

# FTD、ISE、DUO、およびActive Directoryを介したSSL VPN認証の設定

## 内容

---

[はじめに](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[FTD設定。](#)

[Firepower Management Center\(FMC\)内でのRADIUSサーバの統合  
リモートVPNを設定します。](#)

[ISE設定。](#)

[DUOを外部RADIUSサーバとして統合します。  
FTDをネットワークアクセスデバイスとして統合します。](#)

[DUO構成。](#)

[DUOプロキシインストール。  
DUOプロキシをISEおよびDUOクラウドと統合します。  
DUOをActive Directoryと統合します。  
DUO Cloud経由でActive Directory\(AD\)からユーザーアカウントをエクスポートします。  
Cisco DUO Cloudにユーザを登録します。](#)

[設定検証手順。](#)

[一般的な問題。](#)

[正常動作シナリオ。](#)

[Error11353外部RADIUSサーバはなし。フェールオーバーを実行できない  
RADIUSセッションはISEライブログに表示されません。  
その他のトラブルシューティング。](#)

---

## はじめに

このドキュメントでは、Cisco ISEとAAA用のDUOセキュリティを使用したFirepower Threat DefenseでのSSLVPNの統合について説明します。

## 要件

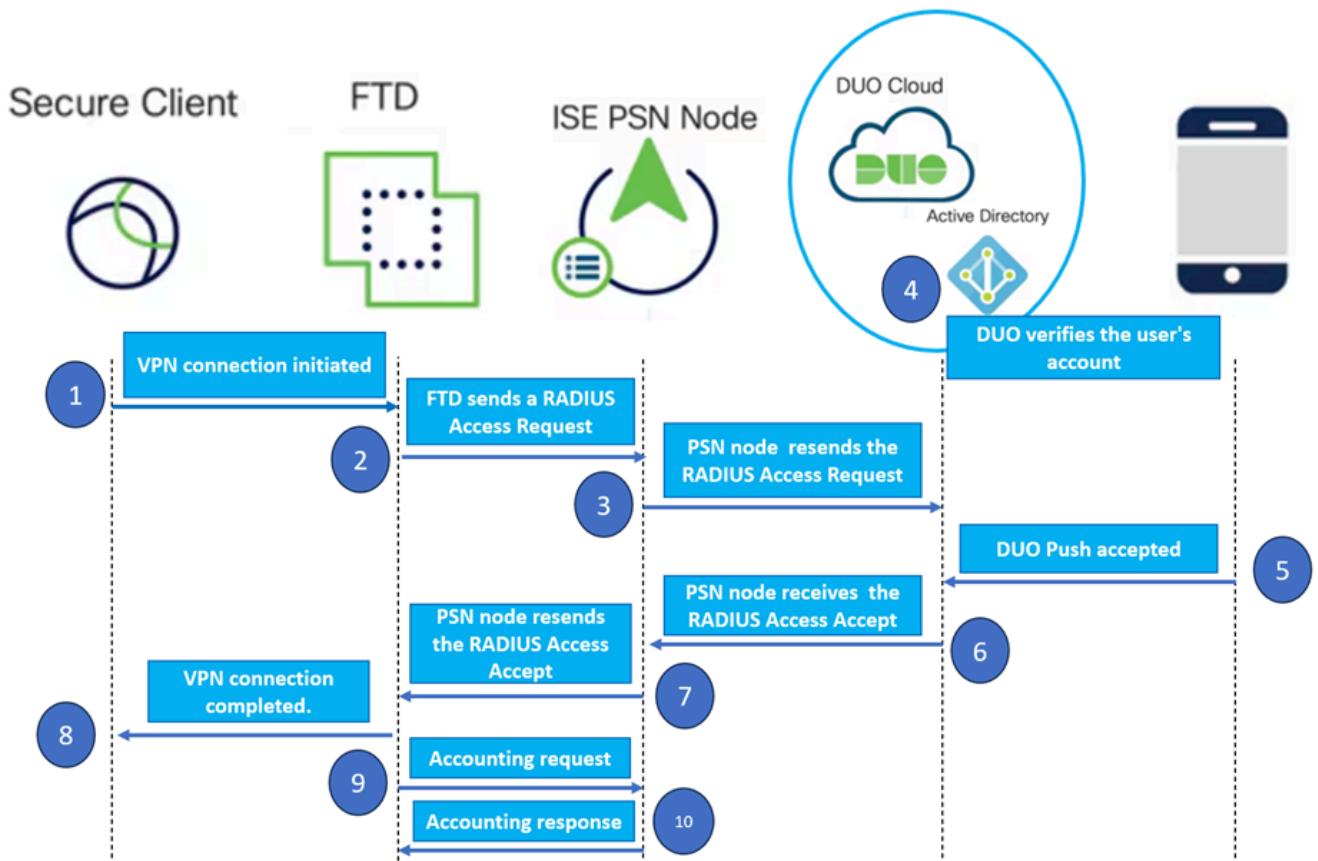
- ISE 3.0以降。
- FMC 7.0以降。
- FTD 7.0以降。
- DUO認証プロキシ。
- ISE Essentialsライセンス
- DUO Essentialsライセンス。

# 使用するコンポーネント

- ISE 3.2 パッチ 3
- FMC 7.2.5
- FTD7.2.5
- プロキシDUO 6.3.0
- Any Connect 4.10.08029

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、クリアな（デフォルト）設定で作業を開始しています。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。

## ネットワーク図



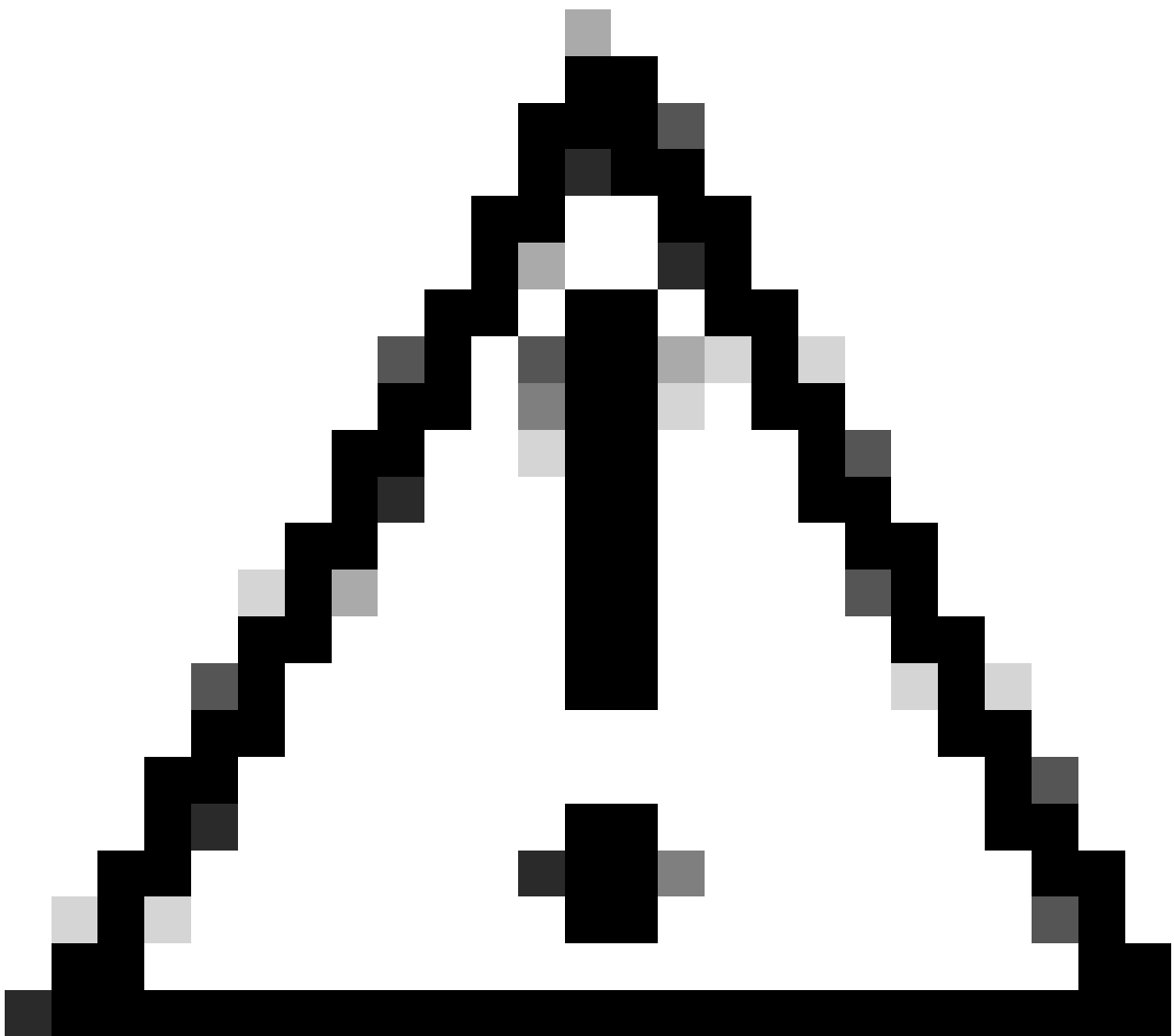
[Topology] :

提案するソリューションでは、Cisco ISEは重要なRADIUSサーバプロキシです。認証ポリシーまたは認可ポリシーを直接評価するのではなく、RADIUSパケットをFTDからDUO認証プロキシに転送するようにISEを設定します。

DUO認証プロキシは、この認証フロー内で専用の仲介者として動作します。Windowsサーバにインストールすることで、Cisco ISEとDUOクラウド間のギャップを埋めます。プロキシの主な機能は、RADIUSパケット内にカプセル化された認証要求をDUOクラウドに送信することです。DUO Cloudは、2要素認証設定に基づいて最終的にネットワークアクセスを許可または拒否しま

