Cisco Prime Infrastructure 2.0 User Guide

September 2013

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

Text Part Number: OL-27936

Cisco Prime Infrastructure 2.0 User Guide

CONTENTS

PART 2 **Designing the Network**

CHAPTER 22

APPENDIX A

Preface

This guide describes how to 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 *Cisco Prime Infrastructure Documentation Overview* for a list of all Prime Infrastructure documentation.

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

Introduction to Cisco Prime Infrastructure

Cisco Prime Infrastructure is a network management tool that supports lifecycle management of 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; see Global Toolbars, page A-1):

- Lifecycle view—Organized as Home, Design, Deploy, Operate, Report, and Administration, and Workflow menus. This User Guide describes features available in the lifecycle view.
- Classic view—Corresponds closely to the GUI in Cisco Prime Network Control System 1.1 or Cisco Wireless Control System (WCS). The *Cisco Prime Infrastructure Classic View Configuration Guide for Wireless Devices, Release 2.0* describes features available in the classic view.

Prime Infrastructure Organization

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

Caution 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 Operators, and Network Engineers
Design	Design feature or device patterns, or *templates*. 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. You can also design Plug and Play profiles and mobility services.	Network Engineers, Designers, and Architects

Table 1-1 Prime Infrastructure Task Areas (continued)

Task Area	Description	Used By
Deploy	Deploy previously defined designs, or *templates*, 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 includes dashboards, the Device Work Center, the Mobility 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. You can view and approve jobs, specify health rules, and manage licenses. You can also perform software updates and configure high availability.	Network Engineers
Workflows	Use the workflows to: • Use the Plug and Play feature to configure new devices and allow any newly connected Cisco IOS device to quickly be discovered, inventoried, and configured. • Set up switches or Cisco Wireless LAN Controllers after they have been added to Prime Infrastructure.	Network Engineers

Adding Licenses

You must purchase licenses to access the Cisco Prime Infrastructure features required to manage your network. Each license also controls the number of devices that you can manage using those features.

You need a base license and the corresponding feature licenses (such as the assurance or the lifecycle license) to get full access to the respective Prime Infrastructure features to manage a set number of devices.

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.

If you need additional information about licensing, see the following

- *Cisco Prime Infrastructure 2.0 Quick Start Guide*—contains descriptions of the different licenses, how to order licenses, and license entitlement.
- *Cisco Prime Infrastructure 2.0 Administrator Guide*—contains information about managing licenses, troubleshooting licensing issues, and verifying license details.

Adding a License to Access Features

You purchase licenses to access the Prime Infrastructure features required to manage your network. Each license also controls the number of devices or the number of devices on which netflow is enabled that you can manage using those features.

To add a new license, follow these steps:

Step 1 Choose **Administration > Licenses**.

Step 2 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**.

See the *Cisco Prime Infrastructure 2.0 Administrator Guide* for information about managing licenses, deleting licenses, troubleshooting licensing issues, and verifying license details.

Adding Devices to Prime Infrastructure

Before You Add Devices

Before you add devices to Cisco Prime Infrastructure, complete the following tasks:

- Configure the Prime Infrastructure server backup to prevent the loss of any data—See Configuring Server Backups, page 3-1.
- Install any Prime Infrastructure updates—See Installing Software Updates, page 3-2.
- Set up email notifications—See Configuring Email Server Settings to Receive Notifications, page 3-2.

Configuring Server Backups

To prevent the loss of any acquired data, configure a Prime Infrastructure server backup before you add devices.

To configure a server backup:

Step 1 Choose **Administration > Background Tasks > Other Background Tasks > Prime Infrastructure Server Backup**.

Step 2 Use the default repository, *defaultRepo*, or complete the required fields to create an external backup repository, then click **Submit**.

By default, the server is backed up weekly and is stored in the */localdisk/defaultRepo* directory with the filename *hostname-backup_date_time*.tar.gpg. You can also specify a different backup schedule.

Note You can configure SFTP as the *defaultRepo* repository through the CLI, and then select that repository in the user interface for the server backup. For more details, see “Backing Up and Restoring Prime Infrastructure” in the Cisco Prime Infrastructure 2.0 Administrator Guide.

Installing Software Updates

Make sure that you have installed any Prime Infrastructure updates by choosing **Administration > Software Update**. If your Prime Infrastructure server has access to cisco.com, you can view and install any updates. If your Prime Infrastructure server does not have access to Cisco.com, see Downloading Software Updates Without Cisco.com Access, page 3-2.

Step 1 Log in to the Prime Infrastructure server and choose **Administration > Software Update**.

Step 2 Click Check for Updates.

Step 3 Enter your cisco.com credentials and select the software updates you want to install.

You might be prompted to restart the Prime Infrastructure server to complete the update.

Downloading Software Updates Without Cisco.com Access

If your Prime Infrastructure server does not have access to cisco.com, you can download software updates by following these steps:

Step 1 Go to www.cisco.com/go/primeinfrastructure, then under Support, select **Download Software for this Product**, then select the required Cisco Prime Infrastructure version.

Step 2 Save the software update file, which has the file extension UBF.

Step 3 Log in to the Prime Infrastructure server and choose **Administration > Software Update**.

Step 4 Click **Upload Update File** and browse to the location where you saved the software update file.

Step 5 Confirm the name and description.

Step 6 Select the software updates you want to install, then click **Install**.

If required, you might be prompted to stop and restart the Prime Infrastructure server.

Configuring Email Server Settings to Receive Notifications

You can configure mail server settings to specify the email addresses that receive notifications when Prime Infrastructure has completed discovering the devices in your network, as well as notifications of alarms and reports.

To configure discovery email notifications:

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

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

Methods for Adding Devices

You can add devices to Prime Infrastructure in one of the following ways:

- Use an automated process—See Adding Devices Using Discovery, page 3-3.
- Import devices from a CSV file—See Importing Devices from Another Source, page 3-7.
- Add devices manually by entering IP address and device credential information—See Adding Devices Manually, page 3-9.

Adding Devices Using Discovery

When you run discovery, Prime Infrastructure discovers the devices and, after obtaining access, collects device inventory data. We recommend that you run discovery when you are first getting started with Prime Infrastructure.

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.

You can discover your devices by:

- Configuring discovery settings—This method is recommended if you want to specify settings and rerun discovery in the future using the same settings. See Running Discovery, page 3-3.
- Running Quick Discovery—Quick Discovery quickly ping sweeps your network and uses SNMP polling to get details on the devices. See Running Quick Discovery, page 3-6.

Understanding the Discovery Process

Prime Infrastructure performs the following steps during the discovery process:

1. Using ICMP ping, determine if each device is reachable. If Prime Infrastructure is unable to reach the device, the device status is *Unreachable*.
2. Verify the SNMP credentials. If the SNMP credentials are not valid, the device status is *Unreachable*.

   The device status is *Reachable* when Prime Infrastructure can reach the device and has verified that the SNMP credentials are correct.
3. Verify Telnet and SSH credentials.
4. Start the inventory collection process to gather all device information.
5. Add the devices to the Device Work Center.

Running Discovery

Prime Infrastructure discovers devices with IPv4 addresses.

To run discovery:

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

Step 2 Click **New**.

Step 3 Enter the Protocol Settings as described in Table 3-1.

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 3-1 Discovery Protocol Settings

Field	Description
Protocol Settings	
Ping Sweep Module	Prime Infrastructure gets a list of IP address ranges from a specified combination of IP address and subnet mask, then pings each IP address in the range to check the reachability of devices. See Sample IPv4 IP Addresses for Ping Sweep, page 3-6 for more information.
CDP Module	Prime Infrastructure reads the cdpCacheAddress and cdpCacheAddressType MIB objects in the cdpCacheTable from CISCO-CDP-MIB on every newly found device as follows: 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. Check the **Cross Router Boundary** check box to specify that Prime Infrastructure should not discover any neighboring routers.
LLDP	Similar to CDP, but it allows the discovery of non-Cisco devices.
Advanced Protocols	
Routing Table	Queries and analyzes routing tables on seed routers to discover subnets and next-hop routers. This process discovers a router for every subnet on its list of known networks.
Address Resolution Protocol	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 flags processed by the ARP Discovery Module, which are part of the DeviceObject. The entries coming out of the ARP Discovery Module do not need to pass through RTDM because (per the router Discovery algorithm) active routers are those that RTDM must process and identify. When the ARP table is fetched and the entries are not already discovered by RTDM, 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. 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. 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. 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.

Table 3-1 Discovery Protocol Settings (continued)

Field	Description
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 that uses the ospfNbrTable and ospfVirtNbrTable MIBs to find neighbor IP addresses.
Filters	

IP Filter	Includes or excludes devices based on IP address. For example, you can enter any of the following strings and specify whether to include or exclude the devices found during discovery:
	`192.0.2.89`
	`192.0.2.*`
	`192.0.[16-32].89`
	`[192-193].*.55.[16-32]`

Advanced Filters	
System Location Filter	Includes or excludes devices based on System Location.
System Object ID Filter	Includes or excludes devices based on the sysObjectID string set on the device.
DNS Filter	Includes or excludes devices based on the domain name string set on the device.
Credential Settings	
SNMPv2 Credential	SNMP community string is a required parameter for discovering devices in the network using SNMPv2. You can enter multiple rows of credentials mapped to a specific IP address, or the IP address can be a wildcard; for example, *.*.*.*, 10.1.1.*. You cannot save or use the discovery settings if you do not specify SNMP credentials.
Telnet Credential	You can specify the Telnet credentials during discovery so that Prime Infrastructure can collect the device configurations and fully manage the devices. If you do not specify Telnet credentials in the discovery settings, Prime Infrastructure discovers the devices but is unable to manage the device until you specify the Telnet credentials.
SSH Credential	For full device support via SSH, you must use SSHv2 with a 1024 bit key. You can configure SSH before running discovery. **Note** We recommend that you select SSHv2 as the protocol for communicating with the device CLI because it allows the use of Web Services Management Agent (WSMA) for configuring devices. (For more information see, Configuring the Device using WSMA, page 13-1.)
SNMP V3 Credential	Prime Infrastructure supports SNMPv3 discovery for devices. The SNMP V3 modes are: • AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. • NoAuthNoPriv—Uses a user name match for authentication. • PrivType—Protocol used to secure the SNMP authentication request. • PrivPassword—Prefixed privacy passphrase for the SNMPv3 user.
Preferred Management IP (how Prime Infrastructure attempts to find the preferred management address for devices)	

Table 3-1 Discovery Protocol Settings (continued)

Field	Description
Use Loopback IP	Prime Infrastructure uses the preferred management IP address from the loop back interface. If the device does not have a loopback interface, Prime Infrastructure uses similar logic to the OSPF algorithm to select the router's preferred management IP address.
Use SysName	Prime Infrastructure gets the preferred management IP address for the device using DNS lookup of the SysName for the device.
Use DNS Reverse Lookup	Prime Infrastructure gets the preferred management IP address by doing a reverse DNS lookup on the device IP address, followed by a forward DNS lookup.

After running discovery, click **Device Work Center**. See Device Work Center, page 10-4 for more information.

Sample IPv4 IP Addresses for Ping Sweep

Table 3-2 Sample IPv4 Seed IP Addresses for Ping Sweep

Subnet Range	Number of Bits	Number of IP Addresses	Sample Seed IP Address	Start IP Address	End IP Address
255.255.240.0	20	4094	10.104.62.11	10.104.48.1	10.104.63.254
255.255.248.0	21	2046	10.104.62.11	10.104.56.1	10.104.63.254
255.255.252.0	22	1022	10.104.62.11	10.104.60.1	10.104.63.254
255.255.254.0	23	510	10.104.62.11	10.104.62.1	10.104.63.254
255.255.255.0	24	254	10.104.62.11	10.104.62.1	10.104.63.254
255.255.255.128	25	126	10.104.62.11	10.104.62.1	10.104.63.126
255.255.255.192	26	62	10.104.62.11	10.104.62.1	10.104.63.62
255.255.255.224	27	30	10.104.62.11	10.104.62.1	10.104.63.30
255.255.255.240	28	14	10.104.62.11	10.104.62.1	10.104.63.14
255.255.255.248	29	6	10.104.62.11	10.104.62.9	10.104.63.14
255.255.255.252	30	2	10.104.62.11	10.104.62.9	10.104.63.10
255.255.255.254	31	0	10.104.62.11		
255.255.255.255	32	1	10.104.62.11	10.104.62.11	10.104.62.11

Running Quick Discovery

If you want to quickly run discovery without specifying and saving your settings, you can use Quick Discovery.

To run Quick Discovery:

Step 1 Choose **Operate > Discovery**.

Step 2 On the top-right side of the page, click **Quick Discovery**.

Step 3 Complete the required fields, then click **Run Now**.

Verifying Discovery

When discovery has completed, you can verify that the process was successful.

To verify successful discovery:

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 3-1 for information about discovery settings.
- Add devices manually. See Adding Devices Manually for more information.

Importing Devices from Another Source

If you have another management system from which you want to import your devices, or if you want to import a spreadsheet that lists all of your devices and their attributes, you can add device information into Prime Infrastructure as explained in the following steps:

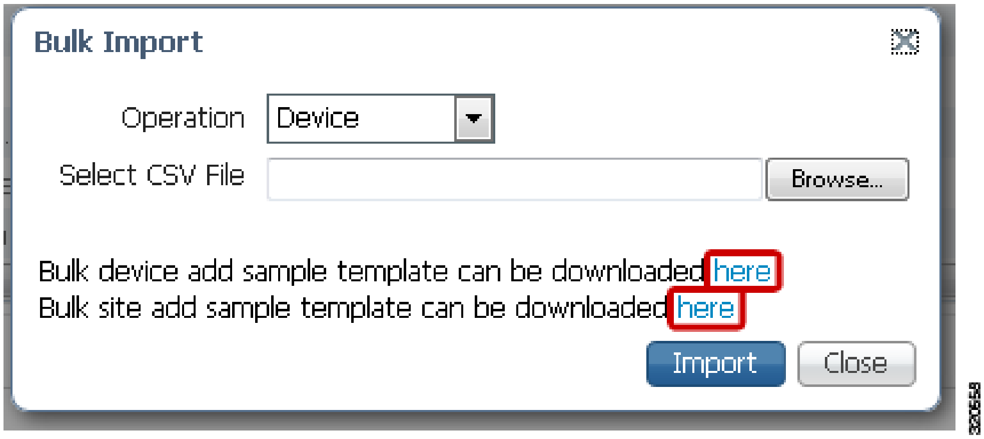
Step 1 Choose **Operate > Device Work Center**, then click **Bulk Import**.

Step 2 From the Operation drop-down menu, choose **Device**.

Step 3 Enter or browse to the CSV file that contains the devices that you want to import.

Step 4 Click the link to download a sample file that contains all of the fields and descriptions for the information that must be contained in your imported file. See Figure 3-1.

Figure 3-1 Downloading a Sample Template for Importing Devices or Sites



Bulk Import

Operation Device

Select CSV File

Bulk device add sample template can be downloaded here

Bulk site add sample template can be downloaded here

Make sure that you retain the required information in the CSV file as explained in CSV File Requirements for Importing Devices, page 3-8.

Step 5 Click **Import**.

Step 6 Check the status of the import by choosing **Administration > Jobs Dashboard**.

Step 7 Click the arrow to expand the job details and view the details and history for the import job.

Note If the importing CSV file contains any UDF parameters, ensure that UDF is configured in **Administration > System Settings > User Defined Field** prior to importing the devices. The UDF column in the CSV file must be begin with **UDF:** as indicated in the sample CSV template.

CSV File Requirements for Importing Devices

If you want to use a CSV file to import your devices or sites from another source into Prime Infrastructure, you can download a sample template by choosing **Operate > Device Work Center**, then clicking **Bulk Import**. Click the link to download a sample template as shown in Figure 3-1.

When you download a sample CSV template for importing devices or sites, the extent to which Prime Infrastructure can manage your devices depends on the information you provide in the CSV file. If you do not provide values for CLI user name, password, and enable password, Prime Infrastructure will have limited functionality and cannot modify device configurations, update device software images, and perform many other valuable functions.

- For Prime Infrastructure to *partially* manage your devices, you must provide the following values in the CSV file:
  - Device IP address
  - SNMP version
  - SNMP read-only community strings
  - SNMP retry value
  - SNMP timeout value

- For Prime Infrastructure to *fully* manage your devices, you must provide the following values in the CSV file:
  - Device IP address
  - SNMP version
  - SNMP read-only community strings
  - SNMP retry value
  - SNMP timeout value
  - Protocol

    You must also provide values for the fields that correspond to the protocol you specify. For example, if you specify SNMPv3, you must specify values for the SNMPv3 fields in the sample CSV file such as the SNMPv3 user name and authorization password.
  - CLI user name
  - CLI password
  - CLI enable password
  - CLI timeout value

Adding Devices Manually

Adding devices manually is helpful if you want to add a single device. If you want to add all devices in your network, we recommend that you run discovery (see Running Discovery) or import devices from a CSV file (see Importing Devices from Another Source, page 3-7).

To add devices manually:

Step 1 Choose **Operate > Device Work Center**, then click **Add**.

Step 2 Complete the fields, then click **Add** to add the device with the settings you specified.

Note User Defined Field (UDF) parameters are available only if you added them under **Administration > System Settings > User Defined Field**. Do not use the special characters : ; and # for UDF field parameters.

Validating That Devices Were Added Successfully

After collecting device information, Prime Infrastructure gathers and displays the configurations and the software images for the devices. To verify that your devices were successfully added to Prime Infrastructure, you can:

- Choose **Operate > Device Work Center** and verify that the devices you added appear in the list. Hover your mouse over the Inventory Collection Status field and click the icon that appears to view details about the information that was collected for the device. Click a device name to view the device configurations and the software images that Prime Infrastructure collected from the devices.

  Table 3-3 describes the possible Admin Status values.

- Choose **Administration > Jobs Dashboard**, then click the arrow to expand the job details and view the details and history for the import job.

See Troubleshooting Unmanaged Devices, page 12-4 for information about how to resolve any errors.

Table 3-3 Descriptions of Device Admin Status

Admin Status	Description
Managed	The inventory collection completed successfully and Prime Infrastructure is managing the device.
Unmanaged	You have exceeded the number of devices allowed by your license. Choose **Administration > Licenses** to view the status of your license. See the *Cisco Prime Infrastructure 2.0 Administrator Guide* for information about managing licenses, troubleshooting licensing issues, and verifying license details.

Verifying Device Credentials

In Prime infrastructure, whenever you are adding/editing the device, device credential verification will happen automatically as part of inventory collection and the report can be viewed at **Report > Report Launch Pad > Device > Device Credential Verification**.

Adding NAM HTTP/HTTPS Credentials

If you are using Cisco Network Analysis Modules (NAMs) to monitor your network, you must add HTTPS 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 these steps 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 that you have 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**.

Exporting Devices

In Prime Infrastructure, you can export device information as a CSV file.

To export devices:

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

Step 2 Select devices and click **Export Device**.

Step 3 Enter an encryption password that will be used to open the exported CSV file.

Step 4 Confirm the encryption Password and click **Export** to export the device information.

Step 5 Double click the ExportDevice.zip file and enter the encryption password to open the ExportDevice.csv file.

Next Steps

Now that you have added devices to Prime Infrastructure, you can create device groups and port groups to simplify management, monitoring, and configuration of similar devices and ports. See Grouping Devices and Ports.

You might also want to:

- Plan for devices that will be added to your network in the future—See Preconfiguring Devices to be Added Later, page 6-1.
- Configure wired and wireless features on your devices using guided, step-by-step instructions—See Getting Help Setting Up Access Switches, page 6-6.

CHAPTER 4

Grouping Devices and Ports

After you add devices to Cisco Prime Infrastructure, you can organize the devices into logical groupings to simplify management, monitoring, and configuration. When you group devices, you can perform operations on the entire group instead of selecting individual devices.

Grouping Devices by Device Type

You can group similar devices together to simplify management and configuration tasks. Depending on your needs, device groups can be based on location, device type, device role, and so on.

A device group that you create can be one of two types:

- Static—Create and name a new device group to which you can add devices using the Add to Group button from **Operate > Device Work Center > Create Group**.
- Dynamic—Create and name a new device group and specify the rules to which devices must comply before they are added to this device group. You do not add devices to dynamic groups. Prime Infrastructure adds devices that match the specified rules to the dynamic group.

To create a device group:

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

Step 2 In the Device Group menu on the left, click ⚙▾, then choose **Create Group**.

Step 3 Enter the name, description, and parent group if applicable.

Step 4 Select one of the following for the new device group:

- Static—You add devices to the group based on your needs.
- Dynamic—You specify the rules to which devices must comply before they are added to this device group. You do not add devices to dynamic groups. Prime Infrastructure adds devices that match the specified rules to the dynamic group

Step 5 Click **Save**.

The device group that you created appears under the User Defined folder.

Step 6 If you created a static group, select the devices to add to the group by choosing **Groups & Sites** > **Add To Group**, then choose the device group from the Select Group list and click **Save**.

Note You do not add devices to dynamic groups. Prime Infrastructure adds devices that match the specified rules to the dynamic group.

Creating Groups of Ports

Creating a port group helps you simplify monitoring and configuration tasks. For example, you might want to create a port group that contains all WAN ports so that you can more easily monitor these key ports. By default, port groups are based on interface type.

A port group that you create can be one of two types:

- Static—Create and name a new port group to which you can add interfaces using the Add to Group button from **Design > Management Tools > Port Grouping**.
- Dynamic—Create and name a new port group and specify the rules to which ports or interfaces must comply before they can be added to this port group.

Note While there is no limit on the number of rules that you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

To create a port group:

Step 1 Choose **Design > Management Tools > Port Grouping**.

Step 2 In the Port Groups menu on the left, click ⚙▾, then choose **Create Group**.

Step 3 Enter the name, description, and parent group if applicable.

Step 4 Select whether the group is static or dynamic:

- Static—You add ports to the group based on your needs.
- Dynamic—You specify the rules to which ports must comply before they are added to this port group. You do not add ports to dynamic groups. Prime Infrastructure adds ports that match the specified rules to the dynamic group.

Step 5 Click the ports you want to add to the port group, click **Add to Group**, then choose the port group from the Select Group list and click **Save**.

Note You do not add ports to dynamic groups. Prime Infrastructure adds ports that match the specified rules to the dynamic group.

Creating Customized Port Groups

You can create a customized, user-defined port group that contains devices or interfaces on which you want to apply configuration changes in one operation.

Step 1 Choose **Design > Management Tools > Port Grouping**.

Step 2 From the Port Groups frame on the left, click ⚙▾, then select **Create Group**.

Leave the default Parent Group field as **User Defined**.

Step 3 Enter a group name and description, then select whether the group is static or dynamic:

- Static—You add ports to the group based on your needs.
- Dynamic—You specify the rules to which ports must comply before they are added to this port group. You do not add ports to dynamic groups. Prime Infrastructure adds ports that match the specified rules to the dynamic group.

The port group you created appears under the User Defined folder.

Step 4 If you created a static port group, add the ports to the group by clicking **Add to Group**, selecting the port group from the Select Group list and clicking **Save**.

Note You do not add ports to dynamic groups. Prime Infrastructure adds ports that match the specified rules to the dynamic group.

Deleting a Port Group

Caution If you are deleting a static port group, make sure that it does not contain any subgroups or members. If you are deleting a dynamic port group, make sure that it does not contain any subgroups; however, the dynamic group can be associated with members.

To delete a port group:

Step 1 Choose **Design > Management Tools > Port Grouping**.

Step 2 Hover your mouse on the name of the name of the port group that you want to delete, then click **Delete Group**.

Grouping Devices by Site

You can group devices by site, or location, to help you manage your network by associating network elements with your organization's physical locations or physical segmentation. They allow you to segment the physical structure of your network, and to monitor and troubleshoot your network based on site 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 and the size and height of any floor, and you can associate images (including photographs and drawings) of these areas with your specifications. For information about the format, version, size, and resolution of the images that you import into Prime Infrastructure, see the "Recommended Parameters for Images" section on page 4-5. 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 been previously created, you can add devices to the site by clicking **Add to Site** from the Device Work Center.

Creating Sites

You can create sites by:

- Automatically creating a site tree map based on the hostname—See "Using Automatic Hierarchy to Create Maps" in the *Cisco Prime Infrastructure Classic View Configuration Guide for Wireless Devices*.
- Importing existing map data—See Importing Site Map Data.
- Using a site map.

Step 1 Choose **Design > Management Tools > Site Map Design**.

Step 2 Choose **Select a command > New Campus/Site** or **New Building**, then click **Go**.

Step 3 Complete the required fields, then click **OK**. See Importing Site Map Data, page 4-4 for information about importing site map information.

Importing Site Map Data

You can import site map information into Prime Infrastructure.Table 4-1 lists the supported format types.

Step 1 Choose **Design > Management Tools > Site Map Design** or **Operate > Maps**.

Step 2 From the Go menu, choose **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**.

Table 4-1 Import Site Map Formats

Format	Description
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).

Related Topic

Recommended Parameters for Images

Recommended Parameters for Images

Images can be in a variety of formats and there are many parameters embedded as metadata in an image. These parameters impact the appearance of the image. The following recommended parameters ensure that images appear clearly:

- Image resolution—For higher zoom, use an image that has at least one dimension (X or Y) exceeding 4096. For example, (4096 x 2160), (3072 x 8192), or (15360 x 25600). Higher the image resolution, more will be the zoom levels. Lower image resolution can provide only 3 zoom levels. There are no restrictions on the supported image resolution. For example, 100 Mega Pixel and 1 Giga Pixel. Image resolutions that are higher than 1 Giga Pixel are also accepted depending on the memory availability.

  Note Files with lower resolution that are used by existing maps can provide 3 or 4 zoom levels depending on the dimensions.

- File formats—The supported file formats are PNG, GIF or JPG.
- RGB settings—Images must have the color space set to RGB. These images must be in eight bit depth or higher. Otherwise, they will appear black on the floor.
- Gamma settings—The black and white images with gamma settings set to maximum and after tile cutting, will appear black on the floor. Such issues cannot be auto-corrected because the images will loose resolution and boundaries. These images must be opened in an image editor and the RGB color space must be added. You may also need to adjust the white balance depending on the image histogram and convert the image to eight bit or higher.
- CAD file format must be AutoCAD version 2010 or earlier. Before you save a CAD file, ensure the following:
  - Zoom images to maximum.
  - Remove unwanted layers from the CAD files, that is, layers that add unnecessary artifacts to CAD files and layers that do not provide significant information about the image on the CAD files.

Associating Endpoints with a Site

Endpoint-Site association rules allow you to associate all of the devices on particular subnet to a site, or location, 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 sites, enabling troubleshooting using Prime Infrastructure's multi-segment analysis features.

Note You can specify multiple rules for the same subnet, allowing you to (for example) specify multiple monitoring data sources or VLANs.

To associate endpoints with a site:

Step 1 Choose **Design > Management Tools > Endpoint-Site Association**.

Step 2 Click **Add Row** to add an Endpoint-Site association rule.

Step 3 Complete the fields as required. See Table 4-2 for field descriptions.

Step 4 Click **Save**.

Table 4-2 Endpoint-Site Association Fields

Field	Description
Site	Select an existing campus to associate with this subnet.
Subnet	Enter the routing prefix (and optional Data Source and VLAN) of the subnetwork to be associated with this site. 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.

Creating Customized Groups

You create your own logical grouping of devices 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 that you created to push the configuration change to all of the devices contained in the group.

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 a device group by hovering your mouse cursor on the device group folder.

You can create a new group that can be one of two types:

- Static—Add devices to a static group using the **Add to Group** button from **Operate > Device Work Center**.
- Dynamic—Specify the rules to which devices must comply to be added to this device group. See Creating Dynamic Device Groups, page 4-7 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.

Device 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, page 4-7.
2. Assign devices to the device group. See Assigning Devices to a Static Group, page 4-8.

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 that 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 a 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.

Creating Dynamic Device Groups

Before you create a dynamic device group, make sure that 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 to the number of rules that 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 ⚙▾, then click **Create Group**.

Step 3 Enter the group name and group description, and select a parent group, if applicable.

Step 4 Select **Dynamic Group** so that you can specify the rules to which all devices must comply to be added to the group. (If you select Static Group, you must assign the devices to the group. Static groups are not rule-based.)

Step 5 Specify the rules that you want to apply to the devices in the group.

Note You can create a rule using the UDF labels defined in **Administration > System Settings > User Defined Field**.

Step 6 Click **Save** to add the device group with the settings you specified.

The device group that you created appears under the user-defined groups.

Assigning Devices to a Static Group

If you created a Static Group, you must assign the devices to the group. Static groups are not rule-based

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

Step 2 Select the device that you want to assign to a group, then click **Add To Group**.

Step 3 Select a group, then click **Save**.

Hiding Empty Groups

A device or port group might be empty if:

- You created a static group and have not added devices to the group.
- You created a dynamic group in which no devices matched the rules you specified for the dynamic group.

By default, Prime Infrastructure displays empty groups. If you do not want to display empty groups, choose **Administration > System Settings > Grouping**, then deselect **Display empty groups**.

Setting Up Network Monitoring

After you add devices to the Cisco Prime Infrastructure inventory and set up device and port groups, you need to set up your devices to allow Prime Infrastructure to monitor the devices.

- Specifying Which Interfaces and Ports to Monitor, page 5-1

You can also configure Prime Infrastructure to monitor more advanced information:

- Getting Enhanced Client Information by Integrating with ISE, page 5-3
- Setting Up Assurance for Performance Monitoring, page 5-4

Specifying Which Interfaces and Ports to Monitor

You create monitoring templates to 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 (see Dashboards and Dashlets, page A-2), and reports.

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

When you create a port group, you must determine which types of ports you want to monitor. The following port groups are typical of most networks:

- Port Type
- User Defined
- WAN Interfaces

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

Setting Up WAN Interface Monitoring

Creating a WAN interface port group allows you to efficiently configure settings on all WAN interfaces in a specific port group. For example, a small branch office might have a problem where the WAN bandwidth is as low as 1.544 Mb/s, and a round trip latency of 300 ms. To watch the WAN bandwidth used by this branch, you set up the interface from the router that connects to the ISP as a WAN interface.

The following procedure shows you how to:

1. Create a port group for the WAN interfaces.
2. Create and deploy a WAN interface health monitoring template on those ports.
3. Verify the utilization and availability of the WAN interfaces from the Site dashboard.

Step 1 To create the port group:

a. Choose **Design > Management Tools > Port Grouping**.

b. Choose the device IP addresses that you know are WAN interfaces and that you want to add to the port group, then choose **Add to Group > Select Group > WAN Interfaces**.

Step 2 To create and deploy a WAN interface health monitoring template:

a. Choose **Design > Configuration > Monitor Configuration.**

b. In the Templates menu on the left, click **Features > Metrics > Interface Health**.

c. Complete the basic template fields, select the attributes that you want to monitor (for example, Interface Availability, ifInErrors, ifOutErrors, inputUtilization, and outputUtilization), then click **Save as New Template**.

d. Choose **Deploy > Configuration Deployment > Monitoring Deployment**.

e. From the Templates menu on the left, click **My Templates**.

f. Select the new template, choose **Deploy > Port Groups > WAN Interfaces,** and click **Submit.**

Step 3 Display the results:

a. Choose **Home > Detail Dashboards > Sites >** ⚙▾ **> Add Dashlets**.

b. Select either of the following:

   – **Top N WAN Interfaces by Utilization**

   – **Top N WAN Interfaces with Issues**

Getting Enhanced Client Information by Integrating with ISE

You can get enhanced information about managed clients using the Cisco Identify Services Engine (ISE) or ACS View servers.

Adding an Identity Services Engine

A maximum of two ISEs can be added toPrime Infrastructure. If you add two ISEs, one should be primary and the other should be standby. When you are adding a standalone node, you can add only one standalone node and cannot add a second node.

To add an Identity Services Engine, follow these steps:

Step 1 Choose **Design > Management Tools > External Management Servers > ISE Servers**.

Step 2 From the Select a command drop-down list, choose **Add Identity Services Engine**.

Step 3 Complete the required fields, then click **Save**.

Note The credentials should be superuser credentials. Otherwise, ISE integration does not work.

Configuring ACS View Servers

If you do not have ISE, you can integrate your Cisco Secure Access Control ACS View server with Prime Infrastructure. To access the ACS View Server tab, you must add a view server with credentials.

Note Prime Infrastructure supports only ACS View Server 5.1 or later.

To configure an ACS View Server, 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 Cisco WLC controller.

Step 5 Specify the number of retries to be attempted.

Step 6 Click **Save**.

Setting Up Assurance for Performance Monitoring

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

Enabling NAM Data Collection

To ensure that you can collect 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 the same time.

Before You Begin

You must specify the HTTP/HTTPS credentials for each NAM (see Adding NAM HTTP/HTTPS Credentials, page 3-10).

Step 1 Choose **Administration > System Settings > Data Sources.**

Step 2 In the **NAM Data Collector** section, select all of the NAMs for which you want to enable data collection.

Step 3 Click **Enable**.

Enabling NetFlow Data Collection

To start collecting NetFlow and Flexible NetFlow data, you must configure your NetFlow-enabled switches, routers, and other devices (ISR/ASR) to export this data to Prime Infrastructure. The following table shows the various device types that support NetFlow and the ways to configure devices to export NetFlow data to Prime Infrastructure.

Table 5-1 NetFlow Support Summary

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
Catalyst 3750-X / 3560-X	15.0(1)SE IP base or IP services feature set and equipped with the network services module.	TCP and UDP traffic	See Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches, page 5-6.
Catalyst 3850	15.0(1)EX	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches, page 5-6. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
Catalyst 4500	15.0(1)XO and 15.0(2)	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches, page 5-6. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
Catalyst 6500	SG15.1(1)SY	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches, page 5-6. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
ISR	15.1(3) T	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI > Collecting Traffic Statistics** To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**

Table 5-1 NetFlow Support Summary (continued)

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
ISR G2	15.2(1) T and 15.1(4)M	TCP and UDP traffic, application response time, Voice and Video	To configure TCP, UDP, and ART, see Configuring NetFlow on ISR Devices, page 5-8. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
ISR G2	15.2(4) M2 or later, 15.3(1)T or later	TCP and UDP traffic, application response time, Voice and Video	To configure TCP, UDP, and ART, see Configuring Application Visibility, page 13-2.
ASR	15.3(1)S1 or later	TCP and UDP traffic, application response time, Voice & Video, HTTP URL visibility	
ISR G3	15.3(2)S or later		

Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches

To manually configure NetFlow to export TCP and UDP traffic on Catalyst 3000, 4000, or 6000 devices, use the following steps to create a user-defined CLI template:

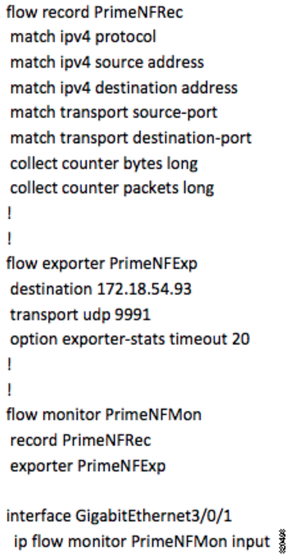
Step 1 Choose **Design > Feature Design > CLI Templates > CLI**, hover your mouse cursor over the information icon and click **New**.

Step 2 Provide a name for the template (for example, Prime_NF_CFG_CAT3K_4K).

Step 3 From the Device Type list, choose **Switches and Hubs**.

Step 4 In the **Template Detail > CLI Content** text box, enter the following commands, modifying them for your network:

Figure 5-1 Catalyst 3000, 4000, and 6000 CLI Commands



```
flow record PrimeNFRec
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
!
flow exporter PrimeNFExp
 destination 172.18.54.93
 transport udp 9991
 option exporter-stats timeout 20
!
!
flow monitor PrimeNFMon
 record PrimeNFRec
 exporter PrimeNFExp

interface GigabitEthernet3/0/1
  ip flow monitor PrimeNFMon input
```

Step 5 Choose **Deploy > Configuration Tasks** to save and deploy the template to the relevant devices**.**

Configuring NetFlow on ISR Devices

To manually configure NetFlow to export MACE traffic on an ISR device, use the following steps to create a user-defined CLI template:

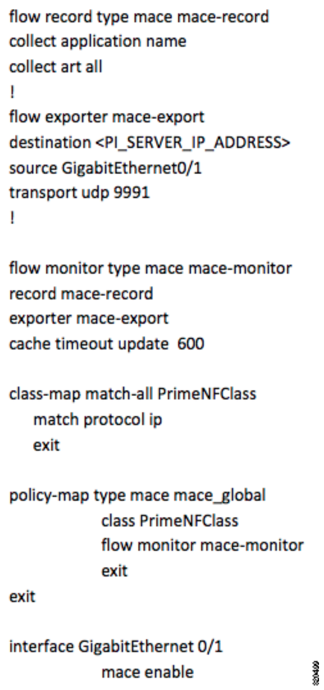
Step 1 Choose **Design > Feature Design > CLI Templates > CLI**, hover your mouse cursor over the information icon and click **New**.

Step 2 Provide a name for the template (for example, Prime_NF_CFG_MACE).

Step 3 From the Device Type list, choose **Routers**.

Step 4 In the **Template Detail > CLI Content** text box, enter the following commands, modifying them for your network:

Figure 5-2 ISR MACE CLI Commands



```
flow record type mace mace-record
collect application name
collect art all
!
flow exporter mace-export
destination <PI_SERVER_IP_ADDRESS>
source GigabitEthernet0/1
transport udp 9991
!

flow monitor type mace mace-monitor
record mace-record
exporter mace-export
cache timeout update  600

class-map match-all PrimeNFClass
   match protocol ip
   exit

policy-map type mace mace_global
            class PrimeNFClass
            flow monitor mace-monitor
            exit
exit

interface GigabitEthernet 0/1
            mace enable
```

Step 5 Choose **Deploy > Configuration Tasks** to save and deploy the template to the relevant devices.

CHAPTER 6

Getting Help Setting Up and Configuring Devices

Cisco Prime Infrastructure provides step-by-step guidance for the following tasks:

- Preconfiguring devices that will be added to your network in the future—See Preconfiguring Devices to be Added Later, page 6-1.
- Setting up access switches after they have been added to Prime Infrastructure—See Getting Help Setting Up Access Switches, page 6-6.

Preconfiguring Devices to be Added Later

You can preconfigure devices that will be added to your network in the future. For example, if you are going to be adding a new branch office, you can use the Plug and Play Setup workflow to create an initial configuration for the branch router and switches. When the new device is added to your network, Prime Infrastructure can quickly discover, inventory, and configure the new device based on settings that you specify in a Plug and Play profile.

Note The **Workflow** menu appears for users with the following privileges only: root, super users, and Config Managers.

When you choose **Workflows > Plug and Play Setup**, Prime Infrastructure guides you through creating a Plug and Play profile that creates a bootstrap configuration file, which creates a bootstrap configuration file and another *config* file that includes Telnet and SSH credentials, to allow new Cisco IOS devices to "call home" to Prime Infrastructure to get further configurations. Using the Plug and Play Setup Workflow eliminates the need to "console" into each device to set it up before it can be managed by Prime Infrastructure.

The Plug and Play Setup workflow is similar in functionality to **Design > Plug and Play Profiles** and **Deploy > Plug and Play Profiles**; however, the workflow, designed more for access switches than routers, provides more guidance to set up new devices.

Note The Plug and Play Setup workflow is most helpful in setting up and configuring Cisco IOS switches and access devices. Cisco IOS devices that support auto DHCP install options can be booted up using the Plug and Play Setup workflow. All other devices (for example, routers that do not have direct network connectivity in the branch, legacy controllers, and APs) must use the Plug and Play feature explained in Automating Device Deployment, page 9-2.

You need to complete the Plug and Play Setup only *once*. After you complete the steps, when a new switch or access device is connected to the network, the device automatically uses the Plug and Play profile, boots up, and then Prime Infrastructure begins managing the device.

Related Topic

- Prerequisites, page 6-3

Supported Devices and Software Images for Plug and Play Setup Workflow

Table 6-1 lists the devices and corresponding software images supported for Workflows > Plug and Play Setup.

Table 6-1 Supported Devices and Image Versions for Workflows > Plug and Play Setup

Supported Devices for Plug and Play	Minimum Software Image Version Supported	Verified Image Version
Catalyst 2960, 2960S	Cisco IOS Release 12.2(55)SE and later	Cisco IOS Release 12.2(55)SE5 and later
Catalyst 2960C	Cisco IOS Release 12.2.55(EX) and later	Cisco IOS Release 12.2.55(EX3) and later
Catalyst 2960-SF	Cisco IOS Release 15.0(2)SE and later	Cisco IOS Release 15.0(2)SE and later
Catalyst 3560V2, 3750v2, 3560-X, 3750-X	Cisco IOS Release 12.2(55)SE and later	Cisco IOS Release 12.2(55)SE and later
Catalyst 3560C	Cisco IOS Release 12.2.55(EX) and later	Cisco IOS Release 12.2.55(EX) and later
Catalyst 4503, 4506, 4507, and 4510 switches and 4000 Series supervisor cards supported: Sup 6E, Sup 6LE	Cisco IOS Release 151-2.SG and later	Cisco IOS Release 151-2.SG and later
Catalyst 4503, 4506, 4507, and 4510 switches and 4000 Series supervisor cards supported: Sup 7E, Sup 7LE (IOS XE)	Cisco IOS XE Release 03.04.00.SG and later	Cisco IOS XE Release 03.04.00.SG and later
Catalyst 3850 switches (IOS XE)	Cisco IOS XE Release 03.02.02.SE and later	Cisco IOS XE Release 03.02.02.SE and later
Cisco 5760 Wireless LAN Controllers (IOS XE)	Cisco IOS XE Release 03.02.02.SE and later	Cisco IOS XE Release 03.02.02.SE and later

Prerequisites

Based on the method that you select to deliver the Plug and Play profile to new devices, you must make sure that you have completed the necessary prerequisites.

- Configure DHCP with the appropriate settings in the network as described in Sample DHCP Server Settings for Auto Install, page 6-3. If DHCP is not available in the network, you can use a different method to apply the bootstrap configuration to your new devices as explained in Sample DHCP Server Settings for Auto Install, page 6-3.
- You must have an existing network connection (distribution/core) available in the branch or campus to where the new device is connecting.
- The branch must have direct connectivity to the Prime Infrastructure server, or you must use the Plug and Play external server to connect to Prime Infrastructure.
- Ensure TFTP is enabled on the PI server by choosing **Administration > System Settings > Server Settings**, then clicking **Enable** under TFTP. TFTP is enabled by default.

Sample DHCP Server Settings for Auto Install

If you select the DHCP-based auto install method to deliver the Plug and Play Profile, you must configure the DHCP server to redirect the switch to the TFTP server by entering the commands described in Table 6-2.

The DHCP-based auto install method follows these steps:

1. The new switch contacts the DHCP server. You must configure the DHCP server to redirect the switch to the TFTP server. See Table 6-2 for more information.
2. The DCHP server points the switch to the new TFTP server where the Plug and Play bootstrap profile resides.
3. The switch loads the bootstrap configuration file, boots up, and then contacts the Plug and Play Gateway.

:

Table 6-2 DHCP Server Settings for Auto Install

Command to Enter	Description
`ip dhcp pool PNP`	Creates a DHCP pool named PNP.
`network 10.106.190.0 255.255.255.224`	Defines the network 10.106.190.0 and subnet mask 255.255.255.224. DHCP uses this pool of IP addresses to assign an IP address to the new device.
`default-router 10.106.190.17`	Configures the default route 10.106.190.17 on the new device.
`option 150 ip 10.77.240.224`	Specifies that the TFTP server IP address 10.77.240.224 is the Prime Infrastructure server IP address.

Getting the Configuration to New Devices

You can choose how to get the bootstrap configuration that is created during the Plug and Play Setup workflow to your new devices:

- **DHCP Auto Install**—If you select the DHCP-based auto install method to deliver the Plug and Play Profile, you must have a distribution network or a network that already has an existing connection to your corporate network. See Sample DHCP Server Settings for Auto Install, page 6-3.
- **Prime Utilities**—If you select the Prime Utilities method to deliver the Plug and Play Profile, after connecting the new devices to the distribution layer, you must use the laptop utility to download the configuration from Prime Infrastructure and apply the configuration to the devices. You must have internet connectivity to the Prime Infrastructure server.
- **File Transfer**—If you select the File Transfer method to deliver the Plug and Play Profile, you can download the TXT file and manually apply the configuration to the devices.

Specifying Device Credentials

The **Workflows > Plug and Play Setup > Create Profile** window is where you provide SNMP, Telnet, and SSH credentials that will be configured on the devices. Prime Infrastructure uses these credentials to contact the devices. By default, Telnet is enabled, but you can enable SSH if applicable.

The following configurations are set by the Plug and Play profile, but you can modify them using the Getting Help Setting Up Access Switches workflow:

- SNMPv2 and SSH Credentials—The SNMP, Telnet, and SSH credentials you specify will be configured on *all* devices that use the Plug and Play profile. You can consider these temporary credentials necessary to allow Prime Infrastructure to contact the devices. You can use the Getting Help Setting Up Access Switches workflow later to modify the device credentials. You can enable Telnet, SSH, or both. If you specify SSH, ensure the device has the K9 image.

  For security purposes, we recommend that do not use “public” or “private” for your community strings.
- Plug and Play Gateway Location—By default, the Prime Infrastructure server acts as the Plug and Play gateway server. You can modify the server by providing the external Plug and Play gateway IP address.

Saving the Plug and Play Profile

As explained in Sample DHCP Server Settings for Auto Install, page 6-3, make sure that you have satisfied the necessary requirements before you specify how you want to deploy or export the Plug and Play profile.

- **Deploy via TFTP**—The profile remains active on the TFTP server and whenever a new switch or access device is connected to the network, the device will automatically use the Plug and Play profile, boot up, and then "call home" to Prime Infrastructure for additional configuration.
- **Email to other operators**—You can email the bootstrap configuration file to an appropriate network engineer who can provision the bootstrap configuration manually to the device, or email the PIN to an appropriate network operator who can use the Prime Infrastructure iPad or laptop utility to provision the configurations on the devices.

Note If you are going to use email to deliver either the bootstrap configuration or the PIN, you must have previously configured the mail server settings under **Administration > System Settings > Mail Server Configuration**.

- Export the bootstrap configuration file (in TXT format) that was created and then manually apply the bootstrap configuration to the devices.

After you save the Plug and Play Profile, the Workflow Status menu at the bottom of the Prime Infrastructure interface refreshes to reflect newly registered devices and any devices on which the workflow failed.

Now that your devices will be able to contact the Prime Infrastructure server, you can specify further configurations that can be applied to the devices. See Getting Help Setting Up Access Switches, page 6-6.

Sample Output from Plug and Play Setup

When you complete the steps in **Workflows > Plug and Play Setup**, Prime Infrastructure creates a bootstrap configuration file, which includes the following commands to allow new Cisco IOS devices to "call home" to Prime Infrastructure.

In the following example, *pi2-pod1-171* is the Prime Infrastructure server hostname.

```
ip host pi2-pod1-171 192.168.138.171

cns trusted-server all-agents pi2-pod1-171

cns id hardware-serial

cns id hardware-serial event

cns id hardware-serial image

cns even pi2-pod1-171 11013 keepalive 120 2 reconnect0time 60

cns exec 80

cns image server http://pi2-pod1-171/cns/HttpMsgDispatcher status
http://pi2-pod1-171/cns/HttpMsgDispatcher

cns config partial pi2-pod1-171 80

cns config initial pi2-pod1-171 80
```

In addition to the bootstrap configuration file, another config file is created in the TFTP location which provisions the credentials you provided on the Create Profile page.

