



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 section contains information on:

- [Configuring Device Discovery Settings](#)
- [Starting Device Discovery](#)
- [Viewing Device Discovery Details](#)
- [Using DCR Features in a Master-Slave Setup](#)
- [Using Device Discovery Features in Various Setup](#)

Configuring Device Discovery Settings

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

Settings	Description
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 display 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 Discovery Settings Summary](#)

Configuring Discovery Module Settings

Device Discovery feature in LMS supports the following Device Discovery modules:

Discovery Modules	Description
Layer 3 Discovery Protocols	
Address Resolution Protocol	Address Resolution Protocol also known as ARP is an Internet Protocol that maps IP Address to a MAC address. This Device Discovery module depends on the Routing Table Device Discovery module.
Border Gateway Protocol	Border Gateway Protocol (BGP) is an exterior gateway protocol. This module uses Border Gateway Peer Table to identify its BGP peer.
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.
Routing Table	Routing Table module queries and analyzes routing tables on seed routers, and discovers the subnets and next-hop routers.
Layer 2 Discovery Protocol	
Cisco Discovery Protocol	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.
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.
Ping Discovery Options	
Ping Sweep On IP Range	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.

Discovery Modules	Description
Others	
Cluster Discovery Module	This module discovers the devices in a DSBU cluster. This queries the Cluster MIB to discover all members of the cluster.
Hot Standby Router Protocol (HSRP)	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. The HSRP Discovery Module uses / in CISCO-HSRP-MIB to find active or standby routers.

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.

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
10.77.209.205|3
10.77.200.213|2
```

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
10:EF:14:32:0:0:0:210|FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
```

- 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.
 - 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: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: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:
- Click **Add** to add a new row.
 - Enter the IP Address (IPv4 or IPv6) of the seed device in the Seed Device field.

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.
 - Back** to navigate to the previous page and change the Device Discovery settings.
-

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

- Click the **Configure** button.

The Module Settings page appears.

- 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](#) 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:

Fields for SNMPv2 Settings	Description
Target	<p>Denotes the target device.</p> <p>Enter the IP Address of the target device. You can also use wildcard characters to specify the target device.</p> <p>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.</p> <p>You should enter only the IPv4 Address of the target device for all other Discovery modules except CDP and Ping Sweep On IP Range.</p> <p>You can also use wildcard characters to specify the target device.</p> <p>Examples for target device:</p> <ul style="list-style-type: none"> • 10. *. [210-220]. * • ABCD:EF12:*. *. *. *. * • 2001:410:1:207:ECFF:FEB9:[1850-1855] <p>Entering a target device is mandatory.</p>
Read Community	<p>Denotes the SNMP Read Community string of the device.</p> <p>Entering the read community string is mandatory.</p>

Fields for SNMPv2 Settings	Description
Timeout	<p>Denotes the time period after which the SNMP query times out.</p> <p>You must enter the timeout value in seconds. The default value of timeout is 3 seconds.</p> <p>The Device Discovery time may increase if you specify a larger value for timeout.</p> <p>The timeout doubles for every retry.</p> <p>For example, if the timeout value is 5 seconds and number of retries is 3:</p> <ul style="list-style-type: none"> • 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	<p>Denotes the number of attempts made to query the device.</p> <p>You can specify any value between 0 to 8 as number of retries.</p> <p>The default number of retries is 2.</p>
Comments	You can enter any remarks in this field.

A popup window appears with the following fields, if you have selected SNMPv3:

Fields for SNMPv3 Settings	Description
Target	<p>Denotes the target device.</p> <p>Enter the IP Address of the target device. You can also use wildcard characters to specify the target device.</p> <p>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.</p> <p>You should enter only the IPv4 Address of the target device for all other Discovery modules, except CDP and Ping Sweep On IP Range.</p> <p>You can also use wildcard characters to specify the target device.</p> <p>Examples for target device:</p> <ul style="list-style-type: none"> • 10. *[210-220].* • ABCD:EF12:*.*.*.*.*.* • 2001:410:1:207:ECFF:FEB9:[1850-1855] <p>Entering a target device is mandatory.</p>
User Name	<p>SNMPv3 username used to access the device.</p> <p>Entering a SNMPv3 username is mandatory for all security levels.</p>
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.

