Administering LMS Server

LMS includes several administrative features to ensure that the server is performing properly. You can manage processes, set up backup parameters, update licensing information, collect server information, manage jobs and resources, and configure system-wide information on the LMS Server.

- Using Daemon Manager
- Managing Processes
- Backing Up Data
- Backup for Cisco Prime Infrastructure
- Licensing Cisco Prime LMS
- Compliance and Audit Manager (CAAM) Server License

This chapter has the following information:

- Using Daemon Manager
- Managing Processes
- Backing Up Data
- Licensing Cisco Prime LMS
- Configuring a Default SMTP Server
- Collecting Server Information
- Collecting Self Test Information
- Messaging Online Users
- Managing Resources
- Collecting Server Information
- Collecting Self Test Information
- Messaging Online Users
- Managing Resources
- Modifying System Preferences
- Configuring Log Files Rotation
- Modifying System Preferences
- Configuring Disk Space Threshold Limit
- Effects of Third Party Backup Utility and Virus Scanner
Using Daemon Manager

The Daemon Manager provides the following services:

- Maintains the startup dependencies among processes.
- Starts and stops processes based on their dependency relationships.
- Restarts processes if an abnormal termination is detected.
- Monitors the status of processes.

The Daemon Manager is useful to applications that have long-running processes that must be monitored and restarted, if necessary. It is also used to start processes in a dependency sequence, and to start transient jobs.

Do not start the Daemon Manager immediately after you stop it. The ports used by the Daemon Manager will be in use for some time after the Daemon Manager is stopped. Wait for at least a minute before you start the Daemon Manager.

If the System resources are less than the resources required to install the application, the Daemon Manager restart displays warning messages that are logged into dmgtd.log.

You cannot start the Daemon Manager if there are non-SSL compliant applications installed on the server when SSL is enabled in LMS.

**Restarting Daemon Manager on Solaris/Soft Appliance**

To restart Daemon Manager on Solaris/Soft Appliance:

**Step 1** Log in as root.

**Step 2** Enter `/etc/init.d/dmgtd stop` to stop the Daemon Manager.

**Step 3** Enter `/etc/init.d/dmgtd start` to start the Daemon Manager.

**Restarting Daemon Manager on Windows**

To restart Daemon Manager on Windows:

**Step 1** Go to the command prompt.

**Step 2** Enter `net stop crmdmgtd` to stop the Daemon Manager.

**Step 3** Enter `net start crmdmgtd` to start the Daemon Manager.

Do not start the Daemon Manager immediately after you stop it. The ports used by Daemon Manager will be in use for some more time even after the Daemon Manager is stopped. Wait for at least one minute before you start the Daemon Manager.

If the System resources are less than the required resources to install the application, Daemon Manager restart displays warning messages that are logged into syslog.log.
Managing Processes

Cisco Prime applications use back-end processes to manage application-specific activities or jobs. The process management tools enable you to manage these backend processes to optimize or troubleshoot the LMS Server.

You can do the following activities:
- View the details of all processes
- Filter and show only processes of a specific state
- Start the processes
- Stop the processes

All mandatory processes are started when you start the system.

See LMS Back-end Processes for a list of Cisco Prime back-end processes used by LMS.

You can manage the Cisco Prime processes through CLI. See Managing Processes Through CLI for more information.

Note
Your role and privileges determine whether you can use this option.

This section contains the following:
- Process States
- Viewing Process Details
- Viewing Processes of a Specific State
- Starting a Process
- Stopping a Process

Process States
The state of the Cisco Prime backend processes fall under either one of the following categories:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running normally</td>
<td>Processes are started and are running normally.</td>
</tr>
<tr>
<td></td>
<td>Sometimes, you find the state of a few processes as follows:</td>
</tr>
<tr>
<td></td>
<td>Program started - No mgt msgs received</td>
</tr>
<tr>
<td></td>
<td>This indicates that the processes are started automatically at boot and are running normally.</td>
</tr>
<tr>
<td>Never started</td>
<td>Processes that cannot start automatically and are to be started by operator or administrator.</td>
</tr>
<tr>
<td>Failed to run</td>
<td>Processes that failed to start because of an error in the system.</td>
</tr>
<tr>
<td>Administratively</td>
<td>Processes that are stopped by the system or by the administrator.</td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
</tr>
</tbody>
</table>
Managing Processes

Viewing Process Details

To view Process details:

**Step 1**
Select **Admin > System > Server Monitoring > Processes**.

The Process Management page appears with all Cisco Prime processes listed.

You can see the following information of a Cisco Prime process in the Process Management window:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProcessName</td>
<td>Name of the process. Describes how the process is registered. See LMS Back-end Processes for more information on process description. For information on suite-specific processes, see the relevant Online help. You cannot view the details of Apache and Tomcat processes or restart them from the user interface. But you can view the details of these processes in Process Status report (Reports &gt; System &gt; Status &gt; Process).</td>
</tr>
<tr>
<td>ProcessState</td>
<td>Process status and a summary of the log file entries for the process. If the process fails, this column is highlighted in red.</td>
</tr>
<tr>
<td>ProcessId</td>
<td>Unique number by which the operating system identifies each running program.</td>
</tr>
<tr>
<td>ProcessRC</td>
<td>Return code. 0 represents normal program operation. Any other number represents an error. See the error log for details.</td>
</tr>
<tr>
<td>ProcessSigNo</td>
<td>Signal number. 0 represents normal program operation. Any other number is the last signal delivered to the program before it terminated.</td>
</tr>
<tr>
<td>ProcessStartTime</td>
<td>Time and date on which the process was started.</td>
</tr>
<tr>
<td>ProcessStopTime</td>
<td>Time and date on which the process was stopped.</td>
</tr>
</tbody>
</table>

**Step 2**
Click the ProcessName link of a process to view its details.

The Process Details popup window appears with the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Name of the process.</td>
</tr>
<tr>
<td>Path</td>
<td>File Location.</td>
</tr>
<tr>
<td>Flags</td>
<td>Flags used to register the process with the Daemon Manager.</td>
</tr>
<tr>
<td>Startup</td>
<td>Method used to start the process (manual or automatic).</td>
</tr>
<tr>
<td>Dependencies</td>
<td>Other processes that are running, and that are required for this process to run.</td>
</tr>
</tbody>
</table>
Step 3 Click OK.

You can click the Refresh icon on the top-right corner of the page to initiate a page refresh and view the updated information of the processes.

**Viewing Processes of a Specific State**
To view processes of a specific state:

---

**Starting a Process**
To start a process:

**Step 1** Select Admin > System > Server Monitoring > Processes. The Process Management page appears.

**Step 2** Select the check box corresponding to the process.

**Step 3** Click Start.

**Stopping a Process**
To stop a process:

**Step 1** Select Admin > System > Server Monitoring > Processes. The Process Management page appears.

**Step 2** Select the check box corresponding to the process.
Step 3  Click Stop.

LMS Back-end Processes

The back-end processes in the LMS Server are required to manage application specific activities and jobs.

Table 3-1 lists the back-end processes in LMS Server, their description and dependent processes.

In LMS 4.2, Compliance and Audit Manager (CAAM) Server is added as a new back-end process.

Log files for most of the processes are located in the following locations:

- On Solaris/Soft Appliance—var/adm/CSCOpx/log
- On Windows—NMSROOT\log, where NMSROOT is your Cisco Prime default installation directory.

You can also manage the Cisco Prime processes through CLI. You can perform the following activities through CLI:

- Viewing Process Details Through CLI
- Viewing Brief Details of Processes
- Viewing Processes Statistics
- Starting a Process
- Stopping a Process

This section contains:

- Server Back-end Processes
- Inventory, Config and Image Management Processes
- Network Topology, Layer 2 Services and User Tracking Processes
- IPSLA Performance Management Processes and Dependency Processes
- Device Performance Management Module Processes
- Fault Management Processes

Server Back-end Processes

Table 3-1 lists the LMS 4.2 Server Back-end processes and their dependency processes.
<table>
<thead>
<tr>
<th>Process Name</th>
<th>Description</th>
<th>Normal Process State</th>
<th>Dependent Process</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>Apache web server used on both UNIX and Windows systems. This hosts the base Cisco Prime home page and all major applications. You cannot view the details of this process or restart this process from the user interface (from Process Management page).</td>
<td>Program started - No mgt msgs received</td>
<td>TomcatMonitor</td>
<td>NMSRoot\MDC\Apache\logs (On Windows) /opt/CSCOpx/MDC/ Apache/logs (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>CmfDbEngine</td>
<td>Sybase database instance used by the base Cisco Prime framework.</td>
<td>Program started - No mgt msgs received</td>
<td>None</td>
<td>NMSRoot/MDC/log/daemons.log (On Solaris/Soft Appliance only)</td>
</tr>
<tr>
<td>CmfDbMonitor</td>
<td>Monitors the CmfDbEngine process and periodically checks for connectivity and SQL errors.</td>
<td>Running normally</td>
<td>CmfDbEngine</td>
<td>NMSRoot\log\CmfDbMonitor.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/CmfDbMonitor.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>CMFOGSServer</td>
<td>Device grouping service in CS that provides grouping capability based on device attributes stored in DCRServer.</td>
<td>Program started - No mgt msgs received</td>
<td>CmfDbMonitor, EssMonitor, DCRServer</td>
<td>NMSRoot\log\CMFOGSServer.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/CMFOGSServer.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>CSDiscovery</td>
<td>Transient process created by Daemon Manager. This process initiates Device Discovery.</td>
<td>Transient Terminated</td>
<td>—</td>
<td>NMSRoot\log\CSDiscovery.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/CSDiscovery.log (On Solaris/Soft Appliance)</td>
</tr>
</tbody>
</table>
### Table 3-1  Cisco Prime LMS 4.2 Server Back-end Processes and their Descriptions

