



## **Cisco Prime Infrastructure 2.0 Administrator Guide**

March 2015

**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-28741-01

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

*Cisco Prime Infrastructure 2.0 Administrator Guide*  
© 2011-2013 Cisco Systems, Inc. All rights reserved.



## **Preface** xi

Audience xi

Related Documentation xi

Obtaining Documentation and Submitting a Service Request xi

xi

---

## **CHAPTER 1**

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

---

## **CHAPTER 2**

**Prime Infrastructure Server Settings** 2-1

Available System Settings 2-1

Configuring Email Settings 2-5

Configuring Global SNMP Settings 2-6

    Viewing SNMP Credential Details 2-8

    Adding a New SNMP Credential Entry 2-9

Configuring Proxy Settings 2-10

Configuring Server Settings 2-11

Configuring TFTP or FTP Servers 2-11

Specifying Administrator Approval for Jobs 2-11

    Approving Jobs 2-12

Specifying Login Disclaimer Text 2-12

Adding Device Information to a User Defined Field 2-12

Managing OUI 2-13

    Adding a New Vendor OUI Mapping 2-13

    Uploading an Updated Vendor OUI Mapping File 2-13

Adding Notification Receivers to Prime Infrastructure 2-14

    Removing a Notification Receiver 2-14

Setting Up HTTPS Access to the Prime Infrastructure Server 2-15

    Generating a Self-Signed Certificate in Prime Infrastructure 2-16

    Generating a Certificate Signing Request (CSR) File 2-16

    Importing a Certificate Authority (CA) Certificate and Key 2-17

Deleting a CA Certificate 2-18

MIB to Prime Infrastructure Alert/Event Mapping 2-19

---

**CHAPTER 3**

**Maintaining Prime Infrastructure Server Health 3-1**

Monitoring Prime Infrastructure Health 3-1

Troubleshooting Prime Infrastructure 3-2

    Launching the Cisco Support Community 3-2

    Opening a Support Case 3-3

Evaluating OVA Size and System Resources 3-3

    Viewing the Number of Devices Prime Infrastructure Is Managing 3-4

Improving Prime Infrastructure Performance 3-4

    Tuning the Server 3-5

        Enabling Server Tuning During Restarts 3-5

        Modifying VM Resource Allocation 3-5

    Compacting the Prime Infrastructure Database 3-6

    Configuring Client Performance Settings 3-6

        Enabling Automatic Client Troubleshooting 3-6

        Enabling Hostname Lookup 3-7

        Specifying for How Long to Retain Client Association History Data 3-7

        Polling Clients When Receiving Client Traps/Syslogs 3-8

        Saving Client Traps as Events 3-8

        Saving 802.1x and 802.11 Client Traps as Events 3-8

Checking the Status of Prime Infrastructure Using CLI 3-8

Recovering Prime Infrastructure Passwords 3-8

Downloading Device Support and Product Updates 3-9

Configuring Support Request Settings 3-10

Stopping Prime Infrastructure 3-11

Removing Prime Infrastructure 3-11

---

**CHAPTER 4**

**Backing Up and Restoring Prime Infrastructure 4-1**

Types of Prime Infrastructure Backups 4-1

Taking Application Backups From the Interface 4-3

Taking Application Backups From the Command Line 4-3

Scheduling Automatic Application Backups 4-4

Taking Appliance Backups	4-4
Using Local Backup Repositories	4-5
Using Remote Backup Repositories	4-5
Types of Prime Infrastructure Restore	4-6
Restoring From Application Backups	4-7
Restoring From Appliance Backups	4-7
Migrating to Another OVA Using Backup and Restore	4-9
Log Information	4-9

---

**CHAPTER 5**
**Maintaining Network Health 5-1**

Configuring Alarm and Event Settings	5-1
Specifying Alarm Clean Up and Display Options	5-1
Changing Alarm Severities	5-3
Configuring Audit Settings	5-4
Setting Up Auditing Configurations	5-4
Choosing the Type of Audit	5-4
Selecting Parameters on Which to Audit	5-5
Deleting Syslogs from Audit Records	5-5
Enabling Change Audit Notifications	5-6
Downloading and Emailing Error Logs	5-6
Enabling SNMP Tracing	5-7
Changing Syslog Logging Options	5-7
Changing Logging Options to Enhance Troubleshooting	5-7
Changing Mobility Service Engine Logging Options	5-9
Downloading Mobility Services Engine Log Files	5-10
Configuring Technical Support Request Settings	5-11

---

**CHAPTER 6**
**Managing Data Collection and Retention 6-1**

Specifying Data Retention Periods	6-2
Prime Infrastructure Historical Data	6-2
Performance Data Aggregation	6-3
Enabling Data Deduplication	6-4
Specifying Where and for How Long to Save Reports	6-4
Controlling Report Storage and Cleanup	6-5

- Specifying Inventory Collection After Receiving Events 6-5
- Device Configuration Settings 6-6
  - Backing up and Rolling Back Configurations 6-6
  - Specifying When to Archive Configurations 6-6
- Controlling Background Data Collection Tasks 6-7
  - Understanding What Data Is Collected and When 6-8
  - Controlling Prime Infrastructure Background Tasks 6-9
- Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure 6-15

---

**CHAPTER 7**

- Configuring Controller and AP Settings 7-1**
  - Configuring SNMP Credentials for Rogue AP Tracing 7-1
  - Configuring Protocols for CLI Sessions 7-2
  - Refreshing Controllers After an Upgrade 7-2
  - Tracking Switch Ports to Rogue APs 7-3
  - Configuring Switch Port Tracing 7-4
    - Establishing Switch Port Tracing 7-6
    - Switch Port Tracing Details 7-6
    - Switch Port Tracing Troubleshooting 7-7

---

**CHAPTER 8**

- Configuring High-Availability and Redundancy 8-1**
  - Configuring High-Availability 8-1
    - Failover and Failback Processes 8-2
      - Failover Scenario 8-2
      - Failback Scenario 8-3
    - High-Availability Notation 8-3
    - Health Monitor 8-3
    - Data Storage 8-5
    - Licensing 8-6
    - Guidelines and Limitations for High-Availability 8-6
    - High-Availability Status 8-7
    - Deploying High-Availability 8-8
    - Configuring High-Availability on the Primary Prime Infrastructure Server 8-9
    - Adding a New Primary Prime Infrastructure Server in Existing High Availability Environment 8-10
    - Removing High Availability Configuration 8-11
      - Remove High Availability Configuration from Primary UI 8-11
      - Remove High Availability Configuration from Primary or Secondary CLI 8-11

Configuring an SSO Server in the High-Availability Environment	8-11
Installing Software Updates in the High-Availability Environment	8-13
Software Update on High-Availability with Primary Alone	8-13
Software Update on High-Availability with Manual Failover Type	8-13
Software Update on High-Availability with Automatic Failover Type	8-14
Troubleshooting Issues in the High-Availability Environment	8-14
Configuring Redundancy	8-15
Prerequisites and Limitations for Redundancy	8-16
Configuring Redundancy Interfaces	8-16
Configuring Redundancy on a Primary Controller	8-17
Configuring Redundancy on a Secondary Controller	8-18
Monitoring the Redundancy States	8-19
Running the Redundancy Status Background Task	8-19
Configuring a Peer Service Port IP and Subnet Mask	8-20
Adding a Peer Network Route	8-20
Resetting and Uploading Files from the Secondary Server	8-21
Disabling Redundancy on Controllers	8-21

---

**CHAPTER 9**

<b>Controlling User Access</b>	9-1
Managing User Accounts	9-1
Viewing Active User Sessions	9-1
Adding Users	9-2
Creating Administrative Users	9-2
Configuring Guest Account Settings	9-3
Disabling User Accounts	9-3
Changing User Passwords	9-3
Changing User Access to Prime Infrastructure Functions	9-4
Changing Password Policy	9-4
Creating User Groups to Control Access to Prime Infrastructure Functions	9-4
Changing Display Preferences	9-5
Using Virtual Domains to Control Access to Sites and Devices	9-6
Understanding Virtual Domain Hierarchy	9-7
Creating a Site-Oriented Virtual Domain	9-10
User Access in Virtual Domains	9-10
Adding Users to Virtual Domains	9-11
Adding Sites and Devices to Virtual Domains	9-11
Changing Virtual Domain Access	9-12

- Virtual Domain RADIUS and TACACS+ Attributes **9-13**
- Auditing User Access **9-13**
  - Accessing the Audit Trail for a User Group **9-14**
  - Viewing Application Logins and Actions **9-14**
  - Viewing Events Initiated by a User **9-14**
- Configuring AAA on Prime Infrastructure **9-15**
  - Setting the AAA Mode **9-15**
  - Adding a TACACS+ Server **9-16**
  - Adding a RADIUS Server **9-16**
    - Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes **9-17**
  - Adding an SSO Server **9-17**
  - Configuring SSO Server AAA Mode **9-17**
- Authenticating AAA Users Through RADIUS Using Cisco Identity Services Engine **9-18**
  - Adding Prime Infrastructure as an AAA Client in ISE **9-19**
  - Creating a New User Group in ISE **9-19**
  - Creating a New User and Adding to a User Group in ISE **9-19**
  - Creating a New Authorization Profile in ISE **9-20**
  - Creating an Authorization Policy Rule in ISE **9-20**
  - Creating a Simple Authentication Policy in ISE **9-21**
  - Creating a Rule-Based Authentication Policy in ISE **9-21**
  - Configuring AAA in Prime Infrastructure **9-22**
- Configuring ACS 4.x **9-22**
  - Adding Prime Infrastructure to an ACS Server for Use with TACACS+ Server **9-22**
  - Adding Prime Infrastructure User Groups into ACS for TACACS+ **9-23**
  - Adding Prime Infrastructure to an ACS Server for Use with RADIUS **9-24**
  - Adding Prime Infrastructure User Groups into ACS for RADIUS **9-25**
  - Adding Prime Infrastructure to a Non-Cisco ACS Server for Use with RADIUS **9-25**
- Configuring ACS 5.x **9-27**
  - Creating Network Devices and AAA Clients **9-27**
  - Adding Groups **9-27**
  - Adding Users **9-27**
  - Creating Policy Elements or Authorization Profiles for RADIUS **9-28**
  - Creating Policy Elements or Authorization Profiles for TACACS+ **9-28**
  - Creating Service Selection Rules for RADIUS **9-28**
  - Creating Service Selection Rules for TACACS+ **9-28**
  - Configuring Access Services for RADIUS **9-29**
  - Configuring Access Services for TACACS+ **9-29**



---

**CHAPTER 10****Advanced Monitoring 10-1**

Enabling NetFlow Monitoring 10-2

WAN Optimization 10-2

---

**CHAPTER 11****Managing Licenses 11-1**

Prime Infrastructure Licensing 11-1

Purchasing a Prime Infrastructure License 11-2

Managing License Coverage 11-3

Verifying License Details 11-3

Adding Licenses 11-4

Deleting Licenses 11-4

Troubleshooting Licenses 11-4

Controller Licensing 11-5

MSE Licensing 11-6

MSE License Structure Matrix 11-7

Sample MSE License File 11-7

Revoking and Reusing an MSE License 11-8

MSE Services Coexistence 11-8

Managing MSE Licenses 11-9

Registering Product Authorization Keys 11-9

Installing Client and wIPS License Files 11-10

Deleting a Mobility Services Engine License File 11-11

Assurance Licensing 11-11

Verifying Assurance License Details 11-11

Adding License Coverage For NetFlow and NAM Devices 11-12

Deleting License Coverage for NetFlow and NAM Devices 11-12

---

**CHAPTER 12****Managing Traffic Metrics 12-1**

Configuring Prime Infrastructure to Use NAM Devices as Data Sources 12-1

Configuring Prime Infrastructure to Use Routers and Switches as Data Sources 12-2

Configuring Mediatrace on Routers and Switches 12-3

Configuring WSMA and HTTP(S) Features on Routers and Switches 12-4

---

**CHAPTER 13**

**Planning Network Capacity Changes** 13-1

---

**INDEX**



## Preface

---

This guide describes how to administer Cisco Prime Infrastructure.

## Audience

This guide is for administrators who are responsible for setting up, maintaining, and configuring Prime Infrastructure. The tasks in this guide are typically performed by administrators only.

## Related Documentation

See the [Cisco Prime Infrastructure Documentation Overview](#) for a list of all Prime Infrastructure guides.



### 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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/c/en/us/td/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 delivers content directly to your desktop using a reader application. The RSS feeds are a free service.





# Introduction to Administering 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.

The **Administration** menu in Prime Infrastructure contains tasks that are typically performed by administrators only.





## Prime Infrastructure Server Settings

---

The following sections contain information about configuring Prime Infrastructure server settings:

- [Available System Settings, page 2-1](#)
- [Configuring Email Settings, page 2-5](#)
- [Configuring Global SNMP Settings, page 2-6](#)
- [Configuring Proxy Settings, page 2-10](#)
- [Configuring Server Settings, page 2-11](#)
- [Configuring TFTP or FTP Servers, page 2-11](#)
- [Specifying Administrator Approval for Jobs, page 2-11](#)
- [Managing OUI, page 2-13](#)
- [Adding Notification Receivers to Prime Infrastructure, page 2-14](#)
- [Setting Up HTTPS Access to the Prime Infrastructure Server, page 2-15](#)
- [MIB to Prime Infrastructure Alert/Event Mapping, page 2-19](#)

### Available System Settings

The **Administration > System Settings** menu contains options to configure or modify Prime Infrastructure settings. You will want to customize many of these settings when you are first implementing Prime Infrastructure, but once in production, modify them only rarely.

[Table 2-1](#) lists the types of settings you can configure or modify from the **Administration > System Settings** menu.

Table 2-1 Available Prime Infrastructure Settings

To do this:	Choose Administration > System Settings > ...	Applicable for:
<ul style="list-style-type: none"> <li>Change which alarms, events, and syslogs are deleted, and how often.</li> <li>Set the alarm types for which email notifications are sent, and how often they are sent.</li> <li>Set the alarm types displayed in the Alarm Summary view.</li> <li>Change the content of alarm notifications sent by email.</li> </ul>	<b>Alarms and Events</b> See <a href="#">Specifying Alarm Clean Up and Display Options</a> , page 5-1.	Wired and wireless devices
Choose whether audit logs are basic or template based and select the device parameters to audit on.	<b>Audit</b> See <a href="#">Setting Up Auditing Configurations</a> , page 5-4.	Wired and wireless devices
Purge syslogs and send the purged logs either to trash or to a remote directory.	<b>Audit Log Purge Settings</b> See <a href="#">Deleting Syslogs from Audit Records</a> , page 5-5.	Not Applicable
Enable Change Audit JMS Notification by selecting the Enable Change Audit JMS Notification check box.	<b>Change Audit Notification</b> See <a href="#">Enabling Change Audit Notifications</a> , page 5-6.	Wired and wireless devices
<ul style="list-style-type: none"> <li>Set the protocol to be used for controller and autonomous AP CLI sessions.</li> <li>Enable autonomous AP migration analysis on discovery.</li> </ul>	<b>CLI Session</b> See <a href="#">Configuring Protocols for CLI Sessions</a> , page 7-2.	Wireless Device
<ul style="list-style-type: none"> <li>Enable automatic troubleshooting of clients on the diagnostic channel.</li> <li>Enable lookup of client hostnames from DNS servers and set how long to cache them.</li> <li>Set how long to retain disassociated clients and their session data.</li> <li>Poll clients to identify their sessions only when a trap or syslog is received.</li> <li>Disable saving of client association and disassociation traps and syslogs as events.</li> <li>Enable saving of client authentication failure traps as events, and how long between failure traps to save them.</li> </ul>	<b>Client</b> See <a href="#">Configuring Client Performance Settings</a> , page 3-6.	Wired and wireless devices
Set basic control parameters used when deploying a device configuration, such as enabling backup of the running configuration, rollbacks, retrieval of <b>show</b> command output from the cache, and the number of CLI thread pools to use.	<b>Configuration</b> See <a href="#">Backing up and Rolling Back Configurations</a> , page 6-6.	Wired and wireless devices
Set basic parameters for the configuration archive, such as protocol, timeout value, number of configuration versions to store, and so forth.	<b>Configuration Archive</b> See <a href="#">Specifying When to Archive Configurations</a> , page 6-6.	Wired and wireless devices



Table 2-1 Available Prime Infrastructure Settings (continued)

To do this:	Choose Administration > System Settings > ...	Applicable for:
Enable auto refresh after a wireless controller upgrade, and process the save configuration trap.	<b>Controller Upgrade Settings</b> See <a href="#">Refreshing Controllers After an Upgrade, page 7-2</a> .	Wireless Device
Enable or disable data deduplication.	<b>Data Deduplication</b> See <a href="#">Enabling Data Deduplication, page 6-4</a> .	Not applicable
Set the retention period for the following data types: Trends, Device Health, Performance, Network Audit, System Health.	<b>Data Retention</b> See <a href="#">Specifying Data Retention Periods, page 6-2</a> .	Wired and wireless devices
Define the device group hierarchy. By default, the hierarchy is as follows: <ul style="list-style-type: none"> <li>• Device Type/Routers</li> <li>• Device Type/Switches and Hubs</li> <li>• Device Type/Routers/Cisco 1000 Voice Series Routers</li> </ul>	<b>Grouping</b>	Wired and wireless devices
Configure the guest account settings to globally remove all the guest accounts whose lifetime has ended. By default, Prime Infrastructure Lobby Ambassador can access all guest accounts irrespective of who created them. If you select the <b>Search and List only guest accounts created by this lobby ambassador</b> check box, the Lobby Ambassadors can access only the guest accounts that have been created by them.	<b>Guest Account Settings</b> See <a href="#">Configuring Guest Account Settings, page 9-3</a> .	Wireless devices
Configure global preference parameters for downloading, distributing, and recommending software Images.	<b>Image Management</b> See the <a href="#">Cisco Prime Infrastructure 2.0 User Guide</a> for information about Image Management.	Wired and wireless devices
Enable inventory collection to allow Prime Infrastructure to collect inventory when it receives a syslog even for a device.	<b>Inventory</b> See <a href="#">Specifying Inventory Collection After Receiving Events, page 6-5</a> .	Wired and wireless devices
Enable job approval to specify the jobs which require administrator approval before the job can run.	<b>Job Approval Settings</b> See <a href="#">Specifying Administrator Approval for Jobs, page 2-11</a> .	Wired and wireless devices
View, add, or delete the Ethernet MAC address available in Prime Infrastructure. if you add multiple Ethernet MAC addresses to this list, then Auto Switch Port Tracing will not scan these ports for Rogue AP.	<b>Known Ethernet MAC Address</b> See <a href="#">Configuring Email Settings, page 2-5</a> .	Not applicable
Change the disclaimer text displayed at the bottom of the login page for all users.	<b>Login disclaimer</b> See <a href="#">Specifying Login Disclaimer Text, page 2-12</a> .	Not Applicable
Enable email distribution of reports and alarm notifications.	<b>Mail server configuration</b> See <a href="#">Configuring Email Settings, page 2-5</a> .	Not Applicable

Table 2-1 Available Prime Infrastructure Settings (continued)

To do this:	Choose Administration > System Settings > ...	Applicable for:
<p>Configure remote event and alarm receivers who will receive notifications from Prime Infrastructure.</p> <p>Alerts and events are sent as SNMPv2 notifications to configured notification receivers. If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is configured. By default, only INFO level events are processed for the selected category. Only SNMPV2 traps are considered for northbound notification.</p>	<p><b>Notification receivers</b></p> <p>See <a href="#">Adding Notification Receivers to Prime Infrastructure, page 2-14</a>.</p>	<p>Wired and wireless devices</p>
<p>Modify the settings for Plug and Play.</p>	<p><b>Plug &amp; Play</b></p>	<p>Wired device</p>
<p>Configure proxies for the Prime Infrastructure server and its local authentication server.</p>	<p><b>Proxy Settings</b></p> <p>See <a href="#">Configuring Proxy Settings, page 2-10</a>.</p>	<p>Not Applicable</p>
<p>Set the path where scheduled reports are stored and how long reports are retained.</p>	<p><b>Report</b></p> <p>See <a href="#">Specifying Where and for How Long to Save Reports, page 6-4</a>.</p>	<p>Wired and wireless devices</p>
<p>Configure rogue AP settings to enable Prime Infrastructure to automatically track the switch port to which the rogue access point is connected in the network.</p>	<p><b>Rogue AP Settings</b></p> <p>See <a href="#">Configuring SNMP Credentials for Rogue AP Tracing, page 7-1</a>.</p>	<p>Wireless device</p>
<p>Configure the FTP, TFTP, HTTP, HTTPS, NTP servers, and Compliance Service used.</p>	<p><b>Server Settings</b></p> <p>See <a href="#">Configuring Server Settings, page 2-11</a>.</p>	<p>Not applicable</p>
<p>Enable the server tuning when you restart the Prime Infrastructure server. The server tuning optimizes the performance of the server by limiting the number of resources the server uses to process client requests.</p>	<p><b>Server Tuning</b></p> <p>See <a href="#">Configuring Client Performance Settings, page 3-6</a>.</p>	<p>Wired and wireless devices</p>
<p>Configure the Cisco WAAS Central Manager IP address in Cisco Prime Infrastructure.</p>	<p><b>Service Container Management</b></p> <p>See <a href="#">Cisco WAAS Central Manager Integration</a>.</p>	<p>Wired device</p>
<p>Set the severity level of any generated alarm.</p>	<p><b>Severity Configuration</b></p> <p>See <a href="#">Changing Alarm Severities, page 5-3</a>.</p>	<p>Wired and wireless devices</p>
<p>Set the SNMP credentials and trace parameters to be used in tracing rogue AP switch ports.</p>	<p><b>SNMP Credentials</b></p> <p>See <a href="#">Configuring SNMP Credentials for Rogue AP Tracing, page 7-1</a>.</p>	<p>Wireless device</p>

Table 2-1 Available Prime Infrastructure Settings (continued)

To do this:	Choose Administration > System Settings > ...	Applicable for:
<p>Set global SNMP polling parameters, including trace display values, reachability parameters and the backoff algorithm.</p> <p><b>Note</b> If you select Exponential (the default value) for the Backoff Algorithm, each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time. If you select to use reachability parameters, the Prime Infrastructure defaults to the global Reachability Retries and Timeout that you configure. If unchecked, Prime Infrastructure always uses the timeout and retries specified.</p>	<p><b>SNMP Settings</b></p> <p>See <a href="#">Configuring Global SNMP Settings, page 2-6</a>.</p>	Wireless device
Configure the settings for creating a technical support request.	<p><b>Support Request Settings</b></p> <p>See <a href="#">Configuring Technical Support Request Settings, page 5-11</a>.</p>	Wired and wireless devices
Set basic and advanced switch port trace parameters.	<p><b>Switch Port Trace</b></p> <p>See <a href="#">Configuring Switch Port Tracing, page 7-4</a>.</p>	Wired device
Add a vendor Organizationally Unique Identifier (OUI) mapping and upload an updated vendor OUI mapping XML file.	<p><b>User Defined OUI</b></p> <p><b>Upload OUI</b></p> <p>See <a href="#">Managing OUI, page 2-13</a>.</p>	Wired and wireless devices
Store additional information about a device.	<p><b>User Defined Field</b></p> <p>See <a href="#">Adding Device Information to a User Defined Field, page 2-12</a>.</p>	Wired device

## Configuring Email Settings

You can configure global email parameters for sending emails from Prime Infrastructure reports, alarm notifications, and so on. This mail server page enables you to configure email parameters in one place. The Mail Server page enables you to set the primary and secondary SMTP server host and port, the email address of the sender, and the email addresses of the recipient.

### Before You Begin

You must configure the global SMTP server before setting global email parameters.

To configure global email parameters:

- 
- Step 1** Choose **Administration > System Settings > Mail Server Configuration**. The Mail Server Configuration page appears.
  - Step 2** Enter the hostname of the primary SMTP server.
  - Step 3** Enter the username of the SMTP server.

**Step 4** Provide a password for logging on to the SMTP server and confirm it.



**Note** Both username and password are optional.

**Step 5** Provide the same information for the secondary SMTP server (only if a secondary mail server is available).

**Step 6** The From text box in the Sender and Receivers portion of the page is populated with *PI@Hostname.domainName*. You can change it to a different sender.

**Step 7** Enter the email addresses of the recipient in the To text box. The email address you provide serves as the default value for other functional areas, such as alarms or reports. Multiple email addresses can be added and should be separated by commas.



**Note** Global changes you make to the recipient email addresses in Step 7 are disregarded if email notifications were set.

You must indicate the primary SMTP mail server and complete the From address text boxes.

If you want all alarm categories applied to the provided recipient list, select the **Apply recipient list to all alarm categories** check box.

**Step 8** Enter the text that you want to append to the email subject.

**Step 9** (Optional) Click the Configure email notification for individual alarm categories link, you can specify the alarm categories and severity levels you want to enable. email notifications are sent when an alarm occurs that matches categories and the severity levels you select.



**Note** You can set each alarm severity by clicking the alarm category, choosing Critical, Major, Minor, or Warning, and providing an email address.

**Step 10** Click the **Test** button to send a test email using the parameters you configured. The results of the test operation appear on the same page. The test feature checks the connectivity to both primary and secondary mail servers by sending an email with a “Prime Infrastructure test email” subject line.

If the test results are satisfactory, click **Save**.

## Configuring Global SNMP Settings

The SNMP Settings page allows you to configure global SNMP settings from Prime Infrastructure.

Any changes you make on this page affect Prime Infrastructure globally. The changes are saved across restarts as well as across backups and restores.



**Note** The default network address is 0.0.0.0, which indicates the entire network. An SNMP credential is defined per network so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. The default community string is *private* for both read and write. You should update the prepopulated SNMP credential with your own SNMP information.

To configure global SNMP settings:

---

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

**Step 2** From the left sidebar menu, choose **SNMP Settings**. The SNMP Settings page appears.

**Step 3** (Optional) Select the Trace Display Values check box to display mediation trace-level logging data values fetched from the controller using SNMP. If unselected, the values do not appear.



---

**Note** The default is unselected for security reasons.

---

**Step 4** For the Backoff Algorithm, choose either **Exponential** or **Constant Timeout** from the drop-down list. If you choose Exponential (the default value), each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time.



---

**Note** Constant Timeout is useful on unreliable networks (such as satellite networks) where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.

---

**Step 5** Determine if you want to use reachability parameters. If selected, Prime Infrastructure defaults to the global Reachability Retries and Timeout that you configure. If unselected, Prime Infrastructure always uses the timeout and retries specified per-controller or per-IOS access point. The default is selected.



---

**Note** Adjust this setting downward if switch port tracing is taking a long time to complete.

---

**Step 6** For the Reachability Retries field, enter the number of global retries used for determining device reachability. The default number is 2. This field is only available if the Use Reachability Parameters check box is selected.



---

**Note** Adjust this setting downward if switch port tracing is taking a long time to complete.

---

**Step 7** For the Reachability Timeout field, enter a global timeout used for determining device reachability. The default number is 2. This field is only available if the Use Reachability Parameters check box is selected.

**Step 8** At the Maximum VarBinds per PDU field, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. The default for the Maximum VarBinds per Get PDU field is 30 and the Maximum VarBinds per Set PDU field is 50.



---

**Note** For customers who have issues with PDU fragmentation in their network, this number can be reduced to 50, which typically eliminates the fragmentation.

---

The maximum rows per table field is configurable and the default value is 200000 rows. The configured value is retained even if you upgrade Prime Infrastructure to a newer version.

**Step 9** Click **Save** to confirm these settings.

---

## Viewing SNMP Credential Details

The SNMP credentials listed in this page will be used only for tracing the Rogue APs Switch Port.

To view or edit details for current SNMP credentials:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **SNMP Credentials**.
  - Step 3** Click the Network Address link to open the SNMP Credential Details page. The details page displays the following information:

General Parameters

- Add Format Type—Display only. See the [“Adding a New SNMP Credential Entry” section on page 2-9](#) for more information regarding Add Format Type.
- Network Address
- Network Mask

SNMP Parameters—Choose the applicable version(s) for SNMP parameters. The SNMP credentials are validated according to which SNMP version(s) are selected.




---

**Note** Enter SNMP parameters for write access, if available. With display-only access parameters, the switch is added but you cannot modify its configuration in Prime Infrastructure. Device connectivity tests use the SNMP retries and timeout parameters configured in Administration > Settings > SNMP Settings.

---

- Retries—The number of times that attempts are made to discover the switch.
- Timeout—The session timeout value in seconds, which specifies the maximum amount of time allowed for a client before it is forced to reauthenticate.
- SNMP v1 Parameters or v2 Parameters—If selected, enter the applicable community in the available text box.
- SNMP v3 Parameters—If selected, configure the following parameters:
  - Username
  - Auth. Type
  - Auth. Password
  - Privacy Type
  - Privacy Password




---

**Note** If SNMP v1 or v2 with default community is configured, the network is open to easy attacks because default communities are well known. SNMP v1 or v2 with a non default community is more secure than a default community, but SNMP v3 with Auth and Privacy type and no default user is the most secure SNMP connection.

---

- Step 4** Click **OK** to save changes or **Cancel** to return to the SNMP Credentials page without making any changes to the SNMP credential details.
-

## Adding a New SNMP Credential Entry

To add a new SNMP credential entry:

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **SNMP Credentials**.
- Step 3** Choose **Add SNMP Entries** from the **Select a command** drop-down list, then click **Go**.
- Step 4** Choose one of the following:
- To manually enter SNMP credential information, leave the Add Format Type drop-down list at SNMP Credential Info. To add multiple network addresses, use a comma between each address. Go to [Step 6](#).
- If you want to add multiple switches by importing a CSV file, choose **File** from the Add Format Type drop-down list. The CSV file allows you to generate your own import file and add the devices you want. Go to [Step 5](#).
- Step 5** If you chose File, click **Browse** to find the location of the CSV file you want to import. Skip to [Step 10](#).
- The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory.
- Sample File:
- ```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_password,snmpv3_privacy_type,snmpv3_privacy_password,network_mask
1.1.1.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
2.2.2.0,v2,private,user1,HMAC-MD5,password3,DES,password4,255.255.255.0
10.77.246.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
```
- The CSV file can contain the following fields:
- ip\_address:IP address
  - snmp\_version:SNMP version
  - network\_mask:Network mask
  - snmp\_community:SNMP V1/V2 community
  - snmpv3\_user\_name:SNMP V3 username
  - snmpv3\_auth\_type:SNMP V3 authorization type. Can be None or HMAC-MD5 or HMAC-SHA
  - snmpv3\_auth\_password:SNMP V3 authorization password
  - snmpv3\_privacy\_type:SNMP V3 privacy type. Can be None or DES or CFB-AES-128
  - snmpv3\_privacy\_password:SNMP V3 privacy password
  - snmp\_retries:SNMP retries
  - snmp\_timeout:SNMP timeout
- Step 6** If you chose SNMP Credential Info, enter the IP address of the switch you want to add. If you want to add multiple switches, use a comma between the string of IP addresses.
- Step 7** In the Retries field, enter the number of times that attempts are made to discover the switch.
- Step 8** Provide the session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.
- Step 9** Choose the applicable versions for the SNMP parameters. The SNMP credentials are validated according to which SNMP versions are selected.

- If SNMP v1 Parameters or v2 Parameters is selected, enter the applicable community in the available text box.
- If SNMP v3 Parameters is selected, configure the following parameters:
  - Username
  - Auth. Type
  - Auth. Password
  - Privacy Type
  - Privacy Password




---

**Note** If SNMP v1 or v2 with default community is configured, the network is open to easy attacks because default communities are well known. SNMP v1 or v2 with a non-default community is more secure than a default community, but SNMP v3 with Auth and Privacy type and no default user is the most secure SNMP connection.

---

**Step 10** Click **OK**.

If Prime Infrastructure can use the SNMP credential listed to access the switch, the switch is added for later use and appears in the Configure > Ethernet Switches page.



**Note**

---

If you manually added switches through the Configure > Ethernet Switches page, then switch port tracing uses the credentials from that page, not the ones listed in the SNMP Credentials page. If the manually added switch credentials have changed, you need to update them from the Configure > Ethernet page.

---

## Configuring Proxy Settings

The Proxy Settings page allows you configure proxies for the Prime Infrastructure server and its local authentication server. If you use a proxy server as a security barrier between your network and the Internet, you need to configure the proxy settings as shown in the following steps:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Proxy Settings**. The Proxy Settings page appears.
  - Step 3** Select the **Enable Proxy** check box to allow proxy settings for the Prime Infrastructure server.
  - Step 4** Enter the required information and click **Save**.
-



## Configuring Server Settings

The Server Settings page allows you to enable or disable the TFTP, FTP, HTTP, HTTPS, or Compliance Service. To turn the server settings on or off:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Server Setting**.
  - Step 3** If you want to modify the FTP and TFTP directories or the HTTP and HTTPS ports that were established during installation, enter the port number (or port number and root where required) that you want to modify and click **Enable** or **Disable**.

The changes are reflected after a restart.