Fields for SNMPv3 Settings	Description
Privacy Algorithm	SNMP V3 privacy algorithm used in AuthPriv mode. The privacy algorithm can be DES, 3DES, AES128, AES192, and AES256.
Timeout	<p>Denotes the time period after which the SNMP query times out.</p> <p>You must enter the timeout value in seconds. The default value of timeout is 3 seconds.</p> <p>The Device Discovery time may increase if you specify a larger value for timeout.</p> <p>The timeout doubles for every retry.</p> <p>For example, if the timeout value is 5 seconds and number of retries is 3:</p> <ul style="list-style-type: none"> • 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	<p>Denotes the number of attempts made to query the device.</p> <p>You can specify any value between 0 to 8 as number of retries.</p> <p>The default number of retries is 2.</p>
Comments	You can enter any remarks in this field.

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.

Configuring Discovery Filter 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.
- 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:

Any Octet can have.	Examples
Numbers between: <ul style="list-style-type: none"> 0 to 255 for an IPv4 Address 0 to FFFF for an IPv6 Address 	<ul style="list-style-type: none"> 10.77.240.225 (IPv4 Address) 001:DB8:0:2AA:FF:C0A8:0:640A (IPv6 Address)
Asterisk (*) as wildcard denoting all numbers from 0 to 255 in an IPv4 Address and 0 to FFFF in an IPv6 Address.	<ul style="list-style-type: none"> 10.*.*.240 (IPv4 Address) 001*:0:2AA:FF*:*: (IPv6 Address)
Range of numbers in the <i>[StartingNumber-EndingNumber]</i> format, where: <ul style="list-style-type: none"> <i>StartingNumber</i> and <i>EndingNumber</i> should be numbers between 0 to 255 in an IPv4 Address and 0 to FFFF in an IPv6 Address <i>StartingNumber</i> should not be greater than or equal to <i>EndingNumber</i> 	<ul style="list-style-type: none"> 10.77.[220-240].[210-220] (IPv4 Address) 001:DB8:0:[EE-FF]:FF:C0A8:0:[100-AA F] (IPv6 Address) <p>The following are the invalid examples of IP Address range:</p> <ul style="list-style-type: none"> 10.77.[250-200].221 10.77.200-250.221 001:DB8:0:[EEEE-FF]: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:

Character	Description	Purpose
.	Period	Matches any character
(Opening parenthesis	Marks the beginning of a group of matched characters
)	Closing parenthesis	Marks the end of a group of matched characters
*	Asterisk	Matches zero or more occurrences of a regular expression specified earlier

Character	Description	Purpose
+	Plus character	Matches one or more occurrences of a regular expression specified earlier
\	Trailing slash	Identifies a special character within a regular expression

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.
 - **Back** to navigate to the previous pages and change the Device Discovery settings.
-

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 Display Name	<p>You can set the display name of the discovered devices in DCR as any one of the following:</p> <ul style="list-style-type: none"> • Sysname—Sysname of the device. • DNS Resolvable Host Name—Fully Qualified Domain Name consisting a hostname and a domain name <p>Select the appropriate check box in the Preferred DCR Display Name panel.</p> <ul style="list-style-type: none"> • 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. <p>Select Yes if you want to append a domain name to display name, else select No.</p> <ul style="list-style-type: none"> • If you select only Sysname and the device is not configured with any Sysname then the Preferred DCR display 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 display 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 display name will be the IP Address of the device. <p> Note You can append domain name only when DNS Resolvable Host Name is selected as preferred DCR Display name and the Device IP is DNS resolvable.</p> <p>The hostname of the device is set as the preferred DCR display name by default.</p>

Global Settings	Description
DCR Administration Settings	<p data-bbox="740 264 1062 296">Update DCR Display Name</p> <p data-bbox="740 310 1515 373">Select this check box if you want to update the display name of the devices that already exist in DCR, in the next Device Discovery cycle.</p> <p data-bbox="740 388 1515 478">For example, consider a device which is discovered by LMS Device Discovery, exists in DCR with the display name as its DNS Resolvable Host Name.</p> <p data-bbox="740 493 1515 619">If you change the Preferred DCR Display Name as Sysname for the next Device Discovery, LMS Device Discovery will update the display name of the device as its IP Address in DCR after the next Device Discovery.</p> <p data-bbox="740 634 1515 697">The display name of devices are not overwritten in the future Device Discovery cycles if you have not selected this option.</p> <p data-bbox="740 711 1101 743">Select a Default Credential Set</p> <p data-bbox="740 758 1515 848">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 in DCR.</p> <p data-bbox="740 863 1515 989">See <i>Configuring Default Credential Sets</i> and <i>Configuring Default Credential Set Policy</i> in Administration Guide for Cisco Prime LAN Management Solution 4.1 for more information on creating default credential sets and policies.</p>

