



## Configuring UCS Domain Policies

- [Domain Policies, on page 1](#)
- [Creating a Port Policy, on page 4](#)
- [Creating an Ethernet Network Group Policy, on page 12](#)
- [Creating an Ethernet Network Control Policy, on page 14](#)
- [Creating a VLAN Policy, on page 16](#)
- [Creating a VSAN Policy, on page 18](#)
- [Creating an NTP Policy, on page 20](#)
- [Creating a Network Connectivity Policy, on page 21](#)
- [Creating an SNMP Policy, on page 23](#)
- [Creating a System QoS Policy, on page 25](#)
- [Creating a Syslog Policy, on page 26](#)
- [Creating a Switch Control Policy, on page 28](#)
- [Creating a Flow Control Policy, on page 35](#)
- [Creating a Link Aggregation Policy, on page 36](#)
- [Creating a Link Control Policy, on page 37](#)
- [Creating a Multicast Policy, on page 39](#)

## Domain Policies

Domain policies in Cisco Intersight allow you to configure various parameters for UCS Fabric Interconnects, including port configuration, network control settings, and VLAN and VSAN settings. A domain policy can be assigned to any number of domain profiles to provide a configuration baseline. Domain policies in Cisco Intersight are a new feature, and native to the application. Policy-based configuration with Domain Profiles is a Cisco Intersight Essentials feature, and is supported on Cisco UCS B-Series M5 and M6 servers and Cisco UCS C-Series M5, M6 and M7 servers, and Cisco UCS X-Series M6 and M7 servers that are in a UCS Domain.

The Domain Policy creation wizard in Cisco Intersight has two pages:

- **General**—The general page allows you to select the organization and enter a name for your policy. Optionally, include a short description and tag information to help identify the policy. Tags must be in the key:value format. For example, Org:IT or Site APJ
- **Policy Details**—The policy details page has properties that are applicable to UCS Domain Policies.

The following list describes the domain policies that you can configure in Cisco Intersight.

- **Port Policy**—Configures the ports and port roles for the Fabric Interconnect. Each Fabric Interconnect has a set of ports in a fixed port module that you can configure. You can enable or disable a port or a port channel.

The port policy is associated with a switch model. The network configuration limits also vary with the switch model.

The maximum number of ports and port channels supported are:

- Ethernet Uplink, Fibre Channel over Ethernet (FCoE) Uplink port channels, and Appliance port channels (combined)—12
  - Ethernet Uplink ports per port channel—16
  - FCoE Uplink ports per port channel—16
  - Ethernet Uplink and FCoE Uplink ports (combined)—31
  - Server ports—54 ports for Cisco UCS 6454 and 108 ports for Cisco UCS 64108 Fabric Interconnects
- **Ethernet Network Control Policy**—Configures the network control settings for appliance ports, appliance port channels, or vNICs.
  - **Ethernet Network Group Policy**—Configures the VLAN settings that include Native VLAN and QinQ VLAN for appliance ports, appliance port channels, or vNICs.
  - **VLAN Configuration Policy**—Creates a connection to a specific external LAN.
  - **VSAN Configuration Policy**—Partitions the Fibre Channel fabric into one or more zones. Each zone defines the set of Fibre Channel initiators and Fibre Channel targets that can communicate with each other in a VSAN.
  - **NTP Policy**—Enables the NTP service to configure a UCS system that is managed by Cisco Intersight to synchronize the time with an NTP server. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers. When you enable the NTP service, Cisco Intersight configures the NTP details on the endpoint. For more information, see [Creating an NTP policy](#).
  - **Network Connectivity Policy**—Specifies the DNS Domain settings that are used to add or update the resource records on the DNS server from the endpoints, and the DNS server settings for IPv4 and IPv6 on an endpoint.
  - **System QoS Policy (Preview)**—Implements network traffic prioritization based on the importance of the connected network by assigning system classes for individual vNICs. Intersight uses Data Center Ethernet (DCE) to handle all traffic inside a Cisco UCS domain. This industry standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. Two virtual lanes are reserved for internal system and management traffic. You can configure quality of service (QoS) for the other six virtual lanes. System classes determine how the DCE bandwidth in these six virtual lanes is allocated across the entire Cisco UCS domain.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic, which provides a level of traffic management, even in an oversubscribed system. For example, you can configure the **Fibre Channel Priority** system class to determine the percentage of DCE bandwidth allocated to FCoE traffic. The configuration setup validates each input on the system class to prevent duplicate or invalid entries.

This feature is in preview and is not meant for use in your production environment. Cisco recommends that you use this feature on a test network or system.

The following list describes the system classes that you can configure.

- **Platinum, Gold, Silver, and Bronze**—A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.
- **Best Effort**—A system class that sets the quality of service for the lane reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class.
- **Fibre Channel**—A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class.
- **Multicast Policy (Preview)**—Configures Internet Group Management Protocol (IGMP) snooping and IGMP querier. IGMP Snooping dynamically determines hosts in a VLAN that should be included in multicast transmissions.

You can create, modify, and delete a multicast policy that can be associated to one or more VLANs. When a multicast policy is modified, all VLANs associated with that multicast policy are re-processed to apply the changes. By default, IGMP snooping is enabled and IGMP querier is disabled. On enabling IGMP querier, you can configure the IPv4 addresses for the local and peer IGMP snooping querier interfaces.

- **Simple Network Management Protocol (SNMP) Policy**—Configures the SNMP settings for sending fault and alert information by SNMP traps from the managed devices. Any existing SNMP Users or SNMP Traps configured previously on the managed devices are removed and replaced with users or traps that you configure in this policy.
- **Syslog Policy**—Enables to configure the local logging and remote logging (minimum severity) for an endpoint. This policy also provides configuration support to store the syslog messages in the local file and the remote syslog server.
- **Switch Control Policy (Preview)**—Enables to configure and manage multiple network operations on the Fabric Interconnects (FI) that include:
  - **Port Count Optimization**—If the VLAN port count optimization is enabled, the Virtual Port (VP) groups are configured on the Fabric Interconnect (FI) and if VLAN port count optimization is disabled, the configured VP groups are removed from the FI.
  - **MAC Aging Time**—Allows to set the MAC aging time for the MAC address table entries. The MAC aging time specifies the time before a MAC entry expires and discards the entry from the MAC address table.
  - **Link Control Global Settings**—Enables configurations of message interval time in seconds and allows to reset the recovery action of an error-disabled port.
- **Flow Control Policy**—Enables configurations for Priority Flow Control for ports and port channels.
- **Link Control Policy**—Enables configurations of Link Control administrative state and configuration (normal or aggressive) mode for ports.

- **Link Aggregation Policy**— Enables to configure Link Aggregation properties. Link Aggregation combines multiple network connections in parallel to increase throughput and to provide redundancy.