The bootstrap configuration file is delivered based on the method you specified:

- **Deploy via TFTP**—Prime Infrastructure copies the bootstrap configuration file, *cisconet.cfg*, and and the *config* credentials file to the Prime Infrastructure TFTP server.
- **Email to other operators**—Prime Infrastructure emails the bootstrap configuration file to the specified email address and copies the *config* credentials file to the Prime Infrastructure TFTP server.

Note If you are going to use email to deliver either the bootstrap configuration or the PIN, you must have previously configured the mail server settings under **Administration > System Settings > Mail Server Configuration**.

- **Export the bootstrap configuration file**—Prime Infrastructure exports the bootstrap configuration file to the client and saves it as *Day-0 Bootstrap Configuration_NEW.txt* and copies the *config* credentials file to the Prime Infrastructure TFTP server.

Verifying Plug and Play Provisioning Status

When a supported device uses the Plug and Play profile to connect to Prime Infrastructure, the device is listed in the Workflow Status window (in the Newly Registered Device column) at the bottom of the Prime Infrastructure interface. You can click a number displayed in the Workflow Status window to go directly to the Assign to Site step in the Getting Help Setting Up Access Switches workflow, which allows you to create more robust configurations for the devices.

If a device takes longer than 10 minutes to synchronize, it is not listed under the Newly Registered Device column in the Workflow Status window. However, the device is listed in the Initial Device Setup workflow with a status of N/A.

Getting Help Setting Up Access Switches

After your devices are added to Prime Infrastructure, you can use the Initial Device Setup workflow to help you configure wired and wireless features on the following devices:

- Supported devices for **wired** features: See Table 6-1.
- Supported devices for **wireless** features:
  - Catalyst 3850 switches
  - Cisco 5760 Wireless LAN Controllers

Related Topics

- Before You Begin, page 6-7
- Assign Devices to Sites

Before You Begin

You must create sites before you use the Initial Device Setup by choosing **Design > Site Map Design**. See Creating Sites for more information.

Related Topic

- Assign Devices to Sites, page 6-7

Assign Devices to Sites

The **Workflows > Initial Device Setup > Assign to Site** window allows you to specify a site to which the devices you want to configure belong. *Unassigned* devices discovered using the Plug and Play Setup workflow (see Preconfiguring Devices to be Added Later, page 6-1) and any discovered devices that were not previously assigned are listed on this window. You must assign each device to a site.

The Initial Device Setup workflow is site-specific. To configure devices in a different site, you repeat the Initial Device Setup workflow and select that appropriate site.

To get details about any device, hover your mouse cursor over a device IP address, then click the icon that appears. See Getting Device Details from the Device 360° View, page A-12 for more information.

If the Status column for any device is *N/A*, either the device was manually added to Prime Infrastructure (without using the Plug and Play Setup workflow), or the Plug and Play Setup workflow completed, but the synchronization took longer than 10 minutes after the device was added to Prime Infrastructure.

Choose Devices

The **Workflows > Initial Device Setup > Choose Other Devices** window displays all new devices you assigned to the specified site, any devices previously assigned to the same site, and any devices that were added to Prime Infrastructure using discovery. This allows you to configure wired and wireless features on new and existing devices at the same time.

Choose whether you want to configure wired or wireless features. The devices displayed correspond to the option you select.

If you select **Add wired features to my device(s)**, only applicable devices in the selected site on which you can configure wired features are displayed. After you select the devices, check the Device Readiness column and see Device Readiness Explanation, page 6-8 for more information.

Choose a configuration mode:

- **Guided mode**—Gives you step-by-step guidance in creating Cisco-recommended device configurations. See Configuring Wired Features Using Guided Mode.
- **Advanced mode**—Uses templates in which you can modify and customize the device configurations. You should be comfortable with CLI templates. See Configuring Wired Features Using Advanced Mode.

If you select **Add wireless features to my device(s)**, applicable devices in the selected site on which you can configure wireless features are displayed. After you select the devices, you can choose to configure guest access as part of the wireless device configuration. Enter the number of access points that you want to deploy and select a mobility domain.

Device Readiness Explanation

The Readiness column indicates whether the devices you selected are ready to be configured. A device can be "not ready" for the following reasons:

- The device is not running the required Cisco IOS version. Table 6-3 lists the required versions.
- Prime Infrastructure was unable to collect inventory details. Choose **Operate > Device Work Center** and make sure the Admin Status for the device is *Managed* and the Inventory Collection Status is *Completed*.

Table 6-3 Required Cisco IOS/IOS XE Releases for Switches to Be in Ready State

Switch Series	Required Cisco IOS/IOS XE Releases
Catalyst 2960, 2960s	12.2(55) and later, or 15.0.1.SE and later
Catalyst 2960-SF	15.0(2)SE and later
Catalyst 3560v2, 3560X, 3750v2, 3750X	12.2(55) and later, or 15.0.1.SE and later
Catalyst 3560c, 2960c	12.2(55)-EX4 and later
Catalyst 3850	IOS XE 03.02.01 SE and later
Catalyst 4500	When running Sup7E and Sup7LE: IOS XE 03.03.02.SG and later When running Sup6E or Sup6LE: 12.2(54)SG and later
5760 Wireless LAN Controller	IOS XE 03.02.01 SE and later

Related Topics

- Configuring Wired Features Using Guided Mode, page 6-8
- Configuring Wired Features Using Advanced Mode, page 6-10
- Configuring Wireless Features, page 6-11

Configuring Wired Features Using Guided Mode

When you choose to configure wired features using the Guided Mode, you are guided step-by-step through configuring the following settings:

1. IP Address Options, page 6-8
2. Device Credentials, page 6-9
3. VLAN and Switching Parameters, page 6-9
4. Auto Smartports and Uplinks, page 6-9
5. Confirmation, page 6-10

IP Address Options

During the **Workflows > Plug and Play Setup** workflow (see Preconfiguring Devices to be Added Later, page 6-1), the DHCP server assigned IP addresses to the devices. The IP Management Options page is where you can modify the IP addresses. Select **Change Device(s) IP Management Address**, enter the necessary values for the device(s) in the Device Management Option table, then click **Save**.

You can edit IP address, hostname, subnet, and gateway values only; you cannot modify the device type and serial number.

If you have a large number of devices, you can simplify this task by exporting a CSV file of all devices, editing the file, then importing the CSV file to overwrite the Device Management Option table.

Device Credentials

During the **Workflows > Plug and Play Setup** workflow (see Preconfiguring Devices to be Added Later, page 6-1), the same SNMP, Telnet and SSH credentials you specified were be configured on *all* devices. The Credentials page is where you can modify the credentials and specify different credentials for various devices. Select **Specify new credentials** and enter the necessary values.

Click **Save Credentials** to save the credentials you entered. When you have new devices that you want to set up and you use the Initial Device Setup workflow again, you can select the credentials that you saved from the **Use Credentials** list. The fields are populated with the values that you previously saved.

When you complete the Initial Device Setup workflow, the device credentials are updated on the devices and in Prime Infrastructure.

VLAN and Switching Parameters

The VLAN and Switching page allows you to configure VLANs and switching parameters. Default VLAN values are provided. Default switching features are selected. The following options are enabled by default and you cannot modify them because they are required by Prime Infrastructure:

- Enable CDP
- Rapid PVST

By default, Spanning Tree is also enabled.

Auto Smartports and Uplinks

By default, the Initial Device Setup workflow enables Cisco Auto Smartports and quality of service (QoS) on switch downlink ports. Auto Smartport macros dynamically configure ports based on the device type detected on the port. You cannot disable Auto Smartports.

The Before You Begin page includes a link to download the supported devices for uplink configuration.

We recommend that you enable uplink-specific features such as EtherChannel and Trunking by selecting one of the options from the pulldown menu:

- Enable Layer 2 Trunking
- Enable Layer 2 Trunking with Etherchannel (PagP)
- Enable Layer 2 Trunking with Etherchannel (LACP)
- Enable Layer 2 Trunking with Etherchannel (Static)

Confirmation

The Confirmation screen is the last step in the Initial Device Setup workflow in which you can view the settings you specified. Click **Deploy** to deploy the configuration. A job is created and the job status information is displayed.

To view the deployed jobs, choose **Administration > Jobs Dashboard** to view the status and details about the job.

If the deployment fails, the number of devices on which the deployment failed appears in the Failed column of the Workflow Status menu at the bottom of the Prime Infrastructure interface. Click the number displayed to go directly to the Choose Other Devices screen to view the device(s) that failed. You can modify necessary settings and repeat the workflow for that device.

Configuring Wired Features Using Advanced Mode

If you want to customize the configuration settings applied to your devices, select **Advanced mode** in The Choose Other Devices page. The Advanced mode uses templates in which you can modify and customize the device configurations. You should be comfortable with CLI templates.

You use the following templates to specify configuration settings:

- System—Allows you to specify new IP addresses to replace the IP addresses that were previously assigned by the DHCP server. You can edit IP address, hostname, subnet, and gateway values only; you cannot modify the device type and serial number.

  If you have many devices, it might be easier to edit these values in a spreadsheet. You can export the list of devices as a CSV file, edit the file, and then import the file to overwrite the table.

- Security—Allows you to specify authentication credentials. Whatever you select as the authentication type, your primary authentication server must match. For example, if you select RADIUS as the authentication method, the primary authentication method must be RADIUS. If you select None as the authentication type, your primary authentication method must be LOCAL. The secondary and other methods can be any authentication type.
- Layer 2—Allows you to configure Spanning Tree, VTP, LLDP, and CDP. By default, Rapid PVST and CDP are enabled because they are required by Prime Infrastructure.
- High Availability—Allows you to configure power and system redundancy. If the High Availability check box is unchecked, redundancy is disabled on the device.
- Interfaces—Allows you to configure VLANs. You can check how many ports your devices have and based on that information, you can split the interfaces into interface patterns.
- Other—Allows you to configure any other commands in the terminal configuration mode.

Configuring Wireless Features

When you choose to configure wireless features, you are guided step-by-step through configuring the following settings:

1. Create Groups, page 6-11
2. Wireless Parameters, page 6-11
3. Wireless LAN Security, page 6-11
4. Guest Access, page 6-11
5. Confirmation, page 6-11

Create Groups

The Create Groups page is where the Mobility Architecture group is automatically defined for the wireless devices that you selected in the Choose Other Devices page. The Mobility Group consists of Mobility Controller, Switch Peer Group, and Mobility Agents. You cannot modify the Mobility Controller and the Mobility Agent that were previously configured. Whereas, you can add Switch Peer Groups.

Wireless Parameters

The Wireless Parameters page allows you to assign **Wireless Management IP**, **Mask**, and **Wireless VLAN ID** for the selected wireless devices. You can also choose to export the list of devices as a CSV file, edit the values, and import the file to overwrite the values for the devices. Then, click **Save**.

Wireless LAN Security

The Wireless LAN Security page allows you to add secure wireless for LAN connectivity. Default values are displayed for the Secure wireless LAN Properties. Based on the security profile and the authentication method that you choose, you must enter the primary and secondary Radius server details.

Guest Access

The Guest Access page is displayed only if you have chosen to configure guest access as part of the wireless device configuration in the Choose Other Devices page. Default values are displayed for the guest WLAN and VLAN fields. Based on the security profile and the authentication method that you select for your guest, you must enter the primary and secondary Radius server details.

Confirmation

The Confirmation page is the last step in the Guided workflow for wireless features in which you can view the settings you specified. Click **Deploy** to deploy the configuration. For more information about the confirmation job status and the workflow status, see the "Confirmation" section on page 6-10.

PART 2

Designing the Network

Planning Your Network Design

Cisco 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.

Types of Configurations

It is important to plan for the following configurations:

- Feature configurations—Identify the features that you want to configure on a given device. You can use a composite template that includes multiple feature templates to define a complete device configuration.
- Device role configurations—Identify your devices and the roles they play. For example, you will want to design templates for routers that function as branch routers, and other templates for routers that function as WAN edge routers. You will also 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.
- Site configurations—Identify the various sites in your network and the different configurations that could be required in 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—While planning your configuration design, consider what relevant information that you want to monitor. For example, you will want to ensure that the features you configured are being monitored. You can define or *design* monitoring templates that dictate how and what to monitor. After you deploy the monitoring templates, the results are displayed in dashboards, dashlets (see Dashboards and Dashlets, page A-2), and reports.

Guidelines for Planning Your Network Design

Consider the following factors 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 one or two 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, then create a composite template that contains these templates.

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

Planning Template Deployments

After you design your network, use the Deploy menu to reuse and deploy the designs you have created. You can deploy feature templates, composite templates, profiles, and so on. You need to determine answers to the following questions before deploying objects:

- What are you deploying? Determine whether you are deploying a configuration template, plug and play profile, etc.
- Where is it being deployed? Determine which devices should be included in the deployment.
- 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 configuration values.

Template Workflow for Switches

The following steps take you through a sample workflow for creating and deploying templates for switches:

1. Create templates for your switches, which can include:
   - *Feature-level* configuration templates (see Creating Feature-Level Configuration Templates, page 8-2)
   - A *monitoring template* that monitors important features that you configured in the configuration templates (see Creating Monitoring Templates, page 8-12)
   - A *composite template* that includes all the templates you want to deploy on the switches in your network (see Creating Composite Templates, page 8-18)
2. Create a 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 the templates, and create a deployment profile that includes:
   - Device profile
   - Deployment target
   - Deployment-specific configuration information

Reusable Policy Objects

To improve efficiency and accuracy in your configuration templates, you can create shared policy objects to include in your configuration templates. You create interface roles or network objects that you can add to your configuration templates.

Interface roles allow you to define policies to specific interfaces on multiple devices without having to manually define the names of each interface. Interface roles can refer to any of the actual interfaces on the device, including physical interfaces, subinterfaces, and virtual interfaces such as loopback interfaces.

If you create an all-Ethernets interface role, you can define identical advanced settings for every Ethernet interface on the device with a single definition. You add this interface role to a configuration template, then deploy the template to the selected devices to configure the Ethernet interfaces.

Interface roles are especially useful when applying policies to new devices. As long as the devices that you are adding share the same interface naming scheme as existing devices, you can quickly deploy the necessary configuration template containing the interface role to the new devices.

Network objects are logical collections of IP addresses that represent networks. Network objects make it easier to manage policies. When you create a network object and include it in a configuration template,

For information about the shared policy objects, see Creating Shared Policy Objects, page 8-20.

Template Testing

Before you roll out a template to a large number of devices, you will want to make sure it is correct and that no further adjustments or modifications are needed. After you create a template, deploy it to a single device to test and troubleshoot your design. You should plan for and schedule full deployment of a composite template.

CHAPTER 8

Designing Device Configurations

You can use Cisco Prime Infrastructure configuration templates to design the set of device configurations that you need to set up 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 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. 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.

Creating Feature-Level Configuration Templates

Prime Infrastructure provides the following types of feature-level configuration templates:

- Features and technologies templates—Configurations that are specific to a feature or technology in a device's configuration. See Creating Features and Technologies Templates, page 8-2.
- 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 the Cisco Prime LAN Management System. See Updating Passwords, page 8-10.
- 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, page 8-18.

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

Creating and Deploying Feature-Level Configuration Templates

To create and deploy a feature-level configuration template, follow these steps:

Step 1 Choose **Design > Configuration**, choose the type of template, and complete the required fields. For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 2 Navigate to the My Templates folder, choose the template that you want to deploy, then click the **Publish** icon to publish the template.

After you publish a configuration task template, you can specify devices, values, and scheduling information to tailor your deployment (see Deploying and Monitoring Configuration Tasks, page 9-2).

Step 3 Click **Deploy** to deploy the template.

Step 4 To verify the status of the template deployment, choose **Administration > Jobs Dashboard**.

Creating Features and Technologies Templates

Features and Technologies templates are templates that are based on device configuration and that 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. Prime Infrastructure does not support every configurable option for all device types. If Prime Infrastructure does not have a Features and Technologies template for the specific feature or parameter that you want to configure, create a CLI template (see Creating CLI Configuration Templates, page 8-4).

Features and Technologies templates simplify the deployment of configuration changes. For example, you can create an SNMP Features and Technologies template and then quickly deploy it to devices you specify. You can also add this SNMP template to a composite template (see Creating Composite Templates, page 8-18). Then later, when you update the SNMP template, the composite template in which the SNMP template is contained automatically has your latest changes.

To create a Features and Technologies template, follow these steps:

Step 1 Choose **Design > Configuration > Feature Design.**

Step 2 In the Features and Technologies menu on the left, choose a template type to create.

Step 3 Complete the fields for that template.

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. 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.

For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 4 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Step 5 To verify the status of a template deployment, choose **Administration > Jobs Dashboard**.

Creating CLI Templates

CLI is a set of re-usable device configuration commands with the ability to parameterize select elements of the configuration as well as add control logic statements. This template is used to generate a device deployable configuration by replacing the parameterized elements (variables) with actual values and evaluating the control logic statements.

This section includes the following topics:

Prerequisites for Creating CLI Templates

Before you create a CLI template, you must:

- 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.

- To know how to use variables and data types, see the "Variables and Data Types" section on page 8-4.

Creating CLI Configuration Templates

Use templates to define device parameters and settings, which you can later deploy to a specified number of devices based on device type.

Before You Begin

Make sure you have satisfied the prerequisites (see Prerequisites for Creating CLI Templates, page 8-3).

Step 1 Choose **Design > Configuration > Feature Design**.

Step 2 Expand the **CLI Templates** folder, then click **CLI**.

Step 3 Enter the required information.

a. In the OS Version field, you can specify an OS image version so that you can filter out devices older than the one you specified.

a. In the Template Detail section, click the **Manage Variables** icon (above the CLI Content field).

This allows you to specify a variable for which you will define a value when you deploy the template.

b. Click **Add Row** and enter the parameters for the new variable (see the "Variables and Data Types" section on page 8-4), then click **Save**.

c. Enter the CLI information. In the CLI field, you must enter code using Apache VTL (see http://velocity.apache.org/engine/devel/vtl-reference-guide.html). For more information about different CLI command formats, see:

- Adding Multi-line Commands, page 8-7
- Adding Enable Mode Commands, page 8-7
- Adding Interactive Commands, page 8-7

d. (Optional) To change the variables, click **Form View** (a read-only view), click the **Manage Variables** icon, then make your changes (see the "Variables and Data Types" section on page 8-4).

Step 4 Click **Save As New Template**.

Step 5 Click **Publish** to publish the template, click **Deploy** and specify the deployment options (see Creating and Deploying Feature-Level Configuration Templates, page 8-2), then click **OK**.

Step 6 To verify the status of a template deployment, choose **Administration > Jobs Dashboard**.

Note To duplicate a CLI template, expand the **System Templates - CLI**, hover your mouse cursor over the quick view picker icon next to CLI, and then click **Duplicate**. using the and Save as new template

Variables and Data Types

You can use variables as placeholders to store values. The variables have names and data types. Table 8-1 lists data types that you can configure in the Manage Variables page.

Table 8-1 Data Types

Data Type	Description
String	Enables you to create a text box for CLI template. To specify a validation expression and a default value, click the Expand icon and configure the Default Value and Validation Expression fields.
Integer	Enables you to create a text box that accepts only numeric value. If you want to specify a range for the integer, click the Expand icon and configure the Range From and To fields. To specify a validation expression and a default value, click the Expand icon and configure the Default Value and Validation Expression fields.
DB	Enables you to specify a database type. See the "Managing Database Variables in CLI Templates" section on page 8-5.
IPv4 Address	Enables you to create a text box that accepts only IPv4 address for CLI template. To specify a validation expression and a default value, click the Expand icon and configure the Default Value and Validation Expression fields.
Drop-down	Enables you to create a list box for CLI template. To specify a validation expression and a default value, click the Expand icon and configure the Default Value field (with comma separated value for multiple list which appears in the UI).
Check box	Enables you to create a check box for CLI template. To specify a validation expression and a default value, click the Expand icon and configure the Default Value field.
Radio Button	Enables you to create a radio button for CLI template. To specify a validation expression and a default value, click the Expand icon and configure the Default Value field.
Text Area	Enables you to create a text area which allows multiline values for CLI template. To specify a validation expression and a default value, click the Expand icon and configure the Default Value and Validation Expression fields.

Managing Database Variables in CLI Templates

You can use database (DB) variables for the following reasons:

- DB variable is one of the data types in CLI templates. You can create DB variables to find the exact device and generate the accurate commands.
- DB variables are pre-defined variables. All other variables are user-defined variables.
- To view the pre-defined DB variables go to the following path.

```
Cd/opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate
```

Note You can find the CLITemplateDbVariablesQuery.properties file inside the InventoryTagsInTemplate folder that contains the list of pre-defined DB variables.

- For example, SysObjectID, IPAddress, ProductSeries, ImageVersion are DB variables.When a device is added in to Prime Infrastructure, the complete details of the device is collected in the DB variables. That is, OID of the devices is collected in SysObjeectID, product series in ProductSeries, image versions of the device in ImageVersion and so on.
- Using the data collected by the DB variables, accurate commands can be generated to the device.
- You can select the DB variable in the Type field (using the Managed Variables page). Expand the name field and fill-in default value field with any of the DB variables which you want to use.
- 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, create a CLI template that contains the following commands:

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

where *$interfaceNameList* is the database variable type whose value will be retrieved from the database. *$interfaceNameList* has a default value of `IntfName`. You need to create the interfaceNameList variable as DB data type (using the managed variable dialog box) and add set the default to `IntfName`. If you have not specified a default value, you can specify it when you deploy the CLI template.

To populate *interfaceNameList* with the value from the database, you must create a properties file to capture the query string and save it in the /opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate folder. This is a sample of a property file called interface.properties:

```
# for interface name tag->Name
IntfName=select name from EthernetProtocolEndpoint u where owningEntityId =
```

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 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.

Using Validation Expression

The values that you define in the Validation Expression are validated with the associated component value at deploy flow. For example, if you enter a default value and a validation expression value in the design flow, this will be validated during the deploy flow. That is, if the default value does not match with the entered value in the validation expression, you will encounter an get error at design flow.

Note The validation expression value works only for the string data type field.

Example:

Choose CLI > Manage Variables > Add Row. Choose string data type and then click the expand icon and configure the regular expression which will not allow a space in that text box.

Enter the following expression in the validating expression field.

```
^[\S]+$
```

Default value (optional)—ncs

The value should match with regular expression in validation expression field.)

Result:

Save the template, click Deploy, and then select a device. Try to enter a space in the text field. You will encounter a regular expression error.

Adding Multi-line Commands

To enter multi-line commands in the CLI Content area, use the following syntax:

```
<MLTCMD>First Line of Multiline Command
Second Line of Multiline Command
......
......
Last Line of Multiline Command</MLTCMD>
```

where:

- <MLTCMD> and </MLTCMD> tags are case-sensitive and must be entered as uppercase.
- The multi-line commands must be inserted between the <MLTCMD> and </MLTCMD> tags.
- Do not start this tag with a space.
- Do not use <MLTCMD> and </MLTCMD> in a single line.

Example 1:

```
<MLTCMD>banner_motd ~ Welcome to
Cisco. You are using
Multi-line commands.
~</MLTCMD>
```

Example 2:

```
<MLTCMD>banner motd ~ ${message}
~</MLTCMD>
```

where “message” is a multi-line input variable.

Adding Enable Mode Commands

Use this syntax to add enable mode commands to your CLI templates:

```
#MODE_ENABLE
<<commands >>
#MODE_END_ENABLE
```

Adding Interactive Commands

An interactive command contains the input that must be entered following the execution of a command.

To enter an interactive command in the CLI Content area, use the following syntax:

```
CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question
2<R>command response 2
```

where <IQ> and <R> tag are case-sensitive and must be entered as uppercase.

For example:

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Combining Interactive Enable Mode Commands

Use this syntax to combine interactive Enable Mode commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

For example:

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>XXX
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Adding Interactive Multiline Commands

This is an example of an interactive command that contains multiple lines:

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
@</MLTCMD>
#ENDS_INTERACTIVE
```

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 > Feature Design**.

Step 2 Expand the **CLI Template** folder, 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 and click **Manage Variables** (the icon above the CLI Content field).

You can use this same procedure to edit an existing variable created from copied code.

Step 5 Fill out the required information, then click **Save > Add**.

Step 6 To view the new variable, click **Form View**.

Exporting a CLI Configuration Template

If you have CLI templates in any other Prime Infrastructure server, you can export them as an XML file and import them into your current Prime Infrastructure server.

Step 1 Choose **Design > Configuration > Feature Design**.

Step 2 Expand the **CLI Template** folder, then click **System Templates - CLI**.

Step 3 Select the template(s) that you want to export.

Step 4 Click the **Export** icon at the top right of the CLI template page.

Importing a CLI Configuration Template

Step 1 Choose **Design > Configuration > Feature Design**.

Step 2 Expand the **CLI Template** folder, then hover your mouse cursor over the quick view picker icon next to **CLI**.

Step 3 Click **Show All Templates**.

Step 4 Click the **Import** icon at the top right of the CLI template page.

Step 5 Click **Select Templates** to navigate to your file, then click **OK**.

Exporting CLI Variables

You can export the CLI variables into a CSV file while deploying a CLI configuration template. You can use the CSV file to make necessary changes in the variable configuration and import it into Prime Infrastructure at a later time.

Step 1 Choose **Deploy > Configuration Tasks**.

Step 2 Expand the **CLI Template**.

Step 3 Select the template that you want to deploy.

Step 4 Select the device whose variables you want to export.

Step 5 Click the **Export** icon at the top right of the CLI template page.

Step 6 Click **OK**.

Importing CLI Variables

Step 1 Choose **Deploy > Configuration Tasks**.

Step 2 Expand the **CLI Template**.

Step 3 Select the template that you want to deploy.

Step 4 Select the device to which you want to import variables.

Step 5 Click the **Import** icon at the top right of the CLI template page.

Step 6 Click **OK**.

Updating Passwords

To comply with SoX (Sound eXchange, a free cross-platform digital audio editor), you might want to update the password for the network devices once every six months. To make the changes in a rolling fashion, you plan to perform the operation once for two regions every three months.

In this example, there are four custom dynamic groups, one for each region based on the cities in every region: North Region, South Region, East Region, and West Region. You must update the enable password for all of the devices in the north and south region. After this is complete, you plan to set another job to occur for the West and East region devices to occur three months later.

Before You Begin

The devices in these regions must have an assigned location attribute.

Step 1 If the four groups, North Region, South Region, East Region, and West Region, have not been created:

a. Choose **Operate > Device Work Center**, then mouse-over **User Defined** and choose **Add SubGroup.**

b. In the Create Sub-Group area, enter:

- Group Name: `North Region`

- Group Description: `List of devices in the north region`
- Filter: **Location > Contains >** `SJC-N`

  To determine the location of a device, choose **Operate > Device Work Center > (gear icon) > Columns > Location.**

  The devices for the new group appear under Device Work Center > User Defined > North.

c. Do the same for south, east, and west regions.

Step 2 To deploy the password template:

a. Choose **Deploy > Configuration Tasks > CLI Templates > System Templates-CLI**.

b. Select the **Enable Password-IOS** template and click **Deploy**.

c. In the Device Selection area, open the User Defined groups and select the **North Region** and **South Region** groups.

d. In the Value Selection area, enter and confirm the new enable password, then click **Apply**.

e. In the Schedule area, enter a name for the job, the date and time to deploy the new template (or click **Now**), then click **OK**.

Step 3 After the job has run, choose **Administration > Jobs Dashboard** to view the status of the job (see Monitoring Jobs, page 10-6).

Tagging Templates

You can label a set of templates by providing an intuitive name to tag the templates. Tagging a configuration template helps you:

- Search a template using the tag name in the search field
- Use the tagged template as a reference to configure more devices
- Publish the tagged template and make it ready for deployment

Tagging a New Configuration Template

To tag a new configuration template and publish the tagged template, follow these steps:

Step 1 Choose **Design > Configuration > Feature Design.**

Step 2 Expand the Features and Technologies folder, choose an appropriate subfolder, and then choose a template type.

Step 3 Complete the required fields, enter a tag name in the **Tags** field, then click **Save as New Template**.

Step 4 Click **Publish** to publish the template, click **Deploy** and specify the deployment options (see Creating and Deploying Feature-Level Configuration Templates, page 8-2), then click **OK**.

Tagging an Existing Template

To tag an existing template, follow these steps:

Step 1 Choose **Design > Configuration > Feature Design.**

Step 2 In the Features and Technologies menu on the left, expand the **My Templates** folder and choose the template you want to update.

Step 3 Enter a tag name in the **Tag as** field, then click **Save**.

Step 4 Click **Publish** to publish the template, click **Deploy** and specify the deployment options (see Creating and Deploying Feature-Level Configuration Templates, page 8-2), then click **OK**.

Associating a Tag With Multiple Templates

You can tag a new tag name or associate an existing tag with multiple templates.

Step 1 Choose **Design > Configuration > Feature Design.**

Step 2 Click the Tag icon drop-down arrow on the navigation toolbar of the Templates column.

Step 3 Enter a tag name in the **Tag as** field.

Step 4 In the My Templates folder, click the templates that are to be associated with the tag.

To associate all of the templates in the folder with the tag, select the box beside the My Templates folder.

Then click **Apply.**

Creating Monitoring Templates

Prime Infrastructure provides several types of monitoring templates.

- Metrics—Use monitoring templates to enable Prime Infrastructure to monitor network device metrics and alert you of changing conditions before the issues impact their operation (see Monitoring Network Device Metrics, page 8-13). For an example of how to create a template that collects metrics, see Example: Creating Health Monitoring Templates, page 8-13.
- NetFlow—You can monitor the different types of NetFlow traffic (see Monitoring NetFlow Traffic, page 8-13).
- Thresholds—Use monitoring templates to define thresholds (see Defining Thresholds, page 8-14). When the thresholds that you specify are reached, Prime Infrastructure issues an alarm. For examples of how to create various types of thresholds, see:
  - Defining Alarm Thresholds, page 11-5
  - Example: Defining Health Monitoring Thresholds, page 8-14

Monitoring Network Device Metrics

Use monitoring templates to monitor network device metrics and alert you of changing conditions before the issues impact their operation.

Step 1 Choose **Design > Configuration > Monitor Configuration**.

Step 2 Expand the Features menu on the left and choose **Metrics**, then click one of the types of metrics.

Step 3 Complete the required fields, click **Save**, then click **Save As New Template**.

Step 4 You can now deploy the template (see Deploying Monitor Configuration Templates, page 8-17).

Example: Creating Health Monitoring Templates

You can 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 they impact operations.

To create a health monitoring template, follow these steps:

Step 1 Choose **Design > Configuration > Monitor Configuration**.

Step 2 Expand the Features menu on the left and choose **Metrics**; then click **Device Health** or **Interface Health**.

Step 3 Complete the required fields. For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide.*

Step 4 Choose **Interface Health > Metric Parameters** and select the parameters you want to monitor. To modify a parameter setting, click the parameter name, description, or polling frequency value and change the field, then click **Save**.

Step 5 Click **Save as New Template**, then deploy the template (see Deploying Monitor Configuration Templates, page 8-17).

Monitoring NetFlow Traffic

Use NetFlow monitoring templates to monitor NetFlow traffic.

Step 1 Choose **Design > Configuration > Monitor Configuration**.

Step 2 Expand the Features menu on the left and choose **NetFlow**, then click one of the types of NetFlow traffic.

Step 3 Complete the required fields, click **Save**, then click **Save As New Template**.

Step 4 You can now deploy the template (see Deploying Monitor Configuration Templates, page 8-17).

Defining Thresholds

Use monitoring templates to define thresholds. When the thresholds you specify are reached, Prime Infrastructure issues an alarm.

Step 1 Choose **Design > Configuration > Monitor Configuration**.

Step 2 Expand the Features menu on the left and choose **Threshold**.

Step 3 Complete the basic template fields.

Step 4 Under the Feature Category, choose one of the available metrics.

Step 5 Under Metric Parameters, choose the threshold setting that you want to change, then click **Edit Threshold Setting**. Enter a new value, choose the alarm severity when the threshold is met or exceeded, and click **Done**.

Step 6 Click **Save as New Template**.

Step 7 You can now deploy the template (see Deploying Monitor Configuration Templates, page 8-17).

Example: Defining Health Monitoring Thresholds

Use monitoring templates to define thresholds. When the thresholds you specify are reached, Prime Infrastructure issues an alarm.

Before You Begin

Before you can define health-monitoring threshold values:

1. Choose **Design > Monitoring Configuration** > **Features** > **Metrics**.
2. Create an Interface Health Monitoring template.

To define monitoring thresholds, follow these steps:

Step 1 Choose **Design > Configuration > Monitor Configuration**.

Step 2 Expand the Features menu on the left and choose **Threshold**.

Step 3 Complete the required fields. For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 4 In the Metric Parameters area, select the parameter for the threshold that 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; if you are using a default template, all available parameters are displayed.

Step 5 Enter a new value and choose the alarm severity for the threshold, then click **Done**.

Step 6 Click **Save as New Template**, then deploy the template (see Deploying Monitor Configuration Templates, page 8-17).

Table 8-2 Monitoring Template Threshold Parameters

Field	Description
Feature Category	Choose one of the available metrics. In this example, choose either: • 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.
Template Instance	Select a default template or a previously created template. **Note** If there is no default template for the Feature Category you selected, then before you can define threshold values you must create the necessary template under **Design > Configuration > Monitor Configuration** > **Features** > **Metrics**.
Type	Select the type of metric. This list is auto-populated based on the selected Feature Category.

Health Monitoring Template Metrics

Prime Infrastructure polls SNMP objects to gather monitoring information for the following health monitoring templates under **Design > Configuration > Monitor Configuration** > **Features** > **Metrics**:

- Device Health—Table 8-3 describes the device health parameters that are polled.
- Interface Health—Table 8-4 describes the interface parameters that are polled.
- Class Based Quality of Service—Table 8-5 describes the QoS parameters that are 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 8-3 Device Health Monitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
Device Availability	All SNMP devices	SNMPv2-MIB	sysUpTime
CPU Utilization	Cisco IOS devices, Cisco Nexus 7000 Series	CISCO-PROCESS-MIB	cpmCPUTotalPhysicalIndex cpmCPUTotal1minRev

Table 8-3 Device Health Monitoring Metrics (continued)

Metric	Devices Polled	MIB	MIB Objects Included
Memory Pool Utilization	Cisco IOS devices	CISCO-MEMORY-POOL-MIB ciscoMemoryPoolUsed / (ciscoMemoryPoolUsed + ciscoMemoryPoolFree)) * 100	ciscoMemoryPoolName ciscoMemoryPoolType ciscoMemoryPoolUsed ciscoMemoryPoolFree
	Cisco Nexus 7000 Series	CISCO-MEMORY-POOL-MIB (cempMemPoolUsed / (cempMemPoolUsed + cempMemPoolFree)) * 100	
Env Temp	ASR, Cisco Nexus 7000 Series	CISCO-ENVMON-MIB	entSensorValue
	Catalyst 2000, 3000, 4000, 6000, ISR	CISCO-ENVMON-MIB	ciscoEnvMonTemperatureStatusValue
Largest Free Buffer Percentage	Cisco IOS devices	CISCO-MEMORY-POOL-MIB	ciscoMemoryPoolLargestFree ciscoMemoryPoolFree
Total Number of Buffer Misses	Cisco IOS devices	OLD-CISCO-MEMORY-MIB	bufferSmHit, bufferMdHit, bufferBgHit, bufferLgHit, bufferHgHit, bufferSmMiss, bufferMdMiss, bufferBgMiss, bufferLgMiss, bufferHgMiss

Table 8-4 Interface Health Monitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
Interface Availability	Cisco IOS devices, Cisco Nexus 7000 Series	IF-MIB	ifOperStatus ifOutOctets ifHighSpeed ifInOctets if InErrors ifOutErrors ifInDiscards ifOutDiscards
Input Broadcast Packet Percentage	Cisco IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifInErrors, ifInDiscards, ifInUnknownProtos ifHCInBroadcastPkts, ifHCInMulticastPkts

Table 8-4 Interface Health Monitoring Metrics (continued)

Metric	Devices Polled	MIB	MIB Objects Included
Input Queue Drop Percentage	Cisco IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifHCInUcastPkts, ifInDiscards, ifInUnknownProtos, locIfInputQueueDrops
Output Queue Drop Percentage	Cisco IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCOutBroadcastPkts, ifHCOutMulticastPkts, ifHCOutUcastPkts, ifOutDiscards, ifOutUnknownProtos, locIfOutputQueueDrops

Table 8-5 Class-Based, QoS, Health-Monitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
QOS calculation	Cisco IOS devices	CISCO-CLASS-BASED-QOS-MIB	cbQosCMDropByte64 cbQosCMPostPolicyByte64 cbQosCMPrePolicyByte64

Deploying Monitor Configuration Templates

Step 1 Choose **Deploy > Configuration Deployment > Monitoring Deployment.**

Step 2 Find the template you created and click **Deploy**, then click **OK**.

Creating Composite Templates

Create a composite template if you have a collection of existing features or CLI templates that you want to apply collectively to devices. For example, when you deploy a branch, you need to specify the minimum configurations for the branch router. Creating a composite template allows you to create a set of required features that include:

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

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

If you have multiple similar devices replicated across a branch, you can create and deploy a *master (golden) composite template* for all of the devices in the branch. You can use this master composite template to:

- Simplify deployment and ensure consistency across your device configurations.
- Compare against an existing device configuration to determine if there are mismatches.
- Create new branches.

Step 1 Choose **Design > Feature Design > Configuration > Composite Templates > Composite Templates.**

Step 2 Provide the required information.

- From the **Device Type** drop-down list, choose the devices to which all of the templates contained in the composite template apply. For example, if your composite template contains one 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 list.

  Note If a device type is dimmed, the template cannot be applied on that device type.

- In the Template Detail area, choose the templates to include in the composite template.

  Using the arrows, put the templates in the composite in 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 3 Click **Save as New Template**. After you save the template, deploy it to your devices (see Creating and Deploying Feature-Level Configuration Templates, page 8-2).

Related Topic

- Grouping Configuration Templates with Devices, page 8-19

Grouping Configuration Templates with Devices

You might want to associate a set of configuration templates with specific devices. If you have devices that require the same configuration, you can create a *configuration group* that associates configuration templates with devices. Creating a configuration group allows you to quickly deploy new templates without remembering to which devices the new templates should be deployed.

Composite templates allow you to group smaller templates together, but only configuration groups specify the relationship between the templates and the groups of devices to which those templates apply. You can also specify the order in which the templates in the configuration group are deployed to the devices.

Before you create a configuration group, you should:

- Create configuration templates for the devices in your configuration group. See Creating and Deploying Feature-Level Configuration Templates, page 8-2.
- Determine which devices should be included in the configuration group.

Step 1 Choose **Design** > **Configuration Groups**.

Step 2 Hover your mouse cursor over Configuration Group in the left pane, then click **New**.

Step 3 Complete the required fields. The device types displayed depend on what you select from the Device Type field.

Step 4 Where needed, change a template's order in the group by selecting it and clicking the up or down arrow.

Step 5 Click **Save as a New Configuration Group**.

Step 6 Click **Publish** to publish the group, click **Deploy** and specify the deployment options (see Creating and Deploying Feature-Level Configuration Templates, page 8-2), then click **OK**.

Table 8-6 describes the possible configuration group states.

Table 8-6 Design > Configuration Group Status Descriptions

Status	Description
Deployed	All devices in the configuration group are in *Deployed* status.
Pending	One or more devices in the configuration group have changes that have not yet been deployed. For example, if you add a new device to the configuration group, the status of the new device is *Pending*. If you modify a configuration template to which the configuration group is associated, all devices in the configuration group have the status *Pending*.
Scheduled	Indicates that a configuration group deployment is scheduled. When a configuration group is *Scheduled*, any devices in the group that are *Pending* or *Failed* are changed to *Scheduled*. If a device is *Deployed*, it remains *Deployed* and its status does not change to *Scheduled*.
Failed	Deployment has failed for one or more devices in the configuration group.

Creating Shared Policy Objects

Policy objects enable you to define logical collections of elements. They are reusable, named components that can be used by other objects and policies. They also eliminate the need to define a component each time that you define a policy.

Objects are defined globally. This means that the definition of an object is the same for every object and policy that references it. However, many object types (such as interface roles) can be overridden at the device level. This means that you can create an object that works for most of your devices, then customize the object to match the configuration of a particular device that has slightly different requirements.

Creating Interface Roles

An interface role allows you to dynamically select a group of interfaces without having to manually define the interfaces on each device. For example, you can use interface roles to define the zones in a zone-based firewall configuration template. You might define an interface role with a naming pattern of DMZ*. When you include this interface role in a template and deploy the template, the configuration is applied to all interfaces whose name begins with “DMZ” on the selected devices. As a result, you can assign a policy that enables anti-spoof checking on all DMZ interfaces to all relevant device interfaces with a single action.

Step 1 Choose **Design** > **Configuration > Shared Policy Objects.**

Step 2 In the Templates menu on the left, choose **Shared > Interface Role**.

Step 3 From the Interface Role page, click **Add Object**.

Step 4 From the Add Interface Role page, create matching rules for the interface role.

When you deploy the zone-based template, for example, all of the interfaces on the device that match the specified rules will become members of the security zone represented by this interface role. You can match interfaces according to their name, description, type, and speed.

Step 5 Click **OK** to save the configurations.

Creating Network Objects

Network objects are logical collections of IP addresses or subnets that represent networks. Network objects make it easier to manage policies.

There are separate objects for IPv4 and IPv6 addresses; the IPv4 object is called “networks/hosts,” and the IPv6 object is called “network/hosts-IPv6.” Except for the address notation, these objects are functionally identical, and in many instances the name network/host applies to either type of object. Note that specific policies require the selection of one type of object over the other, depending on the type of address expected in the policy.

You can create shared policy objects to be used in the following configuration templates:

- Zone-based firewall templates—See Configuring a Zone-Based Firewall Template, page 13-40
- Application Visibility—See Configuring Application Visibility, page 13-2

Note Cisco Prime Infrastructure 2.0 supports IPv4 network objects only.

Step 1 Choose **Design** > **Configuration > Shared Policy Objects** > **Shared > IPv4 Network Object**.

Step 2 From the Network Object page, click **Add Object** and add a group of IP addresses or subnets.

Step 3 Click **OK** to save the configurations.

Creating Wireless Configuration Templates

The following sections describe how to create wireless configuration templates for:

- Lightweight access points
- Autonomous access points
- Switches
- Converting autonomous access points to lightweight access points

Creating Lightweight AP Configuration Templates

To create a template for a lightweight access point, follow these steps:

Step 1 Choose **Design > Configuration > Wireless Configuration > Lightweight AP Configuration Templates**.

Step 2 From the **Select a command** drop-down list, choose **Add Template,** then click **Go**.

Step 3 Enter a name and description for the template and click **Save**. If you are updating an already existing template, click the applicable template in the Template Name column.

Step 4 Click each of the tabs and complete the required fields. For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Creating Autonomous AP Configuration Templates

To create a template for an autonomous access point, follow these steps:

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

Step 2 From the **Select a command** drop-down list, choose **Add Template,** then click **Go**. If you are updating an already existing template, click the applicable template in the Template Name column.

Step 3 Enter a name for the template and the applicable CLI commands.

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

Creating Switch Location Configuration Templates

To configure a location template for a switch, follow these steps:

Step 1 Choose **Design > Configuration > Wireless Configuration > Switch Location Configuration**.

Step 2 From the **Select a command** drop-down list, choose **Add Template,** then click **Go**.

Step 3 Enter the required fields. For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Creating Autonomous AP Migration Templates

To make a transition from an autonomous solution to a unified architecture, autonomous access points must be converted to lightweight access points.

Note After an access point has been converted to lightweight, the previous status or configuration of the access point is not retained.

To create an autonomous AP migration template, follow these steps:

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

Step 2 From the **Select a command** drop-down list, choose **Add Template,** then click **Go**. If you are updating an already existing template, click the applicable template in the Template Name column.

Step 3 Complete the required fields. For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 4 To view the migration analysis summary, choose **Operate > Wireless > Migration Analysis**.

Creating Controller Configuration Groups

By creating a configuration 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 configuration groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected configuration groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected configuration 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.

By choosing **Design > Configuration > Wireless Configuration** > **Controller Configuration Groups**, you can view a summary of all configuration groups in the Prime Infrastructure database. Choose **Add Configuration Groups** from the **Select a command** drop-down list to display a table with the following columns:

- Group Name—Name of the configuration group.
- Templates—Number of templates applied to the configuration group.

Creating a New Configuration Group

To create a configuration group, follow these steps:

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

Step 2 From the **Select a command** drop-down list, choose **Add Config Group**, then click **Go**.

Step 3 Enter the new configuration group name. It must be unique across all groups.

- If Enable Background Audit is selected, the network and controller audits occur for this configuration group.

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

- If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.

Step 4 Other templates created in Prime Infrastructure can be assigned to a configuration group. The same WLAN template can be assigned to more than one configuration 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 configuration 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**. The Config Groups page appears.

After you create a configuration group, Prime Infrastructure allows you to choose and configure multiple controllers by choosing the template that you want to push to the group of controllers.

- General—Allows you to enable mobility group.

  To enable the Background Audit option, set template-based audit in **Administration > System > Audit Settings**.
- Controllers—For details, see Adding or Removing Controllers from a Configuration Group, page 8-25.
- Country/DCA—For details, see Configuring Multiple Country Codes, page 8-26.
- Templates—Allows you to select the configuration templates that you have already created.
- Apply/Schedule—For details, see Applying or Scheduling Configuration Groups, page 8-27.
- Audit—For details, see Auditing Configuration Groups, page 8-27.
- Reboot—For details, see Rebooting Configuration Groups, page 8-28.
- Report—Allows you to view the most recent report for this group.

Adding or Removing Controllers from a Configuration Group

To add or remove controllers from a configuration group, follow these steps:

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

Step 2 Click a group name in the Group Name column, then click the **Audit** tab.

The columns in the table display the IP address of the controller, the configuration group name the controller belongs to, and the mobility group name of the controller.

Step 3 Click to highlight the row of the controller that you want to add to the group, then click **Add**.

Note If you want to remove a controller from the group, highlight the controller in the Group Controllers area and click **Remove**.

Step 4 Click the **Apply/Schedule** tab, click **Apply** to add or remove the controllers to the configuration groups, then click **Save Selection**.

Note You cannot add or configure Cisco Catalyst 3850 Series Switches or Cisco 5700 Series Wireless LAN Controllers using the Classic view. To add or configure these devices, use the Lifecycle view.

Configuring Multiple Country Codes

You can configure one or more countries on a controller. After countries are configured on a controller, the corresponding 802.11a/n DCA channels are available for selection. At least one DCA channel must be selected for the 802.11a/n network. When the country codes are changed, the DCA channels are automatically changed in coordination.

Note 802.11a/n and 802.11b/n networks for controllers and access points must be disabled before configuring a country on a controller. To disable 802.11a/n or 802.11b/n networks, choose **Configure** > **Controllers**, select the desired controller that you want to disable, choose **802.11a/n** or **802.11b/g/n** from the left sidebar menu, and then choose **Parameters**. The Network Status is the first check box.

To add multiple controllers that are defined in a configuration group and then set the DCA channels, follow these steps:

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

Step 2 From the **Select a command** drop-down list, choose **Add Config Groups**, then click **Go**.

Step 3 Create a configuration group by entering the group name and mobility group name.

Step 4 Click **Save**, then click the **Controllers** tab.

Step 5 Highlight the controllers that you want to add, and click **Add**. The controller is added to the Group Controllers page.

Step 6 Click the **Country/DCA** tab. The Country/DCA page appears. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Step 7 Select the **Update Country/DCA** check box to display a list of countries from which to choose.

Step 8 Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes page. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking **Save Selection**.

Note A minimum of 1 and a maximum of 20 countries can be configured for a controller.

Applying or Scheduling Configuration 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 of the controllers in a configuration group, follow these steps:

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

Step 2 Click a group name in the Group Name column, then choose the **Apply/Schedule** tab.

Step 3 Click **Apply** to start the provisioning of mobility groups, mobility members, and templates to all of the controllers in the configuration 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 configuration group functions during the apply provisioning.

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

Step 4 Enter a starting date in the text box or use the calendar icon to choose a start date.

Step 5 Choose the starting time using the hours and minutes drop-down lists.

Step 6 Click **Schedule** to start the provisioning at the scheduled time.

Auditing Configuration 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 window or log out of Prime Infrastructure. The process continues, and you can return to this page later to view a report.

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

To perform a configuration group audit, follow these steps:

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

Step 2 Click a group name in the Group Name column, then click the **Audit** tab.

Step 3 Click to highlight a controller on the Controllers tab, choose **>> (Add)**, and **Save Selection**.

Step 4 Click to highlight a template on the Templates tab, choose **>> (Add)**, and **Save Selection**.

Step 5 Click **Audit** to begin the auditing process.

A report is generated and the current configuration on each controller is compared with that in the configuration 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 6 Click **Details** to view the Controller Audit report details.

Step 7 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 8 Click **Close** to return to the Controller Audit Report page.

Rebooting Configuration Groups

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

Step 2 Click a group name in the Group Name column, then click the **Reboot** tab.

Step 3 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 4 Click **Reboot** to reboot all controllers in the configuration group at the same time. During the reboot, you can leave this page or log out 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.

Retrieving Configuration Group Reports

To display all recently applied reports under a specified group name, follow these steps:

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

Step 2 Click a group name in the Group Name column, then 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 3 If you want to view the scheduled task reports, click the **click here** link at the bottom of the page.

Creating wIPS Profiles

Prime Infrastructure provides several predefined 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.

Predefined profiles include:

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

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 Hover your mouse cursor over the profile name to view the Profile ID and version.

- **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.

To create a wIPS profile, follow these steps:

Step 1 Select **Design > Configuration > Wireless Configuration > wIPS Profiles**.

Step 2 From the **Select a command** drop-down list, choose **Add Profile**, then click **Go**.

Step 3 Enter a profile name in the Profile Name text box of the Profile Parameters page.

Step 4 Select the applicable pre-defined profile, or choose **Default** from the drop-down list.

Step 5 Choose **Save > Next**.

Note When you select **Save**, the profile is saved to the Prime Infrastructure database with no changes and no mobility services engine or controller assignments. The profile appears in the profile list.

Step 6 To edit and delete current groups or add a new group:

a. From the **Select a command** drop-down list on the SSID Group List page, choose **Add Group** or **Add Groups from Global List**, then click **Go**.

b. Enter the group name and one or more SSID groups, then click **Save**.

Step 7 To determine which policies are included in the current profile, choose **Profile Configuration**. 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. Using this page, you can:

- Enable or disable an entire branch or an individual policy by selecting or unselecting the check box for the applicable branch or policy.

  Note By default, all policies are selected.

- Click an individual policy to display the policy description. Use the Policy Rules page add, edit, delete, and reorder the current policy rule settings.

  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.

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

- Configure the following settings:
  - Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues. Threshold options vary based on the selected policy.

    When the threshold is reached for a policy, an alarm is triggered. 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 8 When the profile configuration is complete, select **Next** to proceed to the MSE/Controller(s) page.

Step 9 In the Apply Profile page, select the mobility services engine and controller(s) to which you want to apply the current profile, then click **Apply** to apply the current profile to the selected mobility services engine/controller(s).

Note You can also apply a profile directly from the profile list. From the Profile List page, select the profile that you want to apply and click **Apply Profile** from the **Select a command** drop-down list. Then click **Go** to access the Apply Profile page.

Creating Custom SNMP Polling Templates

You can design custom SNMP polling templates to monitor third-party or Cisco devices and device groups. Using this feature, you can:

- Upload the SNMP MIB for the device type, then choose devices and attributes to poll and the polling frequency.
- Upload a single MIB definition file, or a group of MIBs with their dependencies as a ZIP file.
- Deploy the custom SNMP polling template the same way as other monitoring templates.
- Display the results as 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.

You can create a maximum of 25 custom SNMP polling templates.

To create a custom SNMP polling template, follow these steps:

Step 1 Choose **Design > Configuration > Custom SNMP Templates**.

Step 2 Click the **Basic** tab and enter the required information. When specifying MIB information:

- Specify a filename extension only if you are uploading a ZIP file.
- If you are uploading a ZIP file, ensure that all dependent MIB files are either included in the ZIP or already present in the system.
- Ensure your upload file and the MIB definition have the same name (for example: Do not rename the ARUBA-MGMT-MIB definition file to ARUBA_MGMT). If you are uploading a ZIP file, you may name it as you please, but the MIB files packaged inside it must also follow this convention (for example: MyMibs.zip is acceptable, as long as all MIB files in the ZIP match their MIB names).

Step 3 Click **Save**.

Step 4 Specify the polling parameters for your new template:

a. On the Monitor Configuration Templates page, expand the Features menu, choose **Custom SNMP**, and select your new custom SNMP template.

b. Complete the basic template fields, then select a polling frequency, then click **Save as New Template**.

Step 5 To deploy the template:

a. Choose **Deploy > Configuration Deployment > Monitoring Deployment.** Find the template you created and click **Deploy**.

b. Check the boxes for the devices to which you want to deploy this template, then click **Submit**.

Step 6 To view the SNMP polling data, create a generic dashlet (see Creating Generic Dashlets, page A-7) using the name of the template that you created in Step 4.

Note To view the SNMP polling date for ASR device, you should use the s**how platform hardware qfp active datapath utilization | inc Processing** command for CPU utilization and **show platform hardware qfp active infrastructure exmem statistics | sec DRAM** command for memory utilization.

Deploying Templates and Tasks

The Deploy menu allows you to deploy previously configured tasks, profiles, and software immediately or at a future time.

Planning Template Deployments

Before deploying any object, answer the following questions:

- What are you deploying? Determine whether you are deploying a template, Plug and Play profile, and so on.
- Where is being deployed? Determine which devices should be included in the deployment.
- When is it being deployed? Determine when the deployment should happen.

You can plan your template deployments based on the following device conditions:

- Existing devices—You can deploy a template to a device that is already in your network.
- New devices that are known—You can deploy a 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.

Deploying and Monitoring Configuration Tasks

After you publish a template and want to deploy it to one or many devices, you can specify the devices, values, and scheduling information to tailor your deployment.

To deploy and manage a template:

Step 1 Choose **Deploy > Configuration Deployment > Configuration Tasks**.

Step 2 From the left sidebar menu, open the folder that contains the type of template that you want to deploy.

Step 3 Select the check box of the template that you want to deploy, then click **Deploy**.

Step 4 Provide the information described in the following table, then click **OK**.

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	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 that you want to change, enter a new value, and click **Apply**. You can also update the variables for all selected devices. Click **All Selected Devices** and update variables to apply the changes on all selected devices at the same time. If you want to update variables for a particular device in the list that need not be applicable to other devices, then choose the device and update its variables. All of the other devices will continue to use the variables that were previously defined except for the device for which variables are updated. **Note** The changes you make apply only to the specific configuration you are deploying. To change the configuration template for all future deployments, choose **Design > Configuration > Feature Design** and change the template.
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.

Step 5 Use the Monitoring Deployment option to manage deployed templates. To quickly redeploy, deactivate, undeploy, or view the deployment history for a template, choose **Deploy > Configuration Deployment > Monitoring Deployment**.

Automating Device Deployment

Cisco Prime Infrastructure helps automate the deployment of new devices on the network by obtaining and applying the necessary software image and configuration on a new network device. Using features such as Cisco Network Services (CNS) call-home and Cisco IOS auto-install (which uses DHCP and TFTP), Prime Infrastructure reduces the time a new device takes to join the network and become functional.

The Plug and Play feature of Prime Infrastructure allows you to create templates to define features and configurations that you can reuse and apply to new devices. You can streamline new device deployment by creating bootstrap templates, which define the necessary initial configuration, to communicate with Prime Infrastructure. You can specify (and *predeploy*) software images and configurations for devices that will be added to the network in the future.

Automating Device Deployment Using Plug and Play Profiles

The Prime Infrastructure Plug and Play feature allows you to perform an initial provisioning of a software image and configuration on a new device.

To automate the deployment of a new device on your network:

Step 1 Create a Plug and Play profile (see Creating Plug and Play Profiles, page 9-6).

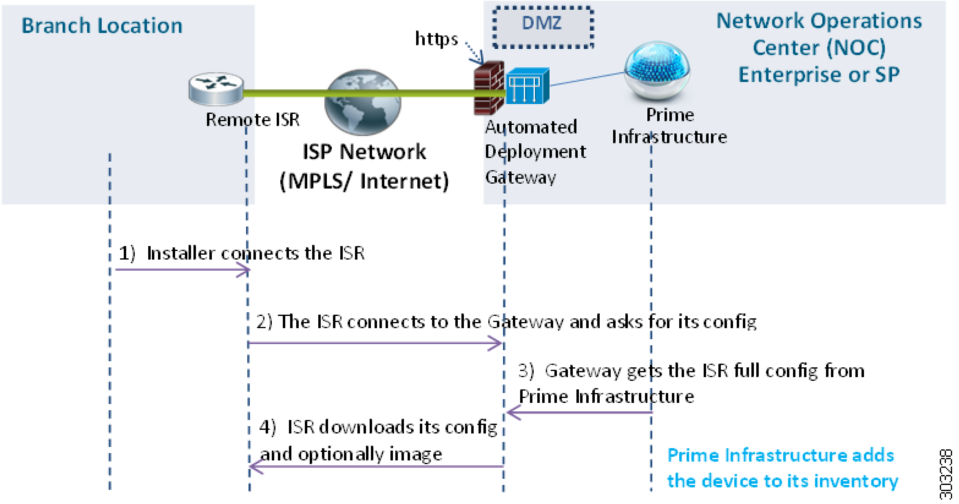
Step 2 Based on the Plug and Play method, add a new device with CNS capabilities to the network, and apply a bootstrap configuration to activate the CNS agent on the device. Use any of the bootstrap delivery methods that Prime Infrastructure supports, or use your own mechanism (see Delivering and Applying the Bootstrap, page 9-7).

When you apply the bootstrap configuration:

1. The device uses the call-home agent capability to connect to the Prime Infrastructure server.
2. Automated deployment is initiated.
3. The Prime Infrastructure server receives the ID of the new device and verifies that the device ID matches the device ID in any of the Plug and Play preprovisioning definitions. If there is no match for the device ID, Prime Infrastructure matches the device type with any of the existing type-based Plug and Play preprovisioning definitions.
4. If there is a match, Prime Infrastructure applies the software image and the configuration specified in the matched Plug and Play profile on the device and adds the device to its inventory.

After the bootstrap configuration is applied to the device, the installer connects the device to a WAN at the remote site. The device connects to the Plug and Play gateway using its serial number, and downloads the full configuration and (optional) Cisco IOS image (see Figure 9-1).

Figure 9-1 Plug and Play Branch Deployment


Branch Location
https
DMZ
Network Operations Center (NOC) Enterprise or SP
Remote ISR
ISP Network (MPLS/ Internet)
Automated Deployment Gateway
Prime Infrastructure
1) Installer connects the ISR
2) The ISR connects to the Gateway and asks for its config
3) Gateway gets the ISR full config from Prime Infrastructure
4) ISR downloads its config and optionally image
Prime Infrastructure adds the device to its inventory
303238

Prerequisites for Using Plug and Play Profiles

Before you can use the Plug and Play feature, you must:

1. Set up the Cisco Prime Plug and Play gateway.

Note It is not mandatory to set up Cisco Prime Plug and Play gateway. In Cisco Prime Infrastructure Release 2.0, Plug and Play gateway is integrated with Prime Infrastructure. If the user explicitly wants the gateway setup, then Cisco Prime Plug and Play gateway can be set up. Do not execute the **cns config retrieve** or **cns image retrieve** command on a device that has been added using the Plug and Play feature.

2. Use a CLI template to create a bootstrap configuration template (see Creating a Bootstrap Configuration Template, page 9-4).
3. Download the software image (see Downloading Software Images, page 9-5). This step is optional.
4. Create a configuration template (see Creating a Configuration Template, page 9-6).

Creating a Bootstrap Configuration Template

A bootstrap configuration template should have the minimum required CLI configurations so that the new device can communicate with the Prime Infrastructure Plug and Play gateway server.

Note You can also use the **Design > Feature Design >CLI Templates > System Templates-CLI > Plug And Play Bootstrap** to create the bootstrap template.

To create a bootstrap configuration template for CNS devices:

Step 1 Choose **Design > Feature Design > CLI Template folder > CLI**.

Step 2 When you create the bootstrap template, enter “Bootstrap” in the tag field associated with the CLI template. Then the new bootstrap template will be listed in the Bootstrap Template column when a Plug and Play profile is being created.

The CLI template should have these configurations for the device CNS agent to connect to the Prime Infrastructure Plug and Play gateway server:

- IP reachability to the Prime Infrastructure Plug and Play gateway server (if required)
- CNS configurations

For more information, see Creating CLI Configuration Templates, page 8-4.

The CNS configurations for Plug and Play deployment 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 event <PnP Gateway server fully qualified host name> 11011 keep alive 120 2
reconnect-time 60
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
cns config partial <PnP Gateway server fully qualified host name> 80
cns config initial <PnP Gateway server fully qualified host name> 80
```