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Description</th>
<th>Normal Process State</th>
<th>Dependent Process</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSRegistryServer</td>
<td>Registry Server for other CS processes such as DCRServer and CMFOGSServer and provides the backbone for inter-process communication for DCRServer and CMFOGSServer. Sometimes, the Tomcat process may start this process. In such cases, the process status is displayed as follows: Administrator has shut down this server. You can ignore this error message.</td>
<td>Running normally</td>
<td>—</td>
<td>NMSRoot\log\CSRegistryServer.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCRServer</td>
<td>Device List and Credential Repository Server that provides the repository for shared device list and credentials to be used across applications.</td>
<td>Running normally</td>
<td>TomcatMonitor, CmfDbMonitor, EssMonitor</td>
<td>NMSRoot\log\DCRServer.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCRDevicePoll</td>
<td>Transient process created by Daemon Manager. This process initiates Device Polling.</td>
<td>Transient Terminated</td>
<td>—</td>
<td>NMSRoot\log\DCRDevicePoll.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/DCRDevicePoll.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>diskWatcher</td>
<td>Monitors disk space availability on the LMS Server. See Configuring Disk Space Threshold Limit for more information.</td>
<td>Running normally</td>
<td>—</td>
<td>NMSRoot\log\diskWatcher.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/diskWatcher.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDS</td>
<td>Legacy Event Distribution engine. This is currently used by some applications to send and receive event messages.</td>
<td>Running normally</td>
<td>NameService-Monitor</td>
<td>NMSRoot\log\EDS.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
</tbody>
</table>
### Table 3-1  Cisco Prime LMS 4.2 Server Back-end Processes and their Descriptions

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Description</th>
<th>Normal Process State</th>
<th>Dependent Process</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDS-GCF</td>
<td>EDS - Generic Consumer Framework process. It is an extension to EDS that allows Generic Event Consumers to provide a pluggable event interface.</td>
<td>Running normally</td>
<td>EDS, CmfDb-Monitor</td>
<td>NMSRoot\log\EDS-GCF.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>ESS</td>
<td>Event Services Software. The new engine that handles distribution of events between processes. This is slated to eventually replace EDS.</td>
<td>Program started - No mgt msgs received</td>
<td>—</td>
<td>NMSRoot\log\ESS.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>EssMonitor</td>
<td>Monitors ESS process to check if events related functionality works properly. This process shuts down automatically when the ESS process fails or does not function properly.</td>
<td>Running normally</td>
<td>ESS</td>
<td>NMSRoot\log\EssMonitor.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>EventFramework</td>
<td>Event management bus, LMS uses this to facilitate event transmissions between daemons.</td>
<td>Program started - No mgt msgs received</td>
<td>EssMonitor</td>
<td>No log files</td>
</tr>
<tr>
<td>FDRewinder</td>
<td>Enables the rotation of log files functionality using logrot.</td>
<td>Never started</td>
<td>—</td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>(Solaris/Soft Appliance Only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>jrm</td>
<td>Job and Resource Manager. This allows scheduling of jobs to be run at specific times. It also allows locking and unlocking of resources.</td>
<td>Program started - No mgt msgs received</td>
<td>CmfDbMonitor, NameService-Monitor, EDS, EssMonitor</td>
<td>NMSRoot\log\jrm.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>LicenseServer</td>
<td>Provides Licensing functionality for evaluation and file based licensing mechanisms.</td>
<td>Program started - No mgt msgs received</td>
<td>—</td>
<td>NMSRoot\log\LicenseServer.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
</tbody>
</table>
### Table 3-1  Cisco Prime LMS 4.2 Server Back-end Processes and their Descriptions

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Description</th>
<th>Normal Process State</th>
<th>Dependent Process</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>NameService-Monitor</td>
<td>Name Service agent that monitors objects and messages and acts as a gateway between the JacORB clients and the Name Server.</td>
<td>Running Normally</td>
<td>NameServer</td>
<td>NMSRoot/log\NameServiceMonitor.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>NameServer</td>
<td>Object Request Broker for the JacORB framework used in Cisco Prime.</td>
<td>Program started - No mgt msgs received</td>
<td></td>
<td>NameServer.log (On Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)</td>
</tr>
</tbody>
</table>
| Tomcat              | Java servlet engine used on Windows, Solaris and Soft Appliance systems hosting applications based on the Cisco Prime desktop.  
You cannot view the details of this process or restart this process from the user interface (from Process Management page).                        | Program started - No mgt msgs received |                   | NMSRoot/log\tomcat/logs/stdout.log (On Windows)                                                    |
|                     |                                                                                                                                                                                                            |                                       |                   | /opt/CSCOpx/MDC/tomcat/logs/stdout.log(On Solaris/Soft Appliance)                                  |
| TomcatMonitor       | Monitors the health of the Tomcat process and shuts down automatically when Tomcat fails or does not function properly.                                                                                  | Running normally                      | Tomcat            | NMSRoot/log\TomcatMonitor.log (On Windows)                                                        |
|                     |                                                                                                                                                                                                            |                                       |                   | /var/adm/CSCOpx/log/daemons.log (On Solaris/Soft Appliance)                                       |
## Inventory, Config and Image Management Processes

Table 3-2 lists Inventory, Config and Image Management processes, and their dependency processes.

### Table 3-2 Inventory, Config and Image Management Processes and Dependency Processes

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Dependency (Sequential)</th>
<th>Log Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMEDbEngine</td>
<td>None</td>
<td>NA</td>
<td>System service: the database engine for Inventory, Config and Image Management applications.</td>
</tr>
<tr>
<td>ConfigMgmtServer</td>
<td>EssentialsDM</td>
<td>dcmaservice.log</td>
<td>Configuration Management service performs the following tasks,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Collects the configuration for the LMS managed devices on request from jobs or user Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Archives new version if there is a difference between the fetched configuration and the latest configuration in archive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Parses the configuration based on configlet rules and generates differences between the configurations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Logs change record for every new version of archived running configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Detects config changes on the device and triggers configuration collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Caches the device and NetConfig template mapping information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Populates the database with NetShow system-defined command sets and NetShow commands by retaining them from device packages.</td>
</tr>
<tr>
<td>ConfigUtilityService</td>
<td>EssentialsDM</td>
<td>cfgutilservice.log</td>
<td>ConfigUtilityService parses the archived configurations of the devices for assessing the technology readiness of the devices. It does config and CLI parsing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ConfigUtilityService also performs OGS grouping attributes updates at the end of Inventory collection.</td>
</tr>
<tr>
<td>SyslogCollector</td>
<td>ESS</td>
<td>SyslogCollector.log</td>
<td>Filters and sends the syslog objects to various SyslogAnalyzer services subscribed to it.</td>
</tr>
</tbody>
</table>
### Table 3-2  
**Inventory, Config and Image Management Processes and Dependency Processes (continued)**

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Dependency (Sequential)</th>
<th>Log Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EssentialsDM</td>
<td>ESS</td>
<td>EssentialsDM_Server.log</td>
<td>It publishes a dummy Common Services Transport Mechanism (CSTM) service name to synchronize publishing of service names with CSTM. All other LMS services that publish service names with CSTM are made dependant on this service either directly or indirectly. After adding devices to LMS, this service triggers for Inventory and Configuration collection. System service that monitors the accessibility of the LMS database engine that helps to ensure that the system is not started until the database engine is ready.</td>
</tr>
<tr>
<td></td>
<td>DCRSServer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LMSDbEngine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWiseUI.log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWiseConfiguration.log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWiseMonitoring.log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWiseCollection.log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWiseNative.log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWiseComplianceCheck.log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWiseNativeCompliance.log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWisePurge.log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnergyWiseNativePolicy.log</td>
<td></td>
</tr>
<tr>
<td>CTMJrmServer</td>
<td>EssentialsDM JRM</td>
<td>CTMJrmServer.log</td>
<td>This service is a proxy to the JRM service. This is used by LMS to connect to the JRM service. It hides all the direct interaction with JRM.</td>
</tr>
<tr>
<td></td>
<td>jrm</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tomcat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ChangeAudit</td>
<td>EssentialsDM CTMJrmServer</td>
<td>ChangeAudit.log</td>
<td>Change Audit program that provides back-end database services for applications that want to log network changes and for Change Audit reports and Automated actions.</td>
</tr>
<tr>
<td></td>
<td>jrm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Managing Processes

If you stop or restart any of these processes you must stop and restart their dependency processes. See Table 3-2 for the list of dependent processes.

You can stop and restart the process using **Admin > System > Server Monitoring > Processes**.