## Creating a Port Policy

The port policy is used for configuring the port parameters such as unified ports that carry Ethernet or Fibre Channel traffic, port roles and speed.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **Port**, and then click **Start**.
5. On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Switch Model</b>	Select any one of the following switch models: <ul style="list-style-type: none"> <li>• Cisco UCS 64108 Fabric Interconnect</li> <li>• Cisco UCS 6454 Fabric Interconnect</li> <li>• Cisco UCS 6536 Fabric Interconnect</li> </ul> <p><b>Note</b> The switch models provide different network configuration capabilities to the policy. The switch model cannot be changed once the policy is created.</p>
<b>Description (Optional)</b>	Provide a short description
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

6. On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Unified Ports</b>	By default, all the unconfigured ports are Ethernet ports. Use the blue slider to select a range of Fibre Channel ports. The selected Fibre Channel ports are highlighted in blue.

Property	Essential Information
<b>Fibre Channel (FC)</b>	Displays the port range selected for Fibre Channel.  <b>Note</b> <ul style="list-style-type: none"> <li>Valid FC port range for Cisco UCS 6454 Fabric Interconnect: <b>Port 1-16</b></li> <li>Valid FC port range for Cisco UCS 64108 Fabric Interconnect: <b>Port 1-16</b></li> <li>Valid FC port range for Cisco UCS 6536 Fabric Interconnect: <b>Port 33-36</b></li> </ul>
<b>Ethernet</b>	Displays the port range selected for Ethernet.

7. On the **Breakout Options** page, configure the breakout ports on Fibre Channel or Ethernet.

**Note**

To configure breakout port, you must upgrade your Fabric Interconnect firmware to firmware version 4.2(2a) and above.

In Cisco UCS 6536 Fabric Interconnect, only FC breakout is supported.

- Select the ports for breakout either by clicking on the valid ports within the graphic image or by selecting the port number in the table present below the image.

Following are the breakout port range for different Cisco UCS Fabric Interconnects:

- Cisco UCS 64108 Fabric Interconnect, the valid breakout port range is 97—108
  - Cisco UCS 6454 Fabric Interconnect, the valid breakout port range is 49—54
  - Cisco UCS 6536 Fabric Interconnects. the valid breakout port range is 1—36
- Click **Configure**.  
A pop-up window appears. It displays the admin speeds that can be set for the breakout ports.  
Ethernet breakout ports can be configured with three options : no breakout, Admin speed of 4x10G, and Admin speed of 4x25G  
FC breakout ports can be configured in three different **Admin Speed**: 4x8G, 4x16G, and 4x32G
  - Select the desired speed.



**Note** You can configure Ethernet breakout and switch between breakout speeds without requiring a FI reboot.

Changing the FC breakout speeds does not require FI reboot.

Switching from the Ethernet breakout to the FC breakout and vice versa, or from the Ethernet port to the FC breakout port and vice versa, requires an FI reboot each time.

- Click **Set**.
- Click **Next**.

8. On the **Port Roles** page, select the ports that have to be configured for port roles either in the graphic image or by selecting in the table present below the graphic image.

<b>Selected Ports</b>	Indicates the port number(s) selected.
<b>Name</b>	The user determined port name.
<b>Type</b>	The type can be <b>Ethernet</b> or <b>FC</b> .

<b>Role</b>	<p>Select the port role type:</p> <p>The roles for an Ethernet port are:</p> <ul style="list-style-type: none"> <li>• <b>Unconfigured</b>—Default</li> <li>• <b>Server</b>—All server traffic travels through the input or output (I/O) module to server ports on the fabric interconnect. <ul style="list-style-type: none"> <li><b>Note</b> <ul style="list-style-type: none"> <li>• For Cisco UCS 6454 Fabric Interconnect, the maximum number of server ports allowed is 54. For Cisco UCS 64108 Fabric Interconnect, the maximum number of server ports allowed is 108.</li> <li>• For Cisco UCS 6536 Fabric Interconnect, server roles are not supported on 10G breakout ports.</li> <li>• Server port configuration is supported for discovering direct-attach Cisco UCS C-Series servers only after configuring breakout port on Ports 49-54 for Cisco UCS 6454 Fabric Interconnect and on Ports 97-108 for Cisco UCS 64108 Fabric Interconnect.</li> <li>• Discovering chassis, blade server connected to chassis, or rack servers connected to FEX are not supported after configuring breakout port on Ports 49-54 for Cisco UCS 6454 Fabric Interconnect and on Ports 97-108 for Cisco UCS 64108 Fabric Interconnect.</li> </ul> </li> </ul> </li> <li>• <b>Ethernet Uplink</b>—Ethernet traffic passes through the unified uplink port <ul style="list-style-type: none"> <li><b>Note</b> The maximum number of combined Ethernet Uplink ports and FCoE Uplink ports allowed is 31.</li> </ul> </li> <li>• <b>Appliance</b>—Allows the Network File System to connect directly with the Fabric Interconnects, without traffic having to pass through the uplink ports.</li> </ul> <p>The roles for an FC port are:</p> <ul style="list-style-type: none"> <li>• <b>FC Uplink</b> —FC traffic passes through the FC uplink port. To specify the role of an FC port as an FC Uplink port the VSAN scope of the port must have been created as Storage and Uplink, or as Uplink in the VSAN Configuration policy.</li> <li>• <b>FC Storage</b>—FC port acts as a storage port. To specify the role of an FC port as an FC Storage port the VSAN scope of the port must have been created as Storage and Uplink, or as Storage in the VSAN Configuration policy. Moreover, the FC has to be in the switching mode.</li> <li>• <b>Unconfigured</b>—Unconfigured is the default role of the port.</li> </ul>
-------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Admin Speed</b>	<p>The administrative port speed. The options are:</p> <ul style="list-style-type: none"> <li>• 1GBPS</li> <li>• 10GBPS</li> <li>• 25GBPS</li> <li>• 40GBPS</li> <li>• 100GBPS</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Admin Speed cannot be selected for any role on breakout ports.</li> <li>• For Cisco UCS 6536 Fabric Interconnect, only 25G/40G/100G connectivity is supported for server ports.</li> </ul> <p><b>Note</b> When the 25GBPS admin speed is selected, <b>Enable 25GBPS Copper Cable Negotiation</b> is automatically enabled for any copper cable that is more than 3 meters.</p> <p>Enable 25GBPS Copper Cable Negotiation:</p> <ul style="list-style-type: none"> <li>• Supports only on Appliance, Ethernet Uplink, FCoE Uplink port roles.</li> <li>• Does not support breakout ports.</li> <li>• Supports firmware versions 4.2(1a) or higher.</li> <li>• Supports only for the FEC configuration set to Auto.</li> </ul>
<b>VSAN ID</b>	The VSAN ID of an FC port as specified in the VSAN Configuration policy.
<b>FEC</b>	<p>The forward error correction configuration for the port:</p> <ul style="list-style-type: none"> <li>• Auto</li> <li>• C191—Supported with 25GBPS and 100GBPS Admin speed</li> </ul> <p><b>Note</b> C191 is not present for <i>Server Port</i> role.</p> <ul style="list-style-type: none"> <li>• C174—Supported with 25GBPS Admin speed</li> </ul>
<b>Priority</b>	Select the priority of the port for routing traffic and ensuring QoS.
<b>Mode</b>	Select the port mode. Port mode can be Trunk or Access.



