Configure SSL VPN Authentication through FTD, ISE, DUO and Active Directory

Contents

Introduction

This document describes the integration of SSLVPN in **Firepower Threat Defense** using Cisco ISE and DUO Security for AAA.

Requirements

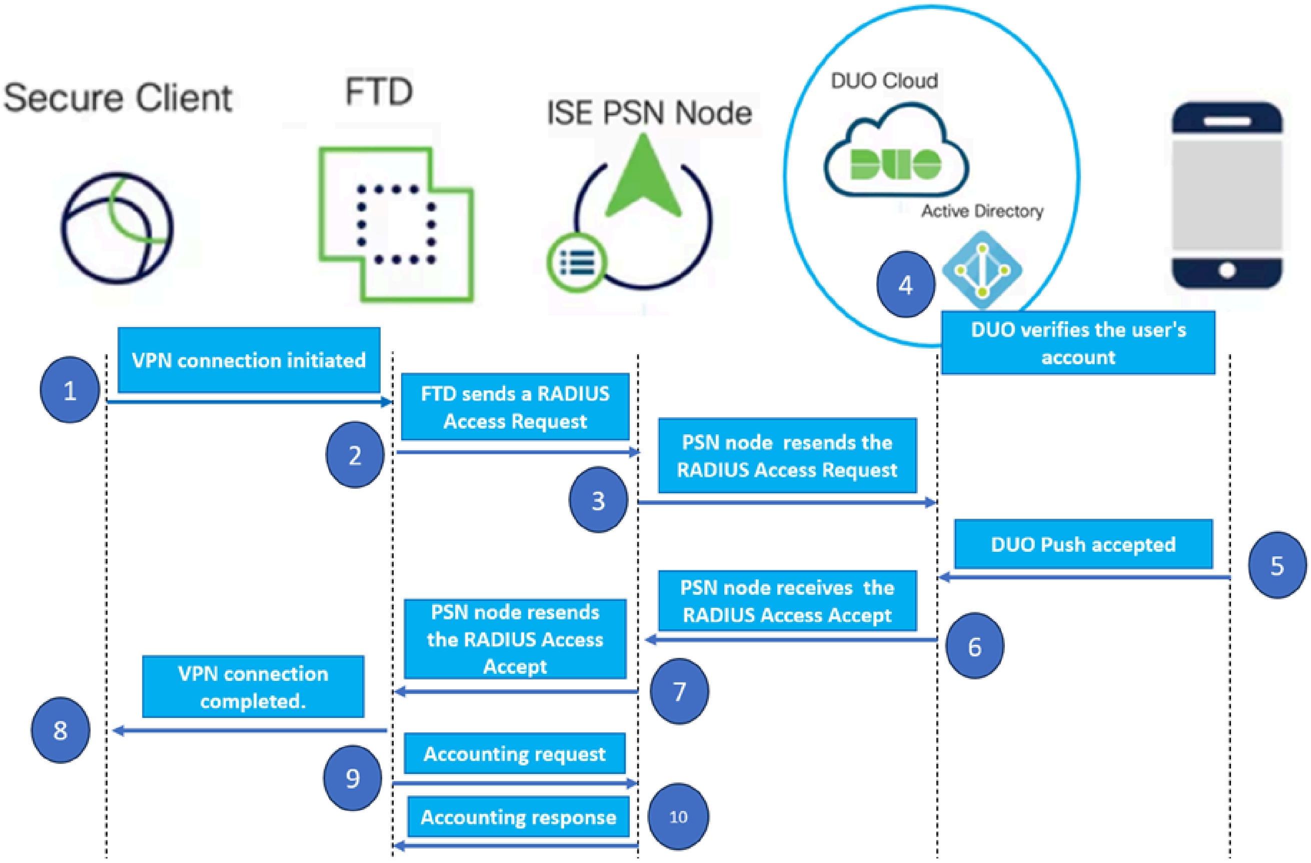
- ISE 3.0 or higher.
- FMC 7.0 or higher.
- FTD 7.0 or higher.
- DUO Authentication Proxy.
- ISE Essentials Licensing
- DUO Essentials Licensing.

