Prime Infrastructure Server Settings

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

Available System Settings

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

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

Table 2-1 Available Prime Infrastructure Settings

To do this:	Choose Administration > System Settings > ...	Applicable for:
• 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** See Specifying Alarm Clean Up and Display Options, page 5-1.	Wired and wireless devices
Choose whether audit logs are basic or template based and select the device parameters to audit on.	**Audit** See Setting Up Auditing Configurations, page 5-4.	Wired and wireless devices
Purge syslogs and send the purged logs either to trash or to a remote directory.	**Audit Log Purge Settings** See Deleting Syslogs from Audit Records, page 5-5.	Not Applicable
Enable Change Audit JMS Notification by selecting the Enable Change Audit JMS Notification check box.	**Change Audit Notification** See Enabling Change Audit Notifications, page 5-6.	Wired and wireless devices
• Set the protocol to be used for controller and autonomous AP CLI sessions. • Enable autonomous AP migration analysis on discovery.	**CLI Session** See Configuring Protocols for CLI Sessions, page 7-2.	Wireless Device
• 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** See Configuring Client Performance Settings, page 3-6.	Wired and wireless devices
Set basic control parameters used when deploying a device configuration, such as enabling backup of the running configuration, rollbacks, retrieval of **show** command output from the cache, and the number of CLI thread pools to use.	**Configuration** See Backing up and Rolling Back Configurations, page 6-6.	Wired and wireless devices
Set basic parameters for the configuration archive, such as protocol, timeout value, number of configuration versions to store, and so forth.	**Configuration Archive** See Specifying When to Archive Configurations, page 6-6.	Wired and wireless devices

Table 2-1 Available Prime Infrastructure Settings (continued)

To do this:	Choose Administration > System Settings > ...	Applicable for:
Enable auto refresh after a wireless controller upgrade, and process the save configuration trap.	**Controller Upgrade Settings** See Refreshing Controllers After an Upgrade, page 7-2.	Wireless Device
Enable or disable data deduplication.	**Data Deduplication** See Enabling Data Deduplication, page 6-4.	Not applicable
Set the retention period for the following data types: Trends, Device Health, Performance, Network Audit, System Health.	**Data Retention** See Specifying Data Retention Periods, page 6-2.	Wired and wireless devices
Define the device group hierarchy. By default, the hierarchy is as follows: • Device Type/Routers • Device Type/Switches and Hubs • Device Type/Routers/Cisco 1000 Voice Series Routers	**Grouping**	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.	**Guest Account Settings** See Configuring Guest Account Settings, page 9-3.	Wireless devices
Configure global preference parameters for downloading, distributing, and recommending software Images.	**Image Management** See the *Cisco Prime Infrastructure 2.0 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 even for a device.	**Inventory** See Specifying Inventory Collection After Receiving Events, page 6-5.	Wired and wireless devices
Enable job approval to specify the jobs which require administrator approval before the job can run.	**Job Approval Settings** See Specifying Administrator Approval for Jobs, page 2-11.	Wired and wireless devices
View, add, or delete the Ethernet MAC address available in Prime Infrastructure. if you add multiple Ethernet MAC addresses to this list, then Auto Switch Port Tracing will not scan these ports for Rogue AP.	**Known Ethernet MAC Address** See Configuring Email Settings, page 2-5.	Not applicable
Change the disclaimer text displayed at the bottom of the login page for all users.	**Login disclaimer** See Specifying Login Disclaimer Text, page 2-12.	Not Applicable
Enable email distribution of reports and alarm notifications.	**Mail server configuration** See Configuring Email Settings, page 2-5.	Not Applicable

Table 2-1 Available Prime Infrastructure Settings (continued)

