Inventory Management with Cisco Prime
LAN Management Solution 4.2

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25948-01
Inventory Management with Cisco Prime LAN Management Solution 4.2

CONTENTS

Preface ix
  Audience ix
  Document Conventions x
  Product Documentation x
  Obtaining Documentation and Submitting a Service Request xii

Notices xiii
  OpenSSL/Open SSL Project iii-xiii
  License Issues iii-xiii

CHAPTER 1

Overview of Inventory Management 1-1
  Understanding the Inventory Dashboard 1-2
    Discrepancies Portlet 1-2
    Device Change Audit Portlet 1-2
    Hardware Summary Portlet 1-4
    Software Summary Portlet 1-4
    Calendar Portlet 1-5
  Understanding the Device Status Dashboard 1-5
    Network Data Collection Summary 1-6
    Device Discovery Summary 1-6
    Job Information Status 1-7
    Device Performance Management Summary 1-8
    IPSLA Collector Information 1-9
    IPSLA Device Categorization 1-11
    Device Credentials Verification Error Summary 1-11
    Config Protocol Summary 1-11
    Inventory Device Status 1-12

CHAPTER 2

Device and Credential Repository 2-1
  Understanding DCR 2-1
    Device Types 2-2
    Device Attributes 2-4
      Mandatory Device Attributes 2-4
    Device Credentials 2-5
      Device Credentials in DCR 2-5
CHAPTER 3

Discovering Devices 3-1

Configuring Device Discovery Settings 3-2
Configuring Discovery Module Settings 3-3
Configuring Seed Device Settings 3-9
IPv4 and IPv6 Addresses as Seed Devices 3-9
Options to Specify Seed Devices 3-10
Specifying Seed Devices in a File 3-10
Specifying Module Specific Seed Devices 3-12
Specifying Global Seed Devices 3-14
Configuring SNMP Settings 3-15
Configuring Discovery Filter Settings 3-18
Important Notes on Configuring Discovery Filters 3-18
Patterns in IP Address Filter Rules 3-19
Regular Expressions in Filter Rules 3-20
Specifying Discovery Filter Settings 3-20
Configuring Global Discovery Settings 3-22
Viewing Custom Discovery Settings Summary 3-29
Starting Custom Discovery 3-31
Viewing Discovery Details 3-32
Viewing Discovery Summary 3-32
Total Devices Discovered 3-35
Reachable Devices 3-35
Unreachable Devices 3-36
Devices Newly Added to DCR 3-37
Devices Updated to DCR 3-38
Activities Performed From Device Discovery Details Windows 3-38
Using DCR Features in a Master-Slave Setup 3-39
Standard Discovery 3-40
Using Device Discovery Features in Various Setup 3-42
Using Device Discovery in Master-Slave Setup 3-42
Running Device Discovery within NAT Setup 3-42

CHAPTER 4

Managing Devices and Credentials 4-1

Managing Devices in DCR 4-1
Managing Auto Update Servers  4-47
  Adding, Editing, and Deleting Auto Update Server  4-48
Configuring Device Selector  4-48
  Using Device Selector  4-49
  Selecting Devices for Device Management Tasks  4-50
Searching Devices  4-51
  Performing Simple Search  4-51
  Performing Advanced Search  4-52

**CiscoView**  5-1
CiscoView Features  5-2
Starting CiscoView  5-3
Navigating in CiscoView  5-3
  Using the Options Bar  5-4
  Using the Tools Bar  5-5
  Using the Device Selector of CiscoView  5-5
  Understanding the Color Legend  5-8
  Using the Context Menu of CiscoView  5-9
  Selecting a Device or its Components in the Chassis View  5-10
Viewing Devices Not Available in the DCR  5-11
Setting Preferences for CiscoView  5-12
Generating Interface Report for CiscoView  5-12
Device Packages  5-13
  Device Package Updates  5-13
Device Management in CiscoView  5-14
  Understanding Categories in CiscoView  5-14
  Editing Categories in CiscoView  5-14
  Configuring Devices in CiscoView  5-15
    Add IP Addresses for Other Management Workstations  5-16
    Limit Device Access Privileges for Other Management Workstations  5-16
    Verify Device Configurations and Device Access  5-17
    Edit Configuring and Monitoring Tables  5-17
  Monitoring Devices in CiscoView  5-17
  Viewing System Information in CiscoView  5-18
  Configuring Devices Using CiscoView  5-18
  Setting CiscoView Debugging Options and Display Logs  5-19
CHAPTER 6  
CiscoView Mini-RMON Manager 6-1
Starting CiscoView Mini-RMON Manager 6-2
Navigating in CiscoView Mini-RMON Manager 6-3
Setting Up CiscoView Mini-RMON Manager 6-3
Configuring a System 6-4
Setting Up Alarm Thresholds 6-5
Creating and Modifying an Alarm 6-6
Setting Up Statistics Collection on Ethernet Ports 6-9
Setting Up Historical Statistics Collection on Ethernet Ports 6-9
Enabling or Modifying History Collection on a Port 6-10
Viewing Alarm Events 6-11
Latest Alarm Events 6-11
Alarm Current Settings 6-12
Alarm Events Log 6-14
Alarm Thresholds 6-15
Alarm Event Log for Selected Alarm Thresholds 6-17
Viewing Traffic Statistics 6-17
Current Traffic Statistics 6-18
Current Traffic Details 6-19
Total Traffic And Utilization 6-21
Errors in Current Traffic Statistics 6-22
Packet Distribution 6-22
Traffic Statistics History 6-23
Details of Traffic History 6-24
Error Details in Traffic History 6-25

CHAPTER 7  
Inventory Tools 7-1
Working With SmartCase 7-1

APPENDIX A  
CLI Tools A-1
Using Discovery Features Through CLI A-1
Starting, Stopping, and Viewing Device Discovery Through CLI A-1
Using DCR Features Through CLI A-2
Adding Devices Using CLI A-3
Adding Devices Using dcrcli in Shell Mode A-3
Adding Devices Using dcrcli in Batch Mode A-4
Deleting Devices Using CLI A-4
Editing Devices Using CLI A-5
Listing the Attributes A-6
Contents

Listing the Device IDs  A-6
Import Devices Using CLI  A-7
Export Devices Using CLI  A-11

APPENDIX B

Frequently Asked Questions  B-1
Device Discovery FAQ  B-1
Device Management FAQ  B-5

INDEX
Preface

Inventory Management in Cisco Prime LAN Management Solution (LMS) 4.2 groups the various activities in LMS involved in managing your network devices. You can add devices, discover devices, manage them, manage groups using Inventory Management.

It also provides various Inventory Tools like Ciscoview, Mini-RMON, and SmartCase.

This preface details about related documents that support Getting Started feature, and demonstrates the styles and conventions used in this guide. This preface contains:

• Audience
• Document Conventions
• Product Documentation

Audience

This guide is for users who are skilled in network administration and management, or network operators who use this guide to make configuration changes of devices using LMS. The network administrator or operator should be familiar with the following:

• Basic Network Administration and Management
• Basic Solaris System Administration
• Basic Windows System Administration
• Basic LMS Administration
Document Conventions

Table 1 describes the conventions followed in the user guide.

Table 1  Conventions Used

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td><em>italic</em> font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><code>screen</code> font</td>
</tr>
<tr>
<td>Information you enter</td>
<td><strong>boldface screen</strong></td>
</tr>
<tr>
<td>Variables you enter</td>
<td><em>italic screen</em> font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Selecting a menu item in paragraphs</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
<tr>
<td>Selecting a menu item in tables</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
</tbody>
</table>

Note  Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Product Documentation

Note  We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes on the product documentation that is available.

Table 2  Product Documentation

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>
- PDF version part of Cisco Prime LMS 4.2 Product DVD. |
<p>| <strong>Context-sensitive online help</strong>                                             | Select an option from the navigation tree, then click Help.                        |</p>
<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>
  • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
  • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
  • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
  • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
  • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
  • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
  • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
Table 2  Product Documentation (continued)

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>
   • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
   • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
   • PDF version part of Cisco Prime LMS 4.2 Product DVD. |
   • PDF version part of Cisco Prime LMS 4.2 Product DVD. |

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:
Copyright © 1998-2007 The OpenSSL Project. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:
Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.
   The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].
Overview of Inventory Management

Inventory Management in Cisco Prime LAN Management 4.2 groups the various activities in LMS involved in managing your inventory: your network devices. You can access these features from the Inventory menu in the Cisco Prime LMS home page.

Tools in the Inventory menu are:

- Ciscoview
- Mini-RMON
- Device Center
- SmartCase

Device Administration in the Inventory menu allows you to:

- Add, Import, Manage Devices
- Manage Device State
- Discovery
- Device Aliases
- Device Allocation Policy
- Add as Managed Devices
- IPSLA Devices
- Manage Auto Update Server

User Tracking Settings in the Inventory menu are:

- Acquisition Actions
- Acquisition Summary

The Inventory menu has the following dashboards to provide real-time updates of the network and allows you to monitor and troubleshoot problems if any:

- Understanding the Inventory Dashboard
- Understanding the Device Status Dashboard
Understanding the Inventory Dashboard

To access the Inventory Dashboard select **Inventory > Dashboard > Inventory**.

This section explains how to configure the following Inventory dashboard portlets:

- Discrepancies Portlet
- Device Change Audit Portlet
- Hardware Summary Portlet
- Software Summary Portlet
- Calendar Portlet

**Discrepancies Portlet**

You can view the type and count of discrepancies, such as network inconsistencies and anomalies or wrong configurations in the discovered network, using the Discrepancies portlet.

The Discrepancy portlet gives a description of the discrepancy, the impact it has on the network, and ways to resolve it.

LMS 4.0 provides reports on discrepancies in the discovered network, enabling identification of configuration errors such as link-speed mismatches on either end of a connection. Discrepancies are computed at the end of each data collection schedule.

Table 1-1 lists the Discrepancies portlet details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the discrepancy such as network inconsistencies, anomalies or misconfigurations in the network.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of deviations. Click the number corresponding to the deviation to navigate to the Unacknowledged Discrepancy Report in the application.</td>
</tr>
</tbody>
</table>

You can click the portlet name in the title bar to navigate directly to the Reports page. Select **Discrepancies** from the TOC to navigate to the Network Discrepancy page.

**Device Change Audit Portlet**

In the Device Change Audit portlet, you can view the changes in the inventory and configuration information for all the devices after every Inventory or Configuration Collection.

However, the VLAN config change details will not be displayed.

The changes in the exception period are displayed in red.

Table 1-2 lists the Device Change Audit portlet details.
Table 1-2: Device Change Audit Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Device name as entered in the Device and Credential Repository. Mouse hover over any device to see more details about the device like:</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• Device Type</td>
</tr>
<tr>
<td></td>
<td>• OS Type</td>
</tr>
<tr>
<td></td>
<td>• Image Version</td>
</tr>
<tr>
<td></td>
<td>• Time of last config change</td>
</tr>
<tr>
<td></td>
<td>• Time of last inventory change</td>
</tr>
<tr>
<td></td>
<td>• Location</td>
</tr>
<tr>
<td></td>
<td>• Contact</td>
</tr>
<tr>
<td></td>
<td>• Fault Count</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of the user who performed the change on the device. This is the name entered when the user logged in. The User Name field may not always reflect the user name. The User Name is reflected only when:</td>
</tr>
<tr>
<td></td>
<td>• Config change was performed using LMS</td>
</tr>
<tr>
<td></td>
<td>• Config change was performed outside LMS, and the network has username based on AAA security model where the authentication is performed by a AAA server (such as TACACS/RADIUS or local server)</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Date and the time at which the application communicated the network change or when Change Audit saw the change record.</td>
</tr>
<tr>
<td>Message</td>
<td>Brief summary of the network change. You can click the Message link to navigate to the 24 Hour Inventory Change Report details page.</td>
</tr>
</tbody>
</table>

You can click the portlet name in the title bar to navigate directly to the Reports page.
Hardware Summary Portlet

In the Hardware Summary portlet, you can view a pie graph that displays the distribution of all managed Cisco devices in the inventory.

Table 1-3 lists Hardware Summary portlet details.

Table 1-3 Hardware Summary

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Management</td>
<td>Percentage of network management used.</td>
</tr>
<tr>
<td>DSL and Long Reach Ethernet</td>
<td>Percentage of Ethernet used.</td>
</tr>
<tr>
<td>Security and VPN</td>
<td>Percentage of security and VPN used.</td>
</tr>
<tr>
<td>Switches and Hubs</td>
<td>Percentage of switches and hubs used.</td>
</tr>
<tr>
<td>Routers</td>
<td>Percentage of routers used.</td>
</tr>
<tr>
<td>Count</td>
<td>Count of the devices.</td>
</tr>
</tbody>
</table>

For instance, you can click the number corresponding to Switches and Hubs to navigate to the Hardware Report details page.

The graph plots the percentage count of devices, based on Cisco MetaData Framework (MDF) categorization of devices.

Each section represents the device category, the device count and percentage of total devices. The graph displays the device category and the percentage of distribution in the network.

You can click the portlet name in the title bar to navigate directly to the Reports page.

Software Summary Portlet

In the Software Summary portlet, you can view the software version information and count for selected devices such as Cisco Interfaces and Modules, Switches and Hubs, Universal Gateways and Access Servers, and Routers.

Table 1-4 lists the Software Summary portlet details.

Table 1-4 Software Summary

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Categories</td>
<td>Categories of devices used in the application.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Software version of the device categories.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of the device.</td>
</tr>
</tbody>
</table>

For instance, you can click on the number corresponding to Switches and Hubs to navigate to the Software Report details page.

You can click the portlet name in the title bar to navigate directly to the Reports page.
Calendar Portlet

In the Calendar portlet, you can view the jobs scheduled for the current month or day. When you launch the portlet, a calendar of the current month appears with the details of scheduled jobs in the Job Summary grid.

You can click the Day tab to view the jobs scheduled for the current day.

Table 1-5 lists the Calendar portlet details.

Table 1-5 Calendar Portlet details

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to a job.</td>
</tr>
<tr>
<td></td>
<td>For periodic jobs such as Daily and Weekly, the job IDs are in the</td>
</tr>
<tr>
<td></td>
<td>number.x format. The x represents the number of instances of the job.</td>
</tr>
<tr>
<td></td>
<td>For example, 1001.3 indicates that this is the third instance of the job ID</td>
</tr>
<tr>
<td></td>
<td>1001.</td>
</tr>
<tr>
<td>Scheduled at</td>
<td>Date and time at which the job was scheduled.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Type of the job.</td>
</tr>
<tr>
<td></td>
<td>For example, Inventory Collection, SyslogDefaultPurge, and Net Config Job.</td>
</tr>
<tr>
<td>Job Description</td>
<td>Description of the job provided by the job creator.</td>
</tr>
<tr>
<td></td>
<td>It can contain alphanumeric characters.</td>
</tr>
</tbody>
</table>

Understanding the Device Status Dashboard

To access the Device Status Dashboard, select Inventory > Dashboards > Device Status or Admin > Dashboards > Device Status.

The Device Status Dashboard has the following portlets:

- Network Data Collection Summary
- Device Discovery Summary
- Job Information Status
- Device Performance Management Summary
- IPSLA Collector Information
- Device Credentials Verification Error Summary
- Config Protocol Summary
- Inventory Device Status
Network Data Collection Summary

In the Data Collection Summary portlet you can view the details of the operations carried out. The details displayed are the date and time at which the operation was last completed, the type of the operation, and the result of the operation.

You can configure the refresh time in the portlets.

*Table 1-6* lists the Network Data Collection Summary portlet details.

*Table 1-6  Network Data Collection Summary*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Type of operation such as Data Collection and User Tracking Acquisitions (End Hosts) and so on.</td>
</tr>
<tr>
<td>Last Completion Time</td>
<td>Date and time at which the operation was last completed.</td>
</tr>
<tr>
<td>Result</td>
<td>Result of the operation.</td>
</tr>
<tr>
<td></td>
<td>Click the required link from the Result column to view the Report.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the Data Collection. The two states are idle or active.</td>
</tr>
</tbody>
</table>

Device Discovery Summary

In the Device Discovery Summary portlet, you can view the summary of the discovered devices, the total number of devices discovered, reachable devices, unreachable devices, devices added to DCR and devices updated to DCR.

You can configure the refresh time in the portlets.

*Table 1-7* displays the Device Discovery Summary portlet details.

*Table 1-7  Device Discovery Summary Portlet*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Status</td>
<td>Status of the discovery whether it is in the initializing, running or complete status.</td>
</tr>
<tr>
<td>Discovery Start Time</td>
<td>Displays the Day, month, date, and time when the discovery started.</td>
</tr>
<tr>
<td>Discovery End Time</td>
<td>Displays the Day, month, date, and time when the discovery ended.</td>
</tr>
<tr>
<td>Total Devices Discovered</td>
<td>Number of devices found.</td>
</tr>
<tr>
<td></td>
<td>You can click the number to navigate to the Device Discovery Report for all devices discovered.</td>
</tr>
<tr>
<td>Reachable Devices</td>
<td>Number of devices that are reachable.</td>
</tr>
<tr>
<td></td>
<td>You can click the number to navigate to the Device Discovery Report for Reachable devices.</td>
</tr>
<tr>
<td>Unreachable Devices</td>
<td>Number of unreachable devices.</td>
</tr>
<tr>
<td></td>
<td>You can click the number to navigate to the Device Discovery Report for Unreachable devices.</td>
</tr>
<tr>
<td></td>
<td>The Device Discovery Report page for unreachable devices will be updated with the list of neighbors along with other information such as IP Address, System Name, SysObjectID, FoundByModules, and Status.</td>
</tr>
</tbody>
</table>
Table 1-7  Device Discovery Summary Portlet

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices Newly Added to DCR</td>
<td>Number of devices added to DCR. You can click the number to navigate to the Device Discovery Report for Devices Newly Added to DCR.</td>
</tr>
<tr>
<td>Devices Updated to DCR</td>
<td>Number of devices updated to DCR. You can click the number to navigate to the Device Discovery Report for Devices Updated in DCR.</td>
</tr>
</tbody>
</table>

Job Information Status

In Job Information portlet, you can view up to 20 report job details. The job details displayed are job ID, job type, status, job description, and the scheduled time of the job.

You can configure the Job Information Status portlet to:

- Set the number of jobs to be displayed in the portlet
- Set the Refresh time.

To configure the Job Information Status portlet:

Step 1  Move the mouse over the title bar of the Job Information Status portlet to view the icons.

Step 2  Click the Configuration icon. You can:

- Select **Show only my jobs** check box to display only your jobs in the Job Information Status portlet. By default, the portlet displays all the jobs in the Job Information Status portlet.
- Select **Ascending** to display the jobs in the ascending order based on the time schedule.
- Select **Descending** to display the jobs in the descending order based on the time schedule.
- Select the jobs from the **Show Last Jobs** drop-down list to display the last jobs in the portlet. For example if you select 3, the last three jobs based on the time scheduled will be displayed in the portlet.
- Select the jobs from the **Show Next Jobs** drop-down list to display the next jobs in the portlet. For example if you select 4, the next four jobs based on the time scheduled will be displayed in the portlet.

*Note*  Show Last Jobs and Show Next Jobs are two groups and the sorting (Ascending and Descending) is done within the group based on the time schedule. If two or more jobs have the same time schedule, the sorting is done based on their Job ID.

- Select the hour and minute from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh frequency.

Step 3  Click **Save** to view the portlet with the changed settings.
Device Performance Management Summary

The Device Performance Management Summary portlet displays the summary of the monitoring component in LMS 4.0. Table 1-8 lists Device Performance Management Summary portlet details.

Table 1-8 Device Performance Management Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices Managed</td>
<td>Displays the number of devices that are managed.</td>
</tr>
<tr>
<td>Objects Monitored</td>
<td>Displays the number of objects that are monitored</td>
</tr>
<tr>
<td>Failure Variables</td>
<td>Displays the number of failure variables. Click the number to view the Poller Failure Report.</td>
</tr>
<tr>
<td>Average Polled Variables per Minute</td>
<td>Displays the average polled variables per minute.</td>
</tr>
<tr>
<td>Number of Pollers with Missed Polling Cycles</td>
<td>Displays the number of pollers with missed polling cycles. Missed polling cycles are the number of polling interval cycles missed during polling.</td>
</tr>
<tr>
<td>License Status and Limit</td>
<td>Displays the license status and the total limit of the devices that can be managed by the application.</td>
</tr>
<tr>
<td>Last Purge Time</td>
<td>Displays the date and time of the last purge</td>
</tr>
<tr>
<td>Next Purge Due</td>
<td>Displays the date and time for the next purge. You can click this link to navigate to the Data Purge Settings page.</td>
</tr>
</tbody>
</table>

You can customize and configure the Device Performance System Summary portlet.

To configure the Device Performance System Summary:

**Step 1** Move the mouse over the title bar of the Device Performance System Summary portlet to view the icons.

**Step 2** Click the configuration icon.

You can select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh frequency.

**Step 3** Click Save to view the portlet with the changed settings.

Hardware-based MIB Object Polling Support

LMS supports polling up to 100,000 MIB object variables. If the object polled exceeds the limit of 100,000, performance of the system may be slower.

Hardware-based MIB objects polling support is explained in Table 1-9.

Table 1-9 MiB objects polling support for different hardware configuration

<table>
<thead>
<tr>
<th>Operating System</th>
<th>CPU Count</th>
<th>RAM Space (GB)</th>
<th>Swap Space (GB)</th>
<th>Number of MIB Objects Polled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>6000</td>
</tr>
<tr>
<td>Soft Appliance</td>
<td>2</td>
<td>4</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 1  Overview of Inventory Management

Understanding the Device Status Dashboard

If the system hardware configuration is lesser than the recommended configuration, supported number of MIB objects polled is 3000.

Polling MIB Objects Exceeding Limit

When the Automonitoring Pollers or User-defined Pollers poll devices with more instances, more MIB variables may be polled than the recommended MIB objects limit. If the number of MIB objects polled exceeds the recommended MIB object count, a message appears at the top of the portlet displaying the count of recommended MIB variables and the polled MIB variables. You can click the link provided for polled MIB variables count to see Performance Managed MIB Object details in a pop up window.

The Performance Managed MIB Object details window displays the following information:

- Poller Name
- Average MIB Objects/Minute
- No of MIB Objects

Reducing Number of MIB Objects Polled

If you do not want the Poller to poll a device for a MIB variable, you can deactivate it. You can also select multiple Pollers and deactivate them at the same time.

See Deactivating a Poller in Monitoring and Troubleshooting With Cisco Prime LAN Management Solution 4.2 to deactivate the pollers to stop polling a device.

### IPSLA Collector Information

A collector is an entity that encompasses a source router, a target device, an operation, and the collector schedule details.

You can configure the refresh time in the portlets.

**Table 1-10** lists IPSLA Collector Information portlet details.
Understanding the Device Status Dashboard

Table 1-10  IPSLA Collector Information Portlet

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Displays the state of the collector. The states are:</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Deleting</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td></td>
<td>• Scheduled</td>
</tr>
<tr>
<td></td>
<td>• Dormant</td>
</tr>
<tr>
<td></td>
<td>• Config Failed</td>
</tr>
<tr>
<td></td>
<td>• Source Not Responding</td>
</tr>
<tr>
<td></td>
<td>• Completed</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Stopped and Configuring</td>
</tr>
<tr>
<td>Number of Collectors</td>
<td>Displays the number of collectors in the respective state.</td>
</tr>
<tr>
<td>Licensed Collectors</td>
<td>Displays the total number of licensed collectors.</td>
</tr>
</tbody>
</table>

**Note**
You can click the number link to navigate to the IPSLA Collector Management page.

Table 1-11 lists the Collector Information status details

Table 1-11  Collector Information State

<table>
<thead>
<tr>
<th>Collector Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleting</td>
<td>Collector is marked for deletion.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>Collector is scheduled for a future date and time.</td>
</tr>
<tr>
<td>Dormant</td>
<td>Collector is in dormant state and will start polling at the next polling interval.</td>
</tr>
<tr>
<td>Config Failed</td>
<td>Configuration of the collector failed on the source router.</td>
</tr>
<tr>
<td>Source Not Responding</td>
<td>Source router is not responding to configuration or reconfiguration of the collector, or for polling the statistics. This problem can occur if credentials are invalid, or the device is not reachable.</td>
</tr>
<tr>
<td>Completed</td>
<td>Collector has reached its end time and LMS will not poll this collector again.</td>
</tr>
<tr>
<td>Running</td>
<td>Collector is configured in the source router and polling is in progress.</td>
</tr>
<tr>
<td>Stopped</td>
<td>Collector has been manually stopped and is not being polled by LMS.</td>
</tr>
<tr>
<td>Configuring</td>
<td>Configuration of the collector is in progress.</td>
</tr>
</tbody>
</table>

For more information, see *Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 4.0*.
**IPSLA Device Categorization**

The devices added from DCR are categorized based on the availability of IP SLA. IP SLA is a feature built into Cisco Internetworking Operating System (IOS) and is used by most Cisco routers and switches.

IPSLA source is a device from which you initiate operations for measuring network performance statistics. IPSLA targets are destination devices for which you want to gather network performance statistics. However, some target devices are Responder enabled.

You must configure the refresh time in the portlets.

*Table 1-12* lists Device Categorization portlet details.

### Table 1-12 Device Categorization

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSLA</td>
<td>IPSLA is a technology portfolio embedded in most devices that run on Cisco IOS software. IPSLA allows you to analyze IP service levels for IP applications and services. You can use this information to increase productivity, to lower operational costs, and to reduce the frequency of network outages. IP SLA uses active traffic monitoring - the generation of traffic in a continuous, reliable and predictable manner - for measuring network performance. Count Lists the number of IP SLA enabled devices in LMS. Click the number to view the IPSLA Devices details.</td>
</tr>
</tbody>
</table>

For more information, see *Monitoring and Troubleshooting with CiscoWorks LAN Management Solution 4.0*.

**Device Credentials Verification Error Summary**

The Device Credentials Verification Error Summary portlet displays the different type of errors in devices with credentials such as SNMP, Telnet, and SSH.

The device count along is also displayed.

You can configure the refresh time in the portlets.

*Table 1-13* lists the Device Credentials Verification Error Summary details.

### Table 1-13 Device Credentials Verification Error Error Summary Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential</td>
<td>Credential details such as SNMP, Telnet, and SSH.</td>
</tr>
<tr>
<td>No.of Devices</td>
<td>Number of devices with errors.</td>
</tr>
</tbody>
</table>

**Config Protocol Summary**

In Config Protocol Summary portlet, you can view the configuration protocol usage details for successful configuration fetches.
You can configure the refresh time in the portlets.

Table 1-14 lists the Config Protocol Summary details.

**Table 1-14  Config Protocol Summary Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocols used by LMS to fetch configuration.</td>
</tr>
<tr>
<td>Config Type</td>
<td>The Configuration types for the various protocols. The available types are:</td>
</tr>
<tr>
<td></td>
<td>• Running — Count of the successful running configuration fetches for each protocol</td>
</tr>
<tr>
<td></td>
<td>• Startup — Count of the successful startup configuration fetches for each protocol</td>
</tr>
<tr>
<td></td>
<td>• VLAN — Count of the successful VLAN configuration fetches for each protocol. This configuration fetch is supported by only Telnet and SSH protocols.</td>
</tr>
<tr>
<td></td>
<td>Click the Count link to view a detailed report for a protocol and corresponding Config Type. The detailed report shows the list of devices which are accessed using a particular protocol and for which Config Fetch is successful.</td>
</tr>
<tr>
<td>Example:</td>
<td>If you click on a Count link, 20, for Telnet protocol and Running config type, a detailed report is generated with the following fields:</td>
</tr>
<tr>
<td></td>
<td>– Device Name — Device name of each device.</td>
</tr>
<tr>
<td></td>
<td>– Accessed At — Date and time at which each device was accessed for Config Fetch purpose.</td>
</tr>
<tr>
<td></td>
<td>– Config Type — Configuration type for each device.</td>
</tr>
<tr>
<td></td>
<td>– File Type — Configuration file type for each device.</td>
</tr>
<tr>
<td></td>
<td>– This detailed report shows only the devices for which Telnet has successfully fetched configurations.</td>
</tr>
<tr>
<td></td>
<td>You can use the export icon to export the list of devices from this detailed report to the device selector.</td>
</tr>
<tr>
<td>Config NeverCollected</td>
<td>The count of devices for which configuration fetch has never happened.</td>
</tr>
<tr>
<td></td>
<td>Click the Count link to launch the Configuration Never Collected Device page.</td>
</tr>
<tr>
<td>Edit Protocol Order</td>
<td>Click this button, if you want to change the transport protocol order.</td>
</tr>
</tbody>
</table>

**Inventory Device Status**

In Inventory Device Status portlet, you can view the number of devices along with its configurations and inventory collection status (Managed State, Suspended State, Unmanaged State, Devices not matching the Policy).

Table 1-15 lists Inventory Device Status portlet details.
To configure Inventory Device Status:

**Step 1** Click the Configuration icon.

**Step 2** Select the minute and hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed at the changed Refresh frequency.

**Step 3** Select the Show Zero Counts check box to view the device status is zero.

**Step 4** Click **Save** to view the portlet with the configured settings.

You can click the portlet name in the title bar to navigate directly to the Device Management State Summary details page.

---

### Table 1-15  Inventory Device Status Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Device Status</td>
<td>The status of the device. The states are:</td>
</tr>
<tr>
<td></td>
<td>• Managed State</td>
</tr>
<tr>
<td></td>
<td>• Suspended State</td>
</tr>
<tr>
<td></td>
<td>• Unmanaged State</td>
</tr>
<tr>
<td></td>
<td>• Managed Devices not matching the Policy</td>
</tr>
<tr>
<td>Count</td>
<td>The number of devices.</td>
</tr>
<tr>
<td></td>
<td>You can click the number corresponding to the device state to view the</td>
</tr>
<tr>
<td></td>
<td>corresponding page.</td>
</tr>
</tbody>
</table>

---

OL-25948-01

Inventory Management with Cisco Prime LAN Management Solution 4.2

1-13
Device and Credential Repository

The Device and Credential Repository (DCR) is a common repository of devices, their attributes, and credentials. The Device and Credential Admin provides an interface to administer DCR. See, Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.

To access DCR, select Inventory > Device Administration > Add / Import / Manage Devices.

This section contains Understanding DCR.

For more information on:
- Discovering devices, see Discovering Devices.
- Managing devices, see Managing Devices and Credentials.
- AUS servers, see Managing Auto Update Servers.

**Understanding DCR**

DCR provides:
- A central place where you can add or import new devices.
- Easier and faster access to device and credential data.
- Secure data persistence, access and transport.
- Rationalized and controlled replication, with less user-level data reconciliation.
- Better integration with third-party and Cisco network-management applications.

DCR also:
- Stores device attributes and credentials, permits dynamic creation of attribute types, and permits default grouping and filtering.
- Supports proxy device attributes, unreachable devices, and pre-provisioning of devices.
- Allows you to populate the repository by importing devices from many sources. It also allows you to export device data to be used with third-party network management systems such as NetView and HP OpenView Network Node Manager.
- Uses a unique Internal Device Identifier to access device details, and detects duplicate devices based on specific attributes.
- Encrypts credential data stored in the repository. Access to device data is permitted only by secured channel and client authentication.
- Supports IPv6 and SNMP v3.
Understanding DCR

This section contains the following:

- Device Types
- Device Attributes
- Device Credentials
- DCR Architecture

Device Types

DCR supports the following four types of device:

- **Standard type**
  Devices such as Routers, Switches, Hubs, and other common devices are managed using this management type.

- **AUS Managed devices**
  The Cisco Prime Auto Update Server is a web-based interface for upgrading device configuration files and software images on firewalls that use the auto update feature. You can use this interface to add, edit, and delete devices.

- **Cluster Managed devices**
  The Cisco clusters and their member devices are managed using this device management type.

- **CNS Managed devices**
  The CNS managed devices refer to the devices managed by Cisco Networking Services.

- **Non-Cisco Devices**
  Many Non Cisco devices are categorized as Non-Cisco Devices. The sysOIDs of the supported Non-Cisco Devices in LMS are available in the mdfdata_NonCisco.xml located at:
    - `\NMSROOT\lib\classpath\com\cisco\nm\cwcs\mdf\mdfdata_NonCisco.xml` (on Windows)
    - `/opt/CSCOpx/lib/classpath/com/cisco/nm/cwcs/mdf/mdfdata_NonCisco.xml` (on Solaris and Soft Appliance)

The Non-Cisco Devices that are not listed in the above file will be classified as Unknown devices.

- Non-Cisco Devices are not considered for license check in UDM. If these devices match the device management policy, they will be in managed state.
- Once the Non-Cisco Devices are moved to the managed state, it triggers the MIB II level of Inventory for Inventory, Config and Image Management support and data collection.
- Config and SWIM functionalities are not supported. Only system and interface information (MIB II) is collected for Non-Cisco devices through Inventory.
- For IPSLA Performance Management, Target can be a non-Cisco device but responder should be a Cisco device.
- For Device Performance Management:
  - Non-Cisco devices will be managed using MIB II variables automatically
  - Support for third party MIBs for Non-Cisco devices. The third party MIB file should have .my extension.
- Interface-related system-defined pollers will not work as Interface pollers are dependant on the Network Topology, Layer 2 Services and User Tracking module, and the Inventory, Config and Image Management module for getting the PMC port details. If you create a user-defined poller, devices can be polled using the Interface-related template.

- The following five system-defined templates can be used for Non-Cisco devices:
  - Device Availability
  - Interface Availability
  - Interface Utilization
  - Interface Errors
  - PoE PSE Consumption

- In LMS 4.2, for Fault Management, Non-Cisco devices will be moved to known state and trap support is provided for Non-Cisco devices.

The following are the list of events that are supported for Non-Cisco and Unknown devices:
  - Unresponsive
  - OperationallyDown
  - Flapping
  - Duplicate
  - HighBroadcastRate
  - HighDiscardRate
  - HighErrorRate
  - HighQueueDropRate
  - HighUtilization – On interfaces only
  - All Pass-Through Standard SNMP Traps

---

**Note**

For Non-Cisco and Unknown devices, only interface and ports details are managed.

- For CiscoView, Non-Cisco devices are not supported
- For Network Topology, Layer 2 Services and User Tracking:
  - Data collection will collect non-Cisco device detail like, sysOID, hostname, syslocation.
  - The device selector will not show the non-Cisco devices.
  - Topology services will show non-Cisco device in unconnected view.
  - The delete device, data collection, rediscover, telnet and SSH menu items will be enabled for non-Cisco devices.
  - User Tracking will not discover users and hosts in a network connected to non-CDP devices.
  - The device attributes, port attributes, VLAN report, Change Management IP, IVR configure and Add to critical poller menu item will be disabled for non-Cisco devices.
Device Attributes

Device attributes are unique to each device and are used to identify device properties, such as device name and host name. See Mandatory Device Attributes for more information on mandatory device attributes.

The following attributes are stored in the repository:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host_name</td>
<td>Device Host name.</td>
</tr>
<tr>
<td>domain_name</td>
<td>Domain name of the device.</td>
</tr>
<tr>
<td>management_ip_address</td>
<td>IP Address used to access the device. Both IPv4 and IPv6 address types are supported.</td>
</tr>
<tr>
<td>device_identity</td>
<td>Identifies pre-provisioning devices. The value is application specific.</td>
</tr>
<tr>
<td>display_name</td>
<td>Device name, as you want it to be represented in reports or graphical displays. Can be derived from Host Name, Management IP Address or Device Identity.</td>
</tr>
<tr>
<td>sysObjectID</td>
<td>sysObjectID value of Cisco or non-Cisco devices. It may be UNKNOWN if the facility that populates the repository is not aware of the value.</td>
</tr>
<tr>
<td>mdf_type</td>
<td>Normative name for the device type as described in Cisco’s Meta Data Framework (MDF) database or other vendor’s MDF database. Each device type has a unique normative name defined in MDF.</td>
</tr>
<tr>
<td>DCR Device ID</td>
<td>Internally generated unique sequential number that identifies the device record in the DCR database. The DCR clients should know the value to access device details from the repository.</td>
</tr>
</tbody>
</table>

User Defined Fields (UDF)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http_mode</td>
<td>Current transport mode.</td>
</tr>
<tr>
<td>http_port</td>
<td>The HTTP Port.</td>
</tr>
<tr>
<td>https_port</td>
<td>The HTTPS Port.</td>
</tr>
<tr>
<td>cert_common_name</td>
<td>Certificate Common Name.</td>
</tr>
</tbody>
</table>

Individual applications interact with the repository to get the device list, device attributes, and device credentials.

Mandatory Device Attributes

The mandatory attributes are:

- Management IP Address or Host Name or Device Identity.
• Device Name.
Apart from these attributes, there are few attributes that are mandatory for each management type of devices. They are:
• CNS managed devices — CNS Server is mandatory.
• AUS managed devices — Auto Update Device ID and Auto Update Server fields are mandatory.
• DSBU Cluster managed devices — DSBU member number is sufficient.
The Device Name and the Host Name/Domain Name combination must be unique for each device in DCR. A device will be considered duplicate if:
• The Device Name of a device is the same as the Device Name of any other device.
• The Host Name/Domain Name combination of a device is the same as that of any other device.
• Auto Update Device ID is the same as Auto Update Device ID of any other device (when the device is AUS managed)
• Cluster and Member Number, together is the same as that of any other device (when the device is Cluster managed)

Note
DFM is the only application in LMS that does not consider the device name configured in DCR. Instead, DFM does its own resolution on the IP address to get a hostname. Ensure that DNS or host file is properly configured so that the IP address being managed by DFM resolves to a hostname, and that hostname resolves back to that IP address.

Device Credentials

Device credentials are values that are used by applications to access and operate on devices. It is typically a SNMP community string or a user ID and password. A device credential accesses a managed device such as a switch or router.

Credentials are encrypted and stored in DCR. The maximum length of a credential after encryption is 128 characters and credentials must not exceed this limit.