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Dependency (Sequential)</th>
<th>Log Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICServer</td>
<td>ESS CTMJrmServer</td>
<td>IC_Server.log</td>
<td>This is a service that collects and stores Inventory information from the device using SNMP. It also detects changes that occurred between the last time Inventory was collected for a device, and the current Inventory collection.</td>
</tr>
<tr>
<td>SyslogAnalyzer</td>
<td>ESS EssentialsDM CTMJrmServer jrm</td>
<td>SyslogAnalyzer.log for Windows AnalyzerDebug.log for Solaris/Soft Appliance</td>
<td>It takes the filter definition from the user and sends it to the various Syslog Collectors it is subscribed to. Receives the syslogs from the Syslog collector and inserts them into the database and also takes automated actions from the user.</td>
</tr>
<tr>
<td>PMCOGSServer</td>
<td>LMSOGSServer</td>
<td>PMCOGSServer.log</td>
<td>Port and Module group administration service. This is used for managing Port and Module groups.</td>
</tr>
<tr>
<td>ANIDbEngine</td>
<td>None</td>
<td>None</td>
<td>System service: Database engine for Topology and Identity Services.</td>
</tr>
<tr>
<td>ANIServer</td>
<td>EDS ANIDbEngine</td>
<td>ani.log</td>
<td>System service: Collects device information for Topology and Identity Services.</td>
</tr>
<tr>
<td>MACUHIC</td>
<td>EssMonitor ANIDbEngine</td>
<td>macuhic.log</td>
<td>System service: Receives and processes SNMP traps for Dynamic UT</td>
</tr>
<tr>
<td>UTLITE</td>
<td>EssMonitor ANIDbEngine</td>
<td>utlite.log</td>
<td>System service: Receives and processes the UTLITE data</td>
</tr>
<tr>
<td>UTMajorAcquisition</td>
<td>ANIServer</td>
<td>ut.log</td>
<td>UTMajor Acquisition is a transient process. System service: Collects end hosts information.</td>
</tr>
<tr>
<td>UTManager</td>
<td>EssMonitor ANIDbEngine</td>
<td>utm.log</td>
<td>System service: Queries external system for Dynamic UT</td>
</tr>
<tr>
<td>VNMServer</td>
<td>ANIDbEngine</td>
<td>Vnmserver.log</td>
<td>System service: Handles VRF Lite Services like configuration, VRF Lite collector job scheduling</td>
</tr>
<tr>
<td>WlseUHIC</td>
<td>ANIDbEngine</td>
<td>wlseuhic.log</td>
<td>System service: Collects information from Wlse Device</td>
</tr>
<tr>
<td>Compliance and Audit Manager (CAAM) Server</td>
<td>Essentials DM</td>
<td>caam_server.log cammserverui.log caamserversetemploid.log</td>
<td>The Compliance and Audit Manager server collects information from the Inventory and Configuration management servers and stores the details in a database.</td>
</tr>
</tbody>
</table>

Table 3-2 Inventory, Config and Image Management Processes and Dependency Processes (continued)
Network Topology, Layer 2 Services and User Tracking Processes

Table 3-3 lists Inventory, Config and Image Management processes, and their dependency processes.

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Dependency (Sequential)</th>
<th>Log Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANIDbEngine</td>
<td>None</td>
<td>None</td>
<td>System service: Database engine for Topology and Identity Services.</td>
</tr>
<tr>
<td>ANIServer</td>
<td>EDS</td>
<td>ani.log</td>
<td>System service: Collects device information for Topology and Identity Services.</td>
</tr>
<tr>
<td></td>
<td>ANIDbEngine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MACUHIC</td>
<td>EssMonitor</td>
<td>macuhic.log</td>
<td>System service: Receives and processes SNMP traps for Dynamic UT</td>
</tr>
<tr>
<td></td>
<td>ANIDbEngine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTLITE</td>
<td>EssMonitor</td>
<td>utlite.log</td>
<td>System service: Receives and processes the UTLITE data</td>
</tr>
<tr>
<td></td>
<td>ANIDbEngine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTMajorAcquisition</td>
<td>ANIServer</td>
<td>ut.log</td>
<td>UTMajor Acquisition is a transient process. System service: Collects end hosts information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTManager</td>
<td>EssMonitor</td>
<td>utm.log</td>
<td>System service: Queries external system for Dynamic UT</td>
</tr>
<tr>
<td></td>
<td>ANIDbEngine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DCRServer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VNMServer</td>
<td>ANIDbEngine</td>
<td>Vnmserver.log</td>
<td>System service: Handles VRF Lite Services like configuration, VRF Lite collector job scheduling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WlseUHIC</td>
<td>ANIDbEngine</td>
<td>wlseuhic.log</td>
<td>System service: Collects information from Wlse Device</td>
</tr>
</tbody>
</table>
IPSLA Performance Management Processes and Dependency Processes

Table 3-4 lists the LMS 4.2 Performance Management processes and their dependency processes.

Table 3-4 LMS 4.2 IPSLA Performance Management Process and the Dependency Processes

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Description</th>
<th>Dependency (Sequential)</th>
<th>Default State</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPMProcess</td>
<td>Provides core function of managing IPSLA Performance Management Devices, Collectors and Operations in LMS.</td>
<td>DCRServer, IpmDbEngine jrm</td>
<td>Program Started</td>
<td>ipmserver.log,dmgtd.log</td>
</tr>
<tr>
<td>IPMOGSServer</td>
<td>IPSLA Performance Management group administration service. This is used for managing IPSLA Performance Management collector groups. It is also used for IPSLA Performance Management Collector selector.</td>
<td>CmfDbMonitor, EssMonitor, DCRServer, IpmDbEngine</td>
<td>Program Started</td>
<td>IPMOGSServer.log, IPMOGSClient.log</td>
</tr>
<tr>
<td>IpmDbEngine</td>
<td>IPSLA Performance Management Database Engine service. It is used for managing and storing IPSLA Performance Management related information on the database</td>
<td>NA</td>
<td>Program Started</td>
<td>dmgtd.log</td>
</tr>
</tbody>
</table>

Device Performance Management Module Processes

Table 3-5 gives a description of key processes in Device Performance Management module.

Table 3-5 Key Processes in LMS 4.2 Device Performance Management Module

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Description</th>
<th>Dependent Process</th>
<th>Default State</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPMDbEngine</td>
<td>This is the Device Performance Management database engine process. If this process is down, you will not be able to access Device Performance Management module of LMS, and polling, threshold monitoring, and trendwatch monitoring will fail.</td>
<td>None</td>
<td>Started</td>
<td>None</td>
</tr>
</tbody>
</table>
Managing Processes

Table 3-5  Key Processes in LMS 4.2 Device Performance Management Module

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Description</th>
<th>Dependent Process</th>
<th>Default State</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPMDbMonitor</td>
<td>Responsible for monitoring the UPMDbEngine process.</td>
<td>UPMDbEngine</td>
<td>Started</td>
<td>UPMDbMonitor.log</td>
</tr>
<tr>
<td>UPMPProcess</td>
<td>Responsible for the Polling engine, Threshold monitoring and Poller Management features of LMS. If this process is down, poller management, threshold management, trendwatch management will fail.</td>
<td>DCRServer, UPMDbMonitor</td>
<td>Started</td>
<td>upm_process.log</td>
</tr>
</tbody>
</table>

Fault Management Processes

Table 3-6 provides a complete list of Fault Management-related Cisco Prime processes. Logs for most of these processes are provided in Table 1-2.

Table 3-6  Fault Management Related Processes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Dependency</th>
<th>Default State</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdapterServer/AdapterServer 1</td>
<td>Event adapter takes events from backend servers.</td>
<td>None</td>
<td>Program Started</td>
<td>adapterServer.log, adapterServer1.log, daemons.log</td>
</tr>
<tr>
<td>DataPurge</td>
<td>Data Purge—Starts as scheduled in the GUI and purges the Fault History database.</td>
<td>jrm</td>
<td>Administrator has shut down this server</td>
<td>DPS.log, daemons.log</td>
</tr>
</tbody>
</table>
Table 3-6  Fault Management Related Processes (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Dependency</th>
<th>Default State</th>
<th>Log Files</th>
</tr>
</thead>
</table>
| DfmBroker           | Fault Management Broker maintains a registry about Fault Management domain managers, that register the following information with the broker when its initialization is complete:  
• Application name of the domain manager  
• Hostname on which the domain manager is running  
• TCP port at which the HTTP server is listening  
When a client needs to connect to the domain manager, it first connects to the broker to determine the hostname and TCP port the HTTP service of that server is listening.  
It then disconnects from the broker and establishes a connection to the domain manager.  
The DfmBroker log file is located at NMSROOT/objects/smarts/local/logs/brstart.log. | None          | Program Started | brstart.log        |
| DFMLogServer        | Controls Fault Management logs.                                              | None          | Program Started | DfmLogService.log, daemons.log |
| DFMMultiProcLogger  | Handles processes with multiple threads.                                     | None          | Program Started | MultiProcLogger.log, daemons.log |
| DFMOGSServer        | Fault Grouping Service Server evaluates group membership.                   | DfmBroker     | Running Normally | DFMOGSServer.log      |
| DfmServer/DfmServer | Infrastructure device domain manager, a program that provides backend services for Fault Management. Services include SNMP data retrieval and event analysis. The DfmServer log is NMSROOT/objects/smarts/logs/DFM.log.  
If there are two instances of the DfmServer running, each will have a log file, DFM.log and DFM1.log. | DfmBroker     | Running Normally | DFM.log, DFM1.log     |
| DFMCTMStartup       | Handles interprocess communication.                                          | None          | Administrator has shut down this server | DFMCTMStartup.log, daemons.log |
| EPMDbEngine         | Event Promulgation Module (EPM) database engine—Repository for the EPM module. | None          | Program Started | EPM.log              |
| EPMSServer          | Sends events to notification services.                                        | EPMDbEngine   | Running Normally | EPM.log              |
### Table 3-6  Fault Management Related Processes (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Dependency</th>
<th>Default State</th>
<th>Log Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>FHDDBengine</td>
<td>Fault History database engine—Repository for alerts and events.</td>
<td>None</td>
<td>Program Started</td>
<td>daemons.log</td>
</tr>
<tr>
<td>FHPurgeTask</td>
<td>Fault History purge task.</td>
<td>None</td>
<td>Transient terminated</td>
<td>FHCollector.log, FHUI.log</td>
</tr>
<tr>
<td>FHSserver</td>
<td>Fault History server, a program that runs backend services for Fault History.</td>
<td>EPMServer, EPMDbEngine, FHDBEngine</td>
<td>Running Normally</td>
<td>FHSserver.log</td>
</tr>
<tr>
<td>Interactor</td>
<td>Provides inventory and device information to the Detailed Device View (DDV); updates the DDV with events.</td>
<td>InventoryCollector</td>
<td>Program Started</td>
<td>Interactor.log</td>
</tr>
<tr>
<td>Interactor 1</td>
<td>Provides inventory and device information to the Detailed Device View (DDV); updates the DDV with events.</td>
<td>Inventory Collector 1</td>
<td>Program Started</td>
<td>Interactor1.log</td>
</tr>
<tr>
<td>InventoryCollector / InventoryCollector 1</td>
<td>Synchronizes voice device inventory with infrastructure device inventory. Handles all inventory events, such as adding and deleting devices.</td>
<td>ESS, TISServer, DFMOGSServer</td>
<td>Running Normally/Program Started</td>
<td>InventoryCollector.log, InventoryCollector1.log</td>
</tr>
<tr>
<td>INVDBengine</td>
<td>Inventory database engine—Repository for devices.</td>
<td>None</td>
<td>Program Started</td>
<td>daemons.log</td>
</tr>
<tr>
<td>NOSserver</td>
<td>Notification Server monitors alerts and sends notifications based on subscriptions.</td>
<td>EPMDbEngine, EPMServer, INVDBEngine, DFMOGSServer</td>
<td>Running Normally</td>
<td>nos.log</td>
</tr>
<tr>
<td>PTMServer</td>
<td>Polling and thresholds server.</td>
<td>DFMOGSServer</td>
<td>Running Normally</td>
<td>PTMServer.log</td>
</tr>
<tr>
<td>PMServer</td>
<td>PMServer is used for the Partition Manager functionality for the Fault Management module of LMS. When you add a device to the Fault Management module, it is always added to the default partition 0. All the debug logs related to PMServer can be found at NMSROOT/log/dfmLogs/PM</td>
<td>INVDBEngine EssMonitor</td>
<td>Running Normally</td>
<td>PMServer.log (For Windows) daemons.log (For Solaris/Soft Appliance)</td>
</tr>
<tr>
<td>TISServer</td>
<td>Inventory server.</td>
<td>EssMonitor, INVDBEngine</td>
<td>Program Started</td>
<td>TISServer.log</td>
</tr>
</tbody>
</table>
Backing Up Data

