Configure Single Sign-On

Table 1: Feature History

Feature Name	Release Information	Description
Single Sign-On Using Microsoft Entra ID	Cisco vManage Release 20.8.1	This feature adds support for Microsoft Entra ID as an external identity provider (IdP) for single sign-on of Cisco SD-WAN Manager users. You can configure Microsoft Entra ID as an external IdP using Cisco SD-WAN Manager and the Microsoft Entra ID administration portal. **Note** The solution formerly known as Azure Active Directory (Azure AD) is now called Microsoft Entra ID.
Configure Multiple IdPs for Single Sign-On Users of Cisco SD-WAN Manager	Cisco vManage Release 20.10.1	With this feature, you can configure up to three IdPs for providing different levels of access for single sign-on users of Cisco SD-WAN Manager.

Information About Single Sign-On

This chapter describes how to configure single sign-on (SSO) for Cisco Catalyst SD-WAN.

Cisco Catalyst SD-WAN is generally compatible with SAML 2.0-compliant identity providers (IdPs), when configured according to industry standards. Cisco has tested and verified the following IdPs:

- Okta

- Active Directory Federation Services (ADFS)
- PingID
- Microsoft Entra ID

Note Because Cisco SD-WAN Manager supports the SAML2.0 standard, if you deploy an IdP other than those listed above and it does not work with Cisco SD-WAN Manager as expected, we recommend that you follow up with the IdP provider to troubleshoot the issue.

Note For Cisco vManage Release 20.3.x through Cisco vManage Release 20.11.x, and for Cisco Catalyst SD-WAN Manager Release 20.12.1 and later, use IdP SAML metadata with 2048-bit key signature certificate for SSO authentication because metadata with 1024-bit key signature certificate is not supported.

SSO enables secured access to multiple applications or websites with a single set of credentials. SSO requires the following components:

- Identity provider IdP: This system stores user data, maintains and supports the authentication mechanism, for example, Okta, ADFS, PingID, and Microsoft Entra ID.
- Service provider: This system hosts the website or application of interest, for example, Cisco SD-WAN Manager.
- Users: People with a registered account with the IdP and the service provider.

To integrate IdPs with service providers, the SSO uses security assertion mark-up language (SAML). SAML is an XML-based communication standard that allows you to share identities among multiple organizations and applications.

The following steps describe the intergration of IdPs with service providers:

1. Whenever a network administrator tries to log in to a service provider using an IdP, the service provider first sends an encrypted message to the IdP.
2. The IdP decrypts the message and validates the credentials of the network administrator by comparing the information with the IdP's database.
3. After the validation, the IdP sends an encrypted message to the service provider. The service provider decrypts the message from the IdP, and the administrator is allowed to access the service provider.
4. In general, IdP and service provider exchange information based on predefined standards. This standard is a set of certificates called SAML.

After completing the above process, the administrator is redirected to the IdP portal. The administrator must enter IdP credentials to log in to Cisco SD-WAN Manager.

Note The privileges for a particular administrator are provided based on the information available about that administrator in the IdP's database.

The Simple Object Access Protocol (SOAP) is not supported for Single Sign-On (SSO) in Cisco SD-WAN Manager. Instead, Cisco SD-WAN Manager supports only the POST method for SSO.

Benefits of Single Sign-On

With a properly deployed SSO solution, you can do the following:

- Eliminate weak passwords for each cloud application
- Streamline the secured access process
- Provide one-click access to cloud applications

Prerequisites for Single Sign-On

- In Cisco SD-WAN Manager, ensure that the identity provider settings (**Administration Settings** > **Identity Provider Settings**) are set to **Enabled**.

  For more information on enabling identiy provider, see Enable an Identity Provider in Cisco SD-WAN Manager.
- Availability of SAML metadata files for configuring IdP and service provider.
- Cisco SD-WAN Manager requires access to an internet connection that doesn't have a firewall restriction for Cisco SD-WAN Manager to reach the SSO.