To do this:	Choose Administration > System Settings > ...	Applicable for:
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.	**Notification receivers** See Adding Notification Receivers to Prime Infrastructure, page 2-14.	Wired and wireless devices
Modify the settings for Plug and Play.	**Plug & Play**	Wired device
Configure proxies for the Prime Infrastructure server and its local authentication server.	**Proxy Settings** See Configuring Proxy Settings, page 2-10.	Not Applicable
Set the path where scheduled reports are stored and how long reports are retained.	**Report** See Specifying Where and for How Long to Save Reports, page 6-4.	Wired and wireless devices
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.	**Rogue AP Settings** See Configuring SNMP Credentials for Rogue AP Tracing, page 7-1.	Wireless device
Configure the FTP, TFTP, HTTP, HTTPS, NTP servers, and Compliance Service used.	**Server Settings** See Configuring Server Settings, page 2-11.	Not applicable
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.	**Server Tuning** See Configuring Client Performance Settings, page 3-6.	Wired and wireless devices
Configure the Cisco WAAS Central Manager IP address in Cisco Prime Infrastructure.	**Service Container Management** See Cisco WAAS Central Manager Integration.	Wired device
Set the severity level of any generated alarm.	**Severity Configuration** See Changing Alarm Severities, page 5-3.	Wired and wireless devices
Set the SNMP credentials and trace parameters to be used in tracing rogue AP switch ports.	**SNMP Credentials** See Configuring SNMP Credentials for Rogue AP Tracing, page 7-1.	Wireless device

Table 2-1 Available Prime Infrastructure Settings (continued)

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

Configuring Email Settings

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

Before You Begin

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

To configure global email parameters:

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

Step 2 Enter the hostname of the primary SMTP server.

Step 3 Enter the username of the SMTP server.

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

Note Both username and password are optional.

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

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

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

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

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

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

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

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

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

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

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

Configuring Global SNMP Settings

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

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

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

To configure global SNMP settings:

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

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

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

Note The default is unselected for security reasons.

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

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

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

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

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

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

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

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

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

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

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

Viewing SNMP Credential Details

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

To view or edit details for current SNMP credentials:

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

Step 2 From the left sidebar menu, choose **SNMP Credentials**.

Step 3 Click the Network Address link to open the SNMP Credential Details page. The details page displays the following information:

General Parameters

- Add Format Type—Display only. See the "Adding a New SNMP Credential Entry" section on page 2-9 for more information regarding Add Format Type.
- Network Address
- Network Mask

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

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

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

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

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

Adding a New SNMP Credential Entry

To add a new SNMP credential entry:

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

Step 2 From the left sidebar menu, choose **SNMP Credentials**.

Step 3 Choose **Add SNMP Entries** from the **Select a command** drop-down list, then click **Go**.

Step 4 Choose one of the following:

To manually enter SNMP credential information, leave the Add Format Type drop-down list at SNMP Credential Info. To add multiple network addresses, use a comma between each address. Go to Step 6.

If you want to add multiple switches by importing a CSV file, choose **File** from the Add Format Type drop-down list. The CSV file allows you to generate your own import file and add the devices you want. Go to Step 5.

Step 5 If you chose File, click **Browse** to find the location of the CSV file you want to import. Skip to Step 10.

The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory.

Sample File:

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_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 CSV file can contain the following fields:

- ip_address:IP address
- snmp_version:SNMP version
- network_mask:Network mask
- snmp_community:SNMP V1/V2 community
- snmpv3_user_name:SNMP V3 username
- snmpv3_auth_type:SNMP V3 authorization type. Can be None or HMAC-MD5 or HMAC-SHA
- snmpv3_auth_password:SNMP V3 authorization password
- snmpv3_privacy_type:SNMP V3 privacy type. Can be None or DES or CFB-AES-128
- snmpv3_privacy_password:SNMP V3 privacy password
- snmp_retries:SNMP retries
- snmp_timeout:SNMP timeout

Step 6 If you chose SNMP Credential Info, enter the IP address of the switch you want to add. If you want to add multiple switches, use a comma between the string of IP addresses.

Step 7 In the Retries field, enter the number of times that attempts are made to discover the switch.

Step 8 Provide the session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.

Step 9 Choose the applicable versions for the SNMP parameters. The SNMP credentials are validated according to which SNMP versions are selected.

