Configuring UCS Chassis Policies

Chassis Policies

Chassis policies in Cisco Intersight allow you to configure various parameters of the chassis, including IP pool configuration, VLAN settings, SNMP authentication, and SNMP trap settings. A chassis policy can be assigned to any number of chassis profiles to provide a configuration baseline for a chassis.

To view the Chassis Policies table view, from the **Service Selector** drop-down list, choose **Infrastructure Service**. Navigate to **Configure > Policies**.

The Chassis 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 Chassis Policies.

Chassis Policies can also be cloned by using the **Policy Clone** wizard with properties that are similar to the existing policies. The clone policy action is available on both the policies list and detailed views. For more information, see Cloning a Policy.

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

- **IMC Access Policy**—Enables you to configure and manage your network by mapping the IP pools to the chassis profile. This policy allows you to configure a VLAN and associate it with an IP address using the IP pool.

Note Only In-Band configuration is supported for Chassis IMC Access Policy.

- **SNMP Policy**—Configures the SNMP settings for sending fault and alert information by SNMP traps from the managed devices. 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. If you have not added any users or traps in the policy, the existing users or traps on the input/output module (IOM) are removed.

- **Power Policy**—Enables the management of power usage for the chassis. This policy allows you to configure the redundancy mode of the Chassis Power Supply Units (PSUs) and allocate power to the chassis. You can view the redundancy health, redundancy mode, input power health, and output power health of the chassis in the properties section of the **General** tab on the Chassis details view page. For Cisco UCS X9508 Chassis, you can configure Power Save Mode and Dynamic Power Reallocation.
- **Thermal Policy**—Allows the user to set the value of the Fan Control Mode for the chassis. The Fan Control Mode controls the speed of the chassis fan to maintain optimal server cooling.

Creating an IMC Access Policy

IMC Access policy allows to provide a VLAN ID and enables to associate it with an IP address from the selected IP pool.

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 **IMC Access**, 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.
Tag (optional)	Enter a tag in the key value format.
Description (optional)	Enter a short description.

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

Property	Essential Information
VLAN ID	Enter the VLAN ID to be used for server access over the inband network. The field value can be between 4 and 4093.
IPv4 address configuration	Select to determine the type of network for this policy. **Note** You can select only IPv4 address configuration or both IPv4 and IPv6 configurations.
IPv6 address Configuration	Select to determine the type of network for this policy. You can select only IPv6 address configuration or both IPv4 and IPv6 configurations. **Important** IPv6 is supported only on UCS-IOM-2408

Property	Essential Information	
IP Pool	**Select IP Pool**	Click to view and select the IP pool list on the right pane.

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. If you have not added any users or traps in the policy, the existing users or traps on the input/output module (IOM) are removed.

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
Organization	Select the organization.
Name	Enter a name for your policy.
Tag (optional)	Enter a tag in the key value format.
Description (optional)	Enter a short description.

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

Property	Essential Information
Enable SNMP	Displays the state of the SNMP Policy on the endpoint. Enable this option for the endpoint to send SNMP traps to the designated host.
Access Community String	Enter the SNMPv1, SNMPv2 community string or the SNMPv3 username. This field allows maximum of 18 characters. **Note** If the field is empty, it indicates that the SNMPv1 and SNMPv2c users are disabled.

Property	Essential Information
Trap Community String	Enter the SNMP community group name used for sending SNMP trap to other devices. **Note** This field is applicable only for SNMPv2c trap host or destination.
SNMP Users	
Name	Enter the SNMP username. This field must have a minimum of 1 and a maximum of 31 characters.
Security Level	Select the security mechanism for communication between the agent and the manager that include: • AuthPriv • AuthNoPriv
Auth Type	Select **SHA** as the authorization protocol for authenticating the user **Note** The **MD5** authorization protocol is not supported.
Auth Password	Enter the authorization password for the user.
Auth Password Confirmation	Enter the authorization password confirmation for the user.
Privacy Type	Select **AES** as the privacy protocol for the user.
Privacy Password	Enter the privacy password for the user.
Privacy Password Confirmation	Enter the privacy password confirmation for the user.
SNMP Trap Destinations	
Enable	Enable this option to allow and deploy the SNMP policy.
SNMP Version	Select **v2** or **v3** as the SNMP version for the trap.
User	Select the SNMP user for the trap. You can define maximum of 15 trap users. **Note** This field is applicable only to SNMPv3.