す。

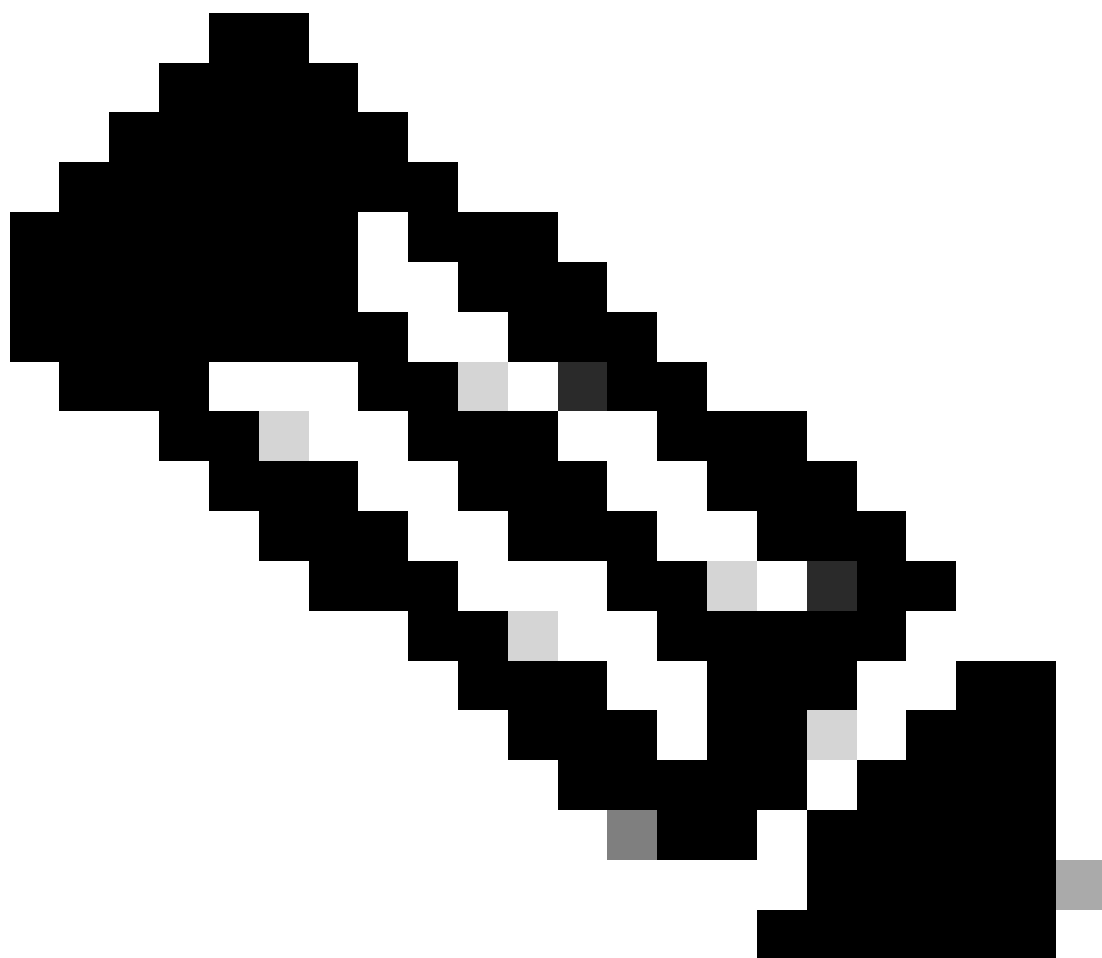
1. ユーザは、一意のユーザ名とパスワードを入力してVPN認証プロセスを開始します。
2. ファイアウォール脅威対策(FTD)が、認証要求をCisco Identity Services Engine(ISE)に送信します。
3. Policy Services Node (PSN)は、認証要求をDUO認証プロキシサーバに転送します。その後、DUO認証サーバはDUOクラウドサービスを介して資格情報を検証します。
4. DUO Cloudは、同期データベースに対してユーザー名とパスワードを検証します。



注意： DUOクラウドで最新のユーザーデータベースを維持するには、DUOクラウドと組織のActive Directory間の同期がアクティブになっている必要があります。

5. DUOクラウドは、認証に成功すると、セキュアで暗号化されたプッシュ通知を通じて、ユーザーが登録したモバイルデバイスへのDUOプッシュを開始します。ユーザーはDUOプッシュを承認して身元を確認し、続行する必要があります。

6. ユーザーがDUOプッシュを承認すると、DUO認証プロキシ・サーバーは、ユーザーが認証要求を受け入れたことを示す確認をPSNに送信します。
7. PSNノードは、ユーザが認証されたことを通知する確認をFTDに送信します。
8. FTDは認証確認を受信し、適切なセキュリティ対策が実施されているエンドポイントへのVPN接続を確立します。
9. FTDは、正常なVPN接続の詳細をログに記録し、記録と監査の目的でアカウントティングデータをISEノードに安全に送信します。
10. ISEノードは、アカウントティング情報を自身のライフログに記録し、すべてのレコードが安全に保存され、将来の監査またはコンプライアンスチェックのためにアクセスできることを確認します。



注：

このガイドの設定では、次のネットワークパラメータを使用します。

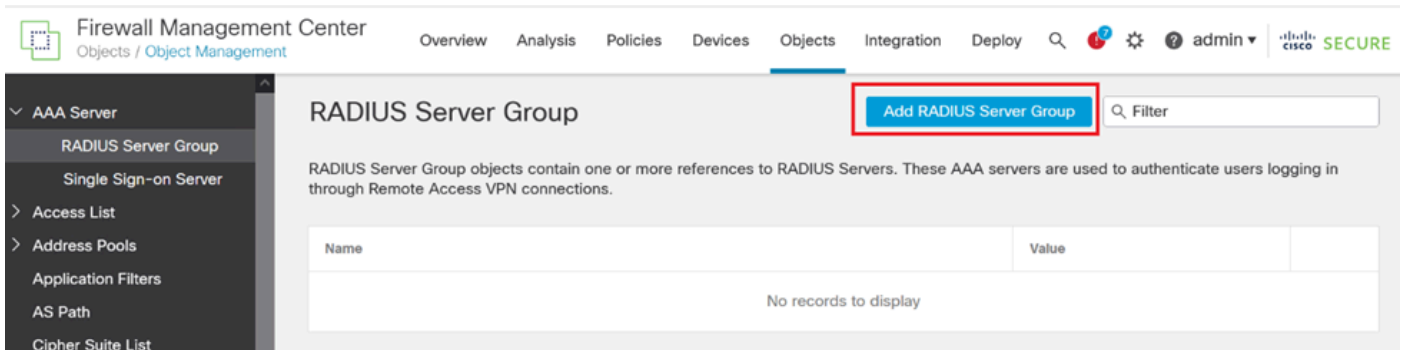
- プライマリネットワークサーバ(PNS)ノードIP:10.4.23.21
- ピアVPNのFirepower Threat Defense(FTD)IP:10.4.23.53
- DUO認証プロキシIP: 10.31.126.207
- ドメイン名 : testlab.local

## コンフィギュレーション

FTD設定。

Firepower Management Center(FMC)内でのRADIUSサーバの統合

1. Webブラウザを起動し、FMCのIPアドレスを入力してグラフィカルユーザインターフェイス(GUI)を開き、FMCにアクセスします。
2. Objectsメニューに移動し、AAA Serverを選択してから、RADIUS Server Groupオプションに進みます。
3. Add RADIUS Server Groupボタンをクリックして、RADIUSサーバーの新しいグループを作成します。



RADIUSサーバグループ。

4. ネットワークインフラストラクチャ内で明確に識別できるように、新しいAAA RADIUSサーバグループの内容を表す名前を入力します。
5. グループ設定で適切なオプションを選択して、新しいRADIUSサーバの追加に進みます。

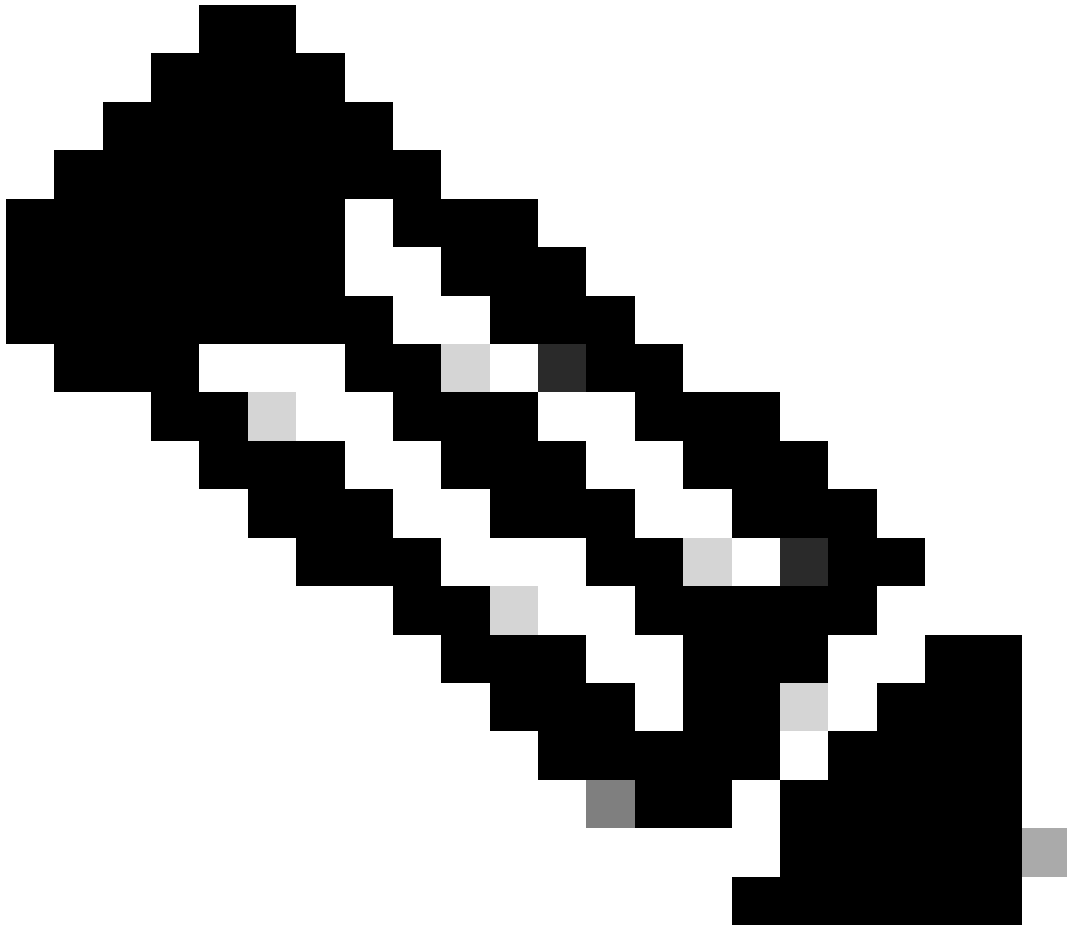
RADIUS Servers (Maximum 16 servers)

