

# Configure AnyConnect with SAML Authentication on FTD Managed via FMC

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Components Used](#)

### [Background Information](#)

### [Configuration](#)

#### [Get the SAML IdP Parameters](#)

#### [Configuration on the FTD via FMC](#)

### [Verify](#)

### [Troubleshoot](#)

---

## 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 Firepower Management Center (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
- 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 and higher) and authorization (version 7.0 and higher).
  - 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.

## Guidelines and Limitations for SAML 2.0

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

 Note: All of the SAML configurations 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:

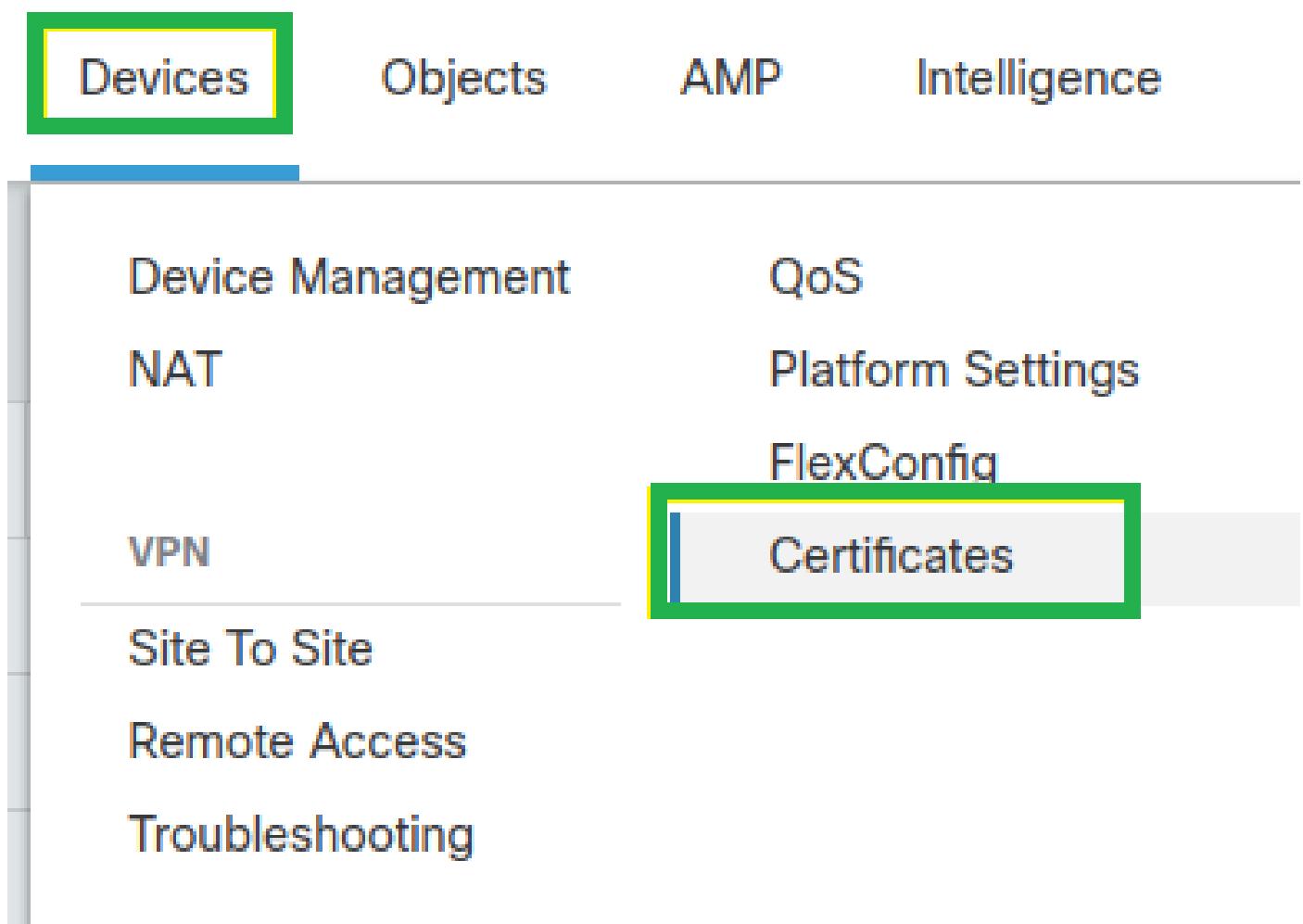
```

<?xml version="1.0?">
<EntityDescriptor xmlns="urn: oasis:names:tc:SAML:2.0:metadata" entityID="http://saml.lab.local/adfs/services/trust" EntityID url="http://saml.lab.local/adfs/services/trust">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
  <RoleDescriptor xmlns="urn: oasis:names:open:org:wsfed:federation/2007/06" protocolSupportEnumeration="http://docs.oasis-open.org/ws-trust/2005/02/http://docs.oasis-open.org/ws-fed/federation/2007/06#s1-type=Ted-ApplicationServiceType">
    <RoleDescriptor xmlns="urn: oasis:names:open:org:wsfed:federation/2007/06" protocolSupportEnumeration="http://docs.oasis-open.org/ws-trust/2005/02/http://docs.oasis-open.org/ws-fed/federation/2007/06#s1-type=Ted-SecurityTokenServiceType">
      <KeyDescriptor use="signing">