- 
- Note** After you enable the compliance service and restart the server, you must synchronize inventory to generate the PSIRT and EOX reports.
- 

## Configuring TFTP or FTP Servers

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

## Specifying Administrator Approval for Jobs

You might want to control which jobs (for example, configuration overwrite jobs) must be approved by an administrator before they can run. When an administrator rejects an approval request for a job, the job is removed from the Prime Infrastructure database.

By default, job approval is disabled on all job types.

To specify which jobs require administrator approval before the job can run:

- 
- Step 1** Choose **Administration > System Settings > Job Approval Settings**.
  - Step 2** Select the **Enable Job Approval** check box
  - Step 3** From the list of job types, use the arrows to move any jobs for which you want to enable job approval to the list in the right. By default, job approval is disabled so all jobs appear in the list on the left.

- Step 4** To specify a customized job type, enter a string using regular expressions in the Job Type field, then click **Add**. For example, to enable job approval for all job types that start with Config, enter *Config.\**
- Step 5** Click **Save**.
- 

## Approving Jobs

If you have previously specified that a job must be approved by an administrator (see [Specifying Administrator Approval for Jobs, page 2-11](#)) before the job can run, the administrator must approve the job.

Choose **Administration > Jobs Approval** to:

- View the list of jobs that need approval.
- Approve any listed jobs—After an administrator approves a job, the job is enabled and runs per the schedule specified in the job.
- Reject the approval request for any listed jobs—After an administrator rejects a job, the job is deleted from the Prime Infrastructure database.

## Specifying Login Disclaimer Text

The Login Disclaimer page allows you to enter disclaimer text at the top of the Prime Infrastructure Login page for all users.

To enter login disclaimer text:

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Login Disclaimer**.
- Step 3** Enter your login disclaimer text in the available text box, then click **Save**.
- 

## Adding Device Information to a User Defined Field

The User Defined Fields (UDFs) are used to store the additional information about a device such as device location attributes, for example area, facility, floor, etc. UDF attributes are used whenever a new device is added, imported or exported using **Operate > Device Work Center**.

To add a UDF:

- 
- Step 1** Choose **Administration > System Settings > User Defined Field**.
- Step 2** Click **Add Row** to add a UDF.
- Step 3** Enter the field label and description in the corresponding fields.
- Step 4** Click **Save** to add a UDF.
-

# Managing OUI

Prime Infrastructure relies on the IEEE Organizational Unique Identifier (OUI) database to identify the client vendor name mapping. Prime Infrastructure stores vendor OUI mappings in an XML file named vendorMacs.xml. This file is updated for each release of Prime Infrastructure. With the OUI update, you can perform the following:

- Change the vendor display name for an existing OUI.
- Add new OUIs to Prime Infrastructure.
- Refresh the vendorMacs.xml file with new vendor OUI mappings and upload it to Prime Infrastructure.

This section contains the following topics:

- [Adding a New Vendor OUI Mapping, page 2-13](#)
- [Uploading an Updated Vendor OUI Mapping File, page 2-13](#)

## Adding a New Vendor OUI Mapping

The User Defined OUI List page displays a list of vendor OUI mappings that you created. This page allows you to add a new vendor OUI mapping, delete an OUI entry, and update the vendor name for an OUI that is existing in the vendorMacs.xml file.

When you add an OUI, Prime Infrastructure verifies the vendorMacs.xml file to see if the OUI exists. If the OUI exists, Prime Infrastructure updates the vendor name for the OUI. If the OUI does not exist, Prime Infrastructure adds a new OUI entry to the vendor OUI mapping.

To add a new vendor OUI mapping:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **User Defined OUI**. The User Defined OUI page appears.
  - Step 3** Choose **Add OUI Entries** from the **Select a Command** drop-down list, then click **Go**.
  - Step 4** In the OUI field, enter a valid OUI. The format is aa:bb:cc.
  - Step 5** Click **Check** to verify if the OUI exists in the vendor OUI mapping.
  - Step 6** In the Name field, enter the display name of the vendor for the OUI.
  - Step 7** Select the **Change Vendor Name** check box to update the display name of the vendor, if the OUI exists in the vendor OUI mapping, then click **OK**.
- 

## Uploading an Updated Vendor OUI Mapping File

The updated vendorMacs.xml file is posted on cisco.com, periodically. You can download and save the file to a local directory using the same filename, vendorMacs.xml. You can then, upload the file to Prime Infrastructure. Prime Infrastructure replaces the existing vendorMacs.xml file with the updated file and refreshes the vendor OUI mapping. However, it does not override the new vendor OUI mapping or the vendor name update that you made.

To upload the updated vendor OUI mapping file:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Upload OUI**. The Upload OUI From File page appears.
  - Step 3** Browse and select the vendorMacs.xml file that you downloaded from Cisco.com, then click **OK**.
- 

## Adding Notification Receivers to Prime Infrastructure

The Notification Receiver page displays current notification receivers that support guest access. Alerts and events are sent as SNMPv2 notifications to configured notification receivers. You can view current or add additional notification receivers.

To access the Notification Receiver page:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear in this page.
  - Step 3** Choose **Add Notification Receiver** from the **Select a command** drop-down list, then click **Go**.
  - Step 4** Enter the server IP address and name.
  - Step 5** Click either the **North Bound** or **Guest Access** radio button.  
The Notification Type automatically defaults to UDP.
  - Step 6** Enter the UDP parameters including Port Number and Community. The receiver that you configure should be listening to UDP on the same port that is configured.
  - Step 7** If you selected North Bound as the receiver type, specify the criteria and severity. Alarms for the selected category only are processed. Alarms with the selected severity matching the selected categories are processed.
  - Step 8** Click **Save** to confirm the Notification Receiver information.  
By default, only INFO level events are processed for the selected Category.  
Only SNMPV2 traps are considered for North Bound notification.
- 

## Removing a Notification Receiver

To delete a notification receiver:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear on this page.
  - Step 3** Select the check boxes of the notification receivers that you want to delete.
  - Step 4** Choose **Remove Notification Receiver** from the **Select a command** drop-down list, then click **Go**.

**Step 5** Click **OK** to confirm the deletion.

### Sample Log File from North Bound SNMP Receiver

The following sample output shows the `ncs_nb.log` file generated by Prime Infrastructure. This log file is located in the log file directory on Prime Infrastructure server (`/opt/CSColumos/logs`). The log output helps you troubleshoot when alarms are not being received by the North Bound SNMP receiver.

```
2013-12-02 17:11:53,868 [main] INFO services - Queue type is order
2013-12-02 17:11:53,870 [main] INFO services - Starting the notification thread..
2013-12-02 17:11:53,871 [NBNotifier] INFO services - Fetching the head of the queue
2013-12-02 17:11:53,871 [NBNotifier] INFO services - The Queue is empty
2013-12-02 17:11:53,871 [main] INFO notification - Setting the NB process flag
2013-12-02 17:41:50,839 [Task Scheduler Worker-10] ERROR notification - Unable to get OSS
list
2013-12-03 08:22:39,227 [main] INFO services - Queue type is order
2013-12-03 08:22:39,229 [main] INFO services - Starting the notification thread..
2013-12-03 08:22:39,231 [NBNotifier] INFO services - Fetching the head of the queue
2013-12-03 08:22:39,231 [NBNotifier] INFO services - The Queue is empty
2013-12-03 08:22:39,231 [main] INFO notification - Setting the NB process flag
2013-12-03 08:44:40,287 [main] INFO services - Queue type is order
2013-12-03 08:44:40,289 [main] INFO services - Starting the notification thread..
2013-12-03 08:44:40,290 [NBNotifier] INFO services - Fetching the head of the queue
2013-12-03 08:44:40,290 [NBNotifier] INFO services - The Queue is empty
2013-12-03 08:44:40,290 [main] INFO notification - Setting the NB process flag
2013-12-03 08:56:18,864 [Task Scheduler Worker-8] ERROR notification - Unable to get OSS
list
```

## Setting Up HTTPS Access to the Prime Infrastructure Server

The Prime Infrastructure server can support secure HTTPS client access. Certificates can be self-signed or can be attested by a digital signature from a certificate authority (CA). Certificate Authorities are entities that validate identities and issue certificates. The certificate issued by the CA binds a particular public key to the name of the entity that the certificate identifies, such as the name of a server or device. Only the public key that the certificate certifies works with the corresponding private key possessed by the entity that the certificate identifies.

To view an existing SSL certificate for the Prime Infrastructure server, you must

- 
- Step 1** Log in to the CLI of Prime Infrastructure server as root user.
- Step 2** Change to the `/opt/CSColumos` directory and enter the following command:
- ```
jre/bin/keytool -list -alias tomcat -keystore conf/keystore -storepass changeit -v
```
- The existing SSL Certificate details are displayed.
- Step 3** To view the list of CA Certificates that exist in the Prime Infrastructure trust store, enter the following command in Prime Infrastructure admin mode:
- ```
ncs key listcacerts
```

## Generating a Self-Signed Certificate in Prime Infrastructure

To generate a self-signed SSL certificate in Prime Infrastructure:

---

**Step 1** Log in to the CLI of the Prime Infrastructure server in admin mode.

**Step 2** Enter the following command in the admin prompt (admin #):

**ncs key genkey –newdn**

A new RSA key and self-signed certificate with domain information is generated. You are prompted for the distinguished name fields for the certificate. It is important to specify the fully qualified domain name (FQDN) of the server as the domain name that will be used to access Prime Infrastructure.

**Step 3** To make the certificate valid, restart the Prime Infrastructure processes by issuing the following commands in this order:

- **ncs stop**

- **ncs start**

---

## Generating a Certificate Signing Request (CSR) File

An SSL certificate can also be obtained from a third party. To set up this support, you must:

1. Generate a Certificate Signing Request file.
2. Submit the signing request to a Certificate Authority you choose.
3. Apply the signed Security Certificate file to the server.

---

**Step 1** Generate a Certificate Signing Request (CSR) file for the Prime Infrastructure server:

- a. At the Prime Infrastructure appliance, exit to the command line.
- b. At the command line, log in using the administrator ID and password used to install Prime Infrastructure.
- c. Enter the following command to generate the CSR file in the default backup repository:

- **ncs key genkey -newdn -csr *CertName.csr* repository *RepoName***

where:

- *CertName* is an arbitrary name of your choice (for example: **MyCertificate.csr**).
- *RepoName* is any previously configured backup repository (for example: **defaultRepo**).

**Step 2** Copy the CSR file to a location you can access. For example:

**copy disk:/RepoName/CertName.csr ftp://your.ftp.server.**

**Step 3** Send the CSR file to a Certificate Authority (CA) of your choice.



**Note**

---

Once you have generated and sent the CSR file for certification, do *not* use the **genkey** command again to generate a new key on the same Prime Infrastructure server. If you do, importing the signed certificate file will result in mismatches between keys in the file and on the server.

---

- Step 4** You will receive a signed certificate file with the same filename, but with the file extension CER, from the CA. Before continuing, ensure:
- There is only one CER file. In some cases, you may receive chain certificates as individual files. If so, concatenate these files into a single CER file.
  - Any blank lines in the CER file are removed.
- Step 5** At the command line, copy the CER file to the backup repository. For example:
- **copy ftp://your.ftp.server/CertName.cer disk:RepoName**
- Step 6** Import the CER file into the Prime Infrastructure server using the following command:
- **ncs key importsignedcert CertName.cer repository RepoName**
- Step 7** Restart the Prime Infrastructure server by issuing the following commands in this order:
- **ncs stop**
  - **ncs start**
- Step 8** If the Certificate Authority who signed the certificate is not already a trusted CA: Instruct users to add the certificate to their browser trust store when accessing the Prime Infrastructure login page.
- 

## Importing a Certificate Authority (CA) Certificate and Key

To import a CA certificate to a trust store in Prime Infrastructure:

- Step 1** At the command line, log in using the administrator ID and password and enter the following command:
- ```
ncs key importcert aliasname ca-cert-filename repository repositoryname
```
- where
- *aliasname* is a short name given for this CA certificate.
  - *ca-cert-filename* is the CA certificate file name.
  - *repositoryname* is the repository name configured in Prime Infrastructure where the ca-cert-filename is hosted.
- Step 2** To import an RSA key and signed certificate to Prime Infrastructure, enter the following command in admin mode:
- ```
ncs key importkey key-filename cert-filename repository repositoryname
```
- where
- *key-filename* is the RSA private key file name.
  - *cert-filename* is the certificate file name.
  - *repositoryname* is the repository name configured in Prime Infrastructure where the key-file and cert-file are hosted.
- Step 3** Restart the Prime Infrastructure server by issuing the following commands in this order:
- **ncs stop**
  - **ncs start**
-

## Deleting a CA Certificate

To delete a CA certificate from Prime Infrastructure, at the command line, log in using the administrator ID and password and enter the following command

```
ncs key deletecacert <aliasname>
```

where *aliasname* is the short name of the CA certificate, which you can obtain by issuing the command **ncs key listcacert**.



# MIB to Prime Infrastructure Alert/Event Mapping

Table 2-2 summarizes the Cisco-Prime Infrastructure-Notification-MIB to Prime Infrastructure alert/event mapping.

**Table 2-2 Cisco-Prime Infrastructure-Notification-MIB to Prime Infrastructure Alert/Event Mapping**

| Field Name and Object ID       | Data Type                     | Prime Infrastructure Event/Alert field         | Description                                                                                                                                                                                                                                                                                 |
|--------------------------------|-------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cWNotificationTimestamp        | DateAndTime                   | createTime - NmsAlert<br>eventTime - NmsEvent  | Creation time for alarm/event.                                                                                                                                                                                                                                                              |
| cWNotificationUpdatedTimestamp | DateAndTime                   | modTime - NmsAlert                             | Modification time for Alarm.<br>Events do not have modification time.                                                                                                                                                                                                                       |
| cWNotificationKey              | SnmpAdminString               | objectId - NmsEvent<br>entityString- NmsAlert  | Unique alarm/event ID in string form.                                                                                                                                                                                                                                                       |
| cWNotificationCategory         | CWirelessNotificationCategory | NA                                             | Category of the Events/Alarms.<br>Possible values are:<br>unknown<br>accessPoints<br>adhocRogue<br>clients<br>controllers<br>coverageHole<br>interference<br>contextAwareNotifications<br>meshLinks<br>mobilityService<br>performance<br>rogueAP<br>rrm<br>security<br>wcs<br>switch<br>ncs |
| cWNotificationSubCategory      | OCTET STRING                  | Type field in alert and<br>eventType in event. | This object represents the subcategory of the alert.                                                                                                                                                                                                                                        |
| cWNotificationServerAddress    | InetAddress                   | N/A                                            | Prime Infrastructure IP address.                                                                                                                                                                                                                                                            |

Table 2-2 Cisco-Prime Infrastructure-Notification-MIB to Prime Infrastructure Alert/Event Mapping (continued)

| Field Name and Object ID               | Data Type       | Prime Infrastructure Event/Alert field                                     | Description                                                                                                                                                                                                                                 |
|----------------------------------------|-----------------|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cWNotificationManagedObjectAddressType | InetAddressType | N/A                                                                        | The type of Internet address by which the managed object is reachable.<br>Possible values:<br>0—unknown<br>1—IPv4<br>2—IPv6<br>3—IPv4z<br>4—IPv6z<br>16—DNS<br>Always set to “1” because Prime Infrastructure only supports IPv4 addresses. |
| cWNotificationManagedObjectAddress     | InetAddress     | getNode() value is used if present                                         | getNode is populated for events and some alerts. If it is not null, then it is used for this field.                                                                                                                                         |
| cWNotificationSourceDisplayName        | OCTET STRING    | sourceDisplayName field in alert/event.                                    | This object represents the display name of the source of the notification.                                                                                                                                                                  |
| cWNotificationDescription              | OCTET STRING    | Text - NmsEvent<br>Message - NmsAlert                                      | Alarm description string.                                                                                                                                                                                                                   |
| cWNotificationSeverity                 | INTEGER         | severity - NmsEvent,<br>NmsAlert                                           | Severity of the alert/event:<br>critical(1)<br>major(2)<br>minor(3)<br>warning(4)<br>clear(5)<br>info(6)<br>unknown(7)                                                                                                                      |
| cWNotificationSpecialAttributes        | OCTET STRING    | All the attributes in alerts/events apart from the base alert/event class. | This object represents the specialized attributes in alerts like APAssociated, APDisassociated, RogueAPAlert, CoverageHoleAlert, and so on. The string is formatted in property=value pairs in CSV format.                                  |
| cWNotificationVirtualDomains           | OCTET STRING    | N/A                                                                        | Virtual Domain of the object that caused the alarm. This field empty for the current release.                                                                                                                                               |



# Maintaining Prime Infrastructure Server Health

This section contains the following topics:

- [Monitoring Prime Infrastructure Health, page 3-1](#)
- [Troubleshooting Prime Infrastructure, page 3-2](#)
- [Evaluating OVA Size and System Resources, page 3-3](#)
- [Improving Prime Infrastructure Performance, page 3-4](#)
- [Checking the Status of Prime Infrastructure Using CLI, page 3-8](#)
- [Recovering Prime Infrastructure Passwords, page 3-8](#)
- [Downloading Device Support and Product Updates, page 3-9](#)
- [Configuring Support Request Settings, page 3-10](#)
- [Stopping Prime Infrastructure, page 3-11](#)
- [Removing Prime Infrastructure, page 3-11](#)

## Monitoring Prime Infrastructure Health

To view the system health dashboards, choose **Administration > Admin Dashboard**. [Table 3-1](#) describes the information displayed on the dashboards.

**Table 3-1 Administration > Admin Dashboard Information**

| To view this information...                                                                                                                                                                                                                                                       | Select this tab... | And see this dashlet  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------|
| Prime Infrastructure server memory and CPU statistics over time.                                                                                                                                                                                                                  | Health             | System Health         |
| Alarms and events issued against the Prime Infrastructure server itself, including a list of events, times events occurred, and their severities.                                                                                                                                 |                    | System Alarms         |
| General health statistics for the Prime Infrastructure server, such as the number of jobs scheduled and running, the number of supported MIB variables, how much polling the server is doing, and the number of users logged in.                                                  |                    | System Information    |
| The relative proportion of the Prime Infrastructure server database taken up by data on discovered device inventory (“Lifecycle Clients”), their current status and performance data (“Lifecycle Statistics”), and the server’s own system data (“Infrastructure” and “DB-Index”) |                    | DB Usage Distribution |

Table 3-1 Administration &gt; Admin Dashboard Information (continued)

| To view this information...                                                                                                                                                                                                                                     | Select this tab... | And see this dashlet       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------|
| How quickly the Prime Infrastructure server is responding to user service requests for information, such as device reachability, alarms and events, and so on. Shows the maximum, minimum, and average response times for each API underlying a client service. | API Health         | API Response Time Summary  |
| The trend over time in how quickly the Prime Infrastructure server is responding to user service requests.                                                                                                                                                      | Service Details    | API Response Time Trend    |
| The activity level for each of the logged-in Prime Infrastructure users, measured by the number of service requests each is generating.                                                                                                                         |                    | API Calls Per Client Chart |
| The trend over time in the total number of service requests logged-in clients are generating,                                                                                                                                                                   |                    | API Request Count Trend    |

## Troubleshooting Prime Infrastructure

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 3-2](#).
- Open a support case with Cisco Technical Support. See [Opening a Support Case, page 3-3](#).

## 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 one of the following:
- **Operate > Alarms & Events**, click on an alarm, then choose **Troubleshoot > Support Forum**.
  - From the device 360° view (rest your cursor on a device IP address, then click the icon that appears), click the Support Community icon. See “Getting Device Details from the Device 360° View” in the [Cisco Prime Infrastructure 2.0 User Guide](#).
- Step 2** On 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**

Choose one of the following:

- **Operate > Alarms & Events**, click on an alarm, then choose **Troubleshoot > Support Case**.
- From the device 360° view (rest your cursor on a device IP address, then click the icon that appears), click the Support Request icon. See “Getting Device Details from the Device 360° View” in the [Cisco Prime Infrastructure 2.0 User Guide](#).

**Step 2**

Enter your Cisco.com username and password.

**Step 3**

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 4**

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 5**

Click **Create Service Request**.

## Evaluating OVA Size and System Resources

Your Prime Infrastructure system implementation should match the recommendations on appropriate OVA sizes given in the [System Requirements](#) section of the *Cisco Prime Infrastructure 2.0 Quick Start Guide*.

Note that the device, interface, and flow record recommendations given in the *Quick Start Guide* are all maximums; an OVA of a given size has been tuned to handle *no more than* this number of devices, interfaces, and flows per second. Also note that the system requirements for RAM, disk space, and processors are all minimums; you can increase any of these resources and either store more data for a longer period, or process incoming flows more quickly.

As your network grows, you will approach the maximum device/interface/flow rating for your OVA. You will want to check on this from time to time. You can do so using the information available to you on the Admin dashboards, as explained in [Monitoring Prime Infrastructure Health, page 3-1](#)

If you find Prime Infrastructure is using 80 percent or more of your system resources or the device/interface/flow counts recommended for the size of OVA you have installed, we recommend that you address this using one or more of the following approaches, as appropriate for your needs:

- Recover as much existing disk space as you can, following the instructions in [Compacting the Prime Infrastructure Database, page 3-6](#).
- Add more disk space—VMWare OVA technology enables you to easily add disk space to an existing server. You will need to shut down the Prime Infrastructure server and then follow the [instructions VMWare provides](#) on expanding physical disk space. You will need to add a new disk; you cannot extend the size of the existing disk. Once you restart the virtual appliance, Prime Infrastructure automatically makes use of the additional disk space.
- Limit collection—Not all data that Prime Infrastructure is capable of collecting will be of interest to you. For example, if you are not using the system to report on wireless radio performance statistics, you need not collect or retain that data, and can disable the Radio Performance collection task. Alternatively, you may decide that you need only the aggregated Radio Performance data, and can disable retention of raw performance data. For details on how to do this, see [Specifying Data Retention Periods, page 6-2](#).
- Shorten retention—Prime Infrastructure defaults set generous retention periods for all of the data it persists and for the reports it generates. You may find that some of these periods exceed your needs, and that you can reduce them without negative effects. For details on this approach, see [Controlling Report Storage and Cleanup, page 6-5](#) and [Specifying Data Retention Periods, page 6-2](#).
- Off load backups and reports—You can save space on the Prime Infrastructure server by saving reports and backups to a remote server. For details, see [Using Remote Backup Repositories, page 4-5](#).
- Migrate to a new server—Set up a new server that meets at least the minimum RAM, disk space, and processor requirements of the next higher level of OVA. Back up your existing system, then restore it to a VM on the higher-rated server. For details, see [Restoring From Application Backups, page 4-7](#).

## Viewing the Number of Devices Prime Infrastructure Is Managing

To check the total number of devices and interfaces that Prime Infrastructure is managing, choose **Administration > Licenses**.

To check the total system disk space usage, choose **Administration > Appliance**, then click the **Appliance Status** tab and click **Disk Usage**.

## Improving Prime Infrastructure Performance

You can improve Prime Infrastructure's speed and scalability by making a variety of changes:

- [Tuning the Server, page 3-5](#)
- [Compacting the Prime Infrastructure Database, page 3-6](#)
- [Configuring Client Performance Settings, page 3-6](#)

## Tuning the Server

You can improve Prime Infrastructure's performance and scalability by increasing the amount of RAM, CPU, and disk space allocated to the Prime Infrastructure server virtual machine (or VM).

Successful server tuning requires you to complete the following workflow:

1. Changes to the VM include a risk of failure. Take an application backup before making any changes to the VM. See [Taking Application Backups From the Interface, page 4-3](#).
2. Although it is enabled by default, you should ensure that the Server Tuning option is enabled before making changes to the VM. See [Enabling Server Tuning During Restarts, page 3-5](#).
3. Perform the resource modifications in the VM, then restart the VM and the server. See [Modifying VM Resource Allocation, page 3-5](#).

### Enabling Server Tuning During Restarts

Prime Infrastructure can adjust to make use of expanded VM resources automatically, as long as the "Enable Server Tuning during restart option" is enabled. It is enabled by default.

To enable automatic server tuning after VM changes:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Server Tuning**.
  - Step 3** Select the **Enable Server Tuning during restart** check box, then click **Save**.
- 

### Modifying VM Resource Allocation

Use the following steps to make changes to the Virtual Appliance RAM, CPU or disk space resource allocations.

Be sure to back up the Prime Infrastructure server before attempting these types of changes (see [Backing Up and Restoring Prime Infrastructure, page 4-1](#)).

- 
- Step 1** Shut down Prime Infrastructure
    - a. Log in as admin.
    - b. At the command line, enter `admin# ncs stop`.
  - Step 2** Shut down the Virtual Appliance:
    - a. Login as admin.
    - b. At the command line, enter `admin# halt`.
  - Step 3** Launch the vSphere Client, right click the Virtual Appliance, then click **Edit Settings**.
  - Step 4** To change the RAM allocation, select **Memory** and change the **Memory Size** as desired. Then click **OK**.
  - Step 5** To change the CPU allocation, select **CPUs** and select the **Number of Virtual Processors** you want from the drop-down list. Then click **OK**.
  - Step 6** To add a new disk (you cannot expand the size of the existing disk):
    - a. Click **Add....**

- b. Select **Hard Disk**, then click **Next**.
- c. Check **Create a new virtual disk**, then click **Next**.
- d. Enter the desired **Disk Size** and specify a **Location** for the new virtual disk, then click **Next**.
- e. With the Advanced Options displayed, click **Next**, then click **Finish**.

**Step 7** Power on the Virtual Appliance and restart Prime Infrastructure.

---

## Compacting the Prime Infrastructure Database

You can reclaim disk space by compacting the Prime Infrastructure database.

**Step 1** Open a console session and log in to the server as admin. Enter the admin password when prompted.

**Step 2** At the command line, enter the following command to compact the application database:

```
admin# ncs cleanup
```

**Step 3** When prompted, answer Yes to the deep cleanup option.

---

## Configuring Client Performance Settings

You can configure the following client processes to improve Prime Infrastructure performance and scalability. This section contains the following topics:

- [Enabling Automatic Client Troubleshooting, page 3-6](#)
- [Enabling Hostname Lookup, page 3-7](#)
- [Specifying for How Long to Retain Client Association History Data, page 3-7](#)
- [Polling Clients When Receiving Client Traps/Syslogs, page 3-8](#)
- [Saving Client Traps as Events, page 3-8](#)
- [Saving 802.1x and 802.11 Client Traps as Events, page 3-8](#)

### Enabling Automatic Client Troubleshooting

The **Administration > System Settings > Client** page allows you to enable automatic client troubleshooting on a diagnostic channel for your third-party wireless clients running Cisco Compatible Extensions (CCX).

With this feature enabled, Prime Infrastructure will process the `client ccx test-association` trap that invokes a series of tests on each CCX client. Clients are updated on all completed tasks, and an automated troubleshooting report is produced (it is located in `dist/acs/win/webnms/logs`). When each test is complete, the location of the test log is updated in the client details pages, in the V5 or V6 tab, in the Automated Troubleshooting Report group box. You can use the Export button to export the logs.

When this feature is not enabled, Prime Infrastructure still raises the trap, but automated troubleshooting is not initiated.



**Note**

Automatic client troubleshooting is only available for clients running CCX version 5 or version 6. For a list of CCX-certified partner manufacturers and their CCX client devices, see the [Cisco Compatible Extensions Client Devices](#) page.

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Client**. The Client page appears.
- Step 3** Under **Process Diagnostic Trap**, select the **Automatically troubleshoot client on diagnostic channel** check box, then click **Save**.
- 

## Enabling Hostname Lookup

DNS lookup can take a considerable amount of time. Because of this, you can enable or disable the DNS lookup for client hostname. It is set to Disable by default.

To enable hostname lookup:

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Client**.
- Step 3** Click the **Lookup client host names from DNS server** check box.
- Step 4** Enter the number of days that you want the hostname to remain in the cache, then click **Save**.
- 

## Specifying for How Long to Retain Client Association History Data

Client association history can take a lot of database and disk space. This can be an issue for database backup and restore functions. The retaining duration of a client association history can be configured to help manage this potential issue.

To configure data retention parameters:

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Client**.
- Step 3** Enter or edit the following data retention parameters, then click **Save**.
- **Dissociated Clients (days)**—Enter the number of days that you want Prime Infrastructure to retain the data. The default is 7 days. The valid range is 1 to 30 days.
  - **Client session history (days)**—Enter the number of days that you want Prime Infrastructure to retain the data. The default is 32 days. The valid range is 7 to 365 days.
-

## Polling Clients When Receiving Client Traps/Syslogs

In a busy network, you might want to disable polling while the client traps are received because if there are a lot of client which tends to associate/disassociate, PI will get a lot of traps to process, this may impact PI performance. When you disable polling, PI will not track device traps during client association/disassociation and will learn about the client status once in XX minutes when PI polls the device. In this case, it will be impossible to debug client issues assuming that client moved from one place to another. This option is disabled by default. Choose **Administration > System Settings > Client**. If you select the **Poll clients when client traps/syslogs received** check box, Prime Infrastructure polls clients to identify client sessions.

## Saving Client Traps as Events

In some deployments, Prime Infrastructure might receive large amounts of client association and disassociation traps. Saving these traps as events can cause slow server performance. In addition, other events that might be useful could be aged out sooner than expected because of the amount of traps being saved.

To ensure that Prime Infrastructure does not save client association and disassociation traps as events, choose **Administration > System Settings > Client**, then unselect the **Save client association and disassociation traps as events** check box. Click **Save** to confirm this configuration change. This option is disabled by default.

## Saving 802.1x and 802.11 Client Traps as Events

You have to save the Save 802.1x and 802.11 client authentication failed traps as events for debugging purpose. To do this, choose **Administration > System Settings > Client**, then select the **Save 802.1x and 802.11 client authentication fail traps as events** check box.

# Checking the Status of Prime Infrastructure Using CLI

To check the status of Prime Infrastructure from the CLI:

---

**Step 1** Log in to the system as **admin** by entering the following command:

```
ssh admin server_IP_or_hostname
```

Enter the following CLI:

```
# ncs status
```

---

## Recovering Prime Infrastructure Passwords

You can change Prime Infrastructure application root user or FTP user password. To recover the passwords and regain access to Prime Infrastructure, follow these steps:

---

**Step 1** Log in to Prime Infrastructure command-line interface as an admin user.

**Step 2** Enter the following command:

```
ncs password root password password
```

Where *password* is the root user login password. You can enter a password not exceeding 80 characters.

To change the FTP user password, enter the following command:

```
ncs password ftpuser username password password
```

Example of the command usage:

```
ncs-appliance/admin# ncs password root password <newpassword>
CompilerOracle: exclude org/snmp4j/Snmp.send
Loading USER - root
Validating new password..
Resetting password ..
Resetting password COMPLETED.
EXECUTION STATUS : Success
ncs-appliance/admin#
```

You must now be able to login to Prime Infrastructure web interface with the new root password.

---

## Downloading Device Support and Product Updates

Device Package updates and software updates for major Prime Infrastructure product releases are integrated into update bundles. These bundles are available for download directly from Cisco.

To install update bundles for Prime Infrastructure:

---

**Step 1** Depending on your connectivity, do one of the following:

- If Prime Infrastructure has external connectivity:
  - Choose **Administration > Software Update**.
  - Click **Check for Updates**.
  - Enter your Cisco.com login credentials.
- If Prime Infrastructure does not have external connectivity:
  - Go to [Cisco.com/go/primeinfrastructure](https://Cisco.com/go/primeinfrastructure).
  - Under Support, select **Download Software**.
  - Choose **Cisco Prime Infrastructure**, then select the correct version of Prime Infrastructure.
  - From the page that appears, download the latest update file (with the extension .ubf).



---

**Note** Be sure to download the software updates that match your Prime Infrastructure version. For example, software updates for Release 1.1 can be installed only on Prime Infrastructure 1.1.

---

- Choose **Administration > Software Update**.
- Click **Upload Update File** and browse to locate the update bundles you downloaded.

The Software Updates table appears.

**Table 3-2** Software Updates Table

| Field            | Description                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name             | The names of software updates that have been downloaded from Cisco.com.                                                                                                                       |
| Published Date   | Date at which the software was published to Cisco.com. The Software Updates table always shows the published dates in chronological order (oldest to most recent).                            |
| Requires Restart | If the update requires a restart, the value of this field is <b>yes</b> .                                                                                                                     |
| Pending Restart  | If a restart is pending for the update to be complete, the value of this field is <b>yes</b> .                                                                                                |
| Installed        | If the software is already installed, this field has a green check mark. If the update bundle has not yet been installed, this field is blank.                                                |
| Description      | To see a detailed description of the software update bundle, select the radio button to the right of the description. A dialog box appears, showing the list of patches in that update bundle |

- Step 2** To install the software updates:
- a. Choose the software updates you want to install, and click **Install**.



**Note** When you choose an update, all the uninstalled updates published prior to the update you have chosen are also auto-selected. In Prime Infrastructure, it is mandatory to install software updates incrementally, because older updates are sometimes prerequisites to more recent updates. This behavior also occurs in uninstallation.

