are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients, tags, and interferers are already pre-positioned so that the test can be run on a regularly scheduled basis.
- **On-Demand Accuracy Testing**—Employed when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

Both are configured and executed through a single page.

This section contains the following topics:

- [Enabling the Location Accuracy Tool, page 17-4](#)
- [Using Scheduled Accuracy Testing to Verify Accuracy of Current Location, page 17-5](#)
- [Using On-demand Accuracy Testing to Test Location Accuracy, page 17-6](#)

Enabling the Location Accuracy Tool



Note

You must enable the **Advanced Debug** option in Prime Infrastructure to use the Scheduled and On-demand location accuracy tool testing features. The Location Accuracy Tool does not appear as an option on the Operate > Operational Tools > Wireless menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in Prime Infrastructure:

- Step 1** In Prime Infrastructure, choose **Operate > Maps**.

Step 2 Choose **Properties** from the Select a command drop-down list, and click **Go**.

Step 3 In the page that appears, select the **Enabled** check box to enable the Advanced Debug Mode. Click **OK**.



Note If Advanced Debug is already enabled, you do not need to do anything further. Click **Cancel**.

You can now run location accuracy tests on the mobility services engine using the Location Accuracy Tool.

Use the Select a command drop-down list to create a new scheduled or on-demand accuracy test, to download logs for last run, to download all logs, or to delete a current accuracy test.



Note

- You can download logs for accuracy tests from the Accuracy Tests summary page. To do so, select an accuracy test and from the Select a command drop-down list, choose either **Download Logs** or **Download Logs for Last Run**. Click **Go**.
- The Download Logs option downloads the logs for all accuracy tests for the selected test(s).
- The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test:

Step 1 Choose **Operate > Operational Tools > Wireless > Location Accuracy Tool**.

Step 2 Choose **New Scheduled Accuracy Test** from the Select a command drop-down list.

Step 3 Enter a Test Name.

Step 4 Choose the **Area Type** from the drop-down list.

Step 5 Campus is configured as Root Area, by default. There is no need to change this setting.

Step 6 Choose the Building from the drop-down list.

Step 7 Choose the Floor from the drop-down list.

Step 8 Choose the begin and end time of the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.



Note When entering the test start time, be sure to allow enough time prior to the test start to position testpoints on the map.

Step 9 Test results are viewed in the Accuracy Tests > Results page. Reports are in PDF format.



Note If you choose the e-mail option, an SMTP Mail Server must first be defined for the target e-mail address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.

Step 10 Click **Position Testpoints**. The floor map appears with a list of all clients, tags, and interferers on that floor with their MAC addresses.

Step 11 Select the check box next to each client, tag, and interferer for which you want to check the location accuracy.

When you select a MAC address check box, two icons appear on the map. One icon represents the actual location and the other represents the reported location.



Note To enter a MAC address for a client or tag or interferer that is not listed, select the **Add New MAC** check box, enter the MAC address, and click **Go**. An icon for the element appears on the map. If the newly added element is on the location server but on a different floor, the icon is displayed in the left-most corner (0,0 position).

Step 12 If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map. Only the actual location icon can be dragged.

Step 13 Click **Save** when all elements are positioned. A dialog box appears confirming successful accuracy testing.

Step 14 Click **OK** to close the confirmation dialog box. You are returned to the Accuracy Tests summary page.



Note The accuracy test status is displayed as **Scheduled** when the test is about to execute. A status of **Running** is displayed when the test is in process and **Idle** when the test is complete. A **Failure** status appears when the test is not successful.

Step 15 To view the results of the location accuracy test, click the test name and then click the **Results** tab in the page that appears.

Step 16 In the Results page, click the **Download** link under the Saved Report heading to view the report.

The Scheduled Location Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram.
- A cumulative error distribution graph.
- An error distance over time graph.
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location), and error distance over time for each MAC.

Using On-demand Accuracy Testing to Test Location Accuracy

An On demand Accuracy Test is run when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

To run an On-demand Accuracy Test:

-
- Step 1** Choose **Operate > Operational Tools > Wireless > Location Accuracy Tool**.
- Step 2** From the Select a command drop-down list, choose **New On demand Accuracy Test**.
- Step 3** Enter a Test Name.
- Step 4** Choose **Area Type** from the drop-down list.
- Step 5** Campus is configured as Root Area, by default. There is no need to change this setting.
- Step 6** Choose the Building from the drop-down list.
- Step 7** Choose the Floor from the drop-down list.
- Step 8** Choose the Destination point for the test results. Test results are viewed in the Accuracy Tests > Results page. Reports are in PDF format.
- Step 9** Click **Position Testpoints**. The floor map appears with a red crosshair at the (0,0) coordinate.
- Step 10** To test the location accuracy and RSSI of a particular location, select either client or tag or interferer from the drop-down list on the left. A list of all MAC addresses for the selected option (client or tag or interferer) displays in a drop-down list to its right.
- Step 11** Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.
- Step 12** From the Zoom percentage drop-down list, choose the zoom percentage for the map.
The X and Y text boxes are populated with the coordinates based on the position of the red cross hair in the map.
- Step 13** Click **Start** to begin collection of accuracy data.
- Step 14** Click **Stop** to finish collection. You should allow the test to run for at least two minutes before clicking Stop.
- Step 15** Repeat [Step 11](#) to [Step 14](#) for each testpoint that you want to plot on the map.
- Step 16** Click **Analyze Results** when you are finished mapping the testpoints.
- Step 17** Click the **Results** tab in the page that appears.
The On-demand Accuracy Report includes the following information:
- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
 - An error distance histogram
 - A cumulative error distribution graph
-

Configuring Audit Summary

Choose **Operate > Operational Tools > Wireless > Configuration Audit** to launch the Config Audit Summary page.

This page provides a summary of the following:

- Total Enforced Config Groups—Identifies the count of config group templates, which are configured for Background Audit and are enforcement enabled.

Click the link to launch the Config Group page to view config groups with Enforce Configuration enabled.

- **Total Mismatched Controllers**—Identifies the number of mismatched controllers. Mismatched controllers indicate that there were configuration differences found between Prime Infrastructure and the controller during the last audit.

Click the link to launch the controller list sorted in the mismatched audit status column. Click an item in the Audit Status column to view the audit report for this controller.

- **Total Config Audit Alarms**—Identifies the number of alarms generated when audit discrepancies are enforced on config groups.

Click the link to view all config audit alarm details.



Note

If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- **Most recent 5 config audit alarms**—Lists the most recent configuration audit alarms including the object name, event type, date, and time for the audit alarm.

Click **View All** to view the applicable Alarm page that includes all configuration audit alarms.

Configuring Migration Analysis

Choose **Operate > Operational Tools > Wireless > Migration Analysis** to launch the Migration Analysis Summary page.



Note

You can also access the migration analysis summary by choosing **Design > Wireless Configuration > Autonomous AP Migration Templates** and choosing **View Migration Analysis Summary** from the Select a command drop-down list.

The autonomous access points are eligible for migration only if all the criteria has a pass status. A red X designates ineligibility, and a green check mark designates eligibility. These columns represent the following:

- **Privilege 15 Criteria**—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- **Software Version**—Conversion is supported only from 12.3(7)JA releases excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- **Role Criteria**—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
 - root
 - root access point
 - root fallback repeater
 - root fallback shutdown
 - root access point only

Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

This section contains the following topics:

- [Upgrading Autonomous Access Points, page 17-9](#)
- [Viewing a Firmware Upgrade Report, page 17-10](#)
- [Viewing a Role Change Report, page 17-10](#)

Upgrading Autonomous Access Points

You can choose to upgrade the autonomous access points manually or automatically. In the Migration Analysis page, you can select the access point with the software version listed as failed and choose **Upgrade Firmware (Manual or Automatic)** from the Select a command drop-down list. This process upgrades the autonomous firmware image of the Cisco IOS access point to a supported version.

Prime Infrastructure uses a Telnet-based connection to upgrade the access point firmware. If you choose the automatic option, the internal TFTP server is used with the default images present in Prime Infrastructure. The default images per device type are as follows:

- ap801-k9w7-tar.124-10b.JA3.tar
- ap802-k9w7-tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar
- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

If you choose the manual option, an additional page with TFTP server IP, file path, and file path name appears. The final page is the Report page.

Changing Station Role to Root Mode

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role. If the role shows as ineligible, choose **Change Station Role to Root Mode** from the Select a command drop-down list to change the mode.

Running Migration Analysis

Choose **Run Migration Analysis** from the Select a command drop-down list of the Migration Analysis Summary page. The resulting migration analysis summary shows the current status of different criteria. Initially, migration analysis is run automatically when the access point is discovered.

Viewing the Migration Analysis Report

You can choose **View Migration Analysis Report** from the Select a command drop-down list of the Migration Analysis Summary page to generate a report. The report includes the following:

- Access point address
- Status
- Timestamp
- Access point logs

Viewing a Firmware Upgrade Report

Choose **View Firmware Upgrade Report** from the Select a command drop-down list to view a current report of the upgrade status for the selected access point.

The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the firmware upgrade.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

See the [“Upgrading Autonomous Access Points” section on page 17-9](#) for more information.

Viewing a Role Change Report

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role.

To view a report of these role changes, choose **View Role Change Report** from the Select a command drop-down list. The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the role change.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

Monitoring Radio Resource Management (RRM)

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points.

Radio Resource Management (RRM), built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment.

Prime Infrastructure would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into Prime Infrastructure events as informational and were maintained by the event dispatcher. The reason behind the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load, and the like) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

Radio Resource Management (RRM) statistics helps to identify trouble spots and provides possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (worst performing access points, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, pre-coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).

**Note**

The RRM dashboard information is only available for lightweight access points.

This section contains the following topics:

- [Channel Change Notifications, page 17-11](#)
- [Transmission Power Change Notifications, page 17-11](#)
- [RF Grouping Notifications, page 17-11](#)
- [Viewing the RRM Dashboard, page 17-11](#)

Channel Change Notifications

Notifications are sent to Prime Infrastructure RRM dashboard when a channel change occurs. Channel changes depend on the Dynamic Channel Assignment (DCA) configuration where the mode can be set to *auto* or *on demand*. When the mode is *auto*, channel assignment is periodically updated for all lightweight access points which permit this operation. When the mode is set to *on demand*, channel assignments are updated based on request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

When a channel change trap is received and a channel change had occurred earlier, the event is marked as Channel Revised; otherwise, the event is marked as Channel Changed. Each event for channel change can be caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur. For example, suppose a channel change is caused by signal, interference, or noise. When the reason code is received in the notification, the reason code is refactored across the reasons. If three reasons caused the event to occur, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events are received with the same reason code, all of the three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

Notifications are sent to Prime Infrastructure RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has three modes: Automatic, Off and Leader. When the grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When the grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping automatic, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

Viewing the RRM Dashboard

Choose **Operate > Operational Tools > Wireless > Radio Resource Management** to access the RRM dashboard.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups.



Note To get the latest number of RF Groups, you have to run the configuration sync background task.

- The RRM Statistics portion shows network-wide statistics
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
 - Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio(s) improved the channel plan of the system as evaluated by the algorithm.
 - WiFi Interference
 - Load
 - Radar
 - Noise
 - Persistent Non-WiFi Interference
 - Major Air Quality Event
 - Other
- The Channel Change shows all events complete with causes and reasons.
- The Configuration Mismatch portion shows comparisons between leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour period.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups (derived from all the controllers which are currently managed by Prime Infrastructure).
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the preset value.



Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- **Channel Change Causes**—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- **Channel Change - APs with channel changes**—Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- **Coverage Hole - APs reporting coverage holes**—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event (threshold based) are displayed.
- **Aggregated Percent Max Power APs**—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.

**Note**

This maximum power portion shows the values from the last 24 hours and is poll driven. This occurs every 15 minutes or as configured for radio performance.

- **Percent Time at Maximum Power**—A list of the top five 802.11a/n lightweight access points which have been operating at maximum power.

**Note**

This maximum power portion shows the value from the last 24 hours and is only event driven.

Monitoring RFID Tags

The Monitor > RFID Tags page allows you to monitor tag status and location on Prime Infrastructure maps as well as review tag details.

**Note**

This page is only available in the Location version of Prime Infrastructure.

This section provides information on the tags detected by the location appliance.

Choose **Operate > Operational Tools > Wireless > RFID Tags** to access this section. By default, the [Tag Summary](#) page is displayed.

This section contains the following topics:

- [Tag Summary, page 17-14](#)
- [Searching Tags, page 17-14](#)
- [Viewing RFID Tag Search Results, page 17-14](#)
- [Viewing Tag List, page 17-15](#)

Tag Summary

Choose **Operate > Operational Tools > Wireless > RFID Tags** to access this page.

This page provides information on the number of tags that are detected by MSE. The following fields are displayed in the main data area:

- **Device Name**—Name of the MSE device.
- **Total Tags**—Click the number to view tag details. Clicking the number shows the list of tags located by the MSE. Clicking a MAC address shows the tag details pertaining to that MAC address.

Searching Tags

Use Prime Infrastructure Advanced Search feature to find specific or all tags.

To search for tags in Prime Infrastructure:

Step 1 Click **Advanced Search**.

Step 2 Choose **Tags** from the Search Category drop-down list.

Step 3 Identify the applicable tag search fields including:

- **Search By**—Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.



Note Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.

- **Search In**—Choose MSEs or Prime Infrastructure Controllers.
- **Last detected within**—Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.
- **Tag Vendor**—Select the check box, and choose **Aeroscout**, **G2**, **PanGo**, or **WhereNet**.
- **Telemetry Tags only**—Select the Telemetry Tags only check box to search tags accordingly.

Step 4 Click **Go**.

Viewing RFID Tag Search Results

Use Prime Infrastructure Advanced Search feature located in the top right of Prime Infrastructure page to search for tags by asset type (name, category and group), by MAC address, by system (controller or location appliance), and by area (floor area and outdoor area).



Note

Search fields might change depending on the selected category. When applicable, enter the additional field or filter information to help identify the Search By category.

You can further refine your search using the Advanced search fields and save the search criteria for future use. Saved search criteria can be retrieved from the Saved Searches located in the navigation bar. For more information, see [Advanced Search](#) and [Saved Searches](#) in the [Cisco Prime Infrastructure Configuration Guide, Release 1.2](#).

When you click the MAC address of a tag location in a search results page, the following details appear for the tag:

- Tag vendor



Note This option does not appear when Asset Name, Asset Category, Asset Group or MAC Address are the search criteria for tags.

- Controller to which the tag is associated
- Telemetry data (CCX v1 compliant tags only)
 - Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.



Note The Telemetry data option only appears when MSE (select for location servers), Floor Area, or Outdoor Area are selected as the Search for tags by option.



Note Only those vendor tags that support telemetry appear.

- Asset Information (Name, Category, Group)
- Statistics (bytes and packets received)
- Location (Floor, Last Located, MSE, map)
- Location Notification (Absence, Containment, Distance, All)



Note Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.

- Emergency Data (CCX v1 compliant tags only)

Viewing Tag List

Click the **Total Tags number** link to view the Tags List for the applicable device name. The Tag List contains the following information:

- MAC Address
- Asset Name
- Asset Group
- Asset Category
- Vendor Name

- Mobility Services Engine
- Controller
- Battery Status
- Map Location

Configuring Chokepoints

Chokepoints are low frequency transmitting devices. When a tag passes within range of placed chokepoint, the low-frequency field awakens the tag that in turn sends a message over the Cisco Unified Wireless Network including the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room level accuracy (ranging from few inches to 2 feet depending on the vendor).

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on a Prime Infrastructure map.

This section contains the following topics:

- [Configuring New Chokepoints, page 17-16](#)
- [Editing Current Chokepoints, page 17-18](#)

Configuring New Chokepoints

This section contains the following topics:

- [Adding a Chokepoint to Prime Infrastructure Database, page 17-16](#)
- [Adding a Chokepoint to an Prime Infrastructure Map, page 17-17](#)
- [Removing a Chokepoint from a Prime Infrastructure Map, page 17-18](#)
- [Removing a Chokepoint from Prime Infrastructure, page 17-18](#)

Adding a Chokepoint to Prime Infrastructure Database

To add a chokepoint to Prime Infrastructure database:

-
- Step 1** Choose **Operate > Operational Tools > Wireless > Chokepoints**.
 - Step 2** From the Select a command drop-down list, choose **Add Chokepoint**.
 - Step 3** Click **Go**.
 - Step 4** Enter the MAC address and name for the chokepoint.
 - Step 5** Select the check box to indicate that it is an Entry/Exit Chokepoint.
 - Step 6** Enter the coverage range for the chokepoint.



Note

Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7 Click **OK**.



Note After the chokepoint is added to the database, it can be placed on the appropriate Prime Infrastructure floor map.

Adding a Chokepoint to an Prime Infrastructure Map

To add the chokepoint to a map:

Step 1 Choose **Operate > Maps**.

Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 4 Click **Go**.



Note The Add Chokepoints summary page lists all recently-added chokepoints that are in the database but not yet mapped.

Step 5 Select the check box next to the chokepoint that you want to place on the map.

Step 6 Click **OK**.

A map appears with a chokepoint icon located in the top-left hand corner. You are now ready to place the chokepoint on the map.

Step 7 Left-click the chokepoint icon and drag and place it in the proper location.



Note The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

Step 8 Click **Save**.

You are returned to the floor map and the added chokepoint appears on the map.



Note The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.



Note The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.



Note MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you pass a mouse over its map icon

- Step 9** If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.



Note Do not select the **Save Settings** check box unless you want to save this display criteria for all maps.



Note You must synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing a Chokepoint from a Prime Infrastructure Map

To remove an chokepoint from the map:

- Step 1** Choose **Operate > Maps**.
- Step 2** In the Maps page, choose the link that corresponds to the floor location of the chokepoint.
- Step 3** From the Select a command drop-down list, choose **Remove Chokepoints**.
- Step 4** Click **Go**.
- Step 5** Click **OK** to confirm the deletion.

Removing a Chokepoint from Prime Infrastructure

To remove a chokepoint from Prime Infrastructure:

- Step 1** Choose **Operate > Operational Tools > Wireless > Chokepoints**.
- Step 2** Select the check box of the chokepoint that you want to delete.
- Step 3** From the Select a command drop-down list, choose **Remove Chokepoints**.
- Step 4** Click **Go**.
- Step 5** Click **OK** to confirm the deletion.

Editing Current Chokepoints

To edit a current chokepoint in Prime Infrastructure database and appropriate map:

- Step 1** Choose **Operate > Operational Tools > Wireless > Chokepoints**. The Configure > Chokepoints page displays the following information for each current chokepoint: MAC address, chokepoint name, entry/exit chokepoint, range, static IP address, and map location for the chokepoint.
- Step 2** Click the chokepoint you want to edit in the MAC Address column.

Step 3 Edit the following parameters, as necessary:

- Name
- Entry/Exit Chokepoint—Click to enable.
- Range—Coverage range for the chokepoint.



Note The chokepoint range is product-specific and is supplied by the chokepoint vendor.

- Static IP Address

Step 4 Click **Save**.

Monitoring Interferers

The Monitor > Interferers page allows you to monitor interference devices detected by the CleanAir enabled access points.

This section provides information on the interferers detected by the CleanAir enabled access points. By default, the [Monitoring AP Detected Interferers](#) page is displayed.

This section contains the following topics:

- [Monitoring AP Detected Interferers, page 17-19](#)
- [Monitoring AP Detected Interferer Details, page 17-20](#)
- [Monitoring AP Detected Interferer Details Location History, page 17-21](#)
- [Configuring the Search Results Display, page 17-22](#)

Monitoring AP Detected Interferers

Choose **Operate > Operational Tools > Wireless > Interferers** to view all the interfering devices detected by the CleanAir enabled access points on your wireless network. This page enables you to view a summary of the interfering devices including the following default information:

- Interferer ID—A unique identifier for the interferer. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device. Click this link to know more about the interferer.
- Type—Indicates the category of the interferer. Click to read more about the type of device. A pop-up window appears displaying more details. The categories include the following:
 - Bluetooth link—A Bluetooth link (802.11b/g/n only)
 - Microwave Oven—A microwave oven (802.11b/g/n only)
 - 802.11 FH—An 802.11 frequency-hopping device (802.11b/g/n only)
 - Bluetooth Discovery—A Bluetooth discovery (802.11b/g/n only)
 - TDD Transmitter—A time division duplex (TDD) transmitter
 - Jammer—A jamming device
 - Continuous Transmitter—A continuous transmitter

- DECT-like Phone—A digital enhanced cordless communication (DECT)-compatible phone
- Video Camera—A video camera
- 802.15.4—An 802.15.4 device (802.11b/g/n only)
- WiFi Inverted—A device using spectrally inverted WiFi signals
- WiFi Invalid Channel—A device using non-standard WiFi channels
- SuperAG—An 802.11 SuperAG device
- Canopy—A Motorola Canopy device
- Radar—A radar device (802.11a/n only)
- Xbox—A Microsoft Xbox (802.11b/g/n only)
- WiMAX Mobile—A WiMAX mobile device (802.11a/n only)
- WiMAX Fixed—A WiMAX fixed device (802.11a/n only)
- WiFi AOCI—A WiFi device with AOCI
- Unclassified
- Status—Indicates the status of the interfering device.
 - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
 - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by Prime Infrastructure.
- Severity—Displays the severity ranking of the interfering device.
- Affected Band—Displays the band in which this device is interfering.
- Affected Channels—Displays the affected channels.
- Duty Cycle (%)—The duty cycle of interfering device in percentage.
- Discovered—Displays the time at which it was discovered.
- Last Updated—The last time the interference was detected.
- Floor—The location where the interfering device is present.

Monitoring AP Detected Interferer Details

Choose **Operate > Operational Tools > Wireless > Interferers > Interferer ID** to view this page. This page enables you to view the details of the interfering devices detected by the access points. This page provides the following details about the interfering device.

- Interferer Properties
 - Type—Displays the type of the interfering device detected by the AP.
- Status—The status of the interfering device. Indicates the status of the interfering device.
 - Active—Indicates that the interferer is currently being detected by the CleanAir capable access point.
 - Inactive—Indicates that the interferer is no longer being detected by the CleanAir capable access point or no longer reachable by Prime Infrastructure.
 - Severity—Displays the severity ranking of the interfering device.
 - Duty Cycle (%)—The duty cycle of interfering device in percentage.

- Affected Band—Displays the band in which this device is interfering.
 - Affected Channels—Displays the affected channels.
 - Discovered—Displays the time at which it was discovered.
 - Last Updated—The last time the interference was detected.
- Location
 - Floor—The location where this interfering device was detected.
 - Last Located At—The last time where the interfering device was located.
 - On MSE—The mobility server engine on which this interference device was located.
- Clustering Information
 - Clustered By—Displays the IP address of the controller or the MSE that clustered the interferer information from the access point.
 - Detecting APs—Displays the details of the access point that has detected the interfering device. The details include: Access Point Name (Mac), Severity, and Duty Cycle(%).
- Details—Displays a short description about the interfering type.

Monitoring AP Detected Interferer Details Location History

Choose **Operate > Operational Tools > Wireless > Interferers > Interference Device ID**, then choose **Location History** from the Select a command drop-down list, and click **Go** to view this page.

- Interferer Information—Displays the basic information about the interfering device.
 - Data Collected At—The time stamp at which the data was collected.
 - Type—The type of the interfering device.
 - Severity—The severity index of the interfering device.
 - Duty Cycle—The duty cycle (in percentage) of the interfering device.
 - Affected Channels—A comma separated list of the channels affected.
- Interferer Location History—Displays the location history of the interfering devices.
 - Time Stamp
 - Floor
- Clustering Information
 - Clustered By
- Detecting APs
 - AP Name—The access point that detected the interfering device.
 - Severity—The severity index of the interfering device.
 - Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.
- Location
 - Location Calculated At—Displays the time stamp at which this information was generated.
 - Floor—Displays location information of the interfering device.
 - A graphical view of the location of the interfering device is displayed in a map. Click the Enlarge link to view an enlarged image.

Configuring the Search Results Display

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page.

To edit the columns in the AP Detected Interferers page:

-
- | | |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Choose Operate > Operational Tools > Wireless > Interferers . The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir enabled access points. |
| Step 2 | Click the Edit View link. |
| Step 3 | To add an additional column to the access points table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table. |
| Step 4 | To remove a column from the access points table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table. |
| Step 5 | Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list. |
| Step 6 | Click Reset to restore the default view. |
| Step 7 | Click Submit to confirm the changes. |
-

Configuring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to Prime Infrastructure. This feature allows Prime Infrastructure to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose **Operate > Operational Tools > Wireless > Spectrum Experts**. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address—The MAC address of the spectrum sensor card in the laptop.
- Reachability Status—Specifies whether the Spectrum Expert is successfully running and sending information to Prime Infrastructure. The status appears as reachable or unreachable.

This section contains the following topics:

- [Adding a Spectrum Expert, page 17-22](#)
- [Spectrum Experts Details, page 17-23](#)

Adding a Spectrum Expert

To add a Spectrum Expert:

-
- | | |
|---------------|------------------------------------------------------------------------------------|
| Step 1 | Choose Operate > Operational Tools > Wireless > Spectrum Experts . |
| Step 2 | From the Select a command drop-down list, choose Add Spectrum Expert . |



Note This link only appears when no spectrum experts are added.

- Step 3** Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.



Note To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to Prime Infrastructure.

Spectrum Experts Details

The Spectrum Expert Details page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds providing a real-time look at what is happening on the remote Spectrum Expert and includes the following items:

- Total Interferer Count—As seen by the specific Spectrum Expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferes by category.
- Active Interferer Count Per Channel—Displays the number of interferes grouped by category on different channels.
- AP List—Provides a list of access points detected by the Spectrum Expert that are on channels that have active interferers detected by the Spectrum Expert on those channels.
- Affected Clients List—Provides a list of clients that are currently authenticated/associated to the radio of one of the access points listed in the access point list.

Configuring Wi-Fi TDOA Receivers

This section contains the following topics:

- [Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting, page 17-23](#)
- [Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps, page 17-24](#)

Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset. TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

**Note**

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network.

See [Adding a Mobility Services Engine](#), in the [Cisco Prime Infrastructure Configuration Guide, Release 1.2](#), for details on adding a mobility services engine.

2. Add the TDOA receiver to Prime Infrastructure database and map.

See [Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps](#) for details on adding the TDOA receiver to Prime Infrastructure.

3. Activate or start the partner engine service on the MSE using Prime Infrastructure.

4. Synchronize Prime Infrastructure and mobility services engines.

See [Synchronizing Services](#), in the [Cisco Prime Infrastructure Configuration Guide, Release 1.2](#), for details on synchronization.

5. Set up the TDOA receiver using the AeroScout System Manager.

**Note**

See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* for configuration details at the following URL:
<http://support.aeroscout.com>.

Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps

After the Wi-Fi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on an Prime Infrastructure map.

After adding TDOA receivers to Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than Prime Infrastructure.

**Note**

For more details on configuration options, see the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide* at the following URL:
<http://support.aeroscout.com>.

To add a TDOA receiver to Prime Infrastructure database and appropriate map:

- Step 1** Choose **Operate > Operational Tools > Wireless > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

**Note**

To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

Step 2 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 3 Click **Go**.

Step 4 Enter the MAC address, name and static IP address of the TDOA receiver.

Step 5 Click **OK** to save the TDOA receiver entry to the database.

**Note**

After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate Prime Infrastructure floor map. To do so, continue with [Step 6](#).

**Note**

A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Step 6 To add the TDOA receiver to a map, choose **Operate > Maps**.

Step 7 In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

Step 8 From the Select a command drop-down list, choose **Add WiFi TDOA receivers**.

Step 9 Click **Go**.

**Note**

The All WiFi TDOA Receivers summary page lists all recently-added TDOA receivers that are in the database but not yet mapped.

Step 10 Select the check box next to each TDOA receiver to add it to the map.

Step 11 Click **OK**. A map appears with a TDOA receiver icon located in the top-left hand corner. You are now ready to place the TDOA receiver on the map.

Step 12 Left-click the TDOA receiver icon and drag and place it in the proper location on the floor map.

**Note**

The MAC address and name of the TDOA receiver appear in the left pane when you click the TDOA receiver icon for placement.

Step 13 Click **Save** when the icon is placed correctly on the map. The added TDOA receiver appears on the floor heat map.

**Note**

The icon for the newly added TDOA receiver might or might not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with [Step 14](#).

Step 14 If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

Step 15 Select the **WiFi TDOA Receivers** check box. The TDOA receiver appears on the map.

**Note**

When you place your cursor over a TDOA receiver on a map, configuration details display for that receiver.

Step 16 Click **X** to close the Layers page.

**Note**

Do not choose **Save Settings** from the Layers menu unless you want to save this display criteria for all maps.

Step 17 You can now download the partner engine software to the mobility services engine.



CHAPTER 18

Tracing Application Data Paths

Prime Infrastructure supports tracing of RTP and TCP application traffic paths across endpoints and sites

Tracing data paths depends on Cisco Medianet and Web Services Management Agent (WSMA). Both are built-in features of Cisco IOS and Catalyst OS software images. They help isolate and troubleshoot problems with RTP and TCP data streams. Prime Infrastructure supports all versions of Medianet and WSMA and makes it easy to enable them on any router.

Where Cisco Network Analysis Module (NAM) traffic monitoring data is not available, Prime Infrastructure supports RTP path tracing using Medianet Performance Monitor and IOS NetFlow.

When properly configured, Path Trace can be your most valuable tool in troubleshooting RTP and TCP application problems.

This chapter contains the following sections:

- [Setting Up Path Trace, page 18-1](#)
- [Troubleshooting with Path Trace, page 18-4](#)

Setting Up Path Trace

You cannot use Prime Infrastructure's Path Trace feature until you complete some prerequisite setup tasks. The prerequisite tasks vary according to whether you are monitoring router traffic using Cisco NAMs or not. The following sections explain both sets of tasks:

- [Setting Up Path Trace on Networks With NAMs, page 18-1](#)
- [Setting Up Path Trace on Networks Without NAMs, page 18-2](#)

Setting Up Path Trace on Networks With NAMs

If your network uses NAMs to monitor network traffic, you must complete the following tasks to enable path tracing for both RTP and TCP traffic:

1. Add NAMs to the system. You can do this either automatically, using Discovery, or manually, using bulk import or Device Work Center (see [Discovering the Network](#)).
2. Enable NAM Data collection. You can do this by choosing **Administration > Data Sources > NAM Data Collector** and then enabling data collection on each NAM (see [Enabling NAM Data Collection](#)).

3. Create a Site structure for your organization and use Device Work Center to assign your principal routers to the appropriate Sites. You can do this by choosing **Design > Site Map Design** and adding one or more Campuses (see [Designing Sites](#)).
4. Associate your Sites with Authorized Data Sources. You can do this by choosing **Administration > System Settings > Data Deduplication**, and assigning authoritative data sources for Voice/Video (for RTP data) and Application Response Time (for TCP data). For detailed steps, see [Controlling Background Data Collection Tasks](#), page 26-3.
5. Associate your Sites with Endpoint subnets. You can do this by choosing **Design > Endpoint-Site Association** and then associating subnets with your Sites (see [Associating Endpoints With Sites](#), page 7-3). If you fail to do this, then by default the data collected by NAMs for these endpoints will have their sites set to “Unassigned”.
6. Configure your routers for Mediatrace and WSMA (see [Configuring Routers for Mediatrace and WSMA](#), page 18-4).

Setting Up Path Trace on Networks Without NAMs

If your network is not equipped with Cisco NAMs, you can use Medianet Performance Monitor and NetFlow to enable path tracing of RTP flows. You can use this option only on the Cisco device platforms with at least the software images shown in [Table 18-1](#).

Table 18-1 Routers Supporting Medianet Performance Monitor and Mediatrace

Platform	Minimum IOS Version
Cisco 2900 Series Integrated Services Routers	15.1(3)T
Cisco 3900 Series Integrated Services Routers	15.1(3)T
Cisco ASR 1000 Series Aggregation Services Routers	Cisco IOS XE Software Release 3.5 or later

You will also need to enable TCP path tracing on other routers using Mediatrace and WSMA.

To enable the Path Trace feature in a non-NAM environment:

1. Create a Site structure for your organization and use Device Work Center to assign your principal routers to the appropriate Sites. You can do this by choosing **Design > Site Map Design** and adding one or more Campuses (see [Designing Sites](#)).
2. Associate your Sites with Authorized Data Sources. You can do this by choosing **Administration > System Settings > Data Deduplication**, and assigning authoritative data sources for Voice/Video (for RTP data) and Application Response Time (for TCP data). For detailed steps, see [Controlling Background Data Collection Tasks](#), page 26-3.
3. Associate your Sites with Endpoint subnets. You can do this by choosing **Design > Endpoint-Site Association** and then associating subnets with your Sites (see [Associating Endpoints With Sites](#), page 7-3). If you fail to do this, then by default the data collected for these endpoints will have their sites set to “Unassigned”.
4. Configure your compatible routers for Medianet Performance Monitor (see [Configuring Routers for Medianet Performance Monitor and Mediatrace](#), page 18-3).
5. Configure your routers for Mediatrace and WSMA (see [Configuring Routers for Mediatrace and WSMA](#), page 18-4).

Configuring Routers for Medianet Performance Monitor and Mediatrace

Prime Infrastructure supplies an out-of-the-box template that configures routers so that Medianet can be used to trace RTP paths in the absence of NAM data. This template configures compatible routers to use Medianet Performance Monitor and Cisco IOS NetFlow to export RTP flow metrics to the Prime Infrastructure server.

**Note**

Before you begin this procedure, make sure you have completed all of the tasks in [Setting Up Path Trace on Networks Without NAMs, page 18-2](#).

-
- Step 1** Choose **Design > Configuration Templates > My Templates > OOTB > Medianet-PerfMon**.
- Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
- Step 3** In the Validation Criteria section, select one or more of the Medianet PerfMon-compatible device types listed in [Table 18-1 on page 18-2](#).
- Step 4** In the Validation Criteria section, enter the OS Version for each of the selected device types. This must be at least the minimum IOS version shown in [Table 18-1 on page 18-2](#).
- Step 5** In the Template Detail section, click the Form View tab and complete the fields as follows:
- Flow Exporter Name—Enter a name for the NetFlow exporter on the device types you selected. This can be any collection of characters (for example: `EXPORTER-1`).
 - IP Address—Enter the IP address of the Prime Infrastructure server.
 - Flow Exporter Port—Enter the port on which the NetFlow monitor will receive the exported data. Use the default 9991 port unless you have a special need to override it.
 - Performance Monitor Name—Enter an arbitrary name for the Medianet Performance Monitor caching the data from the flow exporter (for example: `MP-MONITOR-1`).
 - Interface—The name of the interface on the device whose NetFlow data you want to monitor (for example: `ethernet 0/0`).
 - Flow Monitor Name—Enter an arbitrary name for the NetFlow monitor caching the data from the flow exporter (for example: `FLOW-MONITOR-1`).
- Step 6** Click **Save as New Template**. After you save the template, deploy it to your routers using the procedures in [Deploying Templates](#).
-

Configuring Routers for Mediatrace and WSMA

Prime Infrastructure supplies an out-of-the-box template that configures routers so that Medianet and WSMA can be run on them. It enables:

- Mediatrace Responder
- WSMA
- An HTTP server with local authentication policy.

You will want to apply this configuration to every router you want to use when tracing application paths. When applying this configuration, the HTTP user should have the highest privilege level (privilege=15) in order to run Mediatrace commands.



Note

Before you begin this procedure, make sure you have completed all of the tasks in either [Setting Up Path Trace on Networks With NAMs, page 18-1](#) or [Setting Up Path Trace on Networks Without NAMs, page 18-2](#).

-
- Step 1** Choose **Design > Configuration Templates > My Templates > OOTB > Mediatrace-WSMA-Configuration**.
 - Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.
 - Step 3** In the Validation Criteria section, leave “Routers” as the Device Type.
 - Step 4** In the Validation Criteria section, enter the OS Version.
 - Step 5** Click **Save as New Template**. After you save the template, deploy it to your routers using the procedures in [Deploying Templates](#).
-

Troubleshooting with Path Trace

Path Trace is intended primarily as a troubleshooting tool. When data collection is configured properly for this tool (see [Setting Up Path Trace, page 18-1](#)), it shows a table listing all currently active RTP streams or TCP sessions. Using these Path Trace tables and their associated options, you can:

- Quickly identify and select RTP or TCP flows with problems (see [Using the Path Trace Tables, page 18-5](#)).
- Troubleshoot problems with RTP flows (see [Running Path Trace from Selected RTP Flows, page 18-6](#)).
- Troubleshoot problems with TCP flows (see [Running Path Trace from Selected TCP Flows, page 18-7](#)).
- Troubleshoot problems with RTP or TCP flows between any two arbitrary endpoints (see [Launching an Ad Hoc Path Trace From Endpoints, page 18-9](#)).
- Troubleshoot problems with RTP flows starting from the RTP Conversations dashlet (see [Troubleshooting Worst RTP Endpoints Using Dashlets, page 18-10](#)).
- Identify and compare flow performance indicators and data sources (see [Comparing Flow Data From Multiple Sources, page 18-11](#)).

Using the Path Trace Tables

The flow information shown in the RTP Streams and TCP Sessions tables is collected and aggregated from NAM and NetFlow data generated throughout the network.

Many rows in the RTP Streams table are arranged in a tree hierarchy. This will occur whenever an RTP application flow involves more than one data stream. In these cases, all the flows between the two application endpoints are aggregated into a single row with a triangle icon,

By default, Prime Infrastructure refreshes the RTP Streams table data every 60 seconds, automatically. It refreshes TCP Sessions data once every 300 seconds (5 minutes). You can also click either table's **Refresh** button at any time. You can turn off automatic refresh by unselecting **Enable auto refresh**.

To use the Path Trace tables:

-
- Step 1** Choose **Operate > Path Trace**.
- Step 2** In **Application**, choose **RTP or TCP**. The page shows the corresponding table: RTP Streams or TCP Sessions.
- Step 3** Find the flow you want to troubleshoot:
- To review all flows with a particular type of issue: Click on the appropriate column heading to sort on that column.

For example, if you are monitoring RTP performance across the network and want to see the streams with the worst jitter or packet loss, click on the Jitter or Packet Loss column headings to sort the streams on these performance indicators. You can then select any of the streams for troubleshooting.
 - To find a particular flow with a problem: Click the Quick Filter icon and enter a filter criterion under one or more row headings.

For example: An end user having trouble accessing an application may report to you his IP Address and the name of that application. You can do a quick filter on the TCP table for either the Client IP Address or Application ID and then select that session for troubleshooting.
 - To spot issues in RTP subflows: Click the triangle icon next to any aggregated RTP flow.