This section contains the following:
• Device Credentials in DCR
• Secondary Credentials
• SNMP Credentials
• Device Credentials of Other Management Types

Device Credentials in DCR

The following credentials can be associated with a device in DCR:

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary_username</td>
<td>Primary username used to access the device.</td>
</tr>
<tr>
<td>primary_password</td>
<td>Password for the Primary username.</td>
</tr>
</tbody>
</table>
### Understanding DCR

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary_enable_password</td>
<td>Console-enabled password for the device. Allows you to make configuration changes and provides access to a larger set of commands.</td>
</tr>
<tr>
<td></td>
<td>Without the enable password, users are restricted to read-only operations.</td>
</tr>
<tr>
<td>secondary_username</td>
<td>Secondary username used to access the device, when device access using the primary credentials fails.</td>
</tr>
<tr>
<td>secondary_password</td>
<td>Password for the secondary username.</td>
</tr>
<tr>
<td>secondary_enable_password</td>
<td>Console-enabled secondary password for the device. Allows you to make configuration changes and provides access to a larger set of commands, when device access using the primary console-enabled password fails.</td>
</tr>
<tr>
<td></td>
<td>Without the enable password, you cannot make any configuration changes. You can perform read-only operations.</td>
</tr>
<tr>
<td>rxboot_mode_username</td>
<td>Special case username (for example, RxBoot mode in 2500).</td>
</tr>
<tr>
<td>rxboot_mode_password</td>
<td>Password for the Rx Boot Mode user.</td>
</tr>
<tr>
<td>snmp_v2_ro_comm_string</td>
<td>SNMP V2 read-only community string of the device.</td>
</tr>
<tr>
<td>snmp_v2_rw_comm_string</td>
<td>SNMP V2 read/write community string of the device.</td>
</tr>
<tr>
<td>snmp_v3_user_id</td>
<td>SNMP V3 user ID of the device.</td>
</tr>
<tr>
<td>snmp_v3_password</td>
<td>SNMP V3 password of the device.</td>
</tr>
<tr>
<td>snmp_v3_engine_id</td>
<td>SNMP V3 engine ID of the device.</td>
</tr>
<tr>
<td>snmp_v3_auth_algorithm</td>
<td>SNMP V3 authentication algorithm used. Can be MD5 or SHA-1.</td>
</tr>
<tr>
<td>snmp_v3_priv_algorithm</td>
<td>SNMP V3 privacy algorithm used in AuthPriv mode. Can be DES, 3DES, AES128, AES192, and AES256.</td>
</tr>
<tr>
<td>snmp_v3_priv_password</td>
<td>SNMP V3 privacy password of the device in AuthPriv mode.</td>
</tr>
<tr>
<td>http_username</td>
<td>HTTP-interface user ID of the device.</td>
</tr>
<tr>
<td>http_password</td>
<td>HTTP-interface password of the device.</td>
</tr>
<tr>
<td>secondary_http_username</td>
<td>HTTP-interface secondary user ID of the device.</td>
</tr>
<tr>
<td>secondary_http_password</td>
<td>HTTP-interface password for the secondary user ID of the device.</td>
</tr>
</tbody>
</table>

### Additional Credentials for Cluster Managed Devices

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsbu_member_number</td>
<td>Number of the Cluster member. This number represents the order in which the device was added to the cluster.</td>
</tr>
<tr>
<td>parent_dsbu_id</td>
<td>DCR Device ID of the parent Cluster device.</td>
</tr>
</tbody>
</table>

### Auto Update Server Specific Credentials

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aus_url</td>
<td>URL for the AUS device.</td>
</tr>
<tr>
<td>aus_port</td>
<td>Port number of the AUS service running on the AUS device.</td>
</tr>
<tr>
<td>aus_username</td>
<td>User login providing access to the AUS device.</td>
</tr>
<tr>
<td>aus_password</td>
<td>Password for the corresponding aus_username.</td>
</tr>
</tbody>
</table>
Secondary Credentials

DCR stores both the primary and secondary device credentials. Secondary credentials comprise a username, a password and a console-enabled password for the devices. You can use the secondary credentials as a fallback to access the devices if you cannot access them using primary credentials.

For example, assume you have configured devices in your network to be in TACACS mode and you have stored the TACACS credentials as the primary credentials. The local username and password are stored as secondary credentials to access devices. If the AAA server is not running, you cannot access the devices using primary TACACS credentials. Instead, you can use the secondary credentials as a fallback to access the devices in your network.

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto Update Server Managed Device-Specific Credentials</strong></td>
<td></td>
</tr>
<tr>
<td>aus_username</td>
<td>User login providing access to the AUS-managed device.</td>
</tr>
<tr>
<td>aus_password</td>
<td>Password for the corresponding aus_username.</td>
</tr>
<tr>
<td>parent_aus_id</td>
<td>DCR Device ID of the managing AUS device.</td>
</tr>
<tr>
<td><strong>CNS Managed Device Specific Credentials</strong></td>
<td></td>
</tr>
<tr>
<td>parent_cns_id</td>
<td>Device ID of the parent CNS server (CNS Configuration Engine).</td>
</tr>
<tr>
<td>cns_config_id</td>
<td>CNS Config ID of the device.</td>
</tr>
<tr>
<td>cns_image_id</td>
<td>CNS Image ID of the device.</td>
</tr>
<tr>
<td>cns_event_id</td>
<td>CNS Event ID of the device.</td>
</tr>
</tbody>
</table>
Chapter 2      Device and Credential Repository

SNMP Credentials

The SNMP credentials are used to access the devices in the network.

DCR stores both:

- SNMPv2 credentials
- SNMPv3 credentials for all security levels.

The SNMPv3 protocol provides the security features such as message integrity, authentication, and encryption based on the security levels.

The following table lists the SNMP security levels and the SNMP credentials stored in DCR for each level:

<table>
<thead>
<tr>
<th>SNMP Version</th>
<th>Security Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>SNMP Credentials in DCR</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2</td>
<td>NoAuthNoPriv(^1)</td>
<td>Uses a community string match for authentication</td>
<td>Not Supported</td>
<td>• snmp_v2_ro_comm_string&lt;br&gt;• snmp_v2_rw_comm_string</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>NoAuthNoPriv</td>
<td>Uses a username match for authentication</td>
<td>Not Supported</td>
<td>• snmp_v3_user_id</td>
</tr>
<tr>
<td>AuthNoPriv</td>
<td></td>
<td>Provides authentication based on the authentication algorithms (MD5 or SHA)</td>
<td>Not Supported</td>
<td>• snmp_v3_user_id&lt;br&gt;• snmp_v3_password&lt;br&gt;• snmp_v3_auth_algorithm</td>
</tr>
<tr>
<td>AuthPriv</td>
<td></td>
<td>Provides authentication based on the authentication algorithms (MD5 or SHA)</td>
<td>Provides encryption based on the privacy algorithm such as DES, 3DES, AES128, AES192, and AES256</td>
<td>• snmp_v3_user_id&lt;br&gt;• snmp_v3_auth_algorithm&lt;br&gt;• snmp_v3_password&lt;br&gt;• snmp_v3_priv_algorithm&lt;br&gt;• snmp_v3_priv_password</td>
</tr>
</tbody>
</table>

1. SNMPv2 supports only the NoAuthNoPriv security level.

During the configuration of SNMP credentials, if you:

- Specify only SNMPv3 username, this denotes that the SNMPv3 security level is NoAuthNoPriv.
- Specify SNMPv3 username, SNMPv3 password and SNMPv3 authentication algorithm, this indicates that the SNMPv3 security level is AuthNoPriv.
- Specify SNMPv3 username, SNMPv3 password, SNMPv3 authentication algorithm, SNMPv3 privacy algorithm, and SNMPv3 privacy password, this indicates that the security level is AuthPriv.
Device Credentials of Other Management Types

DCR supports Cisco Cluster Management Suites, Auto Update Servers and the managed devices, CNS Configuration Engine and CNS Managed devices, using a mix of standard and additional attributes and credentials.

- Clusters: All the attributes of the Cluster are the same as a normal DCR device.
- Cluster Members: Each cluster member has its own Host Name, sysObjectID, and MDF type, and uses the same Telnet credentials as the Cluster. Each cluster member has the following additional attributes:
  - Member Number: Number of the Cluster member. This number represents the order in which the device is added into the cluster.
  - Device ID of the Parent Cluster record.
- Auto Update Server: This has the following attributes and credentials:
  - URN
  - Username
  - Password
- Auto Update Server managed devices: Apart from having its own attributes and credentials as normal DCR devices in DCR, each Auto Update Server managed device has the following additional attributes:
  - Device Identity: String value that uniquely identifies this device in the parent Auto Update Server.
  - DCR Device ID of the Parent Auto Update Server record.

DCR Architecture

The sharing of device list and credentials among various network management products is achieved through a Client-Server mechanism. The clients are network management applications that use DCR. The server is called the DCR Server.

DCR works based on a Master-Slave model. The DCR mode is set to Standalone, by default.

This section contains:

- Master DCR
- Slave DCR
- Standalone DCR

Master DCR

Refers to the master repository of device list and credential data. The Master hosts the authoritative, or a master-list of all devices and their credentials. All other DCRs in the same management domain that are running in Slave mode, normally shares this list.

There is only one Master repository for each management domain, and it contains the most up-to-date device list and credentials.
DCR Master Server communicates with its Slaves through the HTTPS port. If there is a firewall in between the LMS Servers of the same DCR management domain, you must:

- Open the HTTPS port of LMS Servers for communication.
- Permit the ICMP requests and responses between the LMS Servers.

Only then the peer certificates can be exchanged and the communication could happen between the DCR Master and Slave servers.

Changes to the repository data in DCR Master are properly propagated to Slaves although you block or close the HTTPS port of DCR Slave Server in firewall. However the DCR status of Slave server is displayed as Unreachable in DCR Master.

But you should never block the HTTPS port of DCR Master Server in firewall. Otherwise communication between the servers in the same management domain will not happen.

**Note**

The default HTTPS port is 443. You can change the default HTTPS port number to some other port number.

**Slave DCR**

Refers to a repository that is an exact replica of the Master.

DCR Slaves are slave instances of DCR in other servers and provide transparent access to applications installed in those servers.

Any change to the repository data occurs first in the Master, and those changes are propagated to multiple Slaves. There can be more than one Slave in a management domain.

The Slave:

- Maintains an exact replica of the data managed by the Master for the management domain.
- Has a mechanism to keep itself synchronized with the Master.
- Will first update Master and then update its own repository data. This is in case of repository data updates.

DCR running in Master or Slave mode always has an associated DCR Group ID that indicates the Server’s management domain. This Group ID is generated when a DCR is set to Master mode, and communicated to all Slaves assigned to that Master.

**Standalone DCR**

In Standalone mode, DCR maintains an independent repository of device list and credential data. It does not participate in a management domain and its data is not shared with any other DCR. It does not communicate with or contain registration information about any other Master, Slave, or Standalone DCR.

The DCR mode is set to Standalone, by default, after a fresh installation of Cisco Prime.
CHAPTER 3

Discovering Devices

Device Discovery allows you to discover the devices from the network starting from the seed devices and updates the device information in DCR. Device Discovery data contains the information about the neighboring devices of seed devices you have specified.

Read the following notes before you configure the settings and start the Device Discovery:

- You should have the Network Administrator or Super Admin privileges to configure Device Discovery settings and start Device Discovery.
  However to view the Device Discovery summary, you should have the required privileges. View the Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.
- You can only discover Standard devices and Cluster Managed devices through Device Discovery feature. You cannot discover AUS Managed and CNS Managed devices from the network.
- When DCR or DCR Administration is down, you cannot start Device Discovery. However, you can configure Device Discovery settings.
  Scheduled jobs started before DCR Administration is down completes successfully but DCR is not updated with the new device credentials returned from Device Discovery.
- You can run Device Discovery in a Master-Slave setup. See Using Device Discovery Features in Various Setup for more information.

This chapter contains information on:

- Configuring Device Discovery Settings
- Starting Custom Discovery
- Viewing Discovery Details
- Using DCR Features in a Master-Slave Setup
- Standard Discovery
- Using Device Discovery Features in Various Setup
Configuring Device Discovery Settings

You should configure the following settings to start the Device Discovery:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Module Settings     | Allows you to configure or edit the Device Discovery modules to start Device Discovery.  
                       | See Configuring Discovery Module Settings for more information.                                                                                   |
| Seed Device Settings| Allows you to configure or edit module-specific and global seed devices which are used to initiate Device Discovery.  
                       | See Configuring Seed Device Settings for more information.                                                                                         |
| SNMP Settings       | Allows you to configure or edit the SNMP credentials required to discover the devices from the network.  
                       | See Configuring SNMP Settings for more information.                                                                                               |
| Filter Settings     | Allows you to include or exclude devices from Device Discovery and modify the filter settings.  
                       | Configuring filter settings is optional.                                                                                                         |
                       | See Configuring Discovery Filter Settings for more information.                                                                                   |
| Global Settings     | Allows you to configure or modify other Device Discovery settings such as preferred DCR device name, management IP Address and so on.  
                       | Configuring global settings is optional.                                                                                                         |
                       | See Configuring Global Discovery Settings for more information.                                                                                   |

The Discovery Settings Summary page helps you to configure all these settings and view the summary of the Device Discovery settings.

This section explains the following:

- Configuring Discovery Module Settings
- Configuring Seed Device Settings
- Configuring SNMP Settings
- Configuring Discovery Filter Settings
- Configuring Global Discovery Settings
- Viewing Custom Discovery Settings Summary
Device Discovery feature in LMS supports the following Device Discovery modules:

<table>
<thead>
<tr>
<th>Discovery Modules</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 3 Discovery Protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address Resolution Protocol</td>
<td>• Address Resolution Protocol (ARP) is an Internet Protocol that maps IP Address to a MAC address.</td>
<td>No device side configuration is required.</td>
<td>• If the ARP table is big, it takes more time to find the MAC address.</td>
</tr>
<tr>
<td></td>
<td>• This Device Discovery module depends on the Routing Table Device Discovery module.</td>
<td></td>
<td>• Network devices that do not generate traffic (like switches) may be missing from the ARP table.</td>
</tr>
<tr>
<td></td>
<td>• When this module is enabled, Discovery will query each seed device (and its peers) for their ARP tables via SNMP. The specific objects used are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>– ipNetToMediaNetAddress</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>– ipNetToMediaPhysAddress</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>– ipNetToMediaIfIndex</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>– ipNetToMediaType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Border Gateway Protocol</td>
<td>• Border Gateway Protocol (BGP) is an exterior gateway protocol.</td>
<td>Uses few network and device resources.</td>
<td>Switches or routers that are not BGP neighbors will not get discovered.</td>
</tr>
<tr>
<td></td>
<td>• This module uses Border Gateway Peer Table to identify its BGP peer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When this module is enabled, Discovery will query the BGP routing table on each seed device (and its peers) via SNMP. The object used is bgpPeerRemoteAddr</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Device Discovery Settings

#### Chapter 3: Discovering Devices

<table>
<thead>
<tr>
<th>Discovery Modules</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| **Open Shortest Path First Protocol** | • Open Shortest Path First (OSPF) Protocol is an interior gateway routing protocol.  
• The OSPF Discovery module uses ospfNbrTable and ospfVirtNbrTable MIB to find its neighbor’s IP Addresses.  
• When this module is enabled, Discovery will query the OSPF routing table on each seed device (and its peers) via SNMP. The object used is ospfNbrIpAddr | Uses few network and device resources. | Switches or routers that are not OSPF neighbors will not get discovered. |
| **Routing Table**            | • Routing Table module queries and analyzes routing tables on seed routers, and discovers the subnets and next-hop routers.  
• When this module is enabled, Discovery will query the entire routing table on each seed device (and its peers) via SNMP. The objects used are:  
  - ipRouteNextHop  
  - ipRouteType  
  - ipRouteMask  
  - ipRouteIfIndex  
  - ipRouteDest | No device side configuration is required. | • If the Routing table in a device is big, it takes more time to find the MAC address.  
• Switches and routers that are not a next-hop in the routing table will not get discovered. |
<table>
<thead>
<tr>
<th>Discovery Modules</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Discovery Protocol</td>
<td>Cisco Discovery Protocol discovers devices independent of media and protocol used. This protocol runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. This Device Discovery module queries the CDP Neighbor Table to find out the neighboring devices. When this module is enabled, Discovery will query the CDP cache on each seed device (and its peers) via SNMP. The objects used from the CISCO-CDP-MIB are: - <code>cdpCacheAddressType</code> - <code>cdpCacheAddress</code> - <code>cdpCacheDeviceId</code> - <code>cdpCacheDevicePort</code> - <code>cdpCachePlatform</code> - <code>cdpCacheCapabilities</code> For ATM devices which are running ILMI, the following SNMP objects will be used from the ATM-MIB: - <code>atmInterfaceMyNeighborIpAddress</code> - <code>atmInterfaceMyNeighborIfName</code></td>
<td>Uses few network and device resources. Cisco Discovery Protocol supports IPv6.</td>
<td>CDP needs to be enabled on the interfaces. <strong>Note</strong> Enable only CDP on interfaces that are directly connected to network devices that you own. Interfaces connected to your users or your service provider should not have CDP enabled.</td>
</tr>
</tbody>
</table>
### Configuring Device Discovery Settings

#### Chapter 3  
**Discovering Devices**

**Link Layer Discovery Protocol (LLDP)**
- Link Layer Discovery module uses entPhysicalTable MIB to find its neighbor’s IP Address.
- CDP seed devices are also considered as LLDP seed devices, when LLDP module is selected in discovery.

**Note**
LLDP will support IPv4 devices only.

- When this module is enabled, Discovery will query the LLDP cache on each seed device (and its peers) via SNMP. The objects used from the LLDP-MIB are:
  - lldpRemManAddrOID
  - lldpRemSysCapEnabled

**Ping Discovery Options**
- This module gets a list of IP Address ranges from a specified combination of IP Address and Subnet Mask Device Discovery configuration. This module pings each IP Address in the range to check the reachability of devices.
- The Ping Sweep module does not require seed devices. Instead, you must specify a list of subnets and network masks which will be pinged.

<table>
<thead>
<tr>
<th>Discovery Modules</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Layer Discovery Protocol</td>
<td>- Link Layer Discovery module uses entPhysicalTable MIB to find its neighbor’s IP Address.</td>
<td>The LLDP discovers even the Non Cisco Devices.</td>
<td>The LLDP needs to be enabled on the interfaces.</td>
</tr>
<tr>
<td>(LLDP)</td>
<td>- CDP seed devices are also considered as LLDP seed devices, when LLDP module is selected in discovery.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LLDP will support IPv4 devices only.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- When this module is enabled, Discovery will query the LLDP cache on each seed device (and its peers) via SNMP. The objects used from the LLDP-MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- lldpRemManAddrOID</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- lldpRemSysCapEnabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping Sweep On IP Range</td>
<td>- This module gets a list of IP Address ranges from a specified combination of IP Address and Subnet Mask Device Discovery configuration. This module pings each IP Address in the range to check the reachability of devices.</td>
<td>- No device side configuration is required.</td>
<td>- Uses a lot of LMS server and network resources if the IP ranges are big.</td>
</tr>
<tr>
<td></td>
<td>- The Ping Sweep module does not require seed devices. Instead, you must specify a list of subnets and network masks which will be pinged.</td>
<td>- Discovers IPv6 device.</td>
<td>- Can take a lot of time to complete (hours or days on large deployments)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- IPS may see the ping sweeps as attacks and can deny the LMS server access to the server.</td>
</tr>
</tbody>
</table>
### Discovery Modules

<table>
<thead>
<tr>
<th>Others</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cluster Discovery Module</strong></td>
<td>• This module discovers the devices in a DSBU cluster.</td>
<td>Uses few network and device resources.</td>
<td>Routers and switches that are not cluster members will not get discovered.</td>
</tr>
<tr>
<td></td>
<td>• This queries the Cluster MIB to discover all members of the cluster.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When this module is enabled, Discovery will query switch cluster information from the seed devices (and their peers) using SNMP. The objects used from the CISCO-CLUSTER-MIB are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ccMemberNumber</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ccMemberOperStatus</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ccStatusClusterName</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ccStatusClusterMode</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hot Standby Router Protocol (HSRP)</strong></td>
<td>• This module discovers the devices from the HSRP group which consists of an active router and Standby routers. If the active router fails, one of the Standby router will server as an active router.</td>
<td>Uses few network and device resources.</td>
<td>Switches and routers that are not part of an HSRP group will not get discovered.</td>
</tr>
<tr>
<td></td>
<td>• The HSRP Discovery Module uses / in CISCO-HSRP-MIB to find active or standby routers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When this module is enabled, Discovery will query the HSRP state database on each seed device (and its peers) via SNMP. The objects used from the CISCO-HSRP-MIB are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cHsrpGrpVirtualIpAddr</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cHsrpGrpActiveRouter</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- cHsrpGrpStandbyRouter</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can run Device Discovery for one or more of these Device Discovery modules. You can select the Discovery modules from the Module Settings page.

Other than these Discovery modules, LMS by default supports System Discovery module and running Device Discovery for System module.
Chapter 3      Discovering Devices

Configuring Device Discovery Settings

The System module collects basic device information such as sysName, sysLocation, description, contact and type of services provided by MIB. It also tests transport availability. The System module queries the MIB2 Interface table and IP Address table for a device in order to populate the IP Address table of NGD.

To configure Device Discovery modules:

Step 1  Go to Inventory > Device Administration > Discovery > Settings.

The Device Discovery Settings page appears.

Step 2  Click either:

- The Configure button.

Or

- The Configure link next to the Module Settings field.

The Module Settings page appears.

Step 3  Select one or more of the following Device Discovery modules:

- Address Resolution Protocol (ARP)
- Border Gateway Protocol (BGP)
- Open Shortest Path First Protocol (OSPF)
- Routing Table
- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)
- Ping Sweep On IP Range
- Cluster Discovery Module
- Hot Standby Router Protocol (HSRP)

For example, if you want to discover the devices from a DSBU Cluster, you can select the Cluster Discovery module.

You should select CDP or Ping Sweep On IP Range or both to discover the IPv6 devices from the network.

Note  When you select the Address Resolution Protocol (ARP) module, the Routing Table Device Discovery module is also selected.

Step 4  Either:

- Click Next to configure Seed Devices Settings. See Configuring Seed Device Settings for more information.

Or

- Click Cancel to exit the wizard.

The Finish button is disabled in this page. You can only click the Next button to configure the seed devices.
Configuring Seed Device Settings

Seed devices are the devices used to initiate network discovery. A seed device is the starting point from which LMS Device Discovery discovers the network and its peer or neighbor devices.

You can specify:

- Module specific seed devices—These seed devices are specific to a Device Discovery module that you have selected in the Module Settings page. See Configuring Discovery Module Settings for more information. Devices are discovered for a specific Device Discovery module based on the seed device settings.

- Global seed devices—These seed devices are common to all the Device Discovery modules you have selected for Device Discovery. The Global seed devices are aggregated to the list of module-specific seed devices if you have used any one or both of the following options to specify seed devices:
  - Seed devices from a file
  - Manual addition of seed devices options

See Options to Specify Seed Devices to understand about the options to specify seed devices.

**Note**

- You can specify only a Cisco device as seed device for CDP protocol.
- If you have selected more than one Layer 3 Discovery module and entered different seed devices for selected modules, Device Discovery runs for all the seed devices for all selected Layer 3 Discovery modules.

This section contains:

- IPv4 and IPv6 Addresses as Seed Devices
- Options to Specify Seed Devices
- Specifying Seed Devices in a File
- Specifying Module Specific Seed Devices
- Specifying Global Seed Devices

IPv4 and IPv6 Addresses as Seed Devices

You can specify hostname or IP Address as a seed device.

IPv6 Addresses can be specified as Module-specific seed devices only for the following Device Discovery modules:

- CDP
- Ping Sweep On IP Range

All other Discovery modules except CDP and Ping Sweep On IP Range, accept only IPv4 Addresses as seed devices.

You can configure IPv4 and/or IPv6 Addresses as Global seed devices. However, Global IPv6 seed devices are considered only by the CDP module. The rest of the Discovery modules (except CDP) do not discover devices starting from IPv6 seed devices.
Note: Ping Sweep On IP Range module does not consider Global IPv4/IPv6 addresses of seed devices for Device Discovery.

Options to Specify Seed Devices

You can specify the seed devices using any or all of the following options:

- **Seed devices from DCR**
  IP Address or hostname of all devices stored in DCR are added as seed devices. This is a global option and applies to all the Device Discovery modules.
  
  Ensure that the DCR has at least one device before you choose this option to specify seed devices.
  
  Hop count value of -1 (unlimited number of hops) is used for Device Discovery, by default, when you choose the seed devices from DCR.
  
  Subsequent Device Discoveries by list of seed devices from DCR may discover more devices from the network than the initial Device Discovery cycles.
  
  For example, consider you have scheduled a Device Discovery job with the DCR devices as seed list. The first run may discover 50 devices from the network. The subsequent runs may find devices more than 50 because of unlimited number of hops and add the newly fetched devices to DCR.

- **Seed devices from a file**
  You can enter the IP Addresses or hostname of seed devices in a file and store the input file in the client machine. In the Seed Device Settings page, you can select this input file to specify the list of seed devices for Device Discovery.
  
  The input file should either be a text (.txt) or Comma Separated Value (.csv) file only. See Specifying Seed Devices in a File for more information.

- **Manual addition of seed devices**
  You can manually specify the IP Address or hostname of seed devices when you configure seed devices for Device Discovery. See Specifying Module Specific Seed Devices and Specifying Global Seed Devices for more information.

Specifying Seed Devices in a File

The seed devices file can contain:

- Module specific seed devices
  
  The input seed devices file for module-specific seed devices settings should contain the following in each line:

  **Seed Device | Number**
  
  where **Seed Device** is the IP Address or hostname of the device and **Number** is the hop count or Subnet mask.

  - You can specify the hop count in the input seed devices file for all Discovery modules except Ping Sweep On IP Range.

    For example, the seed devices file for Device Discovery modules can contain the following seed devices:

    10.77.210.220|2
    10.77.210.225|3
The seed devices file for CDP module can contain IPv6 Addresses as seed devices. For example, the seed devices file for the CDP Discovery module can contain the following seed devices:

```
10.77.210.212 | 2
EF12:0:0:0:ABCD:0:0:123 | 3
10.77.209.216 | 3
0:0:0:0:FFFF:33:240:20 | 2
```

- You should specify Subnet mask in the input seed devices file only for Ping Sweep On IP Range module. You can include IPv4 or IPv6 Addresses as seed devices.

For example, the seed devices file for Ping Sweep On IP Range module can contain the following seed devices:

```
10.77.210.220 | 255.255.255.0
10.77.210.225 | 255.255.255.0
ABCD:EF12:0:0:0:0:0:3456 | FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FF00
```

- You can specify CIDR in the input seed devices file for PingSweep module.

For example, the seed devices file for PingSweep module can contain the following seed devices:

```
10.77.215.3/12
10.77.215.3/12
10:EF:14:32:0:0:0:210/64
```

For IPv4, the CIDR range is from 1 to 32.

For IPv6, the CIDR range is from 1 to 128.

---

**Note**

CIDR takes precedence over the subnet mask. For example, if you use seed device 10.77.215.3/12 | 255.255.255.255 in UI it shows only 10.77.215.3/12 and not the subnet mask.

- Global seed devices

The input seed devices file for global seed devices settings should contain only one IP Address in each line.

For example, the seed devices file can contain the following seed devices:

```
10.77.210.220
10.77.210.225
10.77.209.205
10.77.200.213
```
Specifying Module Specific Seed Devices

To configure the seed devices for Device Discovery modules:

**Step 1**
Go to **Inventory > Device Administration > Discovery > Settings**.
The Device Discovery Settings page appears.

**Step 2**
Either:
- Click the **Configure** link next to the Seed Device Settings field.
  - If you have not configured Seed devices earlier, this link will not be available. Instead, the status will be displayed as Not Configured.

Or
a. Click the **Configure** button.
   - The Module Settings page appears.

   b. Click **Next**.
      - You cannot click the Next button unless you have selected one or more Device Discovery modules. See **Configuring Discovery Module Settings** for more information on selecting Device Discovery modules.

The Seed Devices Settings page appears.

**Step 3**
Click **Module Specific** from the Seed devices panel at the left.
The list of modules selected in the Module Settings page is displayed.

**Step 4**
Select a module from the list of displayed modules.
The Seed Devices settings for the selected module appears at the right.

**Step 5**
Enter the name of the file with its full path in the **From File** field, if you want to specify the seed devices from a file.
If you do not know the path, you can click **Browse** and select a file from the list.

**Step 6**
Select **Jump Router Boundaries** to extend Device Discovery beyond the boundaries set by routers on your network.
This option is available only for the CDP and LLDP Modules.
You must be cautious about enabling Discovery to occur beyond router boundaries.
Discovery could take much longer if you do not selectively choose the boundaries by excluding specific IP Addresses.

**Step 7**
Select **Use DCR As Seed List**, if you want to specify the devices in DCR as seed devices.
This option is not available for the Ping Sweep On IP Range option.

**Step 8**
Enter the following fields which appears only for Ping Sweep On IP Range Device Discovery module.
- **ICMP Retry**— No of retries to connect to a device using ICMP protocol if the device is not reachable or network is down. The default is 1 retry.
- **ICMP Timeout**— Time within which the device should send its response to the network. The default timeout is 1000 milliseconds.
- **InterPacket Timeout**— Time delay between two ICMP packets. The default timeout is 20 milliseconds.
**Step 9** Perform the following if you want to specify the seed devices manually:

a. Click **Add** to add a new row.

b. Enter the IP Address or hostname of the seed device in the Seed Device field.

   Ping Sweep On IP Range Device Discovery module supports both CIDR and subnet mask to find the range of IP Addresses. For example, you can enter 192.168.135.0/21 or 192.168.135.0 255.255.248.0 in the Seed Device field.

---

**Note**

Do not add seed devices containing wildcard characters.

c. Enter the number of hops in the Hop Count field.

   This field is available for all Device Discovery modules except Ping Sweep On IP Range. Hop count limits the scope of Device Discovery. Device Discovery cycle may take a longer time if you enter a larger number of hops.

d. Enter the Subnet Mask in the Subnet Mask field.

   The default value is 255.255.255.255. This field is available only for Ping Sweep On IP Range Device Discovery module.

   If you enter the IPv6 Address of a device as seed device, you should enter a valid IPv6 Subnet Mask in this field. For example, you can enter the Subnet Mask for IPv6 seed device as FFFF::FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

   Compressed formats of IPv6 Subnet Mask are not supported for Ping Sweep On IP Range Discovery module. For example, you cannot enter FFFF::FFFF:FFFF:FFFF:FFFF:: as IPv6 Subnet Mask.

---

**Note**

Entering a smaller Subnet Mask value may result in a longer Discovery cycle, as Discovery has to sweep IP Addresses from more networks. For example, the Subnet Mask 255.255.0.0 has to discover more networks than the Subnet Mask 255.255.255.0.

You can also do the following:

- To add more seed devices, click **Add** to introduce more rows and enter the seed devices.
- To delete seed devices, select the check boxes corresponding to the seed devices and click **Delete**.

**Step 10** Click any one of the following:

- **Next** to configure SNMP Settings. See Configuring SNMP Settings for more information.
- **Finish to apply the settings** and exit the wizard.

   The Finish button is disabled when you add the seed device settings for the first time. If disabled, click the Next button to add the SNMP settings.

   You can click the Finish button only when you edit the Seed Device settings.
- **Cancel** to exit the wizard.
- **Back** to navigate to the previous page and change the Device Discovery settings.
Specifying Global Seed Devices

To configure the global seed devices for Device Discovery:

---

**Step 1**
Go to **Inventory > Device Administration > Discovery > Settings**.
The Device Discovery Settings page appears.

**Step 2**
Either:
- Click the **Configure** link next to the Seed Device Settings field.
  If you have not configured Seed devices earlier, this link will not be available. Instead, the status will be displayed as Not Configured.

  Or

  a. Click the **Configure** button.
  The Module Settings page appears.

  b. Click **Next**.
  You cannot click the Next button unless you have selected one or more Device Discovery modules. See **Configuring Discovery Module Settings** for more information on selecting Device Discovery modules.

  The Seed Devices Settings page appears.

**Step 3**
Click **Global** from the Seed devices panel at the left.
The Seed Devices settings common for all the selected modules appears at the right.

**Step 4**
Enter the name of the file with its full path in the From File field, if you want to specify the seed devices from a file.
If you do not know the path, you can click **Browse** and select a file from your machine.

**Step 5**
Select **Use DCR As Seed List**, if you want to specify the devices in DCR as seed devices.

**Step 6**
Perform the following if you want to specify the seed devices manually:

  a. Click **Add** to add a new row.

  b. Enter the IP Address (IPv4 or IPv6) of the seed device in the Seed Device field.

**Note**
Do not add seed devices containing wildcard characters.

You can also do the following:

- To add more seed devices, click **Add** to introduce more rows and enter the seed devices.
- To delete seed devices, select the check boxes corresponding to the seed devices and click **Delete**.

**Step 7**
Click any one of the following:

- **Next** to configure SNMP Settings. See **Configuring SNMP Settings** for more information.
- **Finish** to apply the settings and exit the wizard.
  The Finish button is disabled when you add the seed device settings for the first time. Then, you should click the Next button to add the SNMP settings.
  You can click the Finish button only when you edit the Seed Device settings.
- **Cancel** to exit the wizard.
Configuring SNMP Settings

You should configure SNMP credentials to run Device Discovery. See SNMP Credentials for more information on SNMP credentials.

You must configure at least one set of SNMPv2 or SNMPv3 credentials.

Multiple community strings are supported in LMS Device Discovery. For example, you can define more than one credential set for a same target with different community strings.

To configure SNMP settings:

Step 1
Go to Inventory > Device Administration > Discovery > Settings.

The Device Discovery Settings page appears.

Step 2
Either:

- Click the Configure link next to the SNMP Settings field.
  
  If you have not configured the SNMP settings earlier, this link will not be available. Instead, the status will be displayed as Not Configured.

  Or

  a. Click the Configure button.

  The Module Settings page appears.

  b. Click Next.

  You cannot click the Next button unless you have selected one or more Device Discovery modules. See Configuring Discovery Module Settings for more information on selecting Device Discovery modules.

  The Seed Devices Settings page appears.

  c. Click Next.

  You cannot click the Next button unless you have configured at least one seed device. See Configuring Seed Device Settings for more information to configure seed device settings.

  The SNMP Settings page appears.

Step 3
Select the appropriate radio button to select the SNMP version.

The supported SNMP versions are:

- SNMPv2c
- SNMPv3

Depending upon the radio button you select, the user interface displays appropriate to the SNMP versions selected. See Device Credentials in DCR for information on supported SNMP versions and SNMP credentials.

If you have selected the SNMPv2c radio button, the user interface displays an option to select or deselect SNMPv2c fallback to SNMPv1. By default SNMPv2c fallback to SNMPv1 is selected.

If you have selected the SNMPv3 radio button, the user interface displays an option to select or deselect SNMPv3 fallback to SNMPv2c.
You must configure the respective protocols to enable the fallback options. For example, to fallback to SNMPv2c from SNMPv3, you should have configured SNMPv2c settings. Device Discovery cycle may take a longer time to complete if you have enabled the fallback options.

**Step 4**

Click **Add** to configure SNMP Settings.

If you have configured the SNMP Settings earlier, select a row in the SNMP Settings page and click **Edit** to edit the SNMP settings.

A popup window appears with the following fields, if you have selected SNMPv2:

<table>
<thead>
<tr>
<th>Fields for SNMPv2 Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Target                    | Denotes the target device. Enter the IP Address of the target device. You can also use wildcard characters to specify the target device. You can enter a IPv6 Address in this field if you have selected CDP or Ping Sweep On IP Range or both as Discovery modules. You should enter only the IPv4 Address of the target device for all other Discovery modules except CDP and Ping Sweep On IP Range. You can also use wildcard characters to specify the target device. Examples for target device:  
  - 10. *[210-220].*  
  - ABCD:EF12:*:*:*:*:*:*  
  Entering a target device is mandatory. |
| Read Community            | Denotes the SNMP Read Community string of the device. Entering the read community string is mandatory. |
| Timeout                   | Denotes the time period after which the SNMP query times out. You must enter the timeout value in seconds. The default value of timeout is 3 seconds. The Device Discovery time may increase if you specify a larger value for timeout. The timeout doubles for every retry. For example, if the timeout value is 5 seconds and number of retries is 3:  
  - LMS Device Discovery waits for 5 seconds to get the response from the device for the first try, 10 seconds for second retry, and 20 seconds for last retry.  
  - LMS Device Discovery stops querying the device after 3 retries and the time lapses by 35 seconds. |
| Retries                   | Denotes the number of attempts made to query the device. You can specify any value between 0 to 8 as number of retries. The default number of retries is 2. |
| Comments                  | You can enter any remarks in this field. |
A popup window appears with the following fields, if you have selected SNMPv3:

<table>
<thead>
<tr>
<th>Fields for SNMPv3 Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Target                    | Denotes the target device. Enter the IP Address of the target device. You can also use wildcard characters to specify the target device. You can enter a IPv6 Address in this field if you have selected CDP, or Ping Sweep On IP Range, or both as Discovery modules. You should enter only the IPv4 Address of the target device for all other Discovery modules, except CDP and Ping Sweep On IP Range. You can also use wildcard characters to specify the target device. Examples for target device:  10. *[210-220]  
  ABCD:EF12:*:*:*:*:*:  
  Entering a target device is mandatory. |
| User Name                 | SNMPv3 username used to access the device. Entering a SNMPv3 username is mandatory for all security levels. |
| Auth Password             | SNMP V3 authentication password used to operate the devices in AuthNoPriv and AuthPriv modes. |
| Auth Algorithm            | SNMP V3 authentication algorithm used in AuthNoPriv and AuthPriv modes. The authentication algorithm can be MD5 or SHA-1. |
| Privacy Password          | SNMP V3 privacy password of the device in AuthPriv mode. |
| Privacy Algorithm         | SNMP V3 privacy algorithm used in AuthPriv mode. The privacy algorithm can be DES, 3DES, AES128, AES192, and AES256. |
| Timeout                   | Denotes the time period after which the SNMP query times out. You must enter the timeout value in seconds. The default value of timeout is 3 seconds. The Device Discovery time may increase if you specify a larger value for timeout. The timeout doubles for every retry. For example, if the timeout value is 5 seconds and number of retries is 3:  
  LMS Device Discovery waits for 5 seconds to get the response from the device for the first try, 10 seconds for second retry, and 20 seconds for last retry.  
  LMS Device Discovery stops querying the device after 3 retries and the time lapses by 35 seconds. |
| Retries                   | Denotes the number of attempts made to query the device. You can specify any value between 0 to 8 as number of retries. The default number of retries is 2. |
| Comments                  | You can enter any remarks in this field. |
Configuring Device Discovery Settings

Filters in Device Discovery allow to include or exclude devices from the network based on the following:

- IP Address
- DNS Domain
- SysObjectID
- SysLocation

This section contains:

- Important Notes on Configuring Discovery Filters
- Patterns in IP Address Filter Rules
- Regular Expressions in Filter Rules
- Specifying Discovery Filter Settings

Important Notes on Configuring Discovery Filters

Read the following notes, before you configure Device Discovery filters:

- You can either include or exclude devices based on the filters you have set. You cannot do both.
- You can configure only one filter type for a Device Discovery job. For example, if you want to configure IP Address based filters, you cannot configure other filter types. Even if you configure more filters, the filter applied at the last will be considered. The others will be ignored.

See SNMP Credentials for more information on SNMPv3 credentials and security levels.

**Step 5**
Click **Ok** to close the popup window and return to the SNMP Settings page.

**Step 6**
Use the check box to select a SNMP credential set in the SNMP Settings page and click:

- **Edit** to edit the SNMP settings.
- **Delete** to delete the SNMP settings.
  
  The Delete Confirmation dialog box appears. You should click **OK** to proceed.
  
  You can also select multiple records and delete them.

**Step 7**
Click any one of the following:

- **Next** to configure Discovery Filter Settings. See Configuring Discovery Filter Settings for more information.
- **Finish to apply the settings** and exit the wizard.
  
  The Finish button is disabled when you configure the SNMP Settings for the first time. Then, you should click the Next button to configure Device Discovery filter settings.
  
  You can click the Finish button only when you edit the SNMP settings.
- **Cancel** to exit the wizard.
- **Back** to navigate to the previous pages and change the Device Discovery settings.
Chapter 3  Discovering Devices

Configuring Device Discovery Settings

- Regular expressions are supported for filter types based on DNS Domain, SysObjectID, and SysLocation. IP Address based filter types do not support regular expressions. See Regular Expressions in Filter Rules for more information.
- You can include patterns when creating rules for IP Address filters. See Patterns in IP Address Filter Rules for more information.
- The expressions in filter rules are case sensitive.

