

# 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 metadata.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.

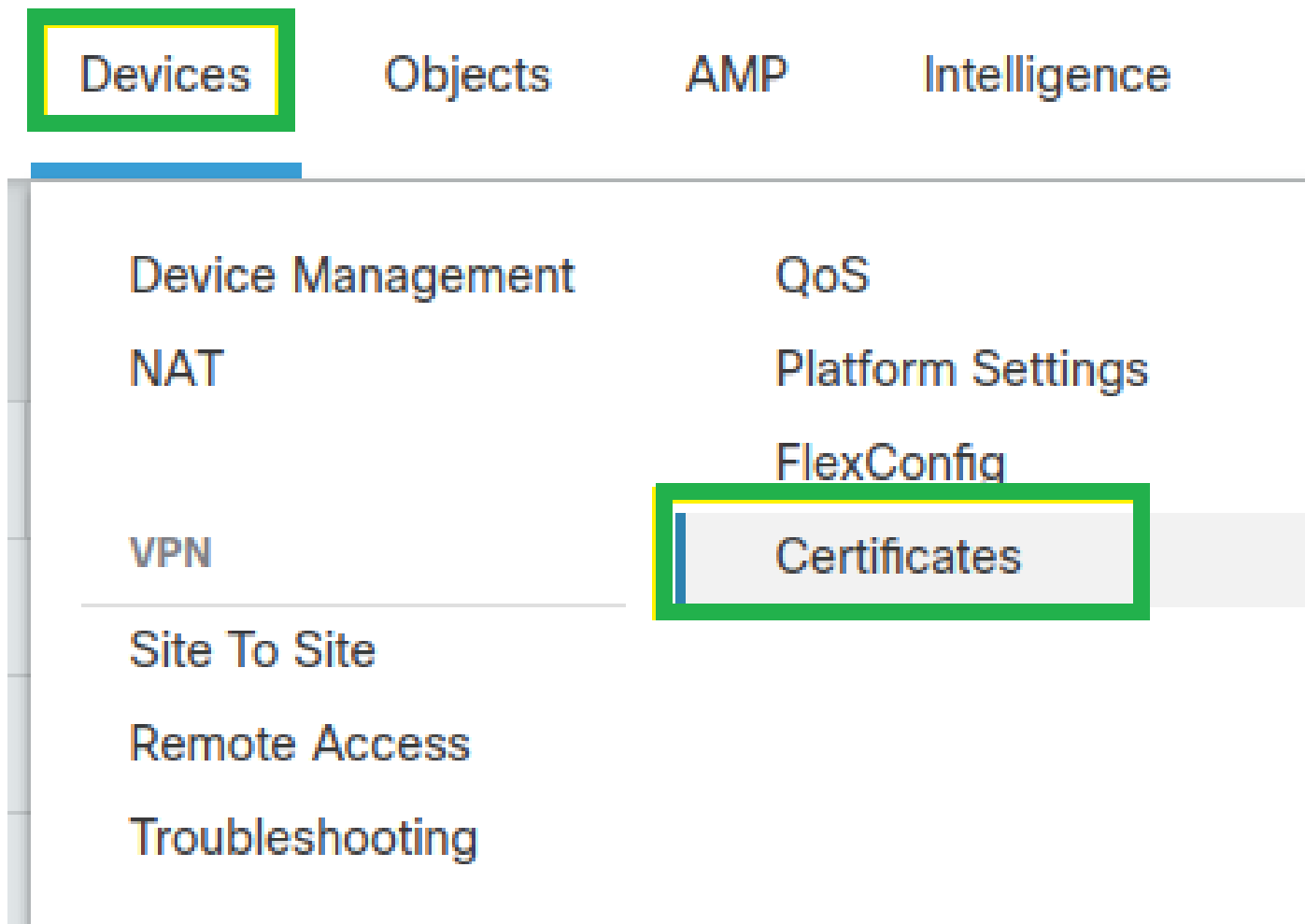
---

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.