Downloading Software Images

To download software images:

Step 1 Choose **Operate > Device Work Center > Software Image Management**.

Step 2 Click **Import**, then specify the source from which the software image is to be imported.

Step 3 Specify the 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 will run only once.

Step 4 Click **Submit**.

Step 5 To view the details of image management job, choose **Administration > Jobs Dashboard**.

Creating a Configuration Template

Use one of the following templates as the configuration template:

- A CLI template (for more information, see Creating CLI Configuration Templates, page 8-4)
- A composite template that contains multiple CLI templates

Creating Plug and Play Profiles

Before creating a Plug and Play profile, you must satisfy the prerequisites (see Prerequisites for Using Plug and Play Profiles, page 9-4).

To create a Plug and Play profile:

Step 1 Select **Design > Plug and Play Profiles > Plug and Play Profile**.

Step 2 Provide the required information. See the *Cisco Prime Infrastructure 2.0 Reference Guide* for field descriptions.

Step 3 Click **Save as New Plug and Play Profile**, then **Save** to confirm the new profile.

Step 4 Click **Publish** to publish your profile and make it available for future deployment.

Step 5 Click **Deploy** to create a pre-provisioning definition for the incoming devices. You can create multiple pre-provisioning definitions for one profile (see Deploying a Plug and Play Profile Based on Device ID, page 9-6).

Deploying a Plug and Play Profile Based on Device ID

To deploy a Plug and Play profile based on the device ID:

Step 1 Choose **Deploy** > **Plug and Play Profiles**.

Step 2 In the Plug and Play Profiles page, select a profile and click **Deploy**.

Step 3 In the Device Provisioning Profiles page, click **Add**.

Note One profile can have multiple provisioning settings that can be applied for different devices.

Step 4 Provide the required information. See the *Cisco Prime Infrastructure 2.0 Reference Guide* for field descriptions.

Step 5 Click **OK**, then click **Close**.

Deployment Based on Device Type

To deploy a Plug and Play profile based on the device type, you do not have to associate the device ID with the deployment profile. Device type-based deployment is useful primarily for switches that use the same set of images and configurations. Matching profiles are identified by the device type (PID) of the incoming device that is specified in the profile during the design phase.

During device type-based deployment:

1. The device type is matched hierarchically; 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, 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 or Cisco Catalyst 2928 Series Switches), then the 'switch_profile' is considered for deployment.

2. If the Prime Infrastructure have multiple matching deployment profiles for a given device type, then Prime Infrastructure chooses the deployment profile that is created or updated recently.

Delivering and Applying the Bootstrap

Prime Infrastructure lets you define a bootstrap configuration template for a device.

Alternatively, the bootstrap configuration can be defined and delivered outside of Prime Infrastructure; for example, from the factory using Cisco Integrated Customization Services.

Exporting the Bootstrap Configuration

The operator can manually apply the bootstrap on the device. After the bootstrap configuration is applied, the Plug and Play deployment is initiated and the administrator can view the configuration status on Prime Infrastructure.

To export the bootstrap configuration:

Step 1 Choose **Deploy** > **Plug and Play Profiles**.

Step 2 From the Plug and Play Profiles page, select a profile from the list and click **Deploy**.

Step 3 From the Device Provisioning Profiles page, select the device profile from the list, click **Bootstrap Configuration > Export Bootstrap**, then click **OK**.

Step 4 After the bootstrap configuration is applied, the Plug and Play deployment is initiated. To check the Plug and Play status, do one of following:

- To check information about all incoming devices, choose **Operate**> **Plug and Play Status**.
- To check the status of a selected device for a selected profile, choose **Deploy** > **Plug and Play Profiles > History**.
- To check the history of deployment, point to the Quick View icon at the right corner of the Current Status field for the device.

Delivering the Bootstrap Configuration Using TFTP

The TFTP protocol 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 other Prime Infrastructure details through the DHCP. In the DHCP server, the TFTP server must be configured as the Prime Infrastructure TFTP server.

To deliver the bootstrap configuration:

Step 1 Choose **Deploy** > **Plug and Play Profiles**.

Step 2 From the Plug and Play Profiles page, select a profile from the list and click **Deploy**.

Step 3 In the Device Provisioning Profiles page, select the Device Profile from the list, click **Bootstrap Configuration > TFTP**, then click **OK**.

Step 4 After the bootstrap configuration is applied, the Plug and Play deployment is initiated. To check the Plug and Play status, choose one of these options:

- To check information about all incoming devices, choose **Operate**> **Plug and Play Status**.
- To check the status of a selected device for a selected profile, choose **Deploy** > **Plug and Play Profiles > History**.
- To check the history of deployment, hover over the Quick View icon at the right corner of the Current Status field for the device.

Emailing the Bootstrap Configuration

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.

Note Before you can email the bootstrap configuration, you must set the email settings under **Administration** > **System Settings > Mail Server Configuration**.

To email the bootstrap configuration to the operator:

Step 1 Choose **Deploy** > **Plug and Play Profile**.

Step 2 From the Plug and Play Profiles page, click **Deploy**.

Step 3 From the Device Provisioning Profiles page, select a profile from the list and click **Bootstrap Configuration > Email Bootstrap**.

Step 4 Enter the email address to which the bootstrap configuration is be sent, then click **OK**.

Step 5 After the bootstrap configuration is applied, the Plug and Play deployment is initiated. To check the Plug and Play status, choose one of these options:

- To check information about all incoming devices, choose **Operate**> **Plug and Play Status**.
- To check the status of a selected device for a selected profile, choose **Deploy** > **Plug and Play Profiles > History**.

- To check the history of deployment, hover over the Quick View icon at the right corner of the Current Status field for the device.

Emailing the PIN

Prime Infrastructure generates a random Personal Identification Number (PIN) per device. This PIN can be used to identify the device and the Plug and Play profile (bootstrap configuration) associated with it. After the pre-provisioning tasks are complete, the administrator must use the **Email PIN** option (available in the pre-provisioning task of the Prime Infrastructure) to email the unique PIN to the deployment engineer. During installation, the deployment engineer uses this PIN to download the bootstrap configuration from the Plug and Play gateway.

To deliver the PIN for the bootstrap configuration:

Step 1 Choose **Deploy** > **Plug and Play Profile**.

Step 2 In the Plug and Play Profiles page, select a profile and click **Deploy**.

Step 3 In the Device Provisioning Profiles page, select the device profile from the list and click **Email PIN**.

Step 4 Enter the email address to which the PIN should be sent and click **OK**.

Step 5 Use one of the following methods to apply the bootstrap configuration:

- If you are applying the bootstrap configuration using the *deployment application*, the Prime Infrastructure Plug and Play deployment application communicates to the Prime Infrastructure and applies the bootstrap configuration on the device.
- If you are *manually* applying the bootstrap configuration using the PIN:
  - Use the PIN to download the bootstrap configuration from the Prime Infrastructure Plug and Play gateway: https://<pnp-gateway-server>/cns/PnpBootstrap.html. You can also register the ISR's serial number during this process.
  - Apply the bootstrap configuration on the device manually, using a console or USB flash.

Note For detailed information about Plug and Play deployment, see the *Cisco Plug and Play Application 2.0 User Guide*.

Step 6 After the bootstrap configuration is applied, the Plug and Play deployment is initiated. To check the Plug and Play status, choose one of these options:

- To check information about all incoming devices, choose **Operate**> **Plug and Play Status**.
- To check the status of a selected device for a selected profile, choose **Deploy** > **Plug and Play Profiles > History**.
- To check the history of deployment, hover over the Quick View icon at the right corner of the Current Status field for the device.

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 "Adding Devices Using Discovery" section on page 3-3.

Prime Infrastructure simplifies WLAN deployments with support for auto-provisioning. Auto provisioning allows Prime Infrastructure to automatically configure a new or replace a current Cisco Wireless LAN Controller (WLC). Prime Infrastructure auto provisioning feature can simplify deployments for customers with a large number of controllers.

Note The controller radio and b/g networks are initially disabled by the Prime Infrastructure startup configuration file. You can turn on those radio networks by using a template, which should be included as one of the automated templates.

Using the Auto Provisioning Filter List

The Auto Provision Filters page allows you to create and edit auto provisioning filters that define the list of allowable devices to be auto provisioned or auto monitored by Prime Infrastructure.

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. Check or uncheck the check box to allow or disallow these privileges.

Filter parameters include:

Parameter	Description
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 Cisco WLC defined in this filter is managed by Prime Infrastructure but not configured by Prime Infrastructure if the Cisco 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 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.

To add an Auto Provisioning Filter:

Step 1 Choose **Deploy > Plug and Play Profiles > Controller Deployment**.

Step 2 Choose **Add Filter** from the **Select a command** drop-down list, then click **Go**.

Step 3 Enter the required parameters.

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.

Step 4 Click **Save**.

Auto Provisioning Primary Search Key Settings

Use the Primary Search Key Setting to set the matching criteria search order.

Step 1 Choose **Deploy > Plug and Play Profiles > Controller Deployment**, then from the left sidebar menu, choose **Setting**.

Step 2 Click to highlight the applicable search key, then use the **Move Up** or **Move Down** buttons to move the search key to a higher or lower priority.

Step 3 Click **Save** to confirm the changes.

Managing Scheduled Configuration Task Templates

The Scheduled Configuration Tasks page allows you to navigate to any templates, configuration tasks, or software download tasks that have been scheduled earlier and provides a filtered view of these tasks. This page displays the summary information about a task. The information includes the template name, last time the task was run, next time the task is scheduled to run, and a link to view the results of previous runs. You can also edit the template, modify the schedule, enable, disable, or delete a scheduled task.

After you create and schedule a configuration template, configuration group, or a software download task, the scheduled task or template is listed in the Scheduled Configuration Tasks page.

Note You cannot create any new scheduled task or template in this page. You can only edit the scheduled task or template that is already created.

You can modify, enable, disable, or delete the following scheduled configuration tasks:

- AP Template
- Config Group
- WLAN Configuration
- Download Software

Managing AP Template Tasks

The AP Template Tasks page allows you to manage current access point template tasks.

Before You Begin

At least one lightweight access point task must exist (see Creating Lightweight AP Configuration Templates, page 8-22).

To modify a current access point template task:

Step 1 Choose **Deploy > Configuration Deployment > Scheduled Configuration Tasks**.

Step 2 Select the template name of the applicable task.

Step 3 In the AP Radio/Template page, click the **Apply/Schedule** tab.

Step 4 Make any necessary changes to the current schedule or access point template, and click **Schedule**.

To enable a current access point template task:

Step 1 Choose **Deploy > Configuration Deployment > Scheduled Configuration Tasks**.

Step 2 Check the check box of the scheduled task to be enabled.

Step 3 Choose **Enable Schedule** from the **Select a command** drop-down list, then click **Go**.

Related Topics

- Managing Scheduled Configuration Task Templates
- Managing AP Template Tasks
- Viewing WLAN Configuration Scheduled Task Results

Viewing WLAN Configuration Scheduled Task Results

Note There is no drop-down command list for WLAN Configuration.

To view and manage all scheduled WLAN tasks in Prime Infrastructure:

Step 1 Choose **Deploy > Configuration Deployment > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **WLAN Configuration** to open the WLAN Configuration Task List page.

Step 3 Select the Task Name link to open the WLAN Schedule Detail page. In this page, you can modify the date and time of the scheduled task.

Step 4 Check the check box of the scheduled task and use the **Select a command** drop-down list to enable, disable, or delete selected tasks.

Related Topics

- Managing Scheduled Configuration Task Templates
- Managing AP Template Tasks

Managing Software Downloads

Use this feature to manage the software download tasks.

Adding a Download Software Task

To add a download software task:

Step 1 Choose **Deploy > Configuration Deployment > Scheduled Configuration Tasks**, then from the left sidebar menu, choose **Download Software**.

Step 2 Choose **Add Download Software Task** from the **Select a command** drop-down list, then click **Go**.

Step 3 Configure the following information:

- General
  - Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Schedule Details
  - Download Type—Select the download type. Check the **Download software to controller** check box to schedule download software to controller or check the **Pre-download software APs** check box to schedule the pre-download software APs. If you select Download software to controller, specify the image details.

    Note The pre-download option is displayed only when all selected controllers are using the Release 7.0.x.x or later.

    Note To see Image Predownload status per AP, enable the task in the Administration > Background Task > AP Image Predownload Task page, and run an AP Image Predownload report from the Report Launch Pad.

  - Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

Note Reboot Type Automatic can be set only when the **Download software to controller** option is selected.

- Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Select the time from the hours and minutes drop-down lists.
- Reboot date/time—This option appears only if select the reboot type "Scheduled". Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

Note Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download.

Note If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller does not reboot. In such a case, wait for the pre-download to finish for all of the APs and reboot the controller manually.

- Notification (Optional)—Enter the email address of recipient to send notifications via email.

Note To receive email notifications, configure Prime Infrastructure mail server in the Administration > Settings > Mail Server Configuration page.

- Image Details—Specify the TFTP or FTP Server Information:

Note Complete these details if you selected the Download software to controller option in Schedule Details area.

TFTP—Specify the TFTP Server Information:

- From the File is Located on drop-down list, choose **Local machine** or **TFTP server**.

Note If you choose TFTP server, choose **Default Server** or **add a New server** from the Server Name drop-down list.

- Specify the IP address of the TFTP server. This is automatically populated if the default server is selected.
- Specify the local filename or click **Browse** to navigate to the appropriate file.
- If you selected TFTP server previously, specify the filename.

FTP—Specify the FTP Server Information:

- FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button.
- From the File is Located on drop-down list, choose **Local machine** or **FTP server**.

Note If you choose FTP server, choose **Default Server** or **add a New server** from the Server Name drop-down list.

- Specify the IP address of the FTP server. This is automatically populated if the default server is selected.
- Specify the local filename, or click **Browse** to navigate to the appropriate file.
- If you selected FTP server previously, specify the filename.

Step 4 Click **Save**.

Modifying a Download Software Task

Before You Begin

At least one download software task must exist (see Adding a Download Software Task, page 9-13).

To modify a download software task:

Step 1 Choose **Deploy > Configuration Deployment > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Click the Task Name link to open the Download Software Task page, make any changes, then click **Save**.

Note Any changes in Download Type (Download/Pre-download) or Server Type (FTP/TFTP) for the task in 'Enabled' state sets the task to 'Disabled' state and all of the existing controllers are disassociated from the task.

Selecting Controllers for the Download Software Task

This page lists all the supported controllers that can be selected for the scheduled image download/pre-download task.

To select a controller for scheduled image download:

Step 1 Choose **Deploy > Configuration Deployment > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Click the Controller to open the Download Software Task details page, then click **Select Controller** to view the controller list.

Note If the pre-download option is chosen for the task, then only the controllers with software Release 7.0.x.x or later are listed.

The Select Controllers page can also be accessed from **Deploy > Configuration Deployment > Scheduled Configuration Tasks > Download Software**, then click the hyperlink in the Select Controller column for any download task that is in the Enabled, Disabled or Expired state.

Note Controllers with Reachability Status 'Unreachable' cannot be selected for Download Software Task.

Step 4 Make any necessary changes, then click **Save**.

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. For more information, see Getting Device Details from the Device 360° View, page A-12.
- 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. There are several reasons a device CLI returned an error:
  - The device configuration was modified directly via CLI (out-of-band changes) and the Prime Infrastructure database is not synchronized with those changes. When you deploy a configuration template, it is assumed that the Prime Infrastructure database is up-to-date with the latest device configuration. We recommend that you run an inventory collection for the failing device from the Device Work Center and make sure all out-of-band changes are up-to-date, and then redeploy the template.
  - One or more devices are not in *Managed* collection state. When you deploy a configuration template, it is assumed that the Prime Infrastructure database is up-to-date with the current device configuration. If a device has a collection status other than *Managed*, for example *Managed with Errors* or *Managed With Warnings*, the template deployment might fail. See Troubleshooting Unmanaged Devices, page 12-4 for more information about device collection status.
  - The device does not have the appropriate Cisco IOS software version or the appropriate license to configure the requested feature. Log in directly to the device on which the template deployment failed and verify that the device supports the CLI that is specified in the template.

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.

PART 3

Operating the Network

This part contains the following sections:

- Managing Reports

CHAPTER 10

Operating and Monitoring the Network

On the Operate tab, Cisco 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 tools that you need for day-to-day monitoring, troubleshooting, maintenance, and operations.

Monitoring Dashboards

Prime Infrastructure automatically displays monitoring data on dashboards and dashlets. Table 10-1 describes the dashboards that are available in **Operate > Monitoring Dashboards** for checking summary information.

Note

- The label "*Edited*" next to a dashlet heading indicates that the dashlet has been customized.
- The dashlet arrangement is maintained after upgrading. To display new dashlets or features in a new release, click **Manage Dashboards**.

You can choose one of the following dashboards in **Operate > Monitoring Dashboards** to view summary information:

Table 10-1 Operate > Monitoring Dashboards

Dashboard	Description
Overview	Network overview information, including device counts, top N devices by CPU and memory utilization, and the device credential summary. To troubleshoot and isolate issues, click a device or interface alarm count to view detailed dashboards, alarms, and events. You can also view information about your software such as version, type, and device count. The Overview-General dashboard also displays user-defined jobs under Job Information Status dashlet. The following dashboards appear on the Overview tab: • **General**—Displays general inventory, memory utilization, device summary information, and so on. • **Client**—Displays client-related information to allow you to monitor clients on the network. • **Security**—Displays rogue access points, top security issues, information on attacks, and so on. • **Mesh**—Displays mesh alarms, mesh packet error rate, worst node hop count, and so on. • **CleanAir**—Displays average air quality, interferers, and so on. • **Context Aware**—Displays historical element counts, allows you to troubleshoot clients, and so on.
Incidents	Alarm and event information, including the sites with the most alarms, the most frequently occurring types of alarms, the distribution of alarms and summary of syslog events by severity, syslog events that match user-configured message type criteria. This dashboard also includes a summary of SNMP reachability for all devices in the network.
Performance	Information about CPU and memory utilization, environmental temperatures, and device and interface availability. The following dashboards appear on the Performance tab: • **Network Device**—Displays top CPU utilization, environmental temperature, memory utilization, and so on. • **Network Interface**—Displays interface availability, utilization information, and so on. • **Service Assurance**—Displays top applications, clients, servers, and so on. • **Service Health**—Displays site-application health information.
Detail Dashboards	Network health summaries for sites, devices, or interfaces. The detail 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, check device reachability status for the site, and so on.

To change the information displayed in the dashboards, see Search Methods.

Table 10-2 describes where to find monitoring information in the Prime Infrastructure dashboards.

Table 10-2 Finding Monitoring Data

To View This Monitoring Data...	Choose this Dashboard...
Alarm information	Operate > Monitoring Dashboards > Incidents
Application information	Operate > Monitoring Dashboards > Detail Dashboards > Application
Client information	Operate > Monitoring Dashboards > Overview > Client
CPU utilization	Operate > Monitoring Dashboards > Overview > General

Table 10-2 Finding Monitoring Data (continued)

To View This Monitoring Data...	Choose this Dashboard...
Device (specific) information	Operate > Monitoring Dashboards > Detail Dashboards > Device
Device (Top N) CPU utilization, memory utilization, and environmental temperature information	Operate > Monitoring Dashboards > Performance > Network Device
Device credential status	Operate > Monitoring Dashboards > Overview > General
Device reachability summary	Operate > Monitoring Dashboards > Detail Dashboards > Site
End user information	Operate > Monitoring Dashboards > Detail Dashboards > End User Experience
Event information	Operate > Monitoring Dashboards > Incidents
Interface information	Operate > Monitoring Dashboards > Detail Dashboards > Interface
Interface status, availability, and utilization information	Operate > Monitoring Dashboards > Performance > Network Interface
Licensing information	Operate > Monitoring Dashboards > Overview > General
Memory utilization	Operate > Monitoring Dashboards > Overview > General
Mesh network information	Operate > Monitoring Dashboards > Overview > Mesh
Security information	Operate > Monitoring Dashboards > Overview > Security
Service assurance information	Operate > Monitoring Dashboards > Performance > Service Assurance
Site information	Operate > Monitoring Dashboards > Detail Dashboards > Site
Syslog Watch and Syslog Summary	Operate > Monitoring Dashboards > Incidents or Operate > Alarms & Events > Syslogs
Utilization statistics	Operate > Monitoring Dashboards > Overview > General
Voice/video information	Operate > Monitoring Dashboards > Detail Dashboards > Voice/Video
WAN information	Operate > Monitoring Dashboards > Detail Dashboards > WAN Optimization

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 **Administration > System Settings > Background Tasks** to view scheduled tasks. The Background Tasks page appears.

Step 2 Choose a command from the drop-down list:

- **Execute Now**—Runs all of the data sets with a checked check box.
- **Enable Tasks**—Enables the data set to run on its scheduled interval.
- **Disable Tasks**—Prevents the data set from running on its scheduled interval.

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 10-3.

Table 10-3 Device Work Center Tasks

Task	Description	Location in Operate > Device Work Center
Manage devices	Add, edit, delete, sync, and export devices, add and delete devices from groups and sites, and perform a bulk import.	Buttons located at the top of the Device Work Center. Refer Adding Devices Manually, Exporting Devices, and Importing Devices from Another Source for more details.
View basic device information and collection status	View basic device information such as reachability status, IP address, device type, and collection status.	Hover your mouse cursor on the IP Address/DNS cell and click the icon to access the 360° view for that device (see Getting Device Details from the Device 360° View). Hover your mouse cursor on the Collection Status cell and click 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 in the left pane of the Device Work Center Page. See Managing Device Groups for more information about creating and using device groups.
Add devices to site groups	After you set up a site group profile, you can add devices to it. To add devices to site groups in Device Work Center, add them to Group and then select site group. To add devices to site maps, go to the Design > Site Map Design page. **Note** A device can belong to one site group hierarchy only. **Note** The devices added to a site group in Device Work Center do not add devices in the Design > Site Map Design page. Similarly, the devices added in the Site Map Design page are not added to site groups in Device Work Center.	**Add to Group** button located at the top of the Device Work Center page under "Groups & Sites".

Table 10-3 Device Work Center Tasks (continued)

Task	Description	Location in Operate > Device Work Center
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 Page.
	View device information and status, and associated modules, alarms, neighbors, and interfaces. See Getting Device Details from the Device 360° View for more information.	Hover your mouse cursor on a device IP address and click the icon that appears.
Create and deploy configuration templates	You can configure device features on the selected device. You can also view the list of applied and scheduled feature templates that were deployed to the device. **Note** Using the Device Work Center, it may not be possible to add configuration for a few controller features. In this case, use the Design page and create a new Template and deploy to the device.	Click the **Configuration** tab at the bottom of the Device Work Center Page. See Configuring Device Features for more information about configuring features on a device.
View device configurations	View archived configurations, schedule configuration rollbacks, and schedule archive collections.	Click **Configuration Archives** at the top of the Device Work Center.
View 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.	Click **Software Image Management** at the top of the Device Work Center. Select a device for which you want to view the recommended software image. Click the **Image** tab. 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 the local repository. You can import the recommended image (see Importing Software Images) or distribute (see Deploying Software Images to Devices) the recommended image.
View interface details	You can view the description, admin status, and operational status of the interface.	Choose a device in the Device Work Center, then click the **Configuration** tab at the bottom of the screen. Click **Interfaces** to view the interface details.
View and modify TrustSec configuration	You can view and modify the TrustSec configuration of a TrustSec-based device.	Choose a device in the Device Work Center, then click the **Configuration** tab at the bottom of the screen. Click **Security >TrustSec > Wired 802_1x**.

Import Policy Updates

Import Policy Updates allows you to manually download the policy updates patch file from Cisco.com and import it into the Compliance and Audit Manager Engine.

To import policy updates:

Step 1 From the Cisco.com home page, navigate to **Products & Services > Cloud and Systems Management**. Click **View All Products**, then click **Routing and Switching Management > Cisco Prime Infrastructure**, select the latest version and then click **Compliance Policy Updates**.

Step 2 Download the CompliancePolicyUpdates.vX-y.jar patch file, where *X* is the major version and *y* is the minor version.

Step 3 Enter your Cisco.com credentials.

Step 4 Save the CompliancePolicyUpdates.vX-y.jar patch file TO your local system.

Step 5 To select the downloaded CompliancePolicyUpdates.vX-y.jar file from your local system, go to the Import Policy Updates page and click **Browse**.

Step 6 To import the CompliancePolicyUpdates.vX-y.jar patch file into the Compliance Engine, click **Upload**.

A message appears indicating the successful importing of policy into the Compliance Engine.

Step 7 After you see the message indicating a successful import, restart the Prime Infrastructure server process to effect the changes. See Restarting the Prime Infrastructure Server, page 10-6.

Note Verify that the Prime Infrastructure server process is restarted to effect the changes.

Restarting the Prime Infrastructure Server

Step 1 To restart the Prime Infrastructure server, log in as the admin user:

```
ssh admin@<server>
```

Step 2 Run the following commands (in the order specified) from the admin prompt:

```
admin# ncs stop
admin# ncs start
```

Monitoring Jobs

Use the Jobs dashboard to:

- View all running and completed jobs and corresponding job details
- Filter jobs to view the specific jobs in 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

Step 1 Choose **Administration > Jobs Dashboard**.

Step 2 Click a job, then perform any of the following actions:

- Click **Run** to start the currently scheduled job immediately. If a job has the status "failed," click **Run** to resubmit the same job, which creates a new scheduled job with the same parameters as the previous job.
- Click **Abort** to stop a discovery job currently in progress and return it to its scheduled state. You cannot abort all jobs. For example, you receive an error message if you try to abort a running configuration job.
- Click **Cancel** to delete any future scheduled jobs for the job you specified. If a job is currently running, it will complete.
- Click the **History** tab to view the history of a job. Hover your mouse over the results in the Status column to display troubleshooting information that can help you determine why a job failed.
- Click the **Details** tab to view job information such as when the job was created, started, or scheduled.

Note When a minute job is scheduled to run recursively, the first trigger of the job falls on nth minute of the hour, as divided by the quartz scheduler, and successive runs will be placed as per the schedule. For example, if you have given the start time as 12:02:00 and you want the job to run every 3 minutes, then the job will be executed at 12:03 (in a minute), with the next recurrence at 12:06, 12:09, and so on. Another example, if you have given the start time as 12:00:00 and you want the job to run every 3 minutes, then the job will be executed at 12:00 (without any delay), with the next recurrence at 12:03, 12:06, and so on.

Monitoring the System Using Reports

Prime Infrastructure reporting helps you monitor the system and network health and troubleshoot problems. You can run a report immediately or schedule it to run at a time that you specify. After you define a report, you can save it for future diagnostic use or schedule it to run on a regular basis. You can save a report in either CSV or PDF format. You can save it to a file on Prime Infrastructure for later download, or email it to a specific email address.

To view a report:

Step 1 Choose **Report > Report Launch Pad**.

Step 2 Click a report name to view the data for that report.

To create a report:

Step 1 Choose **Report > Report Launch Pad**, then click **New** next to the report type that you want to create.

Step 2 Enter the report details, then click one of the save options.

Monitoring and Troubleshooting Network Traffic

In addition to aggregating data from multiple NAMs, Prime Infrastructure with licensed Assurance features makes it easy to actively manage and troubleshoot network problems using multiple NAMs and ASRs.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

Note This feature is supported for NAMs and ASRs. For more information on minimum IOS XE version supported on ASRs, see the *Cisco ASR 1000 Series Aggregation Services Routers Release Notes*.

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, the operator runs the Packet Capture feature against the NAMs or ASRs for each branch, then runs the Packet Decoder to inspect the suspicious traffic.

Step 1 Create a capture session definition:

a. Choose **Operate > Operational Tools > Packet Capture > Capture Sessions**, then click **Create** to create a new capture session definition.

b. Complete the **General** section as needed. Give the session definition a unique name and specify how you want to file the captured data. To capture the full packet, enter 0 in the Packet Slice Size.

c. 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. If you do not create a software filter, it captures everything.

d. In the **Devices** area, you can select:

   - A NAM and its data ports. You can create one capture session per NAM only, whether the capture session is running or not.
   - An ASR and its interfaces.

e. Click **Create and Start All Sessions**.

Prime Infrastructure (with licensed Assurance features) saves the new session definition, then runs separate capture sessions on each of the devices you specified. It stores the sessions as files on the device and displays the list of packet capture files in the **Capture Files** area.

Step 2 To decode a packet capture file:

a. Choose **Operate > Operational Tools > Packet Capture**.

b. Select a PCAP file in a NAM or ASR device.

c. Select **Copy To** to copy the PCAP file to the PI server (the decode operation only runs on files in the PI server).

d. Click **View Jobs t**o confirm that the copy job completed successfully.

e. Open the localhost folder, click the check box for the new capture file, then click **Decode**. The decoded data appears in the bottom pane.

f. A TCP Stream displays the data as the application layer sees it. To view the TCP Stream for a decoded file, select a TCP packet from the Packet List, then click **TCP Stream**. You can view the data as ASCII text or in a HEX dump.

Step 3 To run a packet capture session again, select the session definition in the **Capture Sessions** area and click **Start**.

Diagnosing Site Connectivity Issues and Comparing Configurations

You can use the Prime Infrastructure dashboards to monitor your network and locate problematic devices, and then use the Device Work Center 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 the name of the device for which you see the most alarms.

Step 4 From the 360° view of the device, click the Alarm Browser icon to see the alarms for that device. Expand an alarm to view details about the alarm.

Step 5 To compare the current device configuration with a previous, known good configuration, choose **Operate > Device Work Center**, then select the device whose configuration that you want to change.

Step 6 Click the **Configuration Archive** tab, expand the arrow to view additional options, and select the configuration type and a configuration against which to compare.

Step 7 Change or roll back the configuration. See Rolling Back Device Configuration Versions, page 14-4 for more information.

Monitoring a Controller or a Specific AP

Use these dashlets to filter on a controller or a specific AP:

- Top N Applications
- Top N Clients
- Top N Application Groups (not a default dashlet; you must add it to the Detail Dashboard)
- Client Conversations (not a default dashlet)

Before You Begin

If you have not set up a building, floor, and AP, choose **Operate > Maps**, create a building and a floor under a site, then associate that floor with an AP. For example, site=System Campus, building=bldgN, floor=Floor1.

- To filter site data, use this AP in the Detail Dashboards. Choose **Operate > Monitoring Dashboards > Detail Dashboards > Site**.
- To collect only traffic that is associated with the APs on that floor, choose (for example) **Filters > Site > System Campus > bldgN > Floor1** and click **Go**.

To filter on a controller or a specific AP:

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards**, then click the **Site** tab.

Step 2 To enable filtering on a controller or a specific AP:

a. Click the **Dashlet Options** icon (for one of the dashlets that support filtering), then click the **Enable Controller Filter** check box.

b. Select a controller.

c. Optionally, select an AP.

Step 3 Use the Device dashboard to choose:

- A device assigned to a site
- A device from the list of all devices
- A device that is sending NetFlow information to the Prime Infrastructure server

Step 4 Add the **Top N Applications** and **Top N Hosts** dashlets to **Detail Dashboards > Device**. These dashlets will display, using the NetFlow data being sent, what the top applications are. You can then select a device and see the type of traffic that is going through that device.

Step 5 You can create a similar filter using the **End User Experience** dashboard to select a user name, an IP address, or a MAC address. If you click **Select from Client List** and choose an IP address, the user data will be filled in automatically.

Post-Deployment Application Monitoring

Prime Infrastructure with licensed Assurance features 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.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

In the following workflow, a network administrator is responding to scattered complaints from multiple branches about poor performance for a newly deployed application. The network administrator 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 Choose **Operate > Monitoring Dashboards > Detail Dashboards > Application**.

Step 2 To limit all of the dashlets on this page to the newly deployed application, select the application from the **Filters** line and click **Go**.

Step 3 Add the following dashlets to this dashboard:

- Application Traffic Analysis
- Top N Devices with Most Alarms
- Worst N Clients by ART Metrics
- Worst N Sites by ART Metrics

Step 4 Find 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 5 Compare the data in the **Application Server Performance** dashlet with the data in **Worst N Clients by ART Metrics** and **Worst N Sites by ART Metrics**. See if peaks in server response time match one or more users' experience of poor transaction times, or are more generalized across sites.

Step 6 Check the **Application Traffic Analysis** dashlet 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 7 Check the **Top N Clients** dashlet to identify the largest bandwidth consumers for the application. Then find the **Worst N Sites by ART Metrics**, and compare the information in these two dashlets to see if the biggest bandwidth consumers are also part of the worst-performing sites.

Step 8 Examine the worst site in **Worst N Sites by ART Metrics**. Click 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 9 On the Site Detail Dashboard, check the **Top N Applications** and **Top N Clients** 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 10 On the Site Detail Dashboard, check the **Top N Devices with Most Alarms** to see if any of the site's servers or edge routers currently have alarms that might indicate why the application performance at this site is so poor.

Step 11 On the Incidents Dashboard, check for the **Device Reachability Status** to confirm if the suspect device is still reachable. If it is, to launch its 360 View, hover your mouse cursor on the device IP address, then click the icon that appears.

Step 12 In the Device 360 View:

a. Click the **Interfaces** tab and confirm that sessions for the affected application flow over this device.

b. Click the **Alarms** tab to see a summary of current alarms for the device.

Step 13 If this device seems to be the source of the application performance problem at this site:

a. Click the Alarm Browser icon at the top of the 360 View to see all alarms for this device.

b. Use the **Show** field to limit the alarms shown to those in the time frame of the problems.

