Chapter

4

Discovery

In this chapter

SAN discovery overview

Discovery is the process by which the Management application contacts the devices in your SAN. When you configure discovery, the application discovers devices connected to the SAN. The application illustrates each device and its connections on the Connectivity Map (topology).

When you discover a fabric, the Management application checks to confirm that the seed switch is running a supported Fabric OS version in the fabric, and if it is not, the Management application prompts you to select a new seed switch.

NOTE
Discovery of a Secure Fabric OS fabric in strict mode is not supported.

For a Fabric OS fabric, the seed switch must be the primary Fabric Configuration Server (FCS). If you use a non-primary FCS to discover the fabric, the Management application displays an error and will not allow the discovery to proceed. If the Management application has already discovered the fabric, but afterward you create the FCS policy and the seed switch is not a primary FCS, an event is generated during the next poll.

The Management application cannot discover a fabric that is in the process of actively configuring to form a fabric. Wait until the fabric is formed and stable, then re-attempt the fabric discovery.

After fabric discovery successfully completes, all clients are updated to display the newly discovered fabric.

During fabric discovery, you can define an IPv4 address or IPv6 address for the device; however, the Management application uses the preferred IP format to connect with the device. To configure the preferred IP format, refer to “Configuring the preferred IP format” on page 222.

NOTE
Professional edition can discover only 1 fabric.

NOTE
Professional Plus edition can discover up to 2,560 ports.

NOTE
Professional Plus edition can discover, but not manage the Backbone chassis.Use the device’s Element Manager, which can be launched from the Connectivity Map, to manage the device. This device cannot be used as a Seed switch.

FCS policy and seed switches

The Management application requires that the seed switch is the primary Fabric Configuration Server (FCS) switch at the time of discovery.

Setting time on the fabric will set the time on the primary FCS switch, which will then distribute the changes to other switches.

When FCS Policy is defined, **ConfigDownload** is allowed only from the primary FCS switch, but Management application does not check at the time of download that the switch is the primary FCS Switch.

NOTE
Switches running in Access Gateway mode cannot be used as the seed switch.

NOTE
The Backbone Chassis cannot be used as seed switch to discover and manage edge fabrics. You must discover a seed switch from each edge fabric to discover and manage the edge fabric.

NOTE
The Backbone Chassis can only discover and manage the backbone fabric.

Backbone Chassis discovery requirements

Table 19 details which Backbone Chassis models can be discovered by each version of the Management application and whether or not the model can be discovered as a seed switch or only as a member switch.

TABLE 19 Backbone Chassis discovery

Device	Professional	Professional Plus	Enterprise
8-slot Backbone Chassis as seed switch	No	No	Yes
8-slot Backbone Chassis as member switch	Yes for discovery; however, it cannot be managed.	Yes for discovery; however, it cannot be managed.	Yes
4-slot Backbone Chassis as seed switch	Yes	Yes	Yes
4-slot Backbone Chassis as member switch	Yes	Yes	Yes
16 Gbps 8-slot Backbone Chassis as seed switch	No	No	Yes
16 Gbps 8-slot Backbone Chassis as member switch	Yes for discovery; however, it cannot be managed.	Yes for discovery; however, it cannot be managed.	Yes
16 Gbps 4-slot Backbone Chassis as seed switch	Yes	Yes	Yes
16 Gbps 4-slot Backbone Chassis as member switch	Yes	Yes	Yes

Discovering fabrics

NOTE
Fabric OS devices must be running Fabric OS 5.0 or later.

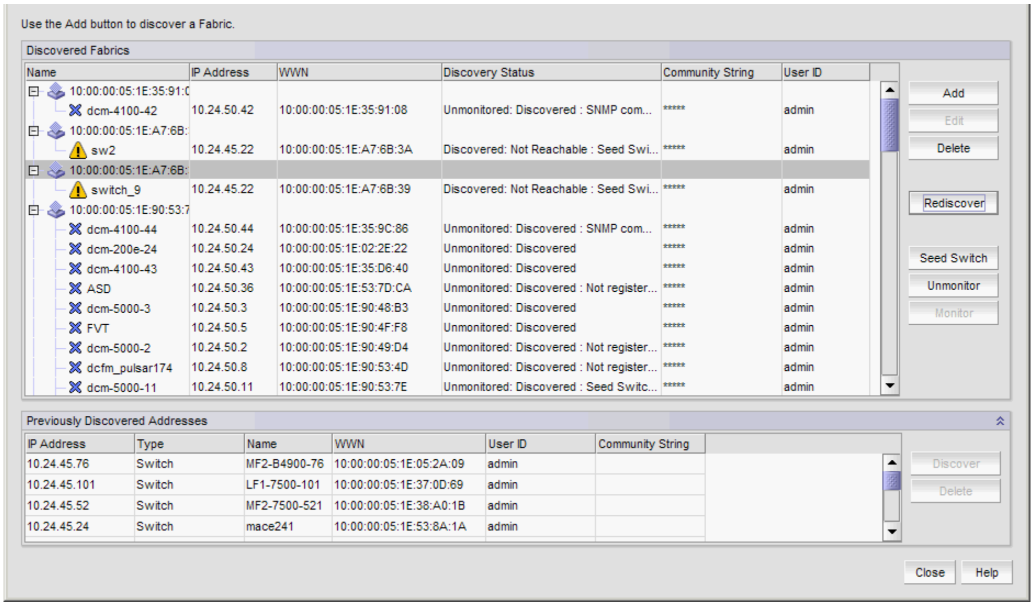
NOTE
Only one copy of the application should be used to monitor and manage the same devices in a subnet.

NOTE
When accessing additional data from the **SAN Inventory** or **SAN Status** widgets, it takes a few moments to populate newly discovered products in the **SAN Products** - *Status* dialog box (where *Status* is the section of the widget you selected).

To discover specific IP addresses or subnets, complete the following steps.

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.



Use the Add button to discover a Fabric.

Discovered Fabrics

Name	IP Address	WWN	Discovery Status	Community String	User ID
10:00:00:05:1E:35:91:(					
dcm-4100-42	10.24.50.42	10:00:00:05:1E:35:91:08	Unmonitored: Discovered : SNMP com...	*****	admin
10:00:00:05:1E:A7:6B:					
sw2	10.24.45.22	10:00:00:05:1E:A7:6B:3A	Discovered: Not Reachable : Seed Swi...	*****	admin
10:00:00:05:1E:A7:6B:					
switch_9	10.24.45.22	10:00:00:05:1E:A7:6B:39	Discovered: Not Reachable : Seed Swi...	*****	admin
10:00:00:05:1E:90:53:7					
dcm-4100-44	10.24.50.44	10:00:00:05:1E:35:9C:86	Unmonitored: Discovered : SNMP com...	*****	admin
dcm-200e-24	10.24.50.24	10:00:00:05:1E:02:2E:22	Unmonitored: Discovered	*****	admin
dcm-4100-43	10.24.50.43	10:00:00:05:1E:35:D6:40	Unmonitored: Discovered	*****	admin
ASD	10.24.50.36	10:00:00:05:1E:53:7D:CA	Unmonitored: Discovered : Not register...	*****	admin
dcm-5000-3	10.24.50.3	10:00:00:05:1E:90:48:B3	Unmonitored: Discovered	*****	admin
FVT	10.24.50.5	10:00:00:05:1E:90:4F:F8	Unmonitored: Discovered	*****	admin
dcm-5000-2	10.24.50.2	10:00:00:05:1E:90:49:D4	Unmonitored: Discovered : Not register...	*****	admin
dcfm_pulsar174	10.24.50.8	10:00:00:05:1E:90:53:4D	Unmonitored: Discovered : Not register...	*****	admin
dcm-5000-11	10.24.50.11	10:00:00:05:1E:90:53:7E	Unmonitored: Discovered : Seed Switc...	*****	admin

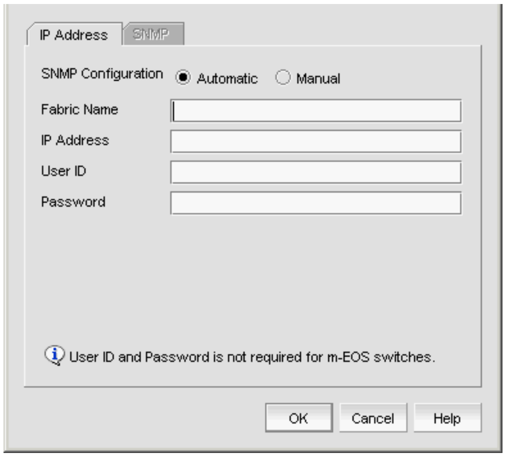
Previously Discovered Addresses

IP Address	Type	Name	WWN	User ID	Community String
10.24.45.76	Switch	MF2-B4900-76	10:00:00:05:1E:05:2A:09	admin	
10.24.45.101	Switch	LF1-7500-101	10:00:00:05:1E:37:0D:69	admin	
10.24.45.52	Switch	MF2-7500-521	10:00:00:05:1E:38:A0:1B	admin	
10.24.45.24	Switch	mace241	10:00:00:05:1E:53:8A:1A	admin	

FIGURE 7 Discover Fabrics dialog box

2. Click **Add** to specify the IP addresses of the devices you want to discover.

   The **Add Fabric Discovery** dialog box displays.


IP Address | SNMP

SNMP Configuration ● Automatic ○ Manual

Fabric Name

IP Address

User ID

Password

User ID and Password is not required for m-EOS switches.

FIGURE 8 **Add Fabric Discovery dialog box (IP Address tab)**

3. Enter a name for the fabric in the **Fabric Name** field.
4. Enter an IP address (IPv4 or IPv6) for a device in the **IP Address** field.

   To configure the preferred IP format for the Management application server to connect with Fabric OS devices, refer to "Configuring the preferred IP format" on page 222. If the product has both an IPv4 and IPv6 address, the Management server uses the preferred address. If a product does not have the preferred address type, the Management server uses the other IP type.

   For seed switch requirements, refer to "Seed switch requirements" on page 67.

NOTE
The Backbone Chassis cannot be used as seed switch to discover and manage edge fabrics. You must discover a seed switch from each edge fabric to discover and manage the edge fabric.

NOTE
The Backbone Chassis can only discover and manage the backbone fabric.

NOTE
Professional and Professional Plus editions cannot manage the Backbone Chassis.

NOTE
Professional edition can discover only 1 fabric.

NOTE
Professional Plus edition can discover up to 2,560 ports.

NOTE
For Admin Domain (AD) devices, you must enable the AD configuration on the switch before discovery; otherwise, end devices associated with the user-configure AD display as missing in the topology. In addition, the Fabric OS switch must have Physical AD visibility.

For Virtual Fabric discovery device requirements, refer to "Virtual Fabrics requirements" on page 834.

To discover a Virtual Fabric device, you must have the following permissions:

- Switch user account with Chassis Admin role permission on the physical chassis.
- Switch and SNMPv3 user account with access rights to all logical switches (all Fabric IDs (1 - 128).

  For information about configuring permissions on a Fabric OS device, refer to the *Fabric OS Administrator's Guide*.:

5. (Fabric OS devices only) Enter the user ID and password for the switch in the **User ID** and **Password** fields.
6. Choose one of the following options:

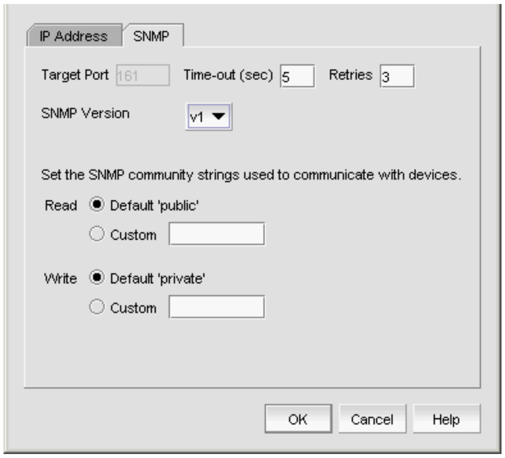
- Select the **Automatic** option to use the default SNMPv3 profile.

  The default SNMPv3 profile uses the following attributes:

Attribute	Value
Timeout	5 seconds
Retries	3
User name	snmpadmin1
Context name	None
Auth Protocol	None
Priv Protocol	None

- Select the **Manual** option to configure SNMP and complete the following steps.

  a. Click the **SNMP** tab.



Target Port 161 Time-out (sec) 5 Retries 3

SNMP Version v1

Set the SNMP community strings used to communicate with devices.

Read ● Default 'public'
○ Custom

Write ● Default 'private'
○ Custom

FIGURE 9 Add Fabric Discovery dialog box (SNMP - v1 tab)

  b. Enter the duration (in seconds) after which the application times out in the **Time-out (sec)** field.

  c. Enter the number of times to retry the process in the **Retries** field.

d. Select the SNMP version from the **SNMP Version** list.

- If you selected v1, continue with step e.
- If you select v3, the SNMP tab displays the v3 required parameters. Go to step i.

  To discover a Fabric OS device (not virtual fabric-capable), you must provide the existing SNMPv3 username present in the switch.

  To discover a Virtual Fabric device, you must configure SNMPv3 and your SNMP v3 user account must be defined as a Fabric OS switch user.

  When you discovers Virtual Fabric-enabled switch with the SNMPv3 username "admin", which is the same as the Fabric OS switch user, the Management application automatically creates an SNMP username "admin" in the switch by replacing the sixth username.

e. Specify the **Read** option by selecting **Default 'public'** or **Custom**.

f. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

g. Specify the **Write** option by selecting **Default 'private'** or **Custom**.

h. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

Go to step 7.

i. If you are configuring a 256-port director, select the **Configure for** *256-Port_Director_Name* check box.

- If you selected **Configure for** *256-Port_Director_Name*, go to step m.
- If you did not select **Configure for** *256-Port_Director_Name*, continue with step j.

j. Enter a user name in the **User Name** field.

k. Enter a context name In the **Context Name** field.

l. Select the authorization protocol in the **Auth Protocol** field.

m. Enter the authorization password in the **Auth Password** field.

- If you selected **Configure for** *256-Port_Director_Name*, go to step 7.
- If you did not select **Configure for** *256-Port_Director_Name*, continue with step n.

n. Select the privacy protocol in the **Priv Protocol** field.

o. Enter the privacy password in the **Priv Password** field.

7. Click **OK** on the **Add Fabric Discovery** dialog box.

   If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays.

   a. Select the **Select** check box for each undiscovered seed switch to discover their fabrics.

   b. Click **OK** on the **Undiscovered Seed Switches** dialog box.

8. Repeat step 2 through step 7 for each fabric you want to discover.

9. Click **Close** on the **Discover Fabrics** dialog box.

Editing the password for multiple devices

You can only edit password for Fabric OS devices in the same fabric.

To edit the password for multiple devices within the same fabric, complete the following steps.

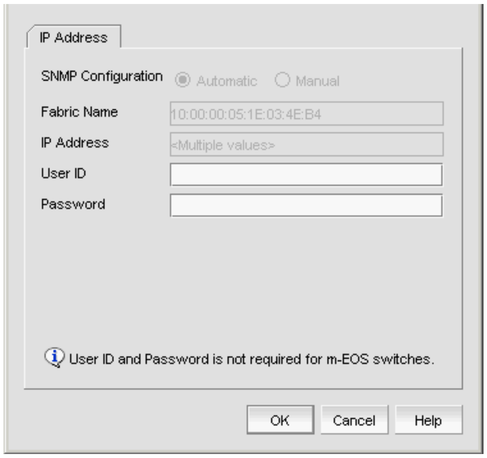
1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.

2. Select multiple devices within the same fabric from the **Discovered Fabrics** table.

3. Click **Edit.**

   The *Fabric_Name* **Edit Switches** dialog box displays.



SNMP Configuration ● Automatic ○ Manual

Fabric Name 10:00:00:05:1E:03:4E:B4

IP Address <Multiple values>

User ID

Password

User ID and Password is not required for m-EOS switches.

FIGURE 10 Edit Switches dialog box

4. Enter the user ID for the switch in the **User ID** field.

5. Enter the password for the switch in the **Password** field.

6. Click **OK.** on the *Fabric_Name* **Edit Switches** dialog box.

   The **Credential Update Status** dialog box displays. This dialog box displays the status of the change on the selected devices. If you selected a logical switch, the updated credentials will be applied to the other logical switches in the same chassis.

   - **IP Address** — The IP address of the device.
   - **WWN** — The world wide name of the device.
   - **Name** — The name of the device.
   - **FID** — The fabric ID of the logical switch.
   - **Fabric Name** — The name of the fabric where device is located.
   - **Status** — The status of the update (such as Success, Failed, or Not Applicable).
   - **Reason** — The reason for the status for Failed or Not Applicable.
     - Failed — Not Reachable
     - Not Applicable — Credentials not applied

7. Click **Close.** on the **Credential Update Status** dialog box.

Configuring SNMP credentials

1. Select **Discover** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select an IP address from the **Discovered Fabrics** table.

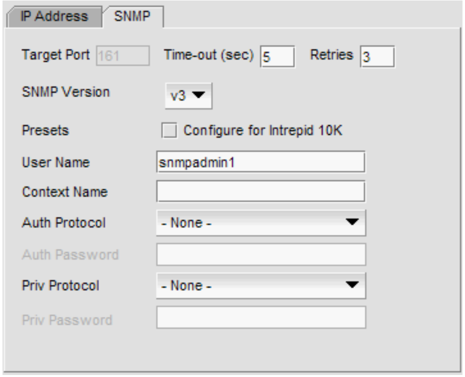
3. Click **Edit**.

   The **Add Fabric Discovery** dialog box displays.

4. To revert to the default SNMPv3 settings, click the **Automatic** option. Go to step 19.

5. To manually configure SNMP, select the **Manual** option. Go to step 6.

6. Click the **SNMP** tab.



Target Port 161 Time-out (sec) 5 Retries 3

SNMP Version v3

Presets □ Configure for Intrepid 10K

User Name snmpadmin1

Context Name

Auth Protocol - None -

Auth Password

Priv Protocol - None -

Priv Password

FIGURE 11 **Add Fabric Discovery dialog box (SNMP tab)**

7. Select the SNMP version from the **SNMP Version** list.
   - If you selected v1, continue with step 8.
   - If you select v3, the **SNMP** tab displays the v3 required parameters. Go to step 12.

     To discover a Virtual Fabric device, you must configure SNMPv3 and your SNMP v3 user account must be defined as a Fabric OS switch user.

8. Specify the **Read** option by selecting **Default 'public'** or **Custom**.

9. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

10. Specify the **Write** option by selecting **Default 'private'** or **Custom**.

11. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

    Go to step 7.

12. If you are configuring a 256-Port director, select the **Configure for** *256-Port_Director_Name* check box.
    - If you selected **Configure for** *256-Port_Director_Name*, go to step 16.
    - If you did not select **Configure for** *256-Port_Director_Name*, continue with step 13.

13. Enter a user name in the **User Name** field.

14. Enter a context name In the **Context Name** field.

15. Select the authorization protocol in the **Auth Protocol** field.

16. Enter the authorization password in the **Auth Password** field.
    - If you selected **Configure for** *256-Port_Director_Name*, go to step 19.
    - If you did not select **Configure for** *256-Port_Director_Name*, continue with step 17.
17. Select the privacy protocol in the **Priv Protocol** field.
18. Enter the privacy password in the **Priv Password** field.
19. Click **OK** on the **Add Fabric Discovery** dialog box.

    If the seed switch is not partitioned, continue with step 20.

    If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays.

    a. Select the **Select** check box for each undiscovered seed switch to discover their fabrics.

    b. Click **OK** on the **Undiscovered Seed Switches** dialog box.
20. Click **Close** on the **Discover Fabrics** dialog box.

Reverting to a default SNMP community string

To revert to the default SNMP parameters, complete the following steps.

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.
2. Select an IP address from the **Discovered Fabrics** table.
3. Click **Edit.**

   The **Add Fabric Discovery** dialog box displays.
4. Select the **Automatic** option.
5. Click **OK** on the **Add Fabric Discovery** dialog box.
6. Click **Close** on the **Discover Fabrics** dialog box.

Rediscovering a fabric

To refresh discovery of a fabric, complete the following steps.

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.
2. Select a fabric in the **Discovered Fabrics** table.
3. Click **Rediscover.**

   The application triggers all fabric and switch level collectors. The status of the refresh displays in the Master Log as an application event for the fabric as well as each switch in the fabric. For example, “Fabric information collection was successful for the fabric - *Fabric_Name*”.
4. Click **Close** on the **Discover Fabrics** dialog box.

Removing a fabric from active discovery

If you decide you no longer want the Management application to discover and monitor a specific fabric, you can delete it from active discovery. Deleting a fabric also deletes the fabric data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a fabric from active discovery, complete the following steps.

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.

2. Select the fabric you want to delete from active discovery in the **Discovered Fabrics** table.
3. Click **Delete.**
4. Click **OK** on the confirmation message.

   The deleted fabric displays in the **Previously Discovered Addresses** table.

5. Click **Close** on the **Discover Fabrics** dialog box.

Rediscovering a previously discovered fabric

To return a fabric to active discovery, complete the following steps.

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.

2. Select the fabric you want to return to active discovery in the **Previously Discovered Addresses** table.
3. Click **Discover.**
4. Click **OK** on the confirmation message.

   The rediscovered fabric displays in the **Discovered Fabrics** table.

5. Click **Close** on the **Discover Fabrics** dialog box.

Deleting a fabric

To delete a fabric permanently from discovery, complete the following steps.

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.

2. Select one or more switches that you want to delete permanently from discovery in the **Previously Discovered Addresses** table.
3. Click **Delete.**
4. Click **OK** on the confirmation message.
5. Click **Close** on the **Discover Fabrics** dialog box.

DCB discovery

You can discover DCB devices from both the SAN and IP tabs. The following sections details the differences between discovery from the SAN tab or the IP tab.

DCB discovery from the SAN tab

- You can discover DCB devices through fabric discovery.
- If you discover a fabric that contains DCB devices on the SAN tab, the DCB devices display on the IP tab in the Network Objects, L2 Topology, IP Topology, and VLAN Topology views. Non-DCB devices do not display on the IP tab.
- If you discover DCB devices through fabric discovery on the SAN tab, the DCB devices are automatically added to IP discovery during rediscovery.
- If the fabric containing DCB devices is unmonitored on the SAN tab, that fabric no longer displays on the SAN tab; however, the DCB devices continue to display on the IP tab.

  Unmonitored fabrics to not refresh data for devices contained in the fabric. If you rediscover the DCB device in an unmonitored fabric from the IP tab, rediscovery fails.
- If the DCB device segments out of a fabric on the SAN tab, the DCB device continues to display on the IP tab until you accept changes to the fabric on the SAN tab (which deletes the device from the fabric).
- If a DCB device joins a fabric on the SAN tab, the DCB device displays on the IP tab as soon as it displays on the SAN tab.
- If you delete a DCB device from fabric discovery, the DCB device no longer displays on the IP tab.
- If you discover a DCB device through fabric discovery, you cannot delete the device from IP discovery.

DCB discovery from the IP tab

- You can discover DCB devices through profile or individual product discovery.
- If you discover a DCB device from the IP tab, the DCB device does not display on the SAN tab.
- If you discover a DCB switch through IP discovery, the DCB device displays as a fabric on the IP tab. Only DCB switches display in the fabric. Non-DCB devices do not display in the fabric on the IP tab.
- If the DCB switch is in AG mode, discovery fails.
- You can only discover chassis-based DCB switches using the IP address (not the CP address).

Viewing the fabric discovery state

The Management application enables you to view device status through the **Discover Setup** dialog box.

To view the discovery status of a device, complete the following steps.

1. Select **Discover** > **Fabrics.**

   The **Discover Fabrics** dialog box displays.

2. Right-click a fabric and select **Expand All** to show all devices in the fabric.

   The **Name** field displays the discovery status icons in front of the device name. The following table illustrates and describes the icons that indicate the current status of the discovered devices.

   TABLE 20 Discovery Status Icons

Icon	Description
✓	Displays when the fabric or host is managed and the management status is okay.
⚠	Displays when the switch is managed and the switch management status is not okay.
✖	Displays when the fabric, switch, or host is not managed or not monitored.

   The **Discovery Status** field details the actual status message text, which varies depending on the situation. The following are samples of actual status messages:

   - Discovered: Seed Switch: Not registered for SNMP Traps
   - Discovered: Seed Switch: Not Manageable: Not registered for SNMP Traps
   - Discovered: Current seed switch is not recommended. Change Seed Switch. : Seed Switch: Not registered for SNMP Traps
   - New Discovery Pending

Troubleshooting fabric discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

1. Verify IP connectivity by issuing a ping command to the switch.

   a. Open the command prompt.

   b. From the Server, type `ping` *`Switch_IP_Address`*.

2. Enter the IP address of the device in a browser to verify the http reachability.

   For example, *http://10.1.1.11*.

Managed count exceeded troubleshooting

The following section states possible issues and the recommended solution when you exceed your managed count limits.

