

Configuring MFA for Ivanti Connect Secure VPN via SAML

16-May-2023•Knowledge Article

Article Number
000025442

Title
Configuring MFA for Ivanti Connect Secure VPN via SAML

Introduction
When adding a Code Sample, please choose the 'Normal (DIV)' formatting, in order to avoid text glitch over the page borders

CyberArk Identity integrates with Ivanti Connect Secure VPN to add multi-factor authentication (MFA) via SAML or RADIUS. This article will walk through the steps for SAML integration.

Step-by-step instructions
When adding a Code Sample, please choose the 'Normal (DIV)' formatting, in order to avoid text glitch over the page borders

Add a new SAML configuration in CyberArk Admin Portal

1. Go to **Apps & Widgets > Web Apps** and click **Add Web Apps**.
2. Select the **Custom** tab, look for **SAML**, then click **Add**.
3. In **Settings**, change the name to something recognizable like "Ivanti Connect Secure". Optionally add a logo.
4. Go to **Trust > Identity Provider Configuration**, then download the Signing Certificate and the Metadata File.

Settings

- Trust
- SAML Response
- Permissions
- Policy
- Account Mapping
- Linked Applications
- Provisioning
- App Gateway
- Workflow
- Changelog
- Secure Web Sessions

Trust

[Learn more](#)

Identity Provider Configuration

Configure your IdP Entity ID / Issuer and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration values

☒ Metadata
☐ Manual Configuration

Metadata

IdP Entity ID / Issuer and Signing Certificate do not need to be edited in most cases. If you need to edit them, edit them first then proceed to the configuration method required by Service Provider.

> IdP Entity ID / Issuer ⓘ

▼ Signing Certificate ⓘ

ABA0577 SHA256 Application Signing Certificate (default)

Thumbprint: AF305DD61DAF5E8CD6DACEE65D5C0E08A09EAE9B
Subject: CN=ABA0577 Application Signing Certificate
Algorithm: sha256RSA
Expires: 12/31/2038 4:00:00 PM

[Download](#)

> Single Sign On URL ⓘ

URL [Copy URL](#)

File [Download Metadata File](#)

XML [Copy XML](#)

Leave the Ivanti Connect Secure SAML settings in the CyberArk Admin Portal open, as we will return to complete additional settings. Open a new browser window or browser tab and log into the Ivanti Connect Secure Admin Console.

Enable SAML authentication in the Ivanti Connect Secure Admin Console

1. Create the Ivanti Connect Secure Entity ID
 - a. Go to **System > Configuration > SAML > Settings**
 - b. Under **Metadata Server Configuration**, enter a hostname in the **Host FQDN for SAML** field, then click **Save Changes**.

C. Click **Update Entity Ids**.

[SAML >](#)

Settings

▼ **Metadata Server Configuration**

Timeout value for metadata fetch request: seconds 1 - 600. Specifies the time in seconds to wait for response of SAML metadata fetch request.

Validity of uploaded/downloaded metadata file: days 0 - 9999. Specifies the time in days after which downloaded/uploaded metadata file expires. 0 means that Connect Secure doesnot enforce any validity on the peer metadata file.

Host FQDN for SAML: The FQDN used for generating URLs for SAML services.

Alternate Host FQDN for SAML: The FQDN used for generating SA's Single Sign-On Service URL when Pulse(NC) Session detection is enabled.

Save Changes

Cancel

Update Entity Ids

2.Import CyberArk's IDP Metadata file

- Enter a **Name**.
- Click **System > Configuration > SAML > New Metadata Provider**.
- Upload CyberArk's Metadata file (already downloaded in a previous step).
- Tick the box **"Accept Unsigned Metadata"**
- Upload CyberArk's Signing Certificate (already downloaded in a previous step).
- Tick the box **"Identity Provider"**

g. Click **Save**.

The screenshot shows the 'CyberArk IDP Metadata' configuration page. Green boxes and arrows highlight the following elements:

- Name:** A text field containing 'CyberArk IDP Metadata'.
- Metadata Provider Location Configuration:** A section header.
- Location:** Radio buttons for 'Local' (selected) and 'Remote'.
- Upload Metadata File:** A 'Browse' button. Below it, text indicates 'No file chosen' and 'Current File: Pulse Secure - IdP Metadata.xml'.
- Metadata Provider Verification Configuration:** A section header.
- Accept Unsigned Metadata:** A checked checkbox.
- Signing Certificate:** A section with details: 'Issued To: Application Signing Certificate', 'Issued By:', 'Valid: Aug 20 00:49:47 2020 GMT - Jan 1 00:00:00 2039 GMT', and 'Details: Other Certificate Details'.
- Upload Certificate:** A 'Browse' button, 'No file chosen' text, and a 'Delete' button.
- Enable Signing Certificate status checking:** An unchecked checkbox with a descriptive note below it.
- Valid Till:** A date field showing '2038-01-19 04:14:07'.
- Metadata Provider Filter Configuration:** A section header.
- Roles:** Checkboxes for 'Identity Provider' (checked), 'Service Provider', and 'Policy Decision Point'.

3. Create a new SAML Identity Provider

a. Go to **Authentication > Auth. Servers**

- b. Under the **New** field, select **SAML Server** and click **New Server**
 - c. Under **Settings**:
 - i. Enter a **Server Name** (ex. Ivanti Connect Secure).
 - ii. Select **Metadata** (all the required fields will be automatically filled)
 - d. Under **Service Provider Metadata Settings**:
 - i. In the **Metadata Validity** field, enter the number of days up to which the metadata is valid (ex. 9999 days)
 - ii. Enter a **Server Name** (ex. Ivanti Connect Secure).
 - e. Click **Save Changes**.
 - f. Under **Service Provider Metadata Settings**, click **Download Metadata** to download the Ivanti Connect Secure metadata.
4. Go to **Users > User Realms**, select **Users > Servers > . Authentication** and apply SAML authentication to all users, else go to **Users > New User Realms** to assign a subset of users through **Role Mapping**. Please see the Ivanti Connect Secure documentation for more details on SAML authentication assignment options.