Patterns in IP Address Filter Rules

When you define a Device Discovery inclusion or exclusion filters based on IP Address, you should follow these guidelines:

- Use the standard IPv4 Address format (4 octets separated by periods) for Discovery modules except CDP and Ping Sweep On IP Range.
- Use IPv4 or IPv6 Address format for CDP and Ping Sweep On IP Range Discovery modules.
- Any octet can have one of the following:

<table>
<thead>
<tr>
<th>Any Octet can have.</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numbers between:</td>
<td>• 10.77.240.225 (IPv4 Address)</td>
</tr>
<tr>
<td>• 0 to 255 for an IPv4 Address</td>
<td>• 001:DB8:0:2AA:FF:C0A8:0:640A (IPv6 Address)</td>
</tr>
<tr>
<td>• 0 to FFFF for an IPv6 Address</td>
<td></td>
</tr>
<tr>
<td>Asterisk (*) as wildcard denoting all numbers from 0 to 255 in an IPv4 Address and 0 to FFFF in an IPv6 Address.</td>
<td>• 10.<em>.</em>.240 (IPv4 Address)</td>
</tr>
<tr>
<td>• 001:<em>:0:2AA:FF:</em>:<em>:</em> (IPv6 Address)</td>
<td></td>
</tr>
<tr>
<td>Range of numbers in the {StartingNumber-EndingNumber} format, where:</td>
<td></td>
</tr>
<tr>
<td>• StartingNumber and EndingNumber should be numbers between 0 to 255 in an IPv4 Address and 0 to FFFF in an IPv6 Address.</td>
<td>• 10.77.220-240.210-220 (IPv4 Address)</td>
</tr>
<tr>
<td>• StartingNumber should not be greater than or equal to EndingNumber</td>
<td>• 001:DB8:0:[EE-FF]:FF:C0A8:0:[100-AA F] (IPv6 Address)</td>
</tr>
</tbody>
</table>

The following are the invalid examples of IP Address range:
- • 10.77.250-200.221 |
- • 10.77.200-250.221 |
- • 001:DB8:0:[EEE-EE]:FF:C0A8:0:[D-5] |
- • 001:DB8:0:AA-BB:FF:C0A8:0:[D-5]

The octets in an IP Address filter can also contain the combination of wildcard characters and range of numbers. Some examples of IP Address filter combinations include:
- 10. 77. [210-230].*
- 10.77.*. [110-210]
- 001:DB8: :*: FF:[C0A-DD8]:0: [5-D]
- [10-20]: [10-20]:[A-F]:2:4: :*: :*

When you define more than one rule for IP Address filter, these rules work together.

For example, if you specify 10.77.*.* and 10.77.210.* as two rules for IP Address inclusion filter, then all the devices matching 10.77.*.* is discovered. The rule 10.77.210.* will never be applied.
Regular Expressions in Filter Rules

Discovery filters based on DNS Domain, SysObjectID, and SysLocation supports regular expressions. You can use the following characters in regular expressions:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Period</td>
<td>Matches any character</td>
</tr>
<tr>
<td>(</td>
<td>Opening parenthesis</td>
<td>Marks the beginning of a group of matched characters</td>
</tr>
<tr>
<td>)</td>
<td>Closing parenthesis</td>
<td>Marks the end of a group of matched characters</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>Matches zero or more occurrences of a regular expression specified earlier</td>
</tr>
<tr>
<td>+</td>
<td>Plus character</td>
<td>Matches one or more occurrences of a regular expression specified earlier</td>
</tr>
<tr>
<td>\</td>
<td>Trailing slash</td>
<td>Identifies a special character within a regular expression</td>
</tr>
</tbody>
</table>

Examples of Regular Expressions in Filter Rules

- **SysObjectID based filter rules**
  - To include all devices with SysObjectID starting with `.1.3.6.1.4..`, you must enter a regular expression `\.1\\3\\6\\1\\4\\(.\)*` as an inclusion filter rule.
  - To exclude all devices with SysObjectID starting with `.1.3.6.1.4.n..`, where n is any number, you must enter a regular expression `\.1\\3\\6\\1\\4\\(.\)+` as an exclusion filter rule.

- **DNS Domain based filter rules**
  - To include all devices whose domain names end with `.cisco.com`, you must enter a regular expression `\.\+\cisco\\.com` as an inclusion filter rule.
  - To exclude all devices whose domain names contain `.cisco..`, you must enter a regular expression `\.\+\cisco\\(.\)+` as an exclusion filter rule.

- **SysLocation based filter rules**
  - To include all devices whose SysLocation name starts with `Che`, you must enter a regular expression `Che\(.\)*` as an inclusion filter rule.
  - To exclude all devices whose SysLocation name starts with `SAN`, you must enter a regular expression `SAN\(.\)*` as an exclusion filter rule.

Specifying Discovery Filter Settings

To configure Device Discovery filter settings:

**Step 1** Go to *Inventory > Device Administration > Discovery > Settings*.

The Device Discovery Settings page appears.

**Step 2** Either:

- Click the Configure link next to the Filter Settings field.
  
  If you have not configured the Filter settings earlier, this link will not be available. Instead, the status will be displayed as Not Configured.
Or
a. Click the Configure button.
   The Module Settings page appears.

b. Click Next.
   You cannot click the Next button unless you have selected one or more Device Discovery modules. See Configuring Discovery Module Settings for more information on selecting Device Discovery modules.
   The Seed Devices Settings page appears.

c. Click Next.
   You cannot click the Next button unless you have configured at least one seed device. See Configuring Seed Device Settings for more information to configure seed device settings.
   The SNMP Settings page appears.

d. Click Next.
   You cannot click the Next button unless you have configured at least one set of SNMP credentials. See Configuring SNMP Settings for more information to configure SNMP settings.

The Filter Settings page appears.

Step 3
Select a filter from Use Filter drop-down list box.
The supported filters are:
- IP Address
- DNS Domain
- SysObjectID
- SysLocation

Step 4
Select either Include Devices or Exclude Devices.

Step 5
Click Add to introduce a row.

Step 6
Enter a value in the row based on the filter type you have selected in the Use Filter drop-down list box.
See Patterns in IP Address Filter Rules and Important Notes on Configuring Discovery Filters before you enter a value for the filter rule.
If you have selected a SysObjectID filter, you can either:
- Enter a value in the text field.
  Or
- Click Select to open the Device Type Selector and select a sysObjectID for the available devices.
You can select only one sysObjectID at a time from the Device Type Selector.

Step 7
Click Add to introduce another row to define another rule.
To delete a rule, select the corresponding row and click Delete.

Step 8
Click any one of the following:
- Next to configure Global Discovery Settings. See Configuring Global Discovery Settings for more information.
- Finish to apply the settings and exit the wizard.
- Cancel to exit the wizard.
Configuring Global Discovery Settings

LMS Device Discovery supports the Jump Router Boundaries option by default. The Jump Router Boundaries option extends Device Discovery beyond the boundaries set by routers within the network. Device Discovery may take longer if you do not selectively choose the boundaries by excluding specific IP Addresses.

You can configure the other Device Discovery settings in the Global Discovery Settings page.

To configure the Global Device Discovery settings:

Step 1
Go to Inventory > Device Administration > Discovery > Settings.
The Device Discovery Settings page appears.

Step 2
Either:

- Click the Configure link next to the Global Settings field.
  If you have not configured the Global settings earlier, this link will not be available. Instead, the status will be displayed as Not Configured.

Or

a. Click the Configure button.
The Module Settings page appears.

b. Click Next.
You cannot click the Next button unless you select one or more Device Discovery modules. See Configuring Discovery Module Settings for more information on selecting Device Discovery modules. The Seed Devices Settings page appears.

c. Click Next.
You cannot click the Next button unless you configure at least one seed device. See Configuring Seed Device Settings for more information to configure seed device settings.
The SNMP Settings page appears.

d. Click Next.
You cannot click the Next button unless you configure at least one set of SNMP credentials. See Configuring SNMP Settings for more information to configure SNMP settings.
The Filter Settings page appears.

e. Click Next.
The Global Settings page appears.

Step 3
Enter the values in the following fields in the Global Settings page.
### Global Settings | Description
--- | ---
Preferred DCR Device Name | You can set the device name of the discovered devices in DCR as any one of the following:
- Sysname—Sysname of the device.
- DNS Resolvable Host Name—Fully Qualified Domain Name consisting a hostname and a domain name

Select the appropriate check box in the Preferred DCR Device Name panel.

- If you select both Sysname and DNS Resolvable Host Name then the discovery will first check whether Sysname is configured in the device. If the Sysname is configured then the discovery will make use of it and will update the DCR with Sysname. If the device is not a resolvable Sysname then it will fall back to check the DNS Resolvable Host Name of the device. If the device is not a DNS Resolvable Hostname, discovery will update the device with IP Address.

Select **Yes** if you want to append a domain name to device name, else select **No**.

- If you select only Sysname and the device is not configured with any Sysname then the Preferred DCR device name will be the IP Address of the device.

- If you select only DNS Resolvable Host Name and the device is not DNS Resolvable Host Name then the Preferred DCR device name will be the IP Address of the device.

- If you select neither Sysname nor DNS Resolvable Host Name then by default the Preferred DCR device name will be the IP Address of the device.

**Note** You can append domain name only when DNS Resolvable Host Name is selected as preferred DCR Device name and the Device IP is DNS resolvable.

The hostname of the device is set as the preferred DCR device name by default.
Configuring Device Discovery Settings

<table>
<thead>
<tr>
<th>Global Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCR Administration Settings</td>
<td>Update DCR Device Name</td>
</tr>
<tr>
<td></td>
<td>Select this check box if you want to update the device name of the devices that already exist in DCR, in the next Device Discovery cycle.</td>
</tr>
<tr>
<td></td>
<td>For example, consider a device which is discovered by LMS Device Discovery, exists in DCR with the device name as its DNS Resolvable Host Name.</td>
</tr>
<tr>
<td></td>
<td>If you change the Preferred DCR Device Name as Sysname for the next Device Discovery, LMS Device Discovery will update the device name of the device as its IP Address in DCR after the next Device Discovery.</td>
</tr>
<tr>
<td></td>
<td>The device name of devices are not overwritten in the future Device Discovery cycles if you have not selected this option.</td>
</tr>
<tr>
<td></td>
<td>Select a Default Credential Set</td>
</tr>
<tr>
<td></td>
<td>Select a default credential set name or select Policy configuration from the drop-down list box, if you want to add the discovered devices with the default credentials to DCR.</td>
</tr>
<tr>
<td></td>
<td>See Configuring Default Credential Sets and Configuring Default Credential Set Policy in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information on creating default credential sets and policies.</td>
</tr>
<tr>
<td>Global Settings</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Preferred Management IP</td>
<td>Select one of the following options as preferred Management IP Address of the device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use LoopBack Address</strong></td>
</tr>
<tr>
<td></td>
<td>Select this option to manage a device in the address assigned to the loopback interface.</td>
</tr>
<tr>
<td></td>
<td>If <strong>Prefer IPv4 over IPv6 Address</strong> is not selected and if there are multiple loopback IP Addresses, the highest loopback address is used to manage the device. See Use LoopBack Address Algorithm for more details.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Prefer IPv4 over IPv6 Address</strong> check-box is checked by default. A discovery done through an IPv6 address will check whether the device discovered has an IPv4 address. If the discovered device has a reachable <strong>IPv4</strong> address, that address is used as the management address, for more details refer to Prefer IPv4 over IPv6 Address Algorithm</td>
</tr>
<tr>
<td></td>
<td>• <strong>Resolve By Name</strong></td>
</tr>
<tr>
<td></td>
<td>LMS Device Discovery uses Domain Name Services (DNS), if available, to perform device name lookups. See Resolve By Name Algorithm for more details.</td>
</tr>
<tr>
<td></td>
<td>Select this option to do name resolution using the device name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Resolve By SysName</strong></td>
</tr>
<tr>
<td></td>
<td>Select this option to contact the DNS Server to pick up the device hostname. See Resolve By SysName Algorithm for more details.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong></td>
</tr>
<tr>
<td></td>
<td>Select this option if you do not want to manage the devices with preferred management IP Address.</td>
</tr>
<tr>
<td></td>
<td>When you select this option, the devices are added in DCR with their IP Addresses.</td>
</tr>
<tr>
<td></td>
<td>The Resolve By Name option is the default option for this field.</td>
</tr>
<tr>
<td></td>
<td>When the preferred management IP Address is set to None, the dual stack devices discovered from the network, are added to DCR with the IP Address available on the neighbor device lists.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter a valid e-mail ID in this field.</td>
</tr>
<tr>
<td></td>
<td>Multiple e-mail IDs are also allowed in this field.</td>
</tr>
<tr>
<td></td>
<td>The system uses the e-mail ID to notify about:</td>
</tr>
<tr>
<td></td>
<td>• Status of immediate or scheduled Device Discovery jobs upon their completion.</td>
</tr>
<tr>
<td></td>
<td>• New Device Discovery schedules.</td>
</tr>
<tr>
<td></td>
<td>• Stopped Device Discovery jobs</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td><strong>There may be a problem in sending e-mails when you have enabled virus scanner in the LMS Server.</strong></td>
</tr>
</tbody>
</table>
Chapter 3      Discovering Devices

Configuring Device Discovery Settings

Step 4
Click any one of the following:
- **Next** to view the summary of Device Discovery settings in the Device Discovery Settings page.
- **Back** to navigate to the previous pages and change the Device Discovery settings.
- **Finish** to save the settings and exit the Discovery Settings wizard.
- **Cancel** to exit the wizard.

### Use LoopBack Address Algorithm
This is the most preferred Management IP Address option. The algorithm operates in the following steps. Once a valid IP is found, the algorithm stops, and a management address is chosen.

1. Discovery searches through all IP (IPv4 and IPv6) addresses configured on the device for the loopback with the HIGHEST IP Address.
- Loopback interfaces are determined as those interfaces with an ifType of 24 (i.e. software Loopback).
- IPv4 addresses are preferred over IPv6 addresses. If no IPv4 addresses exist on any loopback, then an IPv6 address will be chosen.
- Only a reachable IP will be chosen. If the target loopback IP is not SNMP reachable, it will be skipped.

2. If no loopback IP Addresses are found, discovery will move on to ethernet interfaces. The ethernet interface with the HIGHEST IP will be chosen.
- Ethernet interfaces are determined as those interface with an ifType of 6 (ethernetCsmacd) or 26 (ethernet3Mbit).
- IPv4 addresses are preferred over IPv6 addresses. If no IPv4 addresses exist on any ethernet interface, then an IPv6 address will be chosen.
- Only a reachable IP will be chosen. If the target ethernet IP is not SNMP reachable, it will be skipped.

3. If no ethernet interface IP Addresses are found, discovery will move on to token ring interfaces. The token ring interface with the HIGHEST IP will be chosen.
- Token ring interfaces are determined as those interfaces with an ifType of 8 (iso88024TokenBus) or 9 (iso88025TokenRing).
- IPv4 addresses are preferred over IPv6 addresses. If no IPv4 addresses exist on any token ring interface, then an IPv6 address will be chosen.
- Only a reachable IP will be chosen. If the target token ring IP is not SNMP reachable, it will be skipped.

4. If no token ring interface IP Addresses are found, discovery will move on to serial interfaces. The serial interface with the HIGHEST IP will be chosen.
- Serial interfaces are determined as those interfaces with an ifType of 22 (propPointToPointSerial).
- IPv4 addresses are preferred over IPv6 addresses. If no IPv4 addresses exist on any serial interface, then an IPv6 address will be chosen.
- Only a reachable IP will be chosen. If the target serial IP is not SNMP reachable, it will be skipped.

5. If no serial interface IP Addresses are found, discovery will move on to virtual interfaces (e.g. VLAN interfaces). The virtual interface with the HIGHEST IP will be chosen.
- Virtual interfaces are determined as those interfaces with an ifTYpe of 53 (propVirtual).
- IPv4 addresses are preferred over IPv6 addresses. If no IPv4 addresses exist on any virtual interface, then an IPv6 address will be chosen.
- Only a reachable IP will be chosen. If the target virtual IP is not SNMP reachable, it will be skipped.

6. If no matching IP is found, then the management IP Address will be the IP by which the device was found by discovery.
### Prefer IPv4 over IPv6 Address Algorithm

The Prefer IPv4 over IPv6 algorithm for loopback addresses operates in the following steps. Once a valid IP is found, the algorithm stops, and a management address is chosen.

1. Discovery searches through all IPv4 addresses configured on the loopback interface. If many IPv4 addresses are found, HIGHEST IPv4 loopback interface address is chosen as the management IP and the algorithm processing stops.

#### Note

Only a reachable IP will be chosen. If the target loopback IP is not SNMP reachable, it will be skipped.

2. If no IPv4 addresses exist on any loopback, then the algorithm probes down to find IPv4 addresses of Ethernet interfaces. If there are many IPv4 Ethernet addresses found, HIGHEST IPv4 Ethernet address is chosen as the management IP and the algorithm processing stops.

3. If no loopback IPv4 Addresses of Ethernet interfaces are found, discovery will move on to token ring interfaces. If there are many IPv4 token ring addresses found by the discovery, the HIGHEST IPv4 token ring address will be chosen as the management IP and the algorithm processing stops.

4. If no token ring interface IPv4 Addresses are found, discovery will move on to serial interfaces. If there are many IPv4 serial interface addresses are found, the HIGHEST IPv4 serial interface address will be chosen as the management IP and the algorithm processing stops.

5. If no serial interface IPv4 Addresses are found, discovery will move on to virtual interfaces. If there are many IPv4 virtual interface addresses are found, the HIGHEST IPv4 virtual interface address will be chosen as the management IP and the algorithm processing stops.

6. If no matching IPv4 address is found, then the management IP Address will be the IPv6 address returned by discovery.

### Resolve By Name Algorithm

This is the management IP algorithm selected by default. This algorithm works by resolving the IP Address. The algorithm performs the following steps:

1. Perform a system resolver and optionally a direct DNS lookup of the IP Address.
   - If the system resolver lookup succeeds, the direct DNS query is not done.
2. If a hostname is found, resolve the hostname back to an IP Address.
3. If the IP Address returned when resolving the hostname is the same as the discovered IP then the discovered IP becomes the preferred management IP.
4. If the IP returned by the lookup is different from the discovered IP then that new IP is checked for SNMP reachability. If the new IP is reachable, then it becomes the preferred management IP.
5. Any failure will result in the original discovered IP to be the preferred management IP.
6. The hostname found in step 2 will become the DCR hostname of the device.

### Resolve By SysName Algorithm

This option obtains the preferred management IP by looking at the sysName of the device. The algorithm performs the following steps:

1. The value of sysName (if it exists) is looked up using the system resolver.
2. If a valid IP Address is found for the current device, and if the IP is SNMP reachable then it is set as the preferred management IP.
3. If either step 1 or step 2 fails, then the preferred management IP will be set to the originally discovered IP.

Viewing Custom Discovery Settings Summary

The Discovery Settings wizard displays a summary of following settings you have configured:

- Module Settings
- Seed Device Settings
- SNMP Settings
- Filter Settings
- Global Settings

To view the summary of Device Discovery settings:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Go to <strong>Inventory &gt; Device Administration &gt; Discovery &gt; Settings</strong>. The Device Discovery Settings page appears.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Configure</strong> to enter into the Discovery Settings wizard.</td>
</tr>
<tr>
<td>3</td>
<td>Configure one or more of the following settings:</td>
</tr>
<tr>
<td></td>
<td>- Module Settings. See <strong>Configuring Discovery Module Settings</strong> for information.</td>
</tr>
<tr>
<td></td>
<td>- Seed Device Settings. See <strong>Configuring Seed Device Settings</strong> for information.</td>
</tr>
<tr>
<td></td>
<td>- SNMP Settings. See <strong>Configuring SNMP Settings</strong> for information.</td>
</tr>
<tr>
<td></td>
<td>- Filter Settings. See <strong>Configuring Discovery Filter Settings</strong> for information.</td>
</tr>
<tr>
<td></td>
<td>- Global Settings. See <strong>Configuring Global Discovery Settings</strong> for information.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Next</strong>. The Discovery Settings Summary page appears with the summary of Device Discovery settings. See <strong>Table 3-1</strong> for details of the fields.</td>
</tr>
<tr>
<td>5</td>
<td>Click any one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Back</strong> to navigate to the previous pages and change the Device Discovery settings.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Finish to apply the settings</strong> and exit the Discovery Settings wizard.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Cancel</strong> to exit the Discovery Settings wizard.</td>
</tr>
</tbody>
</table>
The Discovery Settings Summary page appears with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module Settings</td>
<td>Displays a Configure link that leads to Module Settings page. See</td>
</tr>
<tr>
<td></td>
<td>Configuring Discovery Module Settings for more information.</td>
</tr>
<tr>
<td>Seed Device Settings</td>
<td>Displays the status as Not Configured for the first time.</td>
</tr>
<tr>
<td></td>
<td>If you have configured Seed Device Settings earlier, this field displays</td>
</tr>
<tr>
<td></td>
<td>a link by name Configure.</td>
</tr>
<tr>
<td></td>
<td>Clicking <strong>Configure</strong> leads to Seed Devices Settings page.</td>
</tr>
<tr>
<td></td>
<td>See Configuring Seed Device Settings for more information.</td>
</tr>
<tr>
<td>SNMP Settings</td>
<td>Displays the status as Not Configured for the first time.</td>
</tr>
<tr>
<td></td>
<td>If you have configured Seed Device Settings earlier, this field displays</td>
</tr>
<tr>
<td></td>
<td>a link by name Configure.</td>
</tr>
<tr>
<td></td>
<td>Clicking <strong>Configure</strong> leads to SNMP Settings page.</td>
</tr>
<tr>
<td></td>
<td>See Configuring SNMP Settings for more information.</td>
</tr>
<tr>
<td>Filter Settings</td>
<td>Displays the status as Not Configured for the first time.</td>
</tr>
<tr>
<td></td>
<td>If you have configured Filter Settings earlier, this field displays a link</td>
</tr>
<tr>
<td></td>
<td>by name Configure.</td>
</tr>
<tr>
<td></td>
<td>Clicking <strong>Configure</strong> leads to Filter Settings page.</td>
</tr>
<tr>
<td></td>
<td>See Configuring Discovery Filter Settings for more information.</td>
</tr>
<tr>
<td>Global Settings</td>
<td>Displays the status as Not Configured for the first time.</td>
</tr>
<tr>
<td></td>
<td>If you have configured Global Settings earlier, this field displays a link</td>
</tr>
<tr>
<td></td>
<td>by name Configure.</td>
</tr>
<tr>
<td></td>
<td>Clicking <strong>Configure</strong> leads to Global Settings page.</td>
</tr>
<tr>
<td></td>
<td>See Configuring Global Discovery Settings for more information.</td>
</tr>
<tr>
<td>Modules Selected</td>
<td>Displays the Device Discovery modules which you have selected in the</td>
</tr>
<tr>
<td></td>
<td>Module Settings page, separated by commas.</td>
</tr>
<tr>
<td>Use DCR as Seed List</td>
<td>Displays:</td>
</tr>
<tr>
<td></td>
<td>• Yes if you have selected this option to specify seed devices.</td>
</tr>
<tr>
<td></td>
<td>• No if you have not selected this option.</td>
</tr>
<tr>
<td>Preferred Management IP</td>
<td>Displays the preferred management IP Address name you have selected in the</td>
</tr>
<tr>
<td></td>
<td>Global Settings page.</td>
</tr>
<tr>
<td>Preferred DCR Device Name</td>
<td>Displays the preferred DCR device name you have selected in the</td>
</tr>
<tr>
<td></td>
<td>Global Settings page based on the fallback order.</td>
</tr>
<tr>
<td>Update DCR Device Name</td>
<td>Displays:</td>
</tr>
<tr>
<td></td>
<td>• Yes if you have selected this option to update the device name in DCR</td>
</tr>
<tr>
<td></td>
<td>after the next Device Discovery cycle.</td>
</tr>
<tr>
<td></td>
<td>• No if you have not selected this option.</td>
</tr>
</tbody>
</table>
Before you start Custom Discovery, ensure that you have configured all the required settings.

To start Custom Discovery:

Go to **Inventory > Device Administration > Discovery > Launch / Summary**. The Discovery Summary page appears.

Or

Go to **Inventory > Device Administration > Discovery > Custom Discovery Settings**. The Device Discovery Settings page appears.

**Step 6**

Click **Start Discovery**.

Custom Discovery starts as an immediate job.

You can also view the status of Custom Discovery from LMS Job Browser page. To go to Job Browser page, click **Admin > Jobs > Browser** from the LMS homepage.

After Custom Discovery starts running, the Start Discovery button changes to **Stop Discovery**.
You can stop Device Discovery by clicking **Stop Discovery**. E-mail notification is sent to the e-mail address configured on stopping the Device Discovery job. You can also stop Device Discovery jobs from Job Browser page.

Stopping Device Discovery may take a while to terminate all the threads and Discovery process. Hence the Stop Discovery button also takes a while to change to Start Discovery.

**Excluding EOBC interface from Device Discovery**

For Devices which have an EOBC interface/module, it will be automatically associated with one or more loopback IP addresses. If there are multiple such devices in the network, the IPs of the EOBC interface can overlap, causing discovery to discard all but one of the devices as duplicate entries of the same device. This interface needs to be excluded from the discovery process.

Do the following for excluding EOBC interface from device discovery:

1. Include the IP addresses of the EOBC interface one below the other in the ignore_device.txt file.
2. Copy the file in `<NMSROOT>/MDC/tomcat/webapps/cwhp/WEB-INF/lib`, where discovery.jar is located.

The EOBC interface IP addresses included in the ignore_device.txt file will be ignored from device discovery.

---

**Viewing Discovery Details**

You can view the details of recently completed Device Discovery and the status of currently running Device Discovery job in LMS.

This section contains the following:

- Viewing Discovery Summary
- Total Devices Discovered
- Reachable Devices
- Unreachable Devices
- Devices Newly Added to DCR
- Devices Updated to DCR

---

**Viewing Discovery Summary**

To view a summary of recently completed Device Discovery, go to the Cisco Prime home page and select **Inventory > Device Administration > Discovery > Launch / Summary**.

The Device Discovery Summary page appears with the following fields:
### Chapter 3  
**Discovering Devices**

#### Viewing Discovery Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Status</td>
<td>Displays the current status of the Device Discovery job. The status of the Device Discovery job could be any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Recent Discovery Information Not Found—This status is displayed:</td>
</tr>
<tr>
<td></td>
<td>- After a fresh installation of LMS.</td>
</tr>
<tr>
<td></td>
<td>- If no immediate or scheduled backup Device Discovery jobs are available.</td>
</tr>
<tr>
<td></td>
<td>- If the recent Device Discovery job fails.</td>
</tr>
<tr>
<td></td>
<td>• Initializing—This status is displayed immediately after you start Device Discovery.</td>
</tr>
<tr>
<td></td>
<td>At the start of Device Discovery, a URN is published to get the latest status of Device Discovery.</td>
</tr>
<tr>
<td></td>
<td>If there are any errors in publishing the URN or in receiving the latest Device Discovery summary, Device Discovery status may not be updated.</td>
</tr>
<tr>
<td></td>
<td>• Running—This status is displayed when the Device Discovery is running.</td>
</tr>
<tr>
<td></td>
<td>• Stopping—This status is displayed after the completion of Device Discovery and before the CSDiscovery process is stopped.</td>
</tr>
<tr>
<td></td>
<td>• Completed—This status is displayed when:</td>
</tr>
<tr>
<td></td>
<td>- The last Device Discovery job is completed successfully.</td>
</tr>
<tr>
<td></td>
<td>- The Device Discovery is stopped.</td>
</tr>
<tr>
<td>Discovery Type</td>
<td>Displays the currently running discovery type e.g. Custom or Standard.</td>
</tr>
<tr>
<td>Discovery Start Time</td>
<td>Displays the starting date and time of Device Discovery.</td>
</tr>
<tr>
<td></td>
<td>The date is displayed in Long Date format.</td>
</tr>
<tr>
<td></td>
<td>For example, the start time is displayed as Thu Aug 09 04:35:34 IST 2007.</td>
</tr>
<tr>
<td>Discovery End Time</td>
<td>Displays the completion date and time of Device Discovery.</td>
</tr>
<tr>
<td></td>
<td>The Device Discovery time may differ across the network depending on the size and the changes in the network.</td>
</tr>
<tr>
<td>Total Devices Discovered</td>
<td>Displays the total number of devices discovered by the recent Device Discovery job.</td>
</tr>
<tr>
<td></td>
<td>When you click the number displayed, the Total Devices Discovered window opens. See Total Devices Discovered for more information.</td>
</tr>
<tr>
<td>Reachable Devices</td>
<td>Displays the number of devices which are SNMP reachable.</td>
</tr>
<tr>
<td></td>
<td>When you click the number displayed, the All Reachable Devices window opens. See Reachable Devices for more information.</td>
</tr>
</tbody>
</table>
Viewing Discovery Details

Chapter 3      Discovering Devices

You can use the refresh icon provided in the Device Discovery Summary page to view the latest Device Discovery status.

Click the **Start Discovery** button to create a new JobID other than the scheduled jobID and create the new config.xml and system-config.xml for the new job and update the existing schedule job settings.

Once discovery gets started, control navigates to discovery summary page to check whether the devices got discovered.
**Total Devices Discovered**

You can view the details of all devices that are discovered by LMS Device Discovery. See *Activities Performed From Device Discovery Details Windows* for other activities you can perform from the Total Devices Discovered details window.

To see the details of all the discovered devices:

**Step 1** Go to **Inventory > Device Administration > Discovery > Launch / Summary**. The Device Discovery Summary page appears.

**Step 2** Click the number displayed in the Total Devices Discovered field. The Total Devices Discovered popup window opens with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Preferred management IP Address of the device. The IP Address can be any of</td>
</tr>
<tr>
<td></td>
<td>the following depending upon your Global Device Discovery settings:</td>
</tr>
<tr>
<td></td>
<td>• Loopback address</td>
</tr>
<tr>
<td></td>
<td>• Address resolved from DNS lookup</td>
</tr>
<tr>
<td></td>
<td>• Address resolved from Sysname</td>
</tr>
<tr>
<td>System Name</td>
<td>System name of the device.</td>
</tr>
<tr>
<td>SysObjectID</td>
<td>sysObjectID value.</td>
</tr>
<tr>
<td>Found By Modules</td>
<td>Displays the name of the Device Discovery modules that discover this</td>
</tr>
<tr>
<td></td>
<td>device during a Device Discovery cycle. For example, if a device is</td>
</tr>
<tr>
<td></td>
<td>discovered by CDP and ARP modules, this field displays CDP, ARP.</td>
</tr>
<tr>
<td></td>
<td>This field displays the value as System if the device is discovered</td>
</tr>
<tr>
<td></td>
<td>by the System Device Discovery module.</td>
</tr>
<tr>
<td>Neighbors</td>
<td>Displays the IP Addresses of the neighboring devices separated by commas.</td>
</tr>
<tr>
<td></td>
<td>The neighbors are displayed only when devices are discovered by Cisco</td>
</tr>
<tr>
<td></td>
<td>Discovery Protocol module. Otherwise, this field is blank.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the device as either Reachable or Unreachable.</td>
</tr>
</tbody>
</table>

**Reachable Devices**

You can view the details of all reachable devices that are discovered by LMS Device Discovery. See *Activities Performed From Device Discovery Details Windows* for other activities you can perform from the Reachable Devices details window.
To see the details of the reachable devices:

**Step 1** Go to **Inventory > Device Administration > Discovery > Launch / Summary**. The Device Discovery Summary page appears.

**Step 2** Click the number displayed in the Reachable Devices field.

The Reachable Devices popup window opens with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Management IP Address of the device returned from Device Discovery.</td>
</tr>
<tr>
<td>System Name</td>
<td>System name of the device.</td>
</tr>
<tr>
<td>SysObjectID</td>
<td>sysObjectID value.</td>
</tr>
<tr>
<td>Found By Modules</td>
<td>Displays the name of the Device Discovery modules that discover this device during a Device Discovery cycle. For example, if a device is discovered by CDP and ARP modules, this field displays CDP, ARP. This field displays the value as System if the device is discovered by the System Device Discovery module.</td>
</tr>
<tr>
<td>Neighbors</td>
<td>Displays the IP Addresses of the neighboring devices separated by commas.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the device as Reachable.</td>
</tr>
</tbody>
</table>

**Unreachable Devices**

You can view the details of all devices that are not reachable by LMS Device Discovery.

See **Activities Performed From Device Discovery Details Windows** for other activities you can perform from the Unreachable Devices details window.

To see the details of the unreachable devices:

**Step 1** Go to **Inventory > Device Administration > Discovery > Launch / Summary**. The Device Discovery Summary page appears.

**Step 2** Click the number displayed in the Unreachable Devices field.

The Unreachable Devices popup window opens with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Management IP Address of the device.</td>
</tr>
<tr>
<td>System Name</td>
<td>System name of the device. This value is blank in the report for all unreachable devices.</td>
</tr>
<tr>
<td>SysObjectID</td>
<td>sysObjectID value. This value is blank in the report for all unreachable devices.</td>
</tr>
</tbody>
</table>
Chapter 3  Discovering Devices

Viewing Discovery Details

You can view the details of devices that are added to DCR by LMS Device Discovery. Devices Newly Added to DCR will be updated every 2 minutes while the discovery is running. See Activities Performed From Device Discovery Details Windows for other activities you can perform from the Devices Added to DCR details window.

To see the details of devices that are newly added to DCR:

**Step 1**
Go to **Inventory > Device Administration > Discovery > Launch / Summary**. The Device Discovery Summary page appears.

**Step 2**
Click the number displayed in the Devices newly Added to DCR field.

The Devices Added to DCR popup window displays the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found By Modules</td>
<td>Displays the name of the Device Discovery modules that are used to discover this device during a Device Discovery cycle. This field displays the value as System if the device is discovered by the System Device Discovery module.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the device as Unreachable.</td>
</tr>
</tbody>
</table>

### Devices Newly Added to DCR

You can view the details of devices that are added to DCR by LMS Device Discovery. Device Newly Added to DCR will be updated every 2 minutes while the discovery is running. See Activities Performed From Device Discovery Details Windows for other activities you can perform from the Devices Added to DCR details window.

To see the details of devices that are newly added to DCR:

**Step 1**
Go to **Inventory > Device Administration > Discovery > Launch / Summary**. The Device Discovery Summary page appears.

**Step 2**
Click the number displayed in the Devices newly Added to DCR field.

The Devices Added to DCR popup window displays the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Management IP Address of the device returned from Device Discovery.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name of the device. The device name can be any of the following depending upon your Global Device Discovery settings:</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• Hostname</td>
</tr>
<tr>
<td></td>
<td>• Fully Qualified Domain Name</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname of the device. DCR does a DNS lookup to update the hostname of devices.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Domain name to which the device belongs.</td>
</tr>
<tr>
<td>SysObjectID</td>
<td>sysObjectID value.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Category, Series, and Model information of devices in DCR.</td>
</tr>
<tr>
<td></td>
<td>For example, Device Type displays Cisco 3000 Router, Cisco Catalyst 8150 CSR Switch and so on.</td>
</tr>
</tbody>
</table>
Devices Updated to DCR

You can view the details of devices that are updated in DCR by LMS Device Discovery. Device Updated to DCR will be updated every 2 minutes while the discovery is running. See Activities Performed From Device Discovery Details Windows for other activities you can perform from the Devices Added to DCR details window.

To see the details of devices that are updated in DCR:

**Step 1**  
Go to **Inventory > Device Administration > Discovery > Launch / Summary**. The Device Discovery Summary page appears.

**Step 2**  
Click the number displayed in the Devices Updated to DCR field.

The Devices Updated to DCR popup window opens with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP Address| Management IP Address of the device. The IP Address can be any of the following depending upon your Global Device Discovery settings:  
  • Loopback address  
  • Address resolved from DNS lookup  
  • Address resolved from Sysname |
| Device Name| Device name of the device. The device name can be any of the following depending upon your Global Device Discovery settings:  
  • IP Address  
  • Hostname  
  • Hostname + Domain Name |
| Hostname  | Hostname of the device.                                                     |
| Domain Name| Domain name to which the device belongs.                                   |
| SysObjectID| sysObjectID value.                                                          |
| Device Type| Category, Series, and Model information of devices in DCR. For example, Device Type displays Cisco 3000 Router, Cisco Catalyst 8150 CSR Switch and so on. |

Activities Performed From Device Discovery Details Windows

You can perform the following activities from the Device Discovery details window:

- Sort the records in ascending order or descending order of any fields.
- Use the navigation buttons provided to navigate between the pages, if the Device Discovery details window has more records.
- View the Device Discovery details in a printer-friendly format.
Using DCR Features in a Master-Slave Setup

DCR works based on a Master-Slave model. The Master Server maintains the master list of device credentials and the Slaves are the instances of the DCR on other servers.

You can configure the Master and Slave servers in a DCR management domain running similar or different versions of LMS.

Tip
We recommend you to:
- Run the same version of the LMS software in all servers in a management domain.
- Configure the DCR Master server and the Slave server with LMS 4.2.
- First, upgrade the DCR Master server to LMS 4.2, and then upgrade the DCR Slave Server to LMS 4.2.

Master-Slave configuration details are as follows:

Master-Slave Configuration Prerequisites
Before you set up the Master and Slave, you have to perform certain tasks to ensure that secure communication takes place between the Master and Slave.

Tip
We recommend you to configure the Master and all its Slaves in the management domain with the same version of LMS software. See Using DCR Features in a Master-Slave Setup for more details.

If machine M is to be the Master and S is to be the Slave:

Step 1 Add a Peer Server User and password in M
For more details, refer Setting up Peer Server Account in Administration of Cisco Prime LAN Management Solution 4.2.

Step 2 Add a System Identity user and password in S. This should be same as the Peer Server User set up in M.
For more details, refer Setting up System Identity Account in Administration of Cisco Prime LAN Management Solution 4.2.

**Step 3** Copy the Self-Signed Certificate of S to M. Also, copy the Self-Signed Certificate of M to S.
For more details, refer Creating Self Signed Certificates and Setting up Peer Server Certificate in Administration of Cisco Prime LAN Management Solution 4.2.

**Step 4** Configure S as Slave and M as Master.

---

**Standard Discovery**

To configure Standard Discovery Settings, complete the following steps:

**Step 1** Go to **Inventory > Device Administration > Discovery > Standard Discovery Settings.**

The Standard Discovery Settings page appears.

**Step 2** Under Seed Device Settings, check the **Use LMS Server Default Gateway As Seed** check box if you want to set the LMS Server Default Gateway as the seed device.

By default, the **Use LMS Server Default Gateway as Seed** check box is checked.

OR

Under Seed Device Settings, check **Use DCR as Seed** check box if you want the devices in DCR to be used as Seed device.

**Step 3** Under Seed Device Settings, check the **Seed Device** check box and enter the list of seed devices.

**Step 4** Under SNMP settings, click on **Edit Policy Configuration.**

The Default Credential Sets Policy Configuration page appears.

**Note** To Add a Default Credential Set Policy, you must create a Default Credential Set. For more information on creating and editing a Default Credential Set Policy, go to **Admin > Network > Device Credential Settings > Default Credential Sets Policy Configuration.**

**Step 5** Under SNMP settings, click on **Edit Default Credentials.**

The Default Credential Sets page appears.

**Note** To Edit a Default Credential Set, you must create a Default Credential Set. For more information on creating and editing a Default Credential Set, go to **Admin > Network > Device Credential Settings > Default Credential Sets.**

**Step 6** Under SNMP settings, click the **Use Policy Configuration Settings** radio button to use the predefined policy configuration settings.

The fallback options **SNMPv2c to SNMPv1 Fallback** and **SNMPv3 to SNMPv2 Fallback** are listed, of which the **SNMPv2c to SNMPv1 Fallback** is checked by default.
Chapter 3      Discovering Devices

Standard Discovery

Note The Use Policy Configuration Settings radio button will be enabled only after adding a Default Credential Set Policy.

Step 7 Under SNMP settings, click the Use Custom Policy Configuration Settings radio button to use the custom policy configuration settings.

The SNMPv2c and SNMPv3 tabs appear. The fallback and the configuration table corresponding to the selected tab will be displayed.

Step 8 Select SNMPv3 to configure SNMPv3.

Step 9 Click Add.