IP Address/Hostname	
No records to display	

RADIUSサーバ。

6. RADIUSサーバーのIPアドレスを指定し、共有秘密キーを入力します。

---



注:正常なRADIUS接続を確立するには、この秘密キーがISEサーバと安全に共有されるようにすることが不可欠です。

---

## New RADIUS Server



IP Address/Hostname:\*

10.4.23.21

*Configure DNS at Threat Defense Platform Settings to resolve hostname*

Authentication Port:\* (1-65535)

1812

Key:\*

●●●●●●●●

Confirm Key:\*

●●●●●●●●

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing  Specific Interface



Cancel

Save

新しいRADIUSサーバ。

7. RADIUSサーバの詳細を設定した後、SaveをクリックしてRADIUSサーバグループの設定を保存します。

## Add RADIUS Server Group



Enable authorize only

Enable interim account update

Interval:\* (1-120) hours

24

Enable dynamic authorization

Port:\* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

10.4.23.21



Cancel

Save

サーバグループの詳細。

8. ネットワーク全体でAAAサーバの設定を完了して実装するには、Deployメニューに移動し、Deploy Allを選択して設定を適用します。

Firewall Management Center  
Objects / Object Management

Overview Analysis Policies Devices Objects Integration **Deploy** admin

AAA Server  
RADIUS Server Group  
Single Sign-on Server  
Access List  
Address Pools  
Application Filters  
AS Path

RADIUS Server Group  
RADIUS Server Group objects contain one or through Remote Access VPN connections.

Name  
ISE

Advanced Deploy **Deploy All**

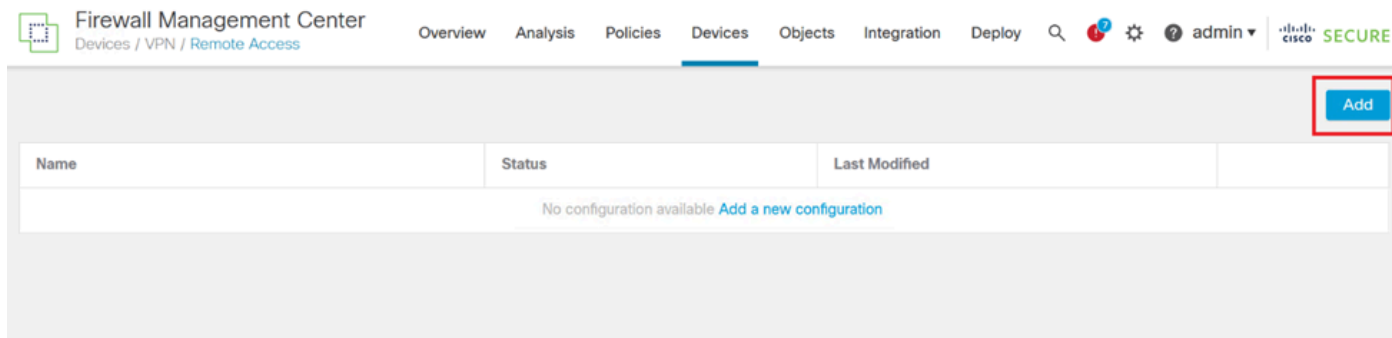
FTD\_01 Ready for Deployment

AAAサーバの導入

リモートVPNを設定します。

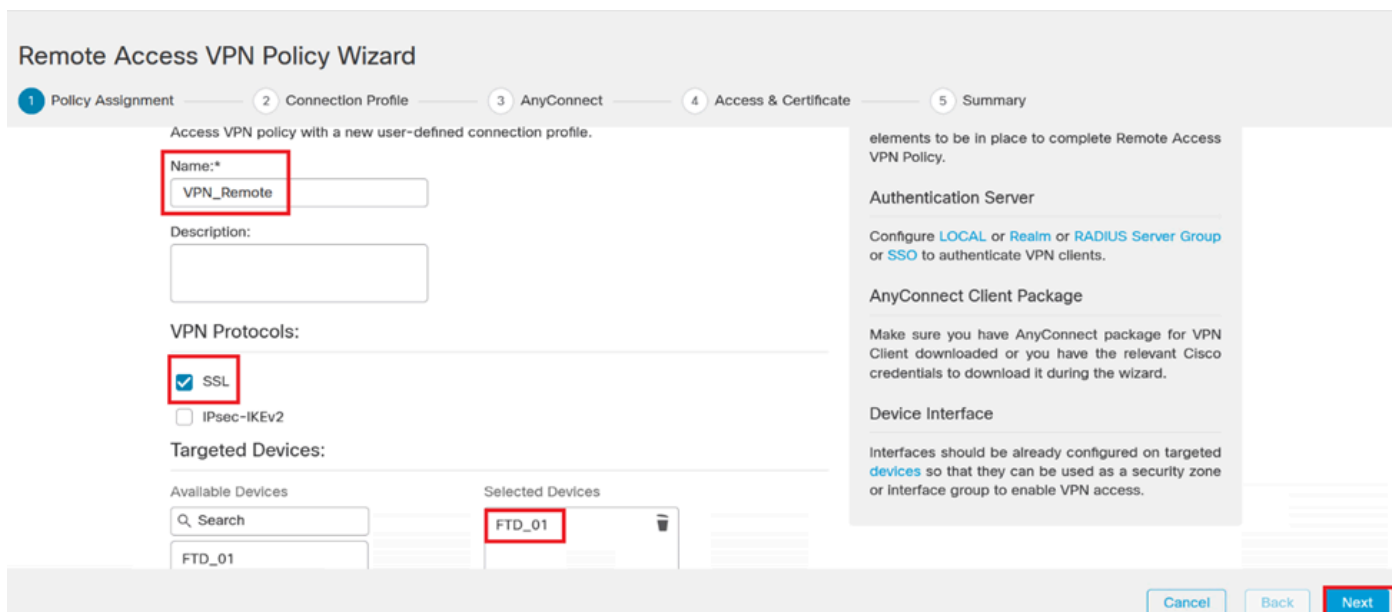


1. FMC GUIでDevices > VPN > Remote Accessの順に移動し、VPN設定プロセスを開始します。
2. Addボタンをクリックして、新しいVPN接続プロファイルを作成します。



VPN接続プロファイル。

3. ネットワーク設定内でVPNを識別しやすくするために、VPNの一意で説明的な名前を入力します。
4. SSL VPNプロトコルを使用して安全な接続を確保するには、SSLオプションを選択します。
5. デバイスのリストから、特定のFTDデバイスを選択します。



VPN設定。

6. 認証設定でPSNノードを使用するようにAAA方式を設定します。

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

### Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: **AAA Only** ▼

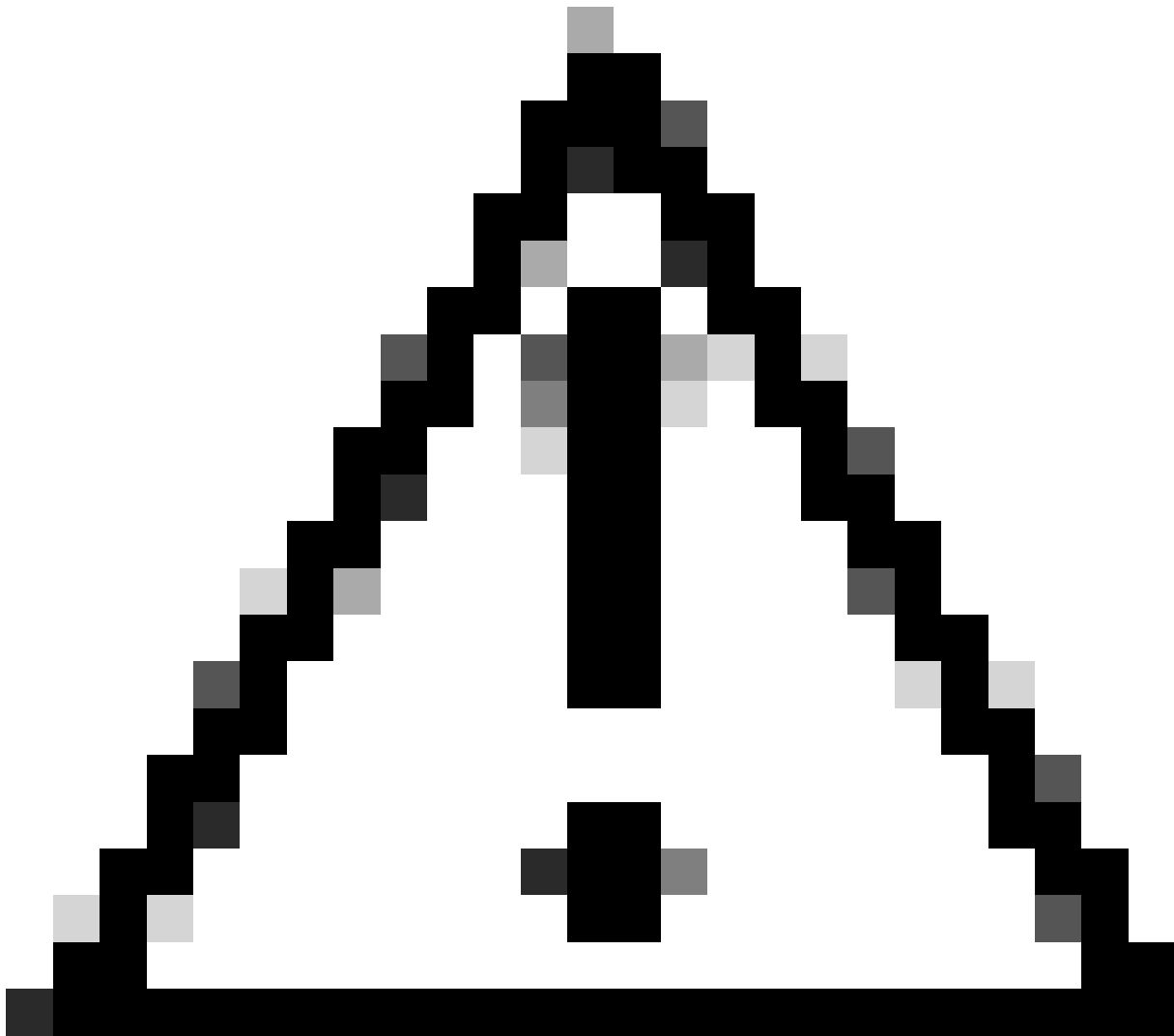
Authentication Server:\* **ISE** ▼ +  
(LOCAL or Realm or RADIUS)  
 Fallback to LOCAL Authentication

Authorization Server: **Use same authentication server** ▼ +  
(realm or RADIUS)

Accounting Server: **ISE** ▼ +  
(RADIUS)

接続プロファイル。

7. VPNの動的IPアドレス割り当てをセットアップします。



注意：たとえば、DHCP VPNプールが選択されています。

#### Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:  ⓘ

IPv6 Address Pools:  ⓘ

IPアドレスプール。

8. 新しいグループポリシーの作成に進みます。

## Group Policy:

---

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:\*  

[Edit Group Policy](#)

グループ ポリシー。

9. グループポリシー設定で、SSLプロトコルが選択されていることを確認します。

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

### VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

VPN プロトコル.