Complete the SAML settings in the CyberArk Admin Portal

1. Return to the Ivanti Connect Secure SAML configurations, in the CyberArk Admin Portal,

Trust
[Learn more](#)

Settings
Trust
SAML Response
Permissions
Policy
Account Mapping
Linked Applications
Provisioning
App Gateway
Workflow
Changelog
Secure Web Sessions

Service Provider Configuration
Select the configuration method specified by Service Provider, and then follow the instructions.

☒ Metadata
☐ Manual Configuration

Metadata
Use one of the following methods to import SP Metadata given by your Service Provider.

URL [Copy URL](#)

File [Download Metadata File](#)

XML [Copy XML](#)

URL [Load](#)

File [Choose File](#)

XML

```
<md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
cacheDuration="P9999DT0H0M0S"
entityID="https://Pulsesecure.cyberlab.fr/dana-na/auth/saml-
endpoint.cgi?p=sp1"><md:SPSSODescriptor
```

2. Leave as **Metadata** and click **Choose File** to upload the Ivanti Connect Secure metadata file that was downloaded from Ivanti Connect Secure in a previous step. Click **Save**.

3. Go to **Account Mapping** and change the **Directory Service field name** to **sAMAccountName** if you log into Ivanti Connect Secure with your sAMAccountName (ex. jsmith). Leave as userprincipalname if you log in with fully qualified domain name like "[jsmith@domain.com](#)".

Settings
Trust
SAML Response
Permissions
Policy
Account Mapping
Linked Applications
Provisioning
App Gateway
Workflow
Changelog
Secure Web Sessions

Account Mapping

[Learn more](#)

☒ Directory Service Field
☐ All users share one name
☐ Account Mapping Script

Directory Service Field

Use the following Directory Service field to supply the user name

Directory Service field name *

4. Go to **Permissions** and add the users, groups, or Roles that will be using The Ivanti Secure Access client. Click **Save**.

Settings
Trust
SAML Response
Permissions
Policy
Account Mapping
Linked Applications
Provisioning
App Gateway
Workflow
Changelog
Secure Web Sessions

Permissions

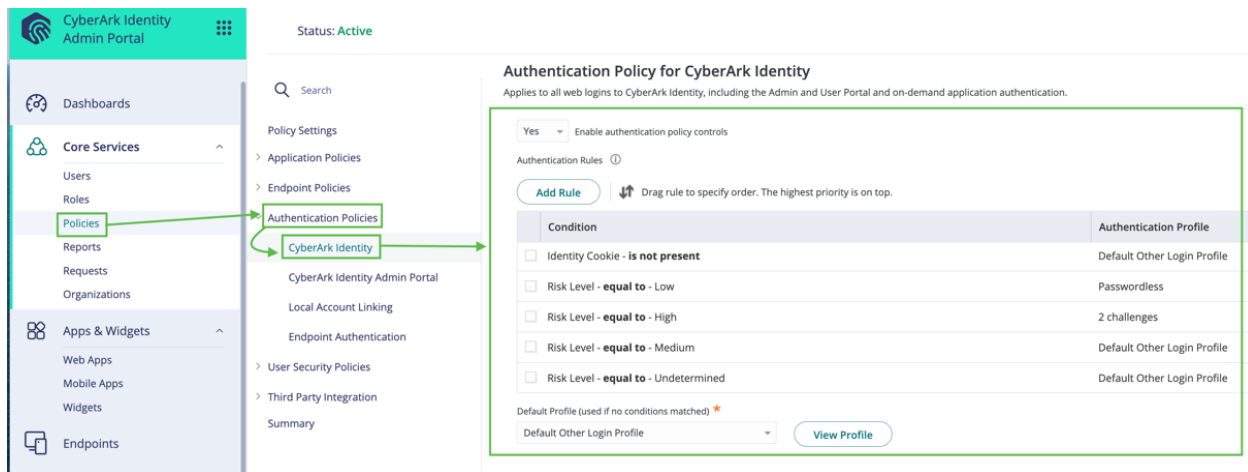
[Learn more](#)

Add

	Name	Grant	View	Manage	Delete	Run	Automatically D...
☐	Application Managers	☒	☒	☒	☒	☐	☐
☐	ReadOnlyAdmin	☐	☒	☐	☐	☐	☐
☐	Set Admin	☒	☒	☒	☒	☐	☐
☐	sws-integration-user\$@v...	☒	☒	☒	☒	☐	☐
☐	System Administrator	☒	☒	☒	☒	☐	☐
☐	Technical Support Access	☐	☒	☐	☐	☐	☐
☐	VPN users	☐	☐	☐	☐	☒	☒

5. Applying MFA policies.

- The first MFA policy that is triggered when logging into The Ivanti Secure Access client will be **Policies > (Policy assigned to the user) > Authentication Policies > CyberArk Identity**. Learn more at <https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/CoreServices/Authenticate/MFA-UserPortal.htm>



- If there are no MFA policies applied in **Policies > Authentication Policies > CyberArk Identity**, MFA policies can be applied in the Ivanti Connect Secure SAML configurations. In the Connect Secure SAML settings, go to **Policy** to configure MFA policies. Learn more at <https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/iDaptiveTrial/appMFATrial.htm>