Problem	Resolution
If you exceed your managed count limit, the Management application displays a “licensed exceeded” message on the topology.	Perform one or more of the following actions to • “Changing your network size” • “Remove a device from active discovery” • “Deleting a fabric” Changing your network size If you are at the maximum network size for your license, contact your preferred network provider. To change the size of your network, complete the following steps. 1 Select **Server** > **Options**. The **Options** dialog box displays. 2 Select **Memory Allocation** in the **Category** list to change the network size. 3 Select the size of the SAN (small, medium, or large) you need. 4 Click **OK** on the confirmation message. 5 Click **Apply** or **OK** to save your work. **NOTE:** Changes to this option take effect after an application restart. **NOTE:** You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **12.X.X** > **Server Management Console**). 6 Click **OK** on the “changes take effect after application restart” message.
	Remove a device from active discovery To remove a fabric from active discovery, complete the following steps. 1 Select **Discover** > **Fabrics**. The managed count exceeded message displays. Managed counts that have been exceeded display with a light red background. Managed counts that are within the grace count limit display with a pale yellow background. 2 Click **OK** on the message. The **Discover Fabrics** dialog box displays. 3 Select the fabric you want to delete from active discovery in the **Discovered Fabrics** table. 4 Click **Delete**. 5 Click **OK** on the confirmation message. The deleted fabric displays in the **Previously Discovered Addresses** table. 6 Click **Close** on the **Discover Fabrics** dialog box.

Problem	Resolution
	Deleting a fabric Before you can delete a fabric permanently from discovery, you must remove it from active discovery. Refer to "Remove a device from active discovery". To delete a fabric permanently from discovery, complete the following steps. 1 Select **Discover > Fabrics**. The managed count exceeded message displays. Managed counts that have been exceeded display with a light red background. Managed counts that are within the grace count limit display with a pale yellow background. 2 Click **OK** on the message. The **Discover Fabrics** dialog box displays. 3 Select one or more switches that you want to delete permanently from discovery in the **Previously Discovered Addresses** table. 4 Click **Delete**. 5 Click **OK** on the confirmation message. 6 Click **Close** on the **Discover Fabrics** dialog box.

Virtual Fabric discovery troubleshooting

The following section state possible issues and the recommended solutions for Virtual Fabric discovery errors.

Problem	Resolution
At the time of discovery, the seed switch is Virtual Fabric-enabled; however, the user does not have Chassis Admin role for the seed switch. At the time of discovery, the user does not have the Chassis Admin role for all other switches in the fabric. After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, the user does not have Chassis Admin role.	Make sure the user account has Chassis Admin role on the Fabric OS device.
At the time of discovery, the seed switch is Virtual Fabric-enabled; however, the user does not have access to all possible logical switches (access to all possible Fabric IDs 1 - 128). At the time of discovery, the user does not have access to all possible logical switches for all other devices in the fabric. After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, the user does not have access to all possible logical switches.	Make sure the user account has access rights to all logical switches (access to all possible Fabric IDs 1 - 128) on the Fabric OS device.
At the time of discovery, SNMP v3 is not configured. At the time of discovery, SNMP v3 is not configured for all other switches in the fabric. After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, SNMP v3 is not configured	Configure the SNMP v3 information for the Virtual Fabric-enabled device.
At the time of discovery or fabric refresh, the SNMP v3 user account does not have the Chassis Admin role.	Make sure the SNMP v3 user account has the Chassis Admin role on the Fabric OS device.
At the time of discovery or refresh, the SNMP v3 user account does not have access to all possible logical switches (access to all possible Fabric IDs 1 - 128). This access is required to obtain performance statistics from all logical switches.	Make sure the SNMP v3 user account has access rights to all logical switches (access to all possible Fabric IDs 1 - 128) on the Fabric OS device.

Problem	Resolution
At the time of discovery or fabric refresh, the SNMP v3 user account does not have a matching Fabric OS switch user account. This is required to obtain performance statistics from all logical switches.	Make sure the SNMP v3 user account is also defined as a Fabric OS switch user.
At the time of fabric refresh, the physical chassis is reachable; however, a previously discovered logical switch is not reachable.	The logical switch has been deleted or the Fabric ID was changed. To find a logical switch, right-click the physical chassis within the **Chassis Group** in the **Product List** and select **Logical Switches**. All logical switches on the selected physical chassis display in a list.

SAN Fabric monitoring

NOTE
Monitoring is not supported on Hosts. The upper limit to the number of HBA and CNA ports that can be monitored at the same time is 32. The same upper limit applies if switch ports and HBA ports are combined. You can select switch ports and adapter ports from a maximum of ten devices.

Fabric monitoring enables discovery of and data collection for the specified fabric and all associated devices. The Management application enables you to view fabric monitoring status through the **Discover Fabrics** dialog box. The following table illustrates and describes the icons that indicate the current status of the discovered switches.

TABLE 21 Monitor Icons

Icon	Description
✓	Displays when the switch is managed and the switch management status is okay.
⚠	Displays when the switch is managed and the switch management status is not okay.
✖	Displays when the fabric or switch is not managed or not monitored.

For Professional and Professional Plus, the default monitoring interval is 120 seconds (minimum interval is 120 seconds).

Table 22 details the default and minimum monitoring intervals used to query the monitored switches:

TABLE 22 Monitor Intervals

SAN Size	Default	Minimum
Small	120 seconds (2 minutes)	60 seconds (1 minute)
Medium	900 seconds (15 minutes)	120 seconds (2 minutes)
Large	1800 seconds (30 minutes)	180 seconds (3 minutes)

To change the monitoring interval, refer to "Configuring asset polling" on page 219.

Stop monitoring of discovered fabrics

NOTE
Monitoring is not supported on Hosts.

When you stop monitoring a fabric, the Management application performs the following actions:

- Stops all data collection for the fabric and all associated devices.
- Unregisters as SNMP trap recipient from the fabric and all associated devices.
- Unregisters as SYSLOG recipient from the fabric and all associated devices.
- Does not perform any scheduled or on demand operations (other than monitor) on the fabric and all associated devices.
- Removes the fabric and all associated devices from product list, topology, and all feature dialog boxes.
- Displays the fabric and all associated devices in the Discovery Fabrics dialog box with the unmonitored icon and prefixes "Unmonitored" to the discovery status

To stop monitoring a fabric and all associated devices, complete the following steps.

1. Select **Discovery** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select the fabric you want to stop monitoring from the **Discovered Fabrics** table.
3. Click **Unmonitor**.
4. Click **Close** on the **Discover Fabrics** dialog box.

Stop monitoring of discovered switches

NOTE
You cannot stop monitoring the seed switch.

When you stop monitoring a switch, the Management application performs the following actions:

- Stops all data collection for the switch.
- Unregisters as SNMP trap recipient from the switch. For Virtual Fabric switches, only unregister as SNMP trap recipient when all Virtual Fabric switches of that chassis are unmonitored.
- Unregisters as SYSLOG recipient from the switch. For Virtual Fabric switches, only unregister as SYSLOG recipient when all Virtual Fabric switches of that chassis are unmonitored.

- Does not perform any scheduled or on demand operations (other than monitor) on the switch.
- Removes the switch from product list, topology, and all feature dialog boxes.
- Displays the switch in the Discovery Fabrics dialog box with the unmonitored icon and prefixes "Unmonitored" to the discovery status.

The following details the behavior that occurs when you unmonitor a switch:

- If you unmonitor a switch, the switch does not display in the topology, but end devices connected to the switch continue to display in the product list and topology (with no connections).
- If you segment an unmonitored switch, you cannot discover it separately until you accept changes in the original fabric.
- If you unmonitor a switch in Access Gateway mode, that switch is unmonitored from all fabrics in which it is participating.
- If you unmonitor a Virtual Fabric switch (logical switch in a chassis), only that partition is unmonitored, but end devices connected to the Virtual Fabric switch continue to display in the product list and topology (with no connections). Any other partitions of the associated chassis continue to be monitored.
- If fabric tracking is enabled and you unmonitor a switch, fabric tracking continues to track the unmonitored switch.
- If fabric tracking is enabled and the unmonitored switch segments out of the fabric, the switch is marked as "missing" in the **Accept Changes** dialog box. If an ISL connected to this switch is disconnected, the ISL is also marked as "missing" in the in the **Accept Changes** dialog box. If a device connected to this switch is disconnected, the device is also marked as "missing" in the product list and topology.
- If fabric tracking is enabled for two managed fabrics and you move an unmonitored switch from one fabric to the other, the unmonitored switches is marked as "missing" in the original fabric and marked as "untrusted" in the new fabric in the **Accept Changes** dialog box.
- If you unmonitor a DCB switch (discovered on the SAN tab), the DCB switch does not display on the SAN tab, but continues to display on the IP tab.

To stop monitoring a switch, complete the following steps.

1. Select **Discovery** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select one or more switches in the same fabric that you want to stop monitoring from the **Discovered Fabrics** table.

   NOTE
   You cannot select switches in different fabrics.

3. Click **Unmonitor**.

   The **Unmonitor Status** dialog box displays with the following details:

   - **IP Address** — The IP address of the switch.
   - **WWN** — The WWN of the switch.
   - **Name** — The name of the switch.
   - **FID** — The FID of the switch.

- **Fabric Name** — The name of the associated fabric.
- **Status** — Whether the unmonitor was successful or failed.
- **Reason** — The reason for the failure. Blank for success.

4. Click **Close** on the **Unmonitor Status** dialog box.
5. Click **Close** on the **Discover Fabrics** dialog box.

Resume monitoring of discovered fabrics

NOTE
Monitoring is not supported on Hosts.

To monitor a fabric and all associated devices, complete the following steps.

1. Select **Discovery** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.
2. Select the fabric you want to monitor from the **Discovered Fabrics** table.
3. Click **Monitor.**

   The **Monitor Status** dialog box displays with the status.

   NOTE
   If there is a unmonitored switch in the fabric, it stays unmonitored.

   The monitor function fails if the fabric has user-defined Admin Domains created or if the fabric is merged with another fabric already in the monitored state.
4. Click **Close** on the **Monitor Status** dialog box.
5. Click **Close** on the **Discover Fabrics** dialog box.

Resume monitoring of discovered switches

NOTE
Monitoring is not supported on Hosts.

NOTE
You can only monitor a switch that is reachable and has valid credentials.

To monitor a switch, complete the following steps.

1. Select **Discovery** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.
2. Select one or more switches that you want to monitor from the **Discovered Fabrics** table.
3. Click **Monitor.**

   The **Monitor Status** dialog box displays with the status.
4. Click **Close** on the **Monitor Status** dialog box.
5. Click **Close** on the **Discover Fabrics** dialog box.

SAN Seed switch

The seed switch must be running a supported Fabric OS version and must be HTTP-reachable.

Sometimes, the seed switch is auto-selected, such as when a fabric segments or when two fabrics merge. Other times, you are prompted (an event is triggered) to change the seed switch, such as in the following cases:

- If, during fabric discovery, the Management application detects that the seed switch is not running a supported version, you are prompted to change the seed switch.
- When one or more switches join the fabric or if the switch firmware is changed on any of the switches in the fabric, the Management application checks to make sure that the seed switch is still running a supported version. If it is not, then you are prompted to either upgrade the firmware on the seed switch or to change the seed switch to a switch running a supported firmware.

If a fabric of switches running only Fabric OS 5.X or later is created due to segmentation, the Management application continues to monitor that fabric, but if any switch with a later Fabric OS version joins the fabric, an event is triggered informing you that the seed switch is not running the latest firmware and you should change to the seed switch running the highest firmware.

ATTENTION
If a seed switch is segmented or merged, historical data such as offline zone DB, profile and reports, and Firmware Download Profile can be lost. Segmentation of a seed switch does not result in formation of a new fabric. If a merge occurs, the historical data is lost only from the second fabric.

You can change the seed switch as long as the following conditions are met:

- The new seed switch is HTTP-reachable from the Management application.
- The new seed switch is a primary FCS.
- The new seed switch is running the latest Fabric OS version in the fabric.

This operation preserves historical and configuration data, such as performance monitoring and user-customized data for the selected fabric.

ATTENTION
If the seed switch firmware is downgraded from Fabric OS 5.2.X to an earlier version, then all RBAC-related data is discarded from the Management application.

If, during the seed switch change, the fabric is deleted, but the rediscovery operation fails (for example, if the new seed switch becomes unreachable using HTTP), then you must rediscover the fabric again. If you rediscover the fabric using a switch that was present in the fabric before the change seed switch operation was performed, then all of the historical and configuration data is restored to the rediscovered fabric. If you rediscover the fabric using a switch that was added to the fabric after the fabric was deleted, then the historical and configuration data is lost.

If multiple users try to change the seed switch of the same fabric simultaneously, only the first change seed switch request is executed; subsequent requests that are initiated before the first request completes will fail.

If another user changes the seed switch of a fabric you are monitoring, and if you have provided login credentials for only that seed switch in the fabric, then you lose connection to the seed switch.

Seed switch requirements

The seed switch must be running Fabric OS 5.0 or later. For a complete list of all supported Fabric OS hardware, refer to “Supported hardware and software” on page lvi.

Seed switch failover

The Management application collects fabric-wide data (such as, fabric membership, connectivity, name server information, zoning, and so on) using the seed switch. Therefore when a seed switch becomes unreachable or there is no valid seed switch, the fabric becomes unmanageable.

When the seed switch cannot be reached for three consecutive fabric refresh cycles, the Management application looks for another valid seed switch in the fabric, verifies that it can be reached, and has valid credentials. If the seed switch meets this criteria, the Management application automatically fails over to the recommended seed switch.

Note that it is possible that auto-failover may occur to a seed switch not running the latest firmware version. In this instance, any functionality which has a direct dependency on the firmware version of the seed switch is affected and restricted by the failover seed switch capabilities.

Changing the seed switch

When you change the seed switch for a fabric, the Management application performs the following checks in the order they are listed:

- Identifies all switches and removes those running unsupported firmware version.
- Identifies which of the remaining switches are running the latest firmware versions.
- Filters out those switches that are not reachable.
- Identifies which switches are Virtual Fabric-enabled switches (Fabric OS only).

  If there are Virtual Fabric-enabled switches, the Management application only uses these switches as recommended seed switches. If there are no Virtual Fabric-enabled switches, continue with the next check.

- Identifies which switches are Virtual Fabric-capable devices (Fabric OS only).

  If there are Virtual Fabric-capable switches, the Management application only uses these switches as recommended seed switches. If there are no Virtual Fabric-capable switches, the Management application uses the list from the second check.

To change the seed switch, complete the following steps.

1. Select **Discovery** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select the fabric for which you want to change the seed switch from the **Discovered Fabrics** table.

   If a device joins or merges with a fabric and fabric tracking is active, you must accept changes to the fabric before the new devices display in the **Seed Switch** dialog box. For more information about fabric tracking, refer to “Fabric tracking” on page 231.

3. Click **Seed Switch**.

   If the fabric contains other switches that are running the latest version and are also HTTP-reachable from the Management application, the **Seed Switch** dialog box appears. Otherwise, a message displays that you cannot change the seed switch.

4. Select a switch to be the new seed switch from the **Seed Switch** dialog box.

   You can select only one switch. Only switches that are running the latest Fabric OS version in the fabric are displayed. The current seed switch is not displayed in this list.

5. Click **OK** on the **Seed Switch** dialog box.

   If you are not already logged in to the seed switch, the **Fabric Login** dialog box displays.

   If you are successfully authenticated, the fabric is deleted from the Management application without purging historical data, and the same fabric is rediscovered with the new seed switch.

6. Click **Close** on the **Discover Fabrics** dialog box.

IP discovery overview

NOTE
Discovery only displays products that are assigned to your area of responsibility (AOR). For more information about user accounts, refer to "Areas of responsibility" on page 250.

NOTE
You must have the Discover Setup - IP privilege to configure and run discovery. For more information about privileges, refer to "User Privileges" on page 1935.

NOTE
You must have the **All IP Products** AOR (area of responsibility) in your user account to discover new products. For more information about user accounts, refer to "User accounts" on page 241.

NOTE
IP discovery requires Internet Control Message Protocol (ICMP) or Telnet support on the device to determine device reachability.

NOTE
DCB devices discovered through Fabric discovery (from the **SAN** tab) are automatically added to IP discovery during rediscovery.

Discovery is the method that the Management application uses to find data networking devices on the network. When the Management application discovers devices, it finds all IP addresses on a device and stores them in the Management application database. The Management application uses the primary address of a product to communicate with the product. The primary address is determined using the following rules:

- If you configure discovery to prefer loopback addresses (refer to "Defining global setting preferences" on page 97), and there are loopback IP addresses configured in the product; and the loopback IP address is reachable from the Management application server, then the loopback IP address is the primary IP address of the product.

- If you did not configure discovery to prefer loopback addresses, the original IP address used to discover the product is the primary IP address of the product.

The primary address is the address that appears on the Network Object Manager and other configuration and display panels in the Management application.

The Management application provides two types of discovery, simple discovery and profile-based discovery.

Simple discovery discovers the device with a specific IP address and/or DNS name. It is triggered by device configuration changes on SNMP traps, certain configuration deployments to a device, and adding device or rediscovering a device from the **Discover Setup – IP** dialog box.

Profile-based discovery allows you to define the discovery policy. It provides more flexible ways to specify IP addresses to discover. It also enables you to discover new devices from already discovered devices.

Profile-based discovery uses the following steps to build a list of candidate IP addresses to probe.

1. Discovery runs one of the following programs:
   - On Windows systems, use ipconfig to find the default gateway.
   - On UNIX systems, use netstat -r -n to determine the "seed" routers and extract IP addresses from the program output.

     Discovery adds these IP addresses to the list of candidate IP addresses.
2. Discovery queries the database to retrieve the IP address for each previously discovered device and adds these IP addresses to the list of candidate IP addresses.
3. Discovery adds the IP addresses from the IP address file to the list of candidate addresses.
4. As the discovery cycle proceeds, discovery adds addresses from the ping sweep address ranges to the list of candidate addresses.
5. Discovery searches for neighbors of a discovered device using the information located in the device's SNMP Link Layer Discovery Protocol (LLDP), Foundry Discovery Protocol (FDP), Cisco Discovery Protocol (CDP), and Address Resolution Protocol (ARP) tables. To search for neighbors, you must configure discovery to search for neighbor addresses (refer to “Configuring advanced discovery profile preferences” on page 116).

After creating the list of candidate IP addresses, discovery uses multiple threads to probe devices. You can define how many threads can be used at one time. Threads operate in parallel, so communication to multiple devices occurs simultaneously. Each thread takes one address from the list of candidate IP addresses and probes it. The first step in probing is to determine whether the device is reachable or not. Discovery provides two methods to determine reachability. The first method uses ICMP ping to probe the device. The second method opens a connection to the IP address (currently to the Telnet port). This serves as a "ping" to confirm that the IP address is reachable and some device is listening. By default, if the device responds by either accepting or rejecting the connection, then the connection is closed and discovery continues.

The next step uses SNMP queries. The first query determines whether the device is a IronWare OS or Network OS device or not. Discovery rotates through a list of candidate SNMP community strings until it finds one that works. For devices that already exist in the database, the community string recorded in the database for that device is tried first.

If you configure discovery to search for neighbor addresses (refer to “Configuring advanced discovery profile preferences” on page 116), the second query scans the device's SNMP ARP table. Discovery adds any IP address from the ARP table to the list of candidate IP addresses.

Similarly, if you configure discovery to search for neighbor addresses (refer to "Configuring advanced discovery profile preferences" on page 116), the third query scans the device's SNMP LLDP, FDP, and CDP tables. Any neighbor IP address is added to the list of candidate IP addresses to probe. Discovery adds any IP address from the LLDP, FDP, and CDP tables to the list of candidate IP addresses.

Discovery also tries to determine the host name of the device by requesting the Management application server operating system to perform various mappings of the device IP addresses to host names and host names back to IP addresses, using whatever mechanism the operating system uses (typically Domain Name Server) to determine the host name for a device.

If discovery determines that the device is reachable and manageable, then discovery uses the full set of SNMP queries to collect asset information from the device. Discovery then adds or updates the device in the database and sends notification to other applications.

Rediscovery updates can occur using any of the following methods:

- Lazy polling.
- Adaptive discovery (triggered by snmp traps).
- Manual rediscovery (refer to "IP Rediscovery" on page 146).

Configuration requirements

Before configuring discovery, obtain the following information:

- SNMPv1 and SNMPv2c read-write community strings or SNMPv3 read-write credentials for the devices to be included in discovery. Make sure that devices you want to manage have the SNMP credentials configured. For more information, refer to "IP SNMP credentials" on page 83.
- Device IP addresses and subnets to probe during discovery. For more information, refer to "Configuring address ranges" on page 104, "Adding user credentials" on page 89, and "Defining global setting preferences" on page 97.

Discovery of IPv6 addresses

The Management application discovers both IPv4 and IPv6 addresses of devices that have the IPv6 MIB objects implemented. The Management application discovers IPv4 addresses of devices running IPv6 that do not have IPv6 MIB support. For more information, refer to "Defining global setting preferences" on page 97.

NOTE
IronWare IPv6 devices must support the set of MIBs presented in Table 23 on page 71. To determine IPv6 MIB object support on the device, refer to the release notes and user documentation for your IPv6 product.

NOTE
Third-party IPv6 devices must support the set of MIBs presented in Table 24 on page 73.

MIB support

IP discovery requires SNMP management information base (MIB) support on the device for management information collection. For a list of required MIBs, refer to Table 23 on page 71 or Table 24 on page 73.

TABLE 23 Required MIB support for IronWare OS devices

IETF standard	MIB name	Required MIB object	Data collected
N/A	Brocade MIB		
IEEE 802.1AB	LLDP-MIB	lldpObjects.lldpRemoteSystemsData	For Layer 2 topology information: Entire lldpObjects.lldpRemoteSystemsData
RFC 1213	MIB-II	mib-2.system mib-2.interfaces.ifTable mib-2.ip.ipAddrTable	From mib-2.interfaces.ifTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange From mib-2.ip.ipAddrTable for IP subnet information: • ipAdEntAddr • ipAdEntNetMask From mib-2.ip.ipAddrTable for Layer 3 topology information: • ipForwarding
RFC 2465	IPv6-MIB	ipv6MIBObjects ipv6NetToMediaTable ipv6MIBObjects.ipv6AddrTable	From ipv6MIBObjects and ipv6NetToMediaTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange From ipv6MIBObjects.ipv6AddrTable for IP subnet information: • ipv6AddrAddress • ipv6AddrPfxLength

TABLE 23 Required MIB support for IronWare OS devices (Continued)

IETF standard	MIB name	Required MIB object	Data collected
RFC 2863	IF-MIB	ifMIBObjects.ifXTable	From ifMIBObjects.ifXTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange
RFC 4363	Q-BRIDGE-MIB	dot1qVlan.dot1qPortVlanTable	For VLAN information: Entire dot1qVlan.dot1qPortVlanTable

Table 24 provides a list of MIB support required for third-party devices.

TABLE 24 Required MIB support for third-party devices

IETF standard	MIB name	Required MIB object	Data collected
RFC 1213	MIB-II	mib-2.system mib-2.interfaces.ifTable mib-2.ip.ipAddrTable	From mib-2.interfaces.ifTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange From mib-2.ip.ipAddrTable for IP subnet information: • ipAdEntAddr • ipAdEntNetMask From mib-2.ip.ipAddrTable for Layer 3 topology information: • ipForwarding
RFC 2465	IPv6-MIB	ipv6MIBObjects ipv6NetToMediaTable ipv6MIBObjects.ipv6AddrTable	From ipv6MIBObjects and ipv6NetToMediaTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange From ipv6MIBObjects.ipv6AddrTable for IP subnet information: • ipv6AddrAddress • ipv6AddrPfxLength
RFC 2863	IF-MIB	ifMIBObjects.ifXTable	From ifMIBObjects.ifXTable for interface level information: • ifName/ifDescr • ifAlias • ifType • ifMtu • ifSpeed • ifPhysAddress • ifAdminStatus • ifOperStatus • ifLastChange

TABLE 24 Required MIB support for third-party devices (Continued)

IETF standard	MIB name	Required MIB object	Data collected
RFC 4133	ENTITY-MIB	entPhysicalTable entAliasMappingTable (if available)	For module (line card) information: Entire entPhysicalTable Entire entAliasMappingTable, if available
RFC 4293	IP-MIB	mib2.ip.ipAddressTable	For ip address and subnet information ipAddressAddrType ipAddressAddr ipAddressIfIndex ipAddressType ipAddressPrefix

VDX/VCS discovery

NOTE
Discovery of a VDX device requires Network OS 2.1.0 or later.

NOTE
Discovery a VCS fabric requires that the seed switch must be running Network OS 2.1.0 or later; however, the fabric can include members running Network OS 2.0.0.

NOTE
VDX/VCS discovery requires read and write IP Discovery privilege. For more information about privileges, refer to "User Privileges" on page 1935.