Configure Single Sign-On Using Okta

Okta provides a secure identity management service that lets you connect any person with any application on any device using single sign-on (SSO).

Note The procedure for configuring SSO using Okta is same for tenant environments and providers.

Note Beginning with Cisco vManage Release 20.3.1, Cisco SD-WAN Manager no longer supports MD5 or SHA-1. All x.509 certificates handled by Cisco SD-WAN Manager need to use at least SHA-256 or a higher encryption algorithm.

Perform the following procedures to configure SSO.

Enable an Identity Provider in Cisco SD-WAN Manager

To configure Okta SSO, use Cisco SD-WAN Manager to enable an identity provider and generate a Security Assertion Markup Language (SAML) metadata file.

From Cisco vManage Release 20.10.1, you can use **Add New IDP Settings** to configure up to three IdPs. For more information on integrating with multiple IdPs, see the chapter Configure Multiple IdPs.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Identity Provider Settings**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.)
3. For Cisco IOS XE Catalyst SD-WAN Release 17.18.x and earlier releases:
   a. Click **Enabled**.
   b. Click **Click here to download the SAML metadata** and save the contents in a text file. This data is used for configuring Okta.
   c. From the metadata that is displayed, make a note of the following information that you need for configuring Okta with Cisco SD-WAN Manager:
      - **Entity ID**
      - **Signing certificate**
      - **Encryption certificate**
      - **Logout URL**
      - **Login URL**

Note Administrators can set up SSO using a single **Entity ID** only. Cisco SD-WAN Manager doesn't support more than one **Entity ID** while setting up SSO.

   d. In the **Upload Identity Provider Metadata** section, click **Select a File** to upload the IdP metadata file.
4. Click **Save**.

Configure SSO on the Okta Website

Note This procedure involves a third-party website. The details are subject to change.

To configure SSO on the Okta website:

1. Log in to the Okta website.

Note Each IdP application gets a customized URL from Okta for logging in to the Okta website.

2. Create a username using your email address.

3. To add Cisco SD-WAN Manager as an SSO application, from the Cisco SD-WAN Manager menu, click **Admin**.
4. Check the upper-left corner to ensure that it shows the **Classic UI** view on Okta.
5. If it shows **Developer Console**, click the down triangle to choose the **Classic UI**.
6. Click **Add Application** under **Shortcuts** to the right to go to the next window, and then click **Create New Application** on the pop-up window.
7. Choose **Web** for the platform, and choose **SAML 2.0** as the **Sign on Method**.
8. Click **Create**.
9. Enter a string as **Application name**.
10. (Optional): Upload a logo, and then click **Next**.
11. On the **SAML Settings for Single sign on URL** section, set the value to the **samlLoginResponse URL** from the downloaded metadata from Cisco SD-WAN Manager.
12. Check the **Use this for Recipient URL and Destination URL** check box.
13. Copy the **entityID** string and paste it in the **Audience URI (SP Entity ID)** field.

    The value can be an IP address or the name of the Cisco SD-WAN Manager site.
14. For **Default RelayState**, leave empty.
15. For **Name ID format**, choose **EmailAddress**.
16. For **Application username**, choose **Okta username**.
17. For **Show Advanced Settings**, enter the fields as indicated below.

Table 2: Fields for Show Advanced Settings

Component	Value	Configuration
Response	Signed	Not applicable
Assertion Signature	Signed	Not applicable
Signature Algorithm	RSA-SHA256	Not applicable
Digest Algorithm	SHA256	Not applicable
Assertion Encryption	Encrypted	Not applicable
Encryption Algorithm	AES256-CBC	Not applicable
Key Transport Algorithm	RSA-OAEP	Not applicable

