

**GUIDE USING SAML**

# Azure Active Directory single sign-on (SSO) integration with Cisco AnyConnect

## Prerequisites

To get started, you need the following items:

* An Azure AD subscription. If you don't have a subscription, you can get a [free account](https://azure.microsoft.com/free/).
* Cisco AnyConnect single sign-on (SSO) enabled subscription.

## Scenario description

In this tutorial, you configure and test Azure AD SSO in a test environment.

* Cisco AnyConnect supports **IDP** initiated SSO.

## Adding Cisco AnyConnect from the gallery

To configure the integration of Cisco AnyConnect into Azure AD, you need to add Cisco AnyConnect from the gallery to your list of managed SaaS apps.

1. Sign in to the Azure portal using either a work or school account, or a personal Microsoft account.
2. On the left navigation pane, select the **Azure Active Directory** service.
3. Navigate to **Enterprise Applications** and then select **All Applications**.
4. To add new application, select **New application**.
5. In the **Add from the gallery** section, type **Cisco AnyConnect** in the search box.
6. Select **Cisco AnyConnect** from results panel and then add the app. Wait a few seconds while the app is added to your tenant.

Alternatively, you can also use the [Enterprise App Configuration Wizard](https://portal.office.com/AdminPortal/home?Q=Docs#/azureadappintegration). In this wizard, you can add an application to your tenant, add users/groups to the app, assign roles, as well as walk through the SSO configuration as well. [Learn more about Microsoft 365 wizards.](https://learn.microsoft.com/en-us/microsoft-365/admin/misc/azure-ad-setup-guides)

Alternatively, you can also use the [Enterprise App Configuration Wizard](https://portal.office.com/AdminPortal/home?Q=Docs#/azureadappintegration). In this wizard, you can add an application to your tenant, add users/groups to the app, assign roles, as well as walk through the SSO configuration as well. You can learn more about O365 wizards [here](https://learn.microsoft.com/en-us/microsoft-365/admin/misc/azure-ad-setup-guides?view=o365-worldwide&preserve-view=true).

## Configure and test Azure AD SSO for Cisco AnyConnect

Configure and test Azure AD SSO with Cisco AnyConnect using a test user called **B.Simon**. For SSO to work, you need to establish a link relationship between an Azure AD user and the related user in Cisco AnyConnect.

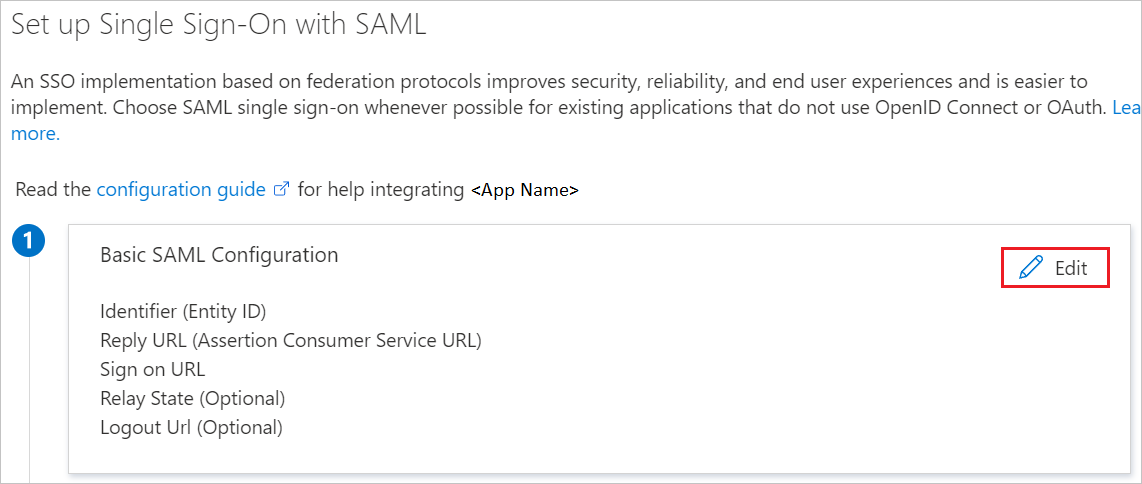
To configure and test Azure AD SSO with Cisco AnyConnect, perform the following steps:

1. [**Configure Azure AD SSO**](https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/cisco-anyconnect#configure-azure-ad-sso) - to enable your users to use this feature.
   1. [**Create an Azure AD test user**](https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/cisco-anyconnect#create-an-azure-ad-test-user) - to test Azure AD single sign-on with B.Simon.
   2. [**Assign the Azure AD test user**](https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/cisco-anyconnect#assign-the-azure-ad-test-user) - to enable B.Simon to use Azure AD single sign-on.
2. [**Configure Cisco AnyConnect SSO**](https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/cisco-anyconnect#configure-cisco-anyconnect-sso) - to configure the single sign-on settings on application side.
   1. [**Create Cisco AnyConnect test user**](https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/cisco-anyconnect#create-cisco-anyconnect-test-user) - to have a counterpart of B.Simon in Cisco AnyConnect that is linked to the Azure AD representation of user.
3. [**Test SSO**](https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/cisco-anyconnect#test-sso) - to verify whether the configuration works.

## Configure Azure AD SSO

Follow these steps to enable Azure AD SSO in the Azure portal.

1. In the Azure portal, on the **Cisco AnyConnect** application integration page, find the **Manage** section and select **single sign-on**.
2. On the **Select a single sign-on method** page, select **SAML**.
3. On the **Set up single sign-on with SAML** page, click the edit/pen icon for **Basic SAML Configuration** to edit the settings.

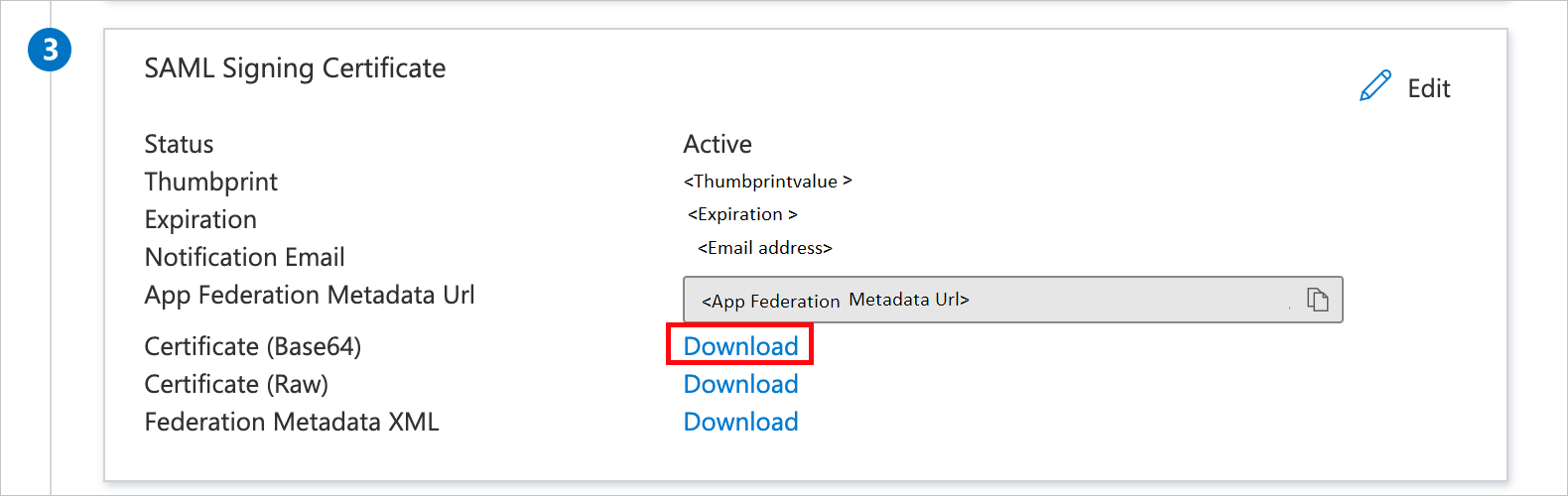


1. On the **Set up single sign-on with SAML** page, enter the values for the following fields (note that the values are case-sensitive):
   1. In the **Identifier** text box, type a URL using the following pattern:  
      https://<SUBDOMAIN>.YourCiscoServer.com/saml/sp/metadata/<Tunnel\_Group\_Name>
   2. In the **Reply URL** text box, type a URL using the following pattern:  
      https://<YOUR\_CISCO\_ANYCONNECT\_FQDN>/+CSCOE+/saml/sp/acs?tgname=<Tunnel\_Group\_Name>