NOTE
You must have the **All IP Products** AOR (area of responsibility) in your user account to discover new products. For more information about user accounts, refer to "User accounts" on page 241.

Network OS devices can only be discovered from the IP tab. You can discover a standalone VDX or VCS-enabled devices as well as VCS fabrics. VDX/VCS devices display in the Network Objects, L2 Topology, Ethernet Fabrics, IP Topology, and VLAN Topology views.

VDX device and VCS fabric discovery uses the Read/Write Login Prompt credentials for authentication (refer to "Adding user credentials" on page 89). You cannot discover VDX devices using root level privileges. If you do not provide discovery credentials, the Management application uses the default switch credentials for the admin account. You can edit the credentials for multiple VDX/VCS devices when they all have same firmware version (refer to "Editing IP device discovery" on page 125).

VCS fabrics display in a tree structure with member nodes. When you discover a new fabric and initial discovery is complete, the fabric automatically tracks the fabric members. Subsequently, if a member is removed from the fabric, a minus (-) icon displays (see table below) next to the product icon.

TABLE 25

⛔	Device Removed

VCS devices use the following to determine reachability:

- Reachable — The VDX/VCS product is online and is accessible by ICMP, Netconf, and SNMP; therefore, it is reachable.
- Degraded Link — The VDX/VCS product is not accessible by one of the following: ICMP, Netconf, or SNMP.
- Not Reachable — The VDX/VCS product is offline and is not accessible by any of the following: ICMP, Netconf, and SNMP.

The following sections detail the VDX/VCS discovery behavior.

Network OS discovery IP address format

You can discover Network OS devices using an IPv4 or IPv6 address. To configure the preferred IP format for the Management application server to connect with Network OS devices, refer to "Configuring the preferred IP format" on page 222.

During discovery, if the product has both an IPv4 and IPv6 address, the Management server uses the preferred address. If a product does not have the preferred address type, the Management server uses the other IP type. If the Management application is not IPv6 capable, the Management application cannot discover products with an IPv6 address directly (as a seed switch). The Management application can discover products with an IPv6 address indirectly when the seed switch has an IPv4 address.

Standalone discovery

- When you discover a VDX device that is not VCS-enabled, it displays as an individual L2 (DCB) device.
- When you enable VCS mode on a discovered VDX device, after rediscovery the VDX displays as a VCS fabric.

VCS fabric discovery

NOTE
Professional edition can only discover a VCS fabric with one member.

NOTE
IP Base edition can only discover a VCS fabric with two members.

- When you discover a VDX device that is VCS-enabled and is not connected to other VCS-enabled devices, it displays as a VCS fabric with one member.
- When you discover a VDX device that is VCS-enabled and is connected to other VCS-enabled devices, it displays as a VCS fabric with all connected VCS-enabled devices as members of the fabric.

- When you discover any member in a VCS fabric through individual IP device discovery, that member acts as the seed switch and discovers all other members in the VCS fabric. The principal switch of the VCS fabric displays as a VCS fabric. The VCS fabric members display as individual L2 (DCB) devices.
- When you discover multiple members in a VCS fabric through profile discovery, the principal switch acts as the seed switch and discovers all other members (not included in profile discovery) in the VCS fabric. The principal switch of the VCS fabric displays as a VCS fabric. The VCS fabric members display as individual L2 (DCB) devices.

VCS fabric rediscovery

Rediscovery is the refreshing of the asset data for the selected product. Rediscovery of a VCS-enabled device or VCS fabric uses the following behavior:

- If you select a fabric seed switch, rediscovery refreshes the fabric membership information.
- If you select a fabric member, rediscovery refreshes the fabric member's asset data.
- If you select a missing fabric member, rediscovery results in the discovery of new fabric or discovery of a standalone switch (dependent on what happened to the disconnected member). You can also delete missing fabric members from discovery (refer to "Deleting IP devices from discovery" on page 131).

NOTE
If you do not have the **All IP Products** AOR in your user account, you cannot rediscover missing fabric members.

Seed switch failover

The Management application uses the seed switch to discover other members in the VCS fabric. When you discover devices through individual discovery, the seed switch is the first member you discover in the VCS fabric. When you discover devices through profile discovery, the seed switch is the principal switch in the VCS fabric.

- If VCS mode is disabled on the seed switch, the Management application triggers rediscovery of the other members in the VCS fabric and selects another member to act as the seed switch.
- If the seed switch becomes unreachable, the Management application selects another member of the VCS fabric to act as the seed switch.
- If the seed switch becomes unreachable from the Management application and looses connectivity with the VCS fabric, the Management application selects another member of the VCS fabric to act as the seed switch.
- If the seed switch looses connectivity with the VCS fabric but is still reachable from the Management application, the VCS fabric splits into two fabrics. When this occurs, the Management application selects another member of the VCS fabric to act as the seed switch and manages the original seed switch as a separate VCS fabric. When two fabrics regain connectivity, the Management application uses the original seed switch as the seed switch for the merged VCS fabric.

VCS fabric split and merge

- If the seed switch looses connectivity with the VCS fabric but is still reachable from the Management application, the Management application selects another member of the VCS fabric to act as the seed switch and manages the original seed switch as a separate VCS fabric.

  When the original seed switch rejoins the original VCS fabric, the Management application uses the original seed switch as the seed switch for the merged VCS fabric.

- If a member (not the seed switch) looses connectivity with the VCS fabric but is still reachable from the Management application, the VCS fabric splits into two fabrics. The Management application treats the member that lost connectivity as a separate VCS fabric.

  When the member rejoins the original VCS fabric, the Management application uses the VCS fabric that was discovered first as the merged VCS fabric.

Network OS 2.0 device limitations

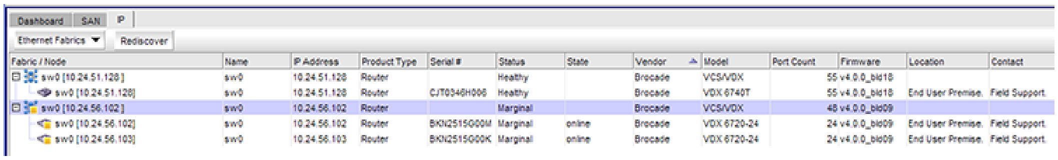
VDX devices running Network OS 2.0.0 cannot be discovered directly. However, if you discover a VCS fabric (running Network OS 2.1.0 or later) that contains VDX devices (running Network OS 2.0.0), the Network OS 2.0.0 devices are included in discovery of the fabric and display on the topology map. Network OS 2.0.0 devices have the following limitations:

- Display as unreachable members in the fabric.
- Assets (ports, LAGs, VLANs, and so on) are not collected.
- TRILL links between Network OS 2.1.0 devices and Network OS 2.0.0 devices do not display.

Logical chassis cluster mode discovery

Logical chassis cluster mode requires Network OS 4.0 or later and is one of two types of VCS modes. In logical chassis cluster mode, both the data and configuration paths are distributed. The entire cluster can be configured from the principal node. The other VCS mode is *fabric cluster mode*, in which the data path for nodes is distributed, but the configuration path is not distributed and each node keeps its configuration database independently. The generic term *VCS mode* applies to both fabric cluster mode and logical chassis mode unless otherwise stated.

The **State** column of the **Discover Setup - IP** Dialog shown in Figure 12 is applicable only to nodes that are members of a logical chassis cluster. The possible node states are described later in this section.



Fabric / Node	Name	IP Address	Product Type	Serial #	Status	State	Vendor	Model	Port Count	Firmware	Location	Contact
sw0 [10.24.51.128]	sw0	10.24.51.128	Router		Healthy		Brocade	VCS/VDX	55	v4.0.0_bld18		
sw0 [10.24.51.128]	sw0	10.24.51.128	Router	CJT0346H006	Healthy		Brocade	VDX 6740T	55	v4.0.0_bld18	End User Premise.	Field Support.
sw0 [10.24.56.102]	sw0	10.24.56.102	Router		Marginal		Brocade	VCS/VDX	48	v4.0.0_bld09		
sw0 [10.24.56.102]	sw0	10.24.56.102	Router	BKN2515G00M	Marginal	online	Brocade	VDX 6720-24	24	v4.0.0_bld09	End User Premise.	Field Support.
sw0 [10.24.56.103]	sw0	10.24.56.103	Router	BKN2515G00K	Marginal	online	Brocade	VDX 6720-24	24	v4.0.0_bld09	End User Premise.	Field Support.

FIGURE 12 Discovery Setup - IP dialog box with node state for logical chassis cluster

Logical chassis cluster discovery includes the following behavior:

- Manual- or profile-based discovery is the same as for a cluster in fabric cluster mode.

- Uses the IP address of any member of the logical chassis cluster for discovery.
- Sets the cluster IP address to the IP address of the principal node.

NOTE
You can change the principal node for the cluster by running the **logical-chassis principal-priority** command from the NOS prompt. For more information, refer to the *Network OS Command Reference*.

- Principal-switch failover does not occur if the cluster is unstable (for example, if the chassis had been disabled for maintenance) because refresh collection will fail.
- If the cluster is configured with a virtual IP address before its discovery, and then discovery is initiated, the cluster IP displays the virtual IP address instead of the IP address of the principal node.
- If the cluster is configured with a virtual IP address after it is discovered by the Management application, the virtual IP address is collected and saved in the database for the next lazy polling or next adaptive collection.
- If another switch becomes the principal switch, the Management application sets the cluster IP address to that of the new principal switch at the next lazy polling or next adaptive collection.
- The **State** column in the **Discover Setup - IP** dialog shown in Figure 12 applies only to nodes that are in logical chassis mode. Possible states are:
    - Online—A node that is currently connected and operational.
    - On discovery, only online members are considered active cluster members. The Management application server collects the device, port, and LAG information of active cluster members. The the Management application client displays the member node as a cluster member in the Ethernet Fabrics topology.
    - Offline—A cluster member node that cannot be reached by the primary cluster node.
    - On refresh, if the member was an active member of a cluster and is now offline, the member is marked as missing. If the member is not online after three consecutive short ticks, auto-discovery gets initiated. If auto-chasing fails, the member remains missing.
    - Rejoining—A node that is in the process of rejoining its cluster.
    - On refresh, if the member was an active member of the cluster and is now rejoining, then the member is marked as missing. If the member is not online after three consecutive short ticks, auto discovery gets initiated. If auto chasing fails, the member remains missing.
    - Replacing—A node that is being replaced.
    - On refresh, if a member node is in the Replacing state, the member is shown as missing.
    - If the member is in the Replacing state for more than three consecutive short ticks, auto-discovery gets initiated. If auto-chasing fails, the member remains missing.

Administratively removing a node from a logical chassis cluster

You can remove a node from a logical chassis cluster by using the Network OS command line interface. For instructions, refer to the *Network OS Administrator's Guide* and the *Network OS Command Reference*, versions 4.0 or later.

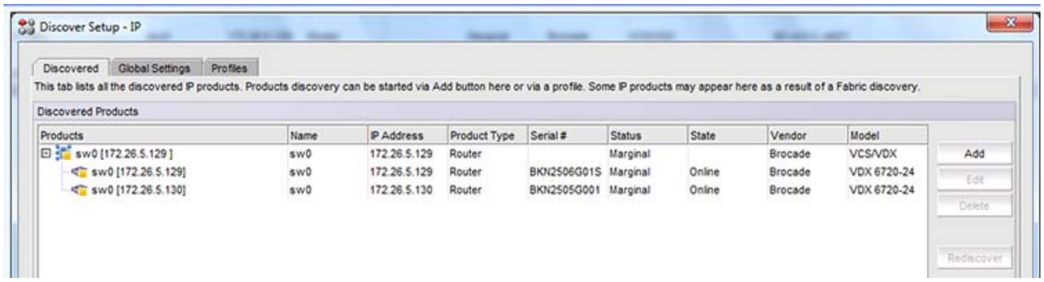
Once the node is removed, all configurations corresponding to that node are removed from the cluster configuration database.

The deleted node gets rebooted automatically and boots in VCS-disabled mode.

The deleted node also gets marked as missing in the cluster.

The Management application initiates auto-discovery immediately, and the deleted node gets rediscovered in its current state.

As an example, Figure 13 shows the **Discover Setup** - **IP** dialog box before the administrator removes a node from the cluster.



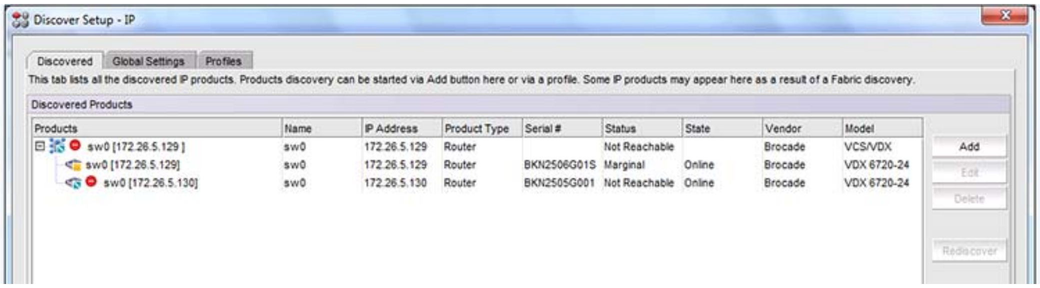
This tab lists all the discovered IP products. Products discovery can be started via Add button here or via a profile. Some IP products may appear here as a result of a Fabric discovery.

Discovered Products

Products	Name	IP Address	Product Type	Serial #	Status	State	Vendor	Model
⊟ sw0 [172.26.5.129]	sw0	172.26.5.129	Router		Marginal		Brocade	VCS/VDX
sw0 [172.26.5.129]	sw0	172.26.5.129	Router	BKN2506G01S	Marginal	Online	Brocade	VDX 6720-24
sw0 [172.26.5.130]	sw0	172.26.5.130	Router	BKN2505G001	Marginal	Online	Brocade	VDX 6720-24

FIGURE 13 Discover Setup - IP dialog box before removal of node

Figure 14 shows the **Discover Setup** - **IP** dialog box after the administrator has removed the node with the IP address of 172.26.5.130 from its logical chassis cluster.



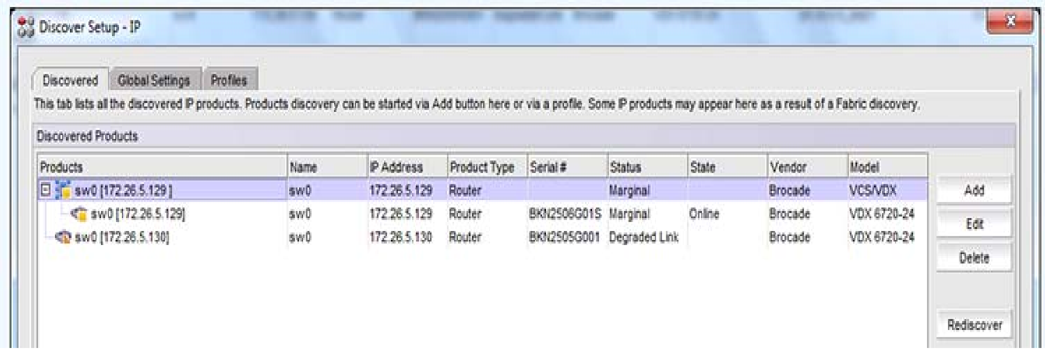
This tab lists all the discovered IP products. Products discovery can be started via Add button here or via a profile. Some IP products may appear here as a result of a Fabric discovery.

Discovered Products

Products	Name	IP Address	Product Type	Serial #	Status	State	Vendor	Model
⊟ ● sw0 [172.26.5.129]	sw0	172.26.5.129	Router		Not Reachable		Brocade	VCS/VDX
sw0 [172.26.5.129]	sw0	172.26.5.129	Router	BKN2506G01S	Marginal	Online	Brocade	VDX 6720-24
● sw0 [172.26.5.130]	sw0	172.26.5.130	Router	BKN2505G001	Not Reachable	Online	Brocade	VDX 6720-24

FIGURE 14 Discover Setup - IP dialog box after disabling the node from logical chassis cluster

Figure 15 shows the **Discover Setup** - **IP** dialog box after The Management application has performed rediscovery. The node with the IP address of 172.26.5.130 is shown as a degraded link.



This tab lists all the discovered IP products. Products discovery can be started via Add button here or via a profile. Some IP products may appear here as a result of a Fabric discovery.

Products	Name	IP Address	Product Type	Serial #	Status	State	Vendor	Model
⊟ sw0 [172.26.5.129]	sw0	172.26.5.129	Router		Marginal		Brocade	VCS/VDX
sw0 [172.26.5.129]	sw0	172.26.5.129	Router	BKN2506G01S	Marginal	Online	Brocade	VDX 6720-24
sw0 [172.26.5.130]	sw0	172.26.5.130	Router	BKN2505G001	Degraded Link		Brocade	VDX 6720-24

FIGURE 15 Discover Setup - IP dialog box after rediscovery

How the Management application handles a cluster mode change

In Network OS release 4.0, an administrator can change the mode of a cluster from fabric cluster mode to logical chassis cluster mode, and vice versa. For instructions, refer to the *Network OS Administrator's Guide* and the *Network OS Command Reference*.

NOTE
All cluster-specific configurations are lost during a cluster-mode change.

On refresh collection, the Management application detects the mode change and retains all database entries related to the cluster.

HyperEdge stack discovery

HyperEdge stacks must contain at least one ICX 6610 device and one ICX 6650 device and all stacking members must be running IronWare 8.0 or later (the exact same version). HyperEdge stacks support up to 8 units in stack. Note that you do not recieve an error or warning message when unit number exceeds 8. However, the HyperEdge stack may stop functioning.

For stacking between ICX 6610 devices, use the 40 Gbps Ethernet ports as the stacking ports.

For stacking between ICX 6610 and ICX 6450 devices, use the 10 Gbps Ethernet ports as the stacking ports. The 10 Gbps Ethernet ports must have the POD license enabled with 10 Gbps speed. On the ICX 6610 device, you must configure a 10 Gbps Ethernet port as a peripheral port. You can connect the ICX 6450 device 10 Gbps Ethernet port to the ICX 6610 device peripheral port.

For stacking between ICX 6450 devices, use the 10 Gbps Ethernet ports as the stacking ports.

If the ICX 6610 device have full Layer 2 and Layer 3 features, HyperEdge stacking extends the ICX 6610 device Layer 3 and other advanced capabilities to the ICX 6450 device to process packets going to ICX 6450 ports.

For HyperEdge stacking management, the master/active and standby units must be the ICX 6610 device. Management of the stacking device is through the master unit only. This includes SNMP, sFlow, syslog, tftp, telnet and ssh traffic. The management port on each member unit (except the master unit) of an HpyerEdge stack, is not visible and does not function.

Configuring IP profile discovery

NOTE
You must have the **All IP Products** AOR (area of responsibility) in your user account to discover new products. For more information about user accounts, refer to "User accounts" on page 241.

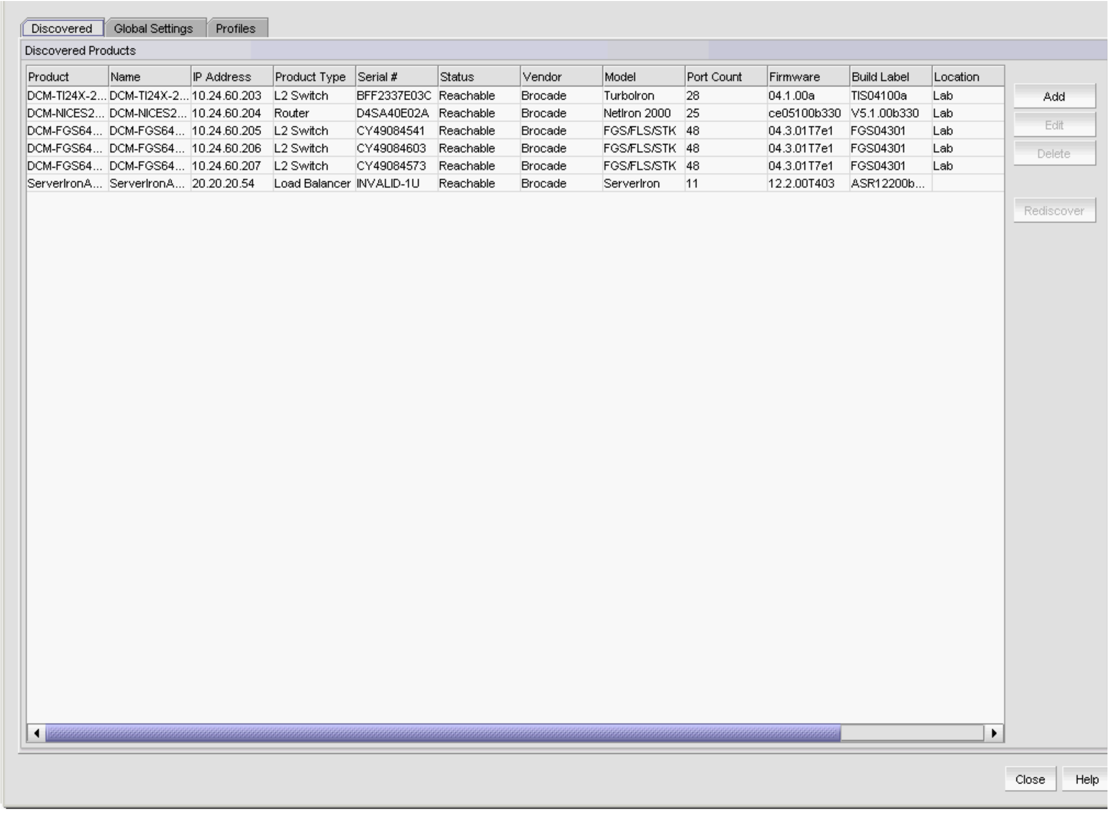
To configure profile discovery, complete the following steps.

1. Select **Discover** > **IP Products**.

   The **Discover Setup - IP** dialog box displays.

   NOTE
   The **Discovered Products** table lists all products discovered through individual product discovery, profile-based discovery, as well as Fabric discovery (from the **SAN** tab).

   NOTE
   DCB devices discovered through Fabric discovery (from the **SAN** tab) are automatically added to IP discovery during rediscovery.



Discovered Products

Product	Name	IP Address	Product Type	Serial #	Status	Vendor	Model	Port Count	Firmware	Build Label	Location
DCM-TI24X-2...	DCM-TI24X-2...	10.24.60.203	L2 Switch	BFF2337E03C	Reachable	Brocade	TurboIron	28	04.1.00a	TIS04100a	Lab
DCM-NICES2...	DCM-NICES2...	10.24.60.204	Router	D4SA40E02A	Reachable	Brocade	NetIron 2000	25	ce05100b330	V5.1.00b330	Lab
DCM-FGS64...	DCM-FGS64...	10.24.60.205	L2 Switch	CY49084541	Reachable	Brocade	FGS/FLS/STK	48	04.3.01T7e1	FGS04301	Lab
DCM-FGS64...	DCM-FGS64...	10.24.60.206	L2 Switch	CY49084603	Reachable	Brocade	FGS/FLS/STK	48	04.3.01T7e1	FGS04301	Lab
DCM-FGS64...	DCM-FGS64...	10.24.60.207	L2 Switch	CY49084573	Reachable	Brocade	FGS/FLS/STK	48	04.3.01T7e1	FGS04301	Lab
ServerIronA...	ServerIronA...	20.20.20.54	Load Balancer	INVALID-1U	Reachable	Brocade	ServerIron	11	12.2.00T403	ASR12200b...	

FIGURE 16 Discover Setup - IP dialog box

2. Click the **Global Settings** tab.
    a. To set SNMP credentials, refer to "IP SNMP credentials" on page 83.
    b. To configure default user names and passwords, refer to "Default IP user credentials" on page 89.
    c. To configure global setting preferences, refer to "Defining global setting preferences" on page 97.
3. Click the **Profiles** tab.
    a. To create a discovery profile, refer to "IP discovery profiles" on page 101.
    b. To include and exclude product types, refer to "IP Object identifier filters" on page 95.
    c. To include and exclude devices and enable ping sweep, refer to "Configuring address ranges" on page 104.
    d. To configure profile preferences, refer to "Configuring advanced discovery profile preferences" on page 116.
4. Click **Start** to start discovery. To run profile discovery, refer to "Starting discovery manually" on page 118.
5. Click **Close** to close the **Discover Setup - IP** dialog box.
6. Click **Yes** on the confirmation message.

Configuring IP simple discovery

NOTE
The **Discovered Products** table lists all products discovered through individual product discovery, profile-based discovery, as well as Fabric discovery (from the **SAN** tab).

NOTE
DCB devices discovered through Fabric discovery (from the **SAN** tab) are automatically added to IP discovery during rediscovery.

NOTE
You must have the **All IP Products** AOR (area of responsibility) in your user account to discover new products. For more information about user accounts, refer to "User accounts" on page 241.

To configure simple discovery, complete the following steps.

