FMCで管理されるFTDでのSAML認証を使用したAnyconnectの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[コンフィギュレーション](#)
[SAML IdPパラメータの取得](#)
[FMCによるFTDの設定](#)
[確認](#)
[トラブルシュート](#)

概要

この文書は次のことについて記述しています **Security Assertion Markup Language (SAML)** fmcを介して管理されるFTDの認証。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- **AnyConnect** FMCでの設定
- SAMLおよびmetatada.xml値

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

> **注：**可能であれば、NTPサーバを使用してFTDとIdPの間で時刻を同期します。それ以外の場合は、時刻が手動で同期されていることを確認します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

この設定により、AnyconnectユーザはSAML Identity Service ProviderとのVPNセッション認証を確立できます。

SAMLの現在の制限事項には、次のようなものがあります。

- FTDのSAMLは、認証（バージョン6.7以降）と認可（バージョン7.0以降）でサポートされています。
- DAP評価で使用可能なSAML認証属性（SAML Authentication Attributeと類似） **RADIUS** 送信された属性 **RADIUS** AAAサーバからの許可応答)はサポートされていません。
- ASAは、DAPポリシーでSAML対応のトンネルグループをサポートします。ただし、username属性はSAML IDプロバイダーによってマスクされるため、SAML認証でusername属性を確認することはできません。

- CA は自分の証明書に署名するので、CA 管理者に連絡し、 **AnyConnect** 組み込みブラウザでは、VPNが試行されるたびに新しいブラウザセッションが使用されるため、IdPがHTTPセッションCookieを使用してログイン状態を追跡する場合、ユーザは毎回再認証を行う必要があります。
- この場合、 **Force Re-Authentication** 設定 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** ～に影響を及ぼさない **AnyConnect** SAML認証を開始しました。

その他の制限またはSAMLについては、ここに記載されているリンクを参照してください。

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

ASAおよびFTDには次の制限事項があります。「」**Guidelines and Limitations for SAML 2.0**「」

> **注**：FTDに実装されるすべてのSAML設定は、IdPによって提供されるmetadata.xmlファイルにあります。

コンフィギュレーション

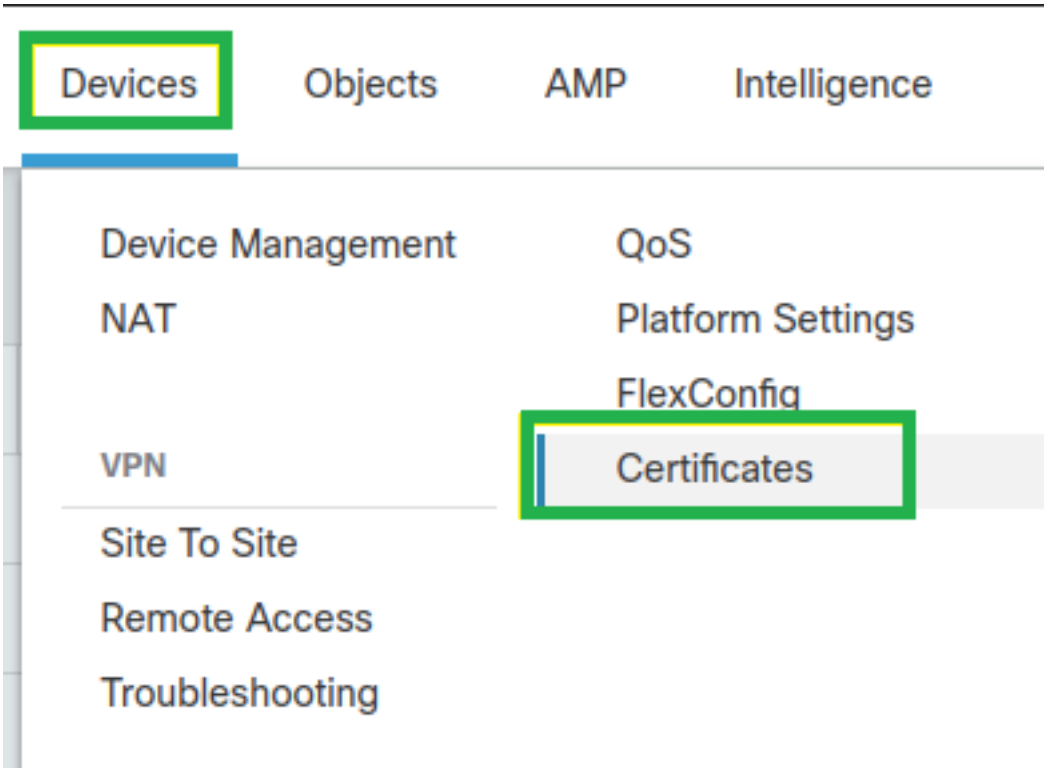
このセクションでは、WLCを設定するための **AnyConnect** FTDでのSAML認証を使用する場合

