Configure the Prime Infrastructure Server

View the Prime Infrastructure Server Configuration

Use this procedure to view Prime Infrastructure server configuration information such as the current server time, kernel version, operating system, hardware information, and so forth.

Step 1 Choose **Administration** > **Dashboards** > **System Monitoring Dashboard**.

Step 2 Click the **Overview** tab.

Step 3 Click **System Information** at the top left of the dashboard to expand the System Information field.

Related Topics

- Overview Dashboard
- Performance Dashboard
- Admin Dashboard

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 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

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
Configure proxies for the Prime Infrastructure server and its local authentication server.	General > Account Credentials > Proxy See Set Up the Prime Infrastructure Proxy Server .	Not Applicable
Configure the settings for creating a technical support request.	General > Account Credentials > Support Request See Set Up Defaults for Cisco Support Requests.	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 About Historical Data Retention.	Wired and wireless devices

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
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 Configure 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 Configure Cisco Product Feedback Settings, on page 41.	Wired and wireless devices
Enable job approval to specify the jobs which require administrator approval before the job can run.	**General** > **Job Approval** See Configure Job Approvers and Approve Jobs.	Wired and wireless devices

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
Change the disclaimer text displayed on the login page for all users.	**General** > **Login Disclaimer** See Create a Login Banner (Login Disclaimer), on page 30.	Prime Infrastructure appliance
Set the path where scheduled reports are stored and how long reports are retained.	**General** > **Report** See Control 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 Configure Server Port and Global Timeout Settings, on page 28.	Prime Infrastructure appliance

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
• 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 Infrastructure software 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
To migrate inventory, site groups,user defined CLI and/or composite templates, associated site maps and cmx data from Prime Infrastructure to Cisco DNA Center.	**Mega Menu > Cisco DNA Center coexistence** See Cisco Prime Infrastructure to Cisco Digital Network Architecture Center Co-existence Guide	Prime Infrastructure to Cisco DNA Center migration.

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
Enable Change Audit JMS Notification by selecting the **Enable Change Audit JMS Notification** check box.	**Mail and Notification** > **Change Audit Notification** See Enable Change Audit Notifications and Configure Syslog Receivers.	Wired and wireless devices
To send job notification mail for every user job	**Mail and Notification** > **Job Notification Mail** See Configure Job Notification Mail for User Jobs	Wired and wireless devices
Enable email distribution of reports and alarm notifications.	**Mail and Notification** > **Mail Server Configuration** See Configure Email Server 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 .	Wireless devices only
Enable auto refresh after a wireless controller upgrade, and process the save configuration trap.	**Network and Device** > **Controller Upgrade** See Refresh Controllers After an Upgrade.	Wireless devices only
Enable Unified AP ping capability setting on the Cisco Prime Infrastructure.	**Network and Device** > **Unified AP Ping Reachability**	Wireless devices only

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
Modify the settings for Plug and Play.	**Network and Device** > **Plug & Play**	Wired devices only
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 Configure Global SNMP Settings, on page 31.	Wireless devices only

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
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 Configure 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 Configure 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 Configure 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

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
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 Archive Device Configurations Before Template Deployment.	Wired and wireless devices
Set basic parameters for the configuration archive, such as protocol, number of configuration versions to store, and so forth.	**Inventory** > **Configuration Archive** See Specify When and How to Archive WLC Configurations.	Wired and wireless devices
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
Configure global preference parameters for downloading, distributing, and recommending software Images.	**Inventory** > **Software Image Management** See the Cisco Prime Infrastructur User Guide for information about Software Image Management.	Wired and wireless devices

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
Enable inventory collection to allow Prime Infrastructure to collect inventory when it receives a syslog event for a device.	**Inventory** > **Inventory** See Specify Inventory Collection After Receiving Events.	Wired and wireless devices
Store additional information about a device.	**Inventory** > **User Defined Fields** See Add Device Information to a User Defined Field, on page 37.	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 Specify Alarm Clean Up, Display and Email Options.	Wired and wireless devices