Component	Value	Configuration
Encryption Certificate	Not applicable	**a.** Copy the encryption certificate from the metadata you downloaded. **b.** Go to www.samltool.com and click **X.509 CERTS**, paste there. Click **Format X.509 Certificate**. **c.** Ensure to remove the last empty line and then save the output (**X.509.cert with header**) into a text file **encryption.cer**. **d.** Upload the file. Mozilla Firefox may not allow you to do the upload. Instead, you can use Google Chrome. You should see the certificate information after uploading to Okta.
Enable Single Logout		Ensure that this is checked.
Single Logout URL		Get from the metadata.
Service provider Issuer		Use the entityID from the metadata.
Signature Certificate		**a.** Obtain from the metadata. Format the signature certificate using www.samltool.com as described. **b.** Save to a file, for example, **signing.cer** and upload.
Authentication context class	X.509 Certificate	Not applicable
Honor Force Authentication	Yes	Not applicable
SAML issuer ID string	SAML issuer ID string	Not applicable
Attribute Statements	Field: **Name**	Value: *Username*
	Field: **Name format (optional)**	Value: Unspecified
	Field: **Value**	Value: *user.login*

Component	Value	Configuration
Group Attribute Statements	Field: **Name**	Value: Groups
	Field: **Name format (optional)**	Value: Unspecified
	Field: **Matches regex**	Value: **.*** **Note** Matches regex with value * matches all user groups in Okta which may cause SSO slowness and that value "netadmin|operator|basic" is preferred to limit the number of unrelated user groups. You can add the custom groups to the regex with an OR operator. For example, netadmin|operator|basic|<custom>.

Note It is mandatory to use the two strings, Username and Groups, exactly as shown above. Otherwise, you may be logged in with the default group of Basic.

18. Click **Next**.
19. For **Application Type**, check **This is an internal app that we have created** (optional).
20. Click **Finish**. This brings you to the Okta application window.
21. Click **View Setup Instructions**.
22. Copy the IdP metadata.
23. In Cisco SD-WAN Manager, navigate to **Identity Provider Settings** > **Upload Identity Provider Metadata**, paste the IdP metadata, and click **Save**.
24. In addition to copy-and-pasting the contents of a file with IdP metadata, you can also upload a file directly using the **Select a file** option.

Assign Users to the Application on the Okta Website

Note This procedure involves a third-party website. The details are subject to change.

To assign users to the application on the Okta website:

1. On the Okta application window, navigate to **Assignments** > **People** > **Assign**.
2. Choose **Assign to people** from the drop-down menu.
3. Click **Assign** next to the user(s) you chose and click **Done**.
4. To add a user, click **Directory** > **Add Person**.

5. Click **Save**.

Configure SSO for Active Directory Federation Services (ADFS)

This section describes how to use Cisco SD-WAN Manager and ADFS to configure SSO.

The configuration of Cisco SD-WAN Manager to use ADFS as an IdP involves two steps:

- Step 1 - Import ADFS metadata to Cisco SD-WAN Manager.
- Step 2- Export Cisco SD-WAN Manager metadata to ADFS.

Step 2 can be further divided into:

- Edit and then import Cisco SD-WAN Manager metadata to ADFS.
- Set up ADFS manually using the information from the Cisco SD-WAN Manager metadata.

Note There is no support for customized certificates for Cisco SD-WAN Manager SSO. If ADFS is configured, the signature and signing certificates are generated from the Cisco SD-WAN Manager metadata.

For more information on configuring ADFS, see Enable an Identity Provider in Cisco SD-WAN Manager. The steps are the same as for configuring Okta as an IdP.

Import Metadata File into ADFS

Note This procedure involves a third-party website. The details are subject to change.

Step 1 - Import ADFS Metadata to Cisco SD-WAN Manager:

1. Download the ADFS metadata file, typically from the ADFS URL: `https://<your ADFS FQDN or IP>/FederationMetadata/2007-06/FederationMetadata.xml`.
2. Save the file as **adfs_metadata.txt**.
3. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Identity Provider Settings** > **Enable**, and then upload **adfs_metadata.txt** to Cisco SD-WAN Manager.