You should back up the database regularly so that you have a safe copy of the database. You can schedule immediate, daily, weekly, or monthly automatic database backups. You should have necessary privileges to use this option.

You cannot back up the database while restoring the database. LMS uses multiple databases to store client application data. These databases are backed up whenever you perform a backup.

Backup requires enough storage space on the target location for the backup to start.

If your current license count is lower than your earlier license count, and you restore the data now, devices that exceed the current licence count will be moved to Suspended state.

⚠️ Caution

You should never backup data to the Cisco Prime Installation directory `NMSROOT/backup`. Sometimes, storing the backup data in this location may corrupt the Cisco Prime installation.

This section explains:

- Scheduling a Backup
- Restoring Data
- Changing the Database Password
- Effects of Backup-Restore on DCR
- Master-Slave Configuration Prerequisites and Restore Operations
- Effects of Backup-Restore on Groups

Scheduling a Backup

You can schedule a backup using the LMS UI or use the backup utility through CLI. See, Backing up Data Using CLI for more information.

To schedule a backup:

1. **Step 1** Select Admin > System > Backup.
   The Backup Job page appears.

2. **Step 2** Enter the appropriate information in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Directory</td>
<td>Location of the backup directory. We recommend that your target location be on a different partition than the Cisco Prime installation location. The backup directory should not contain any special character.</td>
</tr>
<tr>
<td>Generations</td>
<td>Maximum number of backups to be stored in the backup directory.</td>
</tr>
<tr>
<td>Time</td>
<td>From the lists, select the time period between which you want the backup to occur. Use a 24-hour format.</td>
</tr>
</tbody>
</table>
Backing Up Data

Step 3  Click **Apply**.

The Schedule Backup message verifies your schedule and provides the location of backup log files. Examine the log file at the following location to verify backup status:

On Solaris/Soft Appliance:
/var/adm/CSCOpx/log/dbbackup.log

On Windows:
NMSROOT\log\dbbackup.log

You can remove the scheduled backup at any time. Click **Remove** to delete the scheduled backup job. The Remove button appears only if you have scheduled any backup.

---

Restoring Data

The new restore framework supports restore across versions. This enables you to restore data from versions 3.1, 3.2. The restore framework checks the version of the archive.

- If the archive is of the current version, then the restore from current version is run.
- If the backup archive is of an older version, the backup data is converted to LMS format, if needed, and applied to the machine.

You can restore your database by running a script from the command line. You have to shut down and restart Cisco Prime while restoring data.
In all backup-restore scenarios, a backup is taken from a machine A, and the backed up data, say Ab, is restored on the same machine A, or on a different machine B.

Ensure that you do not run any critical tasks during data restoration. Otherwise, you may lose the data of such tasks.

For details on effect of restore operation on DCR modes, and Groups, see Effects of Backup-Restore on DCR and Effects of Backup-Restore on Groups.

**Caution**
Restoring the database from a backup permanently replaces your database with the backed up version.

The list of applications in a backup archive should match the list of applications installed on the LMS Server where you want to restore the data. You should not continue the restore when there is a mismatch, as it may cause problems in the functionality of Cisco Prime applications.

This section explains the following:
- Restoring Data On Solaris/Soft Appliance
- Restoring Data On Windows

### Restoring Data On Solaris/Soft Appliance

To restore the data on Solaris/Soft Appliance:

1. **Step 1** Log in as the superuser, and enter the root password.
2. **Step 2** Stop all processes by entering:
   ```bash
   /etc/init.d/dmgtd stop
   ``
3. **Step 3** Restore the database by entering:
   ```bash
   /opt/CSCOpx/bin/perl /opt/CSCOpx/bin/restorebackup.pl [-t temporary directory] [-gen generationNumber] [-d backup directory] [-h]
   ```
   - **[-t temporary directory]**—The restore framework uses a temporary directory to extract the content of backup archive.
     By default the temporary directory is created under NMSROOT as NMSROOT/tempBackupData. You can customize this, by using this –t option, where you can specify your own temp directory. This is to avoid overloading NMSROOT
   - **[-gen generationNumber]**—Optional. By default, it is the latest generation. If generations 1 through 5 exist, then 5 will be the latest.
   - **[-d backup directory]**—Required. Which backup directory to use.
   - **[-h]**—Provides help. When used with -d <backup directory> syntax, shows correct syntax along with available suites and generations.

   To restore the most recent version, enter:
   ```bash
   /opt/CSCOpx/bin/perl /opt/CSCOpx/bin/restorebackup.pl -d backup directory
   ```
   For example, -d /var/backup

4. **Step 4** Examine the log file in the following location to verify that the database was restored by entering:
   ```bash
   /var/adm/CSCOpx/log/restorebackup.log
   ``
5. **Step 5** Restart the system:
   ```bash
   /etc/init.d/dmgtd start
   ```
Restoring Data On Windows
To restore the data on Windows, make sure you have the correct permissions, and do the following:

Step 1  Stop all processes by entering the following at the command line:
net stop crmdmgtd

Step 2  Restore the database by entering:
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl [ -t temporary directory] [ -gen
  generationNumber] [ -d backup directory] [ -h]

where NMSROOT is the Cisco Prime installation directory. See the previous section for command option
descriptions.

To restore the most recent version, enter the following command:
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup directory

Step 3  Examine the log file in the following location to verify that the database was restored by entering:
NMSROOT\log\restorebackup.log

Step 4  Restart the system by entering:
net start crmdmgtd

Note  For more details on restoring data see Migrating Data to Cisco Prime LAN Management Solution 4.2 in
Installing and Migrating to Cisco Prime LAN Management Solution 4.2

Changing the Database Password

You must enter the database password while installing Cisco Prime. If you do not enter the password,
Cisco Prime generates the password at random. However, we recommend that you change the password
periodically to ensure system security.

Caution  You need to shut down Cisco Prime, change the password and then restart Cisco Prime, for the changes
to take effect. Make sure you are not running any critical tasks. Otherwise, you might lose data.

This section explains the following:
•  Changing Password on Solaris/Soft Appliance
•  Changing Password on Windows
•  Formats Available for Changing the Database Password

Changing Password on Solaris/Soft Appliance
To change the password on Solaris/Soft Appliance:

Step 1  Log in as the superuser, and enter the root password.
Step 2  Stop all processes by entering:
/etc/init.d/dmgtd stop

Step 3  Change to the installation directory by entering:

cd NMSROOT/bin

NMSROOT is your default Cisco Prime installation directory.

Step 4  Enter the following command to list the different formats available for changing the database password:

NMSROOT/bin/perl dbpasswd.pl

Step 5  When prompted, enter the new password and verify it by re-entering it.
The password can contain a maximum of 30 characters.

Step 6  Start all processes by entering:

/etc/init.d/dmgtd start

---

**Changing Password on Windows**

To change the password on Windows:

---

Step 1  At the command line, make sure you have the correct permissions.

Step 2  Stop all processes by entering:

net stop crmdmgtd

Step 3  Change to the Installation Directory by entering:

    cd NMSROOT\bin

NMSROOT is your default Cisco Prime installation directory.

Step 4  Enter the following command to list the different formats available for changing the database password:

    NMSROOT\bin\perl dbpasswd.pl

Step 5  When prompted, enter the new password and verify it by re-entering it.
The password can contain a maximum of 30 characters.