Securing Network Services

Cisco TrustSec Identity-Based Networking Services (IBNS) is an integrated solution consisting of Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. Cisco TrustSec IBNS help enterprises to increase productivity and visibility, reduce operating costs, and enforce policy compliance.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

In Prime Infrastructure, the TrustSec network service design enables you to choose preferred options for provisioning configurations to TrustSec-capable devices to enable 802.1X and other TrustSec functionality. You can configure wired 802_1x devices by creating TrustSec model-based configuration templates and choosing any one of the following navigation paths:

- Design > Network Services > Features-TrustSec > Wired 802_1x.
- Design > Configuration > Feature Design > Features and Technologies > Security > TrustSec > Wired 802_1x

Note that for Catalyst 6000 devices:

- **Security violation as protect** is not available for Catalyst 6000 supervisor devices.
- **Security violation as replace** is available in Cisco IOS Release 15.1(01)SY and later.
- The command **macsec** is not available for Catalyst 6500 supervisor 2T devices.

For more details about configuring TrustSec model-based configuration templates, see Creating Feature-Level Configuration Templates, page 8-2.

Generating a TrustSec Readiness Assessment Report

TrustSec Readiness Assessment displays TrustSec-based device details such as TrustSec version, readiness category, readiness device count, and device percentage displayed in the pie chart.

To generate a TrustSec Readiness Assessment report:

Step 1 Choose **Design > Network Services > Features-TrustSec > Readiness Assessment**.

A pie chart appears with the following types of devices:

- TrustSec Limited Compatibility Devices
- TrustSec Capable Devices
- TrustSec Hardware Incapable Devices
- TrustSec Software Incapable Devices

Step 2 Click **Section view** and click any of the pie chart slices to view the details of the selected TrustSec-based device type.

Step 3 Click **Complete view** to view the details of all TrustSec-based devices.

Step 4 Select the TrustSec version and click **Export** to export the readiness assessment details to a CSV file.

CHAPTER 11

Monitoring Alarms

An *alarm* is a Cisco 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 condition no longer occurs.

What Is an Event?

An *event* is an occurrence or detection of some condition in or 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 result from:

- 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.
- 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 with 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 on the Prime Infrastructure server; for example, rebooting the server.
- By receiving events when the status of an 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 predefined patterns, the event is considered 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.

Recurring Alarms and Events

To reduce the amount of unnecessary alarms and events, Prime Infrastructure detects underlying causes for events and modifies when it issues alarms and events when devices have any of the following problems:

- Repeated restart—When a device repeatedly restarts and is continuously cycling (because, for example, there is a problem with the device or its software), Prime Infrastructure generates a *Repeated Restart* event if the same device sends a cold start or warm start trap a repeatedly within a short time period.
- Flapping—Prime Infrastructure detects when several link up and link down traps are received for the same interface within a short time period and creates a *Flapping* event.
- Module or Link Fault—If a module is down, Prime Infrastructure creates one *Module Down* alarm only, and associates all of the interfaces' link down events to the Module Down alarm. When the module state is restored, Prime Infrastructure clears the module alarm and all interface messages are associated to the cleared alarm.

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 verifying that 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 state changes to a historical event when the fault is resolved in a network.

A cleared alarm represents the end of an alarm's lifecycle. A cleared alarm can be revived if the same fault recurs within a preset period of time. The default is 5 minutes.

Event and Alarm Association

Prime Infrastructure maintains a catalog of events and alarms. This catalog contains a list of events and alarms 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 to raise an event.
3. If an event is raised, Prime Infrastructure decides if the event triggers a new alarm or if it is associated with an existing alarm.

A new event is associated with an existing alarm if the new event is of the same type and occurs on the same source. For example, for an active interface error alarm, if multiple interface error events occur on the same interface, are all associated with the same alarm.

Alarm Status

Table 11-1 provides alarm status descriptions.

Table 11-1 Alarm Status Descriptions

Alarm Status	Description
New	When an event triggers a new alarm or a new event is associated with an existing alarm.

Table 11-1 Alarm Status Descriptions

Alarm Status	Description
Acknowledged	When you acknowledge an alarm, the status changes from New to Acknowledged.
Cleared	A cleared alarm can involve any of the following: • Auto-clear from the device—The fault is resolved on the device and an event is triggered for the device. For example, a device-reachable event clears a 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 the alarm is cleared. • If a fault continues to exist in the network, a new event and alarm are created subsequently, based on event notification (traps/syslogs).

Event and Alarm Severity

Each event has an assigned severity. Events fall broadly into the following severity categories, each with an associated color in Prime Infrastructure:

- Flagging (indicates a fault)—Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- Informational—Info (blue). Some informational events clear flagging events.

For example, a Link Down event might be assigned Critical severity, while its corresponding Link Up event will be 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 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, and time stamp. You can change the status of alarms, and assign, annotate, delete, and specify email notifications from this page.
Hover your mouse 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 and 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.

Where to Find Syslogs

Prime Infrastructure logs all emergency, alert, and critical messages generated by all devices that are managed by Prime Infrastructure.

Prime Infrastructure also logs all SNMP messages and syslogs it receives. To view syslogs, choose **Operate > Alarms & Events**, then click the **Syslogs** tab.

Syslog Pre-defined Filters

Prime Infrastructure uses the following syslog filters:

- Severity 0 and 1
- Severity 2
- Environmental Monitor
- Memory Allocation Failure
- Catalyst Integrated Security Features
- Cisco IOS Firewall Denial of Service

Defining Alarm Thresholds

Use monitoring templates to define thresholds. When the thresholds that you specify are reached, Prime Infrastructure issues an alarm.

Step 1 Choose **Design > Configuration > Monitor Configuration**.

Step 2 Expand the Features menu on the left and choose **Threshold**.

Step 3 Complete the basic template fields. For descriptions of the template parameters, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 4 Under the Feature Category, choose one of the following metrics:

- Device Health—Change threshold values for CPU utilization, memory pool utilization, and environment temperature.
- Interface Health—Change threshold values for the number of outbound packets that are discarded.

Step 5 Under Metric Parameters, choose the threshold setting that you want to change, then click **Edit Threshold Setting**.

Note If you configure multiple threshold settings or parameters, Prime Infrastructure raises an alarm when *any* of the thresholds are reached.

Step 6 Enter a new value, choose the alarm severity to assign when the threshold is met or exceeded, and click **Done**.

Step 7 Click **Save as New Template**.

Step 8 You can now deploy the template (see Deploying Monitor Configuration Templates, page 8-17).

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 Select an alarm, then 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 an alarm and choose **Change Status > Acknowledge**.

If the device generates a new violation on the same interface, Prime Infrastructure does 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 on either the Alarm Summary page or in any alarm list. Also, no emails are generated for acknowledged alarms. 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.

Note When you acknowledge an alarm, a warning message appears 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 show activity for only 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 Settings > 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

You might want to change the schedule for deleting alarms, the alarm severities that are displayed, or alarm email options.

To change alarm and event options:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Alarms and Events**.

Step 3 Change the alarm or event settings, then click **Save**.

Configuring Alarm Severity Levels

A newly generated alarm has a default severity level that you might want to change.

To configure an alarm's severity level:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Severity Configuration**.

Step 3 Check the check box of the alarm condition whose severity level you want to change.

Step 4 From the Configure Security Level drop-down list, choose a severity level, then click **Go**.

Step 5 Click **OK** to confirm the changes.

Getting Help for Alarms

If you receive an alarm in **Operate > Alarms & Events** for which you cannot find a resolution in the Cisco Support Community (click on an alarm, then choose **Troubleshoot > Support Forum**.), you can use Prime Infrastructure to open a support request (click on an alarm, then choose **Troubleshoot > Support Case**). See "Troubleshooting Prime Infrastructure" in the *Cisco Prime Infrastructure 2.0 Administrator Guide* for more information.

CHAPTER 12

Updating Device Inventory

Cisco 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, and schedule the discovery job. See Changing Discovery Settings, page 12-1.
- Changing Discovery Settings
- Scheduling Discovery Jobs
- Monitoring the Discovery Process
- Discovery Protocols and CSV File Formats
- Updating Device Inventory Manually
- Importing Device Inventory
- Troubleshooting Unmanaged Devices
- Managing Device Groups
- Synchronizing Devices

Changing Discovery Settings

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

Step 2 Click **New**. Enter the settings as described in Table 3-1.

Step 3 Click one of the following:

- **Save** to save the settings.
- **Run Now** to save the settings and immediately start the discovery job.

Scheduling Discovery Jobs

To create a discovery job to run at a future time:

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

Step 2 Enter the required settings, then click **Save**. For descriptions of the template parameters, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 3 In the Discovery Settings, select the discovery job that you just created, then click **Schedule**.

Step 4 Enter the schedule information page, 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 the following 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 12-1 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 12-1 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.
Cisco Discovery Protocol (CDP)	Any valid IP address and the hop count, separated by a comma.
Routing table	Any valid IP address and the hop count, separated by a comma.
Address Resolution Protocol (ARP)	Any valid IP address and the hop count, separated by a comma.

Table 12-1 Discovery Protocols and CSV File Formats

Protocol	CSV File Format
Border Gateway Protocol (BGP)	Seed device IP address for any device that is BGP enabled.
Open Shortest Path First (OSPF)	Seed device IP address for any device that is OSPF enabled.

Updating Device Inventory Manually

We recommend that you run discovery to update your device inventory. However, you can also add devices manually, if needed.

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 that you specified.

Importing Device Inventory

If you have another management system to which your devices are to be 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 of 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 12-2 describes the possible reasons a device is unmanageable by Prime Infrastructure:

Table 12-2 Reasons for Unmanageable Device

Possible Reason	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.	• Use the ping and traceroute tools to verify that Prime Infrastructure can reach the device. See Getting Device Details from the Device 360° View for more information. • If the device is reachable, verify that the retry and timeout values set for the device are sufficient. (Choose **Operate > Device Work Center**, select the device, then click **Edit**.) • Verify that SNMP is configured and enabled on the device: – If using SNMPv2, verify that the *read-write* community string configured on the device is the same as that entered in Prime Infrastructure. The read-write community string is required. – If using SMNPv3, verify that the following parameters are configured on the device, and that the configured parameters match those entered in Prime Infrastructure: Username AuthPriv mode (noAuthNoPriv, authNoPriv, authPriv) Authentication algorithm (for example: MD5, SHA) Authentication password Privacy algorithm (for example: AES, DES) Privacy password • Verify that the SNMP credentials configured on the device match the SNMP credentials configured in Prime Infrastructure. • Reenter the SNMP credentials in Prime Infrastructure, then resynchronize the device. (Choose **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.	• Verify that Telnet or SSH is configured and enabled on the device, and that the same protocol is configured on Prime Infrastructure. (Choose **Operate > Device Work Center**, select the device, then click **Edit**.) If the device type requires HTTP, verify that the Prime Infrastructure HTTP parameters match those configured on the device. • Verify that the username, Telnet or SSH passwords, and 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 12-2 Reasons for Unmanageable Device (continued)

Possible Reason	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. We recommend that you allow all CLI commands for the Prime Infrastructure user account; or alternatively, exclude only commands that absolutely must be 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

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 that you created to push the configuration change to all of the devices contained in the group.

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 a device group by hovering your mouse on the device group folder.

You can create a new group that can be one of two types:

- Static—Add devices to a static group using the **Add to Group** button from **Operate > Device Work Center**.
- Dynamic—Specify the rules to which devices must comply 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.

Device 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 a *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 to 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 and group description, and select a parent group, if applicable.

Step 4 Deselect **Static Group** so that you can specify the rules to which all devices must comply to be added to the group, or if you want to manually add the devices to the group; this means that the group will *not* be rule-based.

Step 5 Specify the rules that you want to apply to the devices in the group.

Note You can create a rule using the UDF label defined in Administration > System Settings > User Defined Field.

Step 6 Click **Save** to add the device group with the settings you specified.

The device group that 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 that you want to assign to a group, then click **Add To Group**.

Step 3 Select a group, then click **Save**.

Synchronizing Devices

To synchronize the Prime Infrastructure database with the configuration running on a device, you can force an inventory collection.

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

Step 2 Select the device whose configuration you want synchronized with the configuration stored in the Prime Infrastructure database.

Step 3 Click **Sync**.

CHAPTER 13

Configuring Device Features

Use configuration templates in Prime Infrastructure to design the set of device configurations that you need to set up the devices in a branch or change the feature configuration for a device from the Device Work Center.

Configuring the Device using WSMA

Prime Infrastructure mainly uses the CLI method (over Telnet or SSHv2) to configure the devices. In Cisco Prime Infrastructure 2.0, you can use WSMA (over SSHv2) for configuring specific features on the ASR and ISR devices. Cisco Web Services Management Agent is a more efficient and more robust method to configure the devices. Prime Infrastructure 2.0 supports Zone Based Firewall and Application Visibility configuration via WSMA on the ASR and ISR devices.

To configure Zone Based Firewall or Application Visibility via WSMA:

Step 1 Add or edit the device in Prime Infrastructure to use SSHv2 (rather than Telnet) as the management transport protocol.

a. When you add the device with automatic discovery, enter the SSH credentials.(Adding Devices Using Discovery.)

b. When you add the devices manually (Adding Devices Manually), in Step 2, select SSH2 as the protocol.

Step 2 If the device is also managed by Prime Infrastructure which is not configured to use SSH2, edit the device credentials:

a. Choose **Operate** > **Device Work Center**.

b. Select the device and click **Edit**.

c. Change the protocol to **SSH2**.

d. Click **Update**.

Step 3 Activate a WSMA profile on the device by configuring a WSMA configuration profile as follows:

```
#configure terminal
wsma agent config profile PIwsmaConfigServiceSSH
#exit

#wsma profile listener PIwsmaConfigServiceSSH
no wsse authorization level 15
transport ssh subsys wsma-config
#exit
```

For more information about WSMA, see the *WSMA Configuration Guide*.

Step 4 Configure a configuration archive, which will be used by WSMA for handling transactional configurations and rollbacks by using the following CLI commands on the device:

```
#configure terminal
archive
log config
hidekeys
path flash:roll
maximum 5
#end
```

For more information about configuration archives, see the *Cisco IOS Configuration Fundamentals Command Reference Guide*.

Configuring Application Visibility

The Application Visibility feature allows you to monitor traffic on specific interfaces and generate performance and bandwidth-statistics reports that supply information to the various dashlets and reports in Prime Infrastructure. Devices send these reports to Prime Infrastructure, and each report supplies information to a subset of the Prime Infrastructure dashlets and reports. Prime Infrastructure can configure Application Visibility either through CLI (over Telnet or SSH) or through WSMA. Application Visibility can be configured through WSMA in a more efficient and robust method and we recommend that you use the WSMA protocols for configuring Application Visibility. For more information on using WSMA with Prime Infrastructure, see the section Configuring the Device using WSMA, page 13-1.

The Application Visibility feature is supported on the following platforms:

- ASR platform from Cisco IOS-XE Release 15.3(1)S1 or later
- ISR G2 platform from Cisco IOS Release 15.2(4)M2 or later
- ISR G3 platform from Cisco IOS-XE Release 15.3(2)S or later

- CSR platform from Cisco IOS-XE Release 15.3(2)S or later

Application Visibility is configured differently on the ASR platform running Cisco IOS-XE15.3(1)S1 in comparison to Cisco IOS-XE15.3(2)S or later releases. After an ASR platform Cisco IOS release is upgraded from Cisco IOS-XE15.3(1)S1 to Cisco IOS-XE Releases 15.3(2)S or later, we recommend that you re-configure Application Visibility on those devices.

To simplify configuration, the Application Visibility feature is split into four types of metric and NetFlow reports:

Report	Description
Traffic Statistics	Sends the statistics on the bandwidth consumed by each of the NBAR-recognized applications on a per-user and per-interface basis. This report supplies information to the various application bandwidth dashlets and reports in Cisco Prime Infrastructure as “Top N Applications”, “Application Bandwidth reports”, “Top N clients”, and so on.
HTTP URL Visibility	Sends performance and bandwidth reports for HTTP-based traffic, and this report supplies information to various URL dashlets and reports in Cisco Prime Infrastructure as “Top N URL by hits” and “Top N URL by response time”. **Note** The HTTP URL Visibility tool is not supported on the ISR-G2 device.
Application Response Time	Sends performance-related information for TCP traffic, and this report supplies information to various response time dashlets and reports in Cisco Prime Infrastructure as “applications ART analysis”, “worst N clients by transaction time”, and so on.
Voice/Video Metrics	Sends various RTP key-performance indicators for RTP-based voice/video traffic, and supplies information to dashlets and reports in Cisco Prime Infrastructure under the voice/video category as “worst N RTP streams by packet lost.”

Activating the Application Visibility feature can impact device performance. To minimize the potential impact, the template allows you to select the traffic interfaces to monitor and the reports to generate.

To configure application visibility in your network:

1. (Optional) Set up WSMA on the devices to assure that the devices is configured via the WSMA protocol, rather than CLI (for more information, see Configuring the Device using WSMA, page 13-1). WSMA provides a more robust configuration mechanism.
2. Make sure that your devices are running an up-to-date NBAR protocol packs (see NBAR Protocol Packs, page 13-5).
3. Estimate the potential resources impact on the device (CPU and memory) before activating application visibility on the device (for more information, see Activating or Deactivating a Troubleshooting Session, page 13-9).
4. Activate application visibility on the device, either by creating a template and pushing it across the network (for more information, see Creating an Application Visibility Template, page 13-5), or by enabling AVC on an interface from the Device Work Center (see Enabling Default Application Visibility on an Interface, page 13-7).

Estimating CPU, Memory and NetFlow Resources on ASR Devices

The Device Resource Estimation (DRE) feature allows you to estimate CPU consumption, memory usage, and NetFlow export traffic when you deploy application visibility features on an ASR device. DRE helps you analyze the demands for these resources on ASR devices based on typical pre-defined traffic profiles and device interface speeds.

DRE is supported on all ASRs running Cisco IOS-XE Release 15.3(1)S1 or later with one or more of these modules installed:

- cevModuleASR1000ESP5
- cevModuleASR1000ESP10
- cevModuleASR1000ESP20
- cevModuleASR1001ESP
- cevModuleASR1002FESP

To estimate the resource utilization on a specific device:

Step 1 Choose **Operate > Operational Tools > Device Resource Estimation**.

Step 2 In the Interface column for the device you want estimates on, click the down arrow icon.

The list shows only those interfaces supporting Application Visibility capability.

Step 3 Select **Internet Profile** or **Enterprise Profile**. The device resource estimation is based on a typical traffic profile. Select “Internet Profile” for typical service-provider traffic, or “Enterprise Profile” for a typical enterprise-traffic.

Step 4 Select the interfaces for which you want to estimate the resource utilization.

Speeds shown are those currently configured for each interface. If you want to base the estimate on a different speed, click **Speed (Mbps)** and enter a different value. The changes will be retained as long as you continue working with Device Resource Estimation.

Step 5 Click **Get Estimates**.

The Estimated Resource Usage graph displays the current, additional, and total usage of the CPU and memory, along with the threshold limit for these resources. The estimated and maximum NetFlow export traffic are also given. For devices on which AVC is already enabled, only the current and additional usage is shown.

If resource usage is crossing threshold limits, optimize the problem device by:

- Decreasing current CPU utilization
- Increasing configured memory
- Reduce configured interface speed
- Redirecting traffic to another device

NBAR Protocol Packs

The ability of the device to produce application visibility reports is based on the NBAR technology; NBAR, or Network-Based Application Recognition, is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/User Datagram Protocol (UDP) port assignments.

NBAR is updated frequently to support new applications and protocols, the software update for an NBAR is called a Protocol Pack.

Further information on NBAR protocol packs and information on how to upgrade NBAR protocol pack, see the *NBAR Protocol Packs Guide.*

When you upgrade an NBAR protocol pack on the device, a corresponding Prime Infrastructure update should be performed to update Prime Infrastructure with the supported protocols/applications on the devices.

To achieve that there is a periodic Prime Infrastructure software update (UBF file) issues when new protocol packs are released. Once you upgrade the NBAR protocol pack on the device, you should use Prime Infrastructure software upgrade to make sure Prime is also updated with the latest protocols.

At every point of time the network may contain various platforms (ISR-G2/ASR) running different Cisco IOS software releases and different protocol pack releases. While we do not recommend that you have different protocol pack releases installed on different devices reporting application visibility reports simultaneously, Prime Infrastructure will be able to support this, by configuring only the supported subset of protocols/applications, defined as filtering conditions in your template, on each of the devices, when deploying an application visibility template across multiple devices running different versions of NBAR protocol packs.

Creating an Application Visibility Template

An application visibility monitoring policy is defined on a selected group of interfaces. When you define the template, ensure that you have defined an interface-role object which matches the group of interfaces on which you would like to monitor the traffic and generate netflow reports. See Creating an Interface Role, page 13-40.

To create an Application Visibility template:

Step 1 Choose **Design > Feature Design > Features and Technologies > Application Visibility > AVC Configuration**.

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

Step 3 In the Validation Criteria area, choose a device type from the list and enter the OS version.

Step 4 In the Template Detail area, choose an Interface Role from the drop-down list. The interface role designates the group of interfaces on which you can monitor the traffic and produce Application-Visibility reports. See the Creating an Interface Role, page 13-40 section for information about creating an interface role.

Step 5 In the Traffic Statistics area, you can determine which traffic should be monitored to produce the traffic statistics reports, select the **Off** radio button if you do not want to collect the statistics on data packets.

a. Select the IP address/subnets.You can generate the report only on IPv4 traffic. We recommend to configure the required minimal set of filter.

b. In the Advanced option, you can monitor only ingress or egress traffic or you can monitor both the ingress and egress traffics. Select only the relevant traffic to be monitored to reduce the performance impact on the device. Select the Direction from the drop-down list.

Step 6 In the HTTP URL Visibility area, you can select the traffic that should be monitored to produce the report. Select the **Off** radio button if you do not want to collect URL statistics.

a. Select the IP address/subnets. You can select a specific set of IPv4 addresses or subnets to be monitored.

b. Select the Application from the drop-down list. You can select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all of the enterprise related http-based applications are included in the list.

c. In the Advance options, choose the Sampling Rate and Direction from the drop-down list. Choose the report that runs only on ingress or egress traffic to reduce the performance impact on the device. Also, change the sampling rate for the report. If you collect performance and visibility data for every HTTP transaction, it may lead to high resource consumption on the device. Sampling is used to optimize the resource consumption by collecting the information for “1” out of every “n” http connections where “n” is the selected sampling rate.

Step 7 In the Application Response Time area, you can determine the traffic that should be monitored to produce the application response time reports. Also, optionally set a sampling option for the reports. Select the **Off** radio button if you do not want to collect ART metrics.

a. Select the IP address/subnets. You can select a specific set of IPv4 addresses or subnets to be monitored.

b. Choose the Application from the drop-down list. You can select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all of TCP traffic is monitored.

c. In the Advanced Options, choose the Sampling Rate from the drop-down list. In High scale environments, collecting performance indicators for every TCP conversation can lead to high resources consumption on the device. The sampling option provides the ability to further optimize the resource consumption by collecting the performance indicators for “1” out of every “n” TCP conversation. This advanced option can be used to activate sampling and select the sampling rate for the tool. It is not recommended to activate sampling as activating sampling leads to less accurate results. Sampling should be used when it is necessary to limit the resource consumption on the devices.

Note Sampling option is not applicable for ISR-G2 routers. This option will be ignored for the ISR-G2.

Step 8 In the Voice/Video metrics area, you can determine the traffic that should be monitored to produce the voice/video reports. Select the **Off** radio button if you do not want to collect the voice/video metrics.

a. Choose the IP address/subnets. You can choose a specific set of IPv4 addresses or subnets to be monitored.

Note IP Filtering is not supported on the ISR-G2 router unless all UDP traffic is monitored.

b. Choose the Voice/Video Application from the drop-down list. You can choose a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all RTP enterprise-related applications are monitored.

Step 9 Click **Save as New Template**.

Enabling Default Application Visibility on an Interface

From the Device Work Center, you can view the reports that are generated on each of the interfaces and enable or disable a default Application Visibility configuration on selected interfaces.

When a device does not have an application visibility configuration deployed on it, or it has a default application visibility configuration deployed on it (if all metrics are collected with a set of default parameters), the Device Work Center allows you to enable or disable a default application visibility configuration on the device by selecting interfaces on the device and enabling or disabling the default configuration on the interfaces.

Note When you deploy an application visibility template to the device, the application visibility template configuration will overwrite the default application visibility configuration that was enabled from the Device Work Center.

The default configuration collects all the possible visibility metrics on all applicable IPv4 traffic.

Note The Application Visibility feature is supported on the following platforms:

- ASR platform from Cisco IOS-XE Release 15.3(1)S1 or later
- ISR G2 platform from Cisco IOS Release 15.2(4)M2 or later
- ISR G3 platform from Cisco IOS-XE Release 15.3(2)S later
- CSR platform from Cisco IOS-XE Release 15.3(2)S later

Note Application Visibility is configured differently on the ASR platform running Cisco IOS-XE15.3(1)S1 in comparison to Cisco IOS-XE15.3(2)S or later releases. After an ASR platform Cisco IOS release is upgraded from Cisco IOS-XE15.3(1)S1 to Cisco IOS-XE Releases 15.3(2)S and later, we recommend that you reconfigure Application Visibility on those devices.

If the device does not have any AV configuration deployed on it, select one of the default Application Visibility configuration profiles:

- Default AP for IPv4—Collects all of the possible visibility metrics on all applicable IPv4 traffic
- Default AV for IPv4+IPv6—Collects all of the possible visibility metrics on all IP traffic

If the device has already one of the default configuration deployed on it, you should be able to enable or disable the same configuration on a selected group of interfaces.

To change the default application visibility configuration profile configured on the device, first disable AV on all interfaces and then re-enable it on the selected interfaces with the new profile.

To enable or disable the default application visibility configuration on the specific interface:

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

Step 2 After choosing the device from list, click **Configuration**. The Feature Configuration pane appears.

Step 3 Expand the **Application Visibility folder** and choose **Interfaces**.

Step 4 Do one of the following:

- To activate the default application visibility configuration, select one or more interfaces, then click **Enable Default AVC**. When you enable application visibility on a device that does not have any application visibility configuration deployed on any of its interfaces, choose either the IPv4 profile or the IPv4+IPv6 profile.
- To disable the default application visibility configuration, select one or more interfaces, then click **Disable Default AVC**.

Application Visibility Troubleshooting Sessions

You can collect application visibility data on every flow that goes through the monitored interface. However, because this can have a significant impact on the device performance, application visibility data is collected in an aggregated manner. To further troubleshoot specific flows, you can activate the Application Visibility troubleshooting sessions on the device. The sessions are activated on specific interfaces and on specific traffic. They allow you to collect the non aggregated information on a flow-based level that supplies a raw-netflow report in Prime Infrastructure. This information can be used later to analyze specific flows.

The Application Visibility Troubleshooting feature allows you to:

- Create and activate a troubleshooting session on a specific interface
- Deactivate and delete a troubleshooting session on a specific interface

Caution To avoid overloading the server, we recommend that you configure no more than ten active troubleshooting sessions. Application troubleshooting is not supported on the ISR-G2 platforms.

Note Troubleshooting sessions are configured differently on the ASR platform running Cisco IOS-XE Release 15.3(1)S1 in comparison to Cisco IOS-XE Release15.3(2)S or later releases. After, an ASR platform Cisco IOS Release is upgraded from Cisco IOS-XE Release 15.3(1)S1 to Cisco IOS-XE Release 15.3(2)S or later, we recommend that you deactivate and reactivate active troubleshooting sessions on those devices.

To troubleshoot Application Visibility:

Step 1 Choose **Operate > Application Troubleshooting**.

Step 2 In the AVC Troubleshooting Session page, click **Add** and enter a Session Name.

Step 3 In the Source/Destination IPs field, click **Edit**, and choose the source and destination IP addresses from the drop-down list. You can select the IP traffic and collect Application Visibility troubleshooting information for that specific IP traffic. The options are: on all IPv6 traffic or on all IPv4 traffic or on specific IPv4 addresses/subnets. Also, you can select a list of IP constraint pairs. Each such pair designates a bi-directional symmetric condition on the source and destination IPs of the traffic. For example, the pair: Any IPv4 <=> IPv4 subnet 192.168.0.0/16 matches all of the flows from 192.168.0.0/16 to any other IP and vice-versa (all of the flows from any IP address to 192.168.0.0/16). You can add multiple pair conditions.

Step 4 To add more IP constraints in the format of IP source/destination pairs, click the + icon in the Select Source Destination dialog box.

Note The IP addresses on both sides of the pairs should be of the same IP version.

Step 5 Click **OK**.

Step 6 Choose the device from the Device Table list.

Step 7 Choose the interface from the Interface Table list.

Step 8 Choose the application from the object selector dialog box. When you choose the applications, you can have a combination of Categories, Sub-categories, Encrypted Applications, and Tunneled Applications from the available list. A maximum of 32 applications or categories or attributes can be selected.

Step 9 Click **Save** to automatically activate the session.

Step 10 After the troubleshooting session is activated, click **Launch Report** to generate the Raw NetFlow report.

Activating or Deactivating a Troubleshooting Session

You can activate an inactive troubleshooting session or deactivate an existing troubleshooting session.

To activate or deactivate a troubleshooting session:

Step 1 Choose **Operate > Operational Tools > Application Troubleshooting**.

Step 2 Choose a troubleshooting session from the list and click **Activate** or **Deactivate**.

Step 3 Click **Save**.

Editing or Deleting a Troubleshooting Session

You can edit or delete an inactive troubleshooting session. (To edit or delete an active session, you must deactivate it first.)

To edit or delete a troubleshooting session:

Step 1 Choose **Operate > Operational Tools > Application Troubleshooting**.

Step 2 Do either of the following:

a. Choose a session from the list and click **Edit**.

Caution To avoid overloading the server, we recommend that you configure no more than ten active troubleshooting sessions.

b. Edit and save the troubleshooting session, then click **Activate**.

c. To delete a troubleshooting session, choose a session from the list and click **Delete**.

Creating a VPN Component Template

This section describes how to create various VPN component template.

Creating an IKE Policies Template

Step 1 Choose **Design > Feature Design > Features and Technologies > Security > VPN Components > IKE Policies**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS version. For more information about the required field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 4 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Creating an IKE Settings Template

Step 1 Choose **Design > Feature Design > Features and Technologies > Security > VPN Components > IKE Settings**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version. For more information about the required field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 4 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Creating an IPsec Profile Template

Step 1 Choose **Design > Feature Design> Features and Technologies > Security > VPN Components > IPSec Profile**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Template Detail area, click **Add Row** and enter the required information. A transform set represents a certain combination of security protocols and algorithms. During the IPSec negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform set describes a particular security protocol with its corresponding algorithms. For more information about the required field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 5 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Creating a Preshared Keys Template

Step 1 Choose **Design > Feature Design > Features and Technologies** > **Security > VPN Components > Pre-shared Keys**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

Step 4 In the Template Detail area, click **Add Row** and enter the required information.

Step 5 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Creating RSA Keys Template

Step 1 Choose **Design > Feature Design > Features and Technologies** > **Security > VPN Components > RSA Keys**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Template Detail area, click **Add** and enter the required information.

Step 5 Select the **Exportable** box to generate RSA as an exportable key, then click **OK**.

Step 6 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Creating a Transform Sets Template

Step 1 Choose **Design > Feature Design > Features and Technologies > Security > VPN Components > Transform Sets**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Template Detail area, click **Add Row** and enter the required information.

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 5 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Configuring an Easy VPN Server

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device; for example, any of the following:

- Cisco VPN 3000 concentrator
- Cisco PIX Firewall
- Cisco IOS router that supports the Cisco Unity Client Protocol

After the Cisco Easy VPN server is configured, a VPN connection is created with minimal configuration on an Easy VPN remote, such as a Cisco 800 series or 2800 series router. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

Creating an Easy VPN Server Proxy Setting Template

The Easy VPN Server Proxy feature allows you to specify the settings for Easy VPN clients. Using this feature, you do not have to manually modify the proxy settings of the web browser when you connect to the corporate network using the Cisco IOS VPN client or manually revert the proxy settings when you disconnect from the network.

To create an Easy VPN Server Proxy template:

Step 1 Choose **Design > Feature Design**.

Step 2 From the **Features and Technologies** folder, expand the **Security** subfolder, then click **Easy VPN Server Proxy Setting**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 In the Template detail area enter a name, and choose the settings that you want to associate with the group.

Step 6 Choose the No Proxy Server option or Automatically Detect Proxy Settings option if you want the clients in this group to automatically detect a proxy server when they use the VPN tunnel.

Step 7 Choose the Manual Configuration option to manually configure a proxy server for clients in this group. If you choose this option, you should manually configure a proxy server.

Step 8 Check the **Bypass proxy server for local addresses** check box to prevent the clients from using the proxy server for local (LAN) addresses.

Step 9 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Creating an Easy VPN Remote Template

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server.

Before You Begin

Create an ACL template and publish the ACL template.

To create a Easy VPN Remote template:

Step 1 Choose **Design > Feature Design**.

Step 2 From the **Features and Technologies** folder, expand the **Security** subfolder, then click **Easy VPN Remote**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 In the Easy VPN Remote Interface Configuration area, enter the required information.For more information about the required field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 6 In the Easy VPN Remote connection characteristics area, enter the required information.For more information about the required field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Note If you enable identical addressing, you must first configure Easy VPN Remote in network extension mode.

Step 7 In the Remote Authentication Mechanisms area, choose the authentication method.

Step 8 In the Remote Firewall Settings area, set the firewall settings for the Easy VPN Remote connection.

Step 9 Click **Save As New Template**.

Step 10 Navigate to the My Templates folder and choose the template that you just saved.

Step 11 Click the **Publish** icon at the top-right corner, then click **OK**.

Step 12 Create a composite template (Creating Composite Templates), and add the ACL and Easy VPN Remote templates to the composite template.

Step 13 Use the arrows buttons to arrange the templates in 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 EasyVPN Remote template.

Step 14 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Creating an Easy VPN Server Template

The Easy VPN Server feature introduces server support for the Cisco VPN software client Release 3.x and later and Cisco VPN hardware clients (such as the Cisco 800, Cisco 900, Cisco 1700, VPN 3002, and PIX 501 devices). Using IP Security (IPsec), Easy VPN Server allows a remote end user to communicate with any Cisco IOS Virtual Private Network (VPN) gateway. Also, centrally managed IPsec policies are pushed to the client device by the server and helps the end user to minimize the configuration.

Before You Begin

Do the following:

- Create AAA method list for the group and the user by using the CLI template
- Create an IPsec Profile template
- If you will use Crypto Map, create a Transform Set template
- (Optional) Create a CLI template for RADIUS server group creation or configure the RADIUS server while creating the AAA method list
- (Optional) Create an ACL template for the split tunnel ACL in the ISAKMP Group configuration
- Create a Browser Proxy template for ISAKMP group configuration

To create an Easy VPN Remote template:

Step 1 Choose **Design > Feature Design**.

Step 2 Under the **Features and Technologies** folder, expand the **Security** subfolder, then click **Easy VPN Server**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 In the Interface Configuration area, choose the configuration methods and complete the fields of the interface that is configured on the device.

Step 6 In VPN Components Assembly area, enter the Transform Set profile name that you created in the Transform Set template (Configuring Transform Sets) and complete the fields in this area.

Step 7 In the Group Authorization area, enter the Method List profile name that you created in the CLI template and complete the fields in this area.

Step 8 In the User Authorization area, enter the same Method List profile name that you created in the CLI template, and complete the fields in this area.

Step 9 In the ISAKMP Group configuration area, click **Add Row** to add the ISAKMP Group configuration.

Step 10 In the ISAKMP Group configuration dialog box, enter the ACL profile name that you created in the ACL template and the Browser Proxy profile name that you created in the Browser Proxy template, and complete the fields in this area.

Step 11 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Step 12 Create a composite template (Creating Composite Templates) and add the AAA Method List and Radius server, IPsec Profile (Creating an IPsec Profile Template), ACL Browser Proxy (Creating an Easy VPN Server Proxy Setting Template), and Easy VPN_ Remote templates in the composite template.

Step 13 Using the arrow icons to arrange the templates in a order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, arrange the ACL template first, followed by the EasyVPN_Remote template.

Step 14 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Creating a GSM Profile Template

To create a GSM Profile template:

Step 1 Click **Design > Feature Design**.

Step 2 From the **Features and Technologies** folder, expand the **Interface** subfolder, then choose **Cellular > GSM Profile**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 In the Template Detail area, enter an Access Point Name and select a profile number from the drop-down list.

Step 6 Choose the type of authentication that your service provider uses. (CHAP authentication is more secure than PAP authentication.)

Step 7 Enter the user name given to your by your ISP or your network administrator, and enter a password.

Step 8 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Step 9 Click **OK**.

Creating a Cellular Profile Template

To create a Cellular Profile template:

Note To deploy the Cellular Profile template on any GSM HSPA, HSPA+R7, and LTE-Verizon modem, you should have the GSM profile (Creating a GSM Profile Template) created on the router.

Step 1 Choose **Design > Feature Design**.

Step 2 From the **Features and Technologies** folder, expand the **Interface** subfolder, then choose **Cellular > Cellular Profile**.

Step 3 Enter the basic template information.

Step 4 From the Device Type drop-down list, choose **Routers**.

Step 5 In the Template Detail area, define the interface as Primary WAN Interface or Backup WAN Interface and complete the fields.

Step 6 In the Dialer Configuration area, choose **Yes** to enable the persistent data connection and complete the fields.

Step 7 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Step 8 Click **OK**.

Redirecting HTTP and HTTPS Traffic

ScanSafe Software as a Service (SaaS) Web Security allows you to scan the content of 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 Integrated Services Router (ISR) Web Security with Cisco ScanSafe is enabled and the ISR is configured to redirect web traffic to ScanSafe, the Integrated Services Router (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 ISR receives the response from the web server, it sends the data to the client. This is called *whitelisting* traffic.

See the *Cisco ISR Web Security with Cisco ScanSafe Solution Guide* for more information about ScanSafe.

Creating a ScanSafe Template

To create a ScanSafe template, you must specify:

- The ScanSafe server and interface information
- Whitelist information

To create a ScanSafe template:

Step 1 Choose **Design > Feature Design > Features and Technologies > Security > ScanSafe**.

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

Step 3 In the Validation Criteria area, choose a device type from the list and enter the OS version.

Step 4 In the Template Detail area, enter the required information. For more information about the required field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 5 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Configuring Interfaces

The Interfaces feature helps in setting up physical and logical interfaces. Physical interfaces on a device depend on the device type and its interface processors or port adapters. IPv4 addressing is supported for all interfaces including service modules such as WAN, LAN, and logical interfaces. The following interfaces are supported in this release:

WAN Interfaces

- Configuring a Serial Interface, page 13-17
- Configuring POS Interface, page 13-18
- Configuring a Service Module, page 13-18
- Configuring Controllers, page 13-19

LAN Interfaces

- Creating a Gigabit Ethernet or Fast Ethernet Interface, page 13-20

Logical Interfaces

- Creating a Loopback Interface, page 13-20
- Creating a VLAN Interface, page 13-20
- Creating a Tunnel Interface, page 13-21
- Creating a Virtual Template Interface, page 13-22

Configuring a Serial Interface

To edit or delete the Serial interface:

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

Step 2 After choosing the device from list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 In the Interface page, select the serial interface in the Interface Summary area and click **Edit**.

Step 5 In the Create or Edit Serial Interface page, enter the basic configuration information.

Step 6 Select the encapsulation type as High Level Data Link Control **(HDLC)** or Point-to-Point Protocol (**PPP)** or **Frame Relay**. Use the Advance Configuration area to configure the encapsulations.

Note For controller-based serial interfaces, only interface configurations are supported.

Step 7 Enter an IPv4 address.

Step 8 For Frame Relay encapsulation, use the IETF option to connect to non-Cisco routers. (The Autosense feature is supported only on Frame Relay.)

Note The Autosense feature allows the router to detect the LMI type that is being used, by communicating with the switch and then uses the same type of LMI.

Step 9 For PPP encapsulation, specify the CHAP and PAP configurations with directions.

Step 10 Click **Save**. The Interface Summary page displays the modified interfaces.

Step 11 Click **Save / Deploy** to save the changes in the device.

Configuring POS Interface

To edit and delete the POS interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 In the Interface page, select the POS interface from the Interface Summary area and click **Edit**.

Step 5 In the Create or Edit POS Interface page, enter the basic configuration information.

Step 6 Check the **Enable SPE Scrambling** check box to enable the SPE scrambling.

Step 7 Check the **Send LAIS when Shutdown** check box to send the Line Alarm Indication Signal (LAIS) when the POS interface is in administrative shut down state.

Step 8 Select the encapsulation type as **HDLC** or **PPP** or **Frame Relay** and use the Advance Configuration area to configure the encapsulations.

Step 9 Enter an IPv4 address.

Step 10 In the Advanced Configuration area, select the alarm reporting and alarm reporting threshold options to receive alarms when there is any event.

Step 11 Repeat Step 9 through Step 11 in the Configuring a Serial Interface area.

Configuring a Service Module

To edit or delete the Service Module interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 Select the service module interface from the Interface Summary area and click **Edit**.

Step 5 In the Fast Ethernet interface pane, complete the basic configuration information.

Step 6 Click **OK** to save the changes in the device.

Configuring Controllers

To create or edit the DSL, SHDSL, and VDSL controllers interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 Select the **DSL, SHDSL** or **VDSL** controller from the interface summary area and click **Edit**.

Step 5 In the Edit Controller page, enter the required information.

Step 6 Click **OK**. After you configure the controller, you must configure the DSL, SHDSL or VDSL subinterface.

Step 7 To configure the DSL subinterface, select an ATM interface in the Interface Summary page, and click **Add Subinterface**.

- **a.** In the Create ATM Sub Interface page, choose the encapsulation from the drop-down list.
- **b.** Configure the Permanent Virtual Circuit (PVC) settings.
- **c.** Select a dialer to be associated to the ATM subinterface by using the **Create** or **Associate** dialer options.
- **d.** Click **OK**.

Step 8 To configure the SHDL subinterface, select a SHDSL interface in the Interface Summary page, and click **Add Subinterface**.

- **a.** In the Create SHDSL subinterface page, add the DSL Group and select the DSL pair.
- **b.** Choose the Group Type from the drop-down list.
- **c.** Click **OK**.

Step 9 To configure the VDSL subinterface, select a VDSL interface in the Interface Summary area, and click **Add Subinterface**.

- **a.** In the Create VDSL subinterface page, choose the Operating Mode from the drop-down list.
- **b.** Check the **Annex A mode** check box.
- **c.** Click **OK**.

Creating a Gigabit Ethernet or Fast Ethernet Interface

To create a Gigabit Ethernet or Fast Ethernet interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 Select the Gigabit Ethernet or Fast Ethernet in the Interface Summary area, and click **Edit**.

Step 5 In the Edit Ethernet Interface, complete the basic configuration information.

Step 6 Choose the Primary IP address from the drop-down list.

Step 7 Click **Add Row** and add the Secondary IP address.

Step 8 Click **OK** to save the changes in the device.

Creating a Loopback Interface

To create a Loopback interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration panel appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 On the Interface page, choose **Add Logical Interface > Loopback**.

Step 5 In the Create or Edit Loopback Interface area, enter the basic configuration information.

Step 6 Enter an IPv4 address.

Step 7 Click **OK**.

Step 8 Click **Save / Deploy** to save the changes in the device.

Creating a VLAN Interface

To create a VLAN interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 In the Interface page, click **Add Logical Interface** > **VLAN**.

Step 5 In the Create or Edit VLAN Interface page, complete the basic configuration information.

Step 6 Choose the Primary IP address from the drop-down list.

Step 7 Click **Add Row** and add the Secondary IP address.

Step 8 Click **OK** to save the changes in the device.

Editing a VLAN Interface

To edit the VLAN interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 Select the VLAN interface from the Interface Summary area, and click **Edit**.

Step 5 In the Create or Edit VLAN Interface page, complete the basic configuration information.

Step 6 Choose the Primary IP address from the drop-down list.

Step 7 Click **Add Row** and add the Secondary IP address.

Step 8 Click **OK** to save the changes in the device.

Creating a Tunnel Interface

To create a Tunnel interface:

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 choosing the device, choose **Configuration**. The Feature Configuration panel appears.

Step 4 Expand the **Interface folder**, then choose the **Interfaces**.

Step 5 In the Interface page, choose **Add Logical Interface > Tunnel**.

Step 6 In the Create or Edit Tunnel Interface page, complete the basic configuration information.

Step 7 Choose the Primary IP address from the drop-down list.

Step 8 Click **Add Row** and add the Secondary IP address.

Step 9 Click **OK** to save the changes in the device.

Editing an Existing Tunnel Interface

To edit a Tunnel interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 Select the Tunnel interface in the Interface Summary page, and click **Edit**.

Step 5 In the Create or Edit Tunnel Interface page, complete the basic configuration information.

Step 6 Choose the Primary IP address from the drop-down list.

Step 7 Click **Add Row** and add the Secondary IP address.

Step 8 Click **OK** to save the changes in the device.

Creating a Virtual Template Interface

To create a Virtual Template interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 In the Interface page, click **Add Logical Interface Virtual Template**.

Step 5 In the Create or Edit Virtual Template Interface page, complete the basic configuration information.

Step 6 Choose the Primary IP address from the drop-down list.

Step 7 Click **Add Row** and add the Secondary IP address.

Step 8 Click **OK** to save the changes in the device.

Editing an Existing Virtual Template Interface

To edit a Virtual Template interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

Step 4 Select the Virtual Template interface in the Interface Summary page, and click **Edit**.

Step 5 In the Create or Edit Virtual Template Interface page, complete the basic configuration information.

Step 6 Choose the Primary IP address from the drop-down list.

Step 7 Click **Add Row** and add the Secondary IP address.

Step 8 Click **OK** to save the changes in the device.

Configuring Cellular WAN Interfaces

The Cisco ISRs provide a third-generation (3G) wireless interface that can be used over GSM and Code Division Multiple Access (CDMA) networks. Its primary application is WAN connectivity as a backup data link for critical data applications. However, the 3G wireless interface can also function as the primary WAN connection for the router. The 4G wireless interface is supported only on the 4G-LTE-V modem.

Configuring a CDMA Interfaces

To configure a CDMA interface:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Cellular WAN Interfaces**.

Step 4 For a CDMA Sprint modem:

a. Select a cellular interface with CDMA Sprint modem, and click **Manage Modem**.

b. In the Manage Modem dialog box, select the **OMA-DM** or **Manual** radio button. If you choose the Manual option, complete the fields to manually configure the CDMA Sprint modem, then click **OK**.

Step 5 For a CDMA Verizon modem:

a. Select a cellular interface with CDMA Verizon modem, and click **Manage Modem**.

b. In the Manage Modem dialog box, enter the **Account Activation Information**, then click **OK**.

Step 6 For a CDMA Generic modem:

a. Select a cellular interface with CDMA Generic modem, and click **Manage Modem**.

b. In the Manage Modem dialog box, complete the fields to configure the CDMA Generic Modem, then click **OK**.

Configuring a GSM Interfaces

To configure a GSM interface:

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

Step 2 Choose the device from the list or click **Add** to add a new device, then configure the device.

Step 3 After choosing the device, click **Configuration**. The Feature Configuration pane appears.

Step 4 Expand the **Interface folder**, then choose **Cellular WAN Interfaces**.

Step 5 Select the GSM interface and click **Manage Modem**.

Step 6 In the Manage Modem dialog box, click **Add Row**.

Step 7 Choose the Profile Number from the drop-down list, and enter the Access Point Name, then click **OK**.

Configuring Network Address Translation (NAT)

Network Address Translation (NAT) is a process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. 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. 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. 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. NAT is described in RFC 1631.

A router configured with NAT will have at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit router between a subdomain 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, 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 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 IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S.

NAT Types

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 additional security.

