Troubleshooting

Update an Expired IdP Certificate

To update an expired identity provider (IdP) certificate, use the **Need help signing in** link at the bottom of the Cisco Catalyst SD-WAN Portal **Sign In** window.

1. Navigate to the Cisco Catalyst SD-WAN Portal URL.

2. Click the **Need help signing in** link.

3. Click the **Need to reset IDP** link.

   You are redirected to your Cisco account.

4. Enter your Cisco login credentials.

5. When prompted, set up or enter your MFA credentials.

Reset a Misconfigured IdP

If your IdP is misconfigured, and you are not able to log in, you can configure a new IdP.

1. Navigate to the Cisco Catalyst SD-WAN Portal URL.

2. Click the **Need help signing in** link.

3. Click the **Need to reset IDP** link.

   You are redirected to your Cisco account.

4. Enter your Cisco login credentials.

5. When prompted, set up or enter your MFA credentials.

Delete an IdP

1. Navigate to the Cisco Catalyst SD-WAN Portal URL.

2. Click the **Need help signing in** link.

3. Click the **Need to reset IDP** link.

4. You are redirected to your Cisco account.

5. Enter your Cisco login credentials.

6. When prompted, set up or enter your MFA credentials.

7. Go to IdP details, actions and delete the IDP.

Only the IdP admin can delete the IdP from Cisco Catalyst SD-WAN Portal. If the IdP admin is no longer active, open a TAC case.

Troubleshoot Smart Account Issues

Problem

A Smart Account is not visible in the **Smart Account** drop-down list after logging in to the Cisco Catalyst SD-WAN Portal.

This usually happens when there is no SD-WAN-capable attribute associated with the Smart Account.

Solution

Associate your Cisco DNA subscription with your Smart Account and Virtual Account.

For more information, see Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers.

Contact Cisco Catalyst SD-WAN Technical Support to associate the Smart Account with your Cisco DNA cloud subscription.

Troubleshoot Virtual Account Issues

Problem

The Cisco Catalyst SD-WAN Portal displays an error that the Virtual Account is not SD-WAN capable.

This error indicates that a Cisco DNA subscription is not associated with the Virtual Account.

Solution

For customers with an enterprise agreement, automatic association of Virtual Accounts to an SD-WAN-capable attribute is not available.

To associate a Virtual Account with your Cisco DNA subscription as an enterprise customer, do the following:

1. Submit a cloud-controller provisioning request form through the Enterprise Agreement Workspace for the CloudOps team to provision the controllers.

2. Contact Cisco Catalyst SD-WAN Technical Support to request that the desired Virtual Account become available on the Cisco Catalyst SD-WAN Portal.

3. After the desired Virtual Account is available on the Cisco Catalyst SD-WAN Portal, you can provision the controllers after providing the necessary enterprise agreement contract information.

For more information, see Smart Account and Virtual Accounts.

For more information, see Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers.

If you are unable to associate your Virtual Account with your Cisco DNA subscription, contact Cisco Catalyst SD-WAN Technical Support to associate the Virtual Account with your Cisco DNA cloud subscription.

Troubleshoot Browser Security Issues

Problem

You receive the following error:

```
CSRF Failed: CSRF token missing or incorrect
```

A cross-site request forgery (CSRF) token mismatch is an error whereby the browser is not able to create a secure cookie, or the browser is not able to access the cookie for you to log in.

Solution

This error occurs due to certain security settings on your web browser.

Clear the cache on your browser or try another browser.