The installed software updates appear at the bottom of the table, with a check mark at the **Installed** column.

- b. If the **Pending Restart** value is **yes**, restart Prime Infrastructure to complete the update.
- c. To uninstall any software updates, select the updates and click **Uninstall**.

You can apply the UBF patch on either a standalone Prime Infrastructure 2.0 server or in a Prime Infrastructure 2.0 High Availability (HA) environment. For more details, see [PI 2.0 UBF Patch Readme](#).

## Configuring Support Request Settings

The Support Request Settings page allows you to configure the general support and technical support information.

To configure support request settings:

- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Support Request Settings**. The Support Request Settings page appears.
- Step 3** Configure the following parameters:
  - General Support Settings:
    - Enable interactions directly from the server—Click this check box to allow interactions for support requests, directly from the server.

- Sender E mail Address—Enter the email address of the sender.
- Interactions via client system only—Click this check box to allow interactions for support requests, only through client system.
- Technical Support Provider Information:
  - Cisco—Click this check box if the technical support provider is Cisco. In the Default Cisco.com Username field, enter a default username to log in to Cisco.com. Click **Test Connectivity** to test the connections to the mail server, Cisco support server, and forum server.
  - Third-Party Support Provider—Click this check box if the technical support provider is a third-party. Enter the email address, email subject line format, and website URL of the third-party or partner support provider.

**Step 4** Click **Save Settings**.

---

## Stopping Prime Infrastructure

You can stop Prime Infrastructure at any time by following these steps.



**Note**

If any users are logged in when you stop Prime Infrastructure, their sessions stop functioning.

---

To stop Prime Infrastructure:

---

**Step 1** Log into the system as **admin** by entering the following command:

```
ssh admin server_IP address / hostname
```

**Step 2** Enter the following CLI:

```
# ncs stop
```

---

## Removing Prime Infrastructure

Removing Prime Infrastructure using the following method will permanently delete all data on the server, including server settings and local backups. You will be unable to restore your data unless you have a remote backup.

---

**Step 1** In the VMware vSphere client, right-click the Prime Infrastructure virtual appliance.

**Step 2** Power off the virtual appliance.

**Step 3** From the Disk option, choose **Delete**.

---





## Backing Up and Restoring Prime Infrastructure

---

As with any other system upon which your organization relies, you will need to ensure that Cisco Prime Infrastructure is backed up regularly, so it can be restored in case of hardware or other failure.

- [Types of Prime Infrastructure Backups, page 4-1](#)
- [Taking Application Backups From the Interface, page 4-3](#)
- [Taking Application Backups From the Command Line, page 4-3](#)
- [Scheduling Automatic Application Backups, page 4-4](#)
- [Taking Appliance Backups, page 4-4](#)
- [Using Local Backup Repositories, page 4-5](#)
- [Using Remote Backup Repositories, page 4-5](#)
- [Types of Prime Infrastructure Restore, page 4-6](#)
- [Restoring From Application Backups, page 4-7](#)
- [Restoring From Appliance Backups, page 4-7](#)
- [Migrating to Another OVA Using Backup and Restore, page 4-9](#)
- [Log Information, page 4-9](#)

### Types of Prime Infrastructure Backups

Prime Infrastructure creates two types of backup files:

- **Application backups:** These contain all application code and data, but do not include host-specific settings, such as the server hostname and IP address. You can create these backups using the Prime Infrastructure interface or the command line. By default, Prime Infrastructure creates one application backup every day, automatically, in the default local backup repository.
- **Appliance backups:** These contain all application code, data, and host-specific settings, including the hostname, IP address, subnet mask, and default gateway. You can create appliance backups from the command line only. Prime Infrastructure does not take appliance backups automatically.

By default, application backup files are stored in the `/localdisk/defaultRepo` repository. You can change this default, including specifying remote or local backup repositories, when you run an application or appliance backup from the command line. You can also specify a remote or local backup repository to use for automatic application backups.

All backups created automatically or on-demand from the Prime Infrastructure interface are assigned a filename with the format *host-yyymmdd-hhmm.tar.gpg*, where *host* is the hostname of the server from which the backup was taken, and the other values are the date and time the backup was taken. Backups taken from the command line have the format *filename-yyymmdd-hhmm.tar.gpg*, where *filename* is the filename you specify.



## Taking Application Backups From the Interface

You can take an immediate application backup using the Prime Infrastructure interface.

You can also run an on-demand application backup from the command line (see [Taking Application Backups From the Command Line](#), page 4-3).

- 
- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Under **Other Background Tasks**, find the **Prime Infrastructure Server Backup** task.  
If you want to change the backup repository and maximum number of backups, see the steps under [Scheduling Automatic Application Backups](#), page 4-4.
- Step 3** Select the **Prime Infrastructure Server Backup** task check box.
- Step 4** From the **Select a command** drop-down list, select **Execute Now**.
- Step 5** Click **Refresh** to see the current status of the task.
- 

## Taking Application Backups From the Command Line

You can take an immediate application backup using the command line. Taking an application backup from the command line allows you to specify the backup repository and filename.

You can also take an on-demand application backup using the Prime Infrastructure user interface (see [Taking Application Backups From the Interface](#), page 4-3).

- 
- Step 1** At the Prime Infrastructure virtual appliance, exit to the command line.
- Step 2** At the command line, log in using the administrator ID and password used to install Prime Infrastructure.
- Step 3** Enter the following command to display the list of backups:
- ```
# show repository repositoryName
```
- Where *repositoryName* is the repository alias on which you want to create the backup (for example, RemoteFTP).
- Step 4** Enter the following command to back up the application:
- ```
# backup filename repository repositoryName application NCS
```
- Where:
- filename* is the name you want to give the application backup file (for example, myBackup). The host name, date and time of the backup and the tar.gpg filename extension will be appended to the filename you specify.
  - repositoryName* is the name of the repository where you want to store the backup (for example, RemoteFTP).
-

# Scheduling Automatic Application Backups

You can schedule regular application backups using the Prime Infrastructure user interface.



## Note

Backing up affects the performance of the server. You should schedule application backups to run when the server is less active (for example, in the middle of the night).

## Before You Begin

If you want to back up to a new local or remote repository, you must first create it:

- You can create a local backup repository using the Prime Infrastructure user interface (see [Using Local Backup Repositories, page 4-5](#)).
- To create a remote repository, you must use both the interface and the command line (see [Using Remote Backup Repositories, page 4-5](#)).

To schedule automatic backups of the Prime Infrastructure application:

- 
- Step 1** Choose **Administration > Background Tasks**.
  - Step 2** From **Other Background Tasks** in the left sidebar menu, click **Prime Infrastructure Server Backup**.
  - Step 3** Enter the required information.
  - Step 4** Click **Save**.

The backup file is saved in *ftp-server/directory* (if you have configured a remote FTP repository) or in */localdisk/defaultRepo* with a filename of the format *hostname-yymmdd-hhmmss.tar.gpg* (for example, *MyHost-120806-1748.tar.gpg*).

---

# Taking Appliance Backups

Appliance backups are not automatically created. You may create them as needed, using the command line.

- 
- Step 1** At the Prime Infrastructure virtual appliance, exit to the command line.
  - Step 2** At the command line, log in using the administrator ID and password used to install Prime Infrastructure.
  - Step 3** Enter the following command to display the list of appliance backups:

```
# show repository repositoryName
```

Where *repositoryName* is the repository alias on which you want to create the appliance backup (for example, *RemoteFTP*).

- Step 4** Enter the following command to back up the appliance:

```
# backup filename repository repositoryName
```

Where:

- *filename* is the name you want to give the appliance backup file (for example, *myBackup*) . The date and time of the backup and the *.tar.gpg* filename extension will be appended to the filename you specify (for example, *myBackup-130615-1256.tar.gpg*).

- *repositoryName* is the name of the repository where you want to store the appliance backup (for example, `RemoteFTP`).
- 

## Using Local Backup Repositories

If you want to create local repository, follow these steps:

---

**Step 1** At the command line, log in with the administrator ID and password used to install Prime Infrastructure.

**Step 2** Enter the following commands:

```
# configure terminal
# repository repositoryName
# url disk: /foldername
# end
```

Where disk represents localdisk.

---

You can create new backup repositories as needed, then specify one of them when scheduling an automatic backup or before performing an on-demand backup.

If you want to use a local repository, entering a new repository alias in the Name field and clicking **Submit** will create the new repository as a subdirectory with the name you specified on the Prime Infrastructure server.

If you want to use a repository located on a remote FTP server, see [Using Remote Backup Repositories, page 4-5](#).

---

**Step 1** Choose **Administration > Background Tasks**.

**Step 2** Under **Other Background Tasks**, click **Prime Infrastructure Server Backup**.

**Step 3** Click **Create**.

**Step 4** Enter a unique name for the backup repository.

**Step 5** Click **Submit**.

---

## Using Remote Backup Repositories

You can create backup repositories on a remote FTP server and set up the Prime Infrastructure server to use them. Remote repositories are recommended, as they help ensure that your network management data backups are protected from site failures.

The FTP server hosting your backups can be set up anywhere in your network, as long as the FTP server:

- Has an IP address accessible from the Prime Infrastructure server.
- Has a user with write access to the FTP server disk.

- Has a local subdirectory that matches the repository Name you specify on the Prime Infrastructure server.

Although not required, Cisco strongly recommends that you configure the FTP server backup repository before setting up Prime Infrastructure to use it. If you do not configure it before the first on-demand or automatic backup is triggered, the backup will fail without warning.

- 
- Step 1** At the Prime Infrastructure virtual appliance, exit to the command line.
- Step 2** At the command line, log in with the administrator ID and password used to install Prime Infrastructure.
- Step 3** Enter the following command to enter server configuration mode:
- ```
# configure terminal
```
- Step 4** Enter the following commands to configure a symbolic link to the remote FTP server:
- ```
# repository repositoryName
# url ftp://serverIPorHostname
# user name password plain userPassword
```
- Where:
- *repositoryName* is the name of the remote repository on the FTP server (for example, RemoteFTP).
  - *serverIPorHostname* is the IP address or hostname of the remote FTP server (for example, ftp://192.198.110.100/).
  - *name* is the name of a user with write privileges to the repository on the FTP server.
  - *userPassword* is the corresponding password for that user.
- When you are finished, press **Ctrl+z** to exit configuration mode.
- Step 5** Verify creation of the symbolic link using the following command:
- ```
# show repository repositoryName
```
- Step 6** In the Prime Infrastructure interface, choose **Administration > Background Tasks > Other Background Tasks**.
- Step 7** Click **Prime Infrastructure Server Backup**.
- Step 8** Click **Create**.
- Step 9** Enter the name of the remote FTP repository.
- Step 10** Select **FTP Repository**.
- Step 11** Enter the *serverIPorHostname* and the *name* and *userPassword* of the FTP user.
- Step 12** Click **Submit**.
- 

## Types of Prime Infrastructure Restore

Prime Infrastructure creates two types of restore files:

- **Application restore:** These contain all application code and data, but do not include host-specific settings, such as the server hostname and IP address. You can restore application data from application backup using command line only.

- Appliance restore: These contain all application code, data, and host-specific settings, including the hostname, IP address, subnet mask, and default gateway. You can restore appliance data from appliance backup using command line only.

## Restoring From Application Backups

Follow the steps below to restore Prime Infrastructure from an application backup using the command line. You cannot restore an application backup using the Prime Infrastructure user interface.

You can restore an application backup to the same host you were using or to a different host. Note that you can restore an application backup from an Express to a Standard or Pro installation, or from a Standard to a Pro installation. You cannot restore an application backup taken from a larger installation to a smaller installation (see [Migrating to Another OVA Using Backup and Restore](#), page 4-9).

Application backup files created using the Prime Infrastructure user interface as a scheduled background task are assigned generic filenames of the format *hostname-yyymmdd-hhmm.tar.gpg* (for example, *MyHost-120806-1748.tar.gpg*). Application backups created using Prime Infrastructure interface or the command line will have the filename the user specified in place of the hostname.

- 
- Step 1** At the Prime Infrastructure virtual appliance, exit to the command line.
- Step 2** At the command line, log in using the administrator ID and password used to install Prime Infrastructure.
- Step 3** Enter the following command to display the list of application backups:
- ```
# show repository repositoryName
```
- Where *repositoryName* is the repository alias from which you want to restore the application backup. (for example, *RemoteFTP*).
- Step 4** Identify the application backup file you want to restore and then enter the following command to restore from that file:
- ```
# restore filename repository repositoryName application NCS
```
- Where *filename* is the name of the application backup file from which you want to restore (for example, *myHost-131216-1256.tar.gpg*).
- 

**Note**

In case of older version restore, if the restore is done with NCS process down, then you have to manually make the process up after completion of restore.

---

## Restoring From Appliance Backups

Follow the steps below to restore Prime Infrastructure from an appliance backup using the command line. You cannot restore from an appliance backup using the Prime Infrastructure user interface. You can restore to the same host you were using, or to a different host.

Once the restore is complete, you may need to change the restored server's IP address, subnet mask, and default gateway. These changes are required when:

- The restored host is on the same subnet as the old host, and the old host is still active.
- The restored host is on a different subnet from the old host.

Although not required, we also recommend changing the server hostname under these conditions.

---

**Step 1** At the Prime Infrastructure virtual appliance, exit to the command line.

**Step 2** At the command line, log in using the administrator ID and password used to install Prime Infrastructure.

**Step 3** Enter the following command to display the list of appliance backups:

```
# show repository repositoryName
```

Where *repositoryName* is the repository alias from which you want to pull the appliance backup (for example, RemoteFTP).

**Step 4** Identify the appliance backup file you want to restore and then enter the following command to restore from that file:

```
# restore filename repository repositoryName
```

Where *filename* is the name of the appliance backup file from which you want to restore (for example, myHost-131216-1256.tar.gpg).

**Step 5** Once the restore is complete, if needed, use the command line to change the IP address, subnet mask, default gateway and (optionally) the host name on the restored server. For example:

```
Admin# conf t
Admin# int GigabitEthernet 0
Admin# ip address IPAddress subnetMask
Admin# ip default-gateway GatewayIP
Admin# hostname hostname
Admin# exit
```

---

# Migrating to Another OVA Using Backup and Restore

You will need to migrate your Prime Infrastructure data from an existing installation to a new one whenever you want to:

- Replace the old host entirely, such as after a catastrophic hardware failure. In this case, you can simply use your old OVA installation media to create the new host.
- Use Prime Infrastructure to manage more of your network and when you want to ensure you have adequate processing capacity. In this case, you will want to download installation files for the larger OVA before retiring the smaller one.

It is relatively easy to do this by restoring to the new host an application backup from the old host, as explained in the steps below.

- 
- Step 1** If you have not already done so, set up a remote backup repository for the old host, as explained in [Using Remote Backup Repositories, page 4-5](#).
- Step 2** Take an application backup of the old host on the remote repository, as explained in [Taking Application Backups From the Interface, page 4-3](#).
- Step 3** Install the new host as explained in the [Cisco Prime Infrastructure 2.0 Quick Start Guide](#).
- Step 4** Configure the new host to use the same remote backup repository as the old host, as explained in [Using Remote Backup Repositories, page 4-5](#).
- Step 5** Restore the application backup on the remote repository to the new host, as explained in [Restoring From Application Backups, page 4-7](#).
- 

## Log Information

Database backup and restore related information can be obtained from the below logs:

/opt/CSCOLumos/logs/rman.log

/opt/CSCOLumos/logs/dbadmin\_StdOut.log







## Maintaining Network Health

---

This section contains the following topics:

- [Configuring Alarm and Event Settings, page 5-1](#)
- [Configuring Audit Settings, page 5-4](#)
- [Downloading and Emailing Error Logs, page 5-6](#)
- [Configuring Technical Support Request Settings, page 5-11](#)

### Configuring Alarm and Event Settings

- [Specifying Alarm Clean Up and Display Options, page 5-1](#)
- [Changing Alarm Severities, page 5-3](#)

### Specifying Alarm Clean Up and Display Options

The **Administration > System Settings > Alarms and Events** page enables you to specify when to delete alarms and how to set display and email options for alarms.

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Alarms and Events**. The **Administration > System Settings > Alarms and Events** page appears.
- Step 3** Modify the Alarm and Event Cleanup Options:
- Delete active and cleared alarms after—Enter the number of days after which active and cleared alarms are deleted. You can disable this option by unselecting the check box.
  - Delete cleared security alarms after—Enter the number of days after which Security, Rogue AP, and Adhoc Rogue alarms are deleted.
  - Delete cleared non-security alarms after—Enter the number of days after which non-security alarms are deleted. Non-security alarms include all alarms that do not fall under the Security, Rogue AP, or Adhoc Rogue categories.

- Delete all events after—Enter the number of days after which all the events are deleted. If you want this deletion task to be performed first, set its value smaller than all the other Alarm and Events Cleanup Options.




---

**Note** Prime Infrastructure deletes old alarms nightly, as part of normal data cleanup tasks, and checks the alarm table size once an hour. When the alarm table size exceeds 300K, Prime Infrastructure deletes the oldest cleared alarms until the alarm table size is within 300K. If you want to keep cleared alarms for more than seven days, then you can specify a value more than seven days in the Delete cleared non-security alarms after text box, until the alarm table size reaches 300K.

---

**Step 4** Under Syslog Cleanup Options, in the *Delete all syslogs after* field, enter the number of days after which all syslogs are deleted.

**Step 5** Modify the Alarm Display Options:

- Hide acknowledged alarms—When the check box is selected, Acknowledged alarms do not appear on the Alarm Summary page. This option is enabled by default. Emails are not generated for acknowledged alarms, regardless of severity change.
- Hide assigned alarms—When the check box is selected, assigned alarms do not appear in the Alarm Summary page.
- Hide cleared alarms—When the check box is selected, cleared alarms do not appear in the Alarm Summary page. This option is enabled by default.
- Add controller name to alarm messages—Select the check box to add the name of the controller to alarm messages.
- Add Prime Infrastructure address to email notifications—Select the check box to add Prime Infrastructure address to email notifications.




---

**Note** Changes in these options affect the Alarm Summary page only. Quick searches for alarms for any entity will display all alarms for that entity, regardless of alarm state.

---

**Step 6** Modify the Alarm Email Options:

- Include alarm severity in the email subject line—Select the check box to include alarm severity in the email subject line. This option is enabled by default.
- Include alarm Category in the email subject line—Select the check box to include alarm category in the email subject line. This option is enabled by default.
- Include prior alarm severity in the email subject line—Select the check box to include prior alarm severity in the email subject line.
- Include custom text in the email subject line—Select the check box to add custom text in the email subject line. You can also replace the email subject line with custom text by selecting the Replace the email subject line with custom text check box.
- Include custom text in body of email—Select the check box to add custom text in the body of email.
- Include alarm condition in body of email—Select the check box to include alarm condition in the body of email.
- Add link to Alarm detail page in body of email—Select the check box to add a link to the Alarm detail page in the body of email.

- **Enable Secure Message Mode**—Select the check box to enable a secure message mode. If you select the Mask IP Address and Mask Controller Name check boxes, the alarm emails are sent in secure mode where all the IP addresses and controller names are masked.

**Step 7** Modify the Alarm Other Settings:

- **Controller license count threshold**—Enter the minimum number of available controller licenses you want to maintain. An alarm is triggered if the number of available controller licenses falls below this threshold.
- **Controller access point count threshold**—Enter the maximum number of available controller access points you want to maintain. An alarm is triggered if the number of available access points exceeds this threshold limit.

**Step 8** Click **Save**.

---

## Changing Alarm Severities

You can change the severity level for newly generated alarms.



**Note**

Existing alarms remain unchanged.

---

To change the severity level of newly generated alarms:

---

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

**Step 2** Choose **Severity Configuration** from the left sidebar menu.

**Step 3** Select the check box of the alarm condition whose severity level you want to change.

**Step 4** From the Configure Severity Level drop-down list, choose the new severity level (**Critical**, **Major**, **Minor**, **Warning**, **Informational**, or **Reset to Default**).

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

---

# Configuring Audit Settings

- [Setting Up Auditing Configurations](#), page 5-4
- [Deleting Syslogs from Audit Records](#), page 5-5
- [Enabling Change Audit Notifications](#), page 5-6

## Setting Up Auditing Configurations

The **Administration > System Settings > Audit** page allows you to determine the type of audit and on which parameters the audit is performed.

- [Choosing the Type of Audit](#)—Choose between basic auditing and template based auditing.
- [Selecting Parameters on Which to Audit](#)—Choose to audit on all parameters or on selected parameters for a global audit.

### Choosing the Type of Audit

The audit mode group box allows you to choose between basic auditing and template based auditing. Basic audit is selected by default.

- **Basic Audit**—Audits the configuration objects in Prime Infrastructure database against current WLC device values. Prior to the 5.1.0.0 version of Prime Infrastructure, this was the only audit mode available.




---

**Note** Configuration objects refer to the device configuration stored in Prime Infrastructure database.

---

- **Template-based Audit**—Audits on the applied templates, config group templates (which have been selected for the background audit), and configuration audits (for which corresponding templates do not exist) against current Controller device values.

- 
- Step 1** Choose **Administration > System Settings**.
- Step 2** From the left sidebar menu, choose **Audit**. The Audit page appears.
- Step 3** Choose **Basic Audit** or **Template Based Audit**:
- A basic audit audits the device configuration in Prime Infrastructure database against the current Controller configuration.
  - A template-based audit audits the applied templates, config group templates, and configuration objects (for which corresponding templates do not exist) against current Controller configuration.
- Step 4** Choose if you want the audit to run on all parameters or only on selected parameters. If you select the Selected Parameters radio button, you can access the Configure Audit Parameters configuration page. (See the [“Enabling Change Audit Notifications”](#) section on page 5-6).
- The selected audit parameters are used during network and controller audits.
- Step 5** Click **Save**.
- These settings are in effect when the controller audit or network audit is performed.
-

## Selecting Parameters on Which to Audit

The Audit On group box allows you to audit on all parameters or to select specific parameters for an audit. When the Selected Parameters radio button is selected, you can access the Select Audit Parameters configuration page. The selected audit parameters are used during network and controller audits.

To configure the audit parameters for a global audit:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Audit**.
  - Step 3** Select the **Selected Parameters** radio button to display the Select Audit Parameters link, then click **Save**.
  - Step 4** Click **Select Audit Parameters** to choose the required parameters for the audit in the Administration > System Settings > Audit > Select Audit Parameters page.
  - Step 5** Enter the required information, then click **Submit**. The selected audit parameters are displayed on the Selected Attributes tab.

To access a current Controller Audit Report from the **Configure > Controllers** page, select an object from the Audit Status column.

To audit a controller, choose **Audit Now** from the **Select a command** drop-down list in the **Configure > Controllers** page, or click **Audit Now** directly from the Controller Audit report.

---

## Deleting Syslogs from Audit Records

You should periodically delete (purge) audit records so that you don't have obsolete records taking up space on the server. The **Administration > System Settings > Audit Log Purge Settings** page allows you to purge the syslogs and send the purged logs either to trash or to a remote directory.

To configure the purge settings for syslogs:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Audit Log Purge Settings**.
  - Step 3** In the Keep logs younger than days text box, enter the number of days to define the log purge settings. The logs that are older than the days specified are purged.
  - Step 4** Choose either of the following options to clear the purged logs, then click **Save**.
    - **Send To Trash**—The purged logs are sent to trash.
    - **Remote Directory**—The purged logs are sent to the path specified in the Remote Directory text box.
-

## Enabling Change Audit Notifications

Prime Infrastructure can send notifications to a Java Message Server (JMS) whenever there are changes in inventory or configuration parameters that are part of an audit you have defined.

By default, JMS notification of audit changes is disabled. To enable this feature in Prime Infrastructure, you must check the **Enable Change Audit JMS Notification** check box. Prime Infrastructure sends all change audit notifications in XML format to the topic **ChangeAudit.All**. You must be subscribed to **ChangeAudit.All** to receive the notifications.

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Change Audit Notification**. The Change Audit Notification Settings page appears.
  - Step 3** Select the **Enable Change Audit JMS Notification** check box to enable notifications, then click **Save**.
- 

## Downloading and Emailing Error Logs

Prime Infrastructure logs all error, informational, and trace messages generated by all devices that are managed by Prime Infrastructure. Prime Infrastructure also logs all SNMP messages and Syslogs it receives.

To download and email the logs to use for troubleshooting Prime Infrastructure:

- 
- Step 1** Choose **Administration > Logging**. The General Logging Options Screen appears.
  - Step 2** Choose a message level.
  - Step 3** Select the check boxes within the Enable Log Module option to enable various administration modules. Click **Log Modules** to select all modules.
  - Step 4** In the Log File Settings section, enter the required settings. These settings will be effective after you restart Prime Infrastructure.  
  
By default, the File Prefix field is **ncs-%g-%u.log** where *%g* is a sequential number for the log file, and *%u* is a unique number assigned by the local disk file system. For example, the first log file created is named ncs-1-0.log.
  - Step 5** Click **Download** to download the log file to your local machine.




---

**Note** The logs.zip filename includes a prefix with the hostname, date, and time so that you can easily identify the stored log file. An HTML file that documents the log files is included in the ZIP file.

---

- Step 6** Enter the Email ID or Email IDs separated by commas to send the log file, then click **Send**.




---

**Note** To send the log file in an email, you must have configured an email server.

---

## Enabling SNMP Tracing

You can enable SNMP tracing to access more detailed information about the packets sent and received through SNMP. The SNMP tracing settings you specify are stored and used by the Prime Infrastructure SNMP server. To enable SNMP tracing, follow these steps.

**Note**

When you upgrade from WCS Release 7.x to Prime Infrastructure Release 2.0, the settings under Administration > Logging Options > SNMP Logging Options are not retained.

- 
- Step 1** Choose **Administration > Logging**. The Logging Options page appears.
  - Step 2** Choose the **SNMP Logging Options** from the left sidebar menu.
  - Step 3** Select the **Enable SNMP Trace** check box to enable sending SNMP messages (along with traps) between controllers and Prime Infrastructure, then select the **Display Values** check box to see the SNMP message values.
  - Step 4** Configure the IP address or IP addresses to trace the SNMP traps. You can add up to a maximum of 10 IP addresses in the text box.
  - Step 5** You can configure the maximum SNMP file size and the number of SNMP files.
- 

## Changing Syslog Logging Options

Syslog option allows you to enable the sending of syslog messages relating to the internal operation of Prime Infrastructure, to a third party syslog server. It does not enable the relaying of syslog messages received from network devices, to a third party syslog server.

- 
- Step 1** Choose **Administration > Logging**, then click **Syslog Logging Options**.
  - Step 2** Select the **Enable Syslog** check box to enable sending of Prime Infrastructure system log messages.
  - Step 3** Configure the IP address of Syslog Server to which the system log message have to be sent.
  - Step 4** Choose the **Syslog Facility**. You can choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.
  - Step 5** Click **Save**.
- 

## Changing Logging Options to Enhance Troubleshooting

You can change the amount of data Prime Infrastructure collects to debug an issue. For easily reproduced issues, follow these steps prior to contacting TAC.

To change the amount of troubleshooting data to collect:

- 
- Step 1** In Lifecycle view: Choose **Administration > Logging**.
  - Step 2** From the Message Level drop-down list, choose **Trace**.

**Step 3** Click each check box to enable all log modules.

**Step 4** Reproduce the current problem.



- Step 5** Return to the Logging Options page and click **Download** from the Download Log File section. The logs.zip filename includes a prefix with the hostname, date, and time so that you can easily identify the stored log file. An HTML file that documents the log files is included in the ZIP file.
- Step 6** After you have retrieved the logs, choose **Information** from the Message Level drop-down list.

**Caution**

Leaving the Message Level at *Trace* can adversely affect performance over a long period of time.

## Changing Mobility Service Engine Logging Options

You can use Prime Infrastructure to specify the Mobility Services Engine logging level and types of messages to log.

- Step 1** In Classic view: Choose **Design > Mobility Services > Mobility Services Engines**, then select the name of the mobility services engine that you want to configure.
- Step 2** Choose **System > Logs**, then choose the appropriate options from the Logging Level drop-down list. There are four logging options: Off, Error, Information, and Trace. All log records with a log level of Error or preceding are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

**Caution**

Use Error and Trace only when directed to do so by Cisco TAC personnel.

- Step 3** Select the **Enable** check box next to each element listed in that section to begin logging its events.
- Step 4** Select the **Enable** check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.
- Step 5** To download log files from the server, click **Download Logs**. See the “[Downloading Mobility Services Engine Log Files](#)” section on page 5-10 for more information.
- Step 6** In the Log File Parameters group box, enter the following:
- The number of log files to be maintained in the mobility services engine. You can maintain a minimum of 5 log files and a maximum of 20 log files in the mobility services engine.
  - The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.
- Step 7** In the MAC Address Based Logging Parameters group box, do the following:
- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.
  - Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**. See the “[MAC Address-Based Logging](#)” section on page 5-10 for more information on MAC address-based logging.
- Step 8** Click **Save** to apply your changes.

### MAC Address-Based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

```
/opt/mse/logs/locserver
```

A maximum of five MAC addresses can be logged at a time. The log file format for MAC address aa:bb:cc:dd:ee:ff is:

```
macaddress-debug-aa-bb-cc-dd-ee-ff.log
```

You can create a maximum of two log files for a MAC address. The two log files might consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC address. The MAC log files that are not updated for more than 24 hours are pruned.

## Downloading Mobility Services Engine Log Files

If you need to analyze mobility services engine log files, you can use Prime Infrastructure to download them to your system. Prime Infrastructure downloads a zip file containing the log files.

To download a zip file containing the log files:

- 
- Step 1** In Classic view: Choose **Design > Mobility Services > Mobility Services Engines**.
  - Step 2** Select the name of the mobility services engine to view its status.
  - Step 3** Choose **System > Logs** from the left sidebar menu.
  - Step 4** In the Download Logs group box, click **Download Logs**.
  - Step 5** Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.
-

# Configuring Technical Support Request Settings

You can customize the settings for creating a support case with Cisco Technical Support. For information about creating a support case, see the section “Opening a Support Case” in the *Cisco Prime Infrastructure 2.0 User Guide*.

- 
- Step 1** Choose **Administration > System Settings > Support Request Settings**.
- Step 2** Select the type of interaction the Cisco Support Enabling interactions directly from the Prime Infrastructure server:
- **Enable interactions directly from the server**—Specify this option to create the support case directly from the Prime Infrastructure server. Emails to the support provider are sent from the email address associated with the Prime Infrastructure server or the email address you specify.
  - **Interactions via client system only**—Specify this option to download the information required for your support case to a client machine. You must then email the downloaded support case details and information to the support provider.
- Step 3** Select your technical support provider:
- Click **Cisco** to open a support case with Cisco Technical Support, then enter your Cisco.com credentials. Click **Test Connectivity** to check the connectivity to the following servers:
    - Prime Infrastructure mail server
    - Cisco support server
    - Forum server
  - Click **Third-party Support Provider** to create a service request with a third-party support provider. You will need to enter the provider’s email address, the subject line, and the website URL.
-





## Managing Data Collection and Retention

---

One of the roles of an administrator is to manage Prime Infrastructure's network data collection and retention so that it:

- Scales to fit the real needs of the system's users.
- Minimizes the burden on monitored devices, applications, and network bandwidth.
- Survives hardware failures.

The following topics explain how to achieve these goals and perform other data management tasks.

- [Specifying Data Retention Periods, page 6-2](#)
- [Enabling Data Deduplication, page 6-4](#)
- [Specifying Where and for How Long to Save Reports, page 6-4](#)
- [Controlling Report Storage and Cleanup, page 6-5](#)
- [Specifying Inventory Collection After Receiving Events, page 6-5](#)
- [Device Configuration Settings, page 6-6](#)
- [Controlling Background Data Collection Tasks, page 6-7](#)
- [Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure, page 6-15](#)

# Specifying Data Retention Periods

You can configure retention periods for trend data, device health data, and system health data on an hourly, daily, and weekly basis. You can configure retention periods for performance data on a short, medium, and long term basis.

To set retention periods for aggregated data used in timed calculations and network audit calculations:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Data Retention**. The Data Retention page appears.
  - Step 3** Modify the values as required. See [Table 6-1](#) for the default values.



**Note** For the best interactive graph data views, change the settings to default value.

---

- Step 4** Click **Save**.
- 

## Prime Infrastructure Historical Data

There are two types of historical data in Prime Infrastructure, including the following:

- Aggregated historical data—Numeric data that can be gathered as a whole and aggregated to minimum, maximum, or average. Client count is one example of aggregated historical data.

Use the **Administration > System Settings > Data Retention** page to define the aggregated data retention period. Aggregation types include hourly, daily, and weekly.

The retention period for these aggregation types are defined as Default, Minimum, and Maximum (see [Table 6-1](#)).