1. Select **Discover > IP Products.**

    The **Discover Setup - IP** dialog box displays.
2. To add individual devices, refer to "Adding an IP device to discovery" on page 121.
3. Click **Close** to close the **Discover Setup - IP** dialog box.
4. Click **Yes** on the confirmation message.

IP SNMP credentials

NOTE
The Management application supports SNMPv1, SNMPv2c, and SNMPv3.

The Management application requires SNMP credentials to obtain information from devices and to deploy configurations to devices. Because different devices may have different credentials, discovery can store many sets of credentials to make sure that the correct credentials are available when contacting a device.

Two types of credentials can be used for discovery: SNMPv1 and SNMPv2c read-write community strings and SNMPv3 read-write credentials. If SNMPv1 or SNMPv2c is enabled on a device, use read-write community strings. If SNMPv3 is enabled on a device, use SNMPv3 read-write credentials.

When a device is contacted, discovery tries the credentials in the order that they are listed on the **SNMP** tab on the **Global Setting** tab of the **Discover Setup - IP** dialog box until it finds one that matches the credentials on the device. Discovery tries the SNMPv3 credentials first. If none of the SNMPv3 credentials work, discovery tries the SNMPv1 and SNMPv2c credentials. Discovery must detect the read only credentials to proceed to the read-write credentials. If discovery does not detect any read-write credential, the device may still be discovered; however, all write operations through SNMP (such as configure device) do not execute properly. When a match is found, the device becomes discovered to the Management application, and its properties are saved in the database so that it can be managed by the Management application.

Devices not discovered through profile-based discovery can be added individually. For more information, refer to "Adding an IP device to discovery" on page 121.

Adding SNMPv1 and SNMPv2c credentials

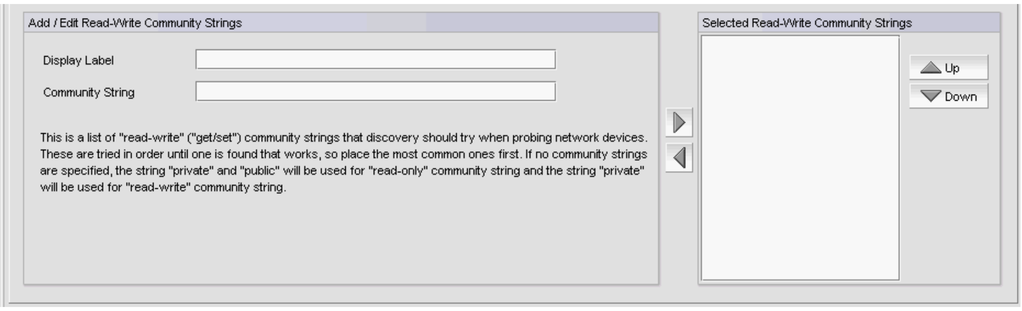
If SNMPv1 or SNMPv2c is enabled, or if you want to use community strings to gain access to the device, define community strings.

To add a SNMPv1 or SNMPv2c read-write community string, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.


Add / Edit Read-Write Community Strings
Display Label
Community String
Selected Read-Write Community Strings
Up
Down

This is a list of "read-write" ("get/set") community strings that discovery should try when probing network devices. These are tried in order until one is found that works, so place the most common ones first. If no community strings are specified, the string "private" and "public" will be used for "read-only" community string and the string "private" will be used for "read-write" community string.

FIGURE 17 **SNMPv1 or SNMPv2c credentials**

4. Enter a unique label to identify the community string in the **Display Label** field of the **Add/Edit Read-Write Community Strings** list.

   This label can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

5. Enter the unique community string in the **Community Strings** field.

   The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

6. Click the right arrow button to add the read-write community string to the **Selected Read-Write Community Strings** list.

   NOTE
   Discovery uses the read-write community string to detect both SNMP read and SNMP write community strings.

   If the devices use multiple community strings, use the **Up** or **Down** buttons to place the most commonly used community string at the top of the **Selected Read-Write Community Strings** list to make discovery run more efficiently.

   NOTE
   If the **Selected Read-Write Community Strings** list does not contain any community strings, the Management application uses the "public" and "private" community strings.

7. Click **Apply** to save your work.

8. Click **Close** to close the **Discover Setup - IP** dialog box.

9. Click **Yes** on the confirmation message.

Adding SNMPv3 credentials

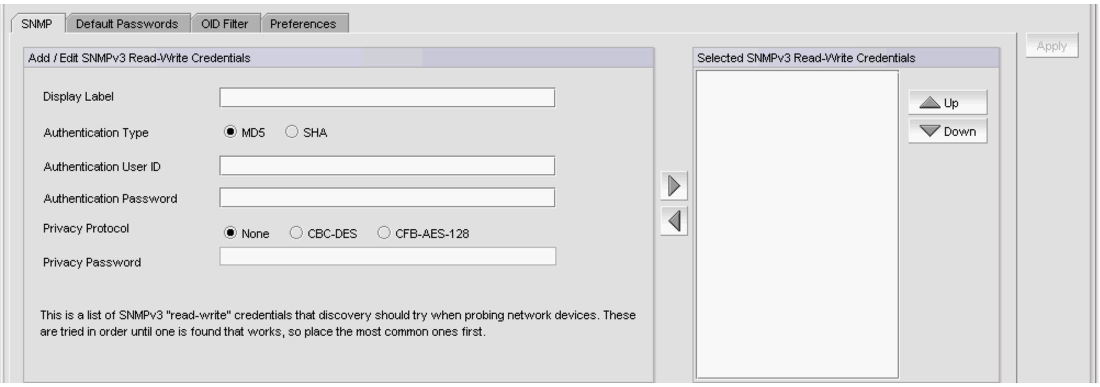
To add SNMPv3 read-write credentials, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.

3. Click the **SNMP** tab.


SNMP
Default Passwords
OID Filter
Preferences
Apply
Add / Edit SNMPv3 Read-Write Credentials
Selected SNMPv3 Read-Write Credentials
Up
Down

Display Label
Authentication Type ● MD5 ○ SHA
Authentication User ID
Authentication Password
Privacy Protocol ● None ○ CBC-DES ○ CFB-AES-128
Privacy Password

This is a list of SNMPv3 "read-write" credentials that discovery should try when probing network devices. These are tried in order until one is found that works, so place the most common ones first.

FIGURE 18 SNMPv3 credentials

4. Enter a unique label to identify the credentials in the **Display Label** field of the **Add/Edit SNMPv3 Read-Write Credentials** area.

   This label can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

5. Enter the SNMPv3 user name in the **User ID** field.

   The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

6. Select one of the following protocols from the **Authentication Protocol** list:

   - None
   - HMAC_MD5
   - HMAC_SHA

7. Enter the SNMPv3 authentication password in the **Authentication Password** field.

   The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password displays as asterisks.

8. Select one of the following protocols from the **Privacy Protocol** list:

   - None
   - CBC-DES
   - CFB_AES-128

   If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

9. Enter the privacy password in the **Privacy Password** field.

   The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password displays as asterisks.

10. Click the right arrow button to add the SNMPv3 read-write credentials to the **Selected SNMPv3 Read-Write Credentials** list.

    NOTE
    If the devices use multiple credentials, use the **Up** or **Down** buttons to place the most commonly used credentials at the top of the **Selected SNMPv3 Read-Write Credentials** list to make discovery run more efficiently.

11. Click **Apply** to save your work.

12. Click **Close** to close the **Discover Setup - IP** dialog box.

13. Click **Yes** on the confirmation message.

Editing SNMPv1 and SNMPv2c credentials

To edit a SNMPv1 or SNMPv2c read-write community string, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.
4. Select the community string you want to edit in the **Selected Read-Write Community Strings** list and click the left arrow button.

   The selected credentials display in the **Add/Edit Read-Write Community Strings** area.

5. Enter a unique label to identify the community string in the **Display Label** field the **Add/Edit Read-Write Community Strings** area.

   This label can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

6. Enter the unique community string in the **Community Strings** field.

   The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

7. Click the right arrow button to add the read-write community string to the **Selected Read-Write Community Strings** list.

   NOTE
   If the devices use multiple community strings, use the **Up** or **Down** buttons to place the most commonly used community string at the top of the **Selected Read-Write Community Strings** list to make discovery run more efficiently.

   NOTE
   If the **Selected Read-Write Community Strings** list does not contain any community strings, the Management application uses the "public" and "private" community strings.

8. Click **Apply** to save your work.
9. Click **Close** to close the **Discover Setup - IP** dialog box.
10. Click **Yes** on the confirmation message.

Editing SNMPv3 credentials

To edit SNMPv3 read-write credentials, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.

4. Select the SNMPv3 credentials you want to edit in the **Selected SNMPv3 Read-Write Credentials** list and click the left arrow button.

   The selected credentials display in the **Add/Edit SNMPv3 Read-Write Credentials** area.

5. Enter a unique label to identify the credentials in the **Display Label** field of the **Add/Edit SNMPv3 Read-Write Credentials** area.

   This label can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

6. Enter the SNMPv3 user name in the **User ID** field.

   The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

7. Select one of the following protocols from the **Authentication Protocol** list:

   - None
   - HMAC_MD5
   - HMAC_SHA

8. Enter the SNMPv3 authentication password in the **Authentication Password** field.

   The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

9. Select one of the following protocols from the **Privacy Protocol** list:

   - None
   - CBC-DES
   - CFB_AES-128

   If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

10. Enter the privacy password in the **Privacy Password** field.

    The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

11. Click the right arrow button to add the SNMPv3 read-write credentials to the **Selected SNMPv3 Read-Write Credentials** list.

    NOTE
    If the devices use multiple credentials, use the **Up** or **Down** buttons to place the most commonly used credentials at the top of the **Selected SNMPv3 Read-Write Credentials** list to make discovery run more efficiently.

12. Click **Apply** to save your work.

13. Click **Close** to close the **Discover Setup - IP** dialog box.

14. Click **Yes** on the confirmation message.

Reordering SNMP credentials in the list

Discovery probes the network for devices, according to the order in the list of SNMPv3 read-write credentials or SNMPv1 or SNMPv2c read-write community strings. Discovery uses the first item to find devices that are associated with those credentials or community strings, then continues down the list. Therefore, place the most commonly used credentials or community strings first.

To rearrange the SNMPv3 read-write credentials or SNMPv1 or SNMPv2c read-write community strings lists, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.
4. Select an entry in the **Selected SNMPv3 Read-Write Credentials** or **Selected Read-Write Community Strings** list and use the **Up** and **Down** buttons to rearrange the entries.
5. Click **Apply** to save your work.
6. Click **Close** to close the **Discover Setup - IP** dialog box.
7. Click **Yes** on the confirmation message.

Deleting SNMP credentials from the list

To delete an entry from the SNMPv3 read-write credentials or SNMPv1 or SNMPv2c read-write community strings lists, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **SNMP** tab.
4. Choose one of the following options:
   - Select the SNMPv3 read-write credentials you want to delete in the **Selected SNMPv3 Read-Write Credentials** list and click the left arrow button.
   - Select the SNMPv1 or SNMPv2c read-write community string you want to delete in the **Selected Read-Write Community Strings** list and click the left arrow button.
5. Click **Apply** to save your work.
6. Click **Close** to close the **Discover Setup - IP** dialog box.
7. Click **Yes** on the confirmation message.

Default IP user credentials

The Management application uses default user names and passwords to access devices when contacting these devices through the command line interface (CLI) on the network. You can enter a list of default names and passwords in the Management application before running discovery. Discovery uses this list to contact devices to determine the correct user name and password for the device. The first time discovery contacts a device, the Management application enters the default names and passwords for the device into the Management application database. This feature saves you the trouble of entering authentication passwords for every newly discovered device.

NOTE
Discovery does not remove an invalid user name or password from the device information unless it is able to replace it with a valid one.

The Management application groups default user names and passwords by the following password types:

- **Read/Write Login Prompt** — The login prompt the device uses when logging in by Telnet or CLI to the device.
- **Read/Write Enable Prompt** — The enable prompt the device uses in CLI mode to go to device enable mode.
- **Enable Super User** — The super user enable password configured on the device for Telnet login. You can configure the super user enable password by using the **enable super-user-password** CLI command. The super user enable password can be used to authenticate users with the super user privilege configured on the device.

You can define more than one password for each password type. Discovery uses the passwords in the order they are listed when it probes the devices.

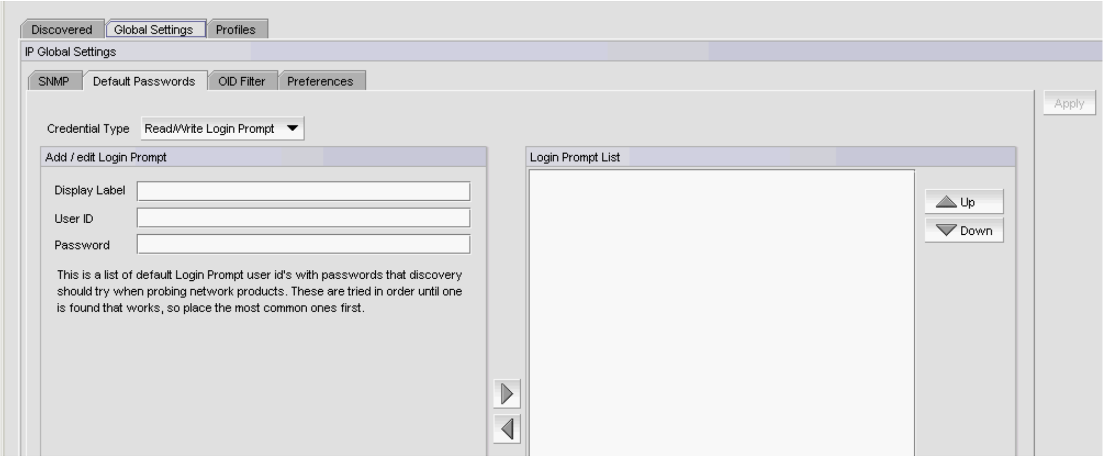
Adding user credentials

To add default user names and passwords, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.

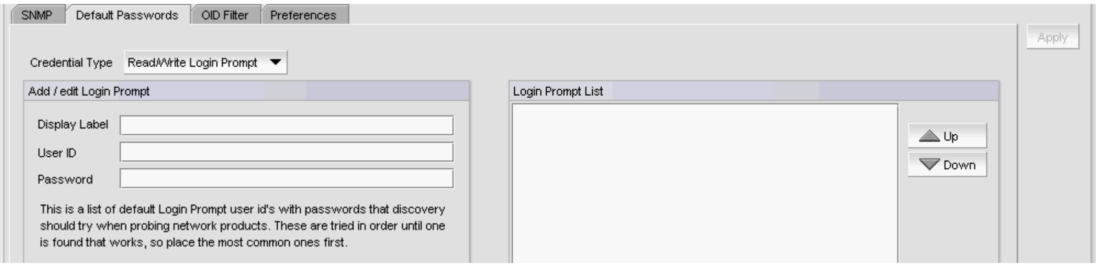


Credential Type Read/Write Login Prompt

This is a list of default Login Prompt user id's with passwords that discovery should try when probing network products. These are tried in order until one is found that works, so place the most common ones first.

FIGURE 19 Default Passwords

4. Enter a login prompt user name and password by selecting **Read/Write Login Prompt** from the **Credential Type** list and completing the following steps.



Credential Type Read/Write Login Prompt

This is a list of default Login Prompt user id's with passwords that discovery should try when probing network products. These are tried in order until one is found that works, so place the most common ones first.

FIGURE 20 Read/Write Login Prompt

a. Enter a unique label to identify the credentials in the **Display Label** field.

   This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

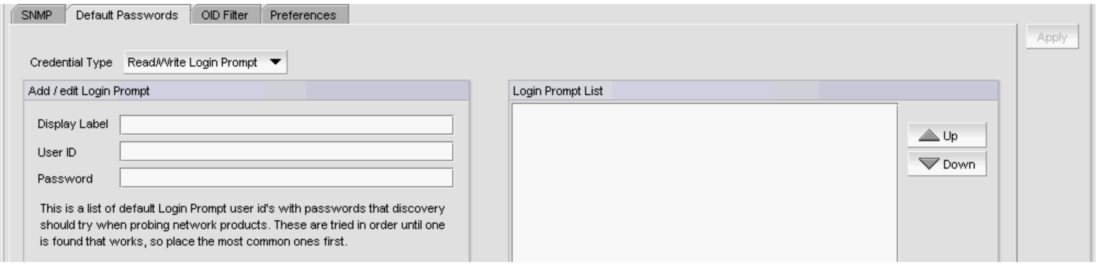
b. Enter the user name in the **User ID** field.

c. Enter the user password in the **Password** field.

d. Click the right arrow button.

e. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Login Prompt** list to make discovery run more efficiently.

5. Enter an enable prompt user name and password by selecting **Read/Write Enable Prompt** from the **Credential Type** list and completing the following steps.



Credential Type: Read/Write Login Prompt

This is a list of default Login Prompt user id's with passwords that discovery should try when probing network products. These are tried in order until one is found that works, so place the most common ones first.

FIGURE 21 **Read/Write Enable Prompt**

   a. Enter a unique label to identify the credentials in the **Display Label** field.

      This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

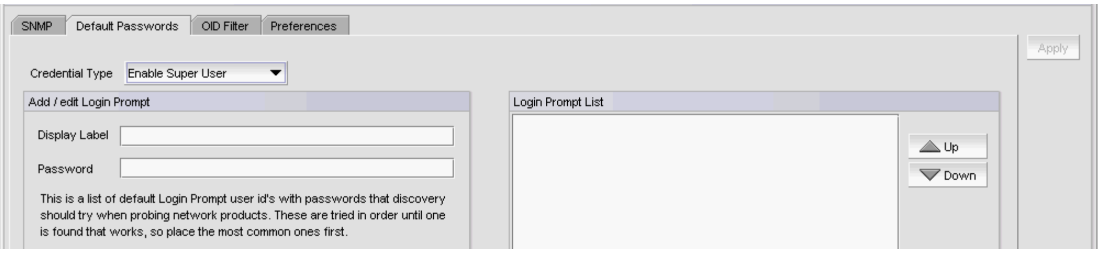
   b. Enter the user name in the **User ID** field.

   c. Enter the user password in the **Password** field.

   d. Click the right arrow button.

   e. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Enable Prompt** list to make discovery run more efficiently.

6. Enter a super user password by selecting **Enable Super User** from the **Credential Type** list and completing the following steps.



Credential Type: Enable Super User

This is a list of default Login Prompt user id's with passwords that discovery should try when probing network products. These are tried in order until one is found that works, so place the most common ones first.

FIGURE 22 **Enable Super User**

   a. Enter a unique label to identify the credentials in the **Display Label** field.

      This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

   b. Enter the super user password in the **Password** field.

   c. Click the right arrow button.

   d. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Enable Super User** list to make discovery run more efficiently.

7. Click **Apply** to save your work.

8. Click **Close** to close the **Discover Setup - IP** dialog box.
9. Click **Yes** on the confirmation message.

Editing login prompt user credentials

To edit a login prompt user name and password, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select **Read/Write Login Prompt** from the **Credential Type** list.
5. Select the user credential entry you want to edit in the **Login Prompt List** and click the left arrow button.

   The selected credentials display in the **Add/edit Login Prompt** area.
6. Edit the unique label to identify the credentials in the **Display Label** field.

   This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.
7. Edit the user name in the **User ID** field.
8. Edit the user password in the **Password** field.
9. Click the right arrow button.
10. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Login Prompt List** to make discovery run more efficiently.
11. Click **Apply** to save your work.
12. Click **Close** to close the **Discover Setup - IP** dialog box.
13. Click **Yes** on the confirmation message.

Editing enable prompt user credentials

To edit an enable prompt user name and password, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select **Read/Write Enable Prompt** from the **Credential Type** list.
5. Select the user credential entry you want to edit in the **Login Prompt List** and click the left arrow button.

   The selected credentials display in the **Add/edit Login Prompt** area.

6. Edit the unique label to identify the credentials in the **Display Label** field.

   This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

7. Edit the user name in the **User ID** field.
8. Edit the user password in the **Password** field.
9. Click the right arrow button.
10. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Login Prompt List** to make discovery run more efficiently.
11. Click **Apply** to save your work.
12. Click **Close** to close the **Discover Setup - IP** dialog box.
13. Click **Yes** on the confirmation message.

Editing enable super user credentials

To edit an enable super user, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select **Enable Super User** from the **Credential Type** list.
5. Select the user credential entry you want to edit in the **Login Prompt List** and click the left arrow button.

   The selected credentials display in the **Add/edit Login Prompt** area.

6. Edit the unique label to identify the credentials in the **Display Label** field.

   This label can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

7. Edit the super user password in the **Password** field.
8. Click the right arrow button.
9. If the devices use multiple user names and passwords, use the **Up** or **Down** buttons to place the most commonly used at the top of the **Login Prompt List** to make discovery run more efficiently.
10. Click **Apply** to save your work.
11. Click **Close** to close the **Discover Setup - IP** dialog box.
12. Click **Yes** on the confirmation message.

Reordering user credentials in the list

Discovery tries the user credentials in order until one set of credentials is found that works, so place the most common ones first.

To rearrange the user credentials, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select one of the following password types from the **Credential Type** list:
   - Read/Write Login Prompt
   - Read/Write Enable Prompt
   - Enable Super User
5. Select an entry in the **Login Prompt List** and use the **Up** and **Down** buttons to rearrange the entries.
6. Click **Apply** to save your work.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

Deleting user credentials from the list

To delete an entry from the SNMPv3 read-write credentials or SNMPv1 or SNMPv2c read-write community strings lists, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Default Passwords** tab.
4. Select one of the following password types from the **Credential Type** list:
   - Read/Write Login Prompt
   - Read/Write Enable Prompt
   - Enable Super User
5. Select an entry in the **Login Prompt List** and click the left arrow button.
6. Click **Apply** to save your work.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

IP Object identifier filters

The object identifier (OID) filter allows you to select which product types to include or exclude from discovery.

If you add a third-party product OID to the **Included Product Types** list during discovery and later move it to the **Excluded Product Types** list, note that you will not be able to discover a new device with that product OID. However, other functionality such as traps, fault management, statistics, performance data collection, product polling for health monitoring and so on continue to run as with any other discovered product.

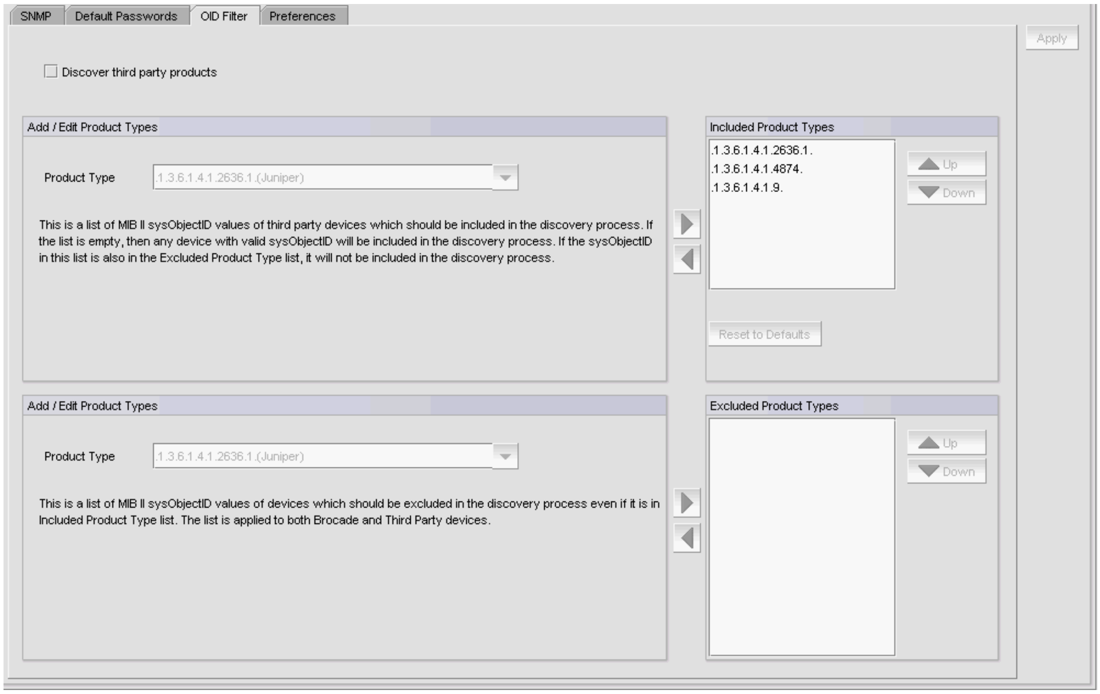
Including product types

To include third-party product types in discovery, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **OID Filter** tab.



□ Discover third party products

Product Type: .1.3.6.1.4.1.2636.1.(Juniper)

This is a list of MIB II sysObjectID values of third party devices which should be included in the discovery process. If the list is empty, then any device with valid sysObjectID will be included in the discovery process. If the sysObjectID in this list is also in the Excluded Product Type list, it will not be included in the discovery process.

