



## CHAPTER 2

# Navigating Cisco Prime Common Services Tasks in LMS 4.2

CiscoPrime Common Services (CS) provides the application infrastructure for all existing CiscoWorks network management solutions for them to share a common model for data storage, user login, user role definitions, user access privileges, and security protocols.

This chapter provides the mapping of CS tasks in LMS 4.2.

It explains:

- [Server Tasks](#)
- [Software Center Tasks](#)
- [Device and Credential Tasks](#)
- [Group Administration Tasks](#)

## Server Tasks

This section provides information on the Common Services Server tasks in LMS 4.2.

- [Security Tasks](#)
- [Report Tasks](#)
- [Admin Tasks](#)

**Table 2-1** Server Tasks

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
<b>Security Tasks</b>			
Setting up browser security mode	CiscoWorks LMS Portal > Common Services > Server > Security > Single Server Name > Browser-Server Security Mode Setup	Admin > Trust Management:Local Server > Browser-Server Security Mode Setup	Common Services provides secure access between the client browser and management server. It does this using SSL (Secure Socket Layer). SSL encrypts the transmission channel between the client, and server.

Table 2-1 Server Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Setting up local user policy	CiscoWorks LMS Portal > Common Services > Server > Security > Single Server Name > Local User Policy Setup	Admin > System: User Management > Local User Policy Setup	<p>You can setup username and password policies for CiscoWorks local users in Common Services. With the new local user policy, you can:</p> <ol style="list-style-type: none"> <li>1. Start the local username with a number</li> <li>2. Include special characters in local username</li> <li>3. Specify the length of local username</li> <li>4. Specify the length of local user password</li> </ol> <p>You can add and delete users, edit user profiles and modify the logged in user credentials</p>
Setting up security certificate	CiscoWorks LMS Portal > Common Services > Server > Security > Single Server Name > Certificate Setup	Admin > Trust Management:Local Server > Certificate Setup	<p>CiscoWorks allows you to create security certificates that enable SSL communication between your client browser and management server. Self signed certificates are valid for five years from the date of creation. When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed CiscoWorks</p>
Setting up Peer Server Accounts	CiscoWorks LMS Portal > Common Services > Server > Security > Multi-Server Trust Management > Peer Server Account Setup	Admin > Trust Management:Multi Server > Peer Server Account Setup	<p>Peer Server Account Setup helps you create users who can programmatically login to CiscoWorks Servers and perform certain tasks. These users should be set up to enable communication among multiple CiscoWorks Servers. Users created using Peer Server Account Setup can authenticate processes running on remote CiscoWorks Servers.</p>

Table 2-1 Server Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Setting up System Identity Setup	CiscoWorks LMS Portal > Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup	Admin > Trust Management:Multi Server > System Identity Setup	Communication between multiple CiscoWorks Servers is enabled by a trust model addressed by certificates and shared secrets. System Identity setup helps you to create a "trust" user on servers that are part of a multi-server setup. This user enables communication among servers that are part of a domain. There can only be one System Identity User for each machine.
Setting up Peer Server Certificate Setup	CiscoWorks LMS Portal > Common Services > Server > Security > Multi-Server Trust Management > Peer Server Certificate Setup	Admin > Trust Management:Multi Server > Peer Server Certificate Setup	You can add the certificate of another CiscoWorks Server into its trusted store. This will allow a CiscoWorks Server to communicate with another using SSL. If a CiscoWorks Server needs to communicate with another CiscoWorks Server, it must possess the certificate of the other server. You can add certificates of any number of peer CiscoWorks Servers to the trusted store. You can add, delete and view the details of the client certificates.
Setting up Single Sign-On Setup	CiscoWorks LMS Portal > Common Services > Server > Security > Multi-Server Trust Management > Single Sign-On Setup	Admin > Trust Management:Multi Server > Single Sign-On Setup	With Single Sign-On (SSO), you can use your browser session to transparently navigate to multiple CiscoWorks Servers without authenticating to each of them. Communication among multiple CiscoWorks Servers is enabled by a trust model addressed by Certificates and shared secrets.