NAT types include:

- Static Address Translation (SAT) —Allows one-to-one mapping between local and global addresses.
- Dynamic Address Translation (DAT)—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). With PAT, thousands of users can be connected to the Internet using only one real global IP address.

Configuring NAT for IP Address Conservation

To configure NAT, perform the following steps:

1. Creating NAT IP Pools (required for Dynamic NAT)
2. Create an ACL template and configure the ACL
3. Creating NAT44 Rules

4. Configuring Interfaces and assign rules on them
5. Setting Up NAT MAX Translation (Optional)

Note The NAT feature is supported on the following: ASR platform from Cisco IOS Release 3.5 or later and ISR platform from Cisco IOS Release 12.4(24)T or later.

Caution CLI changes that begin with "EMS_" are not supported and might cause unexpected behavior.

Creating NAT IP Pools

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

To create an IP pool:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security**, expand the **NAT** subfolder, and then click **IP Pools**. The NAT Pools page appears.

Step 4 Click **Add IP Pool** > **IP+Prefix** or **IP Range + Prefix**, 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 5 Click **SAVE** to deploy the IP pool to the device, or **CANCEL** to cancel your editing.

Step 6 To edit the existing IP Pool, in the NAT IP Pools page do the following:

a. Click in the selected IP Pools parameters row, and edit the parameters. or
b. Select the IP Pools, and click **Edit**. The selected IP Pools opens for editing. You can edit all of the parameters except the pool name.

Step 7 Click **SAVE** to deploy the changes to the device.

Creating NAT44 Rules

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

There are three types of NAT rules:

- Static
- Dynamic
- Dynamic PAT

To create the NAT44 rule:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security**, expand the **NAT** subfolder, and then click **NAT44 Rules**.

Step 4 In the NAT 44 page, click the down arrow icon next to the **Add NAT Rule** button.

- Click **Static** to create Static Rule. For a description of the elements, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.
- Click **Dynamic** to create Dynamic NAT Rule. For a description of the elements, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.
- Click **Dynamic** PAT to create Dynamic PAT Rule. For a description of the elements, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 5 Click **Save** to save and deploy the changes to the device.

Step 6 To edit the existing NAT44 rule in the NAT44 page, do one of the following:

- Click the selected NAT44 rules parameters row, and edit the parameters.
- Select the NAT44 rule, and click **Edit**. The selected NAT44 rule opens for editing. You can edit all of the parameters.

Step 7 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 8 Click **Save** to save the changes in the server.

Configuring Interfaces

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

To configure a virtual interface:

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

Step 2 After choosing the device from list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security**, expand the **NAT** subfolder, and then click **Interfaces**.

In the Interface page, select the interface that you want to change and choose the association from the drop-down list. The options are: Inside, Outside, and None.

Step 4 Click **Save** to save the changes in the server.

Setting Up NAT MAX Translation

The NAT MAX 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. For more information on Configuring the Rate Limiting NAT Translation Feature, see Configuring NAT for IP Address Conservation in *IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S*.

The NAT MAX Translation feature allows you to reset the global translation attribute values.

To set up the MAX Translation:

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 choosing the device, click **Configuration**. The Feature Configuration pane appears.

Step 4 Expand the **Security**, expand the **NAT** subfolder, and then click **Advanced Settings > Max**. **Translation**.

Step 5 Reset the parameter values. Configure the maximum number of NAT entries that are allowed for all of the parameters. A typical range for a NAT rate limit is from 100 to 300 entries.

Step 6 Click **Save** to save the changes in the server.

Configuring DMVPN

The DMVPN feature allows you 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 an 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 Cisco.com login ID).

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

- Configuring Hub and Spoke Topology, page 13-29
- Configuring a DMVPN Fully Meshed Topology, page 13-29
- Configuring a Cluster Topology, page 13-30

Creating a DMVPN Tunnel

To create a DMVPN tunnel:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security** folder, and then click **DMVPN**. Click **Add** to create the DMVPN.

Step 4 In the Device Role and Topology Type area, select the topology and the device role. The options are: Spoke, Hub, and Dynamic Connection between Spokes.

Step 5 In the Multipoint GRE Interface Information area, choose the WAN interface that connects to the Internet from the drop-down list.

Step 6 Enter the IP address of the Tunnel Interface, and Subnet Mask.

Step 7 Complete the fields in the NHRP and Tunnel Parameters area.

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 8 In the Encryption policy field, click the anchored plus button (+) to add the Transform Set Profile (see Security > VPN Components > Transform Sets in the *Cisco Prime Infrastructure 2.0 Reference Guide).*

Step 9 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 10 Choose the IP Compression check box to enable the IP compression for the transform set.

Step 11 Choose the mode for the transform set. The options are: Tunnel mode or Transport mode.

Step 12 In the NHS Server Information area, 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 Release 15.1(2)T or later.

Step 13 In the Routing Information area, choose the routing information. The options are: EIGR, RIPV2, and Other.

Note The routing information is required only for hub configuration.

Step 14 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 15 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 16 Click **OK** to save the configuration to the device.

Configuring Hub and Spoke Topology

To configure the hub and spoke topology:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security** folder, and then click **DMVPN**. Click the **Add** button to create the **DMVPN** tunnel.

Step 4 In the Device Type and Topology area, choose Hub and Spoke as the topology, and select either Hub or Spoke as a device role.

Step 5 Choose 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 6 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 7 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 protocols and the algorithms.

Step 8 Configure the routing protocol to be used.

Step 9 Click **Save** to save the configuration to the device.

Configuring a DMVPN Fully Meshed Topology

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

To configure a DMVPN Fully Meshed topology:

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 pane appears.

Step 4 Expand the Security folder, and then click **DMVPN**. Click the **Add** to create the DMVPN tunnel with fully meshed topology.

Step 5 In 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 in the Configuring Hub and Spoke Topology section.

Step 7 For Fully Mesh spoke topology, in the NHS Server Information area, 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.

Configuring a Cluster Topology

To configure a cluster topology:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 Feature Configuration pane, expand the **Security** folder**,** and then click **DMVPN**. Click **Add** to create the DMVPN tunnel.

Step 4 From the Create DMVPN Tunnel configuration page, select **Spoke** radio button to configure the device role as a spoke.

Step 5 Repeat Step 6 through Step 8 from in the Configuring Hub and Spoke Topology section.

Note The device must be running IOS version of 15.1(2)T or later.

Step 6 Click **Add Row** to configure the cluster related information, and add the Cluster-ID and Maximum Connection values.

Step 7 Click **Expand Row** (next to the radio button) and click **Add Row** to add the NHS server information.

Step 8 Enter the NHS server, the GRE Tunnel IP addresses, and the Priority of this NHS server. Click **Save** to save the NHS server entry configuration.

Step 9 Click **Save** to save the NHS server group information.

Step 10 Click **Save** again to save the NHS group information with the cluster configuration. This will automatically populate the NHS server IP address in the table.

Editing a DMVPN

To edit a DMVPN tunnel:

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 pane appears.

Step 4 Expand the Security folder, and then click **DMVPN.** The available tunnel is displayed.

Step 5 Select the tunnel, and click **Edit**. The Edit DMVPN Tunnel page opens.

Step 6 In 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.

Deleting a DMVPN

To delete a DMVPN tunnel:

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

Step 2 Choose the device from the list to delete the DMVPN tunnel. If the device is not added, click **Add** 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 **Delete**.

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 of the changes that you have made without sending them to the router.

Configuring GETVPN

A Group Encrypted Transport VPN (GETVPN) deployment has three primary components: Group Member, Key Server, and Group Domain of Interpretation protocol. Group Members encrypt and decrypt the traffic, and Key Server distributes the encryption key to all group members. The Key Server decides on a single data encryption key for a given lifetime. Because all Group Members use the same key, any Group Member can decrypt the traffic encrypted by any other Group Member. GDOI protocol is used between the Group Member and Key Server for group key and group Security Association (SA) management. A minimum one Key Server 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 negotiateIPsec between Group Members on a peer-to-peer basis, thereby reducing the resource load on the Group Member routers.

Group Member

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

Key Server

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

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

The keys sends two types to Group Member: 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. The KEK is used to secure rekey messages between the Key Server and the Group Members.

The Key Server sends out rekey messages either because of an impending IPsec SA expiration or because the security policy has changed on the Key Server. Keys can be distributed during rekey using either multicast or unicast transport. the multicast method is more scalable because keys need not be transmitted to each group member individually. Unlike in unicast, The Key Server will not receive acknowledgement from the Group Member about the success of the rekey reception using the multicast rekey method. Usign the unicast rekey method, the Key Server will delete a Group Member from its database if the Group Member does not acknowledge three consecutive rekeys.

Group Domain of Interpretation

Group Domain of Interpretation protocol is used for Group key and group SA management. Group Domain of Interpretation uses Internet Security Association Key Management Protocol (ISAKMP) for authenticating the Group Members and Key Servers. All of the standard ISAKMP authentication schemes like RSA Signature (certificates) and preshared 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.

Creating a GETVPN Group Member

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

To create a GETVPN group member:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security** folder, and then click **GETVPN-GroupMember**. Click **Add** to create the GET VPN group member.

Step 4 In the Add GroupMember dialog box, choose the **General** tab, and enter the Group Name and Group Identity. Choose the Registration Interface from the drop-down list.

Step 5 Enter the Primary Key Server and Secondary Key Server IP addresses. Click **Add Row** or **Delete** 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 6 Click the **row** or **field** to edit the secondary key server IP address.

Step 7 Click **Save** to save the configuration.

Step 8 In the Add Group Member dialog box, choose the **Advanced** tab, and choose the Local Exception ACL and Fail Close ACL from the drop-down list.

If the Fail Close feature is configured, all of 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 9 Choose 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 for this group member.

Step 10 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.

Creating a GETVPN Key Server

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

To create a GETVPN key server:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security** folder, and then click **GETVPN-KeyServer**. Click **Add** to create the GETVPN key server.

Step 4 In the Add Key Server dialog box, choose the **General** tab, and enter the Group Name, Group Identity, WAN IP address, and Priority of this key server.

Step 5 Enter the Co-operative Key Servers IP address. Click **Add Row** or **Delete** to add or delete the Co-operative key server IP address. Click the **row** or **field**, and edit the IP address.

Step 6 In the Add KeyServer dialog box, choose the **Rekey** tab, and choose the Distribution method from the drop-down list.

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 7 In the Add KeyServer dialog box, choose the **GETVPN Traffic** tab, and enter the Traffic to be encrypted, Encryption Policy, and Anti Replay.

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 active.

Step 8 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.

Editing a GETVPN Group Member or Key Server

To edit a GETVPN group member or a GETVPN key server:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In Feature Configuration pane, expand the **Security** folder, and then click **GETVPN-Group Member** or **GETVPN-KeyServer**. The GETVPN-GroupMember or GETVPN-KeyServer summary page opens.

Step 4 In the GETVPN summary page, select the group name and click **Edit**. The Edit GETVPN-GroupMember or GETVPN-Keyserver page appears.

Step 5 In the Edit GETVPN-GroupMember or GETVPN-KeyServer page, you can edit the GETVPN parameters.

Step 6 Click **OK** to save the configurations.

Deleting a GETVPN Group Member or Key Server

To delete a GETVPN group member or GETVPN key server:

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

Step 2 Choose 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 page.

Step 3 After choosing the device, click **Configuration**. The Feature Configuration pane appears.

Step 4 In the Feature Configuration pane, expand the **Security** folder, and then click **GETVPN-Group Member** or **GETVPN-KeyServer**. The GETVPN-GroupMember or GETVPN-KeyServer summary page opens.

Step 5 In the GETVPN summary page, select the group name and click **Delete**.

Step 6 Click **OK** to save the configurations.

Configuring VPN Components

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 network. IKE policies protect the identities of peers during authentication.

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 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 subsequent IKE traffic during the negotiation.

When negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates negotiation sends all of its policies to the remote peer. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies. A match is found when policies from both peers contain the same encryption, hash, authentication, and Diffie-Hellman (D-H) parameter values, and when the remote peer's policy specifies a lifetime that is less than or equal to the lifetime of the policy it is being compared to. If the lifetimes are not identical, the shorter lifetime from the remote peer's policy is used.

The VPN components primarily include the following:

- Configuring IKE Policies, page 13-35
- Configuring IKE Settings, page 13-35

- Configuring IPsec Profiles, page 13-36
- Creating Preshared Keys, page 13-36
- Creating RSA Keys, page 13-37
- Configuring Transform Sets, page 13-38

Configuring IKE Policies

To configure IKE policies:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, Expand the **Security** folder, and then choose **VPN Components > IKE Policies**.

Step 4 Click **Add Row** to create the IKE policies**.**

Step 5 In the IKE Policies page, enter the Priority, Authentication, D-H Group, Encryption, Hash, and Lifetime.

For a description of the elements on the IKE Policies page, see Security > VPN Components > IKE Policies in the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 6 Click **Save** to save the configuration, then click **Save** again to generate the CLI commands.

Configuring IKE Settings

The IKE Settings feature allows you to globally enable IKE for your peer router.

To configure IKE settings:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security** folder, and then choose **VPN Components > IKE Settings.**

Step 4 Check the **Enable IKE** and **Enable Aggressive Mode** check box to enable the IKE policies and the aggressive mode.

Step 5 Choose the IKE Identity from the drop-down list.

Step 6 Enter the **Dead Peer Detection Keepalive** and **Dead Peer Detection Retry** time in seconds.

For a description of the elements on the IKE Settings page, see Security > VPN Components > IKE Settings in the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 7 Click **Save** to save the configuration.

Configuring IPsec Profiles

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 matching 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 VPN remote client grouping.

The IKE Profile feature allows you to create an IPsec profile.

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 **In the** Feature Configuration pane, expand the **Security f**older, and then choose **VPN Components > IPsec Profile.**

Step 4 Click **Add Row** to create the IPsec profile.

Step 5 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 6 Enter the IPsec SA Lifetime in seconds to establish a new SA after the set period of time elapses.

Step 7 To edit the IPsec profile parameters, click **Field** and edit the parameter of that IPsec profile.

Step 8 To delete the IPsec profile, select the IPsec Profile from the list, and click **Delete**.

Step 9 Click **Save** to save the configuration, then click **Save** again to generate the CLI commands.

Creating Preshared Keys

The Pre-shared Keys feature allows you to share a secret key between two peers. This key is used by the IKE during the authentication phase.

To create a preshared key:

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 in the lower part of the page.

Step 3 After selecting the device, click **Configuration**. The Feature Configuration pane appears.

Step 4 Expand the Security folder, and then choose **VPN Components > Pre-Shared Keys**.

Step 5 Click **Add Row** 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 preshared key parameters, click the **Field** and edit the parameter of that preshared key.

Step 8 To delete the pre-shared key, choose the preshared key from the list, and click **Delete**.

Step 9 Click **Save** to save the configuration, then click **Save** again to generate the CLI commands.

Creating 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 is included in the certificate so that peers can use it to encrypt the data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by the peers and to digitally sign transactions when negotiating with the peers.

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, it takes longer to generate, encrypt, and decrypt keys with large modulus values.

To create an RSA keys:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security** folder, and then choose **VPN Components > RSAKeys.**

Step 4 Click **Add Row** to create the RSA keys.

Step 5 The Add RSA Keys dialog box appears.

Step 6 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 7 Check the **Make the Key exportable** check box to generate the RSA as a exportable key.

Step 8 Click **OK** to save the configuration.

Step 9 To import the RSA key, click **Import**. The Import RSA Key dialog box appears.

Step 10 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 11 To import usage-key, enter the public and private key data of both the signature and encryption keys.

Step 12 Click **Import** to import the RSA key.

Step 13 To export the RSA key, choose the RSA key from the list and click **Export**. The Export RSA Key Pair dialog box appears.

Step 14 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 15 Click **OK** to display the exported keys.

Step 16 To delete the RSA key, select the RSA key from the list, and click **Delete**.

Configuring Transform Sets

To define a transform set, specify one to three transforms. Each transform represents an IPsec security protocol (AH or ESP) plus the algorithm that you want to use. When the particular transform set is used during negotiations for IPsec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

To configure a transform sets:

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

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 **In the** Feature Configuration pane, expand the **Security** folder, and then choose **VPN Components > Transform Sets.**

Step 4 Click **Add Row** to create the transform sets.

Step 5 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 6 Specify the mode for a transform set:

- 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 7 Click **Save** to save the configuration, then click **Save** again to save the configuration changes.

Creating a Zone-Based Firewall

The Zone-Based Firewall feature allows you to easily manage Cisco IOS unidirectional firewall policy between groups of interfaces known as *zones*.

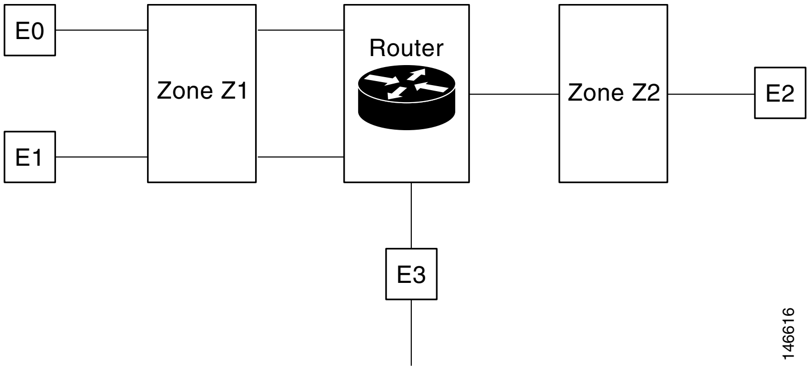
A zone is a group of interfaces that have similar functions or features. For example, on a router, Gigabit Ethernet interface 0/0/0 and Gigabit Ethernet interface 0/0/1 may be connected to the LAN. These two interfaces are similar because they represent the internal network, so they can be grouped into 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.

When an interface is a member of a security zone, all traffic to and from that interface (except traffic going to the router or traffic going to another interface on the same zone) is dropped.

To permit traffic between interfaces that belong to different zones, a firewall policy with concrete rules must be pushed to the device. If the policy permits the traffic between these two zones (through inspect or pass actions) traffic can flow through the zones. Figure 13-1 describes the security zone.

Figure 13-1 Security Zone Diagram



The following describe the relationships between the interfaces and security zones shown in Figure 13-1.

- 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 interfaces E0 and E1 because they are members of the same security zone (Z1).
- If no policies are configured, traffic will not flow between zones (for example, E0 and E2, E1 and E2, E3 and E1, and E3 and E2).
- Traffic can flow between interface E0 or E1 and E2 only when an explicit policy is configured to permit the traffic between zone Z1 and zone Z2.

Traffic can never flow between E3 and interface E0, E1or E2 because E3 is not a part of any security zone.

Prime Infrastructure supports the zone-based firewall feature on Cisco ASR, ISR, and CSR routers. Using Prime Infrastructure, you can configure a zone-based firewall policy template and deploy it to multiple devices. After you deploy the zone-based configuration, you can navigate to the Device Work Center to view the deployed firewall configuration on a specific device.

To monitor the zone-based firewall, check the Zone-Based Firewall Monitor Hits capability on the Device Work Center or the Prime Infrastructure syslog feature, which supports zone-based firewall syslog messages.

Prime Infrastructure can configure Zone-Based Firewall either through CLI (over Telnet or SSH) or through WSMA. Zone-Based Firewall can be configured through WSMA in a more efficient and robust method and we recommend that you use the WSMA protocols for configuring Zone-Based Firewall. For more information on using WSMA with Prime Infrastructure, see Configuring the Device using WSMA, page 13-1.

Configuring a Zone-Based Firewall Template

To configure a zone-based firewall on more than one device, use a zone-based template to make the changes. For zone-based firewall templates, you must first design the zone-based firewall in the network by defining the zones in the network. In Prime Infrastructure 2.0, zones are represented by interface role global object, which dynamically selects the list of interfaces that belong to the zone. Next, define and create network objects in the firewall environment. The Zone-based firewall feature supports only IPv4 network in Prime Infrastructure 2.0 (IPv6 is not supported.)

Note The Zone-Based Firewall feature is supported on the following: ASR platform from Cisco IOS-XE Release 15.2(2)S or later, ISR G2 platform from Cisco IOS Release 15.0(1)M or later, ISR G3 platform from Cisco IOS-XE 15.3(2)S Release or later, and CSR platform from Cisco IOS-XE 15.3(1)S Release or later.

To configure a zone-based firewall template:

1. Define the zones. A security zone is defined as an interface role (see Creating an Interface Role, page 13-40).
2. Define the IPv4 network objects (see Creating an IPv4 Network Object, page 13-41).

   Note Cisco Prime Infrastructure 2.0 supports only IPv4 network objects.

3. Design a firewall policy and deploy it to multiple devices (for more information, see Creating a Policy Rule, page 13-44).
4. Validate the configuration for a specific device (see Creating a Zone-Based Firewall, page 13-38).
5. Modify the global objects and template configuration (see Creating a Zone-Based Firewall Policy Rules Template, page 13-41).
6. Monitor the policy rules (see "Monitoring Policy Rules" section on page 13-45).
7. Monitor the syslog messages (for more information, see "Where to Find Syslogs" section on page 11-5).

To modify security zones, IPv4 network objects, and firewall policies, edit the firewall policy and redeploy it to the relevant devices.

Creating an Interface Role

An Interface role allows you to dynamically select a group of interfaces without having to manually define explicitly interfaces on each device. For example, you can use interface roles to define the zones in a zone-based firewall configuration template. You might define an interface role with a naming pattern of DMZ*. When you include this interface role in a template and deploy the template, the configuration is applied to all interfaces whose names begin with "DMZ" on the selected devices. As a result, you can, for example, assign a policy that enables anti-spoof checking on all DMZ interfaces to all relevant device interfaces with a single action.

For information to create an interface role, see Creating Interface Roles, page 8-20.

Creating an IPv4 Network Object

Network objects are logical collections of IP addresses or subnets that represent networks. Using network objects simplifies policy management.

For information to create an IPv4 network object, see Creating Network Objects, page 8-21.

Defining Device Override

Use the device override feature when a specific device is differed from the general network design.

To define the device override:

Step 1 Choose **Design > Configuration > Shared Policy Objects > Shared > Interface Role** or **IPv4 Network Object**.

Step 2 In the Create/Edit Network Object or Interface Role page, check the Allow Value Override Per Device check box and define the values per specific device. The defined values will override the regular values defined for the Interface Role \ Network Object.

Step 3 Click **OK** to save the configurations.

Creating a Zone-Based Firewall Policy Rules Template

After you create a shared policy objects, create a zone-based firewall policy rules template.

To create a Zone-Based Firewall Policy Rules template:

Step 1 Choose **Design > Feature Design > Features and Technologies > Security > Zone Based Firewall > Policy Rules**.

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

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

Step 4 Enter the required fields. For descriptions of the template parameters, see the Cisco Prime Infrastructure 2.0 Reference Guide.

Step 5 Click **Save as New Template**. After you save the template, deploy it to your devices using the procedures in Creating and Deploying Feature-Level Configuration Templates, page 8-2.

Configuring a Zone-Based Firewall on a Single Device

To configure a zone-based firewall on a single device, use Device Work Center zone-based configuration to make the changes.

- Creating a Security Zone, page 13-42
- Configuring a Default-Zone, page 13-43
- Creating a Policy Rule, page 13-44

- Creating a Service Group, page 13-46
- Assigning TCP/UDP Ports on an Application, page 13-47
- Configuring a Default Parameters Map, page 13-47
- Assigning an Interface for a Zone, page 13-48

Creating a Security Zone

To create a security zone:

Note The Zone Based Firewall feature is supported on the ASR platform on Cisco IOS-XE Release 15.2 (2)S or later, ISR G2 platform on Cisco IOS release 15.0 (1) M or later, ISR G3 platform on Cisco IOS-XE Release 15.3(2)S or later, and CSR platform on Cisco IOS-XE Release 15.3(1)S.

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall > Common Building Blocks**, and then click **Zones**.

Step 4 Click **Add Zone** to create the security zone.

Step 5 Select a **Zone Name**.

Step 6 Select the VRF of the zone.

- **a.** Select a VRF before assigning interfaces to the security zone. Only the interfaces that are assigned to the selected VRF can be assigned to the zone.
- **b.** If the user selects the “global VRF”, only interfaces which are not assigned to any VRF can be assigned to the zone.

Step 7 To assign the interfaces to the security zone, click the down arrow icon. The Interface Object Selector dialog box appears.

- **a.** In the Interface selector dialog box, check the **Interface** check box to select the interface from the list (can be multiple selection).
- **b.** Click **OK** to save the configuration or click **Cancel** to cancel all of the changes that you have made without sending them to the router.

Step 8 In the Advanced options column, click **Configure**. The Advanced Parameters Configuration dialog box appears.

Step 9 Define a set of advanced parameters which would be applicable for the inspected traffic that goes through the interfaces that belongs to the zone. For each parameter, check the check box to the left of the parameter name to override the default value for the parameter and then select the new value for the parameter. (Optional) In the Advanced Parameters Configuration dialog box, do the following:

Note Advanced Parameters option is supported only on ASR1K series devices.

- **a.** Check the **Alert** check box and select the **On** radio button to set the alert.
- **b.** Check the **Maximum Destination** check box to set the maximum destination.
- **c.** Check the **TCP SYN-Flood Rate per Destination** check box to set the TCP flood rate.

d. Check the **Basic Threat Detection Parameters** check box and select 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 10 Click:

- **OK** to save the configuration.
- **Cancel** to exit without saving.

Step 11 To edit the existing security zone parameters, select the zone, and click **Edit** in the Advance options column. The Advanced Parameters Configuration dialog box appears.

Step 12 In the Advanced Parameters Configuration dialog box, edit the values and click **Save** to save the changes. When you hover your mouse on the Advanced Options icon, the configured parameters will be displayed in the quick view window.

Step 13 Enter the description for the zone, then click **Save**.

Editing a Security Zone

To edit a security zone:

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall > Common Building Blocks**, and then click **Zones**.

Step 4 In the Zones page, choose one of the following options:

a. Click the Zone parameters row, and edit the parameters. or

b. Select the zone, and click **Edit**. The selected Zone entity opens for editing.

Step 5 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 and edit the advanced parameters of the zone.

Step 6 Click **Save** to save the configuration.

Configuring a Default-Zone

A default zone is a zone that is automatically assigned to all interfaces that are not assigned to any other zone on device.

To configure a default zone:

Note The Default-Zone feature is supported only on the ASR platform.

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 From the Feature Configuration pane, expand the **Security** subfolder.

Step 3 From the Security subfolder, expand the **Zone Based Firewall > Common Building Blocks**, and then click **Zones**.

Step 4 In the Zones page, click **Enable Default** to enable or disable the default security zone in the device. The default zone will host all of the interfaces that are not related to any zone.

Step 5 Click **OK** to save the configuration.

Creating a Policy Rule

To create a policy rule:

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall** and then click **Policy Rules**. The Policy Rules page appears.

Step 4 From the Policy Rules page, click **Add Rule** and complete the fields. When you add a rule, you can place a rule at the top or bottom of the policy or after/before an existing rule. Firewall Rules are processed according to their order. To control the order of the rules, select the location of the rule in the table and use Add Top or Add Bottom option to add the rule to the top or the bottom of the table. Select a rule and use Add After or Add Before option to add the rule before or after an existing rule.You can place a rule at any given location and later use drag and drop to change its location.

Step 5 (Optional) Enter the firewall rule name. 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 6 Select the source and destination zones for the rule, the rule is applicable only for traffic that flows from the source zone to the destination zone. Note that the source and destination zones must be different.

Step 7 To add the source and the destination IP address, click the **add** icon. The Source/Destination IP address dialog box appears.

a. In the Source/Destination IP address dialog box, check the **Any** check box to set the value to any.

b. Enter the Source/ Destination IP addresses.

c. Click the **+** button to add the new IP address and the subnet.

d. Click the **-** button to remove an IP/subnet.

e. Click **OK** to save the configurations or click **Cancel** to cancel all of the changes that you have made without sending them to the router.

Step 8 (Optional) Set the Service values. To add or remove the service, click the down arrow icon. The Firewall Service dialog box appears. You can also select a predefined Service. For creating services, see "Creating a Service Group" section on page 13-46.

a. In the Firewall Service dialog box, check the service or port-based application check box to select the application or the service for the rule.

b. Select specific TCP / UDP ports by selecting TCP or UDP, close the window and enter the list of ports to be used (separated by commas) in the text box that appears next to the TCP or UDP icon. For viewing port-based applications, see "Assigning TCP/UDP Ports on an Application" section on page 13-47.

c. Use the navigation arrow buttons to navigate backward.

d. 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 **Configure** 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 check box and set the new value.

b. To apply the device default value, uncheck the Parameter check box.

c. To view the firewall rule default parameters, see "Configuring a Default Parameters Map" section on page 13-47.

d. When you hover your mouse over the Advanced Options icon, the configured parameters are displayed in the quick view window.

Table 13-1 lists the elements on the policy rule page.

Step 12 Click **Save** to apply the rule to the device. For description of the elements, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Monitoring Policy Rules

The monitoring feature allows you to monitor policy rules. You can identify the most-used rules, and you can troubleshoot a specific rule and verify hits for the selected rule.

To monitor policy rules:

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall** and then click **Policy Rules**. The Firewall Rules page appears.

Step 4 In the Firewall Rules page, click **Hit Counters** and use one of the following options to analyze the sessions and packets hit counters for the firewall rules.

Step 5 Click the **Show all** option to view the packets and sessions counters for all firewall rules. The packets and sessions counters are displayed in two separate columns.

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. Sessions hit counters are not applicable for Drop/Pass rules. Similarly, packet hit counters are not applicable for Inspection rules.

Step 6 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.

Step 7 Click the **Show for selected rules** option to show the hit counters for a specific rule or a couple of selected rules. The hit counters would be displayed in a pop-up dialog box with a refresh button that allows quick refresh of the data.

Step 8 Use the pre-defined filters options available on the top-right corner of the table to display the rules at the top or bottom based on the packets/sessions counts.

Step 9 Click **Reset All Counters** to discard all of the rules counters on the device. The application will display a warning message before resetting the rules counters.

Editing a Policy Rule

To edit a policy rule:

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall** and then click **Policy Rules**. The Firewall Rules page appears.

Step 4 In the Firewall Rules page, choose one of the following options:

- Click the Rules parameters row and edit the parameters.
- Check the check box to select the rule, and then click **Edit**. The selected Rule opens for edit. You cannot edit the name of the policy rule.
- You can re-order firewall rules by dragging a rule and dropping it in a different location.

Step 5 Click **Save** to apply the changes in the device.

Creating a Service Group

You can create, update or delete a service groups. Service group provides an option to group together several port-based applications to logical groups which could be used in firewall policies.

For example, you can define a browsing service-group object and assign both HTTP and HTTPS applications to it. Then you can use this browsing service-group in firewall rules to permit or deny browsing traffic, rather than selecting both HTTP and HTTPS in those rules.

To create a service group:

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall > Common Building Blocks**, and then click **Service Groups**. The Service Groups page appears.

Step 4 To create the Service Group:

a. In the Service Group page, click **Add Service Group** and enter the Service Group Name. You cannot change the name after creating the Service Group. Also, you cannot create a service group without an application (see Creating Custom Applications, page 17-4).

b. To assign Applications, click the down arrow icon.

c. In the Applications dialog box, check the **Applications** check box to select one or more applications from the list, then click **OK**.

Step 5 To edit an existing Service Group, do one of the following:

- In the Service Groups page, click the Service Group parameters row and edit the parameters.

- Select the service group and click **Edit**. You can add new applications or remove an already selected application.
- To remove an application from the selected list, hover the mouse on the application name and click **X**.

Step 6 Click **Save** to apply your changes to the device.

Assigning TCP/UDP Ports on an Application

You can assign or unassign the Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) ports to an application.

Note When you click **Save** in the following procedure, your changes are deployed on the device. You cannot review the requested operation or remove the request from the pending changes queue.

To assign or unassign TCP/UDP ports for an application:

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall > Common Building Blocks**, and then click **Port Mappings**. The Port Application Mapping page appears.

Note Displays the application name that is driven from the device.

Step 4 To assign or unassign the TCP/UDP ports to an application, click the application and update its TCP/UDP ports value. The TCP/UDP 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 combination of ports and port ranges.
c. Unassign port(s) by deleting the existing port values.

Step 5 Click **Save** to save the configurations.

Configuring a Default Parameters Map

To configure a default parameters:

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall** and then click **Default Parameters**. The Default Parameters page appears.

Step 4 In the Default Parameters page, change the parameters value.

Note You can change the default parameters only on ISR devices.

Step 5 Click **Save** to save the configuration.

Assigning an Interface for a Zone

The interfaces view gives an overview of the interfaces on the device which are applicable for firewall inspection. The view allows viewing and modifying the assignment of those interfaces to security zones.

To assign or unassign an interface for a zone:

Step 1 Choose **Operate > Device Work Center**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall** and then click **Interfaces**.

Step 4 In the Interface page, select the interface that you want to change and click the down arrow icon. The Zone dialog box appears.

Step 5 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 6 Click **Yes** on the warning message if you want to change the assignment of that interface.

Step 7 To un-assign the interface from the specific zone, select the interface and delete the zone information.

Step 8 Click **Save** to save and apply your changes.

Creating a Routing Protocol

A routing protocol specifies how routers:

- Communicate with other routers in a network
- Select routing paths to transmit data between nodes in a computer network
- Share network information with other routers

The following sections describe the routing protocols supported by Prime Infrastructure.

Creating a Static Route

Static routing is the simplest form of routing, where the network administrator manually enters routes into a routing table. 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, because routes that are configured manually must be updated to fix any lost connectivity.

To create a static route:

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

Step 2 Choose 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 pane appears.

Step 4 Expand the **Routing** folder, and then click **Static**. The Static Routing page appears with options to configure IPv4 static routes.

Step 5 To configure an IPv4 static route, do the following:

a. In the **IPv4 Static Routes** page, click **Add Row**, and then complete the fields.

   For Permanent Route, choose either of the following:

   - **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.

Creating a RIP Route

Routing Information Protocol (RIP) is a distance-vector routing protocol that uses hop count as a routing metric. RIP implements a limit of 15 hops in a path from source to a destination, to prevent routing loops. The hop-count limit also limits the size of the networks that RIP supports. RIP sends its routing table every 30 seconds.

The 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:

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

Step 2 Choose 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 pane appears.

Step 4 Expand the **Routing** folder, and then click **RIP**. The RIP Routing page appears with options to configure IPv4 RIP routes.

Step 5 To configure an IPv4 RIP route, do the following:

a. In the **IPv4 RIP Routes** page, select the RIP version.

b. Click **Add Row**, and then complete the fields.

c. Click **Save**.

d. Click **Passive Interface** to select the passive interface that you want to add.

e. Click **Save** to save the configuration.

Creating an EIGRP Route

In EIGRP (an enhanced Interior Gateway Routing Protocol) when an entry in the routing table changes in any of the routers, it notifies its neighbors of the change only, 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 states of their 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:

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

Step 2 Choose 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 pane appears.

Step 4 Expand the **Routing** folder, and then click **EIGRP**. The EIGRP Routing page appears with options to configure IPv4 EIGRP routes.

Step 5 To configure an IPv4 EIGRP route, do the following:

a. In the **IPv4 EIGRP Routes** page, click **Add Row**, and then complete the fields.

b. Click **Save**.

c. Click **Add Interface** to select the passive interface that you want to associate to the Autonomous System (AS) number created.

d. Click **Save** to save the configuration.

Creating an OSPF Route

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 only; it does not send the entire routing table.

To create an OSPF route:

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

Step 2 Choose 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 pane appears.

Step 4 Expand the **Routing** folder, and then click **OSPF**. The OSPF Processes page appears with options to configure IPv4 OSPF processes.

Step 5 To configure an IPv4 OSPF process, do the following:

a. In 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 that 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.

CHAPTER 14

Working with Device Configurations

Cisco Prime Infrastructure archives device configurations and provides information such as the date of last configuration change, status of the configuration jobs, and allows you to compare current and previous configurations. Prime Infrastructure also allows you to roll back to a previously saved configuration in the archive if a configuration deployment fails.

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 choosing **Operate > Configuration Archives**.
- Scheduled—You can schedule when Prime Infrastructure collects the configurations of selected devices and specify recurring collections by choosing **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 back up the running configuration before pushing configuration changes to a device.
- Does not 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**.

- Click **Backup Running Configuration** to have Prime Infrastructure back up the running configuration before pushing configuration changes to a device.
- Click **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 that 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.

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 Features and Technologies 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 a device name.

The device details appear in the lower part of the page.

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 that 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, choose **Administration > Jobs Dashboard**.)

Adding a Wireless LAN Controller

The Cisco Unified Wireless Network (CUWN) solution is based on Wireless LAN Controllers running Airespace Operating System. The wireless LAN controller models include 2100, 2500, 4400, WiSM/WiSM2 (6500 service module), 5500, 7500, 8500. In this solution, access points tunnel the wireless traffic to the controllers through CAPWAP.

The Cisco Unified Access (UA) Wireless Solution is new architecture that provides a converged model where you can manage your wired and wireless network configurations in the same place. This solution includes the 3850 series switch with integrated wireless support. The solution also includes the 5760 series wireless controller, which can act as an aggregation point for many 3850 switches. This platform is based on IOS-XE, so the command structure is similar to other IOS products. In this solution, the wireless traffic can terminate directly on the 3850 switch, so that it can be treated in a similar mode to a wired connection on the switch.

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 that 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 them 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 that you want to roll back, then click **Schedule Rollback**.

Step 4 Specify the rollback and scheduling options.

Step 5 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 the **Number of version to retain** and **Number of days to retain** check boxes.

Step 3 Click **Save**.

Configuring Redundancy on Controllers

The term Redundancy in the Prime Infrastructure refers to the high availability (HA) framework in Cisco WLC. 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 identifier (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.

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 In the Device Group area, 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 In the Device Group area, 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 In the Device Group area, 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 14-9.
- 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
Prime Infrastructure Message	Switch Over Activity triggered. Controller *IP addr*
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

Prime Infrastructure Message	1. Redundancy notification trap triggered by controller *IP addr* having Redundancy-Management IP *IP addr*, Local state is 'Active' and Peer Redundancy-Management IP *IP addr* and peer state 'Disabled' 2. Redundancy notification trap triggered by controller *IP addr* having Redundancy-Management IP *IP addr*, Local state is 'Active' and Peer Redundancy-Management IP *IP addr* and peer state 'StandbyCold' 3. Redundancy notification trap triggered by controller *IP addr* having Redundancy-Management IP *IP addr*, Local state is 'Active' and Peer Redundancy-Management IP *IP addr* 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	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
Prime Infrastructure Message	Redundancy Failure Event trap triggered by controller *IP addr* 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 In the Other Background Tasks area, select the **Redundancy Status** background task.

Step 3 From the Select a command drop-down list, choose **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 In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the primary or active controller. The details of the controller appear in 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 In the Device Group area, 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 In the Device Group area, 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 in 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 Unselect 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 of the ports disabled.

Maintaining Software Images

Manually upgrading your devices to the latest software version can be error prone and time consuming. Cisco Prime Infrastructure simplifies the version management and routine deployment of software updates to your devices by helping you plan, schedule, download, and monitor software image updates. You can also view software image details, view recommended software images, and delete software images.

Prime Infrastructure stores all of 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, you must configure your devices with SNMP read-write community strings that match the community strings entered when the device was added to Prime Infrastructure.

Table 15-1 describes the different processes involved in managing software images and whether the processes are supported in the Unified Wireless LAN Controllers and devices.

Table 15-1 Software Image Management Processes and Supported Devices

Software Image Management Processes	Description	Unified WLCs	3850 Cisco IOS XE 3.2.1	5760 Cisco IOS XE 3.2.1
Image import from device	Ability to import software image from devices that are already deployed to Prime Infrastructure. The software image can then be distributed to other devices.	Not supported because the software image cannot be reassembled into a package.	Supported	Supported

Table 15-1 Software Image Management Processes and Supported Devices (continued)

Software Image Management Processes	Description	Unified WLCs	3850 Cisco IOS XE 3.2.1	5760 Cisco IOS XE 3.2.1
Image import from file	Ability to import software image from known location on a file server to Prime Infrastructure. The software image can then be distributed to other devices.	Supported	Supported	Supported
Image import from URL	Ability to import software image from network accessible locations (URI/URL) to Prime Infrastructure. The software image can then be distributed to other devices.	Supported	Supported	Supported
Image import from Cisco.com	Ability to import software image from a trusted Cisco website to Prime Infrastructure. The software image can then be distributed to other devices.	Supported	Supported	Supported
Image upgrade/distribution	Ability to upgrade software image on the managed devices from Prime Infrastructure. This allows you to update the software image for multiple devices based on demand or at a later point in time as scheduled. The feedback and status are displayed during the upgrade and devices can be restarted, if required. In large deployments, you can stagger reboots so that the service at a site is not completely down during the upgrade window. **Note** Software image distribution for Cisco WiSM2 controllers is not supported.	Supported	Supported	Supported
Image recommendation	Ability to recommend a compatible image for the devices that are managed from Prime Infrastructure.	Not supported because the flash requirement is not available.	Supported	Supported
Image upgrade analysis	Ability to analyze the software images to determine the hardware upgrades required before you can perform the software upgrade.	Not supported because there is no minimum requirement for RAM or ROM. The newly upgraded image replaces the existing image after an upgrade.	Supported	Supported

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 device software images on Cisco.com should be included during inventory collection of the devices. Specifying image management preferences changes the default behavior of your devices.

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 set image management and distribution preferences:

Step 1 Choose **Administration > System Settings > Image Management**.

Step 2 Enter your Cisco.com username and password so that you can access software images from the cisco.com.

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. Hover your mouse cursor on the information icon to view details about the options.

Note To have Prime Infrastructure use SSH and not Telnet, check the **Use SCP for image upgrade and import** option.

The Config Protocol Order field specifies the order in which the protocol is used. For example, if SSH is listed before Telnet, SSH is used first, and Telnet is used next.

Step 5 Click **Save**.

Step 6 Choose **Operate > Image Dashboard** to view all of 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 a software image name to display details about the image.

Step 3 Do any of the following:

- Change image requirements. See Changing Software Image Requirements, page 15-5.
- View the devices on which the software image is running.
- Distribute the image. See Deploying Software Images to Devices, page 15-5.

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 Prime Infrastructure waits for a maximum of 100 minutes for an image to be imported to the Software Image Repository. If an image takes longer than 100 minutes to import, the job fails and Prime Infrastructure displays an error message in **Administration > Jobs Dashboard**.

To import a software image:

Step 1 Choose **Operate > Software Image Management**.

Step 2 Click **Import**.

Step 3 Specify the source from which the software image is imported. You can specify any one of the following sources:

- Device—An existing device.
- Cisco.com
- URL—Specify the FTP URL from where you can import the software image. You can use an HTTP URL where user credentials are not required.
- File—A local file on the client machine.

Note For wireless LAN controllers, you can import software images from Cisco.com, file, or a URL, but not from a device. For more information about Software Image Management Processes and Supported Devices, see Table 15-1.

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 **Administration > Jobs Dashboard** to view the status about the image management job. The Duration field is updated after the job completes.

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 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.

Note Software image distribution for Cisco WiSM2 controllers is not supported.

Step 1 Choose **Deploy > Software Deployment**.

Step 2 Select the software images that 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 of the devices available in Prime Infrastructure, or from the Device Groups list, select the devices that 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 of the devices.

Step 4 Choose the image name in the 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, choose the value displayed in the 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 Choose **Administration > System > Image Management** to change the default distribution options.

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 about the image management job. The Duration field is updated after the job completes.

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, click **Start Recommendation**, then skip ahead to Step 6.
- **Select Image from Local Repository** to select an image stored locally. Then, under Local Repository:
  - Select the **Show All Images** check box to display all images available in the Prime Infrastructure repository.
  - Unselect the **Show All Images** check box to display the software images applicable to the selected device.

Step 5 Select the image to distribute, then click **Apply**.

Step 6 Choose the image name in the 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, choose the value displayed in the 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**.

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?

To analyze software image upgrades:

Step 1 Choose **Operate > Software Image Management**.

Step 2 Click **Upgrade Analysis**.

Step 3 Choose the source of the software image that you want to analyze.

Step 4 Select the devices on which to analyze the software image.

Step 5 Select the images to analyze for the selected devices.

Step 6 Click **Run Report**.

CHAPTER 16

Working with Wireless Operational Tools

The Wireless Operational Tools menu allows you to:

- Add or modify guest user templates
- Perform voice audit on controllers
- Diagnose voice calls in realtime
- Analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags
- View all config audit alarm details
- Configure and run migration analysis, and view the report
- Monitor all nearby access points and discover rogue access points
- Monitor RFID tag status
- Configure and edit chokepoints
- Monitor interference devices detected by the CleanAir enabled access points
- Configure spectrum experts and WiFi TDOA receivers

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 configures a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires.

Note When you configure a guest account with unlimited lifetime, for Catalyst 3850 Switches (Cisco IOS XE 3.2.1) and Cisco 5760 Wireless LAN Controllers, the maximum time period that the guest account will be active is one year.

Step 1 Choose **Operate > Operational Tools > Wireless > Guest User**.

Note To reduce clutter, Cisco 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 Do either of the following:

- To add a new template:

a. Choose **Select a command** > **Add Guest User**, and click **Go**.

b. In the New Controller Template page, complete the fields as described in the *Guest User Controller Templates Field Descriptions* section in the *Cisco Prime Infrastructure 2.0 Reference Guide*.

- To modify an existing template, click the template name link and make your changes.

Step 3 Click **Save**.

Running a Voice Audit on a Controller

Prime Infrastructure provides a voice auditing mechanism to check controller configuration and to ensure that any deviation from the deployment guidelines is highlighted as an Audit Violation. You can run a 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 the *Voice Audit Field Descriptions* section in the *Cisco Prime Infrastructure 2.0 Reference Guide.*

Step 3 Click the **Rules** tab.

Step 4 In the VoWLAN SSID text box, type the applicable VoWLAN SSID.

Note The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.

Step 5 Do either of the following:

- To save the configuration without running a report, click **Save**.
- To save the configuration and run a report, click **Save and Run**.

Step 6 Click the **Report** tab to view the report results.

Running Voice Diagnostics

The Voice Diagnostic tool is an interactive tool that diagnoses voice calls in real time. This tool reports call control errors, clients' roaming history, and the total number of active calls accepted and rejected by an associated AP.

The Voice Diagnostic test is provisioned for multiple controllers; that is, if the AP is associated with more than one controller during roaming, the Voice Diagnostic tool tests all associated controllers. Prime Infrastructure supports testing on controllers whose APs are placed on up to three floors. For example, a Prime Infrastructure map might have floors 1 to 4, with all APs associated to controllers (WLC1, WLC2, WLC3, and WLC4) and placed on the Prime Infrastructure map. If a client on any AP is associated with WLC1 on the first floor and a Voice Diagnostic test is started for that client, a test is also provisioned on WLC2 and WLC3.

The Voice Diagnostic page lists prior test runs, if any. For information about the fields on this page, see the *Voice Diagnostic Field Descriptions* section in the *Cisco Prime Infrastructure 2.0 Reference Guide*.

From the Select a command from the drop-down list, you can start a new test, check the results of an existing test, or delete a test.

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.

To run a Voice Diagnostic test:

Step 1 Choose **Operate > Operational Tools > Wireless > Voice Diagnostics**.

Step 2 From the Select a command drop-down list, choose the New test and click **Go**.

Note You can configure a maximum of two clients for voice call diagnosis. Both clients can be on the same call or can be on a different call.