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

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

Step 10 Click **OK**.

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

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

Configuring Proxy Settings

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

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

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

Step 3 Select the **Enable Proxy** check box to allow proxy settings for the Prime Infrastructure server.

Step 4 Enter the required information and click **Save**.

Configuring Server Settings

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

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

Step 2 From the left sidebar menu, choose **Server Setting**.

Step 3 If you want to modify the FTP and TFTP directories or the HTTP and HTTPS ports that were established during installation, enter the port number (or port number and root where required) that you want to modify and click **Enable** or **Disable**.

The changes are reflected after a restart.

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

Configuring TFTP or FTP Servers

Step 1 Choose **Design > Management Tools > External Management Servers > TFTP/FTP Servers**.

Step 2 From the Select a command drop-down list, choose **Add TFTP/FTP Server** and click **Go**.

Step 3 From the Server Type drop-down list, choose **TFTP**, **FTP**, or **Both**.

Step 4 Enter a user-defined name for the TFTP or FTP server.

Step 5 Enter the IP address of the TFTP or FTP server.

Step 6 Click **Save**.

Specifying Administrator Approval for Jobs

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

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

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

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

Step 2 Select the **Enable Job Approval** check box

Step 3 From the list of job types, use the arrows to move any jobs for which you want to enable job approval to the list in the right. By default, job approval is disabled so all jobs appear in the list on the left.

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

Step 5 Click **Save**.

Approving Jobs

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

Choose **Administration > Jobs Approval** to:

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

Specifying Login Disclaimer Text

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

To enter login disclaimer text:

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

Step 2 From the left sidebar menu, choose **Login Disclaimer**.

Step 3 Enter your login disclaimer text in the available text box, then click **Save**.

Adding Device Information to a User Defined Field

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

To add a UDF:

Step 1 Choose **Administration > System Settings > User Defined Field**.

Step 2 Click **Add Row** to add a UDF.

Step 3 Enter the field label and description in the corresponding fields.

Step 4 Click **Save** to add a UDF.

Managing OUI

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

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

This section contains the following topics:

Adding a New Vendor OUI Mapping

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.

To add a new vendor OUI mapping:

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

Step 2 From the left sidebar menu, choose **User Defined OUI**. The User Defined OUI page appears.

Step 3 Choose **Add OUI Entries** from the **Select a Command** drop-down list, then click **Go**.

Step 4 In the OUI field, enter a valid OUI. The format is aa:bb:cc.

Step 5 Click **Check** to verify if the OUI exists in the vendor OUI mapping.

Step 6 In the Name field, enter the display name of the vendor for the OUI.

Step 7 Select the **Change Vendor Name** check box to update the display name of the vendor, if the OUI exists in the vendor OUI mapping, then click **OK**.

Uploading an Updated Vendor OUI Mapping File

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

To upload the updated vendor OUI mapping file:

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

Step 2 From the left sidebar menu, choose **Upload OUI**. The Upload OUI From File page appears.

Step 3 Browse and select the vendorMacs.xml file that you downloaded from Cisco.com, then click **OK**.

Adding Notification Receivers to Prime Infrastructure

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

To access the Notification Receiver page:

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

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear in this page.

Step 3 Choose **Add Notification Receiver f**rom the **Select a command** drop-down list, then click **Go**.

Step 4 Enter the server IP address and name.

Step 5 Click either the **North Bound** or **Guest Access** radio button.

The Notification Type automatically defaults to UDP.

Step 6 Enter the UDP parameters including Port Number and Community. The receiver that you configure should be listening to UDP on the same port that is configured.

Step 7 If you selected North Bound as the receiver type, specify the criteria and severity. Alarms for the selected category only are processed. Alarms with the selected severity matching the selected categories are processed.

Step 8 Click **Save** to confirm the Notification Receiver information.

By default, only INFO level events are processed for the selected Category.

Only SNMPV2 traps are considered for North Bound notification.

Removing a Notification Receiver

To delete a notification receiver:

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

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear on this page.

