APPENDIX B

Troubleshooting and FAQs

This section provides the following information for the Administration module of LMS:

- Troubleshooting Guidelines
- Frequently Asked Questions

Troubleshooting Guidelines

This section provides guidelines on the following:

- Troubleshooting User Tracking
- Troubleshooting the Cisco Prime LMS Server

Troubleshooting User Tracking

Use the information in Table B-1 to troubleshoot the User Tracking application.

Table B-1 Troubleshooting User Tracking

Symptom	Probable Cause	Possible Solution
User Tracking cannot discover any users or hosts or User Tracking cannot display any IP phones.	There may not be information in the LMS database. The device might not be part of DCR and you must run Device Discovery and Data Collection.	For more details, see • Discovering Devices in *Inventory Management with Cisco Prime LAN Management Solution 4.1* • Administering Data Collection
User Tracking cannot discover certain users or hosts.	The LMS server might not have discovered one or more devices to which users and hosts are connected.	1. Check the Cisco Prime topology for the missing devices 2. Ensure that CDP and SNMP are enabled on the devices, rediscover these devices, 3. Verify that they appear on the topology view.

Table B-1 Troubleshooting User Tracking (continued)

Symptom	Probable Cause	Possible Solution
User Tracking cannot discover certain IP phones.	The LMS server might not have discovered the specific Media Convergence Server (MCS) that runs the instance of Cisco CallManager to which the IP phones are registered.	1. Check the Cisco Prime topology for the missing MCS that runs the instance of Cisco CallManager to which the phones are registered. 2. Ensure that Cisco CallManager is shown as a service running on the MCS and is discovered by the LMS Server. 3. Rediscover all IP phones.
User Tracking table does not contain device name, IP address, and subnet information for some hosts.	User Tracking cannot find the most recent network information. Network changes are not currently reflected in ARP information (routers) or bridge tables (switches). User Tracking does not perform Ping Sweep on large subnets; for example, subnets containing Class A and B addresses. Hence, ARP cache might not have some IP addresses and the User Tracking may not display the IP addresses. In larger subnets, the ping process leads to numerous ping responses that might increase the traffic on your network and result in extensive use of network resources.	Enable Ping Sweeps when User Tracking performs Discovery. Ping Sweeps are enabled by default. To perform Ping Sweep on larger subnets, you can either: • Configure a higher value for the ARP cache time-out on the routers. To configure the value, you must use the arp time-out interface configuration command on devices running Cisco IOS. Or • Use any external software, which will enable you to ping the host IP addresses. This will ensure that when you run User Tracking Acquisition, the ARP cache of the router contains the IP addresses.
You have: • Made changes to the network. • Run User Tracking Major Acquisition. The changes do not appear in the User Tracking display.	A complete Device Discovery process has not run since you added your changes. User Tracking Major Acquisition is not a full network discovery. The process discovers only the user and host data in your network. Changes that you make to your network might not appear after a User Tracking Major Acquisition.	1. Run Device Discovery. 2. Run a complete Data collection. 3. Generate a new report after data collection is complete to see the changes.

Troubleshooting the Cisco Prime LMS Server

Use these tools and suggestions to diagnose problems with the Cisco Prime LMS server:

- Verifying Server Status
- Troubleshooting Suggestions

Verifying Server Status

There are several tools that enable you to gather and analyze information about your Cisco Prime LMS Server. See Table B-2 and Table B-4.

Table B-2 Server Status

Task	Purpose	Action
Administrative Tasks		
Perform self test.	Runs self-tests and generates a report with the results.	Select **Admin > System > Server Monitoring > Selftest**.
All Users		
Check process status.	Checks whether back-end processes are in an interim state.	Select **Admin > System > Server Monitoring > Processes**.
Collect server information.	Provides system information, environment, configuration, logs, and web server information.	Select **Admin > System > Server Monitoring > Collect Server Information** Or Enter the following command: • *NMSROOT*`\bin\perl` *NMSROOT*`\bin\collect.info` (on Windows) • *NMSROOT*`/bin/perl` *NMSROOT*`/bin/collect.info` (on Solaris/Soft Appliance) where *NMSROOT* is the directory where you installed Cisco Prime.

Table B-2 Server Status

Task	Purpose	Action
MDC Support	The MDC Support utility collects: • Log files • Configuration settings • Memory information • Complete system related information • Process status • Host environment information It also collects any other relevant data, into a deliverable tar (compressed form) file to support the MDCs installed. The MDC Support utility also queries CCR for any other support utilities registered, and run them. Other MDCs need to register their own support utilities that will collect their relevant data.	For Windows go to, *NMSROOT*\MDC\bin and run the command: **`MDCSupport.exe`** The utility creates a tar file in *NMSROOT*\MDC\etc directory. If \etc directory is full, or if you want to preserve the data collected previously by not over writing the tar file, you may create another directory by running the following command: **`MDCSupport.exe`** *Directory* For Solaris/Soft Appliance, 1. Set the *LD_LIBRARY_PATH* environment variable to /opt/CSCOpx/MDC/lib: /opt/CSCOpx/lib: 2. Go to /opt/CSCOpx/MDC/bin and run the command: **`./mdcsupport`** The utility creates a tar file in CSCOpx/MDC/etc directory. If \etc directory is full, or if you want to preserve the data collected previously by not over writing the tar file, create another directory by running the following command: **`./mdcsupport`** *Directory* Before you close the command window, ensure that the MDC Support utility has completed its action. If you close the window prematurely, the subsequent instances of MDCSupport Utility will not function properly. If you happen to close the window, delete the mdcsupporttemp directory from *NMSROOT*\MDC\etc *directory*, for subsequent instances to work properly.

Troubleshooting Suggestions

Use the suggestions in Table B-3 to resolve errors or other problems with the Cisco Prime LMS Server.

Table B-3 Troubleshooting Suggestions

Symptom	Probable Cause	Possible Solutions
`Authorization required. Please log in with your username and password.`	Incompatible browser causing cookie failure (unable to retrieve cookie).	Verify that you have **Accept all cookies** enabled. Refer to the installation documentation for supported Internet Explorer and Mozilla Firefox software and setup procedures.
`Daemon Manager could not start. The port is in use.`	The operating system has not yet reallocated the port.	Make sure all Cisco Prime processes are terminated (**/usr/ucb/ps -auxww | grep CSCO**). Wait five to ten minutes, then try to restart the Daemon Manager.
User has forgotten his password.	LMS cannot recover forgotten passwords.	A system administrator-level user must either change the password or delete the user account and add it again.
You are logged out of the Cisco Prime Server.	Changes in the login module configuration file might not be correct. Authentication server might be down and there were no fallback logins set.	1. Log into Cisco Prime LMS Server. 2. Enter the following commands: – *NMSROOT*`\bin\perl` *NMSROOT*`\bin\ResetLoginModule.pl` (on Windows) – *NMSROOT*`/bin/perl` *NMSROOT*`/bin/ResetLoginModule.pl` (on Solaris/Soft Appliance) 3. Restart Daemon Manager.
The Log File Status window displays files that exceed their limit.	Files need to be backed up so that file size will be reset to zero.	1. Stop all processes. 2. Enter the log file maintenance commands: – *NMSROOT*`\cgi-bin\admin\` (on Windows) – *NMSROOT*`/cgi-bin/admin/` (on Solaris/Soft Appliance) 3. Restart all processes.
Error message in the logfile: `Connection Refused. Check the Device is SSH supported or not.`	Device is not SSH enabled or the server is not authorized to initiate SSH connection.	1. Check whether the device is up or not. 2. Try connecting to the device with a commercial SSH client. If you are able to connect, go to step 3. If you are not able to connect, check whether the device is running SSH enabled (K2 or K9) image. • If it is not the correct image, download the appropriate image to the device. • If you have the correct image, check whether you have created RSA key pairs in the device. Creating RSA keys will enable SSH in the device. 3. Check whether your server or network is authorized to initiate SSH connections to device.

Table B-3 Troubleshooting Suggestions (continued)

Symptom	Probable Cause	Possible Solutions
While launching the Group Administration page, the following error message is displayed: `Error in communicating with Group Administration Server.`	The Group Administration server is either not running or yet to be up.	Start the Group Administration server from the user interface or from the CLI. To start the server from the user interface: 1. Select **Admin > System > Server Monitoring > Processes**. The Process Management Dialog Box appears. 2. Check the CMFOGSServer check box in the Process Management dialog box 3. Click **Start**. To start the server from the CLI, enter: *NMSROOT*`/bin/pdexec CMFOGSServer` where *NMSROOT* is the Cisco Prime LMS Installation directory.
DCRServer is down and services are not starting properly.	Check wheter ctm_config.txt file is corrupted.	Make sure the following two files have proper content by checking the contents with the sample ctm_config.txt: • /NMSROOT/MDC/tomcat/shared/lib/ctm_config.txt • /NMSROOT/MDC/tomcat/webapps/cwhp/WEB-INF/lib/ctm_config.txt where *NMSROOT* is the Cisco Prime LMS Installation directory. **Sample ctm_config.txt** *SERVER_PORT=40050* *MAX_VM_PORTS=20* *MAX_THREADS=100* *CTM_SSL=1* *CTM_URL=:443/cwhp/CTMServlet* *MAX_VM_CLIENT_CONNECTION=25* *REGISTRY_LOCATION=NMSROOT\\MDC\\tomcat\\webapps\\cwhp\\WEB-INF\\lib*

See *Installing and Migrating to Cisco Prime LAN Management Solution 4.1* for troubleshooting tips on Cisco Prime installation.