For example: An RTP voice/video flow between any two endpoints will appear in the RTP Streams table as a single flow with a triangle icon. Clicking the icon will show you the four subflows: an incoming and outgoing video subflow, and an incoming and outgoing voice subflow.
- Step 4** To troubleshoot the flow, see the related topics:
- [Running Path Trace from Selected RTP Flows, page 18-6](#)
 - [Running Path Trace from Selected TCP Flows, page 18-7](#)
-

Running Path Trace from Selected RTP Flows

For each RTP flow, the RTP Streams table has a column showing that flow's:

- Type (e.g., voice or video)
- Source IP Address, Site, and User ID
- Destination IP Address Site, and User ID
- Jitter (in milliseconds)
- Packet Loss (in percent)
- Mean Opinion Score
- Traffic Volume
- Stream Start Time

To troubleshoot RTP flows using Path Trace:

-
- Step 1** Choose **Operate > Path Trace**. In **Application**, choose **RTP**. Then find the flow you want using the steps in [Using the Path Trace Tables](#), page 18-5.
- Step 2** Select the flow and click **Trace Service Path**. Prime Infrastructure displays the RTP Stream Details page for the selected flow, with all the routers in the flow's path in the Troubleshooting Status table, in order of their distance from the flow's source endpoint. Routers that are Medianet-capable are indicated by a filmstrip icon.
- Step 3** To run Mediatrace or Traceroute from a router in the flow's path, click on the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.
- Mediatrace can take a minute or more to run, depending on traffic, congestion and the total number of hops between the flow endpoints.
- While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:
- The progress of the operation.
 - Errors encountered during the operation, including router response timeouts and other steps that did not complete.
 - Where non-Medianet-capable routers were encountered and how they were processed.
 - Medianet-capable routers on which Medianet is not configured.
- Step 4** When the operation is complete, the Troubleshooting tab displays a topology map of all the devices between the flow's two endpoints. Device icons in the map will be badged as follows:
- Alarm Severity: Indicates the most severe alarm currently recorded for the device.
 - Flag: Indicates the device on which the Mediatrace or Traceroute was initiated.
 - Filmstrip: Indicates the device is Medianet-capable.
 - Minus sign on red background: Indicates the device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder as explained in [Configuring Routers for Mediatrace and WSMA](#), page 18-4.
 - Minus sign: Indicates the device is unmanaged.

- Step 5** To see key performance metrics for all Medianet-capable devices in the RTP flow's path, click the Medianet Path View tab. Click the subtabs in the Medianet Path View panel to see the performance metrics in numerical and graphic form.



Note The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

- Step 6** Use the appropriate links in the Troubleshooting Status table to launch a Mediatrace or Traceroute operation on a different router, restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Running Path Trace from Selected TCP Flows

For each active TCP flow, the TCP Sessions table has a column showing that flow's:

- Client IP Address, Site, and User ID
- Server IP Address, and Site
- Application ID
- Average Network Time for the Client, WAN, and Server (in milliseconds)
- Maximum and Average Transition Time (in milliseconds)
- Traffic Volume on both the Client and Server (in bytes per second)

To troubleshoot TCP flows using Path Trace:

- Step 1** Choose **Operate > Path Trace**. In **Application**, choose **TCP**. Then find the flow you want using the steps in [Using the Path Trace Tables, page 18-5](#).
- Step 2** Select the flow and click **Start Path Trace**. Prime Infrastructure displays the TCP Stream details page for the selected flow.
- Step 3** To troubleshoot any listed flow: Select the flow and click **Trace Service Path**. Prime Infrastructure displays the TCP Stream Details page for the selected flow, with all the routers in the flow's path in the Troubleshooting Status table, in order of their distance from the flow's source endpoint. Routers with a "filmstrip" icon next to them are Medianet-capable.
- Step 4** To run Mediatrace or Traceroute from a router in the flow's path, click on the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

Mediatrace can take a minute or more to run, depending on traffic, congestion and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- not complete.
- Where non-Medianet-capable routers were encountered and how they were processed.
- Medianet-capable routers on which Medianet is not configured.

Step 5 When the operation is complete, the Troubleshooting tab displays a topology map of all the devices between the flow's two endpoints. Device icons in the map will be badged as follows:

- Alarm Severity: Indicates the most severe alarm currently recorded for the device.
- Flag: Indicates the device on which the Mediatrace or Traceroute was initiated.
- Filmstrip: Indicates the device is Medianet-capable.
- Minus sign on red background: Indicates the device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder as explained in [Configuring Routers for Mediatrace and WSMA, page 18-4](#).
- Minus sign: Indicates the device is unmanaged.

Step 6 To see key performance metrics for all Medianet-capable devices in the TCP flow's path, click the Medianet Path View tab. Click the subtabs in the Medianet Path View panel to see the performance metrics in numerical and graphic form.



Note

The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 7 Use the appropriate links in the Troubleshooting Status table to launch a Mediatrace or Traceroute operation on a different router, restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Launching an Ad Hoc Path Trace From Endpoints

You can quickly launch a Path Trace against all RTP or TCP flows between any two endpoints in the network. This can include either specific flows running between any two endpoints on the same or different sites, or between a pair of routers on two different sites.


This is handy if your network lacks NAM monitoring, or when you are in a hurry and you know at least the IP addresses of the two endpoints of the RTP or TCP flow. You must still navigate to and start the path trace from the appropriate RTP or TCP Path Trace table.

-
- Step 1** Choose **Operate > Path Trace**. In **Application**, choose **RTP** or **TCP**.
- Step 2** Click **Specify Session for Path Trace**.
- Step 3** Specify the required flow endpoint information, as follows:
- For an RTP flow:
 - Select the Source Site.
 - Enter the Source Endpoint IP Address.
 - Enter the Destination EndPoint IP Address.
 - For a TCP flow:
 - Select the Client Site.
 - Enter the Client Endpoint IP Address.
 - Enter Server Endpoint IP Address.
- Step 4** Provide any additional endpoint information you have, as follows:
- For an RTP flow: Select or enter the Source Endpoint Port and Destination Endpoint Port.
 - For a TCP flow: Select or enter the Server Endpoint Port,
- Step 5** Click **Trace Service Path** (for an RTP flow) or **OK** (for a TCP flow). Prime Infrastructure displays the RTP or TCP Stream Details page for the specified flow, with all the routers in the flow's path in the Troubleshooting Status table, in order of their distance from the flow's source or client endpoint. Routers with a "filmstrip" icon next to them are Medianet-capable.
- Step 6** To run Mediatrace or Traceroute from a router in the flow's path, click on the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

Mediatrace can take a minute or more to run, depending on traffic, congestion and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where and how non-Medianet-capable routers were encountered and processed.
- Medianet-capable routers on which Medianet is not configured.

- Step 7** When the operation is complete, the Troubleshooting tab displays a topology map of the all the devices between the flow's two endpoints. Device icons in the map will be badged as follows:
- Alarm Severity: Indicates the most severe alarm currently recorded for the device.
 - Flag: Indicates the device on which the Mediatrace or Traceroute was initiated.
 - Filmstrip: Indicates the device is Medianet-capable.
 - Minus sign on red background: Indicates the device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder as explained in [Configuring Routers for Mediatrace and WSMA, page 18-4](#).
 - Minus sign: Indicates the device is unmanaged.
- Step 8** To see key performance metrics for all Medianet-capable devices in the flow's path, click the Medianet Path View tab. Click the subtabs in the Medianet Path View panel to see the performance metrics in numerical and graphic form.
-  **Note** The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.
- Step 9** Use the appropriate links in the Troubleshooting Status table to launch a Mediatrace or Traceroute operation on a different router, restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Troubleshooting Worst RTP Endpoints Using Dashlets

You can quickly launch a Path Trace against the poorest performing RTP flows in your network using the Worst N RTP End Point Pairs, and RTP Conversation dashlets. This works only for RTP flows.

The RTP Conversations dashlet shows the complete history for a source endpoint, including flows that are no longer active. You will want to select only the most recent flows. If you launch Path Trace on such an inactive flow, you will receive an error message advising you of this fact.

- Step 1** Choose **Operate > Detail Dashboards > End User Experience**.
- Step 2** In the **Worst N RTP End Point Pairs** dashlet, note the Source Address for your worst performing RTP flows.
- Step 3** In the **RTP Conversations** dashlet on the same page, find the most recent conversation for the same Source Address.
- Step 4** Select that conversation in the RTP Conversations dashlet, then click **Troubleshoot > Trace Service** path. Prime Infrastructure displays the RTP Stream Details page for the selected flow, with all the routers in the flow's path in the Troubleshooting Status table, in order of their distance from the flow's source endpoint. Routers that are Medianet-capable are indicated by a filmstrip icon.
- Step 5** To run Mediatrace or Traceroute from a router in the flow's path, click on the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.
- Mediatrace can take a minute or more to run, depending on traffic, congestion and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where and how non-Medianet-capable routers were encountered and processed.
- Medianet-capable routers on which Medianet is not configured.

Step 6 When the operation is complete, the Troubleshooting tab displays a topology map of all the devices between the flow's two endpoints. Device icons in the map will be badged as follows:

- Flag: Indicates the device on which the Mediatrace or Traceroute was initiated.
- Filmstrip: Indicates the device is Medianet-capable.
- Minus sign: Indicates the device is unmanaged.

Step 7 To see key performance metrics for all Medianet-capable devices in the flow's path, click the Medianet Path View tab. Click the subtabs in the Medianet Path View panel to see the performance metrics in numerical and graphic form.



Note The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 8 Use the appropriate links in the Troubleshooting Status table to launch a Mediatrace or Traceroute operation on a different router, restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Comparing Flow Data From Multiple Sources

When interpreting Path Trace performance data, you may find it helpful to:

- Identify the NAM, NetFlow, and other sources reporting this performance data.
- If you have multiple NAM or NetFlow data sources: Compare how those sources are reporting key performance indicators for a particular flow.

To do this, follow these steps.

Step 1 Choose **Operate > Path Trace**. In **Application**, choose **RTP** or **TCP**. Then find the flow you want using the steps in [Using the Path Trace Tables, page 18-5](#)

Step 2 Select the flow and then click **Analyze Path** (for an RTP flow) or **Analyze on Multiple Data Sources** (for a TCP flow). Prime Infrastructure displays the Multiple Data Source KPI Analysis page. It provides a table presenting key performance indicators appropriate for the selected flow, and the data source for each such set of indicators.

Step 3 When you are finished, click **OK**.



CHAPTER 19

Troubleshooting

Troubleshooting Users

When a user complains of issues such as poor voice quality or slow application response time, Prime Infrastructure can help you isolate the source of the problem.

-
- Step 1** In the search box, enter the name of the user (or client) who is experiencing the issue.
The Search Results box appears listing the number of item(s) that owned by the user name you entered.
- Step 2** In the Monitor column, click **View List** to see all devices, both wired and wireless, to which this user is assigned.



Note In order for Prime Infrastructure to classify data as coming from wired or wireless devices, you must configure your NAM on the same switch to which your controller is connected. The NAM needs to view the same traffic the controller is viewing

- Step 3** Select a device for which you want to view further details.
- Step 4** Use the dashboards described in [Table 19-1](#) to gather details about the problems users are experiencing.
-

Table 19-1 *Using Prime Infrastructure Dashboards to Troubleshoot User Problems*

Step	Use This Dashboard...	To Gather This Type of Information
1.	End User Experience	<p>Detailed information about the user, including:</p> <ul style="list-style-type: none"> • All devices being used by the user, which can include desktop computers, notebooks, tablets, cellular phones, etc. • Which of the user's devices, both wired and wireless, are accessing which applications? • Top N applications shows each application's usage, further categorized as wired (green) or wireless (blue). Details about client traffic, conversations and packet loss can be filtered on a wired vs. wireless basis.
2.	Site	<p>Determine if other users at the site are experiencing the same issues, as well as the following details:</p> <ul style="list-style-type: none"> • What clients are associated to the site? • What applications are being used in the site? • Is one application in a site getting all the bandwidth? • How does application response time vary for all users in a site? • Are there site connectivity issues with the site routers to the datacenter or branch? • What is the device health and alarm status of the site router?
3.	Application	<p>Determine if there is a particular application for which all users are experiencing problems, as well as the following details:</p> <ul style="list-style-type: none"> • How is the application server health and performance? • Which clients are the biggest consumers for this application? • Are any clients misusing the application as evidenced by the volume of traffic to/from the client?



PART 5

Assuring Network Services

This part contains the following sections:

- [Troubleshooting Voice/Video Delivery to a Branch Office](#)
- [Troubleshooting Unjoined Access Points](#)
- [Ensuring Consistent Application Experiences](#)
- [Troubleshooting With Multiple NAMs](#)
- [Planning Capacity Changes](#)
- [Post-Deployment Application Monitoring](#)



CHAPTER 20

Troubleshooting Voice/Video Delivery to a Branch Office

To successfully diagnose and resolve problems with application service delivery, network operators must be able to link user experiences of network services with the underlying hardware devices, interfaces, and device configurations that deliver these services. This is especially challenging with RTP-based services like voice and video, where service quality, rather than gross problems like outages, impose special requirements.

Cisco Prime Assurance makes this kind of troubleshooting easy. The following workflow is based on a typical scenario: A user complains to the network operations desk about poor voice quality or choppy video replay at his branch office. The operator first confirms that the user is indeed having a problem with jitter and packet loss that will affect his RTP application performance. He further confirms that other users at the same branch are also having the same problem,. The operator next confirms that there is congestion on the WAN interface on the edge router that connects the local branch to the central voice/video server in the main office. Further investigation reveals that an unknown HTTP application is using a high percentage of the WAN interface bandwidth and causing the dropouts. The operator can then change the unknown application's DSCP classification to prevent it from stealing bandwidth.

Step 1 Select **Operate > Details Dashboards > End User Experience**.

Step 2 Next to **Filters**, specify:

- The IP address of the **Client** machine of the user complaining about poor service.
- The **Time Frame** during which the problem occurred.
- The ID of the problem **Application**.

Click **Go** to filter the Detail Dashboard information using these parameters.

Step 3 Check **RTP Conversations Details** to see the Jitter and Packet Loss statistics for the client experiencing the problem .

Step 4 Check the **User Site Summary** to confirm that other users at the same site are experiencing the same issue with the same application.

Step 5 In the **User Site Summary**, under Device Reachability, hover the mouse over the branch's edge router. Prime Assurance displays a 360 View icon for the device under the Device IP column. Click on the icon to display the 360 View.

Step 6 In the 360 View, click the Alarms tab, to see alarms on the WAN interfaces, or on the Interfaces tab, to see congested WAN interfaces and the top applications running on them.



CHAPTER 21

Troubleshooting Unjoined Access Points


When a lightweight access point initial starts up, it attempts to discover and join a wireless LAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all the configuration details for the device and network. After successfully joining the wireless controller, the access point can be discovered and managed by Prime Infrastructure. Until the access point successfully joins a wireless controller the access point cannot be managed by Prime Infrastructure and does not contain the proper configuration settings to allow client access.

Prime Infrastructure provides you with a tool that diagnoses why an access point cannot join a controller and lists corrective actions.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included in the page. This includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason if known.

To troubleshoot unjoined access points, do the following:

-
- Step 1** Select **Operate > Wireless > Unjoined APs**. The Unjoined APs page appears containing a list of access points that have not been able to join a wireless controller.
 - Step 2** Select the access point that you wish to diagnose, then click **Troubleshoot**. An analysis is run on the access point to determine the reason why the access point was not able to join a wireless controller. After performing the analysis the Unjoined APs page displays the results.
 - Step 3** If the access point has tried to join multiple wireless controllers and has been unsuccessful, the controllers are listed in the left pane. Select a controller.
 - Step 4** In the middle pane you can view what the problem is. It will also list error messages and controller log information.
 - Step 5** In the right pane recommendations for solving the problems are listed. Perform the recommended action.
 - Step 6** If you need to further diagnose a problem, you can run RTTS through the Unjoined AP page. This allows you to see the debug messages from all the wireless controllers that the access point tried to join at one time.

To run RTTS, click the RTTS icon () located to the right of the table. The debug messages appear in the table. You can then examine the messages to see if you can determine a cause for the access point not being able to join the controllers.



CHAPTER 22

Ensuring Consistent Application Experiences

Cisco Wide Area Application Services (WAAS) devices and software help to ensure high-quality WAN end-user experiences across applications at multiple sites. For WAAS deployments to be successful, however, network operations staff must share a common data resource that gives them complete visibility into network performance data throughout every stage of the optimization cycle, including:

- Identifying the sites and applications that are candidates for optimization, so that network designers can plan where WAAS optimization is critical.
- Establishing site and application performance baselines.
- Post-implementation validation that WAN performance and application stability have actually improved
- Ongoing monitoring and troubleshooting of the optimized flows.

Cisco Prime Assurance offers a consistent data resource for each of these stages in performance optimization.

Identifying Optimization Candidates

Follow these steps to identify your network's lowest performing applications, clients, servers, and network links.

Step 1 Select **Operate > WAN Optimization**.

Step 2 Click the **Traffic Analysis** tab. Use the dashlets on this page to identify optimization candidates:

- All the dashlets show the current traffic rate (in bytes per second), average number of concurrent connections, and average transaction time in milliseconds, for every application, client, server or network link.
- **Network Links** also shows the sites for the client and server endpoints of each link, and the average length of time the link exists .
- **Server Traffic** shows both the server IP address and the application it serves.

Step 3 Sort and filter the performance data as needed:

To sort on any column in any dashlet, click on the column heading.

To filter the data displayed in all the dashlets by **Time Frame**, **Site**, or **Application** , enter or select the filter criteria you want on the **Filters** line and click **Go**.

To filter within a dashlet, click on its Filter icon and specify a Quick or Advanced Filter, or use a Preset Filter.

- Step 4** For a quick report of the same data, select **Tools > Reports > Report Launch Pad**. Then select **Performance > WAN Traffic Analysis Summary**. Specify filter and other criteria for the report, then click **Run**.
-

Establishing Performance Baselines

Flow these steps to establish the standard performance characteristics of your candidate applications and sites before implementing WAN optimizations.

- Step 1** Select **Operate > Detail Dashboards**.

- Step 2** Click the **Application** tab. Use the dashlets on this page to establish the performance characteristics of your optimization candidates as currently configured:

- **Worst N Clients by Transaction Time:** For the worst-performing clients and applications: Maximum and average transaction times, and 24-hour performance trend.
- **Worst N Sites by Transaction Time:** The same information for the worst-performing sites and applications.
- **App Server Performance:** For all application servers: the maximum and average server response time, and a 24-hour performance trend.
- **Application Traffic Analysis:** Gives 24-hour application traffic metrics in bytes per second and packets per second. Calculates statistical mean, minimum, maximum, median, and first and second standard deviation for the period,

You can sort by any column in any dashlet by clicking on the column heading.

- Step 3** You can filter the data in the dashlets by **Time Frame**, **Site**, and **Application**.

- Step 4** Click the **Site** tab and use **Top N Applications by Volume**, **Top N Devices with Most Alarms**, **Top N Clients (In and Out)** and **Worst N Clients by Transaction Time** as you did in Step 2.
-

Validating Optimization ROI

Once you have deployed your WAAS changes at candidate sites, follow these steps to validate the return on your optimization investment.

-
- Step 1** Select **Operate > WAN Optimization**.
- Step 2** Click the **Application Performance Analysis** tab. The dashlets on this page show:
- **Transaction Time (Client Experience)**: Graphs average client transaction times (in milliseconds) for the past 24 hours, with separate lines for optimized traffic and pass-through traffic (in which optimization is turned off). With optimization enabled, you should see a drop in the optimized traffic time when compared to the pass-through time.
 - **Average Concurrent Connections (Optimized vs Passthru)**: Graphs the average number of concurrent client and passthrough connections over a specified time period.
 - **Traffic Volume and Compression Ratio**: Graphs the bandwidth reduction ratio between the number of bytes before compression and the number of bytes after compression.
 - **Multi-Segment Network Time (Client LAN-WAN - Server LAN)**: Graphs the network time between the multiple segments.
- Step 3** You can filter the data in the dashlets by **Time Frame**, **Client Site**, **Server Site**, and **Application**.
- Step 4** For a report, select **Tools > Reports > Report Launch Pad**. Then select **Performance > WAN Application Performance Analysis Summary**. Specify filter and other settings for the report, then click **Run**.
-

Monitoring Optimized Flows

Follow these steps to monitor WAAS-optimized WAN traffic.

-
- Step 1** Select **Operate > WAN Optimization > Multi-Segment Analysis**.
- Step 2** Click the **Conversations** tab to see individual client/server sessions, or the **Site to Site** tab to see aggregated site traffic. For each client (or client site) and server (or server site) pair and application in use, these pages show:
- **Average and Max Transaction Time:** The time between the client request and the final response packet from the server. Transaction time will vary with client uses and application types, as well as with network latency. Transaction Time is a key indicator in monitoring client experiences and detecting application performance problems.
 - **Average Client Network Time:** The network time between a client and the local switch or router. In WAAS monitoring, Client Network Time from a WAE client data source represents the network RTT between the client and its edge WAE, while Client Network Time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).
 - **Average WAN Network Time:** The time across the WAN segment (between the edge routers at the client and server locations).
 - **Average Server Network Time:** The network time between a server and NAM probing point. In WAAS monitoring, Server Network Time from a server data source represents the network time between the server and its core WAE.
 - **Average Server Response Time:** The average time it takes an application server to respond to a request. This is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application server resources, such as the CPU, Memory, Disk, or I/O.
 - **Traffic Volume:** The volume of bytes per second in each of the Client, WAN, and Server segments.
- Step 3** Sort and filter the performance data as needed:
- To sort on any column, click on the column heading.
- You can filter the data displayed by **Time Frame**. Or click on the Filter icon and specify a Quick or Advanced Filter, or use a Preset Filter.
-



CHAPTER 23

Troubleshooting With Multiple NAMs

In addition to aggregating data from multiple NAMs as a matter of course, Cisco Prime Assurance makes it easy to actively manage and troubleshoot network problems using multiple NAMs. In the following workflow, a network operator needs to troubleshoot a set of similar authentication violations taking place at multiple branches. Because the operator suspects that the authentication problems are due to a network attack in progress, she runs the Prime Assurance Packet Capture feature against NAMs for each branch, then cross-launches the NAM Traffic Analyzer Packet Decoder to inspect the suspicious traffic.

-
- Step 1** Select **Tools > Packet Capture**.
 - Step 2** Click **Create** to create a new capture session definition.
 - Step 3** Complete the **General** section as needed. Give the session definition a unique name and specify how you want the captured data filed.
 - Step 4** If you want to restrict the captured traffic to particular source or destination IPs, VLANs, applications, or ports, click **Add** in the **Software Filters** section and create filters as needed.
 - Step 5** Click **Add** in the **NAMs** section. Select all the NAMs you want to capture traffic on by clicking the check box next to each NAM. Then click **Add** to add them to the packet capture definition.
 - Step 6** Click **Create and Start All Sessions**. Prime Assurance saves the new session definition, then runs separate capture sessions on each of the NAMs you specified. It stores the sessions as files on the Prime Assurance server, and displays the list of packet capture files in the **Capture Files** section.
 - Step 7** To store the packet-capture files locally, select the files you want and click **Download**. Specify the names you want to store the files under locally and then click **OK**.
 - Step 8** To examine the contents of a packet-capture file, select the file you want to see and select **Decode**. Prime Assurance will cross-launch the NAM Packet Decoder and display the file information.
 - Step 9** To run the packet captures again, select the session definition in the **Capture Sessions** section, then click **Start**.
-





CHAPTER 24

Planning Capacity Changes

Cisco Prime Assurance allows you to view and report a variety of key performance indicators that are critical to maintaining and improving your network's operational readiness and performance quality. This information is especially critical in adapting to ever increasing network loads.

In the following workflow, we take the role of a network administrator who has just been told that a large staff expansion is planned for a branch office. This will add more users to the branch LAN, many of whom will be using WAN applications. We want to monitor the branch's key interfaces for usage and traffic congestion, so we can see if more users on the branch LAN will mean degraded WAN application performance for those users. To be certain we have an adequate picture, we will need to look at both short- and long-term performance trends for all the WAN applications the branch uses.

-
- Step 1** Select **Operate > Performance > Service Assurance**.
- Step 2** In **Top N WAN Interfaces by Utilization**, see the usage statistics for the WAN interfaces on the routers connecting remote branches to the WAN. For each interface, the dashlet shows the site, the IP of the device hosting the WAN interface, the interface name, maximums and average utilization, and the utilization trend line for the past 24 hours.
- Step 3** On the **Filters** line, set the **Time Frame** to **Past 4 Weeks**, so you can see utilization statistics for the past month.
- Step 4** Find the WAN interface for the branch to which you are adding users. In the **Interface** column, click on the interface's name to display that interface's dashboard. The interface dashboard shows the following for this single interface:
- Interface Details
 - Top Applications by Volume
 - Number of Users Over Time
 - Class Map Statistics
 - Interface Tx and Rx Utilization
 - Top N Clients (In and Out)
 - DSCP Classification
 - Top Application Traffic Over Time
- Step 5** Concentrate on **Top Application Traffic Over Time**, which gives a color-coded map of the top 10 applications with the heaviest traffic over this interface.

- Step 6** To get a better idea of the longer-term performance trend, click on the Clock icon next to the dashlet title to change the Time Frame to Past 24 Hours, Past 4 Weeks, or Past 6 Months. To zoom in on particular spikes in the graph, use the Pan and Zoom handles in the lower graph.
- Step 7** For a quick report of the same data as the interface dashboard, select **Tools > Reports > Report Launch Pad**. Then select **Performance > Interface Summary Report**. Specify filter and other criteria for the report, and select the same interface in Report Criteria, then click **Run**.
-



CHAPTER 25

Post-Deployment Application Monitoring

Cisco Prime Assurance lets network operators investigate performance issues starting from any of the many parameters that contribute to them: raw server performance, competition for bandwidth from other applications and users, connectivity issues, device alarms, peak traffic times, and so on. This flexibility makes shorter troubleshooting time and quicker solutions.

In the following workflow, a network administrator is responding to scattered complaints from multiple branches about poor performance for a newly deployed application. He suspects a malfunctioning edge router at the application server site to be the problem, but needs to see if other factors are contributing to the issue.

-
- Step 1** Select **Operate > Detail Dashboards > Application**.
 - Step 2** Limit all the dashlets on this page to the newly deployed application: On the **Filters** line, select the **Application** and click **Go**.
 - Step 3** See the Application **Server Performance** dashlet, which gives statistics on response times for the servers hosting the application. Look for sudden increases in server response time.
 - Step 4** Compare the data in **Application Server Performance** with the data in **Worst N Clients by Transaction Time** and **Worst N Sites by Transaction Time**. See if peaks in server response time match one or more users' experience of poor transaction times, or are more generalized across sites.
 - Step 5** See **Application Traffic Analysis** for peaks in usage. Use the lower graph Pan and Zoom handles to investigate the time frames of observed traffic peaks. Compare the peaks in application response time with these periods of peak usage.
 - Step 6** See **Top N Clients (In and Out)** to identify the largest bandwidth consumers for the application. Then see **Worst N Sites by Transaction Time**. Compare the information in these two dashlets to see if the biggest bandwidth consumers are also part of the worst-performing sites.
 - Step 7** Examine the worst site in **Worst N Sites by Transaction Time**: Click on the site name in the **Site** column. If needed, filter the data on the Site Detail Dashboard by the newly deployed application, as you did in Step 2.
 - Step 8** On the Site Detail Dashboard, see the **Top N Applications by Volume** and **Top N Clients (In and Out)** dashlets to confirm your picture of the top application users on this site and the time periods when performance was a problem for this application.
 - Step 9** See the **Top N Devices with Most Alarms** to see if any of the site's servers or edge routers currently have alarms that may indicate why the application performance at this site is so poor.
 - Step 10** Use **Device Reachability Status** to confirm that the suspect device is still reachable. If it is, click on its Device IP to launch its 360 View.
 - Step 11** In the 360 View:

- Click the **Interfaces** tab and confirm that sessions for the affected application flow over this device.
- Click the **Alarms** tab to see a summary of current alarms for the device.

Step 12 If this device seems to be the source of the application performance problem at this site: Click on the Alarm Browser icon at the top of the 360 View to see all alarms for this device. Use the **Show** field to limit the alarms shown to those in the time frame of the problems.



PART 6

Administering the Network

This part contains the following sections:

- [Managing System Data](#)
- [Maintaining System Health](#)
- [Controlling User Access](#)



CHAPTER 26

Managing System Data

One of the roles of an administrator is to manage Prime Infrastructure's network data collection and retention so that it:

- Scales to fit the real needs of the system's users.
- Minimizes the burden on monitored devices, applications, and network bandwidth.
- Survives hardware failures .

The following sections explain how to achieve these goals, and how to perform other data management tasks.

- [Scaling the System, page 26-1](#)
- [Handling Backups, page 26-7](#)
- [Enabling Data Deduplication, page 26-12](#)

Scaling the System

Your Prime Infrastructure system implementation should match the recommendations on appropriate OVA sizes given in the [System Requirements](#) section of the *Cisco Prime Infrastructure 1.2 Quick Start Guide*.

Note that the device, interface, and flow record recommendations given in the Quick Start Guide are all maximums, so an OVA of a given size has been tuned to handle up to this number of devices, interfaces and flows per second. Also note that the system requirements for RAM, disk space and processors are all minimums, so you can increase any of these resources and either store more data for a longer period, or process incoming flows more quickly.

As your network grows, you will approach the maximum device/interface/flow rating for your OVA. You will want to check on this from time to time (for details, see [Checking on Device and Interface Usage, page 26-2](#) and [Checking on System Disk Usage, page 26-3](#)).

If you find Prime Infrastructure is managing 80 per cent or more of your system resources or of the counts recommended for the size of OVA you have installed, Cisco recommends that you address this using one or more of the following approaches, as appropriate for your needs:

- **Add disk** —VMWare OVA technology enables you to add disk space to an existing server easily. You will need to shut down the Prime Infrastructure server and then follow the [instructions VMWare provides](#) on expanding physical disk space. Once you restart the virtual appliance, Prime Infrastructure will make use of the additional disk space automatically.

- **Limit collection**—Not all data Prime Infrastructure is capable of collecting will be of interest to you. For example: If you are not using the product to report on wireless radio performance statistics, you need not collect or retain that data, and can disable the Radio Performance collection task. Alternatively, you may decide that you need only the aggregated Radio Performance data, and can disable retention of raw performance data. For details on how to do this, see [Controlling Background Data Collection Tasks, page 26-3](#).
- **Shorten retention**—Prime Infrastructure defaults set generous retention periods for all of the data it persists and for the reports it generates. You may find that some of these periods exceed your needs, and that you can reduce them without negative effects. For details on this approach, see [Controlling Report Storage and Cleanup, page 26-4](#) and [Controlling Data Retention, page 26-4](#).
- **Off load backups and reports** —You can save space on the Prime Infrastructure server by saving reports and backups to a remote server. For details, see [Setting Up Remote Repositories, page 26-10](#).
- **Migrate to a new server** —Set up a new server that meets at least the minimum RAM, disk space and processor requirements of the next higher level of OVA. Backup your existing system, then restore it to a VM on the higher-rated server. For details, see [Restoring From Backups, page 26-11](#).

Related Topics

- [Controlling Report Storage and Cleanup, page 26-4](#)
- [Checking on System Disk Usage, page 26-3](#)
- [Controlling Background Data Collection Tasks, page 26-3](#)
- [Controlling Report Storage and Cleanup, page 26-4](#)
- [Controlling Data Retention, page 26-4](#)

Checking on Device and Interface Usage

You can quickly check on the total number of devices and interfaces Prime Infrastructure is managing using **Administration > Licenses**.

Step 1 Choose **Administration > Licenses**.

Step 2 Under **Licenses**, Prime Infrastructure displays:

- **Device Limit:** The maximum number of devices you are licensed to monitor using the product.
 - **Interface Limit:** The maximum number of interfaces you are licensed to monitor.
 - **Device Count:** The actual number of devices being monitored.
 - **Interface Count:** The actual number of interfaces being monitored.
 - **% Used:** The percentage of device licenses actually in use.
 - **% Used (PAM):** The percentage of interface licenses actually in use.
-

Checking on System Disk Usage

You can quickly check on the total system disk space usage using the **Appliance Status** tab under **Administration > Appliance**.

-
- Step 1** Choose **Administration > Appliance > Appliance Status**.
- Under **Disk Usage**, Prime Infrastructure displays the current storage allocation and percentage of use for each of the main disk volumes it uses.
-

Controlling Background Data Collection Tasks

Prime Infrastructure executes scheduled data collection tasks in the background on a regular basis. You can enable or disable these collection tasks, change the interval at which each task is executed, or change the retention period for the data (raw or aggregated) collected during each execution of each task.

Disabling or limiting these background data collection tasks can have a direct impact on how you use Prime Infrastructure, especially for reporting. To help you consider these impacts, take note of the reports this data is used in, which are listed in the Collection Set Details for each task.

-
- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Under **Data Collection Tasks**, under the **Task** heading in the table, click on the name of the task you want to change.
- Step 3** Under **Collection Set Details**, edit the following fields as appropriate:
- **Collection Status:** Indicates whether the collection task is enabled or not. Check the box to enable it, uncheck it to disable it.
 - **Interval:** The number of minutes between executions of this task.
- Step 4** If the collected data is aggregated after collection, edit the following fields as appropriate:
- **Non-Aggregation Data Retain Period:** The number of days for which the aggregated data is persisted in the database.
 - **Retain Aggregation Raw Data:** Indicates whether the raw data collected (before aggregation) is retained or not. Check the box to enable this, uncheck it to disable it. The raw data will be retained for the same period as the aggregated data.
- Step 5** Click **Save**.
-

To enable or disable background data collection tasks in bulk:

-
- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Under **Data Collection Tasks**, click the check box next to each Task you want to enable or disable.
- Step 3** In the **Go** menu, select **Enable Tasks** or **Disable Tasks**.
-

Controlling Report Storage and Cleanup

All scheduled reports are stored in the Scheduled Reports Repository. You will want to ensure that scheduled reports are retained in the report repository for reasonable lengths of time only, and deleted on a regular basis.

The default retention scheme is to retain generated reports for a maximum of 31 days. You can customize this retention period following the steps below.

-
- | | |
|---------------|------------------------------------------------------------------------------------------|
| Step 1 | Select Administration > System Settings . |
| Step 2 | Select Report |
| Step 3 | In Repository Path , specify the report repository path as needed. |
| Step 4 | Under File Retain Period , change the scheduled report retention period as needed |
| Step 5 | Click Save . |
-

Related Topics

- [Scaling the System, page 26-1](#)
- [Controlling Alarm, Event, and Syslog Retention, page 26-5](#)

Controlling Data Retention

In addition to the retention period for background data collection (see [Controlling Background Data Collection Tasks, page 26-3](#)), you can also control the retention periods for broad categories of data used in most Prime Infrastructure dashlets and reports, as explained in the following sections:

- [Controlling Alarm, Event, and Syslog Retention, page 26-5](#)
- [Controlling Health Data Retention, page 26-5](#)
- [Controlling Trend Data Retention, page 26-6](#)
- [Controlling Performance Data Retention, page 26-6](#)
- [Controlling Network Audit Data Retention, page 26-7](#)

Controlling Alarm, Event, and Syslog Retention

As part of managing your system data, you will want to ensure that raw alarm, event and syslog data are retained for reasonable lengths of time only, and deleted on a regular basis.

Data cleanup tasks run nightly to delete old alarms. In addition to the data cleanup task, Prime Infrastructure has an hourly task to check alarm table size. When the alarm table size exceeds 300,000 records, the task deletes the oldest cleared alarms until the alarm table size is within that limit.

The default retention scheme is to retain active alarms, cleared security alarms, events, and syslogs for no more than 30 days. Cleared non-security alarms are retained for 7 days only.

You can customize these retention periods following the steps below.

-
- | | |
|---------------|---------------------------------------------------------------------------------------------------------|
| Step 1 | Select Administration > System Settings . |
| Step 2 | Select Alarms and Events . |
| Step 3 | Under Alarm and Event Cleanup Options , change the alarm and event retention periods, as needed. |
| Step 4 | Under Syslog Cleanup Options , change the syslog retention period as needed. |
| Step 5 | Click Save . |
-

Related Topics

- [Scaling the System, page 26-1](#)

Controlling Health Data Retention

Device Health and System Health data are retained on an hourly, daily and weekly basis.

For Device Health data, the default retention scheme is to retain hourly data for 31 days, daily data for 90 days, and weekly data for 54 weeks.

For System Health data, the default retention scheme is to retain hourly data for 1 day, daily data for 7 days, and weekly data for 54 weeks.

You can customize these retention periods following the steps below.

-
- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | Select Administration > System Settings . |
| Step 2 | Select Data Retention . |
| Step 3 | Under Device Health Data Retain Periods , change the hourly, daily and weekly retention period, as needed. |
| Step 4 | Under System Health Data Retain Periods , change the hourly, daily and weekly retention period, as needed. |
| Step 5 | Click Save . |
-

Related Topics

- [Scaling the System, page 26-1](#)

Controlling Trend Data Retention

Trend data is aggregated and retained on an hourly, daily and weekly basis. The default retention scheme is to retain hourly data for 31 days, daily data for 90 days, and weekly data for 54 weeks.

You can customize the retention period following the steps below.

-
- | | |
|---------------|---------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Select Administration > System Settings . |
| Step 2 | Select Data Retention . |
| Step 3 | Under Trend Data Retain Periods , change the hourly, daily and weekly aggregated data retention period, as needed. |
| Step 4 | Click Save . |
-

Related Topics

- [Scaling the System, page 26-1](#)

Controlling Performance Data Retention

Performance data is retained on a short-, medium- and long-term basis . The default retention scheme is to retain short-term data for 7 days, medium-term data for 31 days, and long-term data for 378 days.

You can customize these retention periods following the steps below.

-
- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Select Administration > System Settings . |
| Step 2 | Select Data Retention . |
| Step 3 | Under Performance Data Retain Periods , change the short, medium and long-term data retention period, as needed. |
| Step 4 | Click Save . |
-

Related Topics

- [Scaling the System, page 26-1](#)

Controlling Network Audit Data Retention

Network audit data is normally deleted after 90 days.

You can customize this retention period following the steps below.

-
- | | |
|---------------|-----------------------------------------------------------------------------------------|
| Step 1 | Select Administration > System Settings . |
| Step 2 | Select Data Retention . |
| Step 3 | Under Network Audit Data Retain Period , change the retention period, as needed. |
| Step 4 | Click Save . |
-

Related Topics

- [Scaling the System, page 26-1](#)

Handling Backups

As with any other system upon which your organization relies, you will need to ensure that Prime Infrastructure is backed up regularly, so it can be restored in case of hardware failure.

Backups are always stored in a repository. You may specify remote or local backup repositories.

Backups are saved as encrypted .tar.gpg files in the specified backup repository.

Related Topics

- [Running Backups On Demand, page 26-8](#)
- [Running Backups From the Command Line, page 26-8](#)
- [Scheduling Automatic Backups, page 26-9](#)
- [Creating Backup Repositories, page 26-9](#)
- [Setting Up Remote Repositories, page 26-10](#)
- [Restoring From Backups, page 26-11](#)

Running Backups On Demand

If you want to execute an immediate system backup using the Prime Infrastructure interface, follow the steps below.

You can also run an on-demand backup from the command line (see [Running Backups From the Command Line](#), page 26-8).

-
- Step 1** Choose **Administration > Background Tasks**.
 - Step 2** Under **Other Background Tasks**, find the **NCS Server Backup** task.
 - Step 3** If you want to change the backup repository and maximum number of backups, click the **NCS Server Backup** link and adjust these values, then click **Save**.
 - Step 4** Check the **NCS Server Backup** task checkbox.
 - Step 5** In the Go menu at the top of the page, select the command **Execute Now**.
 - Step 6** Click **Go**.
 - Step 7** Click **Refresh** to see the current status of the task.
-

Running Backups From the Command Line

If you want to execute an immediate system backup using the command line, follow the steps below. Executing a backup from the command line allows you to specify the backup file name.