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
Configure remote event and alarm receivers who will receive notifications from Prime Infrastructure. Alerts and events are sent as SNMPv2 notifications to configured notification destination. If you are adding a notification destination with the notification type UDP, the destination 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.	**Mail and Notification > Notification Destination** See Configure Alarms Notification Destination. **Alarms and Events > Alarm Notification Policies** See Customize Alarm Notification Policies.	Wired and wireless devices
Set the severity level of any generated alarm.	**Alarms and Events > Alarm Severity and Auto Clear** See Change Alarm Severity Levels.	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

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
	Client and User > Client See Configure Client Performance Settings.	Wired and wireless devices

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 Wired clients to identify their sessions only when a trap or syslog is received. **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		

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
information from enhanced trap received from the compatible Cisco WLCs. 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		

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
• 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.		
Add a vendor Organizationally Unique Identifier (OUI) mapping XML file.	**Client and User** > **User Defined OUI** See Add a New Vendor OUI Mapping.	Wired and wireless devices
Upload an updated vendor OUI mapping XML file.	**Client and User** > **Upload OUI** See Upload an Updated Vendor OUI Mapping File.	Wired and wireless devices

To do this:	Choose Administration > Settings > System Settings >...	Applicable to:
Configure the Cisco WAAS Central Manager IP address in Cisco Prime Infrastructure.	**Services** > **Service Container Management** See Cisco WAAS Central Manager Integration (user guide).	Wired devices only

Secure the Connectivity of the Prime Infrastructure Server

For data security, Prime Infrastructure encrypts data in transit using standard public key cryptography methods and public key infrastructure (PKI). You can obtain more information about these technologies from the internet. Prime Infrastructure encrypts the data that is exchanged between the following connections:

- Between the web server and the web client
- Between a CLI client and the Prime Infrastructure CLI shell interface (handled by SSH)
- Between the Prime Infrastructure and systems such as AAA and external storage

To secure communication between the web server and web client, use the public key cryptography services that are built in as part of the HTTPS mechanism. For that you need to generate a public key for the Prime Infrastructure web server, store it on the server, and then share it with the web client. This can be done using the standard PKI certificate mechanism which not only shares the web server public key with the web client, but also guarantees that the public key belongs to the web server (URL) you are accessing. This prevents any third party from posing as the web server and collecting sensitive information that the web client is sending to the web server.

These topics provide additional steps you can take to secure the web server:

- Cisco recommends that the Prime Infrastructure web server authenticate web clients using certificate-based authentication.
- To secure connectivity between a CLI client and the Prime Infrastructure CLI interface, refer to the security hardening procedures in Best Practices: Server Security Hardening.
- To secure connectivity between the Prime Infrastructure and systems such as AAA and external storage, refer to the recommendations in Best Practices: Server Security Hardening.

Set Up HTTPS Access to Prime Infrastructure

Prime Infrastructure supports secure HTTPS client access. HTTPS access requires that you apply a private key and corresponding 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 “Generate and Apply Self-Signed Certificates”.

- Digitally signed by a Certificate Authority (CA). CAs are organizations (like Cisco and VeriSign) that validate identities and issue certificates. 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 related topic "Import CA-Signed Host Certificates".

Note A private key and self-signed certificate with default parameters is generated at the timeof installation.

Related Topics

Generate and Apply Self-Signed Certificates, on page 18
Import CA-Signed Host Certificates, on page 18
Import Private Key, on page 21
Export Private Key, on page 21

Generate and Apply Self-Signed Certificates

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

Step 1 Start a CLI session with Prime Infrastructure (see How to Connect 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 Restart Prime Infrastructure Using CLI).

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.

Import CA-Signed Host 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 signed server certificates are host-specific. They are preserved in Prime Infrastructure backups, but are restored only if the backup and restore servers have the same host name.

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

Step 1 Start a CLI session with Prime Infrastructure using "admin" credentials and check the existing trusted certificates (see “How to Connect Via CLI”). Do not enter “configure terminal” mode.

PIServer/admin# **ncs key listcacerts**

where **listcacerts** is the command to list the existing trusted certificates.

Step 2 Go to the PI server location "**/opt/CSCOncs/migrate/restore**" and check the imported certificates using "root" CLI credentials.

Step 3 If certificates are found, delete the certificates through "admin" CLI credentials (see “Delete CA-Signed Certificates”). If no certificates are found, go to . Step 4 .