Step 6  Start all processes by entering:

    net start crmdmgtd
## Formats Available for Changing the Database Password

The different formats available and the commands for changing the database passwords on Windows, Solaris and Soft Appliance platforms are tabulated below:

<table>
<thead>
<tr>
<th>Format</th>
<th>Command</th>
</tr>
</thead>
</table>
| Format 1 detects the available datasource names and databases and prompts you to enter and confirm the passwords for each of them. It also allows you to encrypt the password. | On Solaris/Soft Appliance:  
\[ \text{NMSROOT}/bin/perl dbpasswd.pl all \]  
On Windows:  
\[ \text{NMSROOT}\bin\perl dbpasswd.pl all \] |
| Format 2 allows you to list all the databases and datasource names (DSNs) available in the server. | On Solaris/Soft Appliance:  
\[ \text{NMSROOT}/bin/perl dbpasswd.pl listdsn \]  
On Windows:  
\[ \text{NMSROOT}\bin\perl dbpasswd.pl listdsn \] |
| Format 3 allows you to change the database password. | On Solaris/Soft Appliance:  
\[ \text{NMSROOT}/bin/perl dbpasswd.pl dsn=odbc_datasource \]  
On Windows:  
\[ \text{NMSROOT}\bin\perl dbpasswd.pl dsn=odbc_datasource \] |
| Format 4 allows you to change the database password for a specific DSN. It also allows you to enter a new password in the command line using the `npwd` option. | On Solaris/Soft Appliance:  
\[ \text{NMSROOT}/bin/perl dbpasswd.pl dsn=dsn-name npwd=new-password \]  
On Windows:  
\[ \text{NMSROOT}\bin\perl dbpasswd.pl dsn=dsn-name npwd=new-password \] |
| Format 5 allows you to encrypt the existing database password. | On Solaris/Soft Appliance:  
\[ \text{NMSROOT}/bin/perl dbpasswd.pl dsn=dsn-name npwd=new-password \]  
On Windows:  
\[ \text{NMSROOT}\bin\perl dbpasswd.pl dsn=dsn-name npwd=new-password \] |
| Format 6 allows you to change the database password for a specific DSN. Format 6.0 also:  
• Allows you to enter a new password in the command line using the `npwd` option.  
• Allows you to encrypt the password using the `encryption` option. | On Solaris/Soft Appliance:  
\[ \text{NMSROOT}/bin/perl dbpasswd.pl dsn=dsn-name npwd=new-password encryption=yes \]  
On Windows:  
\[ \text{NMSROOT}\bin\perl dbpasswd.pl dsn=dsn-name npwd=new-password encryption=yes \] |

## Effects of Backup-Restore on DCR

Data changes are a normal part of any restore from a backup. However, because Device and Credential Repository (DCR) is a distributed system with varying modes, it is also possible for any restored DCR to:

• Change modes.
For example, a Standalone DCR can be set after a backup to act as a Slave. When the restore is performed, it will be reset to the Standalone mode. It depends on the DCR mode of the machine from which the backup was taken (source machine), and the machine on which the data was restored (target machine).

- Change Master/Slave relationships.

For example, a DCR Slave may be using Master A at the time a backup is taken. Later, the domain may be changed to use Master B, and the Slave reset to use Master B. When the restore is performed, the Slave will attempt to use Master A.

For detailed information on DCR, see *Managing Device and Credentials* in *Inventory Management Guide*.

The following scenarios helps you understand the implications of Restore operations on DCR.

- Restoring Data From a DCR Standalone
- Restoring Data From S1 on S1
- Restoring Data From S1 to M1
- Restoring Data From S1 on M2
- Restoring Data From M1 on M1
- Restoring Data From M1 to M2

**Restoring Data From a DCR Standalone**

If you restore the data backed up from a machine in the Standalone mode, on any machine whose working mode is either Standalone, Master, or Slave, the end mode will be Standalone.

Let X be a machine in Standalone mode.

If you restore the data backed up from X, say X\(b\), on another Standalone machine Y, or a Slave S, or a Master M, the end mode of Y, S, and M will be Standalone. Also, any slave of M will switch to Standalone mode.

Further scenarios can be better explained based on the following DCR set up.

Let us assume there are two DCR domains.

- For Domain 1, you have M1 as Master, and S1, and S2 as Slaves.
- For Domain 2, you have M2 as Master, and S3, and S4 as Slaves.

**Restoring Data From S1 on S1**

Suppose you take a backup from S1. After sometime, you restore the backed up data, say S1\(b\), on S1. S1 will look for its Master M1, and the Master-Slave relation between S1 and M1 will be intact, since M1 is available.

However, note that the restore on S1 will practically be of no effect since S1 and M1 will synchronize after the restore on S1. The changes that have taken place after the backup was taken from S1 will be reflected in S1, even if S1\(b\) is restored on S1.

In the above example, if the restore on S1 is performed when Master M1 is down, or has crashed, the end mode of S1 will be Standalone. This is because S1 will try to contact M1, and will fail because M1 is down.

**Restoring Data From S1 to M1**

Suppose you take a backup from S1 and restore the backed up data, say S1\(b\), on M1. M1 will switch to Standalone mode because, after backup, it will not be able to find a Master. S1 will also switch to Standalone mode.
At the time of backup, if there were 1000 devices in M1, the Slave S1 would also have 1000 devices. Assume more devices are added to M1 after the Backup. S1 will have the up-to-date device list. However, after restore on M1, M1 will have only 1000 devices. In other words, the data on S1 will be more recent than the data on M1.

**Restoring Data From S1 on M2**

Suppose you take a backup from S1 and restore the backed up data, say S1\(_b\), on M2, which is the Master in the DCR Domain 2 in our example.

After the restore, the end mode of M2 will be Slave. That is, M2 will become a Slave of M1. Also, S3, and S4, which were Slaves of M2, will switch to the Standalone mode.

**Restoring Data From M1 on M1**

Suppose you take a back up from M1. After the backup you would be performing several operations that would bring about changes in the Master and the corresponding Slaves; M1, S1, and S2 in our example.

Now, if you restore the backed up data M1\(_b\), on M1 itself. The Master M1 will have data that is older than the data in the Slaves, S1, and S2. In other words, the Slaves will have more recent data than that on the Master.

To avoid this, you must perform the Restore operation in the following sequence:

1. **Step 1** Back up data from the slaves, S1 and S2.
2. **Step 2** Back up data from the Master, M1.
   - This is to ensure that the data backed up from M1 is more recent than the data backed up from S1 and S2.
3. **Step 3** Stop Daemon Manager on all three machines.
4. **Step 4** Restore data on the Master, M1.
5. **Step 5** Restart Daemon Manager on M1.
6. **Step 6** Restore data on S1, and S2 after the Master is up and stable,
7. **Step 7** Restart Daemon Manager on S1, and S2.

This ensures that Master has more recent data than the Slaves.

**Note**

To avoid disturbances to the Master-Slave relationship, and to maintain consistency, it is better to take a back up of all machines at the same time.

**Restoring Data From M1 to M2**

Suppose you take a backup from M1, and restore the backed up data, say M1\(_b\), on M2.

S3, and S4 which were Slaves of M2, will switch to Standalone mode.

**Master-Slave Configuration Prerequisites and Restore Operations**

DCR Master-Slave setup requires you to perform certain tasks prior to Master-Slave configuration, to enable proper, and secure communication between them. This involves copying certificates, and setting up a valid system identity user. For details, see Master-Slave Configuration Prerequisites.
Restore operations can affect Master-Slave relationships because they may modify these pre-configured parameters.

For example, let M1 be the Master, and S1 its Slave. Let X be a standalone server. Suppose you take a backup from S1, and restore the backed up data, say S1b on X.

Now, X has to be in Slave mode.

Since, M1 and S1 already shared a Master-Slave relationship, M1 will have the peer certificate of S1, and S1 will have the certificate of M1.

After the restore operation, X will get the certificate of M1. However, if peer certificate of X is not present on M1, X will not be able to have M1 as its Master.

So you have to ensure that the certificates of the peer machines are in place, before you do a Restore.

Other Master-Slave configuration prerequisites such as System Identity user configuration and Peer Server Account user configuration might get affected by Restore operations.

For example: In M1 you have Joe as a Peer Server User and in S1 you add Joe as a System Identity user. You take a backup from S1.

After you take the backup, say you change the Peer Server User and System Identity User to Bob.

Now if you restore the backed up data, say S1b the system Identity User would not be Bob anymore. This will upset the Master-Slave relationship.

During restore you are prompted to confirm whether you need to overwrite the SSL certificate.

SSL certificates are tied to individual machines. So if you take a backup on one machine and restore it on another, you should be careful not to overwrite the SSL certificate.

However, if you backup data from a machine and restore it to the same machine, you may overwrite the SSL certificate.

**Effects of Backup-Restore on Groups**

Backup-Restore operations have an implication on the way Groups will be displayed in the LMS. The changes in Groups behavior is discussed in relation with the Device and Credential Repository (DCR) mode changes explained in Effects of Backup-Restore on DCR.

If you perform a backup on machine A and restore the backed up data, say Ab, on the same machine, the system-defined groups, and the user-defined groups created after the data backup will be removed.

The following scenarios helps you understand the implications of Restore operations on Groups.

- Restoring Data From a DCR Standalone
- Restoring Data From S1 on S1
- Restoring Data From S1 on M1
- Restoring Data From S1 on M2
- Restoring Data From M1 on M2

**Restoring Data From a DCR Standalone**

The following scenarios have to be considered:

- Restore data from a Standalone machine A to another Standalone machine B:

  The provider group name will change accordingly. That is, the provider group CS @A will become CS@B.
• Restore data from a Standalone machine A to a Master M:
  The Master will switch to Standalone mode. The provider group name will be updated accordingly.
  The Slave groups will be removed from the Master.
  Only the groups pertaining to LMS and the applications installed in the Standalone machine will be
  visible. All dependent Slaves of M will become Standalone.
• Restore data from a Standalone machine A to a Slave S:
  The Slave will switch to Standalone mode. The provider group name is updated accordingly. The
groups pertaining to other Slaves in the domain, and the Master of S, will be removed from S. The
groups UI will be enabled.