The SNMPv3 settings dialog box appears.

Step 10 Click the Credentials Set radio button to use the predefined credential settings.

Step 11 Click the Specify Credentials radio button and enter the required credential settings.

Step 12 Click OK.

The set SNMPV3 configuration details are displayed in the SNMPV3 Configuration table.

Note For configuring SNMPv2 settings select SNMPv2 in Step 8 and repeat Step 9 - Step 12

Step 13 Select a Default Credential Set Name or select Policy Configuration from the Default Credential Set drop-down list if you want to add the discovered devices with the selected default credentials in DCR.

Note For more information on creating Default Credential Sets and Policies, refer Configuring Default Credential Sets and Configuring Default Credential Set Policy in Administration Online Help.

The following points should be taken care during Standard Discovery:

- While creating a default credential set, if SNMP credentials are not given and if policy settings have been configured using this credential set, the Use Policy Configuration option will be enabled and with that option if the discovery is triggered, no devices will be discovered as there are no SNMP credentials.

- If any of the policy is configured with No Default as Credential Set and the Use Policy Configuration has been selected, the discovery can be triggered but no devices will be discovered.

Runtime Behaviors

Once Standard discovery starts, it will proceed with the protocols, namely CDP, LLDP, Routing Protocol and ARP.

The above protocols will fall back in order as follows:

- CDP/LLDP Protocol
- Routing Table Protocol
- ARP

Fallback has been taken as follows; the first protocol in the fallback order will be applied to the seed device to discover devices. During the discovery process, if the first protocol fails or discovers only the already discovered devices, the next in the fallback order will be applied.
Using Device Discovery Features in Various Setup

This section explains you the following:

- Using Device Discovery in Master-Slave Setup
- Running Device Discovery within NAT Setup

Using Device Discovery in Master-Slave Setup

To use Device Discovery features in Master-Slave setup, ensure that you have LMS 4.2 in Master and Slave servers.

You can schedule Device Discovery jobs, run Device Discovery, stop Device Discovery from both Master and Slave servers.

Running Device Discovery within NAT Setup

Running LMS Device Discovery is supported on a LMS Server that is set up within a Network Address Translation (NAT) boundary.

Device Discovery initiated from LMS Server within a NAT environment can discover the devices from the network that are outside the NAT boundary.
Managing Devices and Credentials

Using LMS, you can add devices to DCR (Device Credential and Repository) and manage their credentials.

In LMS 4.2, Unified Device Manager (UDM) provides centralized device management using a centralized policy configuration. You have to configure a single policy to manage the devices. UDM identifies the managed devices after verifying the configured policy and the license count.

This section includes:

- Managing Devices in DCR
- Understanding Unified Device Manager
- Understanding Device States
- Working With Alias Devices
- DCR Server Error
- Managing Auto Update Servers
- Configuring Device Selector

Managing Devices in DCR

To manage the devices in DCR (Device Credential and Repository) and their credentials select Inventory > Device Administration > Add / Import / Manage Devices.

Device Management performs the following functions:

- Adding Devices
- Deleting Devices
- Editing Device Credentials
- Editing Device Identity
- Importing Devices and Credentials
- Exporting Devices and Credentials
- Excluding Devices
- Viewing Devices List
- Understanding Device States
- Managing Device States
Managing Devices in DCR

Chapter 4  Managing Devices and Credentials

- Configuring Device Management Policy
- Adding Managed Devices
- Verifying Device Credentials
- Verifying Device Credentials

You can use:

- Device Selector to search and select the devices to perform device management tasks. See Configuring Device Selector for more information.
- Refresh button to refresh and view the updated device information in local mode.

**Note**
The Device Management UI is not visible in a DCR Slave machine.

**Note**
For more details on Device Management, refer Device Management Functions in Administration of CiscoWorks LAN Management Solution.

Adding Devices

You can use the Adding Devices to add devices, device properties or attributes, and device credentials to the Device and Credential Admin.

You should have the required privileges to add devices to DCR which is determined by the login.

To add devices to the device list:

**Step 1**
Go to the CiscoWorks home page and select Inventory > Device Administration > Add / Import / Manage Devices.

The Device Management page appears.

The Device Management user interface helps you to perform operations on Standard devices, Cluster Managed devices and Auto Update devices. Operations on Auto Update Servers can be performed only at the Auto Update Server Management user interface.

The Device Summary window displays the devices and groups in DCR Administration.

**Step 2**
Click Add.

The Device Properties page appears. The Device Information dialog box provides four device types:

- Standard Type
- Auto Update Type
- Cluster Managed Type
- CNS Managed Type

You can add more than one device at a time. However, you cannot add devices of different management types.
Managing Devices and Credentials

Chapter 4

Managing Devices in DCR

Note

If an IPv6 device is added, a pop-up message which says “For IPv6 devices, only limited support will be provided. Do you want to continue?” is displayed.

Standard Type

To add devices and credentials using Standard type:

Step 1

Select **Standard** from the Select A Management Type drop-down list box.

Step 2

Enter the Device IP Address, the host name, domain name, the device name, and the device type in the corresponding fields.

**Note**

The valid Device Name characters are A-Z, a-z, 0-9, _, -, :, . and the valid Host Name characters are A-Z, a-z, 0-9, ., -, _.

Click **Select** and choose the Domain Name and the Device Type from the list.

DCR uses a device record to represent a Cluster. A Cluster can be added in the Standard Management option by selecting the Device Type field as Cisco Cluster Management Suite.

DSBU Clusters added this way, can then be selected in Cluster Managed Type, for the field Cluster.

You can add a Cisco CNS Configuration Engine under the Standard Management type by selecting the Device Type field as Cisco CNS Configuration Engine. The Cisco CNS Configuration Engine added under the Standard type can be selected in the CNS Server field in the CNS Managed type.

After a Cisco CNS Configuration Engine or DSBU Cluster is successfully added, it will appear under Network Management > Other Network Management Products > Cisco CNS Configuration Engine/Cisco Cluster Management Suite, in the Device Selector.

Step 3

Click **Add to List**.

The device is added to the Added Device List in the window.

To remove the device from the Device List, select the device and click **Remove from List**.

Step 4

Select either **Policy configuration** or a default credential set in the Select a Default Credential Set drop-down list box, if you want to use the default credentials to access the devices.

You can select a default credential set only when you have configured at least one default credential set.

See Configuring Default Credentials in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.

If you have opted to use the default credentials, the primary credentials, secondary credentials, Rx Boot Mode credentials, SNMP credentials, and HTTP credentials will be populated with the corresponding default values. You can click **Finish** to add the devices with default credentials or proceed further to make changes to the value of the credentials.

If you do not want to use the default credentials, select **No Default** in the Select a Default Credential Set drop-down list box.

Step 5

Click **Next**.

The Standard Credentials page appears.

Step 6

Enter the following credentials in the Standard Credentials page.
• Primary Credentials (Username, Password, Enable Password)
• Secondary Credentials (Username, Password, Enable Password)
• Rx Boot Mode Credentials (Username, Password)

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

Re-enter the value of the password in Verify field.

If you do not want to proceed, click **Finish**.

**Step 7** Click **Next**.

The SNMP Credentials page appears.

**Step 8** Enter the following credentials in the SNMP Credentials page:

- **SNMPv2c/SNMPv1 Credentials** (Read-Only Community String, Read-Write Community String)
- **SNMPv3 Credentials** (Mode, Username, Authentication Password, Authentication Algorithm, Privacy Password, Privacy Algorithm, Engine ID)

You must select the SNMPv3 check box to enter the SNMPv3 Credentials. By default, these fields are disabled. When the SNMPv3 check box is selected, the default SNMPv3 mode is AuthPriv.

Re-enter the value of Authentication Password and Privacy Password in the Verify fields.

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

If you do not want to proceed, click **Finish**.

**Step 9** Click **Next**.

The HTTP Settings page appears.

**Step 10** Enter the following credentials in the HTTP Settings dialog box.

- **Primary HTTP Credentials** (Username, Password)
  
  Re-enter the value of the password in Verify field.

- **Secondary HTTP Credentials** (Username, Password)
  
  Re-enter the value of the password in Verify field.

- **Other Attributes** (HTTP Port, HTTPS Port, Certificate Common Name, Current Mode)

  Select the HTTP or HTTPS option for current connection mode.

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

If you do not want to proceed, click **Finish**.

**Step 11** Click **Next**.

The User Defined Fields dialog box appears.

**Step 12** Enter your choices for User Defined Fields.

By default, Device and Credential Admin provides the option to define four attribute fields for a device. These fields are used to store additional user-defined data for the device.

The attribute fields that appear here can be changed in the User Defined Fields page. Go to **Admin > Network > Device Credential Settings > User Defined Fields** to open the User Defined Fields page.

**Step 13** Click **Finish**

A message appears that the devices are added successfully in DCR.
When all the devices are not added in DCR, the Device Status Summary appears. See Device Addition Status Report for more information.

**Step 14**  
Click OK.

The Device Summary page appears with the updated device group information.

---

**Auto Update Type**

You can use this feature to add, edit, and delete devices managed using Auto Update Server.

The Auto Update Server managed device has its own attributes and credentials just like normal devices in DCR. In addition, it will have the following attributes:

- Device Identity: The string value that uniquely identifies the device in parent Auto Update Server.
- The DCR Device ID of the parent Auto Update Server record.

To add devices and credentials using Auto Update type:

**Step 1**  
Select the **Auto Update** from the Select A Management Type drop-down list box.

**Step 2**  
Enter the Device Type, Device Name, Auto Update Device ID, Host Name, Domain Name, and IP Address in the corresponding fields.

**Note**  
The valid Device Name characters are A-Z, a-z, 0-9, _, - , : , . and the valid Host Name characters are A-Z, a-z, 0-9, ., -, _.

To select Auto Update Server, Domain Name, and the Device Type click **Select** and select from the resulting popup windows. For Auto Update Server managed devices, Device Name and Device-Identity are enough for identity.

DCR uses a device record to represent an Auto Update Server. You can also add an Auto Update Server in the Auto Update Server Management page. Auto Update Server added in this way can then be selected for the Auto Update Server field in the Device Properties wizard.

**Step 3**  
Click **Add to List**.

The device gets added to the Added Device List in the window.

To remove the device from the Device List, select the device and click **Remove from List**.

**Step 4**  
Select either **Policy configuration** or a default credential set in the drop-down list box, if you want to use the default credentials to access the devices.

You can select a default credential set only when you have configured at least one default credential set. See Configuring Default Credentials in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.

If you have opted to use the default credentials, the primary credentials, secondary credentials, Rx Boot Mode credentials, SNMP credentials, and HTTP credentials will be populated with the corresponding default values.

If you do not want to use the default credentials, select **No Default** in the **Select a Default Credential Set** drop-down list box.

You can click **Finish** to add the devices with default credentials or proceed further to make changes to the value of the credentials.
Step 5  Click Next.

The Standard Credentials page appears.

Step 6  Enter the following credentials in the Standard Credentials page.
- Primary Credentials (Username, Password, Enable Password)
- Secondary Credentials (Username, Password, Enable Password)
- Rx Boot Mode Credentials (Username, Password)

Re-enter the value of the password in Verify field.

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

If you do not want to proceed, click Finish.

Step 7  Click Next.

The SNMP Credentials page appears.

Step 8  Enter the following credentials in the SNMP Credentials page:
- SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Mode, Username, Authentication Password, Authentication Algorithm, Privacy Password, Privacy Algorithm, Engine ID)

You must select the SNMPv3 check box to enter the SNMPv3 Credentials. By default, these fields are disabled. When the SNMPv3 check box is selected, the default SNMPv3 mode is AuthPriv.

Re-enter the value of Authentication Password and Privacy Password in the Verify fields.

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

If you do not want to proceed, click Finish.

Step 9  Click Next.

The HTTP Settings page appears.

Step 10  Enter the following credentials in the HTTP Settings dialog box.
- Primary HTTP Credentials (Username, Password)
  Re-enter the value of the password in Verify field.
- Secondary HTTP Credentials (Username, Password)
  Re-enter the value of the password in Verify field.
- Other Attributes (HTTP Port, HTTPS Port, Certificate Common Name, Current Mode)
  Select the HTTP or HTTPS option for current connection mode.

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

If you do not want to proceed, click Finish.

Step 11  Click Next.

The Auto Update Server Credential Template dialog box appears.

Step 12  Enter the Auto Update Server managed device credentials (Username, Password) in the corresponding fields.
Note
These are the credentials to login to the Auto Update Server — not to access the managed device.

Re-enter the value of the password in Verify field.

Step 13  Click Next.
The User Defined Fields dialog box appears.

Step 14  Enter your choices for UDFs.
By default, Device and Credential Admin provides the option to define four attribute fields for a device.
These fields are used to store additional user-defined data for the device.
The attribute fields that appear here can be changed in the User Defined Fields page. Go to Admin >
Network > Device Credential Settings > User Defined Fields to open the User Defined Fields page.

Step 15  Click Finish.
A message appears that the devices are added successfully in DCR.
When all the devices are not added in DCR, the Device Status Summary appears. See Device Addition
Status Report for more information.

Step 16  Click OK.
The Device Summary page appears with the updated device group information.

Cluster Managed Type
DCR supports Cisco Clusters and their member devices using a mix of standard and additional attributes
and credentials.
To add devices and credentials using Cluster Managed type:

Step 1  Select Cluster Managed from the Select A Management Type drop-down list box.
Step 2  Enter Device Type, Device Name, Device IP Address, Device Host Name, Domain Name, Cluster, and
Member Number in the corresponding fields. For member devices, member number and device name are
enough for identity.

Note
The valid Device Name characters are A-Z, a-z, 0-9, _, -, :, . and the valid Host Name characters are
A-Z, a-z, 0-9, ., -, _.

The Member Number field is mandatory. The Member Number is the number of the Cluster member.
This number represents the order in which the device is added into the cluster.
Also, Cluster needs to be added before a Cluster Managed device.
For example, if a device X belongs to cluster Y, first add the Cluster Y, and then add the Cluster Managed
device X.

Step 3  Click Add to List.
The device is added to the Added Device List in the window.
To remove a device from the Device List select the device and click Remove from List.
Managing Devices in DCR

Chapter 4      Managing Devices and Credentials

Step 4  Select either Policy configuration or a default credential set in the Select a Default Credential Set drop-down list box, if you want to use the default credentials to access the devices.

You can select a default credential set only when you have configured at least one default credential set. See Configuring Default Credentials in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.

If you have opted to use the default credentials, the primary credentials, secondary credentials, Rx Boot Mode credentials, SNMP credentials, and HTTP credentials will be populated with the corresponding default values.

If you do not want to use the default credentials, select No Default in the Select a Default Credential Set drop-down list box.

If you do not want to proceed further, click Finish.

Step 5  Click Next.

The User Defined Field dialog box appears.

Step 6  Enter your choices for User Defined Fields.

By default, Device and Credential Admin provides the option to define four attribute fields for a device. These fields are used to store additional user-defined data for the device.

The attribute fields that appear here can be changed in the User Defined Fields page. Go to Admin > Network > Device Credential Settings > User Defined Fields to open the User Defined Fields page.

Step 7  Click Finish.

A message appears that the devices are added successfully in DCR.

When all the devices are not added in DCR, the Device Status Summary appears. See Device Addition Status Report for more information.

Step 8  Click OK.

The Device Summary page appears with the updated device group information.

CNS Managed Type

To add devices and credentials using CNS Managed type:

Step 1  Select CNS Managed from the Select A Management Type drop-down list box.

Step 2  Enter the Device IP Address, the hostname, and the domain name.

The device name you want for the device in reports or graphical displays in the corresponding fields.

Step 3  You can also enter or select the domain name.

Note  The valid Device Name characters are A-Z, a-z, 0-9, _, -., ;, ;, and the valid Host Name characters are A-Z, a-z, 0-9, _, -.

Step 4  Click Select and choose CNS Server and the device type from the list.

You can add a Cisco CNS Configuration Engine in the Standard Management option by selecting the Device Type field as Cisco CNS Configuration Engine.
If you add a Cisco CNS Configuration Engine in this way, you can select these engines in the CNS Managed option, for the CNS Server field.

CNS Server and Device Name are mandatory.

**Step 5**
Click Add to List.
The device is added to the Added Device List in the page.
To remove a device from the Device List select the device and click Remove from List.

**Step 6**
Select either Policy configuration or a default credential set in the Select a Default Credential Set drop-down list box, if you want to use the default credentials to access the devices.
You can select a default credential set only when you have configured at least one default credential set. See Configuring Default Credentials in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.
If you have opted to use the default credentials, the primary credentials, secondary credentials, Rx Boot Mode credentials, SNMP credentials, and HTTP credentials will be populated with the corresponding default values. You can click Finish to add the devices with default credentials or proceed further to make changes to the value of the credentials.
If you do not want to use the default credentials, select No Default in the Select a Default Credential Set drop-down list box.

**Step 7**
Click Next.
The Standard Credentials page appears.

**Step 8**
Enter the following credentials in the Standard Credentials page.
- Primary Credentials (Username, Password, Enable Password)
- Secondary Credentials (Username, Password, Enable Password)
- Rx Boot Mode Credentials (Username, Password)
If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.
Re-enter the value of the password in Verify field.
If you do not want to proceed further, click Finish.

**Step 9**
Click Next.
The SNMP Credentials page appears.

**Step 10**
Enter the following credentials in the SNMP Credentials page:
- SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Mode, Username, Authentication Password, Authentication Algorithm, Privacy Password, Privacy Algorithm, Engine ID)
You must select the SNMPv3 check box to enter the SNMPv3 Credentials. By default, these fields are disabled. When the SNMPv3 check box is selected, the default SNMPv3 mode is AuthPriv.
Re-enter the value of Authentication Password and Privacy Password in the Verify fields.
If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.
If you do not want to proceed, click Finish.

**Step 11**
Click Next.
The HTTP Settings page appears.
Step 12 Enter the following credentials in the HTTP Settings dialog box.

- Primary HTTP Credentials (Username, Password)
  Re-enter the value of the password in Verify field.

- Secondary HTTP Credentials (Username, Password)
  Re-enter the value of the password in Verify field.

- Other Attributes (HTTP Port, HTTPS Port, Certificate Common Name, Current Mode)
  Select the HTTP or HTTPS option for current connection mode.

If you have opted to use the default credentials, these credentials will be populated with the default values from DCR. You can edit them and enter your own values.

If you do not want to proceed, click Finish.

Step 13 Click Next.

Step 14 Enter your choices for User Defined Fields.

By default, Device provides the option to define four attribute fields for a device. These fields are used to store additional user-defined data for the device.

The attribute fields that appear here can be changed in the User Defined Fields page. Go to Admin > Network > Device Credential Settings > User Defined Fields to open the User Defined Fields page.

Step 15 Click Finish.

A message appears that the devices are added successfully in DCR.

When all the devices are not added in DCR, the Device Status Summary appears. See Device Addition Status Report for more information.

Step 16 Click OK.

The Device Summary page appears with the updated device group information.

---

Device Addition Status Report

There may be few devices that are not added in DCR. The Device Addition Status report appears when all the devices you have added in the user interface are not added in DCR.

The Device Addition Status report contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of devices added</td>
<td>Displays the number of devices added in DCR.</td>
</tr>
</tbody>
</table>
Managing Devices in DCR

A link is provided for the number of devices displayed for all these fields.
The links for number of devices added, number of error devices, and number of duplicate devices displayed. The link launches the Add Device List Report with the device name and the status of device addition.

### Deleting Devices

You can delete device information from DCR using this feature.

You can select the devices from the Device Selector and delete either all of them or only the devices that are not managed by applications. When a device is deleted, it also gets deleted from all the applications that use DCR.

You should have the required privileges to delete devices from DCR. Your login determines whether you can use this option.

To delete devices:

**Step 1**
Go to the CiscoWorks home page and select **Inventory > Device Administration > Add / Import / Manage Devices**.

The Device Management page appears.

**Step 2**
Select one or more devices from the Device Selector and click **Delete**.

The Delete Devices Confirmation dialog box opens with the following details:

- Number of devices selected for deleting.
- Number of devices that are managed by applications in the current DCR domain.

**Step 3**
Select any one of the following options in the Delete Devices Confirmation dialog box:

- Delete only the device(s) not managed by Applications
Select this option when you want to delete the devices that are not managed by one or more applications. This option is enabled only when you have chosen to delete one or more devices from the device selector that are managed by applications.

- **Delete all the device(s) selected**

Select this option when you want to delete all the selected devices from DCR including the devices managed by applications. However, the device information still remains in the application databases.

**Step 4** Click **Continue**.

All information about the selected devices are deleted from DCR. There may be few devices that are deleted from DCR. See **Editing Device Credentials** for more information.

A message appears stating that the devices are deleted successfully.

The devices deleted are also removed from the device selector. If you have selected larger number of devices to delete, the system may take few minutes to refresh the group information in the device selector.

---

**Editing Device Credentials**

You can edit device information for a single device or for multiple devices using this feature. To edit device information:

**Step 1** Go to the CiscoWorks home page and select **Inventory > Device Administration > Add / Import / Manage Devices**.

The Device Management page appears.

**Step 2** Select one or more devices from the Device Selector and click **Edit Credentials**.

The Credentials Set Selection dialog box appears.

**Step 3** Select a default credential name or Policy Configuration from the **Select a Credential Set to Edit** drop-down list box.

If you do not want to use the default credentials, select **No Default** in the **Select a Default Credential Set** drop-down list box.

**Step 4** Select either one of the following options:

- **Overwrite All Device Credentials**—Overwrites the existing credentials of selected devices with the credentials of the default credential set.

- **Apply Only Missing Device Credentials**—Retains the existing credentials of selected devices. This option applies the credential values defined in the default credential set for only missing or empty credentials.

**Step 5** Click **Next**.

The Standard Credentials dialog box appears with the credential values that you have defined before. If you have selected the Select and Edit Credentials option and do not want to proceed, click **Finish**.

**Step 6** Edit the following credentials depending upon your requirement:

- **Primary Credentials (Username, Password, Enable Password)**
- **Secondary Credentials (Username, Password, Enable Password)**
- **Rx Boot Mode Credentials (Username, Password)**
Auto Update Server Managed Device Credentials (Username, Password)

If you edit the password values of any credentials, you should re-enter the password values in their corresponding Verify fields.

Any changes made here will apply to all devices selected in Step 2. This has one exception.

However, if in Step 2, you have selected devices belonging to different device types, the changes made will apply only to devices of the appropriate type. That is, if a standard-device credential is changed, only the standard devices selected in Step 2 are affected.

If you have completed editing, and do not want to proceed, click Finish.

---

**Step 7**

Click Next.

The SNMP Credentials page appears.

**Step 8**

Edit one or more of following credentials depending upon your requirement:

- SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
- SNMPv3 Credentials (Mode, Username, Authentication Password, Authentication Algorithm, Privacy Password, Privacy Algorithm, Engine ID)

You must select the SNMPv3 check box to enter or edit the SNMPv3 Credentials. By default, these fields are disabled. When the SNMPv3 check box is selected, the default SNMPv3 mode is AuthPriv.

Re-enter the value of Authentication Password and Privacy Password in the Verify fields.

If you have completed editing, and do not want to proceed, click Finish.

**Step 9**

Click Next if you want to edit HTTP Settings.

The HTTP Settings Page opens.

**Step 10**

Edit one or more credentials depending upon your requirement:

- Primary HTTP Credentials (Username, Password)
- Secondary HTTP Credentials (Username, Password)
- Other Attributes (HTTP Port, HTTPS Port, Certificate Common Name, Current Mode)

**Note**

Select the HTTP or HTTPS option for current connection mode.

Re-enter the values in the Verify fields.

If you have completed editing, and do not want to proceed, click Finish.

**Step 11**

Click Next if you want to edit User Defined Fields.

The User Defined Fields window appears. You can edit these fields and click Finish after you complete editing.

**Note**

You cannot edit Auto Update Servers here. Even if you select them in Step 2, they will not be affected. See Adding, Editing, and Deleting Auto Update Server for details on editing Auto Update Server information.

Management Type for a device is defined while you add the device to DCR. You cannot change the Management Type for the device through the edit flow. For example, you cannot change:

- Cisco Cluster Management Suite to any other Management Type and vice versa
• Cisco CNS Configuration Engine to any other Management Type and vice versa
Editing Device Identity

You can edit Device Identity information for a single device in DCR. The Device Name and the Host Name/Domain Name combination must be unique for each device in DCR. When you edit a device, it will be considered as a duplicate if any one of the following occur:

- The Device Name of a device is the same as the Device Name of any other device
- The Host Name/Domain Name combination of a device is the same as that of any other device
- Auto Update Device ID is the same as Auto Update Device ID of any other device (when the device is AUS managed)
- Cluster and Member Number are the same as that of any other device (when the device is Cluster managed)

To edit the Device Identity information:

Step 1  Go to the CiscoWorks home page and select Inventory > Device Administration > Add / Import / Manage Devices.

The Device Management page appears.

Step 2  Select one or more devices from the Device Selector to edit their identity information.

Step 3  Click Edit Identity.

The Device Properties dialog box appears with the list of selected devices, and attributes of the first device in the list.

Step 4  Select a device from the device list to edit its identity information.

The current attributes are automatically populated in the device information fields.

Step 5  Edit the device information, on the right pane.

You can edit the following information:
- Device Type
- Device Name
- Device Identity (Auto Update Device ID, Auto Update Server, CNS Server, Host Name, Domain Name and IP Address)
- Cluster Information (Cluster, Member Number)

You can edit only one device at a time.

Step 6  Select another device from the device list to edit the identity information.

Step 7  Click Apply after you have entered the settings for all the desired devices.
Importing Devices and Credentials

You can import device lists, device properties or attributes and device credentials to the DCR and populate DCR using this feature.

You can:
- Import Using Device and Credential Interface
  or
- Import Devices Using CLI

Import Using Device and Credential Interface

To import device information using Device and Credential Admin Interface:

---

**Step 1**
Go to the CiscoWorks home page and select **Inventory > Device Administration > Add / Import / Manage Devices**.

The Device Management page appears.

**Step 2**
Click **Bulk Import**.

The Import Devices popup window appears.

The options to import device information into DCR are:
- Import From a File. See Importing From a File for information.
- Import From Local NMS. See Importing From Local NMS for information.
- Import From Remote NMS. See Importing From Remote NMS for information.

---

If you import device information from a file, ensure that:
- Each device must have at least two mandatory attributes including the Device Name.
  
  The mandatory attributes are: Device Name, and Management IP Address or Host Name or Device Identity.
  
  For DSBU member devices, DSBU member number and device name are enough for identity.
  
  For AUS managed devices Device Name and Device-Identity are enough. For a CNS managed device, CNS Server is a mandatory attribute.
  
  If you do not know the sysObjectID of the device, specify it as UNKNOWN. If you specify the sysObjectID, the corresponding mdf_type will be automatically updated by DCR.
  
  Specify the correct dcr_device_type of the device. The possible values are:
  
  - 0—Standard Device
  - 1—DSBU Cluster
  - 3—AUS
  - 4—CNS Configuration Engine
• In case of proxy devices (devices that are managed by DSBU cluster or AUS or CNS), make sure that the manager (parent) and managed (child) devices are linked properly. For the proxy managed devices, specify the correct Parent ID attribute field. The following are the parent attributes:
  – parent_dsbu_id for DSBU cluster members
  – parent_aus_id for AUS managed devices
  – parent_cns_id for CNS managed devices
• If the import file type is xml, make sure that it conforms with the dtd available at NMSROOT/objects/dcrimpexp/conf/device.dtd.

Importing From a File

To import from a file:

**Step 1** Enter the file name.
Or
Browse the file system and select the file using the Browse tab.

**Step 2** Select CSV or XML file formats, as required.
Only CSV2.0 and CSV3.0 file formats are supported.

**Step 3** Select either Use data from Import source or Use data from DCR, to resolve conflicts during import.
  • If you select Use data from Import source, the credentials from the import source will be used, and credentials for the device in DCR will be modified.
  • If you select Use data from DCR, the device credentials in DCR will be used.

**Step 4** Schedule the task. To do this:
  a. Select the RunType from the drop-down list.
     You can schedule importing the devices immediately or schedule the import for a later time. The scheduling can be periodic (daily, weekly, or monthly) or for a single instance (once).
  b. Select the date from the date picker.
     The date picker displays the date from the client system.

**Step 5** Enter the Job information, if you have scheduled the task for a later time.
  a. Enter a brief description about the import task in the Job Description field.
  b. Enter a valid e-mail ID in the E-mail field to notify you about the status of import. You can enter multiple e-mail addresses separated by comma.

**Step 6** Select either Policy configuration or a default credential set in the Select a Default Credential Set drop-down list box, if you want to use the default credentials to access the devices.
If you do not want to use the default credentials, select No Default in the Select a Default Credential Set drop-down list box.
You can select a default credential set only when you have configured at least one default credential set. See Configuring Default Credentials in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.
  • If your import source does not have the required device credentials and if you have opted to use default credentials, the device information will be imported into DCR with the values of default credentials.
• If your import source has the required device credentials and if you have opted to use default credentials, the device information will be imported into DCR with the values specified in the import source.

For example, if the default credential set has Standard and SNMP credentials and if your import source has only the Standard credentials, the device will be populated in DCR with the Standard credentials entered in your import source and SNMP credentials configured in the default credential set.

See Configuring Default Credentials in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.

**Step 7** Click **Import**.

A message appears that the import job has been scheduled successfully, if you have scheduled an import job.

---

### Importing From Local NMS

To import from Local NMS:

**Step 1** Select the Network Management System type from the NMS type drop-down list.

HPOV and Netview are supported.

See Installation and Data Migration Guide for Cisco Prime LAN Manager 4.2 for information on supported Network Management Systems.

**Step 2** Enter the install location of the NMS type selected in the Install Location field or click the Browse button to select the install location.

The following table provides you the examples to enter the install location:

<table>
<thead>
<tr>
<th>NMS Type</th>
<th>Platform</th>
<th>Example to enter Install Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP OpenView Network Node Manager</td>
<td>Solaris and Soft Appliance</td>
<td>/opt/OV</td>
</tr>
<tr>
<td>HP OpenView Network Node Manager</td>
<td>Windows</td>
<td>C:\Program Files\HP OpenView</td>
</tr>
<tr>
<td>Netview</td>
<td>Solaris and Soft Appliance</td>
<td>/usr/OV</td>
</tr>
<tr>
<td>Netview</td>
<td>Windows</td>
<td>C:\usr\OV</td>
</tr>
</tbody>
</table>

**Step 3** Select either **Use data from Import source** or **Use data from DCR**, to resolve conflicts during import.

**Step 4** Schedule the task.

To do this:

a. Select the RunType from the drop-down list.

You can schedule importing the devices immediately or schedule the import for a later time. The scheduling can be periodic (daily, weekly, or monthly) or for a single instance (once).

b. Select the date from the date picker.

The date picker displays the date from the client system.

**Step 5** Enter the Job information, if you have scheduled the task for a later time.

a. Enter a brief description about the import task in the Job Description field.
b. Enter a valid e-mail ID in the E-mail field to notify you about the status of import. You can enter multiple e-mail addresses separated by comma.

**Step 6**
Select either **Policy configuration** or a default credential set in the Select a Default Credential Set drop-down list box, if you want to use the default credentials to access the devices.

If you do not want to use the default credentials, select **No Default**.

You can select a default credential set only when you have configured at least one default credential set. See *Configuring Default Credentials* in *Administration Guide for Cisco Prime LAN Management Solution 4.2* for more information.

- If your import source does not have the required device credentials and if you have opted to use default credentials, the device information will be imported into DCR with the values of default credentials.
- If your import source has the required device credentials and if you have opted to use default credentials, the device information will be imported into DCR with the values specified in the import source.

For example, if the default credential set has Standard and SNMP credentials and if your import source has only the Standard credentials, the device will be populated in DCR with the Standard credentials entered in your import source and SNMP credentials configured in the default credential set. See *Configuring Default Credentials* in *Administration Guide for Cisco Prime LAN Management Solution 4.2* for more information.

**Step 7**
Click **Import**.

A message appears that the import job has been scheduled successfully, if you have scheduled an import job.

---

**Importing From Remote NMS**

Before you import from the remote NMS, ensure that:

- The server running third-party NMS (HPOV, NetView) application is reachable from the Cisco Works Server.
- The remote server running 3rd party NMS accepts rsh connections and has a local user who has permission to run executables, such as `ovttopodump` within the 3rd party NMS. This user should have permissions to log into the NMS Server without a password. Also, the `.rohosts` file should be modified to enable login without password.

If you are importing from a remote NMS on host 2 to host 1 (LMS Server), you need to add the following entries in the `.rohosts` file of host2: `host1.domain.com SYSTEM` (on Windows); where `SYSTEM` is a built-in Local System account.

For example, if you are importing from a remote NMS on XYZ.cisco.com to ABC.cisco.com, you need to add `ABC.cisco.com SYSTEM host1.domain.com casuser` (on Solaris and Soft Appliance).
To import from a remote NMS:

**Step 1** Select the Network Management System type from the NMS type drop-down list. HPOV and Netview are supported. 

See *Installation and Data Migration Guide for Cisco Prime LAN Manager 4.2* for information on supported Network Management Systems.

If you select ACS, enter:
- ACS Server Name or IP Address in the Host Name field.
- ACS admin username in the User Name field.
- ACS admin user password in the Password field.
- Port number (default is 2002) in the Port field.
- HTTP or HTTPs protocol in the Protocol field.

**Step 2** Select the Operating System type from the OS type drop-down list.

**Note** Windows is not supported for HPOV and NetView

**Step 3** Enter the Host name, User name, and Install location in the corresponding fields. Make sure that you give the install location of the selected NMS type. For example, enter:
- `/opt/OV` — for HP Openview NNM (Network Node Manager)
- `/usr/OV` — for NetView

**Step 4** Select either **Use data from Import source** or **Use data from DCR**, to resolve conflicts during import.

**Step 5** Schedule the task. To do this:

a. Select the RunType from the drop-down list.
   
   You can schedule importing the devices immediately or schedule the import for a later time. The scheduling can be periodic (daily, weekly, or monthly) or for a single instance (once).

b. Select the date from the date picker.
   
   The date picker displays the date from the client system.

**Step 6** Enter the Job information, if you have scheduled the task for a later time.

a. Enter a brief description about the import task in the Job Description field.

b. Enter a valid e-mail ID in the E-mail field to notify you about the status of import. You can enter multiple e-mail addresses separated by comma.

**Step 7** Select either **Policy configuration** or a default credential set in the Select a Default Credential Set drop-down list box, if you want to use the default credentials to access the devices.

If you do not want to use the default credentials, select **No Default**.

You can select a default credential set only when you have configured at least one default credential set. See *Configuring Default Credentials* in *Administration Guide for Cisco Prime LAN Management Solution 4.2* for more information.

If your import source does not have the required device credentials and if you have opted to use default credentials, the device information will be imported into DCR with the values of default credentials.
If your import source has the required device credentials and if you have opted to use default credentials, the device information will be imported into DCR with the values specified in the import source.

For example, if the default credential set has Standard and SNMP credentials and if your import source has only the Standard credentials, the device will be populated in DCR with the Standard credentials entered in your import source and SNMP credentials configured in the default credential set.

See Configuring Default Credentials in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.

**Step 8** Click Import.

A message appears that the import job has been scheduled successfully, if you have scheduled an import job.

---

**Import Status Report**

The Import Status Report appears at the end of each immediate import operation. The report contains information on:

- **Newly Imported Devices**
  
  This field shows the number of devices that are newly imported during the bulk import operation.

- **Devices Not Imported**
  
  This field shows the devices that are not imported.

The devices that have not been imported might fall under one of the following categories:

<table>
<thead>
<tr>
<th>Devices</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excluded Devices</td>
<td>Devices that are excluded based on the Exclude device list uploaded by the user. These devices will not be imported into DCR.</td>
</tr>
</tbody>
</table>
| Duplicate Devices| Devices whose attribute are same as one of the devices in DCR. A device is considered duplicate if:  
  - The Device Name of a device is the same as that of any other device.  
  - The Host Name and Domain Name combination of a device is the same as that of another device. |
Sample CSV Files and XML Files

You can use CSV 2.0 or CSV 3.0 file or XML formats for import.

You can also perform a DCR Export operation to generate sample CSV or XML files. See Exporting Devices and Credentials for more information.

You should not delete any line from the CSV file generated by DCR export utility including the lines starting with ; (semi colon). However, you can add comments in the CSV file as new lines beginning with ; character.

If you use manually created CSV files for DCR import, we recommend that the CSV files should be in the same format of the files generated by DCR Export utility.

This section provides the following:

- **Sample CSV 2.0 File**
- **Sample CSV 3.0 File**
- **Sample CSV 3.0 File for Auto Update Server Managed Devices**
- **Sample CSV 3.0 File for Cluster Managed Devices**
- **Sample XML File (Standard)**
- **Sample XML File for Auto Update Server Managed Devices**
- **Sample XML File for Cluster Managed Devices**

View Mapping CSV 2.0 to CSV 3.0 Fields to see the details on mapping.
Sample CSV 2.0 File

; This file is generated by the export utility
; If you edit this file, be sure you know what you are doing
; Cisco Systems NM data import, source = export utility; Version = 2.0; Type = Csv
; Here are the columns of the table.
; Columns 1 and 2 are required.
; Columns 3 through 19 are optional.
; Col# = 1: Name (including domain or simply an IP)
; Col# = 2: RO community string
; Col# = 3: RW community string
; Col# = 4: Serial Number
; Col# = 5: User Field 1
; Col# = 6: User Field 2
; Col# = 7: User Field 3
; Col# = 8: User Field 4
; Col# = 9: Name = Telnet password
; Col# = 10: Name = Enable password
; Col# = 11: Name = Enable secret
; Col# = 12: Name = Tacacs user
; Col# = 13: Name = Tacacs password
; Col# = 14: Name = Tacacs enable user
; Col# = 15: Name = Tacacs enable password
; Col# = 16: Name = Local user
; Col# = 17: Name = Local password
; Col# = 18: Name = Rcp user
; Col# = 19: Name = Rcp password
; Here are the rows of data.

172.20.118.156,public,,FHH080600dg,,,,,,,,,,,,,,,
172.20.118.150,public,,FHH0743W022,,,,,,,,,,,,,,,

Sample CSV 3.0 File

; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCSV; Version=3.0

; Start of section 0 - Basic Credentials

; HEADER:management_ip_address,host_name,device_identity,display_name,sysObject
ID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,snmp_v3_user_id,
snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,snmp_v3_priv_password,snmp_v3_prv
iv_algorithm,rxboot_mode_username,rxboot_mode_password,primary_username,primary_password,pri
mon_name,secondary_username,secondary_password,secondary_enable_password,secondary_http_us
ername,secondary_http_password

10.77.203.55,,,10.77.203.55,UNKNOWN,0,UNKNOWN,,userap1,roZes1,,MD5,roZes11,AES128,,
10.77.203.142,,,10.77.203.142,UNKNOWN,0,UNKNOWN,,userap2,roZes2,,SHA-1,roZes22,3DES,,
10.77.209.74,,,10.77.209.74,UNKNOWN,0,UNKNOWN,,v3user,roZes123,,MD5,roZes123,DES,,
10.77.203.210,,,10.77.203.210,UNKNOWN,0,UNKNOWN,,v3user4,roZes123,,SHA-1,roZes123,AES256

; End of CSV file
For a complete list of attributes and their description, use the `lsattr` command in dcrcli. See Listing the Attributes for usage details.