Frequently Asked Questions

This section provides FAQs on the following:

- User Tracking FAQs
- VRF Lite FAQs
- Cisco Prime LMS Server FAQs
- Fault Management FAQs

User Tracking FAQs

This section lists the FAQs on User Tracking:

Q. Why are outdated entries appearing in my User Tracking table?

A. Outdated entries result when:

- A user or host is assigned to new VLAN/port/VTP domain.
- A power failure occurred.
- A workstation has been switched off or removed from the network.

User Tracking does not automatically delete outdated end-user host entries. To delete these entries:

- Manually delete selected entries.

  Or

- Configure delete interval for purging old records more than the given number of days.
- Select **Admin > Network > Purge Settings > User Tracking Purge Policy**

Q. How does User Tracking acquisition process differ from that of the LMS Server?

A. User Tracking is a LMS client application. The LMS Server provides several types of global discoveries, including:

- Device and physical topology acquisition, resulting in baseline network information such as device identity, module and port information, and physical topology. This type of acquisition is required for logical, user, and path acquisition.
- User acquisition, resulting in information about users and hosts on the network.

The LMS Server stores this information in the database. User Tracking discovers the host and user information in the LMS server database, correlates this information, and displays it in the User Tracking Reports.

For more information about the various acquisition processes, see Various Acquisitions in User Tracking.

Q. How does User Tracking user and host acquisition process work?

A. Before collecting user and host information, LMS must complete Data Collection. After the completion of Data Collection User Tracking performs steps described in Table B-4.

Table B-4 User Tracking User and Host Acquisition Process

Process	Description
Performs Ping Sweeps	Pings all IP addresses on all known subnets, if you have Ping Sweeps enabled (the default). This process updates the switch and router tables before User Tracking reads those tables. This ensures that User Tracking displays the most recent information about users and hosts.
Obtains MAC addresses from switches	Reads the switch's bridge forwarding table. The bridge forwarding table provides the MAC addresses of end stations, and maps these MAC addresses to the switch port on which each workstation resides.
Obtains IP and MAC addresses from routers	Reads the Address Resolution Protocol (ARP) table in routers to obtain the IP and corresponding MAC addresses.
Obtains hostnames	Performs a Domain Name Service (DNS) lookup to obtain the hostname for every IP address.
Obtains usernames	Attempts to locate the users currently logged in to the hosts and tries to obtain their username or login ID.
Records discovered information	Records the discovered information in the LMS database.

Q. Why is User Tracking not performing Ping Sweeps on some subnets?

A. The criterion for whether or not User Tracking performs Ping Sweeps on a subnet is the number of hosts in the subnet:

You must check if you have excluded the subnets from Ping Sweep.

If a subnet has 256 or fewer hosts, User Tracking performs Ping Sweeps on that subnet. User Tracking does not perform Ping Sweeps on the subnets, which have more than 256 hosts.

If Ping Sweeps are not performed, User Tracking still obtains information from the router and switch mapping tables during a discovery. For more details on Ping Sweep, see Notes on Ping Sweep Option.

Q. How long does User Tracking maintain data?

A. It depends on the delete interval you have set. For more details, see Deleting User Tracking Purge Policy Details.

Q. Does User Tracking discover users and hosts connected to non-Cisco Discovery Protocol (CDP) devices?

A. LMS does not manage non-CDP devices. Hence User Tracking will not discover users and hosts in the network connected to non-CDP devices.

Q. Where does User Tracking log errors?

A. User Tracking major acquisition errors are logged in the User Tracking error log. Data Collection errors are logged in the respective log file. The log files are located at
Solaris/Soft Appliance : /var/adm/CSCOpx/log
Windows: *NMSROOT*\log
Where *NMSROOT* is the directory where you have installed Cisco Prime.

Q. Why am I getting a parse error when trying to parse some of the output files?

A. A few classes in Optical switches contain special characters with ASCII code higher than 160. Most of the XML parsers do not support these characters and hence fail to parse them.

To overcome this, you have to manually search for those elements with special characters and append CDATA as given in the example below:

If there is an element

```
<checksum> ¢Úo </checksum>
```

Change it to:

```
<checksum> <![CDATA[¢Úo ]]> </checksum>
```

VRF Lite FAQs

This section lists the FAQs on VRF Lite:

Q. What is VRF Lite ?

A. Virtual Routing and Forwarding Lite (VRF Lite) is the one of the simplest form of implementing virtualization technology in an Enterprise network. A Virtual Routing and Forwarding is defined as VPN routing/forwarding instance. A VRF Lite consists of an IP Routing table, a derived forwarding table, a set of interfaces that use the forwarding table and set of routing protocols that determine what goes into the forwarding table. VRF Lite is an application that allows you to pre-provision, provision and monitor Virtual Routing and Forwarding-Lite (VRF Lite) technology on an enterprise network.

Q. What is Network Virtualization?

A. Virtualization deals with extending a traditional IP routing to a technology that helps companies utilize network resources more effectively and efficiently. Using virtualization, a single physical network can be logically segmented into many logical networks. The virtualization technology supports multiple virtual routing instances of a routing table to exist within a single routing device and work simultaneously.

Q. What are the pre-requisites to manage a device using VRF Lite?

A. The pre-requisites to manage a device in VRF Lite are:

1. The device must be managed by LMS.
2. The device must either be L2/L3 or L3 device
3. The devices failing to satisfy pre-requisite # 1 or #2, are not displayed in VRF Lite.

   The device must have the necessary hardware support. For more information on hardware support, see http://www.cisco.com/en/US/products/sw/cscowork/ps563/products_device_support_tables_list.html.

   If the device hardware is not supported then the device will be classified as Other devices
4. If a device supports MPLS VPN MIB, it is classified as a capable device.
5. VTP Server must be support MPLS VPN MIB. If the VTP Server does not support MPLS VPN MIB, VRF Lite will not manage VTP Clients.

Q. The device must be managed by LMS to exercise all the functionality of VRF Lite. The desired device is not listed in the device selector for the VRF Lite configuration workflows. What is the reason for a device not listed in the device selector?

A. A device is not listed in the device selector due to the following reasons:

All VRF Lite Configuration workflows like Create, Edit, Extend, Delete VRF Lite and Edge VLAN Configuration.

A device will not be listed in the Device Selector, if a device does not satisfy the pre-requisites as mentioned in the *Configuring Virtual Routing and Forwarding (VRF)* in *Configuration Management with Cisco Prime LAN Management Solution 4.1*.

If VRF Lite Configuration workflow is either Edit VRF Lite, or Delete VRF Lite or Edge VLAN Configuration then a device will not be listed in the Device Selector, if a device is not participating in the selected VRF Lite.

In the Readiness Report, a device listed as a supported device may be because it is not managed by LMS. You can check if a device is managed by using the Device Management State Summary (**Inventory > Device Administration > Manage Device State**).

In Extend VRF Lite workflow, the devices listed in the Device Selector are the devices that are not participating in the selected VRF Lite.

In Edge VLAN Configuration workflow, the devices listed in the Device Selector are only L2/L3 devices that are not participating in the selected VRF Lite.

Q. What are the different categories in which the devices are managed by Virtual Network Manager? Or what criteria are used by Virtual Network Manager to categorize the devices in the network?

A. Virtual Network Manager identifies the devices based on the minimum hardware and software support required to configure VRF Lite on the devices.

Based on the available hardware and software support in the devices, Virtual Network Manager classifies the devices into following categories:

- VRF Lite Supported Devices– Represents the devices with required hardware and software support available to configure VRF Lite on the devices.
- VRF Lite Capable Devices – Represents the devices with required hardware support available. But the device software must be upgraded to support MPLS VPN MIB. For information on the IOS version that supports MPLS VPN MIB, refer http://tools.cisco.com/ITDIT/MIBS/MainServlet.

  VRF Lite classifies all the devices from Cat 3k and Cat 4k family of devices as VRF Lite Capable devices as these devices do not have the required MPLS VPN MIB support.
- Other – Represents the devices without required hardware support to configure VRF Lite. SysOID of the device needs to be checked.

Q. Sometimes, while performing VRF Lite configuration, I get the following message:

The device(s) with display name(s) are already locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time Or Ensure the devices are not used by configuration workflows and free the devices from **Admin > Network > Resource Browser**.