Included Product Types:
.1.3.6.1.4.1.2636.1.
.1.3.6.1.4.1.4874.
.1.3.6.1.4.1.9.

Product Type: .1.3.6.1.4.1.2636.1.(Juniper)

This is a list of MIB II sysObjectID values of devices which should be excluded in the discovery process even if it is in Included Product Type list. The list is applied to both Brocade and Third Party devices.

FIGURE 23 **OID Filter tab**

4. Select the **Discover third party products** check box to include third-party devices in discovery.

5. In the top **Add/Edit Product Types** area, choose one of the following options:
   - Enter the device's sysObjectID you want to include in the **Product Type** list.
   - Select an existing device sysObjectID from the **Product Type** list.

   Table 26 lists the default third party product types.

   TABLE 26 Default third-party product types

Product sysObjectID	Vendor
.1.3.6.1.4.1.9.	Cisco
.1.3.6.1.4.1.4874.	Juniper
.1.3.6.1.4.1.2636.1.	Juniper

6. Click the right arrow button to add the product type to the **Included Product Types** list.

   The **Included Product Types** list displays the third-party device sysObjectIDs to include in discovery. If this list is empty, discovery includes any device with a valid sysObjectID. If a sysObjectID in this list is also in the **Excluded Product Types** list, discovery excludes it.
7. Click **Apply** to save your work.
8. Click **Close** to close the **Discover Setup - IP** dialog box.
9. Click **Yes** on the confirmation message.

Excluding product types

To exclude third-party product types from discovery, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **OID Filter** tab.
4. In the bottom **Add/Edit Product Types** area, choose one of the following options:
   - Enter the device's sysObjectID you want to include in the **Product Type** list.
   - Select an existing device sysObjectID from the **Product Type** list.

   Table 26 lists the default third party product types.
5. Click the right arrow button to add the product type to the **Excluded Product Types** list.

   The **Excluded Product Types** list displays the third-party device sysObjectiDs to exclude from discovery. If a sysObjectID in this list is also in the **Included Product Types** list, discovery excludes it.
6. Click **Apply** to save your work.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

Deleting product types from the list

To delete an entry from the **Included Product Types** or **Excluded Product Type** list, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **OID Filter** tab.
4. Select an entry from the **Included Product Types** or **Excluded Product Type** list and click the left arrow button.
5. Click **Apply** to save your work.
6. Click **Close** to close the **Discover Setup - IP** dialog box.
7. Click **Yes** on the confirmation message.

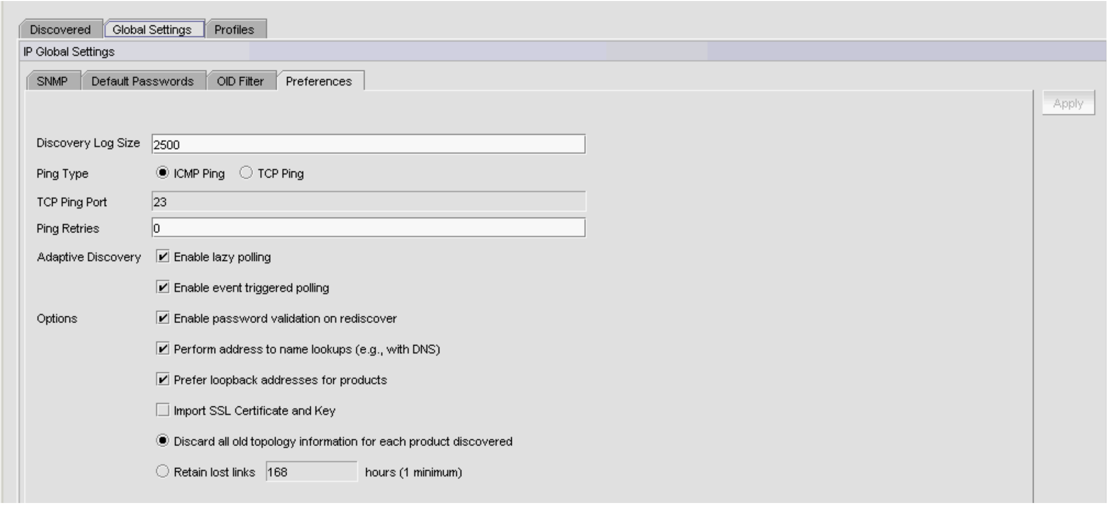
Defining global setting preferences

To define global setting preferences, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Global Settings** tab.
3. Click the **Preferences** tab.



Discovery Log Size 2500

Ping Type ● ICMP Ping ○ TCP Ping

TCP Ping Port 23

Ping Retries 0

Adaptive Discovery ☑ Enable lazy polling

☑ Enable event triggered polling

Options ☑ Enable password validation on rediscover

☑ Perform address to name lookups (e.g., with DNS)

☑ Prefer loopback addresses for products

□ Import SSL Certificate and Key

● Discard all old topology information for each product discovered

○ Retain lost links 168 hours (1 minimum)

FIGURE 24 **Preferences tab**

4. Enter a value (from 32 through 10000) for the number of live discovery log messages to store on the server in the **Discovery Log Size** field.

   The default is 2500.

5. Select one of the following **Ping Type** options:
   - **ICMP Ping** (default). Go to step 7.
   - **TCP Ping**. Continue with step 6.
6. Enter the TCP port number (from 1 through 65536) in the **TCP Ping Port** field.

   The default is 23.
7. Enter the number of times (from 0 through 10) to ping the device when ping is unsuccessful in the **Ping Retries** field.

   The default is 0.
8. Select the **Enable lazy polling** check box to periodically rediscover all devices in the database.

   NOTE
   This setting cannot be disabled for DCB switches.

   The lazy polling function sends login and log messages to the Master Log and the switch console. If you are receiving too many messages due to lazy polling, clear the check box to disable off lazy polling.

   You cannot change the lazy polling interval for IronWare OS or Network OS devices. The lazy polling interval is based on the size of your network. For IronWare OS devices, default values are as follows:
   - Small: 2 minutes
   - Medium: 15 minutes
   - Large: 30 minutes

   For Network OS devices, default values are as follows:
   - Small: 15 minutes
   - Medium: 30 minutes
   - Large: 60 minutes
9. Select the **Enable event triggered polling** check box to enable adaptive discovery on the predefined SNMP traps.

   NOTE
   This setting cannot be disabled for DCB switches.

   NOTE
   Network OS devices must be running version 4.0 or later to enable this setting.

   NOTE
   For Network OS devices, adaptive discovery is also performed for Syslog events.
10. Select the **Enable password validation on rediscover** check box to enable CLI user credential validation when rediscovering devices.
11. Select the **Perform address to name lookups (e.g. with DNS)** check box to configure discovery to use the local DNS server for address-to-name resolution.

12. Select the **Prefer loopback addresses for products** check box to enable discovery to choose an IP address associated with a router loopback interface to be the router primary IP address.

    Clear the check box to configure discovery to select the original IP address used to discover the device.

13. Select the **Import SSL Certificate and Key** check box to enable discovery to download and synchronize certificates from SSL capable Application products.

14. Choose one of the following options:

    - Select the **Discard all old topology information for each product discovered** option to delete all existing device topology data when running discovery.
    - Select the **Retain lost links __ hours (1 minimum)** option to configure how long to retain lost links on the topology maps and enter a value (from 1 through 9999) in the field. The default is 168 hours.

15. Click **Apply** to save your work.

16. Click **Close** to close the **Discover Setup - IP** dialog box.

17. Click **Yes** on the confirmation message.

Configuring event-based collection

If you discover more than 550 IP products, the Management application automatically turns off event-based collection. To restart event-based collection, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

   The **Discover Setup - IP** dialog box displays.

2. Reduce the managed count by completing the following steps.

   a. Select the IP devices you want to remove from discovery in the **Discovered Products** table.

      Select multiple devices by holding down the CTRL key and clicking more than one device.

      NOTE
      You cannot delete an active member from a VCS fabric.

   b. Click **Delete**.

3. Turn on event-based collection by completing the following steps.

   a. Click the **Global Settings** tab.

   b. Click the **Preferences** tab.

   c. Select the **Enable lazy polling** check box to periodically rediscover all devices in the database.

      NOTE
      This settings cannot be disabled for DCB switches.

d. Select the **Enable event triggered polling** check box to enable adaptive discovery on the predefined SNMP traps.

NOTE
This settings cannot be disabled for DCB switches.

NOTE
Network OS devices must be running version 4.0 or later to enable this setting.

NOTE
For Network OS devices, adaptive discovery is also performed for Syslog events.

The lazy polling function sends login and log messages to the Master Log and the switch console. If you are receiving too many messages due to lazy polling, clear the check box to disable off lazy polling.

You cannot change the lazy polling interval for IronWare OS or Network OS devices. The lazy polling interval is based on the size of your network. For IronWare OS devices, default values are as follows:

- Small: 2 minutes
- Medium: 15 minutes
- Large: 30 minutes

For Network OS devices, default values are as follows:

- Small: 15 minutes
- Medium: 30 minutes
- Large: 60 minutes

e. Click **Apply** to save your work.

4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

IP discovery profiles

NOTE
You cannot configure a discovery profile if you do not have the All IP Products AOR (area of responsibility) in your user account.

A discovery profile contains the settings you configure when discovery is run. These settings include address range parameters, ping sweep parameters, SNMP settings, default passwords, and other settings. The Management application is shipped with a default discovery profile named “Default”. You can create more than one discovery profile. You can select one discovery profile to run automatically at startup. After startup, one or more profiles can be run consecutively.

NOTE
The Discovered Products table lists all products discovered through individual product discovery, profile-based discovery, as well as Fabric discovery (from the SAN tab).

NOTE
DCB devices discovered through Fabric discovery (from the SAN tab) are automatically added to IP discovery during rediscovery.

Configuring a discovery profile

NOTE
You cannot configure a discovery profile if you do not have the All IP Products AOR (area of responsibility) in your user account.

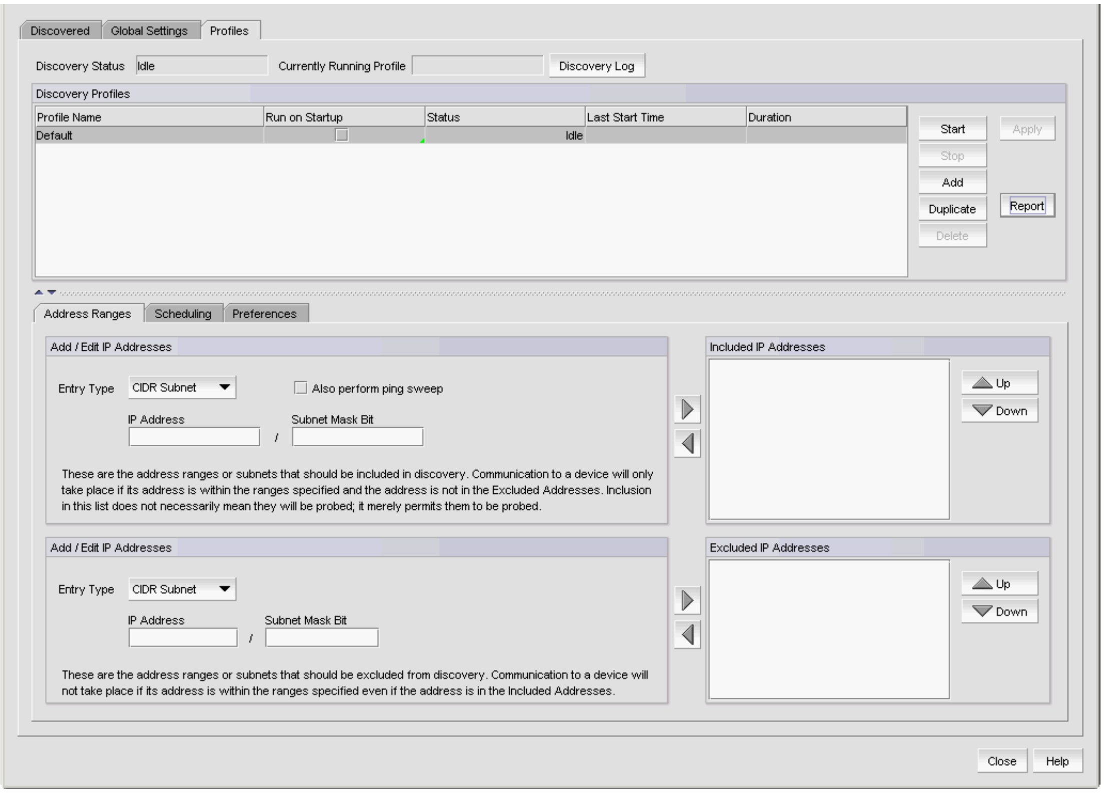
NOTE
DCB devices discovered through Fabric discovery (from the SAN tab) are automatically added to IP discovery during rediscovery.

To configure a discovery profile, complete the following steps.

1. Select Discover > IP Products.

   The Discover Setup - IP dialog box displays.

2. Click the Profiles tab



Discovery Status: Idle

Profile Name	Run on Startup	Status	Last Start Time	Duration
Default	□	Idle		

These are the address ranges or subnets that should be included in discovery. Communication to a device will only take place if its address is within the ranges specified and the address is not in the Excluded Addresses. Inclusion in this list does not necessarily mean they will be probed; it merely permits them to be probed.

These are the address ranges or subnets that should be excluded from discovery. Communication to a device will not take place if its address is within the ranges specified even if the address is in the Included Addresses.

FIGURE 25 Profile tab

3. Click **Add**.

   A new row (named "new_profile") displays in the **Discovery Profiles** table.

4. Click "new_profile" in the **Profile Name** field to enter a unique name for the profile.

   This name can be from 1 through 255 characters long, case sensitive, and allows all printable ASCII characters.

5. Click the **Address Ranges** tab to configure address ranges for the profile.

   For step-by-step instructions, refer to "Configuring address ranges" on page 104.

6. Click the **Scheduling** tab to configure a discovery schedule for the profile.

   For step-by-step instructions, refer to "Scheduling discovery" on page 109.

7. Click the **Preferences** tab to configure preferences for the profile.

   For step-by-step instructions, refer to "Configuring advanced discovery profile preferences" on page 116.

8. Click the **Global Settings** tab.

   To set SNMP credentials, refer to "IP SNMP credentials" on page 83.

   To configure default user names and passwords, refer to "Default IP user credentials" on page 89.

   To configure global setting preferences, refer to "Defining global setting preferences" on page 97.

9. Click **Apply** to save your changes.
10. Click **Close** to close the **Discover Setup - IP** dialog box.
11. Click **Yes** on the confirmation message.

Duplicating a discovery profile

NOTE
You cannot duplicate a discovery profile if you do not have the **All IP Products** AOR (area of responsibility) in your user account.

NOTE
DCB devices discovered through Fabric discovery (from the **SAN** tab) are automatically added to IP discovery during rediscovery.

To duplicate a discovery profile, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab
3. Select the profile you want to copy and click **Duplicate.**

   A new row (named “Copy of *profile_name*”) displays in the **Discovery Profiles** table
4. Click “Copy of *profile_name*” in the **Profile Name** field to enter a unique name for the profile.

   This name can be from 1 through 255 characters long, case sensitive, and allows all printable ASCII characters.
5. Click the **Address Ranges** tab to configure address ranges for the profile.

   For step-by-step instructions, refer to “Configuring address ranges” on page 104 or “Editing address ranges” on page 108.
6. Click the **Scheduling** tab to configure a discovery schedule for the profile.

   For step-by-step instructions, refer to “Scheduling discovery” on page 109.
7. Click the **Preferences** tab to configure preferences for the profile.

   For step-by-step instructions, refer to “Configuring advanced discovery profile preferences” on page 116.
8. Click the **Global Settings** tab.

   To set SNMP credentials, refer to “IP SNMP credentials” on page 83.

   To configure default user names and passwords, refer to “Default IP user credentials” on page 89.

   To configure global setting preferences, refer to “Defining global setting preferences” on page 97.
9. Click **Apply** to save your changes.
10. Click **Close** to close the **Discover Setup - IP** dialog box.
11. Click **Yes** on the confirmation message.

Configuring address ranges

NOTE
DCB devices discovered through Fabric discovery (from the **SAN** tab) are automatically added to IP discovery during rediscovery.

To include and exclude addresses from profile discovery, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab

3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Address Ranges** tab.

4. Include an address range by choosing one of the following options:

   - To include an address range using the CIDR subnet format, refer to "Adding CIDR subnet addresses" on page 105.
   - To include an address range using the subnet format, refer to "Adding subnet addresses" on page 105.
   - To include an address range using the address range format, refer to "Adding IP addresses" on page 106.
   - **To include all addresses, sele**ct all addresses fr**om the Entry Type list.**

5. Select the **Also perform ping sweep** check box to perform ping sweep on the address range.

6. Click the right arrow button to add the address range to the **Included IP Addresses** list.

7. Exclude an address range by choosing one of the following options:

   - To exclude an address range using the CIDR subnet format, refer to "Excluding CIDR subnet addresses" on page 106.
   - To exclude an address range using the subnet format, refer to "Excluding subnet addresses" on page 107.
   - To exclude an address range using the address range format, refer to "Excluding IP addresses" on page 107.

   NOTE
   DCB products discovered through Fabric discovery (on the **SAN** tab) cannot be excluded.

   NOTE
   To exclude a VCS fabric, you must add all members of the VCS fabric to the exclude list.

8. Click the right arrow button to add the address range to the **Excluded IP Addresses** list.

9. Click **Apply** to save your changes.

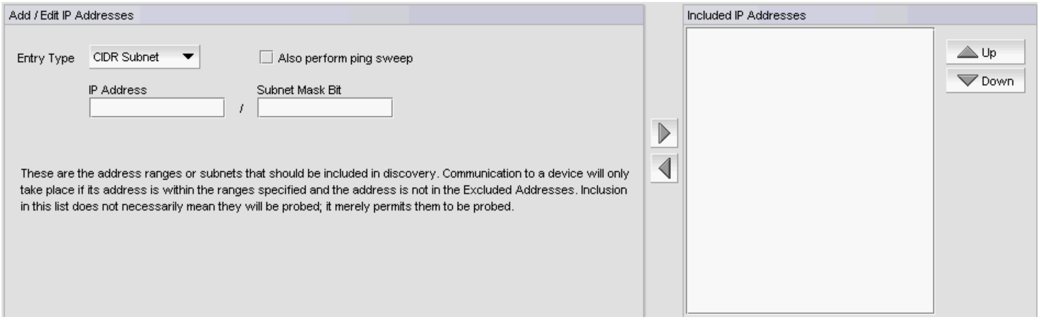
10. Click **Close** to close the **Discover Setup - IP** dialog box.

11. Click **Yes** on the confirmation message.

Adding CIDR subnet addresses

To add CIDR subnet addresses (IPv4 and IPv6), complete the following steps.

1. Select **CIDR Subnet** from the **Entry Type** list.



Entry Type: CIDR Subnet

□ Also perform ping sweep

These are the address ranges or subnets that should be included in discovery. Communication to a device will only take place if its address is within the ranges specified and the address is not in the Excluded Addresses. Inclusion in this list does not necessarily mean they will be probed; it merely permits them to be probed.

FIGURE 26 Include CIDR Subnet

2. Enter the IP address in the **IP Address** field.
3. Enter the number of subnet mask bits in the **Subnet Mask Bits** field.

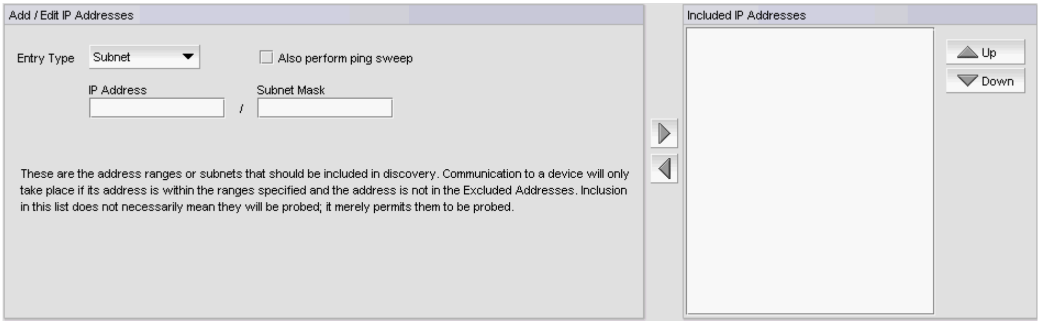
   For IPv4, the number of subnet mask bits is from 0 through 32.

   For IPv6, the number of subnet mask bits is from 0 through128.
4. **To exclude** an address range **using the CIDR Subnet format, refer to** “Excluding CIDR subnet addresses” on page 106.
5. To finish configuring the address ranges, return to “Configuring address ranges” on page 104.

Adding subnet addresses

To add subnet addresses (IPv4 only), complete the following steps.

1. Select **Subnet** from the **Entry Type** list.



Entry Type: Subnet

□ Also perform ping sweep

These are the address ranges or subnets that should be included in discovery. Communication to a device will only take place if its address is within the ranges specified and the address is not in the Excluded Addresses. Inclusion in this list does not necessarily mean they will be probed; it merely permits them to be probed.

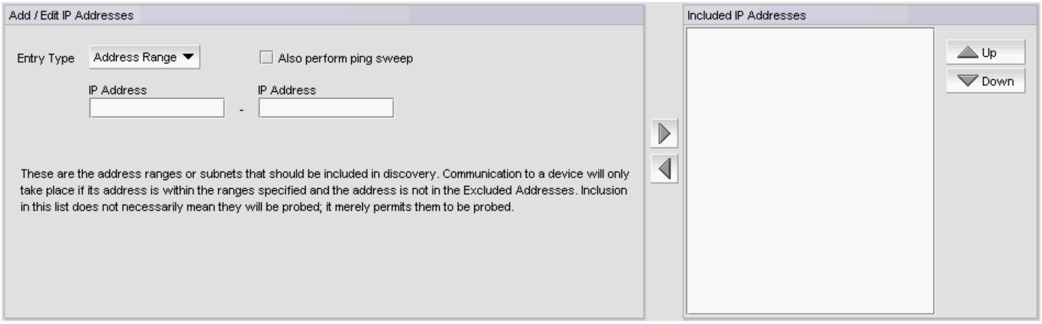
FIGURE 27 Include Subnet

2. Enter the IP address in the **IP Address** field.
3. Enter the subnet mask in the **Subnet Mask** field.
4. **To exclude** an address range **using the Subnet format, refer to** “Excluding subnet addresses” on page 107.
5. To finish configuring the address ranges, return to “Configuring address ranges” on page 104.

Adding IP addresses

To add an IP address range (IPv4 and IPv6), complete the following steps.

1. Select **IP Address** from the **Entry Type** list.



These are the address ranges or subnets that should be included in discovery. Communication to a device will only take place if its address is within the ranges specified and the address is not in the Excluded Addresses. Inclusion in this list does not necessarily mean they will be probed; it merely permits them to be probed.

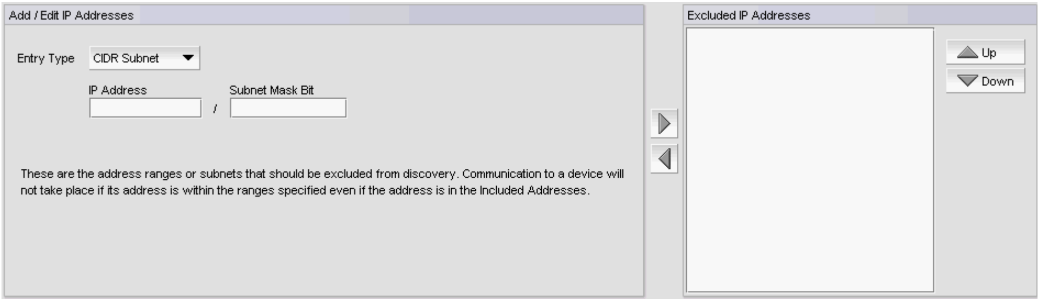
FIGURE 28 Include Address Range

2. Enter the first IP address in the range in the first **IP Address** field.
3. Enter the last IP address in the range in the second **IP Address** field.
4. **To exclude** an address range **using the IP Address format, refer to** “Excluding IP addresses” on page 107**.**
5. To finish configuring the address ranges, return to “Configuring address ranges” on page 104**.**

Excluding CIDR subnet addresses

To exclude CIDR subnet addresses (IPv4 and IPv6), complete the following steps.

1. Select **CIDR Subnet** from the **Entry Type** list.



These are the address ranges or subnets that should be excluded from discovery. Communication to a device will not take place if its address is within the ranges specified even if the address is in the Included Addresses.