PIServer/admin# pi/admin# **ncs key deletecacert** <*certificate name*>

Restart Prime Infrastructure server after deleting the certificates.

Step 4 Enter the following command to generate a CSR file in the default backup repository:

PIServer/admin# **ncs key genkey -newdn -csr <csrfilename> repository <repositoryname>**

where -newdn— Generates a new RSA key and self-signed certificate with domain information.

-csr—Generates a new CSR certificate.

Csrfilename—CSR filename. It is an arbitrary name of your choice (for example: MyCertificate.csr).

repositoryname— file location. The file name can contain up to 80 alphanumeric characters.

Example:

PIServer/admin# ncs key genkey -newdn -csr CSRFile.csr repository <*repositoryname*>

The NCS server is running. Changes will take effect on the next server restart

Enter the fully qualified domain name of the server: **<FQDN>**

Enter the name of your organizational unit: **<organization>**

Enter the name of your organization: **<organization>**

Enter the name of your city or locality: **<city>**

Enter the name of your state or province: **<state>**

Enter the two letter code for your country: **<country code>**

Specify subject alternate names.

If none specified, CN will be used.

Use comma seperated list - DNS:<name>,IP:<address>

DNS:<FQDN>,IP:<IPADDRESS>

Specify the public key algorithm [rsa/ec] : **rsa**

Specify the RSA key size [2048/4096/8192] : **4096**

Specify the signature algorithm [sha256/sha512] : **sha256**

Key and CSR/Certificate will be generated with following details

Subject : /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=DNS:<FQDN>

Subject Alternate Name : DNS:<FQDN>,IP:<IPADDRESS>

Public Key Alg : rsa, 4096

Signature Alg : sha256

Continue [yes] : yes

Generating...

Completed...Changes will take affect on the next server restart

Important While generating CSR certificate through CLI, CSR name field accepts only characters and white space. It does not allow special characters and and numbers.

If you does not provide "Subject Alternate Name" - the CA certificate can be imported only in this machine.

If you provide "Subject Alternate Name" - You can import the CA certificate to be received from CA in any of the servers having the specified FQDN. To import CA certificate in SAN sepcified servers, you need to export private key from the server where you have generated the CSR and import the private key along with the signed certificate in other specified servers.

In SAN List, you should add the current server's FQDN.

Step 5 Send the CSR file to a Certificate Authority (CA) of your choice.

The CA will respond by sending you an signed server certificate and one or more CA certificate files. The CA response will indicate which of the files is:

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

  Combine all the certificates in to one single file by concatenating them. Host certificate should be the first one in the file followed by the CA certificates in the same order as in the chain.

  For example, in linux the following command can be used to combine files:

  cat host.pem subca.pem rootca.pem > servercert.pem

  Note Certificates should be in PEM format

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

PIServer/admin# **ncs key importcacert tomcat** <*certificate_name*> **repository** <*repositoryname*>

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

PIServer/admin# **ncs key importsignedcert <certificate_name> repository <repositoryname>**

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

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

Note If you want to import CA certiifcate to have secure connection between PI and External devices/server use below command:

PIServer/admin# **ncs key importcacert truststore {system | devicemgmt}alias <alias_name> <CA_certifcate_name> repository <repository_name>**

For more information, see How to Connect Via CLI and Restart Prime Infrastructure Using CLI.

Import Private Key

You can generate the private key and signed certificate externally. If you are generating them external, following command can be used to import both key and certificate together.

ncs key importkey <private_key_filename> <certificate_filename> repository <repository_name>

Export Private Key

The following is the command to export private key,

ncs key exportkey <private_key_filename> <certificate_filename> repository <repository_name>

After executing the above command private key will be generated and placed in the file location pointed in the repository.

Set Up Certificate Validation

During secure transactions like TLS/HTTPS connection, user authentication (when certificate based authentication is enabled), Prime Infrastructure will receive certificates from external entities. Prime Infrastructure needs to validate these certificate to ascertain the integrity of the certificate and the identity of the certificate holder. Certificate validation features allows the user to control how the certificates received from other entities are validated.

When the certificate validation is enforced, certificates received from other entities would be accepted by Prime Infrastructure only if that certificate is signed by certificate authority (CA) trusted by Prime Infrastructure. Trust store is where user can maintain the trusted CA certificates. If the signed certificate chain is not rooted to one of the CA certificates in the trust store, validation will fail.

