



Cisco Prime Infrastructure 3.0 Administrator Guide

March 4, 2016

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:

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. 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 3.0 Administrator Guide
© 2011-2016 Cisco Systems, Inc. All rights reserved.



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

CHAPTER 2**Administrator Setup Tasks 2-1**

- Setting Up Operations Center 2-1
 - Before You Begin Setting Up Operations Center 2-2
 - Activating Your Operations Center License 2-2
 - Enabling SSO for Operations Center 2-3
 - Troubleshooting Operations Center SSO Issues 2-4
 - Adding Prime Infrastructure Instances to Operations Center 2-6
 - Disabling Idle User Timeouts for Operations Center 2-6
 - Enabling AAA for Operations Center 2-7
 - Operations Center Next Steps 2-7
- Required Software Versions and Configurations 2-8
 - Configuring SNMP 2-8
 - Configuring NTP 2-9
- Configuring Data Sources for Prime Infrastructure With Assurance 2-9
 - Supported Assurance Data Sources 2-9
 - Configuring Assurance Data Sources 2-10
- Enabling Medianet NetFlow 2-11
- Enabling NetFlow and Flexible NetFlow 2-13
- Deploying Network Analysis Modules (NAMs) 2-14
- Enabling Performance Agent 2-14
- Installing Prime Infrastructure Patches 2-15

CHAPTER 3**Prime Infrastructure Server Settings 3-1**

- Available System Settings 3-2
- Configuring Email Settings 3-6
- Configuring Global SNMP Settings 3-7
 - Viewing SNMP Credential Details 3-8
 - Adding SNMP Credentials 3-9
 - Importing SNMP Credentials 3-10
- Configuring Proxy Settings 3-11

- Configuring Server Port and Global Timeout Settings 3-12
- Enabling Compliance Services 3-13
- Configuring Remote FTP, TFTP, and SFTP Servers 3-14
- Accessing ACS View Servers From Prime Infrastructure 3-14
- Configuring ISE Servers 3-14
- Specifying Administrator Approval for Jobs 3-15
- Approving Jobs 3-15
- Specifying Login Disclaimer Text 3-15
- Adding Device Information to a User Defined Field 3-16
- Managing OUIs 3-16
 - Adding a New Vendor OUI Mapping 3-17
 - Uploading an Updated Vendor OUI Mapping File 3-17
- Adding Notification Receivers to Prime Infrastructure 3-18
 - Removing Notification Receivers 3-18
 - Sample Log File from North-Bound SNMP Receiver 3-19
- Setting Up HTTPS Access to Prime Infrastructure 3-19
 - Generating and Applying Self-Signed Certificates 3-20
 - Obtaining and Importing CA-Signed Certificates 3-20
 - Deleting CA-Signed Certificates 3-21
- MIB to Prime Infrastructure Alert/Event Mapping 3-23
- Product Feedback Data Collection 3-25

CHAPTER 4

- Maintaining Prime Infrastructure Server Health 4-1**
 - Monitoring Prime Infrastructure Health 4-2
 - Troubleshooting Prime Infrastructure 4-2
 - Launching the Cisco Support Community 4-3
 - Opening a Support Case 4-3
 - Evaluating OVA Size and System Resources 4-4
 - Viewing the Number of Devices Prime Infrastructure Is Managing 4-5
 - Improving Prime Infrastructure Performance 4-6
 - Tuning the Server 4-6
 - Enabling Server Tuning During Restarts 4-7
 - Modifying VM Resource Allocation Using VMware vSphere Client 4-7
 - Compacting the Prime Infrastructure Database 4-8
 - Configuring Client Performance Settings 4-8
 - Enabling Automatic Client Troubleshooting 4-9
 - Enabling DNS Hostname Lookup 4-9
 - Specifying How Long to Retain Client Association History Data 4-10

| | |
|---|------|
| Polling Clients When Receiving Client Traps/Syslogs | 4-10 |
| Saving Client Traps as Events | 4-11 |
| Saving 802.1x and 802.11 Client Traps as Events | 4-11 |
| Enabling Enhanced Client Traps | 4-11 |
| Optimizing Memory for Assurance Processing | 4-13 |
| Monitoring Assurance Memory Allocation and Demand | 4-14 |
| Increasing the Assurance Memory Pool Via CLI | 4-14 |
| Balancing Assurance Memory Allocation | 4-15 |
| Resetting Assurance Memory Allocation | 4-15 |
| Resetting the Assurance Memory Pool | 4-16 |
| Managing Data Sources | 4-17 |
| Viewing Current Data Sources | 4-17 |
| Deleting Data Sources | 4-18 |
| Performing Special Administrative Tasks | 4-19 |
| Connecting Via CLI | 4-20 |
| Starting Prime Infrastructure | 4-21 |
| Checking Prime Infrastructure Server Status | 4-21 |
| Checking Prime Infrastructure Version and Patch Status | 4-22 |
| Stopping Prime Infrastructure | 4-22 |
| Restarting Prime Infrastructure | 4-23 |
| Removing Prime Infrastructure | 4-23 |
| Resetting Prime Infrastructure to Defaults | 4-24 |
| Restoring Physical Appliances to Clean State | 4-24 |
| Changing the Prime Infrastructure Host Name | 4-25 |
| Enabling the FTP User | 4-25 |
| Changing the Root User Password | 4-26 |
| Recovering Administrator Passwords on Virtual Appliances | 4-27 |
| Recovering Administrator Passwords on Physical Appliances | 4-28 |
| Getting the Installation ISO Image | 4-29 |
| Keeping Prime Infrastructure Software Updated | 4-30 |
| Viewing Installed and Available Software Updates | 4-30 |
| Getting Software Update Notifications | 4-31 |
| Configuring Software Update Notifications | 4-31 |
| Viewing Details of Installed Software Updates | 4-32 |
| Viewing Installed Updates From the Login Page | 4-32 |
| Viewing Installed Updates From the About Page | 4-32 |
| Installing Software Updates | 4-33 |
| Installing Software Updates from Cisco.com | 4-33 |
| Uploading and Installing Downloaded Software Updates | 4-34 |

| | |
|--|------|
| Using Your Cisco.com Account Credentials with Prime Infrastructure | 4-35 |
| Saving Cisco.com Account Credentials in Prime Infrastructure | 4-35 |
| Deleting Cisco.com Account Credentials | 4-35 |
| Configuring Support Request Settings | 4-36 |
| Managing Disk Space Issues | 4-37 |

CHAPTER 5

Backing Up and Restoring Prime Infrastructure 5-1

| | |
|--|------|
| Backup and Restore Concepts | 5-1 |
| Backup Types | 5-2 |
| Backup Scheduling | 5-2 |
| Backup Repositories | 5-3 |
| Backup Filenames | 5-4 |
| Validating Backups | 5-5 |
| Information Contained in Backup Files | 5-6 |
| Using Backup and Restore to Replace Servers | 5-7 |
| Using Automatic Application Backups | 5-7 |
| Scheduling Automatic Application Backups | 5-8 |
| Triggering Application Backups | 5-8 |
| Specifying Automatic Application Backup Repositories | 5-9 |
| Creating Local Backup Repositories | 5-9 |
| Deleting Local Backup Repositories | 5-10 |
| Using Remote Backup Repositories | 5-11 |
| Types of Backup Repositories | 5-12 |
| Using Remote NFS Backup Repositories | 5-12 |
| Before You Begin NFS Backup Configuration | 5-13 |
| Configuring the NFS Backup Server | 5-14 |
| Configuring Prime Infrastructure to Use the NFS Backup Server | 5-15 |
| Using Remote SFTP Backup Repositories | 5-16 |
| Using Remote FTP Backup Repositories | 5-18 |
| Taking Backups From the Command Line | 5-19 |
| Taking Application Backups | 5-19 |
| Taking Appliance Backups | 5-20 |
| Restoring From Backups | 5-21 |
| Restoring From Application Backups | 5-21 |
| Restoring From Appliance Backups | 5-23 |
| Migrating to Another Virtual Appliance Using Backup and Restore | 5-24 |
| Migrating to Another Physical Appliance Using Backup and Restore | 5-25 |
| Recovering From Failed Restores | 5-26 |
| Managing Disk Space Issues During Backup and Restore | 5-26 |

Using Backup and Restore with Operations Center 5-27

CHAPTER 6
Maintaining Network Health 6-1

- Configuring Alarm and Event Settings 6-1
 - Specifying Alarm Clean Up and Display Options 6-1
 - Changing Alarm Severities 6-3
 - Changing the Auto Clear Interval 6-4
- Enabling Change Audit Notifications 6-4
- Configuring Syslog Message Receivers for System Changes 6-5
- Downloading and Emailing Error Logs 6-6
- Enabling SNMP Tracing 6-6
- Changing Syslog Logging Options 6-7
- Changing Logging Options to Enhance Troubleshooting 6-7
 - Changing Mobility Service Engine Logging Options 6-8
 - MAC Address-Based Logging 6-9
 - Downloading Mobility Services Engine Log Files 6-9
- Configuring Technical Support Request Settings 6-10

CHAPTER 7
Managing Data Collection and Retention 7-1

- Specifying Data Retention by Category 7-2
- Specifying Data Retention By Database Table 7-3
- About Performance Data Retention 7-4
- Specifying Client Data Retrieval and Retention 7-5
- About Historical Data Retention 7-6
- Enabling Data Deduplication 7-7
- Controlling Report Storage and Retention 7-8
- Specifying Inventory Collection After Receiving Events 7-8
- Controlling Configuration Deployment Behavior 7-9
 - Archiving Device Configurations Before Template Deployment 7-9
 - Rolling Back Device Configurations on Template Deployment Failure 7-9
 - Specifying When and How to Archive WLC Configurations 7-10
- Controlling Data Collection Jobs 7-11
 - Scheduling Data Collection Jobs 7-11
 - Pausing and Resuming Data Collection Jobs 7-12
 - Running Data Collection Jobs Immediately 7-12
 - About Data Collection Jobs 7-13
 - Controlling Prime Infrastructure Background Tasks 7-14

Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure 7-21

CHAPTER 8

Configuring Controller and AP Settings 8-1

- Configuring SNMP Credentials for Rogue AP Tracing 8-1
- Configuring Protocols for CLI Sessions 8-2
- Refreshing Controllers After an Upgrade 8-2
- Tracking Switch Ports to Rogue APs 8-3
- Configuring Switch Port Tracing 8-3
 - Establishing Switch Port Tracing 8-6
 - Switch Port Tracing Details 8-6
 - Switch Port Tracing Troubleshooting 8-8
- Frequently Asked Questions on Rogues and Switch Port Tracing 8-9
 - How Do You Configure Auto SPT? 8-9
 - How Does Auto SPT Differ From Manual SPT? 8-10
 - Where Can I See SPT Results (Manual and Auto)? 8-11
 - How Can I Ensure Auto SPT Runs Smoothly? 8-11
 - Why Does Auto SPT Take Longer to Find Wired Rogues? 8-13
 - How Can I Detect Wired Rogues on Trunk Ports? 8-13
 - How Do You Configure Switch Port Location? 8-13
 - How Can I Use the Auto SPT “Eliminate By Location” Feature? 8-14
 - What is the Difference Between “Major Polling” and “Minor Polling”? 8-15

CHAPTER 9

Configuring High Availability 9-1

- How High Availability Works 9-2
 - About the Primary and Secondary Servers 9-3
 - Sources of Failure 9-4
 - File and Database Synchronization 9-4
 - HA Server Communications 9-5
 - Health Monitor Process 9-5
 - Health Monitor Web Page 9-6
 - Using Virtual IP Addressing with HA 9-7
 - Hot Standby Behavior 9-7
- Planning HA Deployments 9-9
 - Network Throughput Restrictions on HA 9-10
 - Using the Local Model 9-11
 - Using the Campus Model 9-11
 - Using the Remote Model 9-12
 - What If I Cannot Use Virtual IP Addressing? 9-13
 - Using SSL Certificates in an HA Environment 9-13

| | |
|---|------|
| Automatic Versus Manual Failover | 9-14 |
| Setting Up High Availability | 9-15 |
| Before You Begin Setting Up High Availability | 9-16 |
| Installing the Secondary Server | 9-17 |
| Registering High Availability on the Primary Server | 9-18 |
| Checking High Availability Status | 9-19 |
| What Happens During HA Registration | 9-19 |
| Patching Paired High Availability Servers | 9-21 |
| Patching New High Availability Servers | 9-23 |
| Monitoring High Availability | 9-24 |
| Accessing the Health Monitor Web Page | 9-25 |
| Triggering Failover | 9-25 |
| Triggering Failback | 9-26 |
| Responding to Other HA Events | 9-27 |
| HA Registration Fails | 9-27 |
| Network is Down (Automatic Failover) | 9-28 |
| Network is Down (Manual Failover) | 9-29 |
| Process Restart Fails (Automatic Failover) | 9-30 |
| Process Restart Fails (Manual Failover) | 9-31 |
| Primary Server Restarts During Sync (Manual Failover) | 9-32 |
| Secondary Server Restarts During Sync | 9-33 |
| Both HA Servers Are Down | 9-33 |
| Both HA Servers Are Powered Down | 9-34 |
| Both HA Servers Are Down and the Secondary Will Not Restart | 9-35 |
| Replacing the Primary Server | 9-36 |
| Recovering From Split-Brain Scenario | 9-37 |
| High Availability Reference Information | 9-38 |
| HA Configuration Mode Reference | 9-38 |
| HA State Reference | 9-39 |
| HA State Transition Reference | 9-40 |
| High Availability CLI Command Reference | 9-41 |
| Resetting the HA Authentication Key | 9-42 |
| Removing HA Via the GUI | 9-42 |
| Removing HA Via the CLI | 9-43 |
| Removing HA During Restore | 9-43 |
| Removing HA During Upgrade | 9-44 |
| Using HA Error Logging | 9-44 |
| Resetting the HA Server IP Address or Host Name | 9-45 |
| Configuring MSE High Availability | 9-45 |

- Overview of the MSE High Availability Architecture 9-45
 - MSE High Availability Pairing Matrix 9-46
 - Guidelines and Limitations for MSE High Availability 9-46
 - Failover Scenario for MSE High Availability 9-47
 - Failback Scenario for MSE High Availability 9-47
 - Licensing Requirements for MSE High Availability 9-47
- Setting Up MSE High Availability: Workflow 9-48
 - Preparing the MSEs for High Availability 9-48
 - Configuring MSE High Availability on Primary MSEs 9-49
 - Configuring MSE High Availability on Secondary MSEs 9-55
 - Replacing Primary MSEs 9-60

CHAPTER 10

Configuring Wireless Redundancy 10-1

- About Wireless Controller Redundancy 10-1
- Prerequisites and Limitations for Redundancy 10-2
- Configuring Redundancy Interfaces 10-3
- Configuring Redundancy on Primary Controllers 10-3
- Configuring Redundancy on Secondary Controllers 10-4
- Monitoring Redundancy States 10-5
- Running the Redundancy Status Background Task 10-5
- Configuring Peer Service Port IPs and Subnet Mask 10-6
- Adding Peer Network Routes 10-6
- Resetting and Uploading Files from the Secondary Server 10-7
- Disabling Redundancy on Controllers 10-8

CHAPTER 11

Controlling User Access 11-1

- Managing User Accounts 11-1
 - Viewing Active User Sessions 11-2
 - Adding User Accounts 11-2
 - Creating Additional Administrative Users 11-3
 - Deleting User Accounts 11-4
 - Configuring Guest Account Settings 11-4
 - Disabling User Accounts 11-5
 - Disabling the Web Root Account 11-6
 - Changing User Passwords 11-6
 - Changing Password Policies 11-7
 - Changing the Global Idle Timeout 11-7
- Using Lobby Ambassadors to Manage Guest User Accounts 11-8

| | |
|--|-------|
| Managing Guest User Accounts: Workflows | 11-9 |
| Creating Lobby Ambassador Accounts | 11-10 |
| Logging in as a Lobby Ambassador | 11-10 |
| Creating Guest User Accounts as a Lobby Ambassador | 11-11 |
| Scheduling Guest User Accounts | 11-11 |
| Printing or Emailing Guest User Details | 11-12 |
| Viewing Lobby Ambassador Activities | 11-12 |
| Saving Guest Accounts on a Device | 11-13 |
| Editing Guest User Credentials | 11-13 |
| Using User Groups to Control Access | 11-14 |
| North Bound API User Group | 11-15 |
| Viewing User Group Privileges and Membership | 11-16 |
| Changing User Group Privileges | 11-16 |
| Changing User Group Memberships | 11-17 |
| Using Virtual Domains to Control Access | 11-17 |
| Understanding Virtual Domains | 11-18 |
| User Access in Virtual Domains | 11-21 |
| Creating Virtual Domains | 11-22 |
| Adding Site Maps to Virtual Domains | 11-23 |
| Adding Network Devices to Virtual Domains | 11-23 |
| Adding Access Points to Virtual Domains | 11-24 |
| Importing Virtual Domains | 11-24 |
| Adding Users to Virtual Domains | 11-25 |
| Adding Virtual Elements to Virtual Domains | 11-26 |
| Changing Virtual Domain Access | 11-27 |
| Deleting Virtual Domains | 11-28 |
| Exporting Virtual Domain RADIUS and TACACS+ Attributes | 11-29 |
| Auditing User Access | 11-30 |
| Accessing the Audit Trail for a User Group | 11-30 |
| Viewing Application Logins and Actions | 11-30 |
| Viewing User-Initiated Events | 11-31 |
| Configuring AAA on Prime Infrastructure | 11-31 |
| Setting the AAA Mode | 11-32 |
| Adding TACACS+ Servers | 11-33 |
| Adding RADIUS Servers | 11-33 |
| Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes | 11-34 |
| Renewing AAA Settings After Installing a New Prime Infrastructure Version | 11-34 |
| Adding SSO Servers | 11-35 |

- Configuring High Availability for SSO 11-35
- Configuring SSO Server AAA Mode 11-36
- Authenticating AAA Users Through RADIUS Using ISE: Workflow 11-37
 - Adding Prime Infrastructure as an AAA Client in ISE 11-37
 - Creating a New User Group in ISE 11-38
 - Creating a New User and Adding to a User Group in ISE 11-39
 - Creating a New Authorization Profile in ISE 11-39
 - Creating an Authorization Policy Rule in ISE 11-40
 - Creating a Simple Authentication Policy in ISE 11-41
 - Creating a Rule-Based Authentication Policy in ISE 11-41
 - Configuring AAA in Prime Infrastructure 11-42
- Configuring ACS 5.x for Prime Infrastructure: Workflow 11-43
 - Creating ACS Network Devices and AAA Clients 11-43
 - Adding ACS Groups 11-44
 - Adding ACS Users 11-44
 - Creating ACS Policy Elements or Authorization Profiles for RADIUS 11-44
 - Creating ACS Policy Elements or Authorization Profiles for TACACS+ 11-45
 - Creating ACS Service Selection Rules for RADIUS 11-45
 - Creating ACS Service Selection Rules for TACACS+ 11-46
 - Configuring ACS Access Services for RADIUS 11-46
 - Configuring ACS Access Services for TACACS+ 11-46

CHAPTER 12

Advanced Monitoring 12-1

- Enabling WAN Optimization 12-3

CHAPTER 13

Managing Licenses 13-1

- Prime Infrastructure Licensing 13-1
 - Purchasing Prime Infrastructure Licenses 13-2
 - Verifying License Details 13-2
 - Adding Licenses 13-3
 - Deleting Licenses 13-3
 - Troubleshooting Licenses 13-4
- Controller Licensing 13-6
- MSE Licensing 13-7
 - MSE License Structure Matrix 13-8
 - Sample MSE License File 13-8
 - Revoking and Reusing an MSE License 13-9
 - MSE Services Coexistence 13-9
 - Managing MSE Licenses 13-10

| | | |
|-------------------|--|-------------|
| | Registering Product Authorization Keys | 13-11 |
| | Installing Client and wIPS License Files | 13-12 |
| | Deleting Mobility Services Engine License Files | 13-13 |
| | Assurance Licensing | 13-13 |
| | Verifying Assurance License Details | 13-14 |
| | Adding License Coverage For NetFlow and NAM Devices | 13-15 |
| | Deleting License Coverage for NetFlow and NAM Devices | 13-15 |
| CHAPTER 14 | Managing Traffic Metrics | 14-1 |
| | Prerequisites for Traffic Metrics With Mediatrace | 14-1 |
| | Configuring Prime Infrastructure to Use NAM Devices as Data Sources | 14-2 |
| | Configuring Prime Infrastructure to Use Routers and Switches as Data Sources | 14-3 |
| | Configuring Mediatrace on Routers and Switches | 14-4 |
| | Configuring WSMA and HTTP(S) Features on Routers and Switches | 14-5 |
| CHAPTER 15 | Planning Network Capacity Changes | 15-1 |
| APPENDIX A | Internal SNMP Trap Generation | A-1 |
| | About Internal Trap Generation | A-1 |
| | Prime Infrastructure SNMP Trap Types | A-2 |
| | Ensuring Trap-Related Background Tasks are Running | A-5 |
| | Generic SNMP Trap Format | A-6 |
| | Prime Infrastructure SNMP Trap Reference | A-7 |
| | Working With Prime Infrastructure Traps | A-12 |
| | Configuring Notifications | A-12 |
| | Configuring Notification Receivers | A-13 |
| | Port Used To Send Traps | A-14 |
| | Configuring Email Notifications for SNMP Traps | A-14 |
| | Configuring Email Server Settings | A-14 |
| | Viewing Events and Alarms for SNMP Traps | A-15 |
| | Filtering Events and Alarms for SNMP Traps | A-15 |
| | Filtering for SNMP Traps Using Quick Filters | A-15 |
| | Filtering for SNMP Traps Using Advanced Filters | A-16 |
| | Purging Alarms for SNMP Traps | A-17 |
| | Troubleshooting Prime Infrastructure SNMP Traps | A-17 |
| APPENDIX B | Best Practices: Server Security Hardening | B-1 |
| | Hardening Server Security | B-1 |

- Disabling Insecure Services **B-2**
- Disabling Root Access **B-2**
- Using SNMPv3 Instead of SNMPv2 **B-3**
 - Using SNMv3 When Adding Devices **B-3**
 - Using SNMv3 When Importing Devices **B-4**
 - Using SNMv3 When Running Discovery **B-4**
- Authenticating With External AAA **B-5**
 - Setting Up External AAA Via GUI **B-5**
 - Setting Up External AAA Via CLI **B-6**
- Enabling NTP Update Authentication **B-7**
- Enabling Certificate-Based OCSP Authentication **B-8**
- Importing Client Certificates Into Web Browsers **B-10**
- Setting Up SSL Certification **B-11**
 - Setting Up SSL Client Certification **B-12**
 - Setting Up SSL Server Certification **B-13**
- Enabling OCSP Settings on the Prime Infrastructure Server **B-13**
- Setting Up Local Password Policies **B-14**
- Disabling Individual TCP/UDP Ports **B-15**
- Checking On Server Security Status **B-16**

CHAPTER C

Configuring High Availability for Plug and Play Gateway C-1

- How Cisco Plug and Play Gateway HA Works **C-1**
 - Cisco Plug and Play Gateway HA Prerequisites **C-2**
- Setting up Cisco Plug and Play Gateway HA **C-2**
 - Setting up Standalone Cisco Plug and Play Gateway for Prime Infrastructure HA **C-2**
 - Prime Infrastructure in HA with Virtual IP Address **C-3**
 - Prime Infrastructure in HA with Different IP Address **C-3**
 - Cisco Standalone Plug and Play Gateway Server HA Setup **C-4**
 - Cisco Plug and Play Gateway Status **C-4**
- Removing Cisco Plug and Play Gateway in HA **C-7**
- Cisco Plug and Play Gateway HA and Prime Infrastructure Combinations **C-7**
- Limitations of Cisco Plug and Play Gateway HA **C-8**

C-8



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.



Administrator Setup Tasks

The Cisco Prime Infrastructure administrator should plan on completing several initial setup tasks soon after the product is installed.

Related Topics

- [Setting Up Operations Center](#)
- [Required Software Versions and Configurations](#)
- [Configuring Data Sources for Prime Infrastructure With Assurance](#)
- [Enabling Medianet NetFlow](#)
- [Enabling NetFlow and Flexible NetFlow](#)
- [Deploying Network Analysis Modules \(NAMs\)](#)
- [Installing Prime Infrastructure Patches](#)

Setting Up Operations Center

Prime Infrastructure Operations Center is a licensed feature that allows you to manage multiple instances of Prime Infrastructure from a single instance. Before you can use Operations Center, you must first:

1. Activate your Operations Center license on the Prime Infrastructure server that will host Operations Center.
2. Enable single sign-on (SSO) on each of the Prime Infrastructure instances that you will manage using Operations Center.
3. Add the Prime Infrastructure instances to Operations Center.
4. (Optional) Disable the personal and global idle-user timeouts for Operations Center and all of its managed instances.
5. (Optional) Configure remote AAA using TACACS+ or RADIUS servers for Operations Center and all of its managed instances,

The Related Topics explain how to complete each of these tasks.

Related Topics

- [Before You Begin Setting Up Operations Center](#)
- [Activating Your Operations Center License](#)
- [Enabling SSO for Operations Center](#)

- [Troubleshooting Operations Center SSO Issues](#)
- [Adding Prime Infrastructure Instances to Operations Center](#)
- [Disabling Idle User Timeouts for Operations Center](#)
- [Enabling AAA for Operations Center](#)
- [Operations Center Next Steps](#)

Before You Begin Setting Up Operations Center

Before setting up Operations Center:

- Verify that the DNS entry for the Prime Infrastructure server that will host the Operations Center matches the host name configured on that server. For example: Running the commands **nslookup ipaddress** and **hostname** on the Prime Infrastructure server that will host the Operations Center should yield the same output.
- Ensure that all users who will access network information using Operations Center have both NBI Read and NBI Write access privileges. You can do this by editing these users' profiles to make them members of the "NBI Read" and "NBI Write" User Groups (see "Changing User Group Memberships" in Related Topics).
- By default, the maximum SSO login sessions for one user is five in Operation Center. This is also applicable for instances. Hence, ensure that the number of Active SSO Sessions does not exceed five, else the managed instances will go to unreachable state.
- Ensure that Prime Infrastructure is upgraded from 2.2.X to 3.0 before upgrading the Operations Center. Inline upgrading is also available for Operations Center.

Related Topics

- [Setting Up Operations Center](#)
- [Changing User Group Memberships](#)

Activating Your Operations Center License

Operations Center does not have a separate installation procedure. After you have installed Prime Infrastructure, you enable Operations Center by activating an Operations Center license on that installed server instance. The number of Prime Infrastructure instances you can manage using Operations Center depends on the license you have purchased.

Operations Center requires a **Cluster Base** License File and **Incremental** License File. For details, see the *Cisco Prime Infrastructure Ordering and Licensing Guide* (in Related Topics).

-
- Step 1** Select **Administration > Licenses and Software Updates > Licenses**. The Licenses Summary page displays.
- Step 2** From the left-hand navigation menu, select **Files > License Files**. The License Files page displays.
- Step 3** Click **Add**. The Add a License File dialog box displays.
- Step 4** Click **Choose File**.
- Step 5** Navigate to your license file, select it, and then click **Open**.
- Step 6** Click **OK**. Your license should now be listed in the Licenses > License Files page.

- Step 7** Log out of Prime Infrastructure and then log back in. The login page that appears should display “Cisco Prime Infrastructure Operations Center”, which indicates the license has been applied.
-

Related Topics

- [Setting Up Operations Center](#)
- [Cisco Prime Infrastructure Ordering and Licensing Guide](#)

Enabling SSO for Operations Center

Complete the following procedure as many times as needed to enable SSO:

1. **First:** On the Prime Infrastructure server that will host Operations Center. This server must act as the SSO server.
2. **Then:** On all the other Prime Infrastructure servers that the Operations Center will manage. These servers must act as the SSO clients.

For additional help, see the related topic, “Troubleshooting Operations Center SSO Issues”.

Please note that you can configure more than one SSO server for Prime Infrastructure. However, the first SSO server you configure will always act as the system SSO server until it fails. In that case, authentication will fall back to the second SSO server, and so on.

-
- Step 1** Select **Administration > Users > Users, Roles & AAA**. The AAA Mode Settings page displays.
- Step 2** In the AAA Mode field, select the **Local** radio button and then click **Save**.
- Step 3** From the left-hand navigation menu, click **SSO Servers** to open the SSO Servers page.
- Step 4** Choose **Select a Command > Add SSO Server > Go**. The Add SSO Servers page displays.
- Step 5** Enter the following information:
- **IP Address:** Enter either the IP address of the server on which you activated your Operations Center license (i.e., Operations Center IP).
Note that you must be consistent in specifying either the IP address or the Domain Name across all of the Operations Center clients (that is, the managed instances of Prime Infrastructure) that you add to the SSO server. This is because the browser cookies that provide the Single Sign-On functionality are stored in the browser according to either the IP address or the Domain Name given here.
 - **DNS Name:** DNS name of the server on which you activated the license. Enter the DNS name only when the forward and reverse DNS lookups are the same. Otherwise setup SSO with the Server IP Address.
 - **Port:** The port used to log in to the SSO server. By default, port 443 is set. Do not change this value.
 - **Retries:** The number of retries to attempt when logging into the SSO server. By default, this value is set to 1.
 - **Certificate Type:** Select the type of SSL/TLS certificate that the SSO server uses. Select from either Self-Signed Certificate or Certificate Authority (CA) certificate type.
- When you are finished, click **Save**. The server should now be listed on the Add SSO Servers page.
- Step 6** From the left-hand navigation menu, select **AAA Mode Settings** to reopen the AAA Mode Settings page.
- Step 7** Click the **SSO** radio button (if it is not already selected) and then click **Save**.

Step 8 After enabling SSO, log out of the instance of Prime Infrastructure on which you enabled SSO and then log back in.

On the login page for the Operations Center instance, you will see “Cisco Operations Center [SSO]”. After you log in, the product title displayed at the top of the page will be “Cisco Prime Infrastructure Operations Center”.

On the login page for each of the managed instances, you will see “Cisco Operations Center [SSO]”. After you log in, the product title will be “Cisco Prime Infrastructure”.

Related Topics

- [Setting Up Operations Center](#)
- [Troubleshooting Operations Center SSO Issues](#)

Troubleshooting Operations Center SSO Issues

As explained in “Enabling SSO for Operations Center”, you must enable single sign-on (SSO) such that the Operations Center server acts as the SSO server and the managed instances of Prime Infrastructure act as SSO clients. Here are some common SSO setup pitfalls and how you can avoid them:

- There are different ways to add the SSO server to the SSO client. Each requires a different level of DNS set up. If you are using:
 - Self-signed setting: This requires both forward and reverse DNS lookup of the SSO server from the SSO client. This means that if you take the Fully Qualified Domain Name (FQDN) of the SSO server and resolve it using DNS, you can take the resulting IP address, do a reverse lookup, and get the original FQDN.
 - CA-signed setting with IP addresses: Neither reverse nor forward DNS mappings are required.
 - CA-signed setting with domain names: Only forward DNS mapping (domain name to IP address) is needed.
- If you are using the self-signed setting: Verify that the DNS entry for the Prime Infrastructure server that will host the Operations Center matches the host name configured on that server. To do this, run **nslookup ip-address**, replacing *ip-address* with the IP address of your Operations Center server. Then log in to the admin console of the Operations Center server and run the **show running-config** command. Ensure that the output of these two commands matches.
- If you are using the self-signed setting: Access the Operations Center server using a browser and check that Common Name (CN) of the certificate matches the FQDN of the Operations Center server. The steps to follow vary with the browser you are using. For example, using Chrome:
 - a. Click on the lock icon displayed at the far left in the browser’s URL box.
 - b. Select **Certificate Information**.
 - c. Expand the **Details** field to view the Common Name of the certificate. It must match the correct FQDN of the server. If the two do not match, the Prime Infrastructure administrator must regenerate the SSO certificate.
- When configuring SSO, leave the “Certificate Type” as “CA”. This will result in fewer checks to verify the certificate on the SSO client side
- Ensure that the SSO Server and clients are all added consistently. For example, use either the IP address or FQDN across all instances. Don’t mix and match these.

Once SSO is configured you can check to see if it is working as expected by logging in to Operations Center (the SSO server) and opening a new browser tab to access one of the Prime Infrastructure instances (an SSO client). SSO should automatically log you into the Prime Infrastructure instance automatically, without requiring you to re-authenticate.

If you are still having Operations Center SSO login and connection issues:

1. Download and examine related Prime Infrastructure logs and, where necessary, use enhanced logging to check for errors and timeouts (for details, see the related topics “Downloading and Emailing Error Logs” and “Changing Logging Options to Enhance Troubleshooting”). Be sure to look at the log files from both Operations Center (the SSO server) and the managed instances (SSO clients) of Prime Infrastructure. Log files of special interest to SSO and Operations Center are:
 - xmpNbiFw.log
 - xmpNbifwPerformance.log: Look at the response times for APIs dispatched from Operations Center to the managed instances.
 - cas.log
 - ncs-*.log
 - XmpUserMgmtRbac.log
 - usermgmt.log:
2. Adjust the values for `cluster.timeout` and `cluster.connectionTimeout` in the file `/opt/CSCOLumos/conf/cluster.properties`. These two properties have the following defaults:
 - `cluster.timeout=40000`: This is the timeout (in milliseconds) for all the requests dispatched from Operations Center.
 - `cluster.connectionTimeout=5000`: This is the timeout used when Operations Center tries to establish initial connections with the managed instances.

If there is a high latency between Operations Center and the managed instances having connection issues, increasing these timeout limits can help.

When you are finished changing these values, restart the Operations Center using the commands explained in “Restarting Prime Infrastructure” (see Related Topics).

Related Topics

- [Enabling SSO for Operations Center](#)
- [Setting Up Operations Center](#)
- [Downloading and Emailing Error Logs](#)
- [Changing Logging Options to Enhance Troubleshooting](#)
- [Restarting Prime Infrastructure](#)

Adding Prime Infrastructure Instances to Operations Center

Once you have configured SSO on Operations Center and the other Prime Infrastructure instances, you must add each of the Prime Infrastructure managed instances to Operations Center.

Prime Infrastructure 3.0 instances can be managed only in Prime Operations Center. Support for Prime Infrastructure 2.2.X (N-1 Version) instances will be provided in later releases.

-
- Step 1** Log in to Prime Infrastructure Operations Center.
- Step 2** Select **Monitor > Manage and Monitor Servers**.
- Step 3** Click **Add**.
- Step 4** Enter the IP address and port number of the instance of Prime Infrastructure that you want to manage using Operations Center. You may also enter an alias for the server. Then click **OK**.
- By default, port 443 is set. Do not change this value.
- Step 5** Repeat these steps to add other Prime Infrastructure servers, up to the license limit.
-

Related Topics

- [Setting Up Operations Center](#)

Disabling Idle User Timeouts for Operations Center

By default, Prime Infrastructure automatically signs out all users whose sessions stay idle for too long. This feature is enabled by default to preserve network bandwidth and Prime Infrastructure processing cycles for active use.

This feature can be annoying for Operations Center users, who will typically have sessions opened not only with Operations Center, but with one or more of the instances of Prime Infrastructure that Operations Center is managing. Idleness in one of these sessions can force a global idle-user timeout for all the sessions, resulting in a sudden logout without warning.

To avoid this inconvenience, Prime Infrastructure administrators must:

1. Disable the global idle user timeout feature, as explained in “Changing the Global Idle Timeout” in Related Topics. Note that the administrator must disable this feature *separately*, on *each* of the Prime Infrastructure managed instances that Operations Center manages.
2. Instruct Operations Center users to disable the user-specific idle-user timeout feature for the Prime Infrastructure managed instances they access, as explained in “Changing Your Idle User Timeout” in Related Topics. Note that each Prime Infrastructure user must disable this feature *separately*, on *each* of the Prime Infrastructure managed instances they access.

Related Topics

- [Setting Up Operations Center](#)
- [Changing the Global Idle Timeout](#)
- [Changing Your Idle User Timeout](#)

Enabling AAA for Operations Center

Operation Center supports local authentication as well as remote AAA using TACACS+ and RADIUS servers. Using remote AAA is optional, but if you want to use it, you must first add a TACACS+ or RADIUS server to Operations Center. Follow this workflow:

1. On the Operations Center instance of Prime Infrastructure, add one or more TACACS+ or RADIUS servers to provide AAA services. For details, see “Adding TACACS+ Servers” or “Adding RADIUS Servers” in related topics. Remember that the shared secret configured on the TACACS+ or RADIUS server must match the shared secret you enter when adding this AAA server to Operations Center.
2. Set the AAA mode on the Operation Center instance, as explained in “Setting the AAA Mode”

Related Topics

- [Setting Up Operations Center](#)
- [Adding TACACS+ Servers](#)
- [Adding RADIUS Servers](#)
- [Setting the AAA Mode](#)

Operations Center Next Steps

When you have completed the setup tasks, you are ready to use Operations Center. See “Monitoring Multiple Prime Infrastructure Instances” for typical tasks you perform when using Operations Center.

Related Topics

- [Monitoring Multiple Prime Infrastructure Instances](#)
- [Setting Up Operations Center](#)

Required Software Versions and Configurations

To work with Prime Infrastructure, your devices must run at least the minimum required software versions shown in the list of supported devices. You can access this list using the Prime Infrastructure user interface: Choose **Help > Supported Devices**.

You must also configure your devices to support SNMP traps and syslogs, and the Network Time Protocol (NTP), as explained in the related topics.

Related Topics

- [Configuring SNMP](#)
- [Configuring NTP](#)

Configuring SNMP

To ensure that Prime Infrastructure can query SNMP devices and receive traps and notifications from them, you must:

- Set SNMP credentials (community strings) on each device you want to manage using Prime Infrastructure.
- Configure these same devices to send SNMP notifications to the Prime Infrastructure server.

Use the following Cisco IOS configuration commands to set read/write and read-only community strings on an SNMP device:

```
admin(config)# snmp-server community private RW
```

```
admin(config)# snmp-server community public RW
```

where *private* and *public* are the community strings you want to set.

After you set the community strings, you can specify that device notifications be sent as traps to the Prime Infrastructure server using the following Cisco IOS global configuration command on each SNMP device:

```
admin(config)# snmp-server host Host traps version community  
notification-type
```

where:

- *Host* is the IP address of the Prime Infrastructure server.
- *version* is the version of SNMP that is used to send the traps.
- *community* is the community string sent to the server with the notification operation.
- *notification-type* is the type of trap to send.

You may need to control bandwidth usage and the amount of trap information being sent to the Prime Infrastructure server using additional commands.

For more information on configuring SNMP, see:

- The `snmp-server community` and `snmp-server host` commands in the [Cisco IOS Network Management Command Reference](#).
- The “Configuring SNMP Support” section and the [list of notification-type values](#) in the [Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2](#).

If you are planning on implementing IPsec tunneling between your devices and the Prime Infrastructure server, be advised that you will not receive syslogs transmitted from those devices to the Prime Infrastructure server after implementing IPsec tunneling because IPsec does not support free-form syslogs. However, IPsec does support SNMP traps. To continue getting SNMP notifications of any kind from these devices, you need to configure your devices to send SNMP traps to the Prime Infrastructure server.

Configuring NTP

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the Prime Infrastructure server. This includes all Prime Infrastructure-related servers: Any remote FTP servers that you use for Prime Infrastructure backups, secondary Prime Infrastructure high-availability servers, the Prime Infrastructure Plug and Play Gateway, VMware vCenter and the ESX virtual machine, and so on.

You specify the default and secondary NTP servers during Prime Infrastructure server installation. You can also use Prime Infrastructure's **ntp server** command to add to or change the list of NTP servers after installation. For details, see the section [Connecting Via CLI](#) in this Guide and the section on the **ntp server** command in the [Command Reference Guide for Cisco Prime Infrastructure](#). Note that Prime Infrastructure cannot be configured as an NTP server; it acts as an NTP client only.

Failure to manage NTP synchronization across your network can result in anomalous results in Prime Infrastructure. Management of network time accuracy is an extensive subject that involves the organization's network architecture, and is outside the scope of this Guide. For more information on this topic, see (for example) the Cisco White Paper [Network Time Protocol: Best Practices](#).

Configuring Data Sources for Prime Infrastructure With Assurance

If you are licensing the Prime Infrastructure Assurance features, you must complete pre-installation tasks so that Assurance can monitor your network interfaces and services. See [Supported Assurance Data Sources](#) for information about these tasks.

Supported Assurance Data Sources

Prime Infrastructure with Assurance needs to collect data from your network devices using the exported data sources shown in [Table 2-1](#). For each source, the table shows the devices that support this form of export, and the minimum version of Cisco IOS or other software that must be running on the device to export the data.

Use [Table 2-1](#) to verify that your network devices and their software are compatible with the type of data sources Prime Infrastructure uses. If needed, upgrade your hardware or software. Note that each software version given is a *minimum*. Your devices can run any later version of the same software or Cisco IOS release train.

You may also need to make changes to ensure that Prime Infrastructure can collect data using SNMP, as explained in [Configuring SNMP](#).

Configuring Assurance Data Sources

Before installing Prime Infrastructure, you should enable the supported devices shown in [Table 2-1](#) to provide Prime Infrastructure with fault, application, and performance data, and ensure that time and date information are consistent across your network. The following topics provide guidelines on how to do this.

Table 2-1 Prime Infrastructure Assurance: Supported Data Sources, Devices and Software Versions

| Device Type | Cisco IOS Releases That Support NetFlow | Supported NetFlow Export Types | NetFlow Configuration |
|--------------------------|--|------------------------------------|---|
| Catalyst 3750-X / 3560-X | 15.0(1)SE IP base or IP services feature set and equipped with the network services module. | TCP and UDP traffic | See the “Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches” section in the Cisco Prime Infrastructure User Guide . |
| Catalyst 3850 | 15.0(1)EX | TCP and UDP traffic, Voice & Video | To configure TCP and UDP traffic, see the “Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches” section in the Cisco Prime Infrastructure User Guide . To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon |
| Catalyst 4500 | 15.0(1)XO and 15.0(2) | TCP and UDP traffic, Voice & Video | To configure TCP and UDP traffic, see the “Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches” section in the Cisco Prime Infrastructure User Guide . To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon |
| Catalyst 6500 | SG15.1(1)SY | TCP and UDP traffic, Voice & Video | To configure TCP and UDP traffic, see the “Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches” section in the Cisco Prime Infrastructure User Guide . To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon |

Table 2-1 Prime Infrastructure Assurance: Supported Data Sources, Devices and Software Versions (continued)

| Device Type | Cisco IOS Releases That Support NetFlow | Supported NetFlow Export Types | NetFlow Configuration |
|-------------|---|--|---|
| ISR | 15.1(3) T | TCP and UDP traffic, Voice & Video | To configure TCP and UDP traffic, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Collecting Traffic Statistics To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon |
| ISR G2 | 15.2(1) T and 15.1(4)M | TCP and UDP traffic, application response time, Voice & Video | To configure TCP, UDP, and ART, see the “Configuring NetFlow on ISR Devices” section in Cisco Prime Infrastructure User Guide . To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon |
| ISR G2 | 15.2(4) M2 or later, 15.3(1)T or later | TCP and UDP traffic, application response time, Voice and Video | To configure TCP, UDP, and ART, see the “Configuring Application Visibility” section in the Cisco Prime Infrastructure User Guide . |
| ASR | 15.3(1)S1 or later | TCP and UDP traffic, application response time, Voice & Video, HTTP URL visibility | |
| ISR G3 | 15.3(2)S or later | | |

Enabling Medianet NetFlow

To ensure that Cisco Prime Infrastructure can make use of Medianet data, your network devices must:

- Enable Medianet NetFlow data export for the basic set of statistics supported in Prime Infrastructure.
- Export the Medianet NetFlow data to the Prime Infrastructure server and port.

Use a configuration like the following example to ensure that Prime Infrastructure gets the Medianet data it needs:

```
flow record type performance-monitor PerfMonRecord
```

```
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
collect application media bytes counter
```

```

collect application media bytes rate
collect application media packets counter
collect application media packets rate
collect application media event
collect interface input
collect interface output
collect counter bytes
collect counter packets
collect routing forwarding-status
collect transport packets expected counter
collect transport packets lost counter
collect transport packets lost rate
collect transport round-trip-time
collect transport event packet-loss counter
collect transport rtp jitter mean
collect transport rtp jitter minimum
collect transport rtp jitter maximum
collect timestamp interval
collect ipv4 dscp
collect ipv4 ttl
collect ipv4 source mask
collect ipv4 destination mask
collect monitor event
flow monitor type performance-monitor PerfMon
  record PerfMonRecord
  exporter PerfMonExporter
flow exporter PerfMonExporter
  destination PrInIP
  source Loopback0
  transport udp PiInPort
policy-map type performance-monitor PerfMonPolicy
  class class-default
! Enter flow monitor configuration mode.
  flow monitor PerfMon
! Enter RTP monitor metric configuration mode.
  monitor metric rtp
! Specifies the minimum number of sequential packets required to identify a stream as being
an RTP flow.
  min-sequential 2
! Specifies the maximum number of dropouts allowed when sampling RTP video-monitoring
metrics.
  max-dropout 2
! Specifies the maximum number of reorders allowed when sampling RTP video-monitoring
metrics.
  max-reorder 4
! Enter IP-CBR monitor metric configuration mode

```

```

monitor metric ip-cbr
! Rate for monitoring the metrics (1 packet per sec)
rate layer3 packet 1
interface interfacename
  service-policy type performance-monitor input PerfMonPolicy
  service-policy type performance-monitor output PerfMonPolicy

```

In this example configuration:

- *PrInIP* is the IP address of the Prime Infrastructure server.
- *PiInPort* is the UDP port on which the Prime Infrastructure server is listening for Medianet data (the default is 9991).
- *interfacename* is the name of the interface (such as GigabitEthernet0/0 or fastethernet 0/1) sending Medianet NetFlow data to the specified *PrInIP*.

For more information on Medianet configuration, see the [Medianet Reference Guide](#).

Enabling NetFlow and Flexible NetFlow

To ensure that Prime Infrastructure can make use of NetFlow data, your network devices must:

- Have NetFlow enabled on the interfaces that you want to monitor.
- Export the NetFlow data to the Prime Infrastructure server and port.

As of version 2.1, Prime Infrastructure supports Flexible NetFlow versions 5 and 9. Note that you must enable NetFlow on each *physical* interface for which you want Prime Infrastructure to collect data. These will normally be Ethernet or WAN interfaces. This applies to physical interfaces only. You do not need to enable NetFlow on VLANs and Tunnels, as they are included automatically whenever you enable NetFlow on a physical interface.

Use the following commands to enable NetFlow on Cisco IOS devices:

```

Device(config)# interface interfaceName
Device(config)# ip route-cache flow

```

where *interfaceName* is the name of the interface (such as fastethernet or fastethernet0/1) on which you want to enable NetFlow.

Once NetFlow is enabled on your devices, you must configure exporters to export NetFlow data to Prime Infrastructure. You can configure an exporter using these commands:

```

Device(config)# ip flow-export version 5
Device(config)# ip flow-export destination PrInIP PiInPort
Device(config)# ip flow-export source interfaceName

```

where:

- *PrInIP* is the IP address of the Prime Infrastructure server.
- *PiInPort* is the UDP port on which the Prime Infrastructure server is listening for NetFlow data. (The default is 9991.)
- *interfaceName* is the name of the interface sending NetFlow data to the specified *PrInIP*. This will cause the source interface's IP address to be sent to Prime Infrastructure as part of NetFlow export datagrams.

If you configure multiple NetFlow exporters on the same router, make sure that only one of them exports to the Prime Infrastructure server. If you have more than one exporter on the same router exporting to the same destination, you risk data corruption.

Use the following commands to verify that NetFlow is working on a device:

```
Device# show ip flow export
Device# show ip cache flow
Device# show ip cache verbose flow
```

For more information on NetFlow configuration, see:

- [Cisco IOS Switching Services Configuration Guide, Release 12.1](#)
- [Flexible NetFlow Configuration Guide, Cisco IOS Release 15.1M&T](#)
- [Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x](#)
- [Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting](#)

Deploying Network Analysis Modules (NAMs)

Ensure that your NAMs are placed appropriately in the network. For more information, see:

- [Cisco Network Analysis Module Software 5.1 User Guide](#)—Includes deployment scenarios and covers a variety of topics, including deploying NAMs in the branch, and deploying NAMs for WAN optimization.
- [Cisco Network Analysis Module Deployment Guide](#)—See the section “Places in the Network Where NAMs Are Deployed”.

If your NAMs are deployed properly, then no other pre installation work is required. When you conduct discovery using Cisco Prime AM, you will need to enter HTTP access credentials for each of your NAMs.

Prime Infrastructure uses a more efficient REST interface to query NAMs. For this reason, it does not support the direct export of NetFlow data from NAMs. Any device exporting NetFlow data must export that NetFlow data directly to Prime Infrastructure, not via a NAM. Exporting NetFlow data from any NAM to Cisco Prime Infrastructure will result in data duplication.

Enabling Performance Agent

To ensure that Prime Infrastructure can collect application performance data, use the Cisco IOS *mace* (for Measurement, Aggregation and Correlation Engine) keyword to configure Performance Agent (PA) data flow sources on your branch-office and data center routers.

For example, use the following commands in Cisco IOS global configuration mode to configure a PA flow exporter on a router:

```
Router (config)# flow exporter mace-export
Router (config)# destination 172.30.104.128
Router (config)# transport udp 9991
```

Use commands like the following to configure flow records for applications with flows across the router:

```
Router (config)# flow record type mace mace-record
Router (config)# collect application name
```

```
Router (config)# collect art all
```

where *application name* is the name of the application whose flow data you want to collect.

To configure the PA flow monitor type:

```
Router (config)# flow monitor type mace mace-monitor
```

```
Router (config)# record mace-record
```

```
Router (config)# exporter mace-export
```

To collect traffic of interest, use commands like the following:

```
Router (config)# access-list 100 permit tcp any host 10.0.0.1 eq 80
```

```
Router (config)# class-map match-any mace-traffic
```

```
Router (config)# match access-group 100
```

To configure a PA policy map and forward the PA traffic to the correct monitor:

```
Router (config)# policy-map type mace mace_global
```

```
Router (config)# class mace-traffic
```

```
Router (config)# flow monitor mace-monitor
```

Finally, enable PA on the WAN interface:

```
Router (config)# interface Serial10/0/0
```

```
Router (config)# mace enable
```

For more information on configuring Performance Agent, see the [Cisco Performance Agent Deployment Guide](#).

Installing Prime Infrastructure Patches

You may need to install patches to get your version of Prime Infrastructure to the level at which upgrade is supported. You can check the Prime Infrastructure version and patch version you are running by using the CLI commands **show version** and **show application**.

Different patch files are provided for each version of Prime Infrastructure and its predecessor products. Download and install only the patch files that match the version of your existing system and that are required before you upgrade to a later version. You can find the appropriate patches by pointing your browser to the [Cisco Download Software navigator](#).

Before installing a patch, you will need to copy the patch file to your Prime Infrastructure server's default repository. Many users find it easy to do this by first downloading the patch file to a local FTP server, then copying it to the repository. You can also copy the patch file to the default repository using any of the following methods:

- cdrom—Local CD-ROM drive (read only)
- disk—Local hard disk storage
- ftp—URL using an FTP server
- http—URL using an HTTP server (read only)
- https—URL using an HTTPS server (read only)
- nfs—URL using an NFS server
- sftp—URL using an SFTP server
- tftp—URL using a TFTP server

-
- Step 1** Download the appropriate point patch to a local resource in your environment:
- With the [Cisco Download Software navigator](#) displayed in your browser, choose **Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Cisco Prime Infrastructure**.
 - Select the version of Cisco Prime Infrastructure that most closely matches the one you are currently using (for example, **Cisco Prime Infrastructure 3.0**).
 - Click **Prime Infrastructure Patches** to see the list of available patches for that version of the product.
 - Next to each patch that is required, click **Download**, then follow the prompts to download the file.
- Step 2** Open a command-line interface session with the Prime Infrastructure server (see [Connecting Via CLI](#) in the *Cisco Prime Infrastructure Administrator Guide*).
- Step 3** Copy the downloaded patch file to the default local repository. For example:

```
admin# copy source path/defaultRepo
```

Where:

- **source** is the downloaded patch file's location and name (for example: ftp://MyFTPServer/pi_9.3.1.0_update.tar.gz).
- **path** is the complete path to the default local backup repository, defaultRepo (for example: /localdisk)

- Step 4** Install the patch:

```
admin# patch install patchFile Repositoryname
```

Where:

- **patchFile** is the name of the patch file you copied to /localdisk/defaultRepo
- **Repositoryname** is the name of the repository.

For example: admin# patch install test.tar.gz defaultRepo



Prime Infrastructure Server Settings

The following topics describe how to configure key Prime Infrastructure server settings.

Related Topics

- [Available System Settings](#)
- [Configuring Email Settings](#)
- [Configuring Global SNMP Settings](#)
- [Configuring Proxy Settings](#)
- [Configuring Server Port and Global Timeout Settings](#)
- [Enabling Compliance Services](#)
- [Configuring Remote FTP, TFTP, and SFTP Servers](#)
- [Accessing ACS View Servers From Prime Infrastructure](#)
- [Configuring ISE Servers](#)
- [Specifying Administrator Approval for Jobs](#)
- [Approving Jobs](#)
- [Specifying Login Disclaimer Text](#)
- [Adding Device Information to a User Defined Field](#)
- [Managing OUIs](#)
- [Adding Notification Receivers to Prime Infrastructure](#)
- [Setting Up HTTPS Access to Prime Infrastructure](#)
- [MIB to Prime Infrastructure Alert/Event Mapping](#)
- [Product Feedback Data Collection](#)

Available System Settings

The **Administration > Settings > System Settings** menu contains options to configure or modify Cisco 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.

The following table lists the types of settings you can configure or modify from the **Administration > Settings > System Settings** menu.

Table 3-1 Available Prime Infrastructure System Settings Options

| To do this: | Choose Administration > Settings > System Settings >... | Applicable to: |
|---|--|--------------------------------|
| Modify the stored cisco.com credentials (user name and password) used to log on to cisco.com and: <ul style="list-style-type: none"> • Check for Cisco software image updates • Open or review Cisco support cases • Check for Prime Infrastructure software updates, including critical fixes, device support, and Prime add-ons You can also access this page from a link on the Administration > Settings > System Settings > Software Update page. | General > Account Credentials | Prime Infrastructure appliance |
| Set the retention period for the following data types: Trends, Device Health, Performance, Network Audit, System Health. | General > Data Retention See Specifying Data Retention by Category . | 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 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. | General > Guest Account See Configuring Guest Account Settings . | Wireless devices only |
| To help Cisco improve its products, Prime Infrastructure collects the product feedback data and sends it to Cisco. | General > Help Us Improve See Product Feedback Data Collection | Wired and wireless devices |
| Enable job approval to specify the jobs which require administrator approval before the job can run. | General > Job Approval See Specifying Administrator Approval for Jobs . | Wired and wireless devices |
| Change the disclaimer text displayed on the login page for all users. | General > Login Disclaimer See Specifying Login Disclaimer Text . | Prime Infrastructure appliance |
| Configure proxies for the Prime Infrastructure server and its local authentication server. | General > Proxy See Configuring Proxy Settings . | Not Applicable |

Table 3-1 Available Prime Infrastructure System Settings Options (continued)

| To do this: | Choose Administration > Settings > System Settings >... | Applicable to: |
|---|--|--------------------------------|
| Set the path where scheduled reports are stored and how long reports are retained. | General > Report See Controlling Report Storage and Retention . | Wired and wireless devices |
| <ul style="list-style-type: none"> • Enable or disable FTP, TFTP, and HTTP/HTTPS server proxies, and specify the ports they communicate over. • See the NTP server name and local time zone currently configured for Prime Infrastructure | General > Server See Configuring Server Port and Global Timeout Settings . | Prime Infrastructure appliance |
| 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. | General > Server Tuning See Tuning the Server . | Wired and wireless devices |
| <ul style="list-style-type: none"> • Specify that you do not want credentials stored on cisco.com when Prime Infrastructure checks cisco.com for Cisco software image updates • Select the kinds of Prime Infrastructuresoftware updates for which you want to receive notifications (includes Critical Fixes, new Device Support, and Prime Add-On products) | General > Software Update | Wired and wireless devices |
| Configure the settings for creating a technical support request. | General > Support Request See Configuring Technical Support Request Settings . | Wired and wireless devices |
| Enable Change Audit JMS Notification by selecting the Enable Change Audit JMS Notification check box. | Mail and Notification > Change Audit Notification See Enabling Change Audit Notifications . | Wired and wireless devices |
| Enable email distribution of reports and alarm notifications. | Mail and Notification > Mail Server Configuration See Configuring Email Settings . | Prime Infrastructure appliance |
| <ul style="list-style-type: none"> • Set the protocol to be used for controller and autonomous AP CLI sessions. • Enable autonomous AP migration analysis on discovery. | Network and Device > CLI Session See Configuring Protocols for CLI Sessions . | Wireless devices only |
| Enable auto refresh after a wireless controller upgrade, and process the save configuration trap. | Network and Device > Controller Upgrade See Refreshing Controllers After an Upgrade . | Wireless devices only |
| Modify the settings for Plug and Play. | Network and Device > Plug & Play | Wired devices only |

Table 3-1 Available Prime Infrastructure System Settings Options (continued)

| To do this: | Choose Administration > Settings > System Settings >... | Applicable to: |
|---|---|--------------------------------|
| <p>Set global SNMP polling parameters, including trace display values, reachability parameters and the backoff algorithm.</p> <p>If you select Exponential 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>Network and Device > SNMP</p> <p>See Configuring Global SNMP Settings.</p> | Wireless devices only |
| 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>Network and Device > Switch Port Trace (SPT) > Auto SPT</p> <p>See Configuring SNMP Credentials for Rogue AP Tracing.</p> | Wireless devices only |
| Set the SNMP credentials and trace parameters to be used in tracing rogue AP switch ports. | <p>Network and Device > Switch Port Trace (SPT) > Manual SPT</p> <p>See Configuring SNMP Credentials for Rogue AP Tracing.</p> | Wireless devices only |
| Set basic and advanced switch port trace parameters. | <p>Network and Device > Switch Port Trace (SPT) > SPT Configuration</p> <p>See Configuring Switch Port Tracing.</p> | Wired devices only |
| 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. | <p>Network and Device > Switch Port Trace (SPT) > Known Ethernet MAC Address</p> | Prime Infrastructure appliance |
| Set basic control parameters used when deploying a device configuration, such as enabling backup of the running configuration, rollbacks, retrieval of show command output from the cache, and the number of CLI thread pools to use. | <p>Inventory > Configuration</p> <p>See Archiving Device Configurations Before Template Deployment.</p> | 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. | <p>Inventory > Configuration Archive</p> <p>See Specifying When and How to Archive WLC Configurations.</p> | Wired and wireless devices |
| Configure Data Center settings. | <p>Inventory > Data Center Settings</p> | Prime Infrastructure appliance |
| Specify IPv4 or IPv6 address preferences | <p>Inventory > Discovery</p> | Wired and wireless devices |
| Determine whether you want to display groups that do not have members or children associated with them. | <p>Inventory > Grouping</p> | Wired and wireless devices |

Table 3-1 Available Prime Infrastructure System Settings Options (continued)

| To do this: | Choose Administration > Settings > System Settings >... | Applicable to: |
|--|---|--------------------------------|
| Configure global preference parameters for downloading, distributing, and recommending software Images. | Inventory > Image Management See the Cisco Prime Infrastructure 3.0 User Guide for information about Image Management. | Wired and wireless devices |
| Enable inventory collection to allow Prime Infrastructure to collect inventory when it receives a syslog event for a device. | Inventory > Inventory See Specifying Inventory Collection After Receiving Events . | Wired and wireless devices |
| Store additional information about a device. | Inventory > User Defined Fields See Adding Device Information to a User Defined Field . | Wired devices only |
| <ul style="list-style-type: none"> • Change which alarms, events, and syslogs are deleted, and how often. • Set the alarm types for which email notifications are sent, and how often they are sent. • Set the alarm types displayed in the Alarm Summary view. • Change the content of alarm notifications sent by email. | Alarms and Events > Alarms and Events See Specifying Alarm Clean Up and Display Options . | Wired and wireless devices |
| Configure remote event and alarm receivers who will receive notifications from Prime Infrastructure. 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. | Alarms and Events > Notification receivers See Adding Notification Receivers to Prime Infrastructure . | Wired and wireless devices |
| Set the severity level of any generated alarm. | Alarms and Events > Alarm Severity and Auto Clear See Changing Alarm Severities . | Wired and wireless devices |
| Configure SNMP traps and events generated for the Prime Infrastructure hardware appliance. | Alarms and Events > System Event Configuration See Internal SNMP Trap Generation | Prime Infrastructure appliance |

Table 3-1 Available Prime Infrastructure System Settings Options (continued)

| To do this: | Choose Administration > Settings > System Settings >... | Applicable to: |
|---|---|----------------------------|
| <ul style="list-style-type: none"> • Enable automatic troubleshooting of clients on the diagnostic channel. • Enable lookup of client hostnames from DNS servers and set how long to cache them. • Set how long to retain disassociated clients and their session data. • Poll clients to identify their sessions only when a trap or syslog is received. • Disable saving of client association and disassociation traps and syslogs as events. • Enable saving of client authentication failure traps as events, and how long between failure traps to save them. | Client and User > Client See Configuring Email Settings . | Wired and wireless devices |
| Add a vendor Organizationally Unique Identifier (OUI) mapping XML file. | Client and User > User Defined OUI See Adding a New Vendor OUI Mapping . | Wired and wireless devices |
| Upload an updated vendor OUI mapping XML file. | Client and User > Upload OUI See Uploading an Updated Vendor OUI Mapping File . | Wired and wireless devices |
| Configure the Cisco WAAS Central Manager IP address in Cisco Prime Infrastructure. | Services > Service Container Management See Cisco WAAS Central Manager Integration . | Wired devices only |

Configuring Email Settings

Administrators must configure email parameters to enable Prime Infrastructure to email reports, alarm notifications, and so on. You must configure the primary SMTP server before you can set the email parameters.