## Configuration on the FTD via FMC

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



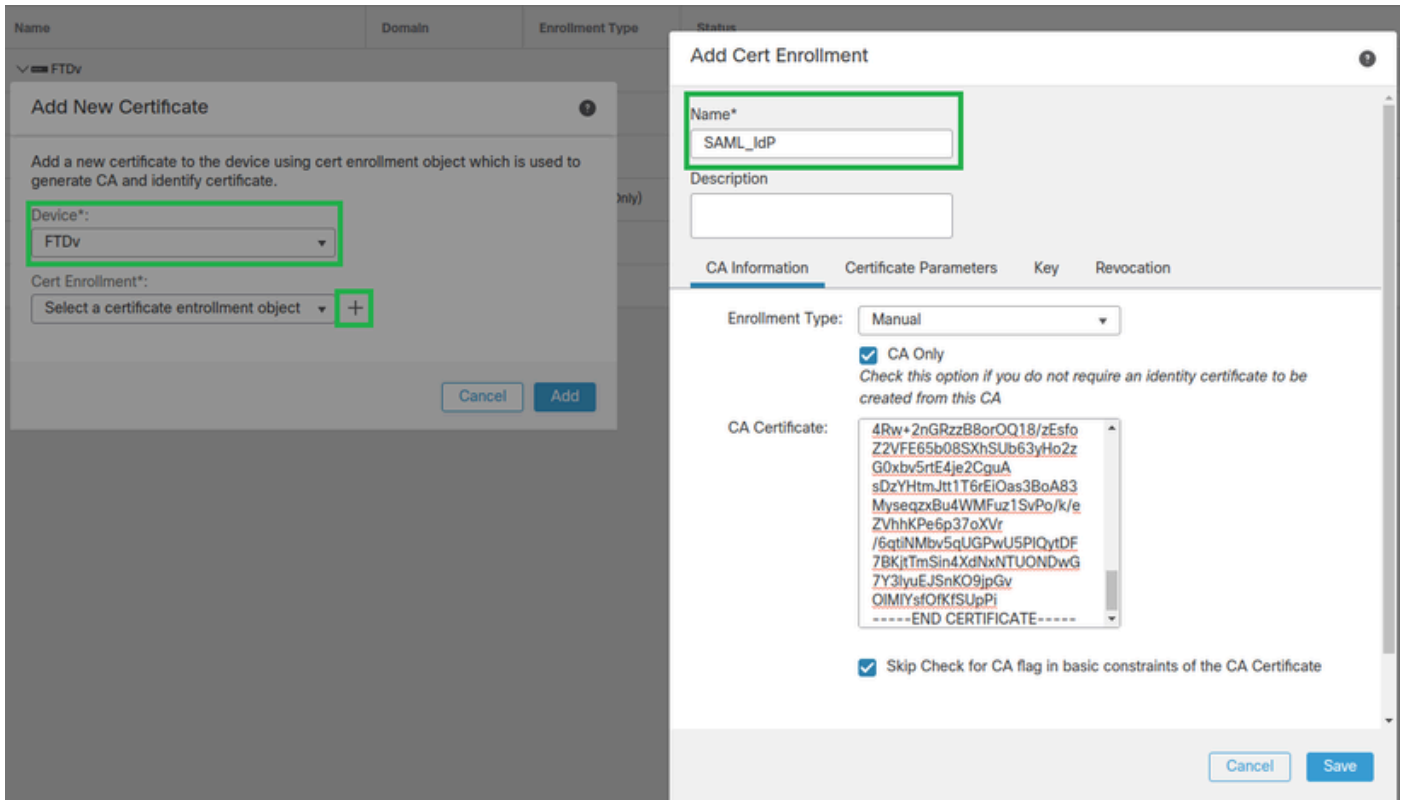
Step 2. Click **Add**. Select the FTD to enroll in this certificate. Under Cert Enrollment, click the plus + sign.

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**, 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\*

Identity Provider Entity ID\*

SSO URL\*

Logout URL

Base URL

Identity Provider Certificate\*



Service Provider Certificate



Request Signature



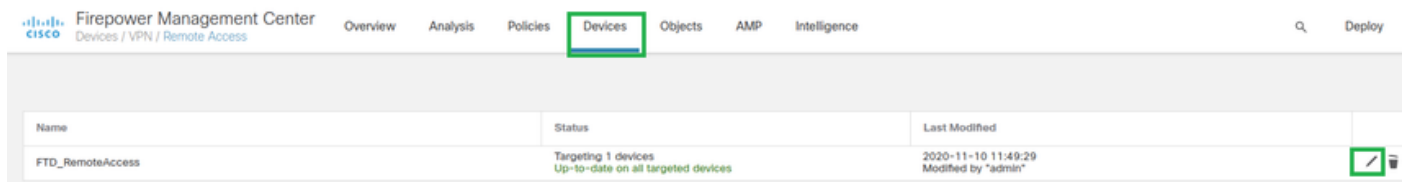
Request Timeout

seconds (1-7200)