<b>Connected Device Type and Device Number</b>	<p>Select the device type and device number for each port or a set of ports.</p> <p><b>Note</b> This option is applicable for Server Roles only.</p> <p>By default, this option is disabled.</p> <p>To enable:</p> <ul style="list-style-type: none"> <li>• Select the ports and click <b>Configure</b>.</li> <li>• Turn the <b>Manual Chassis/Server Numbering</b> button ON.</li> </ul> <p>A table is displayed where you can specify the <b>Connected Device Type</b> and <b>Device Number</b> for each port.</p> <p><b>Note</b> <b>Auto-Fill Numbering</b> can be enabled to edit <b>Connected Device Type</b>, <b>Starting Device Number</b>, and <b>Ports per Device</b> for each port according to your preferences.</p> <ul style="list-style-type: none"> <li>• Click <b>Save</b> to see the <b>Connected Device Type</b> and <b>Device Number</b> columns in the Port Roles list view.</li> </ul> <p><b>Note</b> If the selected <b>Device Number</b> is already allocated for any other server/chassis on any other port then the next available number will be allocated to the server that is discovered. This action will not result in failure of Port Policy deployment.</p> <p><b>Note</b> The Port Policy changes are not applicable for FEX.</p>
<b>Ethernet Network Group</b>	<p>Select the Ethernet Network Group policy that is to be attached to the ethernet uplink or appliance port. The Ethernet Network Group policy specifies the Allowed VLANs and the Native VLAN.</p> <p><b>Note</b> Ethernet Network Group policy applies only for ports with ethernet uplink and appliance roles.</p> <p><b>Note</b> To create Ethernet Network Groups for configuring Disjoint VLANs, ensure that the groups are completely disjoint. Partial overlap of VLANs is not allowed.</p>
<b>Ethernet Network Control</b>	<p>Select the Ethernet Network Control policy that is to be attached to the appliance port. The Ethernet Network Control policy allows you to enable or disable CDP, specify the MAC Register Mode, the action to be taken on uplink fail, the MAC security details and LLDP details.</p> <p><b>Note</b> Ethernet Network Control policy applies only for a port with an appliance role.</p>
<b>Port</b>	<p>Select the valid port range:</p> <ul style="list-style-type: none"> <li>• <b>Port 1-96</b>—Auto, 10GBPS, and 25GBPS</li> <li>• <b>Port 89-96</b>—Auto, 1GBPS, 10GBPS, and 25GBPS</li> <li>• <b>Port 97-108</b>—Auto, 40GBPS, and 100GBPS</li> </ul>

### Port Channels

Click **Create Port Channel** where you can choose the role for the selected ports.

Select the ports for configuration either by clicking on the ports within the graphic image or in the box next to the desired port within the table.

<b>Role</b>	<p>The port channel role type. The role type can be:</p> <ul style="list-style-type: none"> <li>• Ethernet Uplink Port Channel</li> <li>• FC Uplink Port Channel</li> <li>• FCoE Uplink Port Channel</li> <li>• Appliance Port Channel</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• The maximum number of ports allowed for: <ul style="list-style-type: none"> <li>• Ethernet Uplink port channel, FCoE Uplink port channel, and Appliance port channel (combined) is 12</li> <li>• FC uplink port channel is 4</li> <li>• Ethernet ports per port channel is 16</li> <li>• FCoE Uplink ports per port channel is 16</li> </ul> </li> <li>• You cannot combine normal ports and breakout ports for any port channel. For example, Uplink port channel ID 100 with members 1/96 and 1/97/1 are not allowed.</li> <li>• If a port with a speed of 100G in Cisco UCS 6536 Fabric Interconnect, is connected with N9K-C93180YC-FX3, then you must disable <b>Auto Negotiation</b> while assigning the port role.</li> <li>• For FC uplink Port Channel, port channel with different port speed is not allowed. For example, FC uplink port channel ID 101 with member 1/33 with port speed 8Gbps and 1/34 with port speed 16Gbps are not allowed.</li> </ul>
<b>PC ID</b>	Unique Identifier of the port channel, local to this switch.

<b>Admin Speed</b>	<p>The administrative port channel speed options for Uplink, Uplink Port Channel, and FCoE Uplink Port Channel are:</p> <ul style="list-style-type: none"> <li>• 1GBPS</li> <li>• 10GBPS</li> <li>• 25GBPS</li> <li>• 40GBPS</li> <li>• 100GBPS</li> </ul> <p>The administrative port channel speed options for FC Uplink and FC Uplink Port Channel are:</p> <ul style="list-style-type: none"> <li>• 8GBPS</li> <li>• 16GBPS</li> <li>• 32GBPS</li> </ul> <p><b>Note</b> You cannot select Admin Speed for any roles on breakout ports.</p>
<b>Priority</b>	Select the priority of the port channel for routing traffic and ensuring QoS.
<b>Mode</b>	Select the port channel mode. Port channel mode can be Trunk or Access.
<b>Ethernet Network Group</b>	<p>Select the Ethernet Network Group policy that is to be attached to the ethernet uplink or appliance port channel. The Ethernet Network Group policy specifies the Allowed VLANs and the Native VLAN.</p> <p><b>Note</b> Ethernet Network Group policy applies to port channels with ethernet uplink and appliance roles.</p> <p><b>Note</b> To create Ethernet Network Groups for configuring Disjoint VLANs, ensure that the groups are completely disjoint. Partial overlap of VLANs is not allowed.</p>
<b>Ethernet Network Control</b>	<p>Select the Ethernet Network Control policy that is to be attached to the appliance port channel. The Ethernet Network Control policy allows you to enable or disable CDP, specify the MAC Register Mode, the action to be taken on uplink fail, the MAC security details and LLDP details.</p> <p><b>Note</b> Ethernet Network Control policy applies only for a port channel with an appliance role.</p>
<b>Port Channel</b>	Select the valid port channel range between 1 and 256.

**Pin Groups**

Pin Group is used to pin Ethernet/FC traffic from a vNIC/vHBA on a server to an uplink Ethernet/FC port or port channel on the Fabric Interconnect. You can use this pinning to manage the distribution of traffic from the servers. Static pinning is not supported when FI are in Switching Mode (Ethernet and FC).

To configure pinning for a server, you must include the LAN/SAN pin group in the LAN/SAN connectivity policy.

Click **Create Pin Group** to specify the ports/port channels in the FI through which the LAN and SAN data traffic can be made to flow.