Step 2 - Export Cisco SD-WAN Manager Metadata to ADFS:

4. With **Identity Provider Settings** enabled, **Click here to download SAML metadata** and save the contents to a file, which is typically `192.168.1.15_saml_metadata.xml`.
5. After the SAML metadata is downloaded, verify that the signing certificate and the signature certificate are the same.
   a. If the signing certificate and the signature certificate are the same, proceed to Step 6 to edit the Cisco SD-WAN Manager metadata file.

b. If the signing certificate and the signature certificate are not the same, use the signature certificate for the remaining steps, not the signing certificate.

6. Edit the Cisco SD-WAN Manager metadata file by deleting everything from **<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"**> to **</ds:Signature**>.
7. Edit the Cisco SD-WAN Manager metadata file by deleting everything from **<md:KeyDescriptor use="encryption"**> to **</md:KeyDescriptor**>.
8. Import the new modified Cisco SD-WAN Manager metadata file into ADFS, and enter the **entityID** as **Display Name**.
9. Click **Next** until the end.
10. Open **Edit Claim Rule**, and add the following four new custom rules in the exact sequence:

```
@RuleName = "sAMAccountName as Username" c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"]=> issue(store = "Active Directory", types
= ("Username"), query = ";sAMAccountName;{0}", param = c.Value);
```

```
@RuleName = "sAMAccountName as NameID" c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types
=
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"),
query = ";sAMAccountName;{0}", param = c.Value);
```

```
@RuleName = "Get User Groups and save in temp/variable" c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types =
("http://temp/variable1"), query = ";tokenGroups;{0}", param =
c.Value);
```

```
@RuleName = "Parse temp/variable1 and Send Groups Membership" c:[Type
== "http://temp/variable1", Value =~ "(?i)^SSO-"] => issue(Type =
"Groups", Value = RegExReplace(c.Value, "SSO-", ""));
```

11. Verify the final result.
12. In the **Active Directory**, create the following two security groups: **`SSO-Netadmin`** and **`SSO-Operator`**.

Note If you are using different naming convention for the two security groups, then you have to modify the regular expression value **`"(?i)^SSO-"`** in the step above.

Any active directory users who are not members of the two groups will only have **Basic** access to Cisco SD-WAN Manager.

Add ADFS Relying Party Trust

Before you begin

To add an ADFS relying party trust using Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Identity Provider Settings** > **Enable**.
2. Download the ADFS Metadata file, and upload it into Cisco SD-WAN Manager. An example of a URL, `https://<your ADFS FQDN or IP>/FederationMetadata/2007-06/FederationMetadata.xml`.
3. **Click here to download SAML metadata**, and save the contents to a file. An example of a saved file, **192.168.1.15_saml_metadata.xml**.
4. Open the file with an XML editor, and check that the following information is available:
   - **Entity ID**
   - **Signing certificate**
   - **Login URL**
   - **Logout URL**
5. Navigate to `https://www.samltool.com/format_x509cert.php`.
6. For **Signing certificate**, copy Signing certificate from "metadata" [everything between <ds:X509Certificate> and </ds:X509Certificate>].
7. Navigate to the **www.samltool.com** page, click **X.509 CERTS > Format X.509 Certificate**, and paste the copied content.
8. Save the output ("X.509 cert with header") into a text file "Signing.cer". Remember to remove the last empty line.

Add ADFS Relying Party Trust Manually

Note This procedure involves a third-party website. The details are subject to change.

To add ADFS relying party trust manually:

1. Launch **AD FS 2.0 Management**.
2. Navigate to **Trust Relationships > Relying Party Trusts**.
3. Click **Action > Add Relying Party Trust**.
4. Click **Start**.
5. Choose **Enter data about the relying party manually**, and click **Next**.
6. Choose **Display name** and **Notes**, and then click **Next**.