Step 3 Select the check boxes of the notification receivers that you want to delete.

Step 4 Choose **Remove Notification Receiver** from the **Select a command** drop-down list, then click **Go**.

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

Sample Log File from North Bound SNMP Receiver

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

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

Setting Up HTTPS Access to the Prime Infrastructure Server

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

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

Step 1 Log in to the CLI of Prime Infrastructure server as root user.

Step 2 Change to the /opt/CSCOlumos directory and enter the following command:

jre/bin/keytool -list -alias tomcat -keystore conf/keystore -storepass changeit –v

The existing SSL Certificate details are displayed.

Step 3 To view the list of CA Certificates that exist in the Prime Infrastructuretrust store, enter the following command in Prime Infrastructure admin mode:

ncs key listcacerts

Generating a Self-Signed Certificate in Prime Infrastructure

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

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

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

ncs key genkey –newdn

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

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

- ncs stop

- ncs start

Generating a Certificate Signing Request (CSR) File

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

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

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

a. At the Prime Infrastructure appliance, exit to the command line.

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

c. Enter the following command to generate the CSR file in the default backup repository:

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

where:

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

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

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

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

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

Step 4 You will receive a signed certificate file with the same filename, but with the file extension CER, from the CA. Before continuing, ensure:

- There is only one CER file. In some cases, you may receive chain certificates as individual files. If so, concatenate these files into a single CER file.
- Any blank lines in the CER file are removed.

Step 5 At the command line, copy the CER file to the backup repository. For example:

- copy ftp://your.ftp.server/*CertName***.cer disk:***RepoName*

Step 6 Import the CER file into the Prime Infrastructure server using the following command:

- ncs key importsignedcert *CertName***.cer repository** *RepoName*

Step 7 Restart the Prime Infrastructure server by issuing the following commands in this order:

- ncs stop

- ncs start

Step 8 If the Certificate Authority who signed the certificate is not already a trusted CA: Instruct users to add the certificate to their browser trust store when accessing the Prime Infrastructure login page.

Importing a Certificate Authority (CA) Certificate and Key

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

Step 1 At the command line, log in using the administrator ID and password and enter the following command:

ncs key importcacert *aliasname ca-cert-filename* **repository** *repositoryname*

where

- *aliasname* is a short name given for this CA certificate.
- *ca-cert-filename* is the CA certificate file name.
- *repositoryname* is the repository name configured in Prime Infrastructure where the ca-cert-filename is hosted.

Step 2 To import an RSA key and signed certificate to Prime Infrastructure, enter the following command in admin mode:

ncs key importkey *key-filename cert-filename* repository *repositoryname*

where

- *key-filename* is the RSA private key file name.
- *cert-filename* is the certificate file name.
- *repositoryname* is the repository name configured in Prime Infrastructure where the key-file and cert-file are hosted.

Step 3 Restart the Prime Infrastructure server by issuing the following commands in this order:

- ncs stop

- ncs start

Deleting a CA Certificate

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

ncs key deletecacert <*aliasname*>

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

MIB to Prime Infrastructure Alert/Event Mapping

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

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

Field Name and Object ID	Data Type	Prime Infrastructure Event/Alert field	Description
cWNotificationTimestamp	DateAndTime	createTime - NmsAlert 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 2-2 Cisco-Prime Infrastructure-Notification-MIB to Prime Infrastructure Alert/Event Mapping (continued)

Field Name and Object ID	Data Type	Prime Infrastructure Event/Alert field	Description
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: critical(1) major(2) minor(3) warning(4) clear(5) info(6) unknown(7)
cWNotificationSpecialAttributes	OCTET STRING	All the attributes in alerts/events apart from the base alert/event class.	This object represents the specialized attributes in alerts like APAssociated, APDisassociated, RogueAPAlert, CoverageHoleAlert, and so on. The string is formatted in property=value pairs in CSV format.
cWNotificationVirtualDomains	OCTET STRING	N/A	Virtual Domain of the object that caused the alarm. This field empty for the current release.