You can also run an on-demand backup Prime Infrastructure user interface (see [Running Backups On Demand](#), page 26-8).

-
- Step 1** At the Prime Infrastructure virtual appliance, exit to the command line.
 - Step 2** At the command line, log in using the administrator ID and password used to install Prime Infrastructure.
 - Step 3** Enter the following command to display the list of backups:

```
#show repository repositoryName
```

Where *repositoryName* is the repository alias on which you want to create the backup. (for example: RemoteFTP) .
 - Step 4** Enter the following command to back up the application:

```
#backup filename repository repositoryName application NCS
```

Where:

 - *filename* is the name of the backup file (for example: myBackup) . The date and time of the backup, as well as the .tar.gpg filename extension, will be appended to the filename you specify.
 - *repositoryName* is the name of the repository (for example: RemoteFTP) .
-

Scheduling Automatic Backups

You can schedule regular application backups through the Prime Infrastructure user interface. This method ensures that time- and processor-intensive backup processes occur at relatively low-traffic periods of the day.

If you want to back up to a new local or remote location, you must first create it. You can create a local backup repository from the Prime Infrastructure user interface. To create a remote repository, you must use both the interface and the command line. For details on all of these tasks, see [Creating Backup Repositories, page 26-9](#) and [Setting Up Remote Repositories, page 26-10](#).

To schedule automatic backups of the Prime Infrastructure application, follow these steps:

-
- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Under **Other Background Tasks**, click **NCS Server Backup**.
- Step 3** Complete the fields as follows:
- a. **Enabled:** Ensure the box is checked. Uncheck it to disable automatic backups.
 - b. **Max backups to keep:** Enter the maximum number of backups to keep (the default is 2).
 - c. **Backup Repository:** Select the backup repository.
 - d. **Interval:** Enter the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on. The default is 7, the minimum is 1, the maximum is 360.
 - e. **Time of Day:** Enter the time of day when you want the backup to start. Use this format: *hh:mm AM/PM* (for example: 03:00 AM).
- Backing up affects the performance of the server. You should schedule backups to run when the server is less active (for example, in the middle of the night).
- Step 4** Click **Save**.
-

Creating Backup Repositories

You can create new backup repositories as needed. You can then specify this new backup repository when scheduling an automatic backup or before performing an on-demand backup.

If you are only creating a new local backup repository, entering a new alias in the Name field and click Submit will be sufficient to create the new repository under the alias you specified. If the repository you are creating is located on a remote FTP server, you should first set up the server so Prime Infrastructure can write to it. For details, see [Setting Up Remote Repositories, page 26-10](#)

-
- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Under **Other Background Tasks**, click **NCS Server Backup**.
- Step 3** Next to **Backup Repository**, click **Create**.
- Step 4** In the **Name** field, enter a unique alias for the new backup repository. This alias is shown in the Backup Repository dropdown list, which you pick from when scheduling an automatic backup, or performing an on-demand backup.

- Step 5** If you want the new backup repository to be located on a remote FTP server, complete the following additional fields:
- **Type:** Ensure the **FTP Repository** box is checked
 - **FTP Location:** Enter the complete URL of the FTP repository location, including the FTP server address or hostname, and the repository path (for example: `ftp://192.198.110.100/RemoteFTP`).
 - **Username:** Enter the name of a user with write privileges on the remote FTP server.
 - **Password:** Enter the corresponding password.
- Step 6** Click **Submit**.
-

Related Topics

- [Running Backups On Demand, page 26-8](#)
- [Scheduling Automatic Backups, page 26-9](#)
- [Setting Up Remote Repositories, page 26-10](#)

Setting Up Remote Repositories

Follow the steps below to set up a symbolic link to a remote FTP backup repository so that it can be accessed from the Prime Infrastructure server.

You can locate the FTP server anywhere in your network, as long as it is accessible from the Prime Infrastructure server location. You will need to create a user with write access to the server, and a subdirectory on the server that matches the repository alias you create.



Note

Although you are not required to perform this task before creating an FTP repository using the procedure in [Creating Backup Repositories, page 26-9](#), you must do so before the first on-demand or scheduled backup to this repository takes place. If you do not, the backup will fail.

- Step 1** At the Prime Infrastructure virtual appliance, exit to the command line.
- Step 2** At the command line, log in using the administrator ID and password used to install Prime Infrastructure.
- Step 3** Enter the following command to enter server configuration mode:

```
#config t
```

- Step 4** Enter the following commands to configure a symbolic link to the remote FTP server:

```
#repository repositoryName
#url ftp://serverIPorHost
#user name password plain userPassword
```

Where:

- *repositoryName* is the repository alias as entered in the Name field when creating the new backup repository in the Prime Infrastructure user interface (for example: `RemoteFTP`).
- *serverIPorHost* is the IP address or hostname of the remote FTP server ((for example: `ftp://192.198.110.100/`).
- *name* is the name of a user with write privileges to the repository on the FTP server.
- *userPassword* is the corresponding password for that user.

- Step 5** When you are finished, press Ctrl+Z to exit configuration mode.
- Step 6** To verify creation of the symbolic link, enter the following command:
- ```
#show repository repositoryName
```
- 

## Restoring From Backups

Follow the steps below to restore Prime Infrastructure from a backup using the command line. You cannot restore from the Prime Infrastructure user interface.

You can restore to the same host machine you were using, or to a different host. Remember, however, that licenses are node-locked. If you restore to the same host, you must reapply your license files once the restore is complete. If you restore to a different host, you will need to contact Cisco license support team to re-host your licenses, then apply the re-hosted licenses.

Note that you can restore the backup from a Small OVA implementation to a Large or XLarge OVA. You cannot restore from a larger OVA to a smaller OVA.

Backup files created using the Prime Infrastructure user interface (either on demand or as a scheduled background task) are assigned generic filenames of the format `backup-yyymmdd-hhmm.tar.gpg` (for example: `backup-120806-1748.tar.gpg`). Backups created via the command line will have the filename the user specified with the timestamp from the generic format appended to the filename.

Prime Infrastructure server backups are complete application backups, containing all of the application code and all of the data it maintains. However, most machine-specific settings are not included in the backup. If you restore the backup to a different device, you will need to manually re-create these settings. Machine-specific settings include: FTP enable and disable, the FTP port, the FTP root directory, TFTP enable and disable, the TFTP port, the TFTP root directory, HTTP forward enable and disable, the HTTP port, the HTTPS port, the report repository directory, and all high availability settings.

- 
- Step 1** At the Prime Infrastructure virtual appliance, exit to the command line.
- Step 2** At the command line, log in using the administrator ID and password used to install Prime Infrastructure.
- Step 3** Enter the following command to display the list of backups:
- ```
#show repository repositoryName
```
- Where *repositoryName* is the repository alias from which you want to pull the backup. (for example: RemoteFTP).
- Step 4** Identify the backup file you want to restore and then enter the following command to restore from that file:
- ```
#restore filename repository repositoryName application NCS
```
- Where:
- filename* is the name of the backup file (for example: `backup-20120801.tar.gpg`).
  - repositoryName* is the repository alias as entered in the Name field when creating the new backup repository in the Prime Infrastructure user interface (for example: RemoteFTP).
-

# Enabling Data Deduplication

Data Deduplication allows you to identify authoritative sources for each of the following classes of application data:

- Application Response Time (for TCP applications)
- Voice/Video (for RTP applications)

Whenever Prime Infrastructure receives duplicate data about the same network elements and protocols from two or more data sources, it will resolve all such conflicts in the authoritative source's favor.

---

**Step 1** Choose **Administration > System Settings > Data Deduplication**.

**Step 2** Click **Enable Deduplication**.

---



# CHAPTER 27

## Maintaining System Health

This chapter contains the following sections:

- [Monitoring System Health, page 27-1](#)
- [Using System Logs, page 27-2](#)
- [Working with MSE Logs, page 27-3](#)
- [High Availability, page 27-5](#)
- [Configuring High Availability, page 27-6](#)
- [Changing Global Prime Infrastructure Settings, page 27-7](#)
- [Checking the Status of Prime Infrastructure, page 27-11](#)
- [Stopping Prime Infrastructure, page 27-11](#)
- [Backing Up the Database, page 27-12](#)
- [Uninstalling Prime Infrastructure, page 27-13](#)
- [Downloading Device Support and Product Updates, page 27-14](#)
- [Prime Infrastructure Licensing, page 27-15](#)
- [MSE Licensing Overview, page 27-19](#)

## Monitoring System Health

To view the system health dashboards, choose **Administration > Admin Dashboard**. [Table 27-1](#) describes the information displayed on the dashboards.

**Table 27-1**      **Administration > Admin Dashboard Information**

| Health Information Displayed | Description                                                                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Health                | Displays memory and CPU health information over a period of time.                                                                                                                                                                                                                                   |
| System Events                | Displays a list of events, time the event occurred, and the severity of the event.                                                                                                                                                                                                                  |
| System Information           | Displays general system health information such as the server name, number of jobs scheduled and running, the number of supported MIB variables, number of users logged in, etc.<br><br><b>Note</b> The count of internally scheduled jobs are also included in the total number of jobs displayed. |

## Using System Logs

Prime Infrastructure logs all error, informational, and trace messages generated by all devices that are managed by Prime Infrastructure.

Prime Infrastructure also logs all SNMP messages and Syslogs it receives.

You can download and email the logs to use for troubleshooting Prime Infrastructure.

- 
- Step 1** Choose **Administration > Logging**. The General Logging Options Screen appears.
- Step 2** Choose a Message Level.
- Step 3** Check the check boxes within the Enable Log Module option to enable various administration modules. Check the **Log Modules** option to select all modules.
- Step 4** In the Log File Settings portion, enter the following settings. These settings will be effective after restarting Prime Infrastructure.



---

**Note** The log file prefix can include the characters “%g” to sequentially number of files.

---

- Step 5** Click the Download button to download the log file to your local machine.



---

**Note** The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

---

- Step 6** Enter the Email ID or Email IDs separated by commas to send the log file.



---

**Note** To send the log file in a mail you must have Email Server Configured.

---

- Step 7** Click **Submit**.
- 

## Changing Syslog Logging Options

- 
- Step 1** Choose **Administration > Logging**, then click Syslog Logging Options.
- Step 2** Check the **Enable Syslog** check box to enable collecting and processing system logs.
- Step 3** Enter the Syslog Host IP address of the interface from which the message is to be transmitted.
- Step 4** Choose the **Syslog Facility**. You can choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.
- Step 5** Click **Save**.
-

## Customizing Logging Options to Enhance Troubleshooting

The logging screen allows you to customize the amount of data Prime Infrastructure collects in order to debug an issue. For easily reproduced issues, follow these steps prior to contacting TAC. These steps may create a smoother troubleshooting session:

- 
- Step 1** Choose **Administration > Logging**.
  - Step 2** From the Message Level drop-down list, choose **Trace**.
  - Step 3** Check each check box to enable all log modules.
  - Step 4** Reproduce the current problem.
  - Step 5** Return to the Logging Options page.
  - Step 6** Click **Download** from the Download Log File section.



**Note** The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the zip file is an html file that documents the log files.

---

- Step 7** After you have retrieved the logs, choose **Information** from the Message Level drop-down list.



**Caution**

Leaving the Message Level at *Trace* can adversely affect performance over a long period of time.

---

## Working with MSE Logs

This section describes how to configure logging options and how to download log files and contains the following topics:

- [Configuring Logging Options, page 27-3](#)
- [Downloading Mobility Services Engine Log Files, page 27-4](#)

## Configuring Logging Options

You can use Prime Infrastructure to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

- 
- Step 1** Choose **Services > Mobility Services**.
  - Step 2** Click the name of the mobility services engine that you want to configure.
  - Step 3** Choose **System > Logs**. The advanced parameters for the selected mobility services engine appear.
  - Step 4** Choose the appropriate options from the Logging Level drop-down list.  
There are four logging options: Off, Error, Information, and Trace.

All log records with a log level of Error or preceding are logged to a new error log file `locserver-error-%u-%g.log`. This is an additional log file maintained along with the location server `locserver-%u-%g.log` log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

**Caution**

Use Error and Trace only when directed to perform so by Cisco TAC personnel.

- Step 5** Select the **Enabled** check box next to each element listed in that section to begin logging its events.
- Step 6** Select the **Enable** check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.
- Step 7** To download log files from the server, click **Download Logs**. See the [“Downloading Mobility Services Engine Log Files” section on page 27-4](#) for more information.
- Step 8** In the Log File group box, enter the following:
- The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
  - The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.
- Step 9** In the MAC Address Based Logging group box, do the following:
- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.
  - Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.
- See the [“MAC Address-based Logging” section on page 27-4](#) for more information on MAC Address-based logging.
- Step 10** Click **Save** to apply your changes.

## MAC Address-based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the `locserver` directory under the following path:

`/opt/mse/logs/locserver`

A maximum of 5 MAC addresses can be logged at a time. The Log file format for MAC address `aa:bb:cc:dd:ee:ff` is `macaddress-debug-aa-bb-cc-dd-ee-ff.log`

You can create a maximum of two log files for a MAC Address. The two log files might consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files that are not updated for more than 24 hours are pruned.

## Downloading Mobility Services Engine Log Files

If you need to analyze mobility services engine log files, you can use Prime Infrastructure to download them to your system. Prime Infrastructure downloads a zip file containing the log files.

To download a zip file containing the log files, follow these steps:



- 
- Step 1** Choose **Services > Mobility Services**.
- Step 2** Click the name of the mobility services engine to view its status.
- Step 3** From the left sidebar menu, choose **Logs**.
- Step 4** Click **Download Logs**.
- Step 5** Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.
- 

## High Availability

To ensure continued operation in case of failure, Prime Infrastructure provides a high availability or failover framework. When an active (primary) Prime Infrastructure instance fails, a secondary Prime Infrastructure instance takes over operations. Upon failover, a peer of the failed primary Prime Infrastructure is activated on the secondary Prime Infrastructure using the local database and files, and the secondary Prime Infrastructure is fully functional. While the secondary host is in failover mode, the database and file backups of other primary Prime Infrastructure instances continue uninterrupted.

## Guidelines and Limitations for High Availability

Before configuring High Availability, consider the following prerequisites and limitations:

- You must have the extra hardware identical to the primary Prime Infrastructure server to run a standby instance of Prime Infrastructure.
- Prime Infrastructure supports High Availability on both the physical and virtual appliances.
- A reliable high speed wired network must exist between the primary Prime Infrastructure instance and its backup server.
- The primary and secondary Prime Infrastructure instances must be running the same Prime Infrastructure software release.
- Failover should be considered temporary. The failed primary Prime Infrastructure instance should be restored to normal as soon as possible, and failback is reinitiated.
- The primary and secondary host are not required to share the same subnet. They can be geographically separated.
- If a secondary host fails for any reason, all the primary instances are affected, and they run in stand-alone mode without any failover support.
- The ports over which the primary and secondary Prime Infrastructure servers communicate must be open (not blocked with network firewalls, application firewalls, gateways, etc.). The tomcat port is configurable during installation, and its default port is 8082. You should reserve solid database ports from 1315 to 1319.
- Any access control lists imposed between the primary and secondary Prime Infrastructure instance must allow traffic to go between the primary and secondary instances.

## Failover Scenario

When a primary Prime Infrastructure instance fails, the following events take place:

1. The primary Prime Infrastructure instance is confirmed as non-functioning (hardware crash, network crash, or the like) by the health monitor on the secondary Prime Infrastructure instance.
2. If automatic failover has been enabled, Prime Infrastructure is started on the secondary as described in Step 3. If automatic failover is disabled, an e-mail is sent to the administrator asking if they want to manually start failover.
3. The secondary Prime Infrastructure server instance is started immediately (using the configuration already in place) and uses the corresponding database of the primary. After a successful failover, the client should point to the newly activated Prime Infrastructure instance (the secondary Prime Infrastructure). The secondary Prime Infrastructure instance updates all devices with its own address as the trap destination.

**Note**

The redirecting of web traffic to the secondary Prime Infrastructure does not occur automatically. You must use your infrastructure tools to properly configure this redirection.

4. The result of the failover operation is indicated as an event, or a critical alarm is sent to the administrator and to other Prime Infrastructure instances.

## Configuring High Availability

To ensure continued operation in case of failure, you configure high availability on the primary Prime Infrastructure:

**Note**

You must specify the Prime Infrastructure role (either standalone, primary, or secondary) during installation.

**Note**

- Before you configure high availability, you must configure a mail server. See the “Configuring the Mail Server” section.
- If you specify an e-mail address in the HA Configuration page then ensure a mail server is configured and reachable.

**Step 1** Choose **Administration > High Availability**.

**Step 2** Choose **HA Configuration** from the left sidebar menu.

**Step 3** Enter the required information in the fields.

**Note**

You must enter an e-mail address when configuring high availability. Prime Infrastructure tests the e-mail server configuration, and if the test fails (because the mail server cannot connect), the high availability configuration fails.

The default admin e-mail address that you configured in Administration > System Settings > Mail Server Configuration is automatically supplied. Any changes you make to these e-mail addresses must also be entered in the Secondary SMTP Server section of the Administration > System Settings > Mail Server Configuration page.

**Step 4** Click **Save**.

#### Related Topics

- [Guidelines and Limitations for High Availability](#)
- [Failover Scenario](#)

## Changing Global Prime Infrastructure Settings

Use the menu options under the Prime Infrastructure **Administration > System Settings** menu path whenever you need to change settings that affect the product's basic behaviors. You will want to customize many of these settings when you are first implementing Prime Infrastructure, but once in production, change them only rarely.

[Table 27-2](#) lists the types of settings you can change using these menu options, and the detailed procedures in this User Guide that explain their effects and how to change them.

**Table 27-2** *Prime Infrastructure Global Settings*

| To do this:                                                                              | Choose <b>Administration &gt; System Settings &gt; ...</b>                                       |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Change which alarms, events and syslogs are deleted, and how often.                      | <b>Alarms and Events</b><br>See <a href="#">Controlling Background Data Collection Tasks</a> .   |
| Set the alarm types for which email notifications are sent, and how often they are sent. | <b>Alarms and Events</b><br>See <a href="#">Customizing Alarm Email Notifications</a> .          |
| Set the alarm types displayed in the Alarm Summary view.                                 | <b>Alarms and Events</b><br>See <a href="#">Customizing Alarm Display Settings</a> , page 27-11. |
| Change the content of alarm notifications sent by email.                                 | <b>Alarms and Events</b><br>See <a href="#">Customizing Alarm Email Content</a> , page 27-10.    |
| Choose whether audit logs are basic or template based.                                   | <b>Audit</b>                                                                                     |
| Select the device parameters to audit on.                                                | <b>Audit</b>                                                                                     |
| Enable automatic troubleshooting of clients on the diagnostic channel                    | <b>Client</b>                                                                                    |
| Enable lookup of client host names from DNS servers and set how long to cache them       | <b>Client</b>                                                                                    |
| Set how long to retain disassociated clients and their session data                      | <b>Client</b>                                                                                    |
| Poll clients to identify their sessions only when a trap or syslog is received           | <b>Client</b>                                                                                    |
| Disable saving of client association and disassociation traps and syslogs as events      | <b>Client</b>                                                                                    |

**Table 27-2** *Prime Infrastructure Global Settings (continued)*

| <b>To do this:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Choose Administration &gt; System Settings &gt; ...</b>                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Enable saving of client authentication failure traps as events, and how long between failure traps to save them.                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Client</b>                                                                                    |
| Set the protocol to be used for controller and autonomous AP CLI sessions,                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>CLI Session</b>                                                                               |
| Enable autonomous AP migration analysis on discovery                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>CLI Session</b>                                                                               |
| Enable auto refresh after a wireless controller upgrade, and process the save configuration trap.                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>Controller Upgrade Settings</b>                                                               |
| Set the retention period for the following data types: Trends, Device Health, Performance, Network Audit, System Health                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Data Retention</b><br>See <a href="#">Scaling the System, page 26-1</a> .                     |
| Enable or disable data deduplication                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>Data Deduplication</b>                                                                        |
| [Need description]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Guest Account Settings</b>                                                                    |
| Change the disclaimer text displayed at the bottom of the login page for all users.                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>Login disclaimer</b><br>Enter the login disclaimer text and click <b>Save</b> .               |
| Enable email distribution of reports and alarm notifications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>Mail server configuration</b><br>See <a href="#">Configuring the Mail Server, page 27-9</a> . |
| Configure remote event and alarm receivers who will receive notifications from Prime Infrastructure.<br><br><b>Note</b> Alerts and events are sent as SNMPv2 notifications to configured notification receivers. If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is configured. By default, only INFO level events are processed for the selected category. Only SNMPV2 traps are considered for northbound notification. | <b>Notification receivers</b>                                                                    |
| Configure proxies for the Prime Infrastructure server and its local authentication server.                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Proxy Settings</b>                                                                            |
| Set the path where scheduled reports are stored and how long reports are retained.                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Report</b>                                                                                    |
| Configure the FTP, TFTP, HTTP, HTTPS, and NTP servers used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Server settings</b>                                                                           |
| Set the severity level of any generated alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>Severity Configuration</b>                                                                    |
| Set the SNMP credentials and trace parameters to be used in tracing Rogue AP switch ports.                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>SNMP Credentials</b>                                                                          |

**Table 27-2**      **Prime Infrastructure Global Settings (continued)**

| To do this:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Choose Administration > System Settings > ... |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Set global SNMP polling parameters, including trace display values, reachability parameters and the backoff algorithm.<br><br><b>Note</b> If you select Exponential (the default value) for the Backoff Algorithm, each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time. If you select to use reachability parameters, the Prime Infrastructure defaults to the global Reachability Retries and Timeout that you configure. If unchecked, Prime Infrastructure always uses the timeout and retries specified. | SNMP Settings                                 |
| Set basic and advanced switch port trace parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Switch Port Trace                             |
| Configure global preference parameters for downloading, distributing, and recommending software Images.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Image Management                              |
| Set basic control parameters used when deploying a device configuration, such as enabling backup of the running configuration, rollbacks, retrieval of show command output from cache, and the number of CLI thread pools to use.                                                                                                                                                                                                                                                                                                                                                                                                                             | Configuration                                 |
| Set basic parameters for the configuration archive, such as protocol, timeout value, number of configuration versions to store, etc.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Configuration Archive                         |
| [Need description]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Audit Log Purge Settings                      |
| Enable automatic collection of device and interface health data, and deduplication of data on server health.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Monitoring Settings                           |

## Configuring the Mail Server

Prime Infrastructure can send reports and alarm notifications via SMTP email. To enable this functionality, you must first configure one or more SMTP email servers.

Once you have configured the server, you will want to customize your reports and alarm categories to use the function and ensure that the emails are reaching the correct people.

- 
- Step 1**      Select **Administration > System Settings**.
- Step 2**      Select **Mail Server Configuration**.
- Step 3**      Specify at least the following:
- The primary SMTP mail server hostname or IP address, and port,
  - The sender's email address. By default, this is `NCS@Address`, where *Address* is the IP address or host name of the Prime Infrastructure server.
  - A comma-separated list of one or more recipient email addresses.
- Step 4**      Optionally, you may also specify:

- A secondary email server. hostname or IP address, and port.
- Logon server usernames and passwords for the primary and secondary SMTP mail servers.
- Text to be appended to the subject line of every email.
- Whether you want the list of recipients you have specified to receive all alarm emails. If you enable this option, these recipients will be appended to the “To” line of every alarm email the system generates, in addition to any recipients you specified for individual alarm categories and severities.

**Step 5** Click **Test** to test the mail server(s). Make corrections to the configuration as needed.

**Step 6** When you are finished, click **Save**.

---

#### Related Topics

- [Customizing Alarm Email Content, page 27-10](#)

## Customizing Alarm Email Content

By default, alarm email notifications include only the alarm severity and alarm category in the subject line. The body of the email will contain the complete detail for the alarm.

You can customize the content of alarm notifications sent via email. You can:

- Choose to include the alarm’s severity, category, or prior alarm severity in the subject line of the email notification.
- Specify custom text to include in the subject line or body of the email notification.
- Replace the email subject line with the specified custom text.
- Include the current alarm condition or a link to the alarm details (instead of the text of the alarm detail) in the body of the email notification.
- Mask IP addresses and controller names in the body of the email.

These global settings apply to all alarm notifications sent by email.



#### Note

You cannot send alarm emails unless a mail server is configured.

---

**Step 1** Select **Administration > System Settings**.

**Step 2** Select **Alarms and Events**

**Step 3** Under **Alarm Email Options**, make changes as needed.

**Step 4** Click **Save**.

---

#### Related Topic

- [Customizing Alarm Display Settings, page 27-11](#)

## Customizing Alarm Display Settings

By default, the Prime Infrastructure alarm browser and other alarm lists hide all acknowledged or cleared alarms. The Alarm Display Options apply to the Alarm Summary page only. Quick searches or alarms for any entity display all alarms regardless of the acknowledged or assigned state.

You can customize how alarms are displayed using the following steps.

- 
- Step 1** Select **Administration > System Settings**.
- Step 2** Select **Alarms and Events**
- Step 3** Under **Alarm Display Options**, make changes as needed:
- Hide or show acknowledged alarms, assigned alarms, or cleared alarms.
  - Add or remove the controller name in alarm messages
  - Add or remove the Prime Infrastructure server address in all email alarm notifications
- Step 4** When you are finished, click **Save**.
- 

### Related Topics

- [Changing Alarm Status, page 11-6](#)
- [When to Acknowledge Alarms, page 11-6](#)
- [Customizing Alarm Display Settings, page 27-11](#)

## Checking the Status of Prime Infrastructure

To check the status of Prime Infrastructure from the CLI, follow these steps:

- 
- Step 1** Log into the system as **admin** by entering the following command:
- ```
ssh admin NCS(WAN)_server_IP address or hostname
```
- Step 2** Enter the following CLI:
- ```
ncs status
```
- 

## Stopping Prime Infrastructure

You can stop Prime Infrastructure at any time by following these steps:



**Note** If any users are logged in when you stop Prime Infrastructure, their sessions stop functioning.

---

- 
- Step 1** Log into the system as **admin** by entering the following command:
- ```
ssh admin (WAN)_server_IP address or hostname
```

Step 2 Enter the following CLI:

```
# ncs stop
```

Backing Up the Database

This section provides instructions for backing up the Prime Infrastructure database. You can schedule regular backups through the Prime Infrastructure user interface or manually initiate a backup.

**Note**

Machine specific settings (such as FTP enable and disable, FTP port, FTP root directory, TFTP enable and disable, TFTP port, TFTP root directory, HTTP forward enable and disable, HTTP port, HTTPS port, report repository directory, and all high availability settings) are not included in the backup and restore function if the backup is restored to a different device.

This section contains the following topic:

- [Scheduling Automatic Backups](#)

Scheduling Automatic Backups

To schedule automatic backups of the Prime Infrastructure database, follow these steps:

- Step 1** Log into the Prime Infrastructure user interface.
- Step 2** Click **Administration > Background Tasks** to display the Scheduled Tasks page.
- Step 3** Click the **NCS Server Backup** task to display the **NCS Server Backup** page.
- Step 4** Check the **Enabled** check box.
- Step 5** At the **Backup Repository** parameter, Choose an existing backup repository or click create button to create a new repository.
- Step 6** If you are backing up in remote location, select the FTP Repository check box. You need to enter the FTP location, Username and Password of the remote machine.
- Step 7** In the Interval (Days) text box, enter a number representing the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.
Range: 1 to 360
Default: 7
- Step 8** In the Time of Day text box, enter the time when you want the backup to start. It must be in this format: *hh:mm* AM/PM (for example: 03:00 AM).

**Note**

Backing up a large database affects the performance of the Prime Infrastructure server. Therefore, we recommend that you schedule backups to run when the Prime Infrastructure server is idle (for example, in the middle of the night).

- Step 9** Click **Submit** to save your settings.

The backup file is saved as a .zip file in the *ftp-install-dir/ftp-server/root/NCSBackup* directory using this format: *dd-mm-yy_hh-mm-ss.zip* (for example, 10-Dec-12_10-15-22.zip).

Uninstalling Prime Infrastructure

You can uninstall Prime Infrastructure at any time, even while Prime Infrastructure is running.

To uninstall Prime Infrastructure, follow these steps:

-
- Step 1** Log into Prime Infrastructure as **root**, then enter the following command:

```
# ncs stop
```
 - Step 2** Using the Linux CLI, navigate to the */opt/CSCOlumos* directory (or the directory chosen during installation).
 - Step 3** Enter **./Uninstall**.
 - Step 4** Click **Yes** to continue the uninstall process.
 - Step 5** Click **Finish** when the uninstall process is complete.



Note If any part of the */opt/NCS1.0.X.X* directory remains on the hard drive, manually delete the directory and all of its contents. If you fail to delete the previous Prime Infrastructure installation, this error message appears when you attempt to reinstall Prime Infrastructure: **“Cisco Prime Infrastructure is already installed. Please uninstall the older version before installing this version.”**

Recovering the Prime Infrastructure Passwords

You can change the Prime Infrastructure application root user or FTP user password. This option provides a safeguard if you lose the root password. An executable was added to the installer */bin* directory (*passwd.bat* for Windows and *passwd.sh* for Linux). To recover the passwords and regain access to Prime Infrastructure, follow these steps:



Note If you are a Linux user, you must be the root user to run the command.



Note In Linux, use the *passwd.sh* to change the Prime Infrastructure password. The *passwd* is a built-in Linux command to change the OS password.

- Step 1** Change to the Prime Infrastructure bin folder.
- Step 2** For Linux, do one of the following:

- Enter **passwd.sh root-user newpassword** to change the Prime Infrastructure root password. The new password is the root login password you choose.
- Enter **passwd.sh location-ftp-user newuser newpassword** to change the FTP user and password. The newuser and newpassword are the MSE or Location server user and password.

Step 3 The following options are available with these commands:

- -q — to quiet the output
- -pause — to pause before exiting-gui — to switch to the graphical user interface
- -force — to skip prompting for configuration

Step 4 Start Prime Infrastructure.

Downloading Device Support and Product Updates

Device Package updates and software updates for major Prime Infrastructure product releases are integrated into update bundles. These bundles are available for download directly from Cisco.

To install update bundles for Prime Infrastructure:

Step 1 Depending on your connectivity do one of the following:

- If Prime Infrastructure has external connectivity:
 - Choose **Administration > Software Update**.
 - Click **Check for Updates**.
 - Enter your Cisco.com login credentials.
- If Prime Infrastructure does not have external connectivity:
 - Go to Cisco.com/go/ncs.
 - Under Support, select **Download Software**.
 - Select **Cisco Prime Infrastructure** and then select the correct version of Prime Infrastructure
 - From the page that appears, download the latest update file (with the extension .ubf).



Note Be sure to download the software updates that match your Prime Infrastructure version. For example, software updates for release 1.1 can be installed only on Prime Infrastructure 1.1.

- Choose **Administration > Software Update**.
- Click **Upload Update File** and browse to locate the update bundles you downloaded.

The Software Updates table appears. For description of the fields see [Table 27-3](#):

Table 27-3 Software Updates Table

Field	Description
Name	The names of software updates that have been downloaded from Cisco.com.
Published Date	Date at which the software was published to Cisco.com. The Software Updates table always shows the published dates in chronological order (oldest to most recent).
Requires Restart	If the update requires a restart, the value of this field is yes .
Pending Restart	If a restart is pending for the update to be complete, the value of this field is yes .
Installed	If the software is already installed, this field has a green check mark. If the update bundle has not yet been installed, this field is blank.
Description	To see a detailed description of the software update bundle, click the small circle to the right of the description. A dialog box appears, showing the list of patches in that update bundle

Step 2 To install the software updates:

- a. Select the software updates you want to install, and click **Install**.

**Note**

When you choose an update, all the uninstalled updates published prior to the update you have chosen are also auto-selected. In Prime Infrastructure, it is mandatory to install software updates incrementally, because older updates are sometimes prerequisites to more recent updates. This behavior also occurs in uninstallation.

The installed software updates appear at the bottom of the table, with a check mark at the **Installed** column.

- b. If the **Pending Restart** value is **yes**, restart Prime Infrastructure to complete the update.
- c. To uninstall any software updates, select the updates and click **Uninstall**.

Prime Infrastructure Licensing

You purchase licenses to access the Prime Infrastructure features required to manage your network. Each license also controls the number of devices or device interfaces you can manage using those features.

You need a base license and the corresponding feature licenses (such as assurance or lifecycle license) to get full access to the respective Prime Infrastructure features to manage a set number of devices or interfaces.

If you have installed Prime Infrastructure for the first time you may access the lifecycle and assurance features using the built-in evaluation license that is available by default. The default evaluation license is valid for 60 days for 100 devices and 150 interfaces. You can send a request to ask-prime-infrastructure@cisco.com if:

- You need to extend the evaluation period
- You need to increase the device count or interface limit
- You already have a particular feature license and need to evaluate the other feature licenses

You will need to order a base license and then purchase the corresponding feature license before the evaluation license expires. The license that you purchase must be sufficient to:

- Enable access to all the Prime Infrastructure features you want to use to manage your network.
- Include all the devices and interfaces in your network that you want to manage using Prime Infrastructure.

To ensure you have the licenses to achieve the mentioned goals, do the following:

1. Familiarize yourself with the types of license packages available to you, and their requirements. See [Overview of Prime Infrastructure Licensing, page 27-16](#).
2. View the existing licenses. See [Verifying License Details, page 27-17](#) for help on ordering and downloading licenses.
3. Calculate the number of licenses you will need, based both on the package of features you want and the number of devices and device interfaces you need to manage. See [Managing License Coverage, page 27-17](#).
4. Add new licenses. See [Adding Licenses, page 27-18](#).
5. Delete existing licenses. See [Deleting Licenses, page 27-18](#).

If you are already using the Prime Infrastructure or any other network management product and you plan to extend your device or interface coverage, see [Managing License Coverage, page 27-17](#).

Overview of Prime Infrastructure Licensing

You purchase the following licenses based on the features you are required to access:

- Base License—Each Prime Infrastructure management node requires a single base license as a prerequisite for adding feature licenses.
- Lifecycle license—The lifecycle license type is based on the number of managed devices. The lifecycle license provides full access to the following Prime Infrastructure lifecycle management features:
 - Device configuration management and archiving
 - Software image management
 - Basic health and performance monitoring
 - Troubleshooting

You need to order a single base license, and then purchase lifecycle licenses as necessary to access the Prime Infrastructure lifecycle management features. Lifecycle licenses are available in bundle sizes of 25, 50, 100, 500, 1000, 2500, 5000, and 10000 devices and can be combined.

- Assurance license—The Assurance license is based on the number of NetFlow monitored interfaces. The Assurance license provides access to the following Prime Infrastructure Assurance management features:
 - End-to-end application, network, and end-user experience visibility
 - Multi-NAM management
 - Monitoring of WAN optimization

You order a single base license, and then purchase assurance licenses as necessary. Assurance licenses are available in bundle sizes of 50, 100, 500, 1000, and 5000 interfaces and can be combined.

- Special Prime Assurance Manager (PAM) -15 license—The Special PAM-15 license is a stand-alone license for commercial use. This license allows you to access a maximum of 15 managed devices and NetFlow monitored interfaces, in any combination. If you need to add more devices or interfaces you must purchase additional assurance licenses with part numbers that support 50 or more interfaces.

Managing License Coverage

Prime Infrastructure is deployed using a physical or a virtual appliance. You use the standard license center GUI to add new licenses. The new licenses are locked using the standard Cisco Unique Device Identifier (UDI) for a physical appliance and a Virtual Unique Device Identifier (VUDI) for a virtual appliance.

To view the UDI or VUDI, see [Verifying License Details, page 27-17](#).



Note

To move licenses from one physical appliance to another, call the Cisco TAC and ask to have the licenses rehomed to a new UDI.

You can upgrade to Prime Infrastructure 1.2 if you are already using one or more of the following products:

- Prime Infrastructure 1.1
- NCS 1.0 (wired and wireless)
- NCS 1.1 and the corresponding maintenance releases
- WCS 7.0

For ordering information, refer to the Ordering Guide in the Prime Infrastructure [Support](#) page.



Note

If you are using LMS, you need to migrate existing data from the previous installation to the new Prime Infrastructure installation.

Verifying License Details

Before you order new licenses, you might want to get details about your existing licenses. For example, you can verify your existing license type, product ID, device and interface limits, and number of devices and interfaces managed by your system.

To verify license details:

Choose **Administration > Licenses**.

Rest your cursor on the icon that appears next to **Licenses** to view licensing ordering help.

The licensing ordering help screen that appears provides the following information:

- Feature licenses that your system is licensed for,
- Ordering options, and
- UDI or VUDI

Adding Licenses

You need to add new licenses when:

- You have purchased a new prime Infrastructure license.
- You are already using Prime Infrastructure and have bought additional licenses.
- You are upgrading to Prime Infrastructure, see [Managing License Coverage, page 27-17](#).

To add a new license:

-
- | | |
|---------------|---------------------------------------------------------------------------------------------------|
| Step 1 | Choose Administration > Licenses . |
| Step 2 | Under the Summary folder, click Files , then click License Files |
| Step 3 | Select the licenses that you have ordered with the required device limit, then click Add . |
| Step 4 | Browse to the location of the license file, then click OK . |
-

Deleting Licenses

You might need to delete a license when:

- You are using an evaluation license and want to apply a base license.
- You are using a particular feature license and want to apply for a new license to accommodate additional devices.

To delete a license file:

-
- | | |
|---------------|------------------------------------------------------------------------|
| Step 1 | Choose Administration > Licenses . |
| Step 2 | Under the Summary folder, click Files . |
| Step 3 | Click License Files . |
| Step 4 | Select the license file you want to delete, then click Delete . |
-

Troubleshooting Licenses

To troubleshoot licenses, you will need to get details about the licenses that are installed on your system. Click **Help > About Prime Infrastructure** to access your license information.

Table 27-4 provides a few scenarios and tips for troubleshooting:

Table 27-4 Troubleshooting Scenarios

Scenario	Possible Cause	Resolution
Prime Infrastructure reports a Licensing Error.	The license file becomes corrupted and unusable if you make any modifications to the file.	<ol style="list-style-type: none"> 1. Delete the existing license. 2. Download and install a new license.
Unable to add new feature licenses.	The base license is a prerequisite to add any additional feature license.	<ol style="list-style-type: none"> 1. Install the base license 2. Add new licenses
Unable to add licenses because the UDI of the device does not match.	You are adding invalid license which is not meant for that particular system.	Add the license that is ordered for the device.
The state of the devices has changed to unmanaged.	The device limit must be equal to the interface limit. The state of the inventoried devices will change to unmanaged if you add or delete devices or device interfaces.	<ol style="list-style-type: none"> 1. Delete the additional devices or device interfaces. 2. The state of the devices will change to managed after the 24 hours synchronization. <p>To verify that the status of the inventoried devices has changed to “managed” after synchronization:</p> <p>Choose Operate > Device Work Center > Collection Status</p> <p>Hover the mouse over the circle beside the device name to view the collection status details.</p>

MSE Licensing Overview

The MSE packages together multiple product features related to network topology, design such as NMSP, Network Repository along with related Service Engines, and application processes, such as the following:

- Context-Aware Service
- Wireless Intrusion Prevention System (WIPS)

To enable smooth management of MSE and its services, various licenses are offered.