7. Choose **AD FS 2.0 profile**, and click **Next**.
8. Click **Next** to skip **Configure Certificate** page.
9. Click **Enable support for the SAML 2.0 Webs So protocol**.
10. Open a text editor, and open the **10.10.10.15_saml_metadata.xml** file.
11. Copy the vale of the **Location** attribute for **AssertionConsumerService**, and paste it into the **Relying party SAML 2.0 SSO service URL** text box.
12. Click **Next**.
13. Copy the value of the **entityID** attribute, and paste it into the **Relying party trust identifiers** text box.
14. Click **Add**, and click **Next**.
15. Click **Next** to skip to the **Configure Multi-factor Authentication Now** section.
16. Choose **Permit all users to access this relying party**, and click **Next**.
17. Click **Next** to skip to the **Ready to Add Trust** section.
18. Click **Close**.
19. Open **Edit Claim Rules** window, and add the following four new custom rules in this order:
    - `@RuleName = "sAMAccountName as Username" c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]=> issue(store = "Active Directory", types = ("Username"), query = ";sAMAccountName;{0}", param = c.Value);`
    - `@RuleName = "sAMAccountName as NameID" c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"), query = ";sAMAccountName;{0}", param = c.Value);`
    - `@RuleName = "Get User Groups and save in temp/variable" c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("http://temp/variable1"), query = ";tokenGroups;{0}", param = c.Value);`
    - `@RuleName = "Parse temp/variable1 and Send Groups Membership" c:[Type == "http://temp/variable1", Value =~ "(?i)^SSO-"]=> issue(Type = "Groups", Value = RegExReplace(c.Value, "SSO-", ""));`
20. Open the **Edit Claim Rules** window, and verify that the rules display in **Assurance Transform Rules**.
21. Click **Finish**.
22. Open the **Properties** window of the newly created **Relying Party Trust**, and click **Signature**.
23. Click **Add**, and add the **Signing.cer** created in Step 6.
24. In the **Active Directory**, click **General**, and enter the following two security groups in the **Group name** text box:

    SSO-Netadmin

SSO-Operator

Note If you use a different naming convention for the two security groups, then you have to modify the **Regular** expression value for `(?i)^SSO-` mentioned in Step 19.

Note Any active directory user who is NOT a member of these two groups, will only have **Basic** access to Cisco SD-WAN Manager.

Configure SSO for PingID

Cisco SD-WAN Manager supports PingID as an IdP. PingID is an identity management service for authenticating user identities with applications for SSO.

The configuration of Cisco SD-WAN Manager to use PingID as an IdP involves the following steps:

- Import (upload) IdP metadata from PingID to Cisco SD-WAN Manager.
- Download the Cisco SD-WAN Manager SAML metadata file to export to PingID.

Prerequisites:

1. In Cisco SD-WAN Manager, ensure that identity provider settings (**Administration Settings** > **Identity Provider Settings**) are set to **Enabled**.
2. Download the Cisco SD-WAN Manager SAML metadata file to export to PingID.

   For more information on these procedures, see Enable an Identity Provider in Cisco SD-WAN Manager. The steps are the same as for configuring Okta as an IdP.

Perform the following steps for configuring PingID.

Configure SSO on the PingID Administration Portal

Note This procedure involves a third-party website. The details are subject to change.

To configure PingID:

1. Log in to the PingID administration portal.
2. Create a username using your email address.
3. Click the **Applications**.
4. Click **Add Application** and choose **New SAML Application**.

   In the **Application Details** section, **Application Name**, **Application Description**, and **Category** are all required fields.

For logos and icons, PNG is the only accepted graphics format.

5. Click **Continue to Next Step**.

   The **Application Configuration** section appears.