Or

Selected Device(s) are locked as they are used by configuration workflows. You cannot configure these devices. Wait for some time OR Ensure the devices are not used by configuration workflows and free the devices from **Admin > Network > Resource Browser**.

Can I get the details of the user who has locked the devices to perform VRF Lite configuration?

A. You cannot get the details of user who has locked the devices to perform VRF Lite configurations.

Q. What are the details of the VRF Lite log files? In which location are the VRF Lite log files located?

A. The following are the details of the VRF Lite log files:

1. Vnmserver.log – This log file logs the messages pertaining to the VRF Lite Server process.
2. Vnmcollector.log – This log file logs the messages pertaining to the VRF Lite collection.
3. Vnmclient.log – This log file logs the messages related to the User Interface.
4. Vnmutils.log – This log file logs the messages pertaining to the utility classes used by VRF Lite client and server.

The above-mentioned VRF Lite log files are located in the following location:

In Solaris/Soft Appliance : /var/adm/CSCOpx/log/

In Windows: NMSROOT\logs

Q. When is the VRF Lite Collection process triggered?

A. **Manually:**

You can manually schedule to run the VRF Lite Collection process by:

Providing the setting details using **Admin > Collection Settings > VRF Lite > VRF Lite Collector Schedule** option.

Automatically:

If you enable the **Run VRF Lite Collector After Every Data Collection** in the VRF Lite Collector Schedule page. The VRF Lite Collection process will be automatically triggered after the completion of Data Collection.

You can reach the VRF Lite Collector Schedule page using **Admin > Collection Settings > VRF Lite > VRF Lite Collection Settings** page.

Q. After the completion of the Data collection process, the VRF Lite Collector failed to run, What is the reason for failure?

A. Check if the **Run VRF Lite Collector After Every Data Collection** option is enabled in the VRF Lite Collector Schedule page. You can reach the VRF Lite Collector Schedule page from **Admin > Network > VRF Lite Collection Settings** page.

Q. How can I configure SNMP timeout and retries details for VRF Lite?

A. The SNMP timeout and retries details are configured using **Admin > Collection Settings > VRF Lite > VRF Lite SNMP Timeouts and Retries**. By default, all the devices have a timeout of six seconds and retry attempt of 1 second.

Q. What is the reason for VLANs not getting populated in the VLAN to VRF Lite Mapping page in the Create VRF Lite and Extend VRF Lite workflows ?

A. The VLAN to VRF Lite Mapping page lists the links connecting the source and the destination device. The VLANs are not listed in fields displaying the links in the VLAN to VRF Lite Mapping page because VRF Lite tries to find a free VLAN in the devices connected using a link based on the following procedure

1. An SVI, VRF Lite searches for free VLANs in the range 1- 1005
2. An SI, VRF Lite searches for free VLANs in the range 1006-4005

Q. How do I enable the debug messages for Virtual Network Manager?

A. You can enable the debugging levels for a particular module using

- **Admin > System > Debug Settings > VRF Lite Client Debugging Options.**
- **Admin > System > Debug Settings > VRF Lite Collector Debugging**
- **Admin > System > Debug Settings > VRF Lite Server Debugging**
- **Admin > System > Debug Settings > VRF Lite Utility Debugging**

You can manually change the name and the size of the log file. The configuration log files are available under NMSROOT/MDC/tomcat/webapps/vnm/WEB-INF/classes. The changes made will be reflected after approximately 60 seconds.

Q. Why are some port-channels not discovered in VRF Lite?

A. VRF Lite does not support port-channel and GRE Tunnel. Also, Currently VRF Lite supports only 802.1Q

Q. What are the processes newly introduced for VRF Lite ?

A. To run VRF Lite , VRF Lite Server process is newly introduced in the application. The VRF Lite Collector process is executed as a Job.

Q. What is tested number of devices support in VRF Lite?

A. In an Enterprise network, VRF Lite is tested to support the configuration of 32 VRFs with VRF Lite configuration supported in 550 devices in your network. However, at a given time, you can select up to 20 devices and configure VRF Lite using the Create, Edit and Extend VRF Lite workflow.

Q. What are the property files associated with VRF Lite?

A. The following property files are associated with VRF Lite:

1. NMSROOT/vnm/conf/VNMClient.properties – This property file is used to provide the settings for Purge and Home page auto Refresh
2. NMSROOT/vnm/conf/VNMServer.properties – This property file is used to provide the SNMP and VRF Lite Server settings.
3. NMSROOT/vnm/conf/VRFCollectorSnmp.conf – This property file stores the SNMP Timeout and Retries that you have configured.

Q. In the Interface to VRF Lite Mapping page for the Create, Edit and Extend VRF Lite workflow, why are values for the IP Address and SubnetMask fields empty?

A. If the physical interface that links two devices is not configured with an IP Address, then the IP Address and the SubnetMask fields are empty.

Q. What is protocol order for configuration workflows?

A. Configuration workflow uses the protocol order similar to ordering used by NetConfig in Resource Manager Essentials.

Choose the NetConfig as Application Name from using **Admin > Collection Settings > Config > Config Transport Settings** page. You can view the protocol ordering in the Transport Settings page.

Q. What is protocol ordering for troubleshooting?

A. Troubleshooting VRF Lite workflow uses the protocol ordering similar to ordering used by NetShow in Resource Manager Essentials.

Choose the NetShow as Application Name from using **Admin > Collection Settings > Config > Config Transport Settings** page. You can view the protocol ordering in the Transport Settings page.

Q. If you configure commands to be deployed to two different devices, will the commands be deployed parallelly or serially?

A. The commands will be deployed to multiple devices parallelly, where as a series of commands with-in a single device, will be deployed in serial manner.

Q. Which VRF Lite configuration jobs that are failed can be retried?

A. You can retry all the VRF Lite Configuration jobs which are failed. VRF Lite Configuration jobs are the jobs pertaining to Create, Edit, Extend, Delete VRF Lite and Edge VLAN Configuration workflow.

Q. Why is the Monitor Real Time button disabled in the Ping or Traceroute VRF Lite page?

A. The functionality for Monitor Real Time button is provided by IPSLA Performance Management. This button is enabled only when IPSLA Performance Management is enabled in the local server.

Q. Why the FHRP and DHCP configurations are not shown in VRF Lite?

A. VRF Lite does not fetch the details for the FHRP or DHCP configuration from the device. Also, VRF Lite won't put the list of VLANs allowed on a trunk

The Protocols and DHCP Server details for existing or newly created SVIs are not fetched from the selected devices.

Cisco Prime LMS Server FAQs

The following sections lists the Frequently Asked Questions (FAQs) of Cisco Prime LMS application.

General

The section lists you the general FAQs on LMS:

Q. How do I change the IP address of the Cisco Prime LMS Server after installing it, or after running it for a while?

A. You can change the IP address on the server, and then access it using the new IP address.

To change the IP address on Windows:

Step 1 Click **Start > Settings > Network and Dial-up Connections > Local Area Connection**.

The Local Area Connection Status dialog box appears.

Step 2 Click **Properties**.

The Local Area Connection Properties dialog box appears.

Step 3 Select Internet Protocol (TCP/IP) and click **Properties**.

The Internet Protocol (TCP/IP) Properties dialog box appears.

Step 4 Select the radio button **Use the following IP address**.

Step 5 Change the IP address as required, in the IP address field.

For the subnet mask and default gateway values, enter the `ipconfig` command at the command prompt.

The subnet mask and default gateway values appear.

Step 6 Enter these values in the Subnet mask and Default gateway fields.

Step 7 Click **OK** to go back to Local Area Connection Status dialog box.

Step 8 Click **OK.**

Step 9 Restart the server.

To change the IP address on Solaris, use the command ifconfig at the command prompt to change the IP address of the required interface.

For example, at the command prompt, you can enter:

`ifconfig` *interfacename* `inet` *ipv4address*

where the variable *interfacename* represents the name of the interface and *ipv4address* represents the new IP address.

Q. Why do I get the Java Script Not Enabled error after logging into Cisco Prime?

A. This could be because Java Script is disabled in Internet Explorer. You should enable it in IE.

To do so:

Step 1 Launch Internet Explorer and click **Tools > Internet Options**.

Step 2 Click the Security tab and select **Trusted Sites.**

Step 3 Add the Cisco Prime LMS Server to the trusted zone.

Step 4 Clear the selection in **Require server verification for all sites in this zone**.

Step 5 Click **OK** to return to the Security tab.

Step 6 Click the Custom level button from the Security level for this zone panel.

Step 7 Select the Enable option for scripting of Java applets.

Step 8 Click **OK** to return to the Security tab.

Step 9 Click **Apply**.

