

Deploy Cisco Catalyst 8000V Edge Software on Alibaba Cloud

This section provides information helpful when using the Alibaba Cloud instance with Cisco SD-WAN. For detailed information about the Cisco Catalyst 8000V Edge Software deployment process, see the deployment guide for Alibaba Cloud.

Features

The following Cisco Catalyst 8000V features are not supported in an Alibaba Cloud deployment when operating as part of Cisco SD-WAN:

Table 22: Unsupported Features

Feature	Additional Information
Deployment and Licensing	
Cisco SD-WAN Cloud onRamp integration	Connect the Cisco Catalyst 8000V to Cisco SD-WAN by creating a bootstrap file, as described in Create a Bootstrap File for a Cisco Catalyst 8000V Instance Using Cisco vManage , on page 180. Deployment by Cloud onRamp is not supported.
Pay as you go (PAYG) licensing	None

Requirements for the Cisco Catalyst 8000V Instance

The Cisco Catalyst 8000V instance deployed in Alibaba Cloud must meet the following requirements to work with Cisco SD-WAN:

- Alibaba Cloud Elastic Compute Service (ECS) instance type: G5ne
- vCPU: 2
- RAM: 8 GB

The following image options are supported by Cisco SD-WAN:

- ecs.g5ne.large: 2 vCPU and 8 GB RAM
- ecs.g5ne.xlarge: 4 vCPU and 16 GB RAM
- ecs.g5ne.2xlarge: 8 vCPU and 32 GB RAM

Configure the Cisco Catalyst 8000V Instance to Connect to Cisco SD-WAN

When you create a Cisco SD-WAN instance on Alibaba Cloud, create a Day 0 bootstrap file using Cisco vManage and use this bootstrap file on the Cisco Catalyst 8000V instance to onboard the instance to Cisco SD-WAN. When the instance starts up using the bootstrap file, it connects to the Cisco vBond Orchestrator and Cisco vManage controller.

Create a Bootstrap File for a Cisco Catalyst 8000V Instance Using Cisco vManage

1. For instructions on creating a bootstrap file for a cloud-hosted device, using Cisco vManage, see Bootstrap Process for Cisco SD-WAN Cloud-Hosted Devices.
2. In the Alibaba Cloud portal, create an instance of the Cisco Catalyst 8000V. When configuring the instance, use the bootstrap configuration that you created in Cisco vManage.

Deploy the vEdge Cloud routers

vEdge routers, as their name implies, are edge routers that are located at the perimeters of the sites in your overlay network, such as remote office, branches, campuses, and data centers. They route the data traffic to and from their site, across the overlay network.

vEdge routers are either physical hardware routers or software vEdge Cloud router, which run as virtual machines on a hypervisor or an AWS server.

An overlay network can consist of a few or a large number of vEdge routers. A single Cisco vManage, which provides management and configuration services to the vEdge routers, can support up to about 2,000 routers, and a vManage cluster can support up to about 6,000 routers.

To deploy vEdge Cloud routers:

1. For software vEdge Cloud routers, create a VM instance, either on an AWS server, or on an ESXi or a KVM hypervisor.
2. For software vEdge Cloud router, install a signed certificate on the router. In Releases 17.1 and later, Cisco vManage can act as a Certificate Authority (CA) and can automatically generate and installed signed certificates on vEdge Cloud router. In earlier releases, send a certificate signing request to Symantec and then install that certificate on the router so that the router can be authenticated on and can participate in the overlay network.
3. From Cisco vManage, send the serial numbers of all vEdge Cloud routers to Cisco vSmart Controllers and Cisco vBond Orchestrators in the overlay network.
4. Create a full configuration for the vEdge Cloud router. You do this by creating a vManage template for Cisco vBond Orchestrator and attaching that template to the orchestrator. When you attach the vManage template, the initial minimal configuration is overwritten.
5. Prepare hardware vEdge Cloud router for automatic provisioning , which is done using the Cisco SD-WAN zero-touch provisioning (ZTP) tool. The ZTP process allows hardware routers to join the overlay network automatically.

Starting with Release 18.2.0, vEdge Cloud routers that are hosted in countries affected by United States government embargoes cannot connect to overlay network controllers (Cisco vBond Orchestrators, Cisco vManages, and Cisco vSmart Controllers) that are hosted in the Cisco cloud. Any vEdge Cloud router from an embargoed country that attempts to connect to one of these controllers will be disabled. (The vEdge Cloud routers can, however, connect to controllers that are hosted in other clouds). As a result, when a vEdge Cloud router initially attempts to connect to a controller in the Cisco cloud, the router might not come up and might remain in a pending state if the Cisco vBond Orchestrator and the Cisco vManage are unable to communicate with each other or if the Cisco cloud server is down.