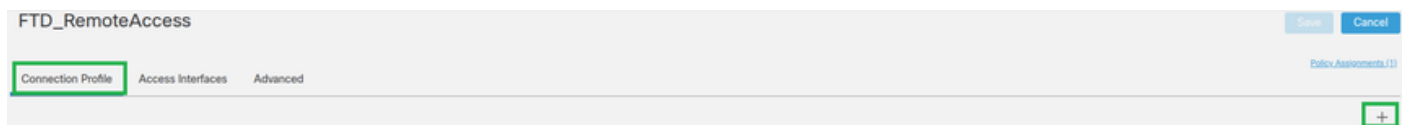
Cancel

Save

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



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



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

## Add Connection Profile



Connection Profile:\* SAML\_TG

Group Policy:\* SAML\_GP +

[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

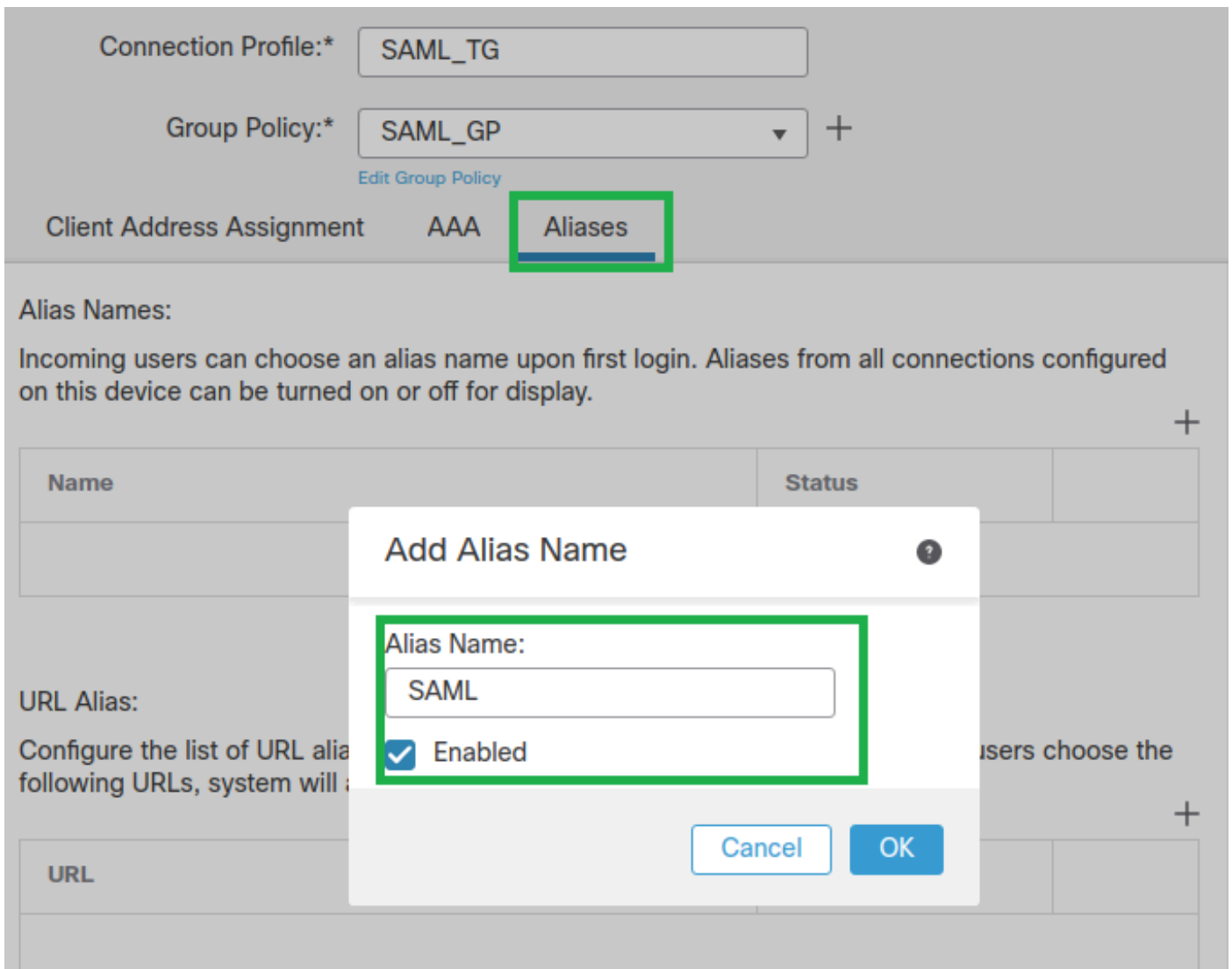
**Accounting**

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.