The subsequent sections are based on the scenarios discussed in the Effects of Backup-Restore on DCR.

**Restoring Data From S1 on S1**
No impact on CS groups.
There may be applications installed on S1. Say you create 10 groups in the Applications before you
backup data from S1. After backup, assume you create 10 more groups in the Applications. After restore,
the 10 groups you created after backup will not be present. This loss of newly added groups also
propagates to other Slaves in the domain.

**Restoring Data From S1 on M1**
After restore, both S1 and M1 will switch to Standalone mode. Both will have only those groups
pertaining to LMS installed on the individual machines. Groups UI is enabled on S1. Also, the other
Slaves of M1 will switch to Standalone mode.

**Restoring Data From S1 on M2**
After restore, M2 will become a Slave of M1. The Groups UI in M2 will be disabled. M2 will pickup all
the groups from M1. Groups in M2 will be propagated to other slaves in the domain. All the slaves of
M2 (before restore) will now switch to Standalone mode.

**Restoring Data From M1 on M2**
Slaves of M2, that is S3 and S4, will switch to Standalone mode. Groups pertaining to S3 and S4 will be
deleted from M2.
In all the cases the System-defined Groups, and the User-defined Groups, are carried over and updated
in the target machine.

---

**Backup for Cisco Prime Infrastructure**

From LMS 4.2.2, Cisco Prime LAN Management Solutions will support data migration to Cisco Prime
Infrastructure (PI) and the device data from LMS 4.2.x versions can be exported to PI 1.2.

The following two procedures will be used to export data from LMS to PI:
• Exporting Device Credentials Repository (DCR) data from LMS—User can export the Device List
  and Credentials to a CSV file that would be shown as a link. The data backup status and backup
  location will be displayed at the bottom of the Export Data to Prime Infrastructure page.
• Exporting complete data of LMS—This option enables you to store data in an external server or LMS server. The default backup location will be populated in the Backup location field at the bottom of the Export Data to Prime Infrastructure page. If the user chooses storing data in external server, the external server credentials namely Server IP or Host name, username, password and backup location will be required.

Licensing Cisco Prime LMS

You must register your software and obtain a product license before you start using an application. You can obtain a product license and license your application, view details of your current software license, or update to a new license from the Licensing page. LMS will authenticate and perform the license check.

If your current license count is lower than your earlier license count, and you restore the data now, devices that exceed the current licence count will be moved to Suspended state.

This section explains:
• **Obtaining a License for Cisco Prime LMS**
• **Licensing the Application**
• **Viewing License Information**
• **Updating Licenses**
• **Ordering LMS licenses**

**Obtaining a License for Cisco Prime LMS**

To obtain a product license for your Cisco Prime applications, register your software at one of the following websites. You will need to provide the Product Authorization Key (PAK), which is printed on a label affixed to the Bundle sub-box.

If you are a registered user of Cisco.com, use this website:

http://www.cisco.com/go/license

If you are not a registered user of Cisco.com, use this website:

http://www.cisco.com/go/license/public

The product license will be sent to the e-mail address you provide during registration. Retain this license with your Cisco Prime software records.

**Licensing the Application**

After you obtain the product license, perform these steps to license your software:

**Step 1** Copy the new license file to the LMS Server, with read permission for casuser/casusers.

**Step 2** Select **Admin > System > License Management**.

The License Information page appears. The License Information page displays the name, version, size, status and expiration date of the license.

**Step 3** Click **Update**.

**Step 4** Enter the path to the new license file in the License field, or click **Browse** to locate the new file.

**Step 5** Click **OK**.
Compliance and Audit Manager (CAAM) Server License

You must have CAAM server license for accessing the following CAAM features in LMS:

- Compliance data collection
- Compliance profile execution
- Compliance Policy and groups
- HIPAA Compliance Reports
- SOX(COBIT) Compliance Reports
• ISO/IEC 27002 Compliance Reports
• NSA Compliance Reports
• PCI DSS Compliance Reports
• Department of Homeland Security (DHS) Checklist Reports
• Defense Information Systems Agency (DISA) Checklists
• Center for Internet Security (CIS) Benchmarks

The following Compliance and Audit Reports are supported only by LMS license and do not require CAAM server license.
• Service Reports
• Lifecycle Management Reports
• Vendor Advisory Reports

## Configuring a Default SMTP Server

This SMTP server is used by default when you add or edit subscriptions for e-mail notifications or send e-mail notifications from the Alerts and Activities display. LMS also provides a facility for specifying a default SMTP server. Specifying a default server here will override the setting used by LMS.

**Step 1** Select **Admin > System > SMTP Default Server.**
**Step 2** Enter a fully qualified SMTP server name.
**Step 3** Click **Apply.**

## Collecting Server Information

This feature helps you to get the required information about the server. The information about the server includes system information, environment, configuration, logs, web server information, device and credentials administration information, and grouping services information.

You can use the collected server information for troubleshooting.

For example, when you have chosen to collect the grouping services information about the server, the following details will be collected and stored:
• Status of LMS grouping server. The status values are Running, and Not Running.
• List of groups created in the LMS grouping server.
• Content of the registry and properties files associated with LMS.
• Status of the grouping server installed on same Cisco Prime Server. The status values are Running, and Not Running.
• List of groups created in the LMS grouping server.
• Content of the properties files associated with other applications.
• Error encountered if the grouping servers are not running or if they are not reachable.
To collect the server information:

**Step 1** Select **Admin > System > Server Monitoring > Collect Server Information**.

The Collect Server Information page appears.

**Step 2** Click **Create** to collect the current server information.

The Collect Server Information popup dialog box appears with a list of options. The available options are:

- **System Information** — Displays the server type, operating system version, installation date of operating system, and other system information.
- **Event Logs** — Displays the logs of events in the LMS Server.
- **Cisco Prime Registry** — Displays the registry entries of Cisco Prime components installed in the server.
- **Tomcat Log Files** — Displays the log files corresponding to the application server.
- **Grouping Service** — Displays the information of grouping servers and the groups created in the grouping server.
- **Application Registry Details** — Displays the information of applications registered with Cisco Prime home page.
- **Device Credentials Admin Information** — Displays the details of DCR mode, status of DCR Master, number of devices in DCR and the contents of DCR configuration files.
- **ODBC Configuration** — Displays the information about the configuration of database connection in the LMS Server.
- **Product Log Files** — Displays the contents of log files of all Cisco Prime components.
- **Environment Variables** — Displays the list of environmental variables set up in the LMS Server.
- **Process Status** — Displays the name of processes, current state of the process, process ID, start and finish time of the process, and other information.
- **Network Configuration** — Displays information about the various configurations in a network.
- **Memory and Harddrive Status** — Displays details of free space and total space of memory and hard disk drives in the LMS Server.
- **JRE Registry** — Displays information about the Java Runtime Environment registry files.

**Step 3** Select the check boxes corresponding to the options you need.

You can use the All check box to select or deselect all the available options.

By default all the check boxes are selected.

**Step 4** Click **OK**.

The server information for the selected components is collected.

Collecting server information may take longer if more components are selected.

To return to the Collect Server Information page, click **Cancel**.

You can click **Refresh** in the Collect Server Information page to see the latest status.
Collecting Self Test Information

You can view self test reports using this option. Self test feature helps to test certain basic functions of the server.

Execute the following steps to receive the system generated self test report to your Email ID.

Step 1 Go to Admin > System > Server Monitoring > Selftest.
Step 2 Select the E-mail text box and enter your Email ID.
Step 3 Click Save.

The system generated self test report will be sent to the specified Email ID.

Execute the following steps to create a self test report.

Step 1 Select Admin > System > Server Monitoring > Selftest.
Messaging Online Users

Step 2  Click Create to perform a selftest and to view the report.
Step 3  Click the Selftest Information at date time link.
        A popup window displays the selftest information report.
        To delete a Selftest Information report, select the checkbox and click Delete.

In LMS 4.2, the selftest report provides the following Hardware Parameters details:

• Memory availability
• Swap
• CPU
• DSN
• Backup status
• Number of MIB objects being polled
• Maximum number of MIB objects that can be managed
• Syslog database size

If the syslog database size exceeds 10 GB you need to purge the syslog records to reclaim space. Do the following to purge syslog records and reclaim the database space:

Note  If you want to backup the syslogs, refer Setting the Syslog Backup Policy.

Step 1  Perform a forced purge of Syslog messages, refer Performing a Syslog Forced Purge.
Step 2  Open RMEDebugToolsReadme.txt from NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\debugtools.
        where NMSROOT is the Cisco Prime installation directory.
Step 3  Refer Syslog DBSpaceReclaimer Tool section in the RMEDebugToolsReadme.txt file and execute the perl script DBSpaceReclaimer.pl.

Note  The perl script will reclaim the space occupied by SyslogFirst.db, SyslogSecond.db and SyslogThird.db files present in the server. The amount of space reclaimed will depend on the purge criteria that you specify. The most effective way to reclaim the space is to purge the records older than 1 day.

Messaging Online Users

You can use the Notify User feature in LMS to broadcast messages to online users.
You can post messages to users with active Cisco Prime browsers. By default, the messages will be received within 60 seconds. You can also change this polling interval.
To send a broadcast message:
Step 1  Select Admin > System > User Management > Notify Users.
The Notify Users page lists all the users currently logged in.

Step 2  Enter the message in the Message field and click Send.
The Status field displays the status of the message.

Note  If you are using Microsoft Internet Explorer, make sure your browser is set to check for updates on every visit to the page.

Managing Resources

LMS provides a Resource Browser for managing resources. You can free locked resources, when necessary, if you have appropriate privileges. All users (including those with Help Desk role alone) can access the Resource browser page. The Refresh icon in the Resource browser is available for all users.