Components Used

- ISE 3.2 Patch 3
- FMC 7.2.5
- FTD 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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.

Network Diagram


Secure Client
FTD
ISE PSN Node
DUO Cloud
Active Directory
1
VPN connection initiated
2
FTD sends a RADIUS Access Request
3
PSN node resends the RADIUS Access Request
4
DUO verifies the user's account
5
DUO Push accepted
6
PSN node receives the RADIUS Access Accept
7
PSN node resends the RADIUS Access Accept
8
VPN connection completed.
9
Accounting request
10
Accounting response

Topology.

In our proposed solution, Cisco ISE is a crucial **RADIUS** Server proxy. Rather than directly evaluating authentication or authorization policies, ISE is configured to forward the RADIUS packets from the FTD to the DUO Authentication Proxy.

The DUO Authentication Proxy operates as a dedicated intermediary within this authentication flow. Installed on a Windows server, it bridges the gap between Cisco ISE and DUOs cloud. The proxy primary function is to transmit authentication requests – encapsulated within RADIUS packets – to the DUO Cloud. The DUO Cloud ultimately allows or denies network access based on the two-factor authentication configurations.

1. The user initiates the VPN authentication process by entering their unique username and password.

2. The Firewall Threat Defense (FTD) sends the authentication request to the Cisco Identity Services Engine (ISE).

3. The Policy Services Node (PSN) forwards the authentication request to the DUO Authentication Proxy Server. Subsequently, the DUO Authentication Server validates the credentials through the DUO Cloud service.

4. The DUO Cloud validates the username and password against its synchronized database.

Caution: The synchronization between the DUO Cloud and the organizations Active Directory needs to be active to maintain an up-to-date user database in the DUO Cloud.

5. Upon successful authentication, the DUO Cloud initiates a DUO Push to the users registered mobile device through a secure, encrypted push notification. The user must then approve the DUO Push to confirm their identity and proceed.

6. Once the user approves the DUO Push, the DUO Authentication Proxy Server sends a confirmation back to the PSN to indicate that the authentication request has been accepted by the user.

7. The PSN node sends the confirmation to the FTD to inform that the user has been authenticated.

8. The FTD receives the authentication confirmation and establishes the VPN connection to the endpoint with the appropriate security measures in place.

9. The FTD logs the details of the successful VPN connection and securely transmits the accounting data back to the ISE node for record-keeping and auditing purposes.

10. The ISE node logs the accounting information in its livelogs, ensuring that all records are stored securely and are accessible for future audits or compliance checks.

Note:

The setup in this guide utilizes the next network parameters:

- Primary Network Server (PNS) Node IP: 10.4.23.21

- Firepower Threat Defense (FTD) IP for Peer VPN: 10.4.23.53

- DUO Authentication Proxy IP: 10.31.126.207

- Domain Name: testlab.local

Configurations

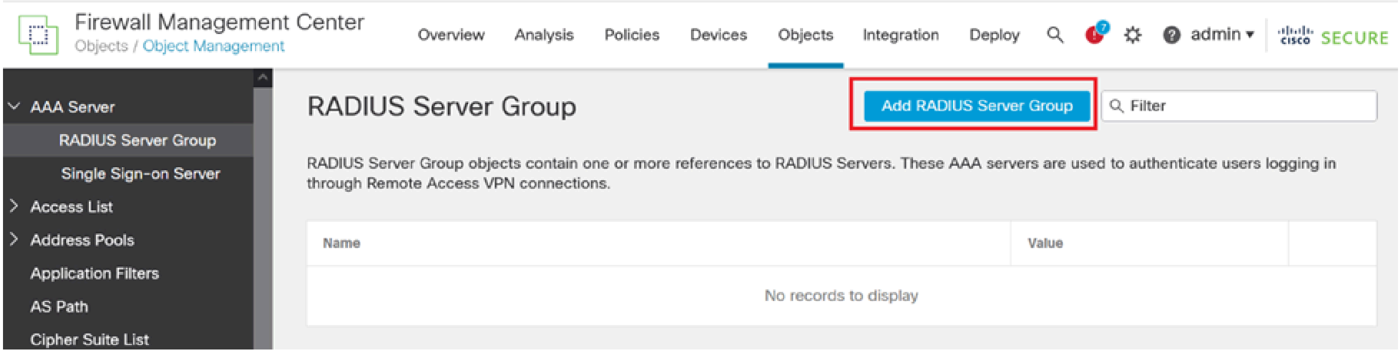
FTD configurations.