10. 新しいVPNプールを作成するか、既存のプールを選択して、VPNクライアントで使用できるIPアドレスの範囲を定義します。

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:



Name

IP Address Range

Name	IP Address Range

Cancel

Save

プールVPN。

11. VPN接続のDNSサーバーの詳細を指定します。

## Add Group Policy



Name:\*

VPN\_Remote\_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server:

+

Secondary DNS Server:

+

Primary WINS Server:

+

Secondary WINS Server:

+

DHCP Network Scope:

+

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel

Save

DNS設定。



警告：この設定では、バナー、スプリットトンネリング、AnyConnect、拡張オプションなどの追加機能はオプションと見なされることに注意してください。

---

12. 必要な詳細を設定したら、Nextをクリックしてセットアップの次のフェーズに進みます。



## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:\*

[Edit Group Policy](#)

Cancel

Back

Next

グループ ポリシー。

13. VPNユーザ用の適切なAnyConnectパッケージを選択します。必要なパッケージがリストされていない場合は、この段階で必要なパッケージを追加できます。

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Select at least one AnyConnect Client image

[Show Re-order buttons](#)

+

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect-win-4.10.08029-we...	anyconnect-win-4.10.08029-webdeploy-k9...	Windows

Cancel

Back

Next

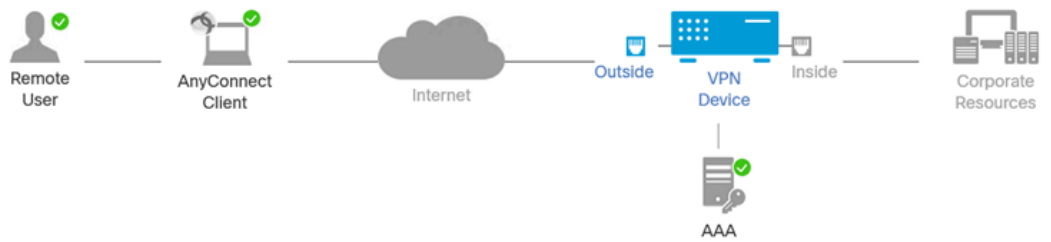
パッケージのインストール

14. VPNリモート機能を有効にするFTDデバイスのネットワークインターフェイスを選択します

。

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary



### Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

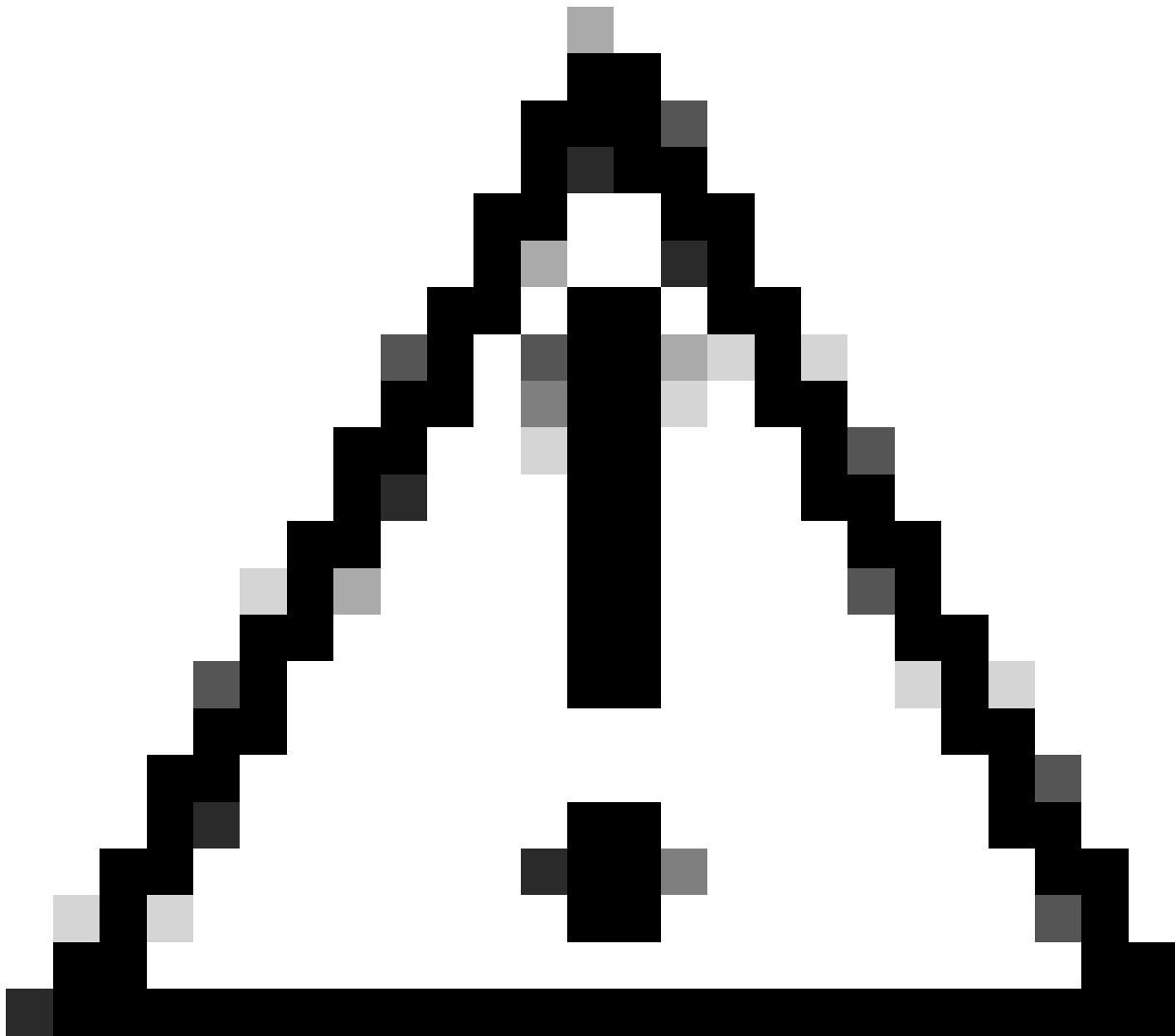
Interface group/Security Zone:\*  +

Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

VPNインターフェイス

15. 使用可能な方法の1つを選択して証明書の登録プロセスを確立し、証明書を作成してファイアウォールにインストールします。これは、セキュアなVPN接続にとって重要です。



注意：たとえば、このガイドでは自己署名証明書が選択されています。

---

## Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*

 +

デバイス証明書。

## Add Cert Enrollment



Name\*

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

SCEP

Enrollment URL:\*

Self Signed Certificate

EST

Challenge Password:

SCEP

Confirm Password:

Manual

PKCS12 File

Retry Period:

1 (Range 0-60)

Retry Count:

10 (Range 0-100)

Fingerprint:

Cancel

Save

証明書登録。

16. 証明書の登録を設定したら、Nextをクリックします。

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Firepower Management Center will configure an RA VPN Policy with the following settings.

Interface group/Security Zone:\*  +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

### Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*  +

### Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

アクセスとサービスの概要

17. すべての設定の概要をレビューして、設定が正確であり、意図した設定が反映されていることを確認します。

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	VPN_Remote
Device Targets:	FTD_01
Connection Profile:	VPN_Remote
Connection Alias:	VPN_Remote
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE (RADIUS)
Authorization Server:	ISE (RADIUS)
Accounting Server:	ISE
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	Pool_VPN
Address Pools (IPv6):	-
Group Policy:	VPN_Remote_Policy
AnyConnect Images:	anyconnect-win-4.10.08029-webdeploy-k9.pkg
Interface Objects:	Outside
Device Certificates:	Cert_Enrollment

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- 1 Access Control Policy Update  
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- 2 NAT Exemption  
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- 3 DNS Configuration  
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- 4 Port Configuration  
SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- 5 Network Interface Configuration  
Make sure to add interface from targeted

VPN設定の概要。

18. VPNリモートアクセス設定を適用してアクティブにするには、Deploy > Deploy Allの順に移動し、選択したFTDデバイスへの展開を実行します。

Firewall Management Center  
Devices / VPN / Edit Connection Profile

Overview Analysis Policies Devices Objects Integration **Deploy** admin

VPN\_Remote  
Enter Description

Connection Profile Access Interfaces Advanced

Name	AAA
DefaultWEBVPGNGroup	Authentication: No Authorization: No Accounting: No
VPN_Remote	Authentication: IS Authorization: IS Accounting: IS

Advanced Deploy **Deploy All**

FTD\_01 Ready for Deployment (1)

1 device is available for deployment

VPN設定を展開しています。

## ISE設定。

DUOを外部RADIUSサーバーとして統合します。

1. Cisco ISE管理インターフェイスで、Administration > Network Resources > External RADIUS Serversの順に移動します。
2. Addボタンをクリックして、新しい外部RADIUSサーバーを構成します。