Global Settings	Description
Preferred Management IP	<p>Select one of the following options as preferred Management IP address of the device:</p> <ul style="list-style-type: none"> • Use LoopBack Address Select this option to manage a device in the address assigned to the loopback interface. If there are multiple loopback IP addresses, the highest loopback address is used to manage the device. • Resolve By Name LMS Device Discovery uses Domain Name Services (DNS), if available, to perform device name lookups. Select this option to do name resolution using the device name. • Resolve By SysName Select this option to contact the DNS Server to pick up the device hostname. • None Select this option if you do not want to manage the devices with preferred management IP Address. When you select this option, the devices are added in DCR with their IP Addresses. <p>The Resolve By Name option is the default option for this field.</p> <p>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.</p>
E-mail	<p>Enter a valid e-mail ID in this field.</p> <p>Multiple e-mail IDs are also allowed in this field.</p> <p>The system uses the e-mail ID to notify about:</p> <ul style="list-style-type: none"> • Status of immediate or scheduled Device Discovery jobs upon their completion. • New Device Discovery schedules. • Stopped Device Discovery jobs <p> Warning There may be a problem in sending e-mails when you have enabled virus scanner in the LMS Server.</p>

Global Settings	Description
Add Discovered Devices to a Group	<p>Add Discovered Devices to a Group</p> <p>Select one of the following, if you want to add the discovered devices to a group:</p> <ul style="list-style-type: none"> • None - If you select this option, Group Name will be disabled. • All Devices - Adds all the discovered devices to selected group. • Devices newly discovered during last run - Adds only the newly discovered devices to specified group, which are not present in the DCR. <p>Group Name</p> <p>Displays the name of the group if you have selected already. You can also change the group name.</p> <p>Click Select to open the Select a Group popup window. In this window, you can either:</p> <ul style="list-style-type: none"> • Specify a new group name <p>or</p> <ul style="list-style-type: none"> • Select an existing group from the list of user-defined groups using the Group Selector. <p>At the end of Device Discovery cycle, all reachable devices discovered will be added to the group you have selected.</p> <p>However, all reachable devices discovered will be added only to All Devices group if:</p> <ul style="list-style-type: none"> • The Grouping Server is down. • LMS server is in DCR Slave mode. <p>Delete Device from Group</p> <p>If you click the Delete Device from Group button, a list of devices added to the specified group will be displayed. You can select the devices to be deleted from the group and click Delete.</p>

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.

Viewing 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:

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

The Device Discovery Settings page appears.

Step 2 Click **Configure** to enter into the Discovery Settings wizard.

Step 3 Configure one or more of the following settings:

- Module Settings. See [Configuring Discovery Module Settings](#) for information.
- Seed Device Settings. See [Configuring Seed Device Settings](#) for information.
- SNMP Settings. See [Configuring SNMP Settings](#) for information.
- Filter Settings. See [Configuring Discovery Filter Settings](#) for information.
- Global Settings. See [Configuring Global Discovery Settings](#) for information.

Step 4 Click **Next**.

The Discovery Settings Summary page appears with the summary of Device Discovery settings. See [Table 3-1](#) for details of the fields.

Step 5 Click any one of the following:

- **Back** to navigate to the previous pages and change the Device Discovery settings.
 - **Finish to apply the settings** and exit the Discovery Settings wizard.
 - **Cancel** to exit the Discovery Settings wizard.
-

The Discovery Settings Summary page appears with the following fields:

Table 3-1 *Fields in Discovery Settings Summary Page*

Field	Description
Module Settings	Displays a Configure link that leads to Module Settings page. See Configuring Discovery Module Settings for more information.
Seed Device Settings	Displays the status as Not Configured for the first time. If you have configured Seed Device Settings earlier, this field displays a link by name Configure. Clicking Configure leads to Seed Devices Settings page. See Configuring Seed Device Settings for more information.