Managing Trust Store

User can manage the trusted CAs in the trust store. Prime Infrastructure provides different trust stores namely – pubnet, system, devicemgmt and user.

- pubnet – Used while validating certificates received from remote hosts when connecting to servers in public network.
- system – Used while validating certificates received from remote systems when connecting to systems within network.
- devicemgmt – Used while validating certificates received from managed devices.
- user – Used to validate user certificates (When certificate based authentication is enabled).

CLIs to Manage Trust Store

The following is the CLI used to manage the trsut store.

- Importing a CA certificate to Trust Store, on page 22
- Viewing a CA Certificate in a Trust Store, on page 22
- Deleting a CA certificate from a trust store, on page 22

Importing a CA certificate to Trust Store

The following is the command to import CA certificate to a trust store:

- ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository <Repository-name> <certificate-file> truststore {devicemgmt | pubnet | system | user}

Viewing a CA Certificate in a Trust Store

The following is the command to view CA certificate in a trust store:

- ncs certvalidation trusted-ca-store listcacerts truststore {devicemgmt | pubnet | system | user}

Deleting a CA certificate from a trust store

The following is the command to delete CA certificate to a trust store:

- ncs certvalidation trusted-ca-store deletecacert alias <ALIAS> truststore {devicemgmt | pubnet | system | user}

Configuring Certificate Validation

User can configure the certificate validation for the following category:

- Enable certificate validation
- Disable certificate validation
- TOFU (Trust-on-first-use) - Trust stores are not used instead the certificate received from remote host is trusted when the connection is made for the first time. If the remote host sends a different certificate for any sub-sequent connection, connection will be rejected.

Enable certificate validation

The following is the command to enable to certificate validation:

- ncs certvalidation certificate-check trust-on-first-use trustzone {devicemgmt | pubnet | system | user}

View Certificate Validation List

The following is the command to view to certificate validation list:

- ncs certvalidation tofu-certs listcerts

Delete Certificate Validation

The following is the command to delete to certificate validation:

- ncs certvalidation tofu-certs deletecert host <host>

Auto Updating CA List

From time to time, Cisco releases a standard set of CA certificates recommended by Cisco. These trust stores can be configured automatically to update the CA list with Cisco trusted CA bundle during software update.

The following is the command to configure auto update CA list:

- ncs certvalidation trusted-ca-store auto-ca-update enable truststore {devicemgmt | pubnet | system | user}

Accessing Certificate Validation Page

Certificate generation is now possible through the Certificate Validation Page available on the UI. This lets you to generate, import or export CSR directly without using the admin CLI command.

To access the Certificate Validation page, navigate to:

The **Administration** > **Settings** > **Certificate** menu contains options to create, import and export certificates in Cisco Prime Infrastructure.

Trusted CAs and Settings:

The imported certificates and the categories are listed here.

- **System** - Communication that happens between PI and other server in system level can be enabled here.
- **Pubnet** - Communication that happens between PI and other server in pubnet level can be enabled here.
- **Device management** – Device management communication between PI and another server can be enabled here.
- **User** – User communication between PI and another server can be enabled here.

Certificate Validation: Details about the validation used when importing or exporting certificates can be selected here.

Pinned TOFU certificates

Lists all the TOFU certificates of other servers which communicates with PI server.

Custom OCSP Responder

Provides the validation details such as the issued date and expiry dates.

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 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.

Field Name and Object ID	Data Type	Prime Infrastructure Event/Alert field	Description
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.

Field Name and Object ID	Data Type	Prime Infrastructure Event/Alert field	Description
cWNotificationManagedObjectAddressType	InetAddressType	N/A	The type of Internet address by which the managed object is reachable. Possible values: 0—unknown 1—IPv4 2—IPv6 3—IPv4z 4—IPv6z 16—DNS Always set to “1” because Prime Infrastructure only supports IPv4 addresses.
cWNotificationManagedObjectAddress	InetAddress	getNode() value is used if present	getNode is populated for events and some alerts. If it is not null, then it is used for this field.
cWNotificationSourceDisplayName	OCTET STRING	sourceDisplayName field in alert/event.	This object represents the display name of the source of the notification.
cWNotificationDescription	OCTET STRING	Text - NmsEvent Message - NmsAlert	Alarm description string.

