



## Configuring System-Related Policies

---

This chapter includes the following sections:

- [Configuring the Chassis/FEX Discovery Policy, page 1](#)
- [Configuring the Chassis Connectivity Policy, page 5](#)
- [Configuring the Rack Server Discovery Policy, page 6](#)
- [Configuring the Aging Time for the MAC Address Table, page 7](#)

## Configuring the Chassis/FEX Discovery Policy

### Chassis/FEX Discovery Policy

The chassis/FEX discovery policy determines how the system reacts when you add a new chassis or FEX. Cisco UCS Manager uses the settings in the chassis/FEX discovery policy to determine the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect and whether to group links from the IOM to the fabric interconnect in a fabric port channel.

#### Chassis Links

If you have a Cisco UCS domain that has some of the chassis wired with 1 link, some with 2 links, some with 4 links, and some with 8 links we recommend that you configure the chassis/FEX discovery policy for the minimum number links in the domain so that Cisco UCS Manager can discover all chassis.



#### Tip

If you want to establish highest available chassis connectivity in a Cisco UCS domain where Fabric Interconnect is connected to different types of IO Modules supporting different max number of uplinks, select platform max value. Setting platform max would ensure that Cisco UCS Manager would discover the chassis including the connections and servers only when maximum supported IOM uplinks are connected per IO Module.

After the initial discovery, you must reacknowledge the chassis that are wired for a greater number of links and Cisco UCS Manager configures the chassis to use all available links.

Cisco UCS Manager cannot discover any chassis that is wired for fewer links than are configured in the chassis/FEX discovery policy. For example, if the chassis/FEX discovery policy is configured for 4 links, Cisco UCS Manager cannot discover any chassis that is wired for 1 link or 2 links. Reacknowledgement of the chassis does not resolve this issue.

The following table provides an overview of how the chassis/FEX discovery policy works in a multi-chassis Cisco UCS domain:

**Table 1: Chassis/FEX Discovery Policy and Chassis Links**

<b>Number of Links Wired for the Chassis</b>	<b>1-Link Discovery Policy</b>	<b>2-Link Discovery Policy</b>	<b>4-Link Discovery Policy</b>	<b>8-Link Discovery Policy</b>	<b>Platform-Max Discovery Policy</b>
<b>1 link between IOM and fabric interconnects</b>	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.
<b>2 links between IOM and fabric interconnects</b>	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link.  After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 link.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.

<b>Number of Links Wired for the Chassis</b>	<b>1-Link Discovery Policy</b>	<b>2-Link Discovery Policy</b>	<b>4-Link Discovery Policy</b>	<b>8-Link Discovery Policy</b>	<b>Platform-Max Discovery Policy</b>
<b>4 links between IOM and fabric interconnects</b>	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link.  After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 links.  After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 link.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	If the IOM has 4 links, the chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 links.  If the IOM has 8 links, the chassis is not fully discovered by Cisco UCS Manager.
<b>8 links between IOM and fabric interconnects</b>	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link.  After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 links.  After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 links.  After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 8 links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 8 links.

### Link Grouping

For hardware configurations that support fabric port channels, link grouping determines whether all of the links from the IOM to the fabric interconnect are grouped into a fabric port channel during chassis discovery. If the link grouping preference is set to port channel, all of the links from the IOM to the fabric interconnect

are grouped in a fabric port channel. If set to no group, links from the IOM to the fabric interconnect are not grouped in a fabric port channel.

Once a fabric port channel is created, links can be added or removed by changing the link group preference and reacknowledging the chassis, or by enabling or disabling the chassis from the port channel.

**Note**

The link grouping preference only takes effect if both sides of the links between an IOM or FEX and the fabric interconnect support fabric port channels. If one side of the links does not support fabric port channels, this preference is ignored and the links are not grouped in a port channel.

## Configuring the Chassis/FEX Discovery Policy

### Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Policies** tab.
- Step 4** Click the **Global Policies** subtab.
- Step 5** In the **Chassis/FEX Discovery Policy** area, complete the following fields:

Name	Description
<b>Action</b> field	<p>Specifies the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect. This can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>1-link</b></li> <li>• <b>2-link</b></li> <li>• <b>4-link</b></li> <li>• <b>8-link</b></li> <li>• <b>Platform Max</b></li> </ul>

Name	Description
<b>Link Grouping Preference field</b>	<p>Specifies whether the links from the IOMs or FEXes to the fabric interconnects are grouped in a port channel. This can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>None</b>—No links are grouped in a port channel</li> <li>• <b>Port Channel</b>—All links from an IOM or FEX to a fabric interconnect are grouped in a port channel</li> </ul> <p><b>Note</b> The link grouping preference only takes effect if both sides of the links between an IOM or FEX and the fabric interconnect support fabric port channels. If one side of the links does not support fabric port channels, this preference is ignored and the links are not grouped in a port channel.</p>

**Step 6** Click **Save Changes**.

### What to Do Next

To customize fabric port channel connectivity for a specific chassis, configure the chassis connectivity policy.