Integrate a RADIUS server within the Firepower Management Center (FMC)

1. Access the FMC by launching your web browser and entering the FMCs IP address to open the Graphical User Interface (GUI).

2. Navigate to the **Objects** menu, select **AAA Server**, and proceed to the **RADIUS Server Group** option.

3. Click the **Add RADIUS Server Group** button to create a new group for RADIUS servers.



RADIUS Server Group

RADIUS Server Group objects contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections.

Name	Value
No records to display	

RADIUS Server Group.

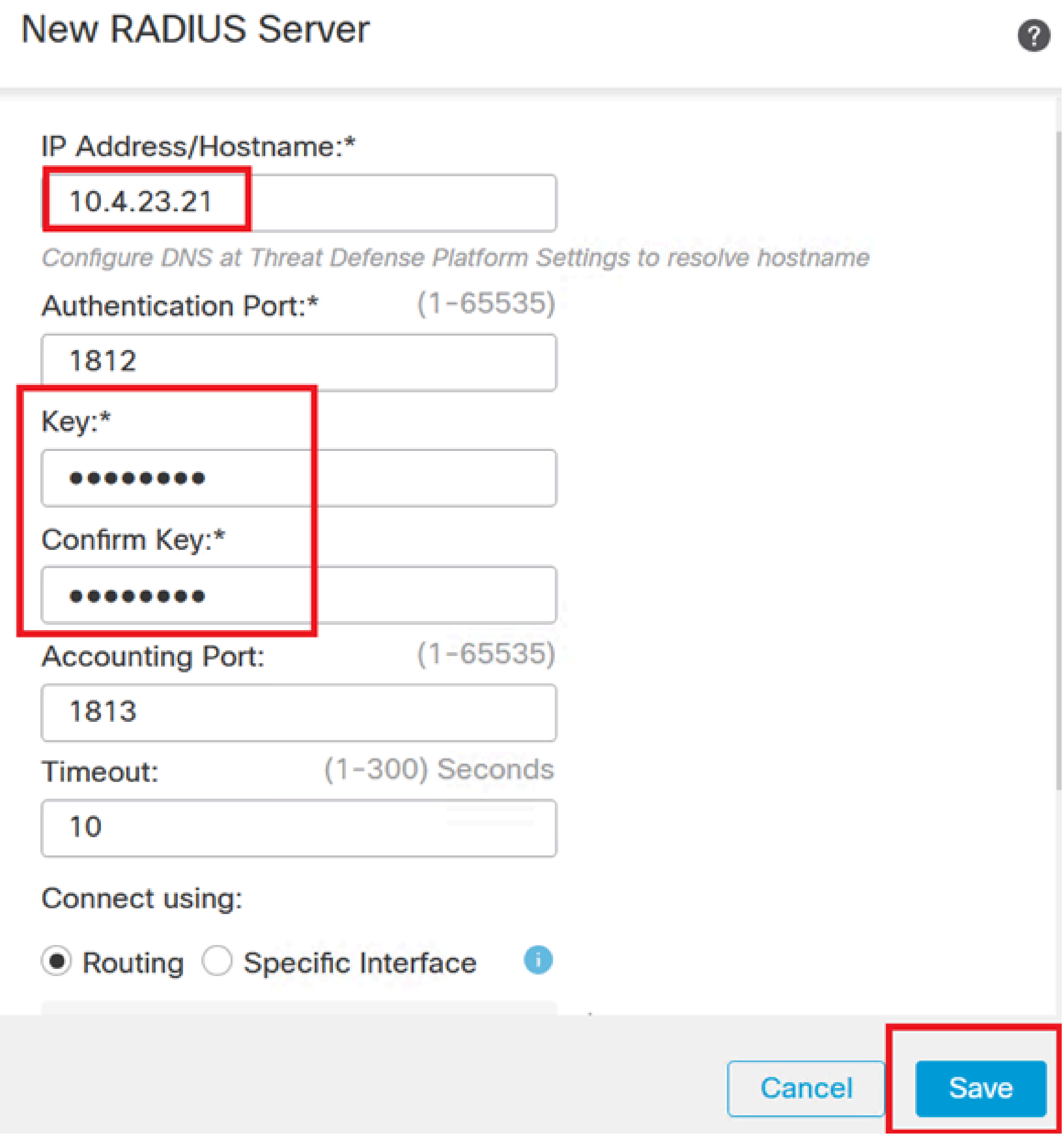
4. Enter a descriptive name for the new AAA RADIUS Server Group to ensure clear identification within your network infrastructure.