Q. In IE 7.0 and IE 8.0, an error message appears when I choose the Telnet option in some portlets?

A. In Microsoft Internet Explorer 7.0 and 8.0 browsers, the Telnet protocol handler is disabled by default. To re-enable the Telnet protocol:

Step 1 Click **Start > Run**. The Run dialog box opens.

Step 2 In the Open box, enter: Regedit, then click **OK**. The Registry Editor opens.

Step 3 Go to the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl.

Step 4 Under the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl**, create a new key named **FEATURE_DISABLE_TELNET_PROTOCOL**.

Step 5 Add a DWORD value named iexplore.exe and set the value to 0 (decimal).

Step 6 Close the Registry Editor.

Step 7 Restart the browser, the Telnet protocol is enabled

Q. What are the specific ports required for Internet HTTP features?

A. Only port number 80 is required for all HTTP interactions between Cisco Prime LMS Server and Cisco.com, including the Software Center interactions.

Q. Why is the display name not available in the home page after importing?

A. The probable causes for this problem could be:

- There is a mismatch between the hostname in the template imported and the hostname specified in the UI during importing.
- The application imported from a remote server does not belong to the server from which it is imported.

Q. How do you ensure to register using a template and launch the links properly?

A. Before you register through a template, you should ensure that:

- The host is reachable.
- Port information specified is correct and reflects the current port of the bundle.
- The application is available and can be launched by entering the application URL in the browser.

Q. Which version of the Java Plug-in should I use for Cisco Prime to function properly?

A. Cisco Prime supports Java Plug-in 1.6.0_19 in all the supported clients and operating systems. We recommend that you do not install any other plug-ins other than this one, for Cisco Prime to function properly.

Q. Why cannot I start my Cisco Prime application?

A. If you cannot start your Cisco Prime application and see error messages, it may be because the web server may not be running. This may occur although **pdshow** indicates that those processes are running. You need to check how your machine resolves its server name and IP address.

The Cisco Prime CORBA applications require name resolution to work properly. Domain Name Service (DNS) is mandatory for Cisco Prime CORBA applications to work properly.

Configure the name resolution mechanism and restart the Cisco Prime LMS Server to access the application correctly.

Q. Why am I unable to launch Cisco Prime from a Windows 2008 client machine?

A. This is caused by the default security settings in the browsers. Sometimes, the META-REFRESH tag is disabled in the browser.

To enable the META-REFRESH tag in the browser:

Step 1 Click **Tools > Internet Options**. The Internet Options dialog box opens.

Step 2 Click the Security tab.

Step 3 Select the Internet zone.

Step 4 Click **Custom level..**. The Security Settings dialog box opens.

Step 5 In the Miscellaneous options, select the **Enable** option for Allow Meta Refresh field.

Step 6 Click **OK**, and then **Apply** to update the settings.

Step 7 Close the IE 7 or IE 8 open windows.

Step 8 Launch a new IE 7 or IE 8 window and login into LMS.

Q. I am locked out of the Cisco Prime LMS Server. Why did this happen, and how do I regain access?

A. There are several reasons why you are locked out. It is probably caused by the changes made using the Select Login Module option. You must replace the incorrect login module with a default configuration, log into Cisco Prime, and return to the login module to correct one or more of the following:

- Session Time out
- Change from SSL mode to non-SSL mode
- Change from non-SSL mode to SSL mode
- Log out from any other Cisco Prime application
- Visit other sites and then return to Cisco Prime

Do *not* alter the existing technologies in the default configuration file.

If all of the parameters listed are correct, see Troubleshooting Suggestions.

Q. Do I need to change the Cisco Prime configuration after changing the IP address?

A. You need not change the Cisco Prime configuration whenever you change the IP address. Cisco Prime uses hostname for most of the communication. Only devices need to point to the new IP address. However, after changing the IP address, you must reboot the system on a Solaris server and restart the Daemon Manager on a Windows server. This is to make the changes effective.

Q. How do I change the hostname of the Cisco Prime LMS Server after installing it, or after running it for a while?

A. To change the hostname of the Cisco Prime LMS Server, you need to update several files and windows registry entries.

You can use the hostnamechange.pl CLI utility to update the new host name information in files and windows registry entries.

See Using LMS Server Hostname Change Scripts for more information.

Q. How do I change the port for osagent in Windows?

A. Before you change the port for osagent in Windows:

- Ensure that the daemons are not running.

  Enter the following command to stop the Daemon Manager:

  ```
  net stop crmdmgtd
  ```

- Backup your Windows registry.

To change the port for osagent in Windows, run the following script at the command prompt:

NMSROOT`\bin\perl` *NMSROOT*`\bin\ChangeOSAGENTPort.pl` *Port_Number*

where, *Port_Number* refers to any unused port number between 1026 to 65535.

The script completes the following:

- Updates the value of the following registry entries with the new port numbers.
  - **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Resource Manager > Current Version > Daemon > RmeOrb**
  - **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Resource Manager > Current Version > Daemon > RmeGatekeeper**
  - **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Resource Manager > Current Version > Environment**
- Changes the value of the port number to new port number in NameServer and NameServiceMonitor processes.
- Changes the value of OSAGENT_PORT and PX_OSA_PORT port numbers in the md.properties file with the new port numbers.

Reboot the server and start the Daemon Manager after you have completed running the script.

Q. How do I change port for osagent in Solaris?

A. Before you change the port for osagent in Solaris:

- Ensure that the daemons are not running.

  Enter the following command to stop the Daemon Manager:

  ```
  /etc/init.d/dmgtd stop
  ```

- Make sure that no CSCO processes are running.
- Back up *NMSROOT*/objects/dmgt/dmgtd.conf file.

To change the port for osagent in Solaris, run the following script at the command prompt:

NMSROOT`/bin/perl` *NMSROOT*`/bin/ChangeOSAGENTPort.pl` *Port_Number*

where, *Port_Number* refers to any unused port number between 1026 to 65535.

The script completes the following:

- Changes the value of the port number to new port number in NameServer and NameServiceMonitor processes.
- Changes the value of OSAGENT_PORT and PX_OSA_PORT port numbers in the md.properties file with the new port numbers.
- Updates the new port number in /etc/services file.
- Updates the entry in /var/sadm/pkg/CSCOmd/pkginfo file.

Reboot the server and start the Daemon Manager after you have completed running the scripts.

Q. How do I ensure that jrm is running fine?

A. To check whether jrm is working on Windows, at the command prompt enter:

cwjava -cw *NMSROOT* **com.cisco.nm.cmf.jrm.jobcli**

To check whether jrm is working on Solaris, at the command prompt enter:

cwjava -cw *NMSROOT* **com.cisco.nm.cmf.jrm.jobcli**

- If you get a message `Established connection with JRM`, then EDS, EDS-GCF and jrm are running.
- If you do not get the above message, contact the technical assistance center with the error message.
- If your jrm in down or inaccessible, you'll get a message while accessing the UIs.

Q. How do I change the casuser password in Windows?

A. You can change the casuser password using resetCasuser.exe. It can be run only by an administrator or casuser. To change the casuser password:

Step 1 Enter *NMSROOT*\setup\support **resetCasuser.exe** at the command prompt

You can:

1. Randomly generate the password
2. Enter the password
3. Exit.

Step 2 Enter **2**, and press **Enter**.

It prompts you to enter the password.

Step 3 Confirm the password.

Note You must know the password policy. If the password entered does not match the password policy, it exits.

Q. How do I change the Cisco Prime user password?

A. See Changing Cisco Prime User Password Through CLI for details.

Q. How do I enable debugging for Session Management Services?

A. To enable debugging for Session Management Services:

Step 1 Go to *NMSROOT*/MDC/tomcat/webapps/classic/WEB-INF/web.xml.

You should edit the following section of the file:

```
<context-param>
<param-name>DEBUG</param-name>
<param-value>false</param-value>
<description>mice debug enabling</description>
</context-param>
```

Step 2 Change `<param-value>`**`false`**`</param-value>` to `<param-value>`**true**`</param-value>`.

Q. What does a diskWatcher process do?

A. The diskWatcher process monitors disk space availability on the Cisco Prime LMS Server.

This process calculates the disk space information of a drive (in Windows machine) or a file system (in Solaris machine) at regular intervals and stores them in diskWatcher.log file.

See Configuring Disk Space Threshold Limit for more information.

Q. Cisco Prime Time is not synchronized with System time. What should I do?

A. You should complete the following:

a. Edit the TIMEZONE file using the vi /etc/TIMEZONE command on a Solaris machine.

b. Set the TZ=*standard_timezone.* For example, you can specify TZ=MET.

c. Save the TIMEZONE file.

d. Reboot the machine.

Now the system displays the modified time zone information. If you need to change the time zone to daylight, you change only the time and date but not the TIMEZONE.

Q. How can I increase the timeout value of Cisco Prime LMS user interface?

A. You can configure the timeout value in the following file.

NMSROOT/MDC/tomcat/webapps/classic/WEB-INF/web.xml

where *NMSROOT* is your Cisco Prime Installation directory.