Note  The System Identity user must configure all the Resource management related tasks. The Browse Resources and Free Resources tasks should be enabled.

To view Resource details:

Step 1  Select Admin > Network > Resource Browser.
The Resource Browser page displays the following details:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Name of the resource currently locked.</td>
</tr>
<tr>
<td>Job ID / Owner</td>
<td>Number assigned to this task at creation time. Identifies all related locked resources, and user who locked the resource.</td>
</tr>
<tr>
<td>Time Locked</td>
<td>Time this lock was established.</td>
</tr>
<tr>
<td>Expire Time</td>
<td>Lock expiration time.</td>
</tr>
</tbody>
</table>

To free locked resources:

Step 1  Select Admin > Network > Resource Browser.
The Resource Browser page appears.

Step 2  Check the check box corresponding to the Job ID.

Step 3  Click Free Resources.
All users (except those with Help Desk and Approver role) can perform the Free Resource operation in the Resource browser.
To view updated resources, click **Refresh**.

## Modifying System Preferences

You can configure system-wide information on the LMS Server using the System Preferences option. It is a way to centrally locate information that is used by Cisco Prime applications.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>System-wide name of the SMTP server used by Cisco Prime applications to deliver reports. The default server name is localhost.</td>
</tr>
<tr>
<td>Administrator E-mail ID</td>
<td>Cisco Prime Administrator e-mail ID. This e-mail address is used as the From Address in all mails sent from LMS Server. There is no default e-mail ID.</td>
</tr>
<tr>
<td>Enable E-mail Attachment</td>
<td>Allows you to enable e-mail attachments in the mails sent from LMS Server. This option helps you to attach PDF or CSV reports with the e-mail after the scheduled jobs have completed. This option is disabled by default.</td>
</tr>
<tr>
<td>Maximum Attachment Size</td>
<td>Maximum size of the e-mail attachments that are allowed to be sent from LMS Server. You can specify the attachment size in KB or MB.</td>
</tr>
<tr>
<td>RCP User</td>
<td>Name used by network device when it connects to LMS Server to run rcp. User account must exist on UNIX systems, and should also be configured on devices as local user in the ip rcmd configuration command. The default RCP username is cwuser.</td>
</tr>
<tr>
<td>SCP User</td>
<td>Name used by network device when it connects to LMS Server to run SCP. The username you have entered here is used for authorization while transferring software images using SCP protocol. You must specify a user name that has SSH authorization on a Solaris system. SCP uses this authorization for transferring the software images. This field is available only if Cisco Prime LMS applications are installed on the LMS Server.</td>
</tr>
<tr>
<td>SCP Password</td>
<td>Enter the password for SCP User in this field. The password you have entered here is used for authentication while transferring software images using SCP protocol. You must specify a user name that has SSH authentication on a Solaris system. SCP uses this authentication for transferring the software images. This field is available only if Cisco Prime LMS applications are installed on the LMS Server.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP Verify Password</td>
<td>Re-enter the SCP password in this field. This field is available only if Cisco Prime LMS applications are installed on the LMS Server.</td>
</tr>
<tr>
<td>Enable crmlogger DNS resolution</td>
<td>Enable the Domain Name Service Resolution for the crmlog service using this field. Note that enabling the DNS Resolution for the crmlog service will slow down the Syslog performance. The crmlog service will stop and start when you enable or disable the Domain Name Service Resolution for crmlog service. If the crmlog registry does not contain the CrmDnsResolution parameter, it will be created automatically when you enable the service. This field is available only on Windows systems.</td>
</tr>
<tr>
<td>Disable Idle Timeout Settings</td>
<td>By default this settings will be enabled and time interval for idle page will be 120 minutes.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>You can choose the time interval ranging from 15, 30, 45, 60 and 120 minutes. A page is considered to be idle when there is no mouse or keyboard movement in a particular screen. If the page is kept idle for the set time period then a pop up redirecting the page to idle page will be displayed. You can click cancel to avoid redirecting to the idle page. If you are redirected to the idle page then click the hyperlink <strong>click here</strong> to return to your previous page.</td>
</tr>
</tbody>
</table>

To edit system preferences:

**Step 1** Select **Admin > System > System Preferences.**

The System Preferences page appears.

**Step 2** Enter the following information:

- SMTP Server
- Administrator E-mail ID
- Maximum Attachment Size
- RCP User

**Caution**

Set this information carefully. If you introduce errors, users may not be able to log in.

**Step 3** Check the Enable crmlogger DNS Resolution check box to enable the Domain Name Service Resolution for the crmlog service, on a Windows system.

**Step 4** Enter the following fields, which are available only if Cisco Prime LMS applications are installed on the LMS Server:

- SCP User
- SCP Password
- SCP Verify Password
Configuring Log Files Rotation

Log files can expand and fill up disk space. Log files rotation helps you manage the log files more efficiently. See Maintaining Log Files for an overview of maintaining the log files in LMS Server.

Logrot is a log rotation program that enables you to control the size growth of the log files. It helps you to:

- Rotate log files while Cisco Prime is running.
- Optionally archive and compress rotated logs.
- Rotate log files only when they have reached a particular size.

Logrot helps you easily add new files. You can configure Logrot either from the UI or from the CLI.

The following log files are maintained by the log rotation program:

- Daemon Manager
- Web server log files

This section explains:

- Configuring Log Files Rotation Settings From the User Interface
- Configuring Log Files For Rotation From the User Interface
- Scheduling Log Files Rotation
- Configuring Logrot Utility
- Running Logrot Script
- Viewing the Scheduled Logrot Job

Configuring Log Files Rotation Settings From the User Interface

To configure log files rotation from the user interface:

**Step 1** Select Admin > System > Log Rotation.

The Log Rotation page appears.

**Step 2** Set your backup directory in the Backup Directory field.

This backup directory stores the rotated log files.

You can also use the Browse button to select a directory from the file browser. The default directory is:

- NMSROOT\log on Windows systems
- /var/adm/CSCOpx/log on Solaris/Soft Appliance systems

If you do not set a backup directory, each log file will be rotated in its current directory.

**Step 3** Select Restart Daemon Manager check box to stop and start the Daemon Manager before the log rotation starts. This is optional.
Configuring Log Files Rotation From the User Interface

To add the log files for rotation:

---

**Step 1**
Select Admin > System > Log Rotation.
The Log Rotation page appears.

**Step 2**
Click Add to add the log files you wish to rotate.
The Configure Logrot page appears.

**Step 3**
Enter the name of the log file in the Select Log File field.
You can enter only one log file at a time.
You should specify log file using its fully-qualified path. If the log files do not exist in the path you have specified, this will not be considered for rotation.
You can also click Browse to select a log file name from the file system.

**Step 4**
Enter the maximum file size in the Maximum Logrot Size field.
The log file will not be rotated until this size is reached.
You can enter the file size in KB or MB. The default file size is 1024 KB. The maximum file size for log rotation is 4096 MB.

**Step 5**
Select a file compression type from Compression Format.
The supported formats are:
- Z—UNIX compression (on Solaris/Soft Appliance only)
- gz—GNU gzip
- bz2—bzip2 (on Solaris/Soft Appliance only)

**Step 6**
Specify the number of backups in the No of Backups field.
If you do not want to keep any archives, enter 0 (the default) for this option.

**Step 7**
Click Apply to save the changes.
To return to the Log Rotation page, click Cancel.

---

To edit the log files that you have configured for rotation:

---

**Step 1**
Select Admin > System > Log Rotation.
The Log Rotation page appears.

**Step 2**
Select a record from the list of log files displayed.

**Step 3**
Click Edit.
The Edit Logrot page appears.

**Step 4**
Edit the name of the log file. The rotated log files will be stored with the new name you have edited.

**Step 5**
Edit the log file size, compression type or number of archive revisions.

**Step 6**
Click Apply to save the changes.
To return to the Log Rotation page, click Cancel.
Scheduling Log Files Rotation
To schedule log files rotation:

Step 1  Select **Admin > System > Log Rotation**.
The Log Rotation page appears.

Step 2  Click **Schedule**.
The Schedule Logrot appears.

Step 3  Select a value in the Hour and Min drop-down lists to specify the time at which the log rotation should start.
You should specify the time in 24-hour format.

Step 4  Select a periodic or immediate backup schedule in the Frequency field.
The available schedule frequencies are:
• Immediate—Log rotation job runs immediately.
• Daily—Log rotation job runs every day at the time specified.
• Weekly—Log rotation job runs once a week on the day and time specified. Select a day from the Day of Week list.
• Monthly—Log rotation job runs once a month on the day and time specified. Select a day from the Day of Month list.

Step 5  Click **Apply** to save the changes.
You can remove a schedule at any time. Click **Remove** to delete the scheduled job. The Remove button is enabled only if you have scheduled a log rotation. To return to the Log Rotation page, click **Cancel**.

Configuring Logrot Utility
Logrot should be installed on the same machine where you have installed LMS.
To configure the Logrot script:

Step 1  Enter:
• `NMSROOT/bin/perl.exe NMSROOT/bin/logrot.pl -c` (on Windows)
• `Run /opt/CSCOpx/bin/logrot.pl -c` (on Solaris/Soft Appliance)
The Logrot configuration menu appears. You have the following options:
• Edit variables.
• Edit log files.
• Quit and save changes.
• Quit without saving change.

Step 2  Select **Edit variables** to set your Backup Directory.
If you do not set a backup directory, each log will be rotated in its current directory.
Step 3  Select **Edit log files** to add log files you wish Logrot to rotate.

You can specify log files using fully-qualified or relative paths. If a relative path is specified, and the log file does not exist in that path, the default log file path for your operating system will be added during rotation (for example, `/var/adm/CSCOpx/log` on Solaris/Soft Appliance).

