Frequently Asked Questions

Frequently Asked Questions

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

Currently, the Cisco Catalyst SD-WAN Portal supports these deployments:

- Cisco Cloud-delivered Catalyst SD-WAN
- Cisco hosted Catalyst SD-WAN

For more information, refer to 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 AWS and Azure.

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

The Cisco Catalyst SD-WAN Portal relies on SD-WAN subscriptions associated to a Virtual Account to determine the cloud SD-WAN Control Component entitlements and facilitate SD-WAN Control Component provisioning. This information indicates whether the Virtual Account is SD-WAN capable. Providing a Virtual Account at the time of SD-WAN license ordering is critical to successful provisioning via the Catalyst SD-WAN Portal.

How to

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

Access the Cisco Catalyst SD-WAN Portal by following the instructions in Access the Cisco Catalyst SD-WAN Portal for the First Time.

If you want to use an identity provider (IdP) to access the portal, follow the instructions in 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, ensuring granular visibility and streamlined provisioning and monitoring of new overlays. To configure role-based access, follow the instructions provided in Manage role-based access.

How do I set up multi-factor 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. [link]

How do I whitelist IP addresses for managing fabric access through the Cisco Catalyst SD-WAN Portal?

In order to whitelist IP addresses through Cisco Catalyst SD-WAN Portal, follow the information provided 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