cWNotificationSeverity	INTEGER	severity - NmsEvent, NmsAlert	Severity of the alert/event:
			cleared(1)
			critical(3)
			major(4)
			minor(5)
			warning(6)
			info(7)

cWNotificationSpecialAttributes	OCTET STRING	All the attributes in alerts/events apart from the base alert/event class.	This object represents the specialized attributes in alerts like APAssociated, APDisassociated, RogueAPAlert, CoverageHoleAlert, and so on. The string is formatted in property=value pairs in CSV format.

Field Name and Object ID	Data Type	Prime Infrastructure Event/Alert field	Description
cWNotificationVirtualDomains	OCTET STRING	N/A	Virtual Domain of the object that caused the alarm. This field is empty for the current release.

Establish an SSH Session With the Prime Infrastructure Server

When you connect to the server, use SSH and log in as the admin user. (See User Interfaces, User Types, and How To Transition Between Them for more information.)

Step 1 Start your SSH session and log in as the Prime Infrastructure admin user.

- From the command line, enter the following, where *server-ip* is the Prime Infrastructure:

```
ssh admin server-ip
```

- Open an SSH client and log in as **admin**.

Note Users can now create and customize new algorithms to connect to SSH or PuTTY.

Step 2 Enter the admin password. The prompt will change to the following:

```
(admin)
```

To view a list of the operations the admin user can perform, enter **?** at the prompt.

To enter admin config mode, enter the following command (note the change in the prompt):

```
(admin) configure terminal
(config)
```

Set Up NTP on the Server

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the Prime Infrastructure server. Failure to manage NTP synchronizations across your network can result in anomalous results in Prime Infrastructure. This includes all Prime Infrastructure-related servers: Any remote FTP servers that you use for Prime Infrastructure backups, secondary Prime Infrastructure high-availability servers, and so on.

You specify the default and secondary NTP servers during Prime Infrastructure server installation. You can also use Prime Infrastructure's **ntp server** command to add to or change the list of NTP servers after installation.

Note Prime Infrastructure cannot be configured as an NTP server; it acts as an NTP client only. Up to three NTP servers are allowed.

Step 1 Log in to the Prime Infrastructure server as the admin user and enter config mode. See Establish an SSH Session With the Prime Infrastructure Server, on page 26.

Step 2 Set up the NTP server using one of the following commands.

For an unauthenticated NTP server setup:

```
ntp server ntp-server-IP
```

For an authenticated NTP server setup:

```
ntp server ntp-server-IP ntp-key-id ntp-type password
```

Where:

- *ntp-server-IP* is the IP address or hostname of the server providing the clock synchronization to the Prime Infrastructure server
- *ntp-key-id* is the md5 key ID md5 key of the authenticated NTP server
- *ntp-type* can be plain or hash
- *password* is the corresponding plain-text md5 password for the NTPv4 server

Set Up the Prime Infrastructure Proxy Server

Use this procedure to configure proxies for the server and, if configured, 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**, then choose **General** > **Account Settings**.

Step 2 Click the **Proxy** tab.

Step 3 Select the **Enable Proxy** check box and enter the required information about the server that has connectivity to Cisco.com and will act as the proxy.

Step 4 Select the **Authentication Proxy** check box and enter the proxy server’s user name and password.

Step 5 Click **Test Connectivity** to check the connection to the proxy server.

Step 6 Click **Save**.

Configure 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.

See the latest Prime Infrastructure Quick Start Guide for more information.

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 Restart Prime Infrastructure Using CLI).

Set Up the SMTP E-Mail Server

To enable Prime Infrastructure to send email notifications (for alarms, jobs, reports, and so forth), the system administrator must configure a primary SMTP email server (and, preferably, a secondary email server).

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Mail and Notification** > **Mail Server Configuration**.

Step 2 Under Primary SMTP Server, complete the Hostname/IP, User Name, Password, and Confirm Password fields as appropriate for the email server you want Prime Infrastructure to use. Enter the IP address of the physical server. and the Enter the hostname of the primary SMTP server.

Note You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.