Step 4  Specify the number of archive revisions. If you do not want to keep any archives, enter 0 (the default) for this option.

Step 5  Specify the maximum file size. The log will not be rotated until this size is reached. The unit is in kilobytes (KB). The default is 1024 KB or 1 MB.

Step 6  Specify the file compression type to be used. It can be:

- Z—UNIX compression (on Solaris/Soft Appliance only)
- gz—GNU gzip
- bz2—bzip2 (on Solaris/Soft Appliance only)

When deleting logfiles, you can choose to delete an individual file, a list of files, or all files matching a certain pattern.

For example, 1-3 means delete files numbered 1 through 3. A list of comma-separated file numbers, for example, 1,21, means delete files numbered 1 and 21. A pattern string `*.log` means delete all files that match the pattern `*.log`.

You can also specify the special pattern, `*`, which means delete all logfiles in the configuration.

---

**Running Logrot Script**

To run the Logrot Script enter:

- On Windows:
  
  Enter `NMSROOT\bin\perl NMSROOT\bin\logrot.pl`

- On Solaris/Soft Appliance:
  
  Run `/opt/CSCOpx/bin/logrot.pl`

You can schedule log rotation so that the utility works on a specified time and day.

The following command line flags are accepted:

- `-v` option to get verbose messages.
- `-s` option shuts down dmgtd before rotating logs.

---

**Caution**

The Restart Delay variable controls the waiting duration (in seconds) before proceeding, after dmgtd is shutdown. This option is only used if the `-s` argument is given to logrot. The default delay is 60 seconds.

- `-c` option reruns the configuration tool.
- `-h` option displays the help.

The following `wrapLogrot` permissions should be checked for proper working of LogRotation.

For Solaris:

```
bash-3.00# ls -l /opt/CSCOpx/bin/wrapLogrot
-r-sr-x--- 1 root casusers 6852 Oct 1 19:08 /opt/CSCOpx/bin/wrapLogrot
```
Configuring Disk Space Threshold Limit

DiskWatcher is a back-end process that monitors disk space availability on LMS Server. This process calculates the disk space information of a drive (on Windows) or a file system (on Solaris/Soft Appliance) where Cisco Prime applications are installed, and stores them in diskWatcher.log file.

Disk space information is calculated for the following directories on LMS Server:

- Cisco Prime Installation directory (on both platforms)
- /var directory (on Solaris/Soft Appliance platform only)
- /tmp directory (on Solaris/Soft Appliance platform only)

The process calculates the disk space availability of the LMS Server directories at a regular interval of approximately one hour.

In Solaris machines, the disk spaces of /opt file system is calculated in the first 30 minutes of every one hour time. The disk spaces of /var file system and /tmp file system are calculated in the next 15 minutes and in the last 15 minutes of an approximate one hour time interval.

This process also alerts you when the disk space is less than the threshold level you have configured in the User Interface. Alerts are sent as urgent messages to logged in users. You can also receive the alert messages through e-mail if you have configured your e-mail ID along with threshold level.
This process records the alert information in the system log files. The alert information is recorded in diskWatcher.log and syslog.log files in Windows machines. They are stored in diskWatcher.log and daemons.log files in Solaris machines.

To configure the disk space threshold limit:

**Step 1** Select **Admin > System > Server Monitoring > DiskWatcher Configuration**.

The DiskWatcher Configuration page appears.

**Step 2** Enter a threshold value in the Threshold for Cisco Prime Installation Directory field to monitor the disk space in the Cisco Prime Installation directory. This is mandatory.

You should enter the threshold value in units of MB or GB.

**Step 3** Enter a threshold value in the Threshold for /var and /tmp Directories field to monitor the disk space in Solaris file systems. This is mandatory.

You should enter the threshold value in units of MB or GB.

**Note** This field is available only on Solaris systems.

**Step 4** Enter a valid e-mail in the E-mail ID field.

You can enter multiple e-mail addresses separated by commas.

The system uses the e-mail addresses to notify about the disk space availability when the disk space is less than the threshold limit you have configured.

There may be a problem in sending e-mails if you have enabled virus scanner in the LMS Server.

**Step 5** Click **Apply** to save the changes or click **Cancel** to reset the values.

---

**Effects of Third Party Backup Utility and Virus Scanner**

Sometimes, the LMS database fails to run and throws the following Sybase Assertion error message:

```text
*** ERROR *** Assertion failed: 100909 (9.0.0.1383).
100909 is the Assertion ID.
```

The following are the scenarios where Assertion Error might appear:

- If you use any third-party backup software to back up a live, running database, the Assertion Error might be thrown.
  
  This is because some of the database pages that have been modified will be in the database server cache, so the database file will be in an inconsistent state.

- If you use any anti-virus software.

  The reason is, Adaptive Server Anywhere performs many reads and writes other than the normal I/O operations, which contribute to the good performance of Adaptive Server Anywhere. However, anti-virus software might detect this as a potential problem and quarantine the file.

  This becomes hazardous if the .log or temporary files are quarantined, and it may cause corruption by interfering with the normal functions of the database. Poor performance can also occur if the anti-virus software is checking all I/O operations performed by the database server.
We recommend that you do not use third-party backup software for backing up a running database.
We also recommend that you configure your anti-virus software so that it must not scan the
\textit{NMSROOT}/databases directory.
\textit{NMSROOT} is the directory where you have installed Cisco Prime.

## Configuring TFTP

This applies only to Solaris.
The TFTP (Trivial File Transfer Protocol) daemon shipped by Cisco Prime LMS supports TCP
(Transmission Control Protocol) Wrappers.
If the TCP Wrapper support is not configured properly in the server where Cisco Prime is installed, the
jobs requiring TFTP may fail.
To ensure that TFTP works properly, check the following configuration files:

- If /etc/hosts.allow file is present, ensure that the command \texttt{in.tftpd} is given as \texttt{in.tftpd:ALL} If the
  command is not there in the file at all, add it as \texttt{in.tftpd:ALL}
- If /etc/hosts.deny file is present, ensure that the command \texttt{in.tftpd} is not there in the file
- If both the files are not present (/etc/hosts.allow and /etc/hosts.deny), you do not need to make any
  changes

\textbf{Note}
The TCP Wrapper software extends the abilities of \texttt{inetd} to provide support for every server daemon
under its control. It provides logging support, returns messages to connections, and permits a daemon to
accept only internal connections.

### Displaying LMS Server Name With Browser Title

Displaying LMS Server name with browser title helps you to identify the server from which the
application window is launched especially in a multi-server setup and Single Sign-On based setup.
You can enable or disable the option of displaying the LMS Server name along with the browser title.
When you choose to display the server name in the browser title, the browser window displays the title
in the following format:

\textit{Hostname} - \textit{ApplicationWindowTitle}

where,

- \textit{Hostname} is the name of the LMS Server
- \textit{ApplicationWindowTitle} is the title of application window launched from LMS Server.

\textbf{Note}
By default, the option of displaying the LMS Server name with the application window title in the
browser is enabled.

For example, if the name of your LMS Server is \texttt{lmsdocultra}, then the title of the Cisco Prime home
page is displayed as \texttt{lmsdocultra - CiscoPrime}.
If you launch LMS from the Cisco Prime LMS, the title of the LMS window is displayed as \texttt{lmsdocultra - LMS Home}. 
You can also enable or disable the display of server name with the browser title by changing the configurations in a properties file.

Configure the `uii-windows.properties` file located at `NMSROOT/lib/classpath` to:

- Enable or disable the option of displaying server name with browser title.
- Change the format of display from `Hostname - ApplicationWindowTitle` to `ApplicationWindowTitle - Hostname` and vice versa.
- Replace hyphen (-) with any other delimiter except empty spaces.
- Trim the spaces between the Hostname, delimiter and Application window title.

### Cisco Prime Integration Application Settings

The Cisco Network Analysis Module Traffic Analyzer (NAM) offers flow-based traffic analysis of applications, hosts, and conversations, performance-based measurements on application, server, and network latency, quality of experience metrics for network-based services such as voice over IP (VoIP) and video. Only NAM 4.1 is supported in LMS 4.2. The Cisco Prime Integration Application Settings page allows you to configure NAM.

To add, edit, or delete the NAM configuration details:

---

**Step 1**

Select **Admin > Cisco Prime Integration > Application Settings**. The Application Settings page appears.

**Step 2**

You can do the following:

- **Add**
  - Click **Add**. The Server Configuration page appears.
  - Select NAM from the drop-down list.
  - Enter the IP Address in the NAM IP field.
  - Enter the user name and password in the corresponding fields.
  - Enter the SNMP read community.
  - Select either HTTP or HTTPS as the protocol.
  - Enter the port number.
  - Click **Add** to add the new NAM configuration details or **Cancel** to return to the NAM Configuration page.

- **Edit**
  - Select a configuration detail that has to be edited.
  - Click **Edit**. The Edit NAM Configuration page appears.
  - Enter the IP Address in the NAM IP field.
  - Enter the user name and password in the corresponding fields.
  - Enter the SNMP read community.
  - Select either HTTP or HTTPS as the protocol.
  - Enter the port number.
  - Click **Edit** to save the changes or **Cancel** to return to the NAM Configuration page.
• **Delete**
  - Select a configuration detail that has to be deleted.
  - Click **Delete**. A confirmation dialog box appears.
  - Click **OK** to confirm or **Cancel** to return to the NAM Configuration page.

• **Filter**
  - In the **Filter By field**, select the filter criteria e.g. ApplicationName from the drop-down list.
  - In the **Matches** text box, enter the matching details e.g. NAM.
  - Click **Go**, to execute the selected filter condition.
  - Click **Clear Filter**, to clear the filter condition.