Note

You must have a Cisco Prime Infrastructure license to use MSE and its associated services.

This section contains the following topics:

- [MSE License Structure Matrix, page 27-20](#)
- [Sample MSE License File, page 27-20](#)
- [Revoking and Reusing an MSE License, page 27-20](#)
- [MSE Services Co-Existence, page 27-21](#)
- [Managing Mobility Services Engine \(MSE\) Licenses, page 27-21](#)

MSE License Structure Matrix

Table 27-5 lists the breakdown of the licenses between the High end, Low end and Evaluation licenses for MSE, Location services, SCM, wIPS and MIR.

Table 27-5 *MSE License Structure Matrix*

	High End	Low End	Evaluation
MSE Platform	High-end appliance and infrastructure platform such as the Cisco 3350 and 3355 mobility services engines.	Low-end appliance and infrastructure platform such as Cisco 3310 mobility services engine.	—
Context Aware Service	25,000 Tags	2000 Tags	Validity 60 days, 100 Tags and 100 Elements.
	25,000 Elements	2000 Elements	
wIPS	3000 access points	2000 access points	Validity 60 days, 20 access points.

Sample MSE License File

The following is a sample MSE license file:

```
FEATURE MSE cisco 1.0 permanent uncounted \
  VENDOR_STRING=UDI=udi,COUNT=1 \
  HOST ID=ANY \
  NOTICE="<LicFileID>MSELICENSE</LicFileID><LicLineID>0</LicLineID> \
  <PAK>dummyPak</PAK>" \
  SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
  45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
  1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

This sample file has 5 license entries. The first word of the first line of any license entry tells you what type of license it is. It can either be a Feature or Increment license. A feature license is a static lone item to license. There can be multiple services engines running in MSE. An Increment license is an additive license. In MSE, the individual service engines are treated as increment licenses.

The second word of the first line defines the specific component to be licensed. For example, MSE, LOCATION_TAG. The third word depicts the vendor of the license, for example Cisco. The fourth word denotes the version of the license, example 1.0. The fifth word denotes the expiration date, this can be permanent for licenses that never expire or a date in the format dd-mm-yyyy. The last word defines whether this license is counted.

Revoking and Reusing an MSE License

You can revoke an MSE appliance license from one system and reuse it on another system. When you revoke a license, the license file is deleted from the system. If you want to reuse the license on another system, then the license needs to be rehosted.

If you want to reuse a license with an upgrade SKU on another system, then you must have the corresponding base license SKU installed in the system to which you want to reuse the upgrade SKU. You cannot reuse the upgrade license SKU in a system if the corresponding base license SKU is deleted from it.

When you revoke a license, MSE restarts the individual service engines to reflect the changes to the licenses. Then the service engines receives the updated capacity from MSE during startup.

MSE Services Co-Existence

With MSE 6.0 and later, you can enable multiple services (Context Aware and wIPS) to run concurrently. Before Version 6.0, mobility services engines only supported one active service at a time.

The following must be considered with co-existence of multiple services:

- Co-existence of services might be impacted by license enforcement. As long as the license is not expired, you can enable multiple services.

**Note**

Limits for individual services differ. For example, a low-end mobility services engine (MSE-3310) tracks a total of 2,000 CAS elements; a high-end mobility services engine (MSE-3350) tracks a total of 25,000 CAS elements.

A low-end mobility services engine has a maximum limit of 2000 wIPS elements; a high-end mobility services engine has a maximum limit of 3000 wIPS elements.

- Expired evaluation licenses prevent the service from coming up.
- If a CAS license is added or removed, this process restarts all services on the mobility services engine including wIPS. If a wIPS license is added or removed, the process does not impact CAS; only wIPS restarts.
- Other services can be enabled in evaluation mode even if a permanent license for the maximum number of elements has been applied.

Whenever one of the services has been enabled to run with its maximum license, another service cannot be enabled to run concurrently because the capacity of the MSE is not sufficient to support both services concurrently. For example, on MSE-3310, if you install a wIPS license of 2000, then you cannot enable CAS to run concurrently. However, evaluation licenses are not subject to this limitation.

Managing Mobility Services Engine (MSE) Licenses

If you choose Files > MSE Files from the left sidebar menu, you can manage the mobility services engine licenses.

This section contains the following topics:

- [Registering Product Authorization Keys, page 27-22](#)
- [Installing Client and wIPS License Files, page 27-23](#)
- [Deleting a Mobility Services Engine License File, page 27-24](#)

The page displays the mobility services engine licenses found and includes the following information:

**Note**

Because tag licenses are added and managed using appropriate vendor applications, tag licenses are not displayed in this page. Refer to the following URL for more information:

<http://support.aeroscout.com>.

Evaluation (demo) licenses are also not displayed.

Tag licenses are installed using the *AeroScout System Manager* only if the tags are tracked using Partner engine. Otherwise the tags will be counted along with the CAS element license.

- MSE License File—Indicates the MSE License.
- MSE—Indicates the MSE name.
- Type—Indicates the type of mobility services engine (client elements, wIPS local mode or wIPS monitor mode access points).
- Limit—Displays the total number of client elements or wIPS monitor mode access points licensed across the mobility services engine.
- License Type—Permanent licenses are the only license types displayed on this page.
 - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

Registering Product Authorization Keys

You receive a product authorization key (PAK) when you order a client, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for install on the mobility services engine. License files are emailed to you after successfully registering a PAK.

Client and wIPS PAKs are registered with Cisco.

**Note**

Tag PAKs are registered with AeroScout. To register your tag PAK, go to this URL:

<http://www.aeroscout.com/content/support>

To register a product authoritative key (PAK) to obtain a license file for install, follow these steps:

Step 1 Open a browser page and go to www.cisco.com/go/license.

**Note**

You can also access this site by clicking the Product License Registration link located on the License Center page of NCS.

Step 2 Enter the PAK and click **SUBMIT**.

Step 3 Verify the license purchase. Click **Continue** if correct. The licensee entry page appears.

**Note**

If the license is incorrect, click the **TAC Service Request Tool** link to report the problem.

Step 4 At the Designate Licensee page, enter the mobility service engine UDI in the host ID text box. This is the mobility services engine on which the license will be installed.

**Note**

UDI information for a mobility services engine is found in the General Properties group box at Services > Mobility Services Engine > *Device Name* > *System*.

- Step 5** Select the **Agreement** check box. Registrant information appears beneath the Agreement check box. Modify information as necessary.

**Note**

Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.

- Step 6** If registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the end user information.
- Step 7** Click **Continue**. A summary of entered data appears.
- Step 8** At the Finish and Submit page, review registrant and end user data. Click **Edit Details** to correct information, if necessary.
- Step 9** Click **Submit**. A confirmation page appears.

Installing Client and wIPS License Files

You can install CAS element licenses and wIPS licenses from Prime Infrastructure.

**Note**

Tag licenses are installed using the *AeroScout System Manager*. Refer to the following URL for additional information:

<http://support.aeroscout.com>.

To add a client or wIPS license to Prime Infrastructure after registering the PAK, follow these steps:

- Step 1** Choose **Administration > License Center**.
- Step 2** From the left sidebar menu, choose **Files > MSE Files**.
- Step 3** From the License Center > Files > MSE Files page, click **Add** to open the Add a License File dialog box.
- Step 4** From the MSE Name drop-down list, choose the mobility services engine to which you want to add the license file.

**Note**

Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

- Step 5** Enter the license file in the License File text box or browse to the applicable license file.
- Step 6** Once displayed in the License File text box, click **Upload**. Newly added license appears in mobility services engine license file list.

**Note**

A Context Aware Service (CAS) restarts if a client or tag license is installed; a wIPS service restarts if a wIPS license is installed.

**Note**

Services must come up before attempting to add or delete another license.

Deleting a Mobility Services Engine License File

To delete a mobility services engine license file, follow these steps:

- Step 1** From the License Center > Files > MSE Files page, select the check box of the mobility services engine license file that you want to delete.
- Step 2** Click **Delete**.
- Step 3** Click **OK** to confirm the deletion.



CHAPTER 28

Controlling User Access

This chapter contains the following sections:

- [Managing Users, page 28-1](#)
- [Managing Lobby Ambassador Accounts, page 28-2](#)
- [Managing Guest User Accounts, page 28-4](#)
- [Changing User Passwords, page 28-8](#)
- [Changing User Privileges, page 28-8](#)
- [Managing User Groups, page 28-8](#)
- [Changing Password Policy, page 28-9](#)
- [Setting the AAA Mode, page 28-10](#)
- [Changing Virtual Domains, page 28-10](#)
- [Auditing Access, page 28-11](#)
- [Viewing Audit Logs, page 28-12](#)
- [Adding TACACS+ Server, page 28-12](#)
- [Adding a RADIUS Server, page 28-13](#)

Managing Users

All Prime Infrastructure users have basic parameters such as user name and password. Users with admin privileges can view active user sessions.

To view active sessions:

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Active Sessions**.
- Step 2** Click the **Audit Trail** icon to for the username for which you want to see the following data:
- User—User login name
 - Operation—Type of operation audited
 - Time—Time operation was audited
 - Status—Success or failure
 - Reason—Failure reason when the user login failed

- **Configuration Changes**—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

**Note**

The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

Adding a User

You can add a user and assign predefined static roles. Besides complete access, you can give administrative access with differentiated privileges to certain user groups. Prime Infrastructure supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Users**.
 - Step 2** Choose **Add a User**, then click **Go**.
 - Step 3** Enter the username, password, and confirm password for the new user, then choose the groups to which this user belongs.
 - Step 4** Click the Virtual Domains tab to assign a virtual domain to this user. See [Changing Virtual Domains](#).
 - Step 5** Click **Save**.
-

Managing Lobby Ambassador Accounts

You can use the Cisco Lobby Ambassador to create guest user accounts in Prime Infrastructure. A guest network provided by an enterprise allows access to the Internet for a guest without compromising the host. The web authentication is provided with or without a supplicant or client, so a guest needs to initiate a VPN tunnel to their desired destinations.

Both wired and wireless guest user access is supported. Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

The network administrator must first set up a lobby ambassador account. This allows a nontechnical person to create and manage guest user accounts on the Prime Infrastructure. Guest user accounts are for visitors such as temporary workers who need network access.

This section contains the following topics:

- [Creating a Lobby Ambassador Account, page 28-3](#)
- [Logging the Lobby Ambassador Activities, page 28-4](#)

Creating a Lobby Ambassador Account


Note

A group that has the SuperUser/administrator privileges (by default) can create a lobby ambassador account.

To create a lobby ambassador account in Prime Infrastructure:

-
- Step 1** Log into Prime Infrastructure user interface as an administrator.
 - Step 2** Choose **Administration > Users, Roles & AAA**.
 - Step 3** From the left sidebar menu, choose **Users**.
 - Step 4** From the Select a command drop-down list, choose **Add User**.
 - Step 5** Click **Go**.
 - Step 6** Enter the username.
 - Step 7** Enter the password. Reenter to confirm the password. Password requirements include the following:
 - The password must have a minimum of eight characters.
 - The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, or special characters.
 - Step 8** In the Groups Assigned to this User section, select the **LobbyAmbassador** check box to access the Lobby Ambassador Defaults tab.

The Lobby Ambassador Defaults tab has the following parameters:

- Profile—The default profile to which the guest users would connect.
- Lifetime—Limited or Unlimited.


Note

By default, the lifetime is limited to eight hours.

- Apply to—From the drop-down list, choose one of the following:
 - **Indoor Area**—Campus, Building, and Floor.
 - **Outdoor Area**—Campus, Outdoor Area.
 - **Controller List**—List of controller(s) on which the selected profile is created.
 - **Config Groups**—Config group names configured on Prime Infrastructure.
- Email ID—The e-mail ID of the host to whom the guest account credentials are sent.
- Description—A brief description of this account.
- Disclaimer—The default disclaimer text.
- Defaults Editable—Select this check box if you want to allow the lobby ambassador to override these configured defaults. This allows the lobby ambassador to modify these Guest User Account default settings while creating Guest Accounts from the Lobby Ambassador portal.


Note

If no default profile is selected on this tab, the defaults are not applied to this Lobby Ambassador. However, the Lobby Ambassador account is created and the Lobby Ambassador can create users with credentials as desired.

- **Max User Creation Allowed**—Select this check box to set limits on the number of guest users that can be created by the Lobby Ambassador in a given time period. The time period is defined in hours, days, or weeks.

Step 9 Click **Save**. The name of the new lobby ambassador account is listed and the account can be used immediately.

Logging the Lobby Ambassador Activities

The following activities are logged for each lobby ambassador account:

- **Lobby ambassador login**—The Prime Infrastructure logs the authentication operation results for all users.
- **Guest user creation**—When a lobby ambassador creates a guest user account, the Prime Infrastructure logs the guest username.
- **Guest user deletion**—When a lobby ambassador deletes the guest user account, the Prime Infrastructure logs the deleted guest username.
- **Account updates**—The Prime Infrastructure logs the details of any updates made to the guest user account. For example, increasing the life time.

To view the lobby ambassador activities:



Note You must have administrative permissions to open this window.

- Step 1** Log into the Prime Infrastructure user interface as an administrator.
- Step 2** Choose **Administration > Users, Roles & AAA > User Groups** from the left sidebar menu to display the User Groups page.
- Step 3** On the User Groups page, click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail page for the lobby ambassador appears.

This page enables you to view a list of lobby ambassador activities over time.

- **User**—User login name
- **Operation**—Type of operation audited
- **Time**—Time operation was audited
- **Status**—Success or failure

Step 4 To clear the audit trail, choose **Clear Audit Trail** from the Select a command drop-down list, and click **Go**.

Managing Guest User Accounts

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.

- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the beginning and the end of the valid time period or configures the account with an unlimited lifetime.

This sections contains the following topics:

- [Logging in to the Prime Infrastructure User Interface as a Lobby Ambassador, page 28-5](#)
- [Adding a New Guest User Account, page 28-6](#)
- [Scheduling a Guest User Account, page 28-6](#)
- [Printing/Emailing User Details, page 28-6](#)
- [Saving Guest Accounts to Device, page 28-7](#)
- [Configuring User Preferences, page 28-7](#)

Logging in to the Prime Infrastructure User Interface as a Lobby Ambassador

When you log in as a lobby ambassador, you have access to the guest user template page in the Prime Infrastructure. You can then configure guest user accounts (through templates).

To log into the Prime Infrastructure user interface through a web browser:

Step 1 Launch Internet Explorer 7.0 or later on your computer.



Note Some Prime Infrastructure features might not function properly if you use a web browser other than Internet Explorer 7.0 or later on a Windows workstation.

Step 2 In the browser address line, enter **https://PI-ip-address** (such as https://1.1.1.1), where *PI-ip-address* is the IP address of the computer on which the Prime Infrastructure is installed. Your administrator can provide this IP address.

Step 3 When the Prime Infrastructure user interface displays the Login window, enter your username and password.



Note All entries are case sensitive.



Note The lobby ambassador can only define guest users templates.

Step 4 Click **Submit** to log into the Prime Infrastructure. The Prime Infrastructure user interface is now active and available for use. The Guest Users page is displayed. This page provides a summary of all created Guest Users.

To exit the Prime Infrastructure user interface, close the browser window or click **Logout** in the upper right corner of the page. Exiting a Prime Infrastructure user interface session does not shut down the Prime Infrastructure on the server.

**Note**

When a system administrator stops the Prime Infrastructure server during a Prime Infrastructure session, the session ends, and the web browser displays this message: “The page cannot be displayed.” Your session does not reassociate to the Prime Infrastructure when the server restarts. You must restart the Prime Infrastructure session.

Adding a New Guest User Account

To create a new guest user account:

- Step 1** In the Guest User list page, choose **Add Guest User** from the Select a command drop-down list, and then click **Go**.
- Step 2** In the Create a Guest User Account page, complete the fields as described in [Table 31-68](#) and [Table 31-69](#).
- Step 3** Click **Save**. The guest user account appears on the Guest User list page.

Scheduling a Guest User Account

To schedule a guest user account:

- Step 1** In the Guest User list page, choose **Schedule Guest User** from the Select a command drop-down list, and then click **Go**.
- Step 2** Complete the fields as described in [Table 31-68](#) and [Table 31-69](#).
- Step 3** Click **Save**.

Printing/Emailing User Details

To print or e-mail user details:

- Step 1** In the Guest User list page, select the check box of the guest user whose details you want to print or e-mail.
- Step 2** From the Select a command drop-down list, choose **Print/Email User Details**.
- Step 3** Click **Go**.
- Step 4** Review the credentials for this guest user and click the Email or Print icon, as applicable.
- Step 5** Click **Back** to return to the previous page.

**Note**

If the Prime Infrastructure reports a failure in sending e-mail, contact the Prime Infrastructure administrator. The e-mail setting on the Prime Infrastructure may not be configured properly.

Saving Guest Accounts to Device

The Save Guest Accounts to Device feature allows you to save respective guest accounts on the controller flash. When selected, all of the guest accounts on the controller are saved for each of the flash memory of controller. This ensures that the guest accounts are retained on the controllers in case the controllers accidentally reboot.

**Note**

This feature is supported on controller Version 4.2.99.0 and later.

To save guest accounts on the controller flash:

- Step 1** In the Guest User list page, choose **Save Guest Accounts on device** from the Select a command drop-down list.
- Step 2** Click **Go**. All guest accounts currently present on each of the WLCs are saved.

Configuring User Preferences

The User Preferences page enables you to control the list page display options and idle timeout options in the Prime Infrastructure.

To configure the user preferences:

- Step 1** Log into the Prime Infrastructure as a lobby ambassador.
- Step 2** From the left sidebar menu, choose **User Preferences**.
- Step 3** Enter the following information:
 - List Pages
 - Items Per List—You can set the number of guest users to display in the Guest Users list page. Choose the number of items to display from the Items Per List Page drop-down list.
 - User Idle Timeout
 - Logout idle user—Select the check box if you want to configure the amount of time, in minutes, that a user session can be idle before the server cancels the session.

**Note**

If the Logout idle user check box is unselected, the user session will not be timed out.

- Logout idle user after—Choose the maximum number of minutes that a server waits for an idle user. The default value is 60 minutes. The minimum value is 15 minutes. The maximum value is 120 minutes.

Step 4 Click **Save**.

Changing User Passwords

To change the password for a user:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **Users**.

Step 2 Select the user name who's password you want to change.

Step 3 Complete password fields, then click **Save**.

Changing User Privileges

Prime Infrastructure uses a list of tasks to control which part of Prime Infrastructure users can access and the functions they can perform in those parts. You change user privileges in Prime Infrastructure by changing the User Group to which each user belongs. You use the User Group Task List to change what users in each group are authorized to do and the screens they can access.

You can also assign the sites or devices to which a virtual domains has access.

To edit the task list for a user group:

Step 1 Choose **Administration > Users, Roles & AAA**, then click **User Groups**.

Step 2 Click on a group name to change the tasks this group is allowed to perform.

Step 3 Click the Members tab to view the users of this group.

Managing User Groups

Prime Infrastructure has pre-defined user groups as described in. You can change the privileges for the users, but you cannot add additional users. When you create a new user, you assign that user to a group.

[Table 28-1](#) describes the Prime Infrastructure default user groups and their privileges.

Table 28-1 Default User Groups

Group Name	Privileges for Users in the Group
System Monitoring	Monitor Prime Infrastructure operations.
ConfigManagers	Monitor and configure Prime Infrastructure operations.

Table 28-1 **Default User Groups**

Group Name	Privileges for Users in the Group
Admin	Monitor and configure Prime Infrastructure operations and perform all system administration tasks except administering Prime Infrastructure user accounts and passwords.
SuperUsers	Monitor and configure Prime Infrastructure operations and perform all system administration tasks including administering Prime Infrastructure user accounts and passwords. Superusers tasks can be changed.
North bound API	Used only with Prime Infrastructure Navigator.
User Assistant	Local net user administration only. User assistants cannot configure or monitor devices.
Lobby Ambassador	Guest access for only configuration and managing of user accounts.
Monitor lite	Monitoring of assets location.
Root	Monitor and configure Prime Infrastructure operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user.

To view user groups and their associated tasks:

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **User Groups**.
- Step 2** Click on a group name to change the tasks this group is allowed to perform.
- Step 3** Click the Members tab to view the users of this group.
-

Changing Virtual Domain Access

To edit the sites or devices to which a virtual domains has access:

-
- Step 1** Choose **Administration > Virtual Domains**.
- Step 2** Select the domain to which you want to assign sites or devices.
- Step 3** Click the **Sites** or **Devices** tab, then move the necessary items from the Available list to the Selected list.
- Step 4** Click **Submit**.

To associate users to Virtual Domains, choose **Administration > Users, Roles & AAA**, then click **Users**. See [Assigning Users to a Virtual Domain](#).

Changing Password Policy

Prime Infrastructure supports various password policy controls, such as minimum length, repeated characters, etc.

To change password policies:

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Local Password Policy**.
- Step 2** Chose the necessary policies, then click **Save**.
-

Setting the AAA Mode

Prime Infrastructure supports local as well as TACACS+ and RADIUS, but you must specify a TACACS+ or RADIUS server first.

To specify a TACACS+ server and then change the AAA mode to TACACS+:

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.
- Step 2** From the command pull-down menu, choose **Add TACACS+ Server**, then click **Go**.
- Step 3** Enter the TACACS+ server parameters, then click **Save**.
- Step 4** Click **AAA Mode**.
- Step 5** Select TACACS+ and specify whether to enable fallback to the local condition.
- Step 6** Click **Save**.
-

Changing Virtual Domains

A Prime Infrastructure Virtual Domain consists of a set of Prime Infrastructure devices and/or maps and restricts a user view to information relevant to these managed objects.

Through a virtual domain, an administrator can ensure that users are only able to view the devices and maps for which they are responsible. In addition, because of the virtual domain filters, users are able to configure, view alarms, generate reports for *only* their assigned part of the network.

The administrator specifies for each user a set of allowed virtual domains. Only one of these can be active for that user at login. The user can change the current virtual domain by selecting a different allowed virtual domain from the Virtual Domain drop-down list at the top of the page. All reports, alarms, and other functionality are now filtered by that virtual domain.

If there is only one virtual domain defined (“root”) in the system AND the user does not have any virtual domains in the custom attributes fields in the TACACS+/RADIUS server, the user is assigned the “root” virtual domain by default. If there is more than one virtual domain, and the user does not have any specified attributes, then the user is blocked from logging in.

To add sites and devices to a virtual domain:

-
- Step 1** Choose **Administration > Virtual Domains**.
- Step 2** From the left Virtual Domain Hierarchy sidebar menu, click the virtual domain to which you want to add a site or device.
- Step 3** Move the sites and devices from the Available to the Selected column, then click **Submit**.
-

To add a user to a virtual domain:

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Users**.
- Step 2** Click on the user you want to add to a virtual domain.
- Step 3** Click the Virtual Domains tab.
- Step 4** Move the virtual domain to which you want to add the user from the Available Virtual Domains column to the Selected Virtual Domains column, then click **Save**.



Note

Each virtual domain may contain a subset of the elements included with its parent virtual domain. When a user is assigned a virtual domain, that user can view the devices that are assigned to its virtual domain.

Auditing Access

Prime Infrastructure maintains an audit record of user access.

To access the audit trail for a user or user's active sessions:

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Active Sessions**.
- Step 2** Click the **Audit Trail** icon to for the username for which you want to see the following data:
- User—User login name
 - Operation—Type of operation audited
 - Time—Time operation was audited
 - Status—Success or failure
 - Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.



Note

The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

To access the audit trail for a user group:

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **User Groups**.
- Step 2** Click the **Audit Trail** icon to for the username for which you want to see the following data:
- User—User login name
 - Operation—Type of operation audited
 - Time—Time operation was audited

- Status—Success or failure
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click on the Details link for more information on the configuration changes done by an individual user.

**Note**

The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

Viewing Audit Logs

Prime Infrastructure provides two types of audit logs:

- Application Audit logs—Logs events that pertain to the Prime Infrastructure features. For example, you can view the application audit log to see when a particular user logged in and what actions were taken.
- Network Audit logs—Logs events related to the devices in your network. For example, you can view the network audit logs to see which user deployed a specific template and the date and time the template was deployed.

To view Application Audit Logs:

-
- Step 1** Choose **Administration > System Audit**.
- Step 2** In the Application Audit Logs page, click to expand the row for which you want to view details about the log.

**Note**

For Application Audit, the User Group column is blank for TACACS+/RADIUS users.

To view Network Audit Logs:

-
- Step 1** Choose **Operate > Network Audit**.
- Step 2** In the Network Audit Logs page, click to expand the row for which you want to view details about the log.
-

Adding TACACS+ Server

To configure Prime Infrastructure so it can communicate with the TACACS+ server:

-
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.

- Step 2** Choose Add TACACS+ Server, then click **Go**.
- Step 3** Enter the TACACS+ server information, then click **Save**.



Note For Prime Infrastructure to communicate with the TACACS+ server, the shared secret you enter on this page must match the shared secret configured on the TACACS+ server.

Adding a RADIUS Server

To configure Prime Infrastructure so it can communicate with the RADIUS server:

- Step 1** Choose **Administration > Users, Roles & AAA**, then click **RADIUS Servers**.
- Step 2** Choose Add Radius Server, then click **Go**.
- Step 3** Enter the RADIUS server information, then click **Save**.



Note For Prime Infrastructure to communicate with the RADIUS server, the shared secret you enter on this page must match the shared secret configured on the RADIUS server.



CHAPTER 29

Reports

The Cisco Prime Infrastructure reporting is necessary to monitor the system and network health as well as troubleshoot problems. A number of reports can be generated to run on an immediate and scheduled basis. Each report type has a number of user-defined criteria to aid in the defining of the reports. The reports are formatted as a summary, tabular, or combined (tabular and graphical) layout. Once defined, the reports can be saved for future diagnostic use or scheduled to run and report on a regular basis.

Reports are saved in either CSV or PDF format and are either saved to a file on Prime Infrastructure for later download or emailed to a specific email address.

The reporting types include the following:

- Current, which provides a snap shot of the data that is not dependent upon time.
- Historical, which retrieves data from the device periodically and stores it in Prime Infrastructure database
- Trend, which generates a report using aggregated data. Data can be periodically collected based from devices on user-defined intervals, and a schedule can be established for report generation.

With Prime Infrastructure, you also have the ability to export any report that you can view, sort reports into logical groups, and archive for long-term storage.

The Reports menu provides access to all Prime Infrastructure reports as well as currently saved and scheduled reports.

- Report Launch Pad—The hub for all Prime Infrastructure reports. From this page, you can access specific types of reports and create new reports.
- Scheduled Run Results—Allows you to access and manage all currently scheduled runs in Prime Infrastructure. In addition, allows you to access and manage on-demand export as well as emailed reports.
- Saved Report Templates—Allows you to access and manage all currently saved report templates in Prime Infrastructure.

This section contains the following topics:

- [Configuring and Managing Reports, page 29-2](#)
- [Managing Scheduled Run Results, page 29-4](#)
- [Managing Saved Report Templates, page 29-4](#)

Configuring and Managing Reports

The Report Launch Pad provides access to all Prime Infrastructure reports from a single page. From this page, you can create and save new reports, view current reports, open specific types of reports, schedule a report to run at a later point in time, and customize the results of a report.

**Tip**

Hover your mouse cursor over the tool tip next to the report type to view more report details.

This section contains the following topics:

- [Creating, Scheduling, and Running New Reports, page 29-2](#)
- [Customizing Report Results, page 29-3](#)

Creating, Scheduling, and Running New Reports

To create and run new reports:

Step 1 Choose **Report > Report Launch Pad**.

The reports are listed by category in the main section of the page and on the left sidebar menu. Click on a category on the left sidebar menu to see the report types for each report category.

Step 2 Find the appropriate report in the main section of the Report Launch Pad.

To view currently saved report templates for a report type, click the report name on the Report Launch Pad, or click on the report type in the navigation on the left side of the Report Launch Pad page. The currently saved templates will be listed in the main section of the page.

Step 3 Click **New** to the right of the report. The Report Details page for the report you selected appears.**Step 4** In the Report Details page, complete the fields as described in [Table 32-1](#). Parameters shown in the Report Details will vary with the report type.

With some reports, you will need to customize the report results. See [Customizing Report Results, page 29-3](#)

Step 5 If you plan to run this report at a later point in time or as a recurring report, enter Schedule parameters as explained in the “Schedule” section of [Table 32-1](#). The Schedule parameters allow you to control when and how often the report must run.**Step 6** When all report parameters have been set, choose one of the following:

- **Run**—Click to run the report without saving the report setup.
- **Save**—Click to save this report setup without immediately running the report. If you have entered Schedule parameters, the report runs automatically at the scheduled data and time.
- **Run and Save**—Click to save this report setup and run the report immediately.
- **Save and Export**—Click to save the report, run it, and export the results to a file. You will be prompted to:
 - Select the exported report’s file format (CSV or PDF).
 - Choose whether to send an email when the report has been generated. If you choose this option, you must enter the destination email address and the email subject line content, and choose whether you want the exported file included as an attachment to the email.

When you are finished, click OK.

- **Save and Email**—Click to save the report, run it, export the results as a file and email the file. You will be prompted to:
 - Select the exported report file format,
 - Enter the destination email address and the email subject line content.

When you are finished, click OK.

- **Cancel**—Click to return to the previous page without running or saving this report.

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

**Note**

You cannot change or update the generated reports together for all sub domains. You can open the generated reports individually through respective subdomains to change the reports. If all reports need to be updated, then delete all the reports created on subdomains and then regenerate the virtual domain reports using the add new report workflow with the changes.

Customizing Report Results

Many reports allow you to customize their results, so that you can include exclude different types of information. If the report you are creating permits this, it will display a **Customize** button. You can click this button to access the Create Custom Report page and customize the report results.

Customizing report results is sometimes required. For example: Adding Flexible NetFlow (FNF) Extension parameters to the Traffic Analysis, Application, or Voice Video Data monitoring templates makes them part of your Prime Infrastructure monitoring setup. But it does not mean the collected FNF extension monitoring data will appear automatically in the corresponding Conversations reports for Core, ART and RTP performance. To ensure this FNF data is included in these Conversations reports, you must add these FNF parameters to the “Data fields to include” column using the Create Custom Report page (see [Table 32-2](#)).

To customize report results:

Step 1 Choose **Report > Report Launch Pad**.

The reports are listed by category in the main section of the page and on the left sidebar menu.

Step 2 Click the Report Title link for the appropriate report to open the Report Details page.

Step 3 Click **Customize** to open the Create Custom Report page.

Step 4 Complete the fields as described in [Table 32-2](#).

Step 5 Click **Apply** to confirm the changes.

**Note**

The changes made in the Create Custom Report page are not saved until you click **Save** on the Report Details page.

Managing Scheduled Run Results

To view all currently scheduled runs in Prime Infrastructure, choose **Report > Scheduled Run Results**.

**Note**

The scheduled report tasks are not visible outside the Virtual Domain they run in. The results of the scheduled report tasks are visible from the Scheduled Run Results page of respective domains.

**Note**

The list of scheduled runs can be sorted by report category, report type, time frame, and report generation method. For information about the fields on this page, see [Table 32-3](#).

The Scheduled Run Results page displays the following information:

- Report Title—Identifies the user-assigned report name.

**Note**

Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Status—Indicates whether or not the report ran successfully.
- Message—Indicates whether or not this report was saved and the file name for this report (if saved).
- Run Date/Time—Indicates the date and time that the report is scheduled to run.
- History—Click the History icon to view all scheduled runs and their details for this report.
- Download—Click the Download icon to open or save a .csv/.pdf file of the report results.

Managing Saved Report Templates

In the Saved Report Templates page, you can create and manage saved report templates. You can also enable, disable, delete, or run currently saved report templates. To open this page in Prime Infrastructure, choose **Report > Saved Report Templates**.

**Note**

The list of saved report templates can be sorted by report category, report type, and scheduled status (enabled, disabled, or expired). For information about the fields on this page, see [Table 32-4](#).

The Saved Report Templates page displays the following information:

- Report Title—Identifies the user-assigned report name.

**Note**

Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Run—Click the **Run** icon to immediately run the current report.



PART 7

References

This part contains the following sections:

- [Prime Infrastructure User Interface](#)
- [Field Reference](#)
- [Field Reference for Reports](#)



CHAPTER 30

Prime Infrastructure User Interface

Prime Infrastructure is a web-based application. Tabs on the user interface are either specific to a particular Cisco Prime product or can be shared across multiple Cisco Prime products. The options on application tabs are displayed when you rest your cursor on the tab.

Not all tabs or options are activated if any of your installed Cisco Prime products are not enabled through licensing.

This chapter contains the following sections:

- [Prime Infrastructure UI Components, page 30-1](#)
- [Common UI Tasks, page 30-5](#)
- [Dashboards and Dashlets, page 30-7](#)
- [Searching for Devices or SSIDs, page 30-8](#)
- [Monitoring Background Tasks, page 30-9](#)

Prime Infrastructure UI Components

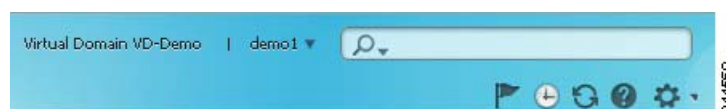
The following sections provide details on the Prime Infrastructure user interface components that are visible on most of the pages:

- [Global Toolbars](#)
- [Filters](#)
- [Data Entry Features](#)

Global Toolbars

Prime Infrastructure contains static global toolbars at the top-right of the page (see [Figure 30-1](#)):

Figure 30-1 *Global Toolbar—Top-right*



- **Virtual Domain name**—Indicates the virtual domain to which you are assigned.

- **Login name**—Indicates your current login name. Click the arrow to change your user preferences, change your password, or log out.
Click the downward arrow next to your login name to switch to a different Prime Infrastructure view:
 - Lifecycle view, which is organized according to home, design, deploy, operate, report and administer menus.
 - Classic view, which closely corresponds to the graphical user interface in Cisco Prime Network Control System 1.1 or Cisco Wireless Control System (WCS).
- **Search**—See [Searching for Devices or SSIDs](#) for more information.
- **Welcome**—Launches the Getting Started wizard that provides guidance for getting started setting up Prime Infrastructure.
- **Current Server Time**—Displays the current time on the Prime Infrastructure server.
- **Refresh**—Refreshes the current active page.
- **Help**—Launches Prime Infrastructure online help.
- **Settings**—Allows you to specify settings for the current active page. Click the down triangle to view available options. The triangle icon does not appear on pages for which you cannot change settings.

Prime Infrastructure contains the following static global toolbar at the bottom-right of the page (see [Figure 30-2](#)):

Figure 30-2 Global Toolbar—Bottom-right



- **Support Cases**—Launches the TAC Services Request where you can open a support request and gather critical information to be attached to the support case. See [Opening a Support Case](#) for more information.
- **Alarm Browser**—Launches the alarm browser within the active page (bottom half of the page).
- **Alarm Summary**—Launches the alarm summary window, displaying all alarms and also indicates the number critical, major, and minor alarms.

Filters

You can use the Filter feature to display specific information on the Prime Infrastructure interface. The Filter icon is provided wherever the data is displayed in a tabular format. The following types of filters are available:

- [Quick Filter](#)
- [Advanced Filter](#)

Quick Filter

This filter allows you to narrow down the data inside a table by applying a filter to a specific table column or columns. To apply different operators, use the Advanced Filter option.

To launch the quick filter, choose **Quick Filter** from the Filter drop-down menu.

To clear the Quick Filter, click the **Filter** button.

Advanced Filter

This filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. For example, you can choose the filter pattern by table column names and operator from the drop-down menu. In addition, you must enter filter criteria based on the data available in the Prime Infrastructure database.

To launch advance filtering, choose **Advanced Filter** from the Filter drop-down list.

Figure 30-3 *Advance Filter*



To save the filter criteria used in the Advance filter (see [Figure 30-3](#)):

1. Enter the advance filter criteria, then click **Go**.
The data is filtered based on the filter criteria.
2. Click the **Save** icon.
The Save Preset Filter window appears.
3. Enter a name for the preset filter and click **Save**.

Data Entry Features

In addition to the checkboxes, dropdown lists and data entry fields common in most user interfaces, Prime Infrastructure uses some specialized data-entry features. These are designed to keep your view of the network as uncluttered as possible, while still making it possible for you to add, update, and save your settings when needed. These specialized data-entry features include:

- [Anchored Fields](#)
- [Edit Tables](#)
- [Data Popups](#)

Anchored Fields

Anchored fields are recognizable by the plus sign {+} embedded in the field at the far right (see [Figure 30-4](#)).

Figure 30-4 *Anchored Field*



Clicking on the plus sign allows you to display an associated data popup (see [Data Popups](#)). You can use the data popup to view or update the settings you want. When you finished, you can “close” the anchored field by clicking the minus (-) sign displayed at the top of the data popup (see [Figure 30-5](#)).

Figure 30-5 Anchored Field with Popup

Encryption Policy

Select the transform sets that should be part of this encryption policy.

Transform sets

Show

<input type="checkbox"/>	Name*	ESP Encryption	ESP Integrity	AH Integrity	Compression	Mode
<input type="checkbox"/>	defaultPolicy	ESP-AES-256	ESP-SHA-HMAC	AH-SHA-HMAC	Disabled	transport

To use anchored fields:

1. Click the anchored field's plus (+) button.
2. With the associated data popup displayed, review or update data as needed.
3. When you are finished, click on the anchored field's minus (-) button.

Edit Tables

Prime Infrastructure uses tables to display many kind of data, including lists of sites, devices, and events. The data is arranged in rows and columns, much like a spreadsheet.

An edit table differs from other tables in that you can add, edit, or delete the data it contains (see [Figure 30-6](#)). Some edit tables also give you access to filters (see [Filters](#)). Edit tables are often displayed in data pop-ups triggered by checkboxes or anchored fields (see [Figure 30-5](#)).

Figure 30-6 Edit Table

☒ Cluster Support

<input checked="" type="checkbox"/>	Cluster ID	Max Connection	Next Hop Server
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

To use edit tables:

1. To add a new row in the edit table:
 - a. Click **Add Row**.
 - b. Complete the fields in the new row.
 - c. When you finished, click **Save**.
2. To delete one or more existing rows in an edit table:
 - d. Click on the row header checkbox (at the extreme left of each row) to select it.
 - e. Click **Delete**.