<b>Pin Group Type</b>	The type of the data traffic that needs to flow to the pinned ports/port channels. The type can be <ul style="list-style-type: none"> <li>• LAN</li> <li>• SAN</li> </ul>
<b>Pin Group Name</b>	The name of the Pin Group. This name will appear in LAN/SAN Connectivity policy creation page, once the Pin Group is created.
<b>Interface Type</b>	The type of the interface on the Fabric Interconnect. <ul style="list-style-type: none"> <li>• Port</li> <li>• Port Channels</li> </ul>
<b>Port Selection</b>	From the available table, you can select the ports and the breakout ports that should be pinned for data traffic flow.  It is enabled by default.

9. Click **Save**.

## Creating an Ethernet Network Group Policy

An Ethernet Network Group policy enables you to manage settings for VLANs on a UCS Server. These settings include defining which VLANs are allowed, designating a Native VLAN, and specifying a QinQ VLAN.

This policy also supports VIC QinQ Tunneling. A QinQ (802.1Qin802.1Q) tunnel allows segregation and isolation of different VLANs within a network. To configure QinQ VLAN, you can specify the desired VLAN ID as part of the VLAN settings for the specific port, port channel, or vNIC. This enables the transmission of multiple VLANs over a single VLAN trunk.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **Ethernet Network Group**, and then click **Start**.

5. On the **General** page, configure the following parameters:

Property	Essential Information
Organization	Select the Organization.
Name	Enter a name for your policy.
Set Tag (Optional)	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.
Description (Optional)	Provide a short description

6. On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>VLAN Settings</b>	
Native VLANs	<p>This property allows you to specify the native VLAN ID for the virtual interface or its corresponding vethernet in a range of 1-4093.</p> <ul style="list-style-type: none"> <li>• If the native VLAN is not already part of the allowed VLANs, it will be automatically added to the list of allowed VLANs.</li> <li>• If QinQ Tunneling is enabled, the native VLAN and Allowed VLAN properties are combined.</li> </ul>
Enable QinQ Tunneling	Slide to enable VIC QinQ (802.1Qin802.1Q) Tunneling.
Allowed VLANs	<p>Refers to the VLANs that are permitted for the virtual interface. You can specify the allowed VLANs by providing a list of comma-separated VLAN IDs and VLAN ID ranges.</p> <p>For example, you can enter VLAN IDs 10, 20, 30-40 to allow VLANs 10, 20, and a range from 30 to 40.</p> <p><b>Note</b> This property is displayed only when <i>Enable QinQ Tunneling</i> slider is disabled.</p>

Property	Essential Information
<b>QinQ VLAN</b>	<p>This property enables the configuration of QinQ Tunneling, that facilitates the encapsulation of multiple VLANs within a single VLAN. The supported VLAN IDs range from 2 to 4093 that allows you to effectively manage and segregate the network traffic.</p> <p><b>Note</b> This property is available only when <i>Enable QinQ Tunneling</i> slider is enabled.</p>



**Note** To make the server an Isolated host or a Community host, specify the ID of an Isolated VLAN or a Community VLAN in both Allowed VLANs and Native VLAN

- Click **Create**.

## Creating an Ethernet Network Control Policy

Ethernet Network Control policies configure the network control settings for the UCS Domain. This policy is applicable only for the Appliance Ports defined in a Port Policy and for the vNICs defined in a LAN Connectivity Policy, on an FI-Attached UCS Servers.

- Log in to Cisco Intersight with your Cisco ID and select admin role.
- From the **Service Selector** drop-down list, select **Infrastructure Service**.
- Navigate to **Configure > Policies**, and then click **Create Policy**.
- Select **Ethernet Network Control**, and then click **Start**.
- On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Description (Optional)</b>	Provide a short description
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

- On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Enable CDP</b>	Enables the Cisco Discovery Protocol (CDP) on an interface.
<b>MAC Register Mode</b>	<p>Determines the MAC addresses to be registered with the switch. This can be:</p> <ul style="list-style-type: none"> <li>• <b>Only Native VLAN</b>—MAC addresses are only added to the native VLAN. This option is the default, and it maximizes the port+VLAN count.</li> <li>• <b>All Host VLANs</b>—MAC addresses are added to all VLANs with which they are associated. Select this option if your VLANs are configured to use trunking but are not running in Promiscuous mode.</li> </ul>
<b>Action on Uplink Fail</b>	<p>Determines how the interface behaves if no uplink port is available when the switch is in end-host mode.</p> <ul style="list-style-type: none"> <li>• <b>Link Down</b>—Changes the operational state of a vNIC to down when uplink connectivity is lost on the switch, and enables fabric failover for vNICs. This is the default option.</li> <li>• <b>Warning</b>—Maintains server-to-server connectivity even when no uplink port is available, and disables fabric failover when uplink connectivity is lost on the switch.</li> </ul>
<b>MAC Security Forge</b>	<p>Determines whether forged MAC addresses are allowed or denied when packets are sent from the server to the switch. This can be:</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>— All server packets are accepted by the switch, regardless of the MAC address associated with the packets. This is the default option.</li> <li>• <b>Deny</b>— After the first packet has been sent to the switch, all other packets must use the same MAC address or they will be silently rejected by the switch. In effect, this option enables port security for the associated vNIC.</li> </ul>

Property	Essential Information
<b>LLDP</b>	<p>Determines whether interfaces can transmit or receive LLDP packets.</p> <ul style="list-style-type: none"> <li>To enable or disable the transmission of LLDP packets on an interface, click <b>Enable Transmit</b>.</li> <li>To enable or disable the receipt of LLDP packets on an interface, click <b>Enable Receive</b>.</li> </ul>

- Click **Create**.

## Creating a VLAN Policy

VLAN policies create a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, including broadcast traffic. You can create VLANs and Private VLANs using the VLAN policy.



**Note** Ensure that each VLAN is associated with a multicast policy. You can edit the existing VLANs and associate them to a multicast policy. You cannot associate a Multicast policy to a Private VLAN.