Sample CSV 3.0 File for Auto Update Server Managed Devices

```
; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCSV; Version=3.0
; Start of section 0 - Basic Credentials
;
;HEADER:management_ip_address,host_name,domain_name,device_identity,display_name,sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,snmp_v3_priv_password,snmp_v3_priv_algorithm,rxboot_mode_username,rxboot_mode_password,primary_username,primary_password,primary_enable_password,http_username,http_password,http_mode,http_port,https_port,cert_common_name,secondary_username,secondary_password,secondary_enable_password,secondary_http_username,secondary_http_password

10.77.203.55,,10.77.203.55,UNKNOWN,0,UNKNOWN,,userap1,roZes1,,MD5,roZes11,AES128,,,,,,
10.77.203.142,,10.77.203.142,UNKNOWN,0,UNKNOWN,,userap2,roZes2,,SHA-1,roZes22,3DES,,,,
10.77.209.74,,10.77.209.74,UNKNOWN,0,UNKNOWN,,v3user,roZes123,,MD5,roZes123,DES,,,,
10.77.203.210,,10.77.203.210,UNKNOWN,0,UNKNOWN,,v3user4,ROzES123,,SHA-1,ROzES123,AES256,,,,,,,,

; Start of section 1 - AUS proxy
;
;HEADER:management_ip_address,host_name,domain_name,device_identity,display_name,aus_username,aus_password,aus_url

1.1.1.1,ons_host1,cisco.com,AUS_ID,ONS1,admin,admin,
10.10.10.1,aus_server,cisco.com,,AUS_SERV1,admin,admin,autoupdate/AutoUpdateServlet

; Start of section 2 - AUS managed
;
;HEADER:management_ip_address,host_name,domain_name,device_identity,display_name,parent_aus_id

1.1.1.1,ons_host1,cisco.com,AUS_ID,ONS1,display_name=AUS_SERV1
```

Sample CSV 3.0 File for Cluster Managed Devices

```
; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCSV; Version=3.0
; Start of section 0 - Basic Credentials
;
;HEADER:management_ip_address,host_name,domain_name,device_identity,display_name,sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,snmp_v3_priv_password,snmp_v3_priv_algorithm,rxboot_mode_username,rxboot_mode_password,primary_username,primary_password,primary_enable_password,http_username,http_password,http_mode,http_port,https_port,cert_common_name,secondary_username,secondary_password,secondary_enable_password,secondary_http_username,secondary_http_password

10.77.203.55,,10.77.203.55,UNKNOWN,0,UNKNOWN,,userap1,roZes1,,MD5,roZes11,AES128,,,,,,
10.77.203.142,,10.77.203.142,UNKNOWN,0,UNKNOWN,,userap2,roZes2,,SHA-1,roZes22,3DES,,,,
```

Sample CSV 3.0 File for Cluster Managed Devices

```
; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCSV; Version=3.0
; Start of section 0 - Basic Credentials
;
;HEADER:management_ip_address,host_name,domain_name,device_identity,display_name,sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,snmp_v3_priv_password,snmp_v3_priv_algorithm,rxboot_mode_username,rxboot_mode_password,primary_username,primary_password,primary_enable_password,http_username,http_password,http_mode,http_port,https_port,cert_common_name,secondary_username,secondary_password,secondary_enable_password,secondary_http_username,secondary_http_password

10.77.203.55,,10.77.203.55,UNKNOWN,0,UNKNOWN,,userap1,roZes1,,MD5,roZes11,AES128,,,,,,
10.77.203.142,,10.77.203.142,UNKNOWN,0,UNKNOWN,,userap2,roZes2,,SHA-1,roZes22,3DES,,,,
```

Mapping CSV 2.0 to CSV 3.0 Fields

The following table provides a mapping between the fields in CSV 2.0 and CSV 3.0:

<table>
<thead>
<tr>
<th>CSV 2.0</th>
<th>CSV 3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (including domain or only an IP Address)</td>
<td>host_name and display_name</td>
</tr>
<tr>
<td>RO community string</td>
<td>snmp_v2_ro_comm_string</td>
</tr>
<tr>
<td>RW community string</td>
<td>snmp_v2_rw_comm_string</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Not used in CSV 3.0</td>
</tr>
<tr>
<td>User Field 1</td>
<td>user_defined_field_0</td>
</tr>
<tr>
<td>User Field 2</td>
<td>user_defined_field_1</td>
</tr>
<tr>
<td>User Field 3</td>
<td>user_defined_field_2</td>
</tr>
<tr>
<td>User Field 4</td>
<td>user_defined_field_3</td>
</tr>
<tr>
<td>Telnet password</td>
<td>primary_password or secondary_password</td>
</tr>
<tr>
<td>Enable password</td>
<td>primary_enable_password or secondary_enable_password</td>
</tr>
<tr>
<td>Enable secret</td>
<td>primary_enable_password or secondary_enable_password</td>
</tr>
<tr>
<td>Tacacs user</td>
<td>primary_username</td>
</tr>
<tr>
<td>Tacacs password</td>
<td>primary_password</td>
</tr>
<tr>
<td>Tacacs enable user</td>
<td>Not used in CSV 3.0</td>
</tr>
<tr>
<td>Tacacs enable password</td>
<td>primary_enable_password</td>
</tr>
<tr>
<td>Local user</td>
<td>primary_username or secondary_username</td>
</tr>
<tr>
<td>Local password</td>
<td>primary_password or secondary_password</td>
</tr>
<tr>
<td>Rcp user</td>
<td>Not used in CSV 3.0</td>
</tr>
<tr>
<td>Rcp password</td>
<td>Not used in CSV 3.0</td>
</tr>
</tbody>
</table>

The order of preference used to set these values in CSV 3.0:

- If Tacacs username, password, enable password are set, then these values will be set as primary_username, primary_password and primary_enable_password.
- If Local username and password are set, then the values will be set as primary_username or secondary_username and primary_password or secondary_password.

The local username and password are matched to secondary_username and secondary_password if primary_username and primary_password is already set with Tacacs credentials.
If Telnet password, Enable password, and Enable secret are set, then the values will be set as primary_password or secondary_password, and primary_enable_password or secondary_enable_password (for both Enable password, and Enable secret).

The Telnet password, Enable password, and Enable Secret are set to secondary credentials, if the primary_password and primary_enable_password are already set with Tacacs or Local credentials.

Sample XML File (Standard)

```xml
<?xml version="1.0"?>
<DEVICES>
  <DEVICE>
    <SET Name="Basic Credentials">
      <DEVATTRIB Name="management_ip_address">10.77.203.55</DEVATTRIB>
      <DEVATTRIB Name="host_name">Switch6009</DEVATTRIB>
      <DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
      <DEVATTRIB Name="display_name">10.77.203.55</DEVATTRIB>
      <DEVATTRIB Name="sysObjectID">UNKNOWN</DEVATTRIB>
      <DEVATTRIB Name="dcr_device_type">0</DEVATTRIB>
      <DEVATTRIB Name="mdf_type">268438100</DEVATTRIB>
      <DEVATTRIB Name="snmp_v2_ro_comm_string">public</DEVATTRIB>
      <DEVATTRIB Name="snmp_v2_rw_comm_string">private</DEVATTRIB>
      <DEVATTRIB Name="primary_username">lab</DEVATTRIB>
      <DEVATTRIB Name="primary_password">lab</DEVATTRIB>
      <DEVATTRIB Name="primary_enable_password">lab</DEVATTRIB>
      <DEVATTRIB Name="secondary_username">lab</DEVATTRIB>
      <DEVATTRIB Name="secondary_password">lab</DEVATTRIB>
      <DEVATTRIB Name="secondary_enable_password">lab</DEVATTRIB>
      <DEVATTRIB Name="snmp_v3_user_id">userap1</DEVATTRIB>
      <DEVATTRIB Name="snmp_v3_password">roZes1</DEVATTRIB>
      <DEVATTRIB Name="snmp_v3_auth_algorithm">MD5</DEVATTRIB>
      <DEVATTRIB Name="snmp_v3_priv_password">roZes11</DEVATTRIB>
      <DEVATTRIB Name="snmp_v3_priv_algorithm">AES128</DEVATTRIB>
    </SET>
  </DEVICE>
</DEVICES>
```

**Note**

For a complete list of attributes and their description, use the `lsattr` command in dcrcli. See [Listing the Attributes](#) for usage details.

Sample XML File for Auto Update Server Managed Devices

```xml
<?xml version="1.0"?>
<DEVICES>
  <DEVICE>
    <SET Name="Basic Credentials">
      <DEVATTRIB Name="management_ip_address">10.77.203.55</DEVATTRIB>
      <DEVATTRIB Name="host_name">Switch6009</DEVATTRIB>
      <DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
      <DEVATTRIB Name="display_name">10.77.203.55</DEVATTRIB>
      <DEVATTRIB Name="sysObjectID">UNKNOWN</DEVATTRIB>
      <DEVATTRIB Name="dcr_device_type">0</DEVATTRIB>
      <DEVATTRIB Name="mdf_type">268438100</DEVATTRIB>
      <DEVATTRIB Name="snmp_v2_ro_comm_string">public</DEVATTRIB>
      <DEVATTRIB Name="snmp_v2_rw_comm_string">private</DEVATTRIB>
      <DEVATTRIB Name="primary_username">lab</DEVATTRIB>
      <DEVATTRIB Name="primary_password">lab</DEVATTRIB>
      <DEVATTRIB Name="primary_enable_password">lab</DEVATTRIB>
      <DEVATTRIB Name="secondary_username">lab</DEVATTRIB>
      <DEVATTRIB Name="secondary_password">lab</DEVATTRIB>
      <DEVATTRIB Name="secondary_enable_password">lab</DEVATTRIB>
    </SET>
  </DEVICE>
</DEVICES>
```
<DEVATTRIB Name="snmp_v3_user_id">userap1</DEVATTRIB>
<DEVATTRIB Name="snmp_v3_password">roZes1</DEVATTRIB>
<DEVATTRIB Name="snmp_v3_auth_algorithm">MD5</DEVATTRIB>
<DEVATTRIB Name="snmp_v3_priv_password">roZes11</DEVATTRIB>
<DEVATTRIB Name="snmp_v3_priv_algorithm">AES128</DEVATTRIB>
</SET>

<DEVICE>
<SET Name="AUS proxy">
<DEVATTRIB Name="aus_username">admin</DEVATTRIB>
<DEVATTRIB Name="aus_password">admin</DEVATTRIB>
</SET>

<SET Name="AUS managed">
<DEVATTRIB Name="device_identity">AUS_ID</DEVATTRIB>
<DEVATTRIB Name="parent_aus_id">display_name=AUS_SERV1</DEVATTRIB>
</SET>
</DEVICE>

<DEVICE>
<SET Name="Basic Credentials">
<DEVATTRIB Name="management_ip_address">10.10.10.1</DEVATTRIB>
<DEVATTRIB Name="host_name">aus_server</DEVATTRIB>
<DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
<DEVATTRIB Name="display_name">AUS_SERV1</DEVATTRIB>
<DEVATTRIB Name="sysObjectID">UNKNOWN</DEVATTRIB>
<DEVATTRIB Name="dcr_device_type">3</DEVATTRIB>
<DEVATTRIB Name="mdf_type">UNKNOWN</DEVATTRIB>
</SET>

<SET Name="AUS proxy">
<DEVATTRIB Name="aus_username">admin</DEVATTRIB>
<DEVATTRIB Name="aus_password">admin</DEVATTRIB>
<DEVATTRIB Name="aus_url">autoupdate/AutoUpdateServlet</DEVATTRIB>
</SET>
</DEVICE>

</DEVICES>

Sample XML File for Cluster Managed Devices
<?xml version="1.0"?>
<DEVICES>
<DEVICE>
<SET Name="Basic Credentials">
<DEVATTRIB Name="management_ip_address">1.1.1.1</DEVATTRIB>
<DEVATTRIB Name="host_name">ons_dev_1</DEVATTRIB>
<DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
<DEVATTRIB Name="display_name">ONS1</DEVATTRIB>
<DEVATTRIB Name="sysObjectID">1.3.6.1.4.1.9.1.406</DEVATTRIB>
<DEVATTRIB Name="dcr_device_type">0</DEVATTRIB>
<DEVATTRIB Name="mdf_type">273612892</DEVATTRIB>
</SET>

<SET Name="DSBU managed">
<DEVATTRIB Name="dsbu_member_number">1</DEVATTRIB>
<DEVATTRIB Name="parent_dsbu_id">display_name=cluster1</DEVATTRIB>
</SET>
</DEVICE>

<DEVICE>
<SET Name="Basic Credentials">
<DEVATTRIB Name="management_ip_address">10.10.10.1</DEVATTRIB>
<DEVATTRIB Name="host_name">host1</DEVATTRIB>
<DEVATTRIB Name="domain_name">cisco.com</DEVATTRIB>
<DEVATTRIB Name="display_name">cluster1</DEVATTRIB>
<DEVATTRIB Name="sysObjectID">Unknown</DEVATTRIB>
<DEVATTRIB Name="dcr_device_type">1</DEVATTRIB>
<DEVATTRIB Name="mdf_type">278283831</DEVATTRIB>
</SET>
</DEVICE>
Exporting Devices and Credentials

This feature helps you in exporting a list of device and their credentials into a file. The device list can be obtained from the Device Selector, or from a CSV file.

You can view the list of attributes that can be exported and edit the Export Format file to specify the credentials you need to export. See Listing the Attributes for viewing the list of attributes.

You can:

- Export Device Credentials Using UI
  or
- Export Devices Using CLI

The device information is exported to files in CSV (only CSV 3.0) and XML formats only. See Sample CSV Files and XML Files for sample CSV and XML files generated by the export utility.

Specifying Device Credentials for Export

The device attributes that are exported are specified in the Export Format files Export_Format_CSV.xml and Export_Format_XML.xml located at the NMSROOT\objects\dcrimpexp\conf directory.

By default, all the device attributes are exported. See Device Attributes for a list of device attributes.

You can:

- Edit the Export Format files to include UDF names in the export device attributes list.
- Enable or disable the option of exporting device credentials to the export format file. See Device Credentials for a list of device credentials that are exported if you enable this option.

Edit the Export format files only when you:

- Add the UDF information in the export device attributes list.
- Change or delete the UDF names when you rename or delete the UDFs respectively in the Device and Credentials Administration user interface.

See Configuring User Defined Fields in Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information on configuring UDFs.

Sample Export Format File with Device Attributes Only

```xml
<?xml version="1.0" ?>
<EXPORT_FORMAT>
  <GROUP Name="Basic Credentials">
    management_ip_address,host_name,domain_name,device_identity,display_name,sysoObjectID,dcr_device_type,mdf_type,http_mode,http_port,https_port,cert_common_name
  </GROUP>
  <GROUP Name="AUS proxy">
    management_ip_address,host_name,domain_name,device_identity,display_name,aus_username,aus_password,aus_url,aus_port
  </GROUP>
  <GROUP Name="AUS managed">
    management_ip_address,host_name,domain_name,device_identity,display_name,parent_aus_id
  </GROUP>
  <GROUP Name="DSBU managed">
    management_ip_address,host_name,domain_name,device_identity,display_name,dsbu_member_number,parent_dsbu_id
  </GROUP>
</EXPORT_FORMAT>
```
<GROUP Name="CNS managed">
management_ip_address,host_name,domain_name,device_identity,display_name,parent_cns_id,cns_config_id,cns_event_id,cns_image_id</GROUP>
</EXPORT_FORMAT>

Sample Export Format File with Device Attributes and Device Credentials

<?xml version="1.0" ?>
<EXPORT_FORMAT>
<GROUP Name="Basic Credentials">
management_ip_address,host_name,domain_name,device_identity,display_name,sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,snmp_v3_priv_password,snmp_v3_priv_algorithm,rxboot_mode_username,rxboot_mode_password,primary_username,primary_password,primary_enable_password,http_username,http_password,http_mode,http_port,https_port,cert_common_name,secondary_username,secondary_password,secondary_enable_password,secondary_http_username,secondary_http_password</GROUP>
<GROUP Name="AUS proxy">
management_ip_address,host_name,domain_name,device_identity,display_name,aus_username,aus_password,aus_url,aus_port</GROUP>
<GROUP Name="AUS managed">
management_ip_address,host_name,domain_name,device_identity,display_name,parent_aus_id</GROUP>
<GROUP Name="DSBU managed">
management_ip_address,host_name,domain_name,device_identity,display_name,dsbu_member_number,parent_dsbu_id</GROUP>
<GROUP Name="CNS managed">
management_ip_address,host_name,domain_name,device_identity,display_name,parent_cns_id,cns_config_id,cns_event_id,cns_image_id</GROUP>
</EXPORT_FORMAT>

Adding User Defined Field Names to Export Format Files

You should add the UDF names in the Export Format file to export the additional information about devices stored in their user-defined fields.

Suppose if you want to export the device information stored in the user_defined_field_0, user_defined_field_1, user_defined_field_2 and user_defined_field_3 fields, you should edit the Export Format file and change the Basic Credentials group as follows:

<GROUP Name="Basic Credentials">
management_ip_address,host_name,domain_name,device_identity,display_name,sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,snmp_v3_priv_password,snmp_v3_priv_algorithm,rxboot_mode_username,rxboot_mode_password,primary_username,primary_password,primary_enable_password,http_username,http_password,http_mode,http_port,https_port,cert_common_name,user_defined_field_0,user_defined_field_1,user_defined_field_2,udf3</GROUP>

If you rename the user_defined_field_3 to udf3 in the user interface, you should change the Basic Credentials section in the Export Format file as follows:

<GROUP Name="Basic Credentials">
management_ip_address,host_name,domain_name,device_identity,display_name,sysObjectID,dcr_device_type,mdf_type,snmp_v2_ro_comm_string,snmp_v2_rw_comm_string,snmp_v3_user_id,snmp_v3_password,snmp_v3_engine_id,snmp_v3_auth_algorithm,snmp_v3_priv_password,snmp_v3_priv_algorithm,rxboot_mode_username,rxboot_mode_password,primary_username,primary_password,primary_enable_password,http_username,http_password,http_mode,http_port,https_port,cert_common_name,udf3</GROUP>
Export Device Credentials Using UI

To export device credentials:

**Step 1** Select Inventory > Device Administration > Add / Import / Manage Devices.

The Device Management page appears.

**Step 2** Click Export.

The Device Export dialog box appears.

You can use either of the following device selection methods:

- Select from Device Selector
  
  Select this option if you want to export devices from DCR to the file that you specify in the Output File Information field. You can select the required devices from the Device Selector of the Device Export dialog box.

- Get Device List from File
  
  Select this option if you want to export devices from a CSV file that is already present in the server, to the file you specify in the Output File Information field.

  You can use this option when the CSV file contains only partial device credentials, and you want to get the full list of credentials. The input CSV file checks for data in DCR, and exports the data to the output file.

- Get Device List from Group
  
  Select this option if you want to export all devices from the selected groups, to the file you specify in the Output File Information field.

  This device selection method is useful when you want to run a scheduled export job. All new devices added to the selected groups are also automatically exported during the future scheduled jobs.

**If you choose to select from the Device Selector:**

- Select the devices to be exported from the Device Selector.
- Enter the location for the output file in the Output File Information panel field or click Browse to select the location.
- Select either CSV or XML as your output file format.

**If you choose to get the device list from a file:**

- From the Input File Selection Panel, click Browse to browse the file system and select the input file [in CSV format] to get the device list.
- Enter the location for the output file in the Output File Information panel field or click Browse to select the location.
- Select either CSV or XML as your output file format.
- From the Device Selector, select the devices for which you need to export credentials.

**If you choose to get the device list from groups:**

- Select the groups whose devices to be exported from the Group Selector.
- Enter the location for the output file in the Output File Information panel field or click Browse to select the location.
- Select either CSV or XML as your output file format.
- From the Device Selector, select the devices for which you need to export credentials.
Step 3  Select **Export Device Credentials** if you want to export the device credentials along with the device attributes.

The device credentials including the passwords are exported to the output file in clear text format if you select this option.

A confirmation message appears.

Step 4  Click **OK** to continue.

Step 5  Select **Send Device Export Report as an E-mail** to send the Exported Devices report as an attachment.

If the report exceeds the maximum attachment size limit configured in System Preferences page, you may not receive the attachment. You will receive the e-mail notification that provides a hyperlink to the System Preferences page.

You should select the Enable Attachment option and enter a larger size in the Maximum Attachment Size field in the System Preferences page to receive the e-mail attachments. Go to **Admin > System > System Preferences**. See *Modifying System Preferences* in *Administration Guide for Cisco Prime LAN Manager Solution 4.2* for details on configuring maximum and minimum size of attachments.

Step 6  Schedule the task.

To do this:

- Select the Run Type from the drop-down list.
  
  You can schedule export immediately or schedule the export for a later time. The scheduling can be periodic (daily, weekly, or monthly) or only for a single instance.

- Select the date from the date picker.
  
  The date picker displays the date from the client system.

Step 7  Enter a description about the job in the Job Description field.

Step 8  Enter an e-mail address or multiple e-mail addresses separated by comma in the E-mail field.

E-mail notifications and the report attachments are sent to the e-mail addresses entered in this field.

Step 9  Click **Export**.

If you schedule an immediate device export, the job starts immediately.

---

You must populate DCR with devices before you export credentials from DCR using Get Device List from File option.

**Note**  We recommend that you use this option to export up to a maximum of 1000 devices.

### Excluding Devices

This feature allows you to specify a file that contains the list of devices that should not be added to DCR using Add or Import operations.

During the Add or Import operations, DCR ensures that the device being added or imported is not listed in the Exclude Device List.

You can also remove the list of devices that are excluded earlier using the Exclude operation.
The file containing the list of excluded devices should be in CSV format. See A Sample CSV Exclude File for a sample CSV file used for Exclude operation.

You can exclude devices by specifying any one or more of the following fields in the CSV file:

- management_ip_address
- host_name and domain_name
- device_identity

If you are using a CSV file generated by the DCR Export utility to exclude devices from Add or Import operations, make sure to remove the sections related to AUS Managed, Cluster Managed and CNS Managed devices from the CSV file.

To exclude devices from Add or Import operations:

---

**Step 1**
Go to the CiscoWorks home page and select **Inventory > Device Administration > Add / Import / Manage Devices**.

The Device Management page appears.

**Step 2**
Click **Exclude**.

The Upload Exclude Devices File dialog box appears.

**Step 3**
Enter the file name or click **Browse** to browse the file system and select the file.

The file that needs to be uploaded must be in CSV format.

**Step 4**
Click **Apply** to upload the file.

The system displays a message that the devices are excluded successfully.

---

**A Sample CSV Exclude File**

; This file is generated by DCR Export utility
Cisco Systems NM Data import, Source=DCR Export; Type=DCRCSV; Version=3.0
;
;Start of section 0 - Basic Credentials
;
;;HEADER:management_ip_address,host_name,domain_name,device_identity
;;
;Dev1Hostname,,10.1.0.60,,
;,,AUSID1
;Dev2Hostname,cisco.com,
;
;;End of CSV file
Viewing Devices List

You can view the devices in the Device List Report using this feature.

To view devices in the Device List Report:

**Step 1**
Go to the CiscoWorks home page and select **Inventory > Device Administration > Add / Import / Manage Devices**.

The Device Management page appears.

**Step 2**
Select the devices you want from the Device Summary list and click **View**.

The Device List Report dialog box appears.

**Step 3**
Select the device.

**Step 4**
Click **View**.

The Device List Report appears with the following details:

<table>
<thead>
<tr>
<th>Table 4-1</th>
<th><strong>Device Attributes Report Fields</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name, as you want it to be represented in graphical displays and other reports.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Category, Series, and Model information of devices in DCR. For example, Device Type displays Cisco 3000 Router, Cisco Catalyst 8150 CSR Switch and so on.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Management IP Address used to access the devices.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Domain name of the device.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Hostname of the device.</td>
</tr>
<tr>
<td>AUS Device ID</td>
<td>Device ID of the devices managed by Auto Update Server.</td>
</tr>
</tbody>
</table>

**Understanding Unified Device Manager**

In LMS 3.2, each application managed devices and there were multiple device sets. In LMS 4.2, Unified Device Manager (UDM) provides centralized device management using a centralized policy configuration. You have to configure a single policy to manage the devices. UDM identifies managed devices after verifying the configured policy and the license count.

*Note*
There is no policy and license check for non-Cisco devices.

The workflow for UDM is:

1. Add or import devices to DCR
   
   Go to **Inventory > Device Administration > Add / Import / Manage Devices**.

2. Discover devices
Go to Inventory > Device Administration > Discovery > Launch / Summary.

   Go to Inventory > Device Administration > Device Allocation Policy.

4. UDM checks the license count and the configured device management policy. If the device matches the license count and device management policy, it will be in managed state.

Important Notes Related to UDM

This section contains:
- Non-Cisco Device Support
- License Limit
- Backup and Recovery
- Device Management in Master-Slave Setup

Device Management in Master-Slave Setup

In LMS 4.0, the Master will behave like an LMS 4.2 server in Standalone mode. It will synchronize the device credentials across all servers.

When a server is converted into Slave:
- All DCR devices in the Slave will be deleted and synchronized with the Master.
- Device Management auto allocation policy will be disabled.

Non-Cisco Device Support

Non-Cisco Devices are not considered for license check in UDM. If these devices match the device management policy, they will be in managed state.

License Limit

The license limit for LMS is the maximum resource count that LMS can manage.

For example:
- For a 300 device license, the maximum number of devices that you can manage will be 300.
- For a 5000 device license, the maximum number of devices that you can manage will be 5000.

Backup and Recovery

During backup restore from a lower version, all the devices that were managed by the application might not satisfy the new policy configured by the user.

After the process of restore and startup of DCR, all the DCR devices will be verified with the LMS 4.2 configured policy and license count. If the devices match the configured policy and license count they will be called as managed devices else they will be called as suspended devices in UDM. All the suspended devices will not be part of any collector process. You must upgrade your license if you wish to manage the devices that are in suspended state due to the mismatch in the license count.
Cisco Nexus 7000 Device Support

When you add the Nexus devices (Cisco Nexus 7000 10-Slot Switch (1.3.6.1.4.1.9.12.3.1.3.612) and Cisco Nexus 7000 18-Slot Switch - N7K-C7018 (1.3.6.1.4.1.9.12.3.1.3.777)) to DCR, you must provide the Netadmin SNMP RO credential. When you provide other SNMP RO credentials, user tracking will not collect end host data.

Dynamic User Tracking is not supported for the Nexus devices as they do not have MAC notification feature. Trap configuration is also not supported.

The Nexus device should have NXOS 5.1(1), 5.1(3) or later. NXOS 5.1(2) is not supported.

To map community with context, configure the device as follows:

```
snmp-server context <context-name> vrf <vrf-name>

snmp-server mib community-map <snmp community> context <context-name>
```

Understanding Device States

The different device states in LMS 4.2 are:

- Managed State
- Suspended State
- Unmanaged State
- Managed Devices not matching the Policy
- Alias Device

Managed State

Devices that match the license count and the configured policy will be in this state. These devices will appear in the appropriate system defined and user defined groups, if the data necessary to resolve group membership is available. You can initiate various tasks and jobs using devices in this state.

You can perform LMS functionalities like Inventory Collection, and Configuration Management on only on managed devices.

You can move managed devices to suspended or unmanaged state.

Suspension State

If you have some devices under maintenance, they cannot be managed during that period. You can select these devices from the managed device list and suspend them. After the maintenance period, you can move these devices back to the managed state.

Suspension devices do not appear in the managed device list device selector. Syslogs from these devices do not cause any automated actions to happen. However, syslogs from devices in this state are collected and reported, and all the history data will be maintained in the system. These devices will be considered for license count in LMS. Traps are not collected from these devices. Collection and other management activities will not happen. You can move suspended devices to unmanaged or managed state.
Unmanaged State

Devices which fail to match the configured policy and license count will be in this state. You can also select some devices from the managed list and make them unmanaged devices. These devices will be available in UDM and DCR. The corresponding events will be sent to the management components like collectors which will remove the history information from their database. You can move the unmanaged device to only the managed state.

Managed Devices not matching the Policy

Managed devices that fail to match the current configured policy will be in this state. After a fresh installation, the number of Managed Devices not matching the Policy will be zero. Devices will move to this state only after you configure a device management policy, and if there are some managed devices that do not match the policy.

Alias Device

When you add a new device to LMS, this device may already exist in LMS, but with:

- Another hostname or IP Address.
- Same IP Address or host name, but, different device name.

These devices are known as alias devices. See, Working With Alias Devices for more information.

Configuring Device Management Policy

To configure the device management policy for UDM:

Step 1  Go to Inventory > Device Administration > Device Allocation Policy. The Device Management Policy page appears with the following fields:
Chapter 4 Managing Devices and Credentials

Understanding Unified Device Manager

Step 2

Click **Apply** to apply the device management policy. The Auto Allocation Settings Summary page appears with the following details:

- Number of new devices that match the policy
- Number of new devices that match the current license limit
- Current License limit

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Auto Mode    | Select this check box to automatically manage devices from DCR according to the device management policy, which you will configure here. This option is enabled by default. If you do not select this check box:  
  - Devices will not be automatically managed in LMS, inspite of adding the devices using **Inventory > Device Administration > Add / Import / Manage Devices > Add**, and discovering them using **Inventory > Device Administration > Discovery > Launch / Summary**.  
  - You have to manually add the devices as managed device using **Inventory > Device Administration > Add as Managed Devices**. |
| Manage All Devices  | Select this option to automatically manage all devices from DCR. This allocation method is dynamic in nature. When you add devices to DCR after applying the settings, they are also added to UDM at runtime. If you delete a device from DCR, the device will also change to unmanaged state. You can use this option only if the Enable Auto Mode check box is checked. The number of devices added into UDM will depend on the license limit. |
| Manage By Groups    | Select this option to automatically manage devices from DCR using device groups. The devices that are part of the selected groups are added to UDM.  
  **Note** Read **Important Notes for Manage By Groups Option** before you use this option.  
  This allocation method is dynamic in nature. When you add new devices to groups after applying the settings, they are also added to UDM at runtime. You can use this option only if you select the Enable Auto Mode check box. The number of devices added UDM will depend on the license limit.  
  **Note** When you configure the UDM policy, you must not select private and subnet groups in the Device Policy Management group selector. |
| Group Selector      | Lists the groups available for auto allocation. Select one or more groups so that devices belonging to those groups are automatically added to UDM. You can use this option only if you select the Enable Auto Mode check box. |
Step 3  Click **OK** to launch the Device Addition Status pop-up which displays:

- Number of devices added
- Number of error devices

Step 4  Click **OK**.

Click **Devices Not Matching the Policy** button to launch the Managed devices list not matching with the policy page. This page has the list of devices which do not match the current policy. This button will be enabled only if you select the Manage By Groups option.

**Important Notes for Manage By Groups Option**

For user-defined groups, the UDM policy configuration will work only if you create these groups using the following group attributes:

- Host Name
- ManagementIPAddress
- Category
- DeviceIdentity
- DisplayName
- DomainName
- MDFId
- Model
- Series
- SystemObjectID
- User_defined_field_0
- User_defined_field_1
- User_defined_field_2
- User_defined_field_3

If you create a user-defined group with other attributes like IPAddress, subnet, and chassis.Modulename, the UDM policy will not work and the corresponding devices will not be moved to managed State in UDM.

**Managing Device States**

This section contains:

- Managed Device List
- Unmanaged Device List
- Suspended Device List
- Managed Devices List Not Matching With The Policy List
- Device State Change Report
To manage device states in LMS 4.0:

Select **Inventory > Device Administration > Manage Device State**.

The Device State Management page appears with the following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device State</td>
<td>Displays the state of the device. The different device states in LMS 4.2 are:</td>
</tr>
<tr>
<td></td>
<td>- Managed State&lt;br&gt;Devices that match the license count and the configured policy.</td>
</tr>
<tr>
<td></td>
<td>- Suspended State&lt;br&gt;If you have some devices under maintenance, they cannot be managed during that period. You can select these devices from the managed device list and suspend them.</td>
</tr>
<tr>
<td></td>
<td>- Unmanaged State&lt;br&gt;Devices that fail to match the configured policy and license count.</td>
</tr>
<tr>
<td></td>
<td>- Managed Devices not matching the Policy&lt;br&gt;Managed devices that fail to match the current configured policy.</td>
</tr>
<tr>
<td></td>
<td>- Alias Devices&lt;br&gt;When you add a new device to LMS, this device may already exist in LMS, but with another hostname or IP Address. This device will be an Alias device.</td>
</tr>
<tr>
<td>Field Description</td>
<td>For more information see <strong>Understanding Device States</strong>,</td>
</tr>
<tr>
<td>Device Count</td>
<td>Displays the total number of devices in the respective state. Click on the number to launch the respective device list page.</td>
</tr>
<tr>
<td></td>
<td>When you click the number of managed devices, it goes to the Managed Device List page, see <strong>Managed Device List</strong>.</td>
</tr>
<tr>
<td></td>
<td>When you click the number of unmanaged devices, it goes to the Unmanaged Device List page, see <strong>Unmanaged Device List</strong>.</td>
</tr>
<tr>
<td></td>
<td>When you click the number of Managed Devices not matching the Policy, it goes to the Managed devices list not matching with the policy page, see <strong>Managed Devices List Not Matching With The Policy List</strong>.</td>
</tr>
<tr>
<td></td>
<td>When you click the number of suspended devices, it goes to the Suspended Device List page, see <strong>Suspended Device List</strong>.</td>
</tr>
<tr>
<td></td>
<td>When you click the number of alias devices, it goes to the Alias Devices page, see <strong>Working With Alias Devices</strong>.</td>
</tr>
</tbody>
</table>

**Managed Device List**

You can view the list of managed devices. You can select a managed device, and unmanage or suspend it. Click the number of managed devices to launch the Managed Device List page. Click **Cancel** to return to the Device State Management page.

Select a managed device from the device selector and click **Unmanage** or **Suspend** to change the device state.

The Device State Change Report pop-up appears. If there is an error in change of device state it will appear in the report. For more information, see **Device State Change Report**.
Unmanaged Device List

You can view the list of unmanaged devices and their details like IP Address, host name, and location. You can select an unmanaged device, and manage it. Click Cancel to return to the Device State Management page.

Select an unmanaged device and:

- Click Manage to change the state of the device to managed state.
- Click Add to Unmanaged List to change the state of more managed devices to unmanaged state. The Managed Device List page appears with the list of all managed devices.

The Device State Change Report pop-up appears. If there is an error in change of device state it will appear in the report. For more information, see Device State Change Report.

Suspended Device List

You can view the list of suspended devices and their details like IP Address, host name, and location. You can select a suspended device, and manage it. Click Cancel to return to the Device State Management page.

Select a suspended device and:

- Click Unmanage to change the state of the device to unmanaged state.
- Click Manage to change the state of the device to managed state.
- Click Add to Suspended List to change the state of more managed devices to suspended state. The Managed Device List page appears with the list of all managed devices.

The Device State Change Report pop-up appears. If there is an error in change of device state it will appear in the report. For more information, see Device State Change Report.

Managed Devices List Not Matching With The Policy List

You can view the list of Managed Devices not Matching the Policy and their details like IP Address, host name, and location. You can select a device, and manage it. Click Cancel to return to the Device State Management page.

Select a device and click Unmanage or Suspend to change the device state.

The Device State Change Report pop-up appears. If there is an error in change of device state it will appear in the report. For more information, see Device State Change Report.

Device State Change Report

The Device State Change Report pop-up appears when you change the state of a device. If there is an error in the change of device state it will appear in the report.

This report shows the following details:

- Total devices—The total number of devices that were configured to change their state.
- Number of devices that changed state —The total number of devices that have changed their state.
- Error devices—The total number of devices that have not changed their state.
Adding Managed Devices

If you do not configure the Device Policy Management using **Inventory > Device Administration > Device Allocation Policy**, you can manually add managed devices.

You can select a device from the device selector, which shows only the unmanaged devices, and add it as a managed device. To do this select **Inventory > Device Administration > Add as Managed Devices**.

If you neither configure the Device Policy Management nor manually add managed devices, devices will not be automatically managed in LMS, inspite of adding the devices in DCR, using **Inventory > Device Administration > Add / Import / Manage Devices > Add**, and discovering them using **Inventory > Device Administration > Discovery > Launch / Summary**.

Working With Alias Devices

When you add a new device to LMS, this device may already exist in LMS, but with another hostname or IP Address. This device will be an Alias device.

This section contains:

- Resolving an Alias Device
- Verifying Device Credentials

The following are the prerequisites for detecting an alias device:

- The alias device is detected when you perform the first inventory collection for a device.
- A device is detected as an alias device only after a successful inventory collection. If a device is detected as an alias device, you can resolve it using **Inventory > Device Administration > Device Aliases**.
- For all devices which are aliased devices, the LMS reruns the alias detection algorithm again. This detection is performed whenever the inventory is collected successfully. For example, this can happen after you correct the IP Address of the device.
- If the inventory collection is partially successful or failed, an alias device may be listed as a Managed Device or as a Unmanaged Device, based on whether the device was reachable or not.
- After resolving alias devices, the devices will be managed state.

You can resolve the alias by selecting one of the devices using **Inventory > Device Administration > Device Aliases** (see Resolving an Alias Device). After you resolve the alias, all the rejected devices are deleted from the LMS database.

LMS detects an alias device using the alias detection algorithm. It:

1. Gets the device IP Address, sysObjectID and the MAC address corresponding to the IP Address of the new device.
2. Refers to LMS database for devices with the same sysObjectID.
3. Refers to LMS database for devices, which returned in step 2 with IPAddresses and MAC addresses that match the addresses of the new device.
4. Compares the port count for the devices that match the criteria described in Step 2 and 3.
5. Identifies the new device as an alias device if the device is returned in Step 4. Otherwise it does not identify the new device as an alias device.
Resolving an Alias Device

To resolve an Alias device:

Note View Permission Report (Reports > System > Users > Permission) to check if you have the required privileges to perform this task.

Step 1 Select Inventory > Device Administration > Device Aliases.
Or
Select Inventory > Device Administration > Manage Device State and click on the Device Count column entry for the Alias Device State.
The Alias Devices dialog box appears. This dialog box contains two panes,

- Managed Devices—Lists the Managed devices that have aliases to the devices.
- Alias Devices—Lists the devices that are aliased to the Managed devices.

Step 2 Select a device from the Normal Devices pane to view the list of aliased devices.

Step 3 Click Show Alias Devices.
The devices that are aliased to the Managed devices appear in the Alias Devices pane. The devices that are in the Managed device state are also listed along with the other alias devices.

Step 4 Select a device you want to resolve from the Alias Devices pane.
You can go to Inventory > Device Administration > Add / Import / Manage Devices and delete an alias device.

Step 5 Click Select.
The selected device is moved to the Managed device state.
After resolving the alias state devices:

- The resolved devices will remain in the Managed state.
- The unresolved devices will be in the unmanaged state and all their history information will be lost.
You can view the state of the device using Inventory > Device Administration > Manage Device State.

Verifying Device Credentials

To verify device credentials, select Inventory > Job Browsers > Device Credentials Verification.
The Device Credential Verification Jobs browser dialog box appears with a detailed list of all scheduled CDA jobs.
The columns in the job browser display the following information:
Chapter 4   Managing Devices and Credentials

Working With Alias Devices

You can do one of the following:

- Click **Report** to generate a report for Device Credential Verification.
- Click **Create** to create a new device credential verification job.