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:S
```

```

<SPSS0Descriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:ietf:params:xml:sec:profiles:saml:1.0:profiles:browser"
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xm1dsig#">
<ds:X509Data>
<ds:X509Certificate>MIIF1zCCBL+gAwIBAgITYAAAABN6dX+H0cOFYwAAAAAAEzANBgkqhkiG9w0BAQsF
ADBAMRUwEwYKCIImiZPyLQGBGRYfBfG9jYwWxEzARBgoJkiaJk/IsZAEZFgNsYWIx
EjAQBgNVBAMTCU1TMjAxMi1DQTAeFw0yMDA0MTEwMTQyMT1aFw0yMjA0MTEwMTQy
MT1aMCMxCzAJBgNVBAYTAkNSMRQwEgYDVQDDAsqLmXhYi5sb2NhbDCCASiWDQYJ
KoZIHvcNAQEBBQADggEPADCCAQoCggEBAKfRmbCfWk+V1f+Y1sIE4hyY6+Qr1yKf
g1wEqL0FHtGVM3re/WmFuD+4sCyU1Vkoijhf2+X8tG7x2WTPKktZM3N7bHpb7oPc
uz8N4GabfAIw287soLM521h6ZM01bWGQ0vxXR+xtCAyqz6JJdK0CNjNEdEkYcaG8
PFRFuy31UPmCqQnEy+GYZipErrWtPwWbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMy
EY4F8sdiC7bt1QQPKG9JIaWny9RvHBmLgj0px2i5Rp5k1JIECD9kHGj44051BEcv
OFY6ecAPv4CkZB6C1oftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC
AuUwggLhMBYGA1UdEQPMA2CCyoubGFilmxvY2FsMB0GA1UdDgQWBRR0kmTIhXT/
EjkMdpC4aM6PTnyKpZafBgNVHSMEGDAWgBTEPQVWH1Hqxd11VIRYSCSCuHTa4TCB
zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049
V010LTVBME5HNDkxQRULENOPUNEUCxDTj1QdWJsaWMTMjBLZXk1MjBTZXJ2aWN1
cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j
ZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNOQ2xhc3M9Y1JMRG1z
dHJpYnV0aW9uUG9pbmQwgbkGCCsGAQUFBwEBBIBGMIgPmIGmBgggrBgEFBQcwAoaB
mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWMTMjBLZXk1MjBT
ZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s
b2NhbD9jQU1cnRpb25MaXN0P2Jhc2U/b2JqZWNOQ2xhc3M9Y2VydG1maWNhdG1v
bkF1dGhvcml0eTA0BgNVHQ8BAf8EBAMCBaAwPQYJKwYBBAGCNxUHBDALgYmKwYB
BAGCNxUIgYKsboLe0U6B4ZUthLbxToW+yFILh4iaWYXgpQUCAWQCAQMwSwYDVR01
BEQwQgYIKwYBBQUHAWEGCCsGAQUFBwMHBgggrBgEFBQcDBGyIKwYBBQUIAgIGCCsG
AQUFBwMFBgggrBgEFBQcDAgYEVR01ADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUF
BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUF
BwMFMAoGCCsGAQUFBwMCMAYGBFUdJQAwdQYJKoZIhvcNAQELBQADggEBAKQnqcaU
fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V
Lmq04X1goaAs6obHrYftSttz/9X1TAe1KbZ0G1RVg9Lb1PiF17kZAxALjLJH1CTG
5EQSC1YqS31sTuarm4WPDJyMShc6h1UpswnCokGRMMgpx2GmDgv4Zf8SzJJ0NI4y
DgMozuObwkNUXuHbiLuoXwvb2Whm11ysidp1+V9kp1RYamyjFUo+agx0E+L1zp8C
i0YEwYKXgKk3CZdwJfnYQuCWjmapYw1LGt5S59Uwegwro6AsUXY335+Z0rY/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
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ftd
</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  
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:

```
<#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.

---