- Log in to Cisco Intersight with your Cisco ID and select admin role.
- From the **Service Selector** drop-down list, select **Infrastructure Service**.
- Navigate to **Configure > Policies**, and then click **Create Policy**.
- Select **VLAN**, and then click **Start**.
- On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Description (Optional)</b>	Provide a short description
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

- On the **Policy Details** page, click **Add VLAN** and configure the following policy details:



**Note** The maximum number of VLANs allowed per Ethernet Network Policy is 3000.



Property	Essential Information
<b>Add VLANs</b>	Click Add VLANs to add VLANs and Private VLANs
<b>Name/Prefix</b>	For a single VLAN, this is the VLAN name. For a range of VLANs, this is the prefix that the system uses for each VLAN name.
<b>VLAN IDs</b>	<p>Enter the VLAN ID number or a number range between 2 and 4093. You can enter a range of IDs using a hyphen, and you can enter multiple IDs or ID ranges separated by commas. Examples of valid VLAN IDs or ID ranges are 50, 200, 2000-2100. You cannot use VLANs from 3915-4042, 4043-4047, 4094, and 4095 because these IDs are reserved for system use.</p> <p>The name that you assign to a VLAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VLAN.</p>
<b>Auto Allow on Uplinks</b>	<p>Used to determine whether this VLAN will be allowed on all uplink ports and port channels in this Fabric Interconnect.</p> <p><b>Enable</b> to allow this VLAN on uplink ports and port channels.</p> <p><b>Disable</b> to configure disjoint VLANs.</p>
<b>Multicast Policy</b>	<p>Click <b>Select Policy</b> and choose a Multicast policy that needs to be associated with VLAN.</p> <p>Click <b>Create New</b> to create a new Multicast policy that will be available to all VLANs.</p> <p><b>Note</b> You cannot add Multicast policy for a Private VLAN.</p>
<b>Enable VLAN Sharing</b>	<b>Enable</b> to create Private VLANs.

Property	Essential Information
Sharing Type	<p>The Sharing type can be:</p> <ul style="list-style-type: none"> <li>• <b>Primary:</b> The Primary VLAN of a Private VLAN. Secondary VLANs are mapped to Primary VLANs.</li> </ul> <p><b>Note</b> You must create the Primary VLAN before creating the Isolated or Community VLANs.</p> <ul style="list-style-type: none"> <li>• <b>Isolated:</b> One of the two Sharing Types of a Secondary VLAN. Only one Isolated VLAN can be mapped to a Primary VLAN.</li> <li>• <b>Community:</b> One of the Sharing Types of a Secondary VLAN. Multiple Community VLANs can be mapped to a Primary VLAN.</li> </ul>
Primary VLAN ID	<p>The Primary VLAN to which a Community or Isolated VLAN is to be mapped.</p> <p><b>Note</b> When a Secondary VLAN is mapped to a Primary VLAN, you cannot modify or delete the Primary VLAN.</p>



**Note** If the VLAN configuration in the domain profile is modified, the corresponding changes in the server profile will take effect only after the server profile is redeployed.

7. Click **Add**.

## Creating a VSAN Policy

With the VSAN policy, you can create Virtual SANs (VSANs) to isolate devices physically connected to the same SAN fabric. VSANs improve security and stability in Fibre Channel fabrics and let you create several logical SANs over a common physical infrastructure.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **VSAN**, and then click **Start**.
5. On the **General** page, configure the following parameters:

Property	Essential Information
Organization	Select the Organization.
Name	Enter a name for your policy.
Description (Optional)	Provide a short description
Add Tag (Optional)	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

6. On the **Policy Details** page, do the following:

- Click **Trunking Mode** to enable or disable Fibre Channel uplink trunking.

If you enable trunking for the named VSANs on a Fabric Interconnect, all named VSANs in the Cisco UCS domain are allowed on all Fibre Channel uplink ports on that Fabric Interconnect. If you configure Fabric Interconnects for Fibre Channel end-host mode, enabling Fibre Channel uplink trunking renders all VSANs with an ID in the range from 3840 to 4079 non-operational.

- Click **Add VSAN** and configure the following policy details:

Property	Essential Information
Name	The user-defined name given to the VSAN configuration.
VSAN Scope	<p>The scope of the VSAN. Indicate if the VSAN is a storage and uplink VSAN, a storage VSAN, or an uplink VSAN</p> <p>VSAN Scope can be:</p> <ul style="list-style-type: none"> <li>Storage and Uplink</li> <li>Storage</li> <li>Uplink</li> </ul> <p><b>Note</b> If you want to create an FC Zone policy for a VSAN, then the VSAN scope must be Storage.</p>
VSAN ID	The unique identifier for the VSAN on the switch. The VSAN ID can be between 1 and 4093.

Property	Essential Information
<b>FCoE VLAN ID</b>	<p>The unique identifier assigned to the VLAN used for Fibre Channel connections.</p> <p>IDs of FCOE VLANs associated with the VSAN configuration must be between 2 and 4093. VLAN IDs from 3915-4042, 4043-4047, 4094, and 4095 are reserved for system use.</p> <p>By default, VLAN 4048 is mapped to VSAN-1 on the switch. Attempting to use VLAN 4048 for FCoE in a VSAN Policy will result in an error. In this case, you need to explicitly configure VSAN-1 to use a different FCOE VLAN ID in the VSAN policy.</p>

- Click **Create**.

## Creating an NTP Policy

The NTP policy enables the NTP service to configure a UCS system that is managed by Cisco Intersight to synchronize the time with an NTP server. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers. When you enable the NTP service, Cisco Intersight configures the NTP details on the endpoint.

- Log in to Cisco Intersight with your Cisco ID and select admin role.
- From the **Service Selector** drop-down list, select **Infrastructure Service**.
- Navigate to **Configure > Policies**, and then click **Create Policy**.
- Select **NTP**, and then click **Start**.
- On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Description (Optional)</b>	Provide a short description
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

- On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Enable NTP</b>	Enables NTP policy configuration.

Property	Essential Information
<b>NTP Servers</b>	A collection of NTP Server IP addresses or hostnames.
<b>Time Zone</b>	A collection of time zones from which you can select a time zone for the endpoint.  This property is applicable to switches and to Cisco IMC (standalone) servers.

When a hostname is used for NTP configuration, DNS server information must be configured in the Network Connectivity policy.

- Click **Create**.

## Creating a Network Connectivity Policy

The Network Connectivity policy enables you to configure and assign IPv4 and IPv6 addresses.

### Dynamic DNS

Dynamic DNS (DDNS) is used to add or update the resource records on the DNS server. When you enable the DDNS option, the DDNS service records the current hostname, Domain name, and the management IP address and updates the resource records in the DNS server.

- Log in to Cisco Intersight with your Cisco ID and select admin role.
- From the **Service Selector** drop-down list, select **Infrastructure Service**.
- Navigate to **Configure > Policies**, and then click **Create Policy**.
- Select **Network Connectivity**, and then click **Start**.
- On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Description (Optional)</b>	Provide a short description
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

- On the **Policy Details** page, configure the following properties:

### Common Properties

Property	Essential Information
<b>Enable Dynamic DNS</b>	Enables Dynamic DNS.  This property is not applicable to Fabric Interconnects.
<b>Dynamic DNS Update Domain</b>	Specify the dynamic DNS Domain. The Domain can be either a main Domain or a sub-Domain.  This property is not applicable to Fabric Interconnects.