Cisco ISE Administration · Network Resources

Network Devices Network Device Groups Network Device Profiles **External RADIUS Servers** RADIUS Server Sequences NAC Managers More

External RADIUS Servers

Selected 0 Total 0

Edit **+ Add** Duplicate Delete

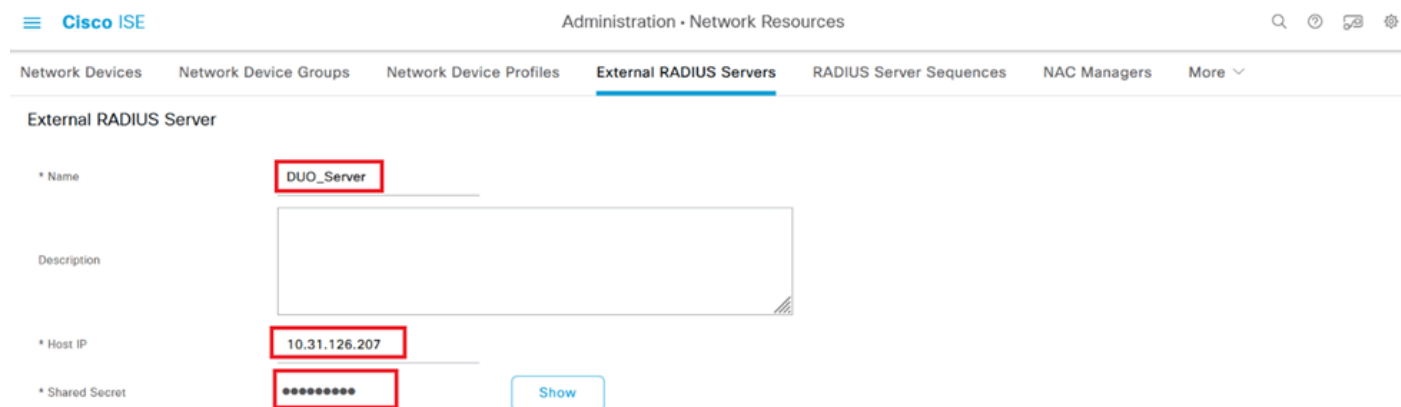
Name	Description
No data available	

外部Radiusサーバ

3. プロキシDUOサーバーの名前を入力します。
4. Proxy DUOサーバの正しいIPアドレスを入力して、ISEとDUOサーバ間の通信が適切であることを確認します。
5. 共有秘密キーを設定します。

注:RADIUS接続を正常に確立するには、この共有秘密キーをプロキシDUOサーバに設定する必要があります。

6. すべての詳細を正しく入力したら、**Submit**をクリックして、新しいProxy DUO Server設定を保存します。



The screenshot shows the Cisco ISE Administration interface for configuring an External RADIUS Server. The breadcrumb navigation is Administration > Network Resources > External RADIUS Servers. The form fields are as follows:

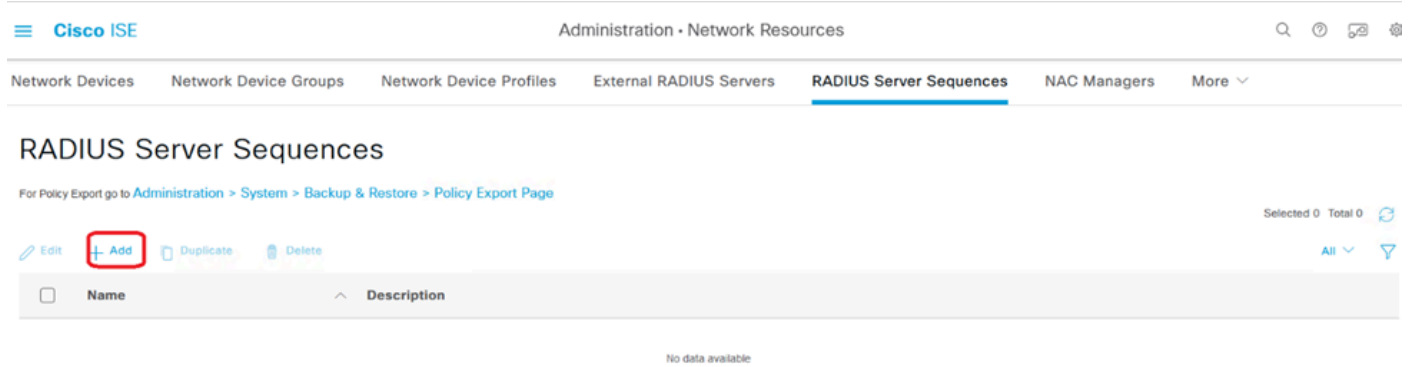
Field	Value
* Name	DUO_Server
Description	
* Host IP	10.31.126.207
* Shared Secret	*****

A "Show" button is located next to the Shared Secret field.

外部RADIUSサーバ

7. Administration > RADIUS Server Sequencesの順に進みます。

8. Addをクリックして、新しいRADIUSサーバーシーケンスを作成します。

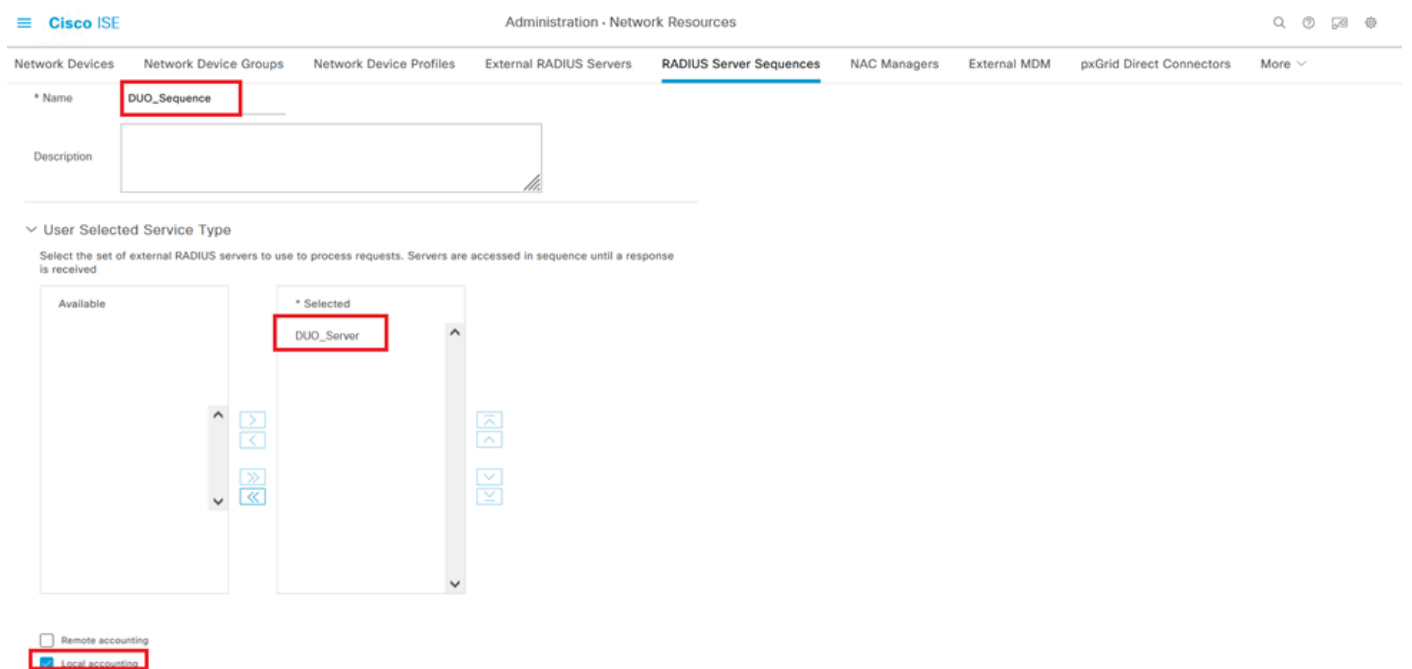


RADIUSサーバーシーケンス

9. RADIUSサーバーシーケンスを識別しやすくするために、別の名前を指定します。

10. このガイドではDUO\_Serverと呼ばれている、以前設定したDUO RADIUSサーバを探し、それを右側の選択済みリストに移動してシーケンスに含めます。

11. Submitをクリックして、RADIUSサーバーシーケンスの設定を完了して保存します。



Radiusサーバーシーケンスの設定。

FTDをネットワークアクセスデバイスとして統合します。

1. システムインターフェイスのAdministrationセクションに移動し、そこからNetwork Resourcesを選択してネットワークデバイスの設定領域にアクセスします。

2. [Network Resources]セクションで、[Add]ボタンを探してクリックし、新しいネットワークアクセスデバイスを追加するプロセスを開始します。













Network Devices

Default Device

Device Security Settings

## Network Devices

Selected 0 Total 0  

 **+ Add**  Duplicate  Import  Export ▾  Generate PAC  Delete ▾  All ▾ 

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
No data available						

ネットワークアクセスデバイス。

- 表示されたフィールドに、ネットワーク内のデバイスを識別するためのネットワークアクセスデバイス名を入力します。
- FTD(Firepower Threat Defense)デバイスのIPアドレスの指定に進みます。
- FMC(Firepower Management Center)のセットアップ中に以前に確立されたキーを入力します。このキーは、デバイス間のセキュアな通信に不可欠です。
- 「発行」ボタンをクリックして、プロセスを完了します。

[Network Devices List](#) > [FTD](#)

## Network Devices

Name

FTD

Description

IP Address ▾

\* IP :

10.4.23.53

/

32



NADとしてFTDを追加します。



## RADIUS Authentication Settings

### RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

●●●●●●●●

Show

Use Second Shared Secret ⓘ

Second Shared Secret

Show

CoA Port

1700

Set To Default

RADIUS設定

DUO構成。

DUOプロキシインストール。

次のリンクをクリックして、『DUO Proxy Download and Installation Guide』にアクセスします。

<https://duo.com/docs/authproxy-reference>

DUOプロキシをISEおよびDUOクラウドと統合します。

1. DUO Security Webサイト(<https://duo.com/>)にログインします。
2. 「アプリケーション」セクションにナビゲートし、「アプリケーションの保護」を選択して続行します。

Dashboard > Applications

# Applications

Protect an Application

Manage your update to the new Universal Prompt experience, all in one place.