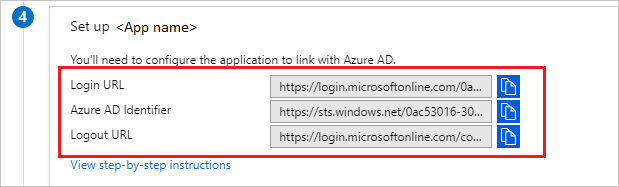
**Note**

For clarification about these values, contact Cisco TAC support. Update these values with the actual Identifier and Reply URL provided by Cisco TAC. Contact the [**Cisco AnyConnect Client support team**](https://www.cisco.com/c/en/us/support/index.html) to get these values. You can also refer to the patterns shown in the **Basic SAML Configuration** section in the Azure portal.

1. On the **Set up single sign-on with SAML** page, in the **SAML Signing Certificate** section, find **Certificate (Base64)** and select **Download** to download the certificate file and save it on your computer.



1. On the **Set up Cisco AnyConnect** section, copy the appropriate URL(s) based on your requirement.



**Note**

If you would like to on board multiple TGTs of the server then you need to add multiple instances of the Cisco AnyConnect application from the gallery. You can also choose to upload your own certificate in Azure AD for all these application instances. That way you can have same certificate for the applications but you can configure different Identifier and Reply URL for every application.

### Create an Azure AD test user

In this section, you'll create a test user in the Azure portal called B.Simon.

1. From the left pane in the Azure portal, select **Azure Active Directory**, select **Users**, and then select **All users**.
2. Select **New user** at the top of the screen.
3. In the **User** properties, follow these steps:
   1. In the **Name** field, enter B.Simon.
   2. In the **User name** field, enter the username@companydomain.extension. For example, B.Simon@contoso.com.
   3. Select the **Show password** check box, and then write down the value that's displayed in the **Password** box.
   4. Click **Create**.

### Assign the Azure AD test user

In this section, you'll enable B.Simon to use Azure single sign-on by granting access to Cisco AnyConnect.

1. In the Azure portal, select **Enterprise Applications**, and then select **All applications**.
2. In the applications list, select **Cisco AnyConnect**.
3. In the app's overview page, find the **Manage** section and select **Users and groups**.
4. Select **Add user**, then select **Users and groups** in the **Add Assignment** dialog.
5. In the **Users and groups** dialog, select **B.Simon** from the Users list, then click the **Select** button at the bottom of the screen.
6. If you are expecting a role to be assigned to the users, you can select it from the **Select a role** dropdown. If no role has been set up for this app, you see "Default Access" role selected.
7. In the **Add Assignment** dialog, click the **Assign** button.

## Configure Cisco AnyConnect SSO

1. You are going to do this on the CLI first, you might come back through and do an ASDM walk-through at another time.
2. Connect to your VPN Appliance, you are going to be using an ASA running 9.8 code train, and your VPN clients will be 4.6+.
3. First you will create a Trustpoint and import our SAML cert.

Copy

config t

crypto ca trustpoint AzureAD-AC-SAML

revocation-check none

no id-usage

enrollment terminal

no ca-check

crypto ca authenticate AzureAD-AC-SAML

-----BEGIN CERTIFICATE-----

…

PEM Certificate Text from download goes here

…

-----END CERTIFICATE-----

quit

1. The following commands will provision your SAML IdP.

Copy

webvpn

saml idp https://sts.windows.net/xxxxxxxxxxxxx/ (This is your Azure AD Identifier from the Set up Cisco AnyConnect section in the Azure portal)

url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2 (This is your Login URL from the Set up Cisco AnyConnect section in the Azure portal)

url sign-out https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 (This is Logout URL from the Set up Cisco AnyConnect section in the Azure portal)

trustpoint idp AzureAD-AC-SAML

trustpoint sp (Trustpoint for SAML Requests - you can use your existing external cert here)

no force re-authentication

no signature

base-url https://my.asa.com

1. Now you can apply SAML Authentication to a VPN Tunnel Configuration.

Copy

tunnel-group AC-SAML webvpn-attributes

saml identity-provider https://sts.windows.net/xxxxxxxxxxxxx/

authentication saml

end

write mem

**Note**

There is a work around with the SAML IdP configuration. If you make changes to the IdP configuration you need to remove the saml identity-provider configuration from your Tunnel Group and re-apply it for the changes to become effective.