6. Make sure that you choose **I have the SAML configuration**.

7. Under the **You will need to download this SAML metadata to configure the application** section, configure the following fields:

   a. For **Signing Certificate**, use the drop-down menu, **PingOne Account Origination Certificate**.

   b. Click **Download** next to **SAML Metadata** to save the PingOne IdP metadata into a file.

   c. Later, you need to import the PingOne IdP metadata file into Cisco SD-WAN Manager to complete the SSO configuration.

      1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

      2. Click **Identity Provider Settings** > **Upload Identity Provider Metadata** to import the saved PingOne IdP metadata file into Cisco SD-WAN Manager.

      3. Click **Save**.

8. Under the **Provide SAML details about the application you are connecting to** section, configure the following fields:

   a. For **Protocol Version**, click **SAMLv2.0**.

   b. On **Upload Metadata**, click **Select File** to upload the saved Cisco SD-WAN Manager SAML metadata file to PingID.

      PingID should be able to decode the metadata file and fill in the other fields.

   c. Verify that the following fields and values are entered correctly.

Field	Value
Assertion Consumer Service (ACS)	<Cisco SD-WAN Manager_URL>/samlLoginResponse
Entity ID	IP address of Cisco SD-WAN Manager
Single Logout Endpoint	<Cisco SD-WAN Manager_URL>/samlLogoutResponse
Single Logout Binding Type	Redirect
Primary Verification Certificate	Name of the certificate
Encrypt Assertion	(Optional) If you do not encrypt the assertion, you might be prone to assertion replay attacks and other vulnerabilities.
Encryption Certification	Name of the certificate
Encryption Algorithm	(Optional) AES_256

Field	Value
Transport Algorithm	RSA_OAEP
Signing Algorithm	RSA_SHA256
Force Re-authentication	False

9. Click **Continue to Next Step**.
10. In the **SSO Attribute Mapping** section, configure the following fields:
    a. Click **Add new attribute** to add the following attributes:
        1. Add **Application Attribute** as **Username**.
        2. Set **Identity Bridge Attribute or Literal Value Value** to **Email**.
        3. Check the **Required** box.
        4. Add another **Application Attribute** as **Groups**.
        5. Check the **Required** check box, and then click on **Advanced**.
        6. In the **IDP Attribute Name or Literal Value** section, click **memberOf**, and in **Function**, click **GetLocalPartFromEmail**.
    b. Click **Save**.
11. Click **Continue to Next Step** to configure the **Group Access**.
12. Click **Continue to Next Step**.
13. Before clicking **Finish**, ensure that the settings are all correct.

Configure SSO for IDPs in Cisco SD-WAN Manager Cluster

1. Create three Cisco SD-WAN Manager single-tenant instances and associated configuration templates. See Deploy Cisco SD-WAN Manager.
2. Create a Cisco SD-WAN Manager cluster consisting of three Cisco SD-WAN Manager instances. See the Cluster Management chapter in the *Cisco Catalyst SD-WAN Getting Started Guide*.
3. Download SAML metadata based on the IDP from the first Cisco SD-WAN Manager instance, and save it into a file.
4. Configure SSO for Okta, ADFS, or PingID.
5. Note and save the SAML response metadata information that you need for configuring Okta, ADFS, or PingID with Cisco SD-WAN Manager.
6. In the first instance of Cisco SD-WAN Manager, navigate to **Administration** > **Settings** > **Identity Provider Settings** > **Upload Identity Provider Metadata**, paste the SAML response metadata information, and click **Save**.

When you log in to the Cisco SD-WAN Manager cluster now, the first instance of Cisco SD-WAN Manager redirects SSO using an IDP. The second and third instances of the cluster also redirect SSO using IDP.

If the first instance of Cisco SD-WAN Manager cluster or the application server isn't available, the second and third instances of the cluster try redirecting SSO using an IDP. However, the SSO login fails for the second and third instances of the Cisco SD-WAN Manager cluster. The only option available for accessing the second and third instances of the Cisco SD-WAN Manager cluster is by using the local device authentication, which is "/login.html".