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <X509Certificate>MIIE2DCCAcAgAwIBAgIQMpbjEXX0LoxUUm/yorLTANBkgkhkIG9wBQAQsfFADoH5YrJAYDVQQDEx1BREZTfNpZ25pbmcgLSbzYW1st.mdhYl5sb2NhbDMeFw0yHDA2HTYwHtU0MjIafw0yHtA2HTYwHtU0MjiaNCpxJAlkBgNVBAM</X509Certificate>
        </KeyInfo>
      </KeyDescriptor>
      <KeyDescriptor use="encryption">
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"/>
        <X509Certificate>MIIE2DCCAcAgAwIBAgIQMpbjEXX0LoxUUm/yorLTANBkgkhkIG9wBQAQsfFADoH5YrJAYDVQQDEx1BREZTfNpZ25pbmcgLSbzYW1st.mdhYl5sb2NhbDMeFw0yHDA2HTYwHtU0MjIafw0yHtA2HTYwHtU0MjiaNCpxJAlkBgNVBAM</X509Certificate>
        </KeyDescriptor>
      <KeyDescriptor use="digest"/>
      <fed:TokenServiceOffered>
        <fed:ClaimTypesOffered>
        <fed:SecurityTokenServiceEndpoint>
          <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
            <localPart>SecurityTokenServiceEndpoint</localPart>
            <address>http://saml.lab.local/adfs/services/trust</address>
          </EndpointReference>
        </fed:SecurityTokenServiceEndpoint>
        <fed:PassiveSecurityTokenEndpoint>
        </fed:PassiveSecurityTokenEndpoint>
      </KeyDescriptor>
      <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
        <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
          <KeyDescriptor use="signing">
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"/>
            <X509Certificate>MIIE2DCCAcAgAwIBAgIQMpbjEXX0LoxUUm/yorLTANBkgkhkIG9wBQAQsfFADoH5YrJAYDVQQDEx1BREZTfNpZ25pbmcgLSbzYW1st.mdhYl5sb2NhbDMeFw0yHDA2HTYwHtU0MjIafw0yHtA2HTYwHtU0MjiaNCpxJAlkBgNVBAM</X509Certificate>
            </KeyInfo>
          </KeyDescriptor>
        </IDPSSODescriptor>
      </SPSSODescriptor>
    </RoleDescriptor>
  </RoleDescriptor>
</EntityDescriptor>