-
- Step 1** Choose **Administration > Settings > System Settings > Mail and Notification > Mail Server Configuration**. The Mail Server Configuration page appears.
- Step 2** Enter the hostname or IP address of the primary SMTP server. Enter the IP address of the physical server. You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.
- Step 3** Enter the username of the SMTP server.
- Step 4** Provide a password for logging on to the SMTP server and confirm it.
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 this to a different sender.
- Step 7** In the “To” text box, enter the email address of the recipient. The email address you provide serves as the default value for other functional areas, such as alarms or reports. If you want to specify multiple recipients, enter multiple email addresses separated by commas.
- Global changes you make to the recipient email addresses in this step 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** In the “Subject” text box, enter the text that you want to appear in the email subject line.
- Step 9** (Optional) Click the Configure email notification for individual alarm categories link. This allows you to specify the alarm categories and severity levels for which you want to enable email notifications. Emails are sent when an alarm occurs that matches the categories and the severity levels you select.
- 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 for 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.

The default network address is 0.0.0.0, which indicates the entire network. SNMP credentials are 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. You should update the pre-populated SNMP credential with your own SNMP information.

- Step 1** Choose **Administration > Settings > System Settings > Network and Device > SNMP**.
- Step 2** (Optional) Select the **Trace Display Values** check box to display mediation trace-level logging data values fetched from the controller using SNMP. If unselected, these values do not appear.
- Step 3** From the Backoff Algorithm list, choose **Exponential** or **Constant Timeout**. If you choose Exponential, 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.
- 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 4** 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.

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

- Step 5** In Reachability Retries, enter the number of global retries used for determining device reachability. This field is only available if the **Use Reachability Parameters** check box is selected.

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



Note

You cannot edit the value of Reachability Timeout. The default value is 2 seconds.

- Step 6** In 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.

This Maximum VarBinds per PDU field enables you to make necessary changes with when you have any failures associated to SNMP.

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. The configured value is retained even if you upgrade Prime Infrastructure to a newer version.

- Step 7** Click **Save** to confirm these settings.

Related Topics

- [Viewing SNMP Credential Details](#)
- [Adding SNMP Credentials](#)
- [Importing SNMP Credentials](#)

Viewing SNMP Credential Details

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

- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.

- Step 2** Click the Network Address link to display the SNMP Credential Details page. The page displays the following information:

General Parameters

- Add Format Type—Display only. For details, see “Adding SNMP Credentials” in Related Topics.
- Network Address
- Network Mask

SNMP Parameters—Choose the applicable versions for SNMP parameters. The SNMP credentials are validated according to which SNMP versions are selected.

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.

- 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

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 3 Click **OK** to save your changes.

Related Topics

- [Configuring Global SNMP Settings](#)
- [Adding SNMP Credentials](#)
- [Importing SNMP Credentials](#)

Adding SNMP Credentials

Prime Infrastructure needs device SNMP credentials to poll your network devices, back up and change their configurations, and so on. You can add SNMP credentials by hand. You can also import them in bulk (see “Importing SNMP Credentials” in Related Topics).

- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.
- Step 2** Choose **Select a command > Add SNMP Entries > Go**.
- Step 3** In the **Add Format Type** drop-down list, choose **SNMP Credential Info**.
- Step 4** Enter the IP address of the switch you want to add. If you want to add multiple switches, use a comma between each IP address.
- Step 5** In the Retries field, enter the number of times that attempts are made to discover the switch.
- Step 6** 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 7** 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

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 8 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 Network Devices page accessible via **Configuration > Network > Network Devices**. If you manually add switches through the Network Devices page, 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 using the Network Devices pages.

Related Topics

- [Configuring Global SNMP Settings](#)
- [Viewing SNMP Credential Details](#)
- [Importing SNMP Credentials](#)

Importing SNMP Credentials

Prime Infrastructure needs device SNMP credentials to poll your network devices, back up and change their configurations, and so on. You can import SNMP credentials in bulk by importing them from a CSV file. You can also add them by hand (see “Adding SNMP Credentials” in Related Topics).

Before You Begin

Make sure you have created a CSV file with the proper format, and that it is available for upload from a folder on the client machine you use to access Prime Infrastructure. Here is a sample SNMP credentials CSV file suitable for import:

```
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 first row of the file is mandatory, as it describes the column arrangement. The IP Address column is also mandatory. 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 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.
- Step 2** Choose **Select a command > Add SNMP Entries > Go**.
- Step 3** In the **Add Format Type** drop-down list, choose **File**.
- Step 4** Click **Browse** to navigate to the CSV file you want to import and select it.
- Step 5** Click **OK** to import the file.

If Prime Infrastructure can use the SNMP credential listed to access the switch, the switch is added for later use and appears in the Network Devices page accessible via **Configuration > Network > Network Devices**. If you manually add switches through the Network Devices page, 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 using the Network Devices pages.

Related Topics

- [Configuring Global SNMP Settings](#)
- [Viewing SNMP Credential Details](#)
- [Adding SNMP Credentials](#)

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 > Settings > System Settings > General > Proxy**.
- Step 2** Select the **Enable Proxy** check box to specify the proxy server IP or host name and port number.
- Step 3** Select the **Authentication Proxy** check box to specify the authentication server user name and password.
- Step 4** Enter the required information and click **Save**.
-

Configuring Server Port and Global Timeout Settings

The Server page allows you to enable or disable Prime Infrastructure's FTP, TFTP, and HTTP/HTTPS services.

FTP and TFTP services are normally enabled by default. HTTP and HTTPS services are disabled by default. You should enable the HTTP/HTTPS services if you use the Plug and Play feature and your devices are configured to use HTTP to acquire the initial configuration in the bootstrap configuration.

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

Step 2 To modify the FTP and TFTP ports 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, then click **Enable** or **Disable**.

The **Global Idle Timeout** is enabled by default and is set to 15 minutes. The Global Idle Timeout setting overrides the **User Idle Timeout** setting in the **My Preferences** page. Only users with administrative privileges can disable the Global Idle Timeout value or change its time limit.

Step 3 Click **Save**.

Related Topics

- [Virtual Appliance Options](#)
- [Physical Appliance Options](#)
- [Understanding System Requirements](#)
- [Cisco Prime Infrastructure Quick Start Guide](#)

Enabling Compliance Services

Compliance Services allow Prime Infrastructure users to run Cisco PSIRT security and EOX obsolete-device compliance reports. This feature also lets users establish baseline device configuration standards, and then audit field configurations against these standards, identifying devices that are non-compliant and how their configuration differ from standards.

Compliance Services are disabled by default. In order to use them, the Prime Infrastructure administrator must enable the feature. You must also re-synchronize the server's device inventory. All users must also log out and then log in in order to see the **Configuration > Compliance** menu option.

Compliance Services are available only on the following Prime Infrastructure server options:

- The Professional virtual appliance. For details, see “Virtual Appliance Options” and “Understanding System Requirements” in Related Topics.
- The Cisco Unified Computing System (UCS) Gen 2 physical appliance. For details, see “Virtual Appliance Options” and “Understanding System Requirements” in Related Topics.

Do not attempt to enable Compliance Services on Express, Express-Plus, or Standard virtual appliances. If you do, the feature itself will not work. In addition, if you enable it and then try to migrate your data to a newly installed Professional or Gen 2 UCS appliance, the settings in the migrated data from the source Express, Express-Plus or Standard server will prevent Compliance Services from working on the target appliance. You can avoid all this by simply leaving the Compliance Services feature disabled on the Express, Express-Plus or Standard virtual appliance, and then migrating your data to the Professional or Gen2 UCS appliance.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Server**.
- Step 2** Next to **Compliance Services**, click **Enable**.
- Step 3** Click **Save**.
- Step 4** Re-synchronize Prime Infrastructure's device inventory: Choose **Inventory > Network Devices**, select **All Devices**, then click the **Sync** icon.
- Step 5** Ask any users who are currently logged in to Prime Infrastructure to log out. They will be able to see the new **Configuration > Compliance** menu option when they log in again.
-

Related Topics

- [Virtual Appliance Options](#)
- [Physical Appliance Options](#)
- [Understanding System Requirements](#)

Configuring Remote FTP, TFTP, and SFTP Servers

Prime Infrastructure uses an integral TFTP/FTP server. This means that third-party TFTP or FTP servers cannot run on the same workstation as Prime Infrastructure, because Prime Infrastructure and the third-party servers use the same communication port.

-
- Step 1** Choose **Administration > Servers > FTP/TFTP/SFTP servers**.
 - Step 2** Choose **Select a command > Add TFTP/FTP/SFTP Server > Go**.
 - Step 3** From the Server Type drop-down list, choose **TFTP, FTP, SFTP**, or **All**.
 - Step 4** Enter a user-defined name for the server.
 - Step 5** Enter the IP address of the server.
 - Step 6** Click **Save**.
-

Accessing ACS View Servers From Prime Infrastructure

Starting with version 3.0, Prime Infrastructure no longer supports access to Cisco Secure Access Control System (ACS) View servers.

Configuring ISE Servers

-
- Step 1** Choose **Administration > Servers > ISE Servers**.
 - Step 2** Choose **Select a command > Add ISE Server**, then click **Go**.
 - Step 3** Enter the ISE server's IP address, user name, and password.
 - Step 4** Confirm the ISE server password.
 - Step 5** Click **Save**.
-

Specifying Administrator Approval for Jobs

You may want certain types of jobs to run only after an administrator approves them. This will include jobs that have a significant impacts on the network (for example, configuration-overwrite jobs). 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.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Job Approval**.
- 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*.*
- Some pre-listed job types are: Discovery, Config, Configuration Archive, Configuration Overwrite, Configuration Rollback, Import, PollerJob, and SWIM Collection. You can add other job types by typing them in the text box provided.
- 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”) before the job can run, the administrator must approve the job.

Choose **Administration > Dashboards > Job Dashboard** 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.

Related Topics

- [Specifying Administrator Approval for Jobs](#)

Specifying Login Disclaimer Text

The Login Disclaimer page allows you to enter disclaimer text displayed on the Prime Infrastructure Login page for all users.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Login Disclaimer**.
- Step 2** 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 additional information about devices, such as device location attributes (for example: area, facility, floor, and so on). UDF attributes are used whenever a new device is added, imported or exported.

-
- Step 1** Choose **Administration > Settings > System Settings > Inventory > 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 OUIs

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.

Related Topics

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

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.

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

Prime Infrastructure allows you to get OUI updates online from the IEEE Registration Authority database (see the link to the RA database in Related Topics). If Prime Infrastructure is unable to reach the IEEE database, a message appears instructing you to save and upload the file to your Prime Infrastructure server.

-
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Upload OUI**. The Upload OUI From File page appears.
 - Step 2** Click **Update online from IEEE** to get OUI updates from the IEEE Registration Authority database (see the link to the RA database in Related Topics). If Prime Infrastructure is unable to reach the IEEE database, a message appears instruction you to save and upload the file.
 - Step 3** Click **OK** after the update completes successfully.

After you upload the vendorMacs.xml file in the **Administration > Settings > System Settings > Upload OUI** page; If the vendor name is not reflected for existing unknown vendor clients in the Unique Clients and Users Summary report, run the `updateUnknownClient.sh` script. This script is located in the `/opt/CSCOlumos/bin` folder.

Related Topics

- [IEEE Registration Authority database](#)

Adding Notification Receivers to Prime Infrastructure

The Notification Receiver page displays current notification receivers that support Northbound access and guest access. Alerts and events are sent as SNMPv2 and SNMPv3 notifications to configured notification receivers. You can view current or add additional notification receivers.

-
- Step 1** Choose **Administration > Settings > System Settings > Alarms and Events > Notification Receivers**. All currently configured servers appear in this page.
- Step 2** Choose **Select a command > Add Notification Receiver**, then click **Go**.
- Step 3** Enter the server IP address and server name.
- Step 4** Click either the **North Bound** or **Guest Access** radio button.
If you select North Bound, the Notification Type automatically defaults to UDP.
- Step 5** Enter the **Port Number** and select **SNMP Version**. The receiver that you configure should be listening to UDP on the same port that is configured.

The SNMP Version options are SNMPV2c and SNMPV3. For SNMPV2c community string is required, whereas if SNMPV3 is selected the Username and Password fields are mandatory, the **Engine ID** specific to Prime Infrastructure will be auto-populated, and select the mode from the **Mode** drop-down list depending on the security level.

The Username and password field supports 32 characters.
- Step 6** If you selected North Bound as the receiver type, specify the criteria and severity for which you want Prime Infrastructure to send notifications. For example, if you select the category **Routers** and the severity **Informational**, Prime Infrastructure forwards informational events that occur on routers to the receiver you specified in Step 4.
- Step 7** Click **Save** to confirm the Notification Receiver information.
-

Removing Notification Receivers

-
- Step 1** Choose **Administration > Settings > System Settings > Alarms and Events > Notification Receivers**. All currently configured servers appear on this page.
- Step 2** Select the check boxes of the notification receivers that you want to delete.
- Step 3** Choose **Select a command > Remove Notification Receiver**, then click **Go**.
- Step 4** 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 Prime Infrastructure

Prime Infrastructure supports secure HTTPS client access. HTTPS access requires that you apply certificate files to the Prime Infrastructure server and that users update their client browsers to trust these certificates.

To accomplish this, you can use certificate files that are either:

- Self-signed. You can generate and apply self-signed certificates as explained in the related topic “Generating and Applying Self-Signed Certificates”.
- Digitally signed by a Certificate Authority (CA). CAs are organizations (like Cisco and VeriSign) that validate identities and issue certificates, often for a fee. Certificates issued by a CA bind a public key to the name of the entity (such as a server or device) identified in the certificate. You can obtain CA certificates from a third-party CA and apply them to the Prime Infrastructure server as explained in “Obtaining and Importing CA-Signed Certificates”.

Related Topics

- [Generating and Applying Self-Signed Certificates](#)
- [Obtaining and Importing CA-Signed Certificates](#)
- [Deleting CA-Signed Certificates](#)

Generating and Applying Self-Signed Certificates

Use Prime Infrastructure to generate and apply self-signed certificates.

Step 1 Start a CLI session with Prime Infrastructure (see “Connecting Via CLI”). Do not enter “configure terminal” mode.

Step 2 Enter the following command to generate a new RSA key and self-signed certificate with domain information:

```
PIServer/admin# ncs key genkey -newdn
```

You will be prompted for the Distinguished Name (DN) 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 Prime Infrastructure (see “Restarting Prime Infrastructure”).

To avoid login complaints, instruct users to add the self-signed certificate to their browsers’ trust stores when they next access the Prime Infrastructure login page.

Related Topics

- [Connecting Via CLI](#)
- [Restarting Prime Infrastructure](#)

Obtaining and Importing CA-Signed Certificates

Use Prime Infrastructure to generate a Certificate Signing Request (CSR) file and send it to a Certificate Authority (CA) for validation. The method you use to send the CSR file to the CA will vary with the CA.

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 CA-signed certificates will result in mismatches between keys in the file and the server.

Note that SSL certificates are host-specific. They are preserved in Prime Infrastructure backups, but are restored only if the backup and restore servers have the same host name.



Note

High Availability Virtual IP is designed to simplify the server management. SSL certificate configuration does not work with the Prime Infrastructure HA Virtual IP deployment.

Step 1 Start a CLI session with Prime Infrastructure (see “Connecting Via CLI”). Do not enter “configure terminal” mode.

Step 2 Enter the following command to generate a CSR file in the default backup repository:

```
PIServer/admin# ncs key genkey -newdn -csr CSRFile.csr repository defaultRepo
```

where *CSRFile* is an arbitrary name of your choice (for example: *MyCertificate.csr*).

Step 3 Copy the CSR file to a location you can access. For example:

```
PIServer/admin# copy disk:/defaultRepo/CSRFile.csr ftp://your.ftp.server
```

Step 4 Send the CSR file to a Certificate Authority (CA) of your choice.

The CA will respond by sending you an SSL server certificate and one or more CA certificate files. All these files will have the filename extension CER. The CA response will indicate which of the files is:

- The SSL server certificate. This is typically given a filename that reflects the host name of the server to which you will apply it.
- The CA certificates, which are typically given filenames that reflect the name of the CA.

Step 5 Before continuing:

- a. Create a single certificate file by concatenating (using the **cat** command) all the CA certificate files into the SSL server certificate file. The resulting concatenated single certificate file *must* have the SSL server certificate content appear first. The CA certificate file contents can appear in the concatenated file in any order.
- b. Remove any blank lines in the concatenated single certificate file using a text editor, **awk**, **sed**, or other OS-native facilities.

Step 6 At the Prime Infrastructure command line, copy the single certificate file to the backup repository. For example:

```
PIServer/admin# copy ftp://your.ftp.server/CertFile.cer disk:defaultRepo
```

where **CertFile.cer** is the single certificate file you created in the previous step.

Step 7 Enter the following command to import the single certificate file into the Prime Infrastructure server:

```
PIServer/admin# ncs key importsigncert CertFile.cer repository defaultRepo
```

Step 8 To activate the CA-signed certificates, restart Prime Infrastructure (see “Restarting Prime Infrastructure”).

If the CA who signed the certificate is not already a trusted CA in your organization: Instruct users to add the CA-signed certificate to their browsers’ trust stores when they next access the Prime Infrastructure login page.

Related Topics

- [Connecting Via CLI](#)
- [Restarting Prime Infrastructure](#)

Deleting CA-Signed Certificates

You can delete CA-signed certificates using the Prime Infrastructure CLI.

Step 1 Start a CLI session with Prime Infrastructure (see “Connecting Via CLI”). Do not enter “configure terminal” mode.

Step 2 List the short names of all the CA-signed certificates on the Prime Infrastructure server:

```
PIServer/admin# ncs key listcacert
```

Step 3 Enter the following command to delete the CA certificate you want:

```
PIServer/admin# ncs key deletcacert shortname
```

where *shortname* is the short name of the CA certificate you want to delete, taken from the listing given in the output of **ncs key listcacert**.

Related Topics

- [Connecting Via CLI](#)

MIB to Prime Infrastructure Alert/Event Mapping

The following table summarizes how the CISCO_WIRELESS_NOTIFICATION_MIB fields and OIDs map to Prime Infrastructure alerts and events.

Table 3-2 CISCO_WIRELESS_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 eventTime - NmsEvent | Creation time for alarm/event. |
| cWNotificationUpdatedTimestamp | DateAndTime | modTime - NmsAlert | Modification time for Alarm. Events do not have modification time. |
| cWNotificationKey | SnmpAdminString | objectId - NmsEvent entityString- NmsAlert | Unique alarm/event ID in string form. |
| cWNotificationCategory | CWirelessNotificationCategory | NA | Category of the Events/Alarms. Possible values are: unknown accessPoints adhocRogue clients controllers coverageHole interference contextAwareNotifications meshLinks mobilityService performance rogueAP rrm security wcs switch ncs |
| cWNotificationSubCategory | OCTET STRING | Type field in alert and eventType in event. | This object represents the subcategory of the alert. |
| cWNotificationServerAddress | InetAddress | N/A | Prime Infrastructure IP address. |

Table 3-2 CISCO_WIRELESS_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. Possible values: 0—unknown 1—IPv4 2—IPv6 3—IPv4z 4—IPv6z 16—DNS 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 Message - NmsAlert | Alarm description string. |
| cWNotificationSeverity | INTEGER | severity - NmsEvent, NmsAlert | Severity of the alert/event: cleared(1) critical(3) major(4) minor(5) warning(6) info(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 is empty for the current release. |

Product Feedback Data Collection

In order to help Cisco improve its products, Prime Infrastructure collects the following data and sends it to Cisco:

- Product information—product type, software version, and installed licenses.
- System information—server operating system and available memory.
- Network information—number and type of devices on your network.

The data is collected on a daily, weekly and monthly basis. It is posted to a REST URL in the Cisco cloud using HTTPS. To view the types of data Cisco collects, choose **Administration > Settings > System Settings > General > Help Us Improve**, and then click **What data is Cisco collecting?**

Product feedback data collection is enabled by default. If you do not want Cisco to collect and transmit this feedback data, choose **Administration > Settings > System Settings > General > Help Us Improve**, select the option **Not at this time, thank you**, and click **Save**.

If you upgraded from a previous version of Prime Infrastructure, the product feedback data collection option you specified in the earlier version is retained after the upgrade for the upgraded server and the restored server. If you had not selected any option for product feedback data collection in the previous version, it will be enabled by default in the upgraded version and the backup and restore server.

If you have configured high availability the data will be collected and sent either from the primary or secondary HA server instance (it is not sent from both the servers).



Maintaining Prime Infrastructure Server Health

The following topics explain tasks you perform in order to maintain the health and performance of Cisco Prime Infrastructure servers.

Related Topics

- [Monitoring Prime Infrastructure Health](#)
- [Troubleshooting Prime Infrastructure](#)
- [Evaluating OVA Size and System Resources](#)
- [Improving Prime Infrastructure Performance](#)
- [Optimizing Memory for Assurance Processing](#)
- [Managing Data Sources](#)
- [Performing Special Administrative Tasks](#)
- [Keeping Prime Infrastructure Software Updated](#)
- [Configuring Support Request Settings](#)
- [Managing Disk Space Issues](#)

Monitoring Prime Infrastructure Health

To view the system health dashboards, choose **Administration > Dashboards > Admin Dashboard**. The following table describes the information displayed on the dashboards.

Table 4-1 Administration > Dashboards > Admin Dashboard Information

| To view this information... | Choose 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 |
| How quickly the Prime Infrastructure server is responding to user service requests for information, such 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

Cisco Prime Infrastructure provides helpful tools for network operators to connect to Cisco experts to diagnose and resolve problems. You can open support cases and track your cases from Prime Infrastructure. If you need help troubleshooting any problems, Prime Infrastructure allows you to:

- Connect with the Cisco Support Community to view and participate in discussion forums (see “Launching the Cisco Support Community”).
- Open a support case with Cisco Technical Support (see “Opening a Support Case”).

Related Topics

- [Launching the Cisco Support Community](#)
- [Opening a Support Case](#)

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.

You must enter your Cisco.com username and password to access and participate in the forums.

To launch the Cisco Support Community:

-
- Step 1** Display the Device 360° View page for the device on which you need support (see “Getting Device Details from the Device 360° View” in Related Topics).
 - Step 2** On the Device 360° View page, choose **Actions > Support Community**.
 - Step 3** If asked to log in, enter your Cisco.com username and password. The Cisco Support Community page displays a list of posts and discussions related to the device for which you need support.
 - Step 4** Using the Cisco Support Community page:
 - Enter additional keyword parameters or select a time-period to filter the discussions that are displayed.
 - Select the **Join the Discussion** link next to any of the related forum discussions to see details of the discussion or ask your own questions.
 - Select **Post a New Question** to post a new question in any of the Cisco Support Community forums
-

Related Topics

- [Getting Device Details from the Device 360° View](#)

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 that it takes to create a support case.

To open a support case or access the Cisco Support Community, you must:

- Have a direct connection to the internet from the Prime Infrastructure server.
- Enter your Cisco.com username and password.

-
- Step 1** Display the Device 360° View page for the device on which you need support (see “Getting Device Details from the Device 360° View” in Related Topics).
 - Step 2** Using the Device 360° View page, choose **Actions > Support Request**.
 - Step 3** If asked to log in, enter your Cisco.com username and password.
 - Step 4** To check on or update an existing case, enter the case number and click **Update Case**. Otherwise, click **Create** to open a new support case.

Prime Infrastructure gathers information about the device and populates the fields for which it can retrieve information. You can enter a Tracking Number that corresponds to your own organization’s trouble ticket system.

- Step 5** Click **Next** and enter a description of the problem.

By default, Prime Infrastructure enters information that it can retrieve from the device. Prime Infrastructure automatically generates the necessary supporting documents such as the technical information for the device, configuration changes, and all device events over the last 24 hours. You can also upload files from your local machine and make them attachments to the support case.

Step 6 Click **Create Service Request**.

Related Topics

- [Getting Device Details from the Device 360° View](#)

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 Quick Start Guide* (see Related Topics).

Note that the limits on devices, interfaces, and flow records 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”.

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”.
- 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 provided by VMware to expand the physical disk space (see “VMware vSphere Documentation” in Related Topics). 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 by Category”.
- 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 Retention”, “Specifying Data Retention by Category”, and “Specifying Data Retention By Database Table.”
- 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”.

- 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 physical or virtual appliance. Back up your existing system, then restore it to a virtual machine on the higher-rated server. For details, see “Migrating to Another OVA Using Backup and Restore”.

Related Topics

- [System Requirements](#)
- [Cisco Prime Infrastructure Quick Start Guide](#)
- [Monitoring Prime Infrastructure Health](#)
- [Compacting the Prime Infrastructure Database](#)
- [VMware vSphere Documentation](#)
- [Specifying Data Retention by Category](#)
- [Specifying Data Retention By Database Table](#)
- [Controlling Report Storage and Retention](#)
- [Using Remote Backup Repositories](#)
- [Migrating to Another Virtual Appliance Using Backup and Restore](#)

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 and Software Updates > Licenses**.

To check the total system disk space usage, choose **Administration > Settings > Appliance**, then click the **Appliance Status** tab. Then under **Inventory**, expand **Disk Usage**.

Related Topics

- [Evaluating OVA Size and System Resources](#)
- [Improving Prime Infrastructure Performance](#)

Improving Prime Infrastructure Performance

You can improve Prime Infrastructure's speed and scalability using several techniques.

Related Topics

- [Tuning the Server](#)
- [Compacting the Prime Infrastructure Database](#)
- [Configuring Client Performance Settings](#)
- [Optimizing Memory for Assurance Processing](#)
- [Monitoring Assurance Memory Allocation and Demand](#)

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 and its 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 (for details, see "Triggering Application Backups" in Related Topics).
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")
3. Perform the resource modifications in the VM, then restart the VM and the server (see "Modifying VM Resource Allocation Using VMware vSphere Client").

Related Topics

- [Triggering Application Backups](#)
- [Enabling Server Tuning During Restarts](#)
- [Modifying VM Resource Allocation Using VMware vSphere Client](#)
- [Improving Prime Infrastructure Performance](#)

Enabling Server Tuning During Restarts

During system start, the Prime Infrastructure server inspects its VM hardware allocations for changes and will adjust to make use of expanded resources automatically.

The “Enable Server Tuning during restart option” is enabled by default and you will not want to change this setting under normal circumstances. If you find that the Prime Infrastructure server is not taking advantage of recent changes to its hardware, such as a larger RAM or disk space allocation, follow the steps below to ensure the tuning feature is enabled,

-
- Step 1** Choose **Administration > Settings > System Settings > General > Server Tuning**.
- Step 2** Select the **Enable Server Tuning during restart** check box, then click **Save**.
-

Related Topics

- [Tuning the Server](#)
- [Improving Prime Infrastructure Performance](#)

Modifying VM Resource Allocation Using VMware vSphere Client

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” in Related Topics).

Please note that Compliance Services features will not work if you expand the RAM, CPU or disk space resource allocations after installation.



Tip

For better performance: If you are changing RAM and CPU resource allocations for the virtual machine on which you run Prime Infrastructure, and you have more than one virtual machine running on the same hardware, you may also want to change your RAM and CPU resource *reservations* using the vSphere Client’s **Resource Allocation** tab. For details, see “VMware vSphere documentation” in Related Topics.

- Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).
- Step 2** Stop Prime Infrastructure using the **ncs stop** command (see “Stopping Prime Infrastructure”).
- Step 3** Halt the VMware virtual appliance:
- ```
PIServer/admin# halt
```
- Step 4** Launch the vSphere Client, right-click the virtual appliance, then click **Edit Settings**.
- Step 5** To change the RAM allocation, select **Memory** and change the **Memory Size** as needed. Then click **OK**.
- Step 6** To change the CPU allocation, select **CPUs** and select the **Number of Virtual Processors** from the drop-down list. Then click **OK**.
- Step 7** To add a new disk (you cannot expand the space of the existing disk):
- Click **Add**.
  - Select **Hard Disk**, then click **Next**.
  - 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 8** Power on the virtual appliance (see “Restarting Prime Infrastructure”)

---

#### Related Topics

- [Backing Up and Restoring Prime Infrastructure](#)
- [VMware vSphere Documentation](#)
- [Connecting Via CLI](#)
- [Stopping Prime Infrastructure](#)
- [Restarting Prime Infrastructure](#)
- [Improving Prime Infrastructure Performance](#)

## Compacting the Prime Infrastructure Database

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

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter the following command to compact the application database:

```
PIServer/admin# ncs cleanup
```

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

---

#### Related Topics

- [Connecting Via CLI](#)
- [Improving Prime Infrastructure Performance](#)

## Configuring Client Performance Settings

You can configure many client processes to improve Prime Infrastructure performance and scalability (see Related Topics).

#### Related Topics

- [Enabling Automatic Client Troubleshooting](#)
- [Enabling DNS Hostname Lookup](#)
- [Specifying How Long to Retain Client Association History Data](#)
- [Polling Clients When Receiving Client Traps/Syslogs](#)
- [Saving Client Traps as Events](#)
- [Saving 802.1x and 802.11 Client Traps as Events](#)
- [Improving Prime Infrastructure Performance](#)

## Enabling Automatic Client Troubleshooting

The **Administration > Settings > System Settings > Client and User > 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 area. Click **Export** to export the logs.

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

Automatic client troubleshooting is only available for clients running CCX Version 5 or 6. For a list of CCX-certified partner manufacturers and their CCX client devices, see the Cisco Compatible Extensions Client Devices page, linked under Related Topics, below.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**. The Client page appears.
- Step 2** In the **Process Diagnostic Trap** area, select the **Automatically troubleshoot client on diagnostic channel** check box, then click **Save**.
- 

### Related Topics

- [Cisco Compatible Extensions Client Devices page](#)
- [Configuring Client Performance Settings](#)
- [Improving Prime Infrastructure Performance](#)

## Enabling DNS Hostname Lookup

DNS lookup can take a considerable amount of time, so Prime Infrastructure has it disabled by default.

You can enable or disable the DNS lookup for client hostnames, and change how long Prime Infrastructure retains the results of previous DNS lookups in its cache.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**.
- Step 2** Select the **Lookup client host names from DNS server** check box.
- Step 3** Enter the number of days that you want the hostname to remain in the cache, then click **Save**.
- 

### Related Topics

- [Configuring Client Performance Settings](#)
- [Improving Prime Infrastructure Performance](#)

## Specifying 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 retention duration of client association history can be configured to help manage this potential issue.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**.
- Step 2** Under Data Retention, change the following parameters as needed:
- **Dissociated Clients**—Enter the number of days that you want Prime Infrastructure to retain the data. The valid range is 1 to 30 days.
  - **Client session history**—Enter the number of days that you want Prime Infrastructure to retain the data. The valid range is 7 to 365 days.
  - **Number of Rows To Keep**—Enter the maximum number of client session records to maintain. The default is 8,000,000.
- Step 3** Click **Save**.
- 

### Related Topics

- [Configuring Client Performance Settings](#)
- [Improving Prime Infrastructure Performance](#)

## Polling Clients When Receiving Client Traps/Syslogs

Under normal circumstances, Prime Infrastructure polls clients on a regular schedule, every few minutes, identifying session information during the poll. You can also choose to have Prime Infrastructure poll clients immediately whenever traps and syslogs are received from them. This helps you discover new clients and their sessions quickly.

This option is disabled by default, as it can affect Prime Infrastructure performance. Busy networks with many clients can generate large amounts of traps and syslogs, especially during peak periods when clients are roaming and associating/disassociating often. In this case, polling clients every time you receive a trap or syslog may be an unnecessary processing burden.

If you enable the Wireless Polling Clients when Receiving Client Traps/Syslogs option, Prime Infrastructure enables Client Authentication, Client Deauthentication, and Client Disassociate Traps on the WLC even if you previously disabled the traps on the WLC. Prime Infrastructure triggers the WLC Sync operation, which enables the client traps on WLC.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client**.
- Step 2** Select the **Poll clients when client traps/syslogs received** check box. Prime Infrastructure will poll clients as soon as a trap or syslog is received, to identify client sessions.
- Step 3** Click **Save**.
- 

### Related Topics

- [Configuring Client Performance Settings](#)
- [Improving Prime Infrastructure Performance](#)

## 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.

Follow the steps below to ensure that Prime Infrastructure does not save client association and disassociation traps as events.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client**.
  - Step 2** Unselect the **Save client association and disassociation traps as events** check box.
  - Step 3** Click **Save** to confirm this configuration change. This option is disabled by default.
- 

### Related Topics

- [Configuring Client Performance Settings](#)
- [Improving Prime Infrastructure Performance](#)

## Saving 802.1x and 802.11 Client Traps as Events

You must enable **Save 802.1x and 802.11 client authentication failed traps as events** for debugging purposes.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client**.
  - Step 2** Select the **Save 802.1x and 802.11 client authentication fail traps as events** check box.
  - Step 3** Click **Save** to confirm this configuration change.
- 

### Related Topics

- [Configuring Client Performance Settings](#)
- [Improving Prime Infrastructure Performance](#)

## Enabling Enhanced Client Traps

To enable enhanced client traps:

- 
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**.
  - Step 2** Select the **Discover Clients from enhanced client traps** check box.
  - Step 3** Make sure that the Prime Infrastructure server is registered as a Trap receiver on Cisco WLC for receiving Client traps. The following trap flags need to be enabled on the devices for enhanced client trap to work:
    - config trapflags client enhanced-802.11-associate enable
    - config trapflags client enhanced-802.11-deauthenticate enable

- `config trapflags client enhanced-authentication enable`
- `config trapflags client enhanced-802.11-stats enable`

**Step 4** To log the incoming enhanced client traps on the Prime Infrastructure side, you can enable client trap logging via ssh to root shell. This generates `clientTraps.log` file under the `/opt/CSColumos/logs` file.

- `/opt/CSColumos/bin/setLogLevel.sh com.cisco.client.traps TRACE`
- 

#### Related Topics

- [Configuring Client Performance Settings](#)
- [Improving Prime Infrastructure Performance](#)

# Optimizing Memory for Assurance Processing

Prime Infrastructure's Assurance features depend heavily on high-volume NetFlow data forwarded to the Prime Infrastructure server by devices, including NAMs. Because Prime Infrastructure always aggregates NetFlow data before storing it, supporting Assurance features with appropriate data is a memory-intensive process.

With more working memory to hold NetFlow data during aggregation, Prime Infrastructure can get this job done faster and more efficiently. This can lead to important performance improvements if your organization licenses Assurance features and makes heavy use of them.

Prime Infrastructure offers features to help you:

- Determine how much memory is currently allocated to Assurance-related data processing, and how completely individual Assurance features are using that memory pool.
- Increase the default pool of memory used to process Assurance-related data.
- Balance the memory allocated to individual Assurance features, so those with the greatest demand for memory get what they need.

The amount of performance improvement you can get from using these features depends on the memory available and how you use Assurance features, but can be substantial. For example: Given a Prime Infrastructure Professional implementation with the recommended minimum hardware Prime Infrastructure can process up to 414,000 NetFlow host records in a single five-minute aggregation cycle. With Assurance memory optimization, maximum processing for the same type of data is closer to 800,000 records per cycle.

You can increase the Assurance memory pool without balancing Assurance memory allocations, and vice versa. But using these two optimization options together is the best way to improve Prime Infrastructure performance when Assurance features are used.

## Related Topics

- [Monitoring Assurance Memory Allocation and Demand](#)
- [Increasing the Assurance Memory Pool Via CLI](#)
- [Balancing Assurance Memory Allocation](#)
- [Resetting Assurance Memory Allocation](#)
- [Resetting the Assurance Memory Pool](#)

## Monitoring Assurance Memory Allocation and Demand

You can quickly see Prime Infrastructure's current Assurance-related memory allocation and usage.

- 
- Step 1** Select **Services > Application Visibility & Control > Data Sources**.
- Step 2** Select the text link **Assurance Memory Statistics** (in the upper right corner of the page). Prime Infrastructure displays:
- The current memory allocation in megabytes for each of the main Assurance feature categories, including Traffic, Performance Routing, Applications, Voice-Video data, Device Health, Lync and other data.
  - The usage of each area's memory allocation over the last 24 hours. The percentage represents the peak memory usage over that period (that is, if 100 percent of the memory allocation is used at any point in the past 24 hours, the usage percentage shown will be 100 percent).
- 

### Related Topics

- [Optimizing Memory for Assurance Processing](#)
- [Increasing the Assurance Memory Pool Via CLI](#)
- [Balancing Assurance Memory Allocation](#)

## Increasing the Assurance Memory Pool Via CLI

You can use the Prime Infrastructure command line to allocate more memory to all types of Assurance-related data processing. Note that using the **ncs tune-resources assurance** command requires a server restart. Once restarted, the server will increase the total pool of memory allocated to all Assurance-related data processing.

- 
- Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).
- Step 2** Enter the following command:
- ```
PIServer/admin# ncs tune-resources assurance
```
- Step 3** Restart the Prime Infrastructure server (see “Restarting Prime Infrastructure”).
-

Related Topics

- [Connecting Via CLI](#)
- [Restarting Prime Infrastructure](#)
- [Optimizing Memory for Assurance Processing](#)

Balancing Assurance Memory Allocation

You can use the Prime Infrastructure interface to automatically balance the allocation of the total Assurance memory pool to individual categories of Assurance-related data processing, ensuring that those Assurance features that need memory the most are getting it.

-
- Step 1** Select **Services > Application Visibility & Control > Data Sources**.
- Step 2** Select the text link **Assurance Memory Statistics** (in the upper right corner of the Data Sources page).
- Step 3** Click **Rebalance**.

Prime Infrastructure will change Assurance memory allocations to individual features as needed, reducing allocations for less-used features and increasing allocations for features where usage over the past 24 hours was at or near 100 percent.

Related Topics

- [Optimizing Memory for Assurance Processing](#)

Resetting Assurance Memory Allocation

You can use the Prime Infrastructure interface to cancel Assurance memory balancing, returning the allocation for each Assurance-related feature to its default value.

-
- Step 1** Select **Services > Application Visibility & Control > Data Sources**.
- Step 2** Select the text link **Assurance Memory Statistics** (in the upper right corner of the Data Sources page).
- Step 3** Click **Reset**.
-

Related Topics

- [Optimizing Memory for Assurance Processing](#)

Resetting the Assurance Memory Pool

You can use the Prime Infrastructure command line to return the Assurance memory pool to the default allocation, disabling all changes created using the **ncs tune-resources assurance** command explained in “Increasing the Assurance Memory Pool Via CLI”.

-
- Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).
- Step 2** Enter the following command:
- ```
PIServer/admin# ncs tune-resources default
```
- Step 3** Restart the Prime Infrastructure server (see “Restarting Prime Infrastructure”).
- 

### Related Topics

- [Increasing the Assurance Memory Pool Via CLI](#)
- [Connecting Via CLI](#)
- [Restarting Prime Infrastructure](#)
- [Optimizing Memory for Assurance Processing](#)

# Managing Data Sources

Prime Infrastructure depends on a variety of sources for accurate gathering and reporting of device, performance and assurance data. These sources include specialized monitoring devices such as NAMs, and protocols running on normal devices, such as Cisco Medianet, NetFlow, Flexible NetFlow, Network Based Application Recognition (NBAR), Performance Monitoring (PerfMon), and Performance Agent.

You will want to manage these sources to ensure that only the correct data is gathered from active sources. The Data Sources page allows you to review your current data sources, and delete those that are no longer active.

For details on the data sources used in dashlets, see “Advanced Monitoring” in Related Topics. For details on setting up individual data sources, see the data-source configuration sections of “Administrator Setup Tasks”, also listed in Related Topics.

## Related Topics

- [Viewing Current Data Sources](#)
- [Deleting Data Sources](#)
- [Viewing Current Data Sources](#)
- [Advanced Monitoring](#)
- [Administrator Setup Tasks](#)
- [Configuring Data Sources for Prime Infrastructure With Assurance](#)
- [Enabling Medianet NetFlow](#)
- [Enabling NetFlow and Flexible NetFlow](#)
- [Deploying Network Analysis Modules \(NAMs\)](#)
- [Enabling Performance Agent](#)

## Viewing Current Data Sources

Use the Data Sources page to review Prime Infrastructure’s current data sources. Access to this page requires administrator privileges

- 
- Step 1** Select **Services > Application Visibility & Control > Data Sources**. Prime Infrastructure displays a summary page that lists each device data source’s:
- **Device Name**—The host name of the data source
  - **Data Source**—The IP address of the data source.
  - **Type**—The type of data the source is sending to Prime Infrastructure (e.g., “Netflow”).
  - **Exporting Device**—The IP address of the device exporting the data to Prime Infrastructure.
  - **Last 5 min Flow Read Rate**—The amount of data Prime Infrastructure has received from this source during the last five minutes.
  - **Last Active Time**—The latest date and time that Prime Infrastructure received data from this source.
- For each Cisco NAM data collector sources, the page lists:
- **Name**—The host name of the NAM.

- **Type**—The type of data the NAM is collecting and sending to Prime Infrastructure (e.g., “Cisco Branch Routers Series Network Analysis Module”).
  - **Host IP Address**—The IP address of the NAM.
  - **Data Usage in System**—Whether the data forwarded by this NAM is enabled for use in Prime Infrastructure.
  - **Last Active Time**—The latest date and time that Prime Infrastructure received data from this NAM.
- 

**Related Topics**

- [Performing Special Administrative Tasks](#)
- [Deleting Data Sources](#)

## Deleting Data Sources

Use the Data Sources page to delete inactive Prime Infrastructure data sources. Access to this page requires administrator privileges.

Note that you cannot delete a NetFlow data source until seven full days have elapsed without receipt of any data from that data source. This delay helps protect the integrity of NetFlow data (which Prime Infrastructure identifies and aggregates according to the source) by giving network operators a full week to ensure that the data source has been retired. If the source remains active during that period and sends data to Prime Infrastructure, data from that source will still be identified and aggregated properly with other data from the same source (instead of being identified as a new source).

- 
- Step 1** Select **Services > Application Visibility & Control > Data Sources**.
  - Step 2** Select the checkbox next to the inactive data source you want to delete.
  - Step 3** Click **Delete**.
  - Step 4** Click **OK** to confirm the deletion.
- 

**Related Topics**

- [Performing Special Administrative Tasks](#)
- [Viewing Current Data Sources](#)

# Performing Special Administrative Tasks

Prime Infrastructure provides administrators with special access in order to perform a variety of infrequent tasks, including

- Connecting to the server via an SSH command-line interface (CLI) session.
- Changing server hardware setup and resource allocations.
- Starting, stopping, and checking on the status of Prime Infrastructure services.
- Running Prime Infrastructure processes accessible only via the CLI.
- Managing access rights, including changing passwords for user IDs with special tasks.
- Removing or resetting Prime Infrastructure.

## Related Topics

- [Connecting Via CLI](#)
- [Starting Prime Infrastructure](#)
- [Checking Prime Infrastructure Server Status](#)
- [Checking Prime Infrastructure Version and Patch Status](#)
- [Stopping Prime Infrastructure](#)
- [Restarting Prime Infrastructure](#)
- [Removing Prime Infrastructure](#)
- [Resetting Prime Infrastructure to Defaults](#)
- [Restoring Physical Appliances to Clean State](#)
- [Changing the Prime Infrastructure Host Name](#)
- [Enabling the FTP User](#)
- [Changing the Root User Password](#)
- [Recovering Administrator Passwords on Virtual Appliances](#)
- [Recovering Administrator Passwords on Physical Appliances](#)
- [Getting the Installation ISO Image](#)
- [Checking High Availability Status](#)

## Connecting Via CLI

Administrators can connect to the Prime Infrastructure server via its command-line interface (CLI). CLI access is required when you need to run commands and processes accessible only via the Prime Infrastructure CLI. These include commands to start the server, stop it, check on its status, and so on.

Before you begin, make sure you:

- Know the user ID and password of an administrative user with CLI access to that server or appliance. Unless specifically barred from doing so, all administrative users have CLI access.
- Know the IP address or host name of the Prime Infrastructure server.

---

**Step 1** Start up your SSH client, start an SSH session via your local machine's command line, or connect to the dedicated console on the Prime Infrastructure physical or virtual appliance.

**Step 2** Log in as appropriate:

- a. If you are using a GUI client: Enter the ID of an active administrator with CLI access and the IP address or host name of the Prime Infrastructure server. Then initiate the connection.

Or

- b. If you are using a command-line client or session: Log in with a command like the following:

```
[localhost]# ssh username@IPHost
```

Where:

- *username* is the user ID of a Prime Infrastructure administrator with CLI access to the server.
- *IPHost* is the IP address or host name of the Prime Infrastructure server or appliance.

Or

- c. If you are using the console: A prompt is shown for the administrator user name. Enter the user name.

Prime Infrastructure will then prompt you for the password for the administrator ID you entered.

**Step 3** Enter the administrative ID password. Prime Infrastructure will present a command prompt like the following: `PIServer/admin#`.

**Step 4** If the command you need to enter requires that you enter “configure terminal” mode, enter the following command at the prompt:

```
PIServer/admin# configure terminal
```

The prompt will change from `PIServer/admin#` to `PIServer/admin/conf#`.

---

### Related Topics

- [Performing Special Administrative Tasks](#)

## Starting Prime Infrastructure

You will need to start Prime Infrastructure after upgrades.

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter the following command to start the Prime Infrastructure server or appliance:

```
PIServer/admin# ncs start
```

---

### Related Topics

- [Connecting Via CLI](#)
- [Stopping Prime Infrastructure](#)
- [Restarting Prime Infrastructure](#)
- [Performing Special Administrative Tasks](#)

## Checking Prime Infrastructure Server Status

You can check on the status of all Prime Infrastructure server or appliance processes at any time, without stopping the server. Technical Assistance personnel may ask you to perform this task when troubleshooting a problem with Prime Infrastructure.

You can also check on the current health of the server using the dashlets on the Admin Dashboard (see “Monitoring Prime Infrastructure Health”).

You can check on the status of High Availability options enabled on the server using the command **ncs ha status** (see “Checking High Availability Status”).

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter the following command to display the current status of Prime Infrastructure processes and services:

```
PIServer/admin# ncs status
```

---

### Related Topics

- [Connecting Via CLI](#)
- [Monitoring Prime Infrastructure Health](#)
- [Checking High Availability Status](#)
- [Performing Special Administrative Tasks](#)

## Checking Prime Infrastructure Version and Patch Status

You can check on the version of a Prime Infrastructure server and the patches applied to it at any time, without stopping the server. You will usually need to do this when upgrading or patching the server software.

- 
- Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).
- Step 2** Enter the following command to display the current status of Prime Infrastructure processes and services:

```
PIServer/admin# show version
```

---

### Related Topics

- [Connecting Via CLI](#)
- [Performing Special Administrative Tasks](#)

## Stopping Prime Infrastructure

You can stop a Prime Infrastructure server or appliance at any time using the command line interface. Any users logged in at the time you stop Prime Infrastructure will have their sessions stop functioning.

- 
- Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).
- Step 2** Enter the following command to stop the Prime Infrastructure server or appliance:

```
PIServer/admin# ncs stop
```

---

### Related Topics

- [Connecting Via CLI](#)
- [Performing Special Administrative Tasks](#)



## Restarting Prime Infrastructure

- 
- Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).
- Step 2** Enter the following command to stop the Prime Infrastructure server or appliance:
- ```
PIServer/admin# ncs stop
```
- Step 3** Wait for the previous command to complete.
- Step 4** Enter the following command to restart the Prime Infrastructure server or appliance:
- ```
PIServer/admin# ncs start
```
- 

### Related Topics

- [Connecting Via CLI](#)
- [Performing Special Administrative Tasks](#)

## Removing Prime Infrastructure

You may need to remove Prime Infrastructure in preparation for a clean “from scratch” re-installation. You can do so by following the steps below

Note that this procedure will delete all your existing data on the server, including all server settings and local backups. You will be unable to restore your data unless you have a remote backup or access to disk-level data recovery methods.

- 
- Step 1** Stop the server (see “Stopping Prime Infrastructure”).
- Step 2** In the VMware vSphere client, right-click the Prime Infrastructure virtual appliance.
- Step 3** Power off the virtual appliance.
- Step 4** Right click on the powered-off virtual appliance and select **Delete from Disk option**.
- 

### Related Topics

- [Stopping Prime Infrastructure](#)
- [Performing Special Administrative Tasks](#)

## Resetting Prime Infrastructure to Defaults

You may need to reset the installed Prime Infrastructure server to factory defaults, removing all user data and customizations, but preserving the installation itself. You can do so by following the steps below.

Note that this procedure will delete all your existing data on the server host except for the default settings supplied with Prime Infrastructure. You will be unable to restore your data unless you have a remote backup or access to disk-level data recovery methods.

- 
- Step 1** Stop the server (see “Stopping Prime Infrastructure”).
  - Step 2** Download the installation ISO image appropriate for your installed version of the Prime Infrastructure virtual or physical appliance server software and burn it to DVD (see “Getting the Installation ISO Image”).
  - Step 3** Power off the virtual appliance.
  - Step 4** Reinstall the appliance or OVA by booting the host from the DVD.
- 

### Related Topics

- [Stopping Prime Infrastructure](#)
- [Getting the Installation ISO Image](#)
- [Performing Special Administrative Tasks](#)

## Restoring Physical Appliances to Clean State

You will want to restore your Prime Infrastructure physical appliance to a clean state in preparation for an RMA return or other hardware retirement.

Note that this procedure will delete all of your existing data on the server, including all server settings, local backups, and the Prime Infrastructure software. You will be unable to restore your data unless you have a remote backup. Restoring the host to a clean state also ensures data security by preventing disk-level data recovery.

- 
- Step 1** Stop the server (see “Stopping Prime Infrastructure”).
  - Step 2** Power off the physical appliance, then power on.
  - Step 3** During the boot sequence, press **Ctrl+H** when prompted. The console displays the RAID Configuration screen.
  - Step 4** Click the virtual drive containing the Prime Infrastructure server.
  - Step 5** Select **slow init** to re-initialize the hard drive. The physical appliance will overwrite the entire drive with zeroes.
- 

### Related Topics

- [Stopping Prime Infrastructure](#)
- [Performing Special Administrative Tasks](#)

## Changing the Prime Infrastructure Host Name

Prime Infrastructure prompts you for a host name when you install the server. For a variety of reasons, you may find there is a mismatch between the host name on the Prime Infrastructure server and the host name elsewhere. If so, you can recover without reinstalling by changing the host name on the server.

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”). Be sure to enter “configure terminal” mode.

**Step 2** Enter the following command:

```
PIServer/admin(config)# hostname newHostName
```

Where *newHostName* is the new host name you want to assign to the Prime Infrastructure server.

**Step 3** Restart the Prime Infrastructure server using the **ncs stop** and **ncs start** commands, as explained in [Restarting Prime Infrastructure](#)

---

### Related Topics

- [Connecting Via CLI](#)
- [Restarting Prime Infrastructure](#)
- [Performing Special Administrative Tasks](#)

## Enabling the FTP User

To use Prime Infrastructure as an FTP server for file transfers and software image management, an administrator must configure an FTP account. Use the steps below to enable the account and set a password for it.

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter the following command:

```
PIServer/admin#ncs password ftpuser username password password
```

Where:

- **username** is an existing Prime Infrastructure user ID with administrator privileges.
- **password** is the login password for **username**.

For example:

```
pi-system-999/admin# ncs password ftpuser root password MyPassword
Initializing...
Updating FTP password.
This may take a few minutes...
Successfully updated location ftp user
pi-system-999/admin#
```

---

### Related Topics

- [Connecting Via CLI](#)

- [Performing Special Administrative Tasks](#)

## Changing the Root User Password

Administrators can change the password associated with this special administrative ID.

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter the following command:

```
PIServer/admin# ncs password root password password
```

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

For example:

```
PIServer/admin# ncs password root password #password#
pi-system-198/admin# ncs password root password #password#
Password updated for web root user
pi-system-198/admin#
```

---

### Related Topics

- [Connecting Via CLI](#)
- [Performing Special Administrative Tasks](#)

## Recovering Administrator Passwords on Virtual Appliances

You can recover (that is, reset) administrator passwords on Prime Infrastructure virtual machines (also known as OVAs) installed on your own hardware.

### Before You Begin

Ensure that you have:

- Physical access to the Prime Infrastructure server.
- A copy of the installation ISO image appropriate for your version of the software. See “Getting the Installation ISO Image” in Related Topics.
- Access to the VMware vSphere client, and to the vSphere inventory, Datastores and Objects functions. If you do not have such access, consult your VMware administrator. You should avoid accessing ESX directly from the vSphere client.

- 
- Step 1** At the Prime Infrastructure OVA server, launch the VMware vSphere client.
- Step 2** Upload the installation ISO image to the data store on the OVA virtual machine, as follows:
- a. In the vSphere inventory, click **Datastores**.
  - b. On the **Objects** tab, select the datastore to which you will upload the file.
  - c. Click the **Navigate to the datastore file browser** icon.
  - d. If needed, click the **Create a new folder** icon and create a new folder.
  - e. Select the folder that you created or select an existing folder, and click the **Upload a File** icon.  
If the Client Integration Access Control dialog box appears, click **Allow** to allow the plug-in to access your operating system and proceed with the file upload.
  - f. On the local computer, find the ISO file and upload it.
  - g. Refresh the datastore file browser to see the uploaded file in the list.
- Step 3** With the ISO image uploaded to a datastore, make it the default boot image, as follows:
- a. Using the VMware vSphere client, right-click the deployed OVA and choose **Power > Shut down guest**.
  - b. Select **Edit Settings > Hardware**, then select **CD/DVD drive 1**.
  - c. Under **Device Type**, select **Datastore ISO File**, then use the **Browse** button to select the ISO image file you uploaded to the datastore.
  - d. Under **Device Status**, select **Connect at power on**.
  - e. Click the **Options** tab and select **Boot Options**. Under **Force BIOS Setup**, select **Next time VM boots, force entry into BIOS setup Screen**. This will force a boot from the virtual machine BIOS when you restart the virtual machine.
  - f. Click **OK**.
  - g. In the VMware vSphere client, right-click the deployed OVA and choose **Power > Power On**.
  - h. In the BIOS setup menu, find the option that controls the boot order of devices and move **DVD/CDROM** to the top.

- Step 4** Follow the steps below to reset a server administrator password:
- a. Save your BIOS settings and exit the BIOS setup menu. The virtual machine will boot from the ISO image and display a list of boot options.
  - b. Enter **3** if you are using the keyboard and monitor to access the OVA, or **4** if you are accessing via command line or console. The vSphere client displays a list of administrator user names.
  - c. Enter the number shown next to the administrator username for which you want to reset the password.
  - d. Enter the new password and verify it with a second entry.
  - e. Enter **Y** to save your changes and reboot.
  - f. Once the virtual machine has rebooted: Using the vSphere client, Click the CD icon and select **Disconnect ISO image**.
- Step 5** Log in with the new administrator password.
- 

**Related Topics**

- [Getting the Installation ISO Image](#)
- [Performing Special Administrative Tasks](#)

## Recovering Administrator Passwords on Physical Appliances

You can recover (reset) administrator passwords on Prime Infrastructure physical appliances.

**Before You Begin**

Ensure that you have:

- Physical access to the Prime Infrastructure appliance.
- A copy of the appliance recovery CD that was supplied with the shipped appliance.

If you have lost the appliance recovery CD, download and burn a DVD copy of the ISO image, as explained in “Getting the Installation ISO Image”. You can then use the DVD to reset administrator passwords on the appliance (see “Recovering Administrator Passwords on Virtual Appliances” for detailed steps).

- 
- Step 1** Place the appliance recovery CD in the appliance's optical drive and reboot the appliance. The vSphere client displays a list of boot options.
- Step 2** Enter **3** to select the **Reset Administrator Password (Keyboard/Monitor)** boot option. The vSphere client displays a list of administrator user names.
- Step 3** Enter the number shown next to the administrator user name for which you want to recover (reset) the password.
- Step 4** Enter the new password and verify it with a second entry.
- Step 5** Enter **Y** to save your changes and reboot.
- Step 6** Log in with the new administrator password.
-

**Related Topics**

- [Getting the Installation ISO Image](#)
- [Recovering Administrator Passwords on Virtual Appliances](#)
- [Performing Special Administrative Tasks](#)

## Getting the Installation ISO Image

Copies of the Prime Infrastructure installation ISO image are needed for some special maintenance operations, such as resetting administrator passwords.

Prime Infrastructure ISO image files have the format `PI-APL-version-K9.iso`, where *version* is the version number of the product. The version number will often contain extended numbering indicating the patch level of the product. For example: If you were using a fully-updated version of Prime Infrastructure 3.0, you would need to download the ZIP archive file `PPI-APL-3.0.0.78-1-K9.iso.zip` from Cisco.com, and then extract the `PI-APL-3.0.0.78-1-K9.iso` ISO image file from the archive file.

If you do not have a copy of the ISO image, you can download it from Cisco.com using the steps below:

- 
- Step 1** On a browser with internet access, link to the Cisco Software Download Navigator (see Related Topics).
  - Step 2** Use the **Find** box to search for “Cisco Prime Infrastructure”.
  - Step 3** From the results list, select the software version you are using (for example, if you were using Prime Infrastructure 3.0, you would select `Cisco Prime Infrastructure 3.0`).
  - Step 4** Select **Prime Infrastructure Software** to display the list of ISOs and other downloadable image files for that software version.
  - Step 5** Download the ISO image from the page.
  - Step 6** When the download is complete, check that the MD5 checksum of the downloaded file matches the checksum shown for the file on its Cisco.com download page. If the checksums do not match, the file is corrupt, and you will need to download it from Cisco.com again.
  - Step 7** If you need the ISO image on disk: Burn the ISO image to a Dual Layer DVD using DVD authoring software. For reliable results, we recommend that you conduct the burn at single (1X) speed and with the “Verify” option turned on.
- 

**Related Topics**

- [Cisco Software Download Navigator](#)
- [Performing Special Administrative Tasks](#)
- [Cisco Prime Infrastructure Appliance Hardware Installation Guide](#)

# Keeping Prime Infrastructure Software Updated

Cisco provides updates to Prime Infrastructure software periodically. These updates fall into the following categories:

- **Critical Fixes**—Provide critical fixes to the software. We strongly recommend that you download and apply all of these updates as soon as they are available.
- **Device Support**—Adds support for managing devices which Prime Infrastructure did not support at release time. These updates are published on a monthly basis.
- **Add-Ons**—Provide new features, which can include new GUI screens and functionality, to supplement the Prime Infrastructure version you are using.

For details on how to find these updates, and how to get notifications when they are released, see “Viewing Installed and Available Software Updates” in Related Topics.

The update notifications that Prime Infrastructure displays are based on the Notification Settings you specify using **Administration > Settings > System Settings > Software Update**. For details, see “Configuring Software Update Notifications”.

For details on installing these updates, see “Installing Prime Infrastructure Software Updates”.

For details on streamlining your software update notifications and installations using your Cisco.com account, see “Using Your Cisco.com Account Credentials with Prime Infrastructure”.

## Related Topics

- [Viewing Installed and Available Software Updates](#)
- [Configuring Software Update Notifications](#)
- [Installing Software Updates](#)
- [Using Your Cisco.com Account Credentials with Prime Infrastructure](#)

## Viewing Installed and Available Software Updates

Prime Infrastructure allows you to:

- Receive notifications when new software updates become available.
- Modify how and when you are notified that new software updates are available.
- View the details of each update.
- See which software updates have been installed.

The following topics explain how to perform each of these tasks.

## Related Topics

- [Getting Software Update Notifications](#)
- [Configuring Software Update Notifications](#)
- [Viewing Details of Installed Software Updates](#)
- [Viewing Installed Updates From the Login Page](#)
- [Viewing Installed Updates From the About Page](#)
- [Keeping Prime Infrastructure Software Updated](#)



## Getting Software Update Notifications

When properly configured, Prime Infrastructure will notify you automatically when new software updates are available.

- 
- Step 1** Choose **Administration > Settings > System settings > General > Account credentials**
- Step 2** Enter a valid Cisco.com user name and password.
- Step 3** Click **Save**.
- Step 4** Choose **Administration > Settings > System Settings > General > Software Update**.
- Step 5** Under Notification Settings, select the categories for which you want updates displayed on the **Administration > Software Update** page.
- Step 6** Click **Save**.

To see notifications: Click on the notifications icon at the top right, next to the alarms icon.

---

### Related Topics

- [Configuring Software Update Notifications](#)
- [Viewing Installed and Available Software Updates](#)
- [Using Your Cisco.com Account Credentials with Prime Infrastructure](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Configuring Software Update Notifications

You can modify the update notifications that Prime Infrastructure displays on the **Administration > Software Update** page. For example, if you do not want to install any updates to Prime Infrastructure, you can disable all notification and prevent Prime Infrastructure from displaying notifications of available updates.

- 
- Step 1** Choose **Administration > Settings > System Settings > General > Software Update**.
- Step 2** Under Notification Settings, select the categories for which you want updates displayed on the **Administration > Software Update** page.
- Step 3** Click **Save**.
- 

### Related Topics

- [Viewing Installed and Available Software Updates](#)
- [Getting Software Update Notifications](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Viewing Details of Installed Software Updates

---

- Step 1** Choose **Administration Settings > Licenses and Software Updates > Software Update**.
- Step 2** Click the **Updates** tab to see the Name, Type, Version and Status for each installed software update.  
To filter this list, click the Filter icon at the right side of the Updates tab and select the categories of installed updates you want to see.
- Step 3** Click the **Files** tab to see the list of installed UBF files and downloaded UBF files which have yet to be installed.  
To delete a software update file that has not yet been installed, select the file and click **Delete**.
- 

### Related Topics

- [Viewing Installed and Available Software Updates](#)
- [Viewing Installed Updates From the Login Page](#)
- [Viewing Installed Updates From the About Page](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Viewing Installed Updates From the Login Page

---

- Step 1** Launch or log out of Prime Infrastructure. The login page displays.
- Step 2** Click **View installed updates**. Prime Infrastructure displays a popup list of the names and versions of all installed software updates.
- Step 3** Click the **Close** button to close the popup list.
- 

### Related Topics

- [Viewing Installed Updates From the About Page](#)
- [Viewing Installed and Available Software Updates](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Viewing Installed Updates From the About Page

---

- Step 1** Click the settings icon at the upper right corner of any Prime Infrastructure page.
- Step 2** Click **About Prime infrastructure**. The About page appears, listing the version of the product and other details
- Step 3** Click **View installed updates**. Prime Infrastructure displays a popup list of the names and versions of all installed software updates.
- Step 4** Click the **Close** button to close the popup list.
-

**Related Topics**

- [Viewing Installed Updates From the Login Page](#)
- [Viewing Installed and Available Software Updates](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Installing Software Updates

Prime Infrastructure periodically provides critical fixes, device support, and add-on updates that you can download and install by choosing **Administration > Software Update**. Depending on your connectivity and preference, you can install software updates by:

- Downloading updates directly from Cisco.com to the Prime Infrastructure server. To use this method, your Prime Infrastructure server must be able to connect externally to Cisco.com. For details, see “Installing Software Updates from Cisco.com” in Related Topics.
- Downloading software update files to a client or server with external connectivity, then uploading them to and installing them on the Prime Infrastructure server. For details, see “Uploading and Installing Downloaded Software Updates” in Related Topics.

**Related Topics**

- [Installing Software Updates from Cisco.com](#)
- [Uploading and Installing Downloaded Software Updates](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Installing Software Updates from Cisco.com

The following steps explain how to install software updates directly from Cisco.com. This procedure assumes that Prime Infrastructure has external connectivity to Cisco.com and that you want to download updates directly from Cisco.com.

- 
- Step 1** Choose **Administration > Licenses and Software Updates > Software Update**.
- Step 2** Click the **download** link at the top of the page to get the latest updates from Cisco.com.
- Step 3** Enter your Cisco.com login credentials. Prime Infrastructure lists the available updates.
- If you receive an error indicating there was a problem connecting to cisco.com, verify your proxy settings by choosing **Administration > Settings > System Settings > General > Proxy**. If your proxy settings are not working, deselect **Enable Proxy**, then click **Save**.
- Step 4** Click **Show Details** to see the details about the updates.
- Step 5** Click **Download** next to the update you want to install.
- Step 6** After the update has been downloaded, click **Install** on the message that appears.
- The Status of Updates section shows the installed software updates.
- Step 7** If prompted to restart the Prime Infrastructure server, follow the steps explained in the related topic, “Restarting Prime Infrastructure”.
-

**Related Topics**

- [Installing Software Updates](#)
- [Restarting Prime Infrastructure](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Uploading and Installing Downloaded Software Updates

The following steps explain how to upload and install software updates. This procedure is useful when your Prime Infrastructure server does not have external connectivity, or you prefer to download files on a different server.

- 
- Step 1** Choose **Administration > Licenses and Software Updates > Software Update**.
  - Step 2** Click the **upload** link at the top of the page.
  - Step 3** On the Upload Update window, click **Cisco Download**, which displays Cisco.com's "Download Software" page.
  - Step 4** Select **Products > Cloud and Systems Management > Routing and Switch Management > Network Management Solutions > Prime Infrastructure**.
  - Step 5** Select the correct version of Prime Infrastructure.
  - Step 6** Select an update software type (such as "Prime Infrastructure Device Packs").
  - Step 7** From the page that appears, click **Download** next to the file containing the updates you want. The file will have a UBF filename extension.

If you have not already stored your Cisco.com credentials (see "Saving Cisco.com Account Credentials in Prime Infrastructure" in Related Topics), you will be prompted to log in to Cisco.com, and to accept your organization's active license agreement with Cisco, before you can download the update file.

Be sure to download software updates that match your Prime Infrastructure version. For example, if you were running Prime Infrastructure 2.2, be sure to download software updates for version 2.2 only.

- Step 8** With the update file downloaded to your client machine, return to the Prime Infrastructure tab and choose **Administration > Licenses and Software Updates > Software Update**.
  - Step 9** Click **Upload** and browse to locate and select the update file you downloaded.
  - Step 10** Click **Install** for the updates you have uploaded.  
The Status of Updates section shows the installed software updates.
  - Step 11** If prompted to restart the Prime Infrastructure server, follow the steps explained in the related topic, "Restarting Prime Infrastructure".
- 

**Related Topics**

- [Installing Software Updates](#)
- [Saving Cisco.com Account Credentials in Prime Infrastructure](#)
- [Restarting Prime Infrastructure](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Using Your Cisco.com Account Credentials with Prime Infrastructure

You can store your Cisco.com account user name and password in Prime Infrastructure. Doing so will allow you to streamline download and installation of software updates, and speed automatic checking and notification of updates.

Note that Prime Infrastructure stores only one set of Cisco.com credentials at a time. The password is stored in secure, encrypted form. It will use this stored user name and password to do all software update notification checks and downloads until such time as another user either deletes the stored credentials (as explained in “Deleting Cisco.com Account Credentials” in Related Topics) or overwrites them by entering a new Cisco.com user name and password.

### Related Topics

- [Saving Cisco.com Account Credentials in Prime Infrastructure](#)
- [Deleting Cisco.com Account Credentials](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Saving Cisco.com Account Credentials in Prime Infrastructure

- 
- Step 1** Choose **Administration > Settings > System settings > Account credentials**
- Step 2** Enter a valid Cisco.com user name and password.
- Step 3** Click **Save**.
- 

### Related Topics

- [Installing Software Updates](#)
- [Restarting Prime Infrastructure](#)
- [Keeping Prime Infrastructure Software Updated](#)

## Deleting Cisco.com Account Credentials

- 
- Step 1** Choose **Administration > Settings > System settings > Account credentials**.
- Step 2** Click **Delete**.
- Step 3** Click **Yes** to confirm the deletion.
- 

### Related Topics

- [Installing Software Updates](#)
- [Restarting Prime Infrastructure](#)
- [Keeping Prime Infrastructure Software Updated](#)

# Configuring Support Request Settings

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

- 
- Step 1** Choose **Administration > Settings > System Settings > Support Request**. The Support Request Settings page appears.
- Step 2** Configure the following parameters:
- General Support Settings:
    - Enable interactions directly from the server—Select this check box to allow interactions for support requests directly from the server.
    - Sender E mail Address—Enter the email address of the support request sender.
    - Interactions via client system only—Select this check box to allow interactions for support requests only through client system.
  - Technical Support Provider Information:
    - Cisco—Select this check box if the technical support provider is Cisco.
    - Default Cisco.com Username—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—Select this check box if the technical support provider is a third party other than Cisco. Enter the email address, email subject line format, and website URL of the support provider.
- Step 3** Click **Save Settings**.
- 

## Related Topics

- [Opening a Support Case](#)
- [Launching the Cisco Support Community](#)

# Managing Disk Space Issues

Whenever disk space on the physical or virtual Prime Infrastructure server reaches 90 percent, the server will trigger a Major alert indicating that the server is low on disk space.

Threshold crossings for these alarms are calculated based on the usage of the Prime Infrastructure `optvol` and `localdiskvol` partitions only. The `optvol` partition contains the Oracle database used to store all of Prime Infrastructure's inventory and network data, while `localdiskvol` stores local application backups, WLC and MSE backups, and reports. The settings that trigger the alarms are defined in the file `PackagingResources.properties`, which you can find in the Prime Infrastructure server in the folder `/opt/CSCOLumos/conf/rfm/classes/com/cisco/packaging`.

We recommend that administrators take action to increase disk space immediately upon receiving the Major alert. You can do this using any combination of the following methods:

- Free up existing database space as explained in “Compacting the Prime Infrastructure Database”.
- Reduce the storage load on the `localdiskvol` partition by setting up and using remote backup repositories, as explained in “Using Remote Backup Repositories”.
- Reduce the storage load on the `optvol` partition by reducing the amount and storage period for which you retain inventory and network data:
  - Reduce the length of time you store client association data and related events, as explained in “Specifying How Long to Retain Client Association History Data” and “Saving Client Traps as Events”.
  - Reduce the length of time you store reports, as explained in “Controlling Report Storage and Retention”.
  - Reduce the retention period for network inventory, performance, and other classes of data, as explained in “Specifying Data Retention by Category” and “Enabling DNS Hostname Lookup”.
- Increase the amount of existing virtual disk space allocated to Prime Infrastructure, as explained in “Modifying VM Resource Allocation Using VMware vSphere Client”. If you are using VMware ESXi 5.5 or later, use the vSphere Web Client to adjust disk space allocation (for details, see the “VMware vSphere documentation” in Related Topics). You can also install additional physical disk storage and then use VMware Edit Settings or the vSphere Web Client to allocate the additional storage to Prime Infrastructure.
- Move the Prime Infrastructure server installation to a server with adequate disk space, as explained in “Migrating to Another OVA Using Backup and Restore” and “Migrating to Another Appliance Using Backup and Restore”.

## Related Topics

- [Compacting the Prime Infrastructure Database](#)
- [Using Remote Backup Repositories](#)
- [Specifying How Long to Retain Client Association History Data](#)
- [Saving Client Traps as Events](#)
- [Controlling Report Storage and Retention](#)
- [Specifying Data Retention by Category](#)
- [Specifying Data Retention By Database Table](#)
- [Enabling DNS Hostname Lookup](#)
- [Modifying VM Resource Allocation Using VMware vSphere Client](#)

- [VMware vSphere Documentation](#)
- [Migrating to Another Virtual Appliance Using Backup and Restore](#)
- [Migrating to Another Physical Appliance Using Backup and Restore](#)





# 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.

## Related Topics

- [Backup and Restore Concepts](#)
- [Using Automatic Application Backups](#)
- [Using Remote Backup Repositories](#)
- [Taking Backups From the Command Line](#)
- [Restoring From Backups](#)
- [Managing Disk Space Issues During Backup and Restore](#)
- [Using Backup and Restore with Operations Center](#)

## Backup and Restore Concepts

Administrators evaluating how to implement a backup routine for Prime Infrastructure should be familiar with the concepts explained in this section.

## Related Topics

- [Backup Types](#)
- [Backup Scheduling](#)
- [Backup Repositories](#)
- [Backup Filenames](#)
- [Validating Backups](#)
- [Information Contained in Backup Files](#)
- [Using Backup and Restore to Replace Servers](#)

## Backup Types

Prime Infrastructure creates two types of backups:

- **Application backups:** These contain all Prime Infrastructure application data, but do not include host-specific settings, such as the server hostname and IP address.
- **Appliance backups:** These contain all application data and host-specific settings, including the hostname, IP address, subnet mask, and default gateway.

Note that:

- Application and appliance backups can be taken from both virtual and hardware appliances.
- Either type of backup can be restored to the same or a new host, as long as the new host has the same or higher hardware and software configuration as the host from which the backup was taken.
- You can only restore an appliance backup to a host running the same version of the Prime Infrastructure server software as the server from which the backup was taken.
- You cannot restore an application backup using the appliance restore command, nor can you restore an appliance backup using the application restore command.

We recommend:

- If you are evaluating Prime Infrastructure: Use the default automatic application backup to the local repository.
- If you are running Prime Infrastructure in a production environment, either as a virtual or hardware appliance: Take regular application backups to a remote backup server. You can use the application backups to restore your server for all failures except complete failure of the server hardware.

### Related Topics

- [Using Automatic Application Backups](#)
- [Using Remote Backup Repositories](#)

## Backup Scheduling

Prime Infrastructure provides automatic, scheduled application backups. This feature is enabled by default, and creates one application backup file every day, automatically, in the default local backup repository.

You can change this schedule as needed. You can also take an automatic application backup at any time from the Prime Infrastructure interface. Appliance backups can only be taken from the command line.

Automatic application backup can create storage-space problems if the backup repository is local to the Prime Infrastructure server. While this is usually acceptable in test implementations, it is not intended to substitute for routine scheduled backups to remote servers in a production environment.

In a production environment, most administrators will:

1. Set up remote repositories to hold the backup files.
2. Use the automatic scheduled application backup to create backups on the remote repositories on a regular schedule.

You can still use the Prime Infrastructure command line to create application or appliance backups at any time, as needed.

**Related Topics**

- [Using Automatic Application Backups](#)
- [Using Remote Backup Repositories](#)
- [Scheduling Automatic Application Backups](#)
- [Specifying Automatic Application Backup Repositories](#)
- [Triggering Application Backups](#)
- [Taking Application Backups](#)
- [Taking Appliance Backups](#)

## Backup Repositories

By default, the automatic application backup feature stores backup files in the local backup repository `/localdisk/defaultRepo`. You can use the Prime Infrastructure interface to change the local automatic application backup repository, or create a new local repository.

You can also specify a remote repository using the Prime Infrastructure interface.

When taking application or appliance backups using the command line, you specify the local or remote repository you want the backup to be stored in. Administrators in production environments normally specify a remote repository, accessed via NFS, SFTP or FTP, as part of the command. NFS is a good choice, as it is typically much faster and more reliable than other protocols.

There is no difference between performing a command line application backup and using the GUI to perform an application backup. Both actions create the same backup file.

Whenever you use NFS to take backups or restore from a backup, make sure the mounted NFS server remains active throughout the backup or restore operation. If the NFS server shuts down at any point in the process, the Prime Infrastructure backup or restore operation will hang without warning or error message.

**Related Topics**

- [Specifying Automatic Application Backup Repositories](#)
- [Using Remote Backup Repositories](#)

## Backup Filenames

Automatically created Prime Infrastructure application backup files are assigned a filename with the format

*host-yymmdd-hhmm\_VERver\_BKSZsize\_CPUcpus\_MEMtarget\_RAMram\_SWAPswap\_type\_CKchecksum.tar.gpg*, where:

- *host* is the host name of the server from which the backup was taken. For example: *MyHost*.
- *yymmdd-hhmm* the date and time the backup was taken. For example: *140827-0745* for a backup created on August 27, 2014, at 7:45AM local time.
- *ver* is the version of Prime Infrastructure from which the backup was taken. For example: *VER2.2.0.0.149* for a backup taken from Prime Infrastructure version 2.2.0.0.149.
- *size* is the total size of the database file. For example: *BKSZ15G* for a 15 Gigabyte file.
- *cpus* is the total number of CPUs in the server from which the backup was taken. For example: *CPU16* for a server with 16 CPUs.
- *target* is the total amount of memory available for the database in the server from which the backup was taken. For example: *MEM4G* for a server with 4 gigabytes of memory available for the database.
- *ram* is the total amount of RAM in the server from which the backup was taken. For example: *RAM16G* for a server with 16 gigabytes of RAM.
- *swap* is the total size of the swap disk on the server from which the backup was taken. For example: *SWAP15G* for a server with 15 gigabytes of swap-disk space.
- *type* is the type of backup file. *APP* indicates an application backup; *SYS* indicates an appliance backup.
- *checksum* is the backup file checksum used to check file integrity.

For example:

*pi-system-71-183-141112-0330\_\_VER2.2.0.0.149\_BKSZ105G\_CPU4\_MEM4G\_RAM11G\_SWAP15G\_APP\_CK128121515.tar.gpg*

Command-line application and appliance backups have the format:

*backupname-yymmdd-hhmm\_VERver\_BKSZsize\_CPUcpus\_MEMtarget\_RAMram\_SWAPswap\_type\_CKchecksum.tar.gpg*,

where *backupname* is the name of the backup file that you specify as part of the backup command. All other values are appended automatically, as with automatically created application backup files.

For example:

- *test-141112-0330\_\_VER2.2.0.0.149\_BKSZ105G\_CPU4\_MEM4G\_RAM11G\_SWAP15G\_APP\_CK128121515.tar.gpg* (for a command-line application backup)
- *test-141112-0330\_\_VER2.2.0.0.149\_BKSZ105G\_CPU4\_MEM4G\_RAM11G\_SWAP15G\_SYS\_CK128121515.tar.gpg* (for a command-line appliance backup)

## Validating Backups

Prime Infrastructure performs the following checks to ensure the validity of backups:

1. Before starting the backup process, disk size, fast-recovery area, and control files are validated.
2. The created backup database is validated to ensure that it can be restored.
3. After the application data is zipped, the zipped file is validated against the files that were backed up.
4. The TAR file is validated to make sure that it is correct and complete.
5. The GPG file is validated to make sure that it is correct.

If you manually transfer the backup file, or if you want to verify that the backup transfer is complete, view the file's md5Checksum and file size.

Another best practice for validating a backup is to restore it to a standalone “test” installation of Prime Infrastructure.

## Information Contained in Backup Files

The table below describes the information contained in backup files. This information is restored to the server from backups.

Note that the `/opt/CSCOLumos/conf/Migration.xml` directory contains all configuration files and reports that are backed up. This directory is included in the backup and is restored.

**Table 5-1** Information Saved and Restored by Prime Infrastructure

| Feature                                             | Information Saved and Restored                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Background job settings                             | Data from the database                                                                                                                                                                                                                                                                               |
| Command Line Interface (CLI) settings               | All CLI information and settings are preserved. This includes the list of backup repositories, the FTP user name, users created using the CLI, AAA information specified via the CLI, and other CLI settings (such as the terminal timeout, and so on).                                              |
| Configuration archive                               | Data from the database                                                                                                                                                                                                                                                                               |
| Configuration templates                             | <ul style="list-style-type: none"> <li>Files in these directories: <ul style="list-style-type: none"> <li><code>/opt/CSCOLumos/conf/ootb</code></li> <li><code>/opt/CSCOLumos/xmp_inventory/dar/customized-feature-parts/CONFIGURATION</code></li> </ul> </li> <li>Data from the database</li> </ul> |
| Credentials                                         | Data from the database                                                                                                                                                                                                                                                                               |
| Inventory                                           | Data from the database                                                                                                                                                                                                                                                                               |
| Licenses                                            | Files in the <code>/opt/CSCOLumos/licenses/</code> directory.                                                                                                                                                                                                                                        |
| Local customizations (i.e., report heap size, etc.) | None. This information is not stored in the backup.                                                                                                                                                                                                                                                  |
| Maps                                                | <ul style="list-style-type: none"> <li>Files in the <code>/opt/CSCOLumos/domainmaps</code> directory</li> <li>Data from database</li> </ul>                                                                                                                                                          |
| Patch history                                       | None. This information is not stored in the backup.                                                                                                                                                                                                                                                  |
| Reports                                             | <ul style="list-style-type: none"> <li>Files in the following directories: <ul style="list-style-type: none"> <li><code>/localdisk/ftp/reports</code></li> <li><code>/localdisk/ftp/reportsOnDemand/</code></li> </ul> </li> <li>Data from the database</li> </ul>                                   |
| Software images                                     | Data from the database                                                                                                                                                                                                                                                                               |
| System settings                                     | <ul style="list-style-type: none"> <li>Files in the <code>/opt/CSCOLumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml</code> directory</li> <li>Data from the database</li> </ul>                                                                                                          |
| User preferences                                    | <ul style="list-style-type: none"> <li>Files in the <code>/opt/CSCOLumos/conf/wap/datastore/webacs/xml/prefs</code> directory</li> <li>Data from the database</li> </ul>                                                                                                                             |
| Users, groups, and roles                            | Data from the database                                                                                                                                                                                                                                                                               |
| Virtual domains                                     | Data from the database                                                                                                                                                                                                                                                                               |

## Using Backup and Restore to Replace Servers

If you must replace your virtual or physical appliance due to hardware failure, you can do so without losing your data, by restoring your most recent backup to a newly installed Prime Infrastructure server. However, if you do this, be sure that the new server is at the same version and patch level as the old server before you restore your data from the backup.

For example: You are running Prime Infrastructure 3.0 on a virtual appliance. You have applied two UBF patches since installation, and are taking regular backups. The virtual appliance hardware suddenly fails and must be replaced. You have a recent application backup, so you will want to install a new 3.0 server and then restore your data from the backup. Before performing the restore, make sure that you have applied to your newly installed server both of the UBF patches that you applied to the old server.

## Using Automatic Application Backups

As explained in the related topic “Backup Scheduling”, automatic application backup is a convenience feature that is enabled by default. It is intended to help you ensure that the important network management data stored in Prime Infrastructure is backed up regularly.

You can store automatic application backups in local or remote repositories. Remote repositories are preferred in production environments.

### Related Topics

- [Backup Scheduling](#)
- [Backup Repositories](#)
- [Backup Filenames](#)
- [Scheduling Automatic Application Backups](#)
- [Triggering Application Backups](#)
- [Specifying Automatic Application Backup Repositories](#)
- [Deleting Local Backup Repositories](#)
- [Using Remote Backup Repositories](#)
- [Using Remote Backup Repositories](#)

## Scheduling Automatic Application Backups

You can use the Prime Infrastructure interface to change the interval between backups, as well as the time of the day they are taken.

Taking backups is resource-intensive and affects Prime Infrastructure server performance. Avoid scheduling automatic application backups so that they take place at peak traffic times.

The **Max UI backups to keep** setting does not apply if you are using remote repositories for automatic application backups. You must monitor and archive or delete old backups on remote repositories using your own methods.

Prime Infrastructure generates a Major “Backup Failure” alarm whenever an automatic application backup fails. You can view these alarms just as you do other Prime Infrastructure alarms (see “Where to Find Alarms” in Related Topics). You can also get email notifications for these alarms if you include the “System” alarm category in your email notification settings (see “Configuring Email Settings”).

- 
- Step 1** Choose **Administration > Settings > Background Tasks**.
- Step 2** Click the **Prime Infrastructure Server Backup** link.
- Step 3** Change the **Max UI backups to keep**, the **Interval** between automatic backups, or the **Time of Day** to take them, as needed
- Step 4** Click **Save**.
- 

### Related Topics

- [Where to Find Alarms](#)
- [Configuring Email Settings](#)
- [Backup Types](#)
- [Backup Repositories](#)
- [Using Remote Backup Repositories](#)

## Triggering Application Backups

You can take application backups at any time by triggering them from the **Prime Infrastructure Server Backup** task. You can also trigger an application backup using the command line (see the related topic “Taking Application Backups”).

Taking a backup is server-intensive and will affect Prime Infrastructure performance. You should avoid triggering an application backup during times of high network traffic.

- 
- Step 1** Choose **Administration > Settings > Background Tasks**.
- Step 2** Select the **Prime Infrastructure Server Backup** task check box.
- Step 3** Choose **Select a command > Execute Now > Go**.
- Step 4** Click **Refresh** to see the current status of the backup task.
-



**Related Topics**

- [Scheduling Automatic Application Backups](#)
- [Taking Application Backups](#)

## Specifying Automatic Application Backup Repositories

You can use the Prime Infrastructure interface to specify a different backup repository for automatic application backups. The backup repository can be local or remote. You can also use the interface to create a new local backup repository if it does not already exist.

You can create a remote FTP repository by specifying it in the Prime Infrastructure interface. If you have already created a remote FTP, NFS, or SFTP repository, you can also use the Prime Infrastructure interface to specify that remote repository as the destination for automatic application backups.

- 
- Step 1** Choose **Administration > Settings > Background Tasks**.
- Step 2** Click the **Prime Infrastructure Server Backup** link.
- Step 3** In **Backup Repository**, select the name of the repository that you want to use during the next automatic application backup. This can be a local or remote repository.
- Step 4** Click **Save**.
- 

**Related Topics**

- [Backup Repositories](#)
- [Creating Local Backup Repositories](#)
- [Deleting Local Backup Repositories](#)
- [Using Remote NFS Backup Repositories](#)
- [Using Remote FTP Backup Repositories](#)

## Creating Local Backup Repositories

Prime Infrastructure stores automatic application backup files in the default local backup repository /localdisk/defaultRepo. You can create a different local backup repository and use it if you prefer.

You can create a remote FTP repository by specifying it in the Prime Infrastructure interface. If you have already created a remote FTP, NFS, or SFTP repository, you can also use the Prime Infrastructure interface to specify that remote repository as the destination for automatic application backups.

- 
- Step 1** Choose **Administration > Settings > Background Tasks**.
- Step 2** Click the **Prime Infrastructure Server Backup** link.
- Step 3** Click **Create**.
- Step 4** Enter the name of the repository you want to create. You can create a local repository or a remote repository.

You can create a remote FTP repository by specifying it in the Prime Infrastructure interface.

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

---

#### Related Topics

- [Backup Repositories](#)
- [Deleting Local Backup Repositories](#)
- [Using Remote Backup Repositories](#)
- [Using Remote NFS Backup Repositories](#)
- [Using Remote FTP Backup Repositories](#)

## Deleting Local Backup Repositories

Locally created backup repositories must be deleted via the command line interface (CLI). You cannot delete them using the Prime Infrastructure interface.

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter the following command to list the local application backup repositories and identify the one that you want to delete:

```
PIServer/admin# sh run | begin repository
```

**Step 3** Enter configuration mode:

```
PIServer/admin# configure terminal
```

**Step 4** Delete the existing repository:

```
PIServer/admin(config)# no repository repositoryName
```

Where *repositoryName* is the name of the repository that you want to delete.

**Step 5** Repeat Step 2 to verify that the repository was deleted.

---

#### Related Topics

- [Connecting Via CLI](#)
- [Creating Local Backup Repositories](#)
- [Specifying Automatic Application Backup Repositories](#)

# Using Remote Backup Repositories

In production environments, we recommend that you use remote repositories for backups, so that your network management data is protected from hardware and site failures. In most cases, this means you will need to:

1. Create one or more remote repositories to hold Prime Infrastructure server backup files. You will need to set these up yourself if your organization does not already have remote backup servers.
2. Specify the remote repository as the destination for automated application backups.
3. If needed: Specify the interval between automatic application backups and the time of day to take them. You will need to monitor and manually archive automatic application backups stored on remote repositories (the **Max backups to keep** setting does not apply with remote repositories).
4. Specify the remote repository as the backup destination when taking an application or appliance backup using the Prime Infrastructure CLI backup commands.

As with any resource that you plan to access remotely, specifying the correct server IP address and login credentials during setup are a requirement for successful use of remote backup repositories with Prime Infrastructure.

## Related Topics

- [Types of Backup Repositories](#)
- [Scheduling Automatic Application Backups](#)
- [Specifying Automatic Application Backup Repositories.](#)
- [Using Remote Backup Repositories](#)
- [Using Remote NFS Backup Repositories](#)
- [Using Remote SFTP Backup Repositories](#)
- [Using Remote FTP Backup Repositories.](#)
- [Taking Application Backups](#)
- [Taking Appliance Backups](#)

## Types of Backup Repositories

Although you can configure Prime Infrastructure to access remote backup resources using many protocols, Prime Infrastructure currently provides documented support for the following types of repositories:

- NFS—NFS is fast, reliable, relatively lightweight, and supports use of staging URLs. You must ensure the remote NFS server remains available and does not shut down while the backup or restore is running. If the remote machine is not available or is powered off, the backup and store process hangs without error messages.

We recommend that you use one or more NFS servers to stage and store your Prime Infrastructure backups. Note that use of backup staging URLs is supported only if you use the NFS protocol.

- FTP and SFTP—Note that, if you have a slow network, there is a possibility that backups to a remote FTP or SFTP repository could be corrupted because of incomplete transfers. Remote FTP repositories must be configured with passwords of 16 characters or less.

### Related Topics

- [Scheduling Automatic Application Backups](#)
- [Specifying Automatic Application Backup Repositories.](#)
- [Using Remote Backup Repositories](#)
- [Using Remote NFS Backup Repositories](#)
- [Using Remote SFTP Backup Repositories](#)
- [Using Remote FTP Backup Repositories.](#)
- [Taking Application Backups](#)
- [Taking Appliance Backups](#)

## Using Remote NFS Backup Repositories

You can create backup repositories on remote NFS server and configure the Prime Infrastructure server to use them.

Prime Infrastructure permits not only remote storage of your backups on NFS servers, but also remote staging: that is, creation, deletion, and marshaling of the many large temporary files used in backup processing. You can choose to stage on the same NFS server on which you store backups, or on another server. Creating an NFS staging URL is optional, but highly recommended, as it allows you to offload all of the disk-space burden imposed by regular backups onto the NFS server.

You must ensure the remote NFS server remains available and does not shut down while the backup or restore is running. If the remote NFS server is not available or is powered off, the backup and store process hangs without error messages.

The workflow for configuring Prime Infrastructure to use NFS repositories is:

1. Gather background information you need to do the NFS backup server configuration.
2. Configure the NFS backup server to work with Prime Infrastructure.
3. Configure Prime Infrastructure to use the NFS backup server.

The following related topics explain how to perform each of these tasks.

**Related Topics**

- [Before You Begin NFS Backup Configuration](#)
- [Configuring the NFS Backup Server](#)
- [Configuring Prime Infrastructure to Use the NFS Backup Server](#)

**Before You Begin NFS Backup Configuration**

Before you begin, make sure:

- You know the IP address of the NFS server on which you want to stage and store Prime Infrastructure backups. The staging and storage folders can be on the same NFS server, or on separate NFS servers. If you plan to stage and store on separate NFS servers, you will need IP addresses for both servers.
- You know the path names of the staging and storage folders on the NFS server. If you choose to stage and store on the same NFS server, the staging and storage folders *must* have different names.
- If you need to configure the NFS server or create the staging and storage folders: You have a login with root privileges on the server. If you are not permitted root privileges on the NFS server, share with your organization's NFS server administrators the configuration requirements given in the related topic, "Configuring the NFS Backup Server".
- You have an administrator user ID with root privileges on the Prime Infrastructure server.
- You have selected a repository name on the Prime Infrastructure server, which will point to the NFS server storage folder.

The steps in the related topics below assume that you want to configure a single NFS server to stage and store your backups. The steps will vary if you will not use NFS staging, or you want the staging and storage to take place on two different NFS servers.

**Related Topics**

- [Using Remote NFS Backup Repositories](#)
- [Configuring the NFS Backup Server](#)

## Configuring the NFS Backup Server

Complete the following tasks before completing the tasks in the related topic, “Configuring Prime Infrastructure to Use the NFS Backup Server”. You will need the information and access privileges explained in “Before You Begin NFS Backup Configuration”.

- 
- Step 1** Log in to the NFS server with a user name that has root privileges, or assume root privileges on the server.
- Step 2** While in root mode, start the NFS service:
- ```
[root@server~]# service portmap start
[root@server~]# service nfs start
```
- Step 3** If they do not already exist, create:
- a staging folder to hold temporary files created during backup processing (for example: /localdisk/staging).
 - a storage folder to hold finished backup files (for example: /localdisk/storage).
- Step 4** Using VI or another editor, modify the NFS server’s /etc/exports file to expose the staging and storage folders to the Prime Infrastructure server that will access them. You can do this by adding lines to the file:
- ```
stagingPath AccessingIP(rw, sync, no_subtree_check)
storagePath AccessingIP(rw, sync, no_subtree_check)
```
- Where:
- *stagingPath* is the path name of the staging folder you created.
  - *storagePath* is the path name of the storage folder you created.
  - *AccessingIP* is the IP address of the Prime Infrastructure server that will be accessing the staging and storage folders on the NFS backup server. This can also be a group of IP addresses under a specified subnet (for example: 172.18.123.0/16).
- Step 5** Load the modified exports file into the Prime Infrastructure server’s running configuration:
- ```
[root@server~]# exportfs -a
```
- Step 6** Disable firewall checks for the staging and storage folders, and start the portmap service. For example:
- ```
[root@server~]# service iptables stop
[root@server~]# chkconfig iptables off
[root@server~]# service portmap start
```
- Step 7** Make the staging and storage folders writable, then exit:
- ```
[root@server~]# chmod 777 stagingPath
[root@server~]# chmod 777 storagePath
[root@server~]# exit
```
-

Related Topics

- [Before You Begin NFS Backup Configuration](#)
- [Configuring Prime Infrastructure to Use the NFS Backup Server](#)

Configuring Prime Infrastructure to Use the NFS Backup Server

Complete the following tasks only after the NFS backup server is properly configured, as explained in the related topic “Configuring the NFS Backup Server”. You will need the information and access privileges explained in “Before You Begin NFS Backup Configuration”.

-
- Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).
- Step 2** Assume root privileges on the server. For example:
- ```
PIServer/admin# root
Enter root password:
Starting root bash shell...
ade #
```
- Step 3** While in root mode, enable NFS communications with the NFS backup server:
- ```
ade# service nfs start
ade# service portmap start
```
- Step 4** Check whether you are able to see the shared stage and storage folders on the remote NFS server from the Prime Infrastructure server:
- ```
ade# rpcinfo -p RemoteServerIP
```
- where *RemoteServerIP* is the IP address of the NFS server hosting the staging and storage folders (for example: *198.168.1.1*).
- If the output of this command does not show the NFS service and its associated ports on the NFS server, you may need to restart the NFS service on the Prime Infrastructure server:
- ```
ade# service nfs restart
```
- Step 5** Exit root mode, then enter config mode and set up Prime Infrastructure to stage its backups on the NFS server:
- ```
ade# exit
PIServer/admin# configure terminal
PIServer/admin(config)# backup-staging-url nfs://RemoteServerIP:/stagingPath
```
- where *stagingPath* is the path name of the staging folder on the NFS server (for example: */localdisk/staging*).
- For example:
- ```
ade# exit
PIServer/admin# configure terminal
PIServer/admin(config)# backup-staging-url nfs://198.168.1.1:/localdisk/staging
```
- Step 6** Set up a named Prime Infrastructure repository to store backups on the NFS server, then exit:
- ```
PIServer/admin(config)# repository RepositoryName
PIServer/admin(config-Repository)# url nfs://RemoteServerIP:/storagePath
PIServer/admin(config-Repository)# exit
PIServer/admin(config)# exit
```

Where:

- **RepositoryName** is the name of the Prime Infrastructure repository (for example: NFSRepo).
- **storagePath** is the path name of the NFS server's storage folder (for example: /localdisk/storage).

For example:

```
PIServer/admin(config)# repository NFSRepo
PIServer/admin(config-Repository)# url nfs://198.168.1.1:/localdisk/storage
PIServer/admin(config-Repository)# exit
PIServer/admin(config)# exit
```

**Step 7** When taking backups at the command line, specify the new repository name in the backup command.

For example:

```
PIServer/admin# backup MyBackupFileName repository MyRepo application NCS
```

To perform backups automatically, specify the new repository name in the Prime Infrastructure web interface.

---

#### Related Topics

- [Configuring the NFS Backup Server](#)
- [Before You Begin NFS Backup Configuration](#)
- [Connecting Via CLI](#)
- [Specifying Automatic Application Backup Repositories](#)

## Using Remote SFTP Backup Repositories

You can create backup repositories on a remote SFTP server and configure the Prime Infrastructure server to use them.

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

- Has an IP address accessible from the Prime Infrastructure server.
- Has a user with write access to the SFTP server disk.
- Has a local shared folder where the backups will be stored.

Other than these requirements, no other configuration is needed on the SFTP backup server.

We recommend using remote NFS repositories.

For the SFTP server details to appear in the Backup Repository drop down list in UI, you should configure the SFTP server using CLI. You can configure the SFTP server only using CLI.



---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter configuration mode:

```
PIServer/admin# configure terminal
```

**Step 3** Configure a symbolic link to the remote SFTP server:

```
PIServer/admin(config)# repository repositoryName
```

```
PIServer/admin(config-Repository)# url sftp://RemoteServerIP//sharedfolder
```

```
PIServer/admin(config-Repository)# user userName password plain userPassword
```

```
PIServer/admin(config-Repository)# exit
```

```
PIServer/admin(config)# exit
```

Where:

- **repositoryName** is the name of the repository (for example: MyRepo or PrimeInfrastructure).
- **RemoteServerIP** is the IP address of the SFTP server hosting the shared backup folder. Note that the example above specifies an absolute path to the shared folder. To specify a relative path to the shared folder, use only one slash in the URL. For example: **url sftp://RemoteServerIP//sharedfolder**
- **sharedfolder** is the name of the shared backup folder on the SFTP server.
- **userName** is the name of a user with write privileges to the repository on the SFTP server.
- **userPassword** is the corresponding password for that user.

**Step 4** Verify creation of the symbolic link:

```
PIServer/admin# show repository repositoryName
```

**Step 5** When taking backups at the command line, specify the new repository as the repository name in the backup command. For example:

```
PIServer/admin# backup MyBackupFileName repository MyRepo application NCS
```

If you want to perform backups automatically, select the repository name you created as the repository name in the Prime Infrastructure web interface.

---

#### Related Topics

- [Connecting Via CLI](#)
- [Using Remote NFS Backup Repositories](#)
- [Taking Application Backups](#)
- [Taking Appliance Backups](#)
- [Specifying Automatic Application Backup Repositories](#)

## Using Remote FTP Backup Repositories

You can create backup repositories on a remote FTP server and configure the Prime Infrastructure server to use them.

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 (FTP 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.
- Has a password of 16 characters or less.

Other than these requirements, no other configuration is needed on the FTP backup server.

We recommend remote NFS repositories.

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter configuration mode:

```
PIServer/admin# configure terminal
```

**Step 3** Configure a symbolic link to the remote FTP server:

```
PIServer/admin(config)# repository repositoryName
```

```
PIServer/admin(config-Repository)# url ftp://RemoteServerIP//sharedfolder
```

```
PIServer/admin(config-Repository)# user userName password plain userPassword
```

```
PIServer/admin(config-Repository)# exit
```

```
PIServer/admin(config)# exit
```

Where:

- **repositoryName** is the name of the repository (for example: MyRepo Or PrimeInfrastructure).
- **RemoteServerIP** is the IP address of the FTP server hosting the shared backup folder.
- **sharedfolder** is the name of the shared backup folder on the FTP server.
- **userName** is the name of a user with write privileges to the repository on the FTP server.
- **userPassword** is the corresponding password for that user. This password must be 16 characters or less.

**Step 4** Verify creation of the symbolic link:

```
PIServer/admin# show repository repositoryName
```

**Step 5** When taking backups at the command line, specify the new remote FTP repository as the repository name in the backup command. For example:

```
PIServer/admin# backup MyBackupFileName repository MyRepo application NCS
```

If you want to perform backups automatically, select the repository name you created as the repository name in the Prime Infrastructure web interface.

---

### Related Topics

- [Connecting Via CLI](#)

- [Using Remote NFS Backup Repositories](#)
- [Taking Application Backups](#)
- [Taking Appliance Backups](#)
- [Specifying Automatic Application Backup Repositories](#)

## Taking Backups From the Command Line

You can take application or appliance backups at any time using the Prime Infrastructure **backup** command.

### Related Topics

- [Taking Application Backups](#)
- [Taking Appliance Backups](#)

## Taking Application Backups

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Display the list of backups:

```
PIServer/admin# show repository repositoryName
```

where *repositoryName* is the repository on which you want to store the backup.

**Step 3** Back up the application:

```
PIServer/admin# backup filename repository repositoryName application NCS
```

where *filename* is the name that you want to give the application backup file (for example, myBackup). The character length of the file name is 26. Other information is appended to the filename automatically, as explained in “Backup Filenames”.

**Step 4** (Optional): Enter the password.

---

### Related Topics

- [Connecting Via CLI](#)
- [Backup Repositories](#)
- [Backup Filenames](#)
- [Using Remote NFS Backup Repositories](#)
- [Using Remote FTP Backup Repositories](#)
- [Taking Appliance Backups](#)

## Taking Appliance Backups

Users of Prime Infrastructure version 3.0 should be aware that appliance backups taken from a 3.0 virtual or physical appliance can be restored to a version 3.0 virtual or physical appliance only.

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Display the list of appliance backups:

```
PIServer/admin# show repository repositoryName
```

where *repositoryName* is the repository on which you want to store the appliance backup.

**Step 3** Back up the appliance:

```
PIServer/admin# backup filename repository repositoryName
```

where *filename* is the name that you want to give the appliance backup file (for example, myBackup). The character length of the file name is 26. Other information is appended to the filename automatically, as explained in “Backup Filenames”

---

### Related Topics

- [Connecting Via CLI](#)
- [Backup Repositories](#)
- [Backup Filenames](#)
- [Using Remote NFS Backup Repositories](#)
- [Using Remote FTP Backup Repositories](#)
- [Taking Application Backups](#)

# Restoring From Backups

You must use the Prime Infrastructure **restore** command to restore from backups. You can restore to the same host that you were using, or to a different host.

You cannot restore portions of a backup.

Note that you must always stop the server before triggering the restore (see “Restarting Prime Infrastructure” in related topics).

## .Related Topics

- [Restarting Prime Infrastructure](#)
- [Backup and Restore Concepts](#)
- [Using Remote Backup Repositories](#)
- [Restoring From Application Backups](#)
- [Restoring From Appliance Backups](#)
- [Migrating to Another Virtual Appliance Using Backup and Restore](#)
- [Migrating to Another Physical Appliance Using Backup and Restore](#)
- [Recovering From Failed Restores](#)

## Restoring From Application Backups

Prime Infrastructure supports restoring from backups of the following releases:

- Prime Infrastructure versions 2.2, 2.2.1, 2.2.2
- Prime Infrastructure 2.2.1 Technology Packages:
  - Data Center Technology Package 1.0.0 for Cisco Prime Infrastructure 2.2.1
  - Wireless Technology Package 1.0.0 for Cisco Prime Infrastructure 2.2.1
- Prime Infrastructure versions 2.2.X and all Cisco.com patches and point patches
- Prime Infrastructure version 3.0

You can restore an application backup from a smaller to a larger OVA installation. You cannot restore an application backup taken from a larger OVA to a smaller OVA (see the related topic “Migrating to Another OVA Using Backup and Restore”).

Users of Prime Infrastructure version 3.0 should know that application backups taken from a version 2.2, 2.2.x, or 3.0 virtual or physical appliance can be restored to a version 3.0 virtual or physical appliance only.

---

**Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

**Step 2** Enter the following command to display the list of application backups:

```
PIServer/admin# show repository repositoryName
```

Where *repositoryName* is the repository from which you want to restore the backup.

**Step 3** Identify the application backup file you want to restore and then enter the following command to restore from that file:

```
PIServer/admin# restore filename repository repositoryName application NCS
```

Where *filename* is the name of the application backup file from which you want to restore.

**Step 4** When the restore is complete, synchronize your device inventory:

- a. Select **Inventory > Device Management > Network Devices**.
- b. Select the checkbox next to **Device Name** to select all devices.
- c. Click **Sync**.

**Step 5** If you had the Compliance Services feature enabled before the restore, you will need to re-enable it after the restore is complete (see “Enabling Compliance Services” in Related Topics)

---

#### Related Topics

- [Connecting Via CLI](#)
- [Backup Types](#)
- [Backup Repositories](#)
- [Backup Filenames](#)
- [Restoring From Appliance Backups](#)
- [Migrating to Another Virtual Appliance Using Backup and Restore](#)
- [Recovering From Failed Restores](#)
- [Enabling Compliance Services](#)

## Restoring From Appliance Backups

Prime Infrastructure 3.0 supports restoring an appliance backup taken from Prime Infrastructure version 3.0 only. Restoring appliance backups taken from an older version of the product (such as 2.2 or 2.2.X or 2.2.X + Cisco.com patches) is not supported in release 3.0. However, you can use an *application* backup to restore an older version of Prime Infrastructure to Prime Infrastructure 3.0.

The following steps show how to change a restored Prime Infrastructure host's IP address, subnet mask, default gateway and host name. You will need to do this when the restored host is:

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

Although not required, we recommend changing the host name under either condition.

- 
- Step 1** Open a CLI session with the Prime Infrastructure server (see [Connecting Via CLI](#)).
- Step 2** Enter the following command to display the list of appliance backups:
- ```
PIServer/admin# show repository repositoryName
```
- Where *repositoryName* is the repository from which you want to restore the backup.
- Step 3** Identify the appliance backup file that you want to restore and then restore from that file:
- ```
PIServer/admin# restore filename repository repositoryName
```
- Where *filename* is the name of the appliance backup file from which you want to restore.
- Step 4** Once the restore is complete: If needed, stop the Prime Infrastructure server and use the command line to change the IP address, subnet mask, default gateway, or host name on the restored server. You will also need to write the changes to the server's running configuration and reboot the physical or virtual appliance. For example:
- ```
PIServer/admin# ncs stop
PIServer/admin# configure terminal
PIServer/admin(config)# int GigabitEthernet 0
PIServer/admin(config-GigabitEthernet)# ip address IPAddress subnetMask
PIServer/admin(config-GigabitEthernet)# exit
PIServer/admin(config)# ip default-gateway GatewayIP
PIServer/admin(config)# hostname hostname
PIServer/admin(config)# exit
PIServer/admin# write mem
PIServer/admin# ncs start
PIServer/admin# exit
```
- Reboot the virtual or physical appliance to write these changes to the operating system.
- Step 5** When the restore is complete, synchronize your device inventory:
- Select **Inventory > Device Management > Network Devices**.
 - Select the checkbox next to **Device Name** to select all devices.
 - Click **Sync**.
- Step 6** If you had the Compliance Services feature enabled before the restore, you will need to re-enable it after the restore is complete (see "Enabling Compliance Services" in Related Topics)
-

Related Topics

- [Connecting Via CLI](#)
- [Backup Types](#)
- [Backup Repositories](#)
- [Backup Filenames](#)
- [Restoring From Application Backups](#)
- [Migrating to Another Physical Appliance Using Backup and Restore](#)
- [Recovering From Failed Restores](#)
- [Enabling Compliance Services](#)

Migrating to Another Virtual Appliance Using Backup and Restore

You will need to migrate your Prime Infrastructure data from an existing virtual appliance (OVA server installation) to a new one whenever you want to:

- Replace the old server entirely, such as after a catastrophic hardware failure. In this case, you can use your old installation media to re-create the new host on a replacement server, then migrate your application data from the old host to the new host.
- Migrate to a larger or more powerful server, so you can use Prime Infrastructure to manage more of your network. In this case, you will want to ensure that you have the OVA installation file and install it on the new server using the larger installation option before retiring the older, smaller one. You can then migrate your application data from the old host.

In both cases, it is relatively easy to migrate your old data to the new virtual appliance by restoring to the new host an appliance or application backup taken from the old host.

-
- | | |
|---------------|---|
| Step 1 | If you have not already done so, set up a remote backup repository for the old host, as explained in the related topic, “Using Remote Backup Repositories”. |
| Step 2 | Take an application backup of the old host on the remote repository (see “Taking Application Backups”). |
| Step 3 | Install the new host (installation steps are in the <i>Cisco Prime Infrastructure Quick Start Guide</i>). |
| Step 4 | Configure the new host to use the same remote backup repository as the old host (see “Using Remote Backup Repositories”). |
| Step 5 | Restore the application backup on the remote repository to the new host (see “Restoring From Application Backups”). |
-

Related Topics

- [Using Remote Backup Repositories](#)
- [Cisco Prime Infrastructure Quick Start Guide](#)
- [Taking Application Backups](#)
- [Using Remote Backup Repositories](#)
- [Restoring From Application Backups](#)

Migrating to Another Physical Appliance Using Backup and Restore

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

- Replace the old appliance entirely, such as after a catastrophic hardware failure. In this case, you can order a replacement appliance, then migrate your data from the old appliance to the new appliance.
- Migrate to a newly installed appliance.

In both cases, it is relatively easy to migrate your old data to the new appliance by restoring to the new appliance an appliance or application backup from the old host.

-
- Step 1** If the old appliance is still functional:
- a. If you have not already done so, set up a remote backup repository for the old appliance (see “Using Remote Backup Repositories” in Related Topics).
 - b. Take an appliance or application backup of the old appliance on the remote repository (see “Taking Appliance Backups” or “Taking Application Backups”, as appropriate).
- Step 2** Configure the new appliance to use the same remote backup repository as the old appliance (see “Using Remote Backup Repositories”).
- Step 3** Restore the appliance or application backup on the remote repository to the new appliance (see “Restoring From Appliance Backups” or “Restoring From Application Backups”, as appropriate). Be sure to follow the procedure appropriate for the type of backup you are restoring. For example: If you took an application backup from the old appliance, you must restore it using the procedure for restoring application backups, not appliance backups.
-

Related Topics

- [Using Remote Backup Repositories](#)
- [Taking Application Backups](#)
- [Taking Appliance Backups](#)
- [Restoring From Appliance Backups](#)
- [Restoring From Application Backups](#)

Recovering From Failed Restores

You may sometimes find that a restore does not complete, or reports a failure. Whenever a restore fails, you run the risk of database corruption, which can prevent further restoration or re-installation. Perform the following steps before attempting another restore or re-installation.

Step 1 Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

Step 2 Enter the following command to reset the corrupted database:

```
PIServer/admin# ncs run reset db
```

Related Topics

- [Connecting Via CLI](#)
- [Restoring From Application Backups](#)
- [Restoring From Appliance Backups](#)

Managing Disk Space Issues During Backup and Restore

If you are experiencing issues with disk space *during* a backup or restore, we suggest that you either:

- Use the VMware **Edit Settings** feature to increase the amount of disk space allocated to the virtual machine (see “Modifying VM Resource Allocation Using VMware vSphere Client” in Related Topics).

If you are using VMware ESXi 5.5 or later, use the vSphereWeb Client to adjust this setting (see the VMware document “Configuring Virtual Machine Hardware in the vSphere Web Client”).

- Use the method explained in “Migrating to Another OVA Using Backup and Restore” (or “Migrating to Another Appliance Using Backup and Restore”) to move your installation to a server with adequate disk space.

If you are unable to create a backup *after* a restore of your existing system, follow the steps explained in “Compacting the Prime Infrastructure Database” to free disk space and create a successful backup.

If you are still unable to create a backup after using the **ncs cleanup** command, set up and use a remote repository (using FTP, SFTP, or NFS) for your backups, as explained in “Using Remote Backup Repositories”.

Related Topics

- [Modifying VM Resource Allocation Using VMware vSphere Client](#)
- [Configuring Virtual Machine Hardware in the vSphere Web Client](#)
- [Migrating to Another Virtual Appliance Using Backup and Restore](#)
- [Migrating to Another Physical Appliance Using Backup and Restore](#)
- [Compacting the Prime Infrastructure Database](#)
- [Using Remote Backup Repositories](#)
- [Managing Disk Space Issues](#)

Using Backup and Restore with Operations Center

Prime Infrastructure instances running Operations Center support restores of application backups taken using the CLI from Prime Infrastructure versions 2.2, 2.2.X, or 3.0 only.

You cannot schedule automatic application backups from the Prime Infrastructure instance running Operations Center.

If you are using Operations Center to manage Prime Infrastructure servers running version 2.2 or 2.2.X: Please ensure these instances are upgraded to Prime Infrastructure 3.0 before attempting to take an application backup of the Prime Infrastructure server running Operations Center.

Related Topics

- [Using Remote Backup Repositories](#)
- [Restoring From Application Backups](#)



Maintaining Network Health

- [Configuring Alarm and Event Settings](#)
- [Enabling Change Audit Notifications](#)
- [Configuring Syslog Message Receivers for System Changes](#)
- [Downloading and Emailing Error Logs](#)
- [Enabling SNMP Tracing](#)
- [Changing Syslog Logging Options](#)
- [Changing Logging Options to Enhance Troubleshooting](#)
- [Configuring Technical Support Request Settings](#)

Configuring Alarm and Event Settings

- [Specifying Alarm Clean Up and Display Options](#)
- [Changing Alarm Severities](#)
- [Changing the Auto Clear Interval](#)

Specifying Alarm Clean Up and Display Options

The **Administration > Settings > System Settings > Alarms and Events** page enables you to specify when and how to clean up, display and email alarms.

-
- Step 1** Choose **Administration > Settings > System Settings > Alarms and Events > Alarms and Events**.
- Step 2** 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.

Cisco Prime Infrastructure deletes old alarms nightly, as part of normal data cleanup tasks, and checks the storage size of the database alarm table once an hour. When the alarm table exceeds the 300,000 limit, Prime Infrastructure deletes the oldest cleared alarms until the alarm table size is within the limit. 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 the limit.

Step 3 In the **Syslog Cleanup Options** area, in the **Delete all syslogs after** text box, enter the number of days after which all aged syslogs are to be deleted.

Step 4 Modify the **Alarm Display Options** as needed:

- Hide acknowledged alarms—When the check box is selected, Acknowledged alarms do not appear in the Alarm 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 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 device name to alarm messages—Select the check box to add the name of the device to alarm messages.

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

Step 5 Modify the alarm **Failure Source Pattern**:

- Select the category you need to customize and click **Edit**.
- Select the failure source pattern from the options available and click **OK**.

The alarms generated for the selected category will have the customized pattern that was set.

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

- Add Prime Infrastructure address to email notifications—Select the check box to add the Prime Infrastructure address to email notifications.
- 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.
- Enable AP count threshold alarm option will be enabled by default, to set the Controller access point count 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. Existing alarms will remain unchanged.

- Step 1** Choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear**.
- Step 2** Expand the categories available under the **Event Types** column, or search for the event type you want by entering all or part of the event text in the Event Types search field just below the column heading.
- Step 3** Change the event severity by performing one of the following tasks:
- Click on the **Severity** field and select a severity level from the drop-down list.
 - Select the check box of the event type whose severity level you want to change, click **Severity Configuration**, and choose a severity level from the **Configure Severity Level** drop-down list, and click **OK**.

The available severity level options are: **Critical**, **Major**, **Minor**, **Warning**, **Informational**, or **Reset to Default**.

Changing the Auto Clear Interval

You can change the auto clear interval for any alarm condition. The alarm generated for the specific alarm condition will be auto cleared in the interval specified. To clear alarms automatically, follow these steps:

-
- Step 1** Choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear**.
- Step 2** Expand the categories available under the **Event Types** column, or search for the event type you want by entering all or part of the event text in the Event Types search field just below the column heading.
- Step 3** Change the Auto Clear Interval by performing one of the following tasks:
- Click on the **Auto Clear Duration** field and enter the duration after which you need to clear the alarm.
 - Select the check box of the event type whose auto clear duration you want to change, click **Alarm Auto Clear**, enter the duration after which you need to clear the alarm, and click **OK**.
-

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 select the **Enable Change Audit 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 > Settings > System Settings > Mail and Notification > Change Audit Notification**.
- Step 2** Select the **Enable Change Audit Notification** check box to enable notifications.
- Step 3** Click **Save**.
-

Configuring Syslog Message Receivers for System Changes

In addition to sending JMS notifications, Prime Infrastructure can send syslog messages to specified receivers to notify you of changes in the following Prime Infrastructure features:

- Device management
- Device community strings and credentials
- User management
- Configuration templates management
- Monitoring templates management
- Job management
- Logins and logouts
- Image distribution
- Configuration changes
- Inventory changes

You can specify as many receivers as you wish for these specialized syslog messages.

If you have configured syslog message notification receivers but are still not receiving syslogs, you may need to change the anti-virus or firewall settings on the destination syslog receiver to permit reception of syslog messages.

-
- Step 1** Choose **Administration > Settings > System Settings > Mail and Notification > Change Audit Notification**.
- Step 2** Click the **Add** button (+) to specify a syslog receiver.
- Step 3** In the Syslog Receiver(s) pane, enter the **IP Address**, **Protocol** and **Port Number** of the syslog receiver.
- Step 4** Click **Save** to save your changes.
- Step 5** Repeat these steps as needed to specify additional syslog receivers.
- To change or delete a syslog message notification receiver: Select it, then click the **Edit** or **Delete (X)** button.
-

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 that it receives. You can download and email the logs to use in troubleshooting Prime Infrastructure:

-
- Step 1** Choose **Administration > Settings > 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 entry 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.

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**.

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.

-
- Step 1** Choose **Administration > Settings > Logging > SNMP Logging Options**.
 - Step 2** Select the **Enable SNMP Trace** check box to enable sending SNMP messages and traps between controllers and Prime Infrastructure, then select the **Display Values** check box to see the SNMP message values.
 - Step 3** Configure the IP addresses on which to trace the SNMP traps. You can add up to 10 IP addresses in the text box.
 - Step 4** You can configure the maximum SNMP log file size and the maximum number of SNMP log files to retain.
 - Step 5** Click **Save**.
-

Changing Syslog Logging Options

-
- Step 1** Choose **Administration > Settings > Logging > Syslog Logging Options**.
- Step 2** Select the **Enable Syslog** check box to enable collecting and processing of system logs.
- Step 3** In **Syslog Host**, enter the IP address of the interface from which the message is to be transmitted.
- Step 4** Choose the **Syslog Facility**. You can choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.
- Step 5** Click **Save**.
-

Changing Logging Options to Enhance Troubleshooting

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

-
- Step 1** In Converged view, choose **Administration > Settings > Logging**.
- Step 2** From the **Message Level** drop-down list, choose **Trace**.
- Step 3** Select 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* for a long period of time can adversely affect performance.

Related Topics

- [Changing Mobility Service Engine Logging Options](#)
- [MAC Address-Based Logging](#)
- [Downloading Mobility Services Engine Log Files](#)

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 Choose **Administration > Settings > Logging**, 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 2 Select the **Enable** check box next to each element listed in that section to begin logging its events.

Step 3 Select the **Enable** check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.

Step 4 To download log files from the server, click **Download Logs**. See “Downloading Mobility Services Engine Log Files” for more information.

Step 5 In the Log File Parameters area, 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 6 In the MAC Address Based Logging Parameters area, 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 choosing the MAC address from the list and clicking **Remove** (see “MAC Address-Based Logging” in Related Topics).

Step 7 Click **Save** to apply your changes.

Related Topics

- [Changing Logging Options to Enhance Troubleshooting](#)
- [MAC Address-Based Logging](#)
- [Downloading Mobility Services Engine Log Files](#)

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.

Related Topics

- [Changing Logging Options to Enhance Troubleshooting](#)
- [Changing Mobility Service Engine Logging Options](#)
- [Downloading Mobility Services Engine Log Files](#)

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** Choose **Services > Mobility Services > Mobility Services Engines**.
 - Step 2** Select the name of the mobility services engine to view its status.
 - Step 3** From the left sidebar menu, choose **System > Logs**.
 - Step 4** In the Download Logs area, 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.
-

Related Topics

- [Changing Logging Options to Enhance Troubleshooting](#)
- [Changing Mobility Service Engine Logging Options](#)
- [MAC Address-Based Logging](#)

Configuring Technical Support Request Settings

You can customize the settings for creating a support case with Cisco Technical Support.

For details on creating a support case, see “Opening a Support Case” in Related Topics.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Support Request**.
- Step 2** Select the type of interaction you prefer:
- **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.
-

Related Topics

- [Opening a Support Case](#)



Managing Data Collection and Retention

One of the roles of an administrator is to manage Cisco 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 related data management tasks.

Related Topics

- [Specifying Data Retention by Category](#)
- [Specifying Data Retention By Database Table](#)
- [About Performance Data Retention](#)
- [Specifying Client Data Retrieval and Retention](#)
- [About Historical Data Retention](#)
- [Enabling Data Deduplication](#)
- [Controlling Report Storage and Retention](#)
- [Specifying Inventory Collection After Receiving Events](#)
- [Controlling Configuration Deployment Behavior](#)
- [Controlling Data Collection Jobs](#)
- [Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure](#)

Specifying Data Retention by Category

Administrators can use Prime Infrastructure's Data Retention page to configure retention periods for the following data categories:

- **Trend Data:** Hourly, daily and weekly aggregated data.
- **Device Health** and **System Health** data: Hourly, daily and weekly data.
- **Performance** data: Short, medium and long-term data.
- **Network Audit** data.

Limiting the amount of data retained can help improve performance and disk storage characteristics. However, for the best interactive graph data views, Cisco recommends that keep the default values.

You can also specify data retention for individual database tables, using maximum age and record attributes. For details, see "Specifying Data Retention By Database Table" in Related Topics.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Data Retention**.
- Step 2** Expand the data category for which you want to specify retention-period values.
- Step 3** Enter the new values as needed.
- Step 4** Click **Save**.
-

Related Topics

- [Specifying Data Retention By Database Table](#)
- [About Historical Data Retention](#)
- [Specifying Client Data Retrieval and Retention](#)
- [About Historical Data Retention](#)

Specifying Data Retention By Database Table

Administrators can use the “Other Data Retention Criteria” section of the Data Retention page to configure retention periods for specific Prime Infrastructure database tables. You specify the retention period using the following attributes:

- **Age (in hours):** Specifies the maximum data retention period in hours for all records in the database.
- **Max Records:** Specifies the maximum number of records to retain in a particular database table. A Max Records value of NA means that the only retention criteria considered is the Age attribute.

The section is categorized into multiple subsections. Each subsection list each database table name, along with the current Age and Max Records used to determine whether an individual record in the table will be retained or discarded. The page also lists the table Age Attribute used to compute the age of the data in the table. The Optical Devices category is not applicable for Prime Infrastructure.

Cisco strongly recommends that you consult with Cisco Technical Assistance Center before changing the values for any of the tables in this section. Doing so without help may affect system performance negatively.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Data Retention**.
 - Step 2** Expand the **Other Data Retention Criteria** section.
 - Step 3** Expand the database table subsection for which you want to specify Age and Max Records values.
 - Step 4** Click on the database table listing and enter the new values as needed.
 - Step 5** Click **Save**.
-

Related Topics

- [Specifying Data Retention by Category](#)
- [About Historical Data Retention](#)
- [Specifying Client Data Retrieval and Retention](#)
- [About Historical Data Retention](#)

About Performance Data Retention

When you choose **Administration > Settings > System Settings > General > Data Retention**, you can modify the retention periods for performance data under **Performance Data Retain Periods**. The performance retention values you specify determine the information that is displayed in performance reports and performance dashboards.

For example, if you don't need any historical data older than 7 days, you can modify the performance data retention values as follows:

- Short-term Data Retain Period—1 day
- Medium term Data Retain Period—3 days
- Long term Data Retain Period—7 days

If you specify these settings, all data displayed in performance reports and performance dashboards data will be for the previous 7 days only. When you generate a performance report (for example, **Reports > Reports > Report Launch Pad > Device > Device Health**), even if you select a Reporting Period longer than the last 7 days, the report contains data from the last 7 days only because that is all the data you've selected to retain.

Similarly, if you view a performance dashboard (for example, **Dashboard > Overview > General > Service Assurance**) and select a Time Frame longer than one week, the dashboard contains data from the last 7 days only because that is all the data you've selected to retain.

For device and interface performance data, Prime Infrastructure uses the values specified in the fields under **Device Health Data Retain Periods**.

Related Topics

- [About Historical Data Retention](#)
- [Specifying Data Retention by Category](#)

Specifying Client Data Retrieval and Retention

Administrators can use Prime Infrastructure's Client page to configure parameters affecting retention of data on network clients, including:

- Data on disassociated clients. The default is seven days, and this applies irrespective of whether the clients will ever attempt to associate again.
- Data on client session histories. You can also specify the maximum number of session entries to keep, specified as rows in the Prime Infrastructure database.
- Cached client host names retrieved from a DNS server.

In addition to these data-retention options, the page allows you to enable and disable options to:

- Automatically troubleshoot clients using a diagnostic channel when traps are received from these clients.
- Automatically retrieve client host names from a DNS server.
- Poll clients when traps or syslogs are received from these clients
- Save as Prime Infrastructure events routine client association and disassociation traps and syslogs. This option is disabled by default, to avoid Prime Infrastructure performance problems on large networks during periods (such as network setup) when these kinds of traps and syslogs may be numerous. You may want to enable this option at all other times.
- Save all 802.1x and 802.11 client authentication-failure traps as Prime Infrastructure events. This option is disabled by default, to avoid Prime Infrastructure performance problems on large networks during periods (such as network setup) when these kinds of traps and syslogs may be numerous. You may want to enable this option if your network is stable.

-
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**.
- Step 2** Under Data Retention, modify the values as required.
- Step 3** Click **Save**.
-

Related Topics

- [About Historical Data Retention](#)
- [About Historical Data Retention](#)
- [Specifying Data Retention by Category](#)
- [About Historical Data Retention](#)

About Historical Data Retention

Prime Infrastructure retains two types of historical data:

1. 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 retention period (and other settings) for each non-aggregated data collection task. For example, you can define the retention period for client association history in **Administration > Settings > System Settings > Client**. By default, the retention period for all non-aggregated historical data is 31 days or 1 million records. This retention period can be increased to 365 days.
2. Aggregated historical data—Numeric data that can be gathered as a whole and summarized as minimums, maximums, or averages. Client count is one example of aggregated historical data.

Types of aggregated historical data include:

- Trend: This includes wireless-related historical information such as client history, AP history, AP utilization, and client statistics.
- Device health: This includes SNMP polled data for wired and wireless devices, such as device availability, and CPU, memory, and interface utilization, and QoS.
- Performance: This includes Assurance data such a traffic statistics, application metrics, and voice metrics.
- Network audit records: This includes audit records for configuration changes triggered by users, and so on.
- System health records: This includes most data shown on Prime Infrastructure administrator dashboards.

The retention periods for these aggregation types are defined as Default, Minimum, and Maximum (see the table below). Use the **Administration > Settings > System Settings > General > Data Retention** page to define aggregated data retention periods. Aggregation types include hourly, daily, and weekly.

Table 7-1 Retention Periods for Aggregated Historical Data

| Trend Data Retention Periods | | | |
|---|----------------|----------------|----------------|
| Period | Default | Minimum | Maximum |
| Hourly | 7 days | 1 days | 31 days |
| Daily | 90 days | 7 days | 365 days |
| Weekly | 54 weeks | 2 weeks | 108 weeks |
| Device Health Data Retention Periods | | | |
| Hourly | 15 days | 1 day | 31 days |
| Daily | 90 days | 7 days | 365days |
| Weekly | 54 weeks | 2 weeks | 108 weeks |
| Performance Data Retention Periods | | | |
| Short-Term Data | 7 days | 1 day | 31 days' |
| Medium-Term Data | 31 days | 7 days | 365 days |
| Long-Term Data | 378 days | 2 days | 756 days |

Table 7-1 Retention Periods for Aggregated Historical Data (continued)

| Network Audit Data Retention Period | | | |
|--------------------------------------|----------|---------|----------|
| All audit data | 7 days | 7 weeks | 365 days |
| System Health Data Retention Periods | | | |
| Hourly | 7 days | 1 day | 31 days |
| Daily | 31 days | 7 days | 365 days |
| Weekly | 54 weeks | 7 weeks | 365 days |

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 data for TCP applications
- Traffic analysis data for all applications
- Voice/Video data for RTP applications

Prime Infrastructure stores all data it receives about network elements and protocols, including any duplicate data that it may receive from multiple sources. When you specify authoritative data sources, only the data from the specified sources is displayed when you view a particular location or site.

The Data Deduplication page allows you to specify one or more authoritative data sources at a specific location. 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 choose to have Prime Infrastructure display only the NAM or the NetFlow data for that location.

-
- Step 1** Choose **Services > Application Visibility & Control > Data Deduplication**.
- Step 2** Select the **Enable Data Deduplication** checkbox and click **Apply**. The Data Deduplication page displays the list of your defined location groups.
- Step 3** To automatically detect authoritative sources at all locations, click **Auto-Detect**. If it can identify them, Prime Infrastructure will fill in the address of an authoritative source in the list box under the column listing sources for each of the classes of application data.
- Step 4** To specify authoritative sources for a class of application data at a specific location:
- Click the location group name.
 - Click the drop-down list box under the class of application data for which you want to specify an authoritative source (for example: click in the list box under “Application Response Time”).
 - From the drop-down list, select the data sources you want to specify as authoritative for that location and application data type. Then click **OK**.
 - Click **Save** to save your selections.

Repeat this step as needed for each location and application data type for which you want to specify authoritative data source.

- Step 5** When you are finished, click **Apply** to save your changes.
-

Controlling Report Storage and Retention

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.

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

-
- Step 1** Choose **Administration > Settings > System Settings > Inventory > Inventory**. The Inventory page appears.
- Step 2** 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 3** 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 4** Click **Save**.
-

Controlling Configuration Deployment Behavior

Administrators can choose to have device configurations backed up or rolled back whenever Prime Infrastructure users deploy new device configuration templates. They can also control how Cisco WLC configurations are archived, as explained in the following related topics.

Related Topics

- [Archiving Device Configurations Before Template Deployment](#)
- [Rolling Back Device Configurations on Template Deployment Failure](#)
- [Specifying When and How to Archive WLC Configurations](#)

Archiving Device Configurations Before Template Deployment

With Backup Device Configuration enabled, Prime Infrastructure automatically backs up all device running and startup configurations before deploying new configuration templates.

-
- Step 1** Choose **Administration > Settings > System Settings > Inventory > Configuration**.
- Step 2** Select the **Backup Device Configuration** check box.
- Step 3** Click **Save**.
-

Related Topics

- [Controlling Configuration Deployment Behavior](#)

Rolling Back Device Configurations on Template Deployment Failure

With **Rollback Configuration** enabled, Prime Infrastructure automatically rolls back each device to its last archived running and startup configurations when any attempt to deploy a new configuration template to the device has failed.

-
- Step 1** Choose **Administration > Settings > System Settings > Configuration**.
- Step 2** Select the **Rollback Configuration** check box.
- Step 3** Click **Save**.
-

Related Topics

- [Controlling Configuration Deployment Behavior](#)

Specifying When and How to Archive WLC Configurations

By default, Prime Infrastructure keeps a backup archive of running configurations for each device running Cisco Wireless LAN Controller (WLC) software whenever it:

- Collects initial out-of-box inventory for these devices
- Receives notification of a configuration change event for these devices

Configuration archiving is supported for devices running Cisco WLC software only. Only running configurations are archived (startup configurations are excluded).

You can change many of the basic parameters controlling Cisco WLC configuration archiving, including:

- The maximum timeout on all Cisco WLC configuration operations (fetch, archive or rollback).
- The maximum time to wait before updating the Cisco WLC configuration archive summary information.
- Whether or not to archive configurations at initial inventory collection, after each inventory synchronization, and on receipt of configuration change events.
- Whether or not to mask security information when exporting archived configurations to files.
- The maximum number of archived configurations for each device and the maximum number of days to retain them.
- The maximum number of thread pools to devote to the archive operation. Increasing the default can be helpful with Prime Infrastructure performance during archiving of changes involving more than 1,000 devices.

You can also tell Prime Infrastructure to ignore for archive purposes any change that involves specified commands on devices of a given family, type, or model. This is useful when you want to ignore insignificant or routine changes in a few parameters on one or many devices.

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

Step 2 On the **Basic** tab, change the basic archive parameters as needed.

Step 3 To specify devices and configuration commands to exclude from archived configurations:

a. Click the **Advanced** tab.

b. In the **Product Family** list, choose the device(s) for which you want to specify configuration commands to exclude.

Use the List/Tree View dropdown, or click the > icons to drill down to individual product types and models for which you want to specify exclude commands.

c. In the **Command Exclude List**, enter (separated by commas) the configuration commands you want to exclude for the currently selected device family, type, or model.

If the device(s) you select has configuration changes and Prime Infrastructure detects that the change is one of the specified commands in the Exclude List, Prime Infrastructure will not create an archived version of the configuration with this change.

d. Click **Save**.

e. To remove a specified set of command exclusions for a device family, type or model, select the device(s) in the Product Family list and click **Reset**.

Related Topics

- [Controlling Configuration Deployment Behavior](#)

Controlling Data Collection Jobs

Prime Infrastructure performs scheduled data collection jobs in the background on a regular basis. You can change each job's schedule, pause or resume it, or execute it immediately.

Disabling or limiting these background data collection jobs 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.

Related Tasks

- [Scheduling Data Collection Jobs](#)
- [Pausing and Resuming Data Collection Jobs](#)
- [Running Data Collection Jobs Immediately](#)
- [About Data Collection Jobs](#)

Scheduling Data Collection Jobs

Data collection jobs run on a regular default schedule, as described in the related topic “About Data Collection Jobs”. You can re-schedule them as needed.

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard > System Jobs**.
- Step 2** Select the category of data collection job you want to re-schedule (e.g., **Inventory, Wireless Poller, or Wireless System**).
- Step 3** Click the check box next to the system job you want to re-schedule.
- Step 4** Click **Edit Schedule** and specify the schedule you want the job to run on.
- You can select the date and time the job is executed. You can choose to have the job recur on a minute, hourly, daily, weekly, monthly or annual basis. You can also specify end times and dates, and total recurrences.
- Step 5** When you are finished, click **Submit**.
-

Related Tasks

- [Controlling Data Collection Jobs](#)
- [Pausing and Resuming Data Collection Jobs](#)
- [Running Data Collection Jobs Immediately](#)
- [About Data Collection Jobs](#)

Pausing and Resuming Data Collection Jobs

You can pause any scheduled data collection job, and resume it if already paused.

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard > System Jobs**.
 - Step 2** Select the category of data collection job you want to pause or resume (e.g., **Inventory**, **Wireless Poller**, or **Wireless System**).
 - Step 3** Click the check box next to the system job you want.
 - Step 4** Click **Pause Series** to stop the job from executing.
If the job is already paused, click **Resume Series** to resume execution on the current schedule.
-

Related Tasks

- [Controlling Data Collection Jobs](#)
- [Scheduling Data Collection Jobs](#)
- [Running Data Collection Jobs Immediately](#)
- [About Data Collection Jobs](#)

Running Data Collection Jobs Immediately

In addition to the steps below, you can run a job immediately by rescheduling it and selecting the time to execute as “Now” (see “Scheduling Data Collection Jobs” in Related Topics).

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard > System Jobs**.
 - Step 2** Select the category of data collection job you want to run (e.g., **Inventory**, **Wireless Poller**, or **Wireless System**).
 - Step 3** Click the check box to select the system job you want to run immediately.
 - Step 4** Click **Run**.
-

Related Tasks

- [Controlling Data Collection Jobs](#)
- [Scheduling Data Collection Jobs](#)
- [Pausing and Resuming Data Collection Jobs](#)
- [About Data Collection Jobs](#)

About Data Collection Jobs

The following tables describe the background data collection jobs Prime Infrastructure performs.

Table 7-2 *Inventory Data Collection Jobs*

| Task Name | Task Status | Default Schedule | Description |
|-------------------------------|-------------|-------------------|--|
| Autonomous AP Inventory | Enabled | 180 minutes | Collects the inventory information for autonomous APs. |
| Switch Inventory | Enabled | Daily at midnight | Collects inventory information for switches. |
| Wireless Controller Inventory | Disabled | Daily at midnight | Collects inventory information for wireless controllers. |

Table 7-3 *Wireless Poller Data Collection Jobs*

| Task Name | Task Status | Default Schedule | Description |
|--|-------------|------------------|--|
| AP Image Pre-Download Status | Disabled | 15 minutes | Allows you to see the Image Pre-download 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 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. |
| 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. |
| 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. |

Table 7-3 Wireless Poller Data Collection Jobs (continued)

| Task Name | Task Status | Default Schedule | Description |
|---------------------------------|-------------|------------------|---|
| Traffic Stream Metrics | Enabled | 8 minutes | Retrieves traffic stream metrics for the clients. |
| Wireless Controller Performance | Enabled | 30 minutes | Collects performance statistics for wireless controllers. |

Table 7-4 Wireless System Data Collection Jobs

| Task Name | Task Status | Default Schedule | Description |
|------------------------------|-------------|------------------|---|
| Interferers | Enabled | 15 minutes | Collects information about the interferers. |
| Mobility Service Performance | Enabled | 15 minutes | Collects information about the performance of mobility service engines. |
| Unmanaged APs | Enabled | 15 minutes | Collects poll information for unmanaged access points. |

Related Tasks

- [Controlling Data Collection Jobs](#)
- [Scheduling Data Collection Jobs](#)
- [Pausing and Resuming Data Collection Jobs](#)
- [Running Data Collection Jobs Immediately](#)

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 choosing **Administration > Settings > System Settings > Background Tasks**, then clicking the hypertext link for that task.

Table 7-5 Background Tasks

| Task Name | Default Schedule | Description | Editable Options |
|----------------------------------|------------------|--|--|
| Appliance Status | 5 minutes | Lets you schedule appliance polling. This task populates the appliance polling details from the Administration > Appliance > Appliance Status page. In addition, this background task populates information such as the performance and fault checking capabilities of the appliance. | Enable—Select this check box to enable appliance status polling. Interval—Enter the interval, in minutes, between polls. The valid range is 1 to 10800 minutes. |
| Autonomous AP Operational Status | 5 minutes | Lets you schedule status polling of autonomous wireless access points. | Enable—Select this check box to enable status polling of autonomous APs. Interval—Valid interval is from 1 to 10080. |

Table 7-5 Background Tasks (continued)

| Task Name | Default Schedule | Description | Editable Options |
|---------------------------------|------------------|---|--|
| Autonomous Client Status | 5 minutes | Lets you schedule status polling of autonomous AP clients. | <p>Enable—Select this check box to enable autonomous client status polling.</p> <p>Interval—Enter the interval, in minutes, between polls. The valid range is 1 to 10800 minutes.</p> |
| Wireless Configuration Audit | Daily at 4 am. | This task performs an audit. It verifies the config for mismatches but does not take actions on it. | <p>Enable—Select this check box to enable configuration synchronization.</p> <p>Enable—Select this check box to enable Network Audit.</p> <p>Enable—Select this check box to enable Security Index calculation.</p> <p>Enable—Select this check box to enable RRM audit.</p> <p>Interval—Enter the interval, in days, between each configuration synchronization. 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> |
| Controller Configuration Backup | Daily at 10 pm | Lets you view controller configuration backup activities. | <p>Enable—Select this check box to enable controller configuration backup.</p> <p>Interval—Enter the interval, in days, between controller configuration backups. The valid range is 1 to 360 days.</p> <p>Time of Day—Enter the time of the day that you want the configuration backup to happen. The valid format is hh:mm AM PM. For example, 12:49 AM.</p> <p>TFTP Server—If selected, also choose in the dropdown the TFTP server to which you want to back up the controller configurations.</p> <p>FTP Server—If selected, enter the user name, password, and port address for the FTP server to which you want to back up the controller configurations.</p> |
| Controller Operational Status | 5 minutes | Lets you schedule controller operational status polling. | <p>Enable—Select this check box to enable controller configuration status polling.</p> <p>Interval—Enter the interval, in minutes, between controller status polls. The valid range is 1 to 10800 minutes.</p> |

Table 7-5 Background Tasks (continued)

| Task Name | Default Schedule | Description | Editable Options |
|-----------------------------------|------------------|---|--|
| Data Cleanup | Daily at 2 am. | Lets you schedule daily data file cleanup. | 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. |
| Device Data Collector | 30 minutes | Lets you schedule data collection based on specified command-line interface (CLI) commands at a configured time interval. | Enabled—Select this check box to enable data collection for a specified controller. Controller IP address—The IP address of the Controller to collect device data from. CLI Commands—Enter the CLI commands, separated by commas, that you want to run on the specified device. Clean Start—Select this check box to enable a clean start before data collection. Repeat—Enter the number of times that you want the data collection to be repeated. Interval—Enter the interval, in days, between each device data collection. The valid range is 1 to 360 days. |
| Guest Accounts Sync | Daily at 1 am. | Lets you schedule guest account polling and synchronization. | Enable—Select this check box to enable guest account synchronization. Interval—Enter the interval, in days, between each guest account synchronization. The valid range is 1 to 360 days. 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. |
| Identity Services Engine Status | 15 minutes | Lets you schedule the Identity Services Engine polling. | Enable—Select this check box to enable Identity Services Engine polling. Interval—Enter the interval, in days, between each Identity Services Engine poll. The valid range is 1 to 360 days. |
| License Status | 4 hours. | Lets you schedule license status polling. | Enable—Select this check box to enable license status polling. Interval—Enter the interval, in days, between each license status poll. The valid range is 1 to 360 days. |
| Lightweight AP Operational Status | 5 minutes. | Lets you schedule Lightweight AP operational status polling. | Enable—Select this check box to enable Lightweight AP Operational Status polling. Interval—Enter the interval, in days, between each Lightweight AP Operational Status poll. The valid range is 1 to 360 days. |

Table 7-5 Background Tasks (continued)

| Task Name | Default Schedule | Description | Editable Options |
|----------------------------------|-----------------------|--|--|
| Lightweight Client Status | 5 minutes. | Lets you discover Lightweight AP clients from the network. | <p>Enable—Select this check box to enable Lightweight Client Status polling.</p> <p>Interval—Enter the interval, in days, between each Lightweight Client Status poll. The valid range is 1 to 360 days.</p> |
| Mobility Service Backup | Every 7 days at 1 am. | Lets you schedule automatic mobility services backups. | <p>Enable—Select this check box to enable automatic mobility service backups.</p> <p>Max UI backups to keep—Enter the maximum number of automatic mobility services backups to keep.</p> <p>Interval—Enter the interval, in days, between each mobility services backup. The valid range is 1 to 360 days.</p> <p>Time of Day—Enter the time of day that you want each mobility services backup to be taken. The valid format is hh:mm AM PM. For example, 12:49 AM.</p> |
| Mobility Service Status | 5 minutes. | Lets you schedule mobility services status polling. | <p>Enable—Select this check box to enable mobility services status polling.</p> <p>Interval—Enter the interval, in days, between each mobility services status poll. The valid range is 1 to 360 days.</p> |
| Mobility Service Synchronization | 60 minutes. | Lets you schedule mobility services synchronization. | <p>Out of Sync Alerts—Select this check box to enable out-of-sync alerts.</p> <p>Smart Synchronization—Select this check box to enable smart synchronization.</p> <p>Interval—Enter the interval, in minutes, between each mobility services synchronization. The valid range is 1 to 10080 minutes.</p> |
| Mobility Status Task | 5 minutes | Lets you schedule status polling of mobility services engines. | <p>Enable—Select this check box to enable mobility status polling.</p> <p>Interval—Enter the interval, in minutes, between each mobility status poll. The valid range is 1 to 10080 minutes.</p> |

Table 7-5 Background Tasks (continued)

| Task Name | Default Schedule | Description | Editable Options |
|---|--|---|--|
| Prime Infrastructure Server Backup | Every 7 days at 1 AM (01:00) | Lets you schedule automatic Prime Infrastructure server backups. The backups created are application backups. | <p>Enabled—Select this check box to enable automatic Prime Infrastructure server backup.</p> <p>Backup Repository—Enter the name of the local or remote backup repository where automatic backups are stored.</p> <p>Max UI backups to keep—Enter the maximum number of automatic backups to keep (affects local repositories only).</p> <p>Interval—Enter the interval, in days, between each automatic Prime Infrastructure backup. The valid range is 1 to 7 days.</p> <p>Time of Day—Enter the time of the day that you want Prime Infrastructure server backups to be taken. Use 24-hour format (for example, 13:49).</p> |
| OSS Server Status | 5 minutes. | Lets you schedule OSS server status polling. | <p>Enable—Select this check box to enable OSS Server polling.</p> <p>Interval—Enter the interval, in minutes, between each OSS server poll. The valid range is 1 to 10080 minutes.</p> |
| Redundancy Status | 60 minutes | Lets you schedule redundancy status polling of primary and secondary controllers. | <p>Enabled—Select this check box to enable Redundancy status polling.</p> <p>Interval—Enter the interval, in minutes, between each poll. The valid range is 1 to 10080 minutes.</p> |
| Switch NMSP and Location Status | 4 hours | Lets you schedule Switch Network Mobility Services Protocol (NMSP) and Civic Location status polling. | <p>Enable—Select this check box to enable Switch NMSP and Civic Location status polling.</p> <p>Interval—Enter the interval, in minutes, between each poll. The valid range is 1 to 10080 minutes.</p> |
| Switch Operational Status | 5 minutes. Full poll is 60 minutes. | Lets you schedule switch operational status polling. | <p>Enable—Select this check box to enable switch status polling.</p> <p>Interval—Enter the interval, in minutes, between each poll. The valid range is 1 to 10080 minutes.</p> <p>Full operational status interval—Enter the interval, in minutes, between full switch operational status polls. The valid range is 1 to 1440 minutes.</p> <p>Create LinkDown Event—Select this check box to have Prime Infrastructure generate alarms for both access and trunk ports.</p> |
| Third party Access Point Operational Status | 3 hours | Lets you schedule operational status polling of third party APs. | <p>Enabled—Select this check box to enable third-party AP operational status polling.</p> <p>Interval—Enter the interval, in hours, between each poll. The valid range is 3 to 4 hours.</p> |

Table 7-5 Background Tasks (continued)

| Task Name | Default Schedule | Description | Editable Options |
|---|------------------|---|---|
| Third party Controller Operational Status | 3 hours | Lets you schedule reachability status polling of third-party controllers. | <p>Enabled—Select this check box to enable reachability status polling of third-party controllers.</p> <p>Interval—Enter the interval, in hours, between status polls. The valid range is 3 to 4 hours.</p> |
| wIPS Alarm Sync | 120 minutes | Lets you schedule wIPS alarm synchronization. | <p>Enable—Select this check box to enable wIPS alarm synchronization.</p> <p>Interval—Enter the interval, in minutes, between each synchronization. The valid range is 1 to 10080 minutes.</p> |
| Wired Client Status | 2 hours. | Lets you schedule wired client status polling. | <p>Enable—Select this check box to enable wired client status polling.</p> <p>Interval—Enter the interval, in hours, between each status poll. The valid range is 1 to 8640 hours.</p> <p>Major Polling—Specify two times of day at which you want to poll all wireless clients for their status. The valid format is hh:mm AM PM. For example, 12:49 AM.</p> |

Related Tasks

- [Controlling Data Collection Jobs](#)
- [About Data Collection Jobs](#)

Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure

Prime Infrastructure supports data migration from Cisco Prime LAN Management Solution (LMS) version 4.2.5 on all platforms. The following LMS data can be imported into Prime Infrastructure using the 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, follow these steps:

-
- Step 1** Identify the server where LMS backup data is stored.
- Step 2** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI” in Related Topics, below).
- Step 3** Enter the following commands to configure the backup location:

```
admin# configure terminal
admin(config)# repository carsapps
admin(config-Repository)# url location
admin(config-Repository)# user root password plain password
admin(config-Repository)# end
```

where:

- **location** is a fully qualified URL, including access protocol, for the location of the LMS backup data. For example: `ftp://10.77.213.137/opt/lms`, `sftp://10.77.213.137/opt/lms`, or `fdisk:foldername`.
- **password** is the root user password.

Step 4 Import the LMS backup into Prime Infrastructure using the following command:

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

Step 5 Exit your CLI session, log back in to the Prime Infrastructure user interface, and verify that your LMS data was imported properly. The following table shows where to look in Prime Infrastructure for the imported LMS data.

| LMS Data | Prime Infrastructure Location |
|--|---|
| DCR Devices | Inventory > Network Devices |
| Static Group | Inventory > Network Devices > User Defined Group |
| Dynamic Group | Inventory > Network Devices > User Defined Group |
| Software Image Management Repository Images | Inventory > Software Images |
| User Defined Templates (Netconfig) | Configuration > Templates > Features & Technologies |
| LMS Local Users | Administration > Users, Roles & AAA > Users |
| MIBs | Monitor > Monitoring Policies. In the menu, click Add, then select Policy Types > Custom MIB Polling. |

Related Topics

- [Connecting Via CLI](#)



Configuring Controller and AP Settings

The following related topics explain how to configure Cisco Prime Infrastructure to trace switch ports and detect rogue access points.

Related Topics

- [Configuring SNMP Credentials for Rogue AP Tracing](#)
- [Configuring Protocols for CLI Sessions](#)
- [Refreshing Controllers After an Upgrade](#)
- [Tracking Switch Ports to Rogue APs](#)
- [Configuring Switch Port Tracing](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

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 Cisco Prime Infrastructure, you can use SNMP credentials on this page to connect to the switch.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**. The Manual SPT page appears.
- Step 2** View or edit the details for a current SNMP credential entry by clicking the **Network Address** link for that entry.
- For details on this task, see “Configuring Global SNMP Settings” and “Viewing SNMP Credential Details” in related topics.
- Note that the default entry is for network 0.0.0.0, which indicates the entire network. SNMP credentials are defined per network, so only network addresses are allowed. The SNMP credentials defined for network 0.0.0.0 is the SNMP credential default. It is used when no specific SNMP credential is defined. You should update the pre-populated SNMP credential with your own SNMP information.
- Step 3** To add a new SNMP entry, choose **Select a command > Add SNMP Entries > Go** (see “Adding SNMP Credentials”).
-

Related Topics

- [Configuring Global SNMP Settings](#)
- [Viewing SNMP Credential Details](#)
- [Adding SNMP Credentials](#)

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.

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.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > CLI Session**.
 - Step 2** Select the **Controller Session Protocol** (you can choose SSH or Telnet; SSH is the default).
 - Step 3** Select the **Autonomous AP Session Protocol** (you can choose SSH or Telnet; SSH is the default).
 - Step 4** 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
 - Step 5** Click **Save**.
-

Refreshing Controllers After an Upgrade

The Controller Upgrade 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.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Controller Upgrade**.
 - Step 2** Select the **Auto refresh After Upgrade** check box to automatically restore the configuration whenever there is a change in the controller image.
 - Step 3** Select the **Process Save Config Trap Enable** check box to determine the action Prime Infrastructure takes when a save config trap is received. When this check box is selected, you can choose either to:
 - **Retain the configuration in the Prime Infrastructure database**
 - or
 - **Use the configuration on the controller currently**
 - Step 4** Click **Save**.
-

Tracking Switch Ports to Rogue APs

Prime Infrastructure can automatically identify the network switch port to which each rogue access point is connected. Note that this feature relies on Automatic Switch Port Tracing, which requires a full Prime Infrastructure license to work.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Auto SPT**. The Auto SPT page appears.
- Step 2** 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 3** 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 4** 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.

**Note**

For effective use of Vendor OUI match to eliminate false positive matches, the switch ports must have their location information configured. The switch ports that are not configured will remain for OUI match after elimination by location.

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.

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 must have 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. Network addresses using /32 subnet masks are not supported in global SNMP credentials configuration. For more guidance, see “Frequently Asked Questions on Rogues and Switch Port Tracing” in Related Topics.
- Switch port configuration—Trunking switch ports must be correctly configured. Switch port security must be disabled.
- Switch Port Tracing is supported only on Cisco Ethernet switches and the following Catalyst switches: 2960, 3560, 3560-E, 3750-E, 3850, 4500 series.
- Switch VLAN settings must be configured accurately. Prime Infrastructure gets switch IP addresses using Cisco Discovery Protocol neighbor information. It then uses VLAN information in the switch to read the switch CAM table entries. If the VLAN information in the switch is not configured properly, Prime Infrastructure will not be able to read the CAM table entries, which results in not being able to trace rogue APs in the switch.
- CDP protocol must be enabled on all switches.
- An Ethernet connection must exist between the rogue access point and the Cisco switch.
- There must be traffic between the rogue access point and the Ethernet switch, for reliable detection of rogue Ethernet Switch Port information, when the difference in the Ethernet mac address is more or less than two.
- The rogue access point must be connected to a switch within the max hop limit.
- 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).

To view the switch port trace details, follow these steps:

-
- Step 1** Add switches with full licenses using the **Configuration > Network > Network Devices** page.
 - Step 2** Enable **Auto switch port tracing** in **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Auto SPT** page.
 - Step 3** Schedule to run wired client status Major Polling background task in **Administration > Dashboards > Job Dashboard** page.
 - Step 4** Click the Trace switch port icon in Rogue AP detail page. New pop up will show details of switch port traced. Click the detail status to check trace status such as started/Found, and so on.
-



Note

- Manual SPT will work, even if you do not add any switch to Prime Infrastructure. But you should configure the SNMP credentials correctly in **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT** page. “Private” is the default credential, and will be used during manual Switch Port Tracing if you do not configure it.

- If a switch is added to Prime Infrastructure by selecting **Configuration > Network > Network Devices**, the SNMP credentials entered for the switch will override any switch SNMP credentials entered here, and will be used for switch port tracing. You can change the switch SNMP credentials in the **Configuration > Network > Network Devices** page. Prime Infrastructure will not require any license for adding switch with SPT and will not display wired clients connected to the switches. The **Monitor > Managed Elements > Network Devices > Device Groups > Device Type > Switches and Hubs** page will not display the switch details added with SPT.
- Prime Infrastructure requires full license for adding switch. The **Monitor > Managed Elements > Network Devices > Device Groups > Device Type > Switches and Hubs** page will display the switch details added with full license. Prime Infrastructure will also display wired clients connected to switches. Location of switches is tracked with MSE.

Step 1 Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > SPT Configuration**.

Step 2 Configure the following basic settings:

- MAC address +1/-1 search—Select the check box to enable.
This search involves the MAC address +1/-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.



Note This hop count value is not applicable for Auto SPT.

- 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.

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.

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

- Step 1** Choose **Dashboard > Wireless > Security**.
- Step 2** In the **Malicious Rogue APs**, **Unclassified Rogue APs**, **Friendly Rogue APs**, **Custom Rogue APs**, and **Adhoc Rogues** dashlets: Click the number links showing how many rogues have been identified in the Last Hour, last 24 Hours, or Total Active. The Alarms window opens, showing alarms for the suspected rogues.
- Step 3** Choose the rogue for which you want to set up switch port tracking by selecting the check box next to it.
- Step 4** Expand the applicable alarm and manually select the **Trace Switch Port** button under the Switch Port Tracing subsection of the alarm details.

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 “Switch Port Tracing Details” for additional information on the Switch Port Tracing Details dialog box.

Related Topics

- [Switch Port Tracing Details](#)

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 related topics:

- “Configuring Switch Port Tracing”
- “Configuring SNMP Credentials for Rogue AP Tracing”

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**.

Related Topics

- [Configuring Switch Port Tracing](#)
- [Configuring SNMP Credentials for Rogue AP Tracing](#)

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.
- Switch Port Tracing is supported only on Cisco Ethernet switches and the following Catalyst switches: 2960, 3560, 3560-E, 3750-E, 3850, 4500 series.
- 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).

Frequently Asked Questions on Rogues and Switch Port Tracing

The following related topics answer a variety of questions about Prime Infrastructure rogue AP detection and switch port tracing (SPT).

Related Topics

- [How Do You Configure Auto SPT?](#)
- [How Does Auto SPT Differ From Manual SPT?](#)
- [Where Can I See SPT Results \(Manual and Auto\)?](#)
- [How Can I Ensure Auto SPT Runs Smoothly?](#)
- [Why Does Auto SPT Take Longer to Find Wired Rogues?](#)
- [How Can I Detect Wired Rogues on Trunk Ports?](#)
- [How Can I Use the Auto SPT “Eliminate By Location” Feature?](#)
- [What is the Difference Between “Major Polling” and “Minor Polling”?](#)

How Do You Configure Auto SPT?

Follow the steps below to configure automatic SPT:

-
- Step 1** Use **Configuration > Network > Network Devices > Add Device** to add switches with a **License Level** of **Full**.
- Step 2** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Auto SPT** and select **Enable Auto Switch Port Tracing**. Click **OK**.
- Step 3** Select **Administration > Settings > Background Tasks > Wired Client Status**. Make sure this task is enabled and that it is scheduled to run at least twice a day.
-

Related Topics

- [Where Can I See SPT Results \(Manual and Auto\)?](#)
- [How Can I Ensure Auto SPT Runs Smoothly?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

How Does Auto SPT Differ From Manual SPT?

Manual SPT runs against individual rogue AP alarms. You must trigger it by clicking on the **Trace Switch Port** icon on the details page for a rogue AP alarm.

Auto SPT runs on batches of alarms, automatically, on the schedule defined for the Wired Client Status background task.

Note that manual SPT triggering depends on CDP being enabled on the access points and switches with appropriate SNMP community strings. For more information on manual SPT and how it works, see the WCS Switch Port Trace Demonstration link in related topics.

Auto and manual SPT also differ in the way they handle licensing and the switch “license level”, which can be set to either “Full” or “Switch Port Trace Only” when adding the switch. These three cases demonstrate the differences:

- **Adding switches with “Full” license level:** Prime Infrastructure consumes a license for every added switch with a full license level. All the wired clients connected to switches can be seen by selecting **Monitor > Managed Elements > Network Devices > Device Type > Switches and Hubs**. You can also use MSE to track switch locations. A “Full” license level is mandatory for Auto SPT to be functional.
- **Adding no Switches:** Manual SPT will still work even without adding any switches. But you must remember to configure SNMP credentials appropriately for all switches, using **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.
- **Adding switches with “Switch Port Trace Only” license level:** If you add a switch to Prime Infrastructure using **Configuration > Network > Network Devices > Add Device**, but select a **Switch Port Trace Only** license level, the SNMP credentials you enter when adding the switch will override the SNMP credentials entered using **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**. The entered credentials will be used for switch port tracing. This is the main difference between not adding switches and adding switches with a license level of “Switch Port Tracing Only”. Prime Infrastructure will not consume any licenses for switches with an SPT-only license level, will not show these switches under **Monitor > Managed Elements > Network Devices > Device Type > Switches and Hubs**, and will not show wired clients connected to these switches.

Related Topics

- [WCS Switch Port Trace Demonstration](#)
- [What is the Difference Between “Major Polling” and “Minor Polling”?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

Where Can I See SPT Results (Manual and Auto)?

-
- Step 1** Display details for the Rogue AP alarm in which you are interested. For example:
- Click the **Alarm Summary** icon at the top of any Prime Infrastructure page. A list of alarm categories appears.
 - Click the **Rogue AP** link in the list. Prime Infrastructure displays the list of rogue AP alarms.
 - Expand the rogue AP alarm you want. The details page for that alarm appears.
- Step 2** In the **Switch Port Tracing** pane, click the **Trace Switch Port** icon. The Switch Port Trace window shows the details of the traced switch port.
- If no SPT has been performed, click **Trace Switch Port(s)** to start tracing. Click the **Show Detail Status** button to get details on the status of the trace as it progresses.
-

Related Topics

- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

How Can I Ensure Auto SPT Runs Smoothly?

The following are recommended best practices for auto SPT:

- Ensure that Prime Infrastructure manages all switches with a **Full** license level.
- Ensure all the switches are managed by and synchronized with Prime Infrastructure, so that wired client discovery is successful.
- For best results, use **Administration > Settings > Background Tasks** to ensure that the following background tasks are running:
 - Switch Inventory/Refresh Config:** Must run periodically.
 - Wired Client Status:** Must be running periodically.
 - Data Cleanup:** Is not disabled and is running periodically.

For Rogue AP tasks, use **Administration > Dashboards > Job Dashboard > System Jobs > Wireless Poller > Rogue AP**.

- Ensure that rogue AP alarms are kept only for the required number of days. Cisco recommends that you keep them for no more than 8 days unless you have special retention requirements. You can configure this by selecting **Administration > Settings > System Settings > Alarms and Events > Alarms and Events** and setting the desired time period in the **Delete cleared security alarms after** field.
- For immediate wired- client detection, use a trap receiver configuration on the switch, which can trigger Prime Infrastructure's client discovery and rogue detection processes. You can enable this by following these steps:
 - Use **Administration > System Settings > Client and User > Client** page to enable the **Poll clients on client traps** option. This is strongly recommended only for a smaller environment (around 50 switches) or for some sensitive ports.

- b. Execute the following commands in the CLI for each switch (these commands may vary slightly for each switch platform):

```
<switchname># conf t
```

```
<switchname>(config)# Snmp-server enable traps mac-notification change move threshold
```

```
<switchname>(config)# Snmp-server host PrInfraIPAddress version 2c comstring mac-notification
```

```
<switchname>(config)# Mac address-table notification change interval 5
```

```
<switchname>(config)# Mac address-table notification change history-size 10
```

```
<switchname>(config)# Mac address-table notification change
```

Where:

- *PrInfraIPAddress* is the IP Address of the Prime Infrastructure server.
 - *comstring* is the community string for the switch
- c. Execute the following commands on the interfaces for each switch (these commands may vary slightly for each switch platform):

```
<switchname>(config)# Interface Intname
```

```
<switchname>(config-if)# description non-identity clients
```

```
<switchname>(config-if)# switchport access vlan ID
```

```
<switchname>(config-if)# switchport mode access
```

```
<switchname>(config-if)# snmp trap mac-notification change added
```

```
<switchname>(config-if)# snmp trap mac-notification change removed
```

Where:

- *Intname* is the interface name
- *ID* is the VLAN ID

Related Topics

- [How Do You Configure Auto SPT?](#)
- [What is the Difference Between “Major Polling” and “Minor Polling”?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

Why Does Auto SPT Take Longer to Find Wired Rogues?

Auto SPT takes relatively longer to find wired rogues than does manual SPT for the following reasons:

1. Auto SPT depends on the wired client discovery process, which happens only when the Wired Client Status major polling background task runs. By default, the major poll for this background task is scheduled to run only after every two minor polls, or once every four hours.
2. Even though the wired rogue AP is connected to a switch, Prime Infrastructure will discover a wired port only when the wired rogue AP is in the “associated” state. Prime Infrastructure always checks whether a wired client’s status is associated or disassociated. If the wired client status is disassociated, Prime Infrastructure shows this as no port connected.
3. Rogue tracing is done in batches. The time taken to find a particular wired rogue depends on the batch in which Prime Infrastructure processes it. If a particular rogue was processed in the previous batch, it takes more time to trace it.
4. The time taken to discover any wired rogue depends upon the number of rogue alarms present in Prime Infrastructure and the interval between Wired Client Status major polls.

Related Topics

- [What is the Difference Between “Major Polling” and “Minor Polling”?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

How Can I Detect Wired Rogues on Trunk Ports?

You can detect wired rogues on trunk ports by following the steps below.

Note that if you are trying to detect rogues on trunk ports for Cisco 2950 switches, you must first install the updated 2950 support in Prime Infrastructure Device Pack 5.0.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > SPT Configuration**.
 - Step 2** Uncheck the **Exclude switch trunk ports** check box, then click **Save**.
 - Step 3** Choose **Administration > Settings > System Settings > Client and User > Client**.
 - Step 4** Check the **Discover wired clients on trunk ports** check box, then click **Save**.

Switches will start detecting wired clients on trunk ports starting with the next execution of a major poll by the Wired Client Status background task.

Related Topics

- [How Do You Configure Auto SPT?](#)
- [What is the Difference Between “Major Polling” and “Minor Polling”?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

How Do You Configure Switch Port Location?

Follow the steps below to configure Switch Port Location:

-
- Step 1** Use **Configuration > Network > Network Devices > Switches and Hubs**.
- Step 2** Click a **Device Name**. By default, Configuration tab opens.
- Step 3** Click **Switch Port Location** in the top right corner.
- Step 4** Select the check box(es) of one or more ports to configure location, and from choose **Configure Location** from the drop-down list, then click **Go**.
- Step 5** In the Map Location group, you can configure the following:
- From the Campus/Site drop-down list, choose the campus map for the switch or switch port.
 - From the Building drop-down list, choose the building map location for the switch or switch port.
 - From the Floor drop-down list, choose the floor map.
 - If you have already saved a file with the Campus/Site, Building, and Floor details, click **Import Civic**. This imports civic information for the MSE using Prime Infrastructure. Enter the name of the text file or browse for the filename, and click **Import**.
- Step 6** In the ELIN and Civic Location group box, you can configure the following:
- Enter the Emergency Location Identifier Number (ELIN) in the ELIN text box. ELIN is a number that can be used by the local public safety answering point (PSAP) to look up the geographic location of the caller in a master database known as the automatic location information (ALI) database. The ELIN also allows the PSAP to contact the emergency caller directly in the event the phone call is disconnected.
 - Complete the required fields on the Civic Address and Advanced tabs.
 - If you have the ELIN and Civic location information saved in a file, you can import it by clicking **Import Switch Location**.
- Step 7** Click **Save**.
-

Related Topics

- [How Can I Use the Auto SPT “Eliminate By Location” Feature?](#)
- [How Do You Configure Switch Port Location?](#)
- [How Do You Configure Auto SPT?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

How Can I Use the Auto SPT “Eliminate By Location” Feature?

“Eliminate by location” is one of the algorithms Prime Infrastructure uses to detect wired rogues. It uses the rogue AP location information to search for the associated switch ports. It helps to reduce false positives during Auto SPT processing, using the floor ID of the detecting APs, and increases accuracy in tracking wired rogues.

When “Eliminate by location” is enabled, the Wired Client Status background task discovers all the wired clients from managed switches. The next time auto SPT runs, switch ports will be filtered based on the “eliminate by location” algorithm.

Follow these steps to enable “eliminate by location”:

-
- Step 1** Integrate Cisco Mobility Service Engine (MSE) with Prime Infrastructure.

- Step 2** Ensure that MSE is in sync with the defined floor area where the detecting APs are placed. MSE should be able to track the rogues.
- Step 3** Add all switches to Prime Infrastructure.
- Step 4** After all switches are added to PI and are in the managed state, all switch ports need to be configured for the algorithm to work. If all switches are not configured with switch ports, then the false positive results occur. You can configure from the **Configuration > Network > Network Devices > Switches and Hubs** > click on a **Device Name** > click **Switch Port Location** in the top right corner.
- Step 5** Place the detecting access points on the map and make sure that the Cisco MSE is synchronized and rogues APs are detected on the floor.
- Eliminate By Location algorithm takes the floor ID of detecting APs and eliminates all others. If some switch ports are not configured, then the value of those ports will be set to Zero and will be considered. Hence the results may contain false positives, which contains the exact floor ID and floor ID which has the value zero.
- Step 6** Configure switch port locations to ensure that all ports are assigned to the correct floor area.
-

Related Topics

- [How Do You Configure Switch Port Location?](#)
- [How Do You Configure Auto SPT?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)

What is the Difference Between “Major Polling” and “Minor Polling”?

The Wired Client Status background task that triggers auto SPT Definitions are as follows:

Major Polling: During a major poll, Prime Infrastructure triggers client discovery on all wired device ports by syncing all of the essential client information with the database. In Prime Infrastructure 2.2, the frequency of this poll was reduced from twice a day. It is now fully configurable.

Minor Polling: During a minor poll, Prime Infrastructure triggers client discovery only on device interfaces and ports which became active recently. Prime Infrastructure uses interface uptime data to detect when a port or interface is recently added or removed by any client.

Related Topics

- [How Does Auto SPT Differ From Manual SPT?](#)
- [Why Does Auto SPT Take Longer to Find Wired Rogues?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#)



Configuring High Availability

To ensure continued operation in case of failure, Cisco Prime Infrastructure provides a high availability (HA) framework. HA uses a pair of linked, synchronized Prime Infrastructure servers to minimize or eliminate the impact of application or hardware failures that may take place on either server.

The following topics explain how to set up and use this feature. The final topic explains how to configure Mobility Service Engines to support a similar high availability feature, which you can then manage using the Prime Infrastructure interface.

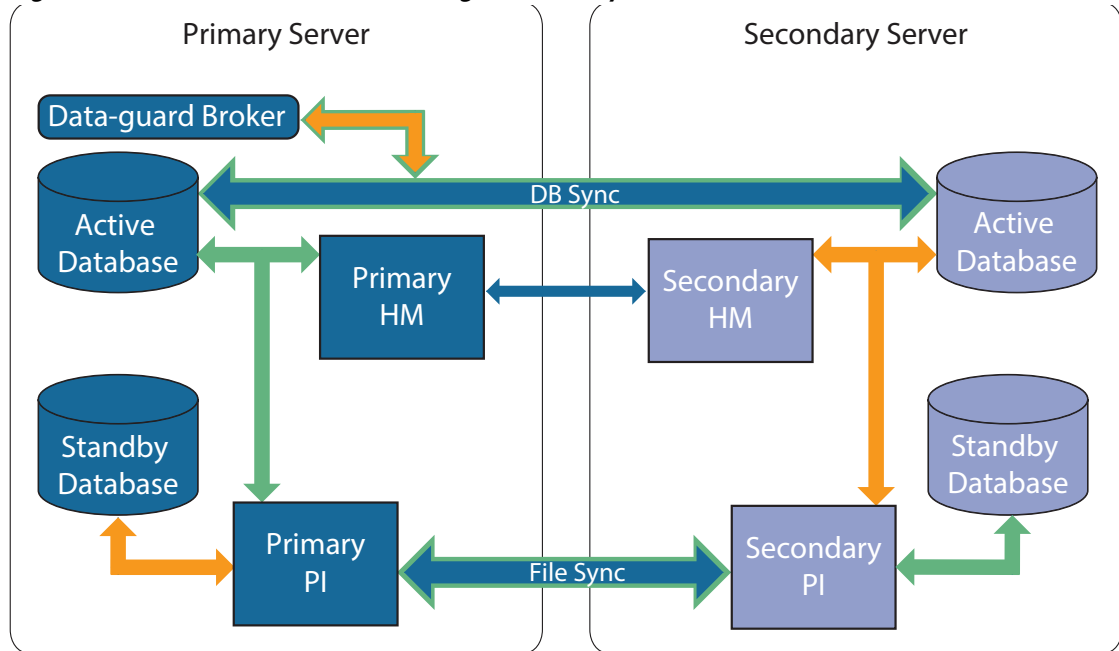
Related Topics

- [How High Availability Works](#)
- [Planning HA Deployments](#)
- [Setting Up High Availability](#)
- [Monitoring High Availability](#)
- [High Availability Reference Information](#)
- [Configuring MSE High Availability](#)

How High Availability Works

The following figure shows the main components and process flow for a Prime Infrastructure High Availability (HA) setup with the primary server in the active state.

Figure 9-1 Prime Infrastructure High Availability (HA) Architecture



An HA deployment consists of two Prime Infrastructure servers: a primary and a secondary. Each of these servers has an active database and a standby backup copy of the active database. Under normal circumstances, the primary server is active: It is connected to its active database while it manages the network. The secondary server is passive, connected only to its standby database, but in constant communication with the primary server.

The Health Monitor processes running on both servers monitor the status of its opposite server. Oracle Recovery Manager (RMAN) running on both servers creates the active and standby databases and synchronizes the databases when there are changes, with the help of Oracle Data Guard Broker running on the primary server.

When the primary server fails, the secondary takes over, connecting to its active database, which is in sync with the active primary database. You can trigger this switch, called a “failover”, either manually, which is recommended, or have it triggered automatically. You then use the secondary server to manage the network while working to restore access to the primary server. When the primary is available again, you can initiate a switch (called a “failback”) back to the primary server and resume network management using the primary.

If you choose to deploy the primary and secondary servers on the same IP subnet, you can configure your devices to send a notifications to Prime Infrastructure at a single virtual IP address. If you choose to disperse the two servers geographically, such as to facilitate disaster recovery, you will need to configure your devices to send notifications to both servers.

Related Topics

- [About the Primary and Secondary Servers](#)
- [Sources of Failure](#)
- [File and Database Synchronization](#)
- [HA Server Communications](#)
- [Health Monitor Process](#)
- [Health Monitor Web Page](#)
- [Using Virtual IP Addressing with HA](#)

About the Primary and Secondary Servers

In any Prime Infrastructure HA implementation, for a given instance of a primary server, there must be one and only one dedicated secondary server.

Typically, each HA server has its own IP address or host name. If you place the servers on the same subnet, they can share the same IP using virtual IP addressing, which simplifies device configuration.

Once HA is set up, you should avoid changing the IP addresses or host names of the HA servers, as this will break the HA setup (see “Resetting the Server IP Address or Host Name” in Related Topics).

Related Topics

- [How High Availability Works](#)
- [Using Virtual IP Addressing with HA](#)
- [Resetting the HA Server IP Address or Host Name](#)

Sources of Failure

Prime Infrastructure servers can fail due to issues in one or more of the following areas:

- **Application Processes:** Failure of one or more of the Prime Infrastructure server processes, including NMS Server, MATLAB, TFTP, FTP, and so on. You can view the operational status of each of these application processes by running the `ncs status` command through the admin console.
- **Database Server:** One or more database-related processes could be down. The Database Server runs as a service in Prime Infrastructure.
- **Network:** Problems with network access or reachability issues.
- **System:** Problems related to the server's physical hardware or operating system.
- **Virtual Machine (VM):** Problems with the VM environment on which the primary and secondary servers were installed (if HA is running in a VM environment).

Related Topics

- [How High Availability Works](#)

File and Database Synchronization

Whenever the HA configuration determines that there is a change on the primary server, it synchronizes this change with the secondary server. These changes are of two types:

1. **Database:** These include database updates related to configuration, performance and monitoring data.
2. **File:** These include changes to configuration files.

Oracle Recovery Manager (RMAN) running on both servers creates the active and standby databases and synchronizes the databases when there are changes, with the help of Oracle Data Guard Broker running on the primary server.

File changes are synchronized using the HTTPS protocol. File synchronization is done either in:

- **Batch:** This category includes files that are not updated frequently (such as license files). These files are synchronized once every 500 seconds.
- **Near Real-Time:** Files that are updated frequently fall under this category. These files are synchronized once every 11 seconds.

By default, the HA framework is configured to copy all the required configuration data, including:

- Report configurations
- Configuration Templates
- TFTP-root
- Administration settings
- Licensing files

Related Topics

- [How High Availability Works](#)

HA Server Communications

The primary and secondary HA servers exchange the following messages in order to maintain the health of the HA system:

- **Database Sync:** Includes all the information necessary to ensure that the databases on the primary and secondary servers are running and synchronized.
- **File Sync:** Includes frequently updated configuration files. These are synchronized every 11 seconds, while other infrequently updated configuration files are synchronized every 500 seconds.
- **Process Sync:** Ensures that application- and database-related processes are running. These messages fall under the Heartbeat category.
- **Health Monitor Sync:** These messages check for the following failure conditions:
 - Network failures
 - System failures (in the server hardware and operating system)
 - Health Monitor failures

Related Topics

- [How High Availability Works](#)

Health Monitor Process

Health Monitor (HM) is the main component managing HA operations. Separate instances of HM run as an application process on both the primary and the secondary server. HM performs the following functions:

- Synchronizes database and configuration data related to HA (this excludes databases that sync separately using Oracle Data Guard).
- Exchanges heartbeat messages between the primary and secondary servers every five seconds, to ensure communications are maintained between the servers.
- Checks the available disk space on both servers at regular intervals, and generates events when storage space runs low.
- Manages, controls and monitors the overall health of the linked HA servers. If there is a failure on the primary server then it is the Health Monitor's job to activate the secondary server.

Related Topics

- [How High Availability Works](#)

Health Monitor Web Page

You control HA behavior using the Health Monitor web page. Each Health Monitor instance running on the primary server or secondary server has its own web page. The following figure shows an example of the Health Monitor web page for a primary server in the “Primary Active” state.

Figure 9-2 Health Monitor Web Page (Primary Server in Active State)

| Time | State | Description |
|--------------------------|--------------------------|--|
| Jun 15, 2015 06:55:18 AM | Primary Active | Failed to send email notification: Notification Email Address is not configured. |
| Jun 15, 2015 06:55:18 AM | Primary Active | Completed failback from Secondary Prime Infrastructure 172.20.116.163 [172.20.116.163] |
| Jun 15, 2015 06:54:04 AM | Primary Failback | Starting to failback from secondary Prime Infrastructure 172.20.116.163 [172.20.116.163] |
| Jun 15, 2015 06:53:19 AM | Primary Syncing | Primary Prime Infrastructure Server started successfully as standby |
| Jun 15, 2015 06:53:19 AM | Primary Syncing | Prime Infrastructure started successfully. Prime Infrastructure server state : Primary Syncing |
| Jun 15, 2015 06:34:47 AM | Health Monitor Available | Health Monitor Started |
| Jun 15, 2015 06:34:45 AM | Health Monitor Available | Health Monitor Started |
| Jun 15, 2015 06:21:55 AM | Primary Active | Failed to send email notification: Notification Email Address is not configured. |
| Jun 15, 2015 06:21:55 AM | Primary Active | Completed HA registration with Secondary server 172.20.116.163 [172.20.116.163] |

| | | | |
|----------|---|-----------|--|
| 1 | Settings area displays Health Monitor state and configuration detail in five separate sections. | 2 | Status indicates current functional status of the HA setup (green check mark indicates that HA is on and working). |
| 3 | Events table displays all current HA-related events, in chronological order, with most recent event at the top. | 4 | Secondary IP Address identifies the IP of the peer server for this primary server (on the secondary server, this field is labeled “Primary IP Address”). |
| 5 | Logging area lets you download Health Monitor log files. | 6 | Message Level field lets you change the logging level (your choice of Error, Informational, or Trace). You must press Save to change the logging level. |
| 7 | State shows current HA state of the server on which this instance of Health Monitor is running. | 8 | Failover Type shows whether you have Manual or Automatic failover configured. |
| 9 | Identifies the HA server whose Health Monitor web page you are viewing. | 10 | Action shows actions you can perform, such as failover or failback. Action buttons are enabled only when Health Monitor detects HA state changes needing action. |

Related Topics

- [How High Availability Works](#)

Using Virtual IP Addressing with HA

Under normal circumstances, you configure the devices that you manage using Prime Infrastructure to send their syslogs, SNMP traps and other notifications to the Prime Infrastructure server's IP address. When HA is implemented, you will have two separate Prime Infrastructure servers, with two different IP addresses. If we fail to reconfigure devices to send their notifications to the secondary server as well as the primary server, then when the secondary Prime Infrastructure server goes into Active mode, none of these notifications will be received by the secondary server.

Setting all of your managed devices to send notifications to two separate servers demands extra device configuration work. To avoid this additional overhead, HA supports use of a virtual IP that both servers can share as the Management Address. The two servers will switch IPs as needed during failover and failback processes. At any given time, the virtual IP Address will always point to the correct Prime Infrastructure server.

Note that you cannot use virtual IP addressing unless the addresses for both of the HA servers and the virtual IP are all in the same subnet. This can have an impact on how you choose to deploy your HA servers (see “Planning HA Deployments” and “Using the Local Model” in Related Topics).

Also note that a virtual IP address is in no way intended as a substitute for the two server IP addresses. The virtual IP is intended as a destination for syslogs and traps, and for other device management messages being sent to the Prime Infrastructure servers. Polling of devices is always conducted from one of the two Prime Infrastructure server IP addresses. Given these facts, if you are using virtual IP addressing, you must open your firewall to incoming and outgoing TCP/IP communication on all three addresses: the virtual IP address as well as the two actual server IPs.

You must use virtual IP addressing if you plan to use HA with Operations Center. You must assign a virtual IP to the Prime Infrastructure instance on which Operations Center is enabled. No virtual IP is needed for any of the instances managed using Operations Center (see “Enabling HA for Operations Center”).

You can enable virtual IP addressing during HA registration on the primary server, by specifying that you want to use this feature and then supplying the virtual IPv4 (and, optionally, IPv6) address you want the primary and secondary servers to share (see “Registering HA on the Primary Server”). To remove Virtual IP addressing after it is enabled, you must remove HA completely (see “Removing HA Via the GUI”).

Related Topics

- [How High Availability Works](#)
- [Setting Up High Availability](#)
- [What If I Cannot Use Virtual IP Addressing?](#)
- [Using SSL Certificates in an HA Environment](#)
- [Removing HA Via the GUI](#)
- [Planning HA Deployments](#)
- [Using the Local Model](#)

Hot Standby Behavior

When the primary server is active, the secondary server is in constant synchronization with the primary server and runs all Prime Infrastructure processes for fast switch over. When the primary server fails, the secondary server immediately takes over the active role within two to three minutes after the failover.

Once issues in the primary server are resolved and it is returned to a running state, the primary server assumes a standby role. When the primary server is in the standby role, the Health Monitor GUI shows “Primary Syncing” state during which the database and files on the primary start to sync with the active secondary.

When the primary server is available again and a failback is triggered, the primary server again takes over the active role. This role switching between the primary and secondary servers happens within two to three minutes.

Related Topics

- [How High Availability Works](#)

Planning HA Deployments

Prime Infrastructure's HA feature supports the following deployment models:

- **Local:** Both of the HA servers are located on the same subnet (giving them Layer 2 proximity), usually in the same data center.
- **Campus:** Both HA servers are located in different subnets connected via LAN. Typically, they will be deployed on a single campus, but at different locations within the campus.
- **Remote:** Each HA server is located in a separate, remote subnet connected via WAN. Each server is in a different facility. The facilities are geographically dispersed across countries or continents.

The following sections explain the advantages and disadvantage of each model, and discusses underlying restrictions that affect all deployment models.

HA will function using any of the supported deployment models. The main restriction is on HA's performance and reliability, which depends on the bandwidth and latency criteria discussed in "Network Throughput Restrictions on HA". As long as you are able to successfully manage these parameters, it is a business decision (based on business parameters, such as cost, enterprise size, geography, compliance standards, and so on) as to which of the available deployment models you choose to implement.

Related Topics

- [Network Throughput Restrictions on HA](#)
- [Using the Local Model](#)
- [Using the Campus Model](#)
- [Using the Remote Model](#)
- [What If I Cannot Use Virtual IP Addressing?](#)
- [Using SSL Certificates in an HA Environment](#)
- [Automatic Versus Manual Failover](#)

Network Throughput Restrictions on HA

Prime Infrastructure HA performance is always subject to the following limiting factors:

- The net bandwidth available to Prime Infrastructure for handling all operations. These operations include (but are not restricted to) HA registration, database and file synchronization, and triggering failback.
- The net latency of the network across the links between the primary and secondary servers. Irrespective of the physical proximity of these two servers, high latency on these links can affect how Prime Infrastructure maintains sessions between the primary and secondary servers.
- The net throughput that can be delivered by the network that connects the primary and secondary servers. Net throughput varies with the net bandwidth and latency, and can be considered a function of these two factors.

These limits apply to at least some degree in every possible deployment model, although some models are more prone to problems than others. For example: Because of the high level of geographic dispersal, the Remote deployment model is more likely to have problems with both bandwidth and latency. But both the Local and Campus models, if not properly configured, are also highly susceptible to problems with throughput, as they can be saddled by low bandwidth and high latency on networks with high usage.

You will rarely see throughput problems affecting a failback or failover, as the two HA servers are in more or less constant communication and the database changes are replicated quickly. Most failovers and failbacks take approximately two to three minutes.

The main exception to this rule is the delay for a full database copy operation. This kind of operation is triggered when the primary server has been down for more than 24 hours and you then bring it back up. In these conditions, Prime Infrastructure will trigger a full database copy operation from the secondary to the primary. No failback is possible during this period, although the Health Monitor page will display any events encountered while the database copy is going on. As soon as the copy is complete, the primary server will go to the “Primary Syncing” state, and you can then trigger failback.

Variations in net throughput during a full database copy operation, irrespective of database size or other factors, can mean the difference between a database copy operation that completes successfully in under an hour and one that does not complete at all. Cisco has tested the impact of net throughput on HA deployment in configurations following the Remote model, using typical Prime Infrastructure database sizes of between 105 GB and 156 GB. Based on these tests, Cisco recommends for a typical database of 125 GB (generating a 10 GB backup file):

- For best results: With sub-millisecond latency, and net throughput of 977 Mbps or more, expect a complete database copy time of one hour or less.
- For good results: With latency of 70 milliseconds, and net throughput of 255 Mbps or more, expect a complete database copy time of two hours or less.
- For acceptable results: With latency of 220 milliseconds or less, and net throughput of 86 Mbps or more, expect a complete database copy time of 4.5 hours or less

With latencies of 330ms or higher, and throughput of 46Mbps or less, you run the risk of the database copy not completing successfully.

Related Topics

- [Planning HA Deployments](#)
- [Using the Remote Model](#)

Using the Local Model

The main advantage of the Local deployment model is that it permits use of a virtual IP address as the single management address for the system. Users can use this virtual IP to connect to Prime Infrastructure, and devices can use it as the destination for their SNMP trap and other notifications.

The only restriction on assigning a virtual IP address is to have that IP address in the same subnet as the IP address assignment for the primary and secondary servers. For example: If the primary and secondary servers have the following IP address assignments within the given subnet, the virtual IP address for both servers can be assigned as follows:

- Subnet mask: 255.255.255.224 (/27)
- Primary server IP address: 10.10.101.2
- Secondary server IP address: 10.10.101.3
- Virtual IP address: 10.10.101.[4-30] e.g., 10.10.101.4. Note that the virtual IP address can be any of a range of addresses that are valid and unused for the given subnet mask.

In addition to this main advantage, the Local model also has the following advantages:

- Usually provides the highest bandwidth and lowest latency.
- Simplified administration.
- Device configuration for forwarding syslogs and SNMP notifications is much easier.

The Local model has the following disadvantages:

- Being co-located in the same data center exposes them to site-wide failures, including power outages and natural disasters.
- Increased exposure to catastrophic site impacts will complicate business continuity planning and may increase disaster-recovery insurance costs.

Related Topics

- [Planning HA Deployments](#)
- [Using the Campus Model](#)
- [Using the Remote Model](#)

Using the Campus Model

The Campus model assumes that the deploying organization is located at one or more geographical sites within a city, state or province, so that it has more than one location forming a “campus”. This model has the following advantages:

- Usually provides bandwidth and latency comparable to the Local model, and better than the Remote model.
- Is simpler to administer than the Remote model.

The Campus model has the following disadvantages:

- More complicated to administer than the Local model.
- Does not permit use of a virtual IP address as the single management address for the system, so it requires more device configuration (see “What If I Cannot Use Virtual IP Addressing?” in Related Topics).

- May provide lower bandwidth and higher latency than the Local model. This can affect HA reliability and may require administrative intervention to remedy (see “Network Throughput Restrictions on HA” in Related Topics).
- While not located at the same site, it will still be exposed to city-, state-, or province-wide disasters. This may complicate business continuity planning and increase disaster-recovery costs.

Related Topics

- [Planning HA Deployments](#)
- [Network Throughput Restrictions on HA](#)
- [Using the Local Model](#)
- [Using the Remote Model](#)
- [What If I Cannot Use Virtual IP Addressing?](#)

Using the Remote Model

The Remote model assumes that the deploying organization has more than one site or campus, and that these locations communicate across geographical boundaries by WAN links. It has the following advantages:

- Least likely to be affected by natural disasters. This is usually the least complex and costly model with respect to business continuity and disaster recovery.
- May reduce business insurance costs.

The Remote model has the following disadvantages:

- More complicated to administer than the Local or Campus models.
- Does not permit use of a virtual IP address as the single management address for the system, so it requires more device configuration (see “What If I Cannot Use Virtual IP Addressing?” in Related Topics).
- Usually provides lower bandwidth and higher latency than the other two models. This can affect HA reliability and may require administrative intervention to remedy (see “Network Throughput Restrictions on HA” in Related Topics).

Related Topics

- [Planning HA Deployments](#)
- [Network Throughput Restrictions on HA](#)
- [Using the Local Model](#)
- [Using the Campus Model](#)
- [What If I Cannot Use Virtual IP Addressing?](#)

What If I Cannot Use Virtual IP Addressing?

Depending on the deployment model you choose, not configuring a virtual IP address may result in the administrator having to perform some additional steps in order to ensure that syslogs and SNMP notifications are forwarded to the secondary server in case of a failover from the primary to the secondary server. The usual method is to configure the devices to forward all syslogs and traps to both servers, usually via forwarding them to a given subnet or range of IP addresses that includes both the primary and secondary server.

This configuration work should be done at the same time HA is being set up: that is, after the secondary server is installed but before HA registration. It must be completed before a failover so that the chance of losing data is eliminated or reduced. Not using a virtual IP address entails no change to the secondary server install procedure. The primary and secondary servers still need to be provisioned with their individual IP addresses, as normal.

Related Topics

- [Planning HA Deployments](#)
- [Network Throughput Restrictions on HA](#)
- [Using the Campus Model](#)
- [Using the Remote Model](#)

Using SSL Certificates in an HA Environment

If you decide to use SSL certification to secure communications between Prime Infrastructure server and users, and also plan to implement HA, you will need to generate separate certificates for both the primary and secondary HA servers.

These certificates must be generated using the FQDN (Fully Qualified Domain Name) for each server. To clarify: You must use the primary server's FQDN to generate the certificate you plan to use for the primary server, and the secondary server's FQDN to generate the certificate you plan to use for the secondary server.

Once you have generated the certificates, import the signed certificates to the respective servers.

Do not generate SSL certificates using a virtual IP address. The virtual IP address feature is used to enable communications between Prime Infrastructure and your network devices.

Related Topics

- [Planning HA Deployments](#)
- [Using Virtual IP Addressing with HA](#)
- [What If I Cannot Use Virtual IP Addressing?](#)

Automatic Versus Manual Failover

Configuring HA for automatic failover reduces the need for network administrators to manage HA. It also reduces the time taken to respond to the conditions that provoked the failover, since it brings up the secondary server automatically.

However, we recommend that the system be configured for Manual failover under most conditions. Following this recommendation ensures that Prime Infrastructure does not go into a state where it keeps failing over to the secondary server due to intermittent network outages. This scenario is most likely when deploying HA using the Remote model. This model is often especially susceptible to extreme variations in bandwidth and latency (see “Planning HA Deployments” and “Network Throughput Restrictions on HA” in Related Topics)

If the failover type is set to Automatic and the network connection goes down or the network link between the primary and secondary servers becomes unreachable, there is also a small possibility that both the primary and secondary servers will become active at the same time. We refer to this as the “split brain scenario”.

To prevent this, the primary server always checks to see if the secondary server is Active. As soon as the network connection or link is restored and the primary is able to reach the secondary again, the primary server checks the secondary server's state. If the secondary state is Active, then the primary server goes down on its own. Users can then trigger a normal, manual failback to the primary server.

Note that this scenario *only* occurs when the primary HA server is configured for Automatic failover. Configuring the primary server for Manual failover eliminates the possibility of this scenario. This is another reason why we recommend Manual failover configuration.

Automatic failover is especially ill-advised for larger enterprises. If a particular HA deployment chooses to go with Automatic failover anyway, an administrator may be forced to choose between the data that was newly added to the primary or to the secondary. This means, essentially, that there is a possibility of data loss whenever a split-brain scenario occurs. For help dealing with this issue, see “Recovering From Split-Brain Scenario” in Related Topics.

To ensure that HA is managed correctly, Cisco recommends that Prime Infrastructure administrators always confirm the overall health of the HA deployment before initiating failover or failback, including:

- The current state of the primary.
- The current state of the secondary.
- The current state of connectivity between the two servers.

Related Topics

- [Planning HA Deployments](#)
- [Network Throughput Restrictions on HA](#)
- [Triggering Failback](#)
- [Recovering From Split-Brain Scenario](#)

Setting Up High Availability

To use the HA capabilities in Prime Infrastructure, you must:

1. Install a second Prime Infrastructure server, which will run as your secondary server.
2. Configure High Availability mode on the primary server.

Related Topics

- [How High Availability Works](#)
- [Planning HA Deployments](#)
- [Before You Begin Setting Up High Availability](#)
- [Installing the Secondary Server](#)
- [Registering High Availability on the Primary Server](#)
- [What Happens During HA Registration](#)
- [Patching Paired High Availability Servers](#)
- [Patching New High Availability Servers](#)
- [Accessing the Health Monitor Web Page](#)
- [Monitoring High Availability](#)
- [High Availability Reference Information](#)

Before You Begin Setting Up High Availability

Before you begin, you will need:

- The Prime Infrastructure installation software. You will use this software to create the secondary HA server. The version of this software must match the version of Prime Infrastructure installed on your primary server. You can use the CLI **show version** command to verify the current version of the primary server software.
- If you have applied patches to your primary server, you must also patch the secondary server to the same level. Choose **Administration > Licenses and Software Updates > Software Update** to see a list of the patches applied to the primary server. Then, after setting up High Availability, follow the procedure in “Patching Paired High Availability Servers” to patch the secondary server to the same level as the primary server.
- A secondary server with hardware and software specifications that match or exceed the requirements for your primary server. For example: If your primary server was installed as a Prime Infrastructure Standard size OVA, your secondary server must also be installed as a Standard server, and must meet or exceed all requirements given for Standard size servers in the *Cisco Prime Infrastructure Quick Start Guide* (see Related Topics).
- The IP address or host name of the secondary server. You will need these when configuring HA on the primary server. Note that if you plan on using the virtual IP feature (see “Virtual IP Addressing”), the secondary server must be on the same subnet as the primary server.
- The virtual IPv4 and IPv6 (if used) IP address you want to use as the virtual IP for both servers. This is required only if you plan to use the virtual IP feature.
- An authentication key of any length. It must contain at least three of the following types of characters: lowercase letters, uppercase letters, digits and special characters. You will enter this authentication key when you install the secondary server. The HA implementation uses this key to authenticate communications between the primary and secondary servers. Administrators also use the key to configure HA in the primary server, and to log on to the secondary server's Health Monitor page to monitor the HA implementation and troubleshoot problems with it.
- A Prime Infrastructure user ID with Administrator privileges on the primary server.
- A valid email address to which HA state-change notifications can be set. Prime Infrastructure will send email notifications for the following changes: HA registration, failure, failover, and failback.
- For acceptable results: Latency of 220 milliseconds or less, and net throughput of 86 Mbps or more, over the link between the primary and secondary servers. Failure to provide at least this link quality will interfere with data replication and may lead to HA failures. For advice on the range of acceptable performance requirements, see “Network Throughput Restrictions on HA”.
- If there is a firewall configured between the primary and the secondary servers, ensure that the firewall permits incoming and outgoing TCP/UDP on the following ports:
 - 8082: Used by the Health Monitor process to exchange heartbeat messages
 - 1522: Used by Oracle to synchronize data
- If you plan on using Operations Center with an HA implementation of Prime Infrastructure: Ensure that all of your HA-enabled Prime Infrastructure servers (both primary and secondary) have fully resolved host names.

Related Topics

- [Setting Up High Availability](#)
- [Patching Paired High Availability Servers](#)

- [Cisco Prime Infrastructure Quick Start Guide](#)
- [Using Virtual IP Addressing with HA](#)
- [Network Throughput Restrictions on HA](#)

Installing the Secondary Server

If your primary server has been patched, be sure to apply the same patches to your secondary server after installation and before registering HA on the primary server.

Make sure you have already decided on an authentication key, as explained in “Before You Begin Setting Up High Availability” in Related Topics.

-
- Step 1** Begin installing the Prime Infrastructure server software on your secondary server just as you would for a primary server. For instructions on installing the server, see the *Cisco Prime Infrastructure Quick Start Guide*.
- Step 2** During the installation, you will be prompted as follows:
- ```
Will this server be used as a secondary for HA? (yes/no)
```
- Enter **yes** at the prompt.
- Step 3** You will then be prompted for the HA authentication key, as follows:
- ```
Enter Authentication Key:
```
- Enter the authentication key at the prompt. Enter it again at the confirmation prompt.
- Step 4** When the secondary server is installed:
- a. Use the CLI **show version** command on both servers, to verify that they are at the same version and patch level (see “Checking Prime Infrastructure Version and Patch Status” in Related Topics).
 - b. Run the `ncs status` command to verify that all processes are up and running on the secondary server (see “Checking Prime Infrastructure Server Status” in Related Topics).
 - c. Register HA on the primary server (see “Registering High Availability on the Primary Server” in Related Topics).
-

Related Topics

- [Setting Up High Availability](#)
- [Before You Begin Setting Up High Availability](#)
- [Cisco Prime Infrastructure Quick Start Guide](#)
- [Checking Prime Infrastructure Version and Patch Status](#)
- [Checking Prime Infrastructure Server Status](#)
- [Registering High Availability on the Primary Server](#)

Registering High Availability on the Primary Server

You always register HA on the primary server. The primary server needs no configuration during installation in order to participate in the HA configuration. The primary only needs to have the IP address or host name of the secondary server, plus the authentication key you set during the secondary installation, an email address for notifications, and the Failover Type. Note that you follow these same steps when re-registering HA.

-
- Step 1** Log in to Prime Infrastructure with a user ID and password that has administrator privileges.
- Step 2** From the menu, select **Administration > Settings > High Availability**. Prime Infrastructure displays the HA status page.
- Step 3** Select **HA Configuration** and then complete the fields as follows:
- **Secondary Server:** Enter the IP address or the host name of the secondary server.
 - **Authentication Key:** Enter the authentication key password you set during the secondary server installation.
 - **Email Address:** Enter the address (or comma-separated list of addresses) to which notification about HA state changes should be mailed. If you have already configured email notifications using the **Mail Server Configuration** page (see “Configuring Email Settings”), the email addresses you enter here will be appended to the list of addresses already configured for the mail server.
 - **Failover Type:** Select either **Manual** or **Automatic**. We recommend that you select **Manual**.
- Step 4** If you are using the virtual IP feature (see “Virtual IP Addressing” in Related Topics): Select the **Enable Virtual IP** checkbox, then complete the additional fields as follows:
- **IPv4 Virtual IP:** Enter the virtual IPv4 address you want both HA servers to use.
 - **IPv6 Virtual IP:** (Optional) Enter the IPv6 address you want both HA servers to use.
- Note that virtual IP addressing will **not** work unless both servers are on the same subnet.
- Step 5** Click **Save** to save your changes. Prime Infrastructure initiates the HA registration process. When registration completes successfully, **Configuration Mode** will display the value **HA Enabled**.
-

Related Topics

- [Setting Up High Availability](#)
- [Before You Begin Setting Up High Availability](#)
- [High Availability Reference Information](#)
- [Configuring Email Settings](#)
- [Automatic Versus Manual Failover](#)
- [Using Virtual IP Addressing with HA](#)

Checking High Availability Status

You can check on the status of the High Availability enabled on a Prime Infrastructure server.

- Step 1** Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).
- Step 2** Enter the following command to display the current status of Prime Infrastructure HA processes:

```
PIServer/admin# ncs ha status
```

Related Topics

- [Setting Up High Availability](#)
- [Connecting Via CLI](#)

What Happens During HA Registration

Once you finish entering configuration information and click the Save button on the HA Configuration page, the primary and secondary HA servers will register with each other and begin copying all database and configuration data from the primary to the secondary server.

The time required to complete the copying is a function of the amount of database and configuration data being replicated and the available bandwidth on the network link between the two servers. The bigger the data and the slower the link, the longer the replication will take. For a relatively fresh server (in operation for a few days), with 100 devices and a 1 GB-per-second link, copying will take approximately 25 minutes.

During HA registration, the primary and secondary server state will go through the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: HA Not Configured | From: HA Not Configured |
| To: HA Initializing | To: HA Initializing |
| To: Primary Active | To: Secondary Syncing |

You can view these state changes on the HA Status page for the primary server, or the Health Monitor web pages for either of the two servers. If you are using the HA Status page, click **Refresh** to view progress. Once the data is fully synchronized, the HA Status page will be updated to show the current state as “Primary Active”, as shown in the following figure.

Figure 9-3 HA Status Page: Primary Active

The screenshot shows the Cisco Prime Infrastructure web interface. The breadcrumb navigation is "Administration / Settings / High Availability". The page title is "HA Status". On the left, there are two tabs: "HA Status" (selected) and "HA Configuration".

Current Configuration

- Secondary Server: 172.20.116.163
- Fallover Type: Manual

Status

- Current State Mode: Primary Active

Events

| Time | State | Description |
|--------------------------|--------------------------|--|
| Jun 15, 2015 06:55:18 AM | Primary Active | Failed to send email notification: Notification Email Address is not configured. |
| Jun 15, 2015 06:55:18 AM | Primary Active | Completed failback from Secondary Prime Infrastructure 172.20.116.163 [172.20.116.163] |
| Jun 15, 2015 06:54:04 AM | Primary Failback | Starting to failback from secondary Prime Infrastructure 172.20.116.163 [172.20.116.163] |
| Jun 15, 2015 06:53:19 AM | Primary Syncing | Primary Prime Infrastructure Server started successfully as standby |
| Jun 15, 2015 06:53:19 AM | Primary Syncing | Prime Infrastructure started successfully. Prime Infrastructure server state : Primary Syncing |
| Jun 15, 2015 06:34:47 AM | Health Monitor Available | Health Monitor Started |
| Jun 15, 2015 06:34:45 AM | Health Monitor Available | Health Monitor Started |

After registration is initiated, there is a small window of time (usually less than five minutes) during which the database process on the primary server is restarted. During this period, the database will be offline. Once the database server is restarted, Prime Infrastructure initiates synchronization between the primary and the secondary HA servers. The synchronization should not have any impact on user activity, although users may observe slow system response until the synchronization is complete. The length of the synchronization is a function of the total database size and, is handled at the Oracle database level by the Oracle RMAN and Data Guard Broker processes. There is no impact on the execution of user- or system-related activity during the sync.

During registration, Prime Infrastructure performs a full database replication to the secondary server. All processes on the secondary server will be running, but the server itself will be in passive mode. If you execute the Prime Infrastructure CLI command `ncs status` on the secondary server while the secondary server is in the “Secondary Syncing” state, the command output will show all processes as running.

Related Topics

- [How High Availability Works](#)
- [Planning HA Deployments](#)
- [Setting Up High Availability](#)

Patching Paired High Availability Servers

If your current Prime Infrastructure implementation has High Availability servers that are not at the same patch level, or you have a new patch you must install on both your HA servers, follow the steps below.

You must start the patch install with the primary server in “Primary Active” state and the secondary server in “Secondary Syncing” state.

Patching of primary and secondary HA servers takes approximately one hour.

-
- Step 1** Ensure that your HA implementation is enabled and ready for update:
- Log in to the primary server using an ID with Administrator privileges.
 - Select **Administration > Settings > High Availability**. The primary server state displayed on the HA Status page should be “Primary Active”.
 - Select **HA Configuration**. The current Configuration Mode should show “HA Enabled”. We recommend that you set the Failover Type to “manual” during the patch installation.
 - Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:
https://ServerIP:8082
where *ServerIP* is the IP address or host name of the secondary server.
 - You will be prompted for the authentication key entered when HA was enabled. Enter it and click **Login**.
 - Verify that the secondary server state displayed on the HM web page is in the “Secondary Syncing” state.
- Step 2** Download the UBF patch and install it on the primary server:
- Point your browser to the software patches listing for Cisco Prime Infrastructure (see Related Topics).
 - Click the **Download** button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.
 - Log in to the primary server using an ID with administrator privileges and choose **Administration > Licenses and Software Updates > Software Update**.
 - Click the **upload** link at the top of the page and browse to the location where you saved the patch file.
 - Select the UBF file and then click **OK** to upload the file.
 - When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.
 - Select the patch file and click **Install**. When the installation is complete, you will see a message confirming this.
 - After the installation is complete on the primary server, verify that the Status of Updates table on the Software Update page shows “Installed” or “Installed [Requires Restart]” for the patch.
- Step 3** Install the same patch on the secondary server:
- Access the secondary server’s HM web page and login if needed.
 - Click the HM web page’s **Software Update** link. You will be prompted for the authentication key a second time. Enter it and click **Login** again.

- c. Click **Upload Update File** and browse to the location where you saved the patch file.
- d. Select the UBF file and then click **OK** to upload the file.
- e. When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.
- f. Select the patch file and click **Install**. When the installation is complete, you will see a message confirming this.
- g. After the installation is complete on the secondary server, verify that the Status of Updates table on the Software Update page shows “Installed” or “Installed [Requires failover]” for the patch.

Step 4 Stop the primary server using the **ncs stop** command as explained in “Stopping Prime Infrastructure”:

Step 5 Failover to the secondary using the secondary server’s HM web page:

- a. Access the secondary server’s HM web page and login if needed
- b. Click **Failover** to initiate a failover from the primary to the secondary server. It will take 2 to 3 minutes for the operation to complete.
- c. Before continuing: Verify that the secondary server state displayed on the HM web page is “Secondary Active”.

Note that, if you currently have the Failover Type configured to “automatic”, all of this will happen automatically.

Step 6 Re-start the primary server:

- a. Run the **ncs start** command (see “Starting Prime Infrastructure”) to start the primary server. Wait for the processes on the primary to restart.
- b. Run the **ncs status** command (see “Checking Prime Infrastructure Server Status”) to verify that the primary’s processes have re-started.
- c. Before continuing: Access the primary server’s HM web page and verify that the primary server state displayed is “Primary Synching”.

Step 7 Failback to the primary using the secondary server’s HM web page:

- a. Access the secondary server’s HM web page and login if needed.
- b. Click **Failback** to initiate a failback from the secondary to the primary server. It will take 2 to 3 minutes for the operation to complete. As soon as failback completes, the secondary server will be automatically restarted in the standby mode. It will take a maximum of 15 minutes for the restart to complete, and it will be synched with the primary server.

You can verify the restart by logging into the secondary server’s HM web page and looking for the message “Prime Infrastructure stopped successfully” followed by “Prime Infrastructure started successfully.”

- c. Before continuing: Run the **ncs ha status** command on both the primary and secondary servers. Verify that the primary server state changes to “Primary Active” and the secondary server state is “Secondary Synching”.

Step 8 Once failback completes, verify the patch installation as follows:

- a. Log in to the primary server and access its Software Update page as you did in step 2, above. The “Status” column on the Status of Updates > Update tab should show “Installed” for the patch.
- b. Access the secondary server’s Software Update page as you did in step 3, above. The “Status” column on the Status of Updates > Updates tab should show “Installed” for the patch.

Related Topics

- [Setting Up High Availability](#)
- [software patches listing for Cisco Prime Infrastructure](#)
- [Stopping Prime Infrastructure](#)
- [Starting Prime Infrastructure](#)
- [Checking Prime Infrastructure Server Status](#)
- [Checking High Availability Status](#)

Patching New High Availability Servers

If you are setting up a new Prime Infrastructure High Availability (HA) implementation and your new servers are not at the same patch level, follow the steps below to install patches on both servers and bring them to the same patch level.

-
- Step 1** Download the patch and install it on the primary server:
- Point your browser to the software patches listing for Cisco Prime Infrastructure (see Related Topics).
 - Click the **Download** button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.
 - Log in to the primary server using an ID with administrator privileges and choose **Administration > Licenses and Software Updates > Software Update**.
 - Click the **upload** link at the top of the page and browse to the location where you saved the patch file.
 - Select the UBF file and click **OK** to upload the file.
 - When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.
 - Select the patch file and click **Install**. When the installation is complete, you will see a message confirming this.
 - After the installation is complete on the primary server, verify that the Status of Updates table on the Software Update page shows “Installed” or “Installed [Requires Restart]” for the patch.
 - Before you continue, restart the primary server as follows:
 - Use the **ncs stop** and **ncs start** commands to restart the server.
 - Use the **ncs status** command to verify that the primary’s Health Monitor and other processes have restarted.
- Step 2** Install the same patch on the secondary server:
- Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:
https://ServerIP:8082
where *ServerIP* is the IP address or host name of the secondary server.
 - You will be prompted for the secondary server authentication key. Enter it and click **Login**.
 - Click the HM web page’s **Software Update** link. You will be prompted for the authentication key a second time. Enter it and click **Login** again.

- d. Click **Upload Update File** and browse to the location where you saved the patch file.
- e. Select the UBF file and click **OK** to upload the file.
- f. When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.
- g. Select the patch file and click **Install**. When the installation is complete, you will see a message confirming this.
- h. After the installation is complete on the secondary server, verify that the Status of Updates table on the Software Update page shows “Installed” or “Installed [Requires failover]” for the patch.
- i. Before you continue, restart the secondary server as follows:
 - Use the **ncs stop** and **ncs start** commands to restart the server.
 - Use the **ncs status** command to verify that the secondary’s Health Monitor and other processes have restarted.

Step 3 Verify that the patch status is the same both servers, as follows:

- a. Log in to the primary server and access its Software Update page as you did in step 1, above. The “Status” column should show “Installed” instead of “Installed [Requires Restart]” for the installed patch.
- b. Access the secondary server’s Health Monitor page as you did in step 2, above. The “Status” column should show “Installed” instead of “Installed [Requires Failover]” for the installed patch

Step 4 Register the servers.

Related Topics

- [Setting Up High Availability](#)
- [software patches listing for Cisco Prime Infrastructure](#)
- [Restarting Prime Infrastructure](#)
- [Checking Prime Infrastructure Server Status](#)
- [Registering High Availability on the Primary Server](#)

Monitoring High Availability

Once you have configured HA and registered it on the primary server, most of your interactions with HA will involve accessing the server Health Monitor web page and responding to email notifications by triggering a failover or failback. These processes, as well as special situations requiring more complicated responses, are covered in the following Related Topics.

Related Topics

- [Accessing the Health Monitor Web Page](#)
- [Triggering Failover](#)
- [Triggering Failback](#)
- [Responding to Other HA Events](#)

Accessing the Health Monitor Web Page

You can access the Health Monitor web page for the primary or secondary server at any time by pointing your browser to the following URL:

```
https://Server:8082
```

where *Server* is the IP address or host name of the primary or secondary server whose Health Monitor web page you want to see.

You can also access the Health Monitor web page for the currently active server by logging in to Prime Infrastructure, selecting **Administration > Settings > High Availability**, and then clicking the **Launch Health Monitor** link at the top right of the HA Status page.

Related Topics

- [Monitoring High Availability](#)

Triggering Failover

Failover is the process of activating the secondary server in response to a detected failure on the primary.

Health Monitor (HM) detects failure conditions using the heartbeat messages that the two servers exchange. If the primary server is not responsive to three consecutive heartbeat messages from the secondary, it is considered to have failed. During the health check, HM also checks the application process status and database health; if there is no proper response to these checks, these are also treated as having failed.

The HA system takes approximately 10 to 15 seconds to detect a process failure on the primary server and initiate a failover. If the secondary server is unable to reach the primary server due to a network issue, it might take more time to initiate a failover. In addition, it may take additional time for the application processes on the secondary server to be fully operational.

As soon as HM detects the failure, it sends an email notification. The email includes the failure status along with a link to the secondary server's Health Monitor web page.

If HA is currently configured for automatic failover, the secondary server will activate automatically and there is no action you need to perform.

If HA is currently configured for manual failover, you must trigger the failover as follows:

-
- | | |
|---------------|--|
| Step 1 | Access the secondary server's Health Monitor web page using the web link given in the email notification, or using the steps in “Accessing the Health Monitor Web Page”. |
| Step 2 | Trigger the failover by clicking the Failover button. |
-

Related Topics

- [How High Availability Works](#)
- [Monitoring High Availability](#)
- [Registering High Availability on the Primary Server](#)
- [Accessing the Health Monitor Web Page](#)

Triggering Failback

Failback is the process of re-activating the primary server once it is back online. It also transfers Active status from the secondary server to the primary, and stops active network monitoring processes on the secondary.

During failback, the secondary server is available except during the period when processes are re-started on the secondary. Both servers' Health Monitor web pages are accessible for monitoring the progress of the failback. Additionally, users can also connect to the secondary server to access all normal functionality, except for these caveats:

- Do not initiate configuration or provisioning activity while the failback is in progress.
- Be aware that, after a successful failback, the secondary server will go into passive (“Secondary Syncing”) mode and control will switch over to the primary server. During this process, Prime Infrastructure will be inaccessible to the users for a few moments.

You must always trigger failback manually, as follows:

Step 1 Access the secondary server's Health Monitor web page using the link given in the email notification, or using the steps in “Accessing the Health Monitor Web Page”.

Step 2 Trigger the failback by clicking the **Failback** button.

The secondary server is automatically restarted in the standby mode after the failback and is automatically synced with the primary server. The primary server will now be the available Prime Infrastructure server.

Related Topics

- [How High Availability Works](#)
- [Monitoring High Availability](#)
- [Accessing the Health Monitor Web Page](#)

Responding to Other HA Events

All the HA related events are displayed on the HA Status page, the Health Monitor web pages, and under the Prime Infrastructure Alarms and Events page. Most events require no response from you other than triggering failover and failback. A few events are more complex, as explained in the related topics.

Related Topics

- [HA Registration Fails](#)
- [Network is Down \(Automatic Failover\)](#)
- [Network is Down \(Manual Failover\)](#)
- [Process Restart Fails \(Manual Failover\)](#)
- [Process Restart Fails \(Manual Failover\)](#)
- [Primary Server Restarts During Sync \(Manual Failover\)](#)
- [Secondary Server Restarts During Sync](#)
- [Both HA Servers Are Down](#)
- [Both HA Servers Are Down and the Secondary Will Not Restart](#)
- [Replacing the Primary Server](#)
- [Recovering From Split-Brain Scenario](#)

HA Registration Fails

If HA registration fails, you will see the following HA state-change transitions for each server (instead of those detailed in “What Happens During HA Registration”):

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: HA Initializing | From: HA Initializing |
| To: HA Not Configured | To: HA Not Configured |

To recover from failed HA registration, follow the steps below.

-
- Step 1** Use ping and other tools to check the network connection between the two Prime Infrastructure servers. Confirm that the secondary server is reachable from the primary, and vice versa.
 - Step 2** Check that the gateway, subnet mask, virtual IP address (if configured), server hostname, DNS, NTP settings are all correct.
 - Step 3** Check that the configured DNS and NTP servers are reachable from the primary and secondary servers, and that both are responding without latency or other network-specific issues.
 - Step 4** Check that all Prime Infrastructure licenses are correctly configured.
 - Step 5** Once you have remedied any connectivity or setting issues, try the steps in “Registering High Availability on the Primary Server” again.
-

Related Topics

- [Responding to Other HA Events](#)
- [What Happens During HA Registration](#)
- [Registering High Availability on the Primary Server](#)

Network is Down (Automatic Failover)

If there is a loss of network connectivity between the two Prime Infrastructure servers, you will see the following HA state-change transitions for each server, assuming that the Failover Type is set to “Automatic”:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Active | From: Secondary Syncing |
| To: Primary Lost Secondary | To: Secondary Lost Primary |
| To: Primary Lost Secondary | To: Secondary Failover |
| To: Primary Lost Secondary | To: Secondary Active |

You will get an email notification that the secondary is active.

-
- Step 1** Check on and restore network connectivity between the two servers. Once network connectivity is restored and the primary server can detect that the secondary is active, all services on the primary will be restarted and made passive automatically. You will see the following state changes:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Lost Secondary | From: Secondary Active |
| To: Primary Failover | To: Secondary Active |
| To: Primary Syncing | To: Secondary Active |

- Step 2** Trigger a failback from the secondary to the primary. You will then see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Syncing | From: Secondary Active |
| To: Primary Failback | To: Secondary Failback |
| To: Primary Failback | To: Secondary Post Failback |
| To: Primary Active | To: Secondary Syncing |

Related Topics

- [Responding to Other HA Events](#)
- [Triggering Failback](#)

Network is Down (Manual Failover)

If there is a loss of network connectivity between the two Prime Infrastructure servers, you will see the following HA state-change transitions for each server, assuming that the Failover Type is set to “Manual”:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Active | From: Secondary Syncing |
| To: Primary Lost Secondary | To: Secondary Lost Primary |

You will get email notifications that each server has lost the other.

- Step 1** Check on and, if needed, restore the network connectivity between the two servers. You will see the following state changes once network connectivity is restored.:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Lost Secondary | From: Secondary Lost Primary |
| To: Primary Active | To: Secondary Syncing |

No administrator response is required.

- Step 2** If network connection cannot be restored for any reason, use the HM web page for the secondary server to trigger a failover from the primary to the secondary server. You will see the following state changes:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Lost Secondary | From: Secondary Lost Primary |
| To: Primary Lost Secondary | To: Secondary Failover |
| To: Primary Failover | To: Secondary Active |

You will get an email notification that the secondary server is now active.

- Step 3** Check and restore network connectivity between the two servers. Once network connectivity is restored and the primary server detects that the secondary server is active, all services on the primary server will be restarted and made passive. You will see the following state changes:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Lost Secondary | From: Secondary Active |
| To: Primary Failover | To: Secondary Active |
| To: Primary Syncing | To: Secondary Active |

- Step 4** Trigger a failback from the secondary to the primary. You will then see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Syncing | From: Secondary Active |
| To: Primary Failback | To: Secondary Failback |
| To: Primary Failback | To: Secondary Post Failback |
| To: Primary Active | To: Secondary Syncing |

Related Topics

- [Responding to Other HA Events](#)
- [Triggering Failback](#)

Process Restart Fails (Automatic Failover)

The Prime Infrastructure Health Monitor process is responsible for attempting to restart any Prime Infrastructure server processes that have failed. Generally speaking, the current state of the primary and secondary servers should be “Primary Active” and “Secondary Syncing” at the time any such failures occur.

If HM cannot restart a critical process on the primary server, then the primary server is considered to have failed. If your currently configured Failover Type is “automatic”, you will see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Active | From: Secondary Syncing |
| To: Primary Uncertain | To: Secondary Lost Primary |
| To: Primary Failover | To: Secondary Failover |
| To: Primary Failover | To: Secondary Active |

When this process is complete, you will get an email notification that the secondary server is now active.

- Step 1** Restart the primary server and ensure that it is running. Once the primary is restarted, it will be in the state “Primary Syncing”. You will see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|------------------------------------|-----------------------------------|
| From: Primary Failover | From: Secondary Active |
| To: Primary Preparing for Failback | To: Secondary Active |
| To: Primary Syncing | To: Secondary Active |

Step 2 Trigger a failback from the secondary to the primary. You will then see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Syncing | From: Secondary Active |
| To: Primary Failback | To: Secondary Failback |
| To: Primary Failback | To: Secondary Post Failback |
| To: Primary Active | To: Secondary Syncing |

Related Topics

- [Responding to Other HA Events](#)
- [Triggering Failback](#)

Process Restart Fails (Manual Failover)

The Prime Infrastructure Health Monitor process is responsible for attempting to restart any Prime Infrastructure server processes that have failed. Generally speaking, the current state of the primary and secondary servers should be “Primary Active” and “Secondary Syncing” at the time any such failures occur. If HM cannot restart a critical process on the primary server, then the primary server is considered to have failed. You will receive an email notification of this failure. If your currently configured Failover Type is “Manual”, you will see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Active | From: Secondary Syncing |
| To: Primary Uncertain | To: Secondary Lost Primary |

Step 1 Trigger on the secondary server a failover from the primary to the secondary. You will then see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Uncertain | From: Secondary Syncing |
| To: Primary Failover | To: Secondary Failover |
| To: Primary Failover | To: Secondary Active |

Step 2 Restart the primary server and ensure that it is running. Once the primary server is restarted, the primary’s HA state will be “Primary Syncing”. You will see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|------------------------------------|-----------------------------------|
| From: Primary Failover | From: Secondary Active |
| To: Primary Preparing for Failback | To: Secondary Active |
| To: Primary Syncing | To: Secondary Active |

Step 3 Trigger a failback from the secondary to the primary. You will then see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Syncing | From: Secondary Active |
| To: Primary Failback | To: Secondary Failback |
| To: Primary Failback | To: Secondary Post Failback |
| To: Primary Active | To: Secondary Syncing |

Related Topics

- [Responding to Other HA Events](#)
- [Triggering Failover](#)
- [Triggering Failback](#)

Primary Server Restarts During Sync (Manual Failover)

If the primary Prime Infrastructure server is restarted while the secondary server is syncing, you will see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Active | From: Secondary Syncing |
| To: Primary Alone | To: Secondary Lost Primary |
| To: Primary Active | To: Secondary Syncing |

The “Primary Alone” and “Primary Active” states occur immediately after the primary comes back online. No administrator response should be required.

Related Topics

- [Responding to Other HA Events](#)

Secondary Server Restarts During Sync

If the secondary Prime Infrastructure server is restarted while syncing with the primary server, you will see the following state transitions:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: Primary Active | From: Secondary Syncing |
| To: Primary Lost Secondary | From: Secondary Lost Primary |
| To: Primary Active | To: Secondary Syncing |

No administrator response should be required.

Related Topics

- [Responding to Other HA Events](#)

Both HA Servers Are Down

If both the primary and secondary servers are down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

-
- Step 1** Restart the secondary server and the instance of Prime Infrastructure running on it. If for some reason you cannot restart the secondary server, see “Both HA Servers Are Down and Secondary Will Not Restart” in Related Topics.
- Step 2** When Prime Infrastructure is running on the secondary, access the secondary server’s Health Monitor web page. You will see the secondary server transition to the state “Secondary Lost Primary”.
- Step 3** Restart the primary server and the instance of Prime Infrastructure running on it. When Prime Infrastructure is running on the primary, the primary will automatically sync with the secondary. To verify this, access the primary server’s Health Monitor web page. You will see the two servers transition through the following series of HA states:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| To: Primary Lost Secondary | To: Secondary Lost Primary |
| To: Primary Active | To: Secondary Syncing |

Related Topics

- [Both HA Servers Are Down and the Secondary Will Not Restart](#)
- [Accessing the Health Monitor Web Page](#)
- [Responding to Other HA Events](#)

Both HA Servers Are Powered Down

If both the primary and secondary servers are powered down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

-
- Step 1** Power on the secondary server and the instance of Prime Infrastructure running on it.
The secondary HA restart will fail at this stage because the primary is not reachable. However, the secondary Health Monitor process will be running with an error.
- Step 2** When Prime Infrastructure is running on the secondary, access the secondary server's Health Monitor web page. You will see the secondary server transition to the state "Secondary Lost Primary".
- Step 3** Power on the primary server and the instance of Prime Infrastructure running on it.
- Step 4** When Prime Infrastructure is running on the primary, the primary will automatically sync with the secondary. To verify this, access the primary server's Health Monitor web page. You will see the two servers transition through the following series of HA states:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| To: Primary Lost Secondary | To: Secondary Lost Primary |
| To: Primary Active | To: Secondary Syncing |

- Step 5** Restart the secondary server and the instance of Prime Infrastructure running on it. This is required because not all processes will be running on the secondary at this point.
If for some reason you cannot restart the secondary server, see "Both HA Servers Are Down and Secondary Will Not Restart" in Related Topics.
- Step 6** When Prime Infrastructure finishes restarting on the secondary server, all processes should be running. Verify this by running the `ncs status` command (see "Checking Prime Infrastructure Server Status" in Related Topics).
-

Related Topics

- [Both HA Servers Are Down and the Secondary Will Not Restart](#)
- [Accessing the Health Monitor Web Page](#)
- [Checking Prime Infrastructure Server Status](#)
- [Responding to Other HA Events](#)

Both HA Servers Are Down and the Secondary Will Not Restart

If both HA servers are down at the same time and the secondary will not restart, you will need to remove the HA configuration from the primary server in order to use it as a standalone until you can replace or restore the secondary server.

The following steps assume that you have already tried and failed to restart the secondary server.

-
- Step 1** Attempt to restart the primary instance of Prime Infrastructure. If the primary is able to restart at all, the restart will abort with an error message indicating that you must remove the HA configuration.
- Step 2** Open a CLI session with the primary Prime Infrastructure server (see “Connecting Via CLI” in Related Topics).
- Step 3** Enter the following command to remove the HA configuration on the primary server:
- ```
PIServer/admin# ncs ha remove
```
- Step 4** You will be prompted to confirm that you want to remove the HA configuration. Answer **Y** to the prompt.
- Step 5** You will be prompted to confirm that you want to remove all the HA database information from both the primary and secondary servers. Answer **N** to this second prompt.
- Step 6** You should now be able to restart the primary instance of Prime Infrastructure without the error message and use it as a standalone.

When you are able to restore or replace the secondary server, proceed as explained in “Registering High Availability on the Primary Server” in Related Topics.

---

### Related Topics

- [Connecting Via CLI](#)
- [Accessing the Health Monitor Web Page](#)
- [Registering High Availability on the Primary Server](#)
- [Removing HA Via the CLI](#)
- [Responding to Other HA Events](#)

## Replacing the Primary Server

Under normal circumstances, the state of your primary and secondary servers will be “Primary Active” and “Secondary Syncing”, respectively. If the primary server fails for any reason, a failover to the secondary will take place, either automatically or manually.

You may find that restoring full HA access requires you to reinstall the primary server using new hardware. If this happens, you can follow the steps below to bring up the new primary server without data loss.

- 
- Step 1** Ensure that the secondary server is currently in “Secondary Active” state. If you have set the Failover Type on the primary server to “manual”, you will need to trigger the failover to the secondary manually.
- Step 2** Ensure that the old primary server you are replacing has been disconnected from the network.
- Step 3** Ensure that the new primary server is ready for use. This will include connecting it to the network and assigning it the same server IP, subnet mask, gateway as the old primary server. You will also need to enter the same authentication key that you entered when installing the secondary server.
- Step 4** Trigger a failback from the secondary to the newly installed primary. You will see the two servers transition through the following series of HA states:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: HA not configured         | From: Secondary Active            |
| To: Primary Failback            | To: Secondary Failback            |
| To: Primary Failback            | To: Secondary Post Failback       |
| To: Primary Active              | To: Secondary Syncing             |

---

### Related Topics

- [Triggering Failover](#)
- [Triggering Failback](#)
- [Responding to Other HA Events](#)



## Recovering From Split-Brain Scenario

As explained in “Automatic Versus Manual Failover” (see Related Topics), the possibility of data loss always exists on the rare occasions when a “split-brain scenario” occurs. The choices and actions available to the Prime Infrastructure administrator in this case are as follows:

1. Choose to go with the newly added data on the primary and forget the data that was added on the secondary. To choose this option:
  - a. Once the network is up, the primary will go down and the HA status of the primary server will be “Primary Failover” and then “Primary Syncing”.
  - b. Remove HA using the primary or secondary CLI (see “Removing HA Via the CLI”).
  - c. Restart the primary server (see “Restarting Prime Infrastructure”).
  - d. Re-register the secondary with the primary using the primary HA Configuration page (see “Registering High Availability on the Primary Server”).
2. Choose to go with the newly added data on the secondary and forget the data that was added on the primary. To choose this option:
  - a. Once the network is up and the primary sees that the secondary server is up, the primary will restart itself automatically, using its standby database. The HA status of the primary server will be “Primary Failover”, transitioning to “Primary Syncing”. You can verify this by logging on to the primary server’s Health Monitor web page.
  - b. Once the primary server’s status is “Primary Syncing”: Using the web browser, confirm that a user can log into the secondary server’s Prime Infrastructure page (for example, <https://x.x.x.x:443>). Do *not* proceed until you have verified this access is possible.
  - c. Once access to the secondary is verified, initiate a failback from the secondary server's Health Monitor web page (see “Triggering Failback”). Users can continue to perform monitoring activities on the secondary server until the switchover to the primary is completed.

### Related Topics

- [Automatic Versus Manual Failover](#)
- [Removing HA Via the CLI](#)
- [Restarting Prime Infrastructure](#)
- [Registering High Availability on the Primary Server](#)
- [Triggering Failback](#)
- [Responding to Other HA Events](#)

# High Availability Reference Information

The following sections supply reference information on HA.

## Related Topics

- [HA Configuration Mode Reference](#)
- [HA State Reference](#)
- [HA State Transition Reference](#)
- [High Availability CLI Command Reference](#)
- [Resetting the HA Authentication Key](#)
- [Removing HA Via the GUI](#)
- [Removing HA Via the CLI](#)
- [Removing HA During Restore](#)
- [Removing HA During Upgrade](#)
- [Using HA Error Logging](#)
- [Resetting the HA Server IP Address or Host Name](#)

## HA Configuration Mode Reference

The following table lists all possible HA configuration modes.

**Table 9-1** High Availability Modes

| Mode              | Description                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HA not configured | HA is not configured on this Prime Infrastructure server                                                                                                         |
| HA initializing   | The HA registration process between the primary and secondary server has started.                                                                                |
| HA enabled        | HA is enabled between the primary and secondary server.                                                                                                          |
| HA alone          | Primary server is now running alone. HA is enabled, but the primary server is out of sync with the secondary, or the secondary is down or otherwise unreachable. |

## Related Topics

- [High Availability Reference Information](#)

## HA State Reference

The following table lists all possible HA states, including those that require no response from you.

**Table 9-2 High Availability States**

| State                          | Server    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stand Alone                    | Both      | HA is not configured on this Prime Infrastructure server                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Primary Alone                  | Primary   | Primary restarted after it lost secondary. Only Health Monitor is running in this state.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| HA Initializing                | Both      | HA Registration process between the primary and secondary server has started.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Primary Active                 | Primary   | Primary server is now active and is synchronizing with secondary server.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Primary Database Copy Failed   | Primary   | Primary servers being restarted will always check to see if a data gap has occurred due to the primary being down for 24 hours or more. If it detects such a gap, it will automatically trigger a data copy from the active secondary server. In rare cases, this database copy can fail, in which case this transition state is set on the primary. All attempts to failback to the primary are blocked until the database copy completes successfully. As soon as it does, the primary state is set to "Primary Syncing". |
| Primary Failover               | Primary   | Primary server detected a failure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Primary Failback               | Primary   | Failback triggered by the User is currently in progress.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Primary Lost Secondary         | Primary   | Primary server is unable to communicate with the secondary server.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Primary Preparing for Failback | Primary   | This state will be set on primary server startup after a failover to the secondary. This state signifies that the primary server has started up in standby mode (because the secondary server is still active) and is ready for failback. Once the primary server is ready for failback, its state will be set to "Primary Syncing".                                                                                                                                                                                        |
| Primary Syncing                | Primary   | Primary server is synchronizing the database and configuration files from the active secondary. Primary gets into this state when primary processes are brought up after failover to secondary and secondary is playing the active role.                                                                                                                                                                                                                                                                                    |
| Primary Uncertain              | Primary   | Primary server's application processes are not able to connect to its database.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Secondary Alone                | Secondary | Primary server is not reachable from secondary after primary server restart.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Secondary Syncing              | Secondary | Secondary server is synchronizing the database and configuration files from the primary.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Secondary Active               | Secondary | Failover from the primary server to the secondary server has completed successfully.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Secondary Lost Primary         | Secondary | Secondary server is not able to connect to the primary server (occurs when the primary fails or network connectivity is lost).<br><br>In case of automatic failover from this state, the secondary will automatically move to Active state. In case of a manual failover, the user can trigger a failover to make the secondary active.                                                                                                                                                                                     |
| Secondary Failover             | Secondary | Failover triggered and in progress.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Secondary Failback             | Secondary | Failback triggered and in progress (database and file replication is in progress).                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 9-2 High Availability States (continued)

| State                   | Server    | Description                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secondary Post Failback | Secondary | This state occurs after failback is triggered, replication of database and configuration files from the secondary to the primary is complete, and Health Monitor has initiated changes of the secondary server's status to Secondary Syncing and the primary server's status to Primary Active. These status changes and associated process starts and stops are in progress. |
| Secondary Uncertain     | Secondary | Secondary server's application processes are not able to connect to secondary server's database.                                                                                                                                                                                                                                                                              |

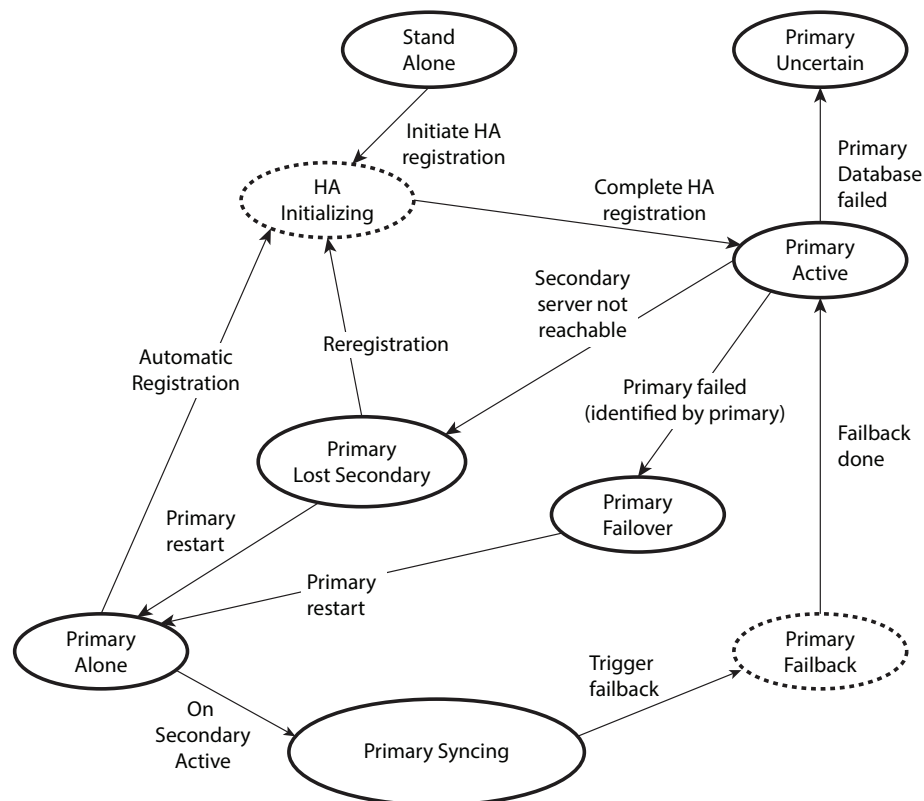
**Related Topics**

- [High Availability Reference Information](#)

## HA State Transition Reference

The following figure details all possible state transitions for the primary server.

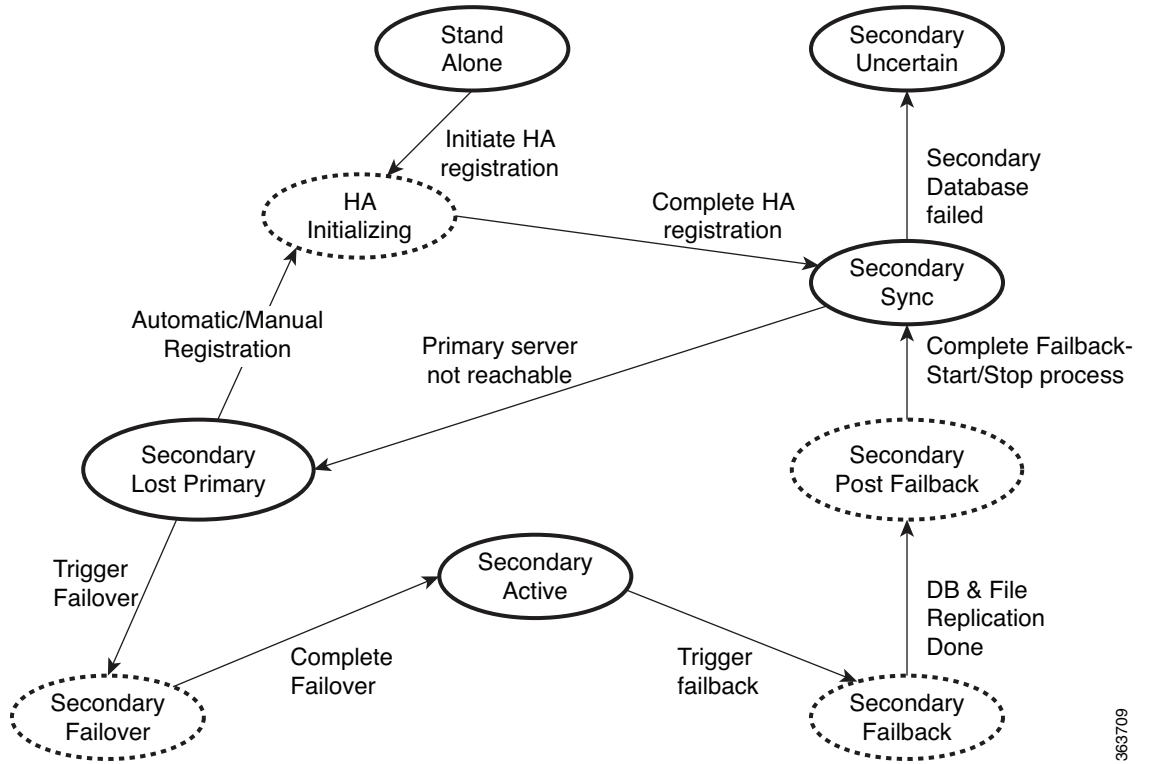
Figure 9-4 Primary Server State Transitions



404588

The following figure details all possible state transitions for the secondary server.

**Figure 9-5 Secondary Server State Transitions**



963709

**Related Topics**

- [High Availability Reference Information](#)

## High Availability CLI Command Reference

The following table lists the CLI commands available for HA management. Log in as admin to run these commands on the primary server (see [Connecting Via CLI](#)):

**Table 9-3 High Availability Commands**

| Command                | Description                                         |
|------------------------|-----------------------------------------------------|
| ncs ha ?               | Get help with high availability CLI commands        |
| ncs ha authkey authkey | Update the authentication key for high availability |
| ncs ha remove          | Remove the High Availability configuration          |
| ncs ha status          | Get the current status for High Availability        |

**Related Topics**

- [High Availability Reference Information](#)

## Resetting the HA Authentication Key

Prime Infrastructure administrators can change the HA authentication key using the `ncs ha authkey` command. You will need to ensure that the new authorization key meets the password standards.

---

**Step 1** Connect to the primary server via CLI. Do not enter “configure terminal” mode.

**Step 2** Enter the following at the command line:

```
admin# ncs ha authkey MyNewAuthKey
```

Where *MyNewAuthKey* is the new authorization key.

---

### Related Topics

- [Before You Begin Setting Up High Availability](#)
- [Connecting Via CLI](#)
- [High Availability Reference Information](#)

## Removing HA Via the GUI

The simplest method for removing an existing HA implementation is via the GUI, as shown in the following steps. You can also remove the HA setup via the command line.

---

**Step 1** Log in to Prime Infrastructure with a user ID that has administrator privileges.

**Step 2** Select **Administration > Settings > High Availability**.

**Step 3** Select **Remove**.

---

### Related Topics

- [Removing HA Via the CLI](#)
- [Connecting Via CLI](#)
- [High Availability Reference Information](#)

## Removing HA Via the CLI

If for any reason you cannot access the Prime Infrastructure GUI on the primary server, administrators can remove the HA setup via the command line, as follows:

---

**Step 1** Connect to the primary server via CLI. Do not enter “configure terminal” mode.

**Step 2** Enter the following at the command line:

```
admin# ncs ha remove
```

---

### Related Topics

- [Removing HA Via the GUI](#)
- [Connecting Via CLI](#)
- [Removing HA Via the CLI](#)
- [High Availability Reference Information](#)

## Removing HA During Restore

Prime Infrastructure does not back up configuration settings related to High Availability.

In order to restore a Prime Infrastructure implementation that is using HA, be sure to restore the backed up data to the primary server only. The restored primary will automatically replicate its data to the secondary server. Running a restore on the secondary server is not needed and will generate an error message if you attempt it.

To restore a Prime Infrastructure implementation that uses HA, follow the steps below.

---

**Step 1** Use the CLI to remove the HA settings from the primary server.

**Step 2** Restore the primary server as needed.

**Step 3** Once the restore is complete, perform the HA registration process again.

---

### Related Topics

- [Removing HA Via the GUI](#)
- [Restoring From Backups](#)
- [Registering High Availability on the Primary Server](#)
- [Connecting Via CLI](#)
- [High Availability Reference Information](#)

## Removing HA During Upgrade

To upgrade a Prime Infrastructure implementation that uses HA, follow the steps below.

- 
- Step 1** Use the CLI to remove the HA settings from the primary server (see “Removing HA Via the CLI” in Related Topics, below).
  - Step 2** Upgrade the primary server as needed.
  - Step 3** Upgrade the secondary server as needed.
  - Step 4** Once the upgrade is complete, perform the HA registration process again.
- 

### Related Topics

- [Removing HA Via the CLI](#)
- [Registering High Availability on the Primary Server](#)
- [Connecting Via CLI](#)
- [High Availability Reference Information](#)

## Using HA Error Logging

Error logging for the High Availability feature is disabled by default, to save disk space and maximize performance. If you are having trouble with HA, the best place to begin is by enabling error logging and to examine the log files.

- 
- Step 1** View the Health Monitor page for the server having trouble.
  - Step 2** In the **Logging** area, in the **Message Level** dropdown, select the error-logging level you want.
  - Step 3** Click **Save**.
  - Step 4** When you want to download the log files: In the **Logs** area, click **Download**. You can open the downloaded log files using any ASCII text editor.
- 

### Related Topics

- [Accessing the Health Monitor Web Page](#)
- [High Availability Reference Information](#)



## Resetting the HA Server IP Address or Host Name

Avoid changing the IP address or hostname of the primary or secondary HA server, if possible. If you must change the IP address or hostname, remove the HA configuration from the primary server before making the change. When finished, re-register HA.

### Related Topics

- [Removing HA Via the GUI](#)
- [Registering High Availability on the Primary Server](#)
- [High Availability Reference Information](#)

## Configuring MSE High Availability

The Cisco Mobility Services Engine (MSE) is a platform for hosting multiple mobility applications. Under an MSE high availability (HA) configuration, an active MSE is backed up by another inactive instance of MSE. The active MSE is called the primary MSE and the inactive MSE is called the secondary MSE.

### Related Topics

- [Overview of the MSE High Availability Architecture](#)
- [Setting Up MSE High Availability: Workflow](#)

## Overview of the MSE High Availability Architecture

The main component of MSE high availability is the health monitor. The health monitor configures, manages, and monitors the HA setup on each MSE. Heartbeat is maintained between the primary and secondary MSE. Health monitor is responsible for setting up the database, file replication, and monitoring the application. When the primary MSE fails and the secondary MSE takes over, the virtual address of the primary MSE is switched transparently to the secondary MSE. Note that:

- Every active primary MSE is backed up by another inactive instance. The purpose of the secondary MSE is to monitor the availability and state of the primary MSE. The secondary MSE becomes active only after the failover procedure is initiated.
- One secondary MSE can support one primary MSE.

The MSEs, Synchronize Services, Synchronization History, High Availability, Context Aware Notifications, and Mobile Concierge pages on the Services tab are available only in the virtual domain in Release 7.3.

The following related topics provide additional details on the MSE high availability architecture.

### Related Topics

- [MSE High Availability Pairing Matrix](#)
- [Guidelines and Limitations for MSE High Availability](#)
- [Failover Scenario for MSE High Availability](#)
- [Failback Scenario for MSE High Availability](#)
- [Licensing Requirements for MSE High Availability](#)
- [Configuring MSE High Availability](#)

## MSE High Availability Pairing Matrix

The following table lists the types of MSE servers that can be paired in a high-availability configuration.

**Table 9-4** MSE High Availability Server Pairing Matrix

| Primary Server Type | Secondary Server Type |      |      |      |      |
|---------------------|-----------------------|------|------|------|------|
|                     | 3355                  | VA-2 | VA-3 | VA-4 | VA-5 |
| 3355                | Y                     | N    | N    | N    | N    |
| VA-2                | N                     | Y    | Y    | Y    | Y    |
| VA-3                | N                     | N    | Y    | Y    | Y    |
| VA-4                | N                     | N    | N    | Y    | Y    |
| VA-5                | N                     | N    | N    | N    | Y    |

### Related Topics

- [Overview of the MSE High Availability Architecture](#)
- [Guidelines and Limitations for MSE High Availability](#)

## Guidelines and Limitations for MSE High Availability

Administrators implementing MSE High Availability and planning to manage it via Prime Infrastructure should observe the following guidelines and limitations:

- Both the health monitor IP and virtual IP should be accessible from Prime Infrastructure.
- The health monitor IP and virtual IP should always be different. The health monitor and virtual interface can be on the same network interface or different interfaces.
- You can use either manual or automatic failover. Failover should be considered temporary. The failed MSE should be restored to normal as soon as possible, and failback should be re-initiated. The longer it takes to restore the failed MSE, the longer you are running with a single MSE without high availability support.
- You can use either manual or automatic failback.
- Both the primary and secondary MSE should be running the same software version.
- High Availability over WAN is not supported.
- High Availability over LAN is supported only when both the primary and secondary MSEs are in the same subnet.
- The ports over which the primary and secondary MSEs communicate must be open (not blocked with network firewalls, application firewalls, gateways, and so on). The following input/output ports should be opened: 80, 443, 8080, 8081, 22, 8001, 1521, 1411, 1522, 1523, 1524, 1525, 9006, 15080, 61617, 59000, 12091, 1621, 1622, 1623, 1624, 1625, 8083, 8084, and 8402.

### Related Topics

- [Overview of the MSE High Availability Architecture](#)
- [MSE High Availability Pairing Matrix](#)

- [Failover Scenario for MSE High Availability](#)

## Failover Scenario for MSE High Availability

When a primary MSE failure is detected, the following events occur:

- The primary MSE is confirmed as non-functioning (hardware fail, network fail, and so on) by the health monitor on the secondary MSE.
- If automatic failover isn't enabled, the secondary MSE starts immediately.
- If manual failover is enabled, an e-mail is sent to the administrator asking if they want to manually start failover. This e-mail is sent only if the e-mail is configured for MSE alarms.
- The result of the failover operation is indicated as an event in the Health Monitor UI, and a critical alarm is sent to Prime Infrastructure.

### Related Topics

- [Overview of the MSE High Availability Architecture](#)
- [Guidelines and Limitations for MSE High Availability](#)
- [Failback Scenario for MSE High Availability](#)

## Failback Scenario for MSE High Availability

When the primary MSE is restored to its normal state, if the secondary MSE is already in failover state for the primary, then failback can be invoked.

Failback can occur only if the secondary MSE is in one of the following states for the primary instance:

- The secondary MSE is actually failing over for the primary MSE.
- Manual failover is configured but the administrator did not invoke it.
- The primary MSE failed but the secondary MSE cannot take over because it has encountered errors.
- Failback can occur only if the administrator starts up the failed primary MSE.

### Related Topics

- [Overview of the MSE High Availability Architecture](#)
- [Failover Scenario for MSE High Availability](#)
- [Licensing Requirements for MSE High Availability](#)

## Licensing Requirements for MSE High Availability

For high availability, an activation license is required on the primary and secondary virtual appliances. No other service license is required on the secondary MSE. It is required only on the primary MSE.

### Related Topics

- [Overview of the MSE High Availability Architecture](#)
- [Failback Scenario for MSE High Availability](#)

## Setting Up MSE High Availability: Workflow

During the installation of the MSE software (or using the MSE setup script), configure some critical elements. Pair up the primary and secondary MSE from the Prime Infrastructure UI.

By default, all MSEs are configured as primary. If you do not want high availability support and are upgrading from an earlier release, you can continue to use the IP address for the MSE. If you want to set up high availability, then you must configure the health monitor IP address. The health monitor then becomes a virtual IP address.

Configuring MSE high availability consists of the following steps:

1. Prepare the MSEs for High Availability
2. Configure the Primary MSE
3. Configure the Secondary MSE

You may also need to reconfigure MSE high availability if you must replace the primary MSE server.

For details, see the corresponding Related Topics, below.

### Related Topics

- [Preparing the MSEs for High Availability](#)
- [Configuring MSE High Availability on Primary MSEs](#)
- [Configuring MSE High Availability on Secondary MSEs](#)
- [Replacing Primary MSEs](#)
- [Configuring MSE High Availability](#)

## Preparing the MSEs for High Availability

To prepare your primary and secondary MSEs for high availability, follow these steps:

- 
- |               |                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Ensure that the network connectivity between the primary and secondary MSEs is functioning and that all the necessary ports are open. |
| <b>Step 2</b> | Install the correct version of MSE on the primary MSE.                                                                                |
| <b>Step 3</b> | Make sure that the same MSE version is installed on the secondary MSE.                                                                |
- 

### Related Topics

- [Configuring MSE High Availability on Primary MSEs](#)
- [Replacing Primary MSEs](#)
- [Configuring MSE High Availability](#)

## Configuring MSE High Availability on Primary MSEs

To configure a primary MSE for high availability, follow these steps:

**Step 1** On the intended primary MSE, enter the following command:

```
/opt/mse/setup/setup.sh
```

The setup script displays the following prompts, which you can answer using the suggested responses given in bold (in this and later steps):

```

Welcome to the Cisco Mobility Services Engine Appliance Setup.
You may exit the setup at any time by typing <Ctrl+c>.