Step 3 (Optional) Complete the same fields under Secondary SMTP Server. SMTP server username and password.

Step 4 Under Sender and Receivers, enter a legitimate email address for Prime Infrastructure.

Step 5 When you are finished, click **Save**.

Enable FTP/TFTP/SFTP Service on the Server

FTP/TFTP/SFTP is used to transfer files between the server and devices for device configuration and software image file management. These protocols are also used in high availability deployments to transfer files to a secondary server. These services are normally enabled by default. If you installed Prime Infrastructure in FIPS mode, they are disabled by default. If you use this page to enable these services, Prime Infrastructure will become non-compliant with FIPS.

SFTP is the secure version of the file transfer service and is used by default. FTP is the unsecured version of the file transfer service; TFTP is the simple, unsecured version of the service. If you want to use either FTP or TFTP, you must enable the service after adding the server.

Step 1 Configure Prime Infrastructure to use the FTP, TFTP, or SFTP server.

a) Choose **Administration** > **Servers** > **TFTP/FTP/SFTP Servers**.

b) From the **Select a command** drop-down list, choose **Add TFTP/FTP/SFTP Server**, then click **Go**.

- From the **Server Type** drop-down list, choose **FTP**, **TFTP**, **SFTP**, or **All**.
- Enter a user-defined name for the server.
- Enter the IP address of the server.

c) Click **Save**.

Step 2 If you want to use FTP or TFTP, enable it on the Prime Infrastructure server.

a) Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

b) Go to the FTP or TFTP area.

c) Click **Enable**.

d) Click **Save**.

Step 3 Restart Prime Infrastructure to apply your changes. See Stop and Restart Prime Infrastructure, on page 30.

Configure Stored Cisco.com Credentials

Prime Infrastructure stores only the username and not the password to log in to Cisco.com while performing the following tasks:

- Checks for product software updates
- Checks for device software image updates

To download the updates and open/review a support case, you are required to enter a password.

If these settings are not configured, Prime Infrastructure will prompt users for their credentials when they perform these tasks. To configure a global Cisco.com user name and password:

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Account Settings**.

Step 2 Under the **Cisco.com Credentials** tab, enter a user name and password, and click **Save**.

Create a Login Banner (Login Disclaimer)

When you have a message that you want to display to all users before they log in, create a login disclaimer. The text will be displayed on the GUI client login page below the login and password fields.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Login Disclaimer**.

Step 2 Enter (or edit) the login disclaimer text.

Note Carriage returns are ignored.

Your changes will take effect immediately.

Stop and Restart Prime Infrastructure

A Prime Infrastructure restart is needed in cases such as after a product software upgrade, log file setting changes, hanging secure port settings, compressing report files, changing service discovery settings, and, configuring LDAP settings. When you stop the Prime Infrastructure server, all user sessions are terminated.

To stop the server, open a CLI session with the server and enter:

```
ncs stop
```

To start or restart the server, open a CLI session with the server and enter:

```
ncs start
```

Configure Global SNMP Settings for Communication with Network Elements

The SNMP Settings page controls the how the server uses SNMP to reach and monitor devices. These settings will determine when a device is considered unreachable. Any changes you make on this page are applied globally and 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. You should update the prepopulated SNMP credential with your own SNMP information.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Network and Device** > **SNMP**.

Step 2 (Optional) Select the **Trace Display Values** check box to display mediation trace-level logging data values that are fetched using SNMP.

Step 3 Choose an algorithm from the **Backoff Algorithm** drop-down list.

- **Exponential**—Each SNMP try will wait twice as long as the previous try, starting with the specified timeout for the first try.
- **Constant**—Each SNMP try will wait the same length of time (timeout). This is useful on unreliable 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 If you do not want to use the timeout and retries specified by the device, configure the following parameters.

Note If switch port tracing is taking a long time to complete, reduce the Reachability Retries value.

- **Reachability Retries**—Enter the number of global retries.
- **Reachability Timeout**—Enter a global timeout.

Step 5 In the **Maximum VarBinds per Get PDU** and **Maximum VarBinds per Set PDU** fields, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. These fields enable you to make necessary changes when you have any failures associated to SNMP. For customers who have issues with PDU fragmentation in their network, the number can be reduced to 50, which typically eliminates the fragmentation.