#### IPv4 Properties

Property	Essential Information
<b>Obtain IPv4 DNS Server Addresses from DHCP</b>	Whether the IPv4 addresses are obtained from Dynamic Host Configuration Protocol (DHCP) or from a specifically configured set of DNS servers. <ul style="list-style-type: none"> <li>• Enabled—Intersight uses DHCP</li> <li>• Disabled—Intersight uses a configured set of IPv4 DNS servers.</li> </ul> This property is not applicable to Fabric Interconnects.
<b>Preferred IPv4 DNS Server</b>	The IP address of the primary DNS server. This property is displayed only when <b>Obtain IPv4 DNS Server Addresses from DHCP</b> is disabled.
<b>Alternate IPv4 DNS Server</b>	The IP address of the secondary DNS server. This property is displayed only when <b>Obtain IPv4 DNS Server Addresses from DHCP</b> is disabled.

  

Property	Essential Information
<b>Enable IPv6</b>	Whether IPv6 is enabled. You can configure IPv6 properties only if this property is enabled.

#### IPv6 Properties

Property	Essential Information
<b>Obtain IPv6 DNS Server Addresses from DHCP</b>	Whether the IPv6 addresses are obtained from Dynamic Host Configuration Protocol (DHCP) or from a specifically configured set of DNS servers. <ul style="list-style-type: none"> <li>• Enabled—Intersight uses DHCP</li> <li>• Disabled—Intersight uses a configured set of IPv6 DNS servers.</li> </ul> This property is not applicable to Fabric Interconnects.
<b>Preferred IPv6 DNS Server</b>	The IP address of the primary DNS server. This property is displayed only when <b>Obtain IPv6 DNS Server Addresses from DHCP</b> is disabled.
<b>Alternate IPv6 DNS Server</b>	The IP address of the secondary DNS server. This property is displayed only when <b>Obtain IPv6 DNS Server Addresses from DHCP</b> is disabled.

7. Click **Create**.

## Creating an SNMP Policy

The SNMP policy configures the SNMP settings for sending fault and alert information by SNMP traps from the managed devices. This policy supports SNMP versions such as SNMPv1, SNMPv2(includes v2c), and SNMPv3. Any existing SNMP Users or SNMP Traps configured previously on the managed devices are removed and replaced with users or traps that you configure in this policy.

Using the SNMP Policy you can enable or disable SNMP, specify the access and community strings, and provide the SNMP user details that is used to retrieve data.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **SNMP**, and then click **Start**.
5. In the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the organization.
<b>Name</b>	Enter a name for your policy.
<b>Tag (optional)</b>	Enter a tag in the key value format. For example, Org: IT or Site: APJ.
<b>Description (optional)</b>	Enter a short description.

6. In the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Enable SNMP</b>	Displays the state of the SNMP Policy on the endpoint. Enable this option for the endpoint to send SNMP traps to the designated host.
<b>Access Community String</b>	Enter the SNMPv1, SNMPv2 community string or the SNMPv3 username. This field allows maximum of 18 characters.
<b>Trap Community String</b>	Enter the SNMP community group name used for sending SNMP trap to other devices.  <b>Note</b> This field is applicable only for SNMPv2c trap host or destination.
<b>System Contact</b>	The contact person responsible for the SNMP implementation. Enter a string up to 64 characters, such as an email address or a name and telephone number.
<b>System Location</b>	The location of host on which the SNMP agent (server) runs.
<b>SNMP Users</b>	
<b>Name</b>	Enter the SNMP username. This field must have a minimum of 1 and a maximum of 31 characters.
<b>Security Level</b>	Select the security mechanism for communication between the agent and the manager that include: <ul style="list-style-type: none"> <li>• AuthPriv</li> <li>• AuthNoPriv</li> </ul>
<b>Auth Type</b>	Select <b>SHA</b> as the authorization protocol for authenticating the user.  <b>Note</b> The MD5 authorization protocol is not supported.
<b>Auth Password</b>	Enter the authorization password for the user.
<b>Auth Password Confirmation</b>	Enter the authorization password confirmation for the user.
<b>Privacy Type</b>	Select <b>AES</b> as the privacy protocol for the user.  <b>Note</b> The <b>DES</b> privacy type is deprecated to meet security standards.
<b>Privacy Password</b>	Enter the privacy password for the user.



Property	Essential Information
Privacy Password Confirmation	Enter the privacy password confirmation for the user.
<b>SNMP Trap Destinations</b>	
Enable	Enable this option to use the SNMP policy.
SNMP Version	Select <b>V2</b> or <b>V3</b> as the SNMP version for the trap.
User	Select the SNMP user for the trap. You can define maximum of 15 trap users.  <b>Note</b> This field is applicable only to SNMPv3.
Trap Type	Select the trap type to receive a notification when a trap is received at the destination: <ul style="list-style-type: none"> <li>• Trap</li> <li>• Inform</li> </ul>
Destination Address	Provide the address to which the SNMP trap information can be sent. You are allowed to define maximum of 10 trap destinations.
Port	Enter the port number for the server to communicate with trap destination. The range is from 1 to 65535. The default is 162.

7. Click **Create**.

## Creating a System QoS Policy

A System Quality of Service (QoS) policy assigns a system class to the outgoing traffic. This system class determines the quality of service for the outgoing traffic.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **System QoS**, and then click **Start**.
5. On the **General** page, configure the following parameters:

Property	Essential Information
Organization	Select the Organization.
Name	Enter a name for your policy.

Property	Essential Information
Description (Optional)	Provide a short description
Add Tag (Optional)	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

6. On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Platinum</b> <b>Gold</b> <b>Silver</b> <b>Bronze</b>	<p>This option enables you to configure the associated QoS class on the fabric interconnect and assign the class to a QoS policy.</p> <p><b>Note</b> The <b>Best Effort</b> or <b>Fibre Channel</b> system classes are enabled by default.</p>
CoS	Set the class of service (CoS) by entering an integer value between 0 and 6, with 0 being the lowest priority and 6 being the highest priority. Set the value to 0 only when you require the system class to be the default system class for traffic if the QoS policy is deleted or the assigned system class is disabled.
Weight	An integer between 1 and 10. If you enter an integer, Cisco UCS determines the percentage of network bandwidth assigned to the priority level as described in the <b>Weight</b> field.
Allow Packet Drops	<p>You can select to allow the packet drop for this system class during transmission.</p> <p>This field is always selected for the <b>Best Effort</b> class, which allows dropped packets, and always not selected for the <b>Fibre Channel</b> class, which never allows dropped packets.</p>
MTU	The maximum transmission unit (MTU) for the channel. You can enter an integer between 1500 and 9216. This value corresponds to the maximum packet size.

7. Click **Create**.

## Creating a Syslog Policy

The Syslog policy defines the minimum severity as logging level from an endpoint. The policy also defines the target destination to store the Syslog messages, and the Hostname or the IP Address, the port information, and the communication protocol for the Remote Logging Servers.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **Syslog**, and then click **Start**.
5. On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Description (Optional)</b>	Provide a short description
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

6. On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Local Logging</b>	
<b>Minimum Severity to Report</b>	Select the lowest severity level to report in the remote log. The severity levels are: <ul style="list-style-type: none"> <li>• 0 Emergency</li> <li>• 1 Alert</li> <li>• 2 Critical</li> <li>• 3 Error</li> <li>• 4 Warning</li> <li>• 5 Notice</li> <li>• 6 Informational</li> <li>• 7 Debug</li> </ul>
<b>Remote Logging - Syslog Server 1 and Syslog Server 2</b>	
<b>Enable</b>	Select this option to enable or disable the Syslog policy.