### Create Cisco AnyConnect test user

In this section, you create a user called Britta Simon in Cisco AnyConnect. Work with [Cisco AnyConnect support team](https://www.cisco.com/c/en/us/support/index.html) to add the users in the Cisco AnyConnect platform. Users must be created and activated before you use single sign-on.

## Test SSO

In this section, you test your Azure AD single sign-on configuration with following options.

* Click on Test this application in Azure portal and you should be automatically signed in to the Cisco AnyConnect for which you set up the SSO
* You can use Microsoft Access Panel. When you click the Cisco AnyConnect tile in the Access Panel, you should be automatically signed in to the Cisco AnyConnect for which you set up the SSO. For more information about the Access Panel, see [Introduction to the Access Panel](https://support.microsoft.com/account-billing/sign-in-and-start-apps-from-the-my-apps-portal-2f3b1bae-0e5a-4a86-a33e-876fbd2a4510).

## Next steps

Once you configure Cisco AnyConnect you can enforce session control, which protects exfiltration and infiltration of your organization’s sensitive data in real time. Session control extends from Conditional Access. [Learn how to enforce session control with Microsoft Defender for Cloud Apps](https://learn.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app).

Reference: <https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/cisco-anyconnect>

**Introduction**

This document describes **Security Assertion Markup Language (SAML)** authentication on FTD managed over FMC.

**Prerequisites**

**Requirements**

Cisco recommends knowledge of these topics:

* **AnyConnect** configuration on FMC
* SAML and metatada.xml values

**Components Used**

The information in this document is based on these software and hardware versions:

* **Firepower Threat Defense (FTD)** version 6.7.0
* **Firepower Management Center (FMC)** version 6.7.0
* ADFS from **AD Server** with SAML 2.0

**Note**: If possible, use an NTP server to synchronize time between the FTD and IdP. Otherwise, verify that the time is manually synchronized between them.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

**Background Information**

The configuration allows Anyconnect users to establish a VPN session authentication with a SAML Identity Service Provider.

Some of the current limitations for SAML are:

* SAML on FTD is supported for authentication (version 6.7 onward) and authorization (version 7.0 onward).
* SAML authentication attributes available in DAP evaluation (similar to **RADIUS** attributes sent in **RADIUS** authorization response from AAA server) are not supported.
* ASA supports SAML-enabled tunnel-group on DAP policy. However, you cannot check the username attribute with SAML authentication, because the username attribute is masked by the SAML Identity provider.
* Because **AnyConnect** with the embedded browser uses a new browser session on every VPN attempt, users must re-authenticate every time if the IdP uses HTTP session cookies to track login state.
* In this case, the **Force Re-Authentication** setting in **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** has no effect on **AnyConnect** initiated SAML authentication.

More limitations or SAML are described in the link provided here.

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa915/configuration/vpn/asa-915-vpn-config/webvpn-configure-users.html#reference_55BA48B37D6443BEA5D2F42EC21075B5>

These limitations apply to ASA and FTD: "**Guidelines and Limitations for SAML 2.0**"

**Note**: All of the SAML configuration to be implemented on the FTD can be found on the metadata.xml file provided by your IdP.