## Configuring the Chassis Connectivity Policy

### Chassis Connectivity Policy

The chassis connectivity policy determines the whether a specific chassis is included in a fabric port channel after chassis discovery. This policy is helpful for users who want to configure one or more chassis differently from what is specified in the global chassis discovery policy. The chassis connectivity policy also allows for different connectivity modes per fabric interconnect, further expanding the level of control offered with regards to chassis connectivity.

By default, the chassis connectivity policy is set to global. This means that connectivity control is configured when the chassis is newly discovered, using the settings configured in the chassis discovery policy. Once the chassis is discovered, the chassis connectivity policy controls whether the connectivity control is set to none or port channel.



#### Note

The chassis connectivity policy is created by Cisco UCS Manager only when the hardware configuration supports fabric port channels. At this time, only the 6200 series fabric interconnects and the 2200 series IOMs support this feature. For all other hardware combinations, Cisco UCS Manager does not create a chassis connectivity policy.

## Configuring a Chassis Connectivity Policy

Changing the connectivity mode for a chassis could result in decreased VIF namespace.



### Caution

Changing the connectivity mode for a chassis results in chassis reacknowledgement. Traffic may be disrupted during this time.

### Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, expand **Equipment > Chassis**.
- Step 3** Click the chassis for which you want to configure the connectivity between the IOMs and fabric interconnects.
- Step 4** In the **Work** pane, click the **Connectivity Policy** tab.
- Step 5** For each IOM in the chassis, choose one of the following values in the **Admin State** field for the chassis and fabric connectivity:
  - **None**—No links are grouped in a port channel
  - **Port Channel**—All links from an IOM to a fabric interconnect are grouped in a port channel.
  - **Global**—The chassis inherits this configuration from the chassis discovery policy. This is the default value.
- Step 6** Click **Save Changes**.

## Configuring the Rack Server Discovery Policy

### Rack Server Discovery Policy

The rack server discovery policy determines how the system reacts when you add a new rack-mount server. Cisco UCS Manager uses the settings in the rack server discovery policy to determine whether any data on the hard disks are scrubbed and whether server discovery occurs immediately or needs to wait for explicit user acknowledgement.

Cisco UCS Manager cannot discover any rack-mount server that has not been correctly cabled and connected to the fabric interconnects. For information about how to integrate a supported Cisco UCS rack-mount server with Cisco UCS Manager, see the appropriate [rack-mount server integration guide](#).

## Configuring the Rack Server Discovery Policy

### Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Policies** tab.
- Step 4** Click the **Global Policies** subtab.
- Step 5** In the **Rack Server Discovery Policy** area, complete the following fields:

Name	Description
Action field	<p>The way Cisco UCS Manager reacts when you add a new rack server. This can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Immediate</b>—Cisco UCS Manager attempts to discover new servers automatically</li> <li>• <b>User Acknowledged</b>—Cisco UCS Manager waits until the user tells it to search for new servers</li> </ul>
Scrub Policy drop-down list	The scrub policy to run on a newly discovered server if that server meets the criteria in the selected server pool policy qualification.

- Step 6** Click **Save Changes**.

## Configuring the Aging Time for the MAC Address Table

### Aging Time for the MAC Address Table

To efficiently switch packets between ports, the fabric interconnect maintains a MAC address table. It dynamically builds the MAC address table by using the MAC source address from the packets received and the associated port on which the packets were learned. The fabric interconnect uses an aging mechanism, defined by a configurable aging timer, to determine how long an entry remains in the MAC address table. If an address remains inactive for a specified number of seconds, it is removed from the MAC address table.

You can configure the amount of time (age) that a MAC address entry (MAC address and associated port) remains in the MAC address table.

## Configuring the Aging Time for the MAC Address Table

### Procedure

- Step 1** In the **Navigation** pane, click the **Equipment** tab.
- Step 2** On the **Equipment** tab, click the **Equipment** node.
- Step 3** In the **Work** pane, click the **Policies** tab.
- Step 4** Click the **Global Policies** subtab.
- Step 5** In the **MAC Address Table Aging** area, complete the following fields:

Name	Description
<b>Aging Time</b> field	<p>The length of time an idle MAC address remains in the MAC address table before it is removed by Cisco UCS. This can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Never</b>—MAC addresses are never removed from the table regardless of how long they have been idle.</li> <li>• <b>Mode Default</b>—The system uses the default value. If the fabric interconnect is set to end-host mode, the default is 14,500 seconds. If it is set to switching mode, the default is 300 seconds.</li> <li>• <b>other</b>—Cisco UCS Manager GUI displays the <b>dd:hh:mm:ss</b> field which allows you to enter a custom value.</li> </ul>
<b>dd:hh:mm:ss</b> field	<p>The length of time a MAC address must remain idle before Cisco UCS removes it from the MAC address table. This field is only visible if you choose <b>other</b> for the aging time.</p> <p>Enter a time in the format days:hours:minutes:seconds.</p>

- Step 6** Click **Save Changes**.