Would you like to configure MSE using:
1. Menu mode
2. Wizard mode
Choose 1 or 2: 1

Mobility Services Engine Setup
Please select a configuration option below and enter the
requested information. You may exit setup at any time by typing <Ctrl +C>.

You will be prompted to choose whether you wish to configure a parameter, skip it, or
reset it to its initial default value. Skipping a parameter will leave it unchanged from
its current value.

Please note that the following parameters are mandatory and must be configured at least
once.

-> Hostname
-> Network interface eth0
-> Timezone settings
-> Root password
-> NTP settings
-> Prime Infrastructure password

You must select option 24 to verify and apply any changes made during this session.

PRESS <ENTER> TO CONTINUE:

Configure MSE:
1) Hostname * 13) Remote syslog settings
2) Network interface eth0 settings* 14) Host access control settings
3) Timezone settings* 15) Audit Rules
4) Root password * 16) Login banner
5) NTP settings * 17) System console restrictions
6) Prime Infrastructure password * 18) SSH root access
7) Display current configuration 19) Single user password check
8) Domain 20) Login and password settings
9) High availability role 21) GRUB password
10) Network interface eth1 settings 22) Root access control
```

```

11) DNS settings
12) Future restart time
Please enter your choice [1 - 24]:

23) Auto start MSE on system boot up
24) ## Verify and apply changes ##

```

**Step 2** Configure the primary MSE hostname:

```

Please enter your choice [1 - 24]: 1
Current Hostname=[mse]
Configure Hostname? (Y)es/(S)kip/(U)se default [Skip]: y
The host name should be a unique name that can identify the device on the network. The
hostname should start with a letter, end with a letter or number, and contain only
letters, numbers, and dashes.

```

```

Enter a Host name [mse]:mse1

```

**Step 3** Configure the primary MSE domain:

```

Please enter your choice [1-24]: 8
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: S

```

**Step 4** Configure the primary MSE network interface eth0 settings.

```

Please enter your choice [1 - 24]: 2
Current eth0 interface IP address=[10.0.0.1]
Current eth0 interface netmask=[255.0.0.0]
Current IPv4 gateway address=[172.20.104.123]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: y
Enter an IP address for first Ethernet interface of this machine.
Enter eth0 IP address [10.0.0.2]:
Enter the network mask for IP address 172.21.105.126
Enter network mask [255.255.255.224]:
Enter the default gateway address for this machine.
Note that the default gateway must be reachable from the first Ethernet interface.
Enter default gateway address [172.20.104.123]:

```

**Step 5** Configure the primary MSE root password:

```

Please enter your choice [1 - 24]: 4
Root password has not been configured
Configure root password? (Y)es/(S)kip/(U)se default [Skip]: y
Changing password for user root.
You can now choose the new password.
A valid password should be a mix of upper and lower case letters, digits, and other
characters. You can use an 8 character long password with characters from all of these
classes. An upper case letter that begins the password and a digit that ends it do not
count towards the number of character classes used.

```

```

Enter new password: password

```

**Step 6** Configure the primary MSE's high availability role:

```

Current role=[Primary]
Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]: y
High availability role for this MSE (Primary/Secondary)
Select role [1 for Primary, 2 for Secondary] [1]: 1
Health monitor interface holds physical IP address of this MSE server.

```

```

This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to
communicate among themselves
Select Health Monitor Interface [eth0/eth1] [eth0]: eth0

Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
"none" implies you do not wish to use direct connect configuration.

Select direct connect interface [eth0/eth1/none] [none]:
Enter a Virtual IP address for the Primary MSE server
Enter Virtual IP address [1.1.1.1]: 10.10.10.11
Enter network mask for IP address 10.10.10.1
Enter network mask [1.1.1.1]: 255.255.255.0
Select to start the server in recovery mode.
You should choose yes only if this primary MSE was paired earlier and you have now lost
the configuration from this box.
And, now you want to restore the configuration from Secondary via Cisco Prime
Infrastructure
Do you wish to start this MSE in HA recovery mode?: (yes/no) [no]:no
Current IP address = [1.1.1.10]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
Enter an IP address for first Ethernet interface of this machine.
Enter eth0 IP address [1.1.1.10]: 10.10.10.12
Enter the network mask for IP address 10.10.10.12
Enter network mask [255.255.255.0]: 255.255.255.0
Enter an default gateway address for this machine.
Note that the default gateway must be reachable from the first Ethernet interface. Enter
default gateway address [1.1.1.1]:10.10.10.1
The second Ethernet interface is currently disabled for this machine.
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: S

```

**Step 7** Configure the primary MSE timezone settings:

```

Please enter your choice [1 - 24]: 3
Current Timezone=[America/New_York]
Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y
Enter the current date and time.
Please identify a location so that time zone rules can be set correctly. Please select a
continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia

```

- 6) Atlantic Ocean
  - 7) Australia
  - 8) Europe
  - 9) Indian Ocean
  - 10) Pacific Ocean
  - 11) UTC - I want to use Coordinated Universal Time.
- #? 2

Please select a country.

- |                        |                             |
|------------------------|-----------------------------|
| 1) Anguilla            | 27) Honduras                |
| 2) Antigua & Barbuda   | 28) Jamaica                 |
| 5) Bahamas             | 31) Montserrat              |
| 6) Barbados            | 32) Netherlands Antilles    |
| 7) Belize              | 33) Nicaragua               |
| 8) Bolivia             | 34) Panama                  |
| 9) Brazil              | 35) Paraguay                |
| 10) Canada             | 36) Peru                    |
| 11) Cayman Islands     | 37) Puerto Rico             |
| 12) Chile              | 38) St Barthelemy           |
| 13) Colombia           | 39) St Kitts & Nevis        |
| 14) Costa Rica         | 40) St Lucia                |
| 15) Cuba               | 41) St Martin (French part) |
| 16) Dominica           | 42) St Pierre & Miquelon    |
| 17) Dominican Republic | 43) St Vincent              |
| 18) Ecuador            | 44) Suriname                |
| 19) El Salvador        | 45) Trinidad & Tobago       |
| 20) French Guiana      | 46) Turks & Caicos Is       |
| 21) Greenland          | 47) United States           |
| 22) Grenada            | 48) Uruguay                 |
| 23) Guadeloupe         | 49) Venezuela               |
| 24) Guatemala          | 50) Virgin Islands (UK)     |
| 25) Guyana             | 51) Virgin Islands (US)     |
| 26) Haiti              |                             |
- #? 47

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
- 7) Eastern Time - Indiana - Pulaski County
- 8) Eastern Time - Indiana - Crawford County
- 9) Eastern Time - Indiana - Pike County
- 10) Eastern Time - Indiana - Switzerland County
- 11) Central Time
- 12) Central Time - Indiana - Perry County



```

13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Mountain Time
18) Mountain Time - south Idaho & east Oregon
19) Mountain Time - Navajo
20) Mountain Standard Time - Arizona
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - Alaska panhandle neck
25) Alaska Time - west Alaska
26) Aleutian Islands
27) Hawaii
#? 21

```

The following information has been given:

United States

Pacific Time

Therefore TZ='America/Los\_Angeles' will be used.

Local time is now: Sun Apr 6 18:45:27 PDT 2020. Universal Time is now: Mon Apr 7 01:45:27 UTC 2020. Is the above information OK?

1) Yes

2) No

#? 1

#### Step 8 Configure the primary MSE DNS settings:

Please enter your choice [1 - 24]: 11

Domain Name Service (DNS) Setup

Enable DNS (yes/no) [no]: y

Default DNS server 1=[8.8.8.8]

Enter primary DNS server IP address:

DNS server address must be in the form #.#.#.#, where # is 0 to 255 or hexadecimal : separated v6 address

Enter primary DNS server IP address [8.8.8.8]:

Enter backup DNS server IP address (or none) [none]:

#### Step 9 Configure the primary MSE NTP settings:

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the

Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

```

Enable NTP (yes/no) [no]: y
Default NTP server 1=[time.nist.gov] Enter NTP server name or address:
NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :
separated v6 address.
Enter NTP server name or [time.nist.gov]:
Enter another NTP server IP address (or none) [none]:
Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Skip]: y
Enter NTP Auth key Number [1]:
Enter NTP Auth key Value (String) [Secret]: Do you want to continue (yes/no) [no]: y

```

**Step 10** Configure the Prime Infrastructure password:

```

Please enter your choice [1 - 24]: 6
Cisco Prime Infrastructure communication password has not been configured. Configure
Prime Infrastructure password? (Y)es/(S)kip/(U)se default [Yes]:
Enter a password for the admin user.
The admin user is used by the Prime Infrastructure and other northbound systems to
authenticate their SOAP/XML session with the server. Once this password is updated, it
must correspondingly be updated on the NCS page for MSE General Parameters so that the
Prime Infrastructure can communicate with the MSE.

```

**Step 11** Verify and apply your changes:

```

Please enter your choice: 24
Please verify the following setup information.
-----BEGIN-----
Hostname=msel
Role= 1, Health Monitor Intercace=eth0, Direct connect interface=none
Virtual IP Address=10.10.10.11, Virtual IP Netmask=255.255.255.0
Eth0 IP address=10.10.10.12, Eth0 network mask=255.0.0.0
Default Gateway=10.10.10.1
Time zone=America/Los_Angeles
Enable DNS=yes, DNS servers=8.8.8.8
Enable NTP=yes, NTP servers=time.nist.gov
Time zone=America/Los_Angeles
Root password is changed.
Cisco Prime Infrastructure password is changed.
-----END-----
You may enter "yes" to proceed with configuration, "no" to make
more changes.
Configuration Changed
Is the above information correct (yes or no): yes

Checking mandatory configuration information...
Root password: Not configured
WARNING
The above parameters are mandatory and need to be configured.

Ignore and proceed (yes/no): yes
Setup will now attempt to apply the configuration. Restarting network services with new
settings. Shutting down interface eth0:

```

The system is minimally configured right now. It is strongly recommended that you run the setup script under `/opt/mse/setup/setup.sh` command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

**Step 12** Reboot the system:

```
[root@mse1]# reboot Stopping MSE Platform
Flushing firewall rules:[OK]
Setting chains to policy ACCEPT: nat filter[OK] Unloading iptables modules:[ok]
Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):
The system is going down for reboot NOW:
```

**Step 13** Start the MSE services:

```
[root@mse1]# /etc/init.d/mseed start
Starting MSE Platform.
```

```
Starting Health Monitor, Waiting to check the status. Starting Health Monitor, Waiting
to check the status. Health Monitor successfully started
Starting Admin process... Started Admin process. Starting database
Database started successfully. Starting framework and services..... Framework and
services successfully started
```

**Step 14** After all services have started, confirm MSE services are working properly by entering the following command:

```
[root@mse1]# getserverinfo
```

### Related Topics

- [Preparing the MSEs for High Availability](#)
- [Configuring MSE High Availability on Secondary MSEs](#)
- [Configuring MSE High Availability](#)

## Configuring MSE High Availability on Secondary MSEs

To prepare your secondary MSE for high availability, follow these steps:

**Step 1** On the intended secondary MSE, enter the following command:

```
/opt/mse/setup/setup.sh
```

The setup script displays the same prompts as for the primary MSE:

**Step 2** Configure the secondary MSE hostname:

```
Please enter your choice [1 - 24]: 1
```

```
Current hostname=[mse1]
```

```
Configure hostname? (Y)es/(S)kip/(U)se default [Yes]: yes
```

The host name should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

```
Enter a hostname [mse]: mse2
```

**Step 3** Configure the secondary MSE domain:

```
Please enter your choice [1-24]: 8
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: S
```

**Step 4** Configure the secondary MSE high availability role:

```
Current role=[Primary]
Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]: High availability role
for this MSE (Primary/Secondary)
Select role [1 for Primary, 2 for Secondary] [1]: 2
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to
communicate among themselves
Select Health Monitor Interface [eth0/eth1] [eth0]: eth0
```

```

Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.This can help reduce latencies in heartbeat response
times, data
replication and failure detection times.Please choose a network interface that you wish
to use for direct connect. You should appropriately configure the respective interfaces.
"none" implies you do not wish to use direct connect configuration.

```

```
Select direct connect interface [eth0/eth1/none] [none]:
Current IP address=[1.1.1.10]
Current eth0 netmask=[255.255.255.0] Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Yes]:
Enter an IP address for first Ethernet interface of this machine. Enter eth0 IP address
[1.1.1.10]: 10.10.10.13
Enter the network mask for IP address 10.10.10.13
Enter network mask [255.255.255.0]:
Enter an default gateway address for this machine.
Note that the default gateway must be reachable from the first Ethernet interface. Enter
default gateway address [1.1.1.1]:10.10.10.1
The second Ethernet interface is currently disabled for this machine. Configure eth1
interface parameters? (Y)es/(S)kip/(U)se default [Yes]: S
```

**Step 5** Configure the secondary MSE timezone settings:

```
Please enter your choice [1 - 24]: 3
Current Timezone=[America/New_York]
Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y
Enter the current date and time.
Please identify a location so that time zone rules can be set correctly. Please select a
continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
```

- 9) Indian Ocean
  - 10) Pacific Ocean
  - 11) UTC - I want to use Coordinated Universal Time.
- #? 2

Please select a country.

- |                        |                             |
|------------------------|-----------------------------|
| 1) Anguilla            | 27) Honduras                |
| 2) Antigua & Barbuda   | 28) Jamaica                 |
| 5) Bahamas             | 31) Montserrat              |
| 6) Barbados            | 32) Netherlands Antilles    |
| 7) Belize              | 33) Nicaragua               |
| 8) Bolivia             | 34) Panama                  |
| 9) Brazil              | 35) Paraguay                |
| 10) Canada             | 36) Peru                    |
| 11) Cayman Islands     | 37) Puerto Rico             |
| 12) Chile              | 38) St Barthelemy           |
| 13) Colombia           | 39) St Kitts & Nevis        |
| 14) Costa Rica         | 40) St Lucia                |
| 15) Cuba               | 41) St Martin (French part) |
| 16) Dominica           | 42) St Pierre & Miquelon    |
| 17) Dominican Republic | 43) St Vincent              |
| 18) Ecuador            | 44) Suriname                |
| 19) El Salvador        | 45) Trinidad & Tobago       |
| 20) French Guiana      | 46) Turks & Caicos Is       |
| 21) Greenland          | 47) United States           |
| 22) Grenada            | 48) Uruguay                 |
| 23) Guadeloupe         | 49) Venezuela               |
| 24) Guatemala          | 50) Virgin Islands (UK)     |
| 25) Guyana             | 51) Virgin Islands (US)     |
| 26) Haiti              |                             |

#? 47

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
- 7) Eastern Time - Indiana - Pulaski County
- 8) Eastern Time - Indiana - Crawford County
- 9) Eastern Time - Indiana - Pike County
- 10) Eastern Time - Indiana - Switzerland County
- 11) Central Time
- 12) Central Time - Indiana - Perry County
- 13) Central Time - Indiana - Starke County
- 14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
- 15) Central Time - North Dakota - Oliver County

```

16) Central Time - North Dakota - Morton County (except Mandan area)
17) Mountain Time
18) Mountain Time - south Idaho & east Oregon
19) Mountain Time - Navajo
20) Mountain Standard Time - Arizona
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - Alaska panhandle neck
25) Alaska Time - west Alaska
26) Aleutian Islands
27) Hawaii
#? 21

```

The following information has been given: United States

Pacific Time

Therefore TZ='America/Los\_Angeles' will be used.

Local time is now: Sun Apr 6 18:45:27 PDT 2014. Universal Time is now: Mon Apr 7 01:45:27 UTC 2014. Is the above information OK?

1) Yes

2) No

#? 1

#### Step 6 Configure the secondary MSE NTP settings:

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: y

Default NTP server 1=[time.nist.gov] Enter NTP server name or address:

NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :  
separated v6 address.

Enter NTP server name or [time.nist.gov]:

Enter another NTP server IP address (or none) [none]:

Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Skip]: y

Enter NTP Auth key Number [1]:

Enter NTP Auth key Value (String) [Secret]: Do you want to continue (yes/no) [no]: y

#### Step 7 Verify and apply your changes:

Please enter your choice: 24

Please verify the following setup information.

```

-----BEGIN-----
Hostname=mse2
Role= 2, Health Monitor Intercace=eth0, Direct connect interface=none

```

```

Eth0 IP address=10.10.10.13, Eth0 network mask=255.255.255.0
Default Gateway=10.10.10.1
Time zone=America/Los_Angeles
Enable NTP=yes, NTP servers=time.nist.gov
Time zone=America/Los_Angeles
-----END-----
You may enter "yes" to proceed with configuration, "no" to make more changes.
Configuration Changed
Is the above information correct (yes or no): yes

Checking mandatory configuration information...
Root password: Not configured
WARNING
The above parameters are mandatory and need to be configured.

Ignore and proceed (yes/no): yes
Setup will now attempt to apply the configuration.
Restarting network services with new settings. Shutting down interface eth0:
The system is minimally configured right now. It is strongly recommended that you run the
setup script under /opt/mse/setup/setup.sh command to configure all appliance related
parameters immediately after installation is complete.
PRESS <ENTER> TO EXIT THE INSTALLER:

```

**Step 8** Reboot the system:

```

[root@mse2 installers]# reboot
Stopping MSE Platform
Flushing firewall rules:[OK]
Setting chains to policy ACCEPT: nat filter[OK] Unloading iptables modules:[ok]
Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):
The system is going down for reboot NOW:

```

**Step 9** Start the MSE services:

```

[root@mse2]# /etc/init.d/msed start
Starting MSE Platform.
Starting Health Monitor, Waiting to check the status. Starting Health Monitor, Waiting
to check the status. Health Monitor successfully started
Starting Admin process... Started Admin process. Starting database
Database started successfully. Starting framework and services..... Framework and
services successfully started

```

**Related Topics**

- [Preparing the MSEs for High Availability](#)
- [Configuring MSE High Availability on Primary MSEs](#)
- [Configuring MSE High Availability](#)

## Replacing Primary MSEs

If for any reason you need to replace a primary MSE, you will want to recover the current pairing information to a newly configured primary MSE, as explained in the following steps.

- 
- Step 1** Configure the MSE as a primary using the setup script.
  - Step 2** Set up a pairing between the primary and secondary MSE using Prime Infrastructure.
  - Step 3** Initiate failover from the primary MSE to the secondary MSE.
  - Step 4** Configure the replacement MSE as a primary using the setup script. The new primary MSE must have the same version of the software as the secondary, and the same settings as the old primary MSE.
  - Step 5** Choose the recovery mode and follow the instructions.
  - Step 6** Initiate the failback to the new primary using Prime Infrastructure.

A new license is required on this new primary MSE, as the original license will not match the UDI of the primary, and will not work.

---

### Related Topics

- [Configuring MSE High Availability on Primary MSEs](#)
- [Configuring MSE High Availability](#)





## Configuring Wireless Redundancy

---

Setting up controller redundancy in a wireless network allows you to reduce network downtime. The following related topics explain wireless controller redundancy and how to configure it properly for management using Cisco Prime Infrastructure.

### Related Topics

- [About Wireless Controller Redundancy](#)
- [Prerequisites and Limitations for Redundancy](#)
- [Configuring Redundancy Interfaces](#)
- [Configuring Redundancy on Primary Controllers](#)
- [Configuring Redundancy on Secondary Controllers](#)
- [Monitoring Redundancy States](#)
- [Running the Redundancy Status Background Task](#)
- [Configuring Peer Service Port IPs and Subnet Mask](#)
- [Adding Peer Network Routes](#)
- [Resetting and Uploading Files from the Secondary Server](#)
- [Disabling Redundancy on Controllers](#)

## About Wireless Controller Redundancy

In a redundancy architecture, one wireless controller is in the Active state and a second controller is in the Standby state. The Standby controller continuously monitors the health of the Active controller via 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.

Stateful switchover of *clients* is not supported. This means that nearly all clients are deauthenticated and forced to re-associate with the new controller in the Active state. The only exceptions to this rule are clients on locally switched WLANs on access points in FlexConnect mode.

## Prerequisites and Limitations for Redundancy

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

- Wireless controller 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 **Configuration > Network > Network Devices**.
  - Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
  - Step 3** Select the group of wireless controllers that match the device you have chosen as the primary controller (for example: Cisco 5500 Series Wireless LAN Controllers). Members of this device group are displayed on the right.
  - Step 4** Click on the **Device Name** of the primary controller.
  - Step 5** Click the **Configuration** tab.
  - Step 6** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration page appears.
  - Step 7** In the Redundancy-Management IP text box, enter an IP address that belongs to the management interface subnet.
  - Step 8** Click **Save**.
- 

## Configuring Redundancy on Primary Controllers

- 
- Step 1** Choose **Configuration > Network > Network Devices**.
  - Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
  - Step 3** Select the group of wireless controllers that match the device for which you have configured the redundancy-management interface IP address (for example: Cisco 5500 Series Wireless LAN Controllers). Members of this device group are displayed on the right.
  - Step 4** Click on the **Device Name** of the controller for which you have configured the redundancy-management interface IP address..
  - Step 5** Click the **Configuration** tab.
  - Step 6** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration page appears.
  - Step 7** 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 8** Click **Save**. The **Enabled** check box for the redundancy mode becomes available.

**Step 9** Select the **Enabled** check box for the redundancy mode to enable the redundancy on the primary controller.

After you enable the redundancy, you cannot modify the Redundancy-Management IP, Peer Redundancy-Management IP, Redundant Unit, and Mobility MAC Address parameters.

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

**Step 10** Click **Save**. The configuration is saved and the system reboots.

---

## Configuring Redundancy on Secondary Controllers

---

**Step 1** Choose **Configuration > Network > Network Devices**.

**Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.

**Step 3** Select the group of wireless controllers that match the device you have selected to act as the secondary controller (for example: Cisco 5500 Series Wireless LAN Controllers). Members of this device group are displayed on the right.

**Step 4** Click on the **Device Name** of the secondary controller.

**Step 5** Click the **Configuration** tab.

**Step 6** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration page appears.

**Step 7** 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 8** Click **Save**. The Enabled check box for the redundancy mode becomes available for editing.

**Step 9** Select the **Enabled** check box for the redundancy mode to enable the redundancy on the secondary controller.

After you enable the redundancy, you cannot modify the Redundancy-Management IP, Peer Redundancy-Management IP, Redundant Unit, and Mobility MAC Address parameters.

You cannot configure the primary controller during the redundancy pair-up process.

**Step 10** Click **Save**. The configuration is saved and the system reboots.

---

## Monitoring Redundancy States

After 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” in Related Topics.

You can view the redundancy state details, including 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.

To view these details, choose **Monitor > Managed Elements > Network Devices > Device Type > Wireless Controller > Controller Group > Controller > Device Details > Redundancy > Redundancy States**.

### Related Topics

- [Cisco Prime Infrastructure Alarms and Events](#)

## Running the Redundancy Status Background Task

When the peer state changes from StandbyCold to StandbyHot, Prime Infrastructure sometimes misses redundancy traps. As a result, the redundancy pair-up process cannot be completed.

To fix this issue, you must run the Redundancy Status background task manually. Running this task:

- Removes the standby controller from Prime Infrastructure.
- Swaps the network route table entries with the peer network route table entries.
- Updates 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 Prime Infrastructure.

- 
- Step 1** Log in to Prime Infrastructure with a user ID that has administrator privileges.
- Step 2** Choose **Administration > Settings > Background Tasks**.
- Step 3** Select the **Redundancy Status** background task.
- Step 4** Choose **Select a command > Execute Now > Go**.
-

## Configuring Peer Service Port IPs 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 the local service port before you configure the peer service port IP address.

- 
- Step 1** Choose **Configuration > Network > Network Devices**.
  - Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
  - Step 3** Select the group of wireless controllers that contains the primary or active controller. Members of this device group are displayed on the right.
  - Step 4** Click on the Device Name of the primary or active controller.
  - Step 5** Click the **Configuration** tab.
  - Step 6** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration page appears.
  - Step 7** Complete the following fields:
    - **Peer Service Port IP**—Enter the IP address of the peer service port.
    - **Peer Service Netmask IP**—Enter the IP address of the peer service subnet mask.
  - Step 8** Click **Save**.
- 

## Adding Peer Network Routes

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.

- 
- Step 1** Choose **Configuration > Network > Network Devices**.
  - Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
  - Step 3** Select the group of wireless controllers that contains the controller for which you have configured the redundancy-management interface IP address. Members of this device group are displayed on the right.
  - Step 4** Click on the Device Name of the controller for which you have configured the redundancy-management interface IP address.
  - Step 5** Click the **Configuration** tab.
  - Step 6** From the left sidebar menu, choose **Redundancy > Peer Network Route**.
  - Step 7** Choose **Select a command > Add Peer Network Route > Go**. The Peer Network Route Details page appears.

- Step 8** Complete 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 pairing process is complete. You can also upload the files from the secondary server to the primary server.

- 
- Step 1** Choose **Configuration > Network > Network Devices**.
- Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the group of wireless controllers that contains the controller for which you have configured the redundancy-management interface IP address. Members of this device group are displayed on the right.
- Step 4** Click on the **Device Name** of the controller for which you have configured the redundancy-management interface IP address.
- Step 5** Click the **Configuration** tab.
- Step 6** From the left sidebar menu, choose **Redundancy > Redundancy Commands**.
- Step 7** Under **Administrative Commands**, choose **Select a command > Reset Standby > Go** to reset the secondary server.
- Step 8** Under **Upload/Download Commands**:
- a. Choose the transport protocol you want to use when uploading files from the secondary to the primary server (**TFTP** is the default).
  - b. Choose **Select a command > Upload File from Standby Controller > Go** to upload files from the secondary to the primary server.
-

# Disabling Redundancy on Controllers

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.

- 
- Step 1** Choose **Configuration > Network > Network Devices**.
  - Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
  - Step 3** Select the group of wireless controllers that contains the controller on which you want to disable redundancy. Members of this device group are displayed on the right.
  - Step 4** Click on the **Device Name** of the controller on which you want to disable redundancy.
  - Step 5** Click the **Configuration** tab.
  - Step 6** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.
  - Step 7** Unselect the **Enabled** check box for the **Redundancy Mode** on the selected controller.
  - Step 8** Click **Save**. The configuration is saved and the system reboots.
-





# Controlling User Access

---

The following topics explain how to control and manage user access to Cisco Prime Infrastructure.

## Related Topics

- [Managing User Accounts](#)
- [Using Lobby Ambassadors to Manage Guest User Accounts](#)
- [Using User Groups to Control Access](#)
- [Using Virtual Domains to Control Access](#)
- [Auditing User Access](#)
- [Configuring AAA on Prime Infrastructure](#)

## Managing User Accounts

The following topics explain how to manage Prime Infrastructure user accounts.

## Related Topics

- [Viewing Active User Sessions](#)
- [Adding User Accounts](#)
- [Creating Additional Administrative Users](#)
- [Deleting User Accounts](#)
- [Configuring Guest Account Settings](#)
- [Disabling User Accounts](#)
- [Disabling the Web Root Account](#)
- [Changing User Passwords](#)
- [Changing Password Policies](#)
- [Changing the Global Idle Timeout](#)

## Viewing Active User Sessions

Administrators can view active Prime Infrastructure user sessions, with details including the user IP address and status.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Active Sessions**. Prime Infrastructure displays a list of the current active user sessions.
- Step 3** Click the **Audit Trail** icon for the username for which you want to see the following data:
- User—User login name
  - Client IP Address—IP address of the user’s client device.
  - Device IP Address—IP address of the device affected by the user operation (if applicable, such as with a device configuration change).
  - Description—Description of the operation the user performed (such as login or logout).
  - Time—Time operation was audited.

Audit trail entries may 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.

---

### Related Topics

- [Adding User Accounts](#)
- [Disabling User Accounts](#)
- [Changing User Passwords](#)

## Adding User Accounts

Administrators can add Prime Infrastructure user accounts and assign predefined static roles to these users. You can also give administrative access with differentiated privileges to certain user groups.

If you are using Operations Center: User accounts created in Operations Center can log in to Operations Center or any of the Prime Infrastructure 2.2 (or later) instances Operations Center is managing. To log into instances of Prime Infrastructure version 2.1.2 from Operations Center, the user ID must exist locally on the 2.1.2 instances. The 2.1.2 instances also must have the required update for Operations Center.

---

- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Choose **Select a command > Add User > Go**.
- Step 4** Enter the username and password, and then confirm the password, for the new user.
- Step 5** Choose the user groups to which this user belongs by selecting the check box next to each user group name (see “Using User Groups to Control Access” in Related Topics).
- Step 6** Click the Virtual Domains tab to assign this user to a virtual domain (see “User Access in Virtual Domains” in Related Topics).

**Step 7** Click **Save**.

---

**Related Topics**

- [Creating Additional Administrative Users](#)
- [Deleting User Accounts](#)
- [Disabling User Accounts](#)
- [Using Lobby Ambassadors to Manage Guest User Accounts](#)
- [Using User Groups to Control Access](#)
- [Adding Users to Virtual Domains](#)

## Creating Additional Administrative Users

Any Prime Infrastructure administrator with sufficient privileges can create additional administrative user accounts with the same or lower privileges.

---

- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Choose **Select a command > Add User > Go**.
- Step 4** Complete the required fields as you would for any new user account.
- Step 5** Click **Admin** to give the new user administrator privileges.
- Step 6** Click **Save**.
- 

**Related Topics**

- [Adding User Accounts](#)
- [Viewing Active User Sessions](#)
- [Disabling User Accounts](#)
- [Changing User Passwords](#)

## Deleting User Accounts

Administrators need not delete Prime Infrastructure user accounts to deny a user access temporarily. Instead, you can lock the account, then unlock it when the user returns.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Select the check box to the left of the name of the user that you want to delete.
- Step 4** Choose **Select a command > Delete User(s) > Go**.
- Step 5** Click **OK**.
- 

### Related Topics

- [Adding User Accounts](#)
- [Viewing Active User Sessions](#)
- [Configuring Guest Account Settings](#)
- [Disabling User Accounts](#)
- [Changing User Passwords](#)
- [Changing Password Policies](#)

## Configuring Guest Account Settings

Prime Infrastructure administrators can choose to:

- Force all expired guest accounts to be deleted automatically.
- Limit Lobby Ambassadors' control over guest accounts to just those accounts they have created.

Both of these options impose restrictions on the latitude lobby ambassadors have to manage these temporary guest accounts. For details on using lobby ambassador accounts, see "Using Lobby Ambassadors to Manage Guest User Accounts" in Related Topics.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Settings > System Settings > General > Guest Account**.
- Step 3** Change radio button selections as follows:
- Select **Automatically remove expired guest accounts** to have guest accounts whose lifetimes have ended moved to the Expired state. Guest accounts in the Expired state are deleted from Prime Infrastructure automatically.
  - Select **Search and List only guest accounts created by this lobby ambassador** to restrict Lobby Ambassadors to modifying only the guest accounts that they have created. By default, any Lobby Ambassador can modify or delete any guest account, irrespective of who created that account.
- Step 4** Click **Save**.
-

**Related Topics**

- [Using Lobby Ambassadors to Manage Guest User Accounts](#)
- [Using User Groups to Control Access](#)
- [Using Virtual Domains to Control Access](#)

## Disabling User Accounts

Administrators can disable a user account so that the user cannot log in to Prime Infrastructure. You might want to disable a user account if, for example, 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. You can later unlock the user account, enabling access to Prime Infrastructure, without having to re-create the user.

User accounts may be disabled automatically if the password is not changed before expiration. Only an administrator can reset the password in this case (see “Changing User Passwords” and “Changing Password Policies” in Related Topics).

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Select the user whose access you want to disable.
- Step 4** Choose **Select a command > Lock User(s) > Go**.

The next time the user tries to log in to Prime Infrastructure, a message appears saying the login failed because the account is locked.

---

**Related Topics**

- [Adding User Accounts](#)
- [Deleting User Accounts](#)
- [Disabling the Web Root Account](#)
- [Changing Password Policies](#)
- [Changing User Passwords](#)

## Disabling the Web Root Account

Prime Infrastructure ships with a default user account called “root”. During Prime Infrastructure installation, a password for the web root account must be entered. This “root” user account and its password are used to log in to the Prime Infrastructure web interface for the first time.

We recommend that you do not use the web root account for normal operations. Instead, create administrative or super- user accounts with all privileges, then disable the web root account that was created when Prime Infrastructure was installed.

To disable the web root account, follow the steps for that account given in “Disabling Root Access” in Related Topics.

### Related Topics

- [Disabling Root Access](#)
- [Disabling User Accounts](#)
- [Adding User Accounts](#)
- [Viewing Active User Sessions](#)

## Changing User Passwords

User passwords are controlled based on the re-use count established when administrators set user password policies.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Change Password**.
- Step 3** Complete the password fields, then click **Save**.
- 

### Related Topics

- [Managing User Accounts](#)
- [Changing Password Policies](#)
- [Adding User Accounts](#)

## Changing Password Policies

Prime Infrastructure supports standard password policies for its own users, including:

- Controls on password minimum length and re-use.
- Forbidden password content, such as common words and user names.
- Rules on other kinds of character choices, including character classes that must be included, repeated characters and common character substitutions.
- Password expiration periods and user warnings associated with password expiry

These password policies affect the passwords of locally administered users only. If you are using a AAA server to authenticate Prime Infrastructure servers, password policies must be set on the AAA server.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Local Password Policy**.
- Step 3** Choose the policies you want enforced, then click **Save**.
- 

### Related Topics

- [Adding User Accounts](#)
- [Configuring AAA on Prime Infrastructure](#)

## Changing the Global Idle Timeout

Prime Infrastructure automatically logs off idle users. It provides two settings that control when and how this happens:

- User idle timeout—Individual users can enable and configure this setting to end their user session when they exceed the timeout. This user idle timeout is enabled by default and set to 15 minutes.
- Global idle timeout—Users with administrator privileges can enable and configure this setting which affects all users, across the system. The global idle timeout setting overrides the user idle timeout setting. The global idle timeout is enabled by default and set to 15 minutes.

The following steps explain how administrators can change the global idle timeout, or disable it if necessary. For details on changing the user timeout preference, see “Changing Your Idle-User Timeout” in Related Topics.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Settings > System Settings > General > Server**.
- Step 3** Under **Global Idle Timeout**:
- Change the check status of the checkbox next to **Logout all idle users** to enable or disable the global idle timeout.
  - From the **Logout all idle users after** drop-down list, choose one of the idle timeout limits.
- Step 4** Click **Save**. You will need to logout and log back in for your changes to take effect.
-

**Related Topics**

- [Viewing Active User Sessions](#)
- [Changing Your Idle-User Timeout](#)

## Using Lobby Ambassadors to Manage Guest User Accounts

Lobby ambassador accounts are a special kind of Prime Infrastructure administrative account used to add, manage and retire temporary guest user accounts. Lobby ambassador accounts have very limited network configuration privileges specified in the lobby ambassador profile, and have access only to those Prime Infrastructure functions used to manage guest accounts.

Typically, an enterprise-supplied guest network allows access to the Internet for a guest without compromising the enterprise's hosts. Web authentication is usually provided without a specialized client, so most guests will need to initiate a VPN tunnel to their desired destination.

Prime Infrastructure permits both wired and wireless guest user access. Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports may be available via a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.
- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the beginning and end of the valid time period.

Any Prime Infrastructure administrator with “SuperUser” or “administrator” privileges can create one or more lobby ambassador accounts, with varying profiles and permissions.

Ensure that you have proper time settings on the devices to see correct lifetimes on guest user accounts after they are discovered.

**Related Topics**

- [Managing Guest User Accounts: Workflows](#)
- [Saving Guest Accounts on a Device](#)
- [Editing Guest User Credentials](#)



## Managing Guest User Accounts: Workflows

Lobby ambassadors can manage guest user accounts following this workflow

1. Create guest user accounts—While logged in as a lobby ambassador, create guest user accounts as needed.
2. Schedule guest user accounts—While logged in as a lobby ambassador, schedule automatic creation of guest user accounts.
3. Print or email guest user details—While logged in as a Lobby Ambassador, print or email the guest user account details to the host or person who will be welcoming the guests.

Prime Infrastructure administrators with full access can manage lobby ambassadors and their work using this workflow:

1. Create lobby ambassador accounts—While logged in as a Prime Infrastructure administrator, create lobby ambassador accounts as needed.
2. View lobby ambassador activities—While logged in as a Prime Infrastructure administrator, supervise the lobby ambassador's activities using the log.

### Related Topics

- [Creating Lobby Ambassador Accounts](#)
- [Creating Guest User Accounts as a Lobby Ambassador](#)
- [Scheduling Guest User Accounts](#)
- [Printing or Emailing Guest User Details](#)
- [Viewing Lobby Ambassador Activities](#)

## Creating Lobby Ambassador Accounts

Before you begin creating Lobby Ambassador accounts, you must ensure that you have proper time settings on the devices (if you do not, you will incorrect account lifetimes on Guest User accounts after they are discovered).

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users, Roles & AAA > Users**.
- Step 3** Choose **Select a command > Add User > Go**.
- Step 4** Complete the required fields as follows:
- In the **Groups Assigned to this User** section, select the **Lobby Ambassador** check box to access the Lobby Ambassador Defaults tab.
  - Complete the required fields on the Lobby Ambassador Defaults tab.
  - Click the Virtual Domains tab to assign a virtual domain for this lobby ambassador account.
  - In the **Available Virtual Domains** list, click to highlight the virtual domain you want this user to access. Then click **Add** to add it to the Selected Virtual Domains list.
- Step 5** Click **Save**.
- 

### Related Topics

- [Managing Guest User Accounts: Workflows](#)
- [Saving Guest Accounts on a Device](#)
- [Editing Guest User Credentials](#)

## Logging in as a Lobby Ambassador

You must use the lobby ambassador username and password to log into the Prime Infrastructure user interface. When you log in as a lobby ambassador, the Guest User page appears and provides a summary of all created Guest Users.

### Related Topics

- [Managing Guest User Accounts: Workflows](#)
- [Saving Guest Accounts on a Device](#)
- [Editing Guest User Credentials](#)

## Creating Guest User Accounts as a Lobby Ambassador

---

- Step 1** Log in to Prime Infrastructure as a lobby ambassador.
- Step 2** Choose **Select a command > Add User Group > Go**.
- Step 3** Complete the required fields on the General and Advanced tabs.
- Step 4** Click **Save**.
- 

### Related Topics

- [Managing Guest User Accounts: Workflows](#)
- [Saving Guest Accounts on a Device](#)
- [Editing Guest User Credentials](#)
- [Field Reference for Guest User Pages](#)

## Scheduling Guest User Accounts

---

- Step 1** Log in to Prime Infrastructure as a lobby ambassador.
- Step 2** Choose **Select a command > Schedule Guest User > Go**.
- Step 3** Configure the required parameters:
- If the **Generate new password on every schedule** and **No days of the week** check boxes are selected, then the user will have one password for the entire time the account is active.
- If the **Generate new password on every schedule** and **Any days of the week** check boxes are selected, then the user will have a new password for each day.
- Step 4** Click **Save**.
- 

### Related Topics

- [Managing Guest User Accounts: Workflows](#)
- [Saving Guest Accounts on a Device](#)
- [Editing Guest User Credentials](#)

## Printing or Emailing Guest User Details

The lobby ambassador can print or e-mail the guest user account details to the host or person who welcomes guests. The email or printed sheet will show the following account details:

- Guest user account name.
- Password for the guest user account.
- Start date and time when the guest user account becomes active.
- End date and time when the guest user account expires.
- Profile ID assigned to the guest user. Your administrator can advise which Profile ID to use.
- Disclaimer information for the guest user.

- 
- Step 1** Log in to Prime Infrastructure as a lobby ambassador.
- Step 2** On the Guest User page, select the check box next to the user name whose account details you want to send.
- Step 3** Choose **Select a command > Print/E-mail User Details > Go**. Then proceed as follows:
- If you are printing, click **Print**. From the Print page, select a printer, and click **Print**.
  - If emailing, click **Email**. From the Email page, enter the subject-line text and the email address of the recipient, then click **Send**.
- 

### Related Topics

- [Managing Guest User Accounts: Workflows](#)
- [Saving Guest Accounts on a Device](#)
- [Editing Guest User Credentials](#)

## Viewing Lobby Ambassador Activities

Prime Infrastructure administrators can supervise lobby ambassadors using the Audit Trail feature.

- 
- Step 1** Log into Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > User Groups**.
- Step 3** Click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail page for the lobby ambassador appears. This page enables you to view a list of lobby ambassador activities over time.
- User login name
  - Type of operation audited
  - Time when the operation was audited
  - Login success or failure
  - Indicates the reason for any login failure (for example, “invalid password”).
-

**Related Topics**

- [Managing Guest User Accounts: Workflows](#)
- [Saving Guest Accounts on a Device](#)
- [Editing Guest User Credentials](#)

## Saving Guest Accounts on a Device

---

- Step 1** Log into Prime Infrastructure as a lobby ambassador.
- Step 2** On the Guest User page, choose **Save Guest Accounts on Device** check box to save guest accounts to a Cisco Wireless LAN Controller (WLC) flash so that they are maintained across WLC reboots.
- 

**Related Topics**

- [Managing Guest User Accounts: Workflows](#)
- [Editing Guest User Credentials](#)

## Editing Guest User Credentials

---

- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Click the user name whose credentials you want to edit.
- Step 4** Modify the required credentials.
- While editing, if the Profile selection is removed (changed to Select a profile), the defaults are removed for this lobby ambassador. The user must reconfigure the defaults to reinforce them.
- Step 5** Click **Save**.
- 

**Related Topics**

- [Managing Guest User Accounts: Workflows](#)
- [Saving Guest Accounts on a Device](#)

## Using User Groups to Control Access

Prime Infrastructure has a list of tasks that control which part of Prime Infrastructure users can access and the functions they can perform when accessing those parts.

To make these access privileges easier to manage, Prime Infrastructure also provides User Groups. User Groups are lists of privileges and a list of users who are members. Any user on the User Group membership list has all of the privileges assigned to that User Group.

You can quickly change any user's privileges by assigning the user to, or removing them from, User Group memberships. If the User Group is editable, you can also use the User Group Task List to change what the users who are members of a specific User Group are authorized to do and the screens they can access.

You can also use any of the four user-defined User Groups to define a special custom set of specific privileges as explained in "Changing User Group Privileges" in Related Topics. You can then assign users to it as needed, as explained in "Changing User Group Memberships".

Prime Infrastructure comes with the set of default User Groups shown in the table below. Note that the functions and privileges of most default User Groups are not editable. You can, however, change the membership of all User Groups, using the steps in "Changing User Group Memberships" in Related Topics.

**Table 11-1**      **Default User Groups**

| User Group           | Provides access to                                                                                                                                                                                                                                  | Editable? |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Admin                | All Prime Infrastructure administration tasks.                                                                                                                                                                                                      | Yes       |
| Config Managers      | All monitoring and configuration tasks.                                                                                                                                                                                                             | Yes       |
| Lobby Ambassador     | User administration for Guest user only. Members of this user group cannot also be members of any other user group.                                                                                                                                 | No        |
| Monitor Lite         | Monitoring of assets only. Members of this user group cannot also be members of any other user group.                                                                                                                                               | No        |
| NBI Credential       | The Northbound Interface Credential API.                                                                                                                                                                                                            | No        |
| NBI Read             | The Northbound Interface Read API.                                                                                                                                                                                                                  | No        |
| NBI Write            | The Northbound Interface Write API.                                                                                                                                                                                                                 | No        |
| North Bound API User | All Northbound Interface APIs. Members of this user group cannot also be members of any other user group. This is a special group that lacks access to the Prime Infrastructure user interface; see "North Bound API User Group" in Related Topics. | No        |
| Root                 | Superuser access to the web root user. This user group is reserved for the local root user only; no other users should be assigned to this user group.                                                                                              | No        |
| Super Users          | All Prime Infrastructure tasks.                                                                                                                                                                                                                     | Yes       |
| System Monitoring    | Monitoring tasks only.                                                                                                                                                                                                                              | Yes       |
| User Assistant       | Local Net user administration only. Members of this user group cannot also be members of any other user group.                                                                                                                                      | No        |

**Table 11-1** *Default User Groups (continued)*

| User Group                     | Provides access to                             | Editable? |
|--------------------------------|------------------------------------------------|-----------|
| User-Defined 1                 | A user-selectable mix of functions.            | Yes       |
| User-Defined 2                 |                                                |           |
| User-Defined 3                 |                                                |           |
| User-Defined 4                 |                                                |           |
| mDNS Policy Admin <sup>1</sup> | All mDNS policy administration functions only. | No        |

1. Do not use RADIUS, TACACS+ or SSO to create users to be included in the “mDNS Policy Admin” group. The AAA server will not have the multicast DNS settings needed to create this type of user.

**Related Topics**

- [Managing User Accounts](#)
- [Viewing User Group Privileges and Membership](#)
- [Changing User Group Privileges](#)
- [Changing User Group Memberships](#)
- [North Bound API User Group](#)

## North Bound API User Group

Prime Infrastructure’s North Bound API user group is a specially privileged group, set up to allow any user who is a member of it to access Prime Infrastructure via its APIs only. Any user assigned to the North Bound API group can issue and get a response for any Prime Infrastructure API, but will not have access to the Prime Infrastructure graphic user interface (GUI). This applies whether the user is also a member of other groups (including the Admin and Super User groups) or not. All other actions and privileges are disabled for members of North Bound API; its members cannot log into the Prime Infrastructure GUI.

The lone exception to this rule is access via the Prime Infrastructure Operations Center GUI. While North Bound API users cannot access an individual Prime Infrastructure server instance, they can still:

- Log in to the Operations Center GUI.
- Add Prime Infrastructure servers to the cluster of servers Operations Center is managing.
- View the status of all the Prime Infrastructure servers in the cluster, and the devices they manage, in a single consolidated report.

**Related Topics**

- [Using User Groups to Control Access](#)

## Viewing User Group Privileges and Membership

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 the table in “Using User Groups to Control Access” (in Related Topics, below) for a list of the user groups available in Prime Infrastructure.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > User Groups**.
- Step 3** Click the Group Name of the user group whose privileges and members you want to see:
- The Tasks Permissions tab shows the privileges assigned to this user group.
  - The Members tab shows the users assigned to this user group.
- 

### Related Topics

- [Using User Groups to Control Access](#)
- [Changing User Group Privileges](#)
- [Changing User Group Memberships](#)

## Changing User Group Privileges

Prime Infrastructure offers a several user groups with editable privileges, such as the System Monitoring and Config Managers user groups (see the table in “Using User Groups to Control Access” for a complete list of user groups and their edit status). You can change the privileges assigned to these editable user groups as needed.

You can also use the four User-Defined user groups to define special sets of specific privileges, as explained below. You can then assign users to these custom user groups as explained in “Changing User Group Memberships” in Related Topics.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > User Groups**.
- Step 3** Click the Group Name of an editable user group.
- Step 4** Using the Tasks Permissions tab:
- Select the checkbox next to each task or function you want to provide to members of this user group.
  - Unselect the checkbox next to each task or function you want remove from this user group’s privileges.
- Step 5** When you are finished, click **Submit**.
- 

### Related Topics

- [Using User Groups to Control Access](#)
- [Viewing User Group Privileges and Membership](#)



- [Changing User Group Memberships](#)

## Changing User Group Memberships

You can quickly change a user's privileges in Prime Infrastructure by changing the user groups to which the user belongs.

You can also assign sites or devices to which a virtual domain has access. For details, see “Using Virtual Domains to Control Access” in Related Topics.

Prime Infrastructure will not permit certain combinations of user group membership. For example, a user cannot be a member of the “Root” and “Lobby Ambassador” user groups at the same time (for details, see the table in “Using User Groups to Control Access”). If you are using RADIUS to authenticate Prime Infrastructure users, make sure that you do not insert invalid user-group membership combinations into the RADIUS user attribute/value pairs.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Click on the user name for the user whose memberships you want to change. The User Details page appears.
- Step 4** On the General tab, under **Groups Assigned to This User**:
- Select the checkbox next to each user group to which you want the user to belong.
  - Unselect the checkbox next to each user group from which you want the user to be removed.
- Step 5** When you are finished, click **Save**.
- 

### Related Topics

- [Using User Groups to Control Access](#)
- [Viewing User Group Privileges and Membership](#)
- [Changing User Group Memberships](#)
- [Using Virtual Domains to Control Access](#)

## Using Virtual Domains to Control Access

A virtual domain is a logical grouping of sites, devices and access points. You choose which of these elements are included in a virtual domain, and which Prime Infrastructure users have access to that virtual domain.

Users with access to a virtual domain can configure devices, view alarms, and generate reports for the parts of the network included in the virtual domain. Users without this access cannot. Users with access to a virtual domain benefit because they can see just the devices and information they care about.

You can add virtual domains after you have added devices to Prime Infrastructure. Each virtual domain that you add must have a name, and can have an optional description, email address, and time zone. Prime Infrastructure uses the email address and time zone that you specify to schedule and e-mail

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.

Before you set up virtual domains, always start by determining which Prime Infrastructure users are responsible for managing particular sites, devices and access points in your network. You can then organize your virtual domains according your organization's physical sites, the device types in your network, the user communities the network serves, or any other characteristic you choose.

#### Related Topics

- [Understanding Virtual Domains](#)
- [User Access in Virtual Domains](#)
- [Creating Virtual Domains](#)
- [Adding Users to Virtual Domains](#)

## Understanding Virtual Domains

To manage Virtual Domains, select **Administration > Users > Virtual Domains**. In the left pane, the Virtual Domains sidebar menu has both List and Tree views, with the Tree view displayed by default. The menu has two icons, **Add New Domain** and **Import Domain(s)**. Just below these icons, a **Search** bar is available.

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

Hover your mouse cursor over "ROOT-DOMAIN" and a pop-up window appears at the cross-hair icon, displaying a summary of this parent virtual domain. You can create sub domains here.

Because network elements are managed hierarchically, user views of devices and access points, as well as some associated features and components – such as report generation, searches, templates, config groups, and alarms – are affected by the user's virtual domain. The following sections describe the effects of virtual-domain partitioning on the following Prime Infrastructure features:

- [Reports](#)
- [Search](#)
- [Alarms](#)
- [Templates](#)
- [Config Groups](#)
- [Maps](#)
- [Access Points](#)
- [Controllers](#)
- [Email Notification](#)

### 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.

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.

Access point templates are visible in the virtual domain in which they were created *only*. You cannot see access points templates in other virtual domains, even if those virtual domains have the same access point added.

If you create a sub (or child) 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.

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.

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 will be displayed for primary, secondary, and tertiary controllers rather than the limited number specified in the partition.

If a controller configuration is modified by multiple virtual domains, complications can 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.

### Related Topics

- [Using Virtual Domains to Control Access](#)
- [User Access in Virtual Domains](#)
- [Creating Virtual Domains](#)
- [Adding Users to Virtual Domains](#)

## User Access in Virtual Domains

A Prime Infrastructure virtual domain consists of a set of Prime Infrastructure devices, maps and access points. The virtual domain restricts the user's view to information relevant to the set of managed objects in that virtual domain.

Using virtual domains, administrators 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 their assigned part of the network *only*.

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 choosing 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-DOMAIN") 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-DOMAIN" 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.

### Related Topics

- [Using Virtual Domains to Control Access](#)
- [Understanding Virtual Domains](#)
- [Creating Virtual Domains](#)
- [Adding Users to Virtual Domains](#)
- [Changing Virtual Domain Access](#)
- [Exporting Virtual Domain RADIUS and TACACS+ Attributes](#)

## Creating Virtual Domains

When first installed, Prime Infrastructure contains only one virtual domain, called “ROOT-DOMAIN”. All other virtual domains must be created by Prime Infrastructure administrators, and are considered children (also known as “sub domains”) of the parent “ROOT-DOMAIN”.

To create a virtual domain, follow the steps below. Note that you can also create many virtual domains at one time by importing a properly formatted CSV file (for details, see “Importing Virtual Domains” in Related Topics).

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Virtual Domains**.
- Step 3** In the Virtual Domains sidebar menu, click the parent virtual domain for your new virtual domain and then click the **Add New Domain** icon.
- You can also create a new child domain of an existing domain by hovering your mouse cursor over the name of the parent virtual domain. You will see a cross-hair icon appear next to the domain name. Click the icon to display a popup summary of the parent, then click **Create Sub Domain** to create a new child domain of that parent.
- Step 4** Enter the new domain’s name in the **Name** text box. This field is required.
- Step 5** If needed, enter the new domain’s time zone, email address, and description. These are optional fields.
- Step 6** Click **Submit** to view a summary of the newly created virtual domain and your changes to it.
- Step 7** Click **Save** to confirm the changes.

Virtual domains are useful when you use them to restrict the view of a particular set of users to a specified set of site maps, network devices, and access points. See the Related Topics to continue creating a useful virtual domain.

---

### Related Topics

- [Adding Site Maps to Virtual Domains](#)
- [Adding Network Devices to Virtual Domains](#)
- [Adding Access Points to Virtual Domains](#)
- [Adding Users to Virtual Domains](#)
- [Importing Virtual Domains](#)

## Adding Site Maps to Virtual Domains

---

- Step 1** Log in to Prime Infrastructure as an administrator.
  - Step 2** Choose **Administration > Users > Virtual Domains**.
  - Step 3** From the Virtual Domains sidebar menu, click a virtual domain to which you want to add site maps.
  - Step 4** On the Site Maps tab, click the **Add** button to view the list of available site maps. Select the required site maps and then click **Select** to add these site maps to the Selected Site Maps table.
  - Step 5** Click **Submit** to view the summary of the virtual domain.
  - Step 6** Click **Save** to confirm the changes.
- 

### Related Topics

- [Adding Network Devices to Virtual Domains](#)
- [Adding Access Points to Virtual Domains](#)
- [Adding Users to Virtual Domains](#)

## Adding Network Devices to Virtual Domains

---

- Step 1** Log in to Prime Infrastructure as an administrator.
  - Step 2** Choose **Administration > Users > Virtual Domains**.
  - Step 3** From the Virtual Domains sidebar menu, click a virtual domain to which you want to add a network device.
  - Step 4** On the Network Devices tab, click the **Add** button and the Select Network Devices pop-up appears. Here, a **Filter By** drop-down list is available to filter the network devices based on functionality.
  - Step 5** From the **Filter By** drop-down list, choose a network device. Select the required devices from the Available Network Devices table and click **Select** to add the devices to the Selected Network Devices table.
  - Step 6** Click **Submit** to view the summary of the virtual domain.
  - Step 7** Click **Save** to confirm the changes.
- 

### Related Topics

- [Adding Site Maps to Virtual Domains](#)
- [Adding Access Points to Virtual Domains](#)
- [Adding Users to Virtual Domains](#)

## Adding Access Points to Virtual Domains

---

- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Virtual Domains**.
- Step 3** From the Virtual Domains sidebar menu, click a virtual domain to which you want to add access points.
- Step 4** On the Access Points tab, click the **Add** button and the Add Access Points pop-up appears. Here, a **Filter By** drop-down list is available to filter the access points based on functionality.
- Step 5** From the **Filter By** drop-down list, choose an access point group. Select the required access points from the Available Access Points table and click **Select** to add the access points to the Selected Access points table.
- Step 6** Click **Submit** to view the summary of the virtual domain.
- Step 7** Click **Save** to confirm the changes.
- 

### Related Topics

- [Adding Site Maps to Virtual Domains](#)
- [Adding Network Devices to Virtual Domains](#)
- [Adding Users to Virtual Domains](#)

## Importing Virtual Domains

If you plan to create many virtual domains, or give them a complex hierarchy, you will find it easier to specify them in a properly formatted CSV file and then import it.

The CSV format allows you to specify the name, description, time zone and email address for each of the virtual domains you create, as well as each domain's parent domain. Adding site maps, network devices, and access points to any one virtual domain must be done separately.

- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Virtual Domains**.
- Step 3** Click the **Import Domain(s)** icon. Prime Infrastructure displays the Import popup.  
Click the sample CSV format link in the popup to download a sample of the CSV format you must use.
- Step 4** Click **Choose File** and navigate to the CSV file you want to import.
- Step 5** Click **Import** to import the CSV file and create the virtual domains you specified.
- 

### Related Topics

- [Creating Virtual Domains](#)
- [Adding Users to Virtual Domains](#)



## 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*.

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.

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.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Click on the user name of the user you want to add to one or more virtual domains. Prime Infrastructure displays the User Details page for the user you selected.
- Step 4** Click the **Virtual Domains** tab.
- Step 5** In the “Available Virtual Domains”, click the virtual domain you want this user to access. Then click **Add** to add it to the “Selected Virtual Domains” column.
- Except for Root Domain, the child Domains are not automatically included in Users, when their parent Domain is added.
- Step 6** When you are finished, click **Save**.
- 

### Related Topics

- [Adding Virtual Elements to Virtual Domains](#)
- [Using Virtual Domains to Control Access](#)
- [Understanding Virtual Domains](#)
- [User Access in Virtual Domains](#)
- [Creating Virtual Domains](#)

## Adding Virtual Elements to Virtual Domains

Each virtual domain can contain a subset of elements. For example, you can add additional maps, controllers, and access points to a virtual domain. Similarly you can add virtual elements into a virtual domain.

Virtual elements in PI are datacenters, clusters and hosts. If you select a virtual element as datacenter then user who belongs to this virtual domain will get access of all child elements like clusters, hosts and VMs under this datacenter. Similarly if you added only clusters as virtual elements, the user will get access to only the hosts and respective VMs that belong to that cluster. Selecting a parent element will provide access to all child elements in those virtual domains.

You can view number of virtual elements available in a virtual domain from Virtual Domain's **Quick View**.

To add a virtual element, follow these steps:

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
  - Step 2** Choose **Administration > Users > Virtual Domains**.
  - Step 3** Click a virtual domain for which you want to add a virtual element.
  - Step 4** Click the Virtual Elements tab, then click **Add**.
  - Step 5** From the list of Available Virtual Elements, select a filter for which you want to view the available virtual elements.
  - Step 6** Select the required virtual element, then click **Select**.
  - Step 7** Click **Submit** to view the summary of the virtual domain.
  - Step 8** Click **Save** to confirm the changes.
- 

### Related Topics

- [Using Virtual Domains to Control Access](#)
- [Understanding Virtual Domains](#)
- [User Access in Virtual Domains](#)
- [Creating Virtual Domains](#)

## Changing Virtual Domain Access

Choose a virtual domain from the Virtual Domains sidebar menu to view or edit its assigned site maps, network devices, access points, and virtual elements. A page with tabs for viewing the currently logged-in virtual domain-available Site Maps, Network Devices, Access Points, and Virtual Elements is displayed.

The Site Maps, Network Devices, Access Points, and Virtual Elements tabs are used to add or remove components assigned to this virtual domain. You can assign any combination of site maps, network devices, access points, and virtual elements to an existing virtual domain.

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.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Virtual Domains**.
- Step 3** Choose a virtual domain from the Virtual Domains sidebar menu.
- Because all site maps, network devices, access points, and virtual elements are included in the partition tree, it can take several minutes to load the complete hierarchy. This time increases if you have a system with a very large number of network devices and access points.
- Step 4** Click the applicable **Site Maps, Network Devices, Access Points, or Virtual Elements** tab.
- Step 5** To add elements to the Selected table, click the **Add** button, check the check boxes of the required elements (Site Maps, Network Devices, Access Points or Virtual Elements) and click **Select**.
- In the **Network Devices** tab, when you click the **Add** button, the Select Network Devices pop-up appears. Here, a **Filter By** drop-down list is available to select the required network devices. From the **Filter By** drop-down list, choose a network device. Select the required devices from the Available Network Devices table and click **Select**.
- In the **Access Points** tab, when you click the **Add** button, the Add Access Points pop-up appears. Here, a **Filter By** drop-down list is available to add the required access points. From the **Filter By** drop-down list, choose an access point. Select the required access points from the Available Access Points table and click **Select**.
- In **Virtual Element** tab, when you click on **Add** button, Add Virtual Element pop-up appears. Here a **Filter By** drop-down list is available to select the required virtual element. Based on the filter, the selected list will be populated with corresponding virtual elements type. Select the required element from the available virtual elements and click **Select**.
- Step 6** The selected elements (Site Maps, Network Devices, Access Points or Virtual Elements) are listed in the Selected table.
- Step 7** To delete elements from the Selected table, first check the check boxes of the required elements (Site Maps, Network Devices, Access Points, or Virtual Elements) to select them, and then click the **Delete** button.
- Step 8** Click **Submit** to view the summary of the virtual domain.
- Step 9** Click **Save** to confirm the changes.

The autonomous AP added through **Administration > Virtual Domains > Network Devices** will be listed under **Administration > Virtual Domains > Access Points**.

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.

If a non-root domain user has added any discovery source then all virtual elements associated with discovery source will be available only to the root-domain user. Root-domain user has to give access to other child virtual-domains. The root-domain user can control the access of any virtual element.

Once you get access of virtual elements in your non-root domain you can create other virtual domains and manage the access to all these virtual element for your child virtual domain.

---

#### Related Topics

- [Using Virtual Domains to Control Access](#)
- [Understanding Virtual Domains](#)
- [User Access in Virtual Domains](#)
- [Creating Virtual Domains](#)

## Deleting Virtual Domains

You can delete a virtual domain from the Virtual Domains sidebar menu using the pop-up summary window that appears when you click on the cross-hair icon next to the domain's name.

Deleting a virtual domain does not delete any site map, network device, access point or user assigned to the domain. You cannot delete a virtual domain that has child virtual domains until all of the children have been deleted.

---

- Step 1** Log in to Prime Infrastructure as an administrator.
  - Step 2** Choose **Administration > Users > Virtual Domains**.
  - Step 3** In the Virtual Domains sidebar menu, hover your mouse cursor over the information icon (i) next to the name of the virtual domain you want to delete. You will see a popup summary of the virtual domain and its assigned site maps, access points, network devices and virtual elements.
  - Step 4** Click the **Delete** link in the popup.
  - Step 5** You will be prompted to confirm that you want to delete this virtual domain. Click **OK** to confirm.
- 

#### Related Topics

- [Creating Virtual Domains](#)
- [Importing Virtual Domains](#)

## Exporting 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 Custom Attributes button on the page 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.

When you create a sub domain for a previously created virtual domain, the sequence numbers for the custom attributes for RADIUS/TACACS are also updated in the existing virtual domain. These sequence numbers are for representation only and do not impact AAA integration.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Virtual Domains**.
- Step 3** In the left sidebar menu, choose the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.
- Step 4** Click the **Export Custom Attributes** link in the upper right corner of the page. The popup Virtual Domain Custom Attributes page displays the list of RADIUS and TACACS+ custom attributes in two separate panes
- Step 5** Click and drag your mouse cursor to select the text in the RADIUS or TACACS+ Custom Attributes list (depending on which server you are currently configuring).
- Step 6** Using your browser menu, copy the text to your clipboard.
- Step 7** Log in to ACS and navigate to the User or Group Setup.
- 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 8** For the applicable user or group, click **Edit Settings**.
- Step 9** Select the check boxes to enable these attributes, then click **Submit + Restart**.
- 

### Related Topics

- [Using Virtual Domains to Control Access](#)
- [Understanding Virtual Domains](#)
- [Creating Virtual Domains](#)

# Auditing User Access

Prime Infrastructure maintains an audit record of user access, allowing you to check on user access and session activity.

## Related Topics

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

## Accessing the Audit Trail for a User Group

---

- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > User Groups**.
- Step 3** 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.

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.

---

## Related Topics

- [Auditing User Access](#)
- [Viewing Application Logins and Actions](#)
- [Viewing User-Initiated Events](#)

## 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.

- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Settings > System Audit**.
- Step 3** In the Application Audit Logs page, click to expand the row for which you want to view log details. For users authenticated via TACACS+ or RADIUS, the User Group column will be blank.
- 

## Related Topics

- [Auditing User Access](#)

- [Viewing User-Initiated Events](#)

## Viewing User-Initiated Events

Prime Infrastructure's network audit logs record all events related to the devices in your network, including user-initiated events. For example, you can view the network audit logs to see which Prime Infrastructure user deployed a specific template and the date and time the template was deployed.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Inventory > Device Management > Network Audit**. The Network Audit Log page displays a list of recent actions, sorted by the name of the device on which the action was performed.
- Step 3** Click to expand the row for which you want to view log details.
- 

### Related Topics

- [Auditing User Access](#)
- [Viewing Application Logins and Actions](#)
- [Viewing User-Initiated Events](#)

## Configuring AAA on Prime Infrastructure

Prime Infrastructure can be configured to communicate with external authentication, authorization, and accounting (AAA) servers. The only user that has permission to configure AAA on Prime Infrastructure is the Root or SuperUser.

Any changes to local user accounts are in effect immediately if you are using Prime Infrastructure internal, or local, AAA mode. If you are using external AAA, such as RADIUS or TACACS+, the user account changes must be copied to the external server. Also note that combinations of Prime Infrastructure user-group memberships that are invalid with local AAA are also invalid when copied to the RADIUS server (even though RADIUS will permit you to create these invalid combinations when you set up RADIUS user attribute/value pairs). For a list of invalid user-group combinations, see the table in "Using User Groups to Control Access".

For information about migrating AAA servers, see the *ACS 5.2 Migration Utility Support Guide* listed in Related Topics.

### Related Topics

- [Setting the AAA Mode](#)
- [Adding TACACS+ Servers](#)
- [Adding RADIUS Servers](#)
- [Adding SSO Servers](#)
- [Configuring SSO Server AAA Mode](#)
- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)
- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [ACS 5.2 Migration Utility Support Guide](#)

- [Using User Groups to Control Access](#)

## Setting the AAA Mode

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

If you add more than one external AAA server, users are authenticated on the second server only if the first server is not reachable or has network problems.

You can use any alphabetical, numerical or special character (except for the single and double quote characters) while entering the shared secret key for a third-party TACACS+ or RADIUS server.

- 
- Step 1** Add one or more RADIUS or TACACS+ servers. For details, see “Adding RADIUS Servers” and “Adding TACACS+ Servers” in Related Topics.
- Step 2** Log in to Prime Infrastructure as SuperUser.
- Step 3** Select **Administration > Users > Users, Roles & AAA > AAA Mode Settings**.
- Step 4** Select **RADIUS** or **TACACS+**. The **Enable Fallback to Local** check box is automatically selected, enabling use of the local database when the external AAA server is down.
- Step 5** With the **Enable Fallback to Local** check box selected, specify the conditions under which the fallback to local Prime Infrastructure user account authentication occurs:
- **ONLY on no server response:** Only when the external server is unreachable or has network problems.
  - **on authentication failure or no server response:** Either when the external server is unreachable or has network problems *or* the external AAA server cannot authenticate the user.
- For AAA mode, SuperUser is always locally authenticated.
- Step 6** Click **Save**.
- 

### Related Topics

- [Adding TACACS+ Servers](#)
- [Adding RADIUS Servers](#)



## Adding TACACS+ Servers

Prime Infrastructure can use a maximum of three AAA servers.

- 
- Step 1** Log in to Prime Infrastructure as SuperUser.
  - Step 2** Choose **Administration > Users > Users, Roles & AAA > TACACS+ Servers**.
  - Step 3** Choose **Select a command > Add TACACS+ Server (IP or DNS) > Go**.
  - Step 4** Enter the TACACS+ server information, then click **Save**.

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.

If you have enabled Prime Infrastructure High Availability and configured a virtual IP feature, the **Local Interface IP** field will offer you a choice between the virtual IP address and the physical IP address of the primary server. Be sure to select the physical IP address as the Local Interface IP.

---

### Related Topics

- [How High Availability Works](#)
- [Using Virtual IP Addressing with HA](#)
- [Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes](#)

## Adding RADIUS Servers

Prime Infrastructure can use a maximum of three AAA servers.

- 
- Step 1** Log in to Prime Infrastructure as SuperUser.
  - Step 2** Choose **Administration > Users > Users, Roles & AAA > RADIUS Servers**.
  - Step 3** Choose **Select a command > Add Radius Server(IP or DNS) > Go**.
  - Step 4** Enter the RADIUS server information.
  - Step 5** Select the authentication type.

The authentication types available are:

- **PAP**—Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication.
- **CHAP**—Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).
- **EAP\_TLS**—Extensible Authentication Protocol - Transport Layer Security is a secure protocol as it supports certificate-based mutual authentication. When EAP-TLS is selected as the authentication type, the generated key must be added to Cisco Prime Infrastructure keystore using **ncs key importsignedcert** admin CLI and the certificate chains must be present in RADIUS server. This does not require Cisco Prime Infrastructure services restart.

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

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 Topics**

- [Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes](#)
- [Renewing AAA Settings After Installing a New Prime Infrastructure Version](#)

## 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 TACACS+ Servers](#)
- [Adding RADIUS Servers](#)
- [Renewing AAA Settings After Installing a New Prime Infrastructure Version](#)

## Renewing AAA Settings After Installing a New Prime Infrastructure Version

If you were using external RADIUS or TACACS+ user authentication before migrating your existing data to a new version of Prime Infrastructure, you must transfer the expanded Prime Infrastructure user task list to your AAA server. After you upgrade Prime Infrastructure, you must re-add any permissions on the TACACS+ or RADIUS server and update the roles in your TACACS server with the tasks from the Prime Infrastructure server. For information, see “Setting the AAA Mode” in Related Topics.

If you changed the IP address of the Prime Infrastructure server during the upgrade process, you will need to log in to Prime Infrastructure as SuperUser and follow the instructions given in “Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes” before other users will be able to log in.

**Related Topics**

- [Adding TACACS+ Servers](#)
- [Adding RADIUS Servers](#)
- [Setting the AAA Mode](#)
- [Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes](#)

## Adding SSO Servers

You can enable Single Sign-On Authentication (SSO) in Prime Infrastructure.

SSO allows Prime Infrastructure users to enter their credentials just once before navigating across multiple SSO-enabled Prime Infrastructure applications. SSO makes it easier for users 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.

Before setting up SSO, you must have an SSO-configured server and know its basic IP information. You must also configure the SSO server's AAA mode. For details on the latter task, see "Configuring SSO Server AAA Mode" in Related Topics.

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > SSO Servers**.
- Step 3** Choose **Select a command > Add SSO Server > Go**.
- Step 4** Enter the SSO server information, then click **Save**.

The maximum number of retries allowed for SSO server authentication requests is three.

The default Port Number is 443, which refers to the port on which the HTTPS is configured. You need to change the Port Number if you configure HTTPS on the Prime Infrastructure SSO Server on a different port.

---

### Related Topics

- [Configuring SSO Server AAA Mode](#)
- [Configuring AAA on Prime Infrastructure](#)

## Configuring High Availability for SSO

You can configure High Availability on the SSO client in the following ways:

- Adding multiple SSO servers. Configure all the SSO servers with the same set of external AAA servers to ensure that they have the same authentication and authorization credentials. The Prime Infrastructure SSO clients will attempt to use the SSO servers in the order in which they were defined, as displayed in the list of SSO servers on the Prime Infrastructure SSO servers page. For example: If the first SSO server is unavailable, the SSO client will fall back to the second SSO server in the list and use it. If the second is unavailable, the SSO client will fall back to the third SSO server — and so on, to the limit of the SSO servers you have defined.
- Create an HA pair for the SSO server: Configure a virtual IP address for the HA primary and secondary servers. For more information on High Availability see "Configuring High Availability" (in Related Topics, below). The Prime Infrastructure SSO clients will be configured with an SSO server with the configured Virtual IP address.

### Related Topics

- [Configuring High Availability](#)

## Configuring SSO Server AAA Mode

Single Sign-On Authentication (SSO) is used to authenticate and manage users in multi-user, multi-repository environments. SSO servers 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.

Prime Infrastructure supports CA and self-signed certificates as long as the Common Name (CN) field of the certificate contains the Fully Qualified Domain Name (FQDN) of the server on both the SSO client and the SSO server. The server must be capable of name resolution from the IP address to the FQDN. In addition, the hostname must match the left-most component of the 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.example.com
Address:
```