```

## Configuration on the FTD via FMC

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



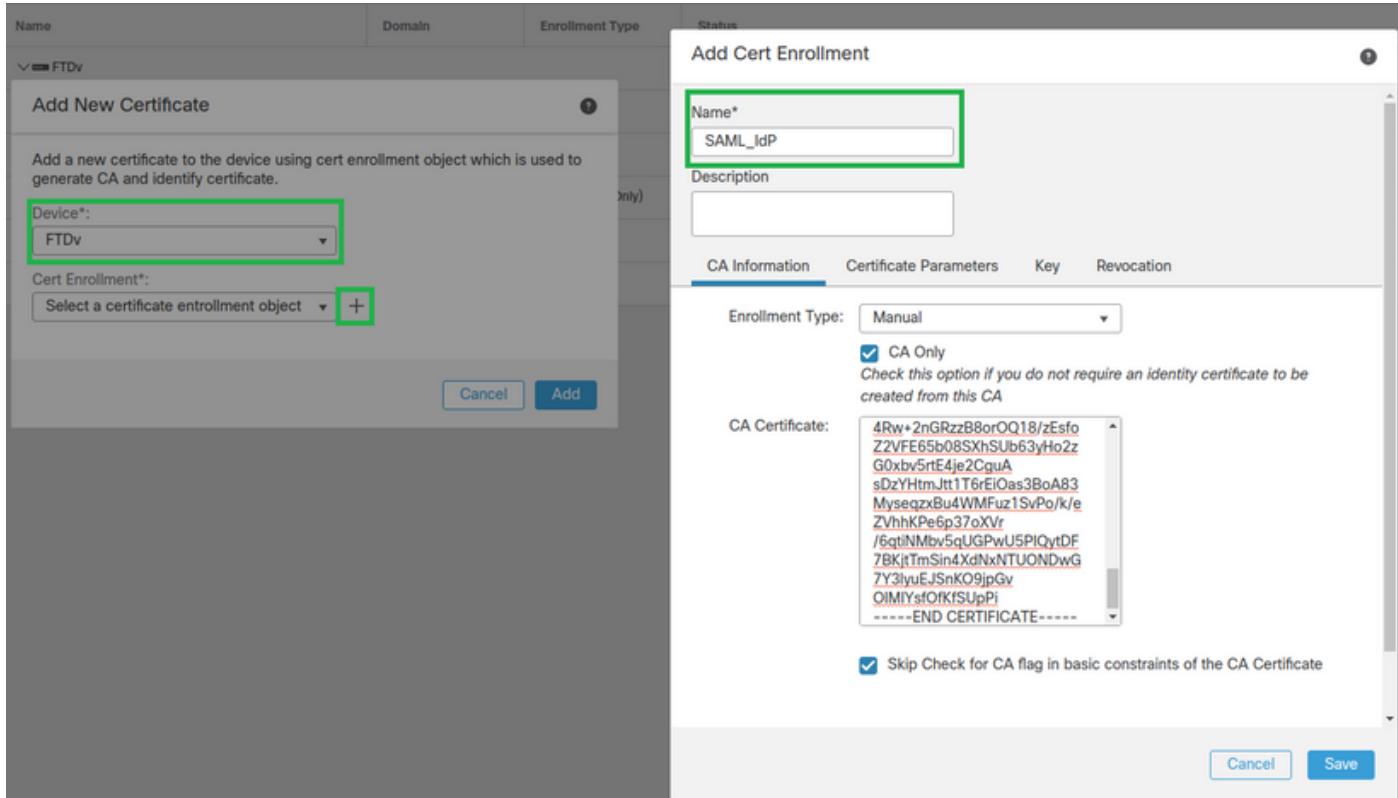
Step 2. Click **Add**. Select the FTD to enroll in this certificate. Under Cert Enrollment, click the plus + sign.

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**.



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**.



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.

## New Single Sign-on Server



Name\*

SAML\_IdP

Identity Provider Entity ID\*

http://saml.lab.local/adfs/services,

SSO URL\*

https://saml.lab.local:444/adfs/ls/

Logout URL

https://saml.lab.local:444/adfs/ls/

Base URL

https://ftd.lab.local

Identity Provider Certificate\*

SAML\_IdP



Service Provider Certificate

SSL\_Wildcard.lab.local



Request Signature

--No Signature--



Request Timeout

Use the timeout set by the provider

seconds (1-7200)

Cancel

Save

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.

The screenshot shows the Firepower Management Center interface. The top navigation bar includes links for Overview, Analysis, Policies, Devices (which is highlighted with a green border), Objects, AMP, and Intelligence. Below the navigation is a search bar and a Deploy button. The main content area displays a table with one row for the connection profile "FTD\_RemoteAccess". The table columns are Name, Status, and Last Modified. The status row contains the text "Targeting 1 devices" and "Up-to-date on all targeted devices". The last modified row shows "2020-11-10 11:49:29" and "Modified by 'admin'". On the far right of the table are three icons: a pencil for editing, a refresh, and a delete.

Name	Status	Last Modified
FTD_RemoteAccess	Targeting 1 devices Up-to-date on all targeted devices	2020-11-10 11:49:29 Modified by "admin"

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

The screenshot shows the configuration page for the "FTD\_RemoteAccess" connection profile. At the top, there are "Save" and "Cancel" buttons. Below them is a "Policy Assignments (1)" section. The main content area has tabs for "Connection Profile" (which is selected and highlighted with a green border), "Access Interfaces", and "Advanced". On the far right of the content area is a green-bordered "+" icon.

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

## Add Connection Profile



Connection Profile:\*

Group Policy:\*  +

[Edit Group Policy](#)

Client Address Assignment    AAA    Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the '*Client Address Assignment Policy*' in the Advanced tab to define the assignment criteria.

Address Pools:



Name	IP Address Range	
VPN_Pool	10.1.1.1-10.1.1.100	VPN_Pool

DHCP Servers:



Name	DHCP Server IP Address	
DHCPServer	192.168.1.41	DHCPServer

[Cancel](#)

[Save](#)

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

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

Connection Profile:\* SAML\_TG

Group Policy:\* SAML\_GP +  
Edit Group Policy

Client Address Assignment AAA Aliases

**Authentication**

Authentication Method: SAML

Authentication Server: SAML\_IdP (SSO)

**Authorization**

Authorization Server:

Allow connection only if user exists in authorization database

**Accounting**

Accounting Server:

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.