**Table 6-1** Data Retention Periods

<b>Trend Data<sup>1</sup> Retain Periods</b>			
<b>Period</b>	<b>Default</b>	<b>Minimum</b>	<b>Maximum</b>
Hourly	15	1	31
Daily	90	7	365
Weekly	54	2	108
<b>Device Health Data<sup>2</sup> Retain Periods</b>			
Hourly	15	1	31
Daily	90	7	365
Weekly	54	2	108
<b>Performance Data<sup>3</sup> Retain Periods</b>			
Short Term Data	7	1	31
Medium Term Data	31	7	365
Long Term Data	378	2	756

**Table 6-1 Data Retention Periods (continued)**

<b>Network Audit Data Retain Period</b>			
Audit Data Retain Period	90	7	365
<b>System Health Data Retain Periods</b>			
Hourly Data Retain Period	1	1	31
Daily Data Retain Period	7	7	365
Weekly Data Retain Period	54	7	365

1. Trend data includes wireless-related historical information such as client history, AP history, AP utilization, and client statistics.
2. Device Health data includes SNMP polled data for wired and wireless devices such as device availability, and CPU, memory, and interface utilization, and QoS.
3. Performance data includes Assurance data such a traffic statistics, application metrics, and voice metrics.

- Non-aggregated historical data—Numeric data that cannot be gathered as a whole (or aggregated). Client association history is one example of non-aggregated historical data.

You can define a non-aggregated retention period in each data collection task and other settings.

For example, you define the retention period for client association history in **Administration > System Settings > Client**. By default, the retention period is 31 days or 1 million records. This retention period can be increased to 365 days.

## Performance Data Aggregation

The Performance Data is aggregated as follows:

- Short-term data is aggregated every 5 minutes.
- Medium-term data is aggregated every hour.
- Long-term is aggregated daily.

## Enabling Data Deduplication

Data Deduplication allows you to identify authoritative sources for each of the following classes of application data:

- Application Response Time (for TCP applications)
- Voice/Video (for RTP applications)

Whenever Prime Infrastructure receives duplicate data about the same network elements and protocols from two or more data sources, it resolves all such conflicts in the authoritative source's favor.

The Data Deduplication page allows you to specify a data source at a specific site. For example, if you have a Network Analysis Module (NAM) at a branch office as well as NetFlow data that is sent from the same branch, you can specify which data source Prime Infrastructure uses.

To enable data deduplication:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Data Deduplication**. The Data Deduplication page appears.
  - Step 3** Select the **Enable Data Deduplication** check box to remove the duplicated information from Prime Infrastructure, then click **Apply**.
- 

## Specifying Where and for How Long to Save Reports

To indicate where the scheduled reports reside and for how many days:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Report**. The Report page appears.
  - Step 3** Enter the path for saving report data files on a local PC. You can edit the existing default path.
  - Step 4** Specify the number of days to retain reports.
  - Step 5** Click **Save**.
-



## Controlling Report Storage and Cleanup

All scheduled reports are stored in the Scheduled Reports Repository. You will want to ensure that scheduled reports are retained in the report repository for reasonable lengths of time only, and deleted on a regular basis. The default retention scheme is to retain generated reports for a maximum of 31 days.

To customize the retention period:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Report**. The Report page appears.
  - Step 3** In **Repository Path**, specify the report repository path on the Prime Infrastructure server.
  - Step 4** In **File Retain Period**, specify the maximum number of days reports should be retained.
  - Step 5** Click **Save**.
- 

## Specifying Inventory Collection After Receiving Events

The Inventory page allows you to specify if Prime Infrastructure must collect inventory when a syslog event is received for a device.

To configure the inventory settings:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Inventory**. The Inventory page appears.
  - Step 3** Select the **Enable event based inventory collection** check box to allow Prime Infrastructure to collect inventory when it receives a syslog event for a device.
  - Step 4** Select the **Enable Syslog and Traps on device** check box to allow Prime Infrastructure to enable syslog and trap notifications on newly added devices.
  - Step 5** Click **Save**.
-

# Device Configuration Settings

- [Backing up and Rolling Back Configurations, page 6-6](#)
- [Specifying When to Archive Configurations, page 6-6](#)

## Backing up and Rolling Back Configurations

You can back up and roll back the running configuration from the **Administration > System Settings > Configuration** page.

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Configuration**.
  - Step 3** Enter the required information.
  - Step 4** Click **Save**.
- 

## Specifying When to Archive Configurations

Configuration archive/rollback is only supported for running-config on devices with WLC software. It is not supported for startup-config.

The configuration changes (such as turning on/off options) that you perform in the **Administration > System Settings > Configuration** page have no relevance to configuration archive operations. The configurations that you perform in this page are related to template deployment. For example, Backup running Configuration is to archive configuration before any template is deployed.

By default, Prime Infrastructure archives up to five device configuration versions for each device for seven days after:

- Every inventory collection
- Prime Infrastructure receives notification of a configuration change event

To change when Prime Infrastructure archives configurations:

- 
- Step 1** Choose **Administration > System Settings > Configuration Archive**.
  - Step 2** Change the necessary settings.
  - Step 3** To have Prime Infrastructure ignore commands for a particular device type, click the **Advanced** tab, choose the device type, and enter the commands to be ignored.

If the device you specify has a change in its configuration and Prime Infrastructure detects that the change is in one of the commands in the exclude list, Prime Infrastructure does not create an archived version of the configuration with this change.

- Step 4** Click **Save**.
-

# Controlling Background Data Collection Tasks

Prime Infrastructure performs scheduled data collection tasks on the background on a regular basis. You can enable or disable these collection tasks, change the interval at which each task is performed, or change the retention period for the data (raw or aggregated) collected during each task.

Disabling or limiting these background data collection tasks can have a direct impact on how you use Prime Infrastructure, especially for reporting. To help you consider these impacts, take note of the reports this data is used in. These reports are listed in the Collection Set Details for each task.

To create a background data collection task:

- 
- Step 1** Choose **Administration > Background Tasks**.
  - Step 2** Under **Data Collection Tasks**, in the **Task** column of the table, click the name of the task that you want to create.
  - Step 3** Enter the required information and click **Save**.
- 

To enable or disable background data collection tasks in bulk:

- 
- Step 1** Choose **Administration > Background Tasks**.
  - Step 2** Under **Data Collection Tasks**, select the check box next to each task you want to enable or disable.
  - Step 3** Choose **Go**, then choose to either enable or disable tasks.
-

## Understanding What Data Is Collected and When

The following table describes the various data collection tasks in Prime Infrastructure.

**Table 6-2** Data Collection Tasks

Task Name	Task Status	Default Schedule	Description
AP Image Pre-Download Status	Disabled	15 minutes	Allows you to see the Image Predownload status of the associated APs in the controllers. To see the status of the access points, the Pre-download software to APs check box should be selected while downloading software to the controller.
Autonomous AP CPU and Memory Utilization	Enabled	15 minutes	Collects information about memory and CPU utilization of autonomous APs.
Autonomous AP Inventory	Enabled	180 minutes	Collects the inventory information for autonomous APs.
Autonomous AP Radio Performance	Enabled	15 minutes	Collects information about radio performance information as well as radio up or down status for autonomous APs.
Autonomous AP Tx Power and Channel Utilization	Enabled	30 minutes	Collects information about radio performance of autonomous APs.
CCX Client Statistics	Disabled	60 minutes	Collects the Dot11 and security statistics for CCX Version 5 and Version 6 clients.
CleanAir Air Quality	Enabled	15 minutes	Collects information about CleanAir air quality.
Client Statistics	Enabled	15 minutes	Retrieves the statistical information for the autonomous and lightweight clients.
Controller Performance	Enabled	30 minutes	Collects performance information for controllers.
Guest Sessions	Enabled	15 minutes	Collects information about the guest sessions.
Interferers	Enabled	15 minutes	Collects information about the interferers.
Media Stream Clients	Enabled	15 minutes	Collects information about media stream for clients.
Mesh link Performance	Enabled	10 minutes	Collects information about the performance of Mesh links.
Mesh Link Status	Enabled	5 minutes	Collects status of the Mesh links.
Mobility Service Performance	Enabled	15 minutes	Collects information about the performance of mobility service engines.
Radio Performance	Enabled	15 minutes	Collects statistics from wireless radios.
Radio Voice Performance	Enabled	15 minutes	Collects voice statistics from wireless radios.
Rogue AP	Enabled	120 minutes	Collects information about the rogue access points.
Switch CPU and Memory Poll	Enabled	30 minutes	Collects information about switch CPU and memory poll.
Switch Inventory	Enabled	Daily at midnight	Collects inventory information for switches.
Traffic Stream Metrics	Enabled	8 minutes	Retrieves traffic stream metrics for the clients.
Unmanaged APs	Enabled	15 minutes	Collects poll information for unmanaged access points.

Table 6-2 Data Collection Tasks (continued)

Task Name	Task Status	Default Schedule	Description
Wireless Controller Inventory	Disabled	Daily at midnight	Collects inventory information for wireless controllers.
Wireless Controller Performance	Enabled	30 minutes	Collects performance statistics for wireless controllers.

## Controlling Prime Infrastructure Background Tasks

The following table describes the background tasks Prime Infrastructure performs. You can manage how and when they are performed by selecting **Administration > System Settings > Background Tasks**, then selecting the hypertext link for that task in the Other Background Tasks area of the page.

Table 6-3 Other Background Tasks

Task Name	Default Schedule	Description	Editable Options
Appliance Status	5 minutes	Lets you view appliance polling details. This task populates the appliance polling details from the <b>Administration &gt; Appliance &gt; Appliance Status</b> page. In addition, this background task populates information such as the performance and fault checking capabilities of the appliance.	Default—Enabled. Interval—Valid interval is from 1 to 10080.
Autonomous AP Operational Status	5 minutes	Lets you view the autonomous AP operational status polling.	Default: Enabled Interval—Valid interval is from 1 to 10080.
Autonomous Client Status	5 minutes	Lets you discover the autonomous AP client from the network.	Default—Enabled.
Configuration Sync	Daily at 4 am.	Lets you view the configuration synchronization.	Enable—Click this check box to enable configuration synchronization. Default: Enabled. Enable—Click this check box to enable Network Audit. Default: Enabled. Enable—Click this check box to enable Security Index calculation. Default: Enabled. Enable—Click this check box to enable RRM audit. Default: Enabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the configuration synchronization to happen. The valid format is hh:mm AM PM. For example, 12:49 AM.

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Controller Configuration Backup	Daily at 10 pm	Lets you view controller configuration backup activities.	<p>Enable—Click this check box to enable controller configuration backup. Default: Disabled.</p> <p>Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days.</p> <p>Time of Day—Enter the time of the day that you want the configuration synchronization to happen. The valid format is hh:mm AM/PM. For example, 12:49 AM.</p> <p>TFTP Server—Select the IP address of the server to which you want to back up the controller configuration.</p>
Controller Operational Status	5 minutes	Lets you schedule and view controller operational status.	<p>Enable—Click this check box to enable Controller Configuration Backup. Default: Enabled.</p> <p>Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days.</p>
Data Cleanup	Daily at 2 am.	Lets you schedule a data cleanup.	<p>Time of Day—Enter the time of the day that you want the data cleanup to happen. The valid format is hh:mm AM/PM. For example, 12:49 AM. Default: Enabled.</p>
Device Data Collector	30 minutes	Lets you schedule data collection based on specified command-line interface (CLI) commands at a configured time interval.	<p>Enabled—Click this check box to enable data collection for a specified controller. The default is Disabled.</p> <p>Controller IP address—The IP address of the Controller to collect data from.</p> <p>CLI Commands—Enter the CLI commands, separated by commas, that you want to run on the specified controller.</p> <p>Clean Start—Click this check box to enable a clean start before data collection.</p> <p>Repeat—Enter the number of times that you want the data collection to happen.</p> <p>Interval—Enter the interval, in days, that you want the data collection to happen. The valid range is 1 to 360 days.</p>

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Guest Accounts Sync	Daily at 1 am.	Schedules guest account polling and synchronization.	<p>Enable—Click this check box to enable guest account synchronization. The default is Enabled.</p> <p>Interval—Enter the interval, in days, that you want the guest account synchronization to happen. The valid range is 1 to 360 days.</p> <p>Time of Day—Enter the time of the day that you want the guest account synchronization to happen. The valid format is hh:mm AM/PM. For example, 12:49 AM.</p>
Identity Services Engine Status	15 minutes	Schedules the Identity Services Engine polling.	<p>Enable—Click this check box to enable Identity Services Engine polling. The default is Enabled.</p> <p>Interval—Enter the interval, in days, that you want the Identity Services Engine polling to happen. The valid range is 1 to 360 days.</p>
License Status	4 hours.	Schedules license status polling.	<p>Enable—Click this check box to enable license status polling. The default is Enabled.</p> <p>Interval—Enter the interval, in days, that you want the license status polling to happen. The valid range is 1 to 360 days.</p>
Lightweight AP Operational Status	5 minutes.	Lets you view Lightweight AP operational status polling.	<p>Enable—Click this check box to enable Lightweight AP Operational Status polling. The default is Enabled.</p> <p>Interval—Enter the interval, in days, that you want the Lightweight AP Operational Status polling to happen. The valid range is 1 to 360 days.</p>
Lightweight Client Status	5 minutes.	Lets you discover Lightweight AP clients from the network.	<p>Enable—Click this check box to enable Lightweight Client Status polling. The default is Enabled.</p> <p>Interval—Enter the interval, in days, that you want the Lightweight Client Status polling to happen. The valid range is 1 to 360 days.</p>
Mobility Service Backup	Every 7 days at 1 am.	Schedules mobility services backup polling.	<p>Enable—Click this check box to enable mobility service backup. The default is disabled.</p> <p>Interval—Enter the interval, in days, that you want the mobility services back up to happen. The valid range is 1 to 360 days.</p> <p>Time of Day—Enter the time of the day that you want the mobility services back up to happen. The valid format is hh:mm AM/PM. For example, 12:49 AM.</p>

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Mobility Service Status	5 minutes.	This task is used to schedule mobility services status polling.	<p>Enable—Click this check box to enable mobility services status polling. The default is Enabled.</p> <p>Interval—Enter the interval, in days, that you want the mobility services status polling to happen. The valid range is 1 to 360 days.</p>
Mobility Service Synchronization	60 minutes.	This task is used to schedule mobility services synchronization.	<p>Out of Sync Alerts—Click this check box if you want to enable out of sync alerts.</p> <p>Smart Synchronization—Click this check box if you want to enable smart synchronization. The default is Enabled.</p> <p>Interval—Enter the interval, in minutes, that you want the mobility services synchronization to happen. The valid range is 1 to 10080 minutes.</p>
Mobility Status Task	5 minutes	This task is used to view the status of mobility services engine(s).	<p>Enable—Click this check box to enable mobility status polling. The default is Enabled.</p> <p>Interval—Enter the interval, in minutes, that you want the mobility status polling to happen. The valid range is 1 to 10080 minutes.</p>
Prime Infrastructure Server Backup	Every 7 days at 1 AM (01:00)	This task is used to schedule Prime Infrastructure server backup.	<p>Enabled—Click this check box to enable automatic Prime Infrastructure server backup. The default is Enabled.</p> <p>Backup Repository—The location of the default backup repository where automatic backups are stored. The default is defaultRepo.</p> <p>Max UI backups to keep—The maximum number of automatic backups to keep (applied only if they are stored in the default local repository).</p> <p>Interval—Enter the interval, in days, at which you want automatic Prime Infrastructure server backups to be taken. The valid range is 1 to 360 days.</p> <p>Time of Day—Enter the time of the day that you want Prime Infrastructure server back up to be taken. Use 24-hour format (for example, 13:49).</p>
OSS Server Status	5 minutes.	This task is used to schedule OSS server status polling.	<p>Enable—Click this check box to enable OSS Server polling. The default is Enabled.</p> <p>Interval—Enter the interval, in minutes, that you want the OSS server polling to happen. The valid range is 1 to 10080 minutes.</p>



Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Redundancy Status	60 minutes	This task is used to view the redundancy status for primary and secondary controllers.	<p>Enabled—Click this check box to enable Redundancy status polling. The default is Disabled.</p> <p>Interval—Enter the interval, in minutes, that you want the Redundancy status polling to happen.</p>
Switch NMSP and Location Status	4 hours	This task is used to schedule the Switch Network Mobility Services Protocol (NMSP) and Civic Location Polling.	<p>Enable—Click this check box to enable Switch NMSP and Civic Location polling. The default is Enabled.</p> <p>Interval—Enter the interval, in minutes, that you want the Switch NMSP and Civic Location Polling to happen. The valid range is 1 to 10080 minutes.</p>
Switch Operational Status	5 minutes. Full poll is 15 minutes.	This task is used to schedule switch operational status polling.	<p>Enable—Click this check box to enable Switch NMSP and Civic Location polling.</p> <p>Interval—Enter the interval, in minutes, that you want the Switch NMSP and Civic Location Polling to happen. The valid range is 1 to 10080 minutes.</p> <p>Full operational status interval—Enter the interval, in minutes. The valid range is 1 to 1440 minutes.</p>
Third party Access Point Operational Status	3 hours	This task is used to schedule the operational status polling of third party APs.	<p>Enabled—Click this check box to enable third party AP operational polling.</p> <p>Interval—Enter the interval, in hours, that you want the third party AP operational status polling to happen. The valid range is 3 to 4 hours.</p>
Third party Controller Operational Status	3 hours	This task is used to schedule the reachability status polling of third party controllers.	<p>Enabled—Click this check box to enable the reachability status polling of third party controllers.</p> <p>Interval—Enter the interval, in hours, that you want the third party controller reachability status polling to happen. The valid range is 3 to 4 hours.</p>

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
wIPS Alarm Sync	120 minutes.	This task is used to schedule wIPS alarm synchronization.	<p>Enable—Click this check box to enable wIPS alarm synchronization. The default is Enabled.</p> <p>Interval—Enter the interval, in minutes, that you want the wIPS alarm synchronization to happen. The valid range is 1 to 10080 minutes.</p>
Wired Client Status	2 hours.	This task is used to schedule wired client status polling.	<p>Enable—Click this check box to enable wired client status polling. The default is Enabled.</p> <p>Interval—Enter the interval, in hours, that you want the wired client status polling to happen. The valid range is 1 to 8640 hours.</p> <p>Major Polling—Specify two time periods that you want the major pollings to happen. The valid format is hh:mm AM/PM. For example, 12:49 AM.</p>

# Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure

Prime Infrastructure supports data migration from Cisco Prime LAN Management Solution (LMS) version 4.2.4 on the Windows NT, Solaris and Linux platforms. The following LMS data can be imported into Prime Infrastructure using CAR CLI:

- Device Credential and Repository (DCR) Devices
- Static Groups
- Dynamic Groups
- Software Image Management Repository Images
- User Defined Templates (Netconfig)
- LMS Local Users
- MIBs

Only the Dynamic Groups containing the rule with the following attributes can be imported from LMS.

- PI attribute Name—LMS attribute name
- Contact—System.Contact
- Description—System.Description
- Location— System.Location
- Management\_Address—Device.ManagementIpAddress
- Name—System.Name
- Product\_Family—Device.Category
- Product\_Series—Device.Series
- Product\_Type—Device.Model
- Software\_Type—System.OStype
- Software\_Version—Image.Version

To migrate LMS data to Prime Infrastructure:

---

**Step 1** Identify the FTP server where LMS backup data is stored, then log in to the Prime Infrastructure server as an admin user.

**Step 2** Configure the backup location in the Admin Console by entering the following commands:

```
admin# config terminal
admin(config)# repository carsapps
admin(config-Repository)# url
      (for example, ftp://10.77.213.137/opt/lms OR sftp://10.77.213.137/opt/lms OR
fdisk:foldername)
admin(config-Repository)# user root password plain xxxxxxxx
admin(config-Repository)# end
```

**Step 3** Import the LMS backup into Prime Infrastructure using the following command:

```
admin# lms migrate repository carsapps
```

**Step 4** Log back in to the Prime Infrastructure user interface.

The following table lists the locations of the imported LMS data:

<b>LMS Data</b>	<b>Location in Prime Infrastructure</b>
DCR Devices	Operate > Device Work Center
Static Group	Operate > Device Work Center > User Defined Group
Dynamic Group	Operate > Device Work Center > User Defined Group
Software Image Management Repository Images	Operate > Device work Center > Software Image Management
User Defined Templates (Netconfig)	Design > Feature Design > OOTB Templates
LMS Local Users	Administration > Users, Roles & AAA > Users
MIBs	Design > Custom SNMP Templates



# Configuring Controller and AP Settings

---

This chapter contains the following topics:

- [Configuring SNMP Credentials for Rogue AP Tracing, page 7-1](#)
- [Configuring Protocols for CLI Sessions, page 7-2](#)
- [Refreshing Controllers After an Upgrade, page 7-2](#)
- [Tracking Switch Ports to Rogue APs, page 7-3](#)
- [Configuring Switch Port Tracing, page 7-4](#)

## Configuring SNMP Credentials for Rogue AP Tracing

The SNMP Credentials page allows you to specify credentials to use for tracing rogue access points. Use this option when you cannot find a specific entry using a number-based entry. When a switch credential is not added to Prime Infrastructure, you can use SNMP credentials on this page to connect to the switch.

To configure SNMP credentials:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **SNMP Credentials**. The SNMP Credentials page appears.
  - Step 3** To view or edit details about a current SNMP entry, click the **Network Address** link. See the [“Configuring Global SNMP Settings” section on page 2-6](#) for more information.



**Note** The default network address is 0.0.0.0, which indicates the entire network. An SNMP credential is defined per network so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. The default community string is *private* for both read and write. You should update the prepopulated SNMP credential with your own SNMP information.

---

- Step 4** To add a new SNMP entry, choose **Add SNMP Entries** from the **Select a command** drop-down list, then click **Go**. See the [“Adding a New SNMP Credential Entry” section on page 2-9](#) for more information.
-

## Configuring Protocols for CLI Sessions

Many Prime Infrastructure wireless features, such as autonomous access point and controller command-line interface (CLI) templates and migration templates, require executing CLI commands on the autonomous access point or controller. These CLI commands can be entered by establishing Telnet or SSH sessions. The CLI session page allows you to select the session protocol. SSH is the default.



**Note** In CLI templates, you are not required to answer the question responses (such as *Yes* or *No* answer to a command, *Press enter to continue*, and so on.). This is automatically performed by Prime Infrastructure.

To configure the protocols for CLI sessions:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **CLI Session**.
  - Step 3** The default controller session protocol SSH is selected. To choose Telnet, select that radio button.
  - Step 4** The default autonomous access point session protocol SSH is selected. To choose Telnet, select the radio button.
  - Step 5** The **Run Autonomous AP Migration Analysis on discovery** radio button is set to **No** by default. Choose **Yes** if you want to discover the autonomous APs as well as perform migration analysis, then click **Save**.
- 

## Refreshing Controllers After an Upgrade

The Controller Upgrade Settings page allows you to auto-refresh after a controller upgrade so that it automatically restores the configuration whenever there is a change in the controller image. To perform an auto-refresh:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Controller Upgrade Settings**.
  - Step 3** Select the **Auto refresh After Upgrade** check box to automatically restore the configuration whenever there is a change in the controller image.
  - Step 4** Determine the action Prime Infrastructure takes when a save config trap is received. When this check box is enabled, you can choose to retain or delete the extra configurations present on the device but not on Prime Infrastructure. The setting is applied to all controllers managed by Prime Infrastructure.

If you select the Auto Refresh on Save Config Trap check box in the **Configure > Controllers > Properties > Settings** page, it overrides this global setting.

It might take up to three minutes for the automatic refresh to occur.

**Step 5** Click **Save**.

Whenever a save config trap is received by Prime Infrastructure, this check box is selected. When this check box is enabled, it determines the action taken by Prime Infrastructure.

When this check box is enabled, the user can choose to retain or delete the extra configurations present on the device and not on Prime Infrastructure.

This setting is applied to all of the controllers managed by Prime Infrastructure. The setting in the **Controllers > Properties** page for processing the save config trap overrides this global setting.

When there is a change in the controller image, the configuration from the controller is automatically restored.

## Tracking Switch Ports to Rogue APs

The **Administration > System Settings > Rogue AP Settings** page allows you to enable Prime Infrastructure to automatically identify the network switch port to which each rogue access point is connected.

**Note**

You must purchase a Lifecycle license in order to use this feature. For more information on ordering Prime Infrastructure licenses, see the [Cisco Prime Infrastructure 2.0 Ordering and Licensing Guide](#).

To configure rogue AP auto trace:

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

**Step 2** From the left sidebar menu, choose **Rogue AP Settings**. The Rogue AP Settings page appears.

**Step 3** Select the **Enable Auto Switch Port Tracing** check box to allow Prime Infrastructure to automatically trace the switch ports to which rogue access points are connected. Then specify the parameters for auto port tracing, including:

- How long to wait between rogue AP-to-port traces (in minutes)
- Whether to trace Found On Wire rogue APs
- Which severities to include (Critical, Major, or Minor).

**Step 4** Select the **Enable Auto Containment** check box to allow Prime Infrastructure to automatically contain rogue APs by severity. Then specify the parameters for auto containment, including:

- Whether to exclude Found On Wire rogue APs detected by port tracing
- Which severities to include in the containment (Critical, Major).
- The containment level (up to 4 APs).

**Step 5** Click **OK**

## Configuring Switch Port Tracing

Currently, Prime Infrastructure provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, Prime Infrastructure gathers the information received from the controllers. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in Prime Infrastructure log and only for rogue access points, not rogue clients.

A rogue client connected to the rogue access point information is used to track the switch port to which the rogue access point is connected in the network.

If you try to set tracing for a friendly or deleted rogue, a warning message appears.

For Switch Port Tracing to successfully trace the switch ports using v3, all of the OIDs should be included in the SNMP v3 view and VLAN content should be created for each VLAN in the SNMP v3 group.

See the [“Configuring Switch Port Tracing” section on page 7-4](#) for information on configuring Switch Port Tracing settings.

The Switch Port Trace page allows you to run a trace on detected rogue access points on the wire.

To correctly trace and contain rogue access points, you must correctly provide the following information:

- Reporting APs—A rogue access point has to be reported by one or more managed access points.
- AP CDP Neighbor—Access point CDP neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials—All switches to be traced must have a management IP address and SNMP management enabled. You can add network address based entries instead of only adding individual switches. The correct write community string must be specified to enable/disable switch ports. For tracing, read community strings are sufficient.
- Switch port configuration—Trunking switch ports must be correctly configured. Switch port security must be disabled.
- Only Cisco Ethernet switches are supported.
- Switch VLAN settings must be properly configured.
- CDP protocol must be enabled on all switches.
- An Ethernet connection must exist between the rogue access point and the Cisco switch.
- You should have some traffic between rogue access points and the Ethernet switch.
- The rogue access point must be connected to a switch within the max hop limit. The default hop count is 2, and the maximum is 10.
- If SNMPv3 is chosen, use the context option and create one for each VLAN, in addition to the one for the main group (which is required for non-VLAN-based MIBs).



**Step 1** Choose **Administration > System Settings > Switch Port Trace**.

**Step 2** Configure the following basic settings:

- **MAC address +/-1 search**—Select the check box to enable.  
This search involves the MAC address +/-1 convention where the wired-side MAC address of the rogue access point is obtained by adding or subtracting the radio MAC address by one.
- **Rogue client MAC address search**—Select the check box to enable.  
When a rogue access point client exists, the MAC address of the client is added to the searchable MAC address list.
- **Vendor (OUI) search**—Select the check box to enable. OUI refers to Organizational Unique Identifier search which searches the first three bytes in a MAC address.
- **Exclude switch trunk ports**—Select the check box to exclude switch trunk ports from the switch port trace.



**Note** When more than one port is traced for a given MAC address, additional checks are performed to improve accuracy. These checks include the: trunk port, non-AP CDP neighbors present on the port, and whether or not the MAC address is the only one on this port.

- **Exclude device list**—Select the check box to exclude additional devices from the trace. Enter into the device list text box each device that you want to exclude from the switch port trace. Separate device names with a comma.
- **Max hop count**—Enter the maximum number of hops for this trace. Keep in mind that the greater the hop count, the longer the switch port trace takes to perform.
- **Exclude vendor list**—Enter in the vendor list text box any vendors that you want to exclude from the switch port trace. Separate vendor names with commas. The vendor list is not case sensitive.

**Step 3** Configure the following advanced settings:

- **TraceRogueAP task max thread**—Switch port tracing uses multiple threads to trace rogue access points. This field indicates the maximum number of rogue access points that can be traced on parallel threads.
- **TraceRogueAP max queue size**—Switch port tracing maintains a queue to trace rogue access points. Whenever you select a rogue access point for tracing, it is queued for processing. This field indicates the maximum number of entries that you can store in the queue.
- **SwitchTask max thread**—Switch port tracing uses multiple threads to query switch devices. This field indicates the maximum number of switch devices that you can query on parallel threads.



**Note** The default value for these parameters should be good for normal operations. These parameters directly impact the performance of switch port tracing and Prime Infrastructure. Unless required, We do not recommend that you alter these parameters.

- **Select CDP device capabilities**—Select the check box to enable.



**Note** Prime Infrastructure uses CDP to discover neighbors during tracing. When the neighbors are verified, Prime Infrastructure uses the CDP capabilities field to determine whether or not the neighbor device is a valid switch. If the neighbor device is not a valid switch, it is not traced.

- Step 4** Click **Save** to confirm changes made. Click **Reset** to return the page to the original settings. Click **Factory Reset** to return settings to the factory defaults.
- 

## Establishing Switch Port Tracing

To establish switch port tracing:

- 
- Step 1** In Prime Infrastructure home page, click the **Security** dashboard.
- Step 2** In the Rogue APs and Adhoc Rogues dashlet, click the number URL, which specifies the number of rogues in the last hour, last 24 hours, or total active. The Alarms window opens.
- Step 3** Choose the rogue you are setting switch port tracking by checking the checkbox.
- Step 4** From the **Troubleshoot** drop-down list, choose **Traceroute**. The Traceroute window opens, and Prime Infrastructure runs a switch port trace.

When one or more searchable MAC addresses are available, Prime Infrastructure uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue switch port.

See the “[Switch Port Tracing Details](#)” section on page 7-6 for additional information on the Switch Port Tracing Details dialog box.

---

## Switch Port Tracing Details

In the Switch Port Tracing Details dialog box, you can enable or disable switch ports, trace switch ports, and view detail status of the access point switch trace. For more information on Switch Port Tracing, see the following topics:

- [Configuring Switch Port Tracing](#)—Provides information on configuring switch port trace settings.
- [Configuring SNMP Credentials for Rogue AP Tracing](#)—Provides information on configuring SNMP switch credentials.

In the Switch Port tracing Details dialog box, do one of the following:

- Click **Enable/Disable Switch Port(s)**—Enables or disables any selected ports.
- Click **Trace Switch Port(s)**—Runs another switch port trace.
- Click **Show Detail Status**—Displays details regarding the switch port traces for this access point.
- Click **Close**.

## Switch Port Tracing Troubleshooting

Switch Port Tracing (SPT) works on a best-effort basis. SPT depends on the following information to correctly trace and contain rogue APs:

- Reporting access points—A rogue access point must be reported by one or more managed access points.
- Access point CDP neighbor—Access point Cisco Discovery Protocol (CDP) neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials
  - All the switches that need to be traced should have a management IP address and SNMP management enabled.
  - With the new SNMP credential changes, instead of adding the individual switches to Prime Infrastructure, network address based entries can be added.
  - The new SNMP credential feature has a default entry 0.0.0.0 with default community string as private for both read/write.
  - The correct write community string has to be specified to enable/disable switch ports. For tracing, a read community string should be sufficient.
- Switch port configuration
  - Switch ports that are trunking should be correctly configured as trunk ports.
  - Switch port security should be disabled.
- Only Cisco Ethernet switches are supported.




---

**Note** The following switches are supported: 3750, 3560, 3750E, 3560E, and 2960.

---

- Switch VLAN settings should be properly configured.
- CDP protocol should be enabled for all the switches.
- An Ethernet connection should exist between the rogue access point and the Cisco switch.
- There should be some traffic between the rogue access point and the Ethernet switch.
- The rogue access point should be connected to a switch within the max hop limit. Default hop is 2. Max hop is 10.
- If SNMPv3 is used, then make sure you use the context option and create one for each VLAN in addition to the one for the main group (which is required for non-VLAN based MIBs).





# Configuring High-Availability and Redundancy

---

The following topics describe how to manage the high-availability framework provided by Cisco Prime Infrastructure and redundancy framework on controllers:

- [Configuring High-Availability, page 8-1](#)
- [Configuring Redundancy, page 8-15](#)

## Configuring High-Availability

To ensure continued operation in case of failure, Prime Infrastructure now provides a high-availability or failover framework. When an active (primary) Prime Infrastructure fails, a secondary Prime Infrastructure takes over operations for the failed primary Prime Infrastructure and continues to provide service. Upon failover, a peer of the failed primary Prime Infrastructure is activated on the secondary Prime Infrastructure using the local database and files, and the secondary Prime Infrastructure runs a fully functional Prime Infrastructure. While the secondary host is in failover mode, the database and file backups of other primary Prime Infrastructure continue uninterrupted.