SAML IdPパラメータの取得

次の図に、SAML IdP metadata.xmlファイルを示します。この出力から、 **AnyConnect** samlのプロファイル：

FMCによるFTDの設定

ステップ1:FMCにIdP証明書をインストールして登録します。移動先 **Devices > Certificates**



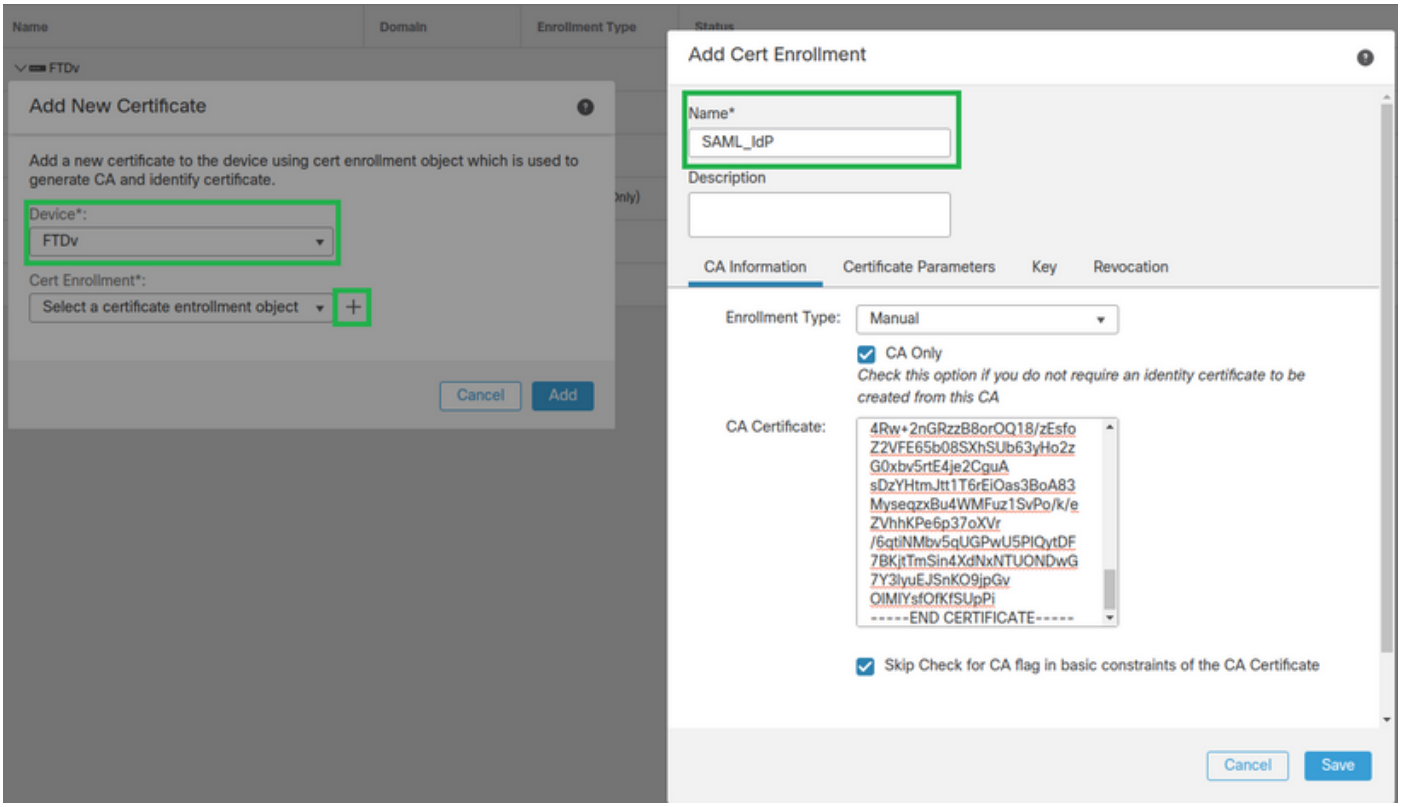
ステップ2:[Click] **Add.**この証明書に登録するFTDを選択します。[Cert Enrollment]で、プラス記号(+) をクリックします