Table 3-1 *Fields in Discovery Settings Summary Page (continued)*

Field	Description
SNMP Settings	<p>Displays the status as Not Configured for the first time.</p> <p>If you have configured Seed Device Settings earlier, this field displays a link by name Configure.</p> <p>Clicking Configure leads to SNMP Settings page.</p> <p>See Configuring SNMP Settings for more information.</p>
Filter Settings	<p>Displays the status as Not Configured for the first time.</p> <p>If you have configured Filter Settings earlier, this field displays a link by name Configure.</p> <p>Clicking Configure leads to Filter Settings page.</p> <p>See Configuring Discovery Filter Settings for more information.</p>
Global Settings	<p>Displays the status as Not Configured for the first time.</p> <p>If you have configured Global Settings earlier, this field displays a link by name Configure.</p> <p>Clicking Configure leads to Global Settings page.</p> <p>See Configuring Global Discovery Settings for more information.</p>
Modules Selected	<p>Displays the Device Discovery modules which you have selected in the Module Settings page, separated by commas.</p>
Use DCR as Seed List	<p>Displays:</p> <ul style="list-style-type: none"> • Yes if you have selected this option to specify seed devices. • No if you have not selected this option.
Preferred Management IP	<p>Displays the preferred management IP address name you have selected in the Global Settings page.</p>
Preferred DCR Display Name	<p>Displays the preferred DCR display name you have selected in the Global Settings page based on the fallback order.</p>
Update DCR Display Name	<p>Displays:</p> <ul style="list-style-type: none"> • Yes if you have selected this option to update the display name in DCR after the next Device Discovery cycle. • No if you have not selected this option.
Use DCR Default Credentials	<p>Displays:</p> <ul style="list-style-type: none"> • Yes if you have selected to use the default credentials. • No if you have not selected to use the default credentials.
E-mail	<p>Displays the e-mail address you have configured in the Global Settings page.</p> <p>See Configuring Global Discovery Settings for more information on E-mail option.</p>
Add Discovered Devices to a Group	<p>Displays:</p> <ul style="list-style-type: none"> • Yes if you have selected to add discovered devices to a group. • No if you have not selected to add discovered devices to a group.

Table 3-1 Fields in Discovery Settings Summary Page (continued)

Field	Description
Selected Group Name	Displays the name of the group selected to add discovered devices at the end of a Device Discovery. The group name selected will be displayed in the format <i>/User Defined Groups/Group Name</i> in a single or multi-server setup.
Configure (button)	Allows you to enter into Discovery Settings wizard and configure Device Discovery settings. See Configuring Device Discovery Settings for more information.
Start Discovery (button)	The Device Discovery starts as an immediate job. Once the Device Discovery is started and running, the Start Discovery button is changed to Stop Discovery. See Starting Device Discovery for more information.

Starting Device Discovery

Before you start Device Discovery, ensure that you have configured all the required settings.

To start Device Discovery:

-
- Step 1** Go to **Inventory > Device Administration > Discovery > Launch / Summary**. The Device Discovery page appears.
- Or
- Go to **Inventory > Device Administration > Discovery > Settings**. The Device Discovery Settings page appears.
- Step 2** Click **Start Discovery**.
- Device Discovery starts as an immediate job.
- You can also view the status of Device Discovery from LMS Job Browser page. To go to Job Browser page, click **Admin > Jobs > Browser** from the LMS homepage.
-

After Device 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.

Viewing Device 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 Device Discovery Summary](#)
- [Total Devices Discovered](#)
- [Reachable Devices](#)
- [Unreachable Devices](#)
- [Devices Newly Added to DCR](#)
- [Devices Updated to DCR](#)

Viewing Device Discovery Summary

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

The Device Discovery Summary page appears with the following fields:

Field	Description
Discovery Status	<p>Displays the current status of the Device Discovery job. The status of the Device Discovery job could be any of the following:</p> <ul style="list-style-type: none"> • Recent Discovery Information Not Found—This status is displayed: <ul style="list-style-type: none"> – After a fresh installation of LMS. – If no immediate or scheduled backup Device Discovery jobs are available. – If the recent Device Discovery job fails. • Initializing—This status is displayed immediately after you start Device Discovery. <p>At the start of Device Discovery, a URN is published to get the latest status of Device Discovery.</p> <p>If there are any errors in publishing the URN or in receiving the latest Device Discovery summary, Device Discovery status may not be updated.</p> • Running—This status is displayed when the Device Discovery is running. • Stopping—This status is displayed after the completion of Device Discovery and before the CSDiscovery process is stopped. • Completed—This status is displayed when: <ul style="list-style-type: none"> – The last Device Discovery job is completed successfully. – The Device Discovery is stopped.
Discovery Start Time	<p>Displays the starting date and time of Device Discovery.</p> <p>The date is displayed in Long Date format.</p> <p>For example, the start time is displayed as Thu Aug 09 04:35:34 IST 2007.</p>
Discovery End Time	<p>Displays the completion date and time of Device Discovery.</p> <p>The Device Discovery time may differ across the network depending on the size and the changes in the network.</p>
Total Devices Discovered	<p>Displays the total number of devices discovered by the recent Device Discovery job.</p> <p>When you click the number displayed, the Total Devices Discovered window opens. See Total Devices Discovered for more information.</p>