**Configuration**

This section describes how to configure **AnyConnect** with SAML authentication on FTD

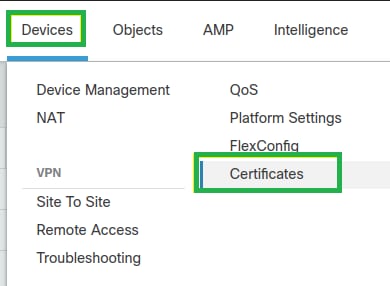
**Get the SAML IdP parameters**

This image shows a SAML IdP metadata.xml file. From the output, you can obtain all values required to configure the **AnyConnect** profile with SAML:

[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-00.png)

**Configuration on the FTD via FMC**

**Step 1.** Install and enroll the IdP certificate on the FMC. Navigate to **Devices > Certificates**

[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-01.png)

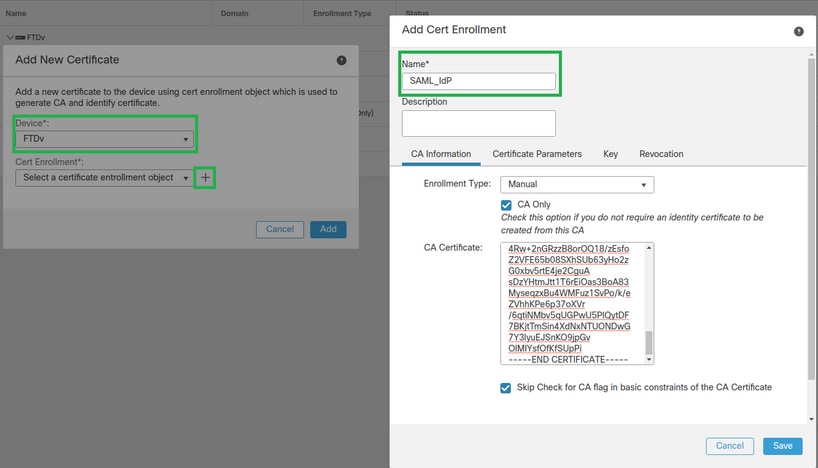
**Step 2.** Click **Add**. Select the FTD to enroll in this certificate. Under Cert Enrollment, click the plus **+** sign

In the **Add Cert Enrollment** section, use any name as a label for the IdP cert. Click **Manual**.

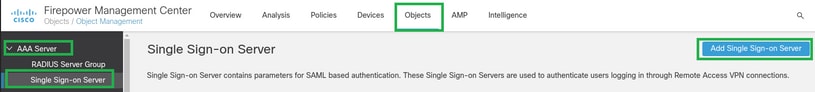
Check the **CA Only** and **Skip Check** for CA flag fields.

Paste the **base64** format IdP CA cert.

Click **Save** and then click **Add**.

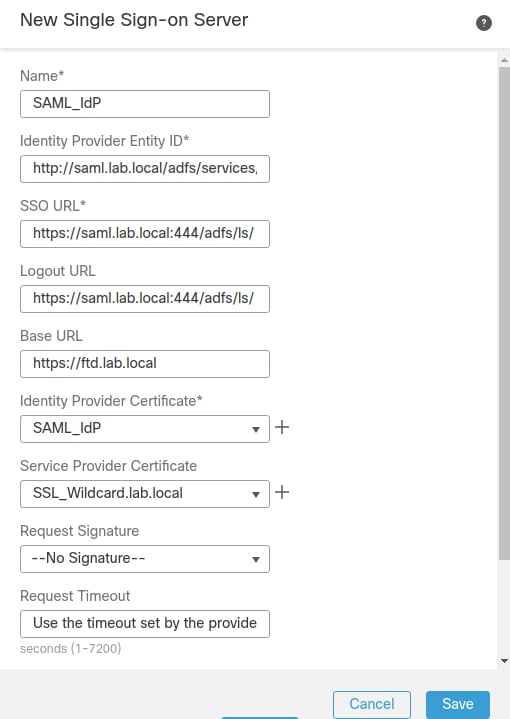
[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-02.png)

**Step 3**. Configure the SAML server settings. Navigate to **Objects > Object Management > AAA Servers > Single Sign-on Server**. Then, select **Add Single Sign-on Server**.

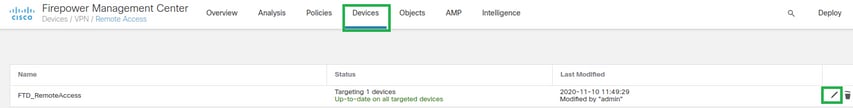
[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-03.png)

**Step 4.** Based on the **metadata.xml** file already provided by your IdP, configure the SAML values on the **New Single Sign-on Server**.