You can also select a job and do one of the following:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to job when it is created. For periodic jobs such as Daily, and Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001. Click on the hyperlink to view the Job details.</td>
</tr>
</tbody>
</table>
| Status       | Status of the job:  
  - Successful—When the job is successful.  
  - Failed—When the job has failed.  
  - Stopped—When the job has been stopped.  
  - Running—When the job is in progress.  
  - Missed Start—When the job is not initiated to run.  
  - Scheduled—When the job is scheduled to run at a later point of time.  
  - Stop Init—When the job is stopped, it goes to Stop Init State before going to Stopped state. |
| Description  | Description of the job, entered at the time of job creation. |
| Owner        | Username of the job creator. |
| Scheduled at | Date and time at which the job was scheduled. |
| Completed at | Date and time at which the job was completed. |
| Schedule Type| Type of job schedule—Immediate, Once, Daily, Weekly, Monthly, 6-Hourly, 12-Hourly. You can specify when you want to run the Device Credential job. To do this, select one of these options from the drop down menu:  
  - Immediate—Runs the report immediately.  
  - Once—Runs the report once at the specified date and time.  
  - Daily—Runs daily at the specified time.  
  - Weekly—Runs weekly on the day of the week and at the specified time.  
  - Monthly—Runs monthly on the day of the month and at the specified time.  
  - 6-Hourly—Runs once in 6 hours.  
  - 12-Hourly—Runs once in 12 hours. For periodic jobs, the subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. |

You can do one of the following:

- Click **Report** to generate a report for Device Credential Verification.
- Click **Create** to create a new device credential verification job.

You can also select a job and do one of the following:
• Click **Edit** to edit a job. You can edit only scheduled jobs.
• Click **Retry** to retry a job
  
  When you retry a failed job, the job will be retried only on the failed devices, even if it was successful on other devices.
• Click **Stop** to stop a job.
• Click **Delete** to delete a job.

For further details see [Creating Device Credentials Verification Jobs](#).

### Creating Device Credentials Verification Jobs

| **Note** | View Permission Report ([Reports > System > Users > Permission](#)) to check if you have the required privileges to perform this task. |

To select the credentials that need to be verified while adding devices:

**Step 1** Select **Inventory > Job Browsers > Device Credentials Verification**.

Or

Select **Admin > Network > Device Credential Settings > Verification Settings**.

The Device Credentials Job Creation dialog box appears.

**Step 2** Click **Create** to create a new device credential verification job.

**Step 3** Select either:

• Device Selector, if you want to schedule report generation for static group of devices.

Or

• Group Selector, if you want to schedule report generation for dynamic group of devices.

**Step 4** Enter the information required to create a job:

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Credentials Options</td>
<td>Select the credentials that need to be checked. You can check the following device credentials:</td>
</tr>
<tr>
<td></td>
<td>• SNMP Read Community String</td>
</tr>
<tr>
<td></td>
<td>• SNMP Write Community String</td>
</tr>
<tr>
<td></td>
<td>• SNMPv3—SNMP version 3 username and password</td>
</tr>
<tr>
<td></td>
<td>• Telnet—Telnet username and password.</td>
</tr>
<tr>
<td></td>
<td>• Telnet Enable Mode User Name and Password.</td>
</tr>
<tr>
<td></td>
<td>• SSH—SSH username and password.</td>
</tr>
<tr>
<td></td>
<td>• SSH Enable Mode User Name and Password</td>
</tr>
<tr>
<td></td>
<td>To view all these credentials select <strong>All</strong>.</td>
</tr>
</tbody>
</table>
### Working With Alias Devices

#### Scheduling

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Type</td>
<td>Specifies the type of schedule for the job:</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Runs the report immediately.</td>
</tr>
<tr>
<td></td>
<td>• 6-hourly—Runs the report every 6 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• 12-hourly—Runs the report every 12 hours, starting from the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Once—Runs the report once at the specified date and time.</td>
</tr>
<tr>
<td></td>
<td>• Daily—Runs daily at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly—Runs weekly on the day of the week and at the specified time.</td>
</tr>
<tr>
<td></td>
<td>• Monthly—Runs monthly on the day of the month and at the specified time.</td>
</tr>
</tbody>
</table>

For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete.

For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.

If you select Immediate, the Date field option will be disabled.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>1. Enter the start date in the <strong>dd Mmm yyyy</strong> format, for example, 02 Jul 2010, or click on the Calendar icon and select the date.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the start time by selecting the hours and minutes from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Description</td>
<td>Enter a description for the report that you are scheduling. This is a mandatory field. Accepts alphanumeric values and special characters. This field is restricted to 256 characters.</td>
</tr>
</tbody>
</table>
### DCR Server Error

The communication error may be due to the following reasons:

- The DNS resolution does not match with server assigned IP Address.
  
  **Workaround:** DNS resolvable IP Address should be same as server IP Address.

- DHCP is enabled in the server.
  
  **Workaround:** DHCP should be disabled in the server.

- The server’s original IP Address may have changed.
  
  **Workaround:** Restart Cisco Prime Daemon Manager.

- CTM registry corruption has occurred due to rebooting the server without stopping the Cisco Prime Daemon Manager.
  
  **Workaround:** Delete the ctmregistry and ctmregistry.backup file in NMSROOT/MDC/tomcat/webapps/cwhp/WEB-INF/LIB and then restart the Cisco Prime Daemon Manager.

- DCR Server and related process might be down.
  
  **Workaround:** Check the processes to make sure DCR Server is running, and restart it if not.

- The hostname change is not done by the hostnamechange.pl in LMS.
  
  **Workaround:** Hostname change should be done using NMSROOT/bin/hostnamechange.pl in LMS.

---

### Field | Description
--- | ---
E-mail | Enter e-mail addresses to which the job sends messages when the job has run. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View/Edit System Preferences dialog box (**Admin > System > System Preferences**).

Configure the Cisco Prime E-mail ID in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**).

When the job starts or completes, an e-mail is sent with the Cisco Prime E-mail ID as the sender’s address.

Attachment | Select this option if you want to send attachments in the job notification mail. Either select:

- CSV if you want the attachment in CSV format.
  
  Or

- PDF if you want the attachment in PDF format. This is the default format.

The CSV and PDF radio options will be enabled only if the Attachment check box is selected.

If the Attachment option is disabled, you can change the settings.

**Step 5** Click **OK**.
Managing Auto Update Servers

Auto Update Servers have the following credentials:

- Auto Update Server URL
- Username
- Password

Note: The Auto Update Server Management UI is not visible in a DCR Slave machine.

Auto Update Server management feature helps you to add, edit, or delete Auto Update Server. See Adding, Editing, and Deleting Auto Update Server for more information.
Adding, Editing, and Deleting Auto Update Server

To add, edit, or delete Auto Update Server:

**Step 1**
Go to **Inventory > Device Administration > Auto Update Server Management**.
The Auto Update Server Management page appears.

**Step 2**
You can do the following:

- **Add**
  - Click **Add** to add Auto Update Server. The Auto Update Server dialog box appears.
  - Enter the Device Name, Domain Name, IP Address, Host, Port, URN, User name, and password in the corresponding fields. Re-enter the password in the Verify field.
  - DCR uses a device record to represent a Auto Update Server.
  - An Auto Update Server added in the Auto Update Server Management UI can be selected for the Auto Update Server field when you add devices using the Auto Update management type.
  - Click **OK**.

- **Edit**
  - Select the device you want to edit from the list and click **Edit**. The Auto Update Server dialog box appears.
  - Edit Device Name, Domain Name, IP Address, Port, URN, User name, and Password fields.
  - Click **OK**.

- **Delete**
  - Select the device you want to delete from the list.
  - Click **Delete**.
  - The Device Deletion Confirmation dialog box opens.
  - Click **OK** to confirm the deletion of AUS Update Servers.

Configuring Device Selector

The improved Device Selector allows you to search the devices in DCR. It helps to locate the devices and perform the various device management tasks quickly. With this improved Device Selector, you need not remember the device type or application group hierarchy to locate the devices.

The devices are categorized under the Device Type based groups, User Defined groups, Subnet Based groups, Application Specific groups or under All Groups.

You can define the settings of the Device Selector pane to customize the display of devices and the order of display. You can customize the top level groups, sub-groups and the list of devices displayed under each group using the Group Customization option.

The Group Ordering option allows you to specify the order of display in which the groups are seen in the Device Selector pane. See **Device Selector Settings** in the **Administration User Guide for LMS 4.0** for more information.
Configuring Device Selector

The Device Selector Settings are specific to each user. You can search for devices using a Simple search or an Advanced search. See Searching Devices for more information.

Tool tips are also provided for devices that contain long names so that you do not have to scroll horizontally to see the complete device name.

This section contains the following information:

- Using Device Selector
- Selecting Devices for Device Management Tasks
- Searching Devices

Using Device Selector

The Device Selector is used to select devices to perform various device management tasks. This lists all devices in a group. The Device Name of the devices entered when you have added the devices in DCR is displayed as the device name in the Device Selector pane.

The Device Selector contains the following components:

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Search Input   | Enter your search expression in this text field. You can enter a single device name or multiple device names in this field. You can enter the following as search inputs for searching multiple devices:  
- Comma separated list of full device names  
- Device names with wildcard characters ? and * to search for multiple devices matching the text string entered in this input field. The wildcard character ? matches single character in a device name and the wildcard character * matches multiple character in a device name.  
- Combination of comma separated list of device names, and device names with wildcard characters. See Performing Simple Search for more information. |
| Search         | Use this icon to perform a Simple search of devices, after you have entered your search input. See Performing Simple Search for more information. |
| Advanced Search| Use this icon to perform an Advanced search of devices. See Performing Advanced Search for more information. |
| All            | This tab lists all the top-level device groups and the device names under each group in a hierarchical format (tree view). The top-level device groups include:  
- All Devices  
- Device Type Groups  
- User Defined Groups  
See Understanding Device Groups in Administration User Guide for LMS 4.0 for more information on types of device groups. |
Chapter 4      Managing Devices and Credentials

Configuring Device Selector

The Device Selector displays the number of devices selected by you at the bottom. When you click the link provided, it launches the Selection Tab.

Tool tips are also provided for devices that contain long names so that you do not have to scroll horizontally to see the complete device name.

Selecting Devices for Device Management Tasks

You can select devices to perform various device management tasks such as editing device credentials and viewing device credentials, using any of these methods:

- Selecting Devices From All Tab
- Selecting Devices From Search Results
- Combination of Selection From All Tab and Search Results

Selecting Devices From All Tab

The All tab lists the top-level device groups and the device names under each group in a hierarchical format (tree view).

You can select the devices from the tree view. The Selection tab shows the flat list of selected devices from the All tab.

You should expand the nodes of the top-level device groups and sub groups to see the list of devices within a group and select the devices you want. We recommend that you do not expand and leave the multiple group nodes open at a time. This may affect the performance of the device selector.

Selecting Devices From Search Results

You can perform a Simple Search or an Advanced Search, and the search results are displayed under the Search Results tab. You can select the devices you want from the Search Results tab. The Selection tab and the All tab, display the devices you have selected from the Search Results tab.

Note

You can perform more than one search and can accumulate your selection of devices.

Component Name | Description
--- | ---
Search Results | This tab displays all your Simple or Advanced search results and you can select all devices, clear all devices, or select a few devices from the list. The Simple search results are based on the device name of the devices added to DCR. The Advanced search results are based on the grouping attributes of the application's grouping services server.

Selection | This tab lists all the devices that you have selected in the All or Search Results tab or through a combination of both. You can also use this tab to deselect the devices you have already selected. You can perform more than one search and can accumulate your selection of devices.

The Device Selector displays the number of devices selected by you at the bottom. When you click the link provided, it launches the Selection Tab.

Tool tips are also provided for devices that contain long names so that you do not have to scroll horizontally to see the complete device name.

Selecting Devices for Device Management Tasks

You can select devices to perform various device management tasks such as editing device credentials and viewing device credentials, using any of these methods:

- Selecting Devices From All Tab
- Selecting Devices From Search Results
- Combination of Selection From All Tab and Search Results

Selecting Devices From All Tab

The All tab lists the top-level device groups and the device names under each group in a hierarchical format (tree view).

You can select the devices from the tree view. The Selection tab shows the flat list of selected devices from the All tab.

You should expand the nodes of the top-level device groups and sub groups to see the list of devices within a group and select the devices you want. We recommend that you do not expand and leave the multiple group nodes open at a time. This may affect the performance of the device selector.

Selecting Devices From Search Results

You can perform a Simple Search or an Advanced Search, and the search results are displayed under the Search Results tab. You can select the devices you want from the Search Results tab. The Selection tab and the All tab, display the devices you have selected from the Search Results tab.

Note

You can perform more than one search and can accumulate your selection of devices.
Combination of Selection From All Tab and Search Results
You can select the devices from the All tab and add more devices to the Selection list from the Simple or Advanced search results in the Search Results tab.

The Selection tab displays the accumulated list from both All and Search Results tabs.

You can enter another search criteria and select more devices. The selected devices are accumulated in the Selection tab.

Searching Devices

With the improved Device Selector, you can search the devices by performing a Simple search or an Advanced search. In both cases, you do not need to remember the name of the devices and the groups in which the devices are grouped.

Note
The search string is not case sensitive in LMS.

This section contains the following:

- Performing Simple Search
- Performing Advanced Search

Performing Simple Search

You can enter your search criteria in the Search Input field and search for the devices using the Search icon. The search results are based on the device name of the devices added in DCR.

Note the following points when you perform a Simple search.

- You can enter a comma separated list of device names to search for multiple devices.
- You can use the wildcard characters * and ? to search for multiple devices that match the text string entered in this input field. Multiple wild card characters are allowed in a search string.
- You can use the combination of comma separated list of device names and wildcard characters in the device names to search for multiple devices.
- If you are not using the wild card characters, make sure that you enter the full device name.

For example, when you enter `device2?`, `*.cisco1`, `*device10*` as search input, the system displays:

- Device names starting with `device2` and with only one character after `device2`
- Device names ending with `cisco1`
- Device names containing the text string `device10`

Note
When IPv6 device is to be searched and the IPv6 address is given in a compressed format in the search, it will fetch and display the IPv6 address managed in the LMS. For e.g. if `2059::C671*` is searched for, the result fetched will be `2059::C671::FEFF:FE8F:7FC1` and `2059::C671::FEFF:FEA0:6B41`. 
Performing Advanced Search

Use the Advanced Search icon to open the Advanced Search popup window and specify a set of rules for performing an Advanced search. The advanced search is based on the grouping attributes of the grouping server.

You can create a rule in the Advanced Search dialog box by either:

- **Using Expressions**
- **Using Rule Text Fields**

You can verify whether the rule you have entered is correct using the Check Syntax button, and reset the rule you have created using the Clear button.

**Using Expressions**

You can use expressions to form a rule in the Advanced Search Dialog box. Each rule expression contains:

- **Device Type** — Object type used for forming a group. All expressions start with the string Device

- **Variables** — Device attributes used to form a device group. The list of variables for advanced search are Category, DeviceIdentity, DisplayName, DomainName, HostName, ManagementIpAddress, MDFFid, Model, Series, SystemObjectID, and the user-defined data, if any.

- **Operators** — Various operators to be used with the rule. The list of operators includes equals, contains, startswith, and endswith. The list of operators changes dynamically with the value of the variable selected.

  For the ManagementIpAddress variable, you can select the range operator other than the standard list of operators. The range operator enables you to search for devices of the specified range of IP Addresses. See **Using IP Address Range to Form a Search Rule** for more information.

- **Value** — Value of the variable. The value field changes dynamically with the value of the variable and operator selected, and this may be a text field or a list box.

After you define the rule settings, click **Add Expression** to add the rule expression.

You can also enter multiple rule expressions using the logical operators. The logical operators include OR, EXCLUDE and AND.

**Using IP Address Range to Form a Search Rule**

The range operator enables you to search the devices of the specified range of IP Addresses. You can select the range operator only for the ManagementIpAddress and IP.Address variables.

You should enter the range of IP Addresses in the Value field, to create a search rule based on IP Address ranges.

When you enter the IP Address range in the text field, you should:

- Specify the range with permissible values for one or more octets in the IP Address.
  - The minimum limit in the range is 0 and the maximum limit is 255.
- Use the hyphen character (-) as a separator between the numbers within a range.
- Specify the range of IP Addresses within the [ and ] characters to create a group rule.
For example, you can enter 10.10.10.[0-255] or 10.10.[0-255].[0-255] in the Value field.
You should not:
- Enter numbers lesser than 0 and greater than 255 in the IP Address range.
- Enter any other characters other than the range separator (-).
- Enter the value of highest limit in the range as less than the value of smallest limit number. For example, you should not enter 10.10.10.[8-4].

**Example for forming a Search Rule Using Expressions**
For example, if you want to search all the devices in the network whose device name contains TestDevice or their IP Addresses within the range 10.10.210.207 to 10.10.212.247, you must perform the following:

---

**Step 1**
Click the Advanced Search icon in the Device Selector pane.
The Define Advanced Search Rule dialog box appears.

**Step 2**
Create a search rule expression. To do so:
a. Select Variable as **DisplayName**
b. Select Operator as **equals**
c. Enter the Value as **TestDevice**

**Step 3**
Click **Add Rule Expression**.
The rule is added into the Rule Text.

**Step 4**
Create another rule expression. To do this:
a. Select **OR** as the logical operator
b. Select Variable as **ManagementIPAddress/IP.Address**
c. Select Operator as **range**
d. Enter the Value as **10.10.[210-212].[207-247]**

**Step 5**
Click **Add Rule Expression**.
The rule is appended into the Rule Text.

**Step 6**
Click **Search** to display the devices that satisfies the specified rule in the Device Selection dialog box.
Using Rule Text Fields

You can use Rule Text Fields to directly enter a rule without building any expressions. Ensure the rule you create follows the syntax Object type.Variable Operator Value.

You can also enter multiple rule expressions using the logical operators.

For example, if you want to search all the devices in the network whose device name contains TestDevice or their SysObjectIDs start with 1.3.12.1.4, you must construct a rule as follows:

Device.DisplayName contains "TestDevice" OR Device.SystemObjectID startswith "1.3.12.1.4"

**Note**

We recommend that you use expressions to construct a complex rule instead of creating them using the Rule Text field. Use the Rule Text field to make any minor edits to the constructed rule.

**Additional Notes**

Read the following notes before you perform a advanced search:

- You cannot use wild card characters in the Value field. Instead you can use the operator as startswith or contains.
- You can use Check Syntax button, when you add or modify a rule manually.
- You must delete the complete rule expression including the logical operator, when you delete a portion of your rule.
- The search string is case-insensitive.
CiscoView

CiscoView is a graphical SNMP-based device management tool that provides real-time views of networked Cisco Systems devices. These views deliver a continuously updated physical and logical picture of device configuration and performance conditions. Simultaneous views are also available for multiple device sessions.

Use CiscoView to:
- View a graphical representation of the device, including component (interface, card, power supply, LED) status.
- Configure parameters for devices, cards, and interfaces.
- Monitor real-time statistics for interfaces, resource utilization, and device performance.
- Set user preferences.
- Perform device-specific operations as defined in each device package.
- Manage groups of stackable devices.

The following topics are described in this section:
- CiscoView Features
- Starting CiscoView
- Navigating in CiscoView
- Viewing Devices Not Available in the DCR
- Setting Preferences for CiscoView
- Generating Interface Report for CiscoView
- Device Packages
- Device Management in CiscoView
- Configuring Devices Using CiscoView
- Setting CiscoView Debugging Options and Display Logs
CiscoView Features

CiscoView operates in client-server mode. In this mode, the device package and basic management functionality are centrally located on the CiscoView server.

In addition to device management, CiscoView provides the following features:

- Internet Protocol version 6 (IPv6) functionality.
  - When the IPv6 device package is installed, CiscoView manages IPv6 functionality using Telnet/SNMP over IPv4 transport using dual stacks.
  - IPv6 management features are launched from the device’s context menu (see Using the Context Menu for more information).

For information on devices on which CiscoView supports IPv6 functionality, see the IPv6 device package readme file on Cisco.com.

- Device list and credentials from a common database. CiscoView inherits device credentials from the Device and Credential Repository. The DCR contains a common list of devices and credentials for all installed Cisco Prime products. The DCR Administration provides an interface to administer the DCR.

For more information on the DCR and DCR Administration, see Administration Guide for Cisco Prime LAN Manager Solution 4.2.

- SNMP version 3 (SNMPv3) support. CiscoView supports SNMPv3 communication with authentication and encryption for greater security. DCR Administration fetches SNMPv3 and SNMPv1 or SNMPv2 device credentials. DCR Administration gives preference to using SNMPv3 device credentials.

- Mini-RMON (Remote Monitoring) functionality. This can be used to set up alarms, collect traffic statistics for a device, and troubleshoot network-related problems. To determine the devices on which CiscoView supports RMON functionality, see CiscoView Mini-RMON Manager.

- HTML-based client. CiscoView provides a lightweight, HTML-based client with added support for Netscape and Mozilla.

- Integration with Software Center:
  You can access the Software Center using Admin > System > Software Center.

- Improved user interface. See Navigating in CiscoView for more information.

To ensure that setup is correct to use CiscoView and perform basic functions within CiscoView, you must perform certain tasks. For more information about your setup, see Installation and Data Migration Guide for Cisco Prime LAN Manager Solution 4.2.
Starting CiscoView

You can start CiscoView from the Inventory tab in the LMS Menu.

To start CiscoView:

**Step 1**
Select **Inventory > Tools > CiscoView** from the CiscoWorks home page.

**Step 2**
Do one of the following:
- In the Enter Device Name or IP Address field, enter the name or IP Address of the device you want to access and click **Go**.
- Perform either a standard or advanced device search. See **To select a device** and **To perform an advanced device search** for more information.
- From the list of all devices managed by DCR Administration (**Inventory > Device Administration > Manage Device State**), navigate and select the device you want to access.

The Device Information page appears, with the Summary and Functions Available panes displayed.

Navigating in CiscoView

When you start CiscoView, the CiscoView desktop opens.

This section contains:

- **Using the Options Bar**
- **Using the Tools Bar**
- **Using the Device Selector of CiscoView**
- **Understanding the Color Legend**
- **Using the Context Menu of CiscoView**
- **Selecting a Device or its Components in the Chassis View**

Table 5-1 describes each component on the CiscoView desktop.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options bar</td>
<td>Allows you to view devices in CiscoView, access the color legend, set debug options, launch Mini-RMON, and change preferences. See Table 5-2 in Using the Options Bar for a description of each option.</td>
</tr>
<tr>
<td>Tools bar</td>
<td>Allows you to view the sitemap of LMS, access online help that is specific to the selected device. You can also see the installed version of LMS, and logout when required. See Table 5-3 in Using the Tools Bar for a description of each option.</td>
</tr>
</tbody>
</table>
Navigating in CiscoView

Table 5-1  CiscoView Desktop Component Descriptions

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Chassis view    | Displays a graphical representation of the back or front device panel after you select a device. Device components are color-coded according to their status. They are refreshed according to the polling frequency you have defined. See Understanding the Color Legend for more information on color status definitions.  
  **Note** If a hot swap is detected, the device is rediscovered and the display redrawn at the next poll. |
| Status bar      | Shows progress, result of device polling, and refreshes. If any error occurs as a result of device polling, the error message will appear in the Status bar.                                      |
| Device Selector handle | Opens and closes the Device Selector (see Using the Device Selector of CiscoView):  
  • When the Device Selector is closed, click the handle to open it.  
  • When the Device Selector is open, click the handle to close it. |

Using the Options Bar

Table 5-2 describes the options on the Options bar.

Table 5-2  Options Bar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name/IP field</td>
<td>You can enter either the name or IP Address of a device and view that device within CiscoView. If the SNMP credentials of the device are not listed in the DCR, you will be prompted to enter the appropriate credentials. See Viewing Devices Not Available in the DCR for more information.</td>
</tr>
<tr>
<td>Color Legend</td>
<td>You can access the color legend. This legend defines the colors to indicate the status of the device components. See Understanding the Color Legend for more information.</td>
</tr>
</tbody>
</table>
| Preferences     | You can set the following global preferences:  
  • Length of time for the SNMP request to timeout  
  • Number of times that CiscoView tries to send an SNMP request  
  • Refresh rate of chassis view (how often the device is polled)  
  • MIB label shown in dialog boxes  
  • Refresh rate of graphs within the device monitoring dialog box  
  See Setting Preferences for CiscoView for more information.  
  For example, to set preferences for a particular device, you need to access the device's context menu. See Using the Context Menu of CiscoView for more information. |
| Mini RMON       | You can launch CiscoView Mini-RMON Manager. See CiscoView Mini-RMON Manager for more information.                                              |
| Debug Options   | You can set the CiscoView debugging options and display logs.                                                                                 |
Using the Tools Bar

Table 5-3 describes the options on the Tools bar.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Prime</td>
<td>Navigates to the Cisco Prime LMS homepage.</td>
</tr>
<tr>
<td>Help</td>
<td>Opens a new window that displays context-sensitive help for the displayed page. The window also contains buttons that allow you to access the Online help, Index, and Search tool. See Device Packages for more information.</td>
</tr>
<tr>
<td>About</td>
<td>Displays the following information:</td>
</tr>
<tr>
<td></td>
<td>• CiscoView release version and copyrights. This refers to the base application that runs all device packages; for example, CiscoView X.X.X.</td>
</tr>
<tr>
<td></td>
<td>• Installation date.</td>
</tr>
<tr>
<td></td>
<td>• Active device package, if applicable; for example, Cat5000 Package, Version X.X.</td>
</tr>
<tr>
<td></td>
<td>• All installed device package information (version numbers are shown in parentheses).</td>
</tr>
<tr>
<td></td>
<td>See Device Packages for more information.</td>
</tr>
</tbody>
</table>

Using the Device Selector of CiscoView

The Device Selector is on the left of the CiscoView desktop. It lists all devices managed by DCR Administration. From here, you can select a device to manage within CiscoView. See Administration Guide for Cisco Prime LAN Manager Solution 4.2 for information on adding devices and setting device credentials. Note the following:

• Auto Update Server (AUS) device and cluster members are filtered from the CiscoView device list.
• In the Local Cisco Prime security mode, the Device Selector lists all the devices in the DCR.

To display the chassis view for a device:

**Step 1** Select **Inventory > Tools > CiscoView**.

**Step 2** Open the Device Selector by clicking the Device Selector handle.

**Step 3** Do one of the following:

• Select a device to manage from the device list.
• Search for a device to manage.
• Perform an advanced device search.
To select a device

Step 1
In the All tab, click either:

- **All Devices** — To view all of the devices managed by DCR Administration.

or

- **Device Type Groups** — To view all devices, organized by groups.

For more information on device groups, see *Administration Guide for Cisco Prime LAN Manager Solution 4.2*.

Step 2
Select a device from the list.

A graphical representation of the device chassis appears.

To search for a device:

Step 1
Enter your search criteria in the Search Input field. Note the following:

- The text string you enter is case-sensitive.

- To search for multiple devices, enter the full device names, separated by commas.

- You can specify one or more wildcard characters (*) in the text string.

- If you are *not* using wildcard characters in your search criteria, make sure to enter complete device names.

Step 2
Click ![Search button]

The Search Results tab lists the devices that meet the search criteria.

If none of the devices managed by DCR Administration meet your search criteria, CiscoView displays the following message: *There are no search results generated for this value.*

Step 3
Select the radio button for that device. A graphical representation of the device chassis appears.

To perform an advanced device search

Step 1
Click ![Advanced search button] to launch the Define Advanced Search Rule dialog box.

*Figure 5-1  Advanced Search*
Step 2  Define a search rule.

You can do so from either the Rule Expression pane or the Rule Text pane. Note the following:

- Text you enter in this dialog box is case-sensitive.
- You cannot specify wildcard characters in an advanced search rule. Instead, set contains as the operator and then enter the value you want to search for, in the text field.
- When you enter a search rule directly in the Rule Text pane, click Check Syntax to verify that the rule you entered is properly formatted.

Step 3  Click Search.

The Search Results tab lists the devices which meet the search criteria you specified. If none of the devices managed by DCR Administration meet your search criteria, CiscoView displays the following message: There are no search results generated for this value.

Step 4  Select the radio button for the device you want to manage.

A graphical representation of the device chassis appears.
To define a search rule:

**Step 1** Ensure that **Device** is the object type selected in the first list.

**Step 2** From the second list, select the device attribute that you want to search by.
For example, you can search for a device by device name, IP Address, or model number.

**Step 3** From the third list, select the appropriate operator for this search rule.
Here, you can specify whether you want CiscoView to search for a specific text string or for all values that contain that string.

**Step 4** In the text field, enter the text string you want to search for.

**Step 5** Click **Add Rule Expression**.
The search rule defined is listed in the Rule Text pane.

**Note** To further refine your search criteria, repeat this procedure.

To define a search rule in the rule text pane:

In the Rule Text pane, you can enter a search rule directly instead of selecting variables from a list. All search rules should be formatted as follows: `object type . variable operator value`.

For example, to search for all devices in your network with device names that contain the words `TestDevice`, you should enter the following rule: `Device.DeviceName contains “TestDevice”`

### Understanding the Color Legend

When a device is selected and displayed in the chassis view, all device components are color-coded according to their status. **Table 5-4** shows each color and its meaning.

<table>
<thead>
<tr>
<th>Color</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cyan (blue-green)   | Port is dormant | Interface cannot pass packets. It is in a pending state, waiting for an external event to place it in the Up state. Interface could have:  
  - Packets to transmit before establishing a connection to a remote system
  - A remote system establishing a connection to the interface; for example, dialing up to a SLIP server
When the expected event occurs, the interface state changes to Up. |
| Orange/Light Brown  | Port is down | Admin status is Down and operational value is also Down. For Catalyst 4000, 5000, and 6000 devices, it can also indicate that the port is not connected. |
| Red                 | Port failed  | Hardware failure in the port or the port is not connected. For Catalyst 4000, 5000, and 6000 devices, orange or light brown indicates that the port is not connected. |
Chapter 5  CiscoView

Navigating in CiscoView

When you select a device in CiscoView, a graphical representation of the device is displayed in the
chassis view. The context menu appears when you right-click a device or its components. Its contents
are context-sensitive and varies according to the device and your selection.

You can view the front or back device panel and select different components (cards, ports, power supply)
and menu options to configure and monitor status for the device.

To access the context menu:

| Step 1 | Select **Inventory > Tools > CiscoView.** |
| Step 2 | Select a device from the Device Selector. |
|        | A graphical representation of the device chassis appears. |
| Step 3 | Right-click the device or its components. |
|        | The context menu appears. |
| Step 4 | Select an option to change. |
|        | The context menu contents vary by device, but contains the following options: |

**Table 5-4  Color Legend Descriptions (continued)**

<table>
<thead>
<tr>
<th>Color</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yellow</td>
<td>Minor failure</td>
<td>Port or interface is Down: both admin and operational status are Down. This does not indicate a fault condition. Yellow can also indicate that the port is disabled.</td>
</tr>
<tr>
<td>Purple</td>
<td>Port is being tested</td>
<td>Admin status is Up, but tests must be performed on the interface. After testing is completed, the interface state changes to Up, Dormant, or Down.</td>
</tr>
<tr>
<td>Green</td>
<td>Port is active</td>
<td>Interface is able to send and receive packets.</td>
</tr>
</tbody>
</table>
Selecting a Device or its Components in the Chassis View

You can select the entire device, or one or more Cisco device components to configure and monitor. For example, you can configure multiple ports or multiple cards in a chassis.

To do this:

**Step 1**  
Select **Inventory > Tools > CiscoView**.

**Step 2**  
Either select a device from the Device Selector  
or  
Enter an IP Address or device name in the Device Name/IP field of the **Options** bar

**Step 3**  
Click **Go**.  
A graphical representation of the device chassis appears.

**Step 4**  
Do one of the following:
- Select the device or a single component.
  - Left-click on the device or component to select it. A yellow border appears around the selection.  
    (To select the entire device, point to an area that does not contain a component before clicking.)  
  - Right-click to display the context menu.
- Select multiple components.
  - Hold down the Ctrl key to select several similar components at once. A yellow border appears around the selected components.  
  - Right-click while holding down the Ctrl key to display the context menu.
### Viewing Devices Not Available in the DCR

In CiscoView, you can also view devices that are not currently available in the DCR.

**Step 1** Select **Inventory > Tools > CiscoView**.

**Step 2** In the Device Name/IP field, enter the IP Address or name of the device you want to view.

**Step 3** Click **Go**.

The SNMP Credentials dialog box appears.

If you enter the IP Address or name of a device that already has credentials configured in the DCR (and thus the Device Selector), CiscoView displays the chassis view for that device. It does not prompt you to enter its SNMP credentials.

**Step 4** In the Select Protocol field, select either the SNMP V3 or SNMP V1/V2C radio button, depending on the type of credentials you want to use for the device.

- If you selected the SNMP V3 radio button:
  - Set the security mode you need.
    - AuthPriv: Provides authentication based on either the HMAC-MD5 or HMAC-SHA algorithm as well as encryption.
    - AuthNoPriv: Provides either HMAC-MD5 or HMAC-SHA authentication.
  - Enter the username and password required for authentication.
  - Specify the authentication algorithm you want to use by selecting either the MD5 or SHA-1 radio button.

- If you selected the AuthPriv security mode, do the following:
  - Enter the privacy password required to view encrypted SNMP packets.
  - Select the desired encryption algorithm: DES (Data Encryption Standard), 3DES, AES128 (Advanced Encryption Standard), AES192, or AES256
  - If you selected the SNMP V1/V2C radio button, enter the appropriate read-only and read-write community strings.

**Step 5** Click **OK**.

The device is displayed in CiscoView.
Setting Preferences for CiscoView

To launch the Device Preferences dialog box:

Step 1  Select Inventory > Tools > CiscoView.
Step 2  Click Preferences from the Options bar.
Step 3  Specify your options as given below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Display Name</td>
<td>Select the IP Address of the device for which you want to set preferences.</td>
</tr>
<tr>
<td>SNMP Timeout</td>
<td>Enter a value (in seconds) in the field. This value represents the length of</td>
</tr>
<tr>
<td></td>
<td>time that elapses before an SNMP request times out.</td>
</tr>
<tr>
<td>SNMP Retry Count</td>
<td>Enter a value in the field. This value is the number of times an SNMP request</td>
</tr>
<tr>
<td></td>
<td>will be sent before the request times out.</td>
</tr>
<tr>
<td>Chassis Polling Frequency</td>
<td>Select a value from the list. The default value varies by device. A typical</td>
</tr>
<tr>
<td></td>
<td>value is every 60 seconds. CiscoView real-time status is based on periodic</td>
</tr>
<tr>
<td></td>
<td>SNMP queries sent to the managed device.</td>
</tr>
<tr>
<td></td>
<td>If you reduce polling frequency (for example, from 10 seconds to 120 seconds),</td>
</tr>
<tr>
<td></td>
<td>it reduces SNMP-based traffic on the network and the workstation overhead</td>
</tr>
<tr>
<td></td>
<td>required for processing.</td>
</tr>
<tr>
<td>Show MIB Label as</td>
<td>• Click Descriptor to display MIB descriptors, for example, sysName.</td>
</tr>
<tr>
<td></td>
<td>• Click Alias to display textual labels, for example, System Name.</td>
</tr>
<tr>
<td>Default Refresh Rate for Monitor Dialogs</td>
<td>Select a value from the list. The monitoring dialog is updated at the selected Refresh rate. The default value is 30 seconds.</td>
</tr>
</tbody>
</table>

Step 4  Click Apply.

Note  The settings specified here are also used by CiscoView Mini-RMON Manager.

Generating Interface Report for CiscoView

You can launch the Device Performance Management Interface Report for multiple ports.
You can generate and view this Interface Report for multiple ports within CiscoView. This report summarizes the activity for the selected ports during the past hour.
To launch this report:

**Step 1** Select **Inventory > Tools > CiscoView**.

**Step 2** Select a device from the device selector.

**Step 3** Right-click the ports for which you want to generate a report while holding down the Ctrl key.

**Step 4** From the context menu, select **Device Performance Management > Interface Report**.

The following devices support this feature:

- Cisco Switches: Catalyst 2940, Catalyst 2950, Catalyst 2955, Catalyst 2960, Catalyst 2970, Catalyst 3550, Catalyst 3560, Catalyst 3750, Catalyst 4000 (running either Catalyst OS or Cisco IOS software), Catalyst 6000 (running either Catalyst OS or Cisco IOS software), ME 2400-24TS-A, ME 3400-24TS-A
- Cisco Routers: Cisco 800, Cisco 1800, Cisco Mobile Wireless Router (MWR) 1900, Cisco 2800, Cisco 3200 Mobile Access Router (MAR), Cisco 3800, Cisco 7000, Cisco 10000, Cisco 10700, Cisco 12000

**Device Packages**

Cisco’s routers and switches are referred to as network devices. Routers and switches must be physically installed in the appropriate chassis and connected to your network (using each specific device’s hardware installation guide).

A software update that enables CiscoView to support new features for a particular device is called a device package. CiscoView uses the device package to display a dynamic panel view of the physical device and all its modules, submodules, and ports.

The CiscoView engine controls and manages physically connected devices through Simple Network Management Protocol (SNMP).

The SNMP system consists of three parts:

- SNMP manager.
- SNMP agent
- MIB.

Each installed device’s SNMP agent uses sets of MIB variables that you can configure, monitor, and modify. You can do this using CiscoView and each installed device package software.

This section contains **Device Package Updates**.

**Device Package Updates**

CiscoView provides support for a considerable range of devices by installing device packages. Additional device packages can be added to CiscoView anytime after the initial product release or installation.

When new device packages become available, they are placed on Cisco.com. Check this site to ensure that you have the latest device release. You can add or update device packages by using Software Center. Software Center (**Admin > System > Software Center > Device Update**).
For more information on using Software Center, see *Administration Guide for Cisco Prime LAN Management Solution 4.2*. Make sure to review the CiscoView release notes for each device package because they supply critical information, notes, and cautions about usage.

### Device Management in CiscoView

CiscoView imports the devices it needs to manage and their SNMP credentials from the device list in the Device and Credential Repository (DCR). DCR serves as a common device repository for all installed Cisco Prime applications.

CiscoView displays the device list using the Groups feature. This feature determines the membership of a group by interpreting and applying the rules that are associated with a group of devices.

DCR Administration provides an interface to administer DCR. It allows you to add new devices or edit the current SNMP credentials for a device. See *Administration Guide for Cisco Prime LAN Management Solution 4.2* for more information.

**Note**

CiscoView supports SNMPv3. If SNMPv1 or SNMPv2 device credentials are also present in the DCR, CiscoView gives preference to the SNMPv3 credentials.

This section contains the following topics:

- Understanding Categories in CiscoView
- Editing Categories in CiscoView
- Configuring Devices in CiscoView
- Monitoring Devices in CiscoView
- Viewing System Information in CiscoView

### Understanding Categories in CiscoView

Categories consist of commands and options specific to a selected device. You can modify or view categories to configure and monitor a device, card, and port.

For example, a Catalyst 6000 device has configuration categories, such as Management, Physical, AAA Configuration, ARP Table, Authentication.

**Note**

Some devices and components have no categories.

### Editing Categories in CiscoView

You can display and change different categories of information for each device, card, and port. Each device has different categories that you can configure and monitor.

The Category list in the Configuration and Monitor dialog boxes shows the categories of information available for the selected device or component.
For example for a Catalyst 6000 device, the configuration categories are Management, Physical, AAA Configuration, ARP Table, Authentication.

## Configuring Devices in CiscoView

Configure a device to define its characteristics, connections, and components (such as cards and ports). You can configure different categories of information for devices and components and also change multiple categories at the same time.

### Prerequisites
Verify these prerequisites before starting the procedure for this scenario:

- SNMP credentials are valid.
- Permissions for IP Addresses are enabled.

To configure devices in CiscoView:

### Step 1
Select **Inventory > Tools > CiscoView**.

### Step 2
Select a device from the Device Selector.

A graphical representation of the device chassis appears.

### Step 3
Select the device or components to configure.

### Step 4
Right-click to display the context menu, then select **Configure**.

The Configuration dialog box appears.

### Step 5
From the Category list, select the category to configure and enter the required information.

Note the following:

- Categories and fields vary by device.
- As you change the information in fields for different categories, the changes are retained.