3. To update an entry in any field in any edit table row:
 - a. Click on the row header or the field itself.
 - b. Edit the contents.
 - c. When you are finished, click **Save**.

Data Popups

A data popup is a window associated with a checkbox, anchored field (see [Anchored Fields](#)), or other data-entry feature. They are displayed automatically when you select the feature, so you can view or update the data associated with that feature. In addition to normal checkboxes, dropdown lists and data-entry fields, data popups can contain edit tables (see [Edit Tables](#)).

To use a data popup:

1. Select the feature that triggers the data popup, such as an anchored field (see [Figure 30-4](#)) or a checkbox (see [Figure 30-6](#)).
2. With the associated popup displayed, view or update the fields as needed.
3. When you are finished, click anywhere outside the data popup. If you entered new information or changed existing information, your changes are saved automatically.

Common UI Tasks

You can perform the following actions from nearly any Prime Infrastructure screen:

- [Changing Your Password](#)
- [Changing Your Active Domain](#)
- [Monitoring Alarms](#)
- [Getting Device Details Using the 360° View](#)
- [Getting Help](#)

Changing Your Password

-
- | | |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Click the down arrow next to your username (at the top-right of the screen, to the left of the search box) and choose Change Password . |
| Step 2 | Click the information icon to review the password policy. |
| Step 3 | Enter a new password as directed. |
| Step 4 | Click Save . |
-

Changing Your Active Domain

-
- | | |
|---------------|--------------------------------------------------------------------------------------|
| Step 1 | Rest your cursor on the Virtual Domain and click the icon that appears to the right. |
| Step 2 | Choose a domain from the list of domains of which you are a member. |
-

Monitoring Alarms

At the bottom of the window, rest your cursor on Alarm Summary or Alarm Browser to get information on the latest active alarms.

Getting Device Details Using the 360° View

The 360° view provides detailed device information including device status, interface status, and associated device information. You can see the 360° view from nearly all screens in which device IP addresses are displayed.

To launch the 360° view of any device, rest your cursor on a device IP address, then click the icon that appears.



Note

The features that appear on the 360° view differ depending on the device type.

Table 30-1 **360° Features**

360° View Feature	Description
Device status	Indicates whether the device is reachable, is being managed, and is synchronized with the Prime Infrastructure database.
Tool icons	Click one of the following icons on top right of the device 360° view: <ul style="list-style-type: none"> Alarm Browser—Launches the Alarm Browser. See Monitoring Alarms for more information. Support Community—Launches the Cisco Support Community. See Launching Cisco Support Community for more information. Support Request—Allows you to open a support case. See Opening a Support Case for more information. Ping—Allows you to ping the device. Traceroute—Allows you to perform a traceroute on the device.
Modules tab	Lists the device modules and their name, type, state, and ports.
Alarms tab	Lists alarms on the device, including the alarm status, time stamp, and category.
Interfaces tab	Lists the device interfaces and the top three applications for each interface.
Neighbors	Lists the device neighbors, including their index, port, duplex status, and sysname.

Getting Help

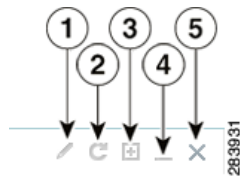
You can access online help by clicking the question mark icon at the top right of any Prime Infrastructure screen.

Dashboards and Dashlets

Dashboards display at-a-glance views of the most important data in your network. A quick scan of a dashboard should let you know if anything needs attention. Dashboards generally provide status and alerts, monitoring, and reporting information. Dashboards contain dashlets with visual displays such as tables and charts.

Dashboards contains dashlets with visual displays such as tables and charts. Rest your cursor on any dashlet, and the icons shown in [Figure 30-7](#) appear at the top-right corner of the dashlet.

Figure 30-7 **Dashlet Icons**



1	Click to change the dashlet title, refresh the dashlet, or change the dashlet refresh interval. (To disable refresh, uncheck Refresh Dashlet.)
2	Refresh the dashlet.
3	Maximize the dashlet. If you maximize the dashlet, a restore icon appears allowing you to restore the dashlet to its default size.
4	Collapse the dashlet so that only its title appears. If you collapse the dashlet, an expand icon appears.
5	Remove the dashlet.

See [Configuring Dashboards](#) for more information.

Configuring Dashboards

Dashboards contains dashlets with visual displays such as tables and charts. Click the Settings icon to change the dashboards.



Note

After upgrading, the arrangement of dashlets in the previous version is maintained. Therefore, dashlets or features added in a new release are not displayed. Click the Settings icon, then choose **Manage Dashboards** to display new dashlets.

Adding Dashboards

- Step 1** Click the **Settings** icon, then choose **Add New Dashboard**.
- Step 2** Enter a name for the new dashboard, then click **Add**.

- Step 3** Choose the new dashboard and add dashlets to it. See [Dashboards and Dashlets](#) for more information.
-

Restoring Default Dashboards

- Step 1** From the Home page, click the **Edit Dashboard** icon.
- Step 2** Click **Manage Dashboards**.
- Step 3** Choose a dashboard from the list.
- Step 4** Click **Reset**.
-

Searching for Devices or SSIDs

Prime Infrastructure provides the following methods for searching for devices or SSIDs:

- [Performing a Quick Search](#)
- [Performing an Advanced Search](#)

You can access the search options from any page within Prime Infrastructure.

Performing a Quick Search

For a quick search, enter a partial or complete IP address or name.



Note

You can also enter a username if you are searching for a client.

To quickly search for a device, follow these steps:

- Step 1** In the Search text box, enter the complete or partial IP address, device name, SSID, or MAC address of the device for which you are searching.
- Step 2** Click **Search** to display all devices that match the Quick Search parameter.
- The search results display the matching item type, the number of items that match your search parameter, and links to the list of matching results.
- Step 3** Click **View List** to view the matching devices from the Monitor or Configuration page.
-

Performing an Advanced Search

To perform a more specific search for a device in Prime Infrastructure, follow these steps:

- Step 1** Click **Advanced Search** from the search menu.
-

Step 2 In the New Search dialog box, choose a category from the Search Category drop-down list

Step 3 Choose all applicable filters or parameters for your search.



Note Search parameters change depending on the category you selected.

Step 4 To save this search, check the **Save Search** check box and enter a unique name for the search in the text box.

Step 5 Click **Go**.

Running a Saved Search



Note Saved searches apply only to the current partition.

To access and run a previously saved search, follow these steps:

Step 1 Click **Saved Search**.

Step 2 Choose a category from the Search Category drop-down list.

Step 3 Choose a saved search from the Saved Search List drop-down list.

Step 4 If necessary, change the current parameters for the saved search.

Step 5 Click **Go**.

Need to move the following section:

Monitoring Background Tasks

A background task is a scheduled program running in the background with no visible pages or other user interfaces. In Prime Infrastructure, background tasks can be anything from data collection to backing up configurations. You can monitor background tasks to see which background tasks are running, check their schedules, and find out whether the task was successfully completed.

Step 1 Choose **Tools > Task Manager > Background Tasks** to view scheduled tasks. The Background Tasks page appears.

Step 2 Choose a command from the drop-down list:

- **Execute Now**—Run all of the data sets with a checked check box.
- **Enable Tasks**—Enable the data set to run on its scheduled interval.
- **Disable Tasks**—Prevent the data set from running on its scheduled interval.



CHAPTER 31

Field Reference

This section provides reference information on Prime Infrastructure fields.

- [Configuration Templates Field Descriptions, page 31-1](#)
- [Designing Mobility Services Engine Field Description, page 31-68](#)
- [Wireless Operational Tools Field Descriptions, page 31-73](#)

Configuration Templates Field Descriptions

The following sections contain field descriptions for configuration templates:

- [Controller Templates Field Descriptions](#)
- [Security Templates Field Descriptions](#)
- [Wireless Configuration Templates Field Descriptions](#)
- [Switch Location Configuration Templates, page 31-80](#)

Controller Templates Field Descriptions

The following sections contain field descriptions for pages found in **Design > Configuration Templates > Features and Technologies > Controller**.

- [Controller > System > General Template](#)
- [Controller > System > Global CDP Configuration Template](#)
- [Controller > System > Dynamic Interface Template](#)
- [Controller > WLANs > WLAN Configuration Template](#)
- [Controller > FlexConnect > FlexConnect AP Groups Template](#)
- [Controller > Security > AAA > RADIUS Auth Servers Template](#)
- [Controller > Security > AAA > LDAP Servers Template](#)
- [Controller > Security > AAA > TACACS+ Servers Template](#)
- [Controller > Security > Local EAP > General - Local EAP Template](#)
- [Controller > Security > Local EAP > Local EAP Profiles Template](#)
- [Controller > Security > Local EAP > EAP-FAST Parameters Template](#)

- [Controller > Security > Wireless Protection Policies > Rogue Policies Template](#)
- [Controller > Security > IP Groups Template](#)
- [Controller > Security > Protocol Groups](#)
- [Controller > Security > 802.11 > Band Select](#)
- [Controller > Security > 802.11 > Media Stream](#)
- [Controller > Security > 802.11 > RF Profiles](#)
- [Controller > 802.11a or n > Parameters](#)
- [Controller > 802.11a or n > CleanAir](#)
- [Controller > 802.11a or n > Media Parameters](#)
- [Controller > 802.11a or n > Roaming Parameters](#)
- [Controller > 802.11a or n > dot11a-RRM > Thresholds](#)
- [Controller > 802.11a or n > dot11a-RRM > DCA](#)
- [Controller > 802.11b or g or n > Parameters](#)
- [Controller > 802.11b or g or n > Media Parameters](#)
- [Controller > 802.11b or g or n > Roaming Parameters](#)
- [Controller > 802.11b or g or n > CleanAir](#)
- [Controller > dot11b-RRM > Thresholds](#)
- [Controller > dot11b-RRM > TPC](#)
- [Controller > dot11b-RRM > DCA](#)
- [Controller > Management > Trap Control](#)
- [Controller > Management > Telnet SSH](#)
- [Controller > Location > Location Configuration](#)
- [Controller > PMIP > Global Config](#)

Controller > System > General Template

Table 31-1 describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > System > General** page.

Table 31-1 **Controller > System > General Template**

Field	Description
802.3x Flow Control Mode	Enable or disable flow control mode.
802.3 Bridging	Enable or disable 802.3 bridging. This 802.3 bridging option is not available for Cisco 5500 and Cisco 2106 series controllers.
Web Radius Authentication	choose the desired Web RADIUS authentication. You can choose to use PAP, CHAP, or MD5-CHAP for authentication between the controller and the client during the user credential exchange.
AP Primary Discovery Timeout	Specify the number of seconds for the AP Primary Discovery Timeout. The default is 120 seconds, and the valid range is 30 to 3600.

Table 31-1 **Controller > System > General Template (continued)**

Field	Description
Back-up Primary Controller IP Address	Specify the Back-up primary and secondary controller details.
Back-up Primary Controller Name	
Back-up Secondary Controller IP Address	
Back-up Secondary Controller Name	
CAPWAP Transport Mode	<p>Specify Layer 2 or Layer 3 transport mode. When set to Layer 3, the lightweight access point uses IP addresses to communicate with the access points; these IP addresses are collected from a mandatory DHCP server. When set to Layer 2, the lightweight access point uses proprietary code to communicate with the access points.</p> <p>Controllers through Version 5.2 use LWAPP and the new controller version uses CAPWAP.</p>
Broadcast Forwarding	Choose to enable or disable broadcast forwarding. The default is disabled.
LAG Mode	<p>Choose Enable or Disable from the LAG Mode drop-down list. Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG).</p> <p>If LAG is enabled on a controller, any dynamic interfaces that you have created are deleted to prevent configuration inconsistencies in the interface database. When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.</p> <p>Interfaces cannot be created with the Dynamic AP Manager flag set. Also, you cannot create more than one LAG on a controller.</p>
Peer to Peer Blocking MOde	Choose to enable or disable peer-to-peer blocking mode. If you choose Disable, any same-subnet clients communicate through the controller. If you choose Enable, any same-subnet clients communicate through a higher-level router.
Over-the-Air Provisioning AP Mode	From the Over Air AP Provision Mode drop-down list, choose enable or disable .
AP Fallback	<p>From the AP Fallback drop-down list, choose enable or disable. Enabling fallback causes an access point that lost a primary controller connection to automatically return to service when the primary controller returns.</p> <p>When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This might cause the controller to reach a saturation point and reject some of the access points. By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points can join the backup controller if the lower priority access points are disjoined. Choose enable from the AP Failover Priority drop-down list if you want to allow this capability.</p>
AP Failover Priority	
Apple Talk Bridging	<p>Choose to enable or disable AppleTalk bridging.</p> <p>This AppleTalk bridging option is not available on Cisco 5500 series controllers.</p>

Table 31-1 **Controller > System > General Template (continued)**

Field	Description
Fast SSID Change	<p>Choose to enable or disable the Fast SSID Change option. If the option is enabled, the client connects instantly to the controller between SSIDs without having much loss of connectivity. Normally, each client is connected to a particular WLAN identified by the SSID. If the client moves out of reach of the connected access point, the client has to reconnect to the controller using a different access point. This normal process consumes some time as the DHCP (Dynamic Host Configuration Protocol) server has to assign an IP address to the client.</p> <p>Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or operating system code upgrade. You might want to enable the controller as the master controller from the Master Controller Mode drop-down list.</p>
Master Controller Mode	Choose to enable or disable access to the controller management interface from wireless clients. Because of IPsec operation, management via wireless is only available to operators logging in across WPA or Static WEP.
Wireless Management	Wireless management is not available to clients attempting to log in via an IPsec WLAN.
Symmetric Tunneling Mode	<p>Choose to enable or disable symmetric tunneling mode. With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Forwarding (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled.</p> <p>All controllers in a mobility group must have the same symmetric tunneling mode.</p> <p>For symmetric tunneling to take effect, you must reboot.</p>
ACL Counters	Use the ACL Counters drop-down list to enable or disable ACL counters. The values per ACL rule can be viewed for each controller.
Default Mobility Domain Name	Enter the operator-defined RF mobility group name in the Default Mobility Domain Name text box.
Mobility Anchor Group Keep Alive Interval	<p>At the Mobility Anchor Group Keep Alive Interval, determine the delay between tries for clients attempting to join another access point. With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.</p> <p>When you hover your mouse cursor over the field, the valid range of values appear.</p>
Mobility ANchor Group Keep Alive Retries	At the Mobility Anchor Group Keep Alive Retries, specify the number of queries to anchor before the client declares it unreachable.
RF Network Name	Enter the RF network group name between 8 and 19 characters. Radio Resource Management (RRM) neighbor packets are distributed among access points within an RF network group. The Cisco access points only accept RRM neighbor packets sent with this RF network name. The RRM neighbor packets sent with different RF network names are dropped.

Table 31-1 **Controller > System > General Template (continued)**

Field	Description
User Idle Timeout	Specify the time out for idle clients. The factory default is 300 seconds. When the timeout expires, the client loses authentication, briefly disassociates from the access point, reassociates, and re-authenticates. Specify the timeout in seconds for the address resolution protocol. The factory default is 300 seconds.
ARP Timeout	Specify the timeout in seconds.
Global TCP Adjust MSS	Select the Global TCP Adjust MMS check box to start checking the TCP packets originating from the client, for the TCP SYN/ TCP ACK packets and MSS value and reset it to the configured value on the upstream and downstream side.
Disable local access	When this check box is selected, the AP will not broadcast local SSIDs or allow access to any of the Ethernet Ports.
Out of Box	Select this check box to create out-of-box RF profiles for both the radios along with out-of-box AP Group.
Web Auth Proxy Redirect Mode	Choose enable or disable Web Auth Proxy Redirect Mode if a manual proxy configuration is configured on the browser of the client; all web traffic going out from the client is destined for the PROXY IP and PORT configured on the browser.
Web Auth Proxy Redirect Port	Enter the Web Auth Proxy Redirect Port. The default ports are 8080 and 3128. The range is 0 to 65535.
AP Retransmit Count	Enter the AP Retransmit Count and Intervals. The AP Retransmit Count default value is 5 and the range is from 3 to 8. The AP Retransmit Interval default value is 3. The range is 2 to 5.
AP Retransmit Interval	

Controller > System > Global CDP Configuration Template

Table 31-2 describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > System > Global CDP Configuration** page.

Table 31-2 **Controller > System > Global CDP Configuration Template**

Field	Description
CDP on controller	Choose enable or disable CDP on the controller. This configuration cannot be applied on WiSM2 controllers.
Global CDP on APs	Choose to enable or disable CDP on the access points.
Refresh Interval	Enter the time in seconds at which CDP messages are generated. The default is 60.
Hold Time	Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
CDP Advertisement Version	Enter which version of the CDP protocol to use. The default is v1.
Ethernet Interface Slot	Select the slots of Ethernet interfaces for which you want to enable CDP. CDP for Ethernet Interfaces fields are supported for Controller Version 7.0.110.2 and later.
Radio Interface Slot	Select the slots of Radio interfaces for which you want to enable CDP. CDP for Radio Interfaces fields are supported for Controller Version 7.0.110.2 and later.

Controller > System > Dynamic Interface Template

Table 31-3 describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > System > Dynamic Interface** page.

Table 31-3 **Controller > System > Dynamic Interface**

Field	Description
Guest LAN	Select to mark the interface as wired.
Quarantine	Enable/disable to quarantine a VLAN. Select the check box to enable.
Netmask	Enter the net mask address of the interface.
LAG Mode	Select this check box to enable or disable LAG Mod. If LAG mode is selected with this interface, then the settings can be applied only to the LAG-enabled controllers.
Primary Port Number	Enter the port currently used by the interface.
Secondary Port Number	Enter a secondary port to be used by the interface when the primary port is down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN controller transfers the interfaces back to the primary port. Primary and secondary port numbers are present only in the Cisco 4400 Series Wireless LAN controllers.
AP Management	Select this check box to enable access point management.
Primary DHCP Server	Enter the IP addresses of the primary DHCP servers.
Secondary DHCP Server	Enter the IP addresses of the secondary DHCP servers.
ACL Name	Choose a name from the list of defined names. From the Add Format Type drop-down list in the Add Interface Format Type group box, choose either Device Info or File . If you choose device info, you must configure the device-specific fields for each controller. If you choose File, you must configure CSV device-specific fields (Interface Name, VLAN Identifier, Quarantine VLAN Identifier, IP Address, and Gateway) for all the managed controllers specified in the CSV file (see Table 31-4). If you choose Device Info, continue to Step 12.

The sample CSV files are as follows.

Table 31-4 **Sample CSV Files**

ip_address	interface_name	vlan_id	quarantine_vlan_id	interface_ip_address	gateway
209.165.200.224	dyn-1	1	2	209.165.200.228	209.165.200.229
209.165.200.225	interface-1	4	2	209.165.200.230	209.165.200.231
209.165.200.226	interface-2	5	3	209.165.200.232	209.165.200.233
209.165.200.227	dyna-2	2	3	209.165.200.234	209.165.200.235

The first row of the CSV file is used to describe the columns included. The CSV files can contain the following fields:

- ip_address
- interface_name

- vlan_id
- quarantine_vlan_id
- interface_ip_address
- gateway

If you choose Apply to Controllers, you advance to the Apply To page where you can configure device-specific fields for each controller.

Use the **Add** and **Remove** options to configure device specific fields for each controllers. If you click **Edit**, a dialog box appears with the current parameter input.

Make the necessary changes in the dialog box, then click **OK**.

**Note**

If you change the interface fields, the WLANs are temporarily disabled, therefore you might lose connectivity for some clients. Any changes to the interface fields are saved only after you successfully apply them to the controller(s).

**Note**

If you remove an interface here, it is removed only from this template and not from the controllers.

Controller > WLANs > WLAN Configuration Template

The following tables describe the fields on the **Design > Configuration Templates > Features and Technologies > Controller > WLANs > WLAN Configuration** page:

- [Table 31-5](#)—General tab
- [Table 31-6](#)—Security tab
- [Table 31-7](#)—QoS tab
- [Table 31-8](#)—Advanced tab
- [Table 31-9](#)—Hot Spot tab

Controller > WLANs > WLAN Configuration > General

[Table 31-5](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > WLANs > WLAN Configuration > General** tab.

Table 31-5 **Controller > WLANs > WLAN Configuration > General**

Field	Description
Wired Lan	<p>Check the box to indicate whether or not this WLAN is a wired LAN.</p> <p>Note Specify if you want guest users to have wired guest access from an Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room and accounts are added to the network using the Lobby Ambassador portal. (The Egress or Ingress interface configurations are applicable for Wired LAN only.)</p> <p>Use the Type drop-down list to select the type of the wired LAN.</p> <ul style="list-style-type: none"> • Guest LAN—Indicates that this wired LAN is a Guest LAN. If you select the Guest LAN option, you need to select an Ingress interface which has not already been assigned to any Guest LAN. • Remote LAN—Indicates that this wired LAN is a Remote LAN.
Profile Name	Enter a name in the Profile Name text box that identifies the WLAN or the guest LAN. Do not use any spaces in the name entered.
SSID	<p>Enter the name of the WLAN SSID. An SSID is not required for a guest LAN.</p> <p>WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes.</p>
Status	Select the Enable check box for the Status field.
Security Policies	Modifications you make in the Security tab appear after you save the template.
Radio Policy	Set the WLAN policy to apply to All (802.11a/b/g/n), 802.11a only, 802.11g only, 802.11b/g only, or 802.11a/g only.
Interface/Interface Group	Choose the available names of interfaces created by the Controller > Interfaces module.
Multicast VLAN	<p>Select the Enable check box to enable the multicast VLAN feature.</p> <p>From the Multicast VLAN Interface drop-down list, choose the appropriate interface name. This list is automatically populated when you enable the multicast VLAN feature</p>
Broadcast SSID	Click to activate SSID broadcasts for this WLAN.

Related Topics

- [Table 31-6](#)—Security tab
- [Table 31-7](#)—QoS tab
- [Table 31-8](#)—Advanced tab
- [Table 31-9](#)—Hot Spot tab

Controller > WLANs > WLAN Configuration > Security

[Table 31-6](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > WLANs > WLAN Configuration > Security** tab.

Table 31-6 **Controller > WLANs > WLAN Configuration > Security**

Field	Description
Layer 2	
None	<p>No Layer 2 security selected.</p> <ul style="list-style-type: none"> FT Enable—Select the check box to enable Fast Transition (FT) between access points. <p>Note Fast transition is not supported with FlexConnect mode.</p> <p>Over the DS—Select the check box to enable or disable the fast transition over a distributed system.</p> <p>Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100.</p> <p>To enable Over the DS or Reassociation Timeout, you should enable fast transition.</p>
802.1X	<p>WEP 802.1X data encryption type:</p> <ul style="list-style-type: none"> 40/64 bit key 104 bit key 152 bit key
Static WEP	<p>Static WEP encryption fields:</p> <ul style="list-style-type: none"> Key sizes: Not set, 40/64, 104, and 152 bit key sizes. Key Index: 1 to 4 (Note 2). Encryption Key: Encryption key required. Key Format: ASCII or HEX. Allowed Shared Key Authentication—Select the check box to enable shared key authentication. <p>Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.</p>
Static WEP-802.1X	<p>Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X fields are displayed at the bottom of the page.</p> <p>Static WEP encryption fields:</p> <ul style="list-style-type: none"> Key sizes: Not set, 40/64, 104, and 152 bit key sizes. Key index: 1 to 4 (Note 2). Encryption Key: Enter encryption key. Key Format: ASCII or HEX. Allowed Shared Key Authentication—Select the check box to enable. 802.1 Data Encryption: 40/64 bit key, 104 bit key, 152 bit key.

Table 31-6 **Controller > WLANs > WLAN Configuration > Security (continued)**

Field	Description
CKIP	<p>Cisco Key Integrity Protocol (CKIP). A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WLAN.</p> <p>Note CKIP is not supported on 10xx APs.</p> <p>When selected, these CKIP fields are displayed.</p> <ul style="list-style-type: none"> Key size: Not set, 40, or 104. Key Index: 1 to 4 Encryption Key: Specify encryption key. Key Format: ASCII or HEX. <p>Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.</p> <p>MMH Mode—Select the check box to enable.</p> <p>Key Permutation—Select the check box to enable</p>
MAC Filtering	<p>Check to filter clients by MAC address.</p> <p>Note The ability to join a controller without specification within a MAC filter list is only supported on mesh access points.</p> <p>Note For releases prior to 4.1.82.0, mesh access points do not join the controller unless they are defined in the MAC filter list.</p> <p>You might want to disable the MAC filter list to allow newly added access points to join the controller. Before enabling the MAC filter list again, you should enter the MAC addresses of the new access points.</p>
Authentication Key Management	<p>Choose the desired type of authentication key management. The choices are 802.1X, CCKM, or PSK.</p> <p>Note If you choose PSK, you must enter the shared key and type (ASCII or hexadecimal).</p> <p>Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.</p>
Layer 3	
Layer 3 Security	<p>Choose between None and VPN Pass Through.</p> <p>Note The VPN passthrough option is not available for the 2106 or 5500 series controllers.</p>

Table 31-6 **Controller > WLANs > WLAN Configuration > Security (continued)**

Field	Description
Web Policy	<p>You can modify the default static WEP (web authentication) or assign specific web authentication (login, logout, login failure) pages and the server source.</p> <ol style="list-style-type: none"> 1. To change the static WEP to passthrough, select the Web Policy check box and choose the Passthrough option from the drop-down list. This option allows users to access the network without entering a username or password. <p>An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.</p> <ol style="list-style-type: none"> 2. Choose the WebAuth on MAC Filter Failure option so that when clients fail on MAC filter, they are automatically switched to webAuth. <p>Note The WebAuth on Mac Filter Failure option works only when the Layer 2 Mac Filtering option is enabled.</p> <ol style="list-style-type: none"> 3. To specify custom web authentication pages, unselect the Global WebAuth Configuration Enable check box. <p>When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:</p> <p>Default Internal—Displays the default web login page for the controller. This is the default value.</p> <p>Customized Web Auth—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose None from the appropriate drop-down list if you do not want to display a customized page for that option.</p> <p>These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.</p> <p>External—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.</p> <p>Note External web auth is not supported for 2106 and 5500 series controllers.</p> <p>You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA page. To do so, continue with Step 4.</p> <p>Note The RADIUS and LDAP servers must be already configured to have selectable options in the Security > AAA page. You can configure these servers in the RADIUS Authentication Servers page and TACACS+ Authentication Servers page.</p> <p>If you selected External as the Web Authentication Type in Step 2, choose Security > AAA, and choose up to three RADIUS and LDAP servers using the drop-down lists.</p> <p>Repeat this process if a second (anchor) controller is being used in the network.</p>

Table 31-6 **Controller > WLANs > WLAN Configuration > Security (continued)**

Field	Description
AAA Server	
Radius Server Overwrite	<p>Check to send the client authentication request through the dynamic interface which is set on the WLAN. When you enable the Radius Server Overwrite Interface option, the WLC sources all radius traffic for a WLAN using the dynamic interface configured on that WLAN.</p> <p>Note You cannot enable Radius Server Overwrite Interface when Diagnostic Channel is enabled.</p> <p>Note The Radius Server Overwrite Interface option is supported in controller Version 7.0.x and later.</p> <p>Select the Enable check boxes, then use the drop-down lists in the RADIUS and LDAP servers section to choose authentication and accounting servers. This selects the default RADIUS server for the specified WLAN and overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority, and so on.</p> <p>If no LDAP servers are chosen here, Prime Infrastructure uses the default LDAP server order from the database.</p>
Interim Update	<p>Select to enable interim update for RADIUS Server Accounting. If you have selected this check box, specify the Interim Interval value. The range is 180 to 3600 seconds, and the default value is 0.</p> <p>Note The Interim Interval can be entered only when Interim Update is enabled.</p>
Local EAP Authentication	<p>Select the Local EAP Authentication check box if you have an EAP profile already configured that you want to enable. Local EAP is an authentication method that allows users and wireless clients to locally authenticate. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.</p>
Allow AAA Override	<p>When you enable AAA Override, and a client has conflicting AAA and controller WLAN authentication fields, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system also uses QoS and ACL provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as identity networking.)</p> <p>For instance, if the corporate WLAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.</p> <p>When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters.</p> <p>The AAA override values might come from a RADIUS server, for example.</p>

Related Topics

- [Table 31-5](#)—General tab
- [Table 31-7](#)—QoS tab
- [Table 31-8](#)—Advanced tab
- [Table 31-9](#)—Hot Spot tab

Controller > WLANs > WLAN Configuration > QoS

Table 31-7 describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > WLANs > WLAN Configuration > QoS** tab.

Table 31-7 **Controller > WLANs > WLAN Configuration > QoS**

Field	Description
Quality of Service (QoS)	Choose Platinum (voice), Gold (video), Silver (best effort), or Bronze (background). Services such as VoIP should be set to gold while non-discriminating services such as text messaging can be set to bronze.
Override Per-User Rate Limits	Data rates on a per-user basis
Average Data Rate	Define the average data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
Burst Data Rate	Define the peak data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
Average Real-Time Rate	Define the average real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
Burst Real-Time Rate	Define the peak real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
Override Per-SSID Rate Limits	Data rates on a per SSID basis
Average Data Rate	Define the average data rate TCP traffic per user or per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
Burst Data Rate	Define the peak data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic in the WLANs.
Average Real-Time Rate	Define the average real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
Burst Real-Time Rate	Define the peak real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic in the WLANs.
WMM Policy	Choose Disabled , Allowed (so clients can communicate with the WLAN), or Required to make it mandatory for clients to have WMM enabled for communication.
7920 AP CAC	Select to enable support on Cisco 7920 phones. If you want WLAN to support older versions of the software on 7920 phones, select the 7920 Client CAC check box to enable it. The CAC limit is set on the access point for newer versions of software.

Related Topics

- [Table 31-5](#)—General tab
- [Table 31-6](#)—Security tab
- [Table 31-8](#)—Advanced tab
- [Table 31-9](#)—Hot Spot tab

Controller > WLANs > WLAN Configuration > Advanced

[Table 31-5](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > WLANs > WLAN Configuration > Advanced** tab.

Table 31-8 *Controller > WLANs > WLAN Configuration > Advanced*

Field	Description
FlexConnect Local Switching	Click to enable FlexConnect local switching. If you enable FlexConnect local switching, the FlexConnect access point handles client authentication and switches client data packets locally. FlexConnect local switching is only applicable to the Cisco 1130/1240/1250 series access points. It is not supported with L2TP or PPTP authentications, and it is not applicable to WLAN IDs 9-16.
FlexConnect Local Auth	Select to enable FlexConnect local authentication. Local authentication is useful where you cannot maintain the criteria a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Thus local authentication reduces the latency requirements of the branch office. Note Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode. Local authentication is not supported in the following scenarios: <ul style="list-style-type: none"> • Guest Authentication cannot be performed on a FlexConnect local authentication enabled WLAN. • RRM information is not available at the controller for the FlexConnect local authentication enabled WLAN. • Local radius is not supported. • Once the client has been authenticated, roaming is supported after the WLC and the other FlexConnects in the group are updated with the client information.
Learn Client IP Address	When you enable hybrid-REAP local switching, the Learn Client IP Address check box is enabled by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.
Diagnostic Channel	Choose to enable the diagnostic channel feature or leave it disabled. The diagnostic channel feature allows you to troubleshoot problems regarding client communication with a WLAN. When initiated by a client having difficulties, the diagnostic channel provides the most robust communication methods with the fewest obstacles to communication.

Table 31-8 **Controller > WLANs > WLAN Configuration > Advanced (continued)**

Field	Description
Aironet IE	Select to enable support for Aironet information elements (IEs) for this WLAN. If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.
IPv6	Select the IPv6 check box. You can configure IPv6 bridging and IPv4 web auth on the same WLAN.
Session Timeout	Check to set the maximum time a client session can continue before requiring reauthorization.
Coverage Hole Detection	Choose to enable or disable coverage hold detection (CHD) on this WLAN. By default, CHD is enabled on all WLANs on the controller. If you disable CHD on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where highly mobile guests are connected to your network for short periods of time.
Override Interface ACL	The Override Interface drop-down lists provides a list of defined access control lists (ACLs). Upon choosing an ACL from the list, the WLAN associates the ACL to the WLAN. Selecting an ACL is optional, and the default for this field is None
Peer to Peer Blocking	<p>You can configure peer-to-peer blocking per WLAN rather than applying the status to all WLANs. From the Peer to Peer Blocking drop-down list, choose one of the following:</p> <ul style="list-style-type: none"> • Disable—Peer-to-peer blocking is disabled, and traffic is bridged locally whenever possible. • Drop—The packet is discarded. • Forward Up Stream—The packet is forwarded on the upstream VLAN, and the decision is made about what to do with the packet. <p>Note For locally switched clients, the Forward Up Stream is same as Drop from 7.2.x version of controllers.</p> <p>If FlexConnect local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down list is dimmed.</p> <p>Note Peer-to-peer blocking does not apply to multicast traffic.</p>
Wi-Fi Direct Clients Policy	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Disabled—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct capable clients. The default is Disabled. • Allow—Allows the Wi-Fi Direct clients to associate with an infrastructure WLAN. • Not-Allow—Disallows the Wi-Fi Direct clients from associating with an infrastructure WLAN. <p>Note Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.</p> <p>Note The Wi-Fi Direct Clients Policy is applicable for controller Version 7.2.x. and later.</p>
Client Exclusion	<p>Select the check box if you want to enable automatic client exclusion. If you enable client exclusion, you must also set the Timeout Value in seconds for disabled client machines. Client machines are excluded by MAC address, and their status can be observed. A timeout setting of 0 indicates that administrative control is required to reenable the client.</p> <p>Note When session timeout is not set, it implies that an excluded client remains and does not timeout from the excluded state. It does not imply that the exclusion feature is disabled.</p>

Table 31-8 Controller > WLANs > WLAN Configuration > Advanced (continued)

Field	Description
Passive Client	<p>Enter the maximum number of clients to be associated in a WLAN in the Maximum Clients text box. The valid range is from 0 to 7000. The default value is 0.</p> <p>Note A value of 0 allows unlimited number of clients to be associated with a WLAN.</p>
Static IP Tunneling	Enable dynamic anchoring of static IP clients by selecting the Static IP Tunneling check box.
Media Session Snooping	<p>This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and Prime Infrastructure. It can be enabled or disabled per WLAN.</p> <p>When media session snooping is enabled, the access point radios that advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.</p>
KTS based CAC	<p>Select the KTS based CAC check box to enable KTS based CAC support per WLAN.</p> <p>WLC supports TSPEC based CAC and SIP based CAC. But there are certain phones that work with different protocols for CAC, which are based on the KTS (Key Telephone System). For supporting CAC with KTS-based SIP clients, WLC should understand and process the bandwidth request message from those clients to allocate the required bandwidth on the AP radio, in addition to handling and sending certain other messages, as part of this protocol.</p> <p>Note The KTS CAC configuration is only supported by Cisco 5508, 7500, WISM2, and 2500 controllers that run controller software Release 7.2.x. This feature is not supported by Cisco 4400 series controllers.</p>
NAC State	Choose SNMP NAC or Radius NAC . SIP errors that are discovered generate traps that appear on the client troubleshooting and alarms screens. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.
Scan Defer Priority	<p>Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitor access points, or other access points in the same location that do not have this WLAN assigned.</p> <p>Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:</p> <ul style="list-style-type: none"> • Bronze marks all downlink traffic to UP= 1. • Silver marks all downlink traffic to UP= 0. • Gold marks all downlink traffic to UP=4. • Platinum marks all downlink traffic to UP=6. <p>Set the Scan Defer Priority by clicking the priority argument and Set the time in milliseconds in the Scan Defer Interval text box. Valid values are 0 through 60000. The default value is 100 milliseconds.</p>

Table 31-8 Controller > WLANs > WLAN Configuration > Advanced (continued)

Field	Description
DTIM Period	<p>In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.</p> <p>Normally, the DTIM value is set to 1 (transmit broadcast and multicast frames after every beacon) or 2 (transmit after every other beacon). For instance, if the beacon period of the 802.11a/n or 802.11b/g/n network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings might be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.</p> <p>However, the DTIM value can be set as high as 255 (transmit broadcast and multicast frames after every 255th beacon) if all 802.11a/n or 802.11b/g/n clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the beacon period is 100 ms and the DTIM value is set to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.</p> <p>Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. We recommend a low DTIM value for 802.11a/n and 802.11b/g/n networks that support such clients.</p> <p>Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n fields. The default value is 1 (transmit broadcast and multicast frames after every beacon).</p>
DHCP Server	<p>Select the check box to override DHCP server,. Another field appears where you can enter the IP address of your DHCP server. For some WLAN configurations, this is required. Three valid configurations are as follows:</p> <ul style="list-style-type: none"> • DHCP Required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server. • DHCP is not required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server or use a static IP address. • DHCP not required and DHCP server IP address 0.0.0.0 - All WLAN clients are forced to use a static IP address. All DHCP requests are dropped. <p>You cannot choose to require a DHCP address assignment and then enter a DHCP server IP address.</p>
MFP Signature Generation	<p>Select to enable signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. Signature generation makes sure that changes to the transmitted management frames by an intruder are detected and reported.</p>
MFP Client Protection	<p>Choose Enabled, Disabled, or Required for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down list is unavailable.</p> <p>Note The Enabled parameter is the same as the Optional parameter that you choose from the MFP Client Protection drop-down list in the WLC graphical user interface.</p> <p>Note Client-side MFP is only available for those WLANs configured to support Cisco Compatible Extensions (version 5 or later) clients, and WPA2 must first be configured.</p>

Table 31-8 **Controller > WLANs > WLAN Configuration > Advanced (continued)**

Field	Description
DTIM Period	Enter a value between 1 and 255 beacon intervals in the 802.11a/n DTIM Period group box of the page. The controller sends a DTIM packet on the 802.11a/n radio for this WLAN based on what is entered as an interval. Note The DTIM configuration is not appropriate for guest LANs.
Client Profiling	Select to enable or disable profiling of all the clients that are associated with the WLAN. Note Client Profiling is not supported with FlexConnect local authentication. Note Client Profiling is configurable only when you select the DHCP Address Assignment check box.
PMIP Mobility	Choose the mobility type from the following options: <ul style="list-style-type: none"> • None—Configures the WLAN with Simple IP. • Mixed—Configures the WLAN with Simple IP and PMIPv6. • PMIPv6—Configures the WLAN with only PMIPv6.

Related Topics

- [Table 31-5](#)—General tab
- [Table 31-6](#)—Security tab
- [Table 31-7](#)—QoS tab
- [Table 31-9](#)—Hot Spot tab

Controller > WLANs > WLAN Configuration > Hot Spot

[Table 31-5](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > WLANs > WLAN Configuration > Hot Spot** tab.

Table 31-9 **Controller > WLANs > WLAN Configuration > Hot Spot**

Field	Description
General	
802.11u Status	Select to enable 802.11u on the WLAN. <ul style="list-style-type: none"> • From the drop-down list, In the HESSID field, enter the Homogenous Extended Service Set Identifier value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.
Internet Access	Select to enable this WLAN to provide Internet services.

Table 31-9 **Controller > WLANs > WLAN Configuration > Hot Spot (continued)**

Field	Description
Network Type	<p>Choose one of the following network types that best describes the 802.11u you want to configure on this WLAN:</p> <ul style="list-style-type: none"> • Private Network • Private Network with Guest Access • Chargeable Public Network • Free Public Network • Emergency Services Only Network • Personal Device Network • Test or Experimental • Wildcard
Network Auth Type	<p>Choose the authentication type that you want to configure for the 802.11u parameters on this network:</p> <ul style="list-style-type: none"> • Not configured • Acceptance of Terms and Conditions • Online Enrollment • HTTP/HTTPS Redirection
OUI List	<p>Enter the following details:</p> <ul style="list-style-type: none"> • OUI name • Is Beacon • OUI Index <p>Click Add to add the OUI (Organizationally Unique Identifier) entry to this WLAN.</p> <ul style="list-style-type: none"> • In the group box,