If email Address is specified in the high-availability configuration, the mail server must be configured and reachable to be notified about the failure.

The following topics describe the high-availability framework provided by Cisco Prime Infrastructure:

- [Failover and Failback Processes, page 8-2](#)
- [High-Availability Notation, page 8-3](#)
- [Health Monitor, page 8-3](#)
- [Data Storage, page 8-5](#)
- [Licensing, page 8-6](#)
- [Guidelines and Limitations for High-Availability, page 8-6](#)
- [High-Availability Status, page 8-7](#)
- [Deploying High-Availability, page 8-8](#)
- [Configuring High-Availability on the Primary Prime Infrastructure Server, page 8-9](#)
- [Adding a New Primary Prime Infrastructure Server in Existing High Availability Environment, page 8-10](#)
- [Removing High Availability Configuration, page 8-11](#)
- [Configuring an SSO Server in the High-Availability Environment, page 8-11](#)

- [Installing Software Updates in the High-Availability Environment, page 8-13](#)
- [Troubleshooting Issues in the High-Availability Environment, page 8-14](#)

## Failover and Failback Processes

There are two processes in high-availability: failover and failback. The following topics describe the failover and failback process:

- [Failover Scenario, page 8-2](#)
- [Failback Scenario, page 8-3](#)

### Failover Scenario

Failover is the process of activating the secondary Prime Infrastructure when the primary Prime Infrastructure fails. Failover can be initiated, either manually or automatically, depending on the failover type that is set during the high-availability configuration. For more information about configuring high-availability, see [“Configuring High-Availability on the Primary Prime Infrastructure Server” section on page 8-9](#).

If high-availability is configured with manual mode, the following events take place:

1. An email notification, containing the failure status and a link to the secondary Prime Infrastructure Health Monitor page, will be sent to the registered email address.
2. Using the link provided in the email notification, you can launch the Health Monitor UI and initiate a failover.

If high-availability is configured with automatic mode, the following events take place:

1. The primary Prime Infrastructure is confirmed as non functioning (because of a hardware crash or a network crash) by the health monitor on the secondary Prime Infrastructure.
2. The secondary Prime Infrastructure instance is started immediately (using the configuration already in place) and uses the database of the primary. After a successful failover, the client should point to the newly activated Prime Infrastructure (the secondary Prime Infrastructure). The secondary Prime Infrastructure updates all wireless controllers with its own address as the trap destination. For wired devices, the trap destination for the primary and secondary Prime Infrastructure must be configured on the devices.




---

**Note** After a failover, for all devices, make sure you change the communication IP address from the primary Prime Infrastructure to the secondary Prime Infrastructure IP address.

---

3. The result of the failover operation is indicated as an event in the Health Monitor UI, or a critical alarm is sent to the administrator and to other Prime Infrastructure instances.



**Note**

---

If an out-of-memory error occurs on the Network Management System (NMS) server, failover must be initiated, either manually or automatically based on the high-availability configuration settings.

---

## Failback Scenario

Failback is the process of making the primary Prime Infrastructure instance as the active instance. Failback must be initiated manually. Use <https://<piip>:8082> to access the Health Monitor UI of the secondary Prime Infrastructure. Within the Health Monitor UI, use the authentication key to log in and initiate the failback process. Before initiating the failback process in the secondary Prime Infrastructure, you must start the primary Prime Infrastructure. The health monitor and the database processes starts.

When failback is initiated, the following events take place:

1. The database information and files are copied to the primary Prime Infrastructure server. The primary server mode changes to Primary Active, and the secondary server mode changes to Secondary Syncing.
2. All processes on the secondary Prime Infrastructure server go down except for the Health Monitor, and all processes on the primary Prime Infrastructure server start.
3. Failback operation takes more time than failover or registration operations when the secondary Prime Infrastructure server was in the active state for a long time.
4. During the failback process, if the primary Prime Infrastructure server goes down, failover is initiated to the secondary Prime Infrastructure server. A new primary Prime Infrastructure is installed with all the configuration settings of the old primary Prime Infrastructure. The secondary Prime Infrastructure is registered with the new primary Prime Infrastructure when the failback is initiated.

## High-Availability Notation

The high-availability implementation requires a secondary server that has sufficient resources (CPU, hard drive, memory, and network connection) to take over operation in the event that the primary system fails. The database instance on the secondary system is a hot standby for the primary instance.

The size of the primary and secondary servers must be the same. For example, if the primary Prime Infrastructure server is the express Open Virtual Appliance (OVA; see <http://www.fileinfo.com/extension/ova>), the secondary Prime Infrastructure server must also have express OVA.

The primary and secondary server can be a mix of a physical and a virtual appliance. For example, if the primary Prime Infrastructure server is a physical appliance, the secondary server can be either a physical appliance or a standard OVA virtual appliance; for example, the server configuration and sizing of standard OVA is the same as the physical appliance. For more information about the OVA options, see *Cisco Prime Infrastructure 2.0 Quick Start Guide*.

## Health Monitor

The Health Monitor is the primary component that manages the Health Monitor operation of the system. Health Monitor is divided into multiple submodules:

**Table 8-1 Health Monitor Submodules**

Name	Description
Core Health Monitor	<ul style="list-style-type: none"> <li>• Configures the overall Health Monitor system.</li> <li>• Maintains the state machine for the Health Monitor system.</li> <li>• Starts and stops the Health Monitor and the Prime Infrastructure Java Virtual Machine (JVM).</li> <li>• Starts, stops, and monitors other submodules within the Health Monitor.</li> <li>• Handles registration of the primary/secondary pair.</li> <li>• Authenticates the Health Monitor-specific session.</li> <li>• Makes all decisions about failover and failback.</li> </ul>
Heart Beat	<p>Maintains communication between the primary and secondary Health Monitors. Communication occurs over HTTPS (the default port is 8082). The timeout value is two seconds. A retry mechanism has been implemented to retry establishing connectivity between the primary Health Monitor and secondary Health Monitor. If the Health Monitor does not receive a response after sending a heartbeat request within the timeout period, it retries establishing communication by sending another heartbeat request. If communication has not been established after three retries, the Health Monitors take appropriate action according to the following defined scenarios:</p> <ul style="list-style-type: none"> <li>• Primary server goes down: This is the classic failover case. In this scenario, when the secondary Health Monitor does not receive heartbeat requests for six seconds (3 retries x 2 seconds), it initiates the failover mechanism on the secondary Prime Infrastructure Health Monitor.</li> <li>• Secondary server goes down: In this scenario, the primary Health Monitor does not receive a heartbeat response from the secondary Health Monitor for six seconds (3 retries x 2 seconds). When this happens, the primary Health Monitor changes its state to PRIMARY_ALONE, raises alarms, and changes into listening mode (waiting to receive any messages from the secondary Health Monitor for reestablishing the link between the primary Health Monitor and the secondary Health Monitor).</li> </ul>
Application Monitor	<p>Communicates with the Prime Infrastructure framework (the Prime Infrastructure JVM) on the local server to retrieve status information. Communication is performed using Simple Object Access Protocol (SOAP) over HTTPS.</p>
DB Monitor	<p>Configures the database for replication. It is not responsible for the database replication itself; this is accomplished using the database proprietary replication protocol.</p>



**Table 8-1 Health Monitor Submodules (continued)**

Name	Description
File Synchronization	<p>This submodule consists of these components:</p> <ul style="list-style-type: none"> <li>• <b>File Archiver:</b> Periodically scans directories looking for files that have been modified, collects any such files, and adds them to a .tar archive.</li> <li>• <b>File Transfer Agent (FTA):</b> Transfers the compressed TAR archive to the destination (the other server, that is, from primary to secondary or from secondary to primary).</li> <li>• <b>File Upload Servlet (FUS):</b> Runs on the secondary server and is the counterpart to the FTA. When it receives a file, the FUS streams it directly to the TAR extractor rather than create the file on the local disk (avoids unnecessary disk activity). The FTA and FUS communicate over HTTPS.</li> <li>• <b>Statistics Collector:</b> Keeps statistics of file transfer operations from the time the server starts.</li> </ul>

## Data Storage

The Prime Infrastructure database is the core data storage element of the system and must be replicated between primary and backup systems in real time without data loss. This is fundamental to the operation of Prime Infrastructure high-availability. Data is stored in one of two ways:

- Prime Infrastructure database
- Application data

Application data is a set of flat files that contains the following data:

- All files under the TFTP root directory: Replicated through batch processing (every 500 seconds). The following real time, batch and Compliance and Audit Manager files are copied from the primary Prime Infrastructure to the secondary Prime Infrastructure:
  - **Batch\_Directory**—\$APPLROOT/domainmaps/, \$APPLROOT/licenses/, \$REPORTREPOSITORY/, \$APPLROOT/conf/sam/, \$APPLROOT/conf/da/, DBDBS=\$DBHOME/dbs
  - **Batch\_File**—=\$APPLROOT/conf/rfm/classes/com/cisco/server/reports/conf/\*.xml, \$APPLROOT/da/pkcapfiles/\*.pcap, \$APPLROOT/conf/rfm/classes/com/cisco/server/resources/MonitorResources.properties, \$APPLROOT/conf/rfm/classes/com/cisco/webui/resources/MonitorResources.properties, \$APPLROOT/conf/ifm\_app\_ui\_wap\_rs.xml, \$APPLROOT/conf/ifm\_bean\_context.xml, \$APPLROOT/tomcat/webapps/webacs/WEB-INF/classes/config/MailServer.properties, \$APPLROOT/tomcat/webapps/webacs/WEB-INF/classes/wap/registry/json/navigation.json, \$APPLROOT/conf/ComplianceEngine.properties, \$APPLROOT/conf/jobapprover.properties
  - **Batch File Copy**—This copies the least frequently used files to a remote machine.
  - **RealTime\_File**—=\$TFTPBOOT/\*-cfg, \$TFTPBOOT/\*.cfg, opt/CSColumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml
  - **Real Time Copy**—This copies the most frequently used files to a remote machine.
- Scheduled generated reports: Replicated in real time (11 seconds).

## Licensing

Only one Prime Infrastructure server license must be purchased; there is no need to purchase a license for the secondary Prime Infrastructure server. The secondary server will use the license from the primary when a failover occurs. The secondary node will simulate the Unique Device Identifier (UDI) information of the primary; thus the secondary server will be able to use the synchronized license from the primary server when the secondary server is active.

The same Prime Infrastructure license file resides on both the primary and secondary Prime Infrastructure servers. Because the Prime Infrastructure JVM is only running on the primary or secondary (not both), the license file is only active on one system at a given point in time.

## Guidelines and Limitations for High-Availability

Before initiating failover, you must consider the following prerequisites and limitations:

- You must have the hardware identical to the primary Prime Infrastructure to run a standby instance of Prime Infrastructure.
- Prime Infrastructure supports high-availability on both the physical and virtual appliance deployment models.
- A reliable high-speed wired network must exist between the primary Prime Infrastructure and its backup Prime Infrastructure.
- The primary and secondary Prime Infrastructure must be running the same Prime Infrastructure software release.
- The OVA file size in both primary and secondary Prime Infrastructure must be the same.
- Both primary and secondary Prime Infrastructure must be reachable on both sides.
- The health monitor process for the secondary Prime Infrastructure must be running during the high-availability registration.
- High reliable network must exist between the primary and secondary Prime Infrastructure.
- For primary Prime Infrastructure to initiate high-availability with a secondary Prime Infrastructure, the secondary Prime Infrastructure services must be running and reachable from the primary Prime Infrastructure. Therefore, you must boot the secondary Prime Infrastructure first, and then boot the primary Prime Infrastructure to initiate high-availability registration.
- Failover should be considered temporary. The failed primary Prime Infrastructure should be restored to normal as soon as possible, and failback is initiated. The longer it takes to restore the failed primary Prime Infrastructure, the longer the other Prime Infrastructure sharing that secondary Prime Infrastructure must run without failover support.
- The latest controller software must be used.
- The primary and secondary host are not required to share the same subnet. They can be geographically separated.
- If a secondary host fails for any reason, all the primary instances are affected, and they run in standalone mode without any failover support.
- The ports over which the primary and secondary Prime Infrastructure communicate must be open (not blocked with network firewalls, application firewalls, gateways, and so on). The tomcat port is configurable during installation, and its default port is 8082. You should reserve 1522 for solid database port.

- Any access control lists imposed between the primary and secondary Prime Infrastructure must allow traffic to go between the primary and secondary Prime Infrastructure.
- The primary Prime Infrastructure must have a sufficient number of licenses for the devices. When failover occurs, the secondary Prime Infrastructure uses the licenses of the primary Prime Infrastructure for the devices.
- A secondary Prime Infrastructure can only support one primary Prime Infrastructure.
- When high-availability is enabled for the first time, synchronizing the servers takes a considerable amount of time. The time it would take would be in the order of 30 minutes or more depending on the size of the database.
- During the high-availability registration, ensure that the bandwidth between the primary Prime Infrastructure and the secondary Prime Infrastructure is 1Gbps.
- Ensure that you remove high-availability from the Prime Infrastructure server before initiating the high-availability registration.

## High-Availability Status

To view high-availability details:

- 
- Step 1** Choose **Administration > High Availability**.
- Step 2** Choose **HA Status** from the left sidebar menu. The following information is displayed:
- Current status
  - Time, state, and description of each event
- 

Table 8-2 provides details about the different statuses of high-availability.

**Table 8-2 High-Availability Statuses**

HA Status	Description
HA Not Configured	High-availability is not configured yet.
Primary Alone	The primary Prime Infrastructure is alone and not synchronizing with the secondary Prime Infrastructure.
HA Initializing	High-availability is initializing.
Primary Active	The primary Prime Infrastructure is synchronizing with the secondary Prime Infrastructure without problems.
Primary Lost Secondary	The primary Prime Infrastructure has lost connectivity with the secondary Prime Infrastructure.
Primary Failback	A failback to the primary Prime Infrastructure is being done.
Primary Uncertain	The primary Prime Infrastructure is uncertain about the state of the secondary Prime Infrastructure.
Secondary Alone	The secondary Prime Infrastructure is alone and not synchronizing with the primary Prime Infrastructure.
Secondary Syncing	The secondary Prime Infrastructure is synchronizing with the primary Prime Infrastructure without problems.

**Table 8-2 High-Availability Statuses (continued)**

HA Status	Description
Secondary Active	High-availability has failed over the primary Prime Infrastructure and the application is running on the secondary Prime Infrastructure and is active.
Secondary Lost Primary	The secondary Prime Infrastructure has lost connectivity with the primary Prime Infrastructure.
Secondary Failover	A failover is being done to the secondary Prime Infrastructure.
Secondary Post Failback	A failback is in the post step.
Secondary Uncertain	The secondary Prime Infrastructure is uncertain about the state of the primary Prime Infrastructure.

## Deploying High-Availability

To deploy high-availability on an existing Prime Infrastructure installation:

- 
- Step 1** Identify and prepare the hardware to run the secondary Prime Infrastructure.
  - Step 2** Ensure that network connectivity between the primary and secondary Prime Infrastructure is functioning, and all necessary ports are open.
  - Step 3** Install the same version of Prime Infrastructure for the secondary server as was installed for the primary server.
  - Step 4** Upgrade the primary Prime Infrastructure and secondary Prime Infrastructure to the new version.
  - Step 5** Start the primary Prime Infrastructure. All processes start, including the Health Monitor.
  - Step 6** Configure the high-availability parameters described in the [“Configuring High-Availability on the Primary Prime Infrastructure Server”](#) section on page 8-9.
  - Step 7** Activate high-availability on the primary Prime Infrastructure. The primary Prime Infrastructure first copies its database to the secondary Prime Infrastructure and then connects to the secondary. The following files are copied over from the primary to the secondary Prime Infrastructure:
    - DB password file
    - All auto provisioning startup config files
    - All domain maps
    - All history reports that are generated by scheduled report tasks

High-availability deployment is complete. Use `https://<piip>:8082` to access the HealthMonitor UI. Within the HealthMonitor UI, use the authentication key to log in.

You can change the authentication key in Prime Infrastructure, view the current status of the health monitor, and remove the configuration settings using the command prompt. Enter the following commands:

- **AL-249-HA-PRIM/admin# ncs ha authkey**—To update the authentication key for high-availability.
- **AL-249-HA-PRIM/admin# ncs ha remove**—To remove the high-availability configuration.
- **AL-249-HA-PRIM/admin# ncs ha status**—To view the current status of high-availability.

For more information about these commands, see the [Command Reference Guide for Cisco Prime Infrastructure, Release 2.0](#).

---

## Configuring High-Availability on the Primary Prime Infrastructure Server

You will need to specify the Prime Infrastructure role (primary or secondary) during installation.

### Before You Begin

1. Before you can configure high-availability, you must configure a mail server. See “[Configuring Email Settings](#)” section on page 2-5 for information about configuring a mail server.
2. If you plan to specify an email address on the HA Configuration page, first make sure that a mail server is configured and reachable.



#### Note

When database transaction logs grow to one-third of the database partition disk space, set the database to standalone mode to prevent transaction logs from growing further. However, a complete *netcopy* is required the next time a database synchronization occurs.

---

To configure high-availability on the primary Prime Infrastructure server:

---

**Step 1** Choose **Administration > High Availability**.

**Step 2** Choose **HA Configuration** from the left sidebar menu. The High Availability Configuration page appears.

The current status of high-availability is shown in the upper portion of the page. For information about different statuses of high-availability, see [Table 8-2](#).

**Step 3** Enter the IP address or hostname of the secondary Prime Infrastructure.



#### Note

If the secondary Prime Infrastructure has a multihomed IP address, the first IP address (eth0) will be registered for high-availability.

---

**Step 4** Enter the authentication key specified during the installation of the secondary Prime Infrastructure.

**Step 5** The default admin email address that you configured in Administration > Settings > E-mail Server is automatically supplied. You can make any necessary changes. Any changes you make to these e-mail addresses must also be entered in the Secondary SMTP Server section of the Administration > Settings > Mail Server page.



#### Note

You must enter an email address when configuring high-availability for failure notifications. Prime Infrastructure tests the email server configuration, and if the test fails (because the mail server cannot connect), Prime Infrastructure cannot send a failure notification. You can still start the high-availability registration.

---

**Step 6** From the Failover Type drop-down list, choose either manual or automatic. If you choose manual, you can trigger the failover operation with a button in the secondary HealthMonitor graphical user interface or with the URL specified in the email that the administrator receives upon failure of the primary Prime Infrastructure. If you choose automatic, the secondary Prime Infrastructure initiates a failover on its own when a failure is detected on the primary.

**Step 7** Click **Save** to retain the configuration and enable high-availability, or click **Remove** to disable high-availability and its settings.

The Remove button is only available if high-availability is already configured. While failover is in progress do not remove HA using CLI.

At this point, the secondary is either reachable with the database, and files are synchronized between health monitors, or the secondary is unreachable, and an error is returned because secondary installation did not occur.

## Adding a New Primary Prime Infrastructure Server in Existing High Availability Environment

To add a new primary Prime Infrastructure server to an existing high availability environment, follow these steps. This new primary Prime Infrastructure uses the existing secondary as the failover server.

Note that any given HA environment must have exactly one primary and one secondary server. You cannot add a new primary server to a given HA environment unless the old primary server is first brought down or removed.

- Step 1** Install the correct version of Prime Infrastructure on the primary Prime Infrastructure.
- Step 2** Start the new primary Prime Infrastructure. All processes start, including the Health Monitor.
- Step 3** Ensure that network connectivity between the new primary and secondary is functioning and that all necessary ports are open.
- Step 4** Make sure that the same Prime Infrastructure release that is loaded on the other primary Prime Infrastructure and secondary Prime Infrastructure is loaded on the new primary Prime Infrastructure.



**Note** Ensure that the IP address and other configuration settings for the new primary Prime Infrastructure are the same as they were for the old primary Prime Infrastructure.

**Step 5** Launch the Health Monitor web UI of the secondary Prime Infrastructure (**Administration > High Availability > HA Status > Launch Health Monitor**).

or

Use `https://<piip>:8082` to access the HealthMonitor UI. Within the HealthMonitor UI, use the authentication key to log in.

**Step 6** On the Health Monitor Details page of the secondary Prime Infrastructure, click **Failback**.

The database and other configuration files are copied from the secondary Prime Infrastructure to the new primary Prime Infrastructure. The registration of the new primary Prime Infrastructure with the existing secondary Prime Infrastructure is started. After the primary Prime Infrastructure connects to the secondary, the Health Monitor on the primary connects to the secondary Health Monitor. They mutually acknowledge each other and start the monitoring.

---

## Removing High Availability Configuration

There are two ways to remove High Availability Configuration:

- [Remove High Availability Configuration from Primary UI](#)
- [Remove High Availability Configuration from Primary or Secondary CLI](#)

### Remove High Availability Configuration from Primary UI

During Primary Active state, you can remove the High Availability from Primary UI. To do this, go to **Administration > High Availability > High Availability Configuration** and click the Remove button. It will remove both the Primary and Secondary High Availability configurations.

### Remove High Availability Configuration from Primary or Secondary CLI

To remove High Availability Configuration from Primary or Secondary CLI:

- 
- Step 1** Login as admin user.
- Step 2** Use `ncs ha remove` command.
- Step 3** Provide your inputs on whether to remove only one server or both servers.
- Based on your input, the High Availability configuration will be removed.
- 

## Configuring an SSO Server in the High-Availability Environment

Single Sign-On Authentication (SSO) is used to authenticate and manage users in a multi-user, multi-repository environment and to store and retrieve the credentials that are used for logging into disparate systems. You can set up Prime Infrastructure as the SSO server for other instances of Prime Infrastructure.

You can choose one of the following options to configure an stateful switchover (SSO) server in the high-availability environment:

- Configure server A as the primary Prime Infrastructure, server B as the secondary Prime Infrastructure, and server C as the SSO server for both servers A and B. When server A fails, server B, which has the secondary Prime Infrastructure installed, is activated and all the machines that are connected to server A will be redirected to server B. During failback, configuration changes are not required. If server C fails, the SSO functionality is disabled and the local authentication is available for other Prime Infrastructure instances.

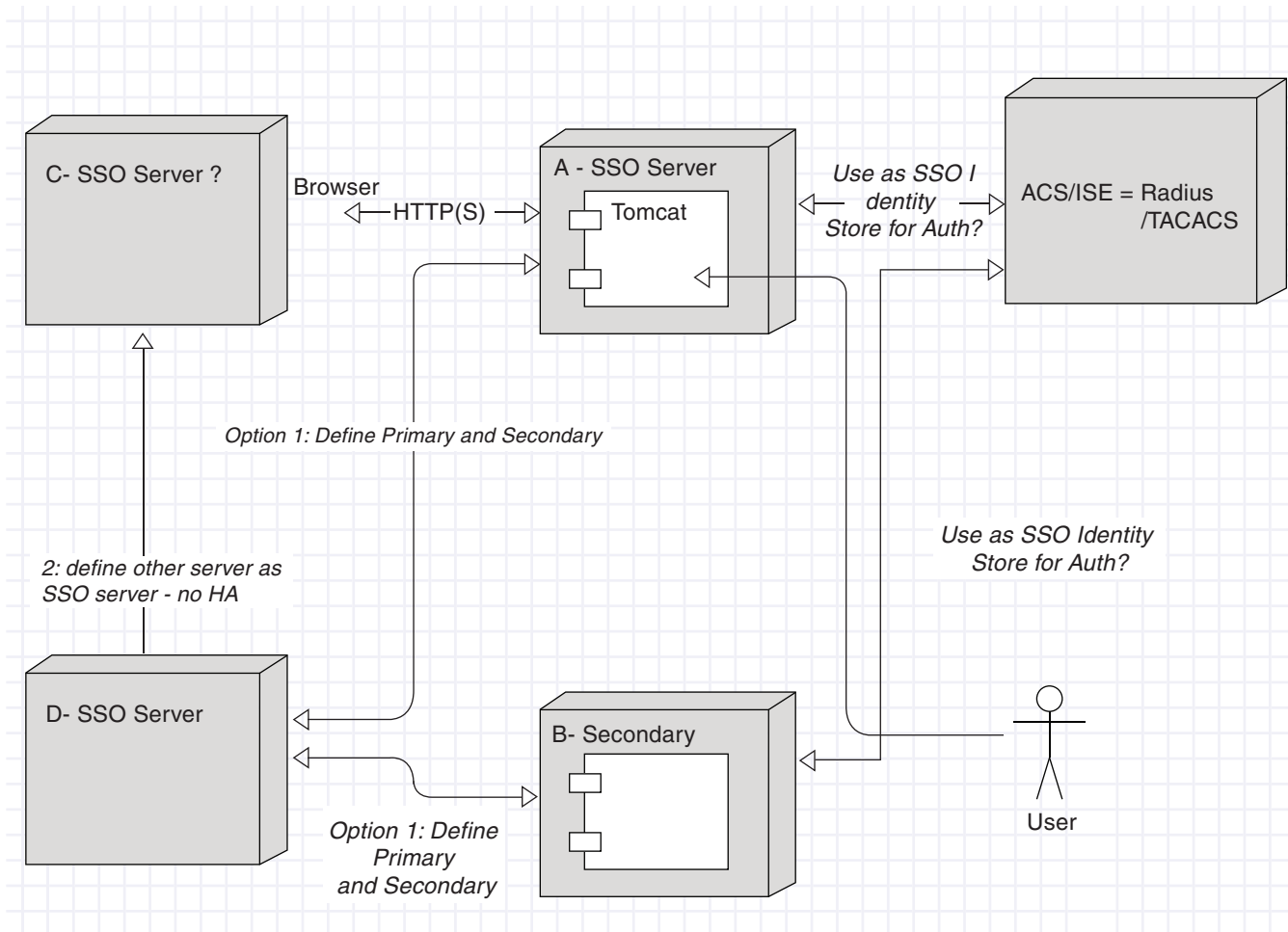
- Configure server A as the primary Prime Infrastructure and SSO server, and configure server B as the secondary Prime Infrastructure. When server A fails, server B, which has the secondary Prime Infrastructure installed is activated. But the machines that are connected to server A will not be redirected to server B because the SSO server is also configured in server A that has failed. For all Prime Infrastructure instances to get redirected to the secondary Prime Infrastructure, the SSO server must be active. So, you must configure server B as the failback option to the SSO server. If server B is not configured as the failback option to the SSO server, you will still be able to authenticate using local authentication but you will not be able to share sessions.

For information about how to add an SSO server, see [Adding an SSO Server, page 9-17](#)

You can also define a AAA server for the primary SSO server. For more information about configuring AAA server mode for an SSO server, see “[Configuring SSO Server AAA Mode](#)” section on page 9-17. When the primary SSO server fails and the secondary SSO server becomes active, the AAA server mode settings that you configured on the primary SSO server will automatically be configured on the secondary SSO server.

[Figure 8-1](#) is an example of how to configure an SSO server in the high-availability environment.

**Figure 8-1 SSO Configuration Options in High-Availability**





## Installing Software Updates in the High-Availability Environment

You can install software updates on the high-availability environment under the following scenarios:

- When the high-availability status is Primary Alone, that is, when the primary Prime Infrastructure is alone and not synchronizing with the secondary Prime Infrastructure.
- When high-availability is configured with manual failover type.
- When high-availability is configured with automatic failover type.

The following topics provide instructions on how to install software updates on the high-availability environment:

- [Software Update on High-Availability with Primary Alone, page 8-13](#)
- [Software Update on High-Availability with Manual Failover Type, page 8-13](#)
- [Software Update on High-Availability with Automatic Failover Type, page 8-14](#)

### Software Update on High-Availability with Primary Alone

To install software updates when the high-availability status is Primary Alone:

- 
- Step 1** Install the primary and secondary Prime Infrastructure servers. Ensure that both servers have the same version of Prime Infrastructure installed.
- Step 2** Download the latest software update file (with the extension .ubf) and install the file on the primary Prime Infrastructure when the high-availability status is Primary Alone. For more information on how to install software updates, see [Downloading Device Support and Product Updates, page 3-9](#).
- Step 3** Restart the primary Prime Infrastructure and complete the high-availability registration between the primary and secondary Prime Infrastructure.
- Step 4** Install the software update file on the secondary Prime Infrastructure.



---

**Note** Restarting the secondary Prime Infrastructure is not required because when the failover is initiated, based on the failover type, the secondary Prime Infrastructure is restarted.

---

If secondary Prime Infrastructure is in synching state, you can use the Software-Update link in the HealthMonitor page to launch the software update page. In other states, you will not be able to find the Software-Update link in HealthMonitor Page. If secondary Prime Infrastructure is in active state, you can navigate to **Admin > Software Update** to update the software in secondary server.

---

### Software Update on High-Availability with Manual Failover Type

To install software updates when the high-availability is configured with manual failover type:

- 
- Step 1** Install the primary and secondary Prime Infrastructure servers. Ensure that both servers have the same version of Prime Infrastructure installed.
- Step 2** Complete the high-availability registration between the primary and secondary Prime Infrastructure servers.

- Step 3** Download the latest software update file (with the extension .ubf) and install the file on the primary Prime Infrastructure. For more information on how to install software updates, see [Downloading Device Support and Product Updates, page 3-9](#).
- Step 4** Restart the primary Prime Infrastructure. The secondary Prime Infrastructure will not be in the active state now because the failover type for the high-availability is configured as manual. The primary Prime Infrastructure attempts to register with the secondary Prime Infrastructure and the high-availability registration is completed.
- Step 5** Install the software update file on the secondary Prime Infrastructure.




---

**Note** Restarting the secondary Prime Infrastructure is not required because when you initiate the failover, the secondary Prime Infrastructure is restarted.

---

## Software Update on High-Availability with Automatic Failover Type

To install software updates when the high-availability is configured with automatic failover type:

- 
- Step 1** Install the primary and secondary Prime Infrastructure servers. Ensure that both servers have the same version of Prime Infrastructure installed.
- Step 2** Complete the high-availability registration between the primary and secondary Prime Infrastructure servers.
- Step 3** Download the latest software update file (with the extension .ubf) and install the file on the primary Prime Infrastructure. For more information on how to install software updates, see [Downloading Device Support and Product Updates, page 3-9](#).
- Step 4** Restart the primary Prime Infrastructure. The secondary Prime Infrastructure will be in the active state now because the failover type for the high-availability is configured as automatic. So, only the health monitor and database processes in the primary Prime Infrastructure starts.
- Step 5** Initiate the failback process.
- Step 6** Install the software update file on the secondary Prime Infrastructure before you stop the primary Prime Infrastructure. When the failover is initiated, the secondary Prime Infrastructure is restarted.
- 

## Troubleshooting Issues in the High-Availability Environment

Following are the possible issues that can occur in the high-availability environment:

- The primary or secondary Prime Infrastructure goes down during the high-availability registration process.
- The primary or secondary Prime Infrastructure goes down during the failback process.
- The secondary Prime Infrastructure goes down during the failover process.

The possible causes for the above issues can be that the database or the NMS server has failed to start.

To avoid these issues:

1. Make sure that you have a backup before starting the high-availability registration or initiating the failback process.
2. If there is any issue with starting the database or the process, complete the following in the primary Prime Infrastructure:
  - a. Run the following command to re-create a new database:  
**/opt/CSCOLumos/bin/dbmigrate.sh recreateDB**  
or run the following command in admin console to re-create a new database:  
**ncs run reset db**
  - b. Run the following command to remove the existing database:  
**rm /opt/CSCOLumos/.dbCreated**
  - c. Stop all the processes.
  - d. Start all the processes.
  - e. Restore the backup and continue with the high-availability registration.

## Configuring Redundancy

The term *redundancy* in the Prime Infrastructure refers to the high-availability framework in controllers. Redundancy in wireless networks allows you to reduce the downtime of the networks. In a redundancy architecture, one controller is in the Active state and a second controller is in the Standby state, which continuously monitors the health of the controller in the Active state through a redundant port. Both controllers share the same configurations including the IP address of the management interface.

The Standby or Active state of a controller is based on the redundancy stock keeping unit (SKU), which is a manufacturing ordered unique device identification (UDI). A controller with redundancy SKU UDI is in the Standby state for the first time when it boots and pairs with a controller that runs a permanent count license. For controllers that have permanent count licenses, you can manually configure whether the controller is in the Active state or the Standby state.

In this release, a stateful switchover of access points (AP SSO) is supported. An AP SSO ensures that the AP sessions are intact even after a switchover.



### Note

---

The stateful switchover of clients is not supported, which means that all clients, with the exception of clients on locally switched WLANs on access points in FlexConnect mode, are deauthenticated and forced to reassociate with the new controller in the Active state.