Note If you log in by using the local device authentication, the **SAML Login** page appears when you log out.

Note When the token is expired for IDP login, refresh the browser or open the SSO in the new tab.

Configure Single Sign-On Using Microsoft Entra ID

Minimum supported releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1

Note The solution formerly known as Azure Active Directory (Azure AD) is now called Microsoft Entra ID.

The configuration of Cisco SD-WAN Manager to use Microsoft Entra ID as an IdP involves the following steps:

1. Export Cisco SD-WAN Manager SAML metadata to Microsoft Entra ID. For details, see Export Cisco SD-WAN Manager SAML Metadata to Microsoft Entra ID.
2. Configure Enterprise Application for SSO in Microsoft Entra ID. For details, see Configure Enterprise Application for SSO in Microsoft Entra ID.
3. Import Microsoft Entra ID SAML Metadata into Cisco SD-WAN Manager. For details, see Import Microsoft Entra ID SAML Metadata into Cisco SD-WAN Manager.

Export Cisco SD-WAN Manager Metadata to Microsoft Entra ID

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Identity Provider Settings** under External Services and then click **Add New IDP Settings**.
3. Toggle IDP Settings to enable the identity provider settings.
4. In the **IDP Name** field, enter a name that references the IdP you are using, and in the **Domain** field, enter a domain that matches the domain names used by the users in your organization’s enterprise application.
5. Click **Click here to download the SAML metadata** and save the metadata XML file.

Configure Enterprise Application for Single Sign-On in Microsoft Entra ID

Note This procedure involves a third-party website. The details are subject to change.

1. Log in to the Microsoft Entra admin center portal with one of these roles: Cloud Application Administrator, Application Administrator, or owner of the service principal.
2. Navigate to **Entra ID** > **Enterprise apps** and create a custom enterprise application.
3. On the single sign-on configuration page of your enterprise application, click **Upload metadata file** to upload the metadata XML file that you previously downloaded from Cisco SD-WAN Manager.
4. Add users and assign them to different group memberships based on their permissions within your organization in the enterprise application.
5. On the single sign-on configuration page of your enterprise application, under Attributes & Claims, click **Edit** and configure the following:

Note Your organization may require additional claims depending on its specific needs.

   a. Create a new claim for the email address attribute, configuring the field values as follows:

Field	Value to enter
Name	emailaddress
Namespace	(Leave this empty as this field is optional)
Source	Attribute
Source attribute	user.mail

   b. Create a claim for the user principal name (UPN) of the user, configuring the field values as follows:

Field	Value to enter
Name	user
Namespace	(Leave this empty as this field is optional)
Source	Attribute
Source attribute	user.userprincipalname

   c. Create a claim to define the groups the users belong to and that are authorized to access application resources, configuring the field values as follows:

Field	Value to enter
Name	Groups

Field	Value to enter
Namespace	(Leave this empty as this field is optional)
Source	Attribute
Source attribute	(Leave this empty as multiple conditions will be configured)
Claim conditions	
User Type	Members
Scoped Groups	(Choose the group(s) to which the user(s) belong that sig in to the application)
Source	Attribute
Value	(Enter the customer attribute that references the user group defined in Cisco SD-WAN Manager without quotes, i.e.: netadmin, operator, basic)

Note These parameters within the claim conditions are important in the Single Sign-On SAML configuration of the enterprise application, since these custom attributes must always match the user groups defined in Cisco SD-WAN Manager. This match determines the privileges or permissions granted to users based on the group to which they belong on Microsoft Entra ID.

6. On the single sign-on configuration page, click **Download** next to Federation Metadata XML to download the XML file that provides identity services to the application.
7. From the Cisco SD-WAN Manager menu, navigate to **Administration** > **Settings** > **Identity Provider Settings** and click **Select a file**. Choose the file you just downloaded from Microsoft Entra ID, then click **Save**.