Property	Essential Information
Trap Type	Select the trap type to receive a notification when a trap is received at the destination: • Trap • Inform
Destination Address	Provide the address to which the SNMP trap information can be sent. You are allowed to define maximum of 15 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 Power Policy for Chassis

This policy enables configuration of power redundancy and power allocation for chassis.

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 **Power**, 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 Tags (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, navigate to **UCS Chassis** tab.
7. Configure the following parameters:

Property	Essential Information
Power Redundancy sets the redundancy mode of the chassis power supplies.	

Property	Essential Information
Grid	Grid mode requires two power sources. If one source fails, the surviving power supplies on the other source provides power to the chassis.
Not Redundant	Power Manager turns on the minimum number of PSUs required to support chassis power requirement. No redundant PSUs are maintained.
N+1	Power Manager turns on the minimum number of PSUs required to support chassis power requirements and one additional PSU for redundancy.
N+2	Power Manager turns on the minimum number of PSUs required to support chassis power requirements and two additional PSUs for redundancy. **Note** This mode is supported only for Cisco-UCSX-9508 chassis.
Power Save Mode	Enable to place additional PSU capacity in Power Save mode, when the requested power is less than the available power. **Note** This property is supported on: • Cisco-UCSX-9508 chassis with the minimum Cisco IMC firmware version of 4.2(1d). • Cisco-UCSB-5108 chassis with the minimum Cisco IMC firmware version of 4.3(2a).
Dynamic Power Rebalancing	Enable for dynamically reallocating power for the servers. When enabled, the power will be rebalanced across various chassis components including blades, Fans, IOMs/IFMs, and XFMs. **Note** This property is supported on: • Cisco-UCSX-9508 chassis with the minimum Cisco IMC firmware version of 4.2(1d). • Cisco-UCSB-5108 chassis with the minimum Cisco IMC firmware version of 4.3(2a).

Property	Essential Information
Extended Power Capacity	Sets the Extended Power Capacity of the Chassis. When this mode is enabled, power is borrowed from the redundant power supplies which increases the power available to the chassis. **Note** This property is supported only on Cisco-UCSX-9508 chassis with the minimum Cisco IMC firmware version of 4.2(1d).
Power Allocation (Watts)	Allows the user to set the maximum power a chassis can consume. The value can range from minimum of system requirement to maximum of available power. Deploying a policy with a Power Allocation of 0 will uncap the chassis budget, that is, the chassis will be able to consume all of the available power. **Note** This property is supported on: • Cisco-UCSX-9508 chassis with the minimum Cisco IMC firmware version of 4.2(1d). • Cisco-UCSB-5108 chassis with the minimum Cisco IMC firmware version of 4.3(2a).

8. Click **Create**.

Creating a Thermal Policy

This policy enables controlling the speed of the chassis fan.

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 **Thermal**, 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
Set Tags (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
Fan Control Mode controls the fan speed of the chassis.	
Balanced	The fans run faster when needed based on the heat generated by the server. When possible, the fans return to the minimum required speed.
Low Power	The fans run at slightly lower minimum speeds than the **Balanced** mode, to consume less power when possible.
High Power	The fans are kept at higher speed to emphasize performance over power consumption. **Note** This mode is supported only for UCS X-Series chassis.
Maximum Power	The fan are always kept at the maximum speed. This option provides the most cooling and consumes most power. **Note** This mode is supported only for UCS X-Series chassis.
Acoustic	The fan speed is reduced to reduce noise levels in acoustic-sensitive environments. **Note** This mode is supported only for UCS X-Series chassis.

7. Click **Create**.