Step 6 Optionally adjust the **Maximum Rows per Table**.

Step 7 Click **Save**.

Configure 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

View SNMP Credential Details, on page 32
Add SNMP Credentials, on page 33
Import SNMP Credentials, on page 34

View 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 “Add 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

Configure Global SNMP Settings, on page 31
Add SNMP Credentials, on page 33
Import SNMP Credentials, on page 34

Add 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

Configure Global SNMP Settings, on page 31
View SNMP Credential Details, on page 32
Import SNMP Credentials, on page 34

Import 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).

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

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_password,
snmpv3_privacy_type,snmpv3_privacy_password,network_mask 1.1.1.0,v2,private,user1,HMAC-MD5,
12345,DES,12345,255.255.255.0 2.2.2.0,v2,private,user1,HMAC-MD5,password3,DES,password4,
255.255.255.0 10.77.246.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
```

The first row of the file is mandatory, as it describes the column arrangement. The IP Address column is also mandatory. The CSV file can contain the following fields:

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

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

Step 2 Choose **Select a command** > Add SNMP Entries > Go.

Step 3 In the **Add Format Type** drop-down list, choose File.

Step 4 Click Browse to navigate to the CSV file you want to import and select it.

Step 5 Click OK to import the file.

If Prime Infrastructure can use the SNMP credential listed to access the switch, the switch is added for later use and appears in the Network Devices page accessible via **Configuration** > **Network** > **Network Devices**. If you manually add switches through the Network Devices page, switch port tracing uses the credentials from that page, not the ones listed in the SNMP Credentials page. If the manually added switch credentials have changed, you need to update them using the Network Devices pages.

Related Topics

Configure Global SNMP Settings, on page 31

View SNMP Credential Details, on page 32

Add SNMP Credentials, on page 33

Enable 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 the secions“Virtual Appliance Options” and “Understanding System Requirements” in the latest latest Cisco Prime Infrastructure Quick Start Guide.
- The Cisco Unified Computing System (UCS) Gen 2 physical appliance. For details, see the sections “Virtual Appliance Options” and “Understand System Requirements” in the latest Cisco Prime Infrastructure Quick Start Guide.
- Standard Prime Infrastructure virtual appliance. For details, see the secion "Prime Infrastructure Minimum Server Requirements" in the latest Cisco Prime Infrastructure Quick Start Guide.

Do not attempt to enable Compliance Services on Express, Express-Plus. 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 or Express-Plus 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 or Express-Plus, 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.

For details, see Virtual Appliance Options and Physical Appliance Options.

Configure 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**.

Configure 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 Directory

Note If you choose TFTP protocol, enter the relative path without a leading slash in the **Protocol Directory** field. If you leave the **Protocol Directory** field empty, the image transfer will use the default home directory of your external server.

Step 6 Click **Save**.

Add 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.

Manage 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 change the vendor display name for an existing OUI, add new OUIs to Prime Infrastructure and refresh the vendorMacs.xml file with new vendor OUI mappings and upload it to Prime Infrastructure.

Related Topics

Add a New Vendor OUI Mapping, on page 37

Upload an Updated Vendor OUI Mapping File, on page 38

Add 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**.

Upload 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.

For more information, see IEEE Registration Authority database.

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
```

Work With Server Internal SNMP Traps That Indicate System Problems

Prime Infrastructure generates internal SNMP traps that indicate potential problems with system components. This includes hardware component failures, high availability state changes, backup status, and so forth. The failure trap is generated as soon as the failure or state change is detected, and a clearing trap is generated if the failure corrects itself. For TCAs (high CPU, memory and disk utilization traps, and so forth), the trap is generated when the threshold is exceeded.

A complete list of server internal SNMP traps is provided in Cisco Prime Infrastructure Alarms, Events, and Supported SNMP Traps and Syslogs. Prime Infrastructure sends traps to notification destination on port 162. This port cannot be customized at present.

You can customize and manage these traps as described in the following topics:

- Customize Server Internal SNMP Traps and Forward the Traps, on page 39
- Troubleshoot Server Internal SNMP Traps, on page 40

Customize Server Internal SNMP Traps and Forward the Traps

You can customize server internal SNMP traps by adjusting their severity or (for TCAs) thresholds. You can also disable and enable the traps. You can find the server internal SNMP traps listed in *Cisco Evolved Programmable Network Manager Supported Alarms*.