For SSO operation, Prime Infrastructure requires that the SSL/TLS certificate hold the FQDN in the Common Name (CN) field. To verify that the certificate used by your Prime Infrastructure server has the FQDN in the CN field, use your browser to view the certificate. If the certificate does not contain the FQDN in the CN field, you must regenerate the certificate. After you regenerate the SSL/TLS certificate, add the SSO server to any or all the SSO clients. The SSO functionality distributes the certificate when the SSO server is added to the SSO client.

To add the SSO server, follow these steps:

- 
- Step 1** Log in to Prime Infrastructure as an administrator.
  - Step 2** Choose **Administration > Users > Users, Roles & AAA > SSO Server AAA Mode**.
  - Step 3** Choose which SSO Server AAA mode you want to use. You can select only one at a time.

Any changes to local user accounts are effective only when you are configured for local mode. 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 4** Click **OK**.
- 

### Related Topics

- [Configuring AAA on Prime Infrastructure](#)
- [Setting Up SSL Certification](#)
- [Configuring AAA on Prime Infrastructure](#)

## Authenticating AAA Users Through RADIUS Using ISE: Workflow

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


Only RADIUS server authentication is supported in ISE.

- 
- Step 1** Add Prime Infrastructure as a AAA client in ISE. For details, see “Adding Prime Infrastructure as an AAA Client in ISE” in Related Topics.
  - Step 2** Create a new User group in ISE. For details, see “Creating a New User Group in ISE”.
  - Step 3** Create a new User in ISE and add that User to the User group created in ISE. For details, see “Creating a New User” and “Adding to a User Group in ISE”.
  - Step 4** Create a new Authorization profile. For details, see “Creating a New Authorization Profile in ISE”.
  - Step 5** Create an Authorization policy rule. For details, see “Creating an Authorization Policy Rule in ISE”.
  - Step 6** Create an Authentication policy. For details, see “Creating a Simple Authentication Policy in ISE” or “Creating a Rule-Based Authentication Policy in ISE”.
  - Step 7** Configure AAA in Prime Infrastructure. For details, see “Configuring AAA in Prime Infrastructure”.
- 

### Related Topics

- [Adding Prime Infrastructure as an AAA Client in ISE](#)
- [Creating a New User Group in ISE](#)
- [Creating a New User and Adding to a User Group in ISE](#)
- [Creating a New Authorization Profile in ISE](#)
- [Creating a Simple Authentication Policy in ISE](#)
- [Creating a Rule-Based Authentication Policy in ISE](#)
- [Configuring AAA on Prime Infrastructure](#)

## Adding 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.
-

**Related Topics**

- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)
- [Creating a New User Group in ISE](#)
- [Creating a New User and Adding to a User Group in ISE](#)
- [Creating a New Authorization Profile in ISE](#)
- [Creating a Simple Authentication Policy in ISE](#)
- [Creating a Rule-Based Authentication Policy in ISE](#)
- [Configuring AAA on Prime Infrastructure](#)

## 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.

- 
- 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**.
- 

**Related Topics**

- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)
- [Adding Prime Infrastructure as an AAA Client in ISE](#)
- [Creating a New User and Adding to a User Group in ISE](#)
- [Creating a New Authorization Profile in ISE](#)
- [Creating a Simple Authentication Policy in ISE](#)
- [Creating a Rule-Based Authentication Policy in ISE](#)
- [Configuring AAA on Prime Infrastructure](#)

## 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.

- 
- 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**.

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

---

### Related Topics

- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)
- [Adding Prime Infrastructure as an AAA Client in ISE](#)
- [Creating a New User Group in ISE](#)
- [Creating a New Authorization Profile in ISE](#)
- [Creating a Simple Authentication Policy in ISE](#)
- [Creating a Rule-Based Authentication Policy in ISE](#)
- [Configuring AAA on Prime Infrastructure](#)

## Creating a New Authorization Profile 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 area, 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 > Users, Roles & AAA > User Groups**. Click **Task List** for the group with appropriate permissions.

- a. Select **cisco - av - pair** and paste Prime Infrastructure user group RADIUS custom attribute next to it. Keep adding one after another.
  - b. Add the Virtual Domain attribute at the end of the last RADIUS custom attribute for each group (for RADIUS custom attributes, see “Exporting Virtual Domain RADIUS and TACACS+ Attributes”).
- Step 6** Save the authorization profile.
- 

### Related Topics

- [Exporting Virtual Domain RADIUS and TACACS+ Attributes](#)
- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)

- [Adding Prime Infrastructure as an AAA Client in ISE](#)
- [Creating a New User Group in ISE](#)
- [Creating a New User and Adding to a User Group in ISE](#)
- [Creating a Simple Authentication Policy in ISE](#)
- [Creating a Rule-Based Authentication Policy in ISE](#)
- [Configuring AAA on Prime Infrastructure](#)

## Creating an Authorization Policy Rule in ISE

- 
- 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**.
- 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**. 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 the ISE > Monitor > Authentications option.
- 

### Related Topics

- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)
- [Adding Prime Infrastructure as an AAA Client in ISE](#)
- [Creating a New User Group in ISE](#)
- [Creating a New User and Adding to a User Group in ISE](#)
- [Creating a New Authorization Profile in ISE](#)
- [Creating a Simple Authentication Policy in ISE](#)
- [Creating a Rule-Based Authentication Policy in ISE](#)
- [Configuring AAA on Prime Infrastructure](#)



## 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*
- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)
- [Adding Prime Infrastructure as an AAA Client in ISE](#)
- [Creating a New User Group in ISE](#)
- [Creating a New User and Adding to a User Group in ISE](#)
- [Creating a New Authorization Profile in ISE](#)
- [Creating a Rule-Based Authentication Policy in ISE](#)
- [Configuring AAA on Prime Infrastructure](#)

## 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. We recommend 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*
- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)
- [Adding Prime Infrastructure as an AAA Client in ISE](#)
- [Creating a New User Group in ISE](#)
- [Creating a New User and Adding to a User Group in ISE](#)
- [Creating a New Authorization Profile in ISE](#)
- [Creating a Simple Authentication Policy in ISE](#)
- [Configuring AAA on Prime Infrastructure](#)

## Configuring AAA in Prime Infrastructure

---

- Step 1** Log in to Prime Infrastructure as *root*, then choose **Administration > Users > 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 > Users > Users, Roles & AAA > AAA Mode Settings**.
- Step 4** Select **RADIUS** as the AAA mode, then click **Save**.
- Step 5** Log out of Prime Infrastructure.
- Step 6** Log in again to Prime Infrastructure as an AAA user that is already defined in ISE. For example, log in as user *ncs-sysmon*.
- 

#### Related Topics

- [Authenticating AAA Users Through RADIUS Using ISE: Workflow](#)
- [Adding Prime Infrastructure as an AAA Client in ISE](#)
- [Creating a New User Group in ISE](#)
- [Creating a New User and Adding to a User Group in ISE](#)
- [Creating a New Authorization Profile in ISE](#)
- [Creating a Simple Authentication Policy in ISE](#)
- [Creating a Rule-Based Authentication Policy in ISE](#)

## Configuring ACS 5.x for Prime Infrastructure: Workflow

If you are configuring ACS 5.x to work with Prime Infrastructure, you will follow this workflow:

1. Create ACS network devices and AAA clients.
2. Add ACS groups.
3. Add ACS users.
4. Create ACS policy elements or authorization profiles for RADIUS or TACACS+, as appropriate.
5. Create ACS service selection rules for RADIUS or TACACS+, as appropriate.
6. Configure ACS access services for RADIUS or TACACS+, as appropriate.

### Related Topics

- [Creating ACS Network Devices and AAA Clients](#)
- [Adding ACS Groups](#)
- [Adding ACS Users](#)
- [Creating ACS Policy Elements or Authorization Profiles for RADIUS](#)
- [Creating ACS Policy Elements or Authorization Profiles for TACACS+](#)
- [Creating ACS Service Selection Rules for RADIUS](#)
- [Creating ACS Service Selection Rules for TACACS+](#)
- [Configuring ACS Access Services for RADIUS](#)
- [Configuring ACS Access Services for TACACS+](#)

## Creating ACS Network Devices and AAA Clients

- 
- Step 1** Log in to the ACS 5.x server and choose **Network Resources > Network Devices and AAA Clients**.
- Step 2** Enter an IP address.
- 

### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Adding ACS Groups](#)

## Adding ACS Groups

- 
- Step 1** Log in to the ACS 5.x server and choose **Users and Identity Stores > Identity Groups**.
- Step 2** Create a group.
- 

### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Creating ACS Network Devices and AAA Clients](#)
- [Adding ACS Users](#)

## Adding ACS Users

- 
- Step 1** Log in to the ACS 5.x server and choose **Users and Identity Stores > Internal Identity Stores > Users**.
- Step 2** Add a user, and then map a group to that user.
- 

### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Adding ACS Groups](#)
- [Creating ACS Policy Elements or Authorization Profiles for RADIUS](#)
- [Creating ACS Policy Elements or Authorization Profiles for TACACS+](#)

## Creating ACS Policy Elements or Authorization Profiles for RADIUS

- 
- Step 1** Log in to the ACS 5.x server and choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click **Create**.
- Step 2** Enter the required information, then click **Submit**.

The **Export Custom Attributes** button 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 users have access to these virtual domains only.

---

### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Adding ACS Users](#)
- [Creating ACS Service Selection Rules for RADIUS](#)
- [Configuring ACS Access Services for RADIUS](#)

## Creating ACS Policy Elements or Authorization Profiles for TACACS+

Before you begin, ensure that you add the relevant Menu Access task so that the ACS 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** Retrieve the appropriate User Group task list attribute/value pairs from Prime Infrastructure:
- Log in to Prime Infrastructure as an administrator and choose **Administration > Users > Users, Roles & AAA > User Groups**. Prime Infrastructure displays the list of User Groups.
  - Display the task list for the user group whose authorizations you want to send to ACS.  
  
For example, if you want to send Admin user group authorizations to ACS: In the **Group Name** column, find the **Admin** group at the top of the list, then click the **Task List** link at the far right, opposite the “Admin” entry. Prime Infrastructure displays separate lists of custom task attributes for TACACS+ and RADIUS.
  - Copy and save the TACACS+ custom attributes to your desktop.
  - Repeat these steps as needed for all the user groups whose tasks you want to add to ACS.
- Step 2** Log in to the ACS Admin GUI, and choose **Policy Elements > Authentication and Permissions > Device Administration > Shell Profiles**.
- Step 3** Click **Create** to create a new ACS shell profile for Prime Infrastructure
- Step 4** Choose the **Custom Attributes** tab, then click **Bulk Edit**.
- Step 5** Copy and paste all the attribute/value pairs you retrieved in Step 1 into the new shell profile.
- Step 6** When you are finished, click **Submit** to create an attribute-based role for Prime Infrastructure.
- 

### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Adding ACS Users](#)
- [Creating ACS Service Selection Rules for TACACS+](#)
- [Configuring ACS Access Services for TACACS+](#)

## Creating ACS Service Selection Rules for RADIUS

- 
- Step 1** Log in to the ACS 5.x server and choose **Access Policies > Access Services > Service Selection Rules**.
- Step 2** Click **Create**.
- Step 3** Enter the required information, then click **OK**.
- 

### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Creating ACS Policy Elements or Authorization Profiles for RADIUS](#)
- [Creating ACS Service Selection Rules for RADIUS](#)

- [Configuring ACS Access Services for RADIUS](#)

## Creating ACS Service Selection Rules for TACACS+

---

- Step 1** Log in to the ACS 5.x server and choose **Access Policies > Access Services > Service Selection Rules**.
- Step 2** Click **Create**.
- Step 3** Enter the required information, then click **OK**.
- 

### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Creating ACS Policy Elements or Authorization Profiles for TACACS+](#)
- [Configuring ACS Access Services for TACACS+](#)

## Configuring ACS 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.  
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**.
- 

### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Creating ACS Service Selection Rules for RADIUS](#)

## Configuring ACS Access Services for TACACS+

---

- Step 1** Log in to the ACS 5.x server and 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.  
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**.
- 

#### Related Topics

- [Configuring ACS 5.x for Prime Infrastructure: Workflow](#)
- [Creating ACS Service Selection Rules for TACACS+](#)







## Advanced Monitoring

Cisco Prime Infrastructure consumes a lot of information from various different sources, including NAM, NetFlow, NBAR, Cisco Medianet, PerfMon, and Performance Agent. The following table depicts the sources of the data for the site dashlets used by Prime Infrastructure:

**Table 12-1** *Site Dashlet Data Sources*

| Dashlet Name                        | NAM | Cisco 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 12-2** *Application-Specific Dashlet Data Sources*

| Dashlet Name                        | NAM | Cisco 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 12-2** 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 | – |

**Related Topics**

- [Enabling Medianet NetFlow](#)
- [Enabling NetFlow and Flexible NetFlow](#)

# Enabling 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 *Using Cisco NAM Hardware in a WAAS Deployment*.

After you have deployed your WAAS changes at candidate sites, you can navigate to **Dashboards > Performance > 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. From the Multi-Segment Analysis display, you can select the:

- **Conversations** tab to see individual client/server sessions.
- **Site to Site** tab to see aggregated site traffic.

The following table describes the key WAAS monitoring dashlets.

**Table 12-3** 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.                                                                                                                                                                                  |

Note that you cannot access Multi-Segment Analysis unless you have purchased and applied Prime Infrastructure Assurance licenses. The WAAS monitoring dashlets will display no data unless you have implemented WAAS at candidate sites.





## Managing Licenses

---

The **Administration > Licenses and Software Updates > Licenses** page allows you to manage Cisco 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 and Software Updates > Licenses** page, you can only view Cisco Wireless LAN Controllers (WLC). You must use Cisco WLC or Cisco License Manager (CLM) to manage Cisco WLC licenses.

### Related Topics

- [Prime Infrastructure Licensing](#)
- [Controller Licensing](#)
- [MSE Licensing](#)
- [Assurance Licensing](#)

## 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 Data Center licenses) 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.

2. View the existing licenses. See 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.
4. Add new licenses.
5. Delete existing licenses.

**Related Topics**

- [Cisco Prime Infrastructure Ordering and Licensing Guide](#)
- [Verifying License Details](#)
- [Adding Licenses](#)
- [Deleting Licenses](#)

## Purchasing Prime Infrastructure Licenses

Prime Infrastructure licenses control the features you can use and the number of devices you can manage using those features. For more information about Prime Infrastructure license types and how to order them, see the Cisco Prime Infrastructure 2.2 Ordering and Licensing Guide.

You can ignore warning messages like “Base license is missing” or “Multiple base licenses present, use only one” displayed in the **Administration > Licenses and Software Updates > Licenses > Files > License Files** area.

**Related Topics**

- [Cisco Prime Infrastructure Ordering and Licensing Guide](#)

## Verifying License Details

Before you order new licenses, you might want to get details about your existing licenses. For example, number of devices managed by your system.

To verify license details, choose **Administration > Licenses and Software Updates > Licenses**.

**Related Topics**

- [Prime Infrastructure Licensing](#)
- [Controller Licensing](#)
- [MSE Licensing](#)
- [Assurance Licensing](#)

## 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.

- 
- Step 1** Choose **Administration > Licenses and Software Updates > Licenses**.
- Step 2** In the **Summary** folder, click **Files**, then click **License Files**.
- Step 3** Click **Add**.
- Step 4** Browse to the location of the license file, then click **OK**.
- 

### Related Topics

- [Deleting Licenses](#)
- [Troubleshooting Licenses](#)
- [MSE License Structure Matrix](#)
- [Verifying Assurance License Details](#)

## 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.

- 
- Step 1** Choose **Administration > Licenses and Software Updates > Licenses**.
- Step 2** Click **Files > License Files**.
- Step 3** Select the license file you want to delete, then click **Delete**.
- 

### Related Topics

- [Adding Licenses](#)
- [Troubleshooting Licenses](#)
- [MSE License Structure Matrix](#)
- [Verifying Assurance License Details](#)

## Troubleshooting Licenses

To troubleshoot licenses, you will need to get details about the licenses that are installed on your system. to:

- Get a quick list of the licenses you have: Click **Help > About Prime Infrastructure**
- Get license details: Choose **Administration > Licenses and Software Updates > Licenses**.

When troubleshooting licenses, it is important to remember that Prime Infrastructure has six types of licenses:

- **Base:** Required for every Prime Infrastructure installation. The requirement stems primarily from the need to do accurate royalty accounting by knowing how many Prime Infrastructure instances have been purchased. A Base license is required for each instance of Prime Infrastructure, and is a prerequisite for all other license types.
- **Lifecycle:** Regulates the total number of devices under Prime Infrastructure management.
- **Assurance:** Regulates the total number of NetFlow devices under Prime Infrastructure management.
- **Collector:** Regulates the total number of NetFlow data flows per second that Prime Infrastructure can process.
- **Data Center:** Regulates the number of blade servers being managed by UCS device(s) in Prime Infrastructure. The license count matches the number of blades or rack units associated with any UCS device.

Datacenter licenses are specific only to UCS devices (Blade count). Other Data Center devices, such as Nexus switches and MDS devices, are managed using a normal Lifecycle license.

- **Data Center Hypervisor:** Regulates the total number of host(s) managed by Prime Infrastructure management. This license manages Discovery Sources (Vcenters) in Prime Infrastructure. This license type was introduced with Prime Infrastructure version 3.0.

Lifecycle, Assurance and Data Center licenses are supplied in either evaluation or permanent form (there is no explicit evaluation version of the Base, Collector, or Data Center Hypervisor licenses):

- **Evaluation:** These licenses permit or extend access to Prime Infrastructure for a pre-set period. You can apply only one evaluation license of each type (that is, only one Lifecycle evaluation license, one Assurance evaluation license, and so on). You cannot apply an evaluation license over a permanent form of the same license.
- **Permanent License:** These permit access to Prime Infrastructure features as specified and are not time-limited. Permanent licenses can be applied over evaluation licenses, and can also be applied incrementally (that is, you can have multiple permanent Assurance licenses, and so on).

Prime Infrastructure also performs the following basic license checks:

- A Lifecycle license is a required prerequisite for Assurance licenses.
- An Assurance license is a required prerequisite for Collector licenses.
- Lifecycle, Data Center and Data Center Hypervisor licenses can be added independently of each other.

Also note that:

- Prime Infrastructure 3.0 enables the user to set threshold limit for generating an alarm for all licenses except Data Center Hypervisor license. To set threshold limit for licenses, see “Configuring Notifications” in Related Topics.



- Prime Infrastructure hides Assurance-related features, menu options and links until an Assurance license is applied. Even if you have purchased an Assurance license, these features remain hidden until you apply it.
- Whenever you apply an Assurance license, you automatically apply a Collector license permitting an instance of Prime Infrastructure to process up to 20,000 NetFlow data flows per second. Collector licenses permitting 80,000 flows per second can be applied only with the Professional or equivalent configurations, due to the hard disk requirements imposed by this data rate.
- You can add Lifecycle, Assurance and Data Center permanent licenses incrementally. However, you can add only one Collector 80K license, and then only with the Professional or equivalent configuration.

The following table provides some scenarios and tips for troubleshooting.

**Table 13-1 Troubleshooting Scenarios**

| Scenario                                           | Possible Cause                                                                                                                                                                                                                                                                                                                                                   | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prime Infrastructure reports a Licensing error.    | The license file may be corrupted and unusable. This can occur anyone attempts to modify the license 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 licenses.                        | Some types of license must be added in the correct order. The Base license is a prerequisite for adding Lifecycle licenses. A Lifecycle license is a prerequisite for adding an Assurance or Data Center license. An Assurance license is a prerequisite for adding a Collector license (a Collector license is added automatically with the Assurance license). | <ol style="list-style-type: none"> <li>1. Add the Base license</li> <li>2. Add Lifecycle licenses</li> <li>3. Add Assurance licenses</li> <li>4. Add Datacenter licenses</li> <li>5. Add Collector licenses</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 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>Monitor &gt; Network Devices</b></li> <li>2. Check the Inventory Collection Status column for the row listing the devices in which you are interested. This will give you a summary of current collection status efforts for those devices.</li> <li>3. For details about the collection status, hover the mouse cursor over the cross-hair icon in the Inventory Collection Status column.</li> </ol> |

#### Related Topics

- [Configuring Notifications](#)
- [Adding Licenses](#)

- [Deleting Licenses](#)
- [MSE License Structure Matrix](#)
- [Verifying Assurance License Details](#)

## Controller Licensing

To view controller licenses, choose **Administration > Licenses and Software Updates > Licenses**, then select **Files > Controller Files** from the left sidebar menu.



### 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.

You can have both a WPlus and a 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.

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.

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.

You must have a Cisco Prime Infrastructure license to use MSE and its associated services.

### Related Topics

- [MSE License Structure Matrix](#)
- [Sample MSE License File](#)
- [Revoking and Reusing an MSE License](#)
- [MSE Services Coexistence](#)
- [Managing MSE Licenses](#)

## MSE License Structure Matrix

The following table lists the breakdown of the licenses between the High end, Low end and Evaluation licenses for MSE, Location services, SCM, wIPS, and MIR.

**Table 13-2** *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          |

### Related Topics

- [Sample MSE License File](#)
- [Revoking and Reusing an MSE License](#)
- [MSE Services Coexistence](#)
- [Managing MSE Licenses](#)

## 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.

**Related Topics**

- [MSE License Structure Matrix](#)
- [Revoking and Reusing an MSE License](#)
- [MSE Services Coexistence](#)
- [Managing MSE Licenses](#)

## 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.

**Related Topics**

- [MSE License Structure Matrix](#)
- [Sample MSE License File](#)
- [MSE Services Coexistence](#)
- [Managing MSE Licenses](#)

## 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.

#### Related Topics

- [MSE License Structure Matrix](#)
- [Sample MSE License File](#)
- [Revoking and Reusing an MSE License](#)
- [Managing MSE Licenses](#)

## Managing MSE Licenses

To view Mobility Services Engine (MSE) licenses, choose **Administration > Licenses and Software Updates > Licenses**, then select **Files > MSE Files** from the left sidebar menu.

The page displays the MSE licenses found and includes the following information:

- **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.

Tag licenses are installed using the *AeroScout System Manager* only if the tags are tracked using the Partner engine. Otherwise the tags will be counted along with the CAS element license. Because tag licenses are added and managed using appropriate vendor applications, tag licenses are not displayed in this page. For more information, see the AeroScout Support Page in Related Topics. Evaluation (demo) licenses are also not displayed.

#### Related Topics

- [AeroScout Support Page](#)
- [Registering Product Authorization Keys](#)
- [Installing Client and wIPS License Files](#)
- [Deleting Mobility Services Engine License Files](#)

## 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.

Tag PAKs are registered with AeroScout. To register your tag PAK, navigate to the AeroScout Support Page given in Related Topics.

To register a product authoritative key (PAK) and obtain a license file for installation, follow these steps:

- 
- Step 1** Point your browser to the Cisco Product License Registration Portal (see Related Topics). 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. If the license is incorrect, click the **TAC Service Request Tool** link to report the problem.
- Step 4** In 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. UDI information for a mobility services engine is found in the General Properties area at **Services > Mobility Services Engine > Device Name > System**.
- Step 5** Select the **Agreement** check box. Registrant information appears beneath the check box. Modify information as necessary. 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**.
- 

### Related Topics

- [AeroScout Support Page](#)
- [Cisco Product License Registration Portal](#)
- [Installing Client and wIPS License Files](#)
- [Deleting Mobility Services Engine License Files](#)

## Installing Client and wIPS License Files

You can install CAS element licenses and wIPS licenses from Prime Infrastructure.

Tag licenses are installed using the AeroScout System Manager (see the AeroScout Support Page in Related Topics).

To add a client or wIPS license to Prime Infrastructure after registering the PAK, follow these steps

- 
- Step 1** Choose **Administration > Licenses and Software Updates > Licenses**.
- Step 2** From the left sidebar menu, choose **Files > MSE Files**.
- Step 3** 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.

---

### Related Topics

- [AeroScout Support Page](#)
- [Installing Client and wIPS License Files](#)
- [Deleting Mobility Services Engine License Files](#)



## Deleting Mobility Services Engine License Files

- 
- Step 1** Choose **Administration > Licenses and Software Updates > Licenses**, then select **Files > MSE Files** from the left sidebar menu.
- Step 2** Select the check box of the mobility services engine license file that you want to delete.
- Step 3** Click **Delete**, then click **OK** to confirm the deletion.
- 

### Related Topics

- [Registering Product Authorization Keys](#)
- [Installing Client and wIPS License Files](#)

## Assurance Licensing

As explained in “Purchasing Prime Infrastructure Licenses” (see Related Topics), 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”, “Deleting Licenses” and “Troubleshooting Licenses”.

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.

### Related Topics

- [Purchasing Prime Infrastructure Licenses](#)
- [Verifying Assurance License Details](#)
- [Adding Licenses](#)
- [Deleting Licenses](#)
- [Troubleshooting Licenses](#)

## 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 13-3** 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 and Software Updates &gt; Licenses &gt; Summary.</b>                                                       |
| The total number of Assurance licenses you have and the files associated with them.                                                                  | <b>Administration &gt; Licenses and Software Updates &gt; Licenses &gt; Files.</b>                                                         |
| A list of the devices sending NetFlow or NAM polling data to Prime Infrastructure.                                                                   | <b>Administration &gt; Licenses and Software Updates &gt; Licenses &gt; Assurance Licenses (link is in upper right corner of the page)</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 Licenses page, as well as on the , Summary and Files > License Files pages is always updated whenever you add or delete Assurance licenses. Addition or removal of devices covered under these added or deleted Assurance licenses takes place as part of a System Defined Job, which runs automatically once every 12 hours. It can take up to 12 hours for the added or deleted devices to appear.

You can always access the **Administration > Licenses and Software Updates > Licenses > Assurance Licenses page** from the **Assurance Licenses** link in the upper right corner of the **Administration > Licenses and Software Updates > Licenses > Summary** and **Administration > Licenses and Software Updates > Licenses > Files** pages.

### Related Topics

- [Verifying Assurance License Details](#)
- [Installing Client and wIPS License Files](#)
- [Deleting Mobility Services Engine License Files](#)

## 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 and Software Updates > Licenses > Assurance Licenses** (the **Assurance Licenses** link is in the upper right corner of the page).
- 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**.
- 

### Related Topics

- [Deleting License Coverage for NetFlow and NAM Devices](#)

## 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 and Software Updates > Licenses > Assurance Licenses** (the **Assurance Licenses** link is in the upper right corner of the page).
- 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**.
- 

### Related Topics

- [Adding License Coverage For NetFlow and NAM Devices](#)





## Managing Traffic Metrics

---

Cisco 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 software and Catalyst switches that help isolate and troubleshoot problems with RTP and TCP data streams. Prime Infrastructure supports all versions of Cisco 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 Cisco Medianet Performance Monitor and Cisco IOS NetFlow. When properly configured, Mediatrace can be your most valuable tool when troubleshooting RTP and TCP application problems.

### Related Topics

- [Prerequisites for Traffic Metrics With Mediatrace](#)
- [Configuring Mediatrace on Routers and Switches](#)
- [Configuring WSMA and HTTP\(S\) Features on Routers and Switches](#)

## Prerequisites for Traffic Metrics With Mediatrace

Before you can use Prime Infrastructure's Mediatrace feature, you must complete the prerequisite setup tasks shown under Related Topics, below. These prerequisite tasks are required to enable Cisco routers (ISRs, ISR G2s, ASRs) and NAM devices to act as data (metrics collection) sources to monitor network traffic (RTP and TCP) performance metrics.

### Related Topics

- [Configuring Prime Infrastructure to Use NAM Devices as Data Sources](#)
- [Configuring Prime Infrastructure to Use Routers and Switches as Data Sources](#)

## Configuring Prime Infrastructure to Use NAM Devices as Data Sources

If your network uses Cisco 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 to Prime Infrastructure” in Related Topics).
- Step 2** Enable NAM Data collection. To do this:
- Choose **Services > Application Visibility & Control > Data Sources**.
  - In the NAM Data Collector section, select each NAM and click **Enable** to enable data collection on the selected NAMs (see “Enabling NAM Data Collection”).
- Step 3** Create a site structure for your organization and assign your principal routers to the appropriate sites:
- Choose **Maps > Site Maps**.
  - Add one or more campuses, buildings, and floors (for details, see “Working With Maps”).
- Step 4** Associate your sites with authorized data sources:
- Choose **Services > Application Visibility & Control > Data Deduplication**.
  - Click **Enable Data Deduplication**, then click **Apply**. You can then assign authoritative sources for ART, Traffic Analysis and Voice/Video data (see “Enabling Data Deduplication”).
- Step 5** Associate your sites with endpoint subnets:
- Choose **Services > Application Visibility & Control > Endpoint Association**.
  - Associate subnets with your sites (see “Associating Endpoints With Sites”).
- If you fail to do this, the data collected for these endpoints will have their sites set to “Unassigned.”
- Step 6** Configure your routers for Mediatrace and WSMA (see “Using Mediatrace”).
- 

### Related Topics

- [Adding Devices to Prime Infrastructure](#)
- [Enabling NAM Data Collection](#)
- [Working With Maps](#)
- [Enabling Data Deduplication](#)
- [Associating Endpoints With Sites](#)
- [Controlling Data Collection Jobs](#)
- [Associating Endpoints with a Location](#)
- [Using Mediatrace](#)

## 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.

- 
- Step 1** Create a site structure for your organization and assign your principal routers to the appropriate sites:
- Choose **Maps > Site Maps**.
  - Add one or more campuses, buildings, and floors (for details, see “Working With Maps”).
- Step 2** Associate your sites with authorized data sources:
- Choose **Services > Application Visibility & Control > Data Deduplication**.
  - Click **Enable Data Deduplication**, then click **Apply**. You can then assign authoritative sources for ART, Traffic Analysis and Voice/Video data (see “Enabling Data Deduplication”).
- Step 3** Associate your sites with endpoint subnets:
- Choose **Services > Application Visibility & Control > Endpoint Association**.
  - Associate subnets with your sites (see “Associating Endpoints With Sites”).
- 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 Cisco Medianet Performance Monitor (see “Configuring Mediatrace on Routers and Switches”).
- Step 5** Configure your routers for Mediatrace and WSMA (see “Using Mediatrace”).
- 

### Related Topics

- [Working With Maps](#)
- [Enabling Data Deduplication](#)
- [Associating Endpoints With Sites](#)
- [Configuring Mediatrace on Routers and Switches](#)
- [Using Mediatrace](#)

# 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 that you want to include in your results whenever you are tracing service paths.

See “Enabling NetFlow Data Collection” in Related Topics 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](#)
- [Configuring Prime Infrastructure to Use Routers and Switches as Data Sources](#)

To configure the Mediatrace-Responder-Configuration template, follow these steps:

- 
- Step 1** Choose **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Mediatrace-Responder-Configuration**.
- Step 2** Enter the required information for the template (see the field reference for the template, in Related Topics).
- Step 3** Click **Save as New Template** and give the new template a name and description. Click **Save**.
- Step 4** Click **Deploy** to deploy the new template (see “Deploying Templates”).
- 

## Related Topics

- [Enabling NetFlow Data Collection](#)
- [Field Reference: Mediatrace-Responder-Configuration](#)
- [Deploying Templates](#)



# 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 you did when following the instructions in “Configuring Mediatrace on Routers and Switches” (see Related Topics).

- 
- Step 1** Choose **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > HTTP-HTTPS Server and WSMA Configuration-IOS**.
- Step 2** Enter the required information for the template (see the field reference for the template, in Related Topics).
- Be sure to enable the HTTP protocol. WSMA over HTTPS is *not supported* in the current version of Prime Infrastructure.
- Step 3** Click **Save as New Template** and give the new template a name and description. Click **Save**.
- Step 4** Click **Deploy** to deploy the new template (see “Deploying Templates”).
- When adding a device to Prime Infrastructure, you must provide the HTTP user and password for the device.
- 

## Related Topics

- [Configuring Mediatrace on Routers and Switches](#)
- [Field Reference: HTTP-HTTPS Server and WSMA Configuration-IOS](#)
- [Deploying Templates](#)
- [Adding Devices to Prime Infrastructure](#)





## Planning Network Capacity Changes

---

Cisco Prime Infrastructure with 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 the features described in this chapter, your Prime Infrastructure implementation must include Assurance licenses. These features are 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. Choose **Monitor > Monitoring Policies** and create an Interface Health template.
  - b. Choose **Inventory > Group Management > Port Groups**, select the interfaces and click **Add to Group**, then select **WAN Interfaces** as the group.
- Enable SNMP polling.

- 
- Step 1** Choose **Dashboard > Overview > General**.
- Step 2** To view the usage statistics for the WAN interfaces on the routers connecting remote branches to the WAN, choose **Network Interface**
- Step 3** If it is not already there, add the **Top N Interface Utilization** dashlet. For each interface, this dashlet shows the Device Name and IP of the device hosting the WAN interface, the interface name and speed, and Transmit/Receive maximum, average and last-pollled utilization.
- Step 4** To see the utilization statistics for the past month, click the **Clock** icon next to the **Top N Interface Utilization** dashlet title to change the **Time Frame** on the **Filters** line to **Past 4 Weeks**.

- Step 5** In the **Top N Interface Utilization** dashlet, find the WAN interface for the branch to which you are adding users.
- Step 6** In the **Interface** column, click the interface's name to display the **Dashboard > Performance > Interface** page for that interface. The page shows the following dashlets for this single interface:
- Interface Details
  - Interface Tx and Rx Utilization
  - Top N Applications
  - Top N Clients
  - Number of Clients Over Time
  - DSCP Classification
  - QoS Class Map Statistics
  - oS Class Map Statistics Trend
  - Top Application Traffic Over Time
- Step 7** Concentrate on the **Top Application Traffic Over Time** dashlet on this page. This dashlet gives a color-coded map of the top ten applications with the heaviest traffic over this interface.
- Step 8** To get a better idea of the longer-term performance trend, click the **Clock** icon next to the **Top Application Traffic Over Time** 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 9** For a quick report of the same data as the interface page, choose **Reports > Report Launch Pad**. Then choose **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 15-1** 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 |         |        |         |



# Internal SNMP Trap Generation

---

**Revised: November 11, 2015,**

When properly configured, Prime Infrastructure will send SNMP traps to notification receivers, to notify them on the following events, occurring within the Prime Infrastructure system itself:

- Any crash or failure of an internal software process on the Prime Infrastructure server.
- High Availability (HA) state changes, including Registration, Failover, and Failback.
- High CPU, memory or disk utilization.
- CPU, disk, fan, or Power Supply Unit (PSU) failures.
- Backup failure, certification expiry and licenses violations.

This appendix and the following related topics provide reference information on these internal SNMP traps and how to use them to manage Prime Infrastructure.

## Related Topics

- [About Internal Trap Generation](#)
- [Prime Infrastructure SNMP Trap Types](#)
- [Ensuring Trap-Related Background Tasks are Running](#)
- [Generic SNMP Trap Format](#)
- [Prime Infrastructure SNMP Trap Reference](#)
- [Working With Prime Infrastructure Traps](#)

## About Internal Trap Generation

You can edit the severity associated with each of these internal SNMP traps. You can also change the threshold limits on CPU, memory and disk utilization traps (these SNMP traps are sent when the system hardware exceeds the configured thresholds).

For other events (such as CPU, disk, fan, and PSU failures, or HA state changes), an SNMP trap is sent as soon as the failure or HA state-change is detected.

SNMP traps are generated based on customized threshold and severities for the following:

- Server Process Failures
- High Availability Operations
- CPU Utilization

- Memory Utilization
- Disk Utilization
- Disk Failure
- Fan Failure
- PSU Failure
- Backup Failure
- Certificate Expiry

Prime Infrastructure does not send SNMPv2 Inform or SNMPv3 notifications.

## Prime Infrastructure SNMP Trap Types

The following table lists the SNMP traps that Prime Infrastructure generates for its own functions. The listing is by trap type. The table describes the circumstances under which each trap is generated as well as suggested operational responses (where applicable).

**Table A-1** Prime Infrastructure SNMP Trap Types

| Trap Type                 | Trap                 | Description                                                                                                                                                                                                                                                                                                               |
|---------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appliance Process Failure | FTP, MATLAB, TFTP    | Whenever the FTP, MATLAB, or TFTP process on Prime Infrastructure server fails, the server will generate a failure trap and the server's instance of Health Monitor will try to restart the process automatically. If Health Monitor cannot restart it after 3 tries, the HA server will send another failure trap.       |
| Appliance Process Failure | NMS                  | Whenever the NMS process on a server starts or fails, the Prime Infrastructure server's Health Monitor thread will generate a corresponding trap.<br><br>To stop or restart the process, connect to the server via CLI and log in as admin. Then execute the <i>nms stop</i> or <i>nms start</i> command, as appropriate. |
| HA Operations             | Registration Trigger | Prime Infrastructure generates this trap whenever the primary server initiates HA registration (whether registration fails or succeeds). Once HA registration is triggered, the primary server generates the trap, indicating the start of the operation.                                                                 |
| HA Operations             | Registration Success | When HA registration is successful, the primary server generates this trap, indicating success.                                                                                                                                                                                                                           |
| HA Operations             | Registration Failure | When HA registration fails for any reason, the primary or secondary server on which the failure occurred, generates a trap indicating the failure. The trap contains details about the failure. For assistance, contact the Cisco Technical Assistance Center (TAC).                                                      |

Table A-1 Prime Infrastructure SNMP Trap Types (continued)

| Trap Type      | Trap               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HA Operations  | Failover Trigger   | <p>This trap is generated whenever the Prime Infrastructure primary server fails and, as part of a failover, the secondary server tries to become active (whether failover fails or succeeds, and whether the secondary server comes up or fails to do so). If the HA configuration (set during registration) has a Manual failover type, users must trigger the failover. Otherwise, the Health Monitor will trigger failover to the secondary server automatically.</p> <p>One trap will be generated to indicate that the failover was triggered. Because the trap is sent before the failover completes, it will not be logged on the secondary server.</p>                                                                                       |
| HA Operations  | Failover Success   | When the triggered failover operation is successful, the secondary server generates a trap indicating success. Users can view the trap in the secondary server's alarm browser.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| HA Operations  | Failover Failure   | When the triggered failover operation fails, a trap will be generated indicating the failure. Users can view the trap in the hm-#-#.log (see <a href="#">Troubleshooting Prime Infrastructure SNMP Traps</a> ). The trap contains details about the failure. For assistance, contact Cisco TAC. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.                                                                                                                                                                                                                                                                                                                                                       |
| HA Operations  | Failback Trigger   | This trap is generated whenever a failback to the primary server is triggered on the secondary server (whether or not the failback is successful). Once the primary server is restored, a user must trigger a failback from the secondary server to the primary server using the <b>Failback</b> button on the secondary server Health Monitor web page (there is no automatic Failback option). Once triggered, the secondary server generates the trap indicating the start of the operation.                                                                                                                                                                                                                                                       |
| HA Operations  | Failback Success   | When the triggered failback operation is successful, the secondary server generates a trap indicating success. Failback success sets the primary server to the ‘Active’ state and the secondary server to the ‘Sync’ state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| HA Operations  | Failback Failure   | <p>When the triggered failback operation fails, a trap will be generated indicating this failure. Since the failure can occur on either server, the server on which it occurred will generate the trap. Users can view the trap in the hm-#-#.log and on the northbound management server.</p> <p>A failback failure triggers an automatic rollback, in which the secondary server tries to return to its previous ‘Active’ state. Failure of this operation will cause the secondary server to generate an additional trap indicating rollback failure. The failure traps contain details about the failures. For assistance, contact Cisco TAC. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.</p> |
| Hardware Traps | CPU Utilization    | Traps will be sent only when the usage exceeds the preset threshold value for CPU utilization. To view these traps, check the jobs and active sessions for the server that generated the trap.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Hardware Traps | Disk Utilization   | Traps will be sent only when the disk usage exceeds the set threshold limit for Disk utilization. To respond, try to free up disk space under the /opt and /localdisk partitions. Do not delete folders under /opt/CSCOlumos without guidance from Cisco TAC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Hardware Traps | Memory Utilization | Traps will be sent to the SNMP trap receiver, only when memory usage exceeds the set threshold limit for memory utilization.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table A-1 Prime Infrastructure SNMP Trap Types (continued)

| Trap Type       | Trap               | Description                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware Traps  | Disk Failure       | Traps will be sent to the SNMP trap receiver when disk failure is detected. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.                                                                                                                                           |
| Hardware Traps  | Fan Failure        | Traps will be sent to the SNMP trap receiver when fan failure is detected. The bad or missing fan will be identified in the trap or alarm message. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.                                                                    |
| Hardware Traps  | PSU Failure        | Traps will be sent to the SNMP trap receiver when PSU failure is detected. The problematic power supply will be identified in the trap or alarm message. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.                                                              |
| Threshold Traps | Backup Failure     | Traps will be sent to the SNMP trap receiver when failure of the daily background task of Prime Infrastructure server backup is detected. The background task runs everyday and takes a backup of the server at the scheduled time. If the backup fails due to insufficient disk space, the event will be processed. If the backup is taken successfully, the alarm will be cleared. |
| Threshold Traps | Backup Threshold   | Informs users when Prime Infrastructure scheduled daily backup has not been taken for a threshold number of days. The default threshold is seven days. If no backup has been taken for seven days, users are notified by this event.                                                                                                                                                 |
| Threshold Traps | Certificate Expiry | Traps will be sent to the SNMP trap receiver when the certificate is about to expire. A critical trap is sent when the certificate is set to expire in 15 days and a major trap is sent when the certificate expiry is in 60 days.                                                                                                                                                   |
| System Traps    | Lifecycle          | Lifecycle license is used to manage devices. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.                                                                                                                                                      |
| System Traps    | Data Center        | Data Center license is used to manage Data Center devices. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.                                                                                                                                        |
| System Traps    | Assurance          | Assurance License is used to display the devices that pump NetFlow to Prime Infrastructure. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.                                                                                                       |
| System Traps    | Collector          | Collector License is used to display the volume of NetFlow pumped to Prime Infrastructure. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.                                                                                                        |
| System Traps    | Lifecycle License  | Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License.                                                                                                            |



**Table A-1** Prime Infrastructure SNMP Trap Types (continued)

| Trap Type    | Trap                | Description                                                                                                                                                                                                                                                               |
|--------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Traps | Data Center License | Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License. |
| System Traps | Assurance License   | Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License. |
| System Traps | Collector License   | Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License. |

## Ensuring Trap-Related Background Tasks are Running

The following table lists Prime Infrastructure background tasks that must be running in order to ensure that certain kinds of internal trap information are received. If you are not receiving these types of traps, select **Administration > Settings > Background Tasks** and then click on the appropriate background task link to ensure the task is enabled and running on the correct schedule.

**Table A-2** Trap-Related Background Tasks

| Trap Type       | Trap                             | Background Task Link               |
|-----------------|----------------------------------|------------------------------------|
| Hardware Traps  | All Hardware traps               | Appliance Status                   |
| Threshold Traps | Backup Failure, Backup Threshold | Prime Infrastructure server backup |
| Threshold Traps | Certificate Expiry               | Guest Account Sync                 |
| System Traps    | All System Traps                 | License Status                     |

# Generic SNMP Trap Format

The following shows the syntax of SNMP trap notifications for Prime Infrastructure:

**Component:** Component Name, **Server:** Primary, Secondary or Standalone, **Type:** Process, Sync, Activity, etc., **Service:** Service Name, **When:** Phase in the Prime Infrastructure Lifecycle, **State:** HA and HM state of the server, **Result:** Warning, Failure, Success, Information, Exception, **MSG:** Free-form text of the message for a given SNMP Trap

Table A-3 describes possible values for each of the generic trap format attributes.

**Table A-3** Values for Generic SNMP Trap Format Attributes

| Attribute | Value                                                                                                                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Component | Health Monitor or High Availability                                                                                                                                                                         |
| Server    | From which server (Primary, Secondary or Standalone) was this trap sent?                                                                                                                                    |
| Type      | Which type of action (Process, Sync, Activity, etc.) resulted in this trap?                                                                                                                                 |
| Service   | Which Prime Infrastructure service reported this issue? The possible values include Registration, Failover, Failback, NMS, NCS, Health Monitor, All, Prime Infrastructure, Database, Disk Space, and so on. |
| When      | At what point in the Prime Infrastructure server's life cycle (Startup, Shutdown, etc.) did this happen?                                                                                                    |
| State     | What is the server state (Standalone, Failover, Failback, Registration, etc.)?                                                                                                                              |
| Result    | For which condition is this SNMP trap being reported?                                                                                                                                                       |
| MSG       | Freeform text providing more details specific to each SNMP trap.                                                                                                                                            |

# Prime Infrastructure SNMP Trap Reference

The tables below provide details for each class of SNMP trap notification generated in Prime Infrastructure. The mapped OID for the WCS northbound notification MIB is 1.3.6.1.4.1.9.9.712.1.1.2.1.12. This OID is referenced by Prime Infrastructure's software- and hardware-related traps. The trap OID for the northbound MIB will always be 1.3.6.1.4.1.9.9.712.0.1. For details, consult the listing for [CISCO-WIRELESS-NOTIFICATION-MIB](#).