Property	Essential Information
Hostname/IP Address	<p>Enter the hostname or IP address of the Syslog server to store the Cisco IMC log. You can set an IPv4 or IPv6 address or a domain name as the remote system address.</p> <p><b>Note</b> If you have both IPv4 and IPv6 as the remote logging addresses, ensure to configure IPv4 and IPv6 in the Fabric Interconnect through the command-line interface (CLI).</p>
Minimum Severity To Report	<p>Select the lowest severity level to report in the remote log. The severity levels are:</p> <ul style="list-style-type: none"> <li>• 0 Emergency</li> <li>• 1 Alert</li> <li>• 2 Critical</li> <li>• 3 Error</li> <li>• 4 Warning</li> <li>• 5 Notice</li> <li>• 6 Informational</li> <li>• 7 Debug</li> </ul>

7. Click **Create**.

## Creating a Switch Control Policy

The Switch Control policy supports VLAN port count optimization, configuring MAC address aging time, and configuring Link Control Global settings.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **Switch Control**, and then click **Start**.
5. In the **General** page, configure the following parameters:

Property	Essential Information
Organization	Select the organization.
Name	Enter a name for your policy.

Property	Essential Information
Tag (optional)	Enter a tag in the key value format. For example, Org: IT or Site: APJ.
Description (optional)	Enter a short description.

6. On the Policy Details page, configure the following parameters:

Property	Essential Information
<b>Switching Mode</b>	
<b>Ethernet</b>	<p>Specify the Ethernet switching mode. The switching mode can be End Host or Switch.</p> <p>In End Host mode, the Fabric Interconnects appear to the upstream devices as end hosts with multiple links. In this mode, the switch does not run Spanning Tree Protocol and avoids loops by following a set of rules for traffic forwarding.</p> <p>In Switch mode, the switch runs Spanning Tree Protocol to avoid loops, and broadcast and multicast packets are handled in the conventional way.</p>
<b>FC</b>	<p>Specify the FC switching mode. The switching mode can be End Host or Switch.</p> <p>End-host mode allows the Fabric Interconnect to act as an end host to the connected Fibre Channel networks, representing all servers (hosts) connected to it through vHBAs. The end-host mode is achieved by pinning (dynamically pinned or hard pinned) vHBAs to Fibre Channel uplink ports, which makes the Fibre Channel ports appear as server ports (N-ports) to the rest of the fabric. When in end-host mode, the Fabric Interconnect avoids loops by ensuring that uplink ports do not receive traffic from one another.</p> <p>Switch mode is the traditional Fibre Channel switching mode. Switch mode allows the Fabric Interconnect to connect directly to a storage device. Enabling Fibre Channel switch mode is useful in POD models where there is no SAN (for example, a single Cisco UCS system connected directly to storage), or where a SAN exists (with an upstream MDS).</p>
<b>VLAN Port Count</b>	

Property	Essential Information
Enable VLAN Port Count Optimization	<p>Select to enable the VLAN port count optimization. This option is disabled by default.</p> <p><b>Note</b> PV Count with VLAN Port Count Optimization Enabled on Cisco UCS 6400 Series and 6500 Series FI in IMM is 108000.</p>
System Reserved VLANs	

Property	Essential Information
Reserved VLAN Start ID	

Property	Essential Information
	<p>Select this option to specify the Start ID of the reserved VLAN range. By default, the Start ID is 3915. VLAN ID with Start ID + 127 cannot be used in configuring VLAN or VSAN policy. For example, if the VLAN Start ID is changed to 3912, the Reserved VLAN range is 3912-4039. The Reserved VLAN range cannot be used for user-defined VLAN or VSAN policy.</p> <p><b>Note</b> Before you begin:</p> <ul style="list-style-type: none"> <li>• Remove any existing VLANs in the new reserved VLAN range.</li> <li>• Ensure that there are no VLANs or FCoE VLANs in the reserved VLAN block being used in the VLAN or VSAN policy. In other words, ensure that the VLAN and VSAN policies in both Fabric Interconnect A and B do not conflict with the reserved VLAN range.</li> <li>• If the Reserved VLAN Start ID is changed, VLANs in the old range which are not included in the new range will be available for VLAN and VSAN policies after the new switch control policy is deployed.</li> <li>• The default reserved VLAN range is 3916–4095. This system reserved VLAN range can be changed but note that VLANs 1002-1005 are blocked for internal use and cannot be used as part of system reserved range.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Fabric Interconnect reboots for the changes to take effect. Reboot occurs only once even if multiple changes are made.</li> <li>• On a device unclaim, the previously configured reserved VLAN will not be removed. On a subsequent claim, users will have to configure reserved VLAN via the Switch Control</li> </ul>



Property	Essential Information
	Policy if they intend to use a new range.
<b>Reserved VLAN End ID</b>	The End ID of the reserved VLAN range. The system blocks 128 reserved VLANs from the specified VLAN Start ID. By default, the End ID is 4042. This ID cannot be used in configuring VLAN policy.
<b>MAC Address Table Aging Time</b>	
<b>Default</b>	Select this option to set the default MAC address aging time to 14500 seconds for the End-Host mode.
<b>Custom</b>	Select this option to allow the user to configure the MAC address aging time on the switch.  For the switch model UCS-FI-6454 or higher versions, the valid time range is 120 to 918000 seconds. After the time range is defined by the user, the switch resets the defined time to its lower multiple of 5.
<b>Never</b>	Select this option to disable the MAC address aging process. This option ensures the MAC entries never expire and are not discarded from the MAC address table.
<b>Aging Time (Seconds)</b>	Define the MAC address aging time in seconds. This field is valid only when the <b>Custom</b> option is selected.
<b>Unidirectional Link Detection (UDLD) Global Settings</b>	
<b>Message Interval</b>	Define the UDLD probe message interval (time in seconds) on ports that are in advertisement mode and are bidirectional.  <b>Note</b> The valid message interval time ranges between 7 and 90 Seconds.
<b>Recovery Action</b>	Select <b>Reset</b> to recover an error-disabled port.  <b>Note</b> The option <b>None</b> is selected by default.
<b>Fabric port-channel vHBA</b>	