Note Prime Infrastructure does not send SNMPv2 Inform or SNMPv3 notifications.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **System Event Configuration**.

Step 2 For each SNMP event you want to configure:

a) Click on the row for that event.

b) Set the **Event Severity** to Critical, Major, or Minor, as needed.

c) For the CPU, disk, memory utilization, and other hardware traps, Enter the **Threshold** percentage (from 1–99). These events will send the associated SNMP traps when the utilization exceeds the threshold limit. (You cannot set thresholds for events for which the threshold setting is shown as NA.) These events send traps whenever the associated failure is detected.

d) For backup threshold and certificate expiry (critical), enter the **Threshold** in days (from *x*–*y*, where *x* is the minimum number of days and *y* is the maximum number of days).

e) To control whether a trap is to generated or not, set the **Event Status**.

Step 3 In the **Other Settings**, enter the desired value for **Create and Clear Alarm Iteration**.

Step 4 To save all of your trap changes, click **Save** (below the table).

Step 5 If you want to configure receivers for the server internal SNMP traps, refer to the procedures in the following topics, depending on whether you want to send the information as an email or trap notification.

Troubleshoot Server Internal SNMP Traps

Cisco Prime Infrastructure Alarms, Events, and Supported SNMP Traps and Syslogs provides a complete list of server internal SNMP traps, their probable cause, and recommended actions to remedy the problem. If that document does not provide the information you need, follow this procedure to troubleshoot and get more information about Prime Infrastructure server issues.

Step 1 Ping the notification destination from the Prime Infrastructure server to ensure that there is connectivity between Prime Infrastructure and your management application.

Step 2 Check if any firewall ACL settings are blocking port 162, and open communications on that port if needed.

Step 3 Log in to Prime Infrastructure with a user ID that has Administrator privileges. Select **Administration > Logging** and download the log files. Then compare the activity recorded in these log files with the activity you are seeing in your management application:

- ncs_nbi.log: This is the log of all the northbound SNMP trap messages Prime Infrastructure has sent. Check for messages you have not received.
- ncs-# -# .log: This is the log of most other recent Prime Infrastructure activity. Check for hardware trap messages you have not received.
- hm-# -# .log: This is the log of all Health Monitor activity. Check for recent messages about High Availability state-changes and application-process failures that you have not received.

The messages you see in these logs should match the activity you see in your management application. If you find major differences, open a support case with Cisco Technical Assistance Center (TAC) and attach the suspect log files with your case. See Open a Cisco Support Case.

Set Up Defaults for Cisco Support Requests

By default, users can create Cisco support requests from different parts of the Prime Infrastructure GUI. If desired, you can configure the sender e-mail address and other e-mail characteristics. If you do not configure them, users can supply the information when they open a case.

If you do not want to allow users to create requests from the GUI client, you can disable that feature.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Account Settings**.

Step 2 Click the **Support Request** tab.

Step 3 Select the type of interaction you prefer:

- Enable interactions directly from the server—Specify this option to create the support case directly from the Prime Infrastructure server. E-Mails to the support provider are sent from the e-mail address associated with the Prime Infrastructure server or the e-mail address you specify.

- Interactions via client system only—Specify this option to download the information required for your support case to a client machine. You must then e-mail the downloaded support case details and information to the support provider.

Step 4 Select your technical support provider:

- Click **Cisco** to open a support case with Cisco Technical Support, enter your Cisco.com credentials, then click **Test Connectivity** to check the connectivity to the following servers:
  - Prime Infrastructure mail server
  - Cisco support server
  - Forum server
- Click **Third-party Support Provider** to create a service request with a third-party support provider. Enter the provider's e-mail address, the subject line, and the website URL.

Configure Cisco Product Feedback Settings

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.

This feature is enabled by default. Data is collected on a daily, weekly, and monthly basis and is posted to a REST URL in the Cisco cloud using HTTPS. Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Help Us Improve**, and:

- To view the types of data Cisco collects, click **What data is Cisco collecting?**
- To disable this feature, select **Not at this time, thank you**, then click **Save**.

Note If you have 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 server).