内 **Add Cert Enrollment** IdP証明書のラベルとして任意の名前を使用します。クリック **Manual.**

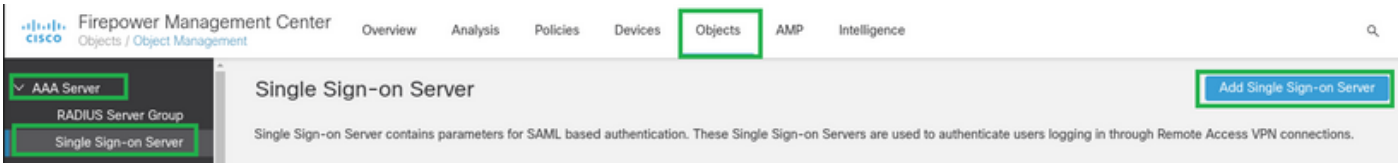
次を確認します。 **CA Only** と **Skip Check** CAフラグフィールドの場合。

貼り付け **base64** format IdP CA cert

クリック **Save** 次に、 **Add.**

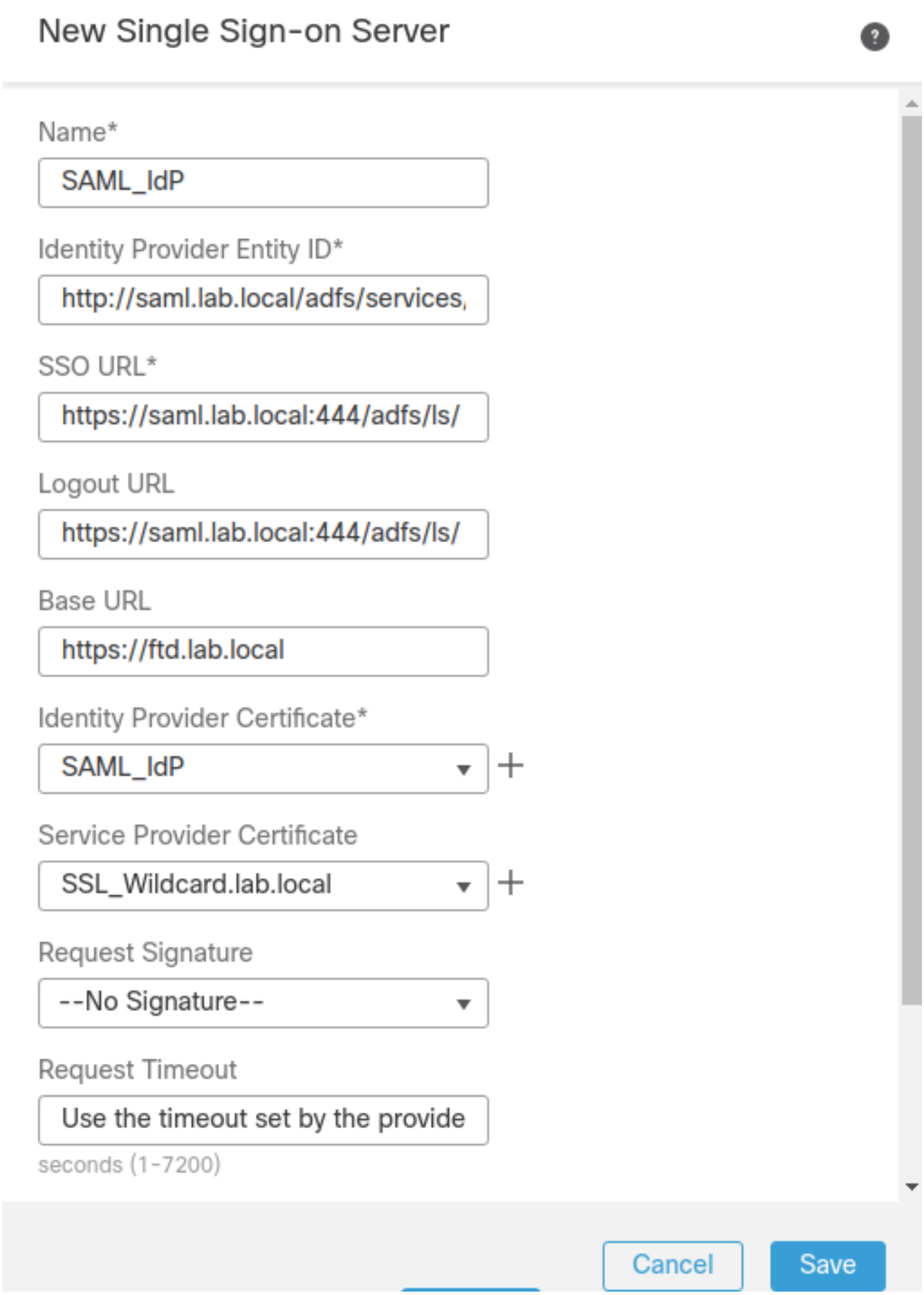


ステップ3:SAMLサーバの設定を行います。移動先 **Objects > Object Management > AAA Servers > Single Sign-on Server**.次に、 **Add Single Sign-on Server**.

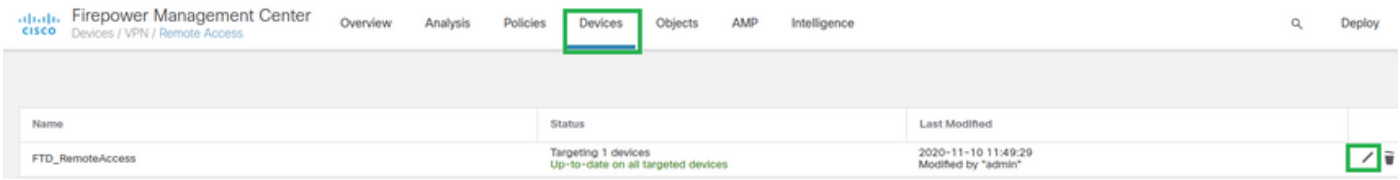


ステップ4:次に基づく **metadata.xml** ファイルはIdPによってすでに提供されています。 **New Single Sign-on Server**.