---

This topic contains the following topics:

- [Prerequisites and Limitations for Redundancy, page 8-16](#)
- [Configuring Redundancy Interfaces, page 8-16](#)
- [Configuring Redundancy on a Primary Controller, page 8-17](#)
- [Configuring Redundancy on a Secondary Controller, page 8-18](#)
- [Monitoring the Redundancy States, page 8-19](#)
- [Running the Redundancy Status Background Task, page 8-19](#)
- [Configuring a Peer Service Port IP and Subnet Mask, page 8-20](#)

- [Adding a Peer Network Route, page 8-20](#)
- [Resetting and Uploading Files from the Secondary Server, page 8-21](#)
- [Disabling Redundancy on Controllers, page 8-21](#)

## Prerequisites and Limitations for Redundancy

Before configuring redundancy, you must consider the following prerequisites and limitations:

- The redundancy is supported only on the 5500, 7500, 8500, and Wism2 controllers.
- The primary and secondary controllers must be of the same hardware model.
- The primary and secondary controllers must be running the same Controller software release.
- The IP addresses of the management, redundancy management, and peer redundancy management interfaces must be in the same subnet.
- The service port IP address and route information is maintained for each device.
- If the redundancy is enabled on a controller, the Prime Infrastructure or any other device cannot manage the standby controller.
- You cannot enable the redundancy on a controller if the controller is added to the Prime Infrastructure through the service port. You must delete the controller and add it through the management interface to enable the redundancy on that controller.
- When there is an audit mismatch between a controller and the Prime Infrastructure, you must not restore the redundancy parameters from the Prime Infrastructure on to the controller. However, you can refresh the redundancy parameters in the Prime Infrastructure.
- Before you enable the redundancy, you must download the certificates for each device.
- Configuration is downloaded from the network to the active controller, and then the details are transferred to the standby controller through the redundancy interface.
- When an old active controller pairs up with the new active controller, the control is not transferred back to the old active controller and it becomes the standby controller for the new active controller.

## Configuring Redundancy Interfaces

There are two redundancy interfaces: redundancy-management interface and redundancy-port interface. The redundancy-management interface is a local physical management interface that shares the subnet mask, gateway, and VLAN ID from the management interface. You must configure only the IP address for the redundancy-management interface to enable redundancy on the primary and secondary controllers. The IP address for the redundancy-port interface is auto-generated and it is used internally.

- 
- Step 1** Choose **Operate > Device Work Center**.
  - Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
  - Step 3** Select the controller that you have chosen as the primary controller. The details of the device appear on the lower part of the page.
  - Step 4** Click the **Configuration** tab.
  - Step 5** From the left sidebar menu, choose **System > Interfaces**. The Interfaces list page appears.



**Note** If you are in the Classic view, choose **Configure > Controllers > Ctrl IP addr > System > Interfaces** to access the Interfaces list page.

- 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. From the Lifecycle view, choose **Operate > Device Work Center > Device Type > Wireless Controller > Controller > Configuration > Redundancy > Global Configuration** to access the Global Configuration details page. If you are in the Classic view, choose **Configure > Controllers > Ctrl IP addr > Redundancy > Global Configuration** to access the Global Configuration details page.

## Configuring Redundancy on a Primary Controller

To configure redundancy on a primary or active controller:

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the primary controller for which you have configured the redundancy-management interface IP address. The details of the controller appear on the lower part of the page.
- Step 4** Click the **Configuration** tab.
- Step 5** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.



**Note** If you are in the Classic view, choose **Configure > Controllers > Ctrl IP addr > Redundancy > Global Configuration** to access the Global Configuration details page.

- 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 parameters.



**Note** You cannot configure this controller during the redundancy pair-up process.

**Step 9** Click **Save**. The configuration is saved and the system reboots.

## Configuring Redundancy on a Secondary Controller

To configure redundancy on a secondary or standby controller:

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

**Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.

**Step 3** Select the controller that you have chosen as a secondary controller. The details of the controller appear on the lower part of the page.

**Step 4** Click the **Configuration** tab.

**Step 5** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration Details page appears.



**Note** If you are in the Classic view, choose **Configure > Controllers > Ctrl IP addr > Redundancy > Global Configuration** to access the Global Configuration details page.

**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 parameters.



**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 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.
- **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.
- **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 these traps, see [Cisco Prime Infrastructure Alarms and Events](#).

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. From the Lifecycle view, choose **Operate > Device Work Center > Device Type > Wireless Controller > Controller > Device Details > Redundancy > Redundancy States** to view these details. If you are in the Classic view, choose **Monitor > Controllers > Ctrl IP addr > Redundancy > Redundancy States** to view these details.

## Running the Redundancy Status Background Task

Sometimes when the peer state changes from StandbyCold to StandbyHot, the redundancy traps are missed by the Prime Infrastructure. As a result, the redundancy pair-up process cannot be completed. To fix this issue, you must run the Redundancy Status background task manually.

To run the Redundancy Status background task:

- Step 1** Choose **Administration > Background Tasks**.
- Step 2** Under the Other Background Tasks section, select the **Redundancy Status** background task.
- Step 3** From the Select a command drop-down list, select **Execute Now**.
- Step 4** Click **Go**.

When traps are missed by the Prime Infrastructure, you must run this background task to complete the following:

- Remove the standby controller from the Prime Infrastructure.
- Swap the network route table entries with the peer network route table entries.
- Update the redundancy state information and system inventory information.

Once the redundancy pair-up process is completed, the redundancy state for the active controller becomes Paired and the standby controller is removed from the Prime Infrastructure.

## Configuring a Peer Service Port IP and Subnet Mask

You can configure a peer service port IP address and a subnet mask only when the state of the peer controller is in StandbyHot. Ensure that DHCP is disabled on local service port before you configure the peer service port IP address.

To configure the peer service port IP and subnet mask:

- 
- Step 1** Choose **Operate > Device Work Center**.
  - Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
  - Step 3** Select the primary or active controller. The details of the controller appear on the lower part of the page.
  - Step 4** Click the **Configuration** tab.
  - Step 5** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.



**Note** If you are in the Classic view, choose **Configure > Controllers > Ctrl IP addr > Redundancy > Global Configuration** to access the Global Configuration details page.

---

- Step 6** In the Peer Service Port IP field, enter the IP address of the peer service port.
  - Step 7** In the Peer Service Netmask IP field, enter the IP address of the peer service subnet mask.
  - Step 8** Click **Save**.
- 

## Adding a Peer Network Route

You can add a peer network route on an active controller only when the state of the peer controller is in StandbyHot. A new network route table is maintained. When the standby controller becomes active, the entries of the network route table swaps with the entries of the peer network route table.

To add a peer network route:

- 
- Step 1** Choose **Operate > Device Work Center**.
  - Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
  - Step 3** Select the primary controller for which you have configured the redundancy-management interface IP address. The details of the controller appear on the lower part of the page.
  - Step 4** Click the **Configuration** tab.
  - Step 5** From the left sidebar menu, choose **Redundancy > Peer Network Route**.





**Note** If you are in the Classic view, choose **Configure > Controllers > Ctrl IP addr > Redundancy > Peer Network Route** to access the Peer Network Route list page.

- 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 following fields:
- IP Address—Enter the IP address of the peer network route.
  - IP Netmask—Enter the subnet mask of the peer network route.
  - Gateway IP Address—Enter the IP address of the peer network route gateway.
- Step 9** Click **Save**. The peer network route is added.

## Resetting and Uploading Files from the Secondary Server

You can reset the secondary server when the secondary server is in the StandbyHot state and the high-availability pair-up process is complete. You can also upload the files from the secondary server to the primary server.

To reset the secondary server and upload files:

- Step 1** Choose **Operate > Device Work Center > Device Type > Wireless Controller > Controller**.
- Step 2** Select the primary server for which you have configured the redundancy-management interface IP address, then click the **Configuration** tab.
- Step 3** From the left sidebar menu, choose **Device Details > Redundancy > Redundancy Commands**.



**Note** If you are in the Classic view, choose **Configure > Controllers > Ctrl IP addr > Redundancy > Redundancy Commands**.

- Step 4** Choose **Reset Standby** to reset the secondary server.
- Step 5** Choose **Upload File from Standby Controller** to upload files from the secondary server to primary server.

## Disabling Redundancy on Controllers

To disable redundancy on a controller:

- Step 1** Choose **Operate > Device Work Center**.
- Step 2** Under the Device Group group box, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the controller for which you want to disable the redundancy. The details of the controller appear on the lower part of the page.

- Step 4** Click the **Configuration** tab.
- Step 5** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.



---

**Note** If you are in the Classic view, choose **Configure > Controllers > Ctrl IP addr > Redundancy > Global Configuration** to access the Global Configuration details page.

---

- Step 6** Deselect the **Enabled** check box for the redundancy mode to disable the redundancy on the selected controller.
- Step 7** Click **Save**. The configuration is saved and the system reboots.
- When you disable redundancy on the controller, both active and standby controllers reboot. You must refresh the configuration from the device to remove any audit mismatches in the redundancy parameters. The active controller becomes a standalone controller and the standby controller reboots with all the ports disabled.
-



# Controlling User Access

---

This chapter contains the following topics:

- [Managing User Accounts, page 9-1](#)
- [Creating User Groups to Control Access to Prime Infrastructure Functions, page 9-4](#)
- [Changing Display Preferences, page 9-5](#)
- [Using Virtual Domains to Control Access to Sites and Devices, page 9-6](#)
- [User Access in Virtual Domains, page 9-10](#)
- [Auditing User Access, page 9-13](#)
- [Configuring AAA on Prime Infrastructure, page 9-15](#)

## Managing User Accounts

You can perform the following actions on user accounts:

- [Viewing Active User Sessions, page 9-1](#)
- [Adding Users, page 9-2](#)
- [Creating Administrative Users, page 9-2](#)
- [Configuring Guest Account Settings, page 9-3](#)
- [Disabling User Accounts, page 9-3](#)
- [Changing User Passwords, page 9-3](#)
- [Changing User Access to Prime Infrastructure Functions, page 9-4](#)
- [Changing Password Policy, page 9-4](#)

## Viewing Active User Sessions

All Prime Infrastructure users have basic parameters such as a username and password. Users with admin privileges can view active user sessions.

To view active sessions:

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Active Sessions**.
- Step 2** Click the **Audit Trail** icon for the username for which you want to see the following data:

- User—User login name
- Operation—Type of operation audited
- Time—Time operation was audited
- Status—Success or failure
- Reason—Failure reason when the user login failed
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click the Details link for more information on the configuration changes done by an individual user.



**Note** The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

## Adding Users

You can add a user and assign predefined static roles to that user. Besides complete access, you can give administrative access with differentiated privileges to certain user groups.

Prime Infrastructure supports user authentication via integration with external TACACS+ and RADIUS servers (see [Configuring AAA on Prime Infrastructure, page 9-15](#)). Note that Prime Infrastructure supports case-sensitive user names, while TACACS+ and RADIUS do not. If you plan to use external user authentication, be sure to avoid creating variations of user names that are only distinguished by their case. For example, if you create Prime Infrastructure users named User, USER and user, Prime Infrastructure will treat them as three different users, while external AAA servers will validate all three of them as the same user. If these three users have different privileges, this can lead to security problems.

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Users**.
  - Step 2** Choose **Add a User**, then click **Go**.
  - Step 3** Enter the username, password, and confirm password for the new user, then choose the groups to which this user belongs.
  - Step 4** Click the Virtual Domains tab to assign a virtual domain to this user (see [User Access in Virtual Domains, page 9-10](#)), then click **Save**.
- 

## Creating Administrative Users

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Users**.
  - Step 2** Choose **Select a command > Add User**, then click **Go**.
  - Step 3** Complete the required fields, then click **Admin** to give the user administrator privileges.
  - Step 4** Click **Save**.
-

## Configuring Guest Account Settings

The **Administration > System Settings > Guest Account Settings** page allows you to globally remove all expired guest accounts.

To configure guest account settings:

- 
- Step 1** Choose **Administration > System Settings**.
  - Step 2** From the left sidebar menu, choose **Guest Account Settings**.
  - Step 3** When the **Automatically remove expired guest accounts** check box is selected, the guest accounts whose lifetime has ended are not retained, and they are moved to the Expired state. Those accounts in the expired state are deleted from Prime Infrastructure.
  - Step 4** By default, a Prime Infrastructure Lobby Ambassador can access all guest accounts irrespective of who created them. If you select the **Search and List only guest accounts created by this lobby ambassador** check box, the Lobby Ambassadors can access only the guest accounts that have been created by them.
  - Step 5** Click **Save**.
- 

## Disabling User Accounts

You can disable a user account so that a user cannot log in to Prime Infrastructure. You might want to disable a user account when a user is on vacation or is temporarily changing job functions. By *locking* the user account, you disable the user's access to Prime Infrastructure. Later, you can *unlock* the user account, enabling access to Prime Infrastructure, without having to re-create the user.

To disable a user's access to Prime Infrastructure:

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Users**.
  - Step 2** Select the user whose access you want to disable, then choose **Select a command > Lock User(s)**.  
The next time the user tries to log in to Prime Infrastructure, a message appears saying the login failed because the account is locked.
- 

## Changing User Passwords

To change the password for a user:

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Users**.
  - Step 2** Select the user whose password you want to change.
  - Step 3** Complete the password fields, then click **Save**.
- 

### Related Topics

- [Adding Users](#)

- [Creating Administrative Users](#)

## Changing User Access to Prime Infrastructure Functions

Prime Infrastructure uses a list of tasks to control which part of Prime Infrastructure users can access and the functions they can perform in those parts. You change user privileges in Prime Infrastructure by changing the User Group to which each user belongs. You use the User Group Task List to change what users in each group are authorized to do and the screens they can access.

You can also assign the sites or devices to which a virtual domain has access.

To change user privileges:

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **User Groups**.
  - Step 2** Click a group name to change the tasks this group is allowed to perform.
  - Step 3** Click the Members tab to view the users of this group.
- 

## Changing Password Policy

Prime Infrastructure supports various password policy controls, such as minimum length, repeated characters, and so on.

To change password policies:

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Local Password Policy**.
  - Step 2** Chose the necessary policies, then click **Save**.
- 

## Creating User Groups to Control Access to Prime Infrastructure Functions

To simplify managing which users can perform which functions, you can assign users to user groups, and then specify which tasks the users in that group are allowed to perform. See [Table 9-1](#) for the default user groups available in Prime Infrastructure

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **User Groups**.
  - Step 2** Click a group name to change the tasks this group is allowed to perform.
  - Step 3** Click the Members tab to view the users of this group.
-

**Table 9-1** Default User Groups

User Group	Description
Admin	Group for Prime Infrastructure Administration.
Config Managers	Group for monitoring and configuration tasks.
Lobby Ambassador	Group to allow Guest user administration only. This group is not editable.
Monitor Lite	Group to allow monitoring of assets only. This group is not editable.
North Bound API	Group to allow access to North Bound APIs. This group is not editable.
Root	Group for root user. This group is not editable.
Super Users	Group to allow all Prime Infrastructure tasks.
System Monitoring	Group for monitoring only tasks.
User Assistant	Group to allow Local Net user administration only. This group is not editable.
User-Defined 1	User definable group.
User-Defined 2	User definable group.
User-Defined 3	User definable group.
User-Defined 4	User definable group.

## Changing Display Preferences

You can specify display options in Prime Infrastructure by choosing **Administration > User Preferences**. [Table 9-2](#) lists the options you can adjust.



**Note** When the non-root users log in to Prime Infrastructure and try to modify the user preferences, the “Permission Denied” message appears, which is an expected behavior.

To change the user-specific settings:

- Step 1** Choose **Administration > User Preferences**.
- Step 2** Use the Items Per List Page drop-down list to configure the number of entries shown on a given list page (such as alarms, events, AP list, and so on).
- Step 3** Specify how often you want the home page refreshed by selecting the **Refresh home page** check box and choosing a time interval from the Refresh home page every drop-down list.
- Step 4** Select the **Logout idle user** check box and configure the Logout idle user after text box, in minutes, that a user session can be idle before the server cancels the session.
- Step 5** If you want the maps and alarms page to automatically refresh when a new alarm is raised by Prime Infrastructure, select the **Refresh Map/Alarms page on new alarm** check box in the Alarms portion of the page.
- Step 6** From the Refresh Alarm count in the Alarm Summary every drop-down list choose a time interval to specify how often to reset.
- Step 7** If you do not want the alarm acknowledge warning message to appear, select the **Disable Alarm Acknowledge Warning Message** check box.

- Step 8** Click **Edit Alarm Categories** to select the alarm categories to display in the Alarm Summary page.
- Step 9** In the **Select Alarms** page, choose the default category to display from the drop-down list, and select the alarm categories and subcategories to display from the alarm toolbar. Click **Save** to save the alarm category list. The selected alarm category and subcategories appear in the User Preferences page.
- Step 10** Click **Save**.

**Table 9-2** User Preference Options

Option	Description
Items Per List	You can set the number of items, such as controllers or access points, to display in pages that list these items. Choose the number of items to display from the Items Per List Page drop-down list.
Use Next Generation Maps	Select the check box if you want to use the Next Generation Maps feature.
Logout idle user	Select the check box if you want to configure the amount of time, in minutes, that a user session can be idle before the server cancels the session. <b>Note</b> If the Logout idle user check box is unselected, the user session does not time out.
Logout idle user after	Choose the maximum number of minutes that a server waits for an idle user. The default value is 60 minutes. The minimum value is 15 minutes. The maximum value is 120 minutes. <b>Note</b> If the Logout idle user check box is unselected, the user session does not time out.
Refresh Map/Alarms page on new alarm	Select the check box to refresh map and alarm pages each time a new alarm is generated.
Refresh Alarm count in the Alarm Summary every	Choose the frequency of the Alarm Summary refresh from the drop-down list (every 5, seconds, 15 seconds, 30 seconds, 1 minute, 2 minutes, or 5 minutes).
Display Alarm Category in Alarm Summary page	Choose the alarm category that you want to display in the minimized Alarm Summary (Alarm Summary, Malicious AP, Unclassified AP, Coverage Holes, Security, Controllers, Access Points, Mobility Services, Mesh Links, Prime Infrastructure, or Performance).
Disable Alarm Acknowledge Warning Message	When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Click this check box to stop the warning message from displaying.
Choose alarms for Alarm Summary Toolbar	To select alarms for the Alarm Summary Toolbar, click <b>Edit Alarm Categories</b> and choose the required alarm categories and subcategories.

## Using Virtual Domains to Control Access to Sites and Devices

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



The email address and time zone that you specify in the Virtual Domains page (Administration > Virtual Domains) are used when scheduling and e-mailing domain specific reports. The scheduled time of the report can be set to the time zone specific to the virtual domain and the scheduled report can be e-mailed to the email address specified for the virtual domain. For more information, see the *Cisco Prime Infrastructure 2.0 User Guide*.

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

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

This section contains the following topics:

- [Understanding Virtual Domain Hierarchy, page 9-7](#)
- [Creating a Site-Oriented Virtual Domain, page 9-10](#)

## Understanding Virtual Domain Hierarchy

Virtual domains are organized hierarchically. Subsets of an existing virtual domain contain the network elements that are contained in the parent virtual domain. The default or “ROOT-DOMAIN” domain includes all virtual domains.

Because network elements are managed hierarchically, some features and components such as report generation, searches, templates, config groups, and alarms are affected.



### Note

---

If the configuration of a controller is modified by multiple virtual domains, complications might arise. To avoid this, manage each controller from only one virtual domain at a time.

---

This section describes the effects of partitioning and contains the following topics:

- [Reports, page 9-7](#)
- [Search, page 9-8](#)
- [Alarms, page 9-8](#)
- [Templates, page 9-8](#)
- [Config Groups, page 9-8](#)
- [Maps, page 9-8](#)
- [Access Points, page 9-9](#)
- [Controllers, page 9-9](#)
- [Email Notification, page 9-10](#)

## Reports

Reports only include components assigned to the current virtual domain. For example, if you create a virtual domain with only access points and no controllers assigned, all controllers are not displayed when you generate a controller inventory report.

If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

Reports are only visible in the current virtual domain. The parent virtual domain cannot view the reports from its subvirtual domain. Client reports such as Client Count only include clients that belong to the current virtual domain. If new clients are assigned to this partition by the administrator, the previous reports do not reflect these additions. Only new reports reflect the new clients.

## Search

Search results only include components that are assigned to the virtual domain in which the search is performed. Search results do not display floor areas when the campus is not assigned to the virtual domain.

The saved searches are only visible in the current virtual domain. The parent virtual domain cannot view these search results. Prime Infrastructure does not partition network lists. If you search a controller by network list, all controllers are returned. Search results do not display floor areas when the campus is not assigned to the virtual domain.

## Alarms

When a component is added to a virtual domain, no previous alarms for that component are visible to that virtual domain. Only new alarms are visible. For example, when a new controller is added to a virtual domain, any alarms generated for that controller prior to its addition do not appear in the current virtual domain.

Alarms are not deleted from a virtual domain when the associated controllers or access points are deleted from the same virtual domain.



---

**Note**

Alarm Email Notifications—Only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and Prime Infrastructure email notification.

---

## Templates

When you create or discover a template in a virtual domain, it is only available to that virtual domain unless it is applied to a controller. If it is applied to a controller and that controller is assigned to a subvirtual domain, the template stays with the controller in the new virtual domain.



---

**Note**

If you create a subvirtual domain and then apply a template to both network elements in the virtual domain, Prime Infrastructure might incorrectly reflect the number of partitions to which the template was applied.

---

## Config Groups

Config groups in a virtual domain can also be viewed by the parent virtual domain. A parent virtual domain can modify config groups for a sub (child) virtual domain. For example, the parent virtual domain can add or delete controllers from a subvirtual domain.

## Maps

You can only view the maps that your administrator assigned to your current virtual domain.

- When a campus is assigned to a virtual domain, all buildings in that campus are automatically assigned to the same virtual domain.

- When a building is assigned to a virtual domain, it automatically includes all of the floors associated with that building.
- When a floor is assigned, it automatically includes all of the access points associated with that floor.

If only floors are assigned to a virtual domain, you lose some ability to choose map-based features. For example, some reports and searches require you to drill down from campus to building to floor. Because campuses and buildings are not in the virtual domain, you are not able to generate these types of reports or searches.

Coverage areas shown in Prime Infrastructure are only applied to campuses and buildings. In a floor-only virtual domain, Prime Infrastructure does not display coverage areas. If a floor is directly assigned to a virtual domain, it cannot be deleted from the virtual domain which has the building to which the floor belongs.

**Note**

---

Search results do not display floor areas when the campus is not assigned to the virtual domain.

---

## Access Points

When a controller or map is assigned to a virtual domain, the access points associated with the controller or map are automatically assigned as well. Access points can also be assigned manually (separate from the controller or map) to a virtual domain.

If the controller is removed from the virtual domain, all of its associated access points are also removed. If an access point is manually assigned, it remains assigned even if its associated controller is removed from the current virtual domain.

If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

If a manually added access point is removed from a virtual domain but is still associated with a controller or map that is assigned to the same virtual domain, the access point remains visible in the virtual domain. Any alarms associated with this access point are not deleted with the deletion of the access point.

When maps are removed from a virtual domain, the access points on the maps can be removed from the virtual domain.

**Note**

---

If you later move an access point to another partition, some events (such as generated alarms) might reside in the original partition location.

---

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, Prime Infrastructure uses the detecting controller.

If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

## Controllers

Because network elements are managed hierarchically, controllers might be affected by partitioning. If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

If you create a partition with only a few controllers, choose **Configure > Access Points**, and click an individual link in the AP Name column, the complete list of Prime Infrastructure-assigned controllers is displayed for primary, secondary, and tertiary controllers rather than the limited number specified in the partition.

**Note**

If a controller configuration is modified by multiple virtual domains, complications might arise. To avoid this, manage each controller from only one virtual domain at a time.

**Email Notification**

Email notification can be configured per virtual domain. An email is sent only when alarms occur in that virtual domain.

**Creating a Site-Oriented Virtual Domain**

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

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

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

- 
- Step 1** Choose **Administration > Virtual Domains**.
  - Step 2** From the left Virtual Domain Hierarchy sidebar menu, click **New**.  
By default, only one virtual domain (*root*) is defined in Prime Infrastructure. The selected virtual domain becomes the parent virtual domain of the newly created, subvirtual domain.
  - Step 3** Enter **Site 1 Routers** for the virtual domain name, then click **Submit**.
  - Step 4** On the Sites tab, move the sites that you want to associate with the virtual domain to the Selected Sites column, then click **Submit**.
  - Step 5** Click **OK** on the confirmation screens.
- 

**User Access in Virtual Domains**

A Prime Infrastructure Virtual Domain consists of a set of Prime Infrastructure devices and/or maps and restricts a user view to information relevant to these managed objects.

Through a virtual domain, an administrator can ensure that users are only able to view the devices and maps for which they are responsible. In addition, because of the virtual domain filters, users are able to configure, view alarms, generate reports for *only* their assigned part of the network.

The administrator specifies for each user a set of allowed virtual domains. Only one of these can be active for that user at login. The user can change the current virtual domain by selecting a different allowed virtual domain from the Virtual Domain drop-down list at the top of the page. All reports, alarms, and other functionality are now filtered by that virtual domain.

If there is only one virtual domain defined (“root”) in the system AND the user does not have any virtual domains in the custom attributes fields in the TACACS+/RADIUS server, the user is assigned the “root” virtual domain by default. If there is more than one virtual domain, and the user does not have any specified attributes, then the user is blocked from logging in.

This section contains the following topics:

- [Adding Users to Virtual Domains, page 9-11](#)
- [Adding Sites and Devices to Virtual Domains, page 9-11](#)
- [Changing Virtual Domain Access, page 9-12](#)
- [Virtual Domain RADIUS and TACACS+ Attributes, page 9-13](#)

## Adding Users to Virtual Domains

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

**Note**

---

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

---

To add a user to a virtual domain:

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **Users**.
  - Step 2** Click the user you want to add to a virtual domain.
  - Step 3** Click the Virtual Domains tab.
  - Step 4** Move the virtual domain to which you want to add the user from the Available Virtual Domains column to the Selected Virtual Domains column, then click **Save**.

**Note**

---

Each virtual domain may contain a subset of the elements included with its parent virtual domain. When a user is assigned a virtual domain, that user can view the devices that are assigned to its virtual domain.

---

## Adding Sites and Devices to Virtual Domains

To add sites and devices to a virtual domain:

- 
- Step 1** Choose **Administration > Virtual Domains**.
  - Step 2** From the left Virtual Domain Hierarchy sidebar menu, click the virtual domain to which you want to add a site or device.

**Step 3** Move the sites and devices from the Available to the Selected column, then click **Submit**.

---

## Changing Virtual Domain Access

Choose a virtual domain from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned maps, controllers, access points, and switches. The Summary page appears. This page includes tabs for viewing the currently logged-in virtual domain-available maps, controllers, access points, and switches.

The Maps, Controllers, Access Points, and Switches tabs are used to add or remove components assigned to this virtual domain.

To assign a site map, controller, access point, or wired device to this domain:

---

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

**Step 2** Choose a virtual domain hierarchy from the Virtual Domain Hierarchy left sidebar menu.



**Note** Because all maps, controllers, and access points are included in the partition tree, it takes several minutes to load. This time increases if you have a system with a significant number of controllers and access points.

---

**Step 3** Click the applicable **Site Maps**, **Controller**, **Access Points**, or **Wired Devices** tab.

**Step 4** In the Available (Site Maps, Controllers, Access Points, or Wired Devices) column, click to highlight the new component(s) you want to assign to the virtual domain. Click **Add** to move the component(s) to the Selected (Site Maps, Controllers, Access Points, or Wired Devices) column.



**Note** To remove a component from the virtual domain, click to highlight the component in the Selected (Site Maps, Controllers, Access Points, or Wired Devices) column, and click **Remove**. The component returns to the Available column.

---



**Note** If you delete a switch, a controller, or an autonomous AP from the ROOT-DOMAIN, the device is removed from Prime Infrastructure. If the device is explicitly associated with the ROOT-DOMAIN or any other virtual domain that is not the child of the current virtual domain and if you delete the device from the current virtual domain, the device is removed from this virtual domain but it is not removed from Prime Infrastructure.

---

**Step 5** Click **Submit** to confirm the changes.

---

After assigning elements to a virtual domain and submitting the changes, Prime Infrastructure might take some time to process these changes depending on how many elements are added.

## Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes page allows you to indicate the appropriate protocol-specific data for each virtual domain. The Export button on the Virtual Domain Hierarchy left sidebar menu preformats the virtual domain RADIUS and TACACS+ attributes. You can copy and paste these attributes into the Access Control Server (ACS) server. This allows you to copy only the applicable virtual domains into the ACS server page and ensures that the users only have access to these virtual domains.

To apply the preformatted RADIUS and TACACS+ attributes to the ACS server:

- 
- Step 1** Choose **Administration > Virtual Domains**.
  - Step 2** From the Virtual Domain Hierarchy left sidebar menu, choose the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.
  - Step 3** Click **Export**.
  - Step 4** Highlight the text in the RADIUS or TACACS+ Custom Attributes list (depending on which one you are currently configuring), go to your browser menu, and choose **Edit > Copy**.
  - Step 5** Log in to ACS.
  - Step 6** Go to User or Group Setup.



**Note** If you want to specify virtual domains on a per-user basis, then you need to make sure you add all of the custom attributes (for example, tasks, roles, virtual domains) information to the User custom attribute page.

---

- Step 7** For the applicable user or group, click **Edit Settings**.
- Step 8** Use your browser Edit > Paste feature to place the RADIUS or TACACS+ custom attributes into the applicable field.
- Step 9** Select the check boxes to enable these attributes, then click **Submit + Restart**.



**Note** For more information on adding RADIUS and TACACS+ attributes to the ACS server, see the [“Adding Prime Infrastructure User Groups into ACS for TACACS+”](#) section on page 9-23 or the [“Adding Prime Infrastructure User Groups into ACS for RADIUS”](#) section on page 9-25.

---

## Auditing User Access

Prime Infrastructure maintains an audit record of user access. This section contains the following topics:

- [Accessing the Audit Trail for a User Group, page 9-14](#)
- [Viewing Application Logins and Actions, page 9-14](#)
- [Viewing Events Initiated by a User, page 9-14](#)

## Accessing the Audit Trail for a User Group

To access the audit trail for a user group:

- 
- Step 1** Choose **Administration > Users, Roles & AAA**, then click **User Groups**.
  - Step 2** Click the **Audit Trail** icon corresponding to the user group name for which you want to see the audit data. The Configuration Changes field provides a Details link if there are any configuration changes. Click the Details link for more information on the configuration changes done by an individual user.




---

**Note** The audit trail entries could be logged for individual device changes. For example, If a template is applied on multiple switches, then there will be multiple audit entries for each switch to which the template has been applied.

---

## Viewing Application Logins and Actions

Application audit logs log events that pertain to the Prime Infrastructure features. For example, you can view the application audit log to see when a particular user logged in and what actions were taken. Prime Infrastructure displays the IP address from which the user has logged in to Prime Infrastructure as well as the pages in Prime Infrastructure the user viewed.

To view application audit logs:

- 
- Step 1** Choose **Administration > System Audit**.
  - Step 2** In the Application Audit Logs page, click to expand the row for which you want to view details about the log.




---

**Note** For Application Audit, the User Group column is blank for TACACS+/RADIUS users.

---

## Viewing Events Initiated by a User

Network audit logs log events related to the devices in your network. For example, you can view the network audit logs to see which user deployed a specific template and the date and time the template was deployed.

To view network audit logs:

- 
- Step 1** Choose **Operate > Network Audit**.
  - Step 2** In the Network Audit Logs page, click to expand the row for which you want to view details about the log.
-



# Configuring AAA on Prime Infrastructure

Authentication, authorization, and accounting (AAA) can be configured for Prime Infrastructure to communicate with servers. The only username that has permissions to configure Prime Infrastructure AAA is *root* or SuperUser. Any changes to local users accounts are in effect when configured for local mode. If using external authentication, for example RADIUS or TACACS+, the user changes must be done on the remote server.

For information about migrating AAA servers, see the [ACS 5.2 Migration Utility Support Guide](#).

This section contains the following topics:

- [Setting the AAA Mode, page 9-15](#)
- [Adding a TACACS+ Server, page 9-16](#)
- [Adding a RADIUS Server, page 9-16](#)
- [Adding an SSO Server, page 9-17](#)
- [Configuring SSO Server AAA Mode, page 9-17](#)
- [Authenticating AAA Users Through RADIUS Using Cisco Identity Services Engine, page 9-18](#)
- [Configuring ACS 4.x, page 9-22](#)
- [Configuring ACS 5.x, page 9-27](#)

## Setting the AAA Mode

Prime Infrastructure supports local as well as TACACS+ and RADIUS, but you must specify a TACACS+ or RADIUS server first.

**Note**

If you add more than one server, user authentication is validated for the second server, only if the first server is not reachable or it has any network problems.

**Note**

You can use alphabets, numbers, and special characters except ‘ (single quote) and “ (double quote) while entering shared secret key for a third-party TACACS+ or RADIUS server.

To specify a TACACS+ server and then change the AAA mode to TACACS+:

- Step 1** Add a TACACS+ Server. For more information, see [Adding a TACACS+ Server, page 9-16](#).
- Step 2** Click **AAA Mode**.
- Step 3** Select TACACS+.
- Step 4** Select the **Enable Fallback to Local** check box if you want to use the local database when the external AAA server is down.