Domain List	<p>Enter the following details:</p> <ul style="list-style-type: none"> • Domain Name—The domain name operating in the 802.11 access network. • Domain Index—Select the domain index from the drop-down list. <p>Click Add to add the domain entry to this WLAN.</p>
OUI List	<p>Enter the following details:</p> <ul style="list-style-type: none"> • Realm Name—The realm name. • Realm Index—The realm index. <p>Click Add to add the domain entry to this WLAN.</p>
MSAP	Click to enable service advertisements.

Table 31-9 **Controller > WLANs > WLAN Configuration > Hot Spot (continued)**

Field	Description
Server Index	<p>If you enabled MSAP, you must provide a server index. Enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.</p> <p>Note MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers. Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.</p>
HotSpot2 Enable	Choose to enable HotSpot2.
WAN Link Status	Select the link status.
WAN SIM Link Status	The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
Down Link Speed	The downlink speed. The maximum value is 4,194,304 kbps.
Up Link Speed	The uplink speed. The maximum value is 4,194,304 kbps.
Operator Name List	<p>Specify the following:</p> <ul style="list-style-type: none"> Operator Name—Specify the name of the 802.11 operator. Operator Index—Select an operator index. The range is from 1 to 32. Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code. <p>Click Add to add the operator details.</p>
Port Config List	<p>Specify the following:</p> <ul style="list-style-type: none"> IP Protocol—The IP protocol that you want to enable. The following options are ESP, FTP, ICMP, and IKEV2. Port No—The port number that is enabled on this WLAN. Status—The status of the port.

Related Topics

- [Table 31-5](#)—General tab
- [Table 31-6](#)—Security tab
- [Table 31-7](#)—QoS tab
- [Table 31-8](#)—Advanced tab

Controller > FlexConnect > FlexConnect AP Groups Template

[Table 31-1](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > FlexConnect > FlexConnect AP Groups** page.

Table 31-10 **Controller > FlexConnect > FlexConnect AP Groups**

Field	Description
General	
Primary RADIUS	Choose the primary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, Prime Infrastructure configured RADIUS server does not apply. A value of 10 indicates that the primary RADIUS server is not configured for this group.
Secondary RADIUS	Note Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, Prime Infrastructure configured RADIUS server does not apply. A value of 0 indicates that the primary RADIUS server is not configured for this group.
FlexConnect AP	An access point Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. If more than one group is applied to the same controller, select the Ethernet MAC check box to unselect an access point from one of the groups. You should save this change or apply it to controllers. Click Add AP . The FlexConnect AP Group page appears.
FlexConnect Configuration	Click the FlexConnect Configuration tab to enable local authentication for a FlexConnect group. Note Make sure that the Primary RADIUS Server and Secondary RADIUS Server fields are set to None on the General tab.
FlexConnect Local Authentication	Click to enable local authentication for this FlexConnect group. The default value is unselected. Note When you attempt to use this feature, a warning message indicates that it is a licensed feature. Note You can click the Users configured in the group link that appears at the bottom of the page to view the list of FlexConnect users. You can create FlexConnect users only after you save the FlexConnect AP Group.
EAP Type	To allow a FlexConnect access point to authenticate clients using LEAP, select the LEAP check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select the EAP-FAST check box. To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key and Confirm EAP-FAST Key text boxes.
Auto Key Generation	To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the Auto Key Generation check box
EAP-FAST Key	Enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
EAP-FAST Authority ID	Enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.
EAP-FAST Authority Info	Enter the authority information of the EAP-FAST server.
EAP-FAST Pac Timeout	Specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.
Image Upgrade	
FlexConnect AP Upgrade	Check to upgrade the FlexConnect access points.

Table 31-10 **Controller > FlexConnect > FlexConnect AP Groups**

Field	Description
Slave Maximum Retry Count	Enter the maximum retries for the slave to undertake to start the download from the master in the FlexConnect group. This option is available only if you select the FlexConnect AP Upgrade check box. Note You are allowed to add an access point as a master access point only if FlexConnect AP Upgrade check box is enabled on the General tab.
VLAN-ACL Mapping	Use the edit table on this tab to add VLAN-ACL mappings.
VLAN ID	Enter a VLAN ID. The valid VLAN ID range is 1—4094.
Ingress ACL	Choose an Ingress ACL.
Egress ACL	Choose an Egress ACL.
WLAN-ACL Mapping	Use the edit table on this tab to add WLAN-ACL mappings.
WLAN ID	WLAN ID.
WLAN Profile Name	Choose a WLAN profile.
Web-Auth ACL	Choose a WebAuth ACL.
Web Policies	Use the edit table on this tab to add or select Web Policy ACLs.
Web-Policy ACL	Choose a WebPolicy ACL. You can add up to a maximum of 16 Web-Policy ACLs.
Local Split	Use the edit table on this tab to add or select Local-Split ACLs
WLAN Profile Name	Choose a WLAN Profile Name from the list.
Local-Split ACL	Choose a Local-Split ACL.
Central DHCP	Use the edit table on this tab to add or select Central DHCP for each WLAN Profile.
WLAN Profile Name	Choose a WLAN Profile Name from the list.
Central DHCP	Choose Enable to enable central DHCP for this profile.
Override DNS	Choose Enable to enable DNS override for this profile.
NAT-PAT	Choose Enable to enable network address and port address translation for this profile.

Controller > Security > AAA > RADIUS Auth Servers Template

Table 31-11 describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > Security > AAA > RADIUS Auth Servers** page.

Table 31-11 **Controller > Security > AAA > RADIUS Auth Servers**

Field	Description
Server Address	Enter the server address.
Port Number	Enter the port address.
Shared Secret Format	Choose either ASCII or hex . Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.
Shared Secret	Enter the RADIUS shared secret used by your specified server.

Table 31-11 **Controller > Security > AAA > RADIUS Auth Servers (continued)**

Field	Description
Confirm Shared Secret	Reenter the RADIUS shared secret used by your specified server.
Key WRAP	<p>Select the check box if you want to enable key wrap. If this check box is enabled, the authentication request is sent to RADIUS servers that have following key encryption key (KEK) and message authenticator code keys (MACK) configured. When enabled, the following fields appear:</p> <ul style="list-style-type: none"> Shared Secret Format: Enter ASCII or hexadecimal. <p>Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in the event a discovered template is applied to another device.</p> <ul style="list-style-type: none"> KEK Shared Secret: Enter the KEK shared secret. MACK Shared Secret: Enter the MACK shared secret. <p>Note Each time the controller is notified with the shared secret, the existing shared secret is overwritten with the new shared secret.</p>
Admin Status	Click if you want to enable administration privileges.
Support for RFC 3576	Click if you want to enable support for RFC 3576. RFC 3576 is an extension to the Remote Authentication Dial In User Service (RADIUS) protocol. It allows dynamic changes to a user session and includes support for disconnecting users and changing authorizations applicable to a user session. With these authorizations, support is provided for Disconnect and Change-of-Authorization (CoA) messages. Disconnect messages immediately terminate a user session, whereas CoA messages modify session authorization attributes such as data filters.
Network User	Click if you want to enable network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
Management User	Click if you want to enable management authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the management user.
Retransmit Timeout	Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller. You can specify a value between 2 and 30 seconds.
IPSec	If you click to enable the IP security mechanism, additional IP security fields are added to the page, and Steps 13 to 19 are required. If you enable IPSec, complete the following fields.
IPsec Authentication	<p>Choose which IP security authentication protocol to use. The options are HMAC-SHA1, HMAC-MD5, and None.</p> <p>Message Authentication Codes (MAC) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions and can be used in combination with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA1 are two constructs of the HMAC using the MD5 hash function and the SHA1 hash function. HMAC also uses a secret key for calculation and verification of the message authentication values</p>

Table 31-11 **Controller > Security > AAA > RADIUS Auth Servers (continued)**

Field	Description
IPsec Encryption	<p>Select the IP security encryption mechanism to use:</p> <ul style="list-style-type: none"> • DES—Data Encryption Standard is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data. • Triple DES—Data Encryption Standard that applies three keys in succession. • AES 128 CBC—Advanced Encryption Standard uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Block Chaining (CBC) mode. • None—No IP security encryption mechanism.
IKE Authentication	The Internet Key Exchange (IKE) authentication is not an editable text box. Internet Key Exchange protocol (IKE) is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how data should be protected. IKE keeps track of connections by assigning a bundle of security associations (SAs) to each connection
IKE Phase 1	Choose either aggressive or main. This sets the IKE protocol. IKE phase 1 is used to negotiate how IKE is protected. Aggressive mode passes more information in fewer packets, with the benefit of a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear
Lifetime	Set the timeout interval (in seconds) when the session expires
IKE Diffie Hellman Group	<p>Set the IKE Diffie Hellman group. The options are group 1 (768 bits), group 2 (1024 bits), or group 5 (1536 bits). Diffie-Hellman techniques are used by two devices to generate a symmetric key where you can publicly exchange values and generate the same symmetric key.</p> <p>Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size</p>

Controller > Security > AAA > LDAP Servers Template

Table 31-12 describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > Security > AAA > LDAP Servers** page.

Table 31-12 **Controller > Security > AAA > LDAP Servers**

Field	Description
Server Address	Enter the IP address of the server.
Port Number	Port number of the controller to which the access point is connected.
Bind Type	Choose Authenticated or Anonymous . If you choose Authenticated, you must enter a bind username and password as well. A bind is a socket opening that performs a lookup. Anonymous bind requests are rejected.
Server User Base DN	Enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.
Server User Attribute	Enter the attribute that contains the username in the LDAP server.
Server User Type	Enter the ObjectType attribute that identifies the user.

Table 31-12 **Controller > Security > AAA > LDAP Servers (continued)**

Field	Description
Retransmit Timeout	Enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.
Admin Status	Check if you want the LDAP server to have administrative privileges.

Controller > Security > AAA > TACACS+ Servers Template

Table 31-13 describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > Security > AAA > TACACS+ Servers** page.

Table 31-13 **Controller > Security > AAA > TACACS+ Servers**

Field	Description
Server Type	Select one or more server types by selecting their respective check boxes. The following server types are available: <ul style="list-style-type: none"> • authentication—Server for user authentication/authorization. • authorization—Server for user authorization only. • accounting—Server for RADIUS user accounting.
Server Address	Enter the IP address of the server.
Port Number	Enter the port number of the server. The default is 49.
Shared Secret Format	Choose either ASCII or hex . Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. Set the key format again in the template in the event a discovered template is applied to another device.
Shared Secret	Enter the TACACS+ shared secret used by your specified server.
Confirmed Shared Secret	Reenter the TACACS+ shared secret used by your specified server.
Admin Status	Check if you want the LDAP server to have administrative privileges.
Retransmit Timeout	Enter the time, in seconds, after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

Controller > Security > Local EAP > General - Local EAP Template

Table 31-14 describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > Security > Local EAP > General - Local EAP** page.

Table 31-14 **Controller > Security > Local EAP > General - Local EAP**

Field	Description
Local Auth Active Timeout	Enter the amount of time (in seconds) that the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fail. The valid range is 1 to 3600 seconds, and the default setting is 1000 seconds
Note	Enter the values specified below if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones. You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. The recommended and default timeout on the Cisco ACS server is 20 seconds. Roaming fails if these values are not set the same across multiple controllers.
Local EAP Identity Request Timeout	1
Local EAP Identity Request Maximum Retries	20
Local EAP Dynamic WEP Key Index	0
Local EAP Request Timeout	20
Local EAP Request Maximum Retries	2
EAPOL-Key Timeout	1000 (in milli-seconds)
EAPOL-Key Max Retries	2
Max Login Ignore Identity Response	Choose Enable to limit the number of devices that can be connected to the controller with the same username.

Controller > Security > Local EAP > Local EAP Profiles Template

[Table 31-15](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > Security > Local EAP > Local EAP Profiles** page.

Table 31-15 **Controller > Security > Local EAP > Local EAP Profiles**

Field	Description
EAP Profile Name	User-defined identification.
Select Profile Methods	Choose the desired authentication type: <ul style="list-style-type: none"> • LEAP—This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point. • EAP-FAST—This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point. • TLS—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication. • PEAP—This authentication type is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.
Certificate Issuer	Determine whether Cisco or another vendor issued the certificate for authentication. Only EAP-FAST and TLS require a certificate.
Check Against CA Certificates	Check if you want the incoming certificate from the client to be validated against the certificate authority (CA) certificates on the controller.
Verify Certificate CN Identity	Check if you want the (CN) in the incoming certificate to be validated against the common name of the CA certificate.
Check Against Date Validity	Check if you want the controller to verify that the incoming device certificate is still valid and has not expired.
Local Certificate Required	Check if a local certificate is required.
Client Certificate Required	Check if a client certificate is required.

Controller > Security > Local EAP > EAP-FAST Parameters Template

[Table 31-16](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > Security > Local EAP > EAP-FAST Parameters** page.

Table 31-16 **Controller > Security > Local EAP > EAP_FAST Parameters**

Field	Description
Time to Live for the PAC	Enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.
Authority ID	Enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.
Authority Info	Enter the authority identifier of the local EAP-FAST server in text format.

Table 31-16 *Controller > Security > Local EAP > EAP_FAST Parameters (continued)*

Field	Description
Server Key and Confirm Server Key	Enter the key (in hexadecimal characters) used to encrypt and decrypt PACs
Anonymous Provision	Check to enable anonymous provisioning. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACs must be manually provisioned

Controller > Security > Wireless Protection Policies > Rogue Policies Template

[Table 31-17](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > Security > Wireless Protection Policies > Rogue Policies** page.

Table 31-17 *Controller > Security > Wireless Protection Policies > Rogue Policies*

Field	Description
Rogue Location Discovery Protocol	<p>Determine whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following:</p> <ul style="list-style-type: none"> • Disable—Disables RLDP on all access points. • All APs—Enables RLDP on all access points. • Monitor Mode APs—Enables RLDP only on access points in monitor mode. <p>Note With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.</p>
Expiration TImeout for Rogue AP and Rogue Client Entries	Enter the expiration timeout (in seconds) for rogue access point entries.
Rogue Detection Report Interval	Enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
Rogue Detection Minimum RSSI	<p>Enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.</p> <p>There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.</p>
Rogue Detection Transient Interval (Enter 0 to Disable)	Enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only
Validate Rogue Clients against AAA	Check to enable the AAA validation of rogue clients.
Detect and Report Adhoc Networks	Check to enable detection and reporting of rogue clients participating in ad hoc networking.

Table 31-17 **Controller > Security > Wireless Protection Policies > Rogue Policies (continued)**

Field	Description
Rogue on Wire	Automatically contains rogues that are detected on the wired network.
Using our SSID	Automatically contains rogues that are advertising your network's SSID. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
Valid Client on Rogue AP	Automatically contains a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.

Controller > Security > IP Groups Template

[Table 31-18](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > IP Groups**

Table 31-18 **Controller > Security > IP Groups**

Field	Description
Name	Name of the template.
Description	Description of the template.
Validation Criteria	Choose a device type from the drop-down list and enter the OS version.
IP Group Name	Lists all the IP address including IPv4 and IPv6 groups. One IP address group can have a maximum of 128 IP address and netmask combinations. For the IP address of any, an any group is predefined. For the IPv6 address of any, an any group is predefined with an IP address type of IPv6.
IP Address	For an IP Group, enter an IPv4 address format. For IPv6 groups, enter an IPv6 address format.
Netmask	Allows the user to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property. A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service. This field does not apply for IPv6 groups.
CIDR	Classless InterDomain Routing. This field does not apply for IPv6 groups. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks. CIDR notation allows the user to add a large number of clients that exist in a subnet range by configuring a single client object.
Prefix Length	Prefix for IPv6 addresses, ranging from 0 to 128.

Controller > Security > Protocol Groups

[Table 31-19](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > Protocol Groups**.

Table 31-19 **Controller > Security > Protocol Groups**

Field	Description
Name	Name of the template.
Description	Description of the template.
Rule Name	The rule name is provided for the existing rules, or you can now enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the fields of a rule, the action for this rule is exercised.

Table 31-19 **Controller > Security > Protocol Groups (continued)**

Field	Description
Protocol	Choose a protocol from the drop-down list: <ul style="list-style-type: none"> Any—All protocols TCP—Transmission Control Protocol UDP—User Datagram Protocol ICMP—Internet Control Message Protocol ESP—IP Encapsulating Security Payload AH—Authentication Header GRE—Generic Routing Encapsulation IP—Internet Protocol Eth Over IP—Ethernet over Internet Protocol Other Port OSPF—Open Shortest Path First Other—Any other IANA protocol (http://www.iana.org/)
Source Port	Enter the source port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
Dest Port	Enter the destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
DSCP (Differentiated Services Code Point)	Choose Any or Specific from the drop-down list. If Specific is selected, enter the DSCP (range of 0 through 255). DSCP is a packet header code that can be used to define the quality of service across the Internet.

Controller > Security > 802.11 > Band Select

Table 31-20 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > Band Select**.

Table 31-20 **Controller > Security > 802.11 > Band Select**

Field	Description
Probe Cycle Count	Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.
Scan Cycle Period Threshold	Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.
Age Out Suppression	Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Table 31-20 **Controller > Security > 802.11 > Band Select (continued)**

Field	Description
Age Out Dual Band	Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.
Acceptable Client RSSI	Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Controller > Security > 802.11 > Media Stream

[Table 31-21](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > Media Stream.**

Table 31-21 **Controller > Security > 802.11 > Media Stream**

Field	Description
Media Stream Name	The name of the media stream.
Multicast Destination Start IP	Start IP address of the media stream to be multicast.
Multicast Destination End IP	End IP address of the media stream to be multicast. Start IP and End IP can be IPv4 or IPv6 multicast address, starting from controller Version 7.2.x.
Maximum Expected Bandwidth	Maximum bandwidth that a media stream can use.
Average Packet Size	Average packet size that a media stream can use.
RRC Periodical Update	Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
RRC Priority	Priority of RRC with the highest at 1 and the lowest at 8.
Traffic Profile Violation	Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
Policy	Appears if the media stream is admitted or denied.

Controller > Security > 802.11 > RF Profiles

[Table 31-22](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > RF Profiles.**

Table 31-22 **Controller > Security > 802.11 > RF Profiles**

Field	Description
Template Name	User-defined name for the template.
Profile Name	User-defined name for the current profile.
Description	Description of the template.
Radio Type	The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.

Table 31-22 **Controller > Security > 802.11 > RF Profiles (continued)**

Field	Description
Minimum Power Level Assignment (-10 to 30 dBm)	Indicates the minimum power assigned. Range: -10 to 30 dBm Default: -10 dBm.
Maximum Power Level Assignment (-10 to 30 dBm)	Indicates the maximum power assigned. Range: -10 to 30 dBm Default: 30 dBm.
Power Threshold v1(-80 to -50 dBm)	Indicates the transmitted power threshold.
Power Threshold v2(-80 to -50 dBm)	Indicates the transmitted power threshold.
Data Rates	<p>Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:</p> <ul style="list-style-type: none"> • 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps. • 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps <p>For each data rate, you must also choose one of these options:</p> <ul style="list-style-type: none"> • Mandatory—Clients must support this data rate to associate to an access point on the controller. • Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate. • Disabled—The clients specify the data rates used for communication.

Controller > 80211a or n > Parameters

Table 31-23 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Parameters**.

Table 31-23 **Controller > 80211a or n > Parameters**

Field	Description
802.11a Network Status	Select the check box to enable 802.11a/n network status.
Client Link	Use this drop-down list to enable Clientlink on all access point 802.11a/n radios that support ClientLink. Otherwise, choose Disable.
Beacon Period	Enter the amount of time between beacons in kilomicroseconds. The valid range is from 20 to 1000 milliseconds.
DTIM Period	Enter the number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count text box is 0. This value is transmitted in the DTIM period field of beacon frames. When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMS let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.
Fragmentation Threshold	Determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
802.11e Max Bandwidth	Enter the percentage for 802.11e maximum bandwidth.

Table 31-23 *Controller > 80211a or n > Parameters (continued)*

Field	Description
Mode	Click the checkbox to enable Cisco Compatible Extension (CCX) Location Measurement. When enabled, this enhances the location accuracy of clients.
Interval	Enter the interval at which CCX Location Measurement signals are broadcast, in seconds. The CCX location measurement interval of the Cisco Compatible Extension can only be changed when measurement mode is enabled.
Data Rate Dropdowns	Select the negotiation type for each data rate. The client and controller negotiate data rates between them. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. However, it is not required that a client uses all the rates marked supported to associate. For each rate, a drop-down list of Mandatory or Supported is available. Each data rate can also be set to Disable to match client settings.
Channel List	From this drop-down list in the Noise/Interference/Rogue Monitoring Channels section, choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Controller > 80211a or n > CleanAir

Table 31-24 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > CleanAir.**

Table 31-24 *Controller > 80211a or n > CleanAir*

Field	Description
Report Interferers	Select the report interferers check box to enable the CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is unselected.
Interferers Ignored/Selected for Reporting	Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.
Persistent Device Propagation	Select the Persistent Device Propagation check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points. Persistent interferers are present at the a location and interfere with the WLAN operations even if they are not detectable at all times.
Air Quality Alarm	Select the Air Quality Alarm check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.
Air Quality Alarm Threshold	If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold field to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.

Table 31-24 **Controller > 80211a or n > CleanAir (continued)**

Field	Description
Air Quality Unclassified Category Alarm	Category AlarmSelect the Air Quality Unclassified category Alarm check box to enable the alarms to be generated for unclassified interference category. CleanAir can detect and monitor unclassified interferences. Unclassified interference are interference that are detected but do not correspond to any of the known interference types.
Air Quality Unclassified Category Severity Threshold	If you selected the Air Quality Unclassified category Alarm check box, enter a value between 1 and 99 (inclusive) in the Air Quality Unclassified Severity Threshold text box to specify the threshold at which you want the unclassified category alarm to be triggered. The default is 20.
Interferers For Security Alarm	Select the Interferers For Security Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is unselected.
Interferers Ignored/Selected for Security Alarms	Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the > and < buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

Controller > 80211a or n > Media Parameters

The following tables describe the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11a or n > Media Parameters** page:

- [Table 31-25](#)—Voice tab
- [Table 31-26](#)—Video tab
- [Table 31-27](#)—General tab

Controller > 80211a or n > Media Parameters > Voice

[Table 31-25](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Media Parameters > Voice** tab.

Table 31-25 **Controller > 80211a or n > Media Parameters > Voice**

Field	Description
Admission Control (ACM)	Select the check box to enable admission control. For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.
CAC Method	If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static. Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
Maximum Bandwidth Allowed	Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

Table 31-25 **Controller > 80211a or n > Media Parameters > Voice (continued)**

Field	Description
Reserved Roaming Bandwidth	Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
Expedited Bandwidth	Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.
SIP CAC	Select the check box to enable SIP CAC. SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.
SIP Codec	Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.
SIP Call Bandwidth	Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.
SIP Sample Interval	Specify the sample interval in milliseconds that the codec must operate in.
Metric Collection	Select the check box to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Related Topics

- [Table 31-26](#)—Video tab
- [Table 31-27](#)—General tab

Controller > 80211a or n > Media Parameters > Video

[Table 31-26](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Media Parameters > Video** tab.

Table 31-26 **Controller > 80211a or n > Media Parameters > Video**

Field	Description
Admission Control (ACM)	Select the check box to enable admission control.
Maximum Bandwidth	Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
Reserved Roaming Bandwidth	Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
CAC Method	If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static. Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
Unicast Video Redirect	Select the Unicast Video Redirect check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.

Table 31-26 **Controller > 80211a or n > Media Parameters > Video (continued)**

Field	Description
Client Minimum Phy Rate	Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
Multicast Direct Enable	Select the Multicast Direct Enable check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
Maximum Number of Streams per Radio	Specify the maximum number of streams per Radio to be allowed.
Maximum Number of Streams per Client	Specify the maximum number of streams per Client to be allowed.
Best Effort QOS Admission	Select the Best Effort QOS Admission check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used. If this is disabled and maximum video bandwidth has been used, then any new client request is rejected.

Related Topics

- [Table 31-25](#)—Voice tab
- [Table 31-27](#)—General tab

Controller > 80211a or n > Media Parameters > General

[Table 31-27](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Media Parameters > General** tab.

Table 31-27 **Controller > 80211a or n > Media Parameters > General**

Field	Description
Maximum Media Bandwidth (0 to 85%)	Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Related Topics

- [Table 31-25](#)—Voice tab
- [Table 31-26](#)—Video tab

Controller > 80211a or n > Roaming Parameters

[Table 31-28](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Roaming Parameters**.

Table 31-28 *Controller > 80211a or n > Roaming Parameters*

Field	Description
Mode	Use the Mode drop-down list to choose one of the configurable modes: default values or custom values. If you select Default, the roaming parameters are unavailable for editing, and have the default values displayed in the text boxes. Select Custom to edit the roaming parameters.
Minimum RSSI	Enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the average received signal power of the client dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. Range: -80 to -90 dBm. Default: -85 dBm
Roaming Hysteresis	Enter a value to indicate how strong the signal strength of a neighboring access point must be for the client to roam to it. This field is intended to reduce the amount of ping ponging between access points if the client is physically located on or near the border between two access points. Range: 2 to 4 dB. Default: 2 dB.
Adaptive Scan Threshold	Enter the RSSI value from the associated access point of the client, below which the client must be able to roam to a neighboring access point within the specified transition time. This field also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold. Range: -70 to -77 dB. Default: -72 dB.
Transition Time	Enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the associated access point of the client is below the scan threshold. Range: 1 to 10 seconds. Default: 5 seconds.

Controller > 80211a or n > dot11a-RRM > Thresholds

Table 31-29 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > dot11a-RRM > Thresholds.**

Table 31-29 *Controller > 80211a or n > dot11a-RRM > Thresholds*

Field	Description
Min Failed Clients	Enter the minimum number of failed clients currently associated with the controller.
Coverage Level	Enter the target range of coverage threshold.
Data RSSI	Enter the Data RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.
Voice RSSI	Enter the Voice RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.
Max Clients	Enter the maximum number of failed clients that are currently associated with the controller.
RF Utilization	Enter the percentage of threshold for 802.11a/n.
Interference Threshold	Enter an interference threshold percentage.
Noise Threshold	Enter a noise threshold between -127 and 0 dBm. When the controller is outside of this threshold, it sends an alarm to Prime Infrastructure.
Coverage Exception Level Per AP	Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Controller > 80211a or n > dot11a-RRM > DCA

Table 31-30 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > dot11a-RRM > DCA.**

Table 31-30 **Controller > 80211a or n > dot11a-RRM > DCA**

Field	Description
Assignment Mode	From the, choose one of three modes: <ul style="list-style-type: none"> Automatic—The transmit power is periodically updated for all access points that permit this operation. On Demand—Transmit power is updated when you click Assign Now. Disabled—No dynamic transmit power assignments occur, and values are set to their global default.
Avoid Foreign AP Interference	Select the check box to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Unselect this check box to have RRM ignore this interference. In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.
Avoid Cisco AP Load	Select the check box to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value. In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better reuse patterns to those access points that carry more traffic load.
Avoid non 802.11 Noise	Select the check box to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference. In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.
Signal Strength Contribution	Always enabled (not configurable). This constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.
Event Driven RRM	Select the check box to disable spectrum event-driven RRM. By default, Event Driven RRM is enabled. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference
Sensitivity Threshold	If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Controller > 802.11b or g or n > Parameters

Table 31-31 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Parameters**.

Table 31-31 **Controller > 802.11b or g or n > Parameters**

Field	Description
Policy Name	Security policy in force.
Beam Forming	Choose Enable or Disable from the drop-down list. Beam forming refers to a general signal processing technique used to control the directionality of the reception or transmission of a signal.
Transmitted Power Threshold	The valid range is from -50 to -80.
Beacon Period	The rate at which the SSID is broadcast by the access point (the amount of time between beacons). The valid range is from 100 to 600 milliseconds.
DTIM Period	<p>The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0. This value is transmitted in the DTIM period field of beacon frames. When client devices receive a beacon that contains a DTIM, they normally “wake up” to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.</p> <p>DTIM period is not applicable in controller Version 5.0.0.0 and later.</p>
Fragmentation Threshold	Determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. The default value is 2346.
802.11e Max Bandwidth	Percentage for 802.11e max bandwidth. The default value is 100.
Dynamic Assignment	<p>From the Dynamic Assignment drop-down list, choose any one of the following dynamic transmit power assignment modes.:</p> <ul style="list-style-type: none"> Automatic—The transmit power is periodically updated for all access points that permit this operation. On Demand—Transmit power is updated when you click Assign Now. Disabled—No dynamic transmit power assignments occur and values are set to their global default. <p>The default is Automatic. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.</p>
Dynamic Tx Power Control	Select this check box to enable DTPC support. If this option is enabled, the transmit power level of the radio is advertised in the beacons and the probe responses.

Table 31-31 **Controller > 802.11b or g or n > Parameters (continued)**

Field	Description
Assignment Mode	<p>From the Assignment Mode drop-down list, choose any one of the following dynamic channel assignment modes:</p> <ul style="list-style-type: none"> Automatic—The channel assignment is periodically updated for all access points that permit this operation. On Demand—Channel assignments are updated when desired. Disabled—No dynamic channel assignments occur and values are set to their global default. <p>The default is Automatic.</p>
Avoid Foreign AP Interference	<p>Enable this Radio Resource Management (RRM) foreign 802.11 interference-monitoring parameter to have Radio Resource Management consider interference from foreign (non-Cisco access points outside the RF/mobility domain) access points when assigning channels to Cisco access points. Disable this field to have Radio Resource Management ignore this interference.</p> <p>In certain circumstances with significant interference energy (dB) and load (utilization) from Foreign access points, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in Cisco access points close to the Foreign access points to increase capacity and reduce variability for the Cisco WLAN Solution.</p>
Avoid Cisco AP Load	<p>Enable this Radio Resource Management (RRM) bandwidth-sensing parameter to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Disable this field to have Radio Resource Management ignore this value.</p> <p>In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel re-use. In these circumstances, Radio Resource Management can assign better re-use patterns to those APs that carry more traffic load.</p>
Avoid non 802.11 Noise	<p>Enable this Radio Resource Management (RRM) noise-monitoring field to have access points avoid channels that have interference from non-Access Point sources, such as microwave ovens or Bluetooth devices. Disable this field to have Radio Resource Management ignore this interference.</p> <p>In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability for the Cisco WLAN Solution.</p>
Signal Strength Contribution	<p>This check box is always enabled (not configurable). Radio Resource Management (RRM) constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.</p>
Data Rates	<p>The data rates set are negotiated between the client and the controller. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. But it is not required that a client be able to use all the rates marked Supported to associate 6, 9, 12, 18, 24, 36, 48, 54 Mbps.</p> <p>For each rate, a drop-down list selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.</p>

Table 31-31 **Controller > 802.11b or g or n > Parameters (continued)**

Field	Description
Channel List	Choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation among a set of managed devices connected to the controller.
Mode	Enable or disable the broadcast radio measurement request. When enabled, this enhances the location accuracy of clients.
Interval	Interval in seconds between measurement requests. Cisco Compatible Extension location measurement interval can be changed only when measurement mode is enabled.

Controller > 802.11b or g or n > Media Parameters

The following tables describe the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Media Parameters** page:

- [Table 31-32](#)—Voice tab
- [Table 31-33](#)—Video tab
- [Table 31-34](#)—General tab

Controller > 802.11b or g or n > Media Parameters > Voice

[Table 31-32](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Media Parameters > Voice** tab.

Table 31-32 **Controller > 802.11b or g or n > Media Parameters > Voice**

Field	Description
Admission Control (ACM)	Select the check box to enable admission control. For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.
CAC Method	If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static. Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
Maximum Bandwidth Allowed	Enter the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
Reserved Roaming Bandwidth	Enter the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
Expedited Bandwidth	Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.

Table 31-32 **Controller > 802.11b or g or n > Media Parameters > Voice (continued)**

Field	Description
SIP CAC	Select the check box to enable SIP CAC. SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.
SIP Codec	Choose the codec name you want to use on this radio from the SIP Codec drop-down list. The available options are G.711, G.729, and User Defined.
SIP Call Bandwidth	Enter the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.
SIP Sample Interval	Enter the sample interval in milliseconds that the codec must operate in.
Max Number of Calls per Radio	Enter the maximum number of calls per radio.
Metric Collection	Select the check box to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Related Topics

- [Table 31-33](#)—Video tab
- [Table 31-34](#)—General tab

Controller > 802.11b or g or n > Media Parameters > Video

[Table 31-32](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Media Parameters > Video** tab.

Table 31-33 **Controller > 802.11b or g or n > Media Parameters > Video**

Field	Description
Admission Control (ACM)	Select the check box to enable admission control.
Maximum Bandwidth	Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
Reserved Roaming Bandwidth	Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
Unicast Video Redirect	Select the Unicast Video Redirect check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
Client Minimum Phy Rate	Choose the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
Multicast Direct Enable	Select the Multicast Direct Enable check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
Maximum Number of Streams per Radio	Specify the maximum number of streams per Radio to be allowed.

Table 31-33 **Controller > 802.11b or g or n > Media Parameters > Video (continued)**

Field	Description
Maximum Number of Streams per Client	Specify the maximum number of streams per Client to be allowed.
Best Effort QOS Admission	Select the Best Effort QOS Admission check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used. If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Related Topics

- [Table 31-32](#)—Voice tab
- [Table 31-34](#)—General tab

Controller > 802.11b or g or n > Media Parameters > General

[Table 31-34](#) describes the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Media Parameters > General** tab.

Table 31-34 **Controller > 80211b or g or n > Media Parameters > General**

Field	Description
Maximum Media Bandwidth (0 to 85%)	Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Related Topics

- [Table 31-32](#)—Voice tab
- [Table 31-33](#)—Video tab

Controller > 802.11b or g or n > Roaming Parameters

[Table 31-35](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Roaming Parameters**.

Table 31-35 **Controller > 802.11b or g or n > Roaming Parameters**

Field	Description
Mode	Choose Default Values or Custom Values from the drop-down list. If you select Default Values, the roaming parameters are unavailable and the default values are displayed.
Minimum RSSI	Enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the client average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. Range: -80 to -90 dBm. Default: -85 dBm.
Roaming Hysteresis	Enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it. This field is intended to reduce the amount of “ping ponging” between access points if the client is physically located on or near the border between two access points. Range: 2 to 4 dB. Default: 2 dB.

Table 31-35 **Controller > 802.11b or g or n > Roaming Parameters (continued)**

Field	Description
Adaptive Scan Threshold	Enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time. This field also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold. Range: -70 to -77 dB. Default: -72 dB
Transition Time	Enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold. Range: 1 to 10 seconds. Default: 5 seconds.

Controller > 802.11b or g or n > CleanAir

Table 31-36 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > CleanAir**

Table 31-36 **Controller > 802.11b or g or n > CleanAir**

Field	Description
CleanAir	Select the check box to enable CleanAir functionality on the 802.11 b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected. If CleanAir is enabled, the Reporting Configuration and Alarm Configuration group boxes appear.
Report Interferers	Select the report interferers check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected. Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.
Air Quality Alarm	Select the Air Quality Alarm check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.
Air Quality Alarm Threshold	If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.
Interferers For Security Alarm	Select the Interferers For Security Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselected it to disable this feature. The default value is unselected. Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the > and < buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

Controller > dot11b-RRM > Thresholds

Table 31-37 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > Thresholds.**

Table 31-37 **Controller > dot11b-RRM > Thresholds**

Field	Description
Min. Failed Clients (#)	Enter the minimum number of failed clients currently associated with the controller.
Coverage Level	Enter the target range of coverage threshold (dB).
Signal Strength	When the Coverage Level field is adjusted, the value of the Signal Strength (dBm) automatically reflects this change. The Signal Strength field provides information regarding what the signal strength is when adjusting the coverage level.
Data RSSI	Enter the Data RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.