FIGURE 29 Exclude CIDR Subnet

2. Enter the IP address in the **IP Address** field.
3. Enter the subnet mask bits in the **Subnet Mask Bits** field.

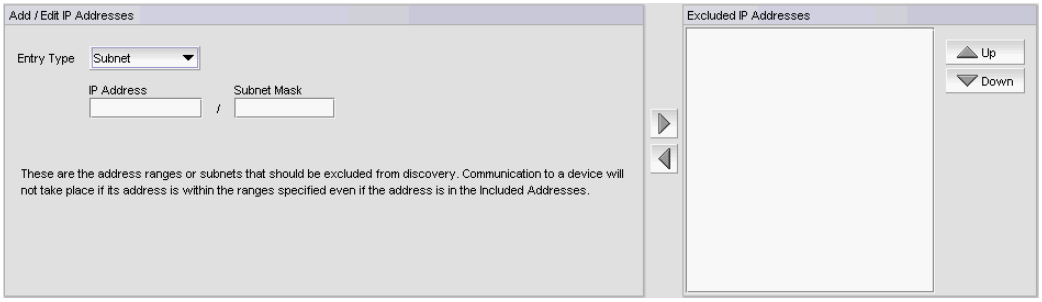
   For IPv4, the subnet mask bits is between 0 and 32.

   For IPv6, the subnet mask bits is between 0 and 128.
4. **To include** an address range **using the CIDR Subnet format, refer to** “Adding CIDR subnet addresses” on page 105**.**
5. To finish configuring the address ranges, return to “Configuring address ranges” on page 104**.**

Excluding subnet addresses

To exclude subnet addresses (IPv4 only), complete the following steps.

1. Select **Subnet** from the Entry Type list.



Entry Type: Subnet

These are the address ranges or subnets that should be excluded from discovery. Communication to a device will not take place if its address is within the ranges specified even if the address is in the Included Addresses.

FIGURE 30 Exclude Subnet

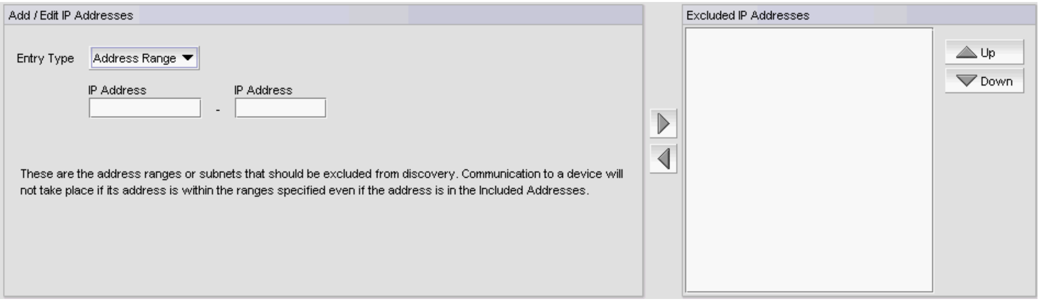
2. Enter the IP address in the **IP Address** field.
3. Enter the subnet mask in the **Subnet Mask** field.
4. **To include** an address range **using the Subnet format, refer to** "Adding subnet addresses" on page 105**.**
5. To finish configuring the address ranges, return to "Configuring address ranges" on page 104**.**

Excluding IP addresses

NOTE
To exclude a VCS fabric, you must add **all** members of the VCS fabric to the exclude list.

To exclude an IP address range (IPv4 and IPv6), complete the following steps.

1. Select **IP Address** from the **Entry Type** list.



Entry Type: Address Range

These are the address ranges or subnets that should be excluded from discovery. Communication to a device will not take place if its address is within the ranges specified even if the address is in the Included Addresses.

FIGURE 31 Exclude Address Range

2. Enter the first IP address in the range in the first **IP Address** field.
3. Enter the last IP address in the range in the second **IP Address** field.
4. **To include** an address range **using the Address Range format, refer to** "Adding IP addresses" on page 106**.**
5. To finish configuring the address ranges, return to "Configuring address ranges" on page 104**.**

Editing address ranges

NOTE
DCB devices discovered through Fabric discovery (from the **SAN** tab) are automatically added to IP discovery during rediscovery.

1. Select **Discover** > **IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab

3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Address Ranges** tab.

4. To edit an included address range, select the address range you want to edit in the **Included IP Addresses** list.

5. Click the left arrow button to display the address range details in the top **Add/Edit IP Addresses** area.

6. Edit the included address range by choosing one of the following options:

   - To edit the included addresses using the CIDR subnet format, refer to "Editing CIDR subnet addresses" on page 109.
   - To edit the included addresses using the subnet format, refer to "Editing subnet addresses" on page 109.
   - To edit the included addresses using the address range format, refer to "Editing IP addresses" on page 109.

7. Select the **Also perform ping sweep check** box to perform ping sweep on the address range.

8. To edit an excluded address range, select the address range you want to edit in the **Excluded IP Addresses** list.

9. Click the left arrow button to display the address range details in the bottom **Add/Edit IP Addresses** area.

10. Edit the excluded address range by choosing one of the following options:

    - To edit the excluded addresses using the CIDR subnet format, refer to "Editing CIDR subnet addresses" on page 109.
    - To edit the excluded addresses using the subnet format, refer to "Editing subnet addresses" on page 109.
    - To edit the excluded addresses using the address range format, refer to "Editing IP addresses" on page 109.

    NOTE
    DCB products discovered through Fabric discovery (on the **SAN** tab) cannot be excluded.

11. Click the right arrow button to add the address range to the **Excluded IP Addresses** list.

12. Click **Apply** to save your changes.

13. Click **Close** to close the **Discover Setup - IP** dialog box.

14. Click **Yes** on the confirmation message.

Editing CIDR subnet addresses

To edit the CIDR subnet address (IPv4 and IPv6) range, complete the following steps.

1. Change the IP address in the **IP Address** field.
2. Change the number of subnet mask bits in the **Subnet Mask Bits** field.

   For IPv4, the number of subnet mask bits is from 0 through 32.

   For IPv6, the number of subnet mask bits is from 0 through 128.
3. To finish editing the address ranges, return to "Editing address ranges" on page 108.

Editing subnet addresses

To edit the subnet address (IPv4 only) range, complete the following steps.

1. Change the IP address in the **IP Address** field.
2. Change the subnet mask in the **Subnet Mask** field.
3. To finish editing the address ranges, return to "Editing address ranges" on page 108.

Editing IP addresses

To edit the IP address range (IPv4 and IPv6), complete the following steps.

1. Change the first IP address in the range in the first **IP Address** field.
2. Change the last IP address in the range in the second **IP Address** field.
3. To finish editing the address ranges, return to "Editing address ranges" on page 108.

Scheduling discovery

You can create multiple schedules (to a maximum of 32) for each profile. When it is time for a schedule to run, discovery handles schedules in the following manner:

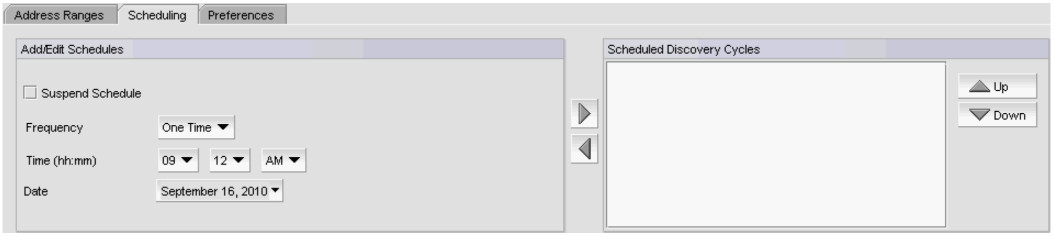
- If discovery is already running for the profile, the scheduled discovery drops.
- If discovery is already running for a different profile, the scheduled discovery is queued. Once all discovery jobs in the queue finish, the scheduled discovery runs.
- If no discovery is running, the scheduled discovery starts.

To schedule a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab

3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Scheduling** tab.



□ Suspend Schedule

Frequency: One Time

Time (hh:mm): 09 12 AM

Date: September 16, 2010

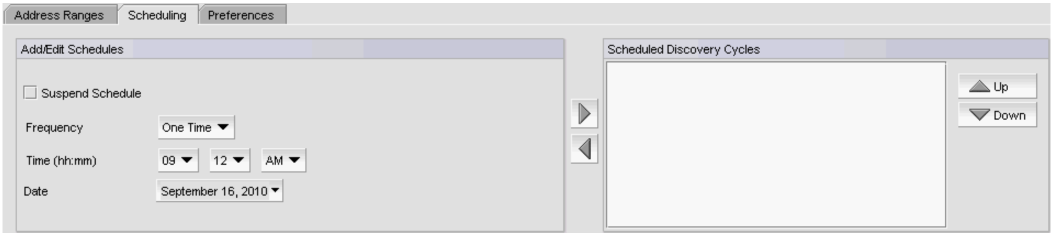
FIGURE 32 Scheduling tab

4. Choose one of the following options to configure the frequency at which discovery runs for the profile:
   - To configure discovery to run only once, refer to "Configuring a one-time discovery schedule" on page 110.
   - To configure hourly discovery, refer to "Configuring an hourly discovery schedule" on page 111.
   - To configure daily discovery, refer to "Configuring a daily discovery schedule" on page 111.
   - To configure weekly discovery, refer to "Configuring a weekly discovery schedule" on page 112.
   - To configure monthly discovery, refer to "Configuring a monthly discovery schedule" on page 112.
   - To configure yearly discovery, refer to "Configuring a yearly discovery schedule" on page 113.
5. Rearrange schedules in the **Scheduled Discovery Cycles** list by selecting an item in the list and clicking the **Up** or **Down** buttons to move it.
6. Click **Apply** to save your changes.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

Configuring a one-time discovery schedule

To configure a one-time discovery schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.



□ Suspend Schedule

Frequency: One Time

Time (hh:mm): 09 12 AM

Date: September 16, 2010

FIGURE 33 Scheduling tab - One Time

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

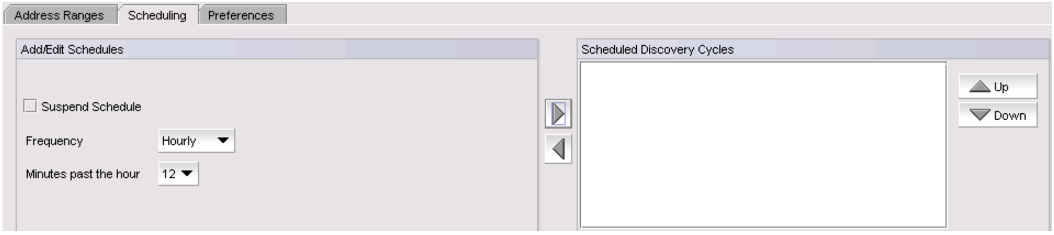
   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Click the **Date** list to select a date from the calendar.
4. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
5. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 109.

Configuring an hourly discovery schedule

To configure an hourly discovery schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.



□ Suspend Schedule

Frequency: Hourly

Minutes past the hour: 12

FIGURE 34 Scheduling tab - Hourly

2. Select the minute past the hour you want discovery to run from the **Minutes past the hour** list.

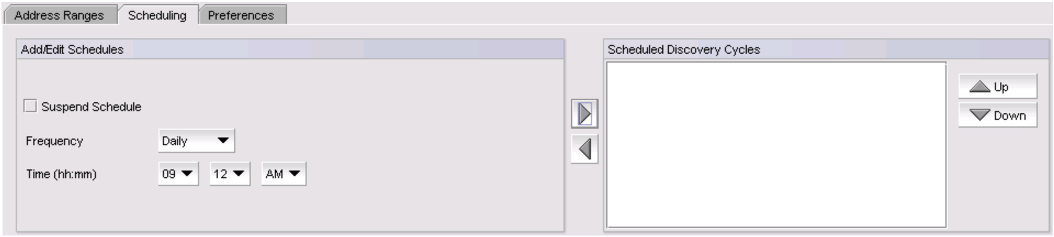
   Where the minute value is from 00 through 59.

3. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 109.

Configuring a daily discovery schedule

To configure a daily discovery schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.



□ Suspend Schedule

Frequency: Daily

Time (hh:mm): 09 12 AM

FIGURE 35 Scheduling tab - Daily

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

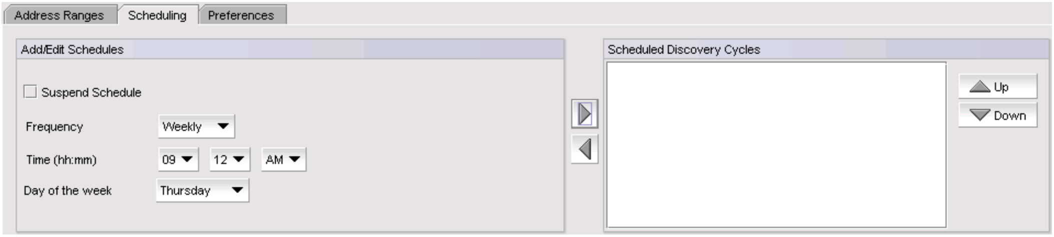
   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 109.

Configuring a weekly discovery schedule

To configure a weekly discovery schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.



□ Suspend Schedule

Frequency: Weekly

Time (hh:mm): 09 12 AM

Day of the week: Thursday

FIGURE 36 Scheduling tab - Weekly

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

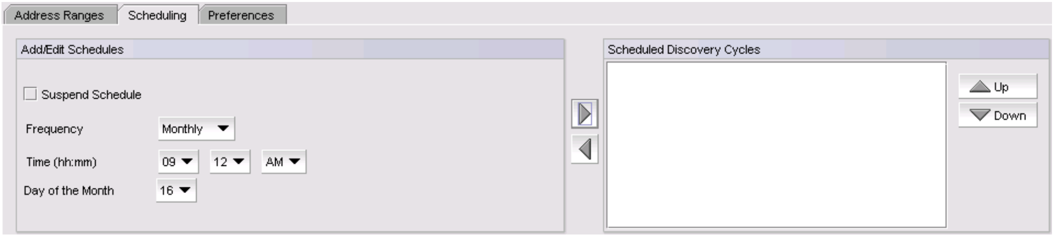
   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want discovery to run from the **Day of the Week** list.
4. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
5. To finish configuring the discovery schedule, return to “Scheduling discovery” on page 109.

Configuring a monthly discovery schedule

To configure a monthly discovery schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.



□ Suspend Schedule

Frequency: Monthly

Time (hh:mm): 09 12 AM

Day of the Month: 16

FIGURE 37 Scheduling tab - Monthly

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

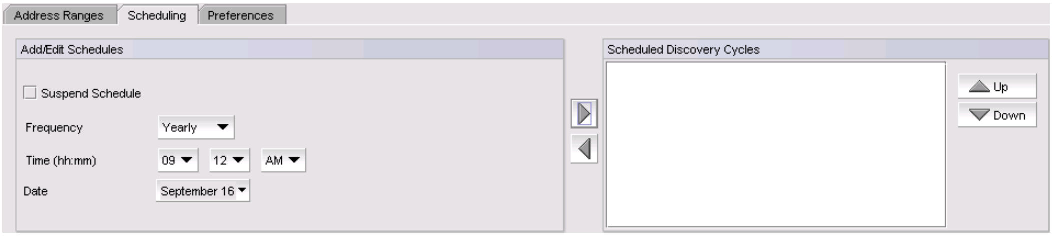
   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Select the day you want discovery to run from the **Day of the Month** list (1 through 31).
4. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
5. To finish configuring the discovery schedule, return to “Scheduling discovery” on page 109.

Configuring a yearly discovery schedule

To configure a yearly discovery schedule, complete the following steps.

1. Select **Yearly** from the **Frequency** list.



□ Suspend Schedule

Frequency: Yearly

Time (hh:mm): 09 12 AM

Date: September 16

FIGURE 38 Scheduling tab - Yearly

2. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

3. Click the **Date** list to select a date from the calendar.
4. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
5. To finish configuring the discovery schedule, return to "Scheduling discovery" on page 109.

Suspending a discovery schedule

To suspend a discovery profile schedule, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab
3. Select the profile for which you want to suspend a discovery schedule in the **Discovery Profiles** table and click the **Scheduling** tab.
4. Select the schedule you want to suspend in the **Scheduled Discovery Cycles** list and click the left arrow button.
5. Click the Suspend check box and click the right arrow button to return the schedule to the **Scheduled Discovery Cycles** list.

   The suspended schedule displays at the bottom of the **Scheduled Discovery Cycles** list.

6. Click **Apply** to save your changes.
7. Click **Close** to close the **Discover Setup - IP** dialog box.
8. Click **Yes** on the confirmation message.

Editing a discovery schedule

To edit a discovery schedule, complete the following steps.

1. Select **Discover** > **IP Products.**

   The **Discover Setup** - **IP** dialog box displays.

2. Click the **Profiles** tab
3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Scheduling** tab.
4. Select the schedule you want to edit from the **Scheduled Discovery Cycles** list.
5. Click the left arrow button to display the schedule in the **Add/Edit Schedules** area.
6. Choose one of the following options to change the discovery schedule:
   - To edit the one-time discovery schedule, refer to "Editing a one-time discovery schedule" on page 114.
   - To edit the hourly discovery schedule, refer to "Editing an hourly discovery schedule" on page 115.
   - To edit the daily discovery schedule, refer to "Editing a daily discovery schedule" on page 115.
   - To edit the weekly discovery schedule, refer to "Editing a weekly discovery schedule" on page 115.
   - To edit the monthly discovery schedule, refer to "Editing a monthly discovery schedule" on page 115.
   - To edit the yearly discovery schedule, refer to "Editing a yearly discovery schedule" on page 116.
7. Rearrange schedules in the **Scheduled Discovery Cycles** list by selecting an item in the list and clicking the **Up** or **Down** buttons to move it.
8. Click **Apply** to save your changes.
9. Click **Close** to close the **Discover Setup** - **IP** dialog box.
10. Click **Yes** on the confirmation message.

Editing a one-time discovery schedule

To edit a one-time discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

2. Click the **Date** list to select a date from the calendar.
3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish editing the discovery schedule, return to "Editing a discovery schedule" on page 114.

Editing an hourly discovery schedule

To edit an hourly discovery schedule, complete the following steps.

1. Select the minute past the hour you want discovery to run from the **Minutes past the Hour** list.

   Where the minute value is from 00 through 59.

2. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
3. To finish editing the discovery schedule, return to “Editing a discovery schedule” on page 114.

Editing a daily discovery schedule

To edit a daily discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

2. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
3. To finish editing the discovery schedule, return to “Editing a discovery schedule” on page 114.

Editing a weekly discovery schedule

To edit a weekly discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

2. Select the day you want discovery to run from the **Day of the Week** list.
3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish editing the discovery schedule, return to “Editing a discovery schedule” on page 114.

Editing a monthly discovery schedule

To edit a monthly discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

2. Select the day you want discovery to run from the **Day of the Month** list (1 through 31).
3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish editing the discovery schedule, return to “Editing a discovery schedule” on page 114.

Editing a yearly discovery schedule

To edit a yearly discovery schedule, complete the following steps.

1. Select the time of day you want discovery to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

2. Click the **Date** list to select a date from the calendar.
3. Click the right arrow button to add the schedule to the **Scheduled Discovery Cycles** list.
4. To finish editing the discovery schedule, return to “Editing a discovery schedule” on page 114.

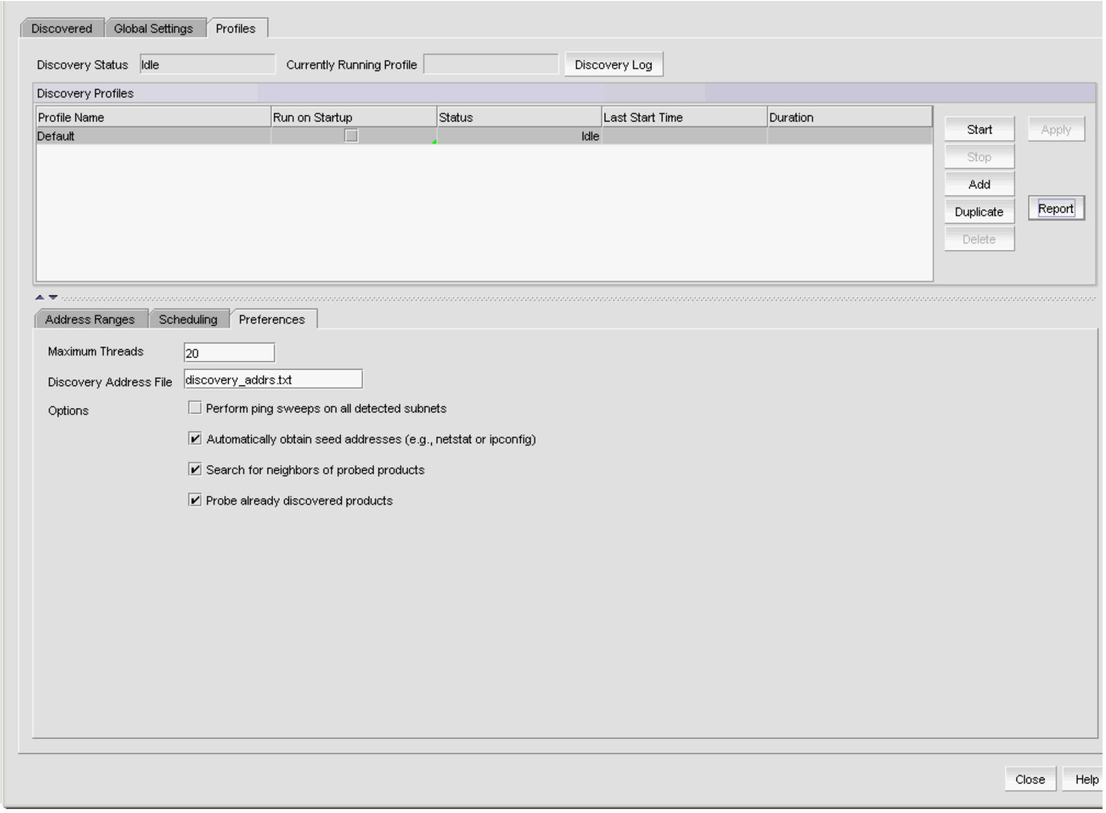
Configuring advanced discovery profile preferences

To configure advanced discovery profile preferences, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the profile you want to edit in the **Discovery Profiles** table and click the **Preferences** tab.



Discovery Status: Idle
Currently Running Profile:

Discovery Profiles

Profile Name	Run on Startup	Status	Last Start Time	Duration
Default	□	Idle		

Maximum Threads: 20
Discovery Address File: discovery_addrs.txt
Options:
- □ Perform ping sweeps on all detected subnets
- ☑ Automatically obtain seed addresses (e.g., netstat or ipconfig)
- ☑ Search for neighbors of probed products
- ☑ Probe already discovered products

FIGURE 39 **Preferences tab**

4. Enter the maximum number (from 1 through 100) of simultaneous connections to devices allowed by discovery in the **Maximum Threads** field.

5. Enter the name of the file that contains specific IP addresses to probe in the **Discovery Address File** field.

   The file supports both IPv4 and IPv6 addresses. This file must be located in the *Install_Home*\conf\discovery\ip folder on the server. The default file is the discovery_addrs.txt file; however, you can create additional files. To create a discovery address file, refer to "Creating a discovery address file" on page 117.

6. Select the **Perform Ping sweeps on all detected subnets** check box to systematically ping all IP addresses in any subnet detected through the normal discovery process.
7. Select the **Automatically obtain seed addresses** check box to use netstat or ipconfig to capture a starting candidate IP address with which to begin the discovery process.
8. Select the **Search for neighbors of probed products** check box to read all ARP, LLDP, FDP, and CDP tables to find neighboring devices.
9. Select the **Probe already discovered products** check box to rediscover devices previously discovered.
10. Click **Apply** to save your changes.
11. Click **Close** to close the **Discover Setup - IP** dialog box.
12. Click **Yes** on the confirmation message.

Deleting a discovery profile

You can delete any of the discovery profiles except the "Default" profile.

To delete a discovery profile, complete the following steps.

1. Select **Discover** > **IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the profile you want to delete in the **Discovery Profiles** table and click **Delete**.
4. Click **Apply** to save your changes.
5. Click **Close** to close the **Discover Setup - IP** dialog box.
6. Click **Yes** on the confirmation message.

Creating a discovery address file

You can configure multiple profiles to use different discovery address files. You can configure multiple profiles to use the same discovery address file.

To create a discovery address file, complete the following steps.

1. Open a text editor (such as Notepad).
2. Enter the IP addresses you want to include in discovery.

```
# discovery_addrs.txt
#
# Discovery reads this file at the
# start of each discovery cycle.
# Discovery probes the IP addresses in
```

```
#this file, as long as they are not
# excluded by any scoping restrictions.
#
10.1.2.54
10.55.2.68
```

3. Select **File > Save**.
4. Browse to the *Install_Home*\conf\discovery\ip folder.

   This file must be saved to the *Install_Home*\conf\discovery\ip folder on the server.
5. Enter a name for the file.
6. Click **Save**.