**Table A-4**      **Appliance Process Failure**

|                                          |                                                                                                                                                                                                                        |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                           | Informs users that a specific Prime Infrastructure server service is down and that the Health Monitor is attempting to restart it.                                                                                     |
| <b>When Sent</b>                         | The trap is sent when Health Monitor tries to restart the process.                                                                                                                                                     |
| <b>OID</b>                               | 1.3.6.1.4.1.9.9.712.1.1.2.1.12                                                                                                                                                                                         |
| <b>Example</b>                           | Component: Health Monitor, Server: Primary, Type: Process, Service: NCS, When: Startup, State: Stand Alone, Result: Warning, MSG: FTP service is down and an attempt will be made to automatically restart the service |
| <b>MSG Content</b>                       | PI <i>servername</i> : serviceName service is down; an attempt will be made to automatically restart the service.                                                                                                      |
| <b>Value Type, Range and Constraints</b> | The <i>servername</i> parameter in the MSG attribute will take the value of the Prime Infrastructure server's host name. This parameter can take one of the following values: NMS Server, FTP, TFTP or MATLAB.         |

**Table A-5**      **Failback**

|                  |                                                                                                                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>   | Informs users that a failback from the secondary server to the primary server has been initiated.                                                                                                                              |
| <b>When Sent</b> | This trap is sent when a failback is initiated from the secondary server to the primary server, irrespective of whether the failback operation fails or succeeds.                                                              |
| <b>OID</b>       | 1.3.6.1.4.1.9.9.712.1.1.2.1.12                                                                                                                                                                                                 |
| <b>Example</b>   | Component: High Availability, Server: Secondary, Type: Process, Service: Database, When: Failback, State: Primary Failback, Result: Failure, MSG: Error in Failback: Failed to recover the primary database using Duplicate DB |

**Table A-6**      **Failover**

|                    |                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>     | Informs users when the secondary server comes up.                                                                                                                                                                       |
| <b>When Sent</b>   | When the primary server is down and, as part of failover, the secondary server comes up, traps are generated, irrespective of whether the failover operation fails or succeeds.                                         |
| <b>OID</b>         | 1.3.6.1.4.1.9.9.712.1.1.2.1.12                                                                                                                                                                                          |
| <b>Example</b>     | Component: High Availability, Server: Secondary, Type: Process, Service: Failover, When: Failover, State: Secondary Synching, Result: Success, MSG: Completed failover from primaryAddressInfo to secondaryAddressInfo. |
| <b>MSG Content</b> | The primaryAddressInfo and secondaryAddressInfo in the MSG attribute will take the IP address or host name of the servers.                                                                                              |

Table A-7 CPU Utilization

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                           | Informs users that CPU utilization has crossed the set threshold limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>When Sent</b>                         | After the CPU utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.                                                                                                                                                                                                                                                                                                                                                               |
| <b>OID</b>                               | .1.3.6.1.4.1.9.9.712.0.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Example</b>                           | CPU Utilization is at 85% and has violated threshold limit of 80%.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Value Type, Range and Constraints</b> | All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Wire Format</b>                       | [OctetString] applicationSpecificAlarmID=Appliance_CPU, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, maybeAutoCleared=false, instanceId=8178170, severity=4, eventType=APPLIANCE_CPU_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=CPU, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: CPU Utilization is at 3% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141 |
| <b>Constraints and Caveats</b>           | Traps are not generated if the issue is resolved before the next polling cycle.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Table A-8 Disk Utilization

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                           | Informs users that disk utilization has crossed the set threshold limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>When Sent</b>                         | After the disk utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>OID</b>                               | .1.3.6.1.4.1.9.9.712.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Examples</b>                          | PI opt disk volume utilization is at 85% and has violated threshold limit of 0%<br>PI opt disk volume is within the recommended disk usage range, less than 80% used<br>PI local disk volume utilization is at 85% and has violated threshold limit of 80%<br>PI local disk volume is within the recommended disk usage range, less than 80% used                                                                                                                                                                                                                                                                                                                       |
| <b>Value Type, Range and Constraints</b> | All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Wire Format</b>                       | [OctetString]<br>applicationSpecificAlarmID=LocaldiskDiskSpace, reportingEntityAddress=10.77.240.246, lastModifiedTimestamp=Sun Mar 23 08:44:06 UTC 2014, alarmCreationTime=2014-03-14 13:29:31.069, eventCount=1, maybeAutoCleared=false, instanceId=483484, severity=1, eventType=NCS_LOW_DISK_SPACE, authEntityId=93093, previousSeverity=MAJOR, category=System(17), transientNameValue={}, source=10.77.240.246, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=PI localdisk volume is within the recommended disk usage range, less than 70% used., isAcknowledged=false, authEntityClass=983576643, displayName=NCS 10.77.240.246 |
| <b>Constraints and Caveats</b>           | Traps are not generated if the issue is resolved before the next polling cycle.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Table A-9**      **Memory Utilization**

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                           | Informs users that memory utilization has crossed the set threshold limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>When Sent</b>                         | After the memory utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>OID</b>                               | .1.3.6.1.4.1.9.9.712.0.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Examples</b>                          | Memory Utilization is at 85% and has violated threshold limit of 80%.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Value Type, Range and Constraints</b> | All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Wire Format</b>                       | [OctetString] applicationSpecificAlarmID=Appliance_MEMORY, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerId=, eventCount=1, maybeAutoCleared=false, instanceId=8178171, severity=4, eventType=APPLIANCE_MEM_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=MEMORY, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: MEMORY Utilization is at 38% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141 |
| <b>Constraints and Caveats</b>           | Traps are not generated if the issue is resolved before the next polling cycle.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table A-10**      **Disk Failure**

|                                |                                                                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | Informs users that a drive is missing or bad.                                                                                                                                                                          |
| <b>When Sent</b>               | Once a disk drive issue is detected, a trap will be generated on the next polling cycle. The system poller job runs every 5 minutes.                                                                                   |
| <b>OID</b>                     | .1.3.6.1.4.1.9.9.712.0.1                                                                                                                                                                                               |
| <b>Example</b>                 | Component: Appliance, Server: Standalone, Type: Hardware, Message: A problem was detected in the RAID device. A rebuild is in progress. Device at enclosure 252 slot ZERO is bad or missing. Drive0 is missing or bad. |
| <b>Constraints and Caveats</b> | Traps are not generated if the issue is resolved before the next polling cycle. If the drive is unplugged at the time of system restart, the trap is generated.                                                        |

**Table A-11**      **Fan Failure**

|                  |                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>   | Informs users when a fan fails.                                                                              |
| <b>When Sent</b> | When a fan fails, a trap is generated on the next polling cycle. The system poller job runs every 5 minutes. |
| <b>OID</b>       | .1.3.6.1.4.1.9.9.712.0.1                                                                                     |

Table A-11 Fan Failure (continued)

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Example</b>                 | Fan is either bad or missing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Wire Format</b>             | [OctetString] applicationSpecificAlarmID=Appliance_Fan1, lastModifiedTimestamp=Sun Apr 13 15:24:11 IST 2014, alarmCreationTime=Sun Apr 13 15:24:11 IST 2014, ownerID=, eventCount=1, maybeAutoCleared=false, instanceId=2875873, severity=4, eventType=APPLIANCE_FAN_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=Fan1, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Fan is either bad or missing, isAcknowledged=false, displayName=NMS: 10.77.240.246 |
| <b>Constraints and Caveats</b> | Traps are not generated if the issue is resolved before the next polling cycle, or the fan is unplugged at the time of system restart.                                                                                                                                                                                                                                                                                                                                                                                                   |

Table A-12 PSU Failure

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | Informs users that a power supply unit is unplugged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>When Sent</b>               | When a power supply is unplugged, a trap is generated on the next polling cycle. The system poller job runs every 5 minutes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>OID</b>                     | .1.3.6.1.4.1.9.9.712.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Example</b>                 | Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Wire Format</b>             | [OctetString] applicationSpecificAlarmID=Appliance_PS1, lastModifiedTimestamp=19 Aug 2015 01:41:26 UTC, alarmCreationTime=19 Aug 2015 01:41:26 UTC, ownerID=, eventCount=1, maybeAutoCleared=false, instanceId=1424089, severity=4, eventType=APPLIANCE_POWER_SUPPLY_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=x.x.x.x, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing, isAcknowledged=false, displayName=NMS:x.x.x.x |
| <b>Constraints and Caveats</b> | If the PSU is unplugged, a Power Supply alarm will be seen in Prime Infrastructure and a trap will be sent. If the PSU is unplugged at the time of system shutdown, and Prime Infrastructure is not up till restart, an alarm will not be generated.                                                                                                                                                                                                                                                                                                                                                                  |

Table A-13 Identify Services Engine down

|                  |                                                                        |
|------------------|------------------------------------------------------------------------|
| <b>Purpose</b>   | Informs users when an ISE is unreachable.                              |
| <b>When Sent</b> | When an ISE is down or unreachable, the trap is generated via polling. |
| <b>Example</b>   | Identity services engine <i>ISEIPAddress</i> is unreachable.           |

Table A-14 License violation

|                  |                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>   | Informs users when the number of devices Prime Infrastructure is actually managing exceeds the number of devices it is licensed to manage.                                                                    |
| <b>When Sent</b> | At 2:10AM, on the day following the completion of the job that added the extra devices to Prime Infrastructure inventory                                                                                      |
| <b>Example</b>   | Number of managed devices <i>N</i> is greater than licensed devices <i>N</i> . Please purchase and install a license that will cover the number of managed devices, or remove unused devices from the system. |

**Table A-15** *Prime Infrastructure does not have enough disk space for backup*

|                  |                                                                                                                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>   | Informs users when Prime Infrastructure does not have sufficient space in the specified directory to perform a backup.                                                                                    |
| <b>When Sent</b> | Whenever Prime Infrastructure runs a server backup job and the backup repository specified (or “defaultrepo”) is 100 percent full. The trap is generated after the job completes.                         |
| <b>Example</b>   | Prime Infrastructure with address <i>localIPAddress</i> does not have sufficient disk space in directory <i>directoryName</i> for backup. Space needed: <i>Needed</i> GB, space available <i>Free</i> GB. |

**Table A-16** *Prime Infrastructure email failure*

|                  |                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>   | Informs users that an attempt to send an email notification has failed.                                                                                                                                              |
| <b>When Sent</b> | This trap is generated by polling when Prime Infrastructure attempts to send an email notification to an invalid user, or email notification is enabled without specifying the email server in Prime Infrastructure. |
| <b>Example</b>   | Prime Infrastructure with address <i>localIPAddress</i> failed to send email. This may be due to possible SMTP misconfiguration or network issues.                                                                   |

**Table A-17** *Northbound OSS server unreachable*

|                  |                                                                                                                                            |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>   | Informs users that a northbound notification server is unreachable.                                                                        |
| <b>When Sent</b> | This trap is generated by polling when a destination northbound notification server is down or unreachable.                                |
| <b>Example</b>   | Northbound notification server <i>OSSIPAddress</i> is unreachable. NCS alarms will not be processed for this server until it is reachable. |

# Working With Prime Infrastructure Traps

The following sections explain how to configure and use Prime Infrastructure trap notifications.

## Related Topics

- [Configuring Notifications](#)
- [Port Used To Send Traps](#)
- [Configuring Email Notifications for SNMP Traps](#)
- [Viewing Events and Alarms for SNMP Traps](#)
- [Filtering Events and Alarms for SNMP Traps](#)
- [Purging Alarms for SNMP Traps](#)
- [Troubleshooting Prime Infrastructure SNMP Traps](#)

## Configuring Notifications

For Prime Infrastructure to send northbound SNMP trap notifications, you must configure the correct settings on both the Prime Infrastructure Event Notification and Notification Receivers pages. Once configured, traps will be generated based on the values associated with the Threshold and Severity for the following SNMP Events:

- Appliance Process Failure
- HA Operations
- CPU, disk and memory utilization
- Disk, fan and PSU Failure
- Backup failure, certification expiry and licenses violations

You can edit the threshold and severity associated with each event, and enable or disable trap generation for the associated event.

- 
- Step 1** Log in to Prime Infrastructure using a user ID with root domain privileges.
- Step 2** Select **Administration > Settings > System Settings > Alarms and Events > System Event configuration**.
- Step 3** For each SNMP event you want to configure:
- a. Click on the row for that event.
  - b. Set the **Event Severity** level to Critical, Major, or Minor, as needed.
  - c. For the CPU, disk, memory utilization, life cycle, data center, assurance, and collector traps: Enter the **Threshold** percentage (from 1-99). These events will send the associated SNMP traps when the utilization exceeds the threshold limit. You cannot set thresholds for events for which the threshold setting is shown as NA. These events send traps whenever the associated failure is detected.
  - d. For backup threshold, certificate expiry, certificate expiry (critical), lifecycle license, data center license, assurance license, and collector license trap: Enter the **Threshold** in days (from x-y, where x is the minimum value and y is the maximum value in days).
  - e. Set the **Event Status** to Enabled or Disabled. If set to Enabled, the corresponding trap will be generated for this event.



**Step 4** When you are finished, click **Save** to save your changes.

---

#### Related Topics

- [Configuring Notification Receivers](#)

## Configuring Notification Receivers

Once you have enabled trap notifications and customized their severities and thresholds, you must configure one or more Notification Receivers to receive the traps.

When you add a Notification Receiver, remember to select the **System** checkbox as one of the Criteria and, set the Severity to the highest severity set under the severity level configured for each trap on the Event Notifications page.

- 
- Step 1** Log in to Prime Infrastructure with a user ID that has administrator privileges.
- Step 2** Select **Administration > Settings > System Settings > Alarms and Events > Notification Receivers**.
- Step 3** From the **Select a command** drop-down list, choose **Add Notification Receiver**, then click **Go**.
- Step 4** Complete at least the following fields:
- IP Address:** Enter the IPv4 or IPv6 address of the server on which the receiver will run.
  - Server Name:** Enter the host name of the server on which the receiver will run.
  - Under **Criteria - Category**, select at least the **System** checkbox.
  - Under **Criteria - Severity**, select the highest **Severity Level** that you set when you configured the trap notifications themselves.  
  
For example: If you selected “Critical” as the **Event Severity** for a PSU failure, select “Critical” as the value in this field.  
  
Alternatively: Select **All** to receive all traps, regardless of severity.
- Step 5** When you are finished, click **Save**.
- 

#### Related Topics

- [Configuring Notifications](#)
- [Port Used To Send Traps](#)
- [Configuring Email Notifications for SNMP Traps](#)
- [Viewing Events and Alarms for SNMP Traps](#)
- [Filtering Events and Alarms for SNMP Traps](#)
- [Purging Alarms for SNMP Traps](#)
- [Troubleshooting Prime Infrastructure SNMP Traps](#)

## Port Used To Send Traps

Prime Infrastructure sends traps to notification receivers on port 162. This port cannot be customized at present. The northbound management system has to register itself through the Notification Receiver web page (see [Configuring Notification Receivers](#)).

## Configuring Email Notifications for SNMP Traps

You can configure Prime Infrastructure to send email notification for alarms and events generated in response to SNMP traps. All of these alarms and events are considered part of the System event category. You can also customize the severity level for which such notifications will be sent.

Note that, for these email notifications to be sent, the Prime Infrastructure administrator must configure at least a primary SMTP email server.

- 
- Step 1** Log in to Prime Infrastructure.
  - Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.
  - Step 3** Click **Email Notification** tab. Prime Infrastructure displays the first Email Notification Settings page.
  - Step 4** In the **Alarm Category** column, click on the **System** category's name. Prime Infrastructure displays a second Email Notification Settings page.
  - Step 5** Under **Send email for the following severity levels**, select all of the severity levels for which you want Prime Infrastructure to send email notifications.
  - Step 6** In **To**, enter the email address to which you want Prime Infrastructure to send email notifications. If you have multiple email addresses, enter them as a comma-separated list.
  - Step 7** Click **Save**. Prime Infrastructure displays the first Email Notification Settings page.
  - Step 8** In the **Enable** column, make sure System is selected, then click **Save**.
- 

### Related Topics

- [Configuring Email Server Settings](#)

## Configuring Email Server Settings

To enable Prime Infrastructure to send email notifications, the system administrator must configure a primary SMTP email server (and, preferably, a secondary email server).

- 
- Step 1** Log in to Prime Infrastructure using a user ID with administrator privileges.
  - Step 2** Select **Administration > Settings > System Settings > Mail and Notification > Mail Server Configuration**.
  - Step 3** Under **Primary SMTP Server**, complete the **Hostname/IP**, **User Name**, **Password** and **Confirm Password** fields as appropriate for the email server you want Prime Infrastructure to use. Enter the IP address of the physical server. You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.
  - Step 4** (Optional) Complete the same fields under **Secondary SMTP Server**.
  - Step 5** Under **Sender and Receivers**, enter a legitimate email address for the Prime Infrastructure server.

**Step 6** When you are finished, click **Save**.

---

#### Related Topics

- [Viewing Events and Alarms for SNMP Traps](#)
- [Filtering Events and Alarms for SNMP Traps](#)
- [Purging Alarms for SNMP Traps](#)
- [Troubleshooting Prime Infrastructure SNMP Traps](#)
- [Configuring Notifications](#)
- [Port Used To Send Traps](#)
- [Configuring Email Notifications for SNMP Traps](#)

## Viewing Events and Alarms for SNMP Traps

Events and Alarms for all of Prime Infrastructure's internal SNMP traps fall under the System category. You can view them in the Prime Infrastructure Alarms and Events dashboard.

---

**Step 1** Log in to Prime Infrastructure.

**Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.

---

## Filtering Events and Alarms for SNMP Traps

You can use the Prime Infrastructure Filter feature to narrow the display of alarms to just those in the System category, or use a combination of criteria and operators to focus the list on very specific alarms. The following sections explain how to do this.

#### Related Topics

- [Filtering for SNMP Traps Using Quick Filters](#)
- [Filtering for SNMP Traps Using Advanced Filters](#)

## Filtering for SNMP Traps Using Quick Filters

Prime Infrastructure's Quick Filters allow you to quickly focus on the data inside a table by applying a filter for a specific table column or columns.

---

**Step 1** Log in to Prime Infrastructure.

**Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.

**Step 3** From the **Show** drop-down list, select **Quick Filter**. Prime Infrastructure displays a table header listing fields on which you can perform a quick filter, including **Severity**, **Message**, and **Category**.

**Step 4** In the **Category** field, enter **System**. Prime Infrastructure displays only System alarms.

**Step 5** To clear the Quick Filter, click the funnel icon shown next to the **Show** box.

---

## Filtering for SNMP Traps Using Advanced Filters

Prime Infrastructure's Advanced Filter allows you to narrow down the data in a table by applying a filter combining multiple types of data with logical operators (such as “Does not contain”, “Does not equal”, “Ends with”, and so on). For example, you can choose to filter the table of alarms based on the Category, then further reduce the data by filtering on Severity (as shown in the steps below). You can also save an Advanced Filter for later re-use.

---

- Step 1** Log in to Prime Infrastructure.
- Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.
- Step 3** From the **Show** drop-down list, select **Advanced Filter**. Prime Infrastructure displays a table header showing criteria for the first rule in the filter.
- Step 4** Complete the first rule as follows:
- In the first field, select **Category** from the drop-down list.
  - In the second field, select **Contains** from the drop-down list.
  - In the third rule field, enter **System**.
  - Click **Go**. Prime Infrastructure displays only System alarms.
- Step 5** Click the plus sign icon to add another rule, then complete the second rule as follows:
- In the first field, select **Severity** from the drop down list
  - In the second field, select **equals (=)** from the drop-down list.
  - In the third rule field, select **Major** from the drop-down list.
  - Click **Go**. Prime Infrastructure displays only System alarms with Major Severity.  
Repeat this step as needed.
- Step 6** To save the Advanced filter, click the **Save** icon and supply a name for the filter.
- Step 7** To clear the Advanced Filter, click **Clear Filter**.
- 

### Related Topics

- [Purging Alarms for SNMP Traps](#)
- [Troubleshooting Prime Infrastructure SNMP Traps](#)
- [Configuring Notifications](#)
- [Port Used To Send Traps](#)
- [Configuring Email Notifications for SNMP Traps](#)
- [Viewing Events and Alarms for SNMP Traps](#)
- [Filtering Events and Alarms for SNMP Traps](#)

## Purging Alarms for SNMP Traps

You can remove an alarm from the list of alarms by changing its status to Acknowledged or Cleared. No e-mails will be generated for these alarms.

- 
- Step 1** Log in to Prime Infrastructure.
  - Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.
  - Step 3** Select an alarm, then choose **Change Status > Acknowledge** or **Change Status > Clear**.
- 

## Troubleshooting Prime Infrastructure SNMP Traps

If you are having trouble with Prime Infrastructure's internal traps and related notifications, check the following:

- 
- Step 1** Ping the notification receiver from the Prime Infrastructure server, to ensure that there is connectivity between Prime Infrastructure and your management application.
  - Step 2** Check if any firewall ACL settings are blocking port 162, and open communications on that port if needed.
  - Step 3** Log in to Prime Infrastructure with a user ID that has administrator privileges. Select **Administration > Settings > Logging** and download the log files. Then compare the activity recorded in these log files with the activity you are seeing in your management application:
    - `ncs_nb.log`: This is the log of all the northbound SNMP trap messages Prime Infrastructure has sent. Check for messages you have not received.
    - `ncs-#-#.log`: This is the log of other recent Prime Infrastructure activity. Check for hardware trap messages you have not received.
    - `hm-#-#.log`: This is the complete log of Health Monitor activity. Check for recent messages about High Availability state-changes and application-process failures that you have not received.

The messages you see in these logs should match the activity you see in your management application. If you find major differences, open a support case with Cisco Technical Assistance Center (TAC) and attach the suspected log files with your case.

---

### Related Topics

- [Prime Infrastructure SNMP Trap Types](#)
- [Prime Infrastructure SNMP Trap Reference](#)
- [Working With Prime Infrastructure Traps](#)





# Best Practices: Server Security Hardening

---

**Revised: November 30, 2015**

This appendix provides background information and advice on the best ways to enhance the security of your Cisco Prime Infrastructure servers.

## Hardening Server Security

The following sections explain how to enhance server security by eliminating or controlling individual points of security exposure.

### Related Topics

- [Disabling Insecure Services](#)
- [Disabling Root Access](#)
- [Using SNMPv3 Instead of SNMPv2](#)
- [Authenticating With External AAA](#)
- [Enabling NTP Update Authentication](#)
- [Enabling Certificate-Based OCSP Authentication](#)
- [Importing Client Certificates Into Web Browsers](#)
- [Enabling OCSP Settings on the Prime Infrastructure Server](#)
- [Setting Up Local Password Policies](#)
- [Checking On Server Security Status](#)

## Disabling Insecure Services

You should disable non-secure services if you are not using them. For example: TFTP and FTP are not secure protocols. These services are typically used to transfer firmware or software images to and from network devices and Prime Infrastructure. They are also used for transferring system backups to external storage. We recommend that you use secure protocols (such as SFTP or SCP) for such services.

To disable FTP and TFTP services:

- 
- Step 1** Log in to Prime Infrastructure with a user ID with administrator privileges.
  - Step 2** Select **Administration > Settings > System Settings > General > Server**.
  - Step 3** Select the **Disable** buttons for **FTP** and **TFTP**.
- 

## Disabling Root Access

Administrative users can enable root shell access to the underlying operating system for trouble shooting purposes. This access is intended for Cisco Support teams to debug product-related operational issues. We recommend that you keep this access disabled, and enable it only when required. To disable root access, run the command **root\_disable** from the command line (see [Connecting Via CLI](#)).

During installation, Prime Infrastructure also creates a web root user account, prompting the installer for the password to be used for this account. The web root account is needed to enable first-time login to the Prime Infrastructure server and its web user interface. We recommend that you never use this account for normal operations. Instead, use it to create user IDs with appropriate privileges for day-to-day operations and network management, and administrative user IDs for managing Prime Infrastructure itself. Once these user accounts are created, disable the default “web root” account created at install time, and create user accounts using your administrative user IDs thereafter.

To disable the root accounts:

- 
- Step 1** Open a CLI session with the Prime Infrastructure server (see [Connecting Via CLI](#)). Do not enter “configure terminal” mode.
  - Step 2** Disable the web root account by entering the following command:  

```
PIServer/admin# ncs webroot disable
```

Prime Infrastructure disables the web root account.
  - Step 3** Disable the root shell account by entering the following command at the prompt:  

```
PIServer/admin# root_disable
```

Prime Infrastructure will prompt you for the root shell account password. Enter it to complete disabling of the root shell account.
-



## Using SNMPv3 Instead of SNMPv2

SNMPv3 is a higher-security protocol than SNMPv2. You can enhance the security of communications between your network devices and the Prime Infrastructure server by configuring the managed devices so that management takes place using SNMPv3 instead of SNMPv2.

You can choose to enable SNMPv3 when adding new devices, when importing devices in bulk, or as part of device discovery. See Related Topics for instruction on how to perform each task.

### Related Topics

- [Using SNMv3 When Adding Devices](#)
- [Using SNMv3 When Importing Devices](#)
- [Using SNMv3 When Running Discovery](#)

## Using SNMv3 When Adding Devices

To specify SNMPv3 when adding a new device:

- 
- Step 1** Select **Inventory > Device Management > Network Devices**
  - Step 2** Choose **Add Device**.
  - Step 3** In the **SNMP Parameters** area, in **Version**, select **v3**.
  - Step 4** Complete the other fields as appropriate, then click **Add**.
- 

### Related Topics

- [Using SNMv3 When Importing Devices](#)
- [Using SNMv3 When Running Discovery](#)
- [Using SNMPv3 Instead of SNMPv2](#)

## Using SNMPv3 When Importing Devices

To specify use of SNMPv3 when importing devices in bulk:

- 
- Step 1** Select **Inventory > Device Management > Network Devices**.
  - Step 2** Choose **Bulk Import**. The Bulk Import page appears.
  - Step 3** Download the device add sample template from the “here” link on the Bulk Import page.
  - Step 4** Edit the template file using any CSV-compatible application. For each row representing a device in the CSV import file:
    - a. In the **snmp version** column, enter **3**.
    - b. Enter appropriate values in the **snmpv3\_user\_name**, **snmpv3\_auth\_type**, **snmpv3\_auth\_password**, **snmpv3\_privacy\_type**, and **snmpv3\_privacy\_password** columns.
    - c. Complete other columns as appropriate for your devices.
  - Step 5** Select **Inventory > Device Management > Network Devices**, then click **Bulk Import** and import your modified CSV file.
- 

### Related Topics

- [Using SNMPv3 When Adding Devices](#)
- [Using SNMPv3 When Running Discovery](#)
- [Using SNMPv3 Instead of SNMPv2](#)

## Using SNMPv3 When Running Discovery

To specify SNMPv3 as part of device discovery:

- 
- Step 1** Select **Inventory > Device Management > Discovery**. The Discovery Jobs page appears.
  - Step 2** Click the **Discovery Settings** link in the upper right corner of the page. The Discovery Settings page appears.
  - Step 3** Choose **New** to add new SNMP v3 credentials.
  - Step 4** Complete the fields as needed.
  - Step 5** Click **Save** to save the SNMPv3 settings and use them thereafter.
- 

### Related Topics

- [Using SNMPv3 When Adding Devices](#)
- [Using SNMPv3 When Importing Devices](#)
- [Using SNMPv3 Instead of SNMPv2](#)

## Authenticating With External AAA

User accounts and password are managed more securely when they are managed centrally, by a dedicated, remote authentication server running a secure authentication protocol such as RADIUS or TACACS+.

You can configure Prime Infrastructure to authenticate users using external AAA servers. You will need to access the **Administration > Users > Users, Roles & AAA** page to set up external authentication via the Prime Infrastructure graphic user interface (GUI). You can also set up external authentication via the command line interface (CLI). See Related Topics for instructions on how to set up AAA using each method.

### Related Topics

- [Setting Up External AAA Via GUI](#)
- [Setting Up External AAA Via CLI](#)

## Setting Up External AAA Via GUI

To set up remote user authentication via the GUI:

- 
- Step 1** Log in to Prime Infrastructure with a user ID that has administrator privileges.
  - Step 2** Select **Administration > Users > Users, Roles & AAA > TACACS+** or **Administration > Users > Users, Roles & AAA > RADIUS**.
  - Step 3** Enter the TACACS+ or RADIUS server IP address and shared secret in the appropriate fields.
  - Step 4** Select **Administration > Users > Users, Roles & AAA > AAA Mode Settings**.
  - Step 5** Set the AAA mode as appropriate.
- 

### Related Topics

- [Authenticating With External AAA](#)
- [Setting Up External AAA Via CLI](#)

## Setting Up External AAA Via CLI

To set up remote user authentication via the CLI:

---

**Step 1** Log in to Prime Infrastructure using the command line, as explained in [Connecting Via CLI](#). Be sure to enter “configure terminal” mode.

**Step 2** At the prompt, enter the following command to setup an external TACACS+ server:

```
PIServer/admin/terminal# aaa authentication tacacs+ server tacacs-ip key plain shared-secret
```

Where:

- *tacacs-ip* is the IP address of an active TACACS+ server.
- *shared-secret* is the plain-text shared secret for the active TACACS+ server.

**Step 3** At the prompt, enter the following command to create a user with administrative authority, who will be authenticated by the above AAA server:

```
PIServer/admin/terminal# username username password remote role admin email emailID
```

Where:

- *username* is the name of the user ID.
  - *password* is the plain-text password for the user.
  - *emailID* is the email address of the user (optional).
- 

### Related Topics

- [Authenticating With External AAA](#)
- [Setting Up External AAA Via GUI](#)

## Enabling NTP Update Authentication

Network Time Protocol (NTP) version 4, which authenticates server date and time updates, is an important way to harden server security. Note that you can configure a maximum of three NTP servers with Prime Infrastructure.

To set up authenticated NTP updates:

---

**Step 1** Log in to Prime Infrastructure using the command line, as explained in [Connecting Via CLI](#). Be sure to enter “configure terminal” mode.

**Step 2** At the prompt, enter the following command to setup an external NTPv4 server:

```
PIServer/admin/terminal# ntp server serverIP userID plain password
```

Where:

- *serverIP* is the IP address of the authenticating NTPv4 server you want to use.
- *userID* is the md5 key id of the NTPv4 server.
- *password* is the corresponding plain-text md5 password for the NTPv4 server.

For example: `ntp server 10.81.254.131 20 plain MyPassword`

**Step 3** To ensure that NTP authentication is working correctly, test it by executing the following commands:

- To check the NTP update details: **sh run**
  - To check NTP sync details: **sh ntp**
-

## Enabling Certificate-Based OCSP Authentication

You can further enhance the security of Prime Infrastructure's interaction with its web clients by setting up certificate-based client authentication using the Online Certificate Status Protocol (OCSP).

With this form of authentication, Prime Infrastructure validates the web client's certificate and its revocation status before permitting the user to access the login page. Checking the revocation status ensures that the issuing Certificate Authority (CA) has not already revoked the certificate.

Prime Infrastructure uses OCSP to check the certificate's revocation status. OCSP is a real-time certificate status check mechanism, which is faster and more reliable than other methods. New, internet standard protocol, not proprietary, most browsers support it, widely accepted, and DOD-compliant.

### Before You Begin

You will want to ensure that:

- Prime Infrastructure is configured to authorize user access via an external AAA server using a secure protocol, such as RADIUS or TACACS+. The US Department of Defense and other security agencies recommend doing so as a way to ensure secure authentication. See “Authenticating With External AAA” in Related Topics for more information. This permits two-factor authentication: certificate authentication takes place separately from user ID and password authentication.
- You have set up a repository to store certificates. There are very few restrictions on how you do this. The repository can be located on storage media local to the Prime Infrastructure server or on a remote host. If it is remote, it can be located on a dedicated server you set up or on a shared certificate server used throughout your organization. Be sure that any remote repository you use is accessible from the Prime Infrastructure server via a supported protocol (NFS, FTP, or SFTP).
- You know the name of the certificate repository, the name of the folder within the repository where certificate files are stored, and the name and password of a user with read/write access to that repository and folder.
- The certificate files exist in the certificate repository.
- Your organization's DNS servers are able to resolve the URLs of the OCSP responders maintained by the CA who issued your certificates. These OCSP responder URLs will be embedded in the certificate files (such as “OCSP.Responder.Service”). IP addresses are not embedded in the certificate files, so these URLs must be resolvable by DNS.

### After You Finish

Once you have enabled this form of authentication, every client web browser used to access Prime Infrastructure must import the client certificates. See “Importing OCSP-Verified Certificates Into Web Clients” in Related Topics for more information.

---

**Step 1** Log in to Prime Infrastructure using the command line, as explained in “Connecting Via CLI” in Related Topics. Be sure to enter “configure terminal” mode.

**Step 2** Run the following commands in the order given to create an alias for the certificate repository and configure Prime Infrastructure to access that alias:

```
PIServer/admin(config)# repository CertRepoName
PIServer/admin(config-repository) # url proto://CAPath
PIServer/admin(config-repository)# user username password type pword
```

Where:

- *CertRepoName* is the name of the certificate repository (for example: **MyCertRepo**)

- *proto* is the name of the protocol used to access the repository (that is: **NFS**, **FTP**, or **SFTP**).
- *CAPath* is the complete URL and path to the location where the certificates are stored..
- *username* is the name of the user who will be accessing the certificates in the repository. This must be an existing user already given permission to access *CAPath*.
- *type* is the password encryption type (either **plain** for plain text, or **hash** for an encrypted password).
- *pwd* is the corresponding password for the user specified in *username* (in plain text or encrypted form, depending on the value of *type*).

**Step 3** Run the following commands to verify that the certificates are available at the path on the certificate repository:

```
PIServer/admin(config-repository)# exit
```

```
PIServer/admin(config)# exit
```

```
PIServer/admin# show repository CertRepoName
```

The last command will return a list of the certificates stored in the repository. The certificates you want should be in the list. For example, if you have more than one certificate file, you might see a listing like this:

```
certnew_latest.cer
```

```
certnew_sub_ca1.cer
```

**Step 4** Run the following command to install the certificates into the Prime Infrastructure keystore repository, creating an alias for each file (if you have more than one certificate file, you will need to run this command more than once):

```
PIServer/admin# ncs key importcert CertAlias CertFile repository CertRepoName
```

Where:

- *CertAlias* is the alias you want to assign to the certificate file. The alias must be unique for each file.
- *CertFile* is the file name of the certificate file stored in *CertRepoName*.

For example: To continue using the sample certificate file names given in Step 3, you might execute the following commands:

```
PIServer/admin# ncs key importcert OCSP-CA-CERT certnew_latest.cer repository
MyCertRepo
```

```
PIServer/admin# ncs key importcert OCSP-SUB-CA-CERT certnew_sub_ca1.cer repository
MyCertRepo
```

**Step 5** After installing the certificates, restart the Prime Infrastructure server as explained in “Restarting Prime Infrastructure”.

**Step 6** Once the server is restarted: Log in to Prime Infrastructure via the command line as you did in Step 1 and display the list of certificates installed in the Prime Infrastructure keystore:

```
PIServer/admin# ncs key listcerts
```

The list of installed certificates should contain the certificates you imported in Step 4.

**Step 7** Run the following command to enable client certificate authentication on Prime Infrastructure:

```
PIServer/admin# ncs run client-auth enable
```

**Step 8** After enabling client certificate authentication: Restart the Prime Infrastructure server again, as explained in “Restarting Prime Infrastructure”.

**Related Topics**

- [Authenticating With External AAA](#)
- [Connecting Via CLI](#)
- [Using Remote Backup Repositories](#)
- [Restarting Prime Infrastructure](#)
- [Importing Client Certificates Into Web Browsers](#)

## Importing Client Certificates Into Web Browsers

Users accessing Prime Infrastructure servers with certificate authentication must import client certificates into their browsers in order to authenticate. Although the process is similar across browsers, the actual details vary with the browser. The following procedure assumes that your users are using a Prime Infrastructure compatible version of Firefox.

**Before You Begin**

You must ensure that the user importing the client certificates has:

- Downloaded a copy of the certificate files to a local storage resource on the client machine
- If the certificate file is encrypted: The password with which the certificate files were encrypted.

- 
- Step 1** Launch Firefox and enter the following URL in the location bar: **about:preferences#advanced**. Firefox displays its **Options > Advanced** tab.
- Step 2** Select **Certificates > View Certificates > Your Certificates**, then click **Import...**
- Step 3** Navigate to the downloaded certificate files, select them, then click **OK** or **Open**.
- Step 4** If the certificate files are encrypted: You will be prompted for the password used to encrypt the certificate file. Enter it and click **OK**.
- The certificate is now installed in the browser.
- Step 5** Press **Ctrl+Shift+Del** to clear the browser cache,
- Step 6** Point the browser to the Prime Infrastructure server using certificate authentication.
- You will be prompted to select the certificate with which to respond to the server authentication requested. Select the appropriate certificate and click **OK**.
- 

**Related Topics**

- [Authenticating With External AAA](#)
- [Using Remote Backup Repositories](#)
- [Enabling Certificate-Based OCSP Authentication](#)



## Setting Up SSL Certification

The Secure Sockets Layer (SSL) Certification is used to ensure secure transactions between a web server and the browsers. Installing the certificates allows your web browser to trust the identity and provide secure communications which are authenticated by a certificate signing authority (CSA).

These certificates are used to validate the identity of the server or website and are used to generate the encryption key used in the SSL. This encryption protects the information being passed between the server and the client.

### Related Topics

- [Setting Up SSL Client Certification](#)
- [Setting Up SSL Server Certification](#)

## Setting Up SSL Client Certification

To set up the SSL *client* certificate authentication, follow the steps below. These steps use the US Department of Defense (DoD) as an example of a Certificate Signing Authority (CSA), but you may use any CSA that authenticates SSL certificates.

Note that access to the `keytool` utility, available in JDK, is required in this method of creating SSL certificates. `Keytool` is a command-line tool used to manage keystores and the certificates.

**Step 1** Create SSL Client Certificate using the below command.

```
% keytool -genkey -keystore nmsclientkeystore -storetype pkcs12 -keyalg RSA -keysize 2048
-alias nmsclient -dname "CN=nmsclient, OU=WNBU, O=Cisco, L=San Jose, ST=CA, C=US"
-storepass nmskeystore
```

Provide the Key Algorithm as RSA and KeySize as 1024 or 2048.

**Step 2** Generate the Certificate Signing Request (CSR) using the below command.

```
% keytool -certreq -keyalg RSA -keysize 2048 -alias nmsclient -keystore nmsclientkeystore
-storetype pkcs12 -file <csrfilename>
```

Provide the Key Algorithm as RSA and KeySize as 1024 or 2048 and provide a certificate file name.

**Step 3** Send the generated CSR file to the US Department of Defense (or your choice of CSA). The DoD issues the corresponding signed certificates.

The CSR reply is through `dod.p7b` file. In addition you should also receive the root CA certificates.

Please make sure to retrieve the PKCS7 encoded certificates; Certificate Authorities provide an option to get the PKCS7 encoded certificates.

**Step 4** Import the CSR reply into the Keystore using the command:

```
% keytool -import dod.p7b -keystore nmsclientkeystore -storetype pkcs12
-storepass nmskeystore
```

**Step 5** Check the formats of root CA certificates received. They must be base-64 encoded. If they are not base-64 encoded, use the OpenSSL command to convert them to this format.

```
% openssl x509 -in rootCA.cer -inform DER -outform PEM -outfile rootCA.crt
% openssl x509 -in DoD-sub.cer -inform DER -outform PEM -outfile rootCA.crt
```

Convert both root CA certificate and sub-ordinate certificates received.

In case you received both root CA certificate and the sub-ordinate certificate, you have to bundle them together using the below command:

```
% cat DoD-sub.crt > ca-bundle.crt
% cat DoD-rootCA.crt >> ca-bundle.crt
```

**Step 6** To set up SSL Client Authentication using these certificates, enable SSL Client Authentication in Apache in the `ssl.conf` file located in `<NCS_Home>/webnms/apache/ssl/backup/` folder.

```
SSLCAcertificationPath conf/ssl.crt
SSLCAcertificationFile conf/ssl.crt/ca-bundle.crt
SSLVerifyClient require
SSLVerifyDepth 2
```

`SSLVerifyDepth` depends on the level of Certificate Chain. In case you have only 1 root CA certificate, this should be set to 1. In case you have a certificate chain (root CA and subordinate CA), this should be set to 2.

**Step 7** Install the DoD root CA certificates in Prime Infrastructure.

**Step 8** Import the nmsclientkeystore in your browser.

---

**Related Topics**

- [Setting Up SSL Certification](#)
- [Setting Up SSL Server Certification](#)

## Setting Up SSL Server Certification

---

**Step 1** Generate the Certificate Signing Request (CSR).

```
% ncs key genkey -csr <csrfilename> repository <repositoryname>
```

**Step 2** Import the Signed Certificate using the below command:

```
% ncs key importcacert <aliasname> <ca-cert-filename> repository <repositoryname>
```

Prime Infrastructure stores the self-signed certificate at /opt/CSCONcs/httpd/conf/ssl.crt. The imported certificates/keys are stored at /opt/CSCONcs/migrate/restore.

---

**Related Topics**

- [Setting Up SSL Certification](#)
- [Setting Up SSL Client Certification](#)

## Enabling OCSP Settings on the Prime Infrastructure Server

Online Certificate Status Protocol (OCSP) enables certificate-based authentication for web clients using OCSP responders. Typically, the OCSP responder's URL is read from the certificate's Authority Information Access (AIA). As a failover mechanism, you can configure the same URL on the Prime Infrastructure server as well.

To set up a custom URL of an OCSP responder, follow the steps below.

---

**Step 1** Log in to the Prime Infrastructure server using the command line, as explained in [Connecting Via CLI](#). Do not enter "configure terminal" mode.

**Step 2** At the prompt, enter the following command to enable client certificate authentication:

```
PIServer/admin# ocsp responder custom enable
```

**Step 3** At the prompt, enter the following command to set the custom OCSP responder URL:

```
PIServer/admin# ocsp responder set url Responder#URL
```

Where:

- **Responder#** is the number of the OCSP responder you want to define (e.g., 1 or 2).
- **URL** is the URL of the OCSP responder, as taken from the client CA certificate.

Note that there should be no space between the **Responder#** and **URL** values.

- Step 4** To delete an existing custom OSCP responder defined on the Prime Infrastructure server, use the following command:

```
PIServer/admin# oosp responder clear url Responder#
```

If you do not already know the number of the OSCP responder you want to delete, use the **show security-status** command to view the OSCP responders currently configured on the server. For details, see [Checking On Server Security Status](#).

---

## Setting Up Local Password Policies

If you are authenticating users locally, using Prime Infrastructure's own internal authentication, you can enhance your system's security by enforcing rules for strong password selection.

Note that these policies affect only the passwords for local Prime Infrastructure user IDs. If you are authenticating Prime Infrastructure users via a centralized or remote AAA server, you can enforce similar protections using the functions of the AAA server.

To enforce local password policies:

---

- Step 1** Log in to Prime Infrastructure with a user ID that has administrator privileges.

- Step 2** Select **Administration > Users > Users, Roles & AAA > Local Password Policy**.

- Step 3** Select the check boxes next to the password policies you want to enforce, including:

- The minimum number of characters passwords must contain.
- No use of the username or "cisco" as a password (or common permutations of these).
- No use of "public" in root passwords.
- No more than three consecutive repetitions of any password character.
- Passwords must contain at least one character from three of the following character classes: upper case, lower case, digit, and special character.
- Whether the password must contain only ASCII characters.
- Minimum elapsed number of days before a password can be reused.
- Password expiration period.
- Advance warnings for password expirations.

If you enable any of the following password policies, you can also specify:

- The minimum password length, in number of characters.
- The minimum elapsed time between password re-uses.
- The password expiry period.
- The number of days in advance to start warning users about future password expiration.

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

## Disabling Individual TCP/UDP Ports

The following table lists the TCP and UDP ports Prime Infrastructure uses, the names of the services communicating over these ports, and the product's purpose in using them. The "Safe" column indicates whether you can disable a port and service without affecting Prime Infrastructure's functionality.

**Table B-1** Prime Infrastructure TCP/UDP Ports

| Port      | Service Name   | Purpose                                                                                                                                      | Safe? |
|-----------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------|
| 21/tcp    | FTP            | File transfer between devices and server                                                                                                     | Y     |
| 22/tcp    | SSHD           | Used by SCP, SFTP, and SSH connections to and from the system                                                                                | N     |
| 69/udp    | TFTP           | File transfer between devices and the server                                                                                                 | Y     |
| 162/udp   | SNMP-TRAP      | To receive SNMP Traps                                                                                                                        | N     |
| 443/tcp   | HTTPS          | Primary Web Interface to the product                                                                                                         | N     |
| 514/udp   | SYSLOG         | To receive Syslog messages                                                                                                                   | N     |
| 1522/tcp  | Oracle         | Oracle/JDBC Database connections: These include both internal server connections and for connections with the High Availability peer server. | N     |
| 8082/tcp  | HTTPS          | Health Monitoring                                                                                                                            | N     |
| 8087/tcp  | HTTPS          | Software updates on HA Secondary Systems                                                                                                     | N     |
| 9991/udp  | NETFLOW        | To receive Netflow streams (enabled if Assurance license installed)                                                                          | N     |
| 61617/tcp | JMS (over SSL) | For interaction with remote Plug&Play Gateway server                                                                                         | Y     |

## Checking On Server Security Status

Prime Infrastructure administrators can connect to the server via CLI and use the **show security-status** command to display the server's currently open TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. For example:

---

**Step 1** Log in to Prime Infrastructure using the command line, as explained in [Connecting Via CLI](#). Do not enter “configure terminal” mode.

**Step 2** Enter the following command at the prompt:

```
PIServer/admin# show security-status
```

Depending on your settings, you will see output like the following:

```
Open TCP Ports: 22 443 1522 8082
Open UDP Ports: 162 514 9991
TFTP Service: disabled
FTP Service: disabled
JMS port (61617): disabled
Root Access: disabled
Client Auth: enabled
OCSP Responder1: http://10.77.167.65/ocsp
OCSP Responder2: http://10.104.178.99/ocsp
```

---



# Configuring High Availability for Plug and Play Gateway

---

This chapter explains how to configure the High Availability (HA) functionality for the Cisco Plug and Play Gateway standalone server and how to incorporate the feature along with HA implemented in Prime Infrastructure (where the primary and secondary servers have two different IP addresses) and Prime Infrastructure 3.0 virtual IP address HA Model.

## How Cisco Plug and Play Gateway HA Works

Prime Infrastructure 3.0 and earlier releases supported a single Cisco Plug and Play Gateway in either of these modes:

- Plug and Play Gateway standalone server mode
- Plug and Play Gateway integrated server mode

HA was not available in both these solutions, and Cisco Plug and Play Gateway does not connect to the secondary Prime Infrastructure server automatically. It has to be manually redirected to the secondary Prime Infrastructure server.

Prime Infrastructure 3.0 supports Plug and Play Gateway in HA. The Cisco Plug and Play HA feature aims at providing the following:

- HA on a standalone server Plug and Play Gateway by providing a secondary standby Plug and Play Gateway.
- HA support between the standalone Plug and Play Gateway and Prime Infrastructure HA.
- HA support for Prime Infrastructure integrated Plug and Play Gateway.

## Cisco Plug and Play Gateway HA Prerequisites

Before using the HA feature on Cisco Plug and Play Gateway, you must:

- Configure the primary and secondary Prime Infrastructure servers and these must be accessible from Plug and Play Gateway standalone servers. See [Configuring High Availability](#) for more details.
- Ensure that the primary and secondary Prime Infrastructure SSL server certificates used for Message Queue Ports 61617 and Health Monitor port 8082 are available for extraction from primary and secondary servers for Prime Infrastructure HA mode with different IP addresses. See [Setting Up High Availability](#) for more details.
- For virtual IP Address based HA, both primary and secondary servers must have the virtual IP address and certificates. See [Using Virtual IP Addressing with HA](#) for more details.
- At least one of the Prime Infrastructure server Message Queue port 61617 port must be active at all times depending on the service which will take the HA role.
- Install the primary and secondary Plug and Play Gateway Virtual Machines. See [Cisco Prime Infrastructure 3.0 Quick Start Guide](#) for details of installation of virtual machines from OVA file.

## Setting up Cisco Plug and Play Gateway HA

This section explains the different methods to configure Cisco Plug and Play Gateway in HA.

### Related Topics

- [Cisco Plug and Play Gateway HA Prerequisites](#)
- [Setting up Standalone Cisco Plug and Play Gateway for Prime Infrastructure HA](#)
- [Cisco Standalone Plug and Play Gateway Server HA Setup](#)
- [Cisco Plug and Play Gateway Status](#)
- [Cisco Plug and Play Gateway HA and Prime Infrastructure Combinations](#)

## Setting up Standalone Cisco Plug and Play Gateway for Prime Infrastructure HA

The Cisco Prime Infrastructure server in HA can be configured in two modes:

- Virtual IP addresses for primary and secondary servers. See [Using Virtual IP Addressing with HA](#) for more details.
- Different IP addresses for primary and secondary servers. See [Setting Up High Availability](#) for more details.

The standalone Cisco Plug and Play Gateway can be configured to work in both of these modes with a slight modification in the setup procedure.

### Related Topics

- [Prime Infrastructure in HA with Virtual IP Address](#)
- [Prime Infrastructure in HA with Different IP Address](#)



## Prime Infrastructure in HA with Virtual IP Address

Prime Infrastructure can be configured with a virtual IP address which floats across the primary and secondary servers, depending on the server that is active. Enter the virtual IP address of Prime Infrastructure in HA while setting up Cisco Plug and Play Gateway.

Integrated Plug and Play Gateway within Prime Infrastructure will work if the same virtual IP address is transferred to the active node. Cisco Plug and Play Gateway integrated with Prime Infrastructure will be configured automatically to use the Prime Infrastructure virtual IP address. No specific configuration is required to configure Cisco Plug and Play Gateway.

### Related Topics

- [Prime Infrastructure in HA with Different IP Address](#)

## Prime Infrastructure in HA with Different IP Address

Prime Infrastructure can be configured with primary and secondary servers having different IP addresses. For configuring Cisco Plug and Play Gateway, run the **pnpp setup advance** command in the advanced setup and enter the following information:

- Primary IP address.
- Enter **y**, when prompted if a secondary server is to be configured.
- Secondary IP address.

See [Command Reference Guide for Cisco Prime Infrastructure 3.0](#) for more details about running the commands.



### Note

Cisco Plug and Play Gateway integrated with Prime Infrastructure will not work when the primary and secondary servers have different IP addresses because the bootstrap configuration needs to be changed according to the active node.

### Related Topics

- [Cisco Plug and Play Gateway HA Prerequisites](#)
- [Setting up Standalone Cisco Plug and Play Gateway for Prime Infrastructure HA](#)
- [Cisco Standalone Plug and Play Gateway Server HA Setup](#)
- [Cisco Plug and Play Gateway Status](#)
- [Cisco Plug and Play Gateway HA and Prime Infrastructure Combinations](#)

## Cisco Standalone Plug and Play Gateway Server HA Setup

Cisco Standalone Plug and Play Gateway can also be configured in HA with a secondary server for failover. Cisco Plug and Play Gateway in HA is always configured with a virtual IP address on the active node. For setting up the standalone Plug and Play Gateway in HA you must:

- Install two reachable Cisco Plug and Play Gateways with different IP addresses.
- Run the **pnp setup** or **pnp setup advance** command on the primary Cisco Plug and Play Gateway. See [Command Reference Guide for Cisco Prime Infrastructure 3.0](#) for more details. The primary server will automatically configure secondary Cisco Plug and Play Gateway at the end of the setup.
- Enter **y** when prompted, if you want to configure HA with primary Cisco Plug and Play Gateway HA server.



### Note

The standalone Cisco Plug and Play Gateway with Prime Infrastructure in HA has automatic failover from primary to secondary. Manual failover is not available.

The standalone Cisco Plug and Play Gateway with Prime Infrastructure in HA can be configured to failback manually or automatically from the secondary to primary server.

Enter the Cisco Plug and Play Gateway virtual IP address, virtual host name, IP address and username and password of the secondary server as part of **pnp setup**. Enter **0** for manual failback and **1** for automatic failback when prompted during the setup.



### Note

We recommend manual failback. Automatic failback is not recommended because in case of scenarios like flapping interface, failover and failback happens continuously.

### Related Topics

- [Cisco Plug and Play Gateway Status](#)
- [How Cisco Plug and Play Gateway HA Works](#)
- [Setting up Cisco Plug and Play Gateway HA](#)
- [Cisco Plug and Play Gateway HA and Prime Infrastructure Combinations](#)

## Cisco Plug and Play Gateway Status

The Cisco Plug and Play Gateway status interface provides additional information regarding the following:

- Cisco Prime Infrastructure HA Status:
  - This displays whether the Cisco Plug and Play Gateway is connected to port 61617 in the primary server IP address or on secondary server IP address.
    - If Cisco Plug and Play Gateway is not connected to Prime Infrastructure, the status is displayed as down. No failover will happen in this case.
    - If the virtual IP address has been entered during setup, the status will display only the address. Cisco Plug and Play Gateway status cannot identify whether it is connected to the primary or secondary server.

- Cisco Plug and Play HA Status:

Along with the status for the different Cisco Plug and Play Gateway processes, it will also display the Cisco Plug and Play Gateway in active mode when both the gateways are up. The status will also show the connection status between the primary and secondary servers as an additional value in the table.

To check the status of the Cisco Plug and Play Gateway server, log in to the gateway server and run the **pnpp status** command. See [Command Reference Guide for Cisco Prime Infrastructure 3.0](#) for more details. The gateway server status is displayed.

See [Command Reference Guide for Cisco Prime Infrastructure 3.0](#) for more details on running the commands.

| SERVICE                                               | MODE       | STATUS    | ADDITIONAL INFO       |
|-------------------------------------------------------|------------|-----------|-----------------------|
| System                                                |            | UP        |                       |
| Event Messaging Bus                                   | PLAIN TEXT | UP        | pid: 6808             |
| CNS Gateway Dispatcher<br>port: 11011                 | PLAIN TEXT | UP        | pid: 7189,            |
| CNS Gateway<br>port: 11013                            | PLAIN TEXT | UP        | pid: 7223,            |
| CNS Gateway<br>port: 11015                            | PLAIN TEXT | UP        | pid: 7262,            |
| CNS Gateway<br>port: 11017                            | PLAIN TEXT | UP        | pid: 7306,            |
| CNS Gateway<br>port: 11019                            | PLAIN TEXT | UP        | pid: 7410,            |
| CNS Gateway<br>port: 11021                            | PLAIN TEXT | UP        | pid: 7493,            |
| CNS Gateway Dispatcher<br>port: 11012                 | SSL        | UP        | pid: 7551,            |
| CNS Gateway<br>port: 11014                            | SSL        | UP        | pid: 7627,            |
| CNS Gateway<br>port: 11016                            | SSL        | UP        | pid: 7673,            |
| CNS Gateway<br>port: 11018                            | SSL        | UP        | pid: 7793,            |
| CNS Gateway<br>port: 11020                            | SSL        | UP        | pid: 7905,            |
| CNS Gateway<br>port: 11022                            | SSL        | UP        | pid: 7979,            |
| HTTPD                                                 |            | UP        |                       |
| Image Web Service                                     | SSL        | UP        |                       |
| Config Web Service                                    | SSL        | UP        |                       |
| Resource Web Service                                  | SSL        | UP        |                       |
| Image Web Service                                     | PLAIN TEXT | UP        |                       |
| Config Web Service                                    | PLAIN TEXT | UP        |                       |
| Resource Web Service                                  | PLAIN TEXT | UP        |                       |
| <b>Prime Infrastructure Broker</b>                    | <b>SSL</b> | <b>UP</b> | <b>Connection: 1,</b> |
| <b>Connection Detail: ::ffff:10.104.105.170:61617</b> |            |           |                       |
| bgl-dt-pnp-ha-216/admin#                              |            |           |                       |
| SERVICE                                               | MODE       | STATUS    | ADDITIONAL INFO       |
| System                                                |            | UP        |                       |
| Event Messaging Bus                                   | PLAIN TEXT | UP        | pid: 6426             |
| CNS Gateway Dispatcher<br>port: 11011                 | PLAIN TEXT | UP        | pid: 7107,            |

```

CNS Gateway | PLAIN TEXT | UP | pid: 7141,
port: 11013
CNS Gateway | PLAIN TEXT | UP | pid: 7180,
port: 11015
CNS Gateway | PLAIN TEXT | UP | pid: 7224,
port: 11017
CNS Gateway | PLAIN TEXT | UP | pid: 7263,
port: 11019
CNS Gateway | PLAIN TEXT | UP | pid: 7309,
port: 11021
CNS Gateway Dispatcher | SSL | UP | pid: 7381,
port: 11012
CNS Gateway | SSL | UP | pid: 7537,
port: 11014
CNS Gateway | SSL | UP | pid: 7581,
port: 11016
CNS Gateway | SSL | UP | pid: 7685,
port: 11018
CNS Gateway | SSL | UP | pid: 7855,
port: 11020
CNS Gateway | SSL | UP | pid: 7902,
port: 11022
HTTPD | | UP |
Image Web Service | SSL | UP |
Config Web Service | SSL | UP |
Resource Web Service | SSL | UP |
Image Web Service | PLAIN TEXT | UP |
Config Web Service | PLAIN TEXT | UP |
Resource Web Service | PLAIN TEXT | UP |
Prime Infrastructure Broker | SSL | UP | Connection: 1,
Connection Detail: ::ffff:10.104.105.170:61617
PnP Gateway Monitoring | SSL | UP | port: 11010
PnP Gateway HA | SSL | UP | Primary Server
is in Active state
bgl-dt-pnp-ha-217/admin#

```

### Related Topics

- [Removing Cisco Plug and Play Gateway in HA](#)
- [Cisco Plug and Play Gateway HA and Prime Infrastructure Combinations](#)
- [Limitations of Cisco Plug and Play Gateway HA](#)
- [How Cisco Plug and Play Gateway HA Works](#)
- [Setting up Cisco Plug and Play Gateway HA](#)

# Removing Cisco Plug and Play Gateway in HA

To delete the HA configuration for Prime Infrastructure with different primary and secondary IP addresses in the standalone Cisco Plug and Play Gateway, run the **pnpl setup advance** advanced setup command and enter **n** when prompted.

For deleting Cisco Plug and Play Gateway HA, run the **pnpl setup** or **pnpl setup advance** command and enter **n** when prompted.

See [Command Reference Guide for Cisco Prime Infrastructure 3.0](#) for more details.

**Note**

When deleting Cisco Plug and Play Gateway HA, the administrator must manually modify the dynamic port allocation **cns event** command and decommission the secondary server, if HA is being turned off. The Cisco Plug and Play Gateway secondary server will continue to run with the virtual IP address if it is not decommissioned.

**Related Topics**

- [Cisco Plug and Play Gateway HA and Prime Infrastructure Combinations](#)
- [Limitations of Cisco Plug and Play Gateway HA](#)
- [How Cisco Plug and Play Gateway HA Works](#)
- [Setting up Cisco Plug and Play Gateway HA](#)

## Cisco Plug and Play Gateway HA and Prime Infrastructure Combinations

The Cisco Plug and Play Gateway functionality allows different configurations for HA with Prime infrastructure. The various combinations, as per the configuration options available, are:

- Standalone Cisco Plug and Play Gateway without HA (Single Cisco Plug and Play Gateway)
  - The Prime Infrastructure server without HA.
  - The Prime Infrastructure server with HA with the virtual IP address.
  - Prime Infrastructure server with HA with the primary and secondary servers having two IP addresses.
- Standalone Cisco Plug and Play Gateway with HA and virtual IP address (Two Cisco Plug and Play Gateways)
  - Prime Infrastructure server without HA.
  - Prime Infrastructure server with HA with the virtual IP address.
  - Prime Infrastructure server with HA with the primary and secondary servers having two IP addresses.
- Integrated Cisco Plug and Play Gateway within Prime Infrastructure
  - Prime Infrastructure server without HA.
  - Prime Infrastructure server with HA with the virtual IP Address.

**Related Topics**

- [Limitations of Cisco Plug and Play Gateway HA](#)
- [How Cisco Plug and Play Gateway HA Works](#)
- [Setting up Cisco Plug and Play Gateway HA](#)
- [Removing Cisco Plug and Play Gateway in HA](#)
- [Cisco Plug and Play Gateway Status](#)

## Limitations of Cisco Plug and Play Gateway HA

The Cisco Plug and Play Gateway HA feature has the following limitations:

- Any Plug and Play requests that are partially completed on the Cisco Plug and Play Gateway during failover and failback (the Prime Infrastructure and Cisco Plug and Play Gateway standalone server) will remain incomplete in the Prime Infrastructure server and these may not be configured successfully on the device.
- Failover and failback takes five to ten minutes during which Cisco Plug and Play Gateway provisioning does not happen. Devices that have received bootstrap with **cns config initial** will continue to reach Cisco Plug and Play Gateway for provisioning. See [Command Reference Guide for Cisco Prime Infrastructure 3.0](#) for more details.
- Devices take time to connect to the backup server once the IP address is moved from the active to standby server depending on the configuration available in the **cns event** command for reconnect time. See [Command Reference Guide for Cisco Prime Infrastructure 3.0](#) for more details.
- Cisco Prime Infrastructure integrated Plug and Play Gateway will support HA if the HA configuration in Prime is based on a virtual IP address. Prime Infrastructure HA with different IP addresses for primary and secondary servers will not support the Plug and Play Gateway HA functionality in the integrated server.
- For the Cisco Prime Infrastructure integrated Plug and Play Gateway, SSLv3 is disabled by default on all Gateway SSL ports (for example, ports 11012, 11014, and so on).

**Related Topics**

- [How Cisco Plug and Play Gateway HA Works](#)
- [Setting up Cisco Plug and Play Gateway HA](#)
- [Removing Cisco Plug and Play Gateway in HA](#)
- [Cisco Plug and Play Gateway HA and Prime Infrastructure Combinations](#)