Voice RSSI	Enter the Voice RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.
Max. Clients	Enter the maximum number of clients able to be associated with the controller.
RF Utilization	Enter the percentage of threshold for this radio type.
Interference Threshold	Enter an interference threshold between 0 and 100 percent.
Noise Threshold	Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to Prime Infrastructure.
Coverage Exception Level	Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Controller > dot11b-RRM > TPC

Table 31-38 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > TPC**

Table 31-38 **Controller > dot11b-RRM > TPC**

Field	Description
TPC Version	Choose TPCv1 or TPCv2 from the drop-down list. The TPCv2 option is applicable only for controller Version 7.2.x or later.
Dynamic Assignment	From the Dynamic Assignment drop-down list, choose one of three modes: Automatic—The transmit power is periodically updated for all access points that permit this operation. On Demand—Transmit power is updated when you click Assign Now. Disabled—No dynamic transmit power assignments occur, and values are set to their global default.
Maximum Power Assignment	Indicates the maximum power assigned. Range: -10 to 30 dB. Default: 30 dB.
Minimum Power Assignment	Indicates the minimum power assigned. Range: -10 to 30 dB. Default: 30 dB.
Dynamic Tx Power Control	Click the check box if you want to enable Dynamic Transmission Power Control.
Transmitted Power Threshold	Enter a transmitted power threshold between -50 and -80.
Control Interval	Shows the transmitted power control interval in seconds (read-only).

Controller > dot11b-RRM > DCA

Table 31-39 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > DCA**.

Table 31-39 **Controller > dot11b-RRM > DCA**

Field	Description
Assignment Mode	From the Dynamic Assignment drop-down list, choose one of three modes: Automatic—The transmit power is periodically updated for all access points that permit this operation. On Demand—Transmit power is updated when you click Assign Now. Disabled—No dynamic transmit power assignments occur, and values are set to their global default.
Avoid Foreign AP Interference	<p>Enable this field to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.</p> <p>In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.</p>
Avoid Cisco AP Load	<p>Enable this bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.</p> <p>In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better re-use patterns to those access points that carry more traffic load.</p>
Avoid non 802.11 Noise	<p>Enable this noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference.</p> <p>In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.</p>
Signal Strength Contribution	The Signal Strength Contribution check box is always enabled (not configurable). constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel re-use. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.
Event Driven RRM	Select the checkbox to disable spectrum event-driven RRM. By default, Event Driven RRM is enabled. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference
Sensitivity Threshold	If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Controller > Management > Trap Control

Table 31-40 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Management > Trap Control**.

Table 31-40 **Controller > Management > Trap Control**

Field	Description
Select All Traps	Select this check box to enable all of the traps on this page.
SNMP Authentication	The SNMPv2 entity has received a protocol message that is not properly authenticated. When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.
Link (Port) Up/Down	Link changes states from up or down.
Multiple Users	Two users log in with the same login ID.
Spanning Tree	Spanning Tree traps. See the STP specification for descriptions of individual parameters.
Rogue AP	Whenever a rogue access point is detected or when a rogue access point was detected earlier and no longer exists, this trap is sent with its MAC address.
Controller Config Save	Notification sent when the configuration is modified.
802.11 Association	A trap is sent when a client is associated to a WLAN. This trap does not guarantee that the client is authenticated.
802.11 Disassociation	The disassociate notification is sent when the client sends a disassociation frame.
802.11 Deauthentication	The deauthenticate notification is sent when the client sends a deauthentication frame.
802.11 Failed Authentication	The authenticate failure notification is sent when the client sends an authentication frame with a status code other than successful.
802.11 Failed Association	The associate failure notification is sent when the client sends an association frame with a status code other than successful.
Excluded	The associate failure notification is sent when a client is excluded.
AP Register	Notification sent when an access point associates or disassociates with the controller.
AP Interface Up/Down	Notification sent when access point interface (802.11a/n or 802.11b/g/n) status goes up or down.
Load Profile	Notification sent when Load Profile state changes between PASS and FAIL.
Noise Profile	Notification sent when Noise Profile state changes between PASS and FAIL.
Interference Profile	Notification sent when Interference Profile state changes between PASS and FAIL.
Coverage Profile	Notification sent when Coverage Profile state changes between PASS and FAIL.
Channel Update	Notification sent when the dynamic channel algorithm of an access point is updated.
Tx Power Update	Notification sent when the dynamic transmit power algorithm of an access point is updated.
User Auth Failure	This trap is to inform you that a client RADIUS authentication failure has occurred.
RADIUS Server No Response	This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
ESP Authentication Failure	IPsec packets with invalid hashes were found in an inbound ESP SA.
ESP Replay Failure	IPsec packets with invalid sequence numbers were found in an inbound ESP SA.

Table 31-40 **Controller > Management > Trap Control (continued)**

Field	Description
Invalid SPI	A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.
IKE Negotiation Failure	An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.
IKE Suite Failure	An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
Invalid Cookie	ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.
WEP Decrypt Error	Notification sent when the controller detects a WEP decrypting error.
Signature Attack	Select the check box to enable the 802.11 security trap.

Controller > Management > Telnet SSH

[Table 31-41](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Management > Telnet SSH**.

Table 31-41 **Controller > Management > Telnet SSH**

Field	Description
Session Timeout	Enter the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The valid range is 0 to 160, and the default is 5.
Maximum Sessions	Enter the number of simultaneous Telnet sessions allowed. The valid range is 0 to 5, and the default is 5. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port.
Allow New Telnet Session	Select Yes to allow new Telnet sessions on the DS port, No to disallow them. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port. The default is Yes.
Allow New SSH Session	Select Yes to allow Secure Shell Telnet sessions, No to disallow them. The default is Yes.

Controller > Location > Location Configuration

The following tables describe the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Media Parameters** page:

- [Table 31-32](#)—General tab
- [Table 31-33](#)—Advanced tab

Controller > Location > Location Configuration > General

[Table 31-42](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Location > Location Configuration > General**.

Table 31-42 **Controller > Location > Location Configuration > General**

Field	Description
RFID Tag Data Collection	Select the check box to enable tag collection. Before the mobility services engine can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command <code>config rfid status enable</code> on the controllers.
Calibrating Client	Select the check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrating clients. Packets are transmitted on all channels. All access points irrespective of channel (and without a channel change) gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic. To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced tab.
Normal Client	Select the check box to have a non-calibrating client. No S36 requests are transmitted to the client. S36 and S60 are client drivers compatible with specific Cisco Compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later. For details, see the Cisco Context Aware and Location FAQ .
Tags, Clients and Rogue APs/Clients	Specify how many seconds should elapse before notification of the found tag, client, rogue AP, or rogue client.
For Clients	Enter the number of seconds after which RSSI measurements for clients should be discarded.
For Calibrating Clients	Enter the number of seconds after which RSSI measurements for calibrating clients should be discarded.
For Tags	Enter the number of seconds after which RSSI measurements for tags should be discarded.
For Rogue APs	Enter the number of seconds after which RSSI measurement for rogue access points should be discarded.

Related Topics

- [Table 31-33](#)—Advanced tab

Controller > Location > Location Configuration > Advanced

[Table 31-43](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Location > Location Configuration > Advanced**.

Table 31-43 **Controller > Location > Location Configuration > Advanced**

Field	Description
RFID Tag Data Timeout	Enter a value in seconds to set the RFID tag data timeout.
Calibrating Client Multiband	Select the check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled on the General tab

Related Topics

- [Table 31-32](#)—General tab

Controller > PMIP > Global Config

[Table 31-44](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > PMIP > Global Config**.

Table 31-44 **Controller > PMIP > Global Config**

Field	Description
Domain Name	The name of the domain.
Maximum Bindings Allowed	Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 to 40000.
Binding Lifetime	Lifetime of the binding entries in the controller. The valid range is between 10 to 65535 seconds. The default value is 65535. The binding lifetime should be a multiple of 4 seconds.
Binding Refresh Time	Refresh time of the binding entries in the controller. The valid range is between 4 to 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4 seconds.
Binding Initial Retry Timeout	Initial timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 1000 seconds.
Binding Maximum Retry Timeout	Maximum timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 32000 seconds.
Replay Protection Timestamp	Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The valid range is between 1 to 255 milliseconds. The default value is 7 milliseconds.
Minimum BRI Retransmit Timeout	Minimum amount of time that the controller waits before retransmitting the BRI message. The valid range is between 500 to 65535 seconds.
Maximum BRI Retransmit Timeout	Maximum amount of time that the controller waits before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 to 65535 seconds. The default value is 2000 seconds.
BRI Retries	Maximum number of times that the controller retransmits the BRI message before receiving the Binding Revocation Acknowledgment (BRA) message. The valid range is between 1 to 10. The default value is 1.

Security Templates Field Descriptions

The following sections contain field descriptions for pages found in **Design > Configuration Templates > Features and Technologies > Security**.

- [Security > DMVPN](#)
- [Security > GETVPN-GroupMember](#)
- [Security > GETVPN-KeyServer](#)
- [Security > ScanSafe](#)

Security > DMVPN

[Table 31-45](#) describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Security > DMVPN**.

Table 31-45 **Security > DMVPN**

Field	Description
Element	Field Description
Template Basic tab	
Name	Enter a name for the DMVPN template.
Description	(Optional) Enter a description for the DMVPN template.
Validation Criteria tab	
Device Type	Choose the device type from the drop-down list.
OS Version	Enter the OS version for the device.
IPsec Information	
Authentication Type	<p>Click the Preshared Keys or Digital Certificates radio button.</p> <ul style="list-style-type: none"> • Preshared Keys—Allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. • Digital Certificates—Authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide nonrepudiation of communication between two peers, meaning that it can be proven that the communication actually took place.
Priority	<p>The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.</p> <p>Valid values range from 1 to 10000. The lower the number, the higher the priority. If you leave this field blank, Security Manager assigns the lowest unassigned value starting with 1, followed by 5, and continuing in increments of 5.</p>
Authenticate	Choose the authentication type from the drop-down list.
Diffie-Hellman Group	<p>The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are:</p> <p>1—Diffie-Hellman Group 1 (768-bit modulus).</p> <p>2—Diffie-Hellman Group 2 (1024-bit modulus).</p> <p>5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group.</p>

Table 31-45 **Security > DMVPN (continued)**

Field	Description
Encryption policy	<p>Choose the encryption policy from the drop-down list. Choose the encryption algorithm from the drop-down list. The encryption algorithm used to establish the Phase 1 SA for protecting phase 2 negotiations:</p> <p>AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys.</p> <p>AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys.</p> <p>AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys.</p> <p>DES—Encrypts according to the Data Encryption Standard using 56-bit keys.</p> <p>3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.</p>
Hash	<p>The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are:</p> <ul style="list-style-type: none"> SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.
Lifetime	<p>The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.</p> <p>You can specify a value from 60 to 2147483647 seconds. The default is 86400.</p>
Transform Set	
Name	Enter the transform set name. The transform set encrypts the traffic on the tunnel.
ESP Encryption Algorithm	<p>The algorithm used to encrypt the payload. Choose the encryption algorithm from the drop-down list. The options are:</p> <ul style="list-style-type: none"> ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm. ESP with the 192-bit AES encryption algorithm. ESP with the 256-bit AES encryption algorithm. ESP with the 168-bit DES encryption algorithm (3DES or Triple DES). Null encryption algorithm.
ESP Integrity Algorithm	<p>The algorithm used to check the integrity of the payload. Choose the integrity algorithm from the drop-down list. The options are:</p> <ul style="list-style-type: none"> ESP with the MD5 (HMAC variant) authentication algorithm. ESP with the SHA (HMAC variant) authentication algorithm.
AH Integrity	<p>Choose the AH integrity from the drop-down list. The options are:</p> <ul style="list-style-type: none"> AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm. AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.

Table 31-45 **Security > DMVPN (continued)**

Field	Description
Compression	Enable the IP compression to compress payload. IP compression with the Lempel-Ziv-Stac (LZS) algorithm.
Mode	Choose the mode to transport the traffic.
Device Role and Topology	
Spoke radio button	Check the Spoke radio button to configure the router as a Spoke in the topology.
Hub radio button	Check the Hub radio button to configure the router as a Hub in the topology.
Dynamic Connection between Spokes	Check the Create Dynamic Connection between spokes check box to configure the dynamic connection between spokes.
EIGRP	Choose the routing information.
RIPV2	Choose the routing information.
Other	Check the Other check box to select other routing protocol.
NHRP and Tunnel Parameters	
Network ID	Enter the NHRP Network ID. The network ID is a globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.
Hold Time	Enter the number of seconds that the Next Hop Resolution Protocol (NHRP) NBMA addresses should be advertised as valid. The default value is 7200 seconds.
Tunnel Key	Enter the tunnel key. The tunnel key is used to enable a key ID for a particular tunnel interface. The range is from 0 to 4294967295.
NHRP Authentication String	Enter the Authentication String.
IP MTU	Enter the MTU size of IP packets that are sent on a particular interface. The default value for Ethernet and the serial interface is 1500. The default value varies depending upon the media type.
TCP Maximum Segment Size	Enter the TCP maximum segment size. The range is from 500 to 1460.
Physical Interface	Enter the physical interface.
NHS Fallback Time	(Optional) Enter the NHS fallback time in seconds. The range is from 0 to 60.
NHS Server	
Cluster ID	Enter the cluster value to form a group having one or more hubs. The range is from 0 to 10.
Max Connections	Enter the maximum number of connections that can be active in a particular group/cluster.
Priority	The priority of the particular hub in a cluster. Depends on the priority of the spoke router that will form a tunnel with the hub devices.
Next Hop server	Enter the IP address of the next-hop server.
Hub's Physical IP Address	Enter the IP address of the hub's physical interface.

Security > GETVPN-GroupMember

Table 31-46 describes the fields on the following page: **Design > Configuration Templates> Features and Technologies > Security > GETVPN-GroupMember**.

Table 31-46 **Security > GETVPN-GroupMember**

Field	Description
Group ID	Enter the Group ID. The Group ID is a unique identity for the GETVPN group member. This can be a number or an IP address.
Group Name	Enter the Group Name for the GETVPN group member.
IKE Authentication Policy	Use this anchored field and its associated popup to specify authentication type and policies for this GETVPN group member.
Pre-Shared Key	Select this radio button to select Pre-Shared Key as the IKE authentication type. If you select this, you must provide the key in the Pre-Shared Key field immediately below the button.
Confirm Secret Key	Enter the pre-shared key again to confirm it. This field is displayed only when you select Pre-Shared Key as the authentication type.
Digital Certificate	Select this radio button to select Digital Certificate as the IKE authentication type. If you choose this authentication type, the router must have a digital certificate issued by a Certificate Authority to authenticate itself.
IKE Policies	Use this edit table to create a set of IKE policies for this GETVPN group member.
Priority	Set the authentication policy's negotiation priority by entering a value from 1 to 10000, with 1 as the highest priority. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.
Authentication	Select the authentication policy's authentication type from the list.
D-H Group	Select the authentication policy's Diffie-Hellman group from the list.
Encryption	Select the authentication policy's encryption type from the list.
Hash	Select the authentication policy's hash type from the list.
IKE Lifetime	Enter the security association (SA) lifetime in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be.
WAN Interface	Enter the registration WAN Interface for the GETVPN group member.
Local Exception Policy ACL	Enter the Local Exception Policy ACL specifying the traffic that the GETVPN group member must send in clear text.
Fail Close ACL	Enter the Fail Close ACL specifying the traffic that must be allowed when GETVPN encryption fails. If the Fail Close ACL feature is configured, all the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.
Primary Key Server	Enter the IP address or host name of the primary encryption key server. The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizing with the secondary key servers.
Secondary Key Servers	Use this edit table to specify the set of secondary key servers. Enter them in order of priority, with the highest priority at the top of the edit table. During periods when the primary key server is down or inaccessible, the accessible secondary key server with the highest priority is elected to serve as the primary key server.
Enable Passive SA	Check the Enable Passive SA check box to enable Passive SA mode on this group member.

Security > GETVPN-KeyServer

Table 31-47 describes the fields on the following page: **Design > Configuration Templates> Features and Technologies > Security > GETVPN-KeyServer.**

Table 31-47 **Security > GETVPN-KeyServer**

Field	Description
Template Detail	
Group Name	Enter the group name for the GETVPN group member template.
Group ID	Enter a unique identity for the GETVPN group member. This can be a number or an IP address. The range is from 0 to 2147483647.
IKE Authentication Policy	
Authorization Type	<p>Click the Preshared Keys or Digital Certificates radio button:</p> <ul style="list-style-type: none"> • Preshared Keys—Preshared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. • Digital Certificates—An authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide nonrepudiation of communication between two peers, meaning that it can be proven that the communication actually took place.
Priority	<p>The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common SA. If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.</p> <p>Valid values range from 1 to 10000. The lower the number, the higher the priority.</p>
Encryption	<p>Choose the encryption algorithm from the drop-down box. The encryption algorithm is used to establish the Phase 1 SA for protecting Phase 2 negotiations:</p> <ul style="list-style-type: none"> • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Hash	<p>The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are:</p> <ul style="list-style-type: none"> • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.

Table 31-47 **Security > GETVPN-KeyServer (continued)**

Field	Description
Diffie-Hellman Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: <ul style="list-style-type: none"> • 1—Diffie-Hellman Group 1 (768-bit modulus). • 2—Diffie-Hellman Group 2 (1024-bit modulus). • 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group.
Lifetime	The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 60 to 2147483647 seconds. The default is 86400.
Registration Interface	Enter the interface to which the crypto map needs to be associated.
Traffic Details	
Local Exception ACL	Choose an ACL for the traffic that must be excluded from the encryption.
Fail Close ACL	Choose an ACL for the traffic that must be sent in clear text until the group member registers with the key server. If the Fail Close feature is configured, all the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.
Key Server Information	
Primary Key Server	Specify the primary key server IP address to which the client connects. The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizing with the secondary key servers. The server with the highest priority is elected as a primary key server.
Secondary Key Server	Specify the secondary key server IP address to which the group member falls back when the primary key server registration fails. A group member can be configured to register to any available key server from a list of all secondary key servers. Group member configuration determines the registration order. The key server defined first is contacted first, followed by the second defined key server, and so on. You can have a maximum of eight key servers for a group member.
Migration	
Enable Passive SA	The Passive SA mode overrides the receive-only SA option on the key server and encrypts all outbound traffic. Use this option to turn on the Passive SA mode on the group member.
Group Name	Enter the group name for the GETVPN group member template.

Security > ScanSafe

Table 31-48 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Security > ScanSafe**.

Table 31-48 **Security > ScanSafe**

Field	Description
Primary Server	Enter the IPv4 address or host name of the primary ScanSafe server.
HTTP Port	Specify the HTTP port to redirect the HTTP requests to the primary server. By default, the ScanSafe uses port 80 for the HTTP traffic. However, you can choose to use different ports for each request type.
HTTPS Port	Specify the HTTPs port to redirect the HTTPS requests to the primary server. By default, the ScanSafe uses the port 443 for HTTPs traffic. However, you can choose to use different ports for each request type.
Secondary Server	Enter the IPv4 address or host name of the secondary ScanSafe server.
HTTP Port (secondary)	Specify the HTTP port to which to redirect the HTTP requests to the secondary server. By default, ScanSafe uses port 80 for HTTP traffic.
HTTPS Port	Specify the HTTPs port to which to redirect the HTTPS requests to the secondary server. By default, ScanSafe uses port 443 for HTTPs traffic.
ScanSafe License	Specify the license key that the ISR sends to the ScanSafe proxy servers to indicate the organization from which the request originated. The license is a 16-byte hexadecimal key.
Server Timeout	Specify the primary ScanSafe server timeout in seconds. The ISR waits for the specified timeout period before polling the ScanSafe proxy server to check its availability.
Session Timeout	Specify the primary ScanSafe session idle timeout in seconds. If the primary server fails, the ISR will use the secondary server as the active ScanSafe proxy server. The ISR automatically falls back to the primary server as long as it is active for three consecutive timeout periods.
Source Interface	Specify the source IPv4 address or interface name on which ScanSafe Web Security is enabled.
Router behavior when ScanSafe server fail to respond	Specify how the ISR router should handle the incoming traffic when it cannot reach the configured ScanSafe proxy servers: Drop all traffic or Allow all traffic. Drop all traffic is the default.
Global User	Enter a Global User when the web authentication (webauth) is not configured under the router's Ingress Interface.
Global User Group	Enter a Global User Group when the web authentication (webauth) is not configured on the router's Egress Interfaces.
User Group Inclusion & Exclusion Info	Use the two edit tables to specify the user group information to be included or excluded during exchanges with the ScanSafe tower. This is used only when web authentication (webauth) is configured on the router's Ingress and Egress interfaces
Notify Whitelist Info to ScanSafe Tower	Select this option to sending the Whitelist information to the ScanSafe Tower and specify the Safe URL, Safe User Agent, and Safe ACL information to be sent.

Wireless Configuration Templates Field Descriptions

The following sections contain field descriptions for pages found in **Design > Wireless Configuration**.

- [Lightweight AP Configuration Templates](#)
- [Autonomous AP Migration Templates](#)

Lightweight AP Configuration Templates

The following tables describe the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates** page:

- [Table 31-49](#)—AP Parameters Tab
- [Table 31-50](#)—Mesh Tab
- [Table 31-51](#)—802.11a/n Tab
- [Table 31-52](#)—802.11a SubBand Tab
- [Table 31-53](#)—802.11b/g/n Tab
- [Table 31-54](#)—CDP Tab
- [Table 31-55](#)—FlexConnect Tab
- [Table 31-56](#)—Select APs Tab
- [Table 31-57](#)—Apply/Schedule
- [Table 31-58](#)—Report Tab

Lightweight AP Configuration Templates> AP Parameters

[Table 31-49](#) describes the fields on the following page: **Design > Wireless Configuration > Lightweight AP Configuration Templates > AP Parameters**.

Table 31-49 *Lightweight AP Configuration Templates> AP Parameters*

Field	Description
Admin Status	Select the Admin and Enabled check box to enable administrative status. To conserve energy, access points can be turned off at specified times during non-working hours. Select the Enabled check box to allow access points to be turned on or off.

Table 31-49 *Lightweight AP Configuration Templates> AP Parameters (continued)*

Field	Description
AP Mode	<p>From the drop-down list, choose one of the following:</p> <ul style="list-style-type: none"> • Local—Default • Monitor—Monitor mode only. Choose Monitor to enable this access point template for Cisco Adaptive WIPS. Once Monitor is selected, select the Enhanced WIPS Engine check box and the Enabled check box. Then select the AP Monitor Mode Optimization check box and choose WIPS from the AP Monitor Mode Optimization drop-down list. • FlexConnect—Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points. FlexConnect must be selected to configure an OfficeExtend access point. When the AP mode is FlexConnect, FlexConnect configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join. • Rogue Detector—Monitors the rogue access points but does not transmit or contain rogue access points. • Bridge • Sniffer—The access point “sniffs” the air on a given channel. It captures and forwards all the packets from the client on that channel to a remote machine that runs airopeek (a packet analyzer for IEEE 802.11 wireless LANs). It includes information on timestamp, signal strength, packet size, and so on. If you choose Sniffer as an operation mode, you are required to enter a channel and server IP address on the AP/Radio Templates 802.11b/g/n or 802.11a/n parameters tab. The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see http://www.wildpackets.com. • SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended. This option is displayed only if the access point is CleanAir-capable. Changing the AP mode reboots the access point.
Enhanced WIPS Engine	Select the Enhanced WIPS engine and the Enabled check box to enable.
AP Sub Mode	Choose an option from the drop-down list.
Country Code	<p>Select the appropriate country code from the drop-down list.</p> <p>Note Changing the country code might cause the access point to reboot.</p>
AP Failover Priority	Choose Low , Medium , High , or Critical from the drop-down list to indicate the access point failover priority. The default priority is low.
Power Injector State	When enabled, this allows you to manipulate power injector settings through NCS without having to go directly to the controllers. If the Enable Power Injector State is selected, power injector options appear.
Primary, Secondary, and Tertiary Controller IP	The Primary/Secondary/Tertiary Controller IP is the Management IP of the controller.

Table 31-49 Lightweight AP Configuration Templates> AP Parameters (continued)

Field	Description
Domain Name Server IP Address	Domain Name Server IP and Domain Name can be configured only on access points which have static IPs.
Encryption	<p>Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients.</p> <p>DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license. Encryption is not available for all access point models.</p> <p>Enabling encryption might impair performance.</p>
Rogue Detection	Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see <i>Cisco Wireless LAN Controller Configuration Guide</i> .
Telnet Access	An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.
Link Latency	<p>You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect access points, for which the link could be a slow or unreliable WAN connection.</p> <p>Note Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.</p>
Reboot AP	Select the check box to enable a reboot of the access point after making any other updates.
AP Failover Priority	Choose Low , Medium , High , or Critical from the drop-down list to indicate the access point failover priority. The default priority is low.
Controllers	Select the Controllers check box to enable the drop-down lists for the primary, secondary, and tertiary controller names.
Override Global Username Password	Select the check box to enable an override for the global username/password. Enter and confirm the new access point username and password in the appropriate text boxes.
Override Supplicant Credentials	<p>Select the Override Supplicant Credentials check box to prevent this access point from inheriting the authentication username and password from the controller. The default value is unselected. The Override Supplicant Credentials option is supported in controller Version 6.0 and later.</p> <ul style="list-style-type: none"> In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point. <p>Note The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.</p>

Lightweight AP Configuration Templates> Mesh

[Table 31-50](#) describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > Mesh** page.

Table 31-50 *Lightweight AP Configuration Templates > Mesh*

Field	Description
Bridge Group Name	<p>Enter a bridge group name (up to 10 characters) in the text box.</p> <p>Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.</p> <p>For mesh access points to communicate, they must have the same bridge group name.</p> <p>For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.</p>
Data Rate (Mbps)	<p>Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.</p> <p>This data rate is shared between the mesh access points and is fixed for the whole mesh network.</p> <p>Do not change the data rate for a deployed mesh networking solution.</p>
Ethernet Bridging	Select the Enable check box. From the Ethernet Bridging drop-down list, enable Ethernet bridging for the mesh access point.
Role	Choose the role of the mesh access point from the drop-down list (MAP or RAP). The default setting is MAP

Related Topics

- [Lightweight AP Configuration Templates> AP Parameters](#)
- [Lightweight AP Configuration Templates> 802.11a/n](#)
- [Lightweight AP Configuration Templates > 802.11a SubBand](#)
- [Lightweight AP Configuration Templates > 802.11b/g/n](#)
- [Lightweight AP Configuration Templates > CDP](#)
- [Lightweight AP Configuration Templates > FlexConnect](#)
- [Lightweight AP Configuration Templates > Select APs](#)
- [Lightweight AP Configuration Templates > Report](#)

Lightweight AP Configuration Templates> 802.11a/n

Table 31-51 describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11a/n** page.

Table 31-51 *Lightweight AP Configuration Templates> 802.11a/n*

Field	Descriptions
Channel Assignment	Choose a Global assignment method or choose Custom to specify a channel.
Admin Status	Select if you want to enable administration privileges.
Antenna Mode	Choose an antenna mode.
Antenna Diversity	Choose enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna.
Antenna Type	Indicate an external or internal antenna.
Antenna Name	Select the Antenna Type check box, then choose the applicable antenna name from the drop-down list.

Table 31-51 *Lightweight AP Configuration Templates > 802.11a/n (continued)*

Field	Descriptions
Power Assignment	Choose a Global assignment method or choose Custom to specify a power assignment.
WLAN Override	Choose Disable or Enable from the drop-down list. The access point must be reset for the WLAN override change to take effect.
Antenna Selection	Select the Antenna Selection check box, then select the appropriate antennas from the list.
CleanAir	Select to enable.

Related Topics

- [Lightweight AP Configuration Templates > AP Parameters](#)
- [Lightweight AP Configuration Templates > Mesh](#)
- [Lightweight AP Configuration Templates > 802.11a SubBand](#)
- [Lightweight AP Configuration Templates > 802.11b/g/n](#)
- [Lightweight AP Configuration Templates > CDP](#)
- [Lightweight AP Configuration Templates > FlexConnect](#)
- [Lightweight AP Configuration Templates > Select APs](#)
- [Lightweight AP Configuration Templates > Report](#)

Lightweight AP Configuration Templates > 802.11a SubBand

[Table 31-52](#) describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11a SubBand** page.

Table 31-52 *Lightweight AP Configuration Templates > 802.11a SubBand*

Field	Description
Admin Status	Click if you want to enable administration privileges.
Channel Assignment	Select the check box and then choose the appropriate channel from the drop-down list. Note The channel number is validated against the radio list of supported channels.
Power Assignment	Select the check box and then choose the appropriate power level from the drop-down list. Note The power level is validated against the radio list of supported power levels.
WLAN Override	Select the check box and then choose Disable or Enable from the drop-down list. Note The access point must be reset for the WLAN override change to take effect.
Antenna Type	Indicate an external or internal antenna.
Antenna Name	Select the Antenna Type check box, then choose the applicable antenna name from the drop-down list.

Related Topics

- [Lightweight AP Configuration Templates > AP Parameters](#)
- [Lightweight AP Configuration Templates > Mesh](#)
- [Lightweight AP Configuration Templates > 802.11a/n](#)

- [Lightweight AP Configuration Templates > 802.11b/g/n](#)
- [Lightweight AP Configuration Templates > CDP](#)
- [Lightweight AP Configuration Templates > FlexConnect](#)
- [Lightweight AP Configuration Templates > Select APs](#)
- [Lightweight AP Configuration Templates > Report](#)

Lightweight AP Configuration Templates > 802.11b/g/n

Table 31-53 describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11b/g/n** page.

Table 31-53 *Lightweight AP Configuration Templates > 802.11b/g/n*

Field	Descriptions
Channel Assignment	Choose a Global assignment method or choose Custom to specify a channel.
Admin Status	Select if you want to enable administration privileges.
Antenna Mode	Choose an antenna mode.
Antenna Diversity	Choose enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna.
Antenna Type	Indicate an external or internal antenna.
Antenna Name	Select the Antenna Type check box, then choose the applicable antenna name from the drop-down list.
Power Assignment	Choose a Global assignment method or choose Custom to specify a power assignment.
WLAN Override	Choose Disable or Enable from the drop-down list. The access point must be reset for the WLAN override change to take effect.
Tracking Optimized Monitor Mode	Select to enable.
Antenna Selection	Select the Antenna Selection check box, then select the appropriate antennas from the list.
CleanAir	Select to enable.

Related Topics

- [Lightweight AP Configuration Templates > AP Parameters](#)
- [Lightweight AP Configuration Templates > Mesh](#)
- [Lightweight AP Configuration Templates > 802.11a/n](#)
- [Lightweight AP Configuration Templates > 802.11a SubBand](#)
- [Lightweight AP Configuration Templates > CDP](#)
- [Lightweight AP Configuration Templates > FlexConnect](#)
- [Lightweight AP Configuration Templates > Select APs](#)
- [Lightweight AP Configuration Templates > Report](#)

Lightweight AP Configuration Templates > CDP

Table 31-54 describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11b/g/n** page.

Table 31-54 **Lightweight AP Configuration Templates > CDP**

Field	Description
Cisco Discovery Protocol on Ethernet Interfaces	Select the check boxes for the ethernet interface slots for which you want to enable CDP.
Cisco Discovery Protocol on Radio Interfaces	Select the checkbox for the radio interfaces slots for which you want to enable CDP.

Related Topics

- [Lightweight AP Configuration Templates> AP Parameters](#)
- [Lightweight AP Configuration Templates> Mesh](#)
- [Lightweight AP Configuration Templates> 802.11a/n](#)
- [Lightweight AP Configuration Templates > 802.11a SubBand](#)
- [Lightweight AP Configuration Templates > 802.11b/g/n](#)
- [Lightweight AP Configuration Templates >FlexConnect](#)
- [Lightweight AP Configuration Templates > Select APs](#)
- [Lightweight AP Configuration Templates > Report](#)

Lightweight AP Configuration Templates >FlexConnect

[Table 31-55](#) describes the fields on the **Lightweight AP Template Details > FlexConnect** page.

Table 31-55 **Lightweight AP Configuration Templates > FlexConnect**

Field	Description
FlexConnect Configuration	<p>Select the check box to enable FlexConnect configuration (including VLAN support, native VLAN ID, and profile name VLAN mappings).</p> <p>Note These options are only available for access points in FlexConnect mode.</p>
OfficeExtend	<p>The default is Enabled.</p> <p>Unselecting the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point configuration and return it to factory default settings, click Clear Config at the bottom of the access point details page. If you want to clear only the access point personal SSID, click Reset Personal SSID at the bottom of the access point details page.</p> <p>When you select Enable for the OfficeExtend AP, several configuration changes automatically occur including: encryption and link latency are enabled; rogue detection, SSH access, and Telnet access are disabled.</p> <p>When you enable the OfficeExtend access point, you must configure at least one primary, secondary, and tertiary controller (including name and IP address).</p>
Least Latency Controller Join	<p>When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.</p> <p>The access point only performs this search once when it initially joins the controller. It does not recalculate the latency measurements of primary, secondary, and tertiary controllers once joined to see if the measurements have changed.</p>

Table 31-55 *Lightweight AP Configuration Templates > FlexConnect (continued)*

Field	Description
Native VLAN ID	The valid native VLAN ID range is 1 to 4094. If you are changing the mode to REAP and if the access point is not already in REAP mode, then all other REAP parameters are not applied on the access point.
VLAN ID ACL Mapping	Enter a VLAN ID and choose the Ingress and Egress ACLs from the drop-down list boxes to map to the VLAN ID specified.
WebAuth ACL Mapping	Enter a WLAN ID and choose the WLAN Profile and WebAuth ACLs from the drop-down list boxes to map to the WLAN ID specified.
WebPolicy ACL Mapping	Choose a WebPolicy ACL from the drop-down list boxes.
Local Split ACL Mapping	Choose a WLAN Profile and Local Split ACL from the drop-down list boxes to map to.

Related Topics

- [Lightweight AP Configuration Templates> AP Parameters](#)
- [Lightweight AP Configuration Templates> Mesh](#)
- [Lightweight AP Configuration Templates> 802.11a/n](#)
- [Lightweight AP Configuration Templates > 802.11a SubBand](#)
- [Lightweight AP Configuration Templates > 802.11b/g/n](#)
- [Lightweight AP Configuration Templates > CDP](#)
- [Lightweight AP Configuration Templates > Select APs](#)
- [Lightweight AP Configuration Templates > Report](#)

Lightweight AP Configuration Templates > Select APs

[Table 31-56](#) describes the fields on the **Lightweight AP Template Details > Select APs** page.

Table 31-56 **Lightweight AP Configuration Templates > Select APs**

Field	Description
Search	<p>Use the Search APs drop-down list to search for and select the APs to which to apply the configuration template:</p> <ul style="list-style-type: none"> • Last Applied AP(s) • Scheduled AP(s) • All • All Mesh MAP AP(s) • All Mesh RAP AP(s) <p>You can also search by the following indices, and will be prompted for additional information as described in the fields below:</p> <ul style="list-style-type: none"> • By Controller • By Controller Name • By Floor Area • By Outdoor Area • By Model • By AP MAC Address • By AP Name, • By AP IP Address Range
Controller	Choose the controller from the drop-down list.
Controller Name	Choose the controller name from the drop-down list
Campus	Choose the campus from the drop-down list.
Building	Choose the building from the drop-down list.
FLoor Area	Choose the floor area from the drop-down list.
Outdoor Area	Choose the outdoor area from the drop-down list.
Models	Choose the model from the drop-down list.
AP MAC Address	Enter the access point MAC address.
AP Name	Enter the complete AP name or the starting characters of the name.
IP Address Range	Enter the range of AP IPv4 addresses. The input text for IP address search can be of two formats X.X.X.* or X.X.X.[0-255]. For example, 10.10.10.* or 10.10.10.[20-50] searches the APs in 10.10.10.10 to 10.10.10.50 IP address range.

Lightweight AP Configuration Templates > Apply/Schedule

[Table 31-57](#) describes the fields on the **Lightweight AP Template Details > Apply/Schedule** page.

Table 31-57 **Lightweight AP Configuration Templates > Select APs**

Field	Description
Schedule	Select the check box to enable scheduling

Table 31-57 *Lightweight AP Configuration Templates > Select APs (continued)*

Field	Description
Start Date	Enter the start date for the scheduled template application, or select the start date by clicking on the calendar icon.
Start Time	Select the starting hour and minute
Recurrence	Select the range of recurrence for this schedule: Daily, Weekly, Hourly, or No Recurrence.

Related Topics

- [Lightweight AP Configuration Templates> AP Parameters](#)
- [Lightweight AP Configuration Templates> Mesh](#)
- [Lightweight AP Configuration Templates> 802.11a/n](#)
- [Lightweight AP Configuration Templates > 802.11a SubBand](#)
- [Lightweight AP Configuration Templates > 802.11b/g/n](#)
- [Lightweight AP Configuration Templates > CDP](#)
- [Lightweight AP Configuration Templates >FlexConnect](#)
- [Lightweight AP Configuration Templates > Report](#)

Lightweight AP Configuration Templates > Report

Table 31-58 describes the fields on the **Lightweight AP Template Details > Report** page.

Table 31-58 *Lightweight AP Configuration Templates > Report*

Field	Description
AP Name	The name of the applicable access point.
Status	Indicates whether the report run was a success, partial failure, failure, or not initiated. For failed or partially failed provisioning, click Details to view the failure details (including what failed and why it failed).
Ethernet MAC	Indicates the Ethernet MAC address for the applicable access point.
Controller	Indicates the controller IP address for the applicable access point.
Map	Identifies a map location for the access point.

Related Topics

- [Lightweight AP Configuration Templates> AP Parameters](#)
- [Lightweight AP Configuration Templates> Mesh](#)
- [Lightweight AP Configuration Templates> 802.11a/n](#)
- [Lightweight AP Configuration Templates > 802.11a SubBand](#)
- [Lightweight AP Configuration Templates > 802.11b/g/n](#)
- [Lightweight AP Configuration Templates > CDP](#)
- [Lightweight AP Configuration Templates >FlexConnect](#)
- [Lightweight AP Configuration Templates > Select APs](#)

Autonomous AP Migration Templates

Table 31-59 describes the fields on the following page: **Design > Wireless Configuration > Autonomous AP Migration Templates.**

Table 31-59 Autonomous AP Migration Templates

Field	Description
Name	Template name.
Description	Enter a description of the template.
DHCP Support	Ensures that after the conversion every access point gets an IP from the DHCP server.
Retain AP HostName	<p>Allows you to retain the same hostname for this access point.</p> <p>The hostname is retained in the CAPWAP, only when you are migrating the AP to CAPWAP for the first time. It might not be retained if you are upgrading an AP for several times. The CAPWAP access points hostname is set to default if autonomous access points hostname has more than 32 characters.</p> <p>If you upgrade the access points to LWAPP from 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, 12.3(11)JA3 autonomous images, the converted access points might not retain their Static IP Address, Netmask, Hostname and Default Gateway.</p>