Table 2-1 Server Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Setting up AAA Mode Setup	CiscoWorks LMS Portal > Common Services > Server > Security > AAA Mode Setup	Admin > System: Authentication Mode Setup	The CiscoWorks Server provides mechanisms used to authenticate users for CiscoWorks applications. CiscoWorks login modules allow administrators to add new users using a source of authentication other than the native CiscoWorks Server mechanism (that is, the CiscoWorks Local login module).
Set up Cisco.com User Account	CiscoWorks LMS Portal > Common Services > Server > Security > Cisco.com Connection Management > Cisco.com User Account Setup	Admin > System: Cisco.com Settings > User Account Setup	Certain Software Center features require Cisco.com access. This means that CiscoWorks must be configured with a Cisco.com account that is to be used when downloading new and updated packages.
Update Proxy Server Setup	CiscoWorks LMS Portal > Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup	Admin > System: Cisco.com Settings > Proxy Server Setup	You can update the proxy server configuration using the Proxy Server set up option.
<b>Report Tasks</b>			
Log File Status Report	CiscoWorks LMS Portal > Common Services > Server > Reports > Log File Status	Reports > System: Status > Log File	The Log File Status Report provides information on log file size and file system utilization.
Permission Report	CiscoWorks LMS Portal > Common Services > Server > Reports > Permission Report	Reports > System:Users > Permission	The Permissions Report provides information on roles and privileges associated with the roles. It specifies the tasks that a user in a particular role can perform.
Who Is Logged On Report	CiscoWorks LMS Portal > Common Services > Server > Reports > Who Is Logged On	Reports > System:Users > Who is Logged On	The Users Logged In Report provides information on users currently logged into Common Services.
Process Status Report	CiscoWorks LMS Portal > Common Services > Server > Reports > Process Status	Reports > System: Status > Process	The Process Status Report shows the status of the processes running on the CiscoWorks Server.

Table 2-1 Server Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Audit Log Report	CiscoWorks LMS Portal > Common Services > Server > Reports > Audit Log	Reports > Audit:System	Audit log report provides information on: <ul style="list-style-type: none"> <li>• User login and logout from CiscoWorks</li> <li>• CiscoWorks Local user addition</li> <li>• CiscoWorks Local user modification</li> <li>• CiscoWorks Local user deletion</li> <li>• Change of CiscoWorks server modes</li> </ul>
<b>Admin Tasks</b>			
Process Management Tools	CiscoWorks LMS Portal > Common Services > Server > Admin > Processes	Admin > System: Server Monitoring > Processes	Process management tools enable you to manage these backend processes to optimize or troubleshoot the CiscoWorks Server.  You can do the following activities: <ul style="list-style-type: none"> <li>• View the details of all processes</li> <li>• Filter and show only processes of a specific state</li> <li>• Start the processes</li> <li>• Stop the processes</li> </ul> All mandatory processes are started when you start the system
Taking backup	CiscoWorks LMS Portal > Common Services > Server > Admin > Backup	Admin > System:Backup	You can schedule immediate, daily, weekly, or monthly automatic database backups. You should have the privileges necessary for using this option.
Edit log file rotation	CiscoWorks LMS Portal > Common Services > Server > Admin > Log Rotation	Admin > System:Log Rotation	Log files can expand and fill up disk space. Log files rotation helps you manage the log files more efficiently. You can add and delete log files for rotation

Table 2-1 Server Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Update a license	CiscoWorks LMS Portal > Common Services > Server > Admin > Licensing	Admin > System: License Management	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.
Collect server information	CiscoWorks LMS Portal > Common Services > Server > Admin > Collect Server Information	Admin > System: Server Monitoring > Collect Server Information	You can collect information about the server including system information, environment, configuration, logs, web server information, device and credentials administration information, and grouping services information.  You can also delete the collected server information
Self Test Information report	CiscoWorks LMS Portal > Common Services > Server > Admin > Self Test	Admin > System: Server Monitoring > Selftest	Self Test Information report helps to test certain basic functions of the server
Notify users	CiscoWorks LMS Portal > Common Services > Server > Admin > Notify Users	Admin > System: User Management > Notify Users	Broadcasts messages to online users.  You can post messages to users with active CiscoWorks browsers. By default, the messages will be received within 60 seconds. You can also change this polling interval.
Stop a job, delete jobs, filter jobs	CiscoWorks LMS Portal > Common Services > Server > Admin > Job Browser > Stop, Delete, Filter	Admin > Jobs: Browser	You can manage jobs using the Job Browser. From the Job browser you can view a listing of jobs and filter jobs based on certain criteria.  Users in Help Desk, Approver, and Network Operator roles are not allowed to stop and delete jobs. All users (including Help Desk) can access the Job Browser page. The Refresh icon in Job browser is available for all users.