### Step 6
When you are done modifying a category, click one of the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Applies your changes and exits the dialog box.</td>
</tr>
<tr>
<td>Apply</td>
<td>Applies your changes. The Configuration dialog box remains open. This allows you to select more categories to view or configure.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels your changes and exits the dialog box.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the dialog box.</td>
</tr>
<tr>
<td>Print</td>
<td>Prints the current category.</td>
</tr>
<tr>
<td>Help</td>
<td>Opens online help that is specific to that device and category.</td>
</tr>
</tbody>
</table>

If a table appears, click one of the following buttons:
After you configure devices using CiscoView, you must:

- Add IP Addresses for Other Management Workstations
- Limit Device Access Privileges for Other Management Workstations
- Verify Device Configurations and Device Access
- Edit Configuring and Monitoring Tables

**Add IP Addresses for Other Management Workstations**

After you configure your device, add new IP Addresses to the IP Permit List. These addresses determine which management workstations are permitted to access this particular device.

**Note**

IP Addresses allow management workstations to access specific devices for configuration. You can add as many IP Addresses to the IP Address list as necessary.

**Step 1** Select **Inventory > Tools > CiscoView**.

**Step 2** From the Device Configuration dialog box, select **IP Permit** from the Category list to display the IP Permit window.

**Step 3** Click **Create**.

The Row Creation dialog box appears.

**Step 4** Enter the appropriate IP Address and IP mask.

**Step 5** Select the appropriate access type from the list and click **OK**.

The new IP Address is added to the IP Permit List.

**Limit Device Access Privileges for Other Management Workstations**

Limit access privileges for other management workstations and monitor unauthorized attempts to access the device.

**Step 1** In the IP Permit window, highlight the IP Address to be deleted from the IP Permit List and click **Delete**.

This disables that particular management workstation from accessing the device.

**Step 2** Reopen the IP Permit window to view any access to the device.

This allows you to monitor unauthorized attempts to access the device.
Verify Device Configurations and Device Access

After you configure your device and limit access to the device by other management workstations, verify that there are no unauthorized workstations accessing the device.

To verify this, view the Access Attempts From Invalid IP Addresses table at the bottom of the window. This table provides information about which management workstations recently attempted to access the device, the time and date of attempted access, and a list of the invalid IP Addresses that were deleted.

If a deleted IP Address is still attempting to access the device, notify the owner of that particular management workstation regarding any recent changes made to the owner’s security level.

Edit Configuring and Monitoring Tables

If you select multiple components for configuring or monitoring, a table appears. A read-write table entry appears with either a combo-box, text box, or check box.

All entries in a monitor table are read-only. You can add, modify, or delete entries from a configuration table. To do this:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select the table row entry that you want to modify.</td>
</tr>
<tr>
<td>2</td>
<td>Either type a new value or select one from the list.</td>
</tr>
<tr>
<td>3</td>
<td>Click Apply.</td>
</tr>
</tbody>
</table>

Monitoring Devices in CiscoView

You can monitor real-time statistics for interfaces, resource utilization, and device performance. CiscoView also allows you to simultaneously monitor multiple categories, such as Ethernet Collisions, Management, Physical, and ARP Table.

CiscoView supports pie, strip, x-y, and bar charts. The chart type displayed, depends on the device and category that you select.

To monitor devices in CiscoView:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Inventory &gt; Tools &gt; CiscoView.</strong></td>
</tr>
<tr>
<td>2</td>
<td>Select a device from the Device Selector. A graphical representation of the device chassis appears.</td>
</tr>
<tr>
<td>3</td>
<td>Select the device or components.</td>
</tr>
<tr>
<td>4</td>
<td>Right-click to display the context menu, and then select <strong>Monitor.</strong> The Monitor dialog box appears and displays a summary of performance charts that vary by device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When a bar graph fills up, it scrolls to the left as polling continues.</td>
</tr>
<tr>
<td>5</td>
<td>Select a category from the Category list.</td>
</tr>
<tr>
<td>6</td>
<td>Select the Refresh Rate (sec) check box and then select a value from the list.</td>
</tr>
</tbody>
</table>
A chart for the selected category appears. It is updated at the selected Refresh rate.
If you need to open another Monitor window, repeat steps 2 through 5.

Note: You can monitor multiple categories simultaneously.

Step 7 Click one of the following buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel</td>
<td>Exits the dialog box.</td>
</tr>
<tr>
<td>Print</td>
<td>Prints current charts.</td>
</tr>
<tr>
<td>Help</td>
<td>Opens online help that is specific to that category and device.</td>
</tr>
</tbody>
</table>

---

**Viewing System Information in CiscoView**

The System Information dialog box displays the following information about the selected device:
- Device Name
- Description (typically indicates the software installed on a device)
- Location
- Contact (name of the individual or group that manages a device)
- Date and time that a device was last initialized on

This section contains Configuring Devices Using CiscoView.

To view system information:

Step 1 Select **Inventory > Tools > CiscoView**.
Step 2 Select a device from the Device Selector.
A graphical representation of the device chassis appears.
Step 3 Click on the device display so that a yellow border appears around the entire device.
Step 4 Right-click to display the Context menu and select **System Info**.
The System Information dialog box appears.

---

**Configuring Devices Using CiscoView**

In this scenario, you are a system administrator who wants to use CiscoView to configure a Catalyst 4000 series device and add IP Addresses to allow other management workstations to access the same device. At the same time, you want to limit access to that particular device for other management workstations.
How to Do It—Procedures
Use the procedures in this section to:
1. Access the Device Configuration Dialog Box
2. Add IP Addresses for Other Management Workstations.

Access the Device Configuration Dialog Box
Access the Device Configuration dialog box to configure your device:

Step 1 Select Inventory > Tools > CiscoView.
Step 2 Select a device from the Device Selector.
A graphical representation of the device chassis appears.
Step 3 Right-click the device.
The context menu appears.
Step 4 Select Configure.
The Device Configuration dialog box appears.
Step 5 Configure your Catalyst 4000 device by entering the required information for that device in the appropriate category fields.
Step 6 Click OK.

Setting CiscoView Debugging Options and Display Logs
You can set a SNMP and activity trace and/or view the trace log. This option records trace information into the cv.log file, which is located at %NMSROOT%/MDC/tomcat, where %NMSROOT% is the directory in which CiscoView is installed.

Step 1 Select Admin > System > Debug settings > CiscoView Debug Options And Display Log.
Or
Select Inventory > Tools > CiscoView. Click the Debug Options link in the Options bar.
The Trace Settings dialog box appears.
Step 2 Select either or both of the following and then click Apply:
• SNMP Trace — Displays SNMP request and response pairs, MIB instance ID, data value, data type, request method, and time stamp.
• Activity Trace — Displays server activity such as which device and dialog boxes are open.
Step 3 Click View Trace to see the trace activity in a separate window.
CiscoView Mini-RMON Manager

CiscoView Mini-RMON Manager provides web-enabled, real-time, remote monitoring (RMON) information to users to facilitate troubleshooting and improve network availability. When you use CiscoView Mini-RMON Manager with some Cisco devices, it provides visibility into network problems before they become critical.

To use this application, you must first install the Mini-RMON patch. This patch makes necessary updates to the CiscoView engine and installs the CiscoView Mini-RMON Manager device package. See Device Packages for more information.

**Note**

Mini-RMON will function in all devices which support the rmon mib object of the RMON-MIB.

This section contains the following topics:

- Starting CiscoView Mini-RMON Manager
- Navigating in CiscoView Mini-RMON Manager
- Setting Up CiscoView Mini-RMON Manager
Starting CiscoView Mini-RMON Manager

To start CiscoView Mini-RMON:

---

**Step 1**  
Select **Inventory > Tools > Mini-RMON**.  
Or  
Select **Monitor > Monitoring Tools > Mini-RMON**.  
The CiscoView Mini-RMON Manager Overview page appears.

**Step 2**  
Do one of the following in the Device Selector pane:
- In the Device Name or IP field, enter the name or IP Address of the device you want to monitor and then click **Go**.  
The SNMP Credentials dialog box appears.
- Perform either a standard or advanced device search. See **To search for a device:** and **To perform an advanced device search** for more information.
- From the list of all devices managed by DCR Administration, navigate to and select the device you want to monitor.

If you selected a device from the list, you can stop here. Otherwise, proceed to Step 3.

**Step 3**  
Enter the appropriate SNMPV1/V2C or SNMPV3 credentials and then click **OK**.
Navigating in CiscoView Mini-RMON Manager

After starting CiscoView Mini-RMON Manager, the application desktop opens. Table 6-1 describes each component on the CiscoView Mini-RMON Manager desktop.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Selector</td>
<td>Allows you to select the device to monitor. You can either enter the IP Address of a device or select it from the list.</td>
</tr>
<tr>
<td>Main window</td>
<td>Displays the active page or dialog box.</td>
</tr>
<tr>
<td>Feature tabs</td>
<td>Serves as the launching point for the threshold management and traffic monitoring pages.</td>
</tr>
<tr>
<td>Options bar</td>
<td>Displays the pages you can access when a particular function tab is selected.</td>
</tr>
<tr>
<td>Tools bar</td>
<td>Allows you to open the Cisco Prime LMS Portal, access Online help, or find out what CiscoView version is installed.</td>
</tr>
</tbody>
</table>

Setting Up CiscoView Mini-RMON Manager

This section describes how to set up a device for monitoring with CiscoView Mini-RMON Manager. The following topics are provided:

- Configuring a System
- Setting Up Alarm Thresholds
- Setting Up Statistics Collection on Ethernet Ports
- Setting Up Historical Statistics Collection on Ethernet Ports
- Viewing Alarm Events
- Viewing Traffic Statistics
Configuring a System

You can enter general information for the mini-RMON monitored device.

**Step 1** Select **Inventory > Tools > Mini-RMON**.
Or
Select **Monitor > Monitoring Tools > Mini-RMON**.

**Step 2** Select a device from the device selector.

**Step 3** Select **Setup > System**. The System Configuration page appears.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name (sysName)</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Contact (sysContact)</td>
<td>Contact person for this managed node, as well as information on how to contact this person.</td>
</tr>
<tr>
<td>Location (sysLocation)</td>
<td>Physical location of this node.</td>
</tr>
<tr>
<td>RMON</td>
<td>Indicates whether RMON functionality is enabled on this device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> By default, RMON functionality is enabled on Cisco IOS devices. However, this is not the case for Catalyst OS devices. If RMON functionality has not already been enabled on the device you want to monitor, you can enable it here.</td>
</tr>
<tr>
<td>System Uptime (sysUpTime)</td>
<td>Date and time the network management portion of the system was last reinitialized.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You cannot modify this object.</td>
</tr>
</tbody>
</table>

**Step 4** Enter the appropriate information.

**Step 5** Click **Apply**.
Setting Up Alarm Thresholds

To access the Setup Alarm Thresholds page:

**Step 1** Select *Inventory > Tools > Mini-RMON.*

Or

Select *Monitor > Monitoring Tools > Mini-RMON.*

**Step 2** Select a device from the device selector.

**Step 3** Select *Setup > Alarms.*

The Setup Alarm Thresholds page appears. The following table describes the fields displayed in the Setup Alarm Thresholds page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Source</td>
<td>Indicates whether the device, as a whole, or a port on that device is the source of an alarm.</td>
</tr>
<tr>
<td>Alarm Variable (alarmVariable)</td>
<td>Indicates the MIB variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.</td>
</tr>
</tbody>
</table>
| Rising Threshold (alarmRisingThreshold) | A threshold for the sampled statistic. A single event occurs when:  
• The current sampled value is greater than or equal to this threshold, and the last sampled value is less than this threshold.  
• The first sample after this entry becomes valid is greater than or equal to this threshold, and the associated Startup Alarm is equal to:  
  - Rising  
  - Rising or Falling.  
After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the Falling Threshold. |
| Falling Threshold (alarmFallingThreshold) | A threshold for the sampled statistic. A single event occurs when:  
• The current sampled value is less than or equal to this threshold, and the last sampled value is greater than this threshold.  
• The first sample, after this entry becomes valid, is less than or equal to this threshold, and the associated Startup Alarm is equal to:  
  - Rising  
  - Rising or Falling.  
After a falling event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the Rising Threshold. |
Chapter 6  CiscoView Mini-RMON Manager

Setting Up CiscoView Mini-RMON Manager

Creating and Modifying an Alarm

Step 1  Select Inventory > Tools > Mini-RMON.

Or
Select Monitor > Monitoring Tools > Mini-RMON.

Step 2  Select a device from the device selector.

Step 3  Select Setup > Alarms. The Setup Alarm Thresholds page appears.

Step 4  You can do one of the following:
• Click Create to launch the Create Alarm dialog box. The Create an Alarm page appears with the fields listed in Table 6-2.
• Select an alarm threshold and click Modify to launch the Modify Alarm dialog box. The Modify an Alarm page appears with the fields listed in Table 6-2.

This section contains Creating and Modifying an Alarm.

### Creating and Modifying an Alarm

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Action (eventType)</td>
<td>The type of notification that the probe will generate for this event.</td>
</tr>
<tr>
<td></td>
<td>There are four possible values:</td>
</tr>
<tr>
<td></td>
<td>• None: no notifications are generated</td>
</tr>
<tr>
<td></td>
<td>• Log: an entry for each event is added to the log table</td>
</tr>
<tr>
<td></td>
<td>• Trap: a SNMP trap is sent to one or more management stations</td>
</tr>
<tr>
<td></td>
<td>• Log and Trap: both a log entry and SNMP trap are generated</td>
</tr>
<tr>
<td>Current Value (alarmValue)</td>
<td>The value of the statistic during the last sampling period. For example,</td>
</tr>
<tr>
<td></td>
<td>if the sample type is &quot;Delta&quot;, this value will be the difference between</td>
</tr>
<tr>
<td></td>
<td>the samples at the beginning and end of the period. If the sample type</td>
</tr>
<tr>
<td></td>
<td>is &quot;Absolute&quot;, this value will be the sampled value at the end of the</td>
</tr>
<tr>
<td></td>
<td>period. This is the value that is compared with the rising and falling</td>
</tr>
<tr>
<td></td>
<td>thresholds. The value during the current sampling period is not made</td>
</tr>
<tr>
<td></td>
<td>available until the period is completed and will remain available until</td>
</tr>
<tr>
<td></td>
<td>the next period completes.</td>
</tr>
</tbody>
</table>

Step 4  Do one of the following:
• Click Create to launch the Create Alarm dialog box.
• Select an alarm threshold and click Modify to launch the Modify Alarm dialog box.
• Select an alarm threshold and click Delete to remove that threshold from the Alarm Thresholds table.
### Table 6-2 Fields for Create and Modify Alarm Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Source</td>
<td>The source of the alarm you are about to create. Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• System – Select a device from the list.</td>
</tr>
<tr>
<td></td>
<td>• Select a port from the list.</td>
</tr>
<tr>
<td></td>
<td>• Other – Specify a MIB variable and enter the appropriate variable in the MIB Variable field.</td>
</tr>
<tr>
<td>Alarm Variable (alarmVariable)</td>
<td>The MIB variable associated with this alarm. If the variable you want to select is not available in the list:</td>
</tr>
<tr>
<td></td>
<td>1. Select Other from the Alarm Variable list.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the appropriate variable in the MIB Variable field.</td>
</tr>
<tr>
<td>Note</td>
<td>You can sample only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks).</td>
</tr>
<tr>
<td>Rising Threshold (alarmRisingThreshold)</td>
<td>A threshold for the sampled statistic.</td>
</tr>
<tr>
<td></td>
<td>A single event occurs when:</td>
</tr>
<tr>
<td></td>
<td>• The current sampled value is greater than or equal to this threshold, and the last sampled value is less than this threshold.</td>
</tr>
<tr>
<td></td>
<td>• The first sample after this entry becomes valid is greater than or equal to this threshold, and the associated Startup Alarm is equal to:</td>
</tr>
<tr>
<td></td>
<td>– Rising</td>
</tr>
<tr>
<td></td>
<td>– Rising or Falling.</td>
</tr>
<tr>
<td></td>
<td>After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the Falling Threshold.</td>
</tr>
<tr>
<td>Falling Threshold (alarmFallingThreshold)</td>
<td>A threshold for the sampled statistic.</td>
</tr>
<tr>
<td></td>
<td>A single event occurs when:</td>
</tr>
<tr>
<td></td>
<td>• The current sampled value is less than or equal to this threshold, and the last sampled value is greater than this threshold.</td>
</tr>
<tr>
<td></td>
<td>• The first sample, after this entry becomes valid, is less than or equal to this threshold, and the associated Startup Alarm is equal to:</td>
</tr>
<tr>
<td></td>
<td>– Rising</td>
</tr>
<tr>
<td></td>
<td>– Rising or Falling.</td>
</tr>
<tr>
<td></td>
<td>After a falling event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the Rising Threshold.</td>
</tr>
</tbody>
</table>
Setting Up CiscoView Mini-RMON Manager

Chapter 6  CiscoView Mini-RMON Manager

Table 6-2  Fields for Create and Modify Alarm Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling Type</td>
<td>The method used for sampling the selected variable and calculating the value to be compared against the thresholds.</td>
</tr>
<tr>
<td>(alarmSampleType)</td>
<td>If the value of this object is Absolute, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</td>
</tr>
<tr>
<td></td>
<td>If the value of this object is Delta, the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds.</td>
</tr>
<tr>
<td>Sampling Interval</td>
<td>Interval, in seconds, over which the data is sampled and compared with the rising and falling thresholds. The range is from 1 to 2147483647.</td>
</tr>
<tr>
<td>(alarmInterval)</td>
<td>You have to be careful when you set this variable using delta value sampling. The interval should be set short enough so that the sampled variable is unlikely to increase or decrease by more than $2^{31} - 1$ during a single sampling interval.</td>
</tr>
<tr>
<td>Alarm Action (eventType)</td>
<td>Choose the type of notification that the probe will generate for this event from:</td>
</tr>
<tr>
<td></td>
<td>• None – No notifications are generated.</td>
</tr>
<tr>
<td></td>
<td>• Log – An entry for each event is added to the log table.</td>
</tr>
<tr>
<td></td>
<td>• Trap – An SNMP trap is sent to one or more management stations</td>
</tr>
<tr>
<td></td>
<td>• Log and Trap – Both a log entry and SNMP trap are generated</td>
</tr>
<tr>
<td>Trap Community</td>
<td>If an SNMP trap is to be sent, it will be sent to the SNMP community specified by this octet string.</td>
</tr>
<tr>
<td>(eventCommunity)</td>
<td></td>
</tr>
<tr>
<td>Startup Alarm</td>
<td>The alarm that is sent when this entry is first set to valid.</td>
</tr>
<tr>
<td>(alarmStartupAlarm)</td>
<td>If the first sample after this entry becomes valid is greater than or equal to the rising threshold and Startup Alarm is equal to Rising, or Rising or Falling, then a single rising alarm is generated.</td>
</tr>
<tr>
<td></td>
<td>If the first sample after this entry becomes valid is less than or equal to the falling threshold and Startup Alarm is equal to Falling, or Rising or Falling, then a single falling alarm is generated.</td>
</tr>
<tr>
<td>Owner (alarmOwner)</td>
<td>The entity that configured this entry and is using the resources assigned to it.</td>
</tr>
</tbody>
</table>
Setting Up Statistics Collection on Ethernet Ports

From this page, you can specify the Ethernet ports CiscoView Mini-RMON Manager will collect network traffic information for.

**Step 1**
Select the Setup tab and then click **Statistics Collection**.

The Setup Statistics Collection on Ethernet Ports page appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name (ifName)</td>
<td>Name of an Ethernet port.</td>
</tr>
<tr>
<td>Collection Status (etherStatsDataSource)</td>
<td>Indicates whether statistics collection is enabled on a particular port.</td>
</tr>
</tbody>
</table>

**Step 2**
Select a port from the Collection Status on Ethernet Ports table:
- Click **Enable** to enable statistics collection on that port.
- Click **Disable** to disable statistics collection on that port.

Setting Up Historical Statistics Collection on Ethernet Ports

From the Enable History Collection on a Port dialog box, you can specify the settings for the collection of historical traffic statistics. To do this:

**Step 1**
Select the Setup tab and then click **Statistics History**.

The Setup Statistics History Collection on Ethernet Ports page appears.

**Step 2**
Go to the bottom of the page and click **Create** to launch the Enable History Collection on a Port dialog box.

**Step 3**
Select a port from the list and then enter the appropriate information.

See, Table 6-3 for more details.

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

This section contains Enabling or Modifying History Collection on a Port.
Enabling or Modifying History Collection on a Port

To enable, modify, or delete history collection on a port:

**Step 1**  Click the Setup tab. From the Options bar, click **Statistics History**.

**Step 2**  Do one of the following:

- Click **Create**. The Traffic History Collection Enabled Ports table appears. See, Table 6-3 for more details.
  
  Or

- Select a port in the Traffic History Collection Enabled Ports table and click **Modify** to edit any value in the table. The Modify History Control Entry page appears. See, Table 6-3 for more details.

  Or

- Select a port in the Traffic History Collection Enabled Ports table and click **Delete** to remove that port from the Traffic History Collection Enabled Ports table.

*Table 6-3  Fields in Traffic History Collection Enabled Ports Table*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name (ifName)</td>
<td><em>Display Only</em>. Name of an Ethernet port. Select a port from the list. You cannot modify this object.</td>
</tr>
<tr>
<td>Buckets (historyControlBucketsRequested)</td>
<td>Requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. When this object is created or modified, the probe should set historyControlBucketsGranted as closely to this object as is possible for the particular probe implementation and available resources.</td>
</tr>
<tr>
<td>Sampling Interval (historyControlInterval)</td>
<td>Interval, in seconds, over which data is sampled for each bucket in the part of the media-specific table associated with this historyControlEntry. This interval can be set to any number of seconds between 1 and 3,600 (1 hour). Because the counters in a bucket may exceed their maximum value without any indication, an administrator should take into account the possibility of overflow in any of the associated counters. It is important to consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This is usually most important for the &quot;octets&quot; counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization. This object cannot be modified if the associated historyControlStatus object is equal to &quot;valid(1)&quot;.</td>
</tr>
<tr>
<td>Owner (historyControlOwner)</td>
<td><em>Display Only</em>. The entity that configured this entry and is using the resources assigned to it. You cannot modify this object.</td>
</tr>
</tbody>
</table>
Viewing Alarm Events

This section contains the following topics:

- Latest Alarm Events
- Alarm Current Settings
- Alarm Events Log
- Alarm Thresholds

Latest Alarm Events

To view the latest alarm events:

**Step 1**
Click the Alarms tab.

**Step 2**
From the Options bar, click **Latest Alarm Events**. The following information appears:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Time (eventLastTimeSent)</td>
<td>Value of sysUpTime when this entry last generated an event. If this entry has not generated any events, the value of this object is zero.</td>
</tr>
<tr>
<td>Source</td>
<td>Indicates whether the device, as a whole, or a port on that device is the source of an alarm.</td>
</tr>
<tr>
<td>Alarm Variable (alarmVariable)</td>
<td>Indicates the MIB variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.</td>
</tr>
<tr>
<td>Description (eventDescription)</td>
<td>Description of this event entry.</td>
</tr>
<tr>
<td>Event Type (eventType)</td>
<td>The type of notification that the probe will generate for this event.</td>
</tr>
<tr>
<td></td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>- None: no notifications are generated</td>
</tr>
<tr>
<td></td>
<td>- Log: an entry for each event is added to the log table</td>
</tr>
<tr>
<td></td>
<td>- Trap: a SNMP trap is sent to one or more management stations</td>
</tr>
<tr>
<td></td>
<td>- Log and Trap: both a log entry and SNMP trap are generated</td>
</tr>
</tbody>
</table>
Alarm Current Settings

To view the alarm current settings:

Step 1  Select **Inventory > Tools > Mini-RMON**.
Or
Select **Monitor > Monitoring Tools > Mini-RMON**.

Step 2  Select a device from the device selector.

Step 3  Select **Alarms > Latest Alarm Events**.

Step 4  Select an alarm event and click **Associated Alarm**. The following information appears:
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Source</td>
<td><em>Display Only</em>. Indicates whether the device, as a whole, or a port on that device is the source of an alarm.</td>
</tr>
<tr>
<td>Alarm Variable (alarmVariable)</td>
<td><em>Display Only</em>. Indicates the MIB variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.</td>
</tr>
</tbody>
</table>
| Current Value (alarmValue) | The value of the statistic during the last sampling period. For example:  
- If the sample type is Delta, this value will be the difference between the samples at the beginning and end of the period.  
- If the sample type is Absolute, this value will be the sampled value at the end of the period.  
This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes. |
| Rising Threshold (alarmRisingThreshold) | A threshold for the sampled statistic. A single event occurs when:  
- The current sampled value is greater than or equal to this threshold, and the last sampled value is less than this threshold.  
- The first sample after this entry becomes valid is greater than or equal to this threshold, and the associated Startup Alarm is equal to:  
  - Rising  
  - Rising or Falling.  
After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the Falling Threshold. |
| Falling Threshold (alarmFallingThreshold) | A threshold for the sampled statistic. A single event occurs when:  
- The current sampled value is less than or equal to this threshold, and the last sampled value is greater than this threshold.  
- The first sample, after this entry becomes valid, is less than or equal to this threshold, and the associated Startup Alarm is equal to:  
  - Rising  
  - Rising or Falling.  
After a falling event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the Rising Threshold. |
| Sampling Type (alarmSampleType) | The method used for sampling the selected variable and calculating the value to be compared against the thresholds.  
If the value of this object is Absolute, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.  
If the value of this object is Delta, the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds. |
Setting Up CiscoView Mini-RMON Manager

Alarm Events Log

To view the alarm events log:

**Step 1** Select **Inventory > Tools > Mini-RMON**.

Or

Select **Monitor > Monitoring Tools > Mini-RMON**.

**Step 2** Select a device from the device selector.

**Step 3** Select **Alarms > Alarm Events Log**. The following information appears:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Time (logTime)</td>
<td>Value of sysUpTime when this log entry was created.</td>
</tr>
<tr>
<td>Description (eventDescription)</td>
<td>Description of this event entry.</td>
</tr>
</tbody>
</table>
Alarm Thresholds

To view the alarm thresholds to events mapping:

**Step 1**  Select **Inventory > Tools > Mini-RMON**.
Or
Select **Monitor > Monitoring Tools > Mini-RMON**.

**Step 2**  Select a device from the device selector.

**Step 3**  Select **Alarms > Alarm Thresholds to Events Mapping**. The following information appears:
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Source</td>
<td>Indicates whether the device, as a whole, or a port on that device is the source of an alarm.</td>
</tr>
<tr>
<td>Alarm Variable (alarmVariable)</td>
<td>Indicates the MIB variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.</td>
</tr>
</tbody>
</table>
| Rising Threshold (alarmRisingThreshold)    | A threshold for the sampled statistic.                                                                                       

A single event occurs when:
- The current sampled value is greater than or equal to this threshold, and the last sampled value is less than this threshold.
- The first sample after this entry becomes valid is greater than or equal to this threshold, and the associated Startup Alarm is equal to:
  - Rising
  - Rising or Falling.

After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the Falling Threshold.

| Falling Threshold (alarmFallingThreshold)  | A threshold for the sampled statistic.                                                                                      

A single event occurs when:
- The current sampled value is less than or equal to this threshold, and the last sampled value is greater than this threshold.
- The first sample, after this entry becomes valid, is less than or equal to this threshold, and the associated Startup Alarm is equal to:
  - Rising
  - Rising or Falling.

After a falling event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the Rising Threshold.

| Current Value (alarmValue)                 | The value of the statistic during the last sampling period. For example, if the sample type is "Delta", this value will be the difference between the samples at the beginning and end of the period. If the sample type is "Absolute", this value will be the sampled value at the end of the period. |

This value is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes.

| Sampling Type (alarmSampleType)            | The method used for sampling the selected variable and calculating the value to be compared against the thresholds.                                                                                      |

If the value of this object is Absolute, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.

If the value of this object is Delta, the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds.
Alarm Event Log for Selected Alarm Thresholds

To view the alarm event log for selected alarm thresholds:

**Step 1** Select Inventory > Tools > Mini-RMON.
Or
Select Monitor > Monitoring Tools > Mini-RMON.

**Step 2** Select a device from the device selector.

**Step 3** Select Alarms > Alarm Thresholds to Events Mapping.

**Step 4** Select an entry in the Alarm Thresholds table and click Alarm Events. The following information appears:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Time (logTime)</td>
<td>Value of sysUpTime when this log entry was created.</td>
</tr>
<tr>
<td>Source</td>
<td>Indicates whether the device, as a whole, or a port on that device is the source of an alarm.</td>
</tr>
<tr>
<td>Alarm Variable (alarmVariable)</td>
<td>Indicates the MIB variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.</td>
</tr>
<tr>
<td>Description (eventDescription)</td>
<td>Description of this event entry.</td>
</tr>
</tbody>
</table>

Viewing Traffic Statistics

This section contains the following topics:

- Current Traffic Statistics
- Current Traffic Details
- Total Traffic And Utilization
- Errors in Current Traffic Statistics
- Packet Distribution
- Traffic Statistics History
- Details of Traffic History
- Error Details in Traffic History
Current Traffic Statistics

To view the current traffic statistics:

**Step 1**  Select **Inventory > Tools > Mini-RMON**.
Or
Select **Monitor > Monitoring Tools > Mini-RMON**.

**Step 2**  Select a device from the device selector.

**Step 3**  Select **Statistics > Current**. The Current Traffic Statistics page appears with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name (ifName)</td>
<td>Name of the Ethernet port.</td>
</tr>
<tr>
<td>Util %</td>
<td>The etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. In the equation below, the differences in the sampled values are Pkts and Octets, respectively, and the number of seconds in the interval is Interval. These values are used to calculate utilization as follows: utilization = ((deltaPkts * 16) + (deltaOctets * 0.8)) / ((deltaTime * 100) * (speed / 10000000)) The result is the utilization percentage of the Ethernet segment.</td>
</tr>
<tr>
<td>Dropped Events (etherStatsDropEvents)</td>
<td>Total number of events in which packets were dropped by the probe due to a lack of resources during this sampling interval. Note that this number is not necessarily the number of packets dropped – it only indicates the number of times this condition was detected.</td>
</tr>
<tr>
<td>CRC Errors (etherStatsCRCAlignErrors)</td>
<td>Total number of packets received during this sampling interval that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Collisions (etherStatsCollisions)</td>
<td>Best estimate of the total number of collisions that occurred on this Ethernet segment during this sampling interval.</td>
</tr>
</tbody>
</table>

**Step 4**  You can do one of the following:
- Select a port and click **Details** to launch the Current Traffic Details dialog box. See **Current Traffic Details** for more information.
- Select a port and click **Monitor** to launch the Total Traffic & Utilization dialog box. See **Total Traffic And Utilization** for more information.
Current Traffic Details

To view the current traffic details:

**Step 1** Select *Inventory > Tools > Mini-RMON.*

Or

Select *Monitor > Monitoring Tools > Mini-RMON.*

**Step 2** Select a device from the device selector.

**Step 3** Select *Statistics > Current.*

**Step 4** Select a port and click *Details.* The Current Traffic Details page appears with the following fields:
## Chapter 6  CiscoView Mini-RMON Manager

### Setting Up CiscoView Mini-RMON Manager

### Field Description

#### Total Traffic & Utilization

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes (etherStatsOctets)</td>
<td>Total number of data octets (including those in bad packets) received on the network (excluding framing bits but including FCS octets) during this sampling interval.</td>
</tr>
<tr>
<td>Packets (etherStatsPkts)</td>
<td>Total number of packets (including bad packets, broadcast packets, and multicast packets) received during this sampling interval.</td>
</tr>
<tr>
<td>Util %</td>
<td>The etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. In the equation below, the differences in the sampled values are Pkts and Octets, respectively, and the number of seconds in the interval is Interval. These values are used to calculate utilization as follows: $\text{utilization} = \frac{(\text{deltaPkts} \times 16) + (\text{deltaOctets} \times 0.8))}{(\text{deltaTime} \times 100) \times (\text{speed} / 10000000)}$ The result is the utilization percentage of the Ethernet segment.</td>
</tr>
</tbody>
</table>

| Broadcast Packets (etherStatsBroadcastPkts) | Total number of good packets received that were directed to the broadcast address. This does not include multicast packets. |
| Multicast Packets (etherStatsMulticastPkts) | Total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address. |

#### Errors

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropped Events (etherStatsDropEvents)</td>
<td>Total number of events in which packets were dropped by the probe due to a lack of resources during this sampling interval. This number is not necessarily the number of packets dropped – it only indicates the number of times this condition was detected.</td>
</tr>
<tr>
<td>CRC Errors (etherStatsCRCAlignErrors)</td>
<td>Total number of packets received during this sampling interval that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Collisions (etherStatsCollisions)</td>
<td>Estimate of the total number of collisions that occurred on this Ethernet segment during this sampling interval.</td>
</tr>
<tr>
<td>Undersize Packets (etherHistoryUndersizePkts)</td>
<td>Total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits, but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Oversize Packets (etherHistoryOversizePkts)</td>
<td>Total number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits, but including FCS octets), but were otherwise well-formed.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
Fragments (etherHistoryFragments) | Total number of packets received during this sampling interval that were less than 64 octets in length and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Note that it is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.

Jabbers (etherHistoryJabbers) | Total number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

**Packet Distribution**

| 64 Octets (etherStatsPkts64Octets) | Total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits, but including FCS octets). |
| 65 to 127 Octets (etherStatsPkts65to127Octets) | Total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). |
| 128 to 255 Octets (etherStatsPkts128to255Octets) | Total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). |
| 256 to 511 Octets (etherStatsPkts256to511Octets) | Total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). |
| 512 to 1023 Octets (etherStatsPkts512to1023Octets) | Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). |
| 1024 to 1518 Octets (etherStatsPkts1024to1518Octets) | Total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). |

**Total Traffic And Utilization**

To view the current traffic details:

**Step 1** Select **Inventory > Tools > Mini-RMON**.

Or

Select **Monitor > Monitoring Tools > Mini-RMON**.

**Step 2** Select a device from the device selector.

**Step 3** Select **Statistics > Current**.

**Step 4** Select a port and click **Monitor** to launch the Total Traffic & Utilization dialog box.
Step 5  Select **Total Traffic & Utilization** from the Category list. The Current Traffic Details page appears. For detailed explanation of the fields in the charts see **Total Traffic & Utilization**.

Step 6  You can enable the automatic refresh of this dialog box.

- Select the Refresh Rate check box.
- Select the refresh interval. The range is from 5 to 100 seconds.
- Click **OK**.

---

### Errors in Current Traffic Statistics

To view the errors in the current traffic details:

Step 1  Select **Inventory > Tools > Mini-RMON**.

Or
Select **Monitor > Monitoring Tools > Mini-RMON**.

Step 2  Select a device from the device selector.

Step 3  Select **Statistics > Current**.

Step 4  Select a port and click **Monitor** to launch the Total Traffic & Utilization dialog box.

Step 5  Select **Errors** from the Category list. The Current Traffic Details page appears. For detailed explanation of the fields in the charts see **Errors**.

Step 6  You can enable the automatic refresh of this dialog box.

- Select the Refresh Rate check box.
- Select the refresh interval. The range is from 5 to 100 seconds.
- Click **OK**.

---

### Packet Distribution

To view the packet distribution in the current traffic details:

Step 1  Select **Inventory > Tools > Mini-RMON**.

Or
Select **Monitor > Monitoring Tools > Mini-RMON**.

Step 2  Select a device from the device selector.

Step 3  Select **Statistics > Current**.

Step 4  Select a port and click **Monitor** to launch the Total Traffic & Utilization dialog box.

Step 5  Select **Packet Distribution** from the Category list. The Current Traffic Details page appears. For detailed explanation of the fields in the charts see **Packet Distribution**.
Step 6 You can enable the automatic refresh of this dialog box.

- Select the Refresh Rate check box.
- Select the refresh interval. The range is from 5 to 100 seconds.
- Click OK.

Traffic Statistics History

To view the error details in Traffic History:

Step 1 Select Inventory > Tools > Mini-RMON.

Or
Select Monitor > Monitoring Tools > Mini-RMON.

Step 2 Select a device from the device selector.

Step 3 Select Statistics > History.

Step 4 Select a port in the Traffic History Collection Enabled Ports table and click Traffic History. The Traffic History page appears with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name (ifName)</td>
<td>Name of the selected Ethernet port.</td>
</tr>
<tr>
<td>Sampling Interval (historyControlInterval)</td>
<td>Interval, in seconds, over which data is sampled for each bucket in the part of the media-specific table associated with this historyControlEntry. This interval can be set to any number of seconds between 1 and 3,600 (1 hour). Because the counters in a bucket may exceed their maximum value without any indication, an administrator should take into account the possibility of overflow in any of the associated counters. It is important to consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This is usually most important for the &quot;octets&quot; counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization. This object cannot be modified if the associated historyControlStatus object is equal to valid(1).</td>
</tr>
<tr>
<td>Owner (historyControlOwner)</td>
<td>The entity that configured this entry and is using the resources assigned to it.</td>
</tr>
</tbody>
</table>
Details of Traffic History

To view the error details in Traffic History:

**Step 1**
Select Inventory > Tools > Mini-RMON.

Or
Select Monitor > Monitoring Tools > Mini-RMON.

**Step 2**
Select a device from the device selector.

**Step 3**
Select Statistics > History.

**Step 4**
Select a port in the Traffic History Collection Enabled Ports table and click Traffic History.

**Step 5**
Select Traffic Details from the Category drop-down list. The Traffic Details page appears with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval Start Time (etherHistoryIntervalStart)</td>
<td>Value of sysUpTime at the start of this sampling interval. If the probe keeps track of the time of day, then it should start the first sample as soon as the next hour begins. This may require the probe to delay the collection of the history's first sample, as each sample must be of the same interval. The sample currently collected is not accessible in this table until the end of its interval.</td>
</tr>
<tr>
<td>Util % (etherHistoryUtilization)</td>
<td>Estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.</td>
</tr>
<tr>
<td>Total Packets (etherHistoryPkts)</td>
<td>Total number of packets (including bad packets, broadcast packets, and multicast packets) received during this sampling interval.</td>
</tr>
<tr>
<td>Total Octets (etherHistoryOctets)</td>
<td>Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Broadcasts (etherHistoryBroadcastPkts)</td>
<td>Total number of good packets received during this sampling interval that were directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Multicasts (etherHistoryMulticastPkts)</td>
<td>Total number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
</tbody>
</table>

**Step 6**
You can enable the automatic refresh of this dialog box.

- Select the Refresh Rate check box.
- Select the refresh interval. The range is from 5 to 100 seconds.
- Click **OK**.
Error Details in Traffic History

To view the error details in Traffic History:

**Step 1**  
Select **Inventory > Tools > Mini-RMON.**  
Or  
Select **Monitor > Monitoring Tools > Mini-RMON.**

**Step 2**  
Select a device from the device selector.

**Step 3**  
Select **Statistics > History.**

**Step 4**  
Select a port in the Traffic History Collection Enabled Ports table and click **Traffic History.**

**Step 5**  
Select **Error Details** from the Category drop-down list. The Error Details page appears with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Interval Start Time (etherHistoryIntervalStart) | Value of sysUpTime at the start of this sampling interval.  
If the probe keeps track of the time of day, then it should start the first sample as soon as the next hour begins. This may require the probe to delay the collection of the history's first sample, as each sample must be of the same interval.  
The sample currently collected is not accessible in this table until the end of its interval. |
| Dropped Events (etherHistoryDropEvents)    | Total number of events in which packets were dropped by the probe due to a lack of resources during this sampling interval.  
This number is not the number of packets dropped; it only indicates the number of times this condition was detected. |
| CRC Errors (etherHistoryCRCAlignErrors)    | Total number of packets received during this sampling interval that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| Collisions (etherHistoryCollisions)        | Estimate of the total number of collisions that occurred on this Ethernet segment during this sampling interval. |
| Undersize Pkts (etherHistoryUndersizePkts) | Total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits, but including FCS octets) and were otherwise well formed. |
| Oversize Pkts (etherHistoryOversizePkts)   | Total number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits, but including FCS octets), but were otherwise well-formed. |
### Setting Up CiscoView Mini-RMON Manager

**Step 6** You can enable the automatic refresh of this dialog box.

- Select the **Refresh Rate** check box.
- Select the refresh interval. The range is from 5 to 100 seconds.
- Click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragments (etherHistoryFragments)</td>
<td>Total number of packets received during this sampling interval that were less than 64 octets in length and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.</td>
</tr>
<tr>
<td>Jabbers (etherHistoryJabbers)</td>
<td>Total number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).</td>
</tr>
</tbody>
</table>
Inventory Tools

You can use tools like CiscoView, Mini-RMON, SmartCase.
For details on Inventory tools see:
- CiscoView
- CiscoView Mini-RMON Manager
- SmartCase. See, Working With SmartCase for more information.