See My Progress Get More Information

0 All Applications 0 End of Support

Export Search

DUOアプリケーション

3. リストで「Cisco ISE RADIUS」オプションを検索し、Protectをクリックしてアプリケーションに追加します。

Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others. Documentation: [Getting Started](#)

Choose an application below to get started.

Cisco ISE RADIUS

Application	Protection Type	Documentation	Protect
Cisco ISE Administrative Web Login	2FA with SSO hosted by Duo (Single Sign-On)	<a href="#">Documentation</a>	<a href="#">Configure</a>
Cisco ISE RADIUS	2FA	<a href="#">Documentation</a>	<a href="#">Protect</a>
Cisco RADIUS VPN	2FA	<a href="#">Documentation</a>	<a href="#">Protect</a>

ISE RADIUSオプション

4. 正常に追加されると、DUOアプリケーションの詳細が表示されます。下にスクロールしてSaveをクリックします。

5. 提供された統合キー、秘密キー、およびAPIホスト名をコピーします。これらは今後の手順で重要です。



Application modified successfully.

[Dashboard](#) > [Applications](#) > Cisco ISE RADIUS

## Cisco ISE RADIUS

[Authentication Log](#) | [Remove Application](#)

Follow the [Cisco ISE RADIUS instructions](#).

### Details

[Reset Secret Key](#)

Integration key

DIX [REDACTED] [Copy](#)

Secret key

.....ywLM [Copy](#)

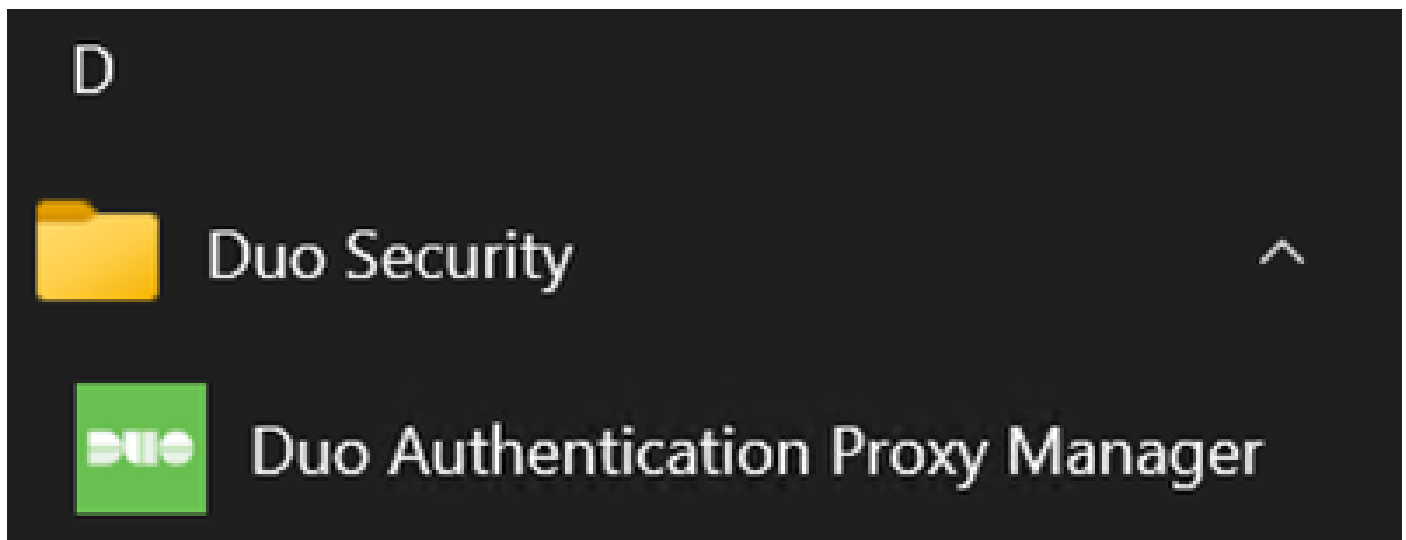
Don't write down your secret key or share it with anyone.

API hostname

[REDACTED] duosecurity.com [Copy](#)

ISEサーバの詳細

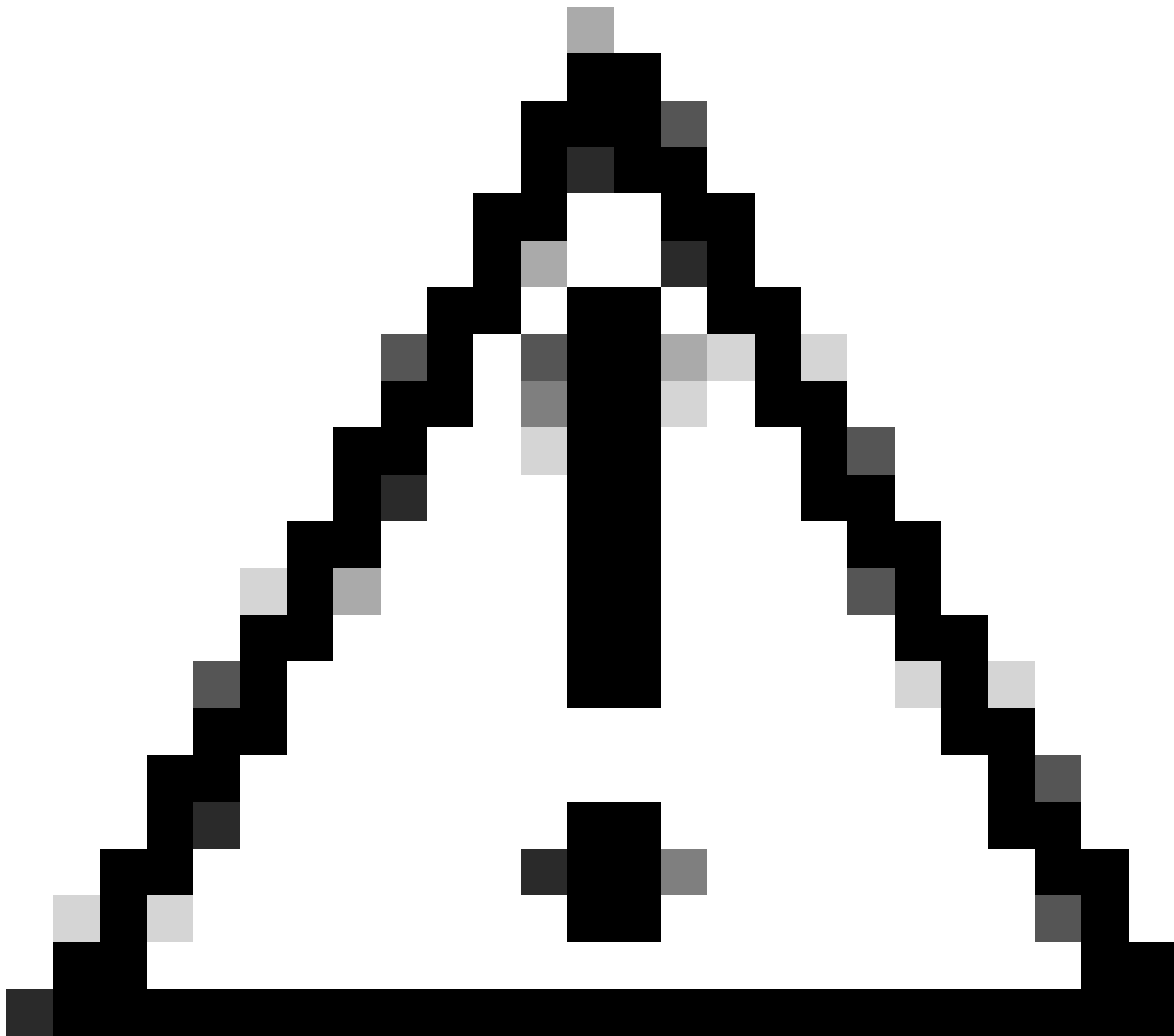
6. システムのDUO Proxy Managerを起動して、セットアップを続行します。



