

Use Cisco Catalyst 8000V as a Cloud Gateway for a fabric

- Information about Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 1
- Use cases for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 2
- Prerequisites for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 2
- Restrictions for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 2
- Configure Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 2

Information about Cisco Catalyst 8000V as a cloud gateway for a fabric

Table 1: Feature History

Feature Name	Release Information	Description
Cisco Catalyst 8000V as a cloud gateway for a fabric	SD-WAN Portal: 2023-05 Cisco Catalyst SD-WAN Control Components Release 20.6.1	This feature lets you configure a Cisco Catalyst 8000V device as the cloud gateway for connecting a virtual private cloud with a private data center.

The Cisco Catalyst 8000V serves as the cloud gateway for connecting a virtual private cloud (VPC) with a private data center.

You can configure a Cisco Catalyst 8000V device as a cloud gateway in these ways, depending on your requirements:

- Create a new fabric and add a Cisco Catalyst 8000V device as the cloud gateway for each region in the fabric.
- Add a Cisco Catalyst 8000V device to each region in an existing fabric.
- Replace Cisco vEdge Cloud in an existing fabric with a Cisco Catalyst 8000V device.

Use cases for Cisco Catalyst 8000V as a cloud gateway for a fabric

You can use Cisco Catalyst 8000V as a cloud gateway in these scenarios:

- Integrating your fabric with a TACACS or RADIUS server for AAA (authentication, authorization, and accounting) when the server resides in a private data center that you access through a VPN.
- Sending syslog information to a private data center that you access through a VPN.

Prerequisites for Cisco Catalyst 8000V as a cloud gateway for a fabric

Before deploying the 8000V as a gateway, confirm these requirements:

- You must have a Cisco SD-WAN Manager administrator username and password.
- You must have a Smart Account administrator username and password.
- You must know the serial number of the 8000V that you are adding to a fabric.

Restrictions for Cisco Catalyst 8000V as a cloud gateway for a fabric

You can use the 8000V as a cloud gateway only in Cisco SD-WAN Cloud-Pro environments.

Configure Cisco Catalyst 8000V as a cloud gateway for a fabric

Before you begin

Obtain the serial number of each 8000V device that you are configuring. Go to Cisco Software Central. In the **Smart Licensing** area, click **Manage Devices** under **Network Plug and Play**.

Configuration procedures

Use this table to find the steps for configuring an 8000V device as a cloud gateway in various scenarios. Choose the scenario that corresponds to your requirements. For each scenario, the table provides the general steps and links to more detailed information.

Scenario	General Steps	Reference
Create a new fabric and add an 8000V device as the cloud gateway for every region in the fabric.	**Step 1:** In the Cisco Catalyst SD-WAN Portal, create a new fabric.	See Create a Cisco Catalyst SD-WAN Cloud Hosted Fabric.
	Step 2: In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway.	See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal, on page 3.
Add an 8000V device to every region in an existing fabric.	In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway.	See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal, on page 3.
Replace Cisco vEdge Cloud with an 8000V device in an existing fabric.	**Step 1:** In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway.	See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal, on page 3.
	Step 2: You can open a support case to request that the existing vEdge Cloud be removed.	See Open a support case for a fabric update, on page 5.

Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal

1. Log in to the Cisco Catalyst SD-WAN Portal with administrator credentials.
2. Click the fabric for which you want to configure a cloud gateway.
3. From the **Actions** drop-down menu, choose **Add Cloud Gateways**.
4. Configure the fields listed in this table.

Note The Cisco Catalyst SD-WAN Portal does not save the usernames and passwords that you enter in these fields.

Field	Description
vManage Admin Credentials	
Username	Enter your Cisco SD-WAN Manager administrator username.
Password	Enter your Cisco SD-WAN Manager administrator password.
Smart Account Admin Credentials	
Username	Enter your Cisco Smart Account administrator username.
Password	Enter your Cisco Smart Account administrator password.

Field	Description
Cloud Gateway Serials	
Serial	The number of fields that appear equals the number of regions in your fabric. Enter the serial number of the Cisco 8000V in each **Serial** field to designate it as a cloud gateway for each region. Ensure that each serial number you enter is unique.
Custom IPs	
System IPs	The number of **System IPs** fields equals the number of regions in your fabric. Optionally, enter an IP address in each field to configure a system interface for the cloud gateway that you are adding. A system interface IP address is persistent and identifies the device. It works like a router ID, which identifies the router from which packets originate. Specify a system IP address using decimal four-part dotted notation as an IPv4 address. Enter only the address because the prefix length (/32) is implicit. Select any IPv4 address except for 0.0.0.0/8, 127.0.0.0/8, and 224.0.0.0/4, or 240.0.0.0/4 and later. If you do not specify a system IP address, the Cisco Catalyst SD-WAN Portal assigns a random IP address. This address might duplicate the IP address of another device. Ensure that the IP address you enter is unused in the existing fabric. This prevents conflicts when provisioning the cloud gateway.

Field	Description
Enable Webhook via Cloud Gateway	This option applies only when Amazon Web Services (AWS) is the cloud provider for a dedicated fabric. To route webhook messages from Cisco SD-WAN Manager through a cloud gateway, select this option. Enabling this option is useful when your webhook server is hosted in your private network and no internet traffic is forwarded to this server. When this option is enabled, a connection is provisioned between your SD-WAN fabric and your private network. Once you enable this option, add a routing table entry on the server to forward network traffic to the webhook server through the cloud gateway. Refer to the email that you receive after the cloud gateway is provisioned for instructions.

5. Click **Submit**.

Open a support case for a fabric update

To open a support case for a fabric update, go to Cisco Support Case Manager, log in with your Cisco credentials, and click **Open New Case**.