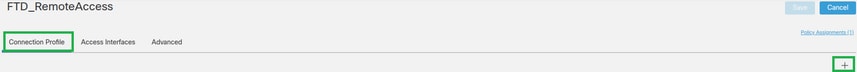
SAML Provider Entity ID: entityID from metadata.xml  
SSO URL: SingleSignOnService from metadata.xml.  
Logout URL: SingleLogoutService from metadata.xml.  
BASE URL: FQDN of your FTD SSL ID Certificate.  
Identity Provider Certificate: IdP Signing Certificate.  
Service Provider Certificate: FTD Signing Certificate.

[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-04.png)

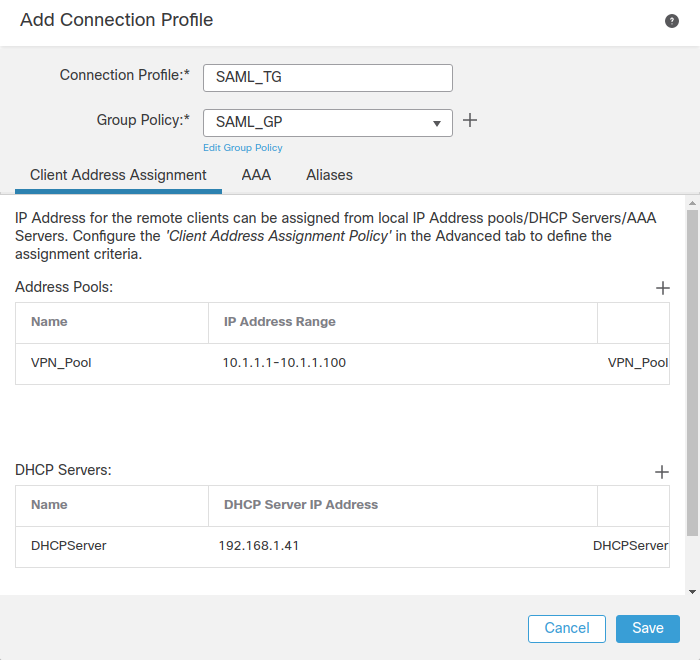
**Step 5.** Configure the **Connection Profile** that uses this authentication method. Navigate to **Devices > Remote Access**  and then edit your current **VPN Remote Access** configuration.

[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-05.png)

**Step 6**. Click on the plus **+** sign and add another **Connection Profile**.

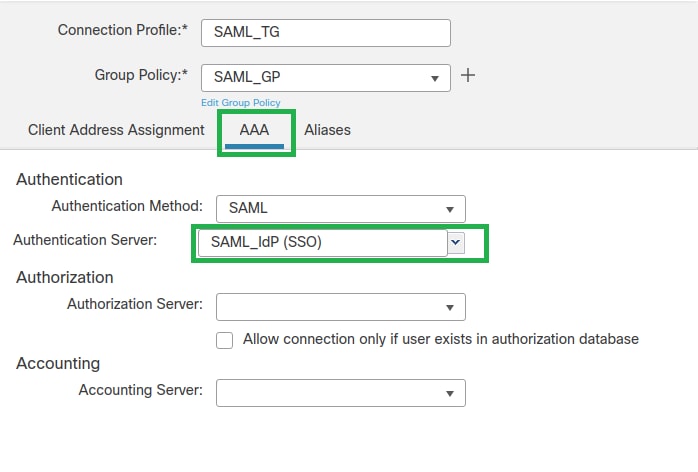
[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-06.png)

**Step 7**. Create the new **Connection Profile** and add the proper VPN, **Pool**, or DHCP Server.

[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-07.png)