**Note** If you choose **ONLY on no server response**, the fallback to local Prime Infrastructure user accounts occurs only when the external server is unreachable or has any network problems. If you choose **on authentication failure or no server response**, the fallback to local Prime Infrastructure user accounts occurs when the external server is unreachable or has network problems *or* there is an authentication failure in the external server.

**Step 5** Click **Save**.

## Adding a TACACS+ Server

You can add only three servers at a time in Prime Infrastructure. To configure Prime Infrastructure so it can communicate with the TACACS+ server:

**Step 1** Choose **Administration > Users, Roles & AAA**, then click **TACACS+**.

**Step 2** From the command pull-down menu, choose **Add TACACS+ Server**, then click **Go**.

**Step 3** Enter the TACACS+ server information, then click **Save**.



**Note** For Prime Infrastructure to communicate with the TACACS+ server, the shared secret you enter on this page must match the shared secret configured on the TACACS+ server.

### Related Topic

- [Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes](#)

## Adding a RADIUS Server

You can add only three servers at a time in Prime Infrastructure. To configure Prime Infrastructure so it can communicate with the RADIUS server:

**Step 1** Choose **Administration > Users, Roles & AAA**, then click **RADIUS Servers**.

**Step 2** Choose **Add Radius Server**, then click **Go**.

**Step 3** Enter the RADIUS server information, then click **Save**.



**Note** For Prime Infrastructure to communicate with the RADIUS server, the shared secret you enter on this page must match the shared secret configured on the RADIUS server.

### Related Topic

- [Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes](#)

## Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes

If you change the IP address of the Prime Infrastructure server after you add a TACACS+ or RADIUS server, you must manually configure the TACACS+ or RADIUS server with the new IP address of the Prime Infrastructure server. Prime Infrastructure stores in cache the local interface on which the RADIUS or TACACS+ requests are sent, and you need to manually edit the RADIUS or TACACS+ server configurations to make sure the Prime Infrastructure IP address is updated.

### Related Topics

- [Adding a TACACS+ Server](#)
- [Adding a RADIUS Server](#)

## Adding an SSO Server

This section describes how to add Single Sign-On Authentication (SSO) servers to Prime Infrastructure. You can enable SSO in Prime Infrastructure. SSO allows you to enter your credentials only once, when you navigate across multiple SSO-enabled Prime Infrastructure applications. SSO makes it easier for you to perform cross-launch operations or use dashlets with content that comes from separate applications. You must have administrator-level privileges to set up SSO.



### Note

Before setting up SSO, you must have an SSO configured server. For information about configuring SSO Server AAA Mode, see [“Configuring SSO Server AAA Mode” section on page 9-17](#).

- Step 1** Choose **Administration > Users, Roles & AAA**, then click **SSO Servers**.
- Step 2** Choose **Add SSO Server**, then click **Go**.
- Step 3** Enter the SSO server information, then click **Save**.



### Note

The number of retries allowed for the SSO server authentication request is from 0 to 3.

## Configuring SSO Server AAA Mode

Single Sign-On Authentication (SSO) is used to authenticate and manage users in a multiuser, multirepository environment and to store and retrieve the credentials that are used for logging in to disparate systems. You can set up Prime Infrastructure as the SSO server for other instances of Prime Infrastructure.



### Note

As Prime Infrastructure does not support CA certificates and self-signed certificates in Java, SSO requires accurate DNS configuration. So, you must define the DNS with fully qualified domain name (FQDN). For example, the **nslookup** command and expected data when configuring DNS with FQDN is:

```
hostname CUSTOMER_PI_HOSTNAME
nslookup CUSTOMER_PI_HOSTNAME
Server: ..
```

Address: ...  
 Name: CUSTOMER\_PI\_HOSTNAME.company.com  
 Address: ....

---

- Step 1** Choose **Administration > Users, Roles & AAA**, then click **SSO Server AAA Mode**.
- Step 2** Choose which SSO Server AAA mode you want to use. Only one can be selected at a time.
- Any changes to local user accounts are effective only when you are configured for local mode (the default). If you use remote authentication, changes to the credentials are made on a remote server. The two remote authentication types are RADIUS and TACACS+. RADIUS requires separate credentials for different locations (East and West Coast). TACACS+ is an effective and secure management framework with a built-in failover mechanism.
- Step 3** Select the **Enable Fallback to Local** check box if you want the administrator to use the local database when the external SSO AAA server is down.
- This check box is unavailable if *Local* was selected as the SSO Server AAA Mode type.
- Step 4** Click **OK**.
- 

## Authenticating AAA Users Through RADIUS Using Cisco Identity Services Engine


You can integrate a Prime Infrastructure with Identity Services Engine (ISE). This section explains Prime Infrastructure user authentication through RADIUS protocol using ISE.

Only the RADIUS protocol is supported for authentication and authorization via ISE.

- Step 1** Add Prime Infrastructure as a AAA client in ISE. For more information, see the [“Adding Prime Infrastructure as an AAA Client in ISE” section on page 9-19](#).
- Step 2** Create a new User group in ISE. For more information, see the [“Creating a New User Group in ISE” section on page 9-19](#).
- Step 3** Create a new User in ISE and add that User to the User group created in ISE. For more information, see the [“Creating a New User and Adding to a User Group in ISE” section on page 9-19](#).
- Step 4** Create a new Authorization profile. For more information, see the [“Creating a New Authorization Profile in ISE” section on page 9-20](#).
- Step 5** Create an Authorization policy rule. For more information, see the [“Creating an Authorization Policy Rule in ISE” section on page 9-20](#).
- Step 6** Create an Authentication policy. For more information, see the [“Creating a Simple Authentication Policy in ISE” section on page 9-21](#) or the [“Creating a Rule-Based Authentication Policy in ISE” section on page 9-21](#).
- Step 7** Configure AAA in Prime Infrastructure. For more information, see the [“Configuring AAA in Prime Infrastructure” section on page 9-22](#).
-

## Adding Prime Infrastructure as an AAA Client in ISE

To add Prime Infrastructure as an AAA client in ISE:

- 
- Step 1** Log in to ISE.
  - Step 2** Choose **Administration > Network Devices**.
  - Step 3** From the left sidebar menu, click the arrow next to Network Devices to expand that option.  
The expanded list shows the already added devices.
  - Step 4** Click any device to view its details.
  - Step 5** From the left sidebar menu, click the arrow next to the  icon, then choose the **Add new device** option.
  - Step 6** In the right pane, enter the required details.
  - Step 7** Enter the Shared key in the Shared Secret text box.
  - Step 8** Click **Save** to add the device.
- 

## Creating a New User Group in ISE

You can create a new user group in ISE. This helps you to classify different privileged Prime Infrastructure users and also create authorization policy rules on user groups.

To create a new user group in ISE:

- 
- Step 1** Choose **ISE > Administration > Groups**.
  - Step 2** From the left sidebar menu, choose **User Identity Groups**, then click **Add**.
  - Step 3** Enter the name and description for the group, then click **Save**.
- 

## Creating a New User and Adding to a User Group in ISE

You can create a new user in ISE and map that user to a user group.

To create a new user and map that user to a user group in ISE:

- 
- Step 1** Choose **ISE > Administration > Identity Management > Identities**.
  - Step 2** From the left sidebar menu, choose **Identities > Users**, then click **Add**.
  - Step 3** Enter the username and password and reenter the password for the user.
  - Step 4** Choose the required user group from the **User Group** drop-down list, then click **Save**.



**Note** You can also integrate ISE with external sources such as Active Directory and Lightweight Directory Access Protocol (LDAP).

---

## Creating a New Authorization Profile in ISE

You can create authorization profiles in ISE.

- 
- Step 1** Choose **ISE > Policy > Policy Elements > Results**.
- Step 2** From the left sidebar menu, choose **Authorization > Authorization Profiles**, then click **Add**.
- Step 3** Enter the name and description for the profile.
- Step 4** Choose **ACCESS\_ACCEPT** from the Access Type drop-down list.
- Step 5** In the Advanced Attribute Settings group box, add Prime Infrastructure User Group RADIUS custom attributes one after another along with the virtual domain attributes at the end.
- User Group RADIUS custom attributes are located in Prime Infrastructure at **Administration > Users, Roles & AAA > User Groups**. Click **Task List** for the group with appropriate permissions.
- Select **cisco - av - pair** and paste Prime Infrastructure User Group RADIUS custom attribute next to it. Keep adding one after another.
  - Add the Virtual Domain attribute at the end of the last RADIUS custom attribute for each group (for RADIUS custom attributes, see [Virtual Domain RADIUS and TACACS+ Attributes](#)).
- Step 6** Save the authorization profile.
- 

## Creating an Authorization Policy Rule in ISE

To create an authorization policy rule:

- 
- Step 1** Choose **ISE > Policy > Authorization**.
- Step 2** From the Authorization Policy page, choose **Insert New Rule Above** from the Actions drop-down list. Create a rule to be used for Prime Infrastructure user login.
- Step 3** Enter a name for the rule in the Rule Name text box.
- Step 4** Choose the required identity group from the Identity Groups drop-down list. For example, choose **Prime Infrastructure-SystemMonitoring-Group**. For more information about creating Identity User Groups, see the [“Creating a New User Group in ISE” section on page 9-19](#).
- Step 5** Choose a permission from the Permissions drop-down list. The permissions are the Authorization profiles. For example, choose **Prime Infrastructure-SystemMonitor authorization profile**. For more information about creating authorization profiles, see the [“Creating a New Authorization Profile in ISE” section on page 9-20](#).
- In this example, we define a rule where all users belonging to Prime Infrastructure System Monitoring Identity Group receive an appropriate authorization policy with system monitoring custom attributes defined.
- Step 6** Click **Save** to save the authorization rule.
- You can also monitor successful and failed authentication using **ISE > Monitor > Authentications**.
-

## Creating a Simple Authentication Policy in ISE

The procedure for configuring a simple authentication policy includes defining an allowed protocols service and configuring a simple authentication policy.

To perform the following task, you must be a Super Admin or System Admin.

- 
- Step 1** Choose **Policy > Authentication**.
  - Step 2** Click **OK** on the message that appears.
  - Step 3** Enter the values as required.
  - Step 4** Click **Save** to save your simple authentication policy.
- 

### Related Topics

[Simple Authentication Policies](#) in the *Cisco Identity Services Engine User Guide, Release 1.2*

## Creating a Rule-Based Authentication Policy in ISE

You can edit the default identity source that you want Cisco ISE to use in case none of the identity sources defined in this rule match the request.

The last row in the policy page is the default policy that will be applied if none of the rules match the request. You can edit the allowed protocols and identity source selection for the default policy.

You cannot specify the “UserName” attribute when configuring an authentication policy when the EAP-FAST client certificate is sent in the outer TLS negotiation. Cisco recommends using certificate fields like “CN” and “SAN,” for example.

It is a good practice to choose Deny Access as the identity source in the default policy if the request does not match any of the other policies that you have defined.

To perform the following task, you must be a Super Admin or System Admin.

- 
- Step 1** Choose **Policy > Authentication**.
  - Step 2** Click the **Rule-Based** radio button.
  - Step 3** Click **OK** on the message that appears.
  - Step 4** Click the action icon and click **Insert new row above** or **Insert new row below** based on where you want the new policy to appear in this list. The policies will be evaluated sequentially.  
  
Each row in this rule-based policy page is equivalent to the simple authentication policy. Each row contains a set of conditions that determine the allowed protocols and identity sources.  
  
Enter the values as required to create a new authentication policy.
  - Step 5** Click **Save** to save your rule-based authentication policies.
- 

### Related Topics

[Rule-Based Authentication Policies](#) in the *Cisco Identity Services Engine User Guide, Release 1.2*

## Configuring AAA in Prime Infrastructure

To configure AAA in Prime Infrastructure:

- 
- Step 1** Log in to Prime Infrastructure as *root*, then choose **Administration > Users, Roles & AAA > RADIUS Servers**.
  - Step 2** Add a new RADIUS server with the ISE IP address, then click **Save**.
  - Step 3** Log in to ISE, then choose **Administration > AAA > AAA Mode Settings**.
  - Step 4** Select **RADIUS** as the AAA mode, then click **Save**.
  - Step 5** Log off of Prime Infrastructure.
  - Step 6** Log in again to Prime Infrastructure as an AAA user defined in ISE.

For example, log in as user *ncs-sysmon*.

For more information about creating users in ISE, see the [“Creating a New User and Adding to a User Group in ISE” section on page 9-19](#).

---

## Configuring ACS 4.x

This section provides instructions for configuring ACS 4.x to work with Prime Infrastructure.

To import tasks into Cisco Secure ACS server, you must add Prime Infrastructure to an ACS server (or non-Cisco ACS server). This section contains the following topics:

- [Adding Prime Infrastructure to an ACS Server for Use with TACACS+ Server, page 9-22](#)
- [Adding Prime Infrastructure User Groups into ACS for TACACS+, page 9-23](#)
- [Adding Prime Infrastructure to an ACS Server for Use with RADIUS, page 9-24](#)
- [Adding Prime Infrastructure User Groups into ACS for RADIUS, page 9-25](#)
- [Adding Prime Infrastructure to a Non-Cisco ACS Server for Use with RADIUS, page 9-25](#)

### Adding Prime Infrastructure to an ACS Server for Use with TACACS+ Server

To add Prime Infrastructure to a TACACS+ server:



#### Note

The instructions and illustrations in this section pertain to ACS Version 4.1 and might vary slightly for other versions or other vendor types. See the Cisco Secure ACS documentation or the documentation for the vendor you are using.

---

- 
- Step 1** Click **Add Entry** in the Network Configuration page of the ACS server.
  - Step 2** In the AAA Client Hostname text box, enter the Prime Infrastructure hostname.
  - Step 3** Enter the Prime Infrastructure IP address in the AAA Client IP Address text box.

Ensure the interface that you use for ACS is the same as that is specified in Prime Infrastructure and it is reachable.



- Step 4** In the Shared Secret text box, enter the shared secret that you want to configure on both Prime Infrastructure and ACS servers.
- Step 5** Choose **TACACS+** in the Authenticate Using drop-down list.
- Step 6** Click **Submit + Apply**.
- Step 7** From the left sidebar menu, choose **Interface Configuration**.
- Step 8** In the Interface Configuration page, click the **TACACS+ (Cisco IOS)** link.  
The TACACS+ (Cisco IOS) Interface Configuration page appears.
- Step 9** In the New Services portion of the page, add NCS in the Service column heading.
- Step 10** Enter **HTTP** in the Protocol column heading.




---

**Note** HTTP must be in uppercase.

---

- Step 11** Select the check box in front of these entries to enable the new service and protocol.




---

**Note** The ACS 4.x configuration is complete only when you specify and enable NCS service with HTTP protocol.

---

- Step 12** Click **Submit**.
- 

## Adding Prime Infrastructure User Groups into ACS for TACACS+

To add Prime Infrastructure User Groups into an ACS server for use with TACACS+ servers:

- Step 1** Log in to Prime Infrastructure.
- Step 2** Choose **Administration > Users, Roles & AAA > User Groups**. The User Groups page appears.
- Step 3** Click the Task List link of the user group that you want to add to ACS. The Export Task List page appears.
- Step 4** Highlight the text inside of the TACACS+ Custom Attributes, go to your browser menu, and choose **Edit > Copy**.
- Step 5** Log in to ACS.
- Step 6** Go to Group Setup. The Group Setup page appears.
- Step 7** Choose which group to use, and click **Edit Settings**. Prime Infrastructure HTTP appears in the TACACS+ setting.
- Step 8** Use Edit > Paste in your browser to place the TACACS+ custom attributes from Prime Infrastructure into this text box.




---

**Note** When you upgrade Prime Infrastructure, you must readd any permissions on the TACACS+ or RADIUS server *and* update the roles in your TACACS+ server with the tasks from the Prime Infrastructure server.

---

- Step 9** Select the check boxes to enable these attributes.

**Step 10** Click **Submit + Restart**.

You can now associate ACS users with this ACS group.



**Note** To enable TACACS+ in Prime Infrastructure, see the [“Adding a TACACS+ Server”](#) section on page 9-16.



**Note** You must add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the [“Using Virtual Domains to Control Access to Sites and Devices”](#) section on page 9-6.

## Adding Prime Infrastructure to an ACS Server for Use with RADIUS

To add Prime Infrastructure to an ACS server for use with RADIUS servers, follow these steps. If you have a non-Cisco ACS server, see the [“Adding Prime Infrastructure to a Non-Cisco ACS Server for Use with RADIUS”](#) section on page 9-25.

**Step 1** Go to Network Configuration on the ACS server.

**Step 2** Click **Add Entry**.

**Step 3** In the AAA Client Hostname text box, enter Prime Infrastructure hostname.

**Step 4** In the AAA Client IP Address text box, enter Prime Infrastructure IP address.



**Note** Ensure the interface that you use for ACS is the same you specified in Prime Infrastructure and it is reachable.

**Step 5** In the Shared Secret text box, enter the shared secret that you want to configure on both Prime Infrastructure and ACS servers.

**Step 6** Choose **RADIUS (Cisco IOS/PIX 6.0)** from the Authenticate Using drop-down list.

**Step 7** Click **Submit + Apply**.

You can now associate ACS users with this ACS group.



**Note** To enable RADIUS in Prime Infrastructure, see the [“Adding a RADIUS Server”](#) section on page 9-16.



**Note** From Prime Infrastructure Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the [“Using Virtual Domains to Control Access to Sites and Devices”](#) section on page 9-6.

## Adding Prime Infrastructure User Groups into ACS for RADIUS

To add Prime Infrastructure user groups into an ACS Server for use with RADIUS servers:

- 
- Step 1** Log in to Prime Infrastructure.
  - Step 2** Choose **Administration > Users, Roles & AAA > User Groups**. The All Groups page appears.
  - Step 3** Click the Task List link of the user group that you want to add to ACS. The Export Task List page appears.
  - Step 4** Highlight the text inside of the RADIUS Custom Attributes, go to the menu of your browser, and choose **Edit > Copy**.



---

**Note** When you upgrade Prime Infrastructure, any permissions on the TACACS+ or RADIUS server must be readded.

---

- Step 5** Log in to ACS.
- Step 6** Go to Group Setup. The Group Setup page appears.
- Step 7** Choose which group to use, and click **Edit Settings**. Find [009\001]cisco-av-pair under Cisco IOS/PIX 6.x RADIUS Attributes.
- Step 8** Use Edit > Paste in your browser to place the RADIUS custom attributes from Prime Infrastructure into this text box.



---

**Note** When you upgrade Prime Infrastructure, any permissions on the TACACS+ or RADIUS server must be readded.

---

- Step 9** Select the check boxes to enable these attributes.
- Step 10** Click **Submit + Restart**.

You can now associate ACS users with this ACS group.



---

**Note** To enable RADIUS in Prime Infrastructure, see the [“Adding a RADIUS Server”](#) section on page 9-16. For information on adding Prime Infrastructure virtual domains into ACS for TACACS+, see the [“Virtual Domain RADIUS and TACACS+ Attributes”](#) section on page 9-13.

---



---

**Note** You must add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the [“Using Virtual Domains to Control Access to Sites and Devices”](#) section on page 9-6.

---

## Adding Prime Infrastructure to a Non-Cisco ACS Server for Use with RADIUS

When you use a RADIUS server to log in to Prime Infrastructure, the AAA server sends back an access=accept message with a user group and a list of available tasks, after the username and password were verified. The access=accept message comes back as a fragmented packet because of the large

number of tasks in some user groups. You can look in the following file to see the tasks associated with a given user group: C:\Program Files\Prime Infrastructure\webnms\webacs\WEB-INF\security\usergroup-map.xml. The tasks are passed back as a vendor specific attribute (VSA), and Prime Infrastructure requires authorization information using the VSA (IETF RADIUS attribute number 26). The VSA contains Prime Infrastructure RADIUS task list information.

The content of the VSA is as follows:

- Type = 26 (IETF VSA number)
- Vendor Id = 9 (Cisco vendor ID)
- Vendor Type = 1 (Custom attributes)
- Vendor Data = Prime Infrastructure task information (for example Prime Infrastructure: task0 = Users and Group)

Each line from Prime Infrastructure RADIUS task list should be sent in its own RADIUS VSA.

In the data portion of the access=access packet, the truncated output sometimes shows only one role sent back for an Admin user group login. The tasks associated with the role start with task0 and increment with task1, task2, and so on. [Table 9-3](#) defines what these attributes in the access=access packet example signify.

```
0000 06 6d 0e 59 07 3d 6a 24 02 47 07 35 d2 12 a4 eb .m.Y.=j$G.5...
0010 a2 5a fa 84 38 20 e4 e2 3a 3a bc e5 1a 20 00 00 .Z..8.....
0020 00 09 01 1a 57 69 72 65 6c 65 73 73 2d 57 43 53 ...Prime Infrastructure
0030 3a 72 6f 6c 65 30 3d 41 64 6d 69 6e 1a 2b 00 00 :role0=Admin.+...
0040 00 09 01 25 57 69 72 65 6c 65 73 73 2d 57 43 53 ...%Prime Infrastructure
0050 3a 74 61 73 6b 30 3d 55 73 65 72 73 20 61 6e 64 :task0=Users and
0060 20 47 72 6f 75 70 73 1a 27 00 00 09 01 21 57 Groups."...!W
0070 69 72 65 6c 65 73 73 2d 57 43 53 3a 74 61 73 6b Prime Infrastructure:task
0080 31 3d 41 75 64 69 74 20 54 72 61 69 6c 73 xx xx 1=Audit Trails.*
```

**Table 9-3** Access=Access Packet Example

Attribute	Description
1a (26 in decimal)	Vendor attribute
2b (43 bytes in decimal)	Length as the total number of bytes to skip and still reach the next TLV (for task0, Users and Groups)
4-byte field	Vendor Cisco 09
01	Cisco AV pair - a TLV for Prime Infrastructure to read
25 (37 bytes in decimal)	Length
hex text string	Prime Infrastructure:task0=Users and Groups
	The next TLV until the data portion is completely processed
255.255.255.255	TLV: RADIUS type 8 (framed IP address)
Type 35 (0x19)	A class, which is a string
Type 80 (0x50)	Message authenticator

To troubleshoot, perform the following tasks:

- Verify if the RADIUS packet is an access accept.
- Verify the task names for the user group in the access accept.

- Look at the different length fields in the RADIUS packet.

## Configuring ACS 5.x

This section provides instructions for configuring ACS 5.x to work with Prime Infrastructure. This section contains the following topics:

- [Creating Network Devices and AAA Clients, page 9-27](#)
- [Adding Groups, page 9-27](#)
- [Adding Users, page 9-27](#)
- [Creating Policy Elements or Authorization Profiles for RADIUS, page 9-28](#)
- [Creating Policy Elements or Authorization Profiles for TACACS+, page 9-28](#)
- [Creating Service Selection Rules for RADIUS, page 9-28](#)
- [Creating Service Selection Rules for TACACS+, page 9-28](#)
- [Configuring Access Services for RADIUS, page 9-29](#)
- [Configuring Access Services for TACACS+, page 9-29](#)

### Creating Network Devices and AAA Clients

To create network devices and AAA clients:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Network Resources &gt; Network Devices and AAA Clients</b> . |
| <b>Step 2</b> | Enter an IP address.   |
- 

### Adding Groups

To add groups:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Users and Identity Stores &gt; Identity Groups</b> . |
| <b>Step 2</b> | Create a group.  |
- 

### Adding Users

To add users:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Users and Identity Stores &gt; Internal Identity Stores &gt; Users</b> . |
| <b>Step 2</b> | Add a user, and then map to group to that user.                                    |
-

## Creating Policy Elements or Authorization Profiles for RADIUS

To create policy elements or authorization profiles for RADIUS:

- 
- Step 1** Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click **Create**.
  - Step 2** Enter the required information, then click **Submit**.
- 

## Creating Policy Elements or Authorization Profiles for TACACS+

To create policy elements or authorization profiles for TACACS+:

### Before You Begin

Ensure that you add the relevant Menu Access task so that the submenus are displayed in Prime Infrastructure. For example, if you add a submenu under the Administration menu, you must first add the Administration Menu Access task so that the submenu is visible under the Administration menu in Prime Infrastructure.

- 
- Step 1** Choose **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, then click **Create**.
  - Step 2** Enter the required information, then click **Submit**.
- 

## Creating Service Selection Rules for RADIUS

To create service selection rules for RADIUS:

- 
- Step 1** Choose **Access Policies > Access Services > Service Selection Rules**, then click **Create**.
  - Step 2** Enter the required information, then click **OK**.
- 


## Creating Service Selection Rules for TACACS+

To create service selection rules for TACACS+:

- 
- Step 1** Choose **Access Policies > Access Services > Service Selection Rules**, then click **Create**.
  - Step 2** Enter the required information, then click **OK**.
-


## Configuring Access Services for RADIUS

To configure access services for RADIUS:

- 
- Step 1** Log in to the ACS 5.x server and choose **Access Policies > Access Services > Default Network Access**.
- Step 2** On the General tab, click the policy structure you want to use. By default, all the three policy structures are selected.
- Step 3** From the Allowed Protocols, click the protocols you want to use.
-  **Note** You can retain the defaults for identity and group mapping.
- 
- Step 4** To create an authorization rule for RADIUS, choose **Access Policies > Access Services > Default Network Access > Authorization**, then click **Create**.
- Step 5** In Location, click **All Locations** or you can create a rule based on the location.
- Step 6** In Group, select the group that you created earlier.
- Step 7** In Device Type, click **All Device Types** or you can create a rule based on the Device Type.
- Step 8** In Authorization Profile, select the authorization profile created for RADIUS, click **OK**, then click **Save**.
- 

## Configuring Access Services for TACACS+

To configure access services for TACACS+:

- 
- Step 1** Choose **Access Policies > Access Services > Default Device Admin**.
- Step 2** On the General tab, click the policy structure you want to use. By default, all the three are selected. Similarly, in Allowed Protocols, click the protocols you want to use.
-  **Note** You can retain the defaults for identity and group mapping.
- 
- Step 3** To create an authorization rule for TACACS+, choose **Access Policies > Access Services > Default Device Admin > Authorization**, then click **Create**.
- Step 4** In Location, click **All Locations**, or you can create a rule based on the location.
- Step 5** In Group, select the group that you created earlier.
- Step 6** In Device Type, click **All Device Types**, or you can create a rule based on the Device Type.
- Step 7** In Shell Profile, select the shell profile created for TACACS+, click **OK**, then click **Save**.
-







## Advanced Monitoring

Cisco Prime Infrastructure consumes a lot of information from various different sources, including NAM, NetFlow, NBAR, medianet, PerfMon, and Performance Agent. The following table depicts the sources of the data for the site dashlets used by Prime Infrastructure:

**Table 10-1** Site Dashlet Data Sources

Dashlet Name	NAM	Medianet	NetFlow	PA	NBAR2
Application Usage Summary	y	y	y	y	y
Top N Application Groups	y	y	y	y	y
Top N Applications	y	y	y	y	y
Top N Applications with Most Alarms	y	y	y	y	y
Top N Clients (In and Out)	y	y	y	y	y
Top N VLANs	y	–	y	y	–
Worst N RTP Streams by Packet Loss	y	y	–	–	–
Worst N Clients by Transaction Time	y	–	–	y	–

The following table shows how Prime Infrastructure populates the application-specific dashlets:

**Table 10-2** Application-Specific Dashlet Data Sources

Dashlet Name	NAM	Medianet	NetFlow	PA	NBAR2
Application Configuration	y	y	y	y	y
Application ART Analysis	y	–	–	y	–
App Server Performance	y	–	–	y	–
Application Traffic Analysis	y	y	–	y	y
Top N Clients (In and Out)	y	–	–	y	–
Worst N Clients by Transaction Time	y	–	–	y	–
Worst N Sites by Transaction Time	y	–	–	y	–
KPI Metric Comparison	y	y	–	y	–

Table 10-2 Application-Specific Dashlet Data Sources (continued)

DSCP Classification	y	–	y	–	–
Number of Clients Over Time	y	–	y	–	–
Top Application Traffic Over Time	y	–	y	–	–
Top N Applications	y	–	y	y	–
Top N Clients (In and Out)	y	–	y	y	–
Average Packet Loss	y	y	–	–	–
Client Conversations	y	–	y	–	–
Client Traffic	y	–	y	–	–
IP Traffic Classification	y	–	y	–	–
Top N Applications	y	–	y	–	–
DSCP Classification	y	–	y	–	–
RTP Conversations Details	y	y	–	–	–
Top N RTP Streams	y	y	–	–	–
Voice Call Statistics	Y	y	–	–	–
Worst N RTP Streams by Jitters	y	y	–	–	–
Worst N RTP Streams by MOS	y	–	–	–	–
Worst N Sites by MOS	y	–	–	–	–
Worst N Site to Site Connections by KPI	y	y	–	y	–

## Enabling NetFlow Monitoring

After NetFlow has been enabled on devices and directed to Prime Infrastructure, you can enable monitoring for NetFlow. Just as for Device and Interface Health, you just need to provision the appropriate monitoring template and deploy it.

- 
- Step 1** Choose **Design > Configuration > Monitor Configuration > Features > NetFlow**.
  - Step 2** Select one of the NetFlow templates, enter the appropriate details, and save the template. Your new template will be stored in My Templates.
  - Step 3** Choose **Deploy > Monitoring Deployment** and deploy the template you just created. After a couple of polling cycles, dashlets should start populating the data.
- 

## WAN Optimization

Cisco Wide Area Application Services (WAAS) devices and software help you to ensure high-quality WAN end-user experiences across applications at multiple sites. For various scenarios for deploying WAAS in your network, see:

[http://wwwin.cisco.com/dss/adbu/waas/collateral/Using NAM in a WAAS Deployment.pdf](http://wwwin.cisco.com/dss/adbu/waas/collateral/Using_NAM_in_a_WAAS_Deployment.pdf)

After you have deployed your WAAS changes at candidate sites, you can navigate to **Operate > Monitoring Dashboards > Detail Dashboards > WAN Optimization** to validate the return on your optimization investment. From this dashboard, you can click:

- **View Multi-Segment Analysis** to monitor WAAS-optimized WAN traffic.
- **Conversations** to see individual client/server sessions.
- **Site to Site** to see aggregated site traffic.

The following table describes the key WAAS monitoring dashlets:

**Table 10-3 Key WAAS Monitoring Dashlets**

Dashlet	Description
Average Concurrent Connections (Optimized versus Pass-through)	Graphs the average number of concurrent client and pass-through connections over a specified time period.
Multi-segment Analysis	Displays WAAS traffic across multiple segments in a conversation or between sites.
Multi-segment Network Time (Client LAN-WAN - Server LAN)	Graphs the network time between the multiple segments.
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 disabled). With optimization enabled, you should see a drop in the optimized traffic time when compared to the pass-through time.
Traffic Volume and Compression Ratio	Graphs the bandwidth reduction ratio between the number of bytes before compression and the number of bytes after compression.





## Managing Licenses

---

The **Administration > Licenses** page allows you to manage Prime Infrastructure, wireless LAN controllers, and Mobility Services Engine (MSE) licenses.

Although Prime Infrastructure and MSE licenses can be fully managed from the **Administration > Licenses** page, you can only view Wireless LAN Controller (WLC). You must use WLC or Cisco License Manager (CLM) to manage WLC licenses.



**Tip**

---

To learn more about Prime Infrastructure licensing, go to [Cisco.com](https://www.cisco.com) to watch a multimedia presentation. Here you can also find the learning modules for a variety of Prime Infrastructure topics. In future releases, we will add more overview and technical presentations to enhance your learning.

---

- [Prime Infrastructure Licensing, page 11-1](#)
- [Controller Licensing, page 11-5](#)
- [MSE Licensing, page 11-6](#)
- [Assurance Licensing, page 11-11](#)

## Prime Infrastructure Licensing

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

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

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. You can send a request to [ask-prime-infrastructure@cisco.com](mailto:ask-prime-infrastructure@cisco.com) if:

- You need to extend the evaluation period
- You need to increase the device count
- You already have a particular feature license and need to evaluate the other feature licenses

You will need to order a base license and then purchase the corresponding feature license before the evaluation license expires. The license that you purchase must be sufficient to:

- Enable access to all the Prime Infrastructure features you want to use to manage your network.

- Include all the devices in your network that you want to manage using Prime Infrastructure.

To ensure you have the licenses to achieve these goals, do the following:

1. Familiarize yourself with the types of license packages available to you, and their requirements. See [Purchasing a Prime Infrastructure License, page 11-2](#).
2. View the existing licenses. See [Verifying License Details, page 11-3](#) for help on ordering and downloading licenses.
3. Calculate the number of licenses you will need, based both on the package of features you want and the number of devices you need to manage. See [Managing License Coverage, page 11-3](#)
4. Add new licenses. See [Adding Licenses, page 11-4](#).
5. Delete existing licenses. See [Deleting Licenses, page 11-4](#).