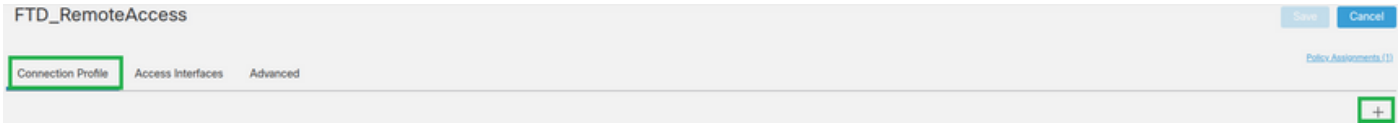
```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.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



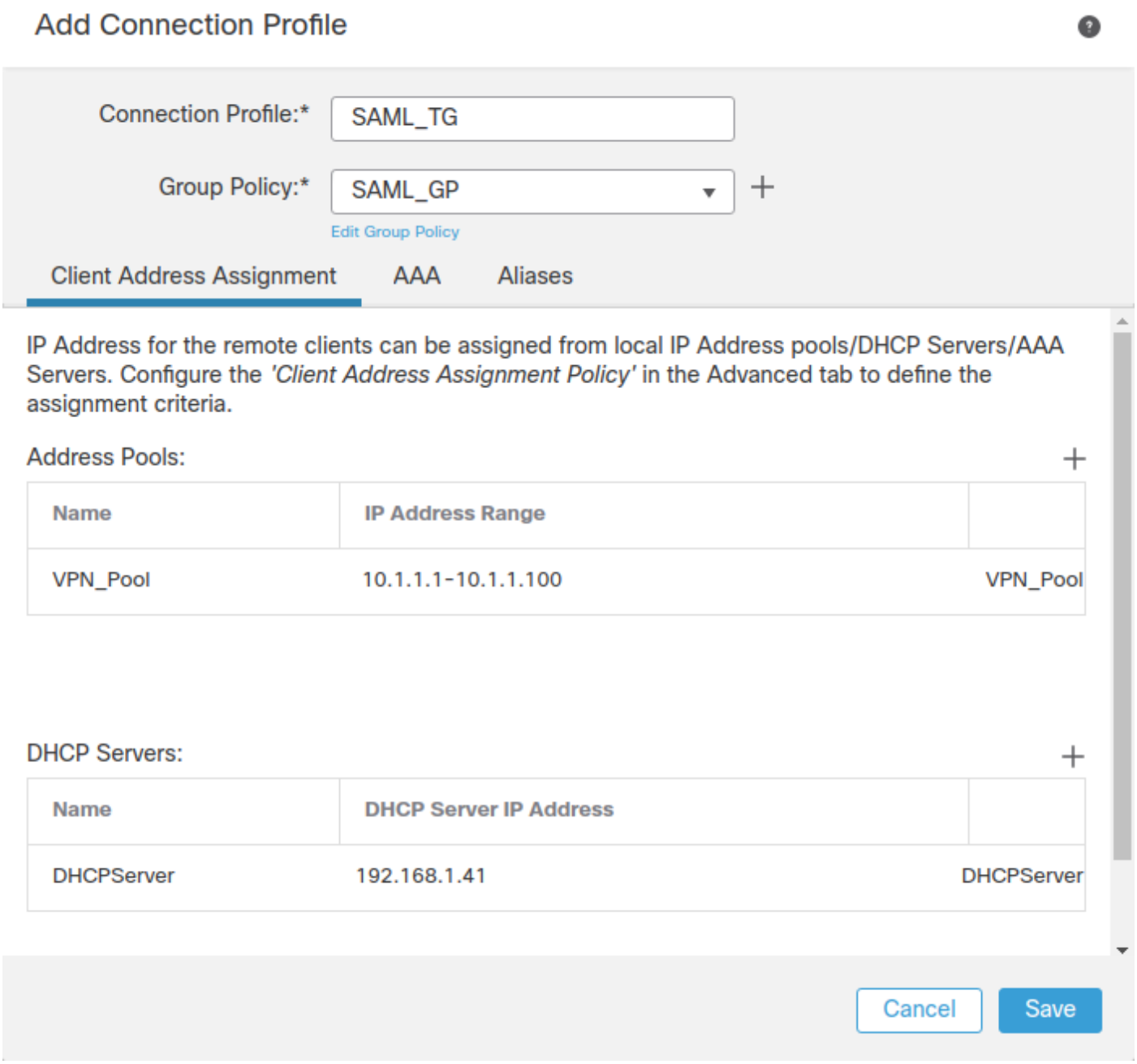
ステップ5:設定 **Connection Profile** この認証方式を使用します。移動先 **Devices > Remote Access** 現在の設定を編集します **VPN Remote Access** ありません。



ステップ6:プラス記号(+)をクリックし、**別の**記号を追加します。 **Connection Profile.**

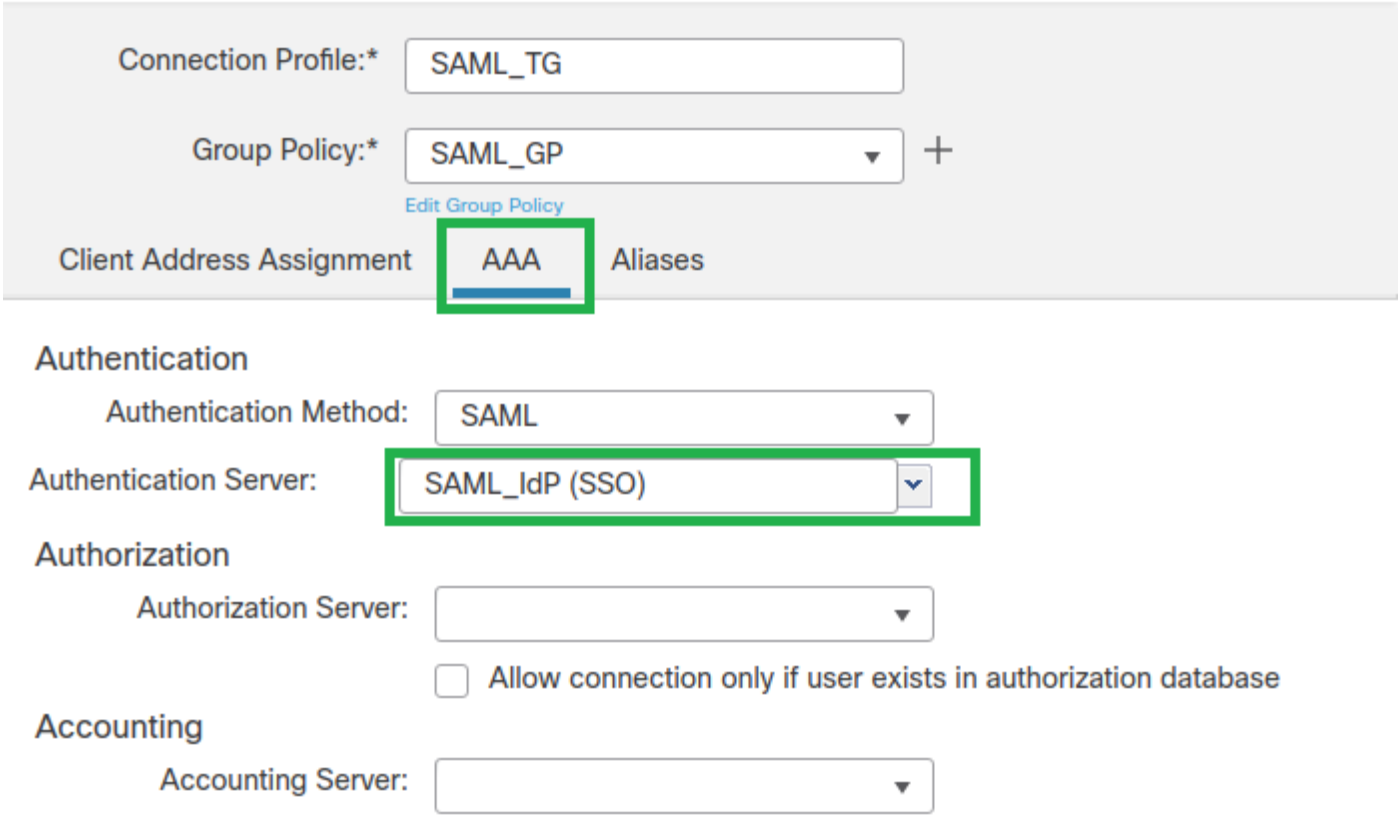


ステップ7：新しいVLANを **Connection Profile** 適切なVPNを追加します **Pool**、またはDHCPサーバ。



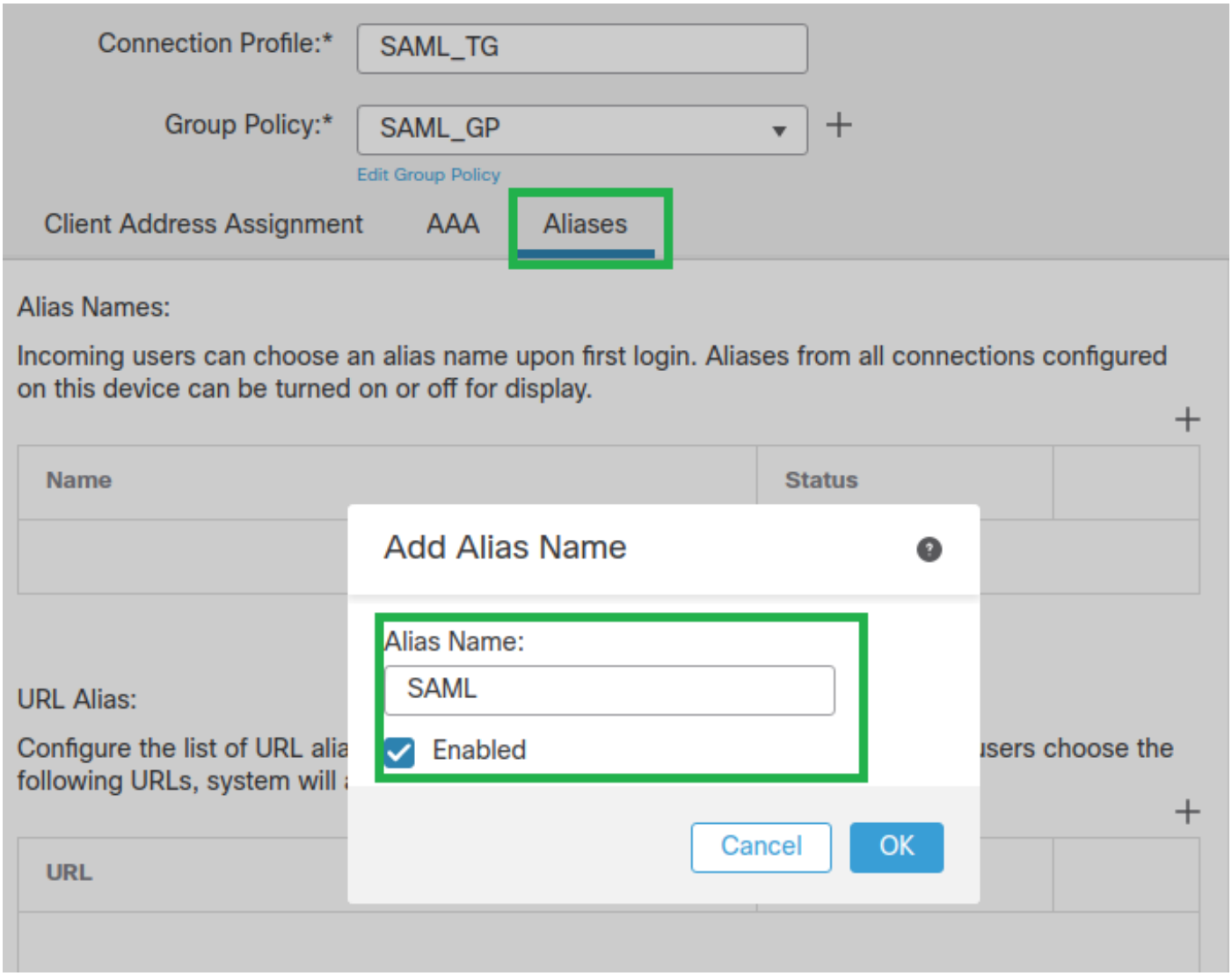
ステップ8:[AAA]タブを選択します。下 **Authentication Method** [SAML]を選択します。