You should change the value of an XML tag by name session-timeout. You should specify the value in minutes. The default timeout value is set to 2 hours.

You cannot disable this option as this may increase the load in the server.

Q. How should I change the syslog port of Cisco Prime from 514 to another number?

A. You can change the syslog port by modifying the value of CrmLogPort registry key located under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmlog\Parameters.

After you have changed the syslog port, you need to restart the syslog service.

Q. What should I do when Daemon Manager and multiple processes are not started on a Windows machine?

A. Sometimes, Windows may prevent to run some processes for security reasons.

You should do the following on a Windows 2003 Operating system:

Step 1 Right-click the My Computer icon on your desktop and click **Properties** to open the System Properties dialog box.

Step 2 Click the Advanced tab.

Step 3 Click **Settings** from the Performance panel to open the Performance Options dialog box.

Step 4 Click the Data Execution Prevention tab.

Step 5 Check whether the java.exe and cwjava.exe are available in the list of blocked programs. If so, remove the programs from the blocked list.

Step 6 Click **OK** to close the Performance Options dialog box.

Step 7 Click **OK** to close the System Properties dialog box.

Step 8 Reboot the server.

Q. I am getting timeout exception in cmdsvc (command service library) during a device connection/socket establishment. How do I change the default timeout and delays in cmdsvc?

A. You can change the default timeout and delays in cmdsvc using the cmdsvc.properties file available in the following directory: *$NMSROOT/objects/cmf/data*

To change the default timeout and delay values:

Step 1 Go to the directory *$NMSROOT/objects/cmf/data*

Step 2 Open the **cmdsvc.properties** file.

Various timeout and delay values are listed in the file.

Step 3 Remove the Hash symbol (#) to uncomment a particular timeout or delay value.

Step 4 Remove the existing timeout or delay value.

Step 5 Enter new timeout or delay value.

Step 6 Save the **cmdsvc.properties** file.

Q. What should I do when the TAC Service Requests feature that displays my current Cisco.com TAC tickets does not use the proxy to connect, even after setting the proxy in proxy server setup?

A. Check whether the following production urls are reachable in the server, where product is installed.

- SASI_SERVER—https://wsgx.cisco.com
- RSR_SERVER—https://wsgx.cisco.com
- CSC_SERVER—https://supportforums.cisco.com
- CCOLOGINURL—https://sso.cisco.com/autho/apps/nmtgSSapp/index.html
- CCOLOGOUTURL—https://sso.cisco.com/autho/logout.html

- CASE_QUERY_URL—https://tools.cisco.com/ServiceRequestTool/query/QueryCaseSearchAction.do?caseType=ciscoServiceRequest&method=doQueryByCase&SRNumber=
- LOGIN_REDIRECT_URL—https://fed.cisco.com/idp/startSSO.ping?PartnerSpId=csc.jivesoftware.com&TargetResource=
- CSC_REDIRECT_URL—https://supportforums.cisco.com

Q. I am unable to access LMS running on Windows 2008 Server, when I use IE, but it works properly in FF, what could be the reason?

A. You are not able to access LMS in IE because of the cache issue. Clear the browser cookies and cache from IE.

Important URLs

Q. What are the URLs that are most commonly used in LMS?

A. The following URLs are most commonly used in LMS and should be added in the proxy server:

General

- http://www.cisco.com

Device update/Software update/Point Patch update

- http://tools.cisco.com/software/catalog/swcs/softwaremetadata
- http://tools.cisco.com/software/catalog/swcs/image
- http://www.cco.cisco.com

IOS image download

- http://www.cisco.com/cgi-bin/smarts/swim/crmiosbridge.pl
- http://www.cisco.com/techsupport

Smart Services

- SASI_SERVER—https://wsgx.cisco.com
- RSR_SERVER— https://wsgx.cisco.com
- CSC_SERVER—https://supportforums.cisco.com
- CCOLOGINURL—https://sso.cisco.com/autho/apps/nmtgSSapp/index.html
- CCOLOGOUTURL— https://sso.cisco.com/autho/logout.html
- CASE_QUERY_URL—https://tools.cisco.com/ServiceRequestTool/query/QueryCaseSearchAction.do?caseType=ciscoServiceRequest
- LOGIN_REDIRECT_URL—https://fed.cisco.com/idp/startSSO.ping?PartnerSpId=csc.jivesoftware.com
- CSC_REDIRECT_URL—https://supportforums.cisco.com

PSIRT

- EoS/EoL Hardware Report—http://www.cisco.com/cisco/software/release.html?mdfid=282253606&flowid=5144&softwareid=280775123&os=Windows&release=4.1.1&relind=AVAILABLE&rellifecycle=&reltype=latest#

- EoS/EoL Software Report—http://www.cisco.com/cisco/software/release.html?mdfid=282253606&flowid=5144&softwareid=280775123&os=Windows&release=4.1.1&relind=AVAILABLE&rellifecycle=&reltype=latest#

Bug Toolkit

- http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl
- http://tools.cisco.com/Support/BTKNotifications/getBugDetails.do??method=getAllBugs
- http://tools.cisco.com/Support/BTKNotifications/getBugDetails.do?method=getAffectedBugdata&bugid=
- http://tools.cisco.com/Support/BTKNotifications/getBugDetails.do?method=getBugsReport

Contract Connection

- http://www.cisco.com/pcgi-bin/front.x/cconx/conx_userinfo.pl
- https://www.cisco.com/cgi-bin/front.x/cconx/conx_recv_data.pl
- https://www.cisco.com/cgi-bin/front.x/cconx/conx_sortdetail_js.pl

Compliance and Audit Management

- Download Contracts—https://apps.cisco.com/CustAdv/ServiceSales/contract/viewContractMgr.do?method=viewContractMgr
- Download Compliance Policy Updates—http://www.cisco.com/cisco/software/release.html?mdfid=284259296&flowid=31102&softwareid=284270571&release=1.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Security

The following are the FAQs on LMS Security:

Q. When I invoke Cisco Prime in the secure mode (HTTPS), there are too many dialog boxes. This makes the process tedious. Is there a way to reduce the number of dialog boxes and steps?

A. Yes. You have the following options:

- If you are using Self-signed certificates in Internet Explorer, install the certificate in the browser's trusted certificate stores, if you are confident about the identity of the server.
- Use a server certificate issued by a prominent third party certificate authority (CA).

- Configure the hostname in your server certificate properly, and use the same hostname to invoke Cisco Prime.

Q. When I invoke Cisco Prime, I am unable to get to the login page directly. Instead, I am facing a security alert related to the site's security certificate. It asks for my input to proceed further. Why?

A. Cisco Prime does not have any control over this behavior. This is an expected browser behavior (Microsoft Internet Explorer or Mozilla Firefox), to ensure proper security.

This appears if any of the following conditions is not satisfied:

- The certificate of the server (Cisco Prime Server in this case) must be issued by trusted Certificate Authority.
- The date of the certificate must be valid. (Each certificate is assigned a validity period. It can range from 21 days to 5 years).
- The name of the certificate and name of the page (or the name typed in the address bar of the browser) are the same.

To view the certificate information:

- Click **View Certificate**, in the alert box for Internet Explorer.
- Click **Examine Certificate** in the alert box for Mozilla Firefox.

The server should be invoked with the name same as the Issued to' field of the certificate.

To install the certificate in Internet Explorer:

Step 1 Click **View Certificate** in the alert box.

The Certificate dialog box displays the Certificate information.

Step 2 Click **Install Certificate**.

Q. My server certificate for Cisco Prime has expired. What should I do?

A. If you are using a self-signed certificate, you can create a new certificate using the Create Self Signed Certificate option. For more information, see Creating Self Signed Certificates.

If you are using a third party issued certificate, you must contact the certificate authority (CA) and renew the certificate. You can use a self-signed certificate till you get the certificate renewed by the CA.

Note Before you perform any certificate management operations—creating or modifying certificates, back up the certificate files, the server private key in particular, and keep them in a safe location.

Q. I have configured the Active Directory Login Module but it does not work. How can I analyze the problem?

A. To analyze the problem, enable the Debug mode for the Active Directory Login module. To do this:

Step 1 Login as Admin.

Step 2 Select **Admin > System > Authentication Mode Setup**.

The Select Login Module dialog box appears.

Step 3 Select a login module from the Available Login Modules list box and Click on **Edit Options**.

The Login Module Options dialog box appears.

Step 4 Select the radio button **True** and click **Finish**.

This enables the Debug option. Enabling debug mode allows the login module to add the detailed progress and failure information to log files. The log files are located at:

NMSROOT/MDC/Tomcat/logs/stdout.log

For all failed login attempts, the log files contain LDAP error messages, which specify the reason for the failure.

For example, if the Usersroot configuration is incorrect, then the login module cannot match the complete DN string with any entries in the Active Directory database.