Table 2-1 Server Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Free locked resources	CiscoWorks LMS Portal > Common Services > Server > Admin > Resource Browser > Free Resources	Admin > Network: Resource Browser > Free Resources	Common Services 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.
Configure system preferences	CiscoWorks LMS Portal > Common Services > Server > Admin > System Preferences	Admin > System: System Preferences	System Preferences option is a way to centrally locate information that is used by CiscoWorks applications. You can apply or cancel the changes made to the system configuration.
Enable debug mode	CiscoWorks LMS Portal > Common Services > Server > Admin > CS Log Configurations	Admin > System: Debug settings > Common Services Log Configurations	Enables the debugging option for Common Services components without restarting the services. When you enable the debugging option for the selected component, the log levels in the respective properties file is changed to DEBUG and the debug messages are recorded in the corresponding log files. You can only enable or disable the debugging option. You cannot choose to set different log levels such as INFO, WARNING, FATAL and ERROR.
Configure disk space threshold limit	CiscoWorks LMS Portal > Common Services > Server > Admin > DiskWatcher Configuration	Admin > System: Server Monitoring > DiskWatcher Configuration	DiskWatcher is a back-end process that monitors disk space availability on CiscoWorks Server. This process calculates the disk space of a drive (on Windows) or a file system (on Solaris) where CiscoWorks applications are installed, and stores them in diskWatcher.log file. You can reset the disk space threshold limit values

# Software Center Tasks

This section provides information on the Common Services Software Center tasks in LMS 4.2:

- [Software Update Tasks](#)
- [Device Update Tasks](#)
- [Schedule Device Download Tasks](#)
- [Activity Log Tasks](#)

**Table 2-2 Software Center Tasks**

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
<b>Software Update Tasks</b>			
Performing Software Updates	CiscoWorks LMS Portal > Common Services > Software Center > Software Update	Admin > System: Software Center > Software Update	Finds software updates on Cisco.com, then downloads these updates to a server location. From the server, you can then install the updates using the procedures recommended in the readme file of the update package.
<b>Device Update Tasks</b>			
Device Updates	CiscoWorks LMS Portal > Common Services > Software Center > Device Update	Admin > System: Software Center > Device Update	You can view a list of all CiscoWorks related device packages on your system using this option. Displays a count of devices supported for each product installed in the system. For device updates the source location could be Cisco.com or the Server Side Directory. The Device Update page lists the product name and the device type count. You can also delete packages that are outdated or that you no longer use.
<b>Schedule Device Download Tasks</b>			
Scheduling Device Package Downloads	CiscoWorks LMS Portal > Common Services > Software Center > Schedule Device Downloads	Admin > System: Software Center > Schedule Device Downloads	Schedules device package downloads and specifies the time, frequency of the downloads, and the download policy.



Table 2-2 Software Center Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
<b>Activity Log Tasks</b>			
Scheduled job details	CiscoWorks LMS Portal > Common Services > Software Center > Activity Log > Scheduled Job Details	Admin > System: Software Center > Scheduled Job Details	Displays the details of scheduled jobs in the software center. Scheduled Job table records and displays the downloads to the server. You can view the log from the server or from any client workstation.
Logs of event details	CiscoWorks LMS Portal > Common Services > Software Center > Activity Log > Event Log	Admin > System: Software Center > Event Log	Displays the logs of events in the software center. The Event Log table shows the list of immediate downloads, installations and uninstallations of device packages. You can view the log from the server or from any client workstation.

## Device and Credential Tasks

This section provides information on the following Common Services Device and Credential tasks in LMS 4.2 :

- [Device DiscoveryTasks](#),
- [Device Management Tasks](#)
- [Auto Update Server Tasks](#)
- [Report Tasks](#)
- [Device Selector Setting Tasks](#)
- [Admin Tasks](#)