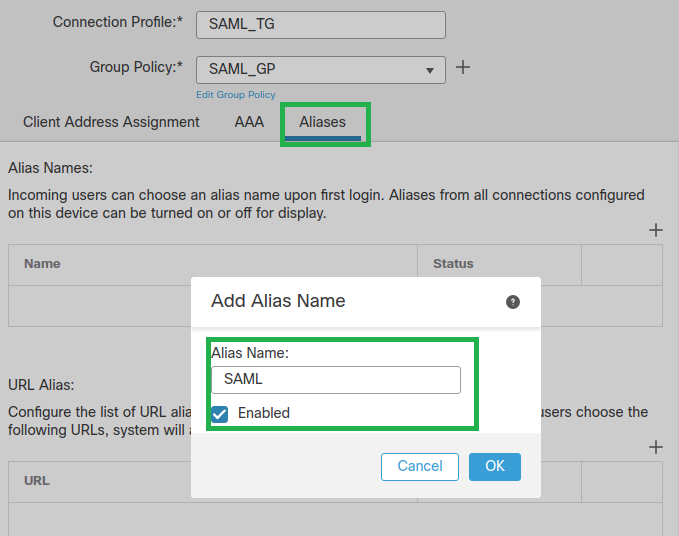
**Step 8.** Select the AAA tab. Under the **Authentication Method** option, select SAML.

Under the **Authentication Server** option, select the SAML object created on Step 4.

[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-08.png)

**Step 9.** Create a group alias to map the connections to this **Connection Profile**. This is the tag that users can see on the **AnyConnect** Software drop-down menu.

When this is configured, click OK and save the complete **SAML Authentication VPN** configuration.

[](https://www.cisco.com/c/dam/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic-09.png)

**Step 10.** Navigate to **Deploy > Deployment** and select the proper FTD  to apply the **SAML Authentication VPN** changes.

**Step 11.** Provide the FTD **metadata.xml** file to the **IdP** so they add the FTD as a trusted device.

On the FTD CLI, run the command **show saml metadata SAML\_TG** where SAML\_TG is the name of the **Connection Profile** created on Step 7.

This is the expected output:

> system support diagnostic-cli  
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.  
firepower> en  
Password:  
firepower# **show saml metadata SAML\_TG**  
  
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
<EntityDescriptor entityID="https://ftd.lab.local/saml/sp/metadata/SAML\_TG" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">  
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  
<KeyDescriptor use="signing">  
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
<ds:X509Data>  
<ds:X509Certificate>MIIF1zCCBL+gAwIBAgITYAAAABN6dX+H0cOFYwAAAAAAEzANBgkqhkiG9w0BAQsF  
ADBAMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxEzARBgoJkiaJk/IsZAEZFgNsYWIx  
EjAQBgNVBAMTCU1TMjAxMi1DQTAeFw0yMDA0MTEwMTQyMTlaFw0yMjA0MTEwMTQy  
MTlaMCMxCzAJBgNVBAYTAkNSMRQwEgYDVQQDDAsqLmxhYi5sb2NhbDCCASIwDQYJ  
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKfRmbCfWk+V1f+YlsIE4hyY6+Qr1yKf  
g1wEqLOFHtGVM3re/WmFuD+4sCyU1VkoiJhf2+X8tG7x2WTpKKtZM3N7bHpb7oPc  
uz8N4GabfAIw287soLM521h6ZM01bWGQ0vxXR+xtCAyqz6JJdK0CNjNEdEkYcaG8  
PFrFUy31UPmCqQnEy+GYZipErrWTpWwbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMy  
EY4F8sdic7btlQQPKG9JIaWny9RvHBmLgj0px2i5Rp5k1JIECD9kHGj44O5lBEcv  
OFY6ecAPv4CkZB6CloftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC  
AuUwggLhMBYGA1UdEQQPMA2CCyoubGFiLmxvY2FsMB0GA1UdDgQWBBROkmTIhXT/  
EjkMdpc4aM6PTnyKPzAfBgNVHSMEGDAWgBTEPQVWHlHqxd11VIRYSCSCuHTa4TCB  
zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049  
V0lOLTVBME5HNDkxQURCLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNl  
cyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j  
ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz  
dHJpYnV0aW9uUG9pbnQwgbkGCCsGAQUFBwEBBIGsMIGpMIGmBggrBgEFBQcwAoaB  
mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBT  
ZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s  
b2NhbD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlv  
bkF1dGhvcml0eTAOBgNVHQ8BAf8EBAMCBaAwPQYJKwYBBAGCNxUHBDAwLgYmKwYB  
BAGCNxUIgYKsboLe0U6B4ZUthLbxToW+yFILh4iaWYXgpQUCAWQCAQMwSwYDVR0l  
BEQwQgYIKwYBBQUHAwEGCCsGAQUFBwMHBggrBgEFBQcDBgYIKwYBBQUIAgIGCCsG  
AQUFBwMFBggrBgEFBQcDAgYEVR0lADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUF  
BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUF  
BwMFMAoGCCsGAQUFBwMCMAYGBFUdJQAwDQYJKoZIhvcNAQELBQADggEBAKQnqcaU  
fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V  
Lmq04X1goaAs6obHrYFtSttz/9XlTAe1KbZ0GlRVg9LblPiF17kZAxALjLJHlCTG  
5EQSC1YqS31sTuarm4WPDJyMShc6hlUpswnCokGRMMgpx2GmDgv4Zf8SzJJ0NI4y  
DgMozuObwkNUXuHbiLuoXwvb2Whm11ysidpl+V9kp1RYamyjFUo+agx0E+L1zp8C  
i0YEwYKXgKk3CZdwJfnYQuCWjmapYwlLGt5S59Uwegwro6AsUXY335+ZOrY/kuLF  
tzR3/S90jDq6dqk=  
</ds:X509Certificate>  
</ds:X509Data>  
</ds:KeyInfo>  
</KeyDescriptor>  
<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://ftd.lab.local/+CSCOE+/saml/sp/acs?tgname=SAML\_TG" />  
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ftd.lab.local/+CSCOE+/saml/sp/logout"/><SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://ftd.lab.local/+CSCOE+/saml/sp/logout"/></SPSSODescriptor>  
</EntityDescriptor>