Step 3 Enter a test name and the length of time to monitor the voice call.

Step 4 Enter the MAC address of the device for which you want to run the voice diagnostic test.

Step 5 Select a device type; if you select a custom phone, enter an RSSI range.

Step 6 Click **StartTest**.

Location Accuracy Tool

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy tool.

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 tool enables you to run either of the following tests:

- **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 prepositioned 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.

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 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**.

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).

Scheduling a Location Accuracy Test

Use the scheduled accuracy testing to verify the accuracy of the current location of non-rogue and rogue clients, interferers, and asset tags. You can get a PDF of the test results at **Accuracy Tests** > **Results**. 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.

To schedule a Location 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 an area type, a building, and a floor from the corresponding drop-down lists.

Note Campus is configured as Root Area, by default. There is no need to change this setting.

Step 5 Choose a beginning and ending time for 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 6 Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.)

Step 7 Click **Position Testpoints**.

Step 8 On the floor map, check the check box next to each client, tag, and interferer for which you want to check location accuracy.

When you check a MAC address check box, two icons appear on the map. One represents the actual location and the other represents the reported location. 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. (You cannot drag the reported location.)

Step 9 (Optional) To enter a MAC address for a client, tag, or interferer that is not listed, check the **Add New MAC** check box, enter the MAC address, and click **Go**.

An icon for the newly added element appears on the map. If the element is on the location server but on a different floor, the icon appears in the left-most corner (in the 0,0 position).

Step 10 When all elements are positioned, click **Save**.

Step 11 Click **OK** to close the confirmation dialog box.

You are returned to the Accuracy Tests summary page.

Step 12 To check the test results, click the test name, click the **Results** tab in the page that appears, and click **Download** under Saved Report.

Running an On-Demand Location Accuracy Test

You can run an On-Demand Accuracy Test when elements are associated but not prepositioned. 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 of a small number of clients, tags, and interferers. You can get a PDF of the test results at **Accuracy Tests** > **Results**. 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

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 an area type, a building, and a floor from the corresponding drop-down lists.

Note Campus is configured as Root Area, by default. There is no need to change this setting.

Step 5 Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.)

Step 6 Click **Position Testpoints**.

Step 7 To test the location accuracy and RSSI of a particular location, select client, tag, or interferer from the drop-down list on the left. A list of all MAC addresses for the selected option (client, tag, or interferer) is displayed in a drop-down list to the right.

Step 8 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 9 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 10 Click **Start** to begin collection of accuracy data, and click **Stop** to finish collection. You must allow the test to run for at least two minutes before stopping the test.

Step 11 Repeat Step 11 to Step 14 for each testpoint that you want to plot on the map.

Step 12 Click **Analyze Results** when you are finished mapping the testpoints, and then click the **Results** tab in the page that appears to view the report.

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—Templates that are configured for Background Audit and are enforcement enabled.
- Total Mismatched Controllers—Configuration differences found between Prime Infrastructure and the controller during the last audit.
- Total Config Audit Alarms—Alarms generated when audit discrepancies are enforced on configuration groups. If enforcement fails, a critical alarm is generated on the configuration group. If enforcement succeeds, a minor alarm is generated on the configuration group. Alarms contain links to the audit report, where you can view a list of discrepancies for each controller.
- Most recent 5 config audit alarms—Includes object name, event type, date, and time of 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.

Autonomous access points are eligible for migration only if all 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—Conversion is supported only from Cisco IOS 12.3(7)JA releases excluding Cisco IOS 12.3(11)JA, Cisco IOS 12.3(11)JA1, Cisco IOS 12.3(11)JA2, and Cisco IOS 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.

Upgrading Autonomous Access Points

You can choose to upgrade autonomous access points manually or automatically. On the Migration Analysis page, select an access point whose software version is shown as failed, and choose **Upgrade firmware (manual)** or **Upgrade firmware (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 on each 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 an access point and a controller is required to send an association request, an 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

On the Migration Analysis Summary page, choose **Select a command** > **Run Migration Analysis**. 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

On the Migration Analysis Summary page, Choose **Select a command** > **View Migration Analysis Report**. The report includes the following:

- Access point address
- Status
- Time stamp
- Access point logs

Viewing a Firmware Upgrade Report

Choose **Select a command** > **View Firmware Upgrade Report** 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.
- Time stamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

Viewing a Role Change Report

Because a wired connection between an access point and a controller is required to send an 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.
- Time stamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

RRM

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points to automatically discover rogue access points.

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.

RRM statistics help to identify trouble spots and provide possible reasons for channel or power-level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on event groupings. The event groupings may include the following:

- Worst performing access points
- Configuration mismatch between controllers in the same RF group
- Coverage holes that were detected by access points based on threshold
- Precoverage holes that were detected by controllers
- Ratios of access points operating at maximum power

Note RRM dashboard information is available only for lightweight access points.

Channel Change Notifications

Notifications are sent to the 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 that 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 defaults.

When a channel change trap is received after an earlier channel change, the event is marked as Channel Revised; otherwise, it is marked as Channel Changed. A channel change event can have multiple causes. The reason code is factored and equated to 1, irrespective of the number of reasons that are possible. For example, suppose a channel change might be caused by signal, interference, or noise. The reason code in the notification is refactored across the reasons. If the event had three causes, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events have the same reason code, all three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

Notifications are sent to the 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 grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With automatic grouping, 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.)

RRM Dashboard

The RRM dashboard is available at **Operate > Operational Tools > Wireless > Radio Resource Management**.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups. To get the latest number of RF Groups, run the configuration synchronization 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 of 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 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.

The Tag Summary page is available at **Operate > Operational Tools > Wireless > RFID Tags**.

Searching RFID Tags

Use the Prime Infrastructure Advanced Search feature to find specific tags or all tags.

To search for tags:

Step 1 Click **Advanced Search**.

Step 2 From the Search Category drop-down list, choose **Tags**.

Step 3 Enter the required information. Note that search fields sometimes change, depending on the category chosen.

Step 4 Click **Go**.

Checking RFID Tag Search Results

To check the search results, click the MAC address of a tag location on a search results page.

Note the following:

- The Tag Vendor option does not appear when Asset Name, Asset Category, Asset Group, or MAC Address is the search criterion.
- Only vendor tags that support telemetry appear.
- The Telemetry data option appears only when MSE (select for location servers), Floor Area, or Outdoor Area is selected as the “Search for tags by” option.
- 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.
- Asset Information, Statistics, Location, and Location Notification details are displayed.
- Only CCX v1 compliant tags are displayed for emergency data.

Viewing Tag List

Click the **Total Tags number** link to view the Tags List for the applicable device name. The Tag List contains the MAC address, asset details, vendor name, mobility services engine, controller, battery status, and map location.

Chokepoints

Chokepoints are low-frequency transmitting devices. When a tag passes within range of a placed chokepoint, the low-frequency field awakens the tag, which, in turn, sends a message over the Cisco Unified Wireless Network that includes 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 is installed and operational, it can be entered into the location database and plotted on a Prime Infrastructure map.

Adding a Chokepoint to the Prime Infrastructure Database

To add a chokepoint to the 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 Specify either an entry or 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**.

After the chokepoint is added to the database, it can be placed on the appropriate Prime Infrastructure floor map.

Adding a Chokepoint to a Prime Infrastructure Map

To add a 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**.

The Add Chokepoints summary page lists all recently added chokepoints that are in the database but not yet mapped.

Step 5 Check 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 corner. You are now ready to place the chokepoint on the map.

Step 7 Click the chokepoint icon and drag it to the proper location.

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**.

The newly created chokepoint icon might or might not appear on the map, depending on the display settings for that floor. 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.

Step 10 Synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing a Chokepoint from the Prime Infrastructure Database

To remove a chokepoint from the Prime Infrastructure database:

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.

Removing a Chokepoint from a Prime Infrastructure Map

To remove a chokepoint from a Prime Infrastructure 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 **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Editing a Chokepoint

To edit a chokepoint in the Prime Infrastructure database and the appropriate map:

Step 1 Choose **Operate > Operational Tools > Wireless > Chokepoints**.

Step 2 In the MAC Address column, click the chokepoint you want to edit.

Step 3 Edit the parameters that you want to change.

Note The chokepoint range is product-specific and is supplied by the chokepoint vendor.

Step 4 Click **Save**.

Monitoring Interferers

In the **Monitor** > **Interferers** page, you can monitor interference devices detected by CleanAir-enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

Table 16-1 lists the menu paths to follow to monitor interferers.

Table 16-1 Menu Paths to Monitor Interferers

To See...	Go To...
AP-detected interferers	**Operate** > **Operational Tools** > **Wireless** > **Interferers**
AP-detected interferer details	**Operate** > **Operational Tools** > **Wireless** > **Interferers** > *Interferer ID*
AP-detected interferer details location history	**Operate** > **Operational Tools** > **Wireless** > **Interferers** > *Interferer ID*, then choose **Select a command** > **Location History** and click **Go**

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.

Adding a Spectrum Expert

To add a spectrum expert:

Step 1 Choose **Operate > Operational Tools > Wireless > Spectrum Experts**.

Step 2 Choose **Select a command** > **Add Spectrum Expert**. (This link appears only if no spectrum experts already exist.)

Step 3 Enter the hostname or IP address of the spectrum expert. If you use the 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 with Prime Infrastructure.

Spectrum Experts Details

The Spectrum Expert Details page provides interference details for a single spectrum expert. This page is updated every 20 seconds, providing a real-time look at what is happening on the remote spectrum expert. This page displays the following:

- Total Interferer Count—As seen by the specific spectrum expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferers by category.
- Active Interferer Count Per Channel—Displays the number of interferers, 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 authenticated and associated with the radio of one of the access points listed in the access point list.

Wi-Fi TDOA Receivers

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.

Enhancing Tag Location Reporting with Wi-Fi TDOA Receivers

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 the Adding a Mobility Services Engine section in the Cisco Prime Infrastructure 2.0 Configuration Guide.
2. Add the TDOA receiver to Prime Infrastructure database and map. See the "Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps" section on page 16-18.
3. Activate or start the partner engine service on the MSE using Prime Infrastructure.
4. Synchronize Prime Infrastructure and mobility services engines. See the Synchronizing Services section in the Cisco Prime Infrastructure 2.0 Configuration Guide.
5. Set up the TDOA receiver using the AeroScout System Manager. 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 a 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 the Prime Infrastructure database and the 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 A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Step 6 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**.

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 corner. You are now ready to place the TDOA receiver on the map.

Step 12 Click the TDOA receiver icon and drag it to the proper location on the floor map.

Step 13 Click **Save**.

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 Check the **WiFi TDOA Receivers** check box.

When you hover your mouse cursor over a TDOA receiver on a map, configuration details appear 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 Download the partner engine software to the mobility services engine.

CHAPTER 17

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.

Note To use this feature, your Cisco Prime Infrastructure implementation must include Assurance licenses.

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 (see Identifying Optimization Candidates, page 17-4).
- Establishing site and application performance baselines (see Establishing Performance Baselines, page 17-5).

  Prime Infrastructure performs baselining for key performance metrics and detects abnormal deviations of baselined values. The key performance metrics include:

  - Server Response Time
  - Client Transaction Time
  - Network Round-Trip Time
  - MOS score
  - Jitters
  - Packet loss
  - Bytes sent/received
  - Interface utilization
  - CPU Utilization
  - Memory Utilization

Prime Infrastructure determines the baseline (mean) for each metric by taking the average values of the metric during the last 30 days. Average values are computed separately for each hour of the day for each monitored entity (such as interface, host, site, or application). For example, the baseline for HTTP response time of a given server between 9AM to 10AM today will be different from the baseline of the same server between 7PM to 8PM yesterday.

Prime Infrastructure also computes the metrics' standard deviations using the last 30 days of data. Similar to averages, standard deviations are computed separately for each hour of the day for each monitored entity.

- Post-implementation validation that WAN performance and application stability have actually improved (see Validating Optimization ROI, page 17-7).

  Because the mean and standard deviation of each metric vary over time, Prime Infrastructure continuously reevaluates the thresholds used to compute the health scores (adaptive thresholds). Prime Infrastructure computes baselines and thresholds every hour, and evaluates health scores every five minutes. In each interval:

  a. Health scores are computed for every application-site combination.

  b. These health scores are aggregated to derive the overall health of each business-critical application (across all sites) and overall health of each site (across all business-critical applications).

  When aggregating across sites/applications, the worst scores are used. For example, if any business-critical application of a given site is rated "red," that site is also rated "red" for that interval. See Health Rules, page 17-3 for more information.

- Ongoing monitoring and troubleshooting of the optimized flows (see Monitoring Optimized Flows, page 17-7).

  Using the baseline means and standard deviations, Prime Infrastructure can monitor application and service health issues by detecting abnormal deviations of key metrics from their baselined values and assign a health scores (red, yellow, or green) for each application and site for each monitoring interval:

  – A red score indicates a highly abnormal deviation from baseline (deviations from baselines with a probability of less than 0.1%).

  – A yellow score indicates a mildly abnormal deviation (deviations with a probability of less than 1%).

  – A green score indicates that the metric is within its normal range.

  – A gray score indicates there is insufficient data for a site/application.

Cisco Prime Infrastructure offers a consistent data resource for each of these stages in performance optimization.

Evaluating Service Health

The Service Health dashboard (**Home > Performance > Service Health**) displays the sites and their business critical applications. Each application for a site is given a score for each of the KPIs (Key Performance Indicators) that are available in the system:

- **Traffic** (megabits per second)
- **Client Experience** (varies based on application type: average transaction time for transaction-based applications such as HTTP, or MOS code for real-time applications such as RTP)
- **Network Performance** (average network time for HTTP, jitter and Package Loss for RTP)

- **Application Response** (applicable only for transaction-based applications such as HTTP)

The KPI scores can come from multiple data sources; scores are computed across all data sources for all of the KPIs, and the overall score in the main dashboard is an aggregate of these scores. Scores are assigned as red, yellow, or green based on the warning and critical threshold values assigned in **Administration > Health Rules**; you can use this option to modify the health rule settings as necessary for your network.

For data to be displayed in Service Health, there must be at least one hour of data. After the first hour, the previous hour's data is overlaid on the data line as the historical data for the next hour. After the first day, standard deviation and mean are based on the hourly data for the previous day.

Note The Site-Application Health Summary dashlet will display data *two hours* after the server has been installed; baseline dashlets will display baseline values after *one hour*.

These scores are stored for seven days. When you view the data for a previous day, the maximum moving time interval is six hours (you can look at up to six hours of data at a time).

Health Rules

The data displayed in the Service Health dashboard (**Home > Performance > Service Health**) is computed using health rules. You can customize the health rules by clicking the desired row and editing the Critical and Warning values.

- Critical—turns red when the data value exceeds the specified Critical value.
- Warning—turns yellow when the data value exceeds the Warning value.

If the health rule does not exceed the specified Critical or Warning values, it is green.

For example, for Traffic Rate, you might specify the T1 the baseline value of 100 Mbps for a given site, application, and datasource, and the standard deviation value of 20 Mbps.

If the Traffic Rate exceeds 161.8 Mbps, which is 100+(3.09 x 20), you see a red bar indicating a critical warning.

You can click any of the colored bars to get further details.

Creating Custom Applications

Use the **Applications and Services** option to create and manage custom applications and services. *Services* are groups of applications. Prime Infrastructure provides a default set of applications and services consistent with the Cisco NBAR standard. (See http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html for more information.)

You can create custom applications that contain the definitions you require and which are not available (either from the device or from Prime Infrastructure). After you create an application, you can deploy the application to the supported devices. Deploying the application definition to the device makes Netflow exported data consistent with Prime Infrastructure and other management tools.

If you deploy a custom application to a device and later want to remove it, you must undeploy the application using the **Applications and Services** option. If you delete the custom application from Prime Infrastructure only, the custom application remains active on the device.

Applications without definitions are displayed as "unknown."

Custom applications are organized under services; services are organized by category and subcategory to align with the Cisco NBAR standard. For more information about NBAR, see http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html.

To create a custom application:

Step 1 Choose **Operate > Applications and Services**, click **All Applications** in the left column, then click **Create**.

Step 2 On the Service Health dashboard, some applications are already set as "Business Critical". To view the currently defined business critical applications and to edit the contents of the Service Health dashboard:

a. Click **All Applications** in the left column, check the check box for the application, then click **Edit**.

b. In the Edit Application box, check the **Business Critical** check box, then click **Update**.

Step 3 Enter any additional required fields, then click **Create**.

Step 4 Push your new application to a NAM or an ASR/ISR:

a. Choose the **User Defined Applications**, from the show drop-down list, and check the new application check box, then click **Deploy**.

b. In the Device Selection dialog box, select the NAM device or the ISR/ASR to which this application is to be deployed, then click **Submit**.

c. Click **View Jobs** to display the status of the deployment job.

Identifying Optimization Candidates

Follow these steps to identify your network's lowest performing applications, clients, servers, and network links.

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards**, then click the **WAN Optimization** tab.

Step 2 Add the following dashlets (see Adding Dashlets, page A-4) to this dashboard:

- Application Traffic
- Server Traffic
- Client Traffic
- Network Links

Step 3 Using these dashlets, identify the optimization candidates:

- All of 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 that client and server endpoints of each link, and the average length of time that the link exists.
- **Server Traffic** shows both the server IP address and the application that it serves.

Step 4 Sort and filter the performance data as needed:

- To sort on any column in any dashlet, click the column heading.
- To filter the data displayed in all of 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 its Filter icon and specify a Quick or Advanced Filter, or use a Preset Filter.

Step 5 For a quick report of the same data:

a. Choose **Report > Report Launch Pad**. Choose **Operate > Performance > WAN Traffic Analysis Summary**.

b. Specify filter and other criteria for the report, then click **Run**.

Establishing Performance Baselines

Follow these steps to establish the standard performance characteristics of your candidate applications and sites before implementing WAN optimizations.

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards**, then click the **Application** tab.

Step 2 Add the following dashlets (see Adding Dashlets, page A-4) to this page:

- Worst N Clients by ART Metrics
- Worst N Sites by ART Metrics
- Application Server Performance
- Application Traffic Analysis

Step 3 Use these dashlets to establish the performance characteristics of your optimization candidates as currently configured:

- **Worst N Clients by ART Metrics**: For the worst-performing clients and applications: Maximum and average transaction times, and 24-hour performance trend.
- **Worst N Sites by ART Metrics**: The same information for the worst-performing sites and applications.

- **Application 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 the column heading. You can also filter the data in the dashlets by **Time Frame**, **Site**, and **Application**.

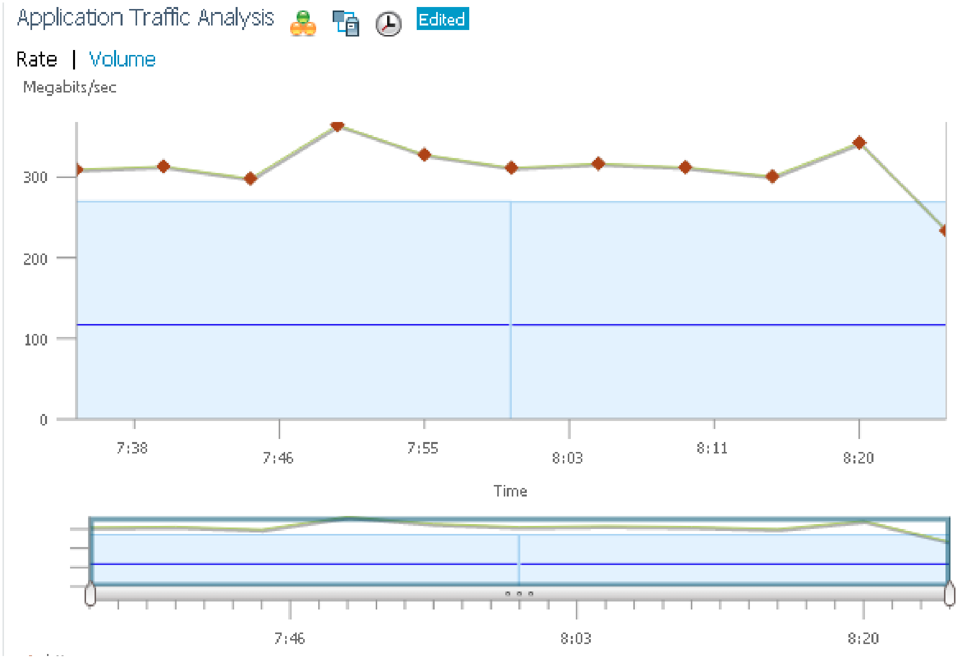
Step 4 Click the **Site** tab and use **Top N Applications, Top N Devices with Most Alarms**, **Top N Clients** and **Worst N Clients by ART Metrics** as you did in Step 3.

Enabling Baselining

Standard deviation and mean values are used to compute the scores in the Service Health dashboard. Baselining is not enabled by default. When baselining is enabled:

- The blue box indicates the standard deviation.
- The blue line indicates the mean value for that hour.

Figure 17-1 Sample Baseline Values



To enable baselining:

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards**, then click the **Application** tab.

Baselining is supported by these dashlets:

- Application Traffic Analysis—Shows the aggregate bandwidth rate/volume for a site/enterprise one application, service, or set of applications.

- Application ART Analysis—Shows the response times for a transaction.

Step 2 To enable application traffic analysis baselining:

a. Open the **Application Traffic Analysis** dashlet, hover your cursor over the dashlet icons and click **Dashlet Options**.

b. Check the **Baseline** check box and save your changes.

Step 3 To enable application response time analysis baselining:

a. Open the **Application ART Analysis** dashlet, hover your cursor over the dashlet icons and click **Dashlet Options**.

b. Choose a metric from the **Metric Type** drop-down list.

If you choose the **Server Response Time** metric, you can select an individual Application Server to see what the response time of that server has been in the past.

c. Check the **Baseline** check box and save your changes.

Validating Optimization ROI

After you have deployed your WAAS changes at candidate sites, follow these steps to validate the return on your optimization investment.

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards.**

Step 2 Click the **WAN Optimization** 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 pass through 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 To generate a report:

a. Choose **Tools > Reports > Report Launch Pad**, then choose **Performance > WAN Application Performance Analysis Summary**.

b. Specify the filter and other settings for the report, then click **Run**.

Monitoring Optimized Flows

Follow these steps to monitor WAAS-optimized WAN traffic.

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards**.

Step 2 Click the **WAN Optimization** tab, open the **Multi-Segment Analysis** dashlet, then click **View Multi-Segment Analysis**.

Step 3 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 4 Sort and filter the performance data as needed:

- To sort any column, click the column heading.
- You can filter the data displayed by **Time Frame**, Or click the Filter icon and specify a Quick or Advanced Filter, or use a Preset Filter.

Working with Wireless Mobility

What Is Mobility?

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another securely and with as little latency as possible. To allow more flexible roaming and to minimize the need for tunnel encapsulation of traffic, Cisco Prime Infrastructure provides a robust mobility architecture that distributes mobility functionality across the network devices.

The following are the key elements of the mobility architecture:

- Mobility Controller (MC)—The MC (for example, Cisco 5700 Series Wireless Controller) is responsible for one or more MAs or switch peer groups, handling roaming within its span of control, and transiting traffic between MAs and/or MCs when co-located with MTE.
- Mobility Agent (MA)—The MA (for example, Catalyst 3850 Switch) resides in the access switch or edge switch that the WAP is directly connected to, and terminates at the CAPWAP tunnel for communications with the WAP.
- Mobility Oracle (MO)—The MO is a top-level control entity responsible for connecting multiple MCs or mobility subdomains in deployments of the largest scale, to enable roaming across very large physical areas.
- Mobility Domain—A roaming domain: a mobile user may roam across all of the devices in this domain (the set of WAPs and all of the control entities associated with it). This typically includes MAs and MCs, and may include a MO (to join multiple subdomains).
- Mobility Sub-Domain—The set of WAPs and associated MAs and one MC, representing a portion of a larger mobility domain (where a MO serves to coordinate roaming between multiple sub-domains).
- Switch Peer Group (SPG)—A group of switches (acting as MAs). An SPG establishes a full mesh of mobility tunnels among the group members to support efficient roaming across the WAPs associated with the switches in the group. An SPG is also intended to limit the scope of interactions between switches during handoffs. An SPG is configured by the Mobility Controller, and every switch in the switch peer group has the same view of the membership. The switches in an SPG might be interconnected by a set of direct tunnels. When a station roams from one switch to another within

the same switch peer group, if the point of presence stays at the original or anchor switch, the traffic can be directly tunneled back to the anchor switch without involving the MTE. This direct tunneling mechanism is a data path optimization and is optional.

- Mobility Group—A mobility group is a set of MCs (and their associated MAs / switch peer groups)
- Mobility Tunnel Endpoint—The Mobility Tunnel Endpoint (MTE) provides data plane services for mobile devices through the use of tunneling. This minimizes the impact of roaming events on the network by keeping the user's point of presence on the network a constant. If the VLAN or subnet of the roamed client is available at the MTE, the MTE could become the point of presence; otherwise it merely functions as a tunnel switching entity that connects the roamed client to access switch or MTE that is the point of presence.

Related Topics

- Mobility Work Center
- Creating a Mobility Domain

Mobility Work Center

The Mobility Work Center is available only in Life Cycle View at **Operate >Mobility Work Center**.

The following information is displayed:

- Device Name—Name of the MC.
- Management IP—Management IP address of the MC.
- Wireless Interface IP—IP address on the MC which is used for mobility protocol.
- Mobility Group—Name of the mobility group the MC belongs to.
- Mobility Role—Shows administrative and operational mobility mode. If Admin and Operational values are different, the device needs reboot for the administrative mode to be effective. It shows MO in addition to mobility mode if Mobility Oracle is enabled on it.

In this page, you can perform the following tasks:

- Create Mobility Domain—See the "Creating a Mobility Domain" section on page 18-3.
- Create Switch Peer Group—To create switch peer groups in MC.
- Change Mobility Role—To change the controllers from MA to MC.
- Delete Domain—Deletes only the domain; it does not delete the controllers from Prime Infrastructure.
- Delete Members—To remove selected MCs from a selected domain.
- Set as Mobility Oracle—To enable MO on a selected MC, if the MC must act as the MO for the entire domain. There can be only one MO per domain. Only Cisco 5760 series controllers support the MO feature.
- Add members to switch peer group—To add members to switch peer group.
- Delete members from switch peer group—To delete members from switch peer group.

Note By default, the Mobility Work Center page displays all of the mobility domains configured in the managed network. To see a list of mobility devices, choose **All Mobility Devices** from the left sidebar.

Related Topics

- What Is Mobility?
- Creating a Mobility Domain

Creating a Mobility Domain

A mobility domain is a collection of controllers that have all been configured with each other's IP addresses, allowing clients to roam between the controllers in the mobility domain.

The Mobility Work Center displays all mobility domains configured in the managed network using Prime Infrastructure. The left sidebar menu shows:

- Domains
- MCs in each domain
- SPGs on each MC
- MAs in each SPG

When a node is selected from the left sidebar, the right pane shows more details. When a domain node is selected from the left sidebar, the right pane displays the MCs in the domain.

To create a mobility domain:

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

Step 2 Click on the left sidebar menu.

Step 3 Enter a name for the mobility domain for the set of MCs that you want to group together.

If a selected MC exists in another domain, it is removed from that domain and added to the new domain.

Step 4 Select mobility domain member devices.

A device can belong to one domain or SPG only.

Step 5 Click **Apply**.

Creating a Switch Peer Group

An MC can have switch peer groups (SPGs), and a switch peer group can have MAs. The MAs in a managed network are listed on the Switch Peer Group page. If you create a switch peer group when you already have one, MAs are moved from the old switch peer group to the new one, and the MC wireless interface IP address is set on all of the MAs.

To create a switch peer group, follow these steps:

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

Step 2 Choose an MC from the left sidebar.

Step 3 Click **Create Switch Peer Group**.

Step 4 Enter a name for the switch peer group that will contain the set of MAs that you want to group together on the selected MC.

If a selected MA exists in another switch peer group, it is removed from that group and added to the new group. You can create multiple switch peer groups on an MC.

Step 5 Select mobility agents.

A device can belong to one domain or SPG only.

Step 6 Click **Apply**.

The SPG that you created appears in the left sidebar. You can navigate to it to see the mobility agents on the selected switch peer group.

Changing a Mobility Role

By default, Cisco 3850 controllers act as MAs. These controllers can be converted to MCs if MCs are needed in the network.

To change a mobility role:

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

Step 2 Choose **All Mobility Devices** from the left sidebar.

Step 3 Select a device and the role that you want to change to:

- Change Role To Mobility Controller—Enables the mobility controller feature on the selected controller.
- Change Role To Mobility Agent—Enables the Mobility Agent feature on the selected controller. When you do this, the MC feature is disabled.

  Converting MAs to MCs (and vice versa) is limited to 3850 devices. For a changed role to take effect, you must reboot the device.
- Assign Mobility Group—Allows you to enter new mobility group name for the selected device.

Step 4 Click **Apply**.

Mobility Anchors

Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN. This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of a client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographic load balancing because WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

Configuring a Guest Anchor Controller for a WLAN

The guest anchor controller is a controller dedicated to guest traffic, and is located in an unsecured network area, often called the demilitarized zone (DMZ). Other internal WLAN controllers from where the traffic originates are located in the enterprise LAN.

Note The Cisco 5760 controller can be a Guest Anchor whereas the Catalyst 3850 switch cannot be a guest anchor but it can be a foreign controller.

You can configure a guest controller as a mobility anchor for a WLAN for load balancing.

Before You Begin

- Ensure that wireless devices are set up in Prime Infrastructure. For more information about setting up wireless devices, see the "Configuring Wireless Features" section on page 6-11.
- Ensure that the wireless devices that you want to configure as mobility anchors for a WLAN are in the same mobility domain.

To configure a guest anchor controller for a WLAN:

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

Step 2 In the Device Group area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the controller that you want to designate as a guest mobility anchor. The details of the device appear in the lower part of the page.

Step 4 Click the **Configuration** tab.

Step 5 From the left sidebar menu, choose **WLANs** > **WLAN Configuration**. The WLAN Configuration page appears.

Note If you are in the Classic view, choose **Configure** > **Controllers** > *Ctrl IP addr* > WLANs > WLAN Configuration to access the WLAN Configuration page.

Step 6 Select the URL of the desired WLAN ID. A tabbed page appears.

Step 7 Click the **Advanced** tab, and then click the **Mobility Anchors** link at the bottom of the page. The Mobility Anchors page appears.

Note You can also access the Mobility Anchors page from the WLAN Configuration page. Select the check box of the desired WLAN ID. From the Select a command drop-down list, choose **Mobility Anchors**, and then click **Go**. The Mobility Anchors page appears.

Step 8 Select the **IP address** check box of the controller to be designated a mobility anchor, and click **Save**.

Configuring the Cisco AppNav Solution

Cisco AppNav, is a hardware and software solution that simplifies network integration of WAN optimization. It also overcomes the challenges related to provisioning, visibility, scalability, asymmetry, and high availability.

- Overview of Cisco AppNav, page 19-1
- Components of Cisco AppNav, page 19-1
- Prerequisites for Configuring Cisco AppNav, page 19-3
- Configuring Cisco AppNav, page 19-3

Overview of Cisco AppNav

The Cisco AppNav solution reduces the dependency on the intercepting switch or router by distributing the traffic among Cisco WAAS devices for optimization by using a powerful class and policy mechanism. You can use ISR-WAAS to optimize traffic based on sites or applications. This includes device-level and template-based configurations.

An intelligent load-balancing mechanism in the Cisco IOS-XE software allows the diversion of TCP traffic to various products, including Cisco WAAS and OneFirewall, where Cisco WAAS is the initial target. Router management is performed through the Cisco Prime Infrastructure network management application.

Components of Cisco AppNav

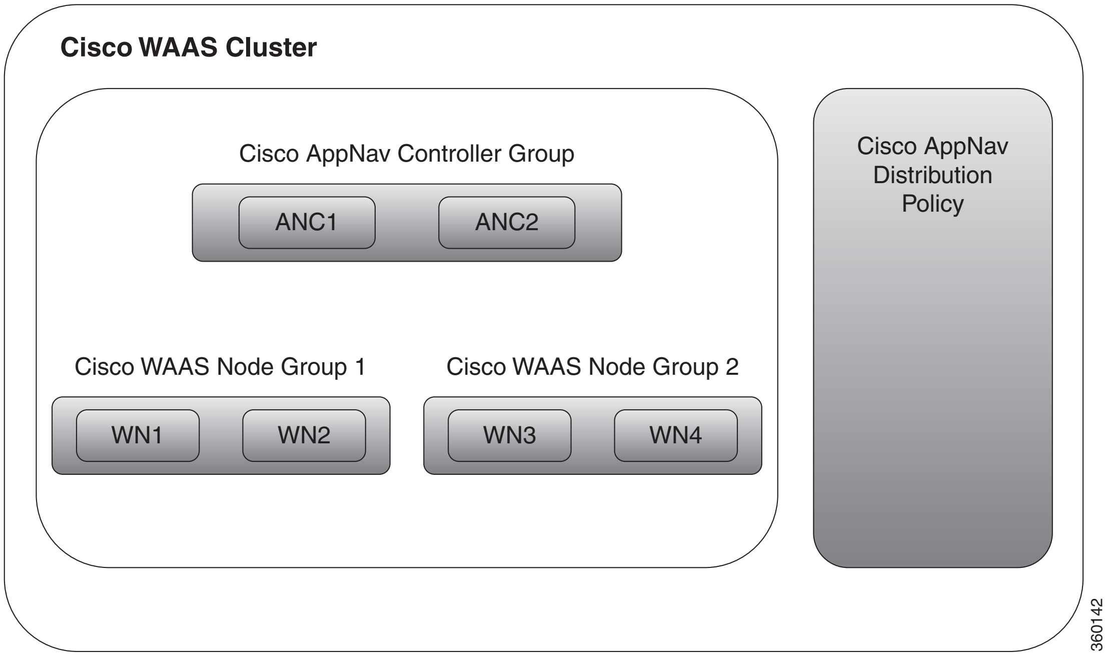
The Cisco AppNav solution, is made up of a distribution unit called the Cisco AppNav Controller (AC), WAAS Service Nodes (SNs). The Cisco AppNav Controller distributes the flow, and the service nodes process the flows. You can group up to four Cisco AppNav-XE (routers) together to form a Cisco AppNav Controller Group (ACG) to support asymmetric flows and high availability. However, must ensure that all of the routers in the ACG are on the same platform and have the same memory capacity.

The Cisco AppNav solution's components perform the following functions:

- AppNav Controller—This is component that intelligently distributes traffic from a router to service nodes. The Cisco AppNav Controller is a part of Cisco IOS-XE Release 3.10 on the Cisco ISR-4400, Cisco CSR, and Cisco ASR 1K platforms.
- Cisco WAAS Service Nodes—These optimize traffic flows and are available in different form factors, for example, standalone appliances and virtualized ISR-WAAS running in a Cisco IOS-XE container.

- Cisco WAAS Central Manager—This is used to monitor and configure the ISR-WAAS.
- This chapter describes the configuration of the Cisco AppNav Controller functions on routers. Figure 19-1 describes the components of Cisco AppNav.

Figure 19-1 Components of Cisco AppNav



The advantages of using the Cisco AppNav components are:

- They can intelligently redirect new flows based on the load on each service node. This includes loads of individual application accelerators.
- If the flows do not require any optimization, service nodes can inform the Cisco AppNav Controller to directly pass the packets, thereby minimizing latency and resource utilization.
- There is minimal impact to traffic when adding or removing service nodes.
- The Cisco AppNav components support VRF. The VRF information is preserved when traffic returns from a service node. However, Prime Infrastructure does not support VRF.
- For specific applications, such as Messaging Application Programming Interface (MAPI) and Virtual desktop infrastructure (VDI), the components ensure that a family of flow is redirected to the same service node.
- Asymmetric flows can be optimized in situations where traffic in one direction goes through one Cisco AppNav Controller and the return traffic goes through a different Cisco AppNav Controller. But both redirect the traffic to the same ISR-WAAS. This is achieved using the Cisco AppNav Controller Group.
- Inter-box high availability is also supported using the Cisco AppNav Controller Group, which means that if one router goes down, traffic can be redirected to a different router in the Cisco AppNav Controller Group enabling uninterrupted flow.

- Intra-box high availability of the Cisco AppNav Controller is supported on those Cisco ASR1000 Series platforms that have dual RP, or dual FP, or both. This means that if the active RP fails, the standby RP takes over or if the active FP fails, the standby FP takes over, and the flows continue uninterrupted.

The Cisco AppNav technology allows IP flows to be intercepted on routers and sent to a set of Cisco WAAS Service Node for processing. The initial application of Cisco AppNav which is supported in Cisco IOS-XE Release 3.10, is in Cisco WAAS.

Prerequisites for Configuring Cisco AppNav

The following are the prerequisites for configuring Cisco AppNav:

- The platform must be Cisco 4451-X ISR, Cisco Integrated Services Routers (ISR) G2, Cisco ASR 1000 Series Aggregation Services Routers, or Cisco Cloud Services Router.
- The software version of above mentioned platforms must be Version 3.10 and later.
- A valid appxk9 license must be enabled on the routers.
- A Cisco WAAS Service Node must be available.

Configuring Cisco AppNav

You must configure some parameters on the router before redirecting the traffic to the Cisco WAAS Service Node. If the Cisco AppNav configuration is generated as a part of installing the Cisco WAAS virtual appliance, it is transparent to the corresponding user. If it is configured using a template or through the Device Work Center, the user is more directly involved.

The Cisco AppNav can be configured in three ways:

- Configuring Cisco AppNav from the Device Work Center, page 19-4
- Configuring Cisco AppNav Using Templates, page 19-5
- Configuring Cisco AppNav Automatically During ISR-WAAS Container Activation, page 19-8

The Cisco AppNav configuration involves the use of the following:

- Controllers—A list of routers that cooperate to redirect traffic. This is a list of IP addresses, exactly one of which must belong to the router on which Cisco AppNav is being configured.
- Cisco WAAS Service Node Groups (SNGs)—There must be one or more SNGs that are the target of redirected traffic and are defined as a set of IP addresses.
- Class Maps—A set of class maps that classify incoming and outgoing traffic. Class maps consist of a set of match conditions that together specify traffic of interest. They can match traffic based on three types of conditions:
  - An access control list (ACL) that selects traffic based on a source and destination IP address and port.
  - A protocol that is used to select traffic that uses the Microsoft port mapper service rather than depending on fixed port numbers. This includes MAPI and a host of other Microsoft protocols.
  - A remote device that matches the traffic that has traversed a particular Cisco WAAS Service Node on the remote end. The remote device is identified by a MAC address.

- Policy maps—A Cisco AppNav policy map is an ordered list of rules, each of which specify what is to be done with some type of traffic. A rule thus consists of a class map and an action. The action is to either redirect to a service node group or to pass through.
- Clusters—A Cisco WAAS cluster is the combination of a policy map, controller group, and a set of service node groups used by the policy map. A cluster can be enabled or disabled. Prime Infrastructure 2.0 allows several clusters to be defined but only one can be enabled at a time. An authentication key is used to secure communication between the controllers and the nodes in a cluster.
- Cisco WAAS interfaces—Traffic can be optimized only on interfaces where Cisco WAAS is enabled.

The WAN optimization template and the Device Work Center both have a default policy. The default policy consists of a number of class maps that match different types of traffic (HTTP, CIFS, TCP, and so on) that is optimized by Cisco ISR-WAAS. The template also includes a policy map containing a rule for each of those class maps. By default, all the matched traffic is redirected to a single service node group.

Configuring Cisco AppNav from the Device Work Center

The Device Work Center allows an administrator to view and modify the configuration of individual devices. The Device Work Center can be used to configure Cisco AppNav when a user has a single or few devices. You can individually edit the configurations that are deployed using a template on the devices.

To configure the Cisco AppNav from the Device Work Center:

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

Step 2 Select the device to be configured.

Step 3 On the Configuration tab in the bottom pane, and click WAN Optimization.

The Cisco AppNav configuration is divided into the following sections:

- AppNav controllers—The Controllers page shows the IP addresses of routers belonging to the same cluster as the router. You must assign one of the addresses to one of the currently selected router's interfaces. Each router's own IP address is shown in a drop-down list. The IP addresses of other routers in the same cluster are listed in a separate table.
- Cisco WAAS clusters —The Cisco WAAS Clusters page is the main Cisco AppNav page. It lists the Cisco WAAS clusters configured on the device and allows new ones to be created. To view the detailed configuration for a cluster, including the policy map, select the cluster, and click **Edit**.
  - In this page, cluster settings and policies can be edited. Expand individual rules by clicking the arrow in the third column. This enables the corresponding rule to be edited as well as the class maps and Cisco WAAS service node groups to be viewed, modified, and created. New rules can be added by clicking **Add Policy**. The order of the rules within a policy map is significant and the table allows the order to modified by dragging rows or selecting a contiguous list of rows and using the Up or Down arrows in the menu bar.
  - To create a new cluster, select **Add WAAS Cluster** on the Cisco WAAS Cluster Overview tab. This launches a wizard that prompts for controllers, Cisco WAAS Service Node, interception interfaces, and some general cluster parameters. After providing the necessary information, click **Finish** for the configuration to take effect.

The wizard creates the cluster with a default policy that works for most small installations. All the TCP flows are redirected to a single node group, with the node group being monitored for overload conditions.

Note Since Prime Infrastructure 2.0 does not support VRFs; therefore, only one Cisco WAAS cluster can be enabled at a time.

- Interception—The Interception page lets the administrator select interfaces on which incoming and outgoing traffic should be redirected (subject to policies). All the WAN interfaces on the router should have Cisco WAAS enabled.
- Advanced Settings—The Advanced Settings folder contains pages for Cisco WAAS service node groups, class maps, and policy maps. Most of this information is also available in the Cisco WAAS Clusters page, but it is helpful to be able to view the definition of these objects directly.
  - Cisco WAAS Node Groups—The Cisco WAAS Node Groups page allows the existing Cisco WAAS node groups to be edited and new ones to be created.
  - Class maps and Policy maps—The Class Maps and Policy Maps page does the same.

Interface Roles

The Cisco AppNav solution redirects traffic only on interfaces on which it has been explicitly enabled. Routers differ in terms of available interfaces and how they are named. Since the templates are intended to be applied to multiple devices, they refer to interface roles instead of actual interfaces.

Interface roles are logical objects that exist only in Prime Infrastructure. They can be used in templates instead of actual interface names. When a template is deployed to a device, the interface role is resolved to a set of actual interfaces.

You can override, the set of interfaces on which Cisco WAAS is enabled during template deployment on a per-device basis. However, we recommend that you to define one or more interface roles and save them as part of the template to simplify the template deployment process.

You can define interface roles in **Design** > **Shared Policy Objects** > **Interface Role**. For more information, see the Creating Interface Roles, page 8-20.

Configuring Cisco AppNav Using Templates

Prime Infrastructure templates contain reusable chunks of configuration that can be deployed to any number of devices. WAN Optimization templates define a policy and other information that can be applied across AppNav routers.

Templates are defined in design view and can later be deployed to one or more devices. As part of the deployment process you can fill in the device-specific parameters and preview the final CLIs before the configuration is pushed to the device. When a template is modified, it is necessary to re-deploy to devices for the changes to take effect.

This method of configuring Cisco AppNav is used when a user needs similar Cisco AppNav configurations on multiple devices. A single template, with similar configurations, and some minor customized values can be deployed to multiple devices at the same type using the deploy option.

To configure the Cisco AppNav using templates:

Step 1 Choose **Design** > **Feature Design**.

Step 2 Choose **Features and Configurations > WAN Optimization**.

Step 3 Select an **AppNav Cluster**.

Step 4 Enter the configuration details on the following tabs:

- Controller IP addresses—A list of controllers can be configured here or during deployment. For example, if the template is used for multiple sites, such as branches, this field must be left empty. However, values can be provided during deployment.
- Service nodes—The Cisco WAAS service node groups are used by the policy map. By default, there is a single service node group called WNG-Default. If the template is used for multiple sites, leave the service node groups empty and add the actual IP addresses during deployment. Enter the following details:
  - Name of the Service Node
  - Description
  - IP address of the Cisco WAAS Service Node
- Interception—Interface roles for which Cisco WAAS should be enabled. During deployment, an actual list of interfaces is presented. You can make a selection of the actual interfaces belonging to the device, for each device. The purpose of the interface roles is to initialize the selection with a default. Therefore, the list of enabled interface roles can be left empty in the template design view. Here you can do the following:
  - Check or uncheck the **Enable WAAS** check box.
- General—A valid cluster ID range is between 1 to 32. Enable the check box to enable or disable a cluster. Enter the following details:
  - Cluster ID
  - Authentication Key
  - After this, check or uncheck the **Enable Distribution** check box.
- Traffic redirection—This is a policy-related configuration, policy-map, class-maps and their relationships with ISR-WAAS groups. A simple setting results in a default policy that redirects all the TCP traffic to one node group. Select the **expert mode** to create custom policies and to redirect different types of TCP traffic to a different ISR-WAAS.

Step 5 Click **Save as Template**.

Step 6 Click **Finish**.

You can view the configured template by choosing **Design** > **Feature Design** > **My Templates**.

Deploying a Cisco AppNav Template

After a Cisco AppNav template is created, you can deploy the template to begin traffic distribution.

To deploy a Cisco AppNav template:

Step 1 Choose **Deploy** > **Configuration Tasks**.

Step 2 Select the **My Templates** folder in the left window pane.

Step 3 Select the Cisco WAAS template to be deployed and click **Deploy**.

You can choose a single device or multiple devices and change the required configurations.

Step 4 In the Value Assignment panel, select each target device, one at a time and complete all the fields for that router:

- Basic Parameters—Includes an indication about whether the cluster is enabled.
- Controllers—The list of controller IP addresses. This must include an IP address assigned to the device itself.
- Node Groups—Enter IP addresses belonging to each of the ISR-WAAS groups used in the policy.
- Interception—A set of WAN interfaces on which Cisco WAAS interception is enabled.

Step 5 Click **Apply**.

Step 6 Click **OK**.

The Cisco AppNav is deployed on multiple devices.

Note When a template is deployed to one or more devices, a job is created. To verify the status of the template deployment, choose **Administration** > **Jobs Dashboard**. After you create a template, it can be edited multiple times depending on the requirements. To view detailed status information about failures, success, or warnings, choose **Job Dashboard** > **More Details on Dashboard** > **Status of the job**. To view the details of the job status, select the icon in the status field.

Configuring Cisco AppNav Automatically During ISR-WAAS Container Activation

This method of configuring Cisco AppNav is available only on Cisco 4451-X ISR devices or platform. Also, the software version required for ISR-WAAS activation must be Version 3.10 or later. In this method, the configuration occurs automatically as part of the installation of the Cisco WAAS virtual appliance node, ISR4451X-WAAS.

- A single service node group contains the new ISR-WAAS is created.
- Class maps are created for different types of traffic optimized by the Cisco WAAS service node.
- A default policy map, that redirects all TCP traffic to the Cisco WAAS service node, is generated.
- A Cisco WAAS cluster is created.
- Cisco WAAS is enabled on interfaces denoted by an interface role (specified at the time of container activation).

For more information on how to configure Cisco AppNav using this method, see the Installing an ISR-WAAS Container, page 20-5.

CHAPTER 20

Configuring the Cisco WAAS Container

The Cisco Wide Area Application Services (Cisco WAAS) container is a powerful WAN optimization acceleration solution.

Note In this chapter, ISR-WAAS device refers to the router and ISR-WAAS container refers to the container.