Verify Single Sign-On Using Microsoft Entra ID

Minimum supported releases: Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1

1. From the Cisco SD-WAN Manager, click your profile name in the upper-right corner of the screen to expand the options, from there click **Log Out** to sign out of the portal.
2. After redirection to the Microsoft authentication screen, sign in with your Microsoft Entra ID SSO credentials (first time the SSO user logs in, the prompt requests a password change).
3. After a successful sign-in, expand the details of your profile again in the upper-right corner of the dashboard and confirm that the user is detected with the SSO role configured in Microsoft Entra ID.

Integrate with Multiple IdPs

The following sections provide information about integrating with multiple IdPs.

Information About Integrating with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

With this feature, you can now configure more than one IdP per tenant in Cisco SD-WAN Manager. This feature supports both single-tenant and multitenant environments.

You can configure up to three IdPs per tenant and a maximum of three IdPs per the provider.

The following fields are added in Cisco SD-WAN Manager **Administration** > **Settings** > **Identity Provider Settings** for configuring multiple IdPs:

- **Add New IDP Settings**
- **IDP Name**
- **Domain**

You can also edit or delete an IdP name and domain name.

For more information on configuring multiple IdPs, see Configure Multiple IdPs.

Benefits of Integrating with Multiple IdPs

- Enables end users to allocate different user access for different functions in the organization
- Provides high level of security and meets compliance requirements
- Reduces operational costs

Restrictions for Integrating with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

- You can configure only three IdPs in a single-tenant deployment and three IdPs per tenant in a multitenancy deployment.

Use Cases for Integrating with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

The following are potential use cases for integrating with multiple IdPs:

- An end user (tenant) requires different types of user access for employees versus contractors.
- An end user requires different types of user access for different functions within the organization.
- An end user requires access to the same IdP, but has a different email address.

Configure Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

The following workflow is for configuring multiple IdPs. For more information on enabling an IdP, see Enable an Identity Provider in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Identity Provider Settings** and choose **Edit**.
3. Click **Add New IDP Settings**.

Note After three IdPs are configured, the **Add New IDP Settings** option is no longer displayed.

4. Click the toggle button to switch between enabling and disabling IdP settings while retaining the existing configuration.
5. Click **IDP Name** and enter a unique name for your IdP.

   Examples:

   - **okta**
   - **idp1**
   - **provider**
   - **msp**

   You can configure a maximum of three IdPs.

Note You cannot map the same domain to multiple IdPs, but you can use the same IdP for multiple domains.

6. Click **Domain** and enter a unique domain name for your IdP, for example, okta.com.

   If the domain name already exists, Cisco SD-WAN Manager generates an error message.

   Alternatively, you can enter a wildcard (*) in the domain name field making it the default domain. If a default domain is configured, you can log in to a domain with your user ID without requiring you to enter an user ID in the email address format (xyz@mystore.com).

Note Only one of the IDPs can be configured as a default IDP.

7. In the **Upload Identity Provider Metadata** section, upload the SAML metadata file you downloaded from your IdP.
8. Click **Save**.
9. After you configure a new IdP name, domain, and sign out of your current Cisco SD-WAN Manager session, you are redirected to a unified SAML login page.

10. In the unified SAML login page, if you require local authentication, remove the **login.html** portion of the URL. This redirects you to the local authentication page.
11. In the unified SAML login page, enter the SSO credentials for your IdP.

Note You are redirected to the unified SAML login page each time you access Cisco SD-WAN Manager after configuring a new IdP name and domain.

Verify Integration with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Identity Provider Settings** and then click **View**.
3. Verify the configured IdP and the corresponding domain.

Troubleshooting Integration with Multiple IdPs

Minimum supported release: Cisco vManage Release 20.10.1

For troubleshooting integration issues with multiple IdPs, you can access the log files at:

- `/var/log/nms/vmanage-server.log` is the log file for enabling and disabling IdP.
- `/var/log/nms/vmanage-sso.log` is the SSO-specific log file.