Migrate over WANLink	<p>Increases the default timeouts for the CLI commands executed on the access point.</p> <p>If you enable this option, the <code>env_vars</code> file stores the remote TFTP server location. This information is copied to the access point. If this option is not selected, then the Prime Infrastructure internal TFTP server is used to copy the <code>env_vars</code> file to the access point.</p>
DNS Address	Enter the DNS address.
Domain Name	Enter the domain name.
Controller IP	Enter controller IP address.
AP Manager IP	<p>Specify the controller the access point should join by entering the access point manager IP address.</p> <p>For SSC-enabled access points, this IP address must be the same as the controller IP field. For MIC-enabled access points, the IP addresses need not match.</p>
User Name	Enter user name.
Password	Enter password for the user name.
TFTP Server IP	Enter the IP address of the Prime Infrastructure server. Prime Infrastructure provides its own TFTP and FTP server during the installation and setup
File Path	Enter the TFTP directory which was defined during Prime Infrastructure setup.
File Name	Enter the CAPWAP conversion file defined in the TFTP directory during Prime Infrastructure setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).
Apply Template	Choose an option by which you want to apply the template for migration.
Notification	Enter the email address of recipient to send notifications.

Designing Mobility Services Engine Field Description

The following section contains field descriptions for designing mobility services engine:

- [Mobility Services Engine Page Field Description, page 31-69](#)
- [High Availability Field Description, page 31-70](#)
- [Adding Trap Destinations for a mobility services engine, page 31-71](#)
- [Adding User to a mobility services engine, page 31-71](#)
- [Adding User Groups, page 31-72](#)
- [Provisioning MSAP service advertisement, page 31-72](#)

Mobility Services Engine Page Field Description

The following section contains field description for pages found in **Design > Mobility Services > Mobility Services Engine** page.

- [Mobility Services Engine Page Field Description, page 31-69](#)
- [Mobility Services Engine > Select a command > Add Location Server, page 31-69](#)

Mobility Services Engine > Select a command > Add Location Server

[Table 31-60](#) describes the fields on the **Design > Mobility Services > Mobility Services Engine > Select a command > Add Location Server** page.

Table 31-60 **Add Location Server**

Field	Description
Device Name	Device Name of the mobility services engine
IP Address	IP address of the mobility services engine.
Contact Name	The mobility service engine administrator.
User Name	The default username is admin. This is Prime Infrastructure communication username configured for MSE.
Password	The default password is admin. This is Prime Infrastructure communication password configured for MSE.
Port	Port number of the mobility services engines device.
HTTPS	When enabled, HTTPS is used for communication between Prime Infrastructure and location server.

Mobility Services Engine > Select a command > Add Mobility Services Engine

[Table 31-61](#) describes the fields on the **Design > Mobility Services > Mobility Services Engine > Select a command > Add a Mobility Services Engine** page.

Table 31-61 **Add a Mobility Services Engine**

Field	Description
Device Name	User-assigned name for the mobility services engine.
IP Address	The IP address of the mobility service engine.
Contact Name	The mobility services engine administrator.

Field	Description
Username	The default username is admin. This is Prime Infrastructure communication username configured for MSE.
Password	The default password is admin. This is Prime Infrastructure communication password configured for MSE.
HTTP	When enabled, HTTP is used for communication between Prime Infrastructure and mobility services engine. By default, Prime Infrastructure uses HTTPS to communicate with MSE.

Mobility Services Engine Database Synchronization

Table 31-61 describes the fields on the **Administration > Background Task > Mobility Service Synchronization** link > **Task > Mobility Service Synchronization > Select a command > Add a Mobility Services Engine** page.

Table 31-62 **Add a Mobility Services Engine**

Field	Description
Device Name	User-assigned name for the mobility services engine.
IP Address	The IP address of the mobility service engine.
Contact Name	The mobility services engine administrator.
Username	The default username is admin. This is Prime Infrastructure communication username configured for MSE.
Password	The default password is admin. This is Prime Infrastructure communication password configured for MSE.
HTTP	When enabled, HTTP is used for communication between Prime Infrastructure and mobility services engine. By default, Prime Infrastructure uses HTTPS to communicate with MSE.

High Availability Field Description

Table 31-63 describes the fields on the **Design > Mobility Services > High Availability** page.

Table 31-63 **Configuring High Availability**

Field	Description
Device Name	Secondary device name with which you want to pair the primary MSE.
IP Address	Secondary IP address which is the health monitor IP address of the secondary MSE.
Contact Name	The mobility services engine administrator.
Failover Type	Specify the failover type. You can choose either Manual or Automatic. After 10 seconds, the system fails over. The secondary server waits for a maximum of 10 seconds for the next heartbeat from the primary server. If it does not get the heartbeat in 10 seconds, it declares a failure.

Field	Description
Failback Type	Specify the failback type. It can be either Manual or Automatic.
Long Failover Wait	Specify the long failover wait in seconds. After 10 seconds, the system fails over.
	The maximum failover wait is 2 seconds.

Adding Trap Destinations for a mobility services engine

Table 31-64 describes the fields on the **Design > Mobility Services > Device Name > System > Trap Destinations > Add Trap Destinations** page.

Table 31-64 Add Trap Destinations

Field	Description
IP Address	IP address of the trap destination
Port No.	Port number for the trap destination. The default port number is 162.
Destination Type	This field is not editable and has a value of Other .
SNMP Version	Select either v2c or v3.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	Username for the SNMP Version 3.
Security Name	Security name for the SNMP Version 3.
Authentication Type	Select one of the following: HMAC-MD5 HMAC-SHA
Authentication Password	Authentication password for the SNMP Version 3.
Privacy Type	Select one of the following: CBC-DES CFB-AES-128 CFB-AES-192 CFB-AES-256
Privacy Password	Privacy password for the SNMP Version 3.

Adding User to a mobility services engine

Table 31-65 describes the fields on the **Design > Mobility Services > Mobility Services Engine > Device Name > Systems Account > Users > Select a command > Add User** page.

Table 31-65 **Add User**

Field	Description
Username	Enter the username
Password	Enter the password
Confirm Password	Re-enter the password
Group Name	Group name to which the user belongs
Permission Level	Choose a permission level. There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for Prime Infrastructure to access a mobility services engine).

Adding User Groups

Table 31-61 describes the fields on the **Design > Mobility Services > Mobility Services Engine > Device > Systems > Accounts > Users > Select a Command > Add Group** page.

Table 31-66 **Design > Mobility Services > Mobility Services Engine > Device Name > Systems > Accounts > Users > Select a command > Add Group**

Field	Description
Group Name	Enter the name of the group.
Permission Level	Choose a permission level. There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for Prime Infrastructure to access a mobility services engine).

Provisioning MSAP service advertisement

Table 31-67 describes the fields on the **Design > Mobility Services > MSAP > Select a command > Add Service Advertisement** page.

Table 31-67 **Design > Mobility Services > MSAP > Select a command > Add Service Advertisement**

Field	Description
General	
Provider Name	Enter the service provider name. It is the name of the provider who wants to provide advertisements to the client.
Icon	Select an icon that is associated with the service provider by clicking the Choose File . This is the icon that is displayed on the client handset.
Venue Name	Enter the venue name at which you want the advertisements to be broadcasted on.
Area Type	Choose the area type where you want to display the service advertisements.
Campus	Choose the campus type where you want to display the service advertisements.
Building	Choose the building name where you want the advertisements to appear.
Floor	Choose the floor type.

Field	Description
Coverage Area	Choose the coverage area.
Selected Map	Shows the selected map position.
SSID	Choose SSIDs on which you want to broadcast the service advertisements.
Display Rule	You can select either the Display everywhere or Display near selected APs radio button. By default, Display everywhere radio button is selected.
Advertisement	
Friendly Name	Enter the service description.
Advertisement Type	Choose the type of advertisement you want to display.

Wireless Operational Tools Field Descriptions

The following sections contain field descriptions for pages found in **Operate > Operational Tools > Wireless**:

- [Guest User Controller Templates Field Descriptions, page 31-73](#)
- [Voice Audit Field Descriptions, page 31-74](#)
- [Voice Diagnostic Field Descriptions, page 31-78](#)

Guest User Controller Templates Field Descriptions

The following tables describe the fields on the **Operate > Operational Tools > Wireless > Guest User > Add Guest User > New Controller Template** page:

- [Table 31-68](#)—General Tab
- [Table 31-69](#)—Advanced Tab

Guest User > Add Guest User > New Controller Template > General Tab

[Table 31-68](#) describes the fields on the **Operate > Operational Tools > Wireless > Guest User > Add Guest User > New Controller Template > General** page.

Table 31-68 *Guest User > Add Guest User > New Controller Template > General Tab Field Descriptions*

Field	Description
User Name	Enter a guest username. The maximum size is 24 characters.
Generate Password	Select the check box to generate a username and password on every schedule of guest user account creation. If this is enabled, a different password is supplied for each day (up to the number of days chosen). If this is disabled (unselected), one password is supplied for a span of days. The generation of a new password on every schedule is optional.

Table 31-68 *Guest User > Add Guest User > New Controller Template > General Tab Field Descriptions (continued)*

Field	Description
Password	Enter a password. Password requirements include the following: <ul style="list-style-type: none"> The password must have a minimum of eight characters. The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, or special characters.
Confirm Password	Reenter the password that you entered in the Password field.
Description	Enter a description of the guest user template.
Disclaimer	The default disclaimer text.
Make this Disclaimer Default	Select the check box to make the disclaimer text as default for this guest user template.

Guest User > Add Guest User > New Controller Template > Advanced Tab

[Table 31-69](#) describes the fields on the **Operate > Operational Tools > Wireless > Guest User > Add Guest User > New Controller Template > Advanced** page.

Table 31-69 *Guest User > Add Guest User > New Controller Template > Advanced Tab Field Descriptions*

Field	Description
Import From File	Select the check box to import bulk guest user templates.
Profile	Select the profile to which the guest users would connect.
User Role	Choose a user role for the guest user from the drop-down list. User roles are predefined by the administrator and are associated with the access of the guest (such as contractor, customer, partner, vendor, visitor, and so on). User Role is used to manage the amount of bandwidth allocated to specific users within the network.
Life Time	Define how long the guest user account remains active by choosing one of the following options: <ul style="list-style-type: none"> Limited—Choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours). Unlimited—There is no expiration date for the guest account.
Apply to	From the drop-down list, choose one of the following: <ul style="list-style-type: none"> Indoor Area—Campus, Building, and Floor. Outdoor Area—Campus, Outdoor Area. Controller List—List of controller(s) on which the selected profile is created. Config Groups—Config group names configured on Prime Infrastructure.

Voice Audit Field Descriptions

The following tables describe the fields on the **Operate > Operational Tools > Wireless > Voice Audit** page:

- [Table 31-70](#)—Controllers Tab
- [Table 31-71](#)—Rules Tab
- [Table 31-72](#)—Report Tab

Voice Audit > Controller Tab

[Table 31-70](#) describes the fields on the **Operate > Operational Tools > Wireless > Voice Audit > Controller** page.

Table 31-70 **Voice Audit > Controller Tab Field Descriptions**

Field	Description
Run audit on	Choose one of the following options: <ul style="list-style-type: none"> • All Controllers—No additional Controller information is necessary. • A Floor Area—From the drop-down lists, choose the applicable campus, building, floor, and controller. • A Single Controller—Choose the applicable controller from the drop-down list.

Voice Audit > Rules Tab

[Table 31-71](#) describes the fields on the **Operate > Operational Tools > Wireless > Voice Audit > Rules** page.

Table 31-71 **Voice Audit > Rules Tab Field Descriptions**

Rule	Rule Details
VoWLAN SSID	Description—Checks whether or not the VoWLAN SSID exists. Rule validity—User-defined VoWLAN SSID.
CAC: 7920	Description—Checks whether or not 7920 AP CAC is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CAC: 7920 Clients	Description—Checks whether or not the 7920 Client CAC is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
DHCP Assignment	Description—Checks whether or not DHCP assignment is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
MFP Client	Description—Checks whether or not MFP Client protection is not set to Required for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Platinum QoS	Description—Checks whether or not QoS is set to Platinum (Voice) for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Non Platinum QoS	Description—Checks that QoS is not set to Platinum for non-VoWLAN. Rule validity—User-defined VoWLAN SSID.

Table 31-71 **Voice Audit > Rules Tab Field Descriptions (continued)**

Rule	Rule Details
WMM	Description—Checks whether or not WMM is enabled for VoWLAN. Rule data—Choose Allowed or Required from the drop-down list. Rule validity—User-defined VoWLAN SSID.
CCKM	Description—Checks whether or not CCKM is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CCKM With No AES- for 792x phones	Description—Check that AES encryption is not enabled with Cisco Centralized Key Management (CCKM) for VoWLAN. This rule is only for 792x phones. Rule validity—User-defined VoWLAN SSID.
TSM	Description—Check that Traffic Stream Metrics (TSM) is Enabled. Rule data—Choose 802.11a/n TSM , 802.11b/g/n TSM , or both check boxes. Rule validity—At least one band must be selected.
DFS	Description—Checks whether the Channel Announcement and Channel Quiet Mode are Enabled for Dynamic Frequency Selection (DFS).
ACM	Description—Checks whether or not Admission Control is enabled. Rule data—Choose 802.11a/n ACM , 802.11b/g/n ACM , or both check boxes. Rule validity—At least one band must be selected.
DTPC	Description—Checks whether or not Dynamic Transmit Power Control is enabled. Rule data—Select 802.11a/n DTPC , 802.11b/g/n DTPC , or both check boxes. Rule validity—At least one band must be selected.
Expedited Bandwidth	Description—Checks whether or not Expedited Bandwidth is enabled. Rule data—Select 802.11a/n Expedited Bandwidth , 802.11b/g/n Expedited Bandwidth , or both check boxes. Rule validity—At least one band must be selected.
Load Based CAC	Description—Checks whether or not Load Based Admission Control (CAC) is enabled. Rule data—Select 802.11a/n Load Based CAC , 802.11b/g/n Load Based CAC (LBCAC) , or both check boxes. Rule validity—At least one band must be selected.
CAC: Max Bandwidth	Description—Checks whether or not Maximum RF Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Allowed Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 0—100%.

Table 31-71 **Voice Audit > Rules Tab Field Descriptions (continued)**

Rule	Rule Details
CAC: Reserved Roaming Bandwidth	<p>Description—Checks whether or not Reserved Roaming Bandwidth for Call Admission Control is configured properly.</p> <p>Rule data—Enter percentages in the text boxes for Maximum Reserved Roaming Bandwidth for 802.11a/n and 802.11b/g/n.</p> <p>Rule validity—Data for at least one band must be provided. The valid range is 0—100%.</p>
Pico Cell mode	<p>Description—Checks whether or not Pico Cell mode is disabled.</p> <p>Rule data—Select 802.11a/n Pico Cell mode, 802.11b/g/n Pico Cell mode, or both check boxes.</p> <p>Rule validity—At least one band must be selected.</p>
Beacon Period	<p>Description—Checks whether or not Beacon Period is configured properly.</p> <p>Rule data—Enter the time (ms) in the text boxes for Beacon Period for 11a/n and 11b/g/n.</p> <p>Rule validity—Data for at least one band must be provided. The valid range is 20—1000. Enter 0 or keep it empty if a band should not be checked.</p>
Short Preamble	Description—Checks whether or not Short Preamble is enabled for 11b/g.
Fragmentation Threshold	<p>Description—Checks whether or not Fragmentation Threshold is configured properly.</p> <p>Rule data—Enter the threshold amount (bytes) in the text boxes for Fragmentation Threshold for 11a/n and 11b/g/n.</p> <p>Rule validity—Data for at least one band must be provided. The valid range is 256—2346. Enter 0 or keep it empty if a band should not be checked.</p>
Data Rate	<p>Description—Checks whether or not Data Rates are configured properly.</p> <p>Data Rate configuration for 11b/g—Select Disabled, Supported, or Mandatory for each Mbps category.</p> <p>Data Rate configuration for 11a—Select Disabled, Supported, or Mandatory for each Mbps category.</p>
Aggressive Load Balancing	Description—Checks whether or not Aggressive Load Balancing is disable.
QoS Profile	Description—Checks that QoS Profiles are not altered from default values.
EAP Request Timeout	<p>Description—Checks whether or not EAP Request Timeout is configured properly.</p> <p>Rule data—Enter the time limit (sec) for the EAP Request Timeout.</p> <p>Rule validity—Data cannot be left blank or as zero. The valid range is 1—120.</p>
ARP Unicast	Description—Checks whether or not ARP Unicast is disabled.

Voice Audit > Report Tab

Table 31-72 describes the fields on the **Operate > Operational Tools > Wireless > Voice Audit > Report** page.

Table 31-72 Voice Audit > Report Tab Field Descriptions

Field	Description
Audit Status	Indicates whether or not the audit is complete.
Start Time and End Time	Indicates the time at which the voice audit starts and ends.
# Total Devices	Indicates the number of devices involved in the voice audit.
# Completed Devices	Indicates the number of devices the tool attempted to audit. Note If a controller is unreachable, the audit skips it. The Voice Audit does not complete any rule checks for that controller.
# Rules	Indicates the number of rules selected for the voice audit.
Report Results	
IP Address	Indicates the IP address for the controller involved in the voice audit.
Rule	Indicates the rule that was applied for this controller.
Result	Indicates the result (Skipped, Violation, Unreachable) of the applied rule. Note If there is no mismatch between the current configuration and a rule value, no results are displayed for that rule.
Details	Defines an explanation for the rule results. Note If the applied rule results in a Violation, the Details link provides additional information including Name, the Device Value, and the Rule Value. Hover your mouse cursor over the link to view the additional details.
Time	Provides a timestamp for the voice audit.

Voice Diagnostic Field Descriptions

The following tables describe the fields on the **Operate > Operational Tools > Wireless > Voice Diagnostic** page:

- [Table 31-73](#)—Voice Diagnostic Test List Page
- [Table 31-74](#)—Voice Diagnostic Test Report Page

Voice Diagnostic Test List Page

[Table 31-73](#) describes the fields on the **Operate > Operational Tools > Wireless > Voice Diagnostic** page.

Table 31-73 Voice Diagnostic Test List Page Field Descriptions

Field	Description
Test Name	Name of the test.
Duration of Test (Minutes)	The duration for which the test is performed. The duration can be either 10, 20, 30, 40, 50, or 60 minutes. The default selection is 10 minutes.
First Client	Displays the First Client details such as the Client MAC address and all the controllers provisioned for the client and if the controllers are not reachable then the failed provisioned controllers are also listed.

Table 31-73 Voice Diagnostic Test List Page Field Descriptions (continued)

Field	Description
Second Client	Displays the Second Client details (if any) such as the Client MAC address and all the controllers provisioned for the client and if the controllers are not reachable then the failed provisioned controllers are also listed.
Start Time	The time when the test was started.
Remaining Time	The time remaining for the test.
State	The state of the test. It can be one of the four states, Running, Completed, Stopped or Aborted.
Problem	The status of the test. Red indicates a problem was discovered in the test. Green indicates the voice diagnostic test that no problems were discovered during the call.

Voice Diagnostic Test Report Page

Table 31-74 describes the tabs on the **Operate > Operational Tools > Wireless > Voice Diagnostic Test Report** page.

Table 31-74 Voice Diagnostic Test Report Page Tab Descriptions

Tab	Description
Summary	
This tab is divided into three areas where top area displays the test and client details, the middle area displays the problems, and the bottom area displays the corresponding log messages.	
Test and Client Details	The test status displays the test details like the Test Name, First Client MAC address, Second Client MAC address, device type, test status, start time, remaining time and the duration of the test. Restart if the test was stopped or completed the test. A stop button is provided to Stop the running test. The Refresh Status Tab and Refresh Client Tab buttons is used to refresh the status and client details. The client details such as the client user name, IP address, MAC address, Vendor, CCX Version, 802.11 state, protocol, SSID, profile-name, and AP details are displayed. You can click the Client MAC address for more client details.
Problems	<p>The Problems pane appears below the test and client status details pane, This pane displays all the problems regarding the current diagnosis. This pane is updated every 5 seconds independently. There is no need to refresh the whole page. You can sort the information in this pane by clicking on any of the pane columns. A pop-up dialog box appears with the Problem detailed description and Suggested action when you click any row of the Problems pane.</p> <p>Note In some cases of inter controller roaming failure, the MAC address in the From AP information is incorrect and may appear as “00:00:00:00:00:00”.</p>
Logs	The Logs pane appears below the Problems pane. This pane displays all the messages exchanged between the controller and the WCS during this diagnosis. You can sort the information in this pane by clicking on any of the pane columns. This pane is updated every 5 sec independently without refreshing the whole page.
Charts	
This tab displays the charts for each client's uplink and downlink traffic. The charts will be updated every 10 secs.	

Table 31-74 Voice Diagnostic Test Report Page Tab Descriptions (continued)

Tab	Description
Client Uplink and DownLink TSM Chart with Roaming	The Client Uplink Traffic Stream Metric (TSM) chart shows the clients which support CCX V4 and above. The TSM data is plotted for every 10 sec. The TSM Chart displays the metrics for a set of series, that can be enabled or disabled using the Select Series button in the chart.
Client Uplink and DownLink QoS Chart	For each interval, QoS will be calculated and shown on the chart. represents the Client Uplink QoS chart. This pie chart provides the total QoS Chart counts and its distribution in three categories. These categories generally indicate the quality of a voice call.
Average Uplink and Downlink AC Queue	The AC Queue displays the type of packets and the number of packets for a series. You can enable or disable the series using the Select Series button.

Roam History

This tab shows the roaming history information in the Roaming Table. This Roaming table displays both the successful and the failed roaming history. The roaming table provides the following information:

- Time at which the roaming of the client happened
- The name of the AP from which the client moved
- The type of Radio from which the client moved
- The IP address of the controller from which the client moved
- The name of the AP to which the client moved
- The IP address of the controller to which the client moved
- The type of radio to which the client moved
- The roaming result, whether it was successful or a failure
- If it was a failure it also provides the reason to the failure

Events

The Event tab shows the event history related to client and AP during a voice call in a list. It will show last 10 events. There is two Event tables available, Client Events and AP Events. Client Specific events during the voice call is shown in the Client Events table and AP Specific events in shown in the AP Event table.

Switch Location Configuration Templates

Table 31-75 describes the fields on the **Design > Wireless Configuration > Switch Location Configuration** page.

Table 31-75 Switch Location Configuration Template Page Field Descriptions

Field	Description
General	
Template Name	
Map Location	
Campus	Choose a campus for the map location for a switch/switch port.
Building	Choose a building for the map location for a switch/switch port.

Table 31-75 *Switch Location Configuration Template Page Field Descriptions (continued)*

Field	Description
Floor	Choose a floor for the map location for a switch/switch port.
Import	Imports the civic information for the campus, building, and floor selected.
ELIN and Civic Location	
ELIN	The Emergency Location Identification Number.
Civic Address tab	The available civic address information for the switch/switch port.
Advanced tab	Detailed information about the switch/switch port location.
NMSP	Select or unselect this check box to enable or disable NMSP for the switch.



CHAPTER 32

Field Reference for Reports

This section provides field descriptions for various reports in Prime Infrastructure.

Field Descriptions

The following sections contain field descriptions for pages found in **Report**:

- [Report Launch Pad, page 32-1](#)
- [Scheduled Run Results, page 32-5](#)
- [Saved Report Templates, page 32-5](#)

Report Launch Pad

The following tables describe the fields on the **Report > Report Launch Pad > Report Type > New** page:

- [Table 32-1](#)—Settings and Schedule
- [Table 32-2](#)—Create Custom Report

Report Launch Pad > *Report Type* > New

[Table 32-1](#) describes the fields on the **Report > Report Launch Pad > Report Type > New** page.

Table 32-1 Report Launch Pad > Report Type > New Field Descriptions

Field	Description
Settings	
Create reports in current and each sub Virtual Domains	<p>Select this check box if you want to create reports not only in current virtual domain but also for each sub virtual domains. Click the View applied Virtual Domains link to view details about the virtual domains such as the name of the virtual domain, e-mail address and the time zone.</p> <p>Note If this check box is enabled and the report is not scheduled, the report template is created and saved in all the subdomains but the report is not run. But if the Create reports in current and sub Virtual Domains check box is checked, and the report is scheduled, then the report is scheduled in all the subdomains and is run at the scheduled time.</p> <p>Note If this check box is enabled, you can only save the report and therefore all other options such as run, run and save, save and export, save and e-mail are not visible in the report details page. This means that the reports can only be created and scheduled to run in sub domains.</p> <p>Note There should be sufficient time interval (at least 30 minutes) between the report creation and report execution as the report creation time varies between different systems.</p>
Report Title	<p>Enter a report name.</p> <p>Note This report title is suffixed with <i>_VirtualDomainName</i> if you select the Create reports in current and each sub Virtual Domains check box. The <i>VirtualDomainName</i> is the name of the virtual domain for which the report has been generated.</p>
Report By	Choose the appropriate Report By category from the drop-down list. The categories differ for each report.
Report Criteria	The field allows you to sort your results depending on the previous Report By selection made. Click Edit to open the Filter Criteria page and select the required filter criteria.
Connection Protocol	<p>Choose one of the following connection protocols:</p> <ul style="list-style-type: none"> • All Clients • All Wired (802.3) • All Wireless (802.11) • All 11u Capable Clients • 802.11a/n • 802.11b/g/n • 802.11a • 802.11b • 802.11g • 802.11n (5 GHz) • 802.11n (2.4 GHz)
SSID	All SSIDs is the default value.

Table 32-1 **Report Launch Pad > Report Type > New Field Descriptions (continued)**

Field	Description
Reporting Period	<p>Select the Select a time period radio button and choose the period of time from the drop-down list.</p> <p>or</p> <p>Select the From radio button and enter the From and To dates and times. You can type a date in the text box or click the calendar icon to choose a date. Choose the hours and minutes from the drop-down lists.</p>
Show	<p>Enter the number of records that you want to be displayed in the report.</p> <p>Note Enter a number between 5 and 1000, or leave the text box blank to display all records.</p>
Schedule	
Scheduling	Select the Enable check box to run the report on the set schedule.
Export Format	<p>Choose CSV or PDF as format to export the report results after a report is run.</p> <p>Note The default file locations for CSV and PDF files are as follows:</p> <p style="margin-left: 40px;">/ncs-ftp/reports/Inventory/ReportTitleName_yyyymmdd_HHMMSS.csv /ncs-ftp/reports/Inventory/ReportTitleName_yyyymmdd_HHMMSS.pdf</p>
Destination	<p>Choose your destination type (File or Email). Enter the applicable file location or the e-mail address.</p> <p>Note If you selected the Create reports in current and each sub Virtual Domains check box, the Email to default Contact in each Virtual Domain radio button appears instead of the Email radio button. You can click the View Contacts link to view the e-mail IDs for the various virtual domains.</p> <p>Note To set the mail server setup for e-mails, choose Administration > Settings, then choose Mail Server from the left sidebar menu to open the Mail Server Configuration page. Enter the SMTP and other required information.</p> <p>Note If an e-mail address is not specified for a subVirtual Domain then the e-mail address of the current Virtual Domain is used if it is specified for the current Virtual Domain.</p>

Table 32-1 Report Launch Pad > Report Type > New Field Descriptions (continued)

Field	Description
Start Date/Time	<p>Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins to run on this data and at this time.</p> <p>Note The time referred here is the NCS server time and not the local time of the browser.</p> <p>Note If you selected Create reports in current and each sub Virtual Domains check box then the Use Virtual Domain time zone check box appears. Select this check box if you want to use the time zone of the virtual domain as the time zone. Click the View time zones link to view the timezones of the various virtual domains.</p>
Recurrence	<p>Select the frequency for the report run from the following options:</p> <ul style="list-style-type: none"> • No Recurrence—The report runs only once (at the time indicated for the Start Date/Time). • Hourly—The report runs on the interval indicated by the number of hours you enter in the Entry text box. • Daily—The report runs on the interval indicated by the number of days you enter in the Every text box. • Weekly—The report runs on the interval indicated by the number of weeks you enter in the Every text box and on the days specified by the selected check boxes. • Monthly—The report runs on the interval indicated by the number of months you enter in the Every text box.

Report Launch Pad > Report Type > New > Customize

Table 32-2 describes the fields on the **Report > Report Launch Pad > Report Type > New > Customize** page.

Table 32-2 Report Launch Pad > Report Type > New > Customize Field Descriptions

Field	Description
Custom Report Name	<p>Choose the report you intend to customize from the drop-down list.</p> <p>Note The Available data fields and Data fields to include column heading selections might change depending on the report selected.</p>
Report View	<p>Specify if the report appears in tabular, graphical, or combined form (both).</p> <p>Note This option is not available on every report.</p>
Available data fields / Data fields to include	<p>Use the Add > and < Remove buttons to move the highlighted fields between the Available data fields and Data fields to include columns.</p> <p>Note Fields that appear in blue font in the Data fields to include column are mandatory fields for the report selected in the Custom Report Name field.</p>

Table 32-2 *Report Launch Pad > Report Type > New > Customize Field Descriptions (continued)*

Field	Description
Change order buttons	Use the Move Up and Move Down buttons to determine the order of the columns in the results table. The higher the column heading appears in the Selected Columns list, the farther left it appears in the results table.
Data field sorting	<p>Indicate your sorting preference (Ascending or Descending). Determine how the report data is sorted.</p> <ul style="list-style-type: none"> You can select four data fields for which you can specify sorting order. Use the Sort by and Then by drop-down lists to choose each data field for sorting. For each sorted data field, choose whether you want it sorted in Ascending or Descending order. <p>Note Only reports in table form (rather than graphs or combined) can be sorted. Only fields that can be sorted appear in the Data field sorting drop-down lists.</p> <p>Note The Sortable fields displayed in the Create Custom Report page list all sortable fields irrespective of the data fields that are in the Data fields to include pane. The report is sorted based on the data field selected even if that column is not displayed in the report.</p>

Scheduled Run Results

Table 32-3 describes the fields on the **Report > Scheduled Run Results** page.

Table 32-3 *Scheduled Run Results Field Descriptions*

Field	Description
Report Category	Choose the appropriate report category from the drop-down list or choose All .
Report Type	Choose the appropriate report type from the drop-down list or choose All . The report Type selections change depending on the selected report category.
From / To	Type the report start (From) and end (To) dates in the text boxes or click the calendar icons to select the start and end dates.
Report Generation Method	<p>Choose one of the report generation method from the following options:</p> <ul style="list-style-type: none"> Scheduled On-demand Export On-demand Email

Saved Report Templates

Table 32-4 describes the fields on the **Report > Saved Report Templates** page.

Table 32-4 *Saved Report Templates Field Descriptions*

Field	Description
Report Category	Choose the appropriate report category from the drop-down list or choose All .
Report Type	Choose the appropriate report type from the drop-down list or choose All . The report Type selections change depending on the selected report category.
Scheduled	Choose All , Enabled , Disabled , or Expired to filter the Saved Report Templates list by scheduled status.



INDEX

Numerics

- 802.11b/g/n Parameters Controller Templates [4-45](#)
- 802.11b/g RRM interval template [4-43](#)
- 802.11b/g RRM threshold templates [4-43](#)
- 802.11h template
 - configuring [4-42](#)
- 802.1n scaling reports [29-2](#)
- 802.1X supplicant credentials [4-13](#)

A

- AAA override [31-12](#)
- access control list template [4-34](#)
- access control list templates [4-32](#)
- access point
 - friendly [4-28](#)
- access point configuration templates [4-61](#)
- access point status
 - viewing [4-66](#)
- Account
 - creating [28-3](#)
- ACL IP group details [4-32](#)
- ACL Protocol Groups
 - configuring [4-36](#)
- ACL template [4-34](#)
 - configuring [4-34](#)
- adding
 - users [28-2](#)
- adding a spectrum expert [17-22](#)
- advanced debug [17-4](#)
- Aironet IE [31-15](#)
- alarms

- config audit [17-8](#)
- severity [11-3](#)
- status [11-3](#)
- alarm severity
 - configuring [11-7](#)
- anonymous provisioning [31-28](#)
- applying CLI commands [4-54](#)
- applying config groups [4-69](#)
- AP policies template [4-26](#)
- APs
 - autonomous
 - templates [4-62](#)
 - new [4-62](#)
 - lightweight access point template [4-61](#)
 - AP Username Password Controller Templates [4-13](#)
 - auditing config groups [4-69](#)
 - auto key generation [31-21](#)
 - automatic backups, scheduling [27-12](#)
 - automatic client exclusion [31-15](#)
 - autonomous access point migration templates [4-63](#)
 - Autonomous AP
 - Migration Templates
 - edit [4-64](#)
 - Autonomous APs
 - template [4-62](#)
 - new [4-62](#)
 - templates [4-62](#)

B

- background scanning
 - on mesh configuration [4-51](#)
 - on templates [4-51](#)

bronze [31-13](#)

C

cascade reboot [4-70](#)

Chokepoint

adding to NCS database [17-16](#)

adding to NCS map [17-17](#)

removing from NCS [17-18](#)

removing from NCS map [17-18](#)

Chokepoints

new [17-16](#)

CIDR notation [4-33](#)

Cisco Prime NCS (WAN)

about [1-1](#)

CLI commands

applying to template [4-54](#)

client exclusion [31-15](#)

happening automatically [31-15](#)

concept [17-7](#)

config audit [17-7](#)

config audit alarms [17-8](#)

config group

downloading sw to controllers [4-71](#)

config group audits [4-69](#)

config groups

applying [4-69](#)

auditing [4-69](#)

creating [4-67](#)

downloading customized webauth [4-72](#)

reporting [4-70](#)

Configure NAT for IP Address Conservation [4-80](#)

Configuring

ACL Protocol Groups [4-36](#)

configuring a client exclusion policy template [4-28](#)

configuring a CPU ACL template [4-34](#)

configuring a high throughput template [4-42](#)

configuring a local EAP general template [4-24](#)

configuring a local EAP profile template [4-24](#)

configuring a manually disabled client template [4-31](#)

configuring a mesh template [4-50](#)

configuring an 802.11h template [4-42](#)

configuring an EAP-FAST template [4-25](#)

configuring an RRM interval template [4-43](#)

configuring an RRM threshold template [4-42](#)

configuring a policy name template [4-39](#)

configuring a roaming parameters template [4-41](#)

configuring a TACACS+ server template [4-23](#)

configuring a trusted AP policies template [4-26](#)

configuring a user authentication priority template [4-54](#)

configuring a user login policies template [4-31](#)

configuring autonomous access point migration template [4-64](#)

configuring EDCA parameters

through a template [4-41](#)

configuring FlexConnect AP groups [4-18](#)

configuring search results [30-9](#)

configuring spectrum experts [17-22](#)

configuring template

ACL [4-31](#)

for rogue AP rule groups [4-28](#)

configuring templates

802.11b/g RRM interval [4-43](#)

access point authentication and MFP [4-26](#)

file encryption [4-30](#)

guest users [17-1](#)

known rogue access point [4-42](#)

local management user [4-53](#)

MAC filter [4-31](#)

RADIUS accounting [4-22](#)

RADIUS authentication [4-22](#)

syslog [4-52](#)

Telnet SSH [4-52](#)

traffic stream metrics QoS [4-15](#)

trap control [4-52](#)

WLAN [4-17](#)

Controller Templates

802.11b/g/n Parameters [4-45](#)

AP Username Password [4-13](#)

SNMP Community [4-11](#)

Voice

802.11b/g/n [4-38](#), [4-40](#), [4-46](#)

Creating Account [28-3](#)

Creating a Lobby Ambassador Account [28-3](#)

creating AP configuration templates [4-61](#)

creating autonomous access point migration templates [4-63](#)

customize report [29-3](#)

D

Deploying DMVPN Template [9-1](#)

Deploying GETVPN Template [4-60](#)

DHCP server

overriding [31-17](#)

DMVPN [4-85](#)

DMVPN Template [4-59](#)

downloading sw to controllers

after adding config group [4-71](#)

downstream delay [4-16](#)

downstream packet loss rate [4-16](#)

Dynamic Multipoint VPN [4-85](#)

E

EAP-FAST template [4-25](#)

EDCA parameters

configuring through a template [4-41](#)

Edit View

general [30-9](#)

enable background audit [4-67](#)

enable enforcement [4-67](#)

Ethernet Switch

credentials

remove [17-22](#)

event

severity [11-3](#)

F

failover mechanism [27-5](#)

file encryption template [4-30](#)

FlexConnect

bandwidth restriction [31-14](#)

FlexConnect AP groups

configuring [4-20](#)

FlexConnect configuration tab [31-21](#)

FlexConnect local switching [31-14](#)

friendly access point template [4-28](#)

friendly rogue [4-27](#)

G

generating migration analysis report [17-9](#)

GET VPN Group Member Template [4-59](#)

GET VPN Key Server Template [4-59](#)

gold [31-13](#)

groups

for rogue access point rules [4-28](#)

Guest User

add [28-6](#)

e-mail [28-6](#)

print [28-6](#)

schedule [28-6](#)

guest user templates [17-1](#)

H

high throughput template

configuring [4-42](#)

historical report type [29-1](#)

I

information elements

Aironet [31-15](#)

interface components

- dashlet [30-2](#)
- filters [30-2](#)
- global toolbar [30-1](#)
- quick view [30-5](#)
- sub-menus [30-2](#)
- tables [30-5](#)

interface group [4-15](#)**K**

KEK

- key encryption key [31-23](#)

key wrap [31-23](#)**L**LAG mode [31-3](#)Learn Client IP Address [31-14](#)legacy syslog template [4-52](#)limitations for high availability [27-5](#)

Lobby Ambassador

- account [28-3](#)
- creating account [28-3](#)

Lobby Ambassador Account

- creating [28-3](#)

Local EAP check box [31-12](#)local EAP profile template [4-24](#)local management user template [4-53, 4-54](#)

local switching

- FlexConnect [31-14](#)

Location Server

- logs [27-3](#)

Logout idle user [28-7](#)

LWAPP template

- new [4-61](#)

M

MACK

- message authenticator code keys [31-23](#)

malicious rogue [4-27](#)management interface [31-4](#)

managing

- faults [11-1](#)
- licenses [27-15](#)

managing current reports [29-3](#)Managing Interface [4-78](#)Managing Interfaces [4-84](#)managing saved reports [29-4](#)

manually disabled client

- template for [4-31](#)

mesh template

- configuring [4-50](#)

metrics

- in QoS [4-15](#)

MFP client protection [31-17](#)

migration analysis

- running [17-9](#)

migration analysis report

- generating [17-9](#)

migration analysis summary [4-64](#)

- viewing [4-64](#)

migration template

- copying [4-65](#)

Migration Templates

- Autonomous APs
- edit [4-64](#)

migration templates

- deleting [4-66](#)

Monitor Tags [17-13](#)most recent audit alarms [17-8](#)multiple syslog template [4-53](#)

N

NAT44 Rule [4-81](#)
 NAT Inside and Outside Addresses [4-80](#)
 NAT IP Pools [4-80](#)
 NCS database
 scheduling automatic backups [27-12](#)
 netmask [4-33](#)
 NTP server template [4-11, 4-14](#)

O

Overview of NAT [4-79](#)

P

packet jitter [4-15](#)
 packet latency [4-15](#)
 packet loss [4-15](#)
 packet loss rate [4-16](#)
 passthrough [31-11](#)
 PEAP [31-27](#)
 peer-to-peer blocking [31-15](#)
 platinum [31-13](#)
 PLR [4-16](#)
 Profile
 List [4-73](#)
 Purpose of NAT [4-79](#)

Q

quick search [30-8](#)

R

RADIUS accounting template [4-22](#)
 RADIUS authentication template [4-22](#)
 RADIUS fallback mode [4-23](#)

reachability status [17-22](#)
 recovering the NCS password [27-13](#)
 report
 running new [29-2](#)
 report launch pad [29-2](#)
 reports
 scheduled runs [29-4](#)
 restoring NCS database
 in high availability environment [27-13](#)
 retain NCS value [4-70](#)
 RF Profiles [4-39](#)
 roaming parameters template
 configuring [4-41](#)
 roaming time [4-15, 4-16](#)
 rogue access point rule groups [4-28](#)
 rogue access point rules
 configuring a template [4-26](#)
 rogue location discovery protocol [31-28](#)
 rogue policies
 template for [4-26](#)
 role criteria [4-65](#)
 root mode
 changing from station role [17-9](#)
 RRM interval template
 configuring [4-43](#)
 RRM threshold template
 configuring [4-43](#)
 rules
 for rogue access point [4-26](#)
 running a new report [29-2](#)
 running migration analysis [17-9](#)

S

saved reports
 managing [29-4](#)
 Save Guest Accounts to Device [28-7](#)
 ScanSafe Templates [4-60](#)
 scheduled run results [29-4](#)

silver [31-13](#)

Sniffer [31-59](#)

SNMP authentication [31-47](#)

SNMP Community

- controller templates [4-11](#)

software

- downloading config groups to controllers [4-71](#)

spectrum expert

- adding [17-22](#)

Spectrum Experts

- details [17-23](#)

spectrum experts

- configuring [17-22](#)

station role

- changing to root mode [17-9](#)

Switch

- credentials
- remove [17-22](#)

symmetric mobility tunneling [31-4](#)

syslog templates [4-52, 4-53](#)

T

TACACS+ server

- configuring a template for [4-23](#)

Tags [17-13](#)

Telnet SSH templates [4-52](#)

template

- configuring for rogue AP rules [4-26](#)

total mismatched controllers [17-8](#)

trace [27-3](#)

traffic stream metrics QoS template [4-15](#)

trap control templates [4-52](#)

trap receiver template [4-51](#)

trend report type [29-1](#)

troubleshooting

- using logging options [27-3](#)

troubleshooting access points [21-1](#)

Types of NAT [4-80](#)

U

unclassified rogue [4-27](#)

unjoined access points [21-1](#)

upgrading autonomous access points [4-66](#)

upstream delay [4-16](#)

upstream packet loss rate [4-16](#)

user credential retrieval priority [4-25](#)

user login policies

- configuring a template [4-31](#)

User Preferences [28-7](#)

users

- adding [28-2](#)

Uses of NAT [4-80](#)

using logging

- for troubleshooting [27-3](#)

using template

- ACL [4-34](#)
- for friendly access point [4-28](#)

using templates

- 802.11b/g RRM interval [4-43](#)
- 802.11b/g RRM threshold [4-43](#)
- local management user [4-53, 4-54](#)
- password policy [4-30](#)
- QoS [4-11](#)
- RADIUS accounting [4-22](#)
- syslog [4-52, 4-53](#)
- Telnet SSH [4-52](#)
- traffic stream metrics QoS [4-15](#)
- trap control [4-52](#)
- trap receiver [4-51](#)
- WLAN [4-17](#)

V

viewing the migration analysis [4-64](#)

Voice

- 802.11b/g/n Controller Templates [4-38, 4-40, 4-46](#)

W

WiFi TDOA Receivers

- adding [17-24](#)
- configure [17-23](#)
- tag location [17-23](#)

wIPS

Profile

- add [4-73](#)

Profile List [4-73](#)

wIPS Profile

- apply [4-76](#)
- delete [4-76](#)

wIPS Profiles

- add [4-73](#)

WLAN AP groups [4-18](#)

WLAN templates [4-17](#)