If you are already using the Prime Infrastructure or any other network management product and you plan to extend your device coverage, see [Managing License Coverage, page 11-3](#).

## Purchasing a Prime Infrastructure License

You purchase the following licenses based on the features you are required to access:

- Base License—Each Prime Infrastructure management node requires a single base license as a prerequisite for adding feature licenses.
- Lifecycle license—The Lifecycle license type is based on the number of managed devices. The lifecycle license provides full access to the following Prime Infrastructure lifecycle management features:
  - Device configuration management and archiving
  - Software image management
  - Basic health and performance monitoring
  - Troubleshooting

You need to order a single base license, and then purchase lifecycle licenses as necessary to access the Prime Infrastructure lifecycle management features. Lifecycle licenses are available in bundle sizes of 25, 50, 100, 500, 1000, 2500, 5000, and 10,000 devices and can be combined.

- Assurance license—The Assurance license is based on the number of NetFlow-monitored devices and Network Analysis Module (NAM) data collection-enabled devices:
  - NetFlow enabled on multiple interfaces in a device counts as one device towards an Assurance license.
  - Multiple NetFlow technologies (such as NetFlow, medianet, Prime Assurance (PA), and Network-Based Application Recognition (NBAR)) enabled on a device count as one device towards an Assurance license.
  - When NetFlow is enabled on a wireless controller, each active AP for which NetFlow is generated counts as one device towards an Assurance license.
  - Each NAM device for which data collection is enabled counts towards an Assurance license.

The Assurance license provides access to the following management features:

- End-to-end application, network, and end-user experience visibility
- Multi-NAM management
- Monitoring of WAN optimization

You can order a single base license, then purchase additional Assurance licenses as necessary. Assurance licenses are available in bundle sizes of 25, 50, 100, 500, 1000, 2500, 5000, and 10,000 devices and can be combined.

- **Collector License**—The Collector license is based on NetFlow processing in flows per second. By default, the Assurance license provides a Collector license to process NetFlow for up to 20,000 flows per second. You can also purchase a Collector license to support up to 80,000 flows per second.

**Note**

---

When you see a warning message as ‘Base license is missing’ or ‘Multiple base licenses present, use only one’ under **Administration > Licenses > Files > License Files**, you can ignore the warning and proceed.

---

## Managing License Coverage

Prime Infrastructure is deployed using a physical or a virtual appliance. You use the standard license center GUI to add new licenses. The new licenses are locked using the standard Cisco Unique Device Identifier (UDI) for a physical appliance and a Virtual Unique Device Identifier (VUDI) for a virtual appliance.

To view the UDI or VUDI, see [Verifying License Details, page 11-3](#).

You can upgrade to Prime Infrastructure 2.0 if you are already using one or more of the following products:

- Prime Infrastructure 1.1.1.24
- Prime Infrastructure 1.2.0.103
- Prime Infrastructure 1.2.1.12
- Prime Infrastructure 1.3.0-20

For ordering information, refer to the Ordering Guide on the Prime Infrastructure [Support](#) page.

**Note**

---

If you are using LMS, you need to migrate existing data from the previous installation to the new Prime Infrastructure installation. For more details on data that can be exported from LMS 4.2.x to PI 2.0, see [Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure, page 6-15](#)

---

## Verifying License Details

Before you order new licenses, you might want to get details about your existing licenses. For example, you can verify your existing license type, product ID, device and interface limits, and number of devices and interfaces managed by your system.

To verify license details, choose **Administration > Licenses**, then rest your cursor on the icon that appears next to **Licenses**.

The licensing ordering help screen that appears provides the following information:

- Feature licenses that your system is licensed for
- Ordering options
- UDI or VUDI

## Adding Licenses

You need to add new licenses when:

- You have purchased a new Prime Infrastructure license.
- You are already using Prime Infrastructure and have bought additional licenses.
- You are upgrading to Prime Infrastructure, see [Managing License Coverage, page 11-3](#).

To add a new license:

- 
- Step 1** Choose **Administration > Licenses**.
  - Step 2** Under the Summary folder, click **Files**, then click **License Files**.
  - Step 3** Select the licenses that you have ordered with the required device limit, then click **Add**.
  - Step 4** Browse to the location of the license file, then click **OK**.
- 

## Deleting Licenses

When you delete licenses from Prime Infrastructure, all licensing information is removed from the server. Make a copy of your original license file in case you want to add it again later. There are several reasons you might want to delete licenses:

- You installed temporary licenses and want to delete them before applying your permanent licenses.
- You want to move your licenses to a different server. You must first delete the licenses from the original server, then send an email to [licensing@cisco.com](mailto:licensing@cisco.com) requesting a re-host for your licenses. You can then apply the re-hosted licenses to the new server.

To delete a license file:

- 
- Step 1** Choose **Administration > Licenses**.
  - Step 2** Under the Summary folder, click **Files**.
  - Step 3** Click **License Files**.
  - Step 4** Select the license file you want to delete, then click **Delete**.
- 

## Troubleshooting Licenses

To troubleshoot licenses, you will need to get details about the licenses that are installed on your system. Click **Help > About** Prime Infrastructure to access your license information.



Table 11-1 provides a few scenarios and tips for troubleshooting:

**Table 11-1 Troubleshooting Scenarios**

Scenario	Possible Cause	Resolution
Prime Infrastructure reports a Licensing Error.	The license file becomes corrupted and unusable if you make any modifications to the file.	<ol style="list-style-type: none"> <li>1. Delete the existing license.</li> <li>2. Download and install a new license.</li> </ol>
Unable to add new feature licenses.	The base license is a prerequisite to add any additional feature license.	<ol style="list-style-type: none"> <li>1. Install the base license</li> <li>2. Add new licenses</li> </ol>
Unable to add licenses because the UDI of the device does not match.	You are adding invalid license which is not meant for that particular system.	Add the license that is ordered for the device.
The state of the devices has changed to unmanaged.	The device limit must be less than or equal to lifecycle license limit. The state of the inventoried devices will change to unmanaged if you add or delete devices.	<ol style="list-style-type: none"> <li>1. Delete the additional devices.</li> <li>2. The state of the devices will change to managed after the 24 hours synchronization.</li> </ol> <p>To verify that the status of the inventoried devices has changed to “managed” after synchronization:</p> <ol style="list-style-type: none"> <li>1. Choose <b>Operate &gt; Device Work Center &gt; Collection Status</b></li> <li>2. Hover the mouse over the circle beside the device name to view the collection status details.</li> </ol>

## Controller Licensing

If you choose Files > Controller Files from the left sidebar menu, you can monitor the controller licenses.



### Note

Prime Infrastructure does not directly manage controller licenses, rather it simply monitors the licenses. To manage the licenses you can use command-line interface (CLI) commands, Web UI, or Cisco License Manager (CLM).

This page displays the following parameters:

- Controller Name
- Controller IP—The IP address of the controller.
- Feature—License features include wplus-ap-count, wplus, base-ap-count, and base.

For every physical license installed, two license files display in the controller: a feature level license and an ap-count license. For example if you install a “WPlus 500” license on the controller, “wplus” and “wplus-ap-count” features display. There are always two of these features active at any one time that combine to enable the feature level (WPlus or Base) and the AP count.



### Note

You can have both a WPlus and Base license, but only one can be active at any given time.

- AP Limit—The maximum capacity of access points allowed to join this controller.
- EULA status—Displays the status of the End User License Agreement and is either Accepted or Not Accepted.
- Comments—User entered comments when the license is installed.
- Type—The four different types of licenses are as follows:
  - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node locked, their usage is recorded on the device. The number of days left displays for the evaluation license with the fewest number of remaining active license days.
  - Extension—Licenses are node locked and metered. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
  - Grace Period—Licenses are node locked and metered. These licenses are issued by Cisco licensing portal as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.




---

**Note** Types other than Permanent display the number of days left until the license expires. Licenses not currently in use do not have their counts reduced until they become “In Use.”

---

- Status
  - In Use—The license level and the license are in use.
  - Inactive—The license level is being used, but this license is not being used.
  - Not In Use—The license level is not being used and this license is not currently recognized.
  - Expired In Use—The license is being used, but is expired and will not be used upon next reboot.
  - Expired Not In Use—The license has expired and can no longer be used.
  - Count Consumed—The ap-count license is In Use.




---

**Note** If you need to filter the list of license files, you can enter a controller name, feature, or type and click **Go**.

---

## MSE Licensing

The MSE packages together multiple product features related to network topology, design such as NMSP, Network Repository along with related Service Engines, and application processes, such as the following:

- Context-Aware Service
- Wireless Intrusion Prevention System (WIPS)

To enable smooth management of MSE and its services, various licenses are offered.

**Note**

You must have a Cisco Prime Infrastructure license to use MSE and its associated services.

This section contains the following topics:

- [MSE License Structure Matrix, page 11-7](#)
- [Sample MSE License File, page 11-7](#)
- [Revoking and Reusing an MSE License, page 11-8](#)
- [MSE Services Coexistence, page 11-8](#)
- [Managing MSE Licenses, page 11-9](#)

## MSE License Structure Matrix

Table 11-2 lists the breakdown of the licenses between the High end, Low end and Evaluation licenses for MSE, Location services, SCM, wIPS, and MIR.

**Table 11-2** *MSE License Structure Matrix*

	High End	Low End	Evaluation
<b>MSE Platform</b>	High-end appliance and infrastructure platform such as the Cisco 3350 and 3355 mobility services engines.	Low-end appliance and infrastructure platform such as Cisco 3310 mobility services engine.	—
<b>Context Aware Service</b>	25,000 Tags	2000 Tags	Validity 60 days, 100 Tags and 100 Elements.
	25,000 Elements	2000 Elements	
<b>wIPS</b>	3000 access points	2000 access points	Validity 60 days, 20 access points.

## Sample MSE License File

The following is a sample MSE license file:

```
FEATURE MSE cisco 1.0 permanent uncounted \
  VENDOR_STRING=UDI=udi,COUNT=1 \
  HOST ID=ANY \
  NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> \
  <PAK>dummyPak</PAK>" \
  SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
  45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
  1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

This sample file has five license entries. The first word of the first line of any license entry tells you what type of license it is. It can either be a Feature or Increment license. A feature license is a static lone item to license. There can be multiple services engines running in MSE. An Increment license is an additive license. In MSE, the individual service engines are treated as increment licenses.

The second word of the first line defines the specific component to be licensed. For example, MSE, LOCATION\_TAG. The third word depicts the vendor of the license, for example Cisco. The fourth word denotes the version of the license, for example 1.0. The fifth word denotes the expiration date; this can be permanent for licenses that never expire or a date in the format dd-mm-yyyy. The last word defines whether this license is counted.

## Revoking and Reusing an MSE License

You can revoke an MSE appliance license from one system and reuse it on another system. When you revoke a license, the license file is deleted from the system. If you want to reuse the license on another system, then the license needs to be rehosted.

If you want to reuse a license with an upgrade stock keeping unit (SKU) on another system, then you must have the corresponding base license SKU installed in the system to which you want to reuse the upgrade SKU. You cannot reuse the upgrade license SKU in a system if the corresponding base license SKU is deleted from it.

When you revoke a license, MSE restarts the individual service engines to reflect the changes to the licenses. Then the service engines receives the updated capacity from MSE during startup.

## MSE Services Coexistence

With MSE 6.0 and later, you can enable multiple services (Context Aware and wIPS) to run concurrently. Before Version 6.0, mobility services engines only supported one active service at a time.

The following must be considered with coexistence of multiple services:

- Coexistence of services might be impacted by license enforcement. As long as the license is not expired, you can enable multiple services.



### Note

Limits for individual services differ. For example, a low-end mobility services engine (MSE-3310) tracks a total of 2,000 CAS elements; a high-end mobility services engine (MSE-3350) tracks a total of 25,000 CAS elements.

A low-end mobility services engine has a maximum limit of 2000 wIPS elements; a high-end mobility services engine has a maximum limit of 3000 wIPS elements.

- Expired evaluation licenses prevent the service from coming up.
- If a CAS license is added or removed, this process restarts all services on the mobility services engine including wIPS. If a wIPS license is added or removed, the process does not impact CAS; only wIPS restarts.
- Other services can be enabled in evaluation mode even if a permanent license for the maximum number of elements has been applied.

Whenever one of the services has been enabled to run with its maximum license, another service cannot be enabled to run concurrently because the capacity of the MSE is not sufficient to support both services concurrently. For example, on MSE-3310, if you install a wIPS license of 2000, then you cannot enable CAS to run concurrently. However, evaluation licenses are not subject to this limitation.

## Managing MSE Licenses

If you choose Files > MSE Files from the left sidebar menu, you can manage the Mobility Services Engine (MSE) licenses.

This section contains the following topics:

- [Registering Product Authorization Keys, page 11-9](#)
- [Installing Client and wIPS License Files, page 11-10](#)
- [Deleting a Mobility Services Engine License File, page 11-11](#)

The page displays the MSE licenses found and includes the following information:



**Note** Because tag licenses are added and managed using appropriate vendor applications, tag licenses are not displayed in this page. Refer to the following URL for more information: <http://support.aeroscout.com>. Evaluation (demo) licenses are also not displayed.

Tag licenses are installed using the *AeroScout System Manager* only if the tags are tracked using Partner engine. Otherwise the tags will be counted along with the CAS element license.

- MSE License File—Indicates the MSE License.
- MSE—Indicates the MSE name.
- Type—Indicates the type of mobility services engine (client elements, wIPS local mode or wIPS monitor mode access points).
- Limit—Displays the total number of client elements or wIPS monitor mode access points licensed across the mobility services engine.
- License Type—Permanent licenses are the only license types displayed on this page.
  - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

## Registering Product Authorization Keys

You receive a product authorization key (PAK) when you order a client, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for installation on the mobility services engine. License files are emailed to you after successfully registering a PAK.

Client and wIPS PAKs are registered with Cisco.



**Note** Tag PAKs are registered with AeroScout. To register your tag PAK, go to this URL: <http://www.aeroscout.com/content/support>

To register a product authoritative key (PAK) and obtain a license file for installation:

**Step 1** Open a browser page and go to [www.cisco.com/go/license](http://www.cisco.com/go/license).




---

**Note** You can also access this site by clicking the Product License Registration link located on the License Center page of Prime Infrastructure.

---

**Step 2** Enter the PAK and click **SUBMIT**.

**Step 3** Verify the license purchase. Click **Continue** if correct. The licensee entry page appears.




---

**Note** If the license is incorrect, click the **TAC Service Request Tool** link to report the problem.

---

**Step 4** At the Designate Licensee page, enter the mobility service engine UDI in the host ID text box. This is the mobility services engine on which the license will be installed.




---

**Note** UDI information for a mobility services engine is found in the General Properties group box at Services > Mobility Services Engine > *Device Name* > *System*.

---

**Step 5** Select the **Agreement** check box. Registrant information appears beneath the Agreement check box. Modify information as necessary.




---

**Note** Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.

---

**Step 6** If registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the end-user information.

**Step 7** Click **Continue**.

**Step 8** At the Finish and Submit page, review registrant and end-user data. Click **Edit Details** to correct information, if necessary, then click **Submit**.

---

## Installing Client and wIPS License Files

You can install CAS element licenses and wIPS licenses from Prime Infrastructure.




---

**Note** Tag licenses are installed using the *AeroScout System Manager*. Refer to the following URL for additional information:  
<http://support.aeroscout.com>.

---

To add a client or wIPS license to Prime Infrastructure after registering the PAK:

---

**Step 1** Choose **Administration > License Center**.

**Step 2** From the left sidebar menu, choose **Files > MSE Files**.

**Step 3** From the License Center > Files > MSE Files page, click **Add** to open the Add a License File dialog box.

**Step 4** From the MSE Name drop-down list, choose the mobility services engine to which you want to add the license file.



---

**Note** Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

---

**Step 5** Enter the license file in the License File text box or browse to the applicable license file.

**Step 6** Once displayed in the License File text box, click **Upload**. Newly added license appears in mobility services engine license file list.



---

**Note** A Context Aware Service (CAS) restarts if a client or tag license is installed; a wIPS service restarts if a wIPS license is installed.

---



---

**Note** Services must come up before attempting to add or delete another license.

---

## Deleting a Mobility Services Engine License File

To delete a mobility services engine license file:

---

**Step 1** From the License Center > Files > MSE Files page, select the check box of the mobility services engine license file that you want to delete.

**Step 2** Click **Delete**, then click **OK** to confirm the deletion.

---

## Assurance Licensing

As explained in [Purchasing a Prime Infrastructure License, page 11-2](#), licenses for Assurance features are based on the number of NetFlow-monitored devices and Network Analysis Module (NAM) data collection-enabled devices you have in your network. You manage, verify, and troubleshoot Assurance licenses much as you do with other feature licenses, as explained in [Adding Licenses, page 11-4](#), [Deleting Licenses, page 11-4](#) and [Troubleshooting Licenses, page 11-4](#).

In addition to these functions, Prime Infrastructure also lets you choose which NetFlow and NAM devices you want to manage using Assurance features. For example, if you have only 50 Assurance feature licenses and more than 50 NetFlow and NAM devices, you can choose to manage only your most critical devices. If you later purchase additional Assurance licenses, you can add license coverage for the devices previously left unmanaged.

## Verifying Assurance License Details

Before you buy new Assurance licenses, you may want to get details about your existing Assurance licenses and how they are being used. You can find Assurance license information using the resources in the following table.

**Table 11-3** Finding Assurance License Information

To see	Choose
The NetFlow-enabled devices in your network that are under Assurance management, as a percentage of the total number of Assurance licenses you have.	<b>Administration &gt; Licenses &gt; Summary.</b>
The total number of Assurance licenses you have and the files associated with them.	<b>Administration &gt; Licenses &gt; Files.</b>
A list of the devices sending NetFlow or NAM polling data to Prime Infrastructure.	<b>Administration &gt; Licenses &gt; Assurance License Manager</b>
The number of Assurance Licenses in use.	
The maximum number of Assurance licenses available to you.	

By default, the total count of Assurance licenses on the Assurance License Manager, Summary and Files pages are always updated whenever you add or delete Assurance licenses. However, note that adding or deleting Assurance licenses is a System Defined Job, which runs automatically once every 12 hours. So it can take up to 12 hours for the Summary, and Assurance License Manager pages to show added or deleted Assurance licenses.

In addition to **Administration > Licenses > Assurance License Manager**, you can always access the Assurance License Manager page using the **Assurance License Manager** link in the upper right corner of the Summary and Files pages.

## Adding License Coverage For NetFlow and NAM Devices

You want to add license coverage for NetFlow or NAM devices when:

- You have purchased new or additional Assurance licenses.
- You have NetFlow and NAM devices not already licensed for Assurance management.

- 
- Step 1** Choose **Administration > Licenses > Assurance License Manager**.
- Step 2** Above the list of devices currently under Assurance management, click **Add Device**.
- Step 3** Select the check box next to each device you want to put under Assurance management, then click **Add License**. Prime Infrastructure adds the devices immediately.
- Step 4** When you are finished, click **Cancel**.
- 

## Deleting License Coverage for NetFlow and NAM Devices

You may need to delete license coverage for a NetFlow or NAM device when:

- You have too many NetFlow and NAM devices for the number of Assurance licenses you have.
- You want to stop using Assurance management features with one or more NetFlow and NAM devices



- 
- Step 1** Choose **Administration > Licenses > Assurance License Manager**. Prime Infrastructure displays the list of devices currently under Assurance management. It also displays the total number of Assurance licenses you have, and the total number of devices under Assurance management.
- Step 2** Select the check box next to each device you want to remove from Assurance management, then click **Remove Device**.
-





## Managing Traffic Metrics

---

Prime Infrastructure supports tracing Real-Time Transport Protocol (RTP) and TCP application traffic paths across endpoints and sites. Tracing data paths depends on Cisco medianet and Web Services Management Agent (WSMA). Both are built-in features of Cisco IOS and Catalyst IOS software images that help isolate and troubleshoot problems with RTP and TCP data streams. Prime Infrastructure supports all versions of medianet and WSMA and makes it easy to enable them on any router.

Where Cisco Network Analysis Module (NAM) traffic monitoring data is not available, Prime Infrastructure supports RTP service path tracing (mediatrace) using Medianet Performance Monitor and Cisco IOS NetFlow. When properly configured, mediatrace can be your most valuable tool when troubleshooting RTP and TCP application problems.


Before you can use Prime Infrastructure's mediatrace feature, you must complete the following prerequisite setup tasks. These prerequisite tasks are required to enable Cisco Routers (ISRs, ISR G2, ASRs) and NAM devices to act as data (metrics collection) sources to monitor network traffic (RTP and TCP) performance metrics.

- [Configuring Prime Infrastructure to Use NAM Devices as Data Sources, page 12-1](#)
- [Configuring Prime Infrastructure to Use Routers and Switches as Data Sources, page 12-2](#)
- [Configuring Mediatrace on Routers and Switches, page 12-3](#)
- [Configuring WSMA and HTTP\(S\) Features on Routers and Switches, page 12-4](#)

## Configuring Prime Infrastructure to Use NAM Devices as Data Sources

If your network uses NAMs to monitor network traffic, complete the following steps to trace service paths for both RTP and TCP traffic:

- 
- Step 1** Add NAMs to the system. You can do this either automatically using Discovery, or manually using bulk import or the Device Work Center (see [Adding Devices Using Discovery](#) in the *Cisco Prime Infrastructure 2.0 User Guide*).
- Step 2** Enable NAM Data collection. To do this:
- a. Choose **Administration > System Settings > Data Sources**.
  - b. Scroll down to the NAM Data Collector section, then enable data collection on each NAM. For more information, see [Enabling NAM Data Collection](#) in the *Cisco Prime Infrastructure 2.0 User Guide*.

- Step 3** Create a site structure for your organization and use the Device Work Center to assign your principal routers to the appropriate sites. To do this:
- Choose **Design > Management Tools > Site Map Design**.
  - Add one or more campuses. For more information, see [Creating Locations or Sites](#) in the *Cisco Prime Infrastructure 2.0 User Guide*.
- Step 4** Associate your sites with authorized data sources. To do this:
- Choose **Administration > System Settings**, then select **Data Deduplication**.
  - Click **Enable Data Deduplication**, then assign authoritative data sources for Voice/Video (for RTP data) and Application Response Time (for TCP data). For more information, see [Controlling Background Data Collection Tasks, page 6-7](#).
- Step 5** Associate your sites with endpoint subnets. To do this:
- Choose **Design > Management Tools > Endpoint-Site Association**.
  - Associate subnets with your sites. For more information, see [Associating Endpoints with a Location](#) in the *Cisco Prime Infrastructure 2.0 User Guide*.
-  **Note** If you fail to do this, by default the data collected by the NAMs for these endpoints will have their sites set to “Unassigned.”
- Step 6** Configure your routers for mediatrace and WSMA (see [Troubleshooting with Mediatrace](#) in the *Cisco Prime Infrastructure 2.0 User Guide*).

## Configuring Prime Infrastructure to Use Routers and Switches as Data Sources

If your network uses cisco routers and switches to monitor network traffic, complete the following steps to enable path tracing for both RTP and TCP flows. See [Enabling NetFlow Data Collection](#) in the *Cisco Prime Infrastructure 2.0 User Guide* to get a list of all the supported routers and switches for mediatrace.

- Step 1** Create a site structure for your organization and use the Device Work Center to assign your principal routers to the appropriate sites. To do this:
- Choose **Design > Management Tools > Site Map Design**.
  - Add one or more campuses. For more information, see [Creating Locations or Sites](#) in the *Cisco Prime Infrastructure 2.0 User Guide*.
- Step 2** Associate your sites with authorized data sources. To do this:
- Choose **Administration > System Settings**, then select **Data Deduplication**.
  - Click **Enable Data Deduplication**, then assign authoritative data sources for Voice/Video (for RTP data) and Application Response Time (for TCP data). For more information, see [Controlling Background Data Collection Tasks, page 6-7](#).

- Step 3** Associate your sites with endpoint subnets. To do this:
- Choose **Design > Management Tools > Endpoint-Site Association**.
  - Associate subnets with your sites. For more information, see [Associating Endpoints with a Location](#) in the *Cisco Prime Infrastructure 2.0 User Guide*.



---

**Note** If you fail to do this, by default the data collected for these endpoints will have their sites set to “Unassigned.”

---

- Step 4** Configure your compatible routers for Medianet Performance Monitor. For more information, see [Configuring Mediatrace on Routers and Switches](#), page 12-3.
- Step 5** Configure your routers for mediatrace and WSMA (see [Troubleshooting with Mediatrace](#) in the *Cisco Prime Infrastructure 2.0 User Guide*).
- 

## Configuring Mediatrace on Routers and Switches

Prime Infrastructure supplies an out-of-the-box template that configures mediatrace on routers and switches. You must apply this configuration to every router and switch you want to use when tracing service paths.

See [Enabling NetFlow Data Collection](#) in the *Cisco Prime Infrastructure 2.0 User Guide* to get a list of all the supported routers and switches for mediatrace.

### Before You Begin

You must complete the following tasks:

- [Configuring Prime Infrastructure to Use NAM Devices as Data Sources](#), page 12-1
- [Configuring Prime Infrastructure to Use Routers and Switches as Data Sources](#), page 12-2

To configure the mediatrace-Responder-Configuration template:

---

- Step 1** Choose **Design > Configuration > Feature Design > CLI Templates > System Templates - CLI > mediatrace-Responder-Configuration**.
- Step 2** Enter the required information. See the *Cisco Prime Infrastructure 2.0 Reference Guide* for field descriptions.
- Step 3** Click **Save as New Template**. After you save the template, deploy it to your routers using the procedures in [Deploying and Monitoring Configuration Tasks](#) in the *Cisco Prime Infrastructure 2.0 User Guide*.
-

# Configuring WSMA and HTTP(S) Features on Routers and Switches

To trace service path details, the Web Services Management Agent (WSMA) over HTTP protocol must run `mediatrace` commands on your routers and switches. Configure this feature on the same set of routers and switches as in the section [Configuring Mediatrace on Routers and Switches](#).

To configure the HTTP-HTTPS Server and WSMA Configuration-IOS template:

---

**Step 1** Choose **Design > Configuration > Feature Design > CLI Templates > System Templates - CLI > HTTP-HTTPS Server and WSMA Configuration-IOS**.

**Step 2** Enter the required information. See the [Cisco Prime Infrastructure 2.0 Reference Guide](#) for field descriptions.



---

**Note** Enable the HTTP protocol. WSMA over HTTPS is *not supported* in the current version of Prime Infrastructure.

---

**Step 3** Click **Save as New Template**. After you save the template, deploy it to your routers using the procedures in [Deploying and Monitoring Configuration Tasks](#) in the *Cisco Prime Infrastructure 2.0 User Guide*.



---

**Note** When adding a device to the Device Work Center, you must provide the HTTP user and password for the device (see [Device Work Center](#) in the *Cisco Prime Infrastructure 2.0 User Guide*).

---



## Planning Network Capacity Changes

Cisco Prime Assurance allows you to view and report a variety of key performance indicators that are critical for maintaining and improving your network's operational readiness and performance quality. This information is especially critical in adapting to ever increasing network loads.



### Note

To use this feature, your Prime Infrastructure implementation must include Assurance licenses. This feature is supported on ASR platforms only.

In the following workflow, we take the role of a network administrator who has just been told that a large staff expansion is planned for a branch office. This change will add more users to the branch LAN, many of whom will be using WAN applications. We want to monitor the branch's key interfaces for usage and traffic congestion, so we can see if more users on the branch LAN will mean degraded WAN application performance for those users. To be certain we have an adequate picture, we will need to look at both short- and long-term performance trends for all the WAN applications the branch uses.

### Before You Begin

- Set up the **Top N WAN Interfaces by Utilization** dashlet:
  - a. Create an Interface Health template from **Design > Monitor Configuration**.
  - b. Deploy this template on the required routers.
  - c. Choose **Design > Management Tools > Port Grouping**, select the interfaces and click **Add to Group**, then select **WAN Interfaces** as the group.
- Enable SNMP polling (see [Enabling SNMP Polling](#) in the *Cisco Prime Infrastructure 2.0 User Guide*).

**Step 1** Choose **Operate > Operational Tools > Device Resource Estimation**.

**Step 2** To view the usage statistics for the WAN interfaces on the routers connecting remote branches to the WAN, choose **Operate > Monitoring Dashboards > Detail Dashboards** and if it is not already there, add the **Top N WAN Interfaces by Utilization** dashlet (see [Adding Dashlets](#) in the *Cisco Prime Infrastructure 2.0 User Guide*).

For each interface, this dashlet shows the site, the IP of the device hosting the WAN interface, the interface name, maximums and average utilization, and the utilization trend line for the past 24 hours.

**Step 3** To see the utilization statistics for the past month, set the **Time Frame** on the **Filters** line to **Past 4 Weeks**.

- Step 4** Find the WAN interface for the branch to which you are adding users. In the **Interface** column, click the interface's name to display that interface's dashboard. The interface dashboard shows the following for this single interface:
- Interface Details
  - Top Applications by Volume
  - Number of Users Over Time
  - Class Map Statistics
  - Interface Tx and Rx Utilization
  - Top N Clients (In and Out)
  - DSCP Classification
  - Top Application Traffic Over Time
- Step 5** Concentrate on **Top Application Traffic Over Time**, which gives a color-coded map of the top ten applications with the heaviest traffic over this interface.
- Step 6** To get a better idea of the longer-term performance trend, click the **Clock** icon next to the dashlet title to change the Time Frame to **Past 24 Hours**, **Past 4 Weeks**, or **Past 6 Months**. To zoom in on particular spikes in the graph, use the Pan and Zoom handles in the lower graph.
- Step 7** For a quick report of the same data as the interface dashboard, select **Report > Report Launch Pad**. Then select **Performance > Interface Summary**. Specify filter and other criteria for the report, select the same interface in Report Criteria, then click **Run**.

The following table shows the ISP profile used to test against (it is very similar to the Caida.org Internet profile).

**Table 13-1** Internet Profile - Traffic Profile per 1Gbps

	TCP	UDP	HTTP	RTP	Total
Connection Rate (flows per second)	5,000	5,000	800	10	10,000
Concurrent Flows	150,000	150,000	50,000	300	300,000
Packet Rate	150,000	40,000	50,000	15,000	199,000
Related Bandwidth (bps)	900Mbps	100Mbps	295Mbps	25Mbps	1GBps
Packet Size (derived)	750	313	738	208	658
Number of Parallel Active Users	60,000	Derived from the number of flows			





---

## A

### AAA

RADIUS [9-17](#)

### adding

users [9-2](#)

adding Cisco Prime Infrastructure as TACACS+ server [9-22](#)

admin users,adding [9-2](#)

aggregated historical data [6-2](#)

alarm cleanup options [5-1](#)

alarm display options [5-2](#)

### Audit Mode

basic audit [5-4](#)

template based audit [5-4](#)

automatic client troubleshooting [3-6](#)

---

## C

### Cisco Prime NCS (WAN)

about [1-1](#)

### client troubleshooting

automatic [3-6](#)

CLI sessions [7-4](#)

configuring global email parameters [2-6](#)

controller upgrade settings [7-2, 7-5, 9-3](#)

---

## E

### email

configuring parameters [2-5](#)

exclude device list [7-5](#)

exclude switch trunk ports [7-5](#)

exclude vendor list [7-5](#)

export task list [9-23](#)

---

## F

failover mechanism [8-1](#)

### FTP

turning on and off [2-11](#)

---

## G

guest account settings [9-3](#)

---

## H

### HTTP

turning on and off [2-11](#)

---

## L

Licensing, Assurance [11-11](#)

limitations for high reliability [8-6](#)

locking user accounts [9-3](#)

login disclaimer [2-12](#)

---

## M

mail server configuration [2-5](#)

### managing

licenses [11-1](#)

traffic metrics [12-1](#)

managing virtual domains [9-12](#)

---

**N**

- non-aggregated historical data [6-3](#)
- non-Cisco ACS server
  - for use with RADIUS [9-25](#)

---

**O**

- OUI search [7-5](#)

---

**R**

- RADIUS [9-17](#)
- RADIUS and TACACS+ attributes
  - virtual domains [9-13](#)
- recovering the NCS password [3-9](#)

---

**S**

- secondary Cisco Prime Infrastructure operation [8-1](#)
- Switch Port Tracing
  - Details [7-6](#)
  - Troubleshooting [7-7](#)

---

**T**

- TFTP
  - turning on and off [2-11](#)
- trace [5-7](#)
- Troubleshooting
  - Switch Port Tracing [7-7](#)
- troubleshooting
  - using logging options [5-7](#)

---

**U**

- upgrade settings
  - for controller [7-2](#)

- user preferences [9-5](#)

## users

- adding [9-2](#)
- administrators, adding [9-2](#)
- disable account [9-3](#)
- locking accounts [9-3](#)
- managing [9-1](#)

---

**V**

- vendor search [7-5](#)
- virtual domains
  - attributes [9-13](#)
  - hierarchy [9-7](#)
  - managing [9-12](#)