Connection Profile:\* SAML\_TG

Group Policy:\* SAML\_GP +

Client Address Assignment AAA Aliases

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Add Alias Name

Name	Status
SAML	

URL Alias:

Configure the list of URL aliases. When user enters one of the following URLs, system will ...

URL

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:

```
<#root>

> 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+H0cOFYwAAAAAAEzANBkqhkiG9w0BAQsF
ADBAMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxEzARBgoJkiaJk/IzZAEZFgNsYWIx
EjAQBgNVBAMTCU1TMjAxMi1DQTAeFw0yMDA0MTEwMTQyMTlaFw0yMjA0MTEwMTQy
MTlaMCMxCzAJBgNVBAYTAkNSMRQwEgYDVQQDDAsqLmxhYi5sb2NhbDCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKfRmbCfwk+V1f+Y1sIE4hyY6+Qr1yKF
g1wEqLOFhtGVM3re/WmFuD+4sCyU1Vkoijhf2+X8tG7x2WTpKKtZM3N7bHpb7oPc
uz8N4GabfAIw287soLM521h6ZM01bWQ0vxXR+xtCAyqz6JJdK0CNjNEdEkYcaG8
PFRFUy31UPmCqQnEy+GYZipErrWTpWwbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMy
EY4F8sdic7bt1QQPKG9JIaWny9RvHBmLgj0px2i5Rp5k1JIECD9kHGj44051BEcv
OFY6ecAPv4CkZB6CloltaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAaOC
AuUwggLhMBYGA1UdEQQPMA2CCyoubGFiLmxvY2FsMB0GA1UdDgQWB0kmTIhXT/
EjkMdpc4aM6PTnyKPzAfBgNVHSMEGDAwBTEPQVWH1Hqxd11VIRYSCSCuHTa4TCB
zQYDVR0fBIHFMICMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049
V010LTVBME5HNDkxQURCLEN0PUNEUCxDTj1QdWJsaWM1MjBLZXk1MjBTZXJ2aN1
cyxDTj1TZXJ2aN1cyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j
ZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNOQ2xhc3M9Y1JMRG1z
dhJpYnV0aW9uUG9pbnQwgbkGCCsGAQUFBwEBBIGsMIGpMGmBgrBqEFBQcwAoA
mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWM1MjBLZXk1MjBT
ZXJ2aN1cyxDTj1TZXJ2aN1cyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s
b2NhbD9jQUN1cnRpZm1jYXR1P2Jhc2U/b2JqZWNOQ2xhc3M9Y2VydG1maWNhdG1v
bkF1dGhcm10eTAOBgNVHQ8BAf8EBAMCBaAwPQYJKwYBBAGCNxUHBDAwLgYmKwYB
BAGCNxUIgYKsboLe0U6B4ZUthLbxToW+yFILh4iaWYXgpQUCAWQCAQMwSwYDVR01
BEQwQgYIKwYBBQUHawEGCCsGAQUFBwMHBgrBqEFBQcDBgYIKwYBBQUIAgIGCCSG
AQUFBwMFBgrBqEFBQcDAgYEVR01ADBfBgkrBqEEAYI3FQoEUjBQMAoGCCsGAQUF
BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAlCMAoGCCsGAQUF
BwMFMAoGCCsGAQUFBwMCAYGBFUdJQAwDQYJKoZIhvcNAQELBQADggEBAKQnqcaU
fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiT
Lmq04X1goaAs6obHrYFtSttz/9X1TAe1KbZ0G1RVg9Lb1PiF17kZAxAJLJH1CTG
5EQSC1YqS31sTuarm4WPDJyMShc6h1UpswnCokGRMMgpx2GmDgv4Zf8SzJJ0NI4y
DgMozuObwkNUXuHbiLuoXwvb2Whm11ysidp1+v9kp1RYamyjFUo+agx0E+L1zp8C
i0YEwYKXgKk3CZdwJfnYQuCwjmapYw1LGt5S59Uwegwro6AsUXY335+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/acs" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ftd/sls" />
</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:

```

<#root>
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  
Audit 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 T0 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 T0 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 T0 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:

```
<#root>

firepower#
show run webvpn

firepower#
show run tunnel-group

firepower#
show crypto ca certificate

firepower#
debug webvpn saml 25
```

---

 **Note:** You can troubleshoot DART from the AnyConnect user PC as well.

---