Starting discovery manually

To start discovery for a profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab.
3. Select the discovery profile on which you want to start discovery in the **Discovery Profiles** table and click **Start**.
4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

Starting discovery automatically

To run discovery for a profile at startup, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab.
3. Select the check box in the **Run on Startup** column for the discovery profile in the **Discovery Profiles** table.

   NOTE
   You can only configure one profile to run discovery on startup.
4. Click **Apply** to save your work.
5. Click **Close** to close the **Discover Setup - IP** dialog box.
6. Click **Yes** on the confirmation message.

Stopping discovery

To stop discovery for a profile, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the discovery profile on which you want to stop discovery in the **Discovery Profiles** table and click **Stop**.
4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

Viewing discovery status

To view discovery status, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Review the status in the **Status** column of the **Discovery Profiles** table.

   Status updates dynamically for any changes. Options include the following statuses:

   - **Running** — Discovery is in progress for the profile.
   - **Waiting** — Discovery will start for this profile once the current profile discovery completes.
   - **Scheduled** — Discovery will be run for this profile at the scheduled time.
   - **Idle** — Discovery is not running.
   - **Terminating** — Discovery for the profile is either completing or has been terminated.

4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

Viewing discovery reports

To view a report for a discovery profile, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Click the **Profiles** tab.
3. Select the discovery profile for which you want to view a report in the **Discovery Profiles** table and click **Report**.

   The report displays with the following information.

   - **Discovery Summary** table — Provides discovery statistics.
   - **Discovery Configuration** table — Records the discovery parameters.
   - **Detail** — Provides discovery process details.

4. Click **Close** to close the **Discover Setup - IP** dialog box.
5. Click **Yes** on the confirmation message.

E-mailing discovery reports

To e-mail a report for a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab.
3. Select the discovery profile for which you want to e-mail a report in the **Discovery Profiles** table and click **Report**.
4. Click **E-mail** to send the report in an e-mail message.
5. Enter an e-mail address in the **E-mail Recipients** field or click the associated button to select an e-mail address from the **Users** list.
6. (Optional) Enter additional e-mail addresses in the **E-mail Recipients** field.

   To send an e-mail message to more than one recipient, separate the e-mail addresses using a semicolon (;) delimiter.
7. Click **Send** to send the report.
8. Click **Close** to close the **Discover Setup - IP** dialog box.
9. Click **Yes** on the confirmation message.

Exporting discovery reports

To export a report for a discovery profile, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab.
3. Select the discovery profile for which you want to export a report in the **Discovery Profiles** table and click **Report**.
4. Choose one of the following options:
   - To export the report to a .csv file, select **Export > Export as CSV.**
   - To export the report to an HTML file, select **Export > Export as HTML.**

   The **File Download** dialog box displays.
5. Click **Save**.

   The **Save As** dialog box displays.
6. Browse to the file location where you want to save the report.
7. Click **Save**.

8. Click **Close** to close the **Discover Setup - IP** dialog box.
9. Click **Yes** on the confirmation message.

Viewing the discovery log

The discovery log displays the status of the current discovery activity. To configure the discovery log size, refer to “Defining global setting preferences” on page 97.

To view the discovery log, complete the following steps.

1. Select **Discover** > **IP Products**.

   The **Discover Setup - IP** dialog box displays.
2. Click the **Profiles** tab.
3. Click **Discovery Log**.

   The **Discovery Status Log** dialog box displays with a list of discovery status messages. If discovery is running, the discovery status messages automatically display and update dynamically in the dialog box with the latest message at the top.
4. Click **Close** to close the **Discovery Status Log** dialog box.
5. Click **Close** to close the **Discover Setup - IP** dialog box.

Individual IP device discovery

Simple discovery discovers the device with a specific IP address. It is triggered by device configuration changes on SNMP traps, certain configuration deployments to a device, and adding device or rediscovering a device.

Adding an IP device to discovery

NOTE
DCB devices discovered through Fabric discovery (from the **SAN** tab) are automatically added to IP discovery during rediscovery.

NOTE
You cannot discover new products if you do not have the **All IP Products** AOR (area of responsibility) in your user account.

To add an individual IP device to discovery, complete the following steps.

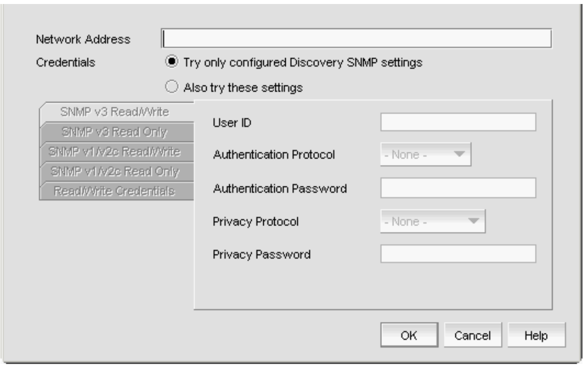
1. Select **Discover** > **IP Products**.

   The **Discover Setup - IP** dialog box displays.

   NOTE
   The **Discovered Products** table lists all products discovered through individual product discovery, profile-based discovery, as well as Fabric discovery (from the **SAN** tab).

2. Click **Add**.

   The **Add product** dialog box displays.



Credentials ● Try only configured Discovery SNMP settings

FIGURE 40 Add product dialog box

3. Choose one of the following options:

   - Enter the IP address (IPv4 or IPv6) of the IP device in the **Network Address** field.
   - Enter the host name or DNS name (up to 64 characters) of the IP device in the **Network Address** field.

NOTE
The Management application does not validate the Network address until you save your work.

4. Select one of the following options:

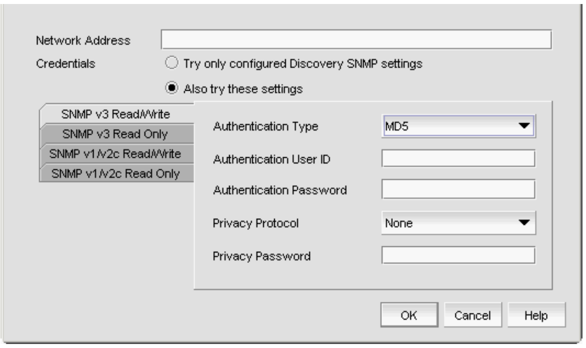
   - **Try only configured Discovery SNMP settings** — Select to use the SNMP settings configured in the **Global Settings** tab to contact the device.
   - **Also try these settings** — Select to use specific SNMP settings to contact the device. If you do not enter SNMP settings or if the settings do not authenticate on the device, the application uses the SNMP settings configured in the **Global Settings** tab to contact the device.

   NOTE
   You can configure both SNMPv3 and SNMPv1/SNMPv2c credentials at the same time; however, discovery tries the SNMPv3 credentials before trying the SNMPv1 and SNMPv2c credentials.

5. Configure the SNMPv3 read-write credentials by completing the following steps.

NOTE
These credentials are not applicable for DCB devices.

   a. Click the **SNMPv3 Read/Write** tab.



Network Address

Credentials ○ Try only configured Discovery SNMP settings

● Also try these settings

Authentication Type MD5

Authentication User ID

Authentication Password

Privacy Protocol None

Privacy Password

FIGURE 41 SNMPv3 credentials

b. Enter the SNMPv3 user name in the User ID field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

c. Select one of the following protocols from the Authentication Protocol list:

- None
- HMAC_MD5
- HMAC_SHA

d. Enter the SNMPv3 authentication password in the Authentication Password field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Select one of the following protocols from the Privacy Protocol list:

- None
- CBC-DES
- CFB_AES-128

If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

f. Enter the privacy password in the Privacy Password field.

The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

6. Configure the SNMPv3 read only credentials by completing the following steps.

a. Click the SNMPv3 Read Only tab.

b. Enter the SNMPv3 user name in the User ID field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

c. Select one of the following protocols from the Authentication Protocol list:

- None
- HMAC_MD5
- HMAC_SHA

d. Enter the SNMPv3 authentication password in the **Authentication Password** field.

   The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Select one of the following privacy protocol types from the **Privacy Protocol** list:

   - None
   - CBC-DES
   - CFB_AES-128

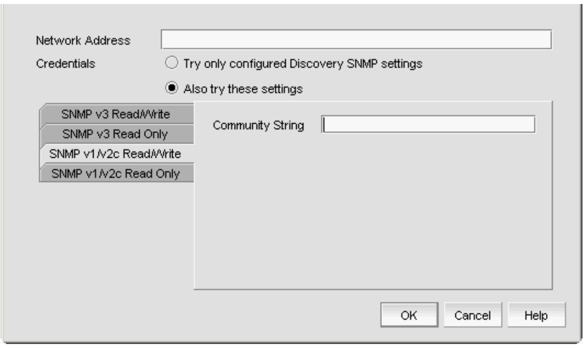
   If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

f. Enter the privacy password in the **Privacy Password** field.

   The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

7. Configure the SNMPv1 and SNMPv2c read-write credentials by completing the following steps.

   a. Click the **SNMPv1/v2c Read/Write** tab.



Network Address

Credentials ○ Try only configured Discovery SNMP settings

● Also try these settings

Community String

FIGURE 42 **SNMPv1/v2c credentials**

   b. Enter the community string in the **Community** field.

   The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

   NOTE
   If you do not enter a community string in the field, discovery uses the "public" and "private" community strings to probe the devices.

8. Configure the SNMPv1 and SNMPv2c read only credentials by completing the following steps.

   a. Click the **SNMPv1/v2c Read Only** tab.

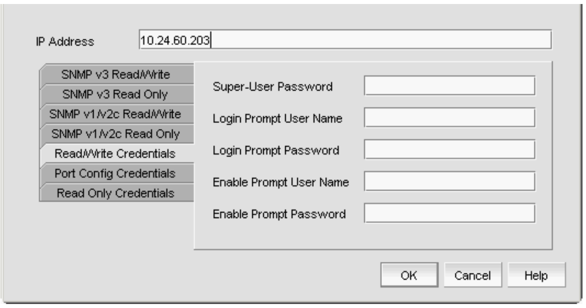
   b. Enter the community string in the **Community** field.

   The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

   NOTE
   If you do not enter a community string in the field, discovery uses the "public" and "private" community strings to probe the devices.

9. Configure the Read/Write credentials by completing the following steps.

   a. Click the **Read/Write Credentials** tab.



IP Address 10.24.60.203

FIGURE 43 Read/Write credentials

   b. Enter the unique user name in the **Login Prompt User Name** field.

      The user name can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

   c. Enter the password in the **Login Prompt Password** field.

      The password can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. The password displays as asterisks. Not applicable to DCB devices.

10. Click **OK** on the **Add product** dialog box.

    The **Discover Setup - IP** dialog box displays with the added IP device in the **Discovered Products** table.

11. Click **Close** to close the **Discover Setup - IP** dialog box.

Editing IP device discovery

NOTE
Although, you can configure third-party product password settings through discovery, the Management application ignores these third-party product settings.

To edit one or more IP devices, complete the following steps.

1. Select **Discover > IP Products**.

   The **Discover Setup - IP** dialog box displays.

2. Select one or more IP devices you want to edit in the **Discovered Products** table.

   Select multiple devices by holding down the CTRL key and clicking more than one device.

   NOTE
   You cannot edit IronWare and Network OS devices at the same time.

   NOTE
   You can only edit multiple Network OS devices that are running the same firmware level.

3. Click **Edit**.

   The **Edit product** dialog box displays.

4. Select one of the following options:

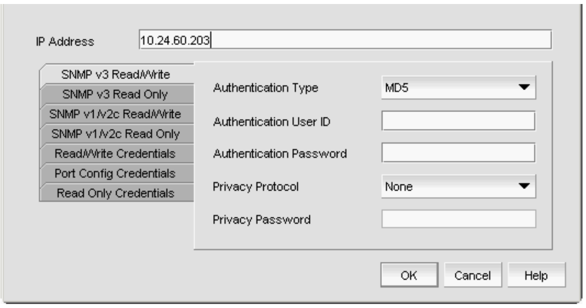
   - **Try only configured Discovery SNMP settings** — Select to use the SNMP settings configured in the **Global Settings** tab to contact the device.
   - **Also try these settings** — Select to use specific SNMP settings to contact the device. If you do not enter SNMP settings or if the settings do not authenticate on the device, the application uses the SNMP settings configured in the **Global Settings** tab to contact the device.

   NOTE
   You can configure both SNMPv3 and SNMPv1/SNMPv2c credentials at the same time; however, discovery tries the SNMPv3 credentials before trying the SNMPv1 and SNMPv2c credentials.

5. Change the SNMPv3 read-write credentials by completing the following steps.

   NOTE
   These credentials are not applicable for DCB devices.

   a. Click the **SNMPv3 Read/Write** tab.



IP Address: 10.24.60.203

Authentication Type: MD5

Privacy Protocol: None

FIGURE 44 **SNMPv3 credentials**

   b. Enter the SNMPv3 user name in the **User ID** field.

   The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

   c. Select one of the following protocols from the **Authentication Protocol** list:

   - None
   - HMAC_MD5
   - HMAC_SHA

   d. Enter the SNMPv3 authentication password in the **Authentication Password** field.

   The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Select one of the following privacy protocol types from the **Privacy Protocol** list:

- None
- CBC-DES
- CFB_AES-128

If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

f. Enter the privacy password in the **Privacy Password** field.

The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

6. Change the SNMPv3 read only credentials by completing the following steps.

a. Click the **SNMPv3 Read Only** tab.

b. Enter the SNMPv3 user name in the **User ID** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

c. Select one of the following protocols from the **Authentication Protocol** list:

- None
- HMAC_MD5
- HMAC_SHA

d. Enter the SNMPv3 authentication password in the **Authentication Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Select one of the following privacy protocol types from the **Privacy Protocol** list:

- None
- CBC-DES
- CFB_AES-128

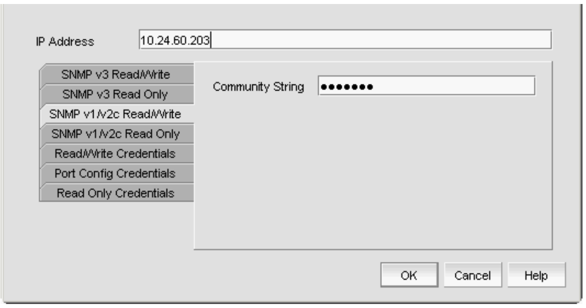
If you select a privacy protocol, the selected protocol encrypts the SNMP request and response packets.

f. Enter the privacy password in the **Privacy Password** field.

The password can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

7. Change the SNMPv1 and SNMPv2c read-write credentials by completing the following steps.

a. Click the **SNMPv1/v2c Read/Write.** tab



IP Address 10.24.60.203

Community String •••••••

FIGURE 45 SNMPv1/v2c settings

b. Enter the unique community string in the **Community** field.

The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

NOTE
If you do not enter a community string in the field, discovery uses the "public" and "private" community strings to probe the devices.

8. Change the SNMPv1 and SNMPv2c read only credentials by completing the following steps.

a. Click the **SNMPv1/v2c Read Only** tab.

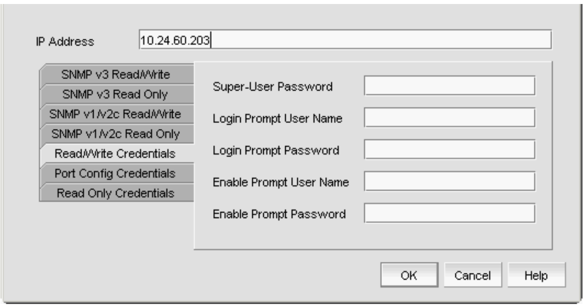
b. Enter the unique community string in the **Community** field.

The community string can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters. The string displays as asterisks.

NOTE
If you do not enter a community string in the field, discovery uses the "public" and "private" community strings to probe the devices.

9. Change the Read/Write credentials by completing the following steps.

a. Click the **Read/Write Credentials** tab.



IP Address 10.24.60.203

FIGURE 46 Read/Write credentials

b. Enter the password in the **Super-User Password** field.

The password can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. Not applicable to DCB devices.

c. Change the unique user name in the **Login Prompt User Name** field.

The user name can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters.

d. Change the password in the **Login Prompt Password** field.

The password can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

e. Change the unique user name in the **Enable Prompt User Name** field.

The user name can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. Not applicable to DCB devices.

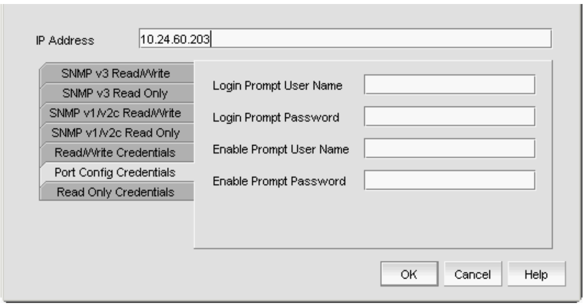
f. Change the password in the **Enable Prompt Password** field.

The password can be from 1 through 200 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks. Not applicable to DCB devices.

10. Change the Port Config credentials by completing the following steps.

NOTE
These credentials are not applicable for DCB, VDX, or VCS devices.

a. Click the **Port Config Credentials** tab.



IP Address 10.24.60.203

FIGURE 47 **Port Config credentials**

b. Change the unique user name in the **Login Prompt User Name** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

c. Change the password in the **Login Prompt Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

d. Change the unique user name in the **Enable Prompt User Name** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

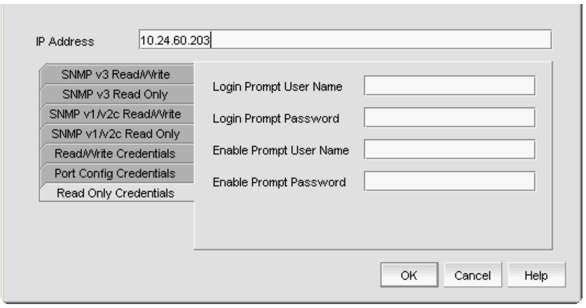
e. Change the password in the **Enable Prompt Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

11. Change the Read Only credentials by completing the following steps.

NOTE
These credentials are not applicable for DCB, VDX, or VCS devices.

a. Click the **Read Only Credentials** tab.



IP Address 10.24.60.203

FIGURE 48 Read Only credentials

a. Change the unique user name in the **Login Prompt User Name** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

b. Change the password in the **Login Prompt Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

c. Change the unique user name in the **Enable Prompt User Name** field.

The user name can be from 1 through 16 characters long, case sensitive, and allows all printable ASCII characters.

d. Change the password in the **Enable Prompt Password** field.

The password can be from 8 through 16 characters long, case sensitive, and allows all printable ASCII characters. The password display as asterisks.

12. Click **OK** on the **Edit product** dialog box.

The **Discover Setup - IP** dialog box displays with the updated IP device in the **Discovered Products** table.

13. Click **Close** to close the **Discover Setup - IP** dialog box.

Deleting IP devices from discovery

To delete one or more IP devices from discovery, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Select the IP devices you want to remove from discovery in the **Discovered Products** table.

   Select multiple devices by holding down the CTRL key and clicking more than one device.

   NOTE
   You cannot delete an active member from a VCS fabric.

3. Click **Delete.**

Host discovery

The Management application enables you to discover individual hosts, import a group of Host from a comma separated values (CSV) file, or import all hosts from discovered fabrics or VM managers.

NOTE
Host discovery requires HCM Agent 2.0 or later.

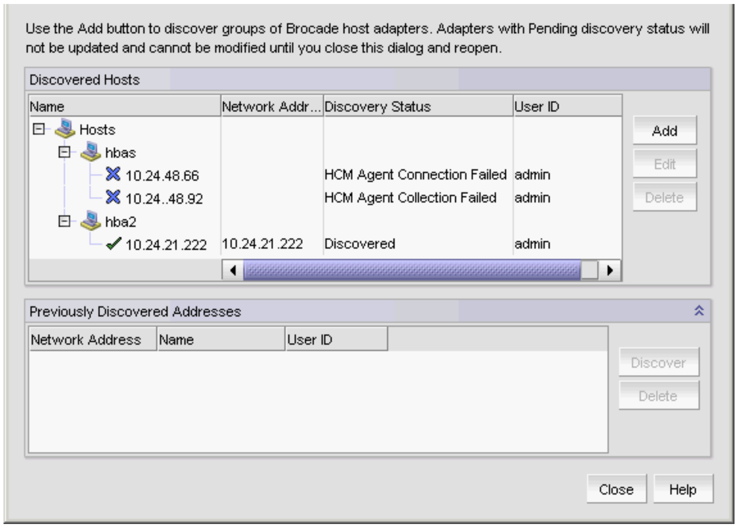
NOTE
SMI and WMI discovery are not supported.

Discovering Hosts by Network address or host name

To discover a Host by Network address or host name, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.



Use the Add button to discover groups of Brocade host adapters. Adapters with Pending discovery status will not be updated and cannot be modified until you close this dialog and reopen.

Discovered Hosts

Name	Network Addr...	Discovery Status	User ID
⊟ Hosts			
⊟ hbas			
✕ 10.24.48.66		HCM Agent Connection Failed	admin
✕ 10.24..48.92		HCM Agent Collection Failed	admin
⊟ hba2			
✓ 10.24.21.222	10.24.21.222	Discovered	admin

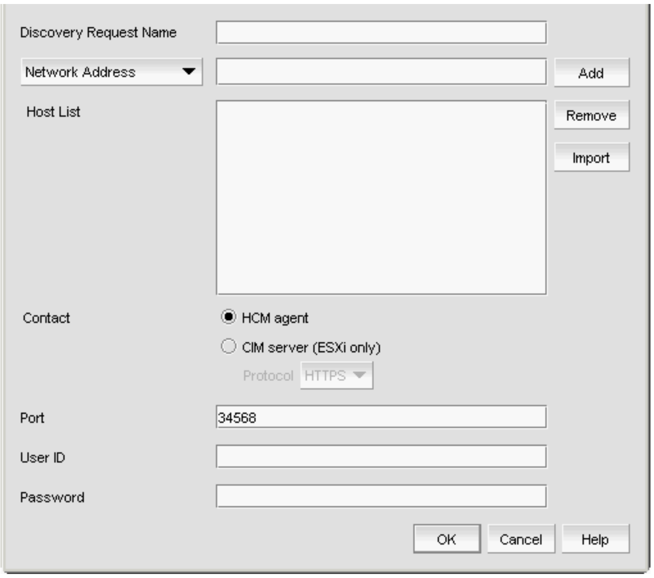
Previously Discovered Addresses

Network Address	Name	User ID

FIGURE 49 Discover Host Adapters dialog box

2. Click **Add**.

   The **Add Host Adapters** dialog box displays.



Discovery Request Name

Network Address

Host List

Contact ● HCM agent
○ CIM server (ESXi only)
Protocol HTTPS

Port 34568

User ID

Password

FIGURE 50 Add Host Adapters dialog box

3. (Optional) Enter a discovery request name (such as, Manual 06/12/2009) in the **Discovery Request Name** field.
4. Select **Network Address** from the list.
5. Enter the IP address (IPv4 or IPv6 formats) or host name in the **Network Address** field.
6. Click **Add**.

   The IP address or host name of the Host displays in the **Host List**.

7. Configure Host credentials by choosing one of the following options:
   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 9.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step 8.

   If you do not need to configure Host credentials, skip to step 13.
8. Configure discovery authentication by choosing one of the following options:
   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.
9. Enter the port number in the **Port** field.

   HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.
10. Enter your username in the **User ID** field.

    HCM agent default is admin. Leave this field blank for the CIM server.
11. Enter your password **Password** field.

    HCM agent default is password. Leave this field blank for the CIM server.
12. Repeat step 5 through step 11 for each Host you want to discover.
13. Click **OK** on the **Add Host Adapters** dialog box.

    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

    A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.
14. Click **Close** on the **Discover Host Adapters** dialog box.

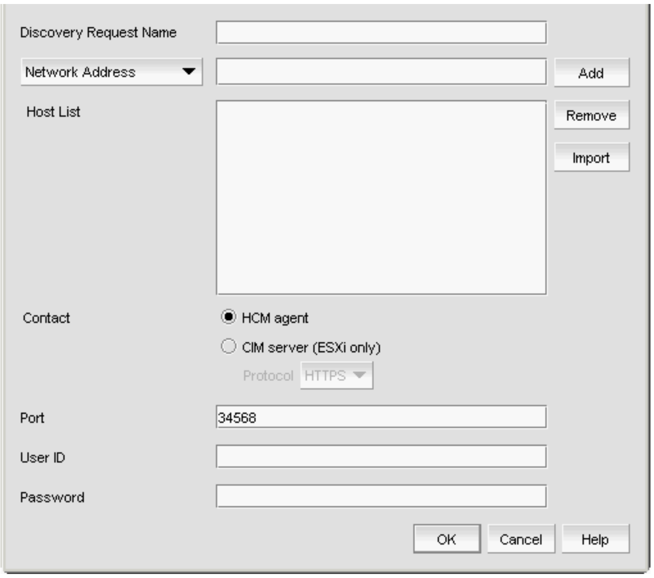
Importing Hosts from a CSV file

To discover Hosts by importing a CSV file, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.
2. Click **Add**.