It indicates which portion of the DN matched and which portion did not match. You can verify your Active Directory setup and the entries for the Usersroot.

In some cases, the log file contains error messages with NameError. This indicates that either you entered a wrong user ID or there is some spelling error in the Usersroot configuration.

Q. What are the minimum and maximum length of user account names? How do I control them?

A. The minimum length of a user account name is 5 characters. The maximum length of a user account name is 255 characters.

You can control the length of user account names using the Local User Policy Setup page. See Setting up Local User Policy for more information.

Q. What are the rules to enter a valid username and password?

A. The username can contain the alphabets in lower and upper cases, numerals, hyphens (-), underscores (_), periods (.), tilde (~), commercial At character (@), number sign (#), Apostrophe ('), solidus or leading slash (/), trailing slash (\), and space.

The username should start with alphabets, numerals and underscore characters.

The password can contain the alphabets, numerals, leading and trailing spaces, and any special characters.

The length of username and password can span from 5 to 256 characters.

Q. Where is the SSL log present?

A. The SSL log is present in the *NMSROOT* directory, where *NMSROOT* is your Cisco Prime Installation directory.

Q. Why am I getting a 403 forbidden error while trying to access Cisco Prime pages?

A. You should check whether the casuser is assigned with the required local security policies.

To check whether the casuser is assigned with the required policies:

Step 1 Click **Start > Settings > Control Panel> Administrative Tools**.

Step 2 Click the Local Security Policy shortcut from the Administrative Tools folder.

The Local Security Policy window opens.

Step 3 Click **Local policies > User Rights Assignment** in the Local Security Policy window.

Step 4 Check whether the casuser is assigned with the following privileges:

- Access this computer from the network
- Log on as a batch job

If the casuser is not assigned with the required privileges, you should run the resetCasuser utility again. Enter the following commands to run the resetCasuser utility:

- *NMSROOT*`/CSCOpx/setup/support/resetCasuser` (On Solaris/Soft Appliance)
- *NMSROOT*`\CSCOpx\setup\support\resetCasuser.exe` (On Windows)

where *NMSROOT refers to the Cisco Prime Installation directory.*

The other possible solutions are:

- Remove or disable the anti-virus software
- Restart Daemon Manager
- Uninstall or disable IIS
- Log on as a batch job
- Disable Cisco Security Agent
- Stop the Daemon Manager and check if there are any Apache or Tomcat processes running. If so, kill the stray processes from the Task Manager or stop them from the Services panel.
- Ensure that the casuser or administrator has the read permission for the CSCOpx, CSCOpx/MDC/tomcat/webapps/cwhp directories, and their inner directories.

Software Center

The following are the FAQs on Software Center:

Q. How do I find out which devices are supported by a particular application?

A. Select **Admin > System > Software Center > Software Update.** Under Applications Installed, click the application name to see a list of the supported devices.

See Selecting Software Updates for more information.

Q. What are the prerequisites for downloading Software Updates from Cisco.com?

A. You should check for the following:

- Valid Cisco.com credentials are configured during Server administration
- Valid proxy details are configured and Cisco Prime support basic authentication of proxy server.

See Downloading Software Updates for more information.

Q. Does the Software Center list only the software updates that are not installed in this machine?

A. The Software Center module lists all software updates including those that are installed. However, it performs the filtering for device updates.

Q. What should I do if I see errors when using Software Center or having issues with LMS not correctly working with supported devices?

A. Under rare circumstances, internal LMS files that contain information on which device support packages are installed and which devices are supported, become corrupted.

If such files become corrupted, you may notice one or more of the following symptoms:

- "HTTP 500" error occurs while trying to view package information from **Admin > System > Software Center > Device Update**. One possible exception is:

  java.util.NoSuchElementException at
  java.util.StringTokenizer.nextToken(StringTokenizer.java:259) at
  com.cisco.nm.xms.psu.ui.gui.model.action.DevUpdate.getPackageMap(Unknown Source) at
  com.cisco.nm.xms.psu.ui.gui.model.action.DevUpdate.perform(Unknown Source)

- The following errors will be seen in *NMSROOT*\log\psu.log:

  ```
  [ <date time > ] ERROR  [CreateMaps : removeDupEntries]  :String index out of
  range: -1
  ```

- Devices shown as supported in "Supported Devices Table for CiscoWorks LAN Management Solution" and may have been working previously, show as not supported/unknown and displays device icons in Device Selectors with a question mark (?) in one or more areas of LMS.
- Various forms of Inventory/Configuration Collection from devices (**Inventory > Dashboards > Device Status > Collection Summary**) fails for all devices of a particular model, but succeeds for other devices with identical configuration, yet different models.
- Specific models of devices are not available in Device Selectors to have reports, jobs or other functionality run on them, however Inventory Collection and/or Config Archive has succeeded for them. This is frequently seen with Configuration related functionality.

To resolve such issues, you can run the *NMSROOT*/bin/reCreatePkgMap.pl script and recreate files which store information on which device support packages are installed and devices they support. Run the following script:

NMSROOT/bin/perl *NMSROOT*/bin/reCreatePkgMap.pl (Solaris/Soft Appliance)

or

NMSROOT\bin\perl *NMSROOT*\bin\reCreatePkgMap.pl (Windows)

where *NMSROOT* is your Cisco Prime installation directory.

If issues persist after running this script, contact the Cisco Technical Asssistance Center for further assistance.

Event Distribution Services and Event System Services

The following are the FAQs on Event Distribution Services and Event System Services:

Q. How do I change the ESS port?

A. You can change the ESS port by running the following commands:

- *NMSROOT*`/objects/ess/conf/Ports2Alternate.pl`
- *NMSROOT*`/objects/ess/conf/Ports2Primary.pl`

where *NMSROOT* is the default installation directory of Cisco Prime.

Q. Why do the EDS process is not starting?

A. You should check:

- If the hostname is correct and is not changed recently.
- If the osagent is in use in port 42342.

If the osagent is not in use, you should:

Step 1 Stop the Daemon Manager.

Step 2 Run the ChangeOSAGENTPort.pl script to change the port number. Enter the following command:

NMSROOT`/bin/perl` *NMSROOT*`/bin/ChangeOSAGENTPort.pl` *Port_number*

where,

NMSROOT — Cisco Prime Installation directory

Port_number— Osagent port

Step 3 Restart the Daemon Manager.

Q. How should I configure EDS in a multi-homed machine?

A. To run Cisco Prime LMS and configure EDS on a multi-homed machine, you must all the IP Addresses in DNS.

Q. Sometimes, I am not able to access CORBA services in Cisco Prime LMS Server from other network?

A. This could because the domain name of the Cisco Prime LMS server may not be resolved.

To access the CORBA services in a server that is not DNS resolvable, you must:

Step 1 Change the value of attribute `jacorb.dns.enable` in orb.properties file from `on` to `off`.

Step 2 Regenerate the self-signed certificate with IP address instead of hostname.

Step 3 Restart the Daemon Manager.

Backup and Restore

The following are the FAQs on Backup and Restore:

- Q.What kind of directory structure does Cisco Prime use when backing up data?
- Q.What should I do when backup fails and displays a `Backup.LOCK file exists` error message?
- Q.Do I need to stop the Daemon Manager before running backup.pl and restorebackup.pl scripts?

Q. What kind of directory structure does Cisco Prime use when backing up data?

A. Cisco Prime uses a standard database structure for backing up all suites and applications. See Table B-5 for a sample directory structure on Cisco Prime LMS Server.

Table B-5 Sample Backup Directory

Directory Path	Description	Usage Notes
/tmp/1	Number of backups	1, 2, 3...
/tmp/2/cmf	Application or suite	Backs up Cisco Prime LMS Server applications.

Table B-5 Sample Backup Directory (continued)

Directory Path	Description	Usage Notes
/tmp/1/cmf/filebackup.tar	Cisco Prime LMS Server application tar files	Application data is stored in the datafiles.txt which are compiled into the tar file.
/tmp/1/cmf/database	Cisco Prime LMS Server database directory	Includes the following files for each database: • *xxx*_DbVersion.txt • *xxx*.db (database files) • *xxx*.log (database log files) • *xxx*.txt (database backup manifest file) where *xxx* is the name of the database.

Q. What should I do when backup fails and displays a `Backup.LOCK file exists` error message?

A. You should try removing the Backup.LOCK file from the Cisco Prime installation directory and start backup again. You can use the CLI program to back up the data. See Backing up Data Using CLI for more information.

Q. Do I need to stop the Daemon Manager before running backup.pl and restorebackup.pl scripts?

A. Daemons should be stopped only before you run restorebackup.pl scripts. You need not stop the Daemon Manager to run the backup.pl scripts.

See Backing up Data Using CLI and Restoring Data for more information.