Table 2-3 Device and Credential Tasks

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
<b>Device DiscoveryTasks</b>			
Device Discovery Settings	CiscoWorks LMS Portal > Common Services > Device and Credentials > Device Discovery > Discovery Settings	Admin > Network: Discovery Settings	Configures the layer 3 and layer 2 protocols and other discovery options before starting the discovery of devices  Also, it displays the list of total devices discovered, number of reachable devices, unreachable devices, and various other details about the devices in the DCR.
Discovery schedule	CiscoWorks LMS Portal > Common Services > Device and Credentials > Device Discovery > Discovery Schedule	Admin > Network: Discovery Settings > Schedule	You can create, view, edit, modify, and delete the device discovery schedule job.
Discovery Logging	CiscoWorks LMS Portal > Common Services > Device and Credentials > Device Discovery > Discovery Logging Configuration	Admin > Network: Discovery Settings > Logging Configuration	Enables the debugging option for components or modules of Common Services Device Discovery without restarting the services. When you enable the debugging option for a selected component, the log levels in the csdiscovery.properties file is changed to DEBUG and the debug messages are recorded in the CSDiscovery.log file.
<b>Device Management Tasks</b>			
Managing Devices	CiscoWorks LMS Portal > Common Services > Device and Credentials > Device Management	Inventory > Device Administration: Add / Import / Manage Devices	The Device Management option in Device and Credentials Administration helps you manage the list of devices and their credentials. Device Management helps you in: <ul style="list-style-type: none"> <li>• Adding Devices</li> <li>• Deleting Devices</li> <li>• Editing Device Credentials</li> <li>• Editing Device Identity</li> <li>• Importing Devices and Credentials</li> <li>• Exporting Devices and Credentials</li> <li>• Excluding Devices</li> <li>• Viewing Devices List</li> </ul>

Table 2-3 Device and Credential Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
<b>Auto Update Server Tasks</b>			
Auto Update Server	CiscoWorks LMS Portal > Common Services > Device and Credentials > Auto Update Server Management	Inventory > Device Administration: Auto Update Server Management	<p>Auto Update Servers have the following credentials:</p> <ul style="list-style-type: none"> <li>• Auto Update Server URL</li> <li>• Username</li> <li>• Password</li> </ul> <p>The Auto Update Server Management UI is not visible in a DCR Slave machine.</p> <p>Auto Update Server management feature helps you in:</p> <ul style="list-style-type: none"> <li>• Adding an Auto Update Server</li> <li>• Editing an Auto Update Server</li> <li>• Deleting an Auto Update Server</li> </ul>
<b>Report Tasks</b>			
Device List Report	CiscoWorks LMS Portal > Common Services > Device and Credentials > Reports > Device List Report	Reports > Inventory:Management Status > Known Device List	The DCR Device List Report displays the complete list of all devices.
Audit Report	CiscoWorks LMS Portal > Common Services > Device and Credentials > Reports > Audit Report	Reports > Audit:Device Administration	The Audit Report displays the complete device list in DCR for a specified period of time.
Excluded Devices Report	CiscoWorks LMS Portal > Common Services > Device and Credentials > Reports > Excluded Devices Report	Reports > Inventory:Management Status > Excluded Devices	The Excluded Devices Report displays the list of devices that should not be added to DCR.
Import Status Report	CiscoWorks LMS Portal > Common Services > Device and Credentials > Reports > Import Status Report	Reports > Inventory:Management Status > Imported Device Status	<p>The Imported Device Status report displays the information about the devices that are imported into DCR from any one of the following import sources:</p> <ul style="list-style-type: none"> <li>• Import File</li> <li>• Local NMS</li> <li>• Remote NMS</li> </ul>

Table 2-3 Device and Credential Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
<b>Device Selector Setting Tasks</b>			
Customization of Device Type Groups	CiscoWorks LMS Portal > Common Services > Device and Credentials > Device Selector Settings > Group Customization	Admin > Network: Display Settings > Group Customization	<p>Provides options to select/remove the Device Selector groups.</p> <p>You can customize the Device Type Based Groups folder to display:</p> <ul style="list-style-type: none"> <li>• All devices in groups, based on their Device Category only</li> <li>• All devices in groups and subgroups, based on their Device Category and Series</li> <li>• All devices in groups and subgroups, based on their Device Category, Series and Model</li> </ul>
Customizing Display Order of Device Groups	CiscoWorks LMS Portal > Common Services > Device and Credentials > Device Selector Settings > Group Ordering	Admin > Network: Display Settings > Group Ordering	<p>Provides options to choose the order in which the existing groups will be displayed.</p> <p>The Group Ordering setup is specific to each user and the changes will be reflected in the Device Selector panes of all applications.</p> <p>The default order of the groups displayed in the Device Selector pane is:</p> <ul style="list-style-type: none"> <li>• All Devices</li> <li>• Device Type Groups</li> <li>• User Defined Groups</li> <li>• Subnet Groups</li> <li>• Application Specific Groups</li> </ul> <p>You can change the order and save the configurations.</p>