5. Proceed to add a new RADIUS Server by selecting the appropriate option within the group configuration.

RADIUS Server.

6. Specify the RADIUS Servers IP address and enter the shared secret key.

Note: It is essential to ensure that this secret key is securely shared with the ISE Server to establish a successful RADIUS connection.



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

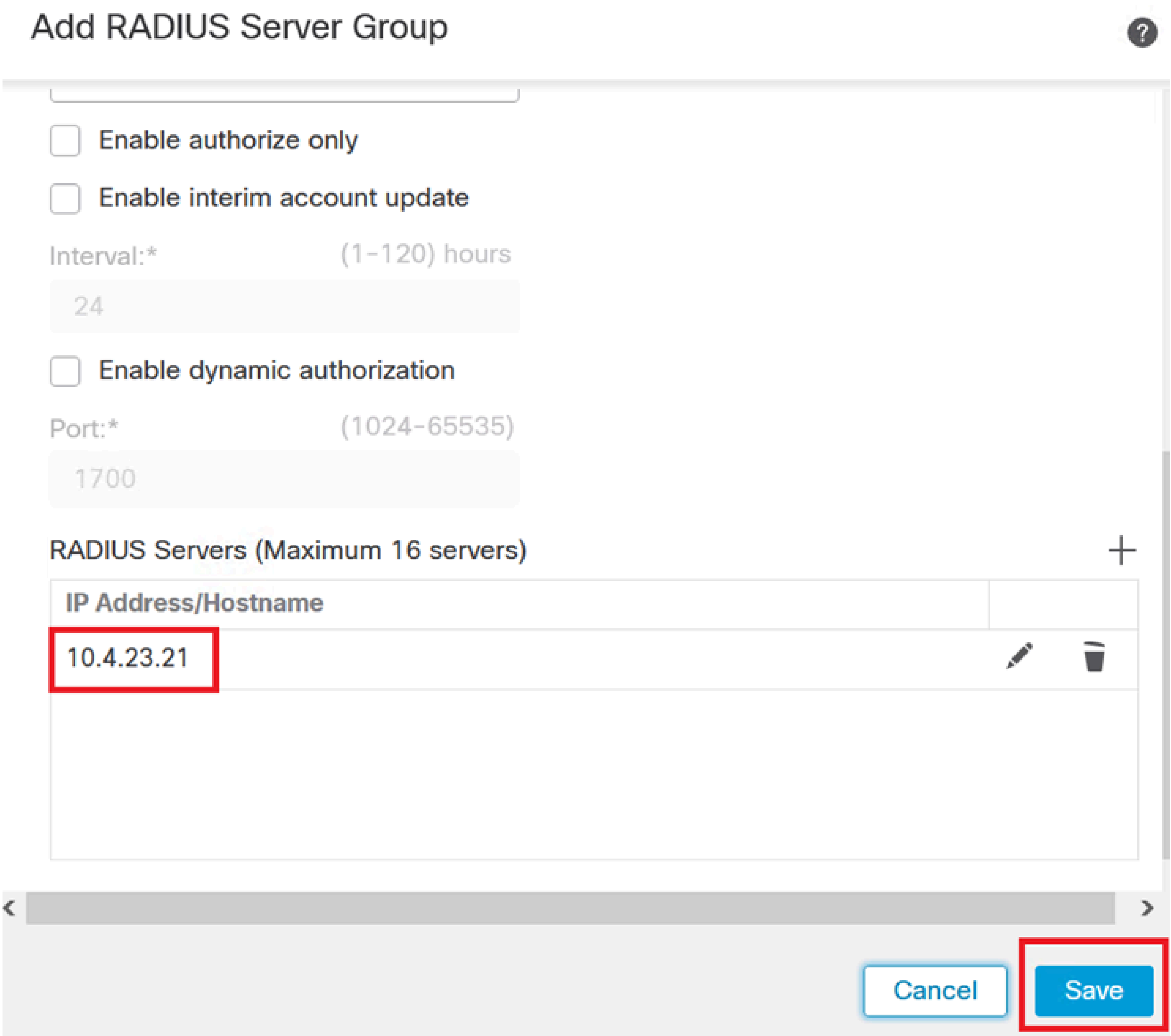
Timeout: (1-300) Seconds 10

Connect using:

● Routing ○ Specific Interface

New RADIUS Server.

7. After configuring the RADIUS Server details, click **Save** to preserve the settings for the RADIUS Server Group.