Working With SmartCase

SmartCase lets you access Cisco.com to open a Cisco.com case or to query and update an existing case. You can submit, review, and update problems or questions about your Cisco products.
SmartCase allows you to Open/Query or Update a case on Cisco.com by launching the Cisco.com Service Request Tool from Resource Manager Essentials.

To launch Cisco.com Service Request Tool:

**Step 1**  Select **Inventory > Tools > SmartCase**.
The Open/Query or Update a Case page appears.

**Step 2**  Click the link provided to launch the Cisco.com Service Request Tool to Open/Query or Update a Case.
The SmartCase.properties file is located at

```
NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\cctool\scase
```

The properties file contains the URL used to launch Cisco.com Service Request Tool. If at any time there is a change in this URL, you must go to the properties file and update the URL.

**Step 3**  Enter your Cisco.com username and password.
This section has the following sections:

- Using Discovery Features Through CLI
- Using DCR Features Through CLI

### Using Discovery Features Through CLI

You can use DiscoveryCli command line utility to:

- Start Device Discovery
- Stop Device Discovery
- View the current status of Device Discovery

You should configure the Device Discovery settings in the user interface to run Device Discovery. See Discovering Devices for more information.

You should have Network Administrator privileges to use DiscoveryCli command line utility.

See Starting, Stopping, and Viewing Device Discovery Through CLI for more information.

### Starting, Stopping, and Viewing Device Discovery Through CLI

To start, stop, and view Device Discovery through CLI:

**Step 1**
Go to `NMSROOT/bin`

**Step 2**
Do one of the following:
- To start:
  - Enter `DiscoveryCli -u CiscoWorks_Username -p CiscoWorks_Password start`

You can optionally enter the CiscoWorks login password in the command line.

Even if you do not enter the password in the command line, the system prompts you to enter the it.

We recommend you to enter the CiscoWorks password when the system prompts for it. This is because the CiscoWorks password entered at the command line is in clear text form.

Example: `DiscoveryCli -u admin -p admin start`. 
Using DCR Features Through CLI

Using Command Line Interface, you can add, delete, and modify devices, and change the DCR modes. You can also view the list of attributes that can be stored in DCR, and view the current DCR mode. The dcrcli provided with LMS helps you perform these tasks using CLI.

The Device Name and the Host Name/Domain Name combination must be unique for each device in DCR. A device will be considered duplicate if:

- The Device Name of a device is the same as that of any other device
- The Host Name/Domain Name combination of a device is the same as that of any other device
- Auto Update Device ID is the same as that of any other device (in case of AUS managed device)
- Cluster and Member Number, together is same as that of any other device (in case of Cluster managed device)

dcrcli operates in both the Shell and Batch modes. The Shell mode is interactive whereas the Batch mode runs the specified command and exits to the prompt after the command is run.

You can set DCRCLIFILE environment to point to the file where LMS password is present. If you set DCRCLIFILE variable, password will not be asked when you run dcrcli in shell or batch mode.

The password file should contain an entry in the format username password. Make sure that there is only one blank space between the username and the password in the password file. For example, if admin is the username and the password for the Cisco Prime user, the password file must contain the following entry:

admin admin

This section has the following:

- Adding Devices Using CLI
- Deleting Devices Using CLI
- Editing Devices Using CLI
- Listing the Attributes
- Listing the Device IDs

• To stop:
  - Enter `DiscoveryCli -u CiscoWorks_Username -p CiscoWorks_Password stop`
  
  You can optionally enter the CiscoWorks login username and password in the command line. If you do not enter them in the command line, the system prompts you to enter the username and password to run the command.

  Example: `DiscoveryCli -u admin -p admin stop`.

• To view:
  - Enter `DiscoveryCli -u CiscoWorks_Username -p CiscoWorks_Password status`
  
  You can optionally enter the CiscoWorks login username and password in the command line. If you do not enter them in the command line, the system prompts you to enter the username and password to run the command.

  Example: `DiscoveryCli -u admin -p admin status`. 

Using DCR Features Through CLI
- Import Devices Using CLI
- Export Devices Using CLI

**Adding Devices Using CLI**

You can devices using `dcrcli` in:
- Shell mode. See *Adding Devices Using dcrcli in Shell Mode*
- Batch mode. See *Adding Devices Using dcrcli in Batch Mode*

**Adding Devices Using dcrcli in Shell Mode**

To add devices using `dcrcli` in Shell mode:

**Step 1** Enter `NMSROOT/bin/dcrcli -u username`.

**Step 2** Enter the password corresponding to the username. If you have set DCRCLIFILE environment, you will not be prompted for the password.

**Step 3** Enter `add -useDefault=value ip=value hn=value di=value dn=value -a attname=value`

**Step 4** Enter `-useDefault=value` in the command line, if you want to add devices with the default credentials in DCR. Otherwise specifying `-useDefault` is optional.

You should enter `-useDefault=Default_Credential_Set_Name` to add the devices with the default credentials defined in the default credential set `Default_Credential_Set_Name`.

*Default_Credential_Set_Name* denotes the name of the default credential set.

See *Listing the Default Credential Sets* in *Administration Guide for Cisco Prime LAN Management Solution 4.2* for details.

To add devices in DCR with the default credentials as defined by default credential sets policies, you should enter `-useDefault=policy configuration` in the command line.

If there are no policies configured or the credential set does not exist, then the devices will be added in DCR without any credentials.

**Step 5** Enter any of the following:
- IP Address (`ip`)
- Hostname (`hn`)
- Device Identity (`di`)

**Step 6** Enter the Device Name (`dn`) and the Attribute name (`-a attname`). You can add multiple attributes.

Examples:

```
add -useDefault=Set1 ip=1.1.1.1 hn=device1 dn=cisco.com -a sysObjectID=1.3.6.1.4.1.9.1.6
add -useDefault=policy configuration ip=1.1.1.1 hn=device1 dn=cisco.com
-`a sysObjectID=1.3.6.1.4.1.9.1.6`
```

**Note** Enter sysObjectID attribute with `-a` option, while adding device using dcrcli.
Adding Devices Using dcrcli in Batch Mode

To add devices using dcrcli in Batch mode:

**Step 1**
Go to NMSROOT/bin

**Step 2**
Enter dcrcli -u Username cmd=add -useDefault=value ip=value hn=value di=value dn=value -a attname=value

Example: dcrcli -u admin cmd=add -useDefault=policy configuration ip=1.1.1.1 hn=device1 dn=router1 -a sysObjectID=1.3.6.1.4.1.9.1.6

Deleting Devices Using CLI

To delete devices using dcrcli in Shell mode:

**Step 1**
Enter NMSROOT/bin/dcrcli -u username.

**Step 2**
Enter the password corresponding to the username.

**Step 3**
Enter del -f id=value hn=value di=value dn=value fn=value

Enter either one of the following:
- Device ID (id)
- Device Name (dn)
- Hostname (hn) and Domain Name (di).
  
  If the domain name is empty, you should enter di=none.
- Filename (fn) containing the devices to delete.
  
  The CSV file should be in CSV 3.0 format. See Sample CSV Files and XML Files for sample CSV files to delete the devices.
  
  You should specify one or more unique attributes to identify a device in the input CSV file. The unique identifiers are Hostname and Domain Name combination, and Device Name.

Enter -f in the command line to delete all the devices including the devices managed by applications. This is optional.

For example, enter del id=54340 to delete a device whose device ID is 54340.

Suppose if you want to delete a device whose hostname is host1, enter del hn=host1 di=none

To delete device using dcrcli in Batch mode:

**Step 1**
Go to NMSROOT/bin

**Step 2**
Enter dcrcli -u Username -f id=value hn=value di=value dn=value fn=value

Example: dcrcli -u admin cmd=del id=54340
### Editing Devices Using CLI

To modify devices using `dcrcli` in Shell mode:

**Step 1**
Enter `NMSROOT/bin/dcrcli -u username`.

**Step 2**
Enter the password.

**Step 3**
Enter `mod -useDefault=value -misCred id=value ip=value hn=value di=value dn=value -a attname=value`.

**Step 4**
Enter `-useDefault=value` in the command line, if you want to modify device credentials in DCR with the default credentials specified in a default credential set or default credential set policies. Otherwise specifying `-useDefault` is optional.

You should enter `-useDefault=Default_Credential_Set_Name` to add the devices with the default credentials defined in the default credential set Default_Credential_Set_Name.

*Default_Credential_Set_Name* denotes the name of the default credential set.

See [Listing the Default Credential Sets in Administration Guide for Cisco Prime LAN Management Solution 4.2](#) for details.

If you want to modify devices in DCR with the default credentials as defined by default credential sets policies, you should enter `-useDefault=policy configuration` in the command line.

**Step 5**
Enter `-misCred` to retain the existing device credentials in DCR and apply the credential value defined in the default credentials for only missing or empty credentials.

You should enter `-misCred` in the command line only when you have entered `-useDefault=value` in the command line.

Specifying `-misCred` is optional.

If you do not specify `-misCred`, the existing device credentials in DCR will be overwritten with the credentials mentioned in the default credential set.

**Step 6**
Enter the Device ID (`id`).

**Step 7**
Enter either the IP Address (`ip`), Hostname (`hn`), or Device Identity (`di`).

**Step 8**
Enter the Device Name (`dn`) and the Attribute name (`-a attname`). You can add multiple attributes.

Example: `mod -useDefault=policy configuration -misCred id=54341 ip=2.2.2.2 dn=cisco.com -a display_name=new_name`

To modify devices using `dcrcli` in Batch mode:

**Step 1**
Go to `NMSROOT/bin`.

**Step 2**
Enter `dcrcli -u Username cmd=mod id=value hn=value di=value dn=value -a attname=value`

For example, to change IP Address and device name, enter:

```
dcrcli -u admin cmd=mod -useDefault=set1-misCred id=77 ip=4.4.4.4 dn=new_display_name
```
Listing the Attributes

To view the list of all attributes in Shell mode:

Step 1 Enter NMSROOT/bin/dcrcli -u username.
Step 2 Enter the password corresponding to the username
Step 3 Enter lsattr
   This lists Attribute Name, Attribute Description, and Attribute Type.
   Attribute Type is a constant that identifies an Attribute Name. For example, Attribute Type 1072 identifies the attribute name display_name.

To view the list of all attributes in Batch mode:

Step 1 Go to NMSROOT/bin
Step 2 Enter dcrcli -u Username cmd=lsattr

Listing the Device IDs

To view the list of device IDs of all devices in DCR in Shell mode:

Step 1 Enter NMSROOT/bin/dcrcli -u username.
Step 2 Enter the password corresponding to the username
Step 3 Enter lsids all dn=value ip=value.
   Enter either all or device name (dn) or IP Address (ip).
   Enter all in the command line to display the device IDs of all devices in DCR. Enter device name (dn) or IP Address (ip) to display the IDs of devices matching the value.

To view the list of all attributes in Batch mode:

Step 1 Go to NMSROOT/bin
Step 2 Enter dcrcli -u Username cmd=lsids all dn=value ip=value
Import Devices Using CLI

You can import using the Command Line Interface (Shell Mode).

Step 1
Enter `NMSROOT/bin/dcrcli -u username`.

Step 2
Enter the password corresponding to the username.

- To import from file:

  Enter `impFile -useDefault=value fn=file name ft=file type cr=conflict resolution option`

  `-useDefault`—Denotes that the default credentials defined in a default credential set or default credential set policies will be used if the import source does not have the required device credentials information.

  The value of `-useDefault` could be `policy configuration` or a default credential set name. This command line argument is optional.

  If there are no policies configured or the credential set does not exist, then the devices will be added in DCR without any credentials.

  See `Listing the Default Credential Sets` in Administration Guide for Cisco Prime LAN Management Solution 4.2 for details.

  For example, if the default credential set has Standard and SNMP credentials and if your import source has only the Standard credentials, the device will be populated in DCR with the Standard credentials entered in your import source and SNMP credentials configured in the default credential set.

  `fn`—File name

  `ft`—File type; CSV and XML are the valid values.

  `cr`—Conflict resolution option. `dcr` and `file` are the valid values. This option is not mandatory. If value is not specified, `dcr` is taken as default.

  Example:

  impFile -useDefault=policy configuration fn=/opt/CSCOpx/test.csv ft=csv

- To import from Local NMS:

  Enter `impNms -useDefault=value nt=NMS type il=Installation location cr=conflict resolution option`

  `-useDefault`—Denotes that the default credentials defined in a default credential set or default credential set policies will be used if the import source does not have the required device credentials information.

  The value of `-useDefault` could be `policy configuration` or a default credential set name. This command line argument is optional.
Using DCR Features Through CLI

See Listing the Default Credential Sets in Administration Guide for Cisco Prime LAN Management Solution 4.2 for details.

If there are no policies configured or the credential set does not exist, then the devices will be added in DCR without any credentials.

\( nt \)— NMS type. Valid values are HPOV and Netview. See Installing and Data Migration With Cisco Prime LAN Management Solution 4.2 for information on supported Network Management Systems.

\( il \) — Installation location of the NMS

Examples:

- `impNms -useDefault=policy configuration nt=HPOV il=/opt/OV` (on Solaris and Soft Appliance)
- `impNms -useDefault=set1 nt=HPOV il=C:\Program Files\HP OpenView` (on Windows)
- `impNms -useDefault=policy configuration nt=Netview il=/usr/OV` (on Solaris and Soft Appliance)
- `impNms -useDefault=set1 nt=Netview il=C:\usr\OV` (on Windows)

To import from Remote NMS:

Enter `impRNms -useDefault=value nt=NMS type hn=hostname un=Remote UserName il=Installation location ot=OS Type cr=conflict resolution option`

- `useDefault`— Denotes that the default credentials defined in a default credential set or default credential set policies will be used if the import source does not have the required device credentials information.

The value of `useDefault` could be `policy configuration` or a default credential set name. This command line argument is optional.

See Listing the Default Credential Sets in Administration Guide for Cisco Prime LAN Management Solution 4.2 for details.

If there are no policies configured or the credential set does not exist, then the devices will be added in DCR without any credentials.

\( nt \) — NMS type. Valid values are HPOV and Netview. See Installing and Data Migration With Cisco Prime LAN Management Solution 4.2 for information on supported Network Management Systems.

\( hn \) — Remote Hostname or IP Address

\( un \) — Remote Username

\( il \) — Installation location of the NMS

\( ot \) — OS Type; Valid values are HPUX, AIX, or SOL

\( cr \) — Conflict resolution option. `dcr` and `file` are the valid values. This option is not mandatory. If value is not specified, `dcr` is taken as default.

The .rhosts file should be modified to allow this user to login to NMS Server without any password.

Examples:

- `impRNms -useDefault=policy configuration nt=HPOV hn=1.2.3.4 un=root il=/opt/OV ot=SOL`
- `impRNms -useDefault=set1 nt=Netview hn=1.2.3.4 un=root il=/usr/OV ot=SOL`
To import from ACS:

In ACS mode, a device with valid IP Address only will be imported to DCR. If a device has IP Address of the form 10.10.1.*, in ACS, then it will not be imported.

Enter `impACS -useDefault=Value | Policy Configuration ot=OS Type hn=ACS Server Name or IP Address un=ACS admin username pwd=ACS admin password prt=port number proto=Protocol cr=conflict resolution option gr=Import devices along with group

- `useDefault`—Denotes that the default credentials defined in a default credential set or default credential set policies will be used if the import source does not have the required device credentials information.
  
  The value of `-useDefault` could be `policy configuration` or a default credential set name. This command line argument is optional.

  See Listing the Default Credential Sets in Administration Guide for Cisco Prime LAN Management Solution 4.2 for details.

  If there are no policies configured or the credential set does not exist, then the devices will be added in DCR without any credentials.

- `ot`—Operating System Type
- `hn`—ACS Server Name or IP Address
- `un`—ACS admin username
- `pwd`—ACS admin password
- `prt`—Port number. Default is 2002.
- `proto`—Protocol type. Valid values are http and https.
- `cr`—Conflict resolution option. `dcr` and `file` are the valid values. This option is not mandatory. If value is not specified, `dcr` is taken as default.
- `gr`—Import devices along with group from ACS.

Example:

```bash
impAcs -useDefault=policy configuration ot=WIN2K hn=1.2.3.4 un=acsadmin pwd=acspwd prt=2002 proto=http
```

The option `cr` is used to prioritize the selection and resolve conflicts during import. If `dcr` is specified as conflict resolution option, credentials for the device, stored in DCR will be used.

This is taken as default if `cr` is not specified. If import source (file or Nms or RNms or ACS) is specified as conflict resolution option, credentials from the import source will be used, and credentials in DCR will be modified.
You can also import using the Command Line Interface (Batch Mode):

To import from file:

**Step 1**  
Go to `NMSROOT/bin`

**Step 2**  
Enter `dcrcli -u Username cmd=impFile -useDefault=value fn=file name ft=file type cr=conflict resolution option`  

To import from Local NMS:

**Step 1**  
Go to `NMSROOT/bin`

**Step 2**  
Enter `dcrcli -u Username cmd=impNms -useDefault=value nt=NMS type il=Installation location cr=conflict resolution`  

To import from Remote NMS:

**Step 1**  
Go to `NMSROOT/bin`

**Step 2**  
Enter `dcrcli -u Username cmd=impRNms -useDefault=value nt=NMS type hn=hostname un=Remote Username cr=conflict resolution`  

To import from ACS:

**Step 1**  
Go to `NMSROOT/bin`

**Step 2**  
Enter `dcrcli -u Username cmd=impAcs -useDefault=value Policy Configuration ot=OS Type hn=ACS Server Name or IP Address un=ACS admin username pwd=ACS admin password prt=port number proto=protocol cr=conflict resolution gr=Import devices along with group`
Export Devices Using CLI

You have the option to export using Command Line Interface.

**Step 1** Enter `NMSROOT/bin/dcrcli -u username`.

**Step 2** Enter the password corresponding to the username.

**Step 3** Enter `exp -expCred fn=filename ft=filetype`.
For `filetype`, CSV or XML are valid values.

You can edit the Export Format file `Export_Format_CSV.xml` or `Export_Format_XML.xml` to specify the credentials.

**Step 4** Enter `-expCred` to export the devices with their attributes and credentials.
If you specify `-expCred`, only the device attributes are exported to the specified output file.

For example,
```
exp -expCred fn=/opt/CSCOpx/test.csv ft=csv
```

Export to ACS Server Using CLI

You have the option to export the devices from DCR to the specified ACS Server using command line interface in Shell mode.

**Step 1** Enter `NMSROOT/bin/dcrcli -u username`.

**Step 2** Enter the password corresponding to the username.

**Step 3** Enter `expAcs hn=value un=value pwd=value prt=value proto=value seckey=value ndg=value fn=value`.
where,
- `hn` — ACS Server Name or IP Address.
- `un` — ACS admin username.
- `pwd` — ACS admin password.
- `prt` — ACS administrative port number.
- `seckey` — ACS Shared Secret Key.
- `ndg` — Network Device Group in ACS.
- `fn` — File Name.

If you do not specify the file name, only unauthorised devices will be exported to the specified ACS server.
To export using Batch mode:

**Step 1**  Go to `NMSROOT/bin`

**Step 2**  Enter `dcrcli -a Username cmd=exp -expCred fn=filename ft=filetype`
Frequently Asked Questions

The following section lists the Frequently Asked Questions (FAQs) of Inventory Management in LMS 4.0:

- Device Discovery FAQ
- Device Management FAQ

Device Discovery FAQ

The following are the FAQs on Device Management:

- Does Device Discovery supports SNMPv1?
- Why the CSDiscovery process is taking longer time to complete?
- What is the meaning of different discovery percentages?
- How can I troubleshoot device discovery stuck at 10%?
- How can I troubleshoot device discovery stuck at 40%?
- How can I troubleshoot device discovery stuck at 90%?

Q. Does Device Discovery supports SNMPv1?
A. No. Device Discovery supports only SNMPv2c and SNMPv3.

Q. Why the CSDiscovery process is taking longer time to complete?
A. This could be because of the following reasons

<table>
<thead>
<tr>
<th>Possible Reason</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCR may have more than 5,000 devices and you might have selected Use DCR As Seed List option for Device Discovery.</td>
<td>Disable the Use DCR As Seed List option and run Device Discovery.</td>
</tr>
<tr>
<td>Debugging option may have been enabled.</td>
<td>Disable Debugging</td>
</tr>
<tr>
<td>Subnet mask vale may be large for Discovery based on Ping Sweep on IP Range.</td>
<td>Enter a smaller value for subnet mask and run Device Discovery.</td>
</tr>
</tbody>
</table>
Q. What is the meaning of different discovery percentages?
A. The following list explains the different discovery percentages:
   - 10% — Startup, where devices have not been handed over to incharge processes yet
   - 40% — Devices have been successfully handed over to incharge processes
   - 70% — Incharge processes have successfully discovered devices and handed the information over to Cisco code
   - 90% — Discovered devices must be placed in appropriate groups. Device information has been sent to OGS and group information from OGS is awaited. From DFM 3.0, this scenario is not available.

Q. How can I troubleshoot device discovery stuck at 10%?
A. If device discovery is stuck at 10%, it means that devices to be discovered have not been communicated to Incharge processes yet. To troubleshoot device discovery stuck at 10%:
   - On Solaris and Soft Appliance:

<table>
<thead>
<tr>
<th>Possible Reason</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP timeout or retries values may be large</td>
<td>Enter a smaller value for ICMP timeout and ICMP retry, and run Device Discovery</td>
</tr>
<tr>
<td>You might have entered a large value for SNMP timeouts or SNMP retries.</td>
<td>Enter a smaller value for SNMP timeout and SNMP retry, and run Device Discovery</td>
</tr>
</tbody>
</table>

**Possible Reason**

**ICMP timeout or retries values may be large**

Enter a smaller value for ICMP timeout and ICMP retry, and run Device Discovery

**You might have entered a large value for SNMP timeouts or SNMP retries.**

Enter a smaller value for SNMP timeout and SNMP retry, and run Device Discovery

---

**Step 1**

Enter the `pdshow` command to check if DfmServer and DfmBroker processes are running.

**Step 2**

Check if there are multiple instances of brstart and sm_server.

The name of binary for DfmBroker is brstart and for DfmServer, it is sm_server.

**Step 3**

Enter the following commandline:

- `/usr/ucb/ps -auxww | grep brstart`
- `/usr/ucb/ps -auxww | grep sm_server`

For example:

```
marver-sol-daily# /usr/ucb/ps -auxww | grep brstart
root 11751 0.1 0.1 984 648 pts/7 S 11:34:49 0:00 grep brstart
```

If you see more than one instance of each process, enter the command `ptree` to get all related process.

For example:

```
marver-sol-daily# ptree 11577
11461 /opt/CSCOpx/objects/dmgt/dmgtd.sol
11577 brstart --output --port=9002 ---user=casuser
11588 /opt/CSCOpx/objects/smarts/bin/system/sm_logerror 131
11604 /opt/CSCOpx/objects/smarts/bin/system/sm_authority
11605 /opt/CSCOpx/objects/smarts/bin/system/sm_logerror 136
```

**Step 4**

 Except for dmgtd.sol, manually terminate all processes found in the `ptree` command by entering the command `kill -9`.
Step 5  Stop the daemon manager by entering `net stop crmdmgtd`.
       Wait for five minutes.

Step 6  Enter `netstat -a | grep 9002` to make sure that port 9002 is not in listening state or timed wait state.

Step 7  Enter `netstat -a | grep 435` to make sure that ports 43501 to port 43508 are not in listening or timed wait state.

If the ports are in listening state, use the Unix utility to find the process that owns the ports and terminate that process.

Step 8  Start the daemon manager by entering `net start crmdmgtd`.

Step 9  Enter the following command: `/objects/smarts/bin/brcontrol`
       The following is an example of the output:
       Broker is located at: localhost:9002 Started: Oct 26 09:42:39 2005
       Domain Host Name Port Proc ID State Last Chg Time
       DFM marver-sol-daily 50449 11589 RUNNING Oct 26 09:42:58 2005

Step 10 Check whether the displayed host name is the host name in DNS or /etc/hosts

- On Windows:

Step 1  Download the tools from the following location: http://www.sysinternals.com/Utilities/PsTools.html

Step 2  Unzip it into a directory.

Step 3  Enter `pdshow DfmServer pdshow DfmBroker` to check whether the processes DfmServer and DfmBroker are running.

Step 4  Enter `/objects/smarts/bin/brcontrol`

Step 5  Check whether the host name is the same as in DNS.

Step 6  Check whether there are multiple instances of brstart and sm_server
       You can use the downloaded Pstool to see one branch each of brstart and sm_serve.
       For example:

       pslist -t
       brstart 5708 8 1 16 8476 1104 264
       brstart 5880 8 7 86 32720 11240 9664
       sm_authority 6452 8 1 52 14376 3616 1528
       sm_server 6332 8 1 16 8476 1104 264
       sm_server 6416 8 124 678 212696 58784 56812
       sm_authority 6444 8 1 47 14376 3572 1528

       There should be only one branch. You need to terminate any extra branches.
Appendix B
Frequently Asked Questions

Device Discovery FAQ

Step 7 Stop the daemon manager by entering `net stop crmdmgtd`.
Wait for five minutes.

Step 8 Enter `netstat -a -n -p tcp` to make sure that ports 9002 and 43501 to 43508 are not in listening state or timed wait state.

Step 9 Start the daemon manager by entering `net start crmdmgtd`.

Q. How can I troubleshoot device discovery stuck at 40%?
A. To troubleshoot device discovery stuck at 40%:

Step 1 Make sure that the device under question is responding to ping messages.

Step 2 Make sure that the device responds to snmpwalk by entering:

```
/objects/smarts/bin/sm_snmp -c --dest= walk
```

Step 3 Enable discovery logging in incharge process by entering:

```
/objects/smarts/bin/dmctl -s DFM
```

Note In some cases, you need to enter your UserID and Password.

Step 4 From dmctl prompt, enter:

```
ICF_TopologyManager::ICF-TopologyManager::DebugEnabled TRUE
```

Step 5 Exit out of dmctl

Step 6 Trigger the rediscovery of the device
The log file from the location `/objects/smarts/local/logs/DFM.log` will have discovery information in detail. It will provide the root cause for the failing device discovery.

Step 7 Restore debug to False.

Q. How can I troubleshoot device discovery stuck at 90%?
A. To troubleshoot devices stuck at 90% discovery:

Step 1 Increase the log level for Inventory Service to debug.

Step 2 Stop the daemon manager by entering `net stop crmdmgtd`

Step 3 Take a backup of the following file:

```
/MDC/tomcat/webapps/triveni/WEB-INF/classes/log4j-ogs.properties
```

Step 4 Replace the string FATAL by string DEBUG
Step 5  Start the daemon manager by entering `net start crmdgtd`.

Step 6  Collect the contents of `/log/dfmLogs/TIS` file by entering:
- On Solaris and Soft Appliance:
  
  `/var/adm/CSCIpx/log/DFMServer.log`
- On Windows:
  
  `/log/DFMServer.log`

**Q.** How can I perform rediscovery of devices in LMS through CLI?

**A.** To perform a rediscovery of:

- All devices:
  
  Enter `dmctl -s DFM invoke ICF_TopologyManager::ICF-TopologyManager discoverAll`
- A specific device:
  
  Enter `dmctl -s DFM invoke ICF_TopologyManager::ICF-TopologyManager ::`

---

**Device Management FAQ**

The following are the FAQs on Device Management:

- Why does the Device selector not appear in the Device administration page?
- What is the maximum number of devices that can be imported to the DCR?
- How to import devices whose sysObjectIds are not known before the Import operation?
- Sometimes, when the data is restored on Master machine the Slave does not receive any events. What should I do?
- Where can I find the DCR log files?
- Why am I getting an Access Denied error while performing Import from Remote NMS?
- How do I include a special character such as comma as part of SNMP Read-Only string in a CSV file?

**Q.** Why does the Device selector not appear in the Device administration page?

**A.** Ensure that CMFOGSServer process is running correctly. If you had invoked the browser soon after starting the Daemon Manager, try closing the browser and invoking Cisco Prime again.

If the browser window is closed without logging out properly, the user cache may not be cleared and the task-to-role mapping may not be synchronized.

**Q.** What is the maximum number of devices that can be imported to the DCR?

**A.** You can add up to 50,000 devices in DCR.

**Q.** How to import devices whose sysObjectIds are not known before the Import operation?

**A.** SysObjectIDs are not mandated for Bulk Import operation. You can leave the field empty or specify `sysObjectID` as `UNKNOWN`, and then perform Import. See Importing Devices and Credentials for more information.
Q. Sometimes, when the data is restored on Master machine the Slave does not receive any events. What should I do?
A. You can try changing the DCR mode of the Slave machine to Standalone and wait for few minutes. Then you can change the mode back to Slave. Ensure that the Auto-sync option is enabled in the applications.

Q. Where can I find the DCR log files?
A. You can find the DCR logs at the following location:
   - NMSROOT\log\DCRServer.log (On Windows)
   - /var/adm/CSCOpx/log/daemons.log (On Solaris and Soft Appliance)
When DEBUG is enabled, the following logs contain the additional information:
   - NMSROOT\log\dcr.log (On Windows)
   - NMSROOT\log\dcrclient.log (On Windows)
   - /var/adm/CSCOpx/log/dcr.log (On Solaris and Soft Appliance)
   - /var/adm/CSCOpx/log/dcrclient.log (On Solaris and Soft Appliance)
See also Maintaining Log Files in Administration of CiscoWorks LAN Management Solution 4.0 for more information.

Q. Why am I getting an Access Denied error while performing Import from Remote NMS?
A. Import from Remote NMS fails if the username and hostname pair is not present in the .rhosts file in the remote server. This is to allow trusted access to the remote system without the need for a password.
   Enter the username and host pair in the .rhosts file in the remote server. To allow all users and hosts, enter in the 1st line of .rhosts file.

Q. How do I include a special character such as comma as part of SNMP Read-Only string in a CSV file?
A. You can specify a string value with a special character by putting quotes around it.
   For example, to specify test,test as a SNMP Read-Only string, you should enter "test,test" in the input CSV file.
INDEX

A
accessing
  CiscoView 5-3
  CiscoView release versions 5-5
  Device Configuration dialog box 5-19
  help 5-5
activity bar 5-4
adding devices to the device list 4-2
  for AUS management 4-5
  for cluster management 4-7
  for standard management 4-3
  using dcrcli A-3
alias devices 4-41
alias devices, managing
  resolving 4-42
AUS (Auto Update Server)
  managing 4-47
    adding 4-48
    setting up 4-5

C
categories
  changing 5-15
  definition 5-14
  editing 5-14
changing
  MIB labels 5-4
chassis view 5-4
  setting refresh rate 5-4
CiscoView
  release versions, understanding 5-13
ciscoview chassis view
  displaying 5-10
  resizing 5-10
ciscoview component selection 5-10
ciscoview device
  configuration 5-10
  monitoring 5-10
  selection 5-10
CiscoView Mini-RMON Manager
  desktop description 6-3
  navigating in 6-3
  overview 6-1
  setting up 6-3
    alarm thresholds 6-5
    enabling statistics collection 6-9
    historical statistics collection 6-9
    system configuration 6-4
    starting 6-2
  ciscoview polling
    chassis view 5-10
  ciscoview selecting
    device 5-10
  ciscoview viewing
    system information 5-10
CM view
  collection data summary 1-6
  Discrepancies 1-2
color legend 5-8
configuring
  categories 5-15
  devices 5-15
  devices (scenario) 5-18
    prerequisites 5-15
procedures 5-19
verification 5-17
job information status 1-7
context menu 5-9

D

DCR
architecture 2-9
  Master DCR 2-9
  Slave DCR 2-10
  Standalone DCR 2-10
AUS management
  adding devices 4-48
CSV file samples 4-22
  CSV 2.0 4-23
  CSV 3.0 4-23
devices, managing 4-1
  adding 4-2
  deleting 4-11
  excluding 4-31
  exporting 4-28
  importing 4-15
  viewing the device list 4-33
Device Selector, using (See Device Selector) 4-48
using features, Master-Slave Setup 3-39

DCR (Device and Credential Repository) CLI interface, using A-2
  adding devices A-3
  deleting devices A-4
  editing devices A-5
  exporting using A-11
  importing using A-7
  listing attributes A-6
debug
  options, and display log 5-19
deleting
devices
  from DCR 4-11

from the device list, using dcrecli A-4
device
  advanced search 5-6
    defining a search rule 5-8
  configuration 5-15
    configuration, scenario 5-18
    procedures 5-19
    verification 5-17
  monitoring 5-17
  search 5-6
Device Admin portlets
  CDA Error Summary 1-11
  Inventory Config Protocol Summary 1-11
  Inventory Device Status 1-12
Device Aliases page 4-41
Device Configuration dialog box, accessing 5-19
device package
  updates 5-13
devices, configuring (scenario) 5-18
  prerequisites 5-15
  procedures 5-19
    Device Configuration dialog box, accessing 5-19
    verification 5-17
devices, discovery
  viewing details 3-32
    devices added to DCR 3-37
    devices updated to DCR 3-38
    reachable devices 3-35
    summary 3-32
    total devices discovered 3-35
    unreachable devices 3-36
devices, discovery settings
    configuring 3-2
    configuring filter settings 3-18
    configuring global settings 3-22
    configuring module settings 3-3
    configuring seed devices 3-9
    configuring SNMP settings 3-15
    viewing 3-30
<table>
<thead>
<tr>
<th>Viewing Summary</th>
<th>Devices, Discovery Starting</th>
<th>Devices, Importing</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias (duplicate) devices</td>
<td>3-31</td>
<td>4-41</td>
</tr>
<tr>
<td>Devices, Managing</td>
<td>4-2</td>
<td></td>
</tr>
<tr>
<td>Adding</td>
<td>4-5</td>
<td></td>
</tr>
<tr>
<td>for AUS management</td>
<td>4-7</td>
<td></td>
</tr>
<tr>
<td>for standard management</td>
<td>4-3</td>
<td></td>
</tr>
<tr>
<td>Alias Devices Resolving</td>
<td>4-42</td>
<td></td>
</tr>
<tr>
<td>Credentials Editing</td>
<td>4-12</td>
<td></td>
</tr>
<tr>
<td>Exporting</td>
<td>4-28</td>
<td></td>
</tr>
<tr>
<td>Importing</td>
<td>4-15</td>
<td></td>
</tr>
<tr>
<td>Deleting</td>
<td>4-11</td>
<td></td>
</tr>
<tr>
<td>Device List, Viewing</td>
<td>4-33</td>
<td></td>
</tr>
<tr>
<td>Excluding</td>
<td>4-31</td>
<td></td>
</tr>
<tr>
<td>Exporting</td>
<td>4-28</td>
<td></td>
</tr>
<tr>
<td>Using CLI</td>
<td>A-11</td>
<td></td>
</tr>
<tr>
<td>Using Device and Credential Admin User Interface</td>
<td>4-30</td>
<td></td>
</tr>
<tr>
<td>Exporting to ACS Server</td>
<td>4-30</td>
<td></td>
</tr>
<tr>
<td>Using CLI</td>
<td>A-11</td>
<td></td>
</tr>
<tr>
<td>Using Device and Credential Admin User Interface</td>
<td>4-30</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Importing Devices and Credentials</th>
<th>4-15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using CLI</td>
<td>A-7</td>
</tr>
<tr>
<td>Using Device and Credential Admin User Interface</td>
<td>4-16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Selector</th>
<th>4-48</th>
</tr>
</thead>
<tbody>
<tr>
<td>Searching Devices</td>
<td>4-51</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>4-52</td>
</tr>
<tr>
<td>Simple Search</td>
<td>4-51</td>
</tr>
<tr>
<td>Selecting Devices</td>
<td>4-50</td>
</tr>
<tr>
<td>Using Device Selector</td>
<td>4-49</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discovery</th>
<th>5-4, 5-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias (duplicate) devices</td>
<td>4-41</td>
</tr>
<tr>
<td>Discovery CLI Interface, Using</td>
<td>A-1</td>
</tr>
<tr>
<td>Start</td>
<td>A-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discovery Features in</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACS Mode</td>
</tr>
<tr>
<td>Master-Slave Setup</td>
</tr>
</tbody>
</table>

| Discovery Filter Settings, Configuring | 3-18 |
| Discovery Global Settings, Configuring | 3-22 |
| Discovery Module Settings, Configuring | 3-3 |
| Discovery Settings | 3-30 |
| Viewing Summary | 3-29 |
| Discovery Settings, Viewing | 3-30 |
| Discovery SNMP Settings | 3-15 |
| Discovery Start | 3-31 |
| Duplicate (alias) Devices | 4-41 |

<table>
<thead>
<tr>
<th>Editing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Credentials in DCR</td>
</tr>
</tbody>
</table>

| Devices in the Device List, Using dcrcli | A-5 |
| Excluding Devices from the Device List | 4-31 |
| Exporting Devices and Credentials | 4-28 |
| Using CLI | A-11 |
| Using Device and Credential Admin User Interface | 4-30 |
| Exporting to ACS Server | A-11 |

<table>
<thead>
<tr>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis View</td>
</tr>
<tr>
<td>Device Selector</td>
</tr>
<tr>
<td>Options Bar</td>
</tr>
<tr>
<td>Status Bar</td>
</tr>
<tr>
<td>Tools Bar</td>
</tr>
</tbody>
</table>

Inventory Portlets
Index

Change Audit  1-2
Hardware Summary  1-4
Software summary  1-4

IPM portlets
  Collector Information  1-9
  Device Categorization  1-11

M
MIB labels  5-4
monitoring devices  5-17

N
navigating in CiscoView  5-3

O
options bar  5-3
  setting preferences  5-4
options bar, using  5-4
overview of CiscoView  5-1
  features  5-2
  device package updates  5-13

P
polling
  performance charts  5-17
preferences, setting  5-12

R
refresh rate
  chassis view  5-4
  monitoring chart  5-17

S
scenarios
  configuring devices  5-18
searching for devices  5-6
  advanced search  5-6
seed devices, configuring  3-9
  selecting
    components  5-10
  setting
    preferences  5-12
setting debugging options
  ciscoview debugging options  5-19
SNMP settings, configuring  3-15
starting CiscoView
  from Device Center  5-3
  system information, viewing  5-18

T
tools bar  5-3
tools bar, using  5-5

U
understanding
  CiscoView release versions  5-13
using
  device selector  5-5
  options bar  5-4
  tools bar  5-5

V
verifying device configuration  5-17
viewing
  CiscoView release version  5-5
  device list  4-33
device performance  5-17
devices not available in the DCR  5-11
installed device package versions  5-5
interface statistics  5-17
viewing system information  5-18