Table 2-3 Device and Credential Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
<b>Admin Tasks</b>			
Administering Device and Credential Repository	CiscoWorks LMS Portal > Common Services > Device and Credentials > Admin > Mode Settings	Admin > Network: Device Credential Settings > Current DCR Settings	<p>The DCR Administration feature allows you to do the following tasks:</p> <ul style="list-style-type: none"> <li>• Changing DCR Mode</li> <li>• Configuring Device Polling</li> <li>• Configuring User Defined Fields</li> <li>• Configuring Default Credentials</li> </ul> <p>To perform these tasks, select Device and Credentials &gt; Admin from the CiscoWorks home page. The Admin page appears with the current DCR Administration settings.</p> <p>You can change the Mode Settings or modify User Defined fields.</p>
Configuring Device Polling Settings	CiscoWorks LMS Portal > Common Services > Device and Credentials > Admin > Device Polling > Device Poll Settings	Admin > Network: Device Credential Settings > Device Poll Settings	Configures a Device Polling policy and schedules a Device Polling job to check whether the devices can be reached.
Unreachable Device Report	CiscoWorks LMS Portal > Common Services > Device and Credentials > Admin > Unreachable Device Report	Reports > Inventory:Management Status > Unreachable Devices	Displays the unreachable devices from the DCR.

Table 2-3 Device and Credential Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Renaming User Defined Fields	CiscoWorks LMS Portal > Common Services > Device and Credentials > Admin > User Defined Fields	Admin > Network: Device Credential Settings > User Defined Fields	<p>The User Defined Fields (UDFs) are used to store the additional information about a device. DCR supports a maximum of ten UDFs.</p> <p>By default, the user interface provides four UDFs:</p> <ul style="list-style-type: none"> <li>• user_defined_field_0</li> <li>• user_defined_field_1</li> <li>• user_defined_field_2</li> <li>• user_defined_field_3</li> </ul> <p>You can add six more UDFs through the user interface. You can rename or delete all the UDFs including the four default UDFs provided by the user interface.</p>

Table 2-3 Device and Credential Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Configuring a Default Credentials Set	CiscoWorks LMS Portal > Common Services > Device and Credentials > Admin > Default Credential Sets	Admin > Network: Device Credential Settings > Default Credential Sets	<p>You can use default credentials to populate newly-added devices in Device Addition flows such as Add and Bulk Import.</p> <p>You can configure multiple default credential sets to a maximum of 50 default credential sets.</p> <p>Each default credential set comprises the following credentials:</p> <ul style="list-style-type: none"> <li>• Primary Credentials (Username, Password, Enable Password)</li> <li>• Secondary Credentials (Username, Password, Enable Password)</li> <li>• SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)</li> <li>• SNMPv3 Credentials (Mode, Username, Authentication Password, Authentication Algorithm, Privacy Password, Privacy Algorithm)</li> <li>• HTTP credentials (Primary HTTP Username and Password, Secondary HTTP Username and Password, HTTP port, HTTPS port, Current Mode)</li> <li>• Auto Update Server Managed Device Credentials (Username and Password)</li> <li>• Rx Boot Mode Credentials (Username, Password)</li> </ul>

Table 2-3 Device and Credential Tasks (continued)

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Setting up a Default Credential Set Policy	CiscoWorks LMS Portal > Common Services > Device and Credentials > Admin > Default Credential Sets Policy Configuration	Admin > Network: Device Credential Settings > Default Credential Sets Policy Configuration	<p>Creates a default credential set policy. You can create default credential set policies based on following policy types:</p> <ul style="list-style-type: none"> <li>• IP Address</li> <li>• Hostname</li> <li>• Display Name</li> </ul> <p>You can also specify the order in which the default credential set policies should be applied for devices that are added or imported into DCR.</p> <p>The default credential set policies are applied in the order in which they appear on the Credentials Sets Policy Configuration page. The default credential set policies appearing at the top of the list are applied first.</p>

## Group Administration Tasks

This section provides information on the Common Services Group Administration tasks in LMS 4.2.

Table 2-4 Group Administration Tasks

LMS 3.2 Task Name	LMS 3.2 Navigation	LMS 4.2 Navigation	Description
Administering Groups	CiscoWorks LMS Portal > Common Services > Groups > Export	Admin > System: Group Management > Device Groups	The Groups feature in Common Services helps you to group devices managed by CiscoWorks applications. It helps in creating, managing, and sharing groups of devices. The groups created using this feature are shared across applications. The groups created in applications can also be viewed from Common Services.