DUOプロキシマネージャ

7. ( オプション ) DUOプロキシサーバーがDUOクラウドに接続するためにプロキシ構成を必要とする場合は、次のパラメーターを入力します :

```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```

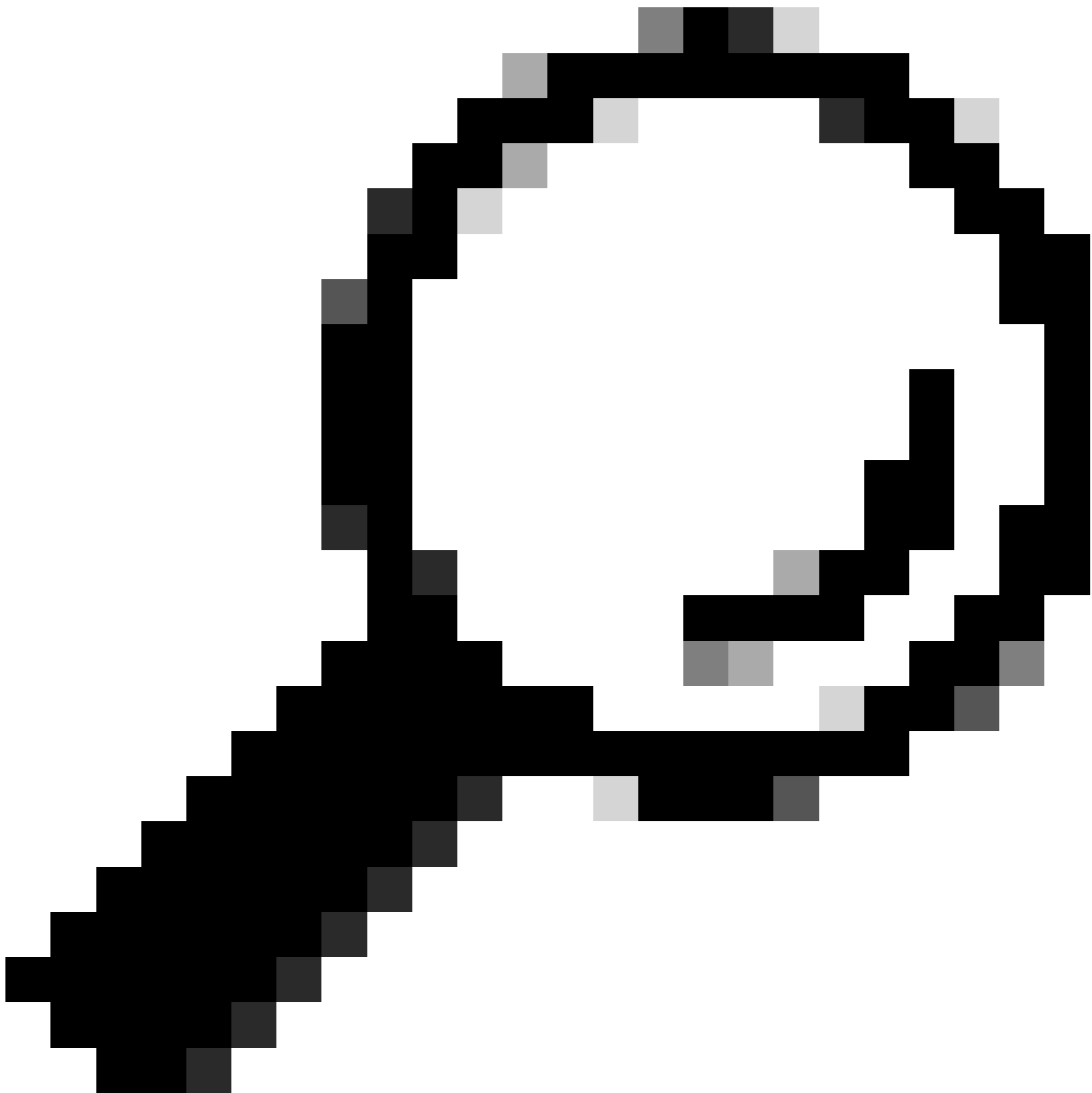


注意:とを実際のプロキシの詳細に置き換えてください。

---

8. ここで、前にコピーした情報を利用して、統合設定を完了します。

```
[radius_server_auto]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
radius_ip_1=<ISE IP address>
radius_secret_1=<secret key configured in the external RADIUS server section>
failmode=safe
port=1812
client=ad_client
```



ヒント: `client=ad_client`という行は、DUOプロキシがActive Directoryアカウントを使用して認証することを示しています。Active Directoryとの同期を完了するには、この情報が正しいことを確認します。

---

DUOをActive Directoryと統合します。

1. DUO認証プロキシをActive Directoryと統合します。

```
[ad_client]
host=<AD IP Address>
service_account_username=<service_account_username>
service_account_password=<service_account_password>
search_dn=DC=<domain>,DC=<TLD>
```

2. Active DirectoryにDUOクラウドサービスで参加します。<https://duo.com/>にログインします。

3. 「Users」に移動し、「Directory Sync」を選択して同期設定を管理します。

Dashboard > Users

## Users

Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

0	0	0	0	0	0
Total Users	Not Enrolled	Inactive Users	Trash	Bypass Users	Locked Out

Select (0) | ... | Export | Search

No users shown based on your search.

ディレクトリ同期

4. [Add New Sync]をクリックし、表示されたオプションから[Active Directory]を選択します。

Dashboard > Users > Directory Sync

## Directory Sync

Add New Sync

Directory Syncs | Connections

You don't have any directories yet.

新しい同期の追加

5. Add new connectionを選択し、Continueをクリックします。

Dashboard > Users > Directory\_Sync > New Active Directory Sync

## New Active Directory Sync

**Connection**  
Set up a new connection using a new Authentication Proxy.

Reuse existing connection

**Add new connection**  
You will be redirected to a new page

**Directory Sync Setup**  
Waiting for connection to directory  
Sync setup is disabled until a connection to the directory has been established.

**Directory Sync Setup**

- Connect to AD
- Add groups
- Review synced attributes

新しいActive Directoryの追加

6. 生成された統合キー、秘密キー、およびAPIホスト名をコピーします。

### Authentication Proxy

#### Configuration metadata

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

**Integration key**

**Secret key**

Don't write down your secret key or share it with anyone.

**API hostname**

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

#### Status

Not connected

- Add Authentication Proxy
- Configure Directory

#### Connected Directory Syncs

User Syncs

[AD\\_Sync](#)

認証プロキシの詳細

7. DUO認証プロキシ構成に戻り、取得した新しいパラメータとActive Directory管理者のサービスアカウント資格情報を使用して[cloud]セクションを構成します。

[cloud]

ikey=<integration key>

skey=<secret key>

api\_host=<API hostname>

service\_account\_username=<your domain>\<service\_account\_username>

service\_account\_password=<service\_account\_password>



8. 「validate」 オプションを選択して構成を検証し、すべての設定が正しいことを確認します。

Authentication Proxy is running Up since: 4/20/2024, 5:43:21 PM Version: 6.3.0 Restart Service Stop Service

Configure: authproxy.cfg Unsaved Changes Output

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skey=[redacted]uXMywLM
8 api_host=[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
16 host=10.4.23.42
17 service_account_username=administrator
18 service_account_password=[redacted]
```

Validate Save

プロキシDUOの設定。

9. 検証後、設定を保存し、DUO認証プロキシ・サービスを再起動して変更を適用します。

Authentication Proxy is running Up since: 4/20/2024, 5:43:21 PM Version: 6.3.0 Restart Service Stop Service

Validation passed  
Configuration has passed validation and is ready to be saved

Configure: authproxy.cfg Unsaved Changes Output

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skey=[redacted]wLM
8 api_host=[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
```

Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes...  
[info] Testing section 'main' with configuration:  
[info] {'http\_proxy\_host': 'cx[redacted]', 'http\_proxy\_port': '3128'}  
[info] There are no configuration problems  
[info] -----  
[info] Testing section 'radius\_server\_auto' with configuration:  
[info] {'api\_host': '[redacted].duosecurity.com', 'client': 'ad\_client', 'failmode': 'safe', 'http\_proxy\_host': '[redacted]', 'http\_proxy\_port': '3128', 'ikey': 'DI[redacted]'}

Validate Save

Restart Serviceオプション

10. DUO管理ダッシュボードに戻り、Active DirectoryサーバーのIPアドレスとユーザー同期用のベースDNを入力します。

---

## Directory Configuration

### Domain controller(s)

Hostname or IP address (1) \*

Port (1) \*

[+ Add Domain controller](#)

The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

---

### Base DN \*

Enter the full distinguished name (DN) of the directory location to search for users and groups. We recommend setting this to the directory root (example: DC=domain,DC=local). If specifying the DN of an OU or container, ensure it is **above both the users and groups to sync**.

---

ディレクトリ設定。

11. システムを非NTLMv2認証に設定するには、Plainオプションを選択します。

---

## Authentication type

- Integrated**  
Performs Windows authentication from a domain-joined system.
- NTLMv2**  
Performs Windows NTLMv2 authentication.
- Plain**  
Performs username-password authentication.

認証タイプ。

12. 新しい設定を保存して、設定が更新されていることを確認します。

 Delete Connection

Save

## Status

Not connected

Add Authentication Proxy



Configure Directory

---

## Connected Directory Syncs

### User Syncs

[AD Sync](#)

Saveオプション

13. 「接続のテスト」機能を使用して、DUOクラウドサービスがActive Directoryと通信できるこ

とを確認します。

## Authentication Proxy

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

**Integration key**  [Copy](#)

**Secret key**  [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

**API hostname**  [Copy](#)

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