Database

The following are the FAQs on Database:

Q. How can I find the version of a Sybase Database?

A. Run the following command:

```
opt/CSCOpx/objects/db/bin64/dbsrv10 -v
```

Q. What if the database is inaccessible?

A. If the server is not able to connect to the database, the database might be corrupt or inaccessible. This can occur if processes are not running. Try the following:

Step 1 Log in to Cisco Prime LMS server as **admin**.

Step 2 Select **Admin > System > Server Monitoring > Processes**.

A list of Cisco Prime back-end processes appears.

You can check if there are any failed process appear in the list.

Step 3 Select **Admin > System > Server Monitoring > Selftest**.

- Click **Create** to create a report.
- Click **Display** to display the report.

Step 4 Select **Admin > System > Server Monitoring > Collect Server Information**.

Step 5 Click **Product Database Status** to get detailed database status.

Step 6 Contact the Cisco TAC or your customer support to get the information you need to access the database and find out details about the problem.

After you have the required information, perform the following tasks for detecting and fixing database errors.

Depending upon the degree of corruption, the database engine may or may not start. For certain corruptions, such as bad indexes, the database can function normally until the corrupt index is accessed.

Database corruptions, such as index corruptions, can be detected by the dbvalid utility, which requires the database engine to be running.

To detect database corruption:

Step 1 Log on as root (on Solaris/Soft Appliance) or with administrator privileges (on Windows).

Step 2 Stop the Daemon manager if it is already running:

- **`/etc/init.d/dmgtd stop`** (on Solaris/Soft Appliance)
- **`net stop crmdmgtd`** (on Windows)

Step 3 Make sure no database processes are running and there is no database log file.

For example, if the database file is /opt/CSCOpx/databases/rme/rme.db, the database log file is /opt/CSCOpx/databases/rme/rme.log. This file is not present if the database process shuts down cleanly.

Step 4 Check if the database files and the transaction log file (*.log) are owned by user casuser if you use Solaris machines. If not, change the ownership of these files to user casuser and group casusers.

Step 5 Run the commands on the command prompt:

`cd` *NMSROOT*`/objects/db/conf`

NMSROOT`/bin/perl configureDb.pl action=validate dsn=cmf`

The **`dbvalid`** command displays a list of tables being validated. The Validation utility scans the entire table, and looks up each record in every index and key, defined on the table. If there are errors, the utility displays a message such as:

```
Validating DBA.xxxx
run time SQL error -- Foreign key parent_is has invalid or duplicate index
entries 1 error reported
```

If the above command reports any error, you may try:

- Restoring from a previous good backup

  or

- Reinitializing database

Caution All the current data will be lost.

To do this, you have to run the following command:

NMSROOT`\bin\perl` *NMSROOT*`\bin\dbRestoreOrig.pl dsn=`*dsn* `dmprefix=`*dmprefix*

For LMS, *dsn* is cmf and *dmprefix* is Cmf.

Apache and Tomcat

The following are the FAQs on Apache and Tomcat:

Q. How do I avoid the SSL port conflict between HPOV and LMS servers and run them both on the same system?

A. The new installer detects IIS web server running on the machine and prompts you to enter a different port number for Cisco Prime LMS Server to avoid the conflict.

Q. Why does the Apache process not come up after installation or why does the process go down suddenly?

A. This could be a problem with the Apache configuration syntax or the validity of the server certificate. You should first check the Apache configuration syntax.

To do this:

On Windows:

Go to *NMSROOT*\MDC\Apache\bin and run the command **`Apache.exe -t -d .`**

Note Do not omit the **`.`**

On Solaris/Soft Appliance:

Go to *NMSROOT*/MDC/Apache/bin and run the command **`./web_server -t`**

If the Apache configuration syntax is correct, a message appears:

```
Syntax OK
```

If the Apache configuration syntax is fine, check the validity of the Server Certificate using the SSL Utility Script.

Q. How do I change web server port numbers?

A. To change the web server port numbers, you must run separate commands for both Windows and Solaris.

On Solaris:

You can change the web server port numbers for the webservers. You can also change both the HTTP and HTTPS port numbers. To change the port numbers you must login as Cisco Prime LMS Server administrator, and run the following command at the prompt:

NMSROOT`/MDC/Apache/bin/changeport`

If you run this command without any command line parameter, Cisco Prime displays:

```
*** CiscoWorks Webserver port change utility ***
Usage: changeport <port number> [-s] [-f]
```

where

port number—The new port number that should be used

`-s`—Changes the SSL port instead of the default HTTP port

`-f`—Forces port change even if Daemon Manager detection FAILS.

Note Do not use this option by default. Use it only when Cisco Prime instructs you to.

For example, you can enter:

`changeport 1744`—Changes the Cisco Prime web server HTTP port to use 1744.

Or,

`changeport` *port number* **`-s`**—Changes the Cisco Prime web server HTTPS port to use the specified port number.

If you change the port after installation, Cisco Prime will not launch from Start menu (**Start > Programs > CiscoWorks > CiscoWorks**).

You have to manually invoke the browser, and specify the URL, with the changed port number.

The restrictions that apply to the specified port number are:

- Port numbers less than 1026 are not allowed. However, you can use 443 as the HTTPS port number.
- The specified port should not be used by any other service or daemon. The utility checks for active listening ports, and ports listed in /etc/services. If there is any conflict, it rejects the specified port.
- The port number must be a numeric value in the range 1026 – 65535. Values outside this range, and non-numeric values are not allowed.
- If port 443 is specified for any of the web servers, that web server process is started as root. This is because ports lower than 1026 are allowed to be used only by root in Solaris.

  However, according to Apache behavior, only the main web server process run as root, and all the child processes run as casuser:casusers. Only the child processes serve the external requests.

  The main process that runs as root monitors the child processes. It does not accept any HTTP requests. Owing to this, Apache ensures that a root process is not exposed to the external world, and thus ensures security.
- If you do not want Cisco Prime processes to run as root, do not use the port 443.

  When you run the utility with the appropriate options, it displays messages on the tasks it performs.

This utility lists all the files that are being updated. Before updating, the utility will back up all affected files in /opt/CSCOpx/conf/backup and creates appropriate unique sub-directories.

It also creates a new file called `index.txt`. This text file contains information about the changed port, a list of all the files that are backed up, and their actual location in the Cisco Prime directory.

- If you do not want Cisco Prime processes to run as root, do not use the ports 80 and 443.

  When you run the utility with the appropriate options, it displays messages on the tasks it performs.

  This utility lists out all the files that are being updated. Before updating, the utility will back up all affected files in /opt/CSCOpx/conf/backup and creates appropriate unique sub-directories.

  It also creates a new file index.txt. This text file contains information about the changed port and a list of all files that are backed up and their actual location in the Cisco Prime directory.

A sample backup maybe similar to:

```
/opt
   |
   `--/CSCOpx
       |
       `--/conf
          |
          `--/backup
            |
            |--README.txt (Note the purpose of this directory as it is initially empty)
            |
            `--/AAAtpaG03_Ciscobak (Autogenerated unique backup directory).
                      |
                      |--index.txt (The backup file list)
                      |--httpd.conf (Webserver config file)
                      |--md.properties (CiscoWorks config elements)
                      |--mdc_web.xml (Common Services application config file)
                      |--regdaemon.key (Common Services config registry key file)
                      |--regdaemon.xml (Common Services config registry data file)
                      |--rootapps.conf (CiscoWorks daemons using privileged ports)
                      |--services (The system /etc/services file)
                      `--ssl.properties (CiscoWorks config elements for SSL mode)
```

Note All of the above files and the unique directories are stored with read only permission to casuser:casusers. To ensure the security of the backup files, only the Cisco Prime LMS Server administrator has write permissions.

The change port utility displays messages to the console during execution. These messages contain information about the directory where the backup files are being stored. These messages are also logged to a file, changeport.log.

This file is saved to the directory:

/var/adm/CSCOpx/log/changeport.log

This file contains the date and time stamps to indicate when the log entries were created.

On Windows:

You can change the web server port numbers for the LMS Webserver. You can also change both the HTTP and HTTPS port numbers.

To change the port numbers you must have administrative privileges. Run the following command at the prompt:

NMSROOT`\MDC\Apache\changeport.exe`

If you run this utility without any command line parameter, Cisco Prime displays the following usage text:

```
*** Common Services Webserver port change utility ***
Usage: changeport <port number> [-s] [-f]
```

where:

port number—The new port number that should be used

-s—Change the SSL port instead of the default HTTP port

-f—Force port change even if Daemon Manager detection fails.

Note Do not use this option by default. Use it only when Cisco Prime instructs you to.

For example, you can enter:

changeport 1744—To change the Cisco Prime web server HTTP port to use 1744.

Or,

changeport *port number* **-s**—Changes the Cisco Prime web server HTTPS port to use the specified port number.

If you change the port after installation, Cisco Prime will not launch from Start menu (**Start > Programs > CiscoWorks > CiscoWorks**). You have to manually invoke the browser and specify the URL, with the changed port number.

