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
- 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: • Check for Cisco software image updates • Open or review Cisco support cases You can also access this page from a link on the **Administration > Settings > System Settings > Software Update** page.	**General > Account Credentials**	Prime Infrastructure appliance
Configure proxies for the Prime Infrastructure server and its local authentication server.	**General > Account Credentials > Proxy** See Configuring Proxy Settings.	Not Applicable
Configure the settings for creating a technical support request.	**General > Account Credentials > Support Request** See Configuring Technical Support Request Settings.	Wired and wireless devices
Configure transport gateway mode to send information over the internet via Smart Call Home Transport Gateway, while smart licensing is enabled.	**General > Account Credentials > Smart Licensing Transport** See Setting Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager.	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

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

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
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
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
• 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
• 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
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
• 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:
Set global SNMP polling parameters, including trace display values, reachability parameters and the backoff algorithm. 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.	**Network and Device > SNMP** See Configuring Global SNMP Settings.	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.	**Network and Device > Switch Port Trace (SPT) > Auto SPT** See Configuring SNMP Credentials for Rogue AP Tracing.	Wireless devices only
Set the SNMP credentials and trace parameters to be used in tracing rogue AP switch ports.	**Network and Device > Switch Port Trace (SPT) > Manual SPT** See Configuring SNMP Credentials for Rogue AP Tracing.	Wireless devices only
Set basic and advanced switch port trace parameters.	**Network and Device > Switch Port Trace (SPT) > SPT Configuration** See Configuring Switch Port Tracing.	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.	**Network and Device> Switch Port Trace (SPT) > Known Ethernet MAC Address**	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.	**Inventory > Configuration** See Archiving Device Configurations Before Template Deployment.	Wired and wireless devices
Set basic parameters for the configuration archive, such as timeout value, number of configuration versions to store, and so forth.	**Inventory > Configuration Archive** See Specifying When and How to Archive WLC Configurations.	Wired and wireless devices
Configure Data Center settings.	**Inventory > Data Center Settings**	Prime Infrastructure appliance
Specify IPv4 or IPv6 address preferences	**Inventory > Discovery**	Wired and wireless devices
Determine whether you want to display groups that do not have members or children associated with them.	**Inventory > Grouping**	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
• 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. • Change how the source of any failure is displayed.	**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:
• 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. Cisco Prime Infrastructure polls both Wireless and Wired clients. **Note** This is not a recommended option to be used in a network with large number of wireless clients. • Enable discover clients from enhanced traps to discover client and session information from enhanced trap received from the compatible Cisco WLCs. **Note** You must configure the WLCs to send the traps using the following CLI commands: – config trapflags client enhanced-802.11-associate – config trapflags client enhanced-802.11-deauthenticate – config trapflags client enhanced-802.11-stats – config trapflags client enhanced-authentication • Enable discover wired clients on trunk ports to discover the unmanaged entity other than switch and router, which is connected to trunk ports. • 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_passw
ord,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 > Account Settings** and select **Proxy** tab.

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 Click **Test Connectivity** to check the connection status and click **Save**.

Configuring Server Port and Global Timeout Settings

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

FTP and TFTP services are normally enabled by default. HTTP services are disabled by default. You should enable HTTP 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, TFTP, or HTTP service status and 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 10 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**.

Step 4 A server restart is required to apply your changes (see "Restarting Prime Infrastructure" in Related Topics).

Related Topics

- Restarting Prime Infrastructure
- 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 back in 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.
- Standard Prime Infrastructure virtual appliance. For details, see Prime Infrastructure Minimum Server Requirements in *Cisco Prime Infrastructure 3.1 Quick Start Guide*.

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**.

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**.

Configuring Software Image Management Servers

You can add up to three software image management servers for image distribution.

Step 1 Click **Administration > Servers > Software Image Management Servers**.

Step 2 Click the add icon and complete the following fields:

- Server Name
- IP Address
- Sites Served
- Description

Step 3 Click **Save**.

Step 4 Click **Manage Protocols** to add the protocols.

Step 5 Click the add icon and complete the following fields:

- Protocol
- Username
- Password
- Protocol Home Directory

Step 6 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.

Pre-listed job types include: Discovery, Config, Configuration Archive, Configuration Overwrite, Configuration Rollback, Import, PollerJob, and SWIM Collection. You can add job types by typing them in the text box provided.

Step 4 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 exists, 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 Click either the **IP Address** or **DNS** radio button.

If you select **IP address**, enter the server IP address and server name or enter the DNS server name if you select **DNS**.

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 **SMNP 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.

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 (.p7b file), which are typically given filenames that reflect the name of the CA.

Step 5 Enter the following command to import the SSL certificate file into the Prime Infrastructure server:

```
PIServer/admin# ncs key importcacert tomcat *.cer repository defaultRepo
```

Step 6 Enter the following command to import the CA certificate file into the Prime Infrastructure server:

```
PIServer/admin# ncs key importsignedcert *.p7b repository defaultRepo
```

Step 7 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

Obtaining and Importing Subject Alternate Names (SAN) CA-Signed Certificates

Prime Infrastructure does not has the provision to generate SAN Certificate Signing Request (CSR). Use Certificate Authority (CA) to generate a SAN Certificate Signing Request (CSR) file.

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.

Step 1 Use Certificate Authority (CA) to generate a SAN Certificate Signing Request (CSR) file.

Step 2 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 one 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 want to apply it.
- The CA certificates, which are typically given filenames that reflect the name of the CA.

Step 3 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 4 At the Prime Infrastructure command line, copy the single certificate file & Private Key to the backup repository. For example:

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

`PIServer/admin#` **copy ftp://your.ftp.server/privatekey.key disk:defaultRepo**

where CertFile .cer is the single certificate file you created in the previous step and privatekey.key is the private key file you received from CA.

Step 5 Enter the following command to import the Private Key into the Prime Infrastructure server:

`PIServer/admin#` **ncs key importkey privatekey.key CertFile.cer repository defaultRepo**

Note You must import Private Key before you import CA certificate.

Step 6 Enter the following command to import the single certificate file into the Prime Infrastructure server:

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

Step 7 To activate the CA-signed certificates, restart Prime Infrastructure, (see Restarting Prime Infrastructure in the Related Topics).

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 deletecacert *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
cWNotificationManagedObject AddressType	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.
cWNotificationManagedObject Address	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.
cWNotificationSourceDisplay Name	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).