```
service_account_username=myusername  
service_account_password=mypassword
```

4. Restart your Authentication Proxy.

5. [Test Connection](#).

接続オプションをテストします。

14. Active Directoryのステータスが、統合の成功を示す「Connected」と表示されていることを確認します。

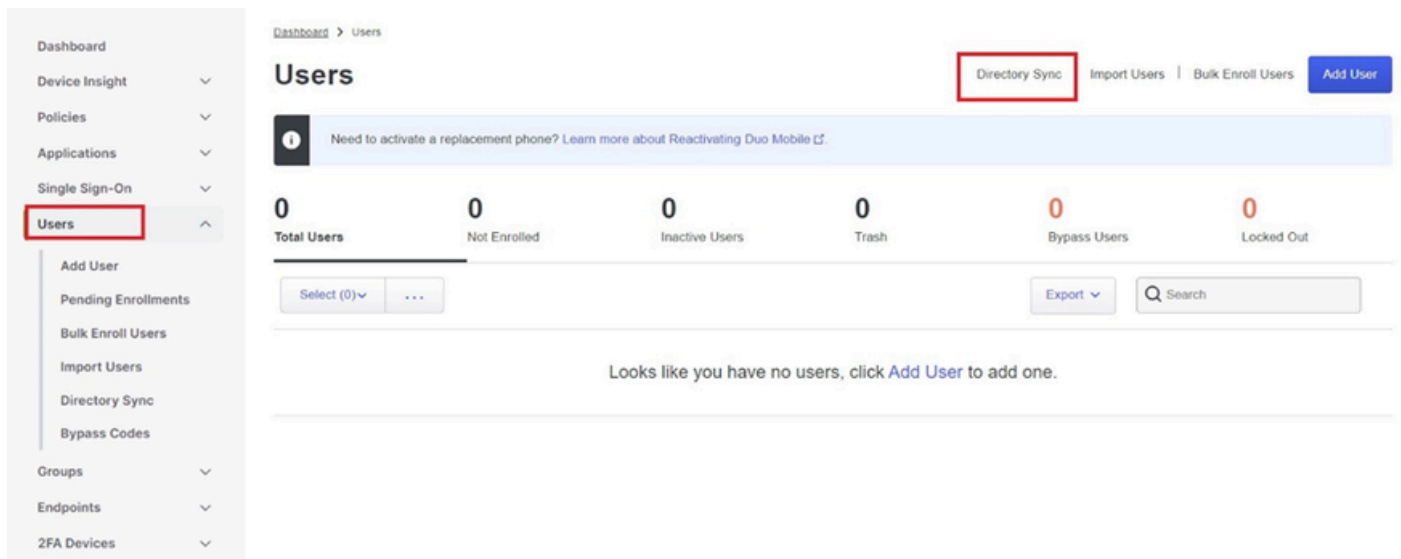
## Status

Connected

ステータスが成功しました。

DUO Cloud経由でActive Directory(AD)からユーザーアカウントをエクスポートします。

1. Duo Admin PanelでUsers > Directory Syncの順に移動し、Active Directoryとのディレクトリ同期に関連する設定を見つけます。

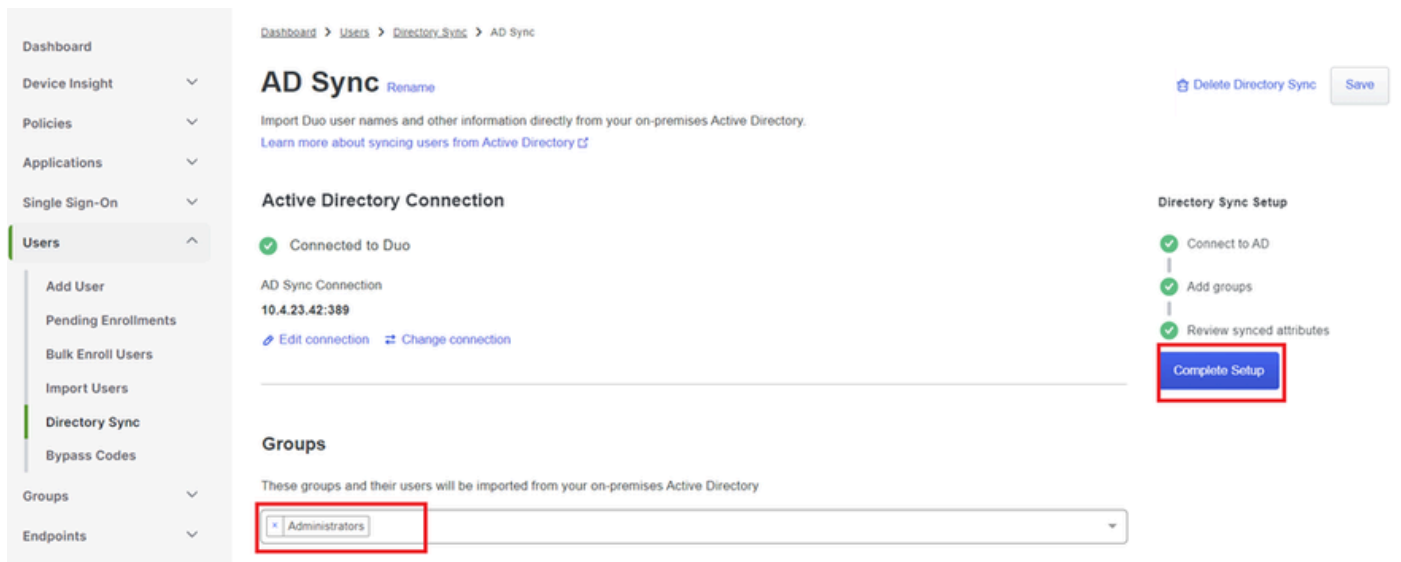


ユーザーリスト。

2. 管理するActive Directory構成を選択します。

3. 構成設定で、Duo Cloudと同期する特定のグループをActive Directory内で識別して選択します。選択範囲に対してフィルタリングオプションを使用することを検討してください。

4. Complete Setupをクリックします。



AD同期。

5. 同期を即時に開始するには、「今すぐ同期」をクリックします。これにより、Active Directory内の指定されたグループからDuo Cloudにユーザーアカウントがエクスポートされ、Duo Security環境内でユーザーアカウントを管理できるようになります。

# AD Sync Rename

Delete Directory Sync No Changes

Import Duo user names and other information directly from your on-premises Active Directory.  
[Learn more about syncing users from Active Directory](#)

## Sync Controls

### Sync status

Scheduled to automatically synchronize every 12 hours, next around 2:00 AM UTC [Pause automatic syncs](#)

[Sync Now](#)

[Troubleshooting](#)

### Active Directory Connection

✓ Connected to Duo

AD Sync Connection

10.4.23.42:389

[Edit connection](#)

[Change connection](#)

同期の開始

Cisco DUO Cloudにユーザを登録します。

ユーザ登録により、コードアクセス、DUOプッシュ、SMSコード、トークンなど、さまざまな方法で本人確認が可能になります。

1. Cisco CloudダッシュボードのUsersセクションに移動します。
2. 登録するユーザーのアカウントを見つけて選択します。

Dashboard > Users

Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

**1** Total Users    **1** Not Enrolled    **1** Inactive Users    **0** Trash    **0** Bypass Users    **0** Locked Out

Select (0) ...    Export    Search

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/>	administrator		oteg			Active	Never authenticated

1 total

ユーザー・アカウント・リスト。

3. 「登録メールの送信」 ボタンをクリックして、登録プロセスを開始します。

## administrator

Logs

Send Enrollment Email

Sync This User



This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.



This user was synced from the directory **AD Sync**. Some fields are read-only.

Username

administrator

Username aliases

[+ Add a username alias](#)

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number for a specific alias

(e.g., Username alias 1 should only be used for Employee ID).

電子メールによる登録。

4. 電子メールの受信トレイを確認し、登録の招待を開いて認証プロセスを完了します。

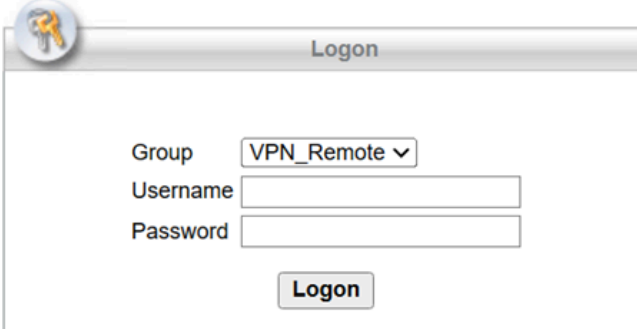
登録プロセスの詳細については、次のリソースを参照してください。

- ユニバーサル登録ガイド : <https://guide.duo.com/universal-enrollment>
- 従来型登録ガイド : <https://guide.duo.com/traditional-enrollment>

設定検証手順。

設定が正確で正常に動作していることを確認するには、次の手順を検証します。

1. Webブラウザを起動し、Firepower Threat Defense(FTD)デバイスのIPアドレスを入力してVPNインターフェイスにアクセスします。



Logon

Group

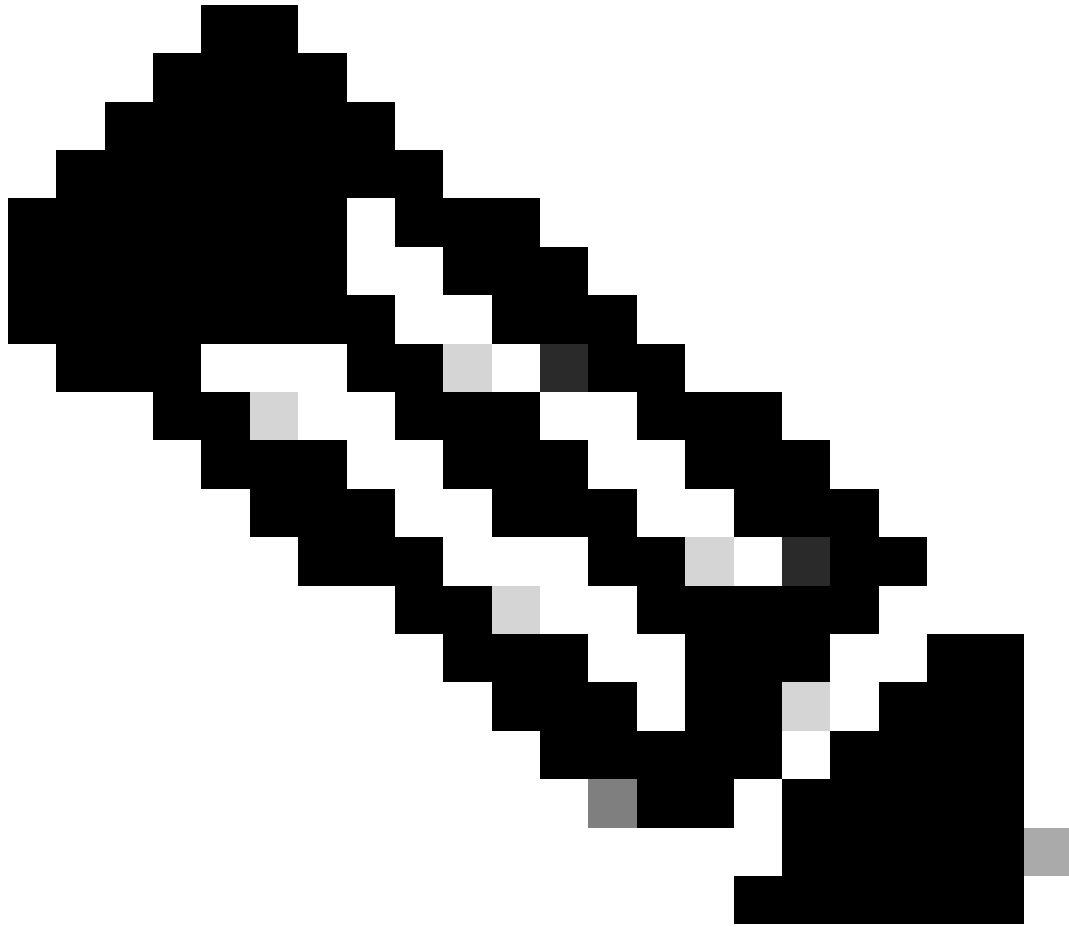
Username

Password

VPNログオン。

2. プロンプトが表示されたら、ユーザー名とパスワードを入力します。





注：クレデンシャルはActive Directoryアカウントの一部です。

---

3. DUOプッシュ通知を受け取ったら、DUO Mobileソフトウェアを使用して承認し、検証プロセスを進めます。

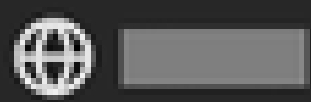


(1) Login request waiting.


[Respond](#)



Are you logging in to Cisco ISE  
RADIUS?



 Unknown

 3:13 PM CST

 administrator

## 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。