Field	Description
Reachable Devices	Displays the number of devices which are SNMP reachable. When you click the number displayed, the All Reachable Devices window opens. See Reachable Devices for more information.
Unreachable Devices	Displays the number of devices which are not SNMP reachable. When you click the number displayed, the All Unreachable Devices details opens. See Unreachable Devices for more information.
Devices Newly Added to DCR	Displays the number of devices that are newly added to DCR by LMS Device Discovery. When you click the number displayed, the Devices Added to DCR window opens. See Devices Newly Added to DCR for more information.
Devices Updated to DCR	Displays the number of devices that are updated in DCR by LMS Device Discovery. When you click the number displayed, the Devices Updated to DCR Devices window opens. See Devices Updated to DCR for more information.

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.

This section contains:

- [Total Devices Discovered](#)
- [Reachable Devices](#)
- [Unreachable Devices](#)
- [Devices Newly Added to DCR](#)
- [Devices Updated to DCR](#)
- [Activities Performed From Device Discovery Details Windows](#)

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

Field	Description
IP Address	Preferred management IP address of the device. The IP address can be any of the following depending upon your Global Device Discovery settings: <ul style="list-style-type: none"> • Loopback address • Address resolved from DNS lookup • Address resolved from Sysname
System Name	System name of the device.
SysObjectID	sysObjectID value.
Found By Modules	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.
Neighbors	Displays the IP Addresses of the neighboring devices separated by commas. The neighbors are displayed only when devices are discovered by Cisco Discovery Protocol module. Otherwise, this field is blank.
Status	Displays the status of the device as either Reachable or Unreachable.

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:

Field	Description
IP Address	Management IP address of the device returned from Device Discovery.
System Name	System name of the device.
SysObjectID	sysObjectID value.
Found By Modules	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.
Neighbors	Displays the IP Addresses of the neighboring devices separated by commas. The neighbors are displayed only when devices are discovered by Cisco Discovery Protocol module. Otherwise, this field is blank.
Status	Displays the status of the device as Reachable.

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

Field	Description
IP Address	Management IP address of the device.
System Name	System name of the device. This value is blank in the report for all unreachable devices.
SysObjectID	sysObjectID value. This value is blank in the report for all unreachable devices.
Found By Modules	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.
Status	Displays the status of the device as Unreachable.

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:

Field	Description
IP Address	Management IP address of the device returned from Device Discovery.
Display Name	Display name of the device. The display name can be any of the following depending upon your Global Device Discovery settings: <ul style="list-style-type: none">• IP Address• Hostname• Fully Qualified Domain Name
Hostname	Hostname of the device. DCR does a DNS lookup to update the hostname of devices.
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.

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:

Field	Description
IP Address	<p>Management IP address of the device.</p> <p>The IP address can be any of the following depending upon your Global Device Discovery settings:</p> <ul style="list-style-type: none"> • Loopback address • Address resolved from DNS lookup • Address resolved from Sysname
Display Name	<p>Display name of the device.</p> <p>The display name can be any of the following depending upon your Global Device Discovery settings:</p> <ul style="list-style-type: none"> • 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	<p>Category, Series, and Model information of devices in DCR.</p> <p>For example, Device Type displays Cisco 3000 Router, Cisco Catalyst 8150 CSR Switch and so on.</p>

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.
- Export the Device Discovery details to a file of CSV or PDF format.
- Set the number of records to be displayed per page, as desired. You can set the number as 20, 50, 100, or 500.

To export the Device Discovery details window:

-
- Step 1** Click the **Export** button on top-right of the window.
The Exporting Report dialog box opens.
- Step 2** Select the required radio button to export the report either in PDF or in CSV format.
- Step 3** Enter the numbers of rows you want to export.
For example, if you want to export the first 10 rows and fourteenth row, you should enter 1-10,14 in the text field.
- Step 4** Click **OK**.
-

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 4.1.
 - First, upgrade the DCR Master server to LMS 4.1, and then upgrade the DCR Slave Server to LMS 4.1.
-

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 4.1 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.