   The **Add Host Adapters** dialog box displays.



Discovery Request Name

Network Address ▼

Host List

Contact

● HCM agent

○ CIM server (ESXi only)

Protocol HTTPS ▼

Port 34568

User ID

Password

FIGURE 51 Add Host Adapters dialog box

3. Enter a discovery request name (such as, MyFabric) in the **Discovery Request Name** field.
4. Click **Import**.

   The **Open** dialog box displays.
5. Browse to the CSV file location.

   The CSV file must meet the following requirements:

   - Comma separated IP address or host names
   - No commas within the values
   - No escaping supported

     For example, XX.XX.XXX.XXX, XX.XX.X.XXX, computername.company.com
6. Click **Open**.

   The CSV file is imported to the **Add Host Adapters** dialog box. During import, duplicate values are automatically dropped. When import is complete, the imported values display in the **Host List**. If the file cannot be imported, an error displays.
7. Verify the imported values in the **Host List**.
8. Configure Host credentials by choosing one of the following options:

   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 10.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step .

   If you do not need to configure Host credentials, skip to step 13.
9. Configure discovery authentication by choosing one of the following options:

   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.

10. Enter the port number in the Port field.

    HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.

11. Enter your username in the User ID field.

    HCM agent default is admin. Leave this field blank for the CIM server.

12. Enter your password Password field.

    HCM agent default is password. Leave this field blank for the CIM server.

13. Click OK on the Add Host Adapters dialog box.

    If an error occurs, a message displays. Click OK to close the error message and fix the problem.

    A Host Group displays in Discovered Hosts table with pending status. To update the status from pending you must close and reopen the Discover Host Adapters dialog box.

14. Click Close on the Discover Host Adapters dialog box.

Importing Hosts from a Fabric

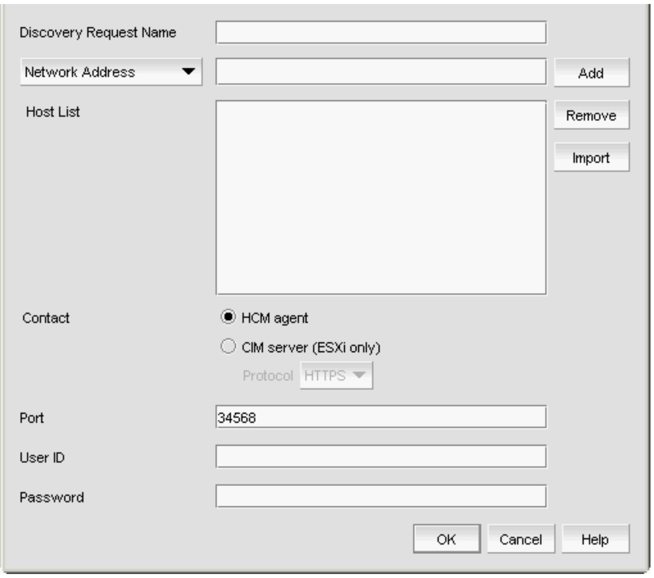
To discover a Host from a discovered fabric, complete the following steps.

1. Select Discover > Host Adapters.

   The Discover Host Adapters dialog box displays.

2. Click Add.

   The Add Host Adapters dialog box displays.



Contact ● HCM agent

Port 34568

FIGURE 52 Add Host Adapters dialog box

3. Enter a discovery request name (such as, MyFabric) in the Discovery Request Name field.

4. Select Hosts in Fabrics from the list.

5. Select All fabrics or an individual fabric from the list.

6. Click **Add**.

   All hosts which are part of a managed fabric and have a registered host name display in the list. If no host with a registered host name exists, an error message displays. Click **OK** to close the error message.

7. Configure Host credentials by choosing one of the following options:

   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 9.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step 8.

   If you do not need to configure Host credentials, skip to step 12.

8. Configure discovery authentication by choosing one of the following options:

   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.

9. Enter the port number in the **Port** field.

   HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.

10. Enter your username in the **User ID** field.

    HCM agent default is admin. Leave this field blank for the CIM server.

11. Enter your password **Password** field.

    HCM agent default is password. Leave this field blank for the CIM server.

12. Click **OK** on the **Add Host Adapters** dialog box.

    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

    A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.

13. Click **Close** on the **Discover Host Adapters** dialog box.

Importing Hosts from a VM manager

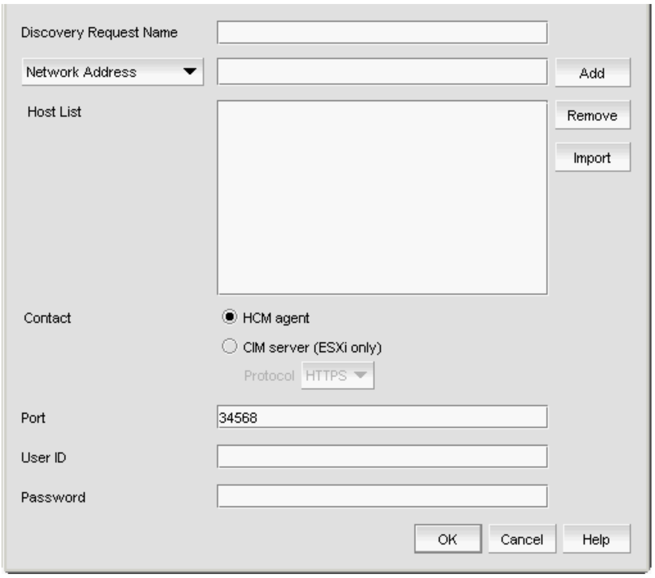
To discover Hosts from a discovered VM manager, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Click **Add**.

   The **Add Host Adapters** dialog box displays.



Discovery Request Name

Network Address

Host List

Contact ● HCM agent

○ CIM server (ESXi only)

Protocol HTTPS

Port 34568

User ID

Password

FIGURE 53 Add Host Adapters dialog box

3. Enter a discovery request name (such as, MyVMManager) in the **Discovery Request Name** field.
4. Select **Hosts from VM Manager** from the import by list.
5. Select **All VM** or an individual VM from the list.
6. Click **Add**.

   All hosts which are part of a discovered VM manager and have a registered host name display in the list. If no host with a registered host name exists, an error message displays. Click **OK** to close the error message.

7. Configure Host credentials by choosing one of the following options:
   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 9.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step 8.

   If you do not need to configure Host credentials, skip to step 12.

8. Configure discovery authentication by choosing one of the following options:
   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.
9. Enter the port number in the **Port** field.

   HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.

10. Enter your username in the **User ID** field.

    HCM agent default is admin. Leave this field blank for the CIM server.

11. Enter your password **Password** field.

    HCM agent default is password. Leave this field blank for the CIM server.

12. Click **OK** on the **Add Host Adapters** dialog box.

    If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

    A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.

13. Click **Close** on the **Discover Host Adapters** dialog box.

Editing Host adapter credentials

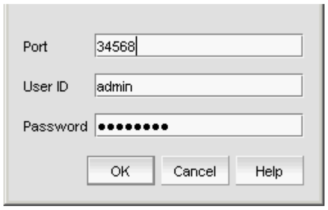
To edit Host credentials, complete the following steps.

1. Select **Discover** > **Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the Host in the **Discovered Hosts** list and click **Edit**.

   The **Edit Host Adapters** dialog box displays.



Port 34568
User ID admin
Password ••••••••

FIGURE 54 **Edit Host Discovery dialog box**

3. Configure Host credentials by choosing one of the following options:

   - To configure HCM agent credentials, select the **HCM agent** option. Go to step 5.
   - To configure CIM server credentials, select the **CIM server (ESXi only)** option. Continue with step 4.

   If you do not need to configure Host credentials, skip to step 8.

4. Configure discovery authentication by choosing one of the following options:

   - To configure discovery with authentication, select the **HTTPS** from the **Protocol** list.
   - To configure discovery without authentication, select the **HTTP** from the **Protocol** list.

5. Enter the port number in the **Port** field.

   HCM agent default is 34568. CIM server HTTPS default is 5989. CIM server HTTP default is 5988.

6. Enter your username in the **User ID** field.

   HCM agent default is admin. Leave this field blank for the CIM server.

7. Enter your password **Password** field.

   HCM agent default is password. Leave this field blank for the CIM server.

8. Click **OK** on the **Edit Host Adapters** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

9. Click **Close** on the **Discover Host Adapters** dialog box.

Removing a host from active discovery

If you decide you no longer want the Management application to discover and monitor a specific host, you can delete it from active discovery. Deleting a host also deletes the host data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a host from active discovery, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to delete from active discovery in the **Discovered Hosts** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.

   The deleted host displays in the **Previously Discovered Addresses** table.

5. Click **Close** on the **Discover Host Adapters** dialog box.

Rediscovering a previously discovered fabric

To return a host to active discovery, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to return to active discovery in the **Previously Discovered Addresses** table.
3. Click **Discover**.
4. Click **OK** on the confirmation message.

   The rediscovered host displays in the **Discovered Hosts** table.

5. Click **Close** on the **Discover Host Adapters** dialog box.

Deleting a host adapter from discovery

To delete a host permanently from discovery, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to delete permanently from discovery in the **Previously Discovered Addresses** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Click **Close** on the **Discover Host Adapters** dialog box.

Viewing the host discovery state

The Management application enables you to view device discovery status through the **Discover Host Adapters** dialog box.

To view the discovery status of a device, complete the following steps.

1. Select **Discover** > **Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Right-click the Hosts node select **Expand All** to show all devices.

   The **Name** field displays the discovery status icons in front of the device name. The following table illustrates and describes the icons that indicate the current status of the discovered devices.

   TABLE 27 Discovery Status Icons

Icon	Description
✓	Displays when the fabric or host is managed and the management status is okay.
✖	Displays when the fabric or host is not managed.

   The **Discovery Status** field details the actual status message text, which varies depending on the situation. The following are samples of actual status messages:

   - Discovered
   - New Discovery Pending
   - Created host structure differs from discovered host; Discovery ignored
   - Brocade HBA Discovery Failed: HCM Agent connection failed
   - HCM Agent collection failed
   - CIM Server Authentication failed
   - CIM Server connection failed

Troubleshooting host discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly. For more complete information about troubleshooting adapters, refer to the *Adapters Troubleshooting Guide*.

1. Verify IP connectivity by issuing a ping command to the host.
   a. Open the command prompt.
   b. From the Server, type `ping` *`Host_IP_Address`*.

2. If the host is responding to ping, but discovery still fails, verify that HCM agent is up or not by browsing to the following URL:

   https://*Host_IP_Address*:34568/JSONRPCServiceApp/JSON-RPC

   If HCM agent is running and reachable, you should receive a prompt of credentials and then show an Error 500 (No Reason) result page.

3. Verify that firewall port 34568 is open.

   There are firewall issues with the HCM Agent on Windows 2008 and VMware systems. When installing the driver package on these systems, open TCP/IP port 34568 to allow agent communication with the Management application.

   - For VMware, use the following commands to open port 34568:
     - `esxcfg-firewall -o 34568,tcp,in,https`
     - `esxcfg-firewall -o 34568,udp,out,https`
   - For Windows, use Windows Firewall and Advanced Service (WFAS) to open port 34568.

VM Manager discovery

The Management application enables you to discover VM managers. VM Manager discovery requires vCenter Server 4.0 or later.

NOTE
vCenter discovery time is dynamically determined based on the number of hosts being managed by the vCenter. For every 50 hosts managed, the vCenter collection period increases 30 minutes. For 0-50 hosts managed, the collection duration is 30 minutes; for 50-100 hosts managed, the collection duration is one hour, and so on.

VM Manager discovery requirements

- Discovery of a vCenter server (refer to "Discovering a VM manager" on page 141, step 4 and step 5), requires a vCenter user with read-only or read-write privilege on the vCenter server node and all objects in the inventory below the vCenter server.
- Enabling the vSphere client plug-in registration (refer to "Discovering a VM manager" on page 141, step 6), requires a vCenter user with, at minimum, the following read-write privileges on the vCenter server node and all objects in the inventory below the vCenter server:
  - Extension > Register extension
  - Extension > Unregister extension
  - Extension > Update extension

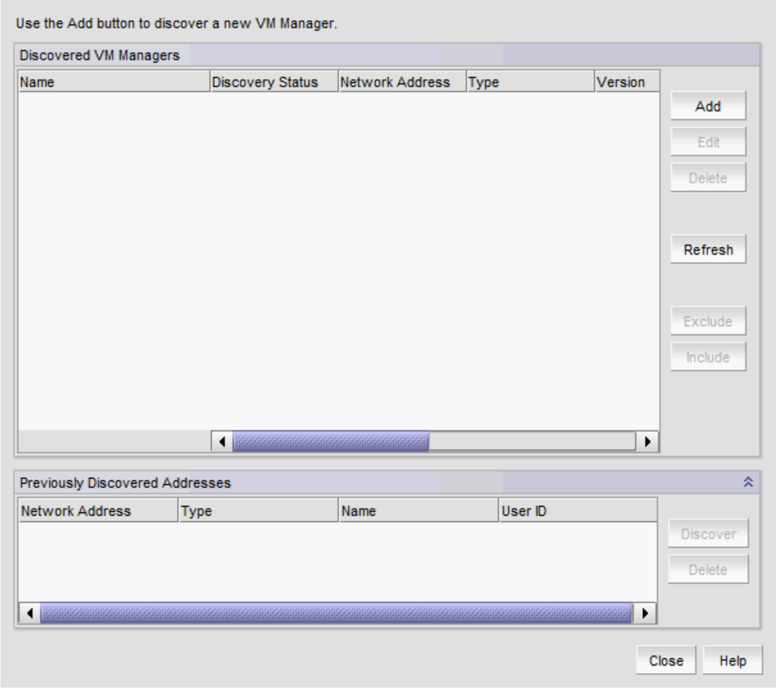
Discovering a VM manager

Before you discover a VM Manager, make sure you meet the discovery requirements (refer to "VM Manager discovery requirements" on page 141).

To discover a VM manager, complete the following steps.

1. Select **Discover > VM Managers.**

   The **Discover VM Managers** dialog box displays.


Use the Add button to discover a new VM Manager.

Discovered VM Managers

Name	Discovery Status	Network Address	Type	Version

Previously Discovered Addresses

Network Address	Type	Name	User ID

FIGURE 55 Discover VM Managers dialog box

2. Click **Add**.

   The **Add VM Manager** dialog box displays.

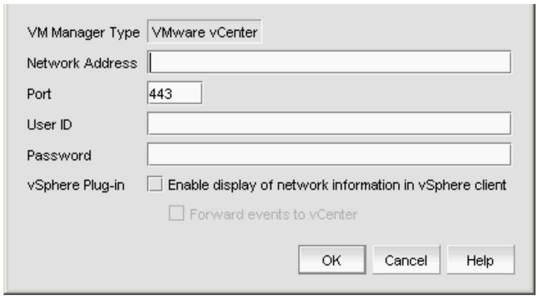

VM Manager Type	VMware vCenter
Network Address	
Port	443
User ID	
Password	
vSphere Plug-in	□ Enable display of network information in vSphere client □ Forward events to vCenter

FIGURE 56 Add VM Manager dialog box

3. Enter the IP address or host name in the **Network Address** field.
4. Enter the VM manager port number in the **Port** field.
5. Enter the VM manager username in the **User ID** field.
6. Enter the VM manager password **Password** field.
7. Select the **Enable display of network information in vSphere client** check box to enable vSphere client plug-in registration.

   Clear to disable vSphere client plug-in registration.

8. Select the Forward event to vCenter check box to enable event forwarding from the Management application to vCenter.

   Clear to disable event forwarding.

9. Click OK on the Add VM Manager dialog box.

   If an error occurs, a message displays. Click OK to close the error message and fix the problem.

   A VM manager displays in Discovered VM Managers table with pending status. To update the status from pending you must close and reopen the Discover VM Managers dialog box.

10. Refresh the Discover VM Managers list by clicking Refresh.

11. Click Close on the Discover VM Managers dialog box.

Editing a VM manager

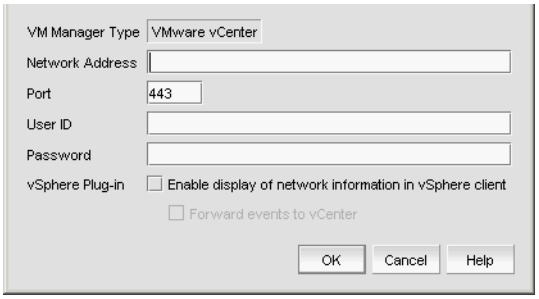
To edit VM manager discovery, complete the following steps.

1. Select Discover > VM Managers.

   The Discover VM Managers dialog box displays.

2. Select the Host in the Discovered VM Managers list and click Edit.

   The Edit VM Manager dialog box displays.



VM Manager Type: VMware vCenter

Port: 443

vSphere Plug-in: ☐ Enable display of network information in vSphere client

☐ Forward events to vCenter

FIGURE 57 Edit VM Manager dialog box

3. Change the VM manager port number in the Port field.

4. Enter the VM manager username in the User ID field.

5. Enter the VM manager user password Password field.

6. Select the Enable display of network information in vSphere client check box to enable vSphere client plug-in registration.

   Clear to disable vSphere client plug-in registration.

7. Select the Forward event to vCenter check box to enable event forwarding from the Management application to vCenter.

   Clear to disable event forwarding.

8. Click **OK** on the **Edit VM Manager** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

9. Refresh the **Discover VM Managers** list by clicking **Refresh**.
10. Click **Close** on the **Discover VM Managers** dialog box.

Excluding a host from VM manager discovery

To exclude host from VM manager discovery complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the Host you want to exclude in the **Discovered VM Managers** list and click **Exclude**.
3. Click **Close** on the **Discover VM Managers** dialog box.

Including a host in VM manager discovery

To include host in VM manager discovery complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select a Host you want to include in the **Discovered VM Managers** list and click **Include**.
3. Click **Close** on the **Discover VM Managers** dialog box.

Removing a VM manager from active discovery

If you decide you no longer want the Management application to discover and monitor a specific VM manager, you can delete it from active discovery. Deleting a VM manager also deletes the data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a VM manager from active discovery, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the VM manager you want to delete from active discovery in the **Discovered VM Managers** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.

   The deleted VM manager displays in the **Previously Discovered Addresses** table.

5. Refresh the **Discover VM Managers** list by clicking **Refresh**.
6. Click **Close** on the **Discover VM Managers** dialog box.

Rediscovering a previously discovered VM manager

To return a VM manager to active discovery, complete the following steps.

1. Select Discover > VM Managers.

   The Discover VM Managers dialog box displays.

2. Select the VM manager you want to return to active discovery in the Previously Discovered Addresses table.
3. Click Discover.
4. Click OK on the confirmation message.

   The rediscovered VM manager displays in the Discovered VM Managers table.

5. Refresh the Discover VM Managers list by clicking Refresh.
6. Click Close on the Discover VM Managers dialog box.

Deleting a VM manager from discovery

To delete a host permanently from discovery, complete the following steps.

1. Select Discover > VM Managers.

   The Discover VM Managers dialog box displays.

2. Select the VM manager you want to delete permanently from discovery in the Previously Discovered Addresses table.
3. Click Delete.
4. Click OK on the confirmation message.
5. Refresh the Discover VM Managers list by clicking Refresh.
6. Click Close on the Discover VM Managers dialog box.

Viewing the VM manager discovery state

The Management application enables you to view device discovery status through the Discover VM Managers dialog box.

To view the discovery status of a device, complete the following steps.

1. Select Discover > VM Managers.

   The Discover VM Managers dialog box displays.

2. Right-click the Hosts node select Expand All to show all devices.

   The Discovery Status field details the actual status message text, which varies depending on the situation.

   The following are samples of actual VMM status messages:

   - Active
   - Failed – Not reachable
   - Failed – Authentication failure

The following are samples of actual ESX host status messages:

- Active
- Discovery pending,
- Excluded,
- Conflict – Existing Host <hostname>

3. Refresh the **Discover VM Managers** list by clicking **Refresh.**
4. Click **Close** on the **Discover VM Managers** dialog box.

Troubleshooting VM manager discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

Verify IP connectivity by issuing a ping command to the switch.

1. Open the command prompt.
2. From the Server, type `ping` *`Device_IP_Address`*.

IP Rediscovery

When you change device configuration using the CLI or Web Management Interface, the updated configuration information does not automatically update in the Management application. You must rediscover devices to update configuration information.

For VCS devices, if you do not have the **All IP Products** AOR (area of responsibility) in your user account, you can not rediscover missing fabric members.

When you rediscover an IP device, the Management application captures and stores all changes to its configuration since the last Discovery or Rediscovery cycle. Once Rediscovery completes, configuration updates display in Network Object view.

Rediscovering IP devices

To rediscover one or more IP devices, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.

2. Select the IP devices you want to rediscover in the **Discovered Products** table.

   For VCS devices, if you do not have the **All IP Products** AOR (area of responsibility) in your user account, you can not rediscover missing fabric members.

   Select multiple devices by holding down the CTRL key and clicking more than one device. You can select up to 32 devices for rediscovery.

   If you select to rediscover multiple devices, you should configure a discovery profile to run in the background. For step-by-step instructions, refer to “Configuring a discovery profile” on page 101.

For VCS devices, rediscovery depends on what part of the fabric you select to rediscover.

- If you select the VCS fabric, rediscovery refreshes the membership information.
- If you select a VCS member, rediscovery refreshes the asset data for the selected member.
- If you select a missing VCS member, rediscovery triggers the discovery of a new fabric (VCS-enabled) or a standalone VDX switch (VCS-disabled).

3. Click **Rediscover**.

   The **Rediscover product** dialog box displays. If you selected more than 10 devices, the client only sends the first 10 devices to the server. When rediscovery is complete on the first device and the server returns the status to the client, the client sends the next device to the server. This process continues until rediscovery is complete.

   The **Rediscover product** dialog box displays the progress status for each product in the **Progress Status** column. If an error occurs the status displays as 'Failed" and an error message displays in the **Description** column.

   Click **Abort** to stop rediscovery for any pending devices. Note that rediscovery continues for all devices already sent to the server. The **Rediscover product** dialog box closes when rediscovery is complete for the active rediscovery devices.

4. Click **OK** on the **Rediscover product** dialog box when rediscovery completes.

Rediscovering IP devices from the Product List

For VCS devices, if you do not have the **All IP Products** AOR (area of responsibility) in your user account, you can not rediscover missing fabric members.

To rediscover one or more IP devices from the Product List, complete the following steps.

1. Select the **IP** tab.
2. Select the IP devices you want to rediscover in the Product List.

   Select multiple devices by holding down the CTRL key and clicking more than one device. You can select up to 32 devices for rediscovery.

   If you select to rediscover a multiple devices, you should configure a discovery profile to run in the background. For step-by-step instructions, refer to "Configuring a discovery profile" on page 101.

3. Click **Rediscover** on the Product List toolbar.

   The **Rediscover product** dialog box displays. If you selected more than 10 devices, the client only sends the first 10 devices to the server. When rediscovery is complete on the first device and the server returns the status to the client, the client sends the next device to the server. This process continues until rediscovery is complete.

   The **Rediscover product** dialog box displays the progress status for each product in the **Progress Status** column. If an error occurs the status displays as 'Failed" and an error message displays in the **Description** column.

   Click **Abort** to stop rediscovery for any pending devices. Note that rediscovery continues for all devices already sent to the server. The **Rediscover product** dialog box closes when rediscovery is complete for the active rediscovery devices.

4. Click **OK** on the **Rediscover product** dialog box when rediscovery completes.

Rediscovering a group

To rediscover all devices in a group, complete the following steps.

1. Select the **IP** tab.
2. Select the group you want to rediscover in the Product List.

   You can select one group at a time.
3. Click **Rediscover** on the Product List toolbar.

   The **Rediscover product** dialog box displays. If you selected more than 10 devices, the client only sends the first 10 devices to the server. When rediscovery is complete on the first device and the server returns the status to the client, the client sends the next device to the server. This process continues until rediscovery is complete.

   The **Rediscover product** dialog box displays the progress status for each product in the **Progress Status** column. If an error occurs the status displays as 'Failed" and an error message displays in the **Description** column.

   Click **Abort** to stop rediscovery for any pending devices. Note that rediscovery continues for all devices already sent to the server. The **Rediscover product** dialog box closes when rediscovery is complete for the active rediscovery devices.
4. Click **OK** on the **Rediscover product** dialog box when rediscovery completes.

Enabling password validation on rediscovery

To define global setting preferences, complete the following steps.

1. Select **Discover > IP Products.**

   The **Discover Setup - IP** dialog box displays.
2. Click the **Global Settings** tab.
3. Click the **Preferences** tab.
4. Select the **Enable password validation on rediscover** check box to enable password validation when rediscovering devices.
5. Click **Apply** to close the **Discover Setup - IP** dialog box.
6. Click **Close** to close the **Discover Setup - IP** dialog box.