Prerequisites for Installing an ISR-WAAS Container

Before you install a Cisco WAAS container, you must configure the following in Prime Infrastructure:

- Cisco WAAS Central Manager Integration, page 20-1
- Interface Roles, page 19-5
- Importing an OVA image, page 20-4

Note Ensure that the name of the ISR-WAAS container does not exceed 22 characters.

Cisco WAAS Central Manager Integration

To manage thee ISR-WAAS with the Cisco WAAS Central Manager, you must register with the Cisco WAAS Central Manager. Registration of ISR-WAAS with Cisco WAAS Central Manager can be done either from the ISR-WAAS CLI, or from the Cisco WAAS Central Manager GUI, or while activating the ISR-WAAS through Prime Infrastructure. The WCM periodically polls the Cisco 4451-X Integrated Services Router (ISR) to retrieve the current status information and perform configuration synchronization.

Cisco WAAS Central Manager Integration

A typical Cisco WAAS deployment consists of both Prime Infrastructure and Cisco WAAS Central Manager applications. Cisco WAAS Central Manager IP is used during ISR-WAAS activation. After ISR-WAAS is activated, it registers with Cisco WAAS Central Manager. Prime Infrastructure needs the IP address of WCM for the following reasons:

- To inform Cisco WAAS Central Manager of the new Cisco ISR-WAAS
- For cross-launching Cisco WAAS Central Manager GUI for monitoring purposes

Note Cisco WAAS Central Manager configuration is a one-time configuration. The Cisco WAAS Central Manager IP address is required for Prime Infrastructure to authenticate itself to Cisco WAAS Central Manager, and is configured in Prime Infrastructure using the Settings menu.

Note If Cisco WAAS Central Manager IP is not configured in Prime Infrastructure, the newly activated ISR-WAAS will not be registered with Cisco WAAS Central Manager.

To configure the Cisco WAAS Central Manager IP address in Prime Infrastructure:

Step 1 Choose **Administration** > **System Settings**.

Step 2 Click **Service Container Management**.

Step 3 Enter the IP address in the **WCM IP Address** text box.

Step 4 Click **Save**.

WCM can be deployed under the following condition:

Prime Infrastructure works only with the active Cisco WAAS Central Manager that is configured in Prime Infrastructure.

After a Cisco WAAS Central Manager failover, one of the following must take place for Prime Infrastructure-Cisco WAAS Central Manager interworking to operate properly again:

- Prime Infrastructure is reconfigured with the IP address of the new Cisco WAAS Central Manager.
- The failed Cisco WAAS Central Manager must become active.

Configuring Single Sign-On

Configuring the Single Sign-On (SSO) feature provides a seamless method to launch Cisco WAAS Central Manager from Network Control System using the existing Prime Infrastructure 2.0 Single Sign-On functionality.

To configure SSO:

Step 1 Choose **Administration** > **User, Roles, AAA** > **SSO Servers**.

Step 2 Select **Add SSO Server** from the drop-down list on the right side of the pane.

Step 3 Enter the Prime Infrastructure IP address and click **GO**.

Step 4 Click **Save**.

Step 5 Select **AAA Mode Settings**.

Step 6 Select the **SSO** radio button.

Step 7 Select the **Enable fallback to local** check box.

Step 8 Click **Save**.

Step 9 Configure the WCM IP address. For information on how to configure the WCM IP address, see the Cisco WAAS Central Manager Integration, page 20-1.

Step 10 After you configure the IP address, log out of Prime Infrastructure and log in to WCM and create a username.

Creating a Username in Cisco WAAS Central Manager

Step 1 Log in to WCM.

Step 2 Choose **Home** > **Admin** > **AAA** > **Users**.

Step 3 Click **Create**.

Step 4 Enter a username that matches the Prime Infrastructure username.

Step 5 Choose **Role Management** and click **admin** to assign a RBAC role to create a user account.

Step 6 Choose **Domain Management** and assign a role and domain.

Step 7 Click **Submit**.

Step 8 Choose **Devices** > **Configure** > **AAA** > **NCS Single Sign-On**.

Step 9 Check the **Enable NCS Single Sign-On** check box and enter the CAS/SSO server URL.

Step 10 Click **Submit** to create the certificate.

Step 11 Click **Submit** after the certificate is created.

Cross-Launching Cisco WAAS Central Manager

You can cross-launch Cisco WAAS Central Manager in the following ways:

- Cross-Launching Cisco WAAS Central Manager on a Single Device, page 20-3
- Cross-Launching Cisco WAAS Central Manager on Multiple Devices, page 20-4

Cross-Launching Cisco WAAS Central Manager on a Single Device

To cross-launch the Cisco WAAS Central Manager from the Device Work Center:

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

Step 2 Select the ISR-WAAS device.

The device details are displayed in the pane below.

Step 3 Click the **Service Container** tab.

Step 4 Select the corresponding ISR-WAAS container and click **Launch WCM**.

Cross-Launching Cisco WAAS Central Manager on Multiple Devices

To cross-launch from the Deployed Services:

Step 1 Choose **Operate** > **Deployed Services**.

Step 2 Select the corresponding ISR-WAAS container and click **Launch WCM**.

Note The Cisco ISR-WAAS Container Lifecycle enables a user to install, uninstall, activate, or deactivate the service container.

Defining Interface Roles

You can define interface roles in **Design** > **Shared Policy Objects** > **Interface Role**. For more information on creating interface roles, see the Creating Interface Roles, page 8-20. Policy objects enable users to define logical collections of elements. Policy Objects are reusable, named components that can be used by other objects and policies. The Shared Policy Objects also eliminate the need to define a component each time you define a policy. For more information on Shared Policy Objects, see the Creating Shared Policy Objects, page 8-20.

Importing an OVA image

To import an OVA image for an ISR-WAAS container:

Step 1 Choose **Operate** > **Service Catalogue**.

Step 2 Select an OVA image from one of the following locations:

- URL
- File

Step 3 Click **Submit** to import the image into Prime Infrastructure.

Step 4 Click **Refresh** to view the imported image in the **Service Catalogue** > **ISR-WAAS** folder.

Configuring Cisco AppNav Automatically During ISR-WAAS Container Activation

A Cisco WAAS container can be configured in two different ways depending on whether you want to configure it on a single router (Installing an ISR-WAAS Container on a Single Router, page 20-6) or multiple routers (Installing an ISR-WAAS Container on Multiple Routers, page 20-6).

Installation of the ISR-WAAS container can be done in two ways. You can either install the container and activate it later, or you can install and activate the container at the same instance.

Note Ensure that the name of the ISR-WAAS container does not exceed 22 characters.

Installing an ISR-WAAS Container

To install an ISR-WAAS container:

Step 1 Choose **Operate** > **Service Catalogue** to import an OVA image. For information on how to import an OVA image, see the Defining Interface Roles, page 20-4.

Step 2 After importing, click **Refresh** to view the imported image.

Step 3 Click **Deploy**.

Step 4 In the Network Deploy Wizard page, select the ISR-WAAS device on which you want to configure the container.

Step 5 Choose the **Install** option and select a Resource Profile from the drop-down list.

Step 6 Click **OK** to install the ISR-WAAS container.

Note To successfully install and activate an ISR-WAAS, you need to have enough memory for each resource profile. For ISR-WAAS-750, you need 4194304 KB memory and two CPUs, for ISR-WAAS-1300, you need 6291456 KB memory and four CPUs, and for ISR-WAAS-2500, you need 8388608 KB memory with six CPUs.

Installing and Activating an ISR-WAAS Container

To install and activate a ISR-WAAS container:

Step 1 Choose **Operate** > **Service Catalogue** to import an OVA image. For information on how to import an OVA image, see the Defining Interface Roles, page 20-4.

Step 2 After importing, click **Refresh** to view the imported image

Step 3 Click **Deploy**.

Step 4 In the Network Deploy wizard screen, select the device on which you want to configure the container

Step 5 Choose the **Install and Activate** option.

Step 6 Choose a Resource Profile from the drop-down list.

Step 7 Select the **Redirect Traffic to WAAS-XE with AppNav-XE** check box.

Step 8 Click **OK** to install and activate the ISR-WAAS container.

Note Once the ISR-WAAS is installed and activated, the Cisco AppNav configuration is automatically configured.

Note To successfully install and activate a ISR-WAAS, you should at least have 8 GB RAM in the router for the 750 resource profile.

Installing an ISR-WAAS Container on a Single Router

To install an ISR-WAAS container on a single router:

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

Step 2 From the list that is displayed, choose the router on which you want to install the ISR-WAAS container.

Step 3 Click the **Service Container** tab.

Step 4 Click **Add** and enter the configuration details in each field. For information about the field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 5 Click **OK**.

Installing an ISR-WAAS Container on Multiple Routers

To install an ISR-WAAS container on multiple routers:

Step 1 Choose **Operate** > **Service Catalogue**.

Step 2 Select the ISR-WAAS folder that contains the imported OVA image.

Step 3 Click **Deploy**.

From the list that is displayed, select the routers on which you want to install the ISR-WAAS container.

After you deploy, you can either click **Install** (Installing an ISR-WAAS Container, page 20-5) or **Install and Activate** (Installing and Activating an ISR-WAAS Container, page 20-5)

Step 4 If you choose **Install and Activate**, enter the following details in the Value Assignment area:

- Enter the ISR-WAAS IP Address/Mask
- Enter the Router IP/ Mask
- Enter the Storage Location.
- Enter a Service Container name
- Select a Resource Profile

Step 5 Click **OK**.

Uninstalling and Deactivating a Cisco WAAS Container

You can deactivate a Cisco WAAS Container either from the Device Work Center or from the Deployed Services. From the Device Work Center, you can deactivate a single ISR-WAAS container, but from the Deployed Services, you can deactivate multiple ISR-WAAS containers.

Uninstalling a Single Cisco ISR-WAAS Container

To uninstall a single ISR-WAAS container from the Device Work Center:

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

Step 2 From the list that is displayed, select the router from which you want to uninstall the Cisco WAAS container by clicking it.

Step 3 Click the **Service Container** tab in the bottom pane.

Step 4 Click **Uninstall**.

Step 5 Click **OK**.

Uninstalling a Multiple Cisco ISR-WAAS Container

To uninstall multiple a Cisco ISR-WAAS containers from the Deployed Services:

Step 1 Choose **Operate** > **Deployed Services**.

Step 2 From the list that is displayed, select the routers from which you want to uninstall the Cisco WAAS containers by clicking them.

Step 3 Click **Uninstall**.

Step 4 Click **OK**.

Note When a Cisco WAAS virtual appliance is uninstalled through Prime Infrastructure, the corresponding Cisco AppNav configuration is removed.

Deactivating a Cisco ISR-WAAS Container

You can deactivate a Cisco ISR-WAAS container in the following two ways:

- Deactivating a Single Cisco ISR-WAAS Container, page 20-8
- Deactivating Multiple Cisco ISR-WAAS Containers, page 20-8

Deactivating a Single Cisco ISR-WAAS Container

To deactivate a single Cisco ISR-WAAS container from the Device Work Center:

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

Step 2 Select a Cisco ISR-WAAS device name from the device group list.

Step 3 Click the **Service Container** tab.

Step 4 Click **Deactivate**.

Deactivating Multiple Cisco ISR-WAAS Containers

To deactivate multiple Cisco WAAS containers from the Deployed Services:

Step 1 Choose **Operate** > **Deployed Services**.

Step 2 Select multiple ISR-WAAS device names from the list.

Step 3 Click **Deactivate**.

CHAPTER 21

Troubleshooting

Cisco Prime Infrastructure provides the following for sophisticated monitoring and troubleshooting of end-user network access.

The following sections describe some typical troubleshooting tasks:

Getting Help from Cisco

Prime Infrastructure provides helpful tools for network operators to connect to Cisco experts to diagnose and resolve problems. You can open support cases and track your cases from Prime Infrastructure. If you need help troubleshooting any problems, Prime Infrastructure allows you to:

- Connect with the Cisco Support Community to view and participate in discussion forums. See Launching the Cisco Support Community, page 21-1.
- Open a support case with Cisco Technical Support. See Opening a Support Case, page 21-2.

Launching the Cisco Support Community

You can use Prime Infrastructure to access and participate in discussion forums in the online Cisco Support Community. This forum can help you find information for diagnosing and resolving problems.

Note You must enter your Cisco.com username and password to access and participate in the forums.

To launch the Cisco Support Community:

Step 1 Choose **Operate > Alarms & Events**, click an alarm, then choose **Troubleshoot > Support Forum**.

Step 2 In the Cisco Support Community Forum page, enter additional search parameters to refine the discussions that are displayed.

Opening a Support Case

You can use Prime Infrastructure to open a support request and to track your support cases. Prime Infrastructure helps you gather critical contextual information to be attached to the support case, reducing the time it takes to create a support case.

Note To open a support case or access the Cisco Support Community, you must:

- Have a direct Internet connection on the Prime Infrastructure server
- Enter your Cisco.com username and password

To open a support case:

Step 1 Chose **Operate > Alarms & Events**, then hover your mouse over the IP address of the device on which the alarm occurred.

Step 2 From the device 360° view, click the **Support Request** icon.

Step 3 Enter your Cisco.com username and password.

Step 4 Click **Create**.

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 5 Click **Next** and 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 6 Click **Create Service Request**.

Checking an End User's Network Session Status

When an end user calls the help desk, typically with a complaint that might not be very specific ("I can't log in" or "The network is really slow"), you will want to get an overall view of the user's current network session status, identify which individual session is associated with the problem, and examine the details for that session.

For example, how is the user attached to the network? Does this person have more than one endpoint (where an endpoint could be, for example, a laptop, desktop, iPad, iPhone, or Android)?

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- Integration with LDAP (to display information about the end user).

To check an end user's network session status:

Step 1 In the system search field (see Search Methods, page A-15), enter the name of the user (or client) who is experiencing the issue. If there are multiple matches, select the correct username from the list of matches.

Step 2 Start the User 360° View (see Getting User Details from the User 360° View, page A-13).

The information that is available from this view typically includes current information about the end user and all of that user's current or recently ended network sessions.

Troubleshooting Authentication and Authorization

Using the User 360° View, you can identify possible problems with the end user's authentication and authorization for network access.

For example, there could be authentication problems (such as the user's password being rejected), or there could be authorization issues (such as the user being placed in a policy category such as "guest" or "quarantine" that might result in unexpected behavior).

Before You Begin

This feature requires integration with an ISE server.

To troubleshoot the network

Step 1 Open the User 360° View for that user and check the value in "Authorization Profile". This is a mnemonic string that is customer-defined, so it might not contain clear information (for example, "standard_employee" or "standard_BYOD" or "Guest").

Step 2 If this field is a link, click it to display information about the user's authorization profile. Based on this information:

- If the end user is associated with the appropriate policy category, this procedure is complete.
- If the end user is not associated with the appropriate policy category, you can hand off the problem (for example, to an ISE admin or help tech) or perform actions outside Prime Infrastructure to investigate why the user was placed in the current policy category (Authorization Profile).

Step 3 Check to see whether there are any indications of authentication errors (authentication failure could be due to various things, including an expired password). The visual indication of authentication errors allows you to see more data related to the authentication errors. At that point, you might need to hand off the problem (for example, to an ISE admin or help tech).

Troubleshooting Network Attachments

Use the following procedure to determine if there are problems with the end user attaching to the network, such as errors on the access port (wired) or radio association problems (wireless).

To troubleshoot network attachments:

Step 1 Open the User 360° View for that user and click the **Go to Client Details** icon (see Getting User Details from the User 360° View, page A-13).

Step 2 If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note the problem and hand it off to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose **Operate > Client and Users**).

Troubleshooting Network Attachment Devices

Use the following procedure to troubleshoot any active alarms or error conditions associated with the network attachment device and port for the end user that might be causing problems for the end user's network session:

Step 1 To view any existing active alarms or error conditions associated with the network attachment device and port for the end user (available for the controller, switch, access point, and site), open the User 360° View for that user and click the **Alarms** tab.

Step 2 To see if a problem has been detected, click the **Go to Client Details** icon (see Getting User Details from the User 360° View, page A-13).

Step 3 If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note that fact and hand off the task to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose **Operate > Client and Users**).

Troubleshooting Site Network Devices

Use the following procedure to determine if there are any existing active alarms or error conditions associated with any of the network devices that are part of the site for the end user that could be causing problems for the user's network session.

Step 1 To view any existing active alarms or error conditions associated with network devices that are part of the site for the end user, open the User 360° View for that user and click the **Alarms** tab.

Step 2 You can choose to view:

- Active alarms list for the site
- List of all site devices (with alarm indications)
- Topo map of site (with alarm indications)

Step 3 If a problem with a site has been detected, an alarm icon will appear next to the site location. Click the icon to view all of the alarms associated with that site.

Step 4 If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note that fact and hand off the task to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose **Operate > Client and Users**).

Troubleshooting Applications

Use the following procedure to determine if there are any problem indications associated with any of the specific applications being run across the network by the end user.

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- That session information (netflow/NAM data, Assurance licenses) is available.

Step 1 To view the applications accessed by the end user and the response time for the applications for the user's devices, open the User 360° View for that user and click the **Applications** tab.

Step 2 This tab displays the following information:

- Endpoint
- Mac address
- Application
- Last one hour volume (in MB)

To get more information about an application, choose **Operate > Monitoring Dashboards > Detail Dashboards**.

Troubleshooting the User Application and Site Bandwidth Utilization

If an end user is experiencing high bandwidth utilization for a site on the interface dashboard, use the following procedure to identify the applications consumed by the user and the bandwidth consumed by every application for a given endpoint owned by the user.

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- For wired sessions, that AAA accounting information is being sent to ISE.
- That session information (netflow/NAM data, Assurance licenses) is available.

Step 1 To view the applications accessed by the end user and the response time for the applications for the user's devices, open the User 360° View for that user and click the **Applications** tab.

Step 2 The Applications tab displays information about the applications accessed by the end user (see Troubleshooting Applications, page 21-5). To get more information about an application, including the bandwidth utilization of the application consumed by the end user (the bandwidth consumed for the conversation), choose **Operate > Monitoring Dashboards > Detail Dashboards**.

Troubleshooting User Problems

You can use the User 360° View to troubleshoot problems reported by users.

Step 1 In the Search field on any page, enter the end user's name.

Step 2 In the Search Results window, hover your mouse over the end user's name in the User Name column, then click the User 360° view icon that appears as shown in Figure A-12.

Step 3 With the User 360° view displayed, identify where the problem is occurring using the information described in Table 21-1.

Table 21-1 Using the User 360° View to Diagnose User Problems

To Gather This Data	Click Here in User 360° View	Additional Information
Information about the device to which the user is attached, such as the endpoint, location, connections, and session information	Click a device icon at the top of the User 360° View.	Click available links to display additional information. For example, you can click the Authorization Profile link to launch ISE. See Troubleshooting Authentication and Authorization, page 21-3
Alarms associated with the device to which the user is attached	Click a device icon at the top of the User 360° View, then click the **Alarms** tab.	Click the Troubleshoot Client icon to go to client troubleshooting. See "Client Troubleshooting" in the *Cisco Prime Infrastructure Classic View Configuration Guide for Wireless Devices, Release 2.0*.
Applications running on the device to which the user is attached	Click a device icon at the top of the User 360° View, then click the **Applications** tab.	Click an application to view the end-user data filtered for the user you specified. See Troubleshooting Applications, page 21-5.

Troubleshooting the User's Experience

If an end user reports a problem with accessing the application, use the User 360° View to troubleshoot the user's experience.

Before You Begin

This feature requires that session information (netflow/NAM data, Assurance licenses) is available.

Step 1 To view the applications accessed by the end user and the response time for the applications for the user's devices, open the User 360° View for that user and click the **Applications** tab.

Step 2 The Applications tab displays information about the applications accessed by the end user (see Troubleshooting Applications, page 21-5). To get more information about an application, choose **Operate > Monitoring Dashboards > Detail Dashboards**.

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.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

Prime Infrastructure with the licensed Assurance features makes this kind of troubleshooting easy. The following workflow is based on a typical scenario: The user complains to the network operations desk about poor voice quality or choppy video replay at the user's branch office. The operator first confirms that the user is indeed having a problem with jitter and packet loss that will affect the user's RTP application performance. The user 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 Choose **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 View **RTP Conversations Details** to see the Jitter and Packet Loss statistics for the client experiencing the problem.

Step 4 View 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 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.

Troubleshooting Unjoined Access Points

When a lightweight access point initially 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 of the configuration details for the device and network. Until the access point successfully joins a wireless controller, it cannot be managed by Prime Infrastructure, and it 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.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

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 on the page. This information 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:

Step 1 Choose **Operate > Wireless > Unjoined APs**.

Step 2 In the Unjoined APs page, select an access point to diagnose, then click **Troubleshoot**.

Step 3 After the troubleshooting analysis runs, check the results in the Unjoined APs page.

If the access point has tried to join multiple wireless controllers but has been unsuccessful, the controllers are listed in the left pane.

Step 4 Select a controller and check the middle pane for:

- A statement of the problem
- A list of error messages
- Controller log information

Step 5 Check the right pane for recommendations for solving any problems, and perform any recommended actions.

Step 6 (Optional) To further diagnose the problem, run RTTS through the Unjoined AP page by clicking the RTTS icon located to the right of the table. Examine the debug messages that appear in the table to determine a cause for the access point being unable to join the controllers.

RTTS Debug commands for Troubleshooting Unjoined Access Points

Table 21-2 contains the list of RTTS debug commands for Legacy controllers and NGWC controllers.

Table 21-2 RTTS Debug commands for Legacy controllers and NGWC controllers

Controller	Commands
Legacy	• debug capwap info enable • debug dot1x all enable • debug mobility directory enable
NGWC	• debug capwap ap error • debug dot1x events • debug capwap ios detail

Troubleshooting RTP and TCP Flows Using Mediatrace

The Mediatrace troubleshooting tool generates a table that lists the currently active RTP streams or TCP sessions. Using these Mediatrace tables and their associated options, you can:

- Identify and select RTP or TCP flows with problems (see Using the Mediatrace Tables, page 21-10).
- Troubleshoot problems with RTP or TCP flows (see Running Mediatrace from Selected RTP or TCP Flows, page 21-11).
- Troubleshoot problems with RTP or TCP flows between any two arbitrary endpoints (see Launching an Ad Hoc Mediatrace From Endpoints, page 21-12).
- Troubleshoot problems with RTP flows starting from the RTP Conversations dashlet (see Troubleshooting Worst RTP Endpoints Using Dashlets, page 21-14).
- Identify and compare flow performance indicators and data sources (see Comparing Flow Data From Multiple Sources, page 21-15).

To configure data collection for Mediatrace, see Managing Metrics in the *Cisco Prime Infrastructure 2.0 Administrator Guide*.

Using the Mediatrace 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, the flows between the two application endpoints are aggregated into a single row with a triangle icon.

By default, Prime Infrastructure automatically refreshes the RTP Streams table data every 60 seconds; you can also use one of the preset filters.

Prime Infrastructure refreshes TCP Sessions data once every 300 seconds (5 minutes); you can use the **Filter by Application** filtering option to include or exclude applications from the list.

You can also click either table’s **Refresh** button at any time. You can turn off automatic refresh by unchecking the **Enable auto refresh** check box.

To use the Mediatrace tables:

Step 1 Choose **Operate > Operational Tools > Mediatrace**.

Step 2 From the **Application** drop-down list, choose **RTP** or **TCP**. The page shows the corresponding table: RTP Streams or TCP Sessions.

Step 3 Find the flow that you want to troubleshoot:

- To review all flows with a particular type of issue, click 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 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 might report the 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, 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 Running Mediatrace from Selected RTP or TCP Flows, page 21-11.

Running Mediatrace from Selected RTP or TCP Flows

To troubleshoot RTP or TCP flows using Mediatrace:

Step 1 Choose **Operate > Operational Tools > Mediatrace**. In the **Application** drop-down list, choose **RTP** or **TCP**, then find the flow that you want by using the steps in Using the Mediatrace Tables, page 21-10.

Step 2 Select the flow and click **Trace Service Path**. Prime Infrastructure displays the RTP or TCP Stream Details page for the selected flow, with all of the routers in the flow's path in the Troubleshooting Status table, in the 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 the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

Note The **Start Mediatrace** link is present when the device is Mediatrace-capable; the **Start Traceroute** link is present when the device is not Mediatrace-capable.

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 where 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 of the devices between the flow's two endpoints. Device icons in the map consist of:

- Alarm Severity—The most severe alarm currently recorded for the device.
- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign on red background—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 Troubleshooting RTP and TCP Flows Using Mediatrace, page 21-10.
- Minus sign—The device is unmanaged.

Step 5 To see key performance metrics, such as CPU and memory utilization, jitter, and packet loss, for all Medianet-capable devices in the RTP or TCP flow's path, click the **Medianet Path View** tab. To see the performance metrics in numerical and graphic form, click the subtabs in the Medianet Path View pane.

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.

Launching an Ad Hoc Mediatrace From Endpoints

You can quickly launch a Mediatrace 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 trace from the appropriate RTP or TCP Mediatrace table.

To launch an ad hoc Mediatrace from two endpoints:

Step 1 Choose **Operate > Operational Tools > Mediatrace**. From the **Application** drop-down list, choose **RTP** or **TCP**.

Step 2 Click **Specify Session for Mediatrace**.

Step 3 Enter the required information:

- 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 that you have:

- 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 of the routers in the flow's path in the Troubleshooting Status table, in the 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 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 where 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—The most severe alarm currently recorded for the device.
- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign on red background—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.
- Minus sign—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 Mediatrace 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 Mediatrace on such an inactive flow, you will receive an error message advising you of this fact.

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards > End User Experience**.

Step 2 In the **Worst N RTP End Point Pairs** dashlet (if this dashlet is not already in the dashboard, see Adding Dashlets, page A-4), note the Source Address for your worst performing RTP flows.

Step 3 In the **RTP Conversations** dashlet in the same page, find the most recent conversation for the same Source Address.

Step 4 Select that conversation in the RTP Conversations dashlet, then choose **Troubleshoot > Trace Service** path. Prime Infrastructure displays the RTP Stream Details page for the selected flow, with all of 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 the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

Note The **Start Mediatrace** link is present when the device is Mediatrace-capable; the **Start Traceroute** link is present when the device is not Mediatrace-capable.

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 where 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 the all of the devices between the flow's two endpoints. Device icons in the map will be badged as follows:

- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign—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. To see the performance metrics in numerical and graphic form, click the subtabs in the Medianet Path View panel.

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 Mediatrace performance data, you might 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 compare flow data from multiple sources:

Step 1 Choose **Operate > Operational Tools > Mediatrace**.

Step 2 From the **Application** drop-down list, choose **RTP** or **TCP**, then find the flow you want using the steps in Using the Mediatrace Tables, page 21-10.

Step 3 Expand a row (for an RTP or TCP flow) to view the details of the key performance indicators appropriate for the selected flow and the data source for each such set of indicators.

Step 4 When you are finished, click **OK**.

CHAPTER 22

Managing Reports

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 or a scheduled basis. Each report type has a number of user-defined criteria to aid in defining the reports. The reports can be formatted as a summary, tabular, or combined (tabular and graphical) layout. After they have been defined, the reports can be saved for future diagnostic use or scheduled to run 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.

Reports include:

- Current—Provides a snapshot of data that is not time-dependent.
- Historical—Retrieves data from the device periodically and stores it in the Prime Infrastructure database.
- Trend—Generates a report using aggregated data. Data can be periodically collected from devices 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. It includes:

- Report Launch Pad—The hub for all Prime Infrastructure reports. From this page, you can access specific types of reports and create new reports (see Managing Reports, page 22-2).
- Scheduled Run Results—Allows you to access and manage all currently scheduled runs in Prime Infrastructure, and to access and manage on-demand exports as well as emailed reports (see Managing Scheduled Run Results, page 22-3).
- Saved Report Templates—Allows you to access and manage all currently saved report templates in Prime Infrastructure (see Managing Saved Report Templates, page 22-4).

For information about the report field descriptions, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

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 later, and customize the results of a report.

Tip To see more report details, rest your cursor over the tool tip next to the report type.

Creating, Scheduling, and Running a New Report

To create, schedule, and run a new report:

Step 1 Choose **Report > Report Launch Pad**.

Step 2 Choose a category from the left sidebar menu to see the report types for each report category, check the check box for the appropriate report in the main area of the Report Launch Pad, then click **New**.

Step 3 In the Report Details page, complete the fields as described in the **Report Launch Pad > Report Type > New** section in the *Cisco Prime Infrastructure 2.0 Reference Guide*. 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 22-3.

Step 4 If you plan to run this report later or as a recurring report, enter Schedule parameters as described in the **Report Launch Pad > Report Type > New** section in the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 5 To run the report, choose one of the following options:

- 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 date 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 generated reports for all subdomains at the same time. You can open and change the reports individually through their respective subdomains. To update all reports, delete the reports created on subdomains and regenerate virtual domain reports 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 template makes those parameters part of your Prime Infrastructure monitoring setup. However, this does not mean that the collected FNF extension monitoring data will automatically appear in the corresponding Conversations reports for Core, Application Response Time (ART), and RTP performance. To ensure that FNF data is included in Conversations reports, you must add the FNF parameters to the “Data fields to include” column using the Create Custom Report page (see **Report Launch Pad > Report Type > New > Customize** section in *Cisco Prime Infrastructure 2.0 Reference Guide*).

To customize report results:

Step 1 Choose **Report > Report Launch Pad**.

Step 2 Click the Report Title link for the appropriate report.

Step 3 In the Report Details page, click **Customize**.

Step 4 On the Create Custom Report page, complete the required information, then click **Apply** to confirm the changes.

Note The changes made in the Create Custom Report page are not saved until you click **Save** in the Report Details page.

Managing Scheduled Run Results

To view all 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 in the Scheduled Run Results page of the respective domains.

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 the Scheduled Run Results section in the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Managing Saved Report Templates

Saved report templates are available at Report > Saved Report Templates. From the Saved Report Templates page, you can create report templates and manage saved report templates. You can also enable, disable, delete, or run saved reports, and you can filter and sort report templates by category, type, and status. For information about the fields on the Saved Report Templates page, and about filtering saved report templates, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

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.
- Virtual Domain—Identifies the name of the virtual domain under which this report is scheduled.
- Run Now—Click the **Run** icon to immediately run the current report.

  Note When you run any domain based report for a sub virtual domain, the report displays all of the device attributes that are mapped to the virtual domain where you are currently logged-in.

Prime Infrastructure Reports

Autonomous AP Reports

The following table describes the various Autonomous AP reports that you can generate in Prime Infrastructure.

Table 22-1 Autonomous AP Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Autonomous AP Memory and CPU Utilization	This report displays the memory and CPU utilization trends of autonomous access points based on the filtering criteria specified during report generation. It could help in identifying unexpected behavior or issues with network performance.	No	No	Graphical	No
Autonomous AP Summary	This report displays the Autonomous AP summary.	Yes	No	Tabular	No

Table 22-1 Autonomous AP Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Autonomous AP Tx Power and Channel	This report displays the channel plan assignment and transmits power level trends of devices based on the filtering criteria used when the report was generated. It can help identify unexpected behavior or issues with network performance.	No	Yes	Graphical	No
Autonomous AP Uptime	This report displays the Autonomous AP uptime.	Yes	No	Tabular	No
Autonomous AP Utilization	This report displays the utilization trends of Autonomous AP radios based on the filtering criteria used when the report was generated. It can help identify current network performance and capacity planning for future scalability needs.	No	No	Graphical	No
Busiest Autonomous APs	This report displays the Autonomous APs with the highest total usage (the sum of transmitting, receiving, and channel usage) on your wireless network.	Yes	No	Tabular	No

CleanAir Reports

The following table describes the various CleanAir reports that you can generate in Prime Infrastructure.

Table 22-2 CleanAir Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Air Quality vs Time	This report displays the air quality index distributions over a period of time for access points on your wireless networks.	Yes	No	Tabular	No
Security Risk Interferers	This report displays the security risk interferers on your wireless network.	Yes	No	Tabular	No
Worst Air Quality APs	This report displays the access points with the lowest air quality index.	Yes	No	Tabular	No
Worst Interferers	This report displays the worst interferers on your wireless network.	Yes	No	Tabular	No

Client Reports

Note When you create a virtual domain, the statistics collection for the virtual domain starts after its creation. Therefore, you do not get the hourly statistics for the previous hours (prior to the creation of the virtual domain) as you get the statistics for the ROOT-DOMAIN.

The following table describes the various Client reports that you can generate in Prime Infrastructure.

Table 22-3 Client Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Busiest Clients	This report displays the busiest and least busy clients on the wireless network by throughput, utilization, and other statistics. You can sort this report by location, by band, or by other parameters. **Note** Busiest Clients reports do *not* include autonomous clients.	Yes	No	Tabular	No
CCX Client Statistics	This report displays the 802.11 and security statistics for Cisco Compatible Extensions v5 clients or Cisco Compatible Extensions v6 clients depending upon the options you choose to run the report. **Note** The CCX Client Statistics report does not contain client information from Cisco 5700 Series Wireless Controller and Cisco Catalyst 3850 Series Switches.	No	No	Tabular	No

Table 22-3 Client Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Client Count	This trending report displays the total number of active clients on your wireless network. The Client Count report displays data on the numbers of clients that connected to the network through a specific device, in a specific geographical area, or through a specific or multiple SSIDs. **Note** Client Count reports include clients connected to autonomous Cisco IOS access points. **Note** When you run the client count report for two different virtual subdomains under the root domain, the data reported might be the same even if the controllers assigned to the two virtual subdomains are different. This is because the report returns data for all of the controllers in the system. If you want to get a separate report for a virtual domain, run the report as a particular virtual domain user other than a root domain user.	No	No	Graphical	No
Client Session	This report provides client sessions for a given period of time. It displays the history of client sessions, statistics, and the duration for which clients are connected to an access point at any given period of time.	Yes	No	Tabular	No

Table 22-3 Client Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Client Summary	The Client Summary is a detailed report that displays various client statistics. When Prime Infrastructure does not receive client traps, it relies on client status polling to discover client associations (the task runs every 5 minutes by default). However, Prime Infrastructure cannot accurately determine when the client was actually associated. Prime Infrastructure assumes the association started at the polling time, which might be later than the actual association time. Therefore, the calculation of the average client throughput can give inaccurate results, especially for short client sessions. **Note** Prime Infrastructure counts only authenticated sessions. If a user fails on DHCP or authentication, Prime Infrastructure might not have a session for it. Also, Prime Infrastructure considers every detected AP association as a session. For instance, if a client roams from one access point to another, Prime Infrastructure can have two association sessions.	Yes	Yes	Various	Yes
Client Traffic	This report displays the traffic by the wireless clients on your network.	No	No	Graphical	No
Client Traffic Stream Metrics	This report displays Traffic Stream Metrics for clients. You can select from the following: • All clients of a given set of SSIDs • All clients • One specific client **Note** The traffic stream metrics and radio performance background tasks must be running prior to generating this report.	Yes	No	Tabular[1]	No
Dormant Clients	This report displays the details of the clients that are disassociated for a specified duration.	No	No	Tabular	No
Mobility Client Summary	This trending report displays the total number of active clients in your wireless network.	No	No	Graphical	No
Posture Status Count	This trending report displays the failed or succeeded client posture status count on your network.	No	No	Graphical	No

Table 22-3 Client Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Throughput	This report displays the ongoing bandwidth used by the wireless clients on your network. **Note** The Throughput report does not include wired clients or clients connected to autonomous Cisco IOS access points.	No	No	Tabular	No
Unique Client Summary	This is a detailed report that displays the summary of all unique client statistics. The report can be filtered by client user, traffic, protocol, and vendor.	Yes	Yes	Tabular	No
Unique Clients	This report displays all unique clients by the time, protocol, and controller filters that you select. A unique client is determined by the MAC address of the client device. These clients are sorted by controller in this report. **Note** The Unique Client report covers any client that started or ended a connection during the time period that you specified when you scheduled the report.	Yes	No	Tabular	No

1. The Subreport Client Summary view is tabular only. Other subreports, such as Client Summary by Protocol, support tabular, and graphical report views are customizable to show either or both.

Compliance Reports

The Configuration Audit report displays the differences between Prime Infrastructure and its controllers. The PCI DSS Compliance report summarizes your Wireless LAN Security components with reference to the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. PCI DSS compliance is required for all merchants and service providers that store, process, or transmit cardholder data. You can find PCI DSS standards at the PCI Security Standards Council website.

The following table describes the various Compliance reports that you can generate in Prime Infrastructure.

Table 22-4 Compliance Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Change Audit Report	This report displays the change audit data such as the inventory and configuration changes of a device.	No	No	Tabular	No

Table 22-4 Compliance Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Network Discrepancy	This report displays discrepancies such as inconsistencies, anomalies, or misconfigurations in your network. **Note** The network discrepancies are computed using database queries. So, if there is any increase in the device count, the performance of this report is impacted. Always use scheduled option to run this report.	Yes	No	Tabular	No
PCI DSS Detailed	This report displays, in detail, the PCI Data Security Standard (DSS) Version 2.0 requirements that are relevant to your wireless network security.	Yes	No	Tabular	No
PCI DSS Summary	This report displays the summarized PCI DSS Version 2.0 requirements that are relevant to your wireless network security.	No	No	Graphical	No
Wireless Configuration Audit	This report displays the configuration differences between Prime Infrastructure and its controllers. You must configure audit mode in the Administration > Settings page. In audit mode, you can perform an audit based on templates or the stored configuration. The report shows the last time an audit was performed using the Configuration Sync background task.	Yes	No	Tabular	No
PSIRT Detailed[1]	This report is generated for devices in the network to check the Cisco Security Advisory Compliance against the customer network.	No	No	Tabular	No
PSIRT Summary[1]	This reports displays a summary of Software versions in the network affected by the posted Cisco Product Security Notices.	No	No	Tabular	No

[1] You must enable the compliance service, restart the server, and synchronize inventory to view and generate the PSIRT reports. For more information about enabling the compliance service, see the *Configuring Server Settings* section in the *Cisco Prime Infrastructure 2.0 Administrator Guide*.

Device Reports

The following table describes the various device reports that you can generate in Prime Infrastructure.

Table 22-5 Device Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
AP Ethernet Port Utilization	This report displays the Tx and Rx utilization of AP Ethernet ports.	No	No	Tabular	No
AP Image Pre-download	This report displays scheduled download software task status.	Yes	Yes	Tabular	Yes
AP Profile Status	This report displays access point load, noise, interference, and coverage profile status.	Yes	No	Tabular	No
AP Radio Downtime Summary	This report shows the time since the radio was down for all of the APs that are managed by Prime Infrastructure.	No	No	Tabular	No
AP Summary	This report displays a list of access points that are broadcasting SSID(s). This report allows you to filter devices by RF group name, mobility group name, access point group name, SSID, location, and other statistics. **Note** This report, by default, displays a list of access points that are broadcasting one or more SSIDs; the All SSIDs filter is chosen by default. Access points that are not broadcasting an SSID are not displayed. **Note** The AP Summary report does not include Autonomous access points. For Autonomous access points, you need to run an Autonomous AP Summary report.	Yes	Yes	Tabular	Yes
Busiest APs	This report displays the access points with the highest total usage (transmitting, receiving, and channel utilization) on your wireless network.	Yes	No	Tabular	No
CPU Utilization	This report displays CPU utilization switch usage on your network.	No	No	Graphical	No
Classmap QOS Statistics	This report displays the Quality of Service (QoS) statistics for the classmap in your network.	Yes	No	Tabular	Yes
Detailed Hardware	This report displays detailed information about the hardware in your network.	No	Yes	Tabular	Yes
Detailed Software	This report displays detailed information about the software in your network.	No	Yes	Tabular	Yes
Device Credential Verification	This report displays the credential status of the devices in your network.	Yes	No	Tabular	Yes
Device Health	This report displays composite details of device health in your network.	Yes	Yes	Tabular	Yes

Table 22-5 Device Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Dmvpn Reports	This report displays Dmvpn data for the devices in your network.	Yes	No	Tabular	Yes
GET VPN Network Status	This report displays the VPN status of the devices in your network.	Yes	No	Tabular	Yes
Identity Capability	This report displays the identity capability summary for the switches in your network.	No	No	Various	No
Interface Availability	This report displays the interfaces with highest or lowest availability of devices in your network. **Note** You must create and deploy an Interface Health template to see this report. See Setting Up WAN Interface Monitoring, page 5-2 for more information.	Yes	Yes	Tabular	Yes
Interface Capacity	This report displays the percentage of interface utilization by the devices in your network.	No	No	Tabular	No
Interface Utilization	This report displays the interfaces with highest or lowest Rx/Tx utilization by the devices in your network.	Yes	Yes	Tabular	Yes
Inventory	This report allows you to generate inventory-related information for controllers, access points, and MSEs managed by Prime Infrastructure. This information includes hardware type and distribution, software distribution, CDP information, and other statistics. **Note** Disassociated access points with values of null or " (double quote) for model and serial number are filtered out of AP Inventory reports.	Yes	Yes	Various[1]	Yes
Memory Utilization	This report displays the memory utilization summary for the switches in your network.	No	No	Graphical	No
Non-Primary Controller APs	This report displays the access points that are not connected to the configured primary controller.	Yes	No	Tabular	Yes
Top AP by Client Count	This report displays associated and authenticated client count over selected duration for access points in your wireless network. This report is sorted by associated client count in ascending order.	Yes	No	Tabular	Yes
VLAN	This report displays the VLAN information for switches in your network.	Yes	No	Tabular	Yes
Wired Detailed Device Inventory	This report displays inventory information about the wired devices in your network.	Yes	Yes	Tabular	No

Table 22-5 ***Device Reports (continued)***

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Wired Device Availability	This report displays the wired devices with the highest availability in your network.	Yes	Yes	Tabular	Yes
Wired Module Detail	This report displays the detailed module information for wired devices in your network.	Yes	No	Tabular	Yes
Wired Port Attribute	This report displays port attribute information such as admin status, operational status, MAC address, and so on.	Yes	No	Tabular	Yes
Wired Up Time	This report displays the access point uptime, the LWAPP uptime, and the LWAPP join time.	Yes	No	Tabular	No
Wired Utilization	This report displays the controller, AP, and MSE usage on your wireless network. These statistics (such as CPU usage, memory usage, link utilization, and radio utilization) can help identify current network performance and help with capacity planning for future scalability needs.	No	No	Graphical	No
EOX Hardware Detailed[2]	This report displays the End of Life/Support announcement dates for devices in the network.	No	No	Tabular	No
EOX Module Detailed[2]	This report gives the End of Life/Support announcement dates for each module in the network.	No	No	Tabular	No
EOX Software Detailed[2]	This report displays the End of Life/Support announcement dates for device software versions in the network.	No	No	Tabular	No
EOX Summary Report[2]	This report displays a summary of the hardware, software, and module types that have End of Life/Support announcement dates and the number of such devices in the network.	No	Yes	Tabular	No
License by Device Type	This report displays the license information of the features configured on the devices in your network.	Yes	No	Tabular	Yes
License by License Type	This report displays the license count for each license type.	Yes	No	Tabular	Yes

[1] The Combined inventory report now contains APs, Controllers, MSEs, Autonomous APs, and Switches. Reports that are filtered by model or version support both tabular and graphical views. These views are customizable with setting such as Count of Controllers by Model. Other reports, such as Controller Inventory, are tabular only.

[2] You must enable the compliance service, restart the server, and synchronize inventory to view and generate the EOX reports. For more information about enabling the compliance service, see the *Configuring Server Settings* section in the *Cisco Prime Infrastructure 2.0 Administrator Guide*.

Guest Reports

The following table describes the various Guest reports that you can generate in Prime Infrastructure.

Table 22-6 Guest Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Guest Accounts Status	This report displays guest account status changes in chronological order. The report filters guest accounts by the guest user who created them. One example of a status change is Scheduled to Active to Expired.	Yes	No	Tabular	No
Guest Association	This report displays the day and time that a guest client associated to and disassociated from a guest profile or SSID over a customizable period of time.	Yes	No	Tabular	No
Guest Count	This report displays the number of guest clients logged into the network per guest profile or SSID over a customizable period of time.	No	No	Tabular	No
Guest User Sessions	This report displays historical session data for a guest user. Data such as amount of data passed, login and logout times, guest IP address, and guest MAC address is available for one month by default. The data retention period can be configured from the Administration > Background Tasks page. This report can be generated for guest users who are associated to controllers running software Version 5.2 or later.	Yes	No	Tabular	No
NCS Guest Operations	This report displays all activities performed by one or all guests, such as creating, deleting, or updating guest user accounts. If a guest user is deleted from Prime Infrastructure, the report still shows an activity performed by the deleted guest user for up to one week after the activity occurred.	Yes	No	Tabular	No

MSE Analytics Reports

The following table describes the various Mobility Services Engine (MSE) Analytics reports that you can generate in Prime Infrastructure.

Table 22-7 MSE Analytics Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Client Location	This report displays location history of a wireless client detected by an MSE.	Yes	No	Tabular	No

Table 22-7 MSE Analytics Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Client Location Density	This report displays a list of wireless clients and their locations detected by MSEs. If multiple MSEs are selected, this list is grouped by MSE in the selected sorting order.	Yes	No	Tabular	Yes
Guest Location Density	This report displays guest clients and their locations detected by the MSEs, based on your filtering criteria.	Yes	No	Tabular	No
Location Notifications by Zone	This report displays the location notifications generated by MSEs.	Yes	No	Tabular	No
Mobile MAC Statistics	Click **Mobile MAC Statistics** from the Report Launch Pad to open the Mobile MAC Statistics Reports page.	No	Yes	Tabular	No
Rogue AP Location Density	This report displays rogue access points and their locations detected by the MSEs, based on your filtering criteria.	Yes	No	Tabular	No
Rogue Client Location Density	This report displays rogue client access points and their locations detected by the MSEs, based on your filtering criteria.	Yes	No	Tabular	No
Service URI Statistics	Click **Service URI Statistics** from the Report Launch Pad to open the Service URI Statistics Reports page.	No	Yes	Tabular	No
Tag Location	This report displays location history of a tag detected by the MSEs, based on your filtering criteria.	Yes	No	Tabular	No
Tag Location Density	This report displays tags and their locations detected by the MSEs, based on your filtering criteria.	Yes	No	Tabular	No
Device Count by Zone	This report provides the number of devices detected by an MSE in the selected zone.	Yes	No	Tabular	Yes
Device Dwell Time by Zone	This report provides the dwell time for a device detected by an MSE.	Yes	No	Tabular	Yes

Mesh Reports

The following table describes the various Mesh reports that you can generate in Prime Infrastructure.

Table 22-8 Mesh Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Alternate Parent	This report displays the number of alternate parents with the same configured mesh group for each mesh access point. This report can be used to determine an access point's capability to handle failures in the mesh path.	Yes	No	Tabular	No
Link Stats	This report displays mesh link and node statistics such as parent access point, link SNR, packet error rate, parent changes, node hops, total transmit packets, mesh path, connected access points, mesh group, data rate, and channel. The mesh link and mesh node statistics can be run individually or combined.	Yes	No	Tabular	No
Nodes	This report displays mesh tree information for each mesh access point such as hop count, number of directly connected children, number of connected access points, and mesh path.	Yes	No	Tabular	No
Packet Stats	This report displays the total number of packets transmitted, packets transmitted per minute, packet queue average, packet dropped count, packets dropped per minute, and errors for packets transmitted by neighbor access points. A report type can be chosen for each data type.	No	No	Graphical	No
Stranded APs	This report displays access points that appear to be stranded. These access points might have joined a controller at one time and are no longer joined to a controller managed by Prime Infrastructure, or they might have never joined a controller managed by Prime Infrastructure.	No	No	Tabular	No
Worst Node Hops	This report displays the worst node hops or backhaul SNR links for the specified reporting period. The information is displayed in both table and graph form. Report types include worst node hops, worst SNR links for all neighbors, and worst SNR links for parent and children only.	Yes	Yes	Various	No

Network Summary Reports

The following table describes the various Network Summary reports that you can generate in Prime Infrastructure.