Add RADIUS Server Group

□ Enable authorize only

□ Enable interim account update

Interval:* (1-120) hours

24

□ Enable dynamic authorization

Port:* (1024-65535)

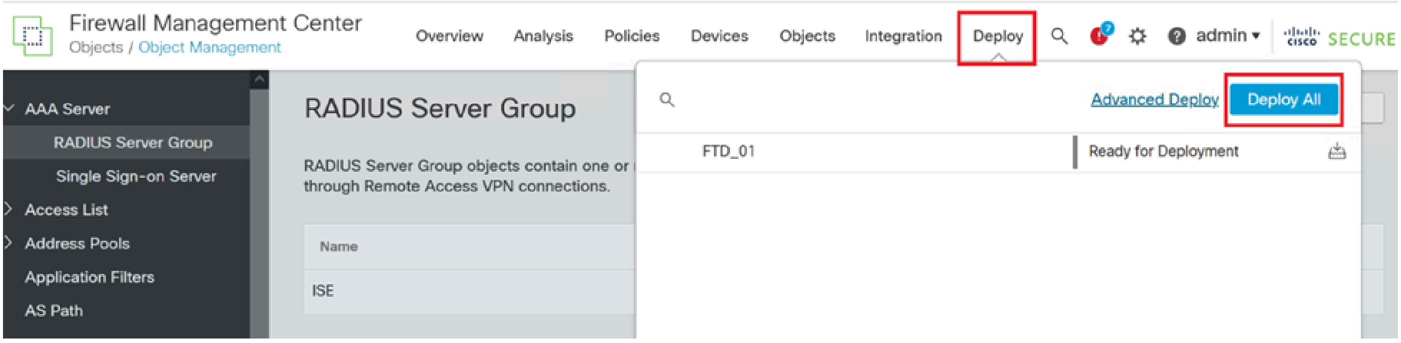
1700

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
10.4.23.21

Server Group details.

8. To finalize and implement the AAA Server configuration across your network, navigate to the **Deploy** menu, then select **Deploy All** to apply the settings.



RADIUS Server Group

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

Name
ISE