The restrictions that apply to the specified port number are:

- Port numbers less than 1026 are not allowed. However, you can use 443 as the HTTPS port number.
- The specified port should not be used by any other service or daemon. The utility checks for active listening ports, and if any conflict is found, the utility rejects the specified port.

  There is no reliable way to determine whether any other service or application is using a specified port. If the service or application is running and actively listening on a port, it can be easily detected.

  However, if the service is currently stopped, there is no way that the utility can determine what port it uses. This is because on Windows there is no common port registry equivalent to /etc/services as in Solaris.
- The port number must be a numeric value in the range 1026 – 65535. Values outside this range, and non-numeric values are not allowed.

When you run the utility with the appropriate options, it displays messages on the actions it is performing.Cisco Prime

It lists out all the files that are being updated. Before updating, the utility backs up all the affected files in CSCOpx\conf\backup, and creates, appropriate, unique, sub-directories.

It also creates a new file called `index.txt`. This text file contains information about the changed port, a list of all the files that are backed up, and their actual location in the Cisco Prime directory.

A sample backup may be similar to:

```
[drive:]
 |
 `--\Program Files
      |
      `--\CSCOpx
           |
           `--\conf
                |
```

```
`--\backup
   |
   |--README.txt (Notes the purpose of this dir as it is initially empty)
   |
   `--\skc03._Ciscobak (Autogenerated unique backup directory).
        |
        |--index.txt      (The backup file list)
        |--httpd.conf     (Webserver config file)
        |--md.properties  (CiscoWorks config elements)
        |--mdc_web.xml    (Common Services application config file)
        |--regdaemon.key  (Common Services config registry key file)
        |--regdaemon.xml  (Common Services config registry data file)
        `--ssl.properties (CiscoWorks config elements for SSL mode)
```

Note All the above files and the unique directories are stored with read only permissions. Only the administrator and casuser have write permissions, to ensure the security of the backup files.

The change port utility displays messages to the console during execution. These messages contain information about the directory where the backup files are being stored. These messages are also logged to a file, changeport.log.

This file is saved to the directory:

NMSROOT\log\changeport.log

This log file contains the date and time stamps to indicate when the log entries were created.

Q. How should I enable or disable web server SSL mode from the command line?

A. To enable or disable the web server SSL mode:

Step 1 Stop the Daemon Manager.

Step 2 Run the ConfigSSL.pl script. Enter the commands:

- *NMSROOT*`/bin/perl ConfigSSL.pl -enable` (to enable the web server SSL mode from the command line)
- *NMSROOT*`/bin/perl ConfigSSL.pl -disable` (to disable the web server SSL mode from the command line)

Step 3 Start the Daemon Manager.

Q. How do I increase Tomcat heap size?

A. To increase Tomcat heap size:

Step 1 Stop the Daemon Manager.

- On Solaris/Soft Appliance:

  Run `/etc/init.d/dmgtd stop`

- On Windows:

  Run `net stop crmdmgtd`

Step 2 Run *NMSROOT*`/bin/perl` *NMSROOT*`/bin/ModifyTomcatHeap.pl` *max heap in MB*

Step 3 Start the Daemon Manager.

- On Solaris/Soft Appliance:

  Run **`/etc/init.d/dmgtd stop`**

- On Windows:

  Run **`net start crmdmgtd`**

If Tomcat is already configured for higher memory than what you specify when you run the command, the following message is displayed:

```
INFO: Tomcat is already configured with a higher heap value.
```

Q. How do I validate a Server certificate?

A. To do this:

Step 1 Navigate to the directory where the SSL Utility Script is located.

On Windows:

a. Go to *NMSROOT*\MDC\Apache

b. Enter *NMSROOT*`\bin\perl SSLUtil.pl`

On Solaris/Soft Appliance:

a. Go to *NMSROOT*/MDC/Apache/bin

b. Enter *NMSROOT*`/bin/perl SSLUtil.pl`

After you have entered this command, the system displays a set of options.

Step 2 Select the fourth option Verify the input Certificate/Certificate Chain by entering 4.

Step 3 Enter the location of the server certificate *NMSROOT*`/MDC/Apache/conf/ssl/server.crt`

The script verifies if the server certificate is valid. If the script reports errors during validation and verification, you have to regenerate the certificate by running **`SignTool.pl`** from the above directory.

Step 4 Enter *NMSROOT*`/bin/perl SignTool.pl [-SSL=true | -SSL=false]`

Note *NMSROOT* is the directory where Cisco Prime is installed.

Q. How do I modify a certificate which is not self-signed?

A. LMS does not allow modifying certificates other than the self-signed certificates.

Q. What is the maximum number of connections allowed by Cisco Prime to access the web interface?

A. Tomcat, the servlet engine, shipped with Cisco Prime handles a maximum of 500 connections or http requests.

Q. What version of Tomcat is installed on my server?

A. To find out the version of Tomcat installed on your server, you should:

Step 1 Navigate to the *NMSROOT*/MDC/tomcat/server/lib directory.

Step 2 Unzip the catalina.jar file available in this directory.

Step 3 Navigate to the location where you have extracted this jar file.

Step 4 Open the Serverinfo.properties file under the orgapachecatalinautil directory.

This file displays the version of Tomcat installed on the Cisco Prime LMS Server.

Q. Why does Apache server does not start during reboot process?

Anti-virus causes the processes to come up slowly after reboot. Delay the anti-virus during startup to solve the issue. Ensure that the NMSROOT folder is excluded correctly from anti-virus and reboot the server after shutting down the anti-virus completely.

Fault Management FAQs

The following section lists the frequently asked questions about Fault Management.

Q. How do I enable Incharge debugging, and execute Incharge commands?

A. Select **Admin > System > Debug Settings > Fault Debugging Settings**. The Fault Debugging Settings page appears. Click the Enable Incharge Debugging, and execute Incharge Commands link. See, Enable Incharge Debugging for more information.

Q. What is the difference between SNMP Raw Trap Forwarding and Processed SNMP Trap alert/event Trap Forwarding? Does LMS support both of these methods?

A. Yes, LMS supports both ways of Trap forwarding.

Raw Trap is forwarded by the Device to Fault Management and Fault Management has to process it. To configure Raw Trap Forwarding, select **Admin > Network > Notification and Action Settings > Fault - SNMP trap forwarding**.

When LMS receives certain SNMP traps, it analyzes the data found in fields such as Enterprise/Generic trap identifier, Specific Trap identifier, and variable-bindings of each SNMP trap message.

If needed, LMS changes the property value of the object property. These are Processed Traps. To configure Processed event/alert trap forwarding, select **Admin > Network > Notification and Action Settings > Fault - SNMP trap forwarding.** This configuration can also send trap notifications if there is a threshold violation in the LMS managed devices**.**

For more information, refer to the *Monitoring and Troubleshooting with Cisco Prime LAN Management Solution 4.1*

Q. How can I receive Syslog messages from the LMS server?

A. To receive Syslog messages from a LMS server:

Step 1 Enable Syslog from **Admin > Network > Notification and Action Settings > Fault - Syslog notification**

Step 2 Point it to any Solaris machine and run the following:

- `/etc/init.d/syslog start`
- `tail -f /var/adm/messages`

Q. How can I create a link to the Java Plug-in in Netscape7.x and Mozilla 1.7.x?

A. Create a symbolic link to the Java Plug-in libjavaplugin_oji.so file in the Netscape 6.x/7.x or Mozilla Plugins directory. To create the link, go to the command prompt and enter:

Step 1 `cd /plugins`

Step 2 `ln -s /plugin/sparc/ns610/libjavaplugin_oji.so .`

Include the period at the end.

For Netscape 6.x/7.x or Mozilla browsers, restart your browser.

In Netscape, go to **Help > About Plug-ins** to confirm that the Java Plug-in is loaded.

Device Performance Management FAQs

Q. Can I set log levels for individual application modules? Where are these log files stored?

A. Yes. You can set log levels for all Device Performance Management modules. Log files are stored at these locations:

- On Windows: *NMSROOT*\log\, where *NMSROOT* is the Cisco Prime DPM installation directory.
- On Solaris/Soft Appliance: /var/adm/CSCOpx/log/

  Report specific logs are stored under DPMReportJobs under the log directory.

IPSLA Performance Management FAQs

This section provides the FAQs on IPSLA Performance Management:

Q. How can I enable debugging in IPSLA Performance Management?

A. Do the following:

Step 1 Select **Admin > System > Debug Settings > IPSLA Debugging Settings**.

The **IPSLA Debugging Settings** page appears.

Step 2 Select the module and log level from the Module and Logging Level drop-down lists.

The various log levels available are FATAL, ERROR, WARN, INFO, and DEBUG.

Step 3 Click **Apply**.

Q. I have problems while migrating the IPSLA Performance Management data. What should I do?

A. Check the following log files for information:

- restorebackup.log
- migration.log
- ipmclient.log
- ipmserver.log