

Frequently Asked Questions

- Frequently Asked Questions, on page 1
- How to, on page 2
- Troubleshooting, on page 2

Frequently Asked Questions

What types of Cisco Catalyst SD-WAN deployments are supported on the Cisco Catalyst SD-WAN Portal?

You can deploy the following types of Cisco Catalyst SD-WAN on the Cisco Catalyst SD-WAN Portal:

- Cisco SD-WAN Cloud
- Cisco SD-WAN Cloud-Pro

See more details in Types of Fabric Network in Cisco Catalyst SD-WAN.

What cloud providers are supported to provision SD-WAN control components in the Cisco Catalyst SD-WAN Portal?

The supported cloud providers for provisioning SD-WAN Control Components in the Cisco Catalyst SD-WAN Portal are Amazon Web Services (AWS) and Microsoft Azure.

What is the role of a Virtual Account in Cisco Catalyst SD-WAN Portal controller provisioning?

The Cisco Catalyst SD-WAN Portal uses SD-WAN subscriptions linked to a Virtual Account to determine which cloud SD-WAN Control Component entitlements are available and to facilitate SD-WAN Control Component provisioning. This information shows whether your Virtual Account supports SD-WAN. Provide a Virtual Account when you order an SD-WAN license to ensure successful provisioning through the Catalyst SD-WAN Portal.

How to

How do I access the Cisco Catalyst SD-WAN Portal?

Use the instructions in Access the Cisco Catalyst SD-WAN Portal for the First Time to access the Cisco Catalyst SD-WAN Portal.

If you want to use an identity provider (IdP) to access the portal, refer to Configure an IdP for the Cisco Catalyst SD-WAN Portal.

How do I configure role-based access in the Cisco Catalyst SD-WAN Portal?

The role-based access control feature in the Cisco Catalyst SD-WAN Portal allows users to be assigned specific roles (Monitor, Overlay Management, or Administration) within designated virtual accounts. This process ensures granular visibility and streamlines provisioning and monitoring of new overlays. To configure role-based access, refer to the instructions provided in Manage role-based access.

How do I set up multifactor authentication (MFA)?

The Cisco Catalyst SD-WAN Portal supports MFA by default, and it is mandatory for users. These one-time password generation options are available:

- Google Authenticator
- Email Authenticator
- Fingerprint sensor on supported computers (such as Apple MacBook)

For more information, refer to Configure Additional MFA Options or Update an Existing MFA Option.

How do I move SD-WAN Control Component SKUs from one Virtual Account to another Virtual Account?

To reassign an order containing SD-WAN Control Component SKUs to a different Virtual Account, open a support case as described in Troubleshooting, on page 2.

How do I add IP addresses to an allow list for managing fabric access through the Cisco Catalyst SD-WAN Portal?

To add IP addresses to an allow list through the Cisco Catalyst SD-WAN Portal, refer to the instructions in Specify the Allowed List of IP Addresses for Managing Controller Access.

Troubleshooting

How do I get support for Cisco Catalyst SD-WAN Portal?

Follow these steps to open a Cisco support case for Catalyst SD-WAN Portal.

1. Go to https://mycase.cloudapps.cisco.com/case.
2. Select **Open New Case** > **Products & Services** > **Open Case**.

3. Enter the appropriate entitlement information. You typically need to include the serial number of a WAN edge device.
4. Click **Next**.
5. Enter your case details.
6. Select **Technology** and search for the appropriate Sub Tech keyword. For Cisco Catalyst SD-WAN Portal issues, select these keywords:
    - Technology: SDWAN - Cisco-Hosted
    - SubTechnology: SDWAN Cloud Infra