下 **Authentication Server** オプションで、手順4で作成したSAMLオブジェクトを選択します。



手順9：接続をこここにマッピングするためのグループエイリアスを作成します **Connection Profile**.これは、ユーザが **AnyConnect** [ソフトウェア]ドロップダウンメニュー

これが設定されたら、[OK]をクリックして完了を保存します **SAML Authentication VPN** ありません。



ステップ10:次に移動 **Deploy > Deployment** 適切なFTDを選択して、 **SAML Authentication VPN** 保存します。

ステップ11:FTDの提供 **metadata.xml** ファイルを**IdP**に保存し、FTDを信頼できるデバイスとして追加します。

FTD CLIで、次のコマンドを実行します **show saml metadata SAML_TG** ここで、SAML_TGは **Connection Profile** ステップ7で作成します。

予想される出力を次に示します。

```
> 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>
```

その後 **metadata.xml** ftdからIdPに提供され、信頼できるデバイスとしてVPN接続の下でテストを実行できます。

確認

次のことを確認します。 **VPN AnyConnect** 次に示すコマンドを使用して、SAMLを認証方式として接続が確立されました。

```
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 : c0a801090000040005faad9a1
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
```

トラブルシュート

FTD CLIの一部の検証コマンドを使用して、SAMLおよびSAML **Remote Access VPN** ブラケットに表示される接続：

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

注：トラブルシューティングが可能 **DART AnyConnect** ユーザPCも同様です

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。