After the **metadata.xml** from the FTD is provided to the IdP and it is as a trusted device, a test under the VPN connection can be performed.

**Verify**

Verify that the **VPN AnyConnect** connection was established with SAML as an authentication method with the commands seen here:

firepower# **show vpn-sessiondb detail anyconnect**  
Session Type: AnyConnect Detailed  
Username : xxxx Index : 4  
Assigned IP : 10.1.1.1 Public IP : 192.168.1.104  
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License : AnyConnect Premium  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384  
Bytes Tx : 12772 Bytes Rx : 0  
Pkts Tx : 10 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : SAML\_GP Tunnel Group : SAML\_TG  
Login Time : 18:19:13 UTC Tue Nov 10 2020  
Duration : 0h:03m:12s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : c0a80109000040005faad9a1  
Security Grp : none Tunnel Zone : 0  
AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1  
AnyConnect-Parent:  
Tunnel ID : 4.1  
Public IP : 192.168.1.104  
Encryption : none Hashing : none  
TCP Src Port : 55130 TCP Dst Port : 443  
**Auth Mode : SAML**  
Idle Time Out: 30 Minutes Idle TO Left : 26 Minutes  
Client OS : linux-64  
Client OS Ver: Ubuntu 20.04.1 LTS (Focal Fossa)  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Linux 4.9.03047  
Bytes Tx : 6386 Bytes Rx : 0  
Pkts Tx : 5 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
SSL-Tunnel:  
Tunnel ID : 4.2  
Assigned IP : 10.1.1.1 Public IP : 192.168.1.104  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
Encapsulation: TLSv1.2 TCP Src Port : 55156  
TCP Dst Port : 443 Auth Mode : SAML  
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes  
Client OS : Linux\_64  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Linux 4.9.03047  
Bytes Tx : 6386 Bytes Rx : 0  
Pkts Tx : 5 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
DTLS-Tunnel:  
Tunnel ID : 4.3  
Assigned IP : 10.1.1.1 Public IP : 192.168.1.104  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384  
Encapsulation: DTLSv1.2 UDP Src Port : 40868  
UDP Dst Port : 443 Auth Mode : SAML  
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes  
Client OS : Linux\_64  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Linux 4.9.03047  
Bytes Tx : 0 Bytes Rx : 0  
Pkts Tx : 0 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

**Troubleshoot**

Some verification commands on the FTD CLI can be used to troubleshoot SAML and **Remote Access VPN** connection as seen in the bracket:

firepower# **show run webvpn**  
firepower# **show run tunnel-group**  
firepower# **show crypto ca certificate**firepower# **debug webvpn saml 25**

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic.html>