Property	Essential Information
<b>Enable the fabric port-channel vHBA reset</b>	<p>A virtual host bus adapter (vHBA) logically connects a virtual machine to a virtual interface on the fabric interconnect and allows the virtual machine to send and receive traffic through that interface. This is currently accomplished by using the fibre channel modes (End Host mode/Switch mode).</p> <p>The port channel operations involve addition or removal of a member link between Fabric Interconnect and I/O Module (IOM). Such operations may result in a long I/O pause or connection drop from virtual machines to its targets and require a vHBA reset support.</p> <p>With the <b>fabric port-channel vHBA reset</b> set to enabled, when the Cisco UCS IOM port-channel membership changes, the Fabric Interconnect sends a Registered State Change Notification (RSCN) packet to each vHBA configured via that Cisco UCS IOM. The RSCN enables the virtual interface card (VIC) or VIC Driver to reset the Fabric port-channel vHBA and to restore the connectivity.</p> <p>By default, the Fabric port-channel vHBA reset is set to disabled.</p> <p>When disabled (default), vHBA reset is done only when all the members of a fabric port-channel are down.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• The feature is supported on Cisco Intersight Infrastructure firmware version 4.1(3e) and above.</li> <li>• ESX NFNIC driver version 5.0.0.37 and later or 4.0.0.87 and later process this RSCN.</li> <li>• Linux FNIC driver version 2.0.0.85 and later process this RSCN.</li> </ul>

7. Click **Create**

**Note**

- On the Policy Details page, all the existing Switch Control policies show the value of Link Control Global Settings fields as blank. These policies display the correct values on policy edit/update.
- When you change the switching mode of a Fabric Interconnect, the Fabric Interconnect goes for a reboot.

## Creating a Flow Control Policy

Configure the Priority Flow Control for each port, to enable the no-drop behavior for the CoS defined by the System QoS Policy and an Ethernet QoS policy. In Auto and On priorities, the Receive and Send link level flow control will be Off.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **Flow Control**, and then click **Start**.
5. On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.
<b>Description (Optional)</b>	Provide a short description

6. On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Priority Flow Control Mode</b>	
<b>Auto</b>	Auto receives and sends the priority flow. This field is enabled by default.
<b>On</b>	Enables priority control flow on the local port.  <b>Note</b> You cannot enable <b>Send</b> and <b>Receive</b> direction at the same time.

Property	Essential Information
<b>Off</b>	Enables Link Level Flow Control on the local port.
	<b>Note</b> You can enable <b>Send</b> and <b>Receive</b> direction at the same time.
	<b>Send</b> When enabled, the link level flow control is configured in the send direction.
	<b>Receive</b> When enabled, the link level flow control is configured in the receive direction.



**Note** If Priority Flow Control is in **Auto/On** mode then the Flow Control cannot be enabled and the options are not listed. To enable Flow Control, you must set the Priority Flow Control in **Off** mode.



**Note** Flow Control should be enabled only on interfaces that are connected to Flow Control capable devices. The following interface types are supported:

- Ethernet uplink ports and port channels

7. Click **Create**.

## Creating a Link Aggregation Policy

This policy can be used to configure Link Aggregation properties.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **Link Aggregation**, and then click **Start**.

5. On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.
<b>Description (Optional)</b>	Provide a short description

6. On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Suspend Individual</b>	
<b>False</b>	Select <b>False</b> to continue to receive PDUs from the peer port.
<b>True</b>	Select <b>True</b> to suspend a port that is not receiving the PDUs from the peer port.
<b>LACP Rate</b>	
<b>Normal</b>	The port is expected to receive 1 PDU every 30 seconds. The timeout for this is 90 seconds.
<b>Fast</b>	The port is expected to receive 1 PDU every 1 second from the peer port. The time out for this is 3 seconds.



**Note** Link Aggregation should be enabled only on interfaces that are connected to link aggregation capable devices. The following interface types are supported:

- Ethernet uplink port channel
- FCoE uplink port channel

7. Click **Create**.

## Creating a Link Control Policy

This policy enables configuration of link control administrative state and configuration (normal or aggressive) mode for ports.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.

2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **Link Control**, and then click **Start**.
5. On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.
<b>Description (Optional)</b>	Provide a short description

6. On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Link Control Administrative State</b>	
The link control state of the port configured and managed by the administrator.	
<b>Link Control Mode</b>	
<b>Normal</b>	Detects unidirectional links caused by misconnected interfaces on fiber-optic connections.
<b>Aggressive</b>	<p>Detects unidirectional links caused by to one-way traffic on fiber-optic and twisted-pair links and by misconnected interfaces on fiber-optic links.</p> <ul style="list-style-type: none"> <li>• When <b>UDLD Administrative State</b> is disabled, the policy cannot be set to <b>Aggressive</b> mode</li> <li>• When configuring the <b>UDLD Mode</b> (normal or aggressive), ensure the same mode is configured on both sides of the unidirectional link.</li> </ul>



**Note** Link Control policy should be enabled only on interfaces that are connected to link control capable devices. The following interface types are supported:

- Ethernet uplink ports
- FCoE uplink ports
- Ethernet uplink port channels
- FCoE uplink port channels

7. Click **Create**.

## Creating a Multicast Policy

The multicast policy is used to configure Internet Group Management Protocol (IGMP) snooping and IGMP querier.



**Note** Ensure that each VLAN is associated with a multicast policy. You can edit the existing VLANs and associate them to a multicast policy.

1. Log in to Cisco Intersight with your Cisco ID and select admin role.
2. From the **Service Selector** drop-down list, select **Infrastructure Service**.
3. Navigate to **Configure > Policies**, and then click **Create Policy**.
4. Select **Multicast**, and then click **Start**.
5. On the **General** page, configure the following parameters:

Property	Essential Information
<b>Organization</b>	Select the Organization.
<b>Name</b>	Enter a name for your policy.
<b>Description (Optional)</b>	Provide a short description
<b>Add Tag (Optional)</b>	Enter a tag in the key:value format. For example, Org: IT or Site: APJ.

6. On the **Policy Details** page, configure the following parameters:

Property	Essential Information
<b>Snooping State</b>	<p>Determines whether IGMP snooping examines IGMP protocol messages within a VLAN to discover which interfaces are connected to hosts or other devices interested in receiving multicast traffic. This can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>—IGMP snooping is used for VLANs associated with this policy.</li> <li>• <b>Disabled</b>—IGMP snooping is not used for associated VLANs.</li> </ul>

Property	Essential Information
<b>Querier State</b>	<p>Determines whether IGMP snooping querier sends out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive IP multicast traffic. This can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>—Periodic IGMP queries are sent out.</li> <li>• <b>Disabled</b>—No IGMP queries are sent out. This is the default option.</li> </ul>
<b>Querier IP Address</b>	<p>The IPv4 address for the IGMP snooping querier interface.</p> <p>This field appears only when <b>Querier State</b> is enabled.</p>
<b>Querier IP Address Peer</b>	<p>(Optional) The IPv4 address for the peer IGMP snooping querier interface. The peer IP address is assigned to FI-B.</p> <p>This field appears only when <b>Querier State</b> is enabled.</p>

7. Click **Create**.