Table 22-9 Network Summary Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
802.11n Summary	This report displays a summary of 802.11n clients and client bandwidth usage at a specified period of time.	No	Yes	Graphical	No
Preferred Calls	This report displays the access points with preferred calls made on the wireless network.	No	No	Graphical	No
Wireless Network Executive Summary	This report displays a quick view of your wireless network.	No	Yes	Various	No

Performance Reports

The following table describes the various Performance reports that you can generate in Prime Infrastructure.

Table 22-10 Performance Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
802.11 Counters	This report displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.	Yes	No	Both	Yes
AP RF Quality	This report displays the RF statistics for each radio over a period of time on your wireless network.	Yes	Yes	Tabular	Yes
AP RF Quality History	This report provides details of client count against RSSI and SNR for each radio over a period of time. You can use this report to analyze RF environment.	Yes	Yes	Tabular	Yes
Coverage Hole	This report identifies the location of potential coverage holes in your network and whether they occur more frequently at a given spot. This report can help you modify RRM settings or determine if additional access points are needed to provide coverage in sparsely deployed areas. It runs on the alarm table and shows both the alarm generation time, the cleared time (if cleared), and the state of the alarm (active or cleared).	Yes	No	Tabular	No

Table 22-10 Performance Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Environmental Temperature	This report displays the environmental temperature data for devices in your network.	Yes	Yes	Tabular	Yes
Interface Errors and Discards	This report displays devices with errors and discards in your network.	Yes	No	Tabular	Yes
Threshold Violation	This report displays the threshold violation event data for your network.	Yes	No	Tabular	Yes
Video Statistics	This report helps you to analyze wireless network usage from a video perspective by providing details such as percentage of bandwidth used by video clients, video calls, roaming video calls, and rejected calls (per video) on your network. To gather useful data for this report, video clients must support Call Admission Control (CAC).	No	No	Graphical	No
VoIP Calls Graph	This report helps you to analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.	No	No	Graphical	No
VoIP Calls Table	This report helps you to analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a table.	No	No	Tabular	No
Voice Statistics	This report helps you to analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To gather useful data for this report, voice clients must support CAC. **Note** Voice Statistics reports only apply to clients that support Call Admission Control (CAC) and have CAC enabled.	No	No	Graphical	No

Table 22-10 Performance Reports (continued)

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Wireless Network Utilization	This report shows the overall network utilization based on the aggregated port utilization of all controllers in your network. These statistics can help identify current network performance and help with capacity planning for future scalability needs. **Note** Average utilization (%) is the percentage of utilization where utilization is calculated as ((Tx+Rx)/bandwidth).	Yes	Yes	Both	Yes
Wireless Traffic Stream Metrics	This report can be useful in determining the current and historical QoS for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.	Yes	Yes	Both	Yes
Wireless Tx Power and Channel	This report displays the channel plan assignment and transmit power-level trends of devices based on the filtering criteria used when the report was generated. It helps to identify unexpected behavior or issues with network performance.	No	No	Graphical	No
Worst RF APs	This report displays the APs with the lowest average RSSI value in your wireless network over a period of time.	Yes	Yes	Tabular	Yes
Application Summary	This report displays the details of the application configuration.	No	Yes	Tabular	Yes
Conversations	This report displays conversation details.	Yes	Yes	Tabular	Yes
End User Summary	This report displays the average RTP packet loss per client.	No	Yes	Tabular	Yes
Site Summary	This report displays the top N clients, worst N clients, top N VLANS, and top N applications by site.	No	Yes	Both	Yes
Voice Video Summary	This report displays the voice call statistics summary.	Yes	Yes	Tabular	Yes
WAN Performance Analysis	This report displays the WAN application traffic volume trend.	No	Yes	Graphical	No
WAN Traffic Analysis Summary	This report displays the WAN application traffic details.	No	Yes	Tabular	Yes

Raw NetFlow Reports

The following table describes the various Raw NetFlow reports that you can generate in Prime Infrastructure.

Table 22-11 Raw NetFlow Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
AVC Troubleshooting	This report displays the AVC traffic details.	Yes	No	Tabular	Yes
Netflow V1	This report displays the data for Netflow V1.	No	No	Graphical	No
Netflow V5	This report displays the data for Netflow V5.	No	No	Graphical	No
Netflow V7	This report displays the data for Netflow V7.	No	No	Graphical	No

Security Reports

The following table describes the various Security reports that you can generate in Prime Infrastructure.

Table 22-12 Security Reports

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Adaptive wIPS Alarm	This report displays wIPS alarms by selected MSEs, controllers, and access points for each alarm type.	Yes	No	Tabular	No
Adaptive wIPS Alarm Summary	This report displays a summary of all adaptive wIPS alarms on your network.	Yes	No	Both	No
Adaptive wIPS Top 10 APs	This report displays the top ten access points with the highest number of generated adaptive wIPS alarms.	Yes	No	Tabular	No
Adhoc Rogue Count Summary	This report displays a summarized count of all ad hoc rogue access points.	No	No	Both	No
Adhoc Rogues	This report displays details for all ad hoc rogue devices detected by your network access points, based on the time they were last seen. Prime Infrastructure receives updates about ad hoc rogues from controllers by using traps or by polling. Last Seen Time is updated any time a trap for the ad hoc rogue is received or the ad hoc rogue is seen during the Prime Infrastructure polling cycle. **Note** This report includes rogue access point alarms with clear severity.	Yes	No	Tabular	No
New Rogue AP Count Summary	This report displays a summarized count of all new rogue access points.	No	No	Both	No

Table 22-12 ***Security Reports (continued)***

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
New Rogue APs	This report displays all rogues detected for the first time on your network within the selected time frame for this report. The value in the Created Time column indicates the time at which the rogue was first detected. **Note** This report includes rogue access point alarms with clear severity.	No	No	Graphical	No
Rogue AP Count Summary	This report displays a summarized count of all rogue access points on your network.	No	No	Both	No
Rogue AP Events	This report displays all rogue access point events received by Prime Infrastructure, based on event time. Any rogue-related trap received by Prime Infrastructure is logged as a rogue event in Prime Infrastructure. A new rogue access point event is created by Prime Infrastructure based on polled data when there is a newly detected rogue access point. In addition, an event is created by Prime Infrastructure when the user changes the state and classification of the rogue access point through the Prime Infrastructure user interface. **Note** One rogue can have multiple events. This report is based on the time stamp of the event.	Yes	No	Tabular	Yes
Rogue APs	Prime Infrastructure gets updates about rogues from controllers by using traps or by polling. The Last Seen Time is updated any time a trap for the rogue is received or rogue is seen during the last Prime Infrastructure polling cycles. This report displays all rogues detected by the access points in your network based on the Last Seen Time of the rogue access points and the selected filtering criteria. The report lists rogue access points based on the time they were last seen. **Note** The report includes rogue access point alarms with clear severity.	Yes	No	Tabular	No
Security Alarm Trending Summary	This report displays a summary of security alarm trends over a period of time.	No	No	Graphical	No

APPENDIX A

Prime Infrastructure User Interface Reference

Cisco 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 hover your cursor on the tab.

> **Note** If any of your installed Cisco Prime products are not yet enabled through licensing, the tabs or options for those products are not activated.

- Prime Infrastructure UI Components, page A-1
- Common UI Tasks, page A-11
- Search Methods, page A-15

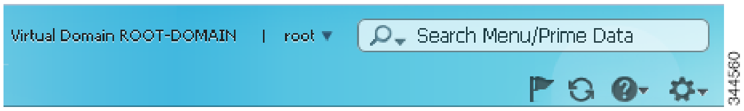
Prime Infrastructure UI Components

The Prime Infrastructure user interface components are visible on most of the pages.

Global Toolbars

Prime Infrastructure pages contain the following static global toolbar at the top right (see Figure A-1.)

Figure A-1 Global Toolbar—Top Right



- **Virtual Domain name**—Indicates the virtual domain to which you are assigned.
- **Login name**—Indicates your 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:

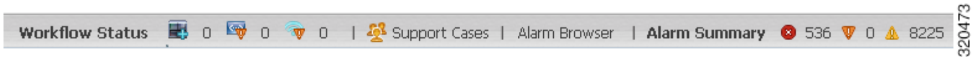
  - Lifecycle view, which is organized according to home, design, deploy, operate, report, and administer menus.

  - 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 Search Methods, page A-15.
- **Welcome**—Launches the Getting Started wizard, which provides guidance for getting started with setting up Prime Infrastructure.
- **Refresh**—Refreshes the active page.
- **Help**—Launches Prime Infrastructure online help and learning modules.
- **Edit Dashboard**—Allows you to add, rename, and manage dashboards.

Prime Infrastructure pages contain the following static global toolbar at the bottom right.

Figure A-2 Global Toolbar—Bottom Right



- **Workflow Status**—Launches the workflow status summary window that displays the site maps, newly registered devices, and any failed wired and wireless workflows.
- **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, page 21-2 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 indicating the number of critical, major, and minor alarms.

Dashboards and Dashlets

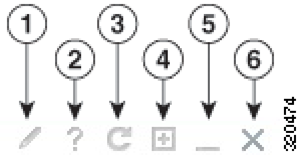
Dashboards display at-a-glance views of the most important data in your network. Dashboards contain *dashlets* that consist of visual displays such as tables and charts.

Note Adobe Flash Player must be installed before you can view the dashlets on a Prime Infrastructure dashboard.

Dashboards generally provide status and alerts, monitoring, and reporting information; a quick scan of a dashboard should let you know if anything needs attention. Use the filters at the top of the dashboards to specify the information that is displayed.

Dashboards contain dashlets that consist of visual displays such as tables and charts. You can drag and drop dashlets to any location in the dashboards. Hover your mouse cursor in any dashlet, and the following icons appear at the top-right corner of the dashboard.

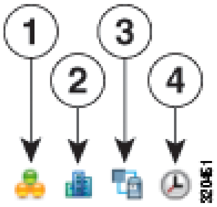
Figure A-3 Dashlet Icons



1	Dashlet options include editing the dashlet title, refreshing the dashlet, or changing the dashlet refresh interval. (To disable refresh, uncheck Refresh Dashlet.)
2	Dashlet help includes a screenshot of the dashlet, a description, the data sources, and any applicable filters.
3	Refresh the dashlet.
4	Maximize the dashlet. A restore icon appears, allowing you to restore the dashlet to its default size.
5	Collapse the dashlet so that only its title appears. An expand icon appears.
6	Remove the dashlet.

Dashlet badges indicate which filters were applied when generating the contents of each dashlet (see Performing a Dashboard Filter, page A-9).

Figure A-4 Dashlet Badges



1	Network aware filter. Use this filter to collect data for all devices, wired devices, wireless devices, or a specific wireless SSID.
2	Site filter. Use this filter to collect data associated with an AP or a controller located at a predefined location.
3	Application filter. Use this filter to collect data based on a service, an application within a service, up to ten separate applications, or all applications.
4	Time frame filter. Use this filter to collect data for a preset time period, or you can specify a beginning and ending date.

You can customize the predefined set of dashlets depending on your network management needs. You can organize the information in user-defined dashboards. The default view comes with default dashboards and pre-selected dashlets for each.

Note

- The label “*Edited*” next to the dashlet heading indicates that the dashlet has been customized. If you reset to the default settings, the Edited label is cleared.
- When an upgrade occurs, the arrangement of dashlets in a previous version is maintained. Because of this, dashlets or features added in a new release are not displayed. Click the **Manage Dashboards** link to discover new dashlets.
- The horizontal and vertical scrollbars are visible if you zoom the dashlets. Reset the zoom level back to zero, or no zoom for viewing the dashlets without the scrollbars.

Adding Dashboards

To add a create a custom dashboard:

Step 1 Click the **Settings** icon and 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 Adding Dashlets, page A-4).

Configuring Dashboards

After an upgrade, the arrangement of dashlets in the previous version is maintained. Therefore, dashlets or features added in a new release are not displayed. To display new dashlets, click the **Settings** icon and choose **Manage Dashboards**.

To restore a dashboard to the default settings:

Step 1 From the home page, click the **Edit Dashboard** icon.

Step 2 Click **Manage Dashboards**, choose a dashboard from the list, and click **Reset**.

Adding Dashlets

A subset of the available dashlets is automatically displayed in the dashboards. To add a dashlet that is not automatically displayed to a dashboard:

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards**.

Step 2 Display the dashboard to which you want to add the dashlet, click the gear icon on the global toolbar, then click **Add Dashlets**.

Step 3 Find the dashboard heading in the drop-down list; you can add any of the dashlets under that heading to that dashboard.

The following table lists the default dashlet options that you can add in your Prime Infrastructure home page.

Table A-1 Default Dashlets

Dashlet	Description
AP Join Taken Time	Displays the access point name and the amount of time (in days, minutes, and seconds) that it took for the access point to join.
AP Threats/Attacks	Displays various types of access point threats and attacks and indicates how many of each type have occurred.
AP Uptime	Displays each access point name and amount of time it has been associated.
Ad hoc Rogues	Displays ad hoc rogues for the previous hour, previous 24 hours, and total active.
Cisco Wired IPS Events	Displays wired IPS events for the previous hour, previous 24 hours, and total active.
Client	Displays the five most recent client alarms with client association failures, client authentication failures, client WEP key decryption errors, client WPA MIC errors, and client exclusions.
Client Authentication Type	Displays the number of clients for each authentication type.
Client Count	Displays the trend of associated and authenticated client counts in a given period of time.
Client Distribution	Displays how clients are distributed by protocol, EAP type, and authentication type.
Client EAP Type Distribution	Displays the count based on the EAP type.
Client Protocol Distribution	Displays the current client count distribution by protocols.
Client Security Events	Displays client security events within the previous 24 hours including excluded client events, WEP decrypt errors, WPA MIC errors, shunned clients, and IPsec failures.
Client Traffic	Displays the trend of client traffic in a given time period.
Client Troubleshooting	Allows you to enter a MAC address of a client and retrieve information for diagnosing the client in the network.
Clients Detected by Context Aware Service	Displays the client count detected by the context aware service within the previous 15 minutes.
Controller CPU Utilization (%)	Displays the average, maximum, and minimum CPU usage.
Controller Memory Utilization	Displays the average, maximum, and minimum memory usage as a percentage for the controllers.
Coverage Areas	Displays the list coverage areas and details about each coverage area.
Friendly Rogue APs	Displays friendly rogue access points for the previous hour, previous 24 hours, and total active.
Guest Users Count	Displays Guest client count over a specified time.

Table A-1 Default Dashlets (continued)

Dashlet	Description
Inventory Detail Status	Displays the Chart summarizing the status for the following device types: • Controllers • Switches • Autonomous APs • Radios • MSEs • Third Party Controllers • Third Party Access Points
Inventory Status	Displays the total number of client controllers and the number of unreachable controllers.
LWAPP Uptime	Displays the access point name and the amount of its uptime in days, minutes, and seconds.
Latest 5 Logged in Guest Users	Displays the most recent guest users to log in.
Mesh AP by Hop Count	Displays the APs based on hop count.
Mesh AP Queue Based on QoS	Displays the APs based on QoS.
Mesh Parent Changing AP	Displays the worst Mesh APs based on changing parents.
Mesh Top Over Subscribed AP	Displays the considered over subscribed APs.
Mesh Worst Node Hop Count2-28	Displays the Worst AP node hop counts from the root AP.
Mesh Worst Packet Error Rate	Displays the worst Mesh AP links based on the packet error rates of the links.
Mesh Worst SNR Link	Displays the worst Mesh AP links based on the SNR values of the links.
Most Recent AP Alarms	Displays the five most recent access point alarms. Click the number in parentheses to open the Alarms page which shows all alarms.
Most Recent Client Alarms	Displays the most recent client alarms.
Most Recent Mesh Alarms	Displays the most recent mesh alarms
Most Recent Security Alarms	Displays the five most recent security alarms. Click the number in parentheses to open the Alarms page.
Recent 5 Guest User Accounts	Displays the most recent guest user accounts created or modified.
Recent Alarms	Displays the five most recent alarms by default. Click the number in parentheses to open the Alarms page.
Recent Coverage Holes	Displays the recent coverage hole alarms listed by access point.
Recent Malicious Rogue AP Alarms	Displays the recent malicious rogue AP alarms.

Table A-1 Default Dashlets (continued)

Dashlet	Description
Recent Rogue Alarms	Displays the five most recent rogue alarms. Click the number in parentheses to open the Alarms page which shows the alarms.
Security Index	Displays the security index score for the wireless network. The security index is calculated as part of the 'Configuration Sync' background task.
Top APs by Client Count	Displays the Top APs by client count.
Unclassified Rogue APs	Displays unclassified rogue access points for the previous hour, previous 24 hours, and total active.
Client Count By Association/Authentication	Displays the total number of clients by Association and authentication in Prime Infrastructure over the selected period of time. • Associated client—All clients are connected regardless of whether it is authenticated or not. • Authenticated client—All clients are connected through a RADIUS or TACACS server. **Note** Client count includes autonomous clients. **Note** The wired clients connected to open ports are counted as authenticated although authentication did not really happen due to open policy. This is also applicable for the wireless clients connected to an OPEN WLAN. When two areas overlap, the color is blended in the dashlet.

Overriding a Dashlet Filter

You can change the filter settings for just one dashlet. For example, to change the time frame during which data is collected for a single dashlet from the default to 24 hours:

Step 1 Navigate to that dashlet and click **Dashlet Options**.

Step 2 Check the **Override Dashlet Time Filter** check box, choose **Past 24 Hours** from the **Time Frame** drop-down list, then click **Save And Close**.

The dashlet displays the last 24 hours of data. The label “Edited” next to the Time Frame dashlet badge with a red diagonal line over the badge indicates that the filter has been customized.

Creating Generic Dashlets

You can add a generic dashlet anywhere; it displays the values for all polled devices.

Before You Begin

You must create at least one custom template (for example, see Creating Custom SNMP Polling Templates, page 8-32).

To create a generic dashlet:

Step 1 Choose **Detail Dashboards > Device > Edit Dashboard > Add Dashlet(s)**.

Step 2 Find the Generic Dashlet and click **Add**. The Generic Dashlet appears on the dashboard.

Step 3 To edit the dashlet, hover your cursor over the Generic Dashlet and click **Dashlet Options**.

Step 4 Rename the dashlet.

Step 5 From the Template Name drop-down list, choose the custom template that you created, then click **Save**.

Filters

You can use the Filter feature to display specific information about 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—See Performing a Quick Filter, page A-8
- Advanced Filter—See Performing an Advanced Filter, page A-8
- Dashboard Filter—See Performing a Dashboard Filter, page A-9

Performing a 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 (see Performing an Advanced Filter, page A-8).

To launch the quick filter, choose **Quick Filter** from the Filter drop-down list.

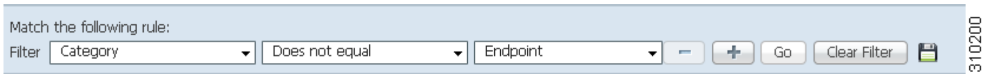
To clear the Quick Filter, click **Filter**.

Performing an 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 the operator from the drop-down list. In addition, you must enter filter criteria based on the data available in the Prime Infrastructure database.

To launch advanced filtering, choose **Advanced Filter** from the Filter drop-down list.

Figure A-5 Advanced Filter



Match the following rule:

Filter: Category | Does not equal | Endpoint

To save the filter criteria used in the Advanced filter:

Step 1 Enter the advanced filter criteria, then click **Go**. The data is filtered based on the filter criteria.

Step 2 After the data is filtered, click the **Save** icon.

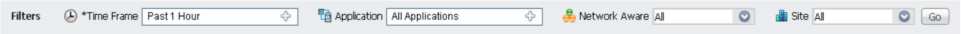
Step 3 In the Save Preset Filter dialog box, enter a name for the preset filter and click **Save**.

Performing a Dashboard Filter

The Filters toolbar allows you to narrow down the data that is displayed in all of the dashlets in a dashboard. Use this toolbar to filter the dashlets data by:

- Time frame—Select one of the preset options or create a custom time frame.
- Applications—Select a service, up to 10 individual applications, or all applications.
- Network Aware—Select wired, wireless, or all networks.
- Site—Select a site, unassigned sites, or all sites.

Figure A-6 Dashboard Filters Toolbar



Filters *Time Frame: Past 1 Hour · Application: All Applications · Network Aware: All · Site: All · Go

To filter the data for all dashlets in a dashboard:

Step 1 Open a dashboard (for example, choose **Operate > Monitoring Dashboards > Detail Dashboards**).

Step 2 Change the settings in any of the **Filters** toolbar options, then click **Go**.

Data Entry Features

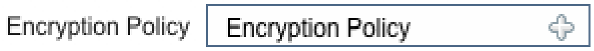
In addition to the check boxes, drop-down lists and data entry fields common in most user interfaces, Prime Infrastructure uses some specialized data-entry features. These features are designed to keep your view of the network as uncluttered as possible, while still making it possible for you to add, update, and save your settings when needed. These specialized data-entry features include:

- Anchored Fields, page A-9
- Edit Tables, page A-10
- Data Popups, page A-10

Anchored Fields

Anchored fields are recognizable by the plus sign (+) embedded in the field at the far right.

Figure A-7 Anchored Field



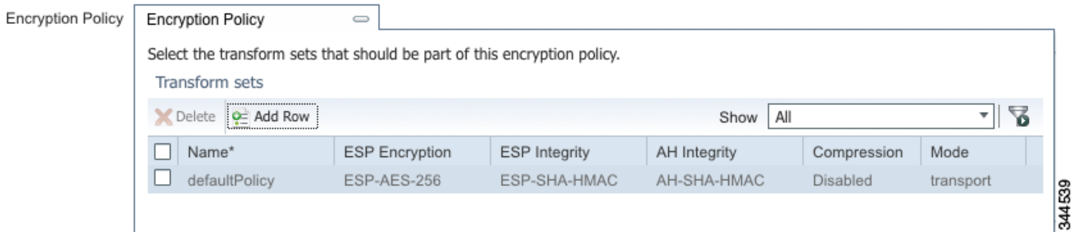
Encryption Policy: Encryption Policy

To use anchored fields:

Step 1 Click the anchored field's plus (+) button.

Step 2 With the associated data popup displayed (see Data Popups, page A-10), review or update the data as needed.

Figure A-8 Anchored Field with Popup



Select the transform sets that should be part of this encryption policy.

□	Name*	ESP Encryption	ESP Integrity	AH Integrity	Compression	Mode
□	defaultPolicy	ESP-AES-256	ESP-SHA-HMAC	AH-SHA-HMAC	Disabled	transport

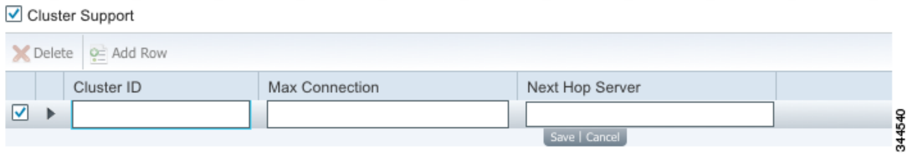
Step 3 When you are finished, click the anchored field’s minus (-) button.

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. Some edit tables also give you access to filters (see Filters, page A-8). Edit tables are often displayed in data popups that are triggered by check boxes or anchored fields.

Figure A-9 Edit Table



		Cluster ID	Max Connection	Next Hop Server
☑	▶			

To use edit tables:

- To add a new row in the edit table:

  Click **Add Row**, complete the fields in the new row, and click **Save**.
- To delete one or more existing rows in an edit table:

  Click the row header check box (at the extreme left of each row), then click **Delete**.
- To update an entry in any field in any edit table row:

  Click the row header or on the field itself, edit the contents, then click **Save**.

Data Popups

A data popup is a window associated with a check box, anchored field (see Anchored Fields, page A-9), or other data-entry feature. It is displayed automatically when you select a feature, so you can view or update the data associated with that feature. In addition to containing check boxes, drop-down lists, and data-entry fields, data popups can also contain edit tables (see Edit Tables, page A-10).

To use a data popup:

1. Select the feature that triggers the data popup, such as an anchored field (see Figure A-7) or a check box (see Figure A-9).
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 window:

- Changing Your Password, page A-11
- Changing Your Active Domain, page A-11
- Monitoring Alarms, page A-11
- Getting Device Details from the Device 360° View, page A-12
- Getting User Details from the User 360° View, page A-13
- Getting Help, page A-15

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 field) and choose **Change Password**.

Step 2 Click the information icon to review the password policy.

Step 3 Enter a new password as directed and click **Save**.

Changing Your Active Domain

Step 1 Hover your mouse 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 Cisco Prime Infrastructure window, hover your mouse cursor on Alarm Summary or Alarm Browser to get information on the latest active alarms.

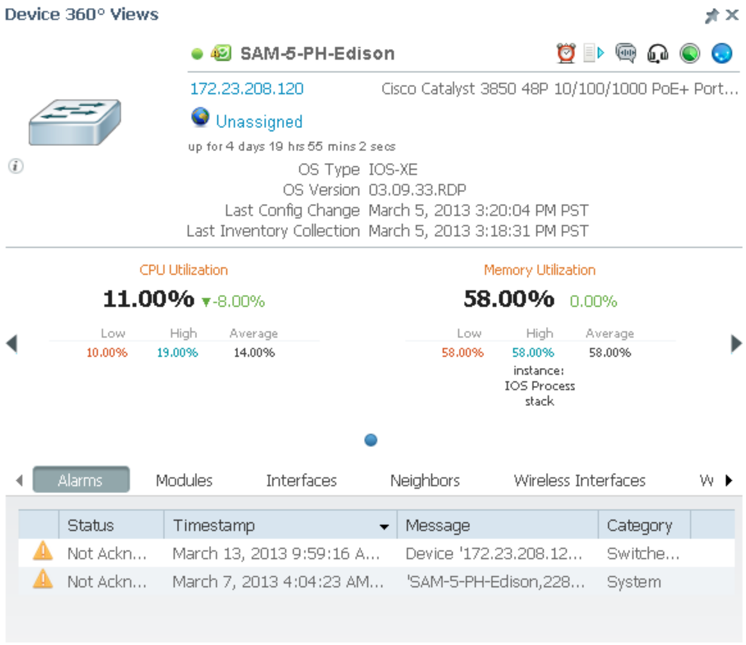
Getting Device Details from the Device 360° View

The Device 360° View provides detailed device information including device status, interface status, and associated device information. You can see the device 360° view from nearly all pages in which device IP addresses are displayed.

To launch the 360° view of any device, hover your mouse cursor on a device IP address, then click the icon that appears.

Note The features that appear in the Device 360° View differ depending on the device type.

Figure A-10 Sample Device 360° View



Device 360° Views

SAM-5-PH-Edison

172.23.208.120 Cisco Catalyst 3850 48P 10/100/1000 PoE+ Port...

Unassigned

up for 4 days 19 hrs 55 mins 2 secs

OS Type IOS-XE
OS Version 03.09.33.RDP
Last Config Change March 5, 2013 3:20:04 PM PST
Last Inventory Collection March 5, 2013 3:18:31 PM PST

CPU Utilization
11.00% ▾-8.00%

Low	High	Average
10.00%	19.00%	14.00%

Memory Utilization
58.00% 0.00%

Low	High	Average
58.00%	58.00% instance: IOS Process stack	58.00%

	Status	Timestamp	Message	Category
⚠	Not Ackn...	March 13, 2013 9:59:16 A...	Device '172.23.208.12...	Switche...
⚠	Not Ackn...	March 7, 2013 4:04:23 AM...	'SAM-5-PH-Edison,228...	System

Table A-2 Device 360° View Features

Device 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 at the top right of the device 360° view: • Alarm Browser—Launches the Alarm Browser. See Monitoring Alarms, page 11-1 for more information. • Device Details—Displays device details. • Support Community—Launches the Cisco Support Community. See Launching the Cisco Support Community, page 21-1. • Support Request—Allows you to open a support case. See Opening a Support Case, page 21-2 for more information. • Ping—Allows you to ping the device. • Traceroute—Allows you to perform a traceroute on the device.
Alarms	Lists alarms on the device, including the alarm status, time stamp, and category.
Modules	Lists the device modules and their name, type, state, and ports.
Interfaces	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.
Wireless Interfaces	Lists the interface names, associated WLANs, VLAN IDs and IP addresses.
WLAN	Lists the WLAN names, SSIDs, security policies, and number of clients.

Getting User Details from the User 360° View

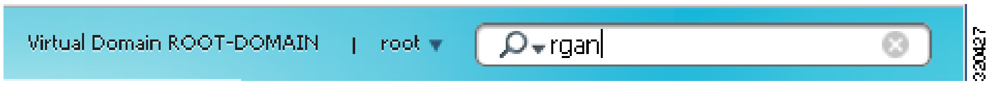
The User 360° View provides detailed information about an end user, including:

- End user network connection and association
- Authentication and authorization
- Possible problems with the network devices associated with the user's network attachment
- Application-related issues
- Other issues in the broader network

To access the 360° view for a user:

Step 1 Enter the user name in the Search field (see Search Methods, page A-15).

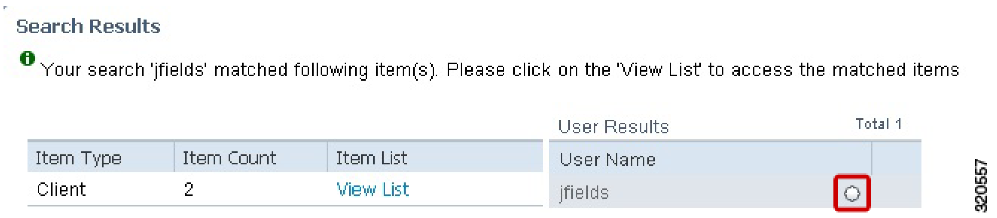
Figure A-11 Sample User Search Entry



Step 2 Multiple matches are displayed in the Search Results dialog. Click **View List** to display the matches.

Step 3 To launch the User 360° View, hover your mouse over the name in the User Name field, then click the icon that appears as shown in Figure A-12.

Figure A-12 Launching User 360° View



Search Results

Your search 'jfields' matched following item(s). Please click on the 'View List' to access the matched items

Item Type	Item Count	Item List
Client	2	View List

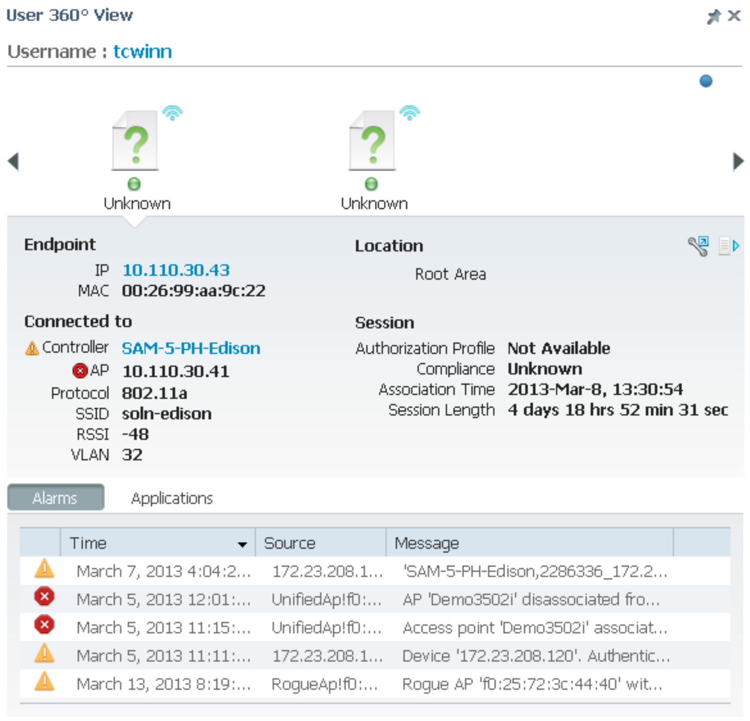
User Results Total 1

User Name
jfields

320557

Step 4 Figure A-13 shows a sample of the User 360° View.

Figure A-13 Sample User 360° View



User 360° View

Username : tcwinn

Endpoint
IP 10.110.30.43
MAC 00:26:99:aa:9c:22

Location
Root Area

Connected to
Controller SAM-5-PH-Edison
AP 10.110.30.41
Protocol 802.11a
SSID soln-edison
RSSI -48
VLAN 32

Session
Authorization Profile Not Available
Compliance Unknown
Association Time 2013-Mar-8, 13:30:54
Session Length 4 days 18 hrs 52 min 31 sec

Alarms Applications

	Time	Source	Message
⚠	March 7, 2013 4:04:2...	172.23.208.1...	'SAM-5-PH-Edison,2286336_172.2...
⊗	March 5, 2013 12:01:...	UnifiedAp!f0:...	AP 'Demo3502i' disassociated fro...
⊗	March 5, 2013 11:15:...	UnifiedAp!f0:...	Access point 'Demo3502i' associat...
⚠	March 5, 2013 11:11:...	172.23.208.1...	Device '172.23.208.120'. Authentic...
⚠	March 13, 2013 8:19:...	RogueAp!f0:...	Rogue AP 'f0:25:72:3c:44:40' wit...

Table A-3 User 360° View Features

User 360° View Feature	Description
User information	Displays key information about the end user.
Endpoint	Displays endpoint information. This feature requires integration with an ISE server.

Table A-3 User 360° View Features

User 360° View Feature	Description
Connected To	Network attachment information: • Network device (access switch or AP + Controller): Visible indication of existence and severity of any active alarms associated with the device • Attachment port: Visible indication of existence and severity of any active alarms associated with the port
Location Session	Displays network session information: • The location is the Prime Infrastructure hierarchy location. • Access Policy (ISE Authorization Profile). Visible indication of the existence of any errors associated with authentication. This feature requires integration with an ISE server. • Endpoint compliance status. This feature requires integration with an ISE server. • Session start time and end time.
Alarms	Click the **Alarms** tab to view a list of alarms and statistics associated with the network session.
Applications	Click the **Applications** tab to view a list of applications and statistics associated with the network session. Session information (Netflow/NAM data, Assurance licenses) must be available.

Getting Help

You can access online help by clicking the question mark icon at the top right of any Prime Infrastructure page.

Search Methods

Prime Infrastructure provides the following search methods:

- Quick Search—See Performing a Quick Search, page A-15
- Advanced Search—See Performing an Advanced Search, page A-16
- Saved Search—See Performing a Saved Search, page A-26

You can access the search options from any page within Prime Infrastructure.

Performing a Quick Search

For a quick search, you can enter a partial or complete IP address or name. You can also enter a username if you are searching for a client.

To quickly search for a device:

Step 1 In the Search text box, enter a search string and.

Step 2 Click **Search** to display all matches for the Quick Search parameter.

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 in Prime Infrastructure:

Step 1 Choose **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, enter a unique name for the search in the text box, and click **Go**.

Note You can decide what information appears on the search results page. See the "Configuring the Search Results Display (Edit View)" section on page A-26 for more information.

The Search categories include the following:

- Alarms—See Searching Alarms, page A-17
- Jobs—See Searching Jobs, page A-17
- Access Points—See Searching Access Points, page A-18
- Controller Licenses—See Searching Controller Licenses, page A-19
- Controllers—See Searching Controllers, page A-19
- Switches—See Searching Switches, page A-20
- Clients—See Searching Clients, page A-20
- Chokepoints—See Searching Chokepoints, page A-22
- Events—See Searching Events, page A-22
- Interferers—See Searching Interferers, page A-23
- Wi-Fi TDOA Receivers—See Searching Wi-Fi TDOA Receivers, page A-24
- Maps—See Searching Maps, page A-24
- Rogue Client—See Searching Rogue Clients, page A-24
- Shunned Client—See Searching Shunned Clients, page A-25
- Tags—See Searching Tags, page A-25
- Device Type—See Searching Device Type, page A-26
- Configuration Versions—See Searching Configuration Versions, page A-26

Searching Alarms

You can configure the following parameters when performing an advanced search for alarms (see Table A-4).

Table A-4 Search Alarms Fields

Field	Options
Severity	Choose **All Severities**, **Critical**, **Major**, **Minor**, **Warning**, or **Clear**.
Alarm Category	Choose **All Types**, **System**, **Access Points**, **Controllers**, **Coverage Hole**, **Config Audit**, **Mobility Service**, **Context Aware Notifications**, **SE Detected Interferers**, **Mesh Links**, **Rogue AP**, **Adhoc Rogue**, **Security**, **Performance**, **Application Performance, Routers, Switches and Hubs,** or **Cisco Interfaces and Modules**.
Condition	Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you have selected an alarm category, this drop-down list would contain the conditions available in that category.
Time Period	Choose a time increment from Any Time to Last 7 days. The default is Any Time.
Acknowledged State	Select this check box to search for alarms with an Acknowledged or Unacknowledged state. If this check box is not selected, the acknowledged state is not taken into search criteria consideration.
Assigned State	Select this check box to search for alarms with an Assigned or Unassigned state or by Owner Name. If this check box is not selected, the assigned state is not part of the search criteria. **Note** If you choose Assigned State > Owner Name, type the owner name in the available text box.

Searching Jobs

You can configure the following parameters when performing an advanced search for jobs (see Table A-5).

Table A-5 Search Jobs Fields

Field	Options
Job Name	Type the name of the job that you want to search.
Job Type	Type the job type that you want to search.
Job Status	Choose **All Status**, **Completed**, **or Scheduled**.

For more information, see the "Monitoring Jobs" section on page 10-6.

Note You can use wildcards such as *, ? in the Job Name and Job Type text box to narrow or broaden your search.

Searching Access Points

You can configure the following parameters when performing an advanced search for access points (see Table A-6).

Table A-6 Search Access Points Fields

Field	Options
Search By	Choose **All APs**, **Base Radio MAC**, **Ethernet MAC**, **AP Name**, **AP Model, AP Location**, **IP Address**, **Device Name**, **Controller IP**, **All Unassociated APs**, **Floor Area**, **Outdoor Area**, **Unassigned APs**, or **Alarms**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select Floor Area, you also must identify its campus and building. Or, if you select Alarms, you can search for access points based on the severity of the alarm.
AP Type	Choose **All Types**, **LWAPP**, or **Autonomous**.
AP Mode	Choose **All Modes**, **Local, Monitor**, **FlexConnect**, **Rogue Detector**, **Sniffer**, **Bridge**, or **SE-Connect**.
Radio Type	Choose **All Radios**, **802.11a**, or **802.11b/g**.
802.11n Support	Select this check box to search for access points with 802.11n support.
OfficeExtend AP Enabled	Select this check box to search for OfficeExtend access points.
CleanAir Support	Select this check box to search for access points which support CleanAir.
CleanAir Enabled	Select this check box to search for access points which support CleanAir and which are enabled.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Controller Licenses

You can configure the following parameters when performing an advanced search for controller licenses (see Table A-7).

Table A-7 Search Controller Licenses Fields

Field	Options
Controller Name	Type the controller name associated with the license search.
Feature Name	Choose **All**, **Plus**, or **Base** depending on the license tier.
Type	Choose **All**, **Demo**, **Extension**, **Grace Period**, or **Permanent**.
% Used or Greater	Choose the percentage of the license use from this drop-down list. The percentages range from 0 to 100.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Controllers

You can configure the following parameters when performing an advanced search for controllers (see Table A-8).

Table A-8 Search Controllers Fields

Field	Options
Search for controller by	Choose **All Controllers**, **IP Address**, or **Controller Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Enter Controller IP Address	This text box appears only if you choose IP Address from the Search for controller by drop-down list.
Enter Controller Name	This text box appears only if you choose Controller Name from the Search for controller by drop-down list.

Table A-8 Search Controllers Fields (continued)

Field	Options
Audit Status	Choose one of the following from the drop-down list: • **All Status** • **Mismatch**—Config differences were found between Prime Infrastructure and controller during the last audit. • **Identical**—No config differences were found during the last audit. • **Not Available**—Audit status is unavailable.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Switches

You can configure the following parameters when performing an advanced search for switches (see Table A-9).

Table A-9 Search Switches Fields

Field	Options
Search for Switches by	Choose **All Switches**, **IP Address**, or **Switch Name**. You can use wildcards (*). For example, if you select IP Address and enter **172***, Prime Infrastructure returns all switches that begin with IP address 172.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Clients

You can configure the following parameters when performing an advanced search for clients (see Table A-10).

Table A-10 Search Clients Fields

Field	Options
Media Type	Choose **All**, **Wireless Clients**, or **Wired Clients**.
Wireless Type	Choose **All**, **Lightweight** or **Autonomous Clients** if you chose Wireless Clients from the Media Type list.

Table A-10 Search Clients Fields (continued)

Field	Options
Search By	Choose **All Clients**, **All Excluded Clients**, **All Wired Clients**, **All Logged in Guests**, **IP Address**, **User Name**, **MAC Address**, **Asset Name**, **Asset Category**, **Asset Group**, **AP Name**, **Controller Name**, **Controller IP**, **MSE IP**, **Floor Area**, **Outdoor Area**, **Switch Name**, or **Switch Type**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select IP address, you must enter the specific IP address for this search.
Clients Detected By	Choose **Prime Infrastructure** or **MSEs**. Clients detected by Prime Infrastructure—Clients stored in Prime Infrastructure databases. Clients detected by MSE—Clients located by Context Aware service in the MSE directly communicating with the controllers.
Client States	Choose **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excluded**.
Posture Status	Choose **All**, **Unknown**, **Passed**, **Failed** if you want to know if the devices are clean or not.
Restrict By Radio Band	Select the check box to indicate a specific radio band. Choose **5 GHz** or **2.4 GHz** from the drop-down list.
Restrict By Protocol	Select the check box to indicate a specific protocol. Choose **802.11a**, **802.11b**, **802.11g**, **802.11n**, or **Mobile** from the drop-down list.
SSID	Select the check box and choose the applicable SSID from the drop-down list.
Profile	Select the check box to list all of the clients associated to the selected profile. **Note** Once the check box is selected, choose the applicable profile from the drop-down list.
CCX Compatible	Select the check box to search for clients that are compatible with Cisco Client Extensions. **Note** Once the check box is selected, choose the applicable version, **All Versions**, or **Not Supported** from the drop-down list.

Table A-10 Search Clients Fields (continued)

Field	Options
E2E Compatible	Select the check box to search for clients that are end–to–end compatible. **Note** Once the check box is selected, choose the applicable version, **All Versions**, or **Not Supported** from the drop-down list.
NAC State	Select the check box to search for clients identified by a certain Network Admission Control (NAC) state. **Note** Once the check box is selected, choose the applicable state from the drop-down list: **Quarantine**, **Acces**s, **Invalid**, and **Not Applicable**.
Include Disassociated	Select this check box to include clients that are no longer on the network but for which Prime Infrastructure has historical records.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Chokepoints

You can configure the following parameters when performing an advanced search for chokepoints (see Table A-11).

Table A-11 Search Chokepoint Fields

Field	Options
Search By	Choose **MAC Address** or **Chokepoint Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select MAC address, you must enter the specific MAC address for this search.

Searching Events

You can configure the following parameters when performing an advanced search for events (see Table A-12).

Table A-12 Search Events Fields

Field	Options
Severity	Choose **All Severities**, **Critical**, **Major**, **Minor**, **Warning**, **Clear**, or **Info. Color coded**.
Event Category	Choose **All Types**, **Access Points**, **Controller**, **Security**, **Coverage Hole, Rogue AP**, **Adhoc Rogue**, **Interference**, **Mesh Links**, **Client**, **Mobility Service**, **Location Notifications**, **Pre Coverage Hole**, or **Prime Infrastructure**.
Condition	Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you selected an event category, this drop-down list contains the conditions available in that category.
Search All Events	Configure the number of records to be displayed in the search results page.

Searching Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table A-13).

Table A-13 Search SE-Detected Interferers Fields

Field	Options
Search By	Choose **All Interferers**, **Interferer ID**, **Interferer Category**, **Interferer Type**, **Affected Channel**, **Affected AP**, **Severity**, **Power**, or **Duty Cycle**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected By	Choose **All Spectrum Experts** or a specific spectrum expert from the drop-down list.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Interferer Status	From this drop-down list, choose **All**, **Active**, or **Inactive**.
Restrict by Radio Bands/Channels	Configure the search by radio bands or channels.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Wi-Fi TDOA Receivers

You can configure the following parameters when performing an advanced search for Wi-Fi TDOA receivers (see Table A-14).

Table A-14 Search Wi-Fi TDOA Receivers Fields

Field	Options
Search By	Choose **MAC Address** or **Wi-Fi TDOA Receivers Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Searching Maps

You can configure the following parameters when performing an advanced search for maps (see Table A-15).

Table A-15 Search Map Fields

Field	Options
Search for	Choose **All Maps**, **Campuses**, **Buildings**, **Floor Areas**, or **Outdoor Areas**.
Map Name	Search by Map Name. Enter the map name in the text box.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Rogue Clients

You can configure the following parameters when performing an advanced search for rogue clients (see Table A-16).

Table A-16 Search Rogue Client Fields

Field	Options
Search for clients by	Choose **All Rogue Clients**, **MAC Address**, **Controller**, **MSE**, **Floor Area**, or **Outdoor Area**.
Search In	Choose **MSEs** or **Prime Infrastructure Controllers**.
Status	Select the check box and choose **Alert**, **Contained**, or **Threat** from the drop-down list to include status in the search criteria.

Searching Shunned Clients

Note When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client.

You can configure the following parameters when performing an advanced search for shunned clients (see Table A-17).

Table A-17 Search Shunned Client Fields

Field	Options
Search By	Choose **All Shunned Clients**, **Controller**, or **IP Address**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Searching Tags

You can configure the following parameters when performing an advanced search for tags (see Table A-18).

Table A-18 Search Tags Fields

Field	Options
Search for tags by	Choose **All Tags**, **Asset Name**, **Asset Category**, **Asset Group**, **MAC Address**, **Controller**, **MSE**, **Floor Area**, or **Outdoor Area**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter 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.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Device Type

You can configure the following parameters when performing an advanced search for device type (see Table A-18).

Table A-19 Search Device Type Fields

Field	Options
Select Device Type	Choose **All**, **Switches and Hubs**, **Wireless Controller**, **Unified AP**, **Autonomous AP**, **Unmanaged AP**, and **Routers**.
Enter Device IP	Enter the IP address of the device selected in the Select Device Type field.

Searching Configuration Versions

You can configure the following parameter when performing an advanced search for configuration versions (see Table A-18).

Table A-20 Search Configuration Versions Fields

Field	Options
Enter Tag	Enter the tag name.

Performing a Saved Search

Note Saved searches apply only to the current partition.

To access and run a previously saved search:

Step 1 Click **Saved Search**.

Step 2 Choose a category from the Search Category drop-down list, then choose a saved search from the Saved Search List drop-down list.

Step 3 If necessary, change the current parameters for the saved search, then click **Go**.

Configuring the Search Results Display (Edit View)

The Edit View page enables you to choose which columns appear in the Search Results page.

Note The Edit View page is available only from the Classic View.

Column names appear in one of the following lists:

- Hide Information—Lists columns that do not appear in the table. The Hide button points to this list.

- View Information—Lists columns that do appear in the table. The Show button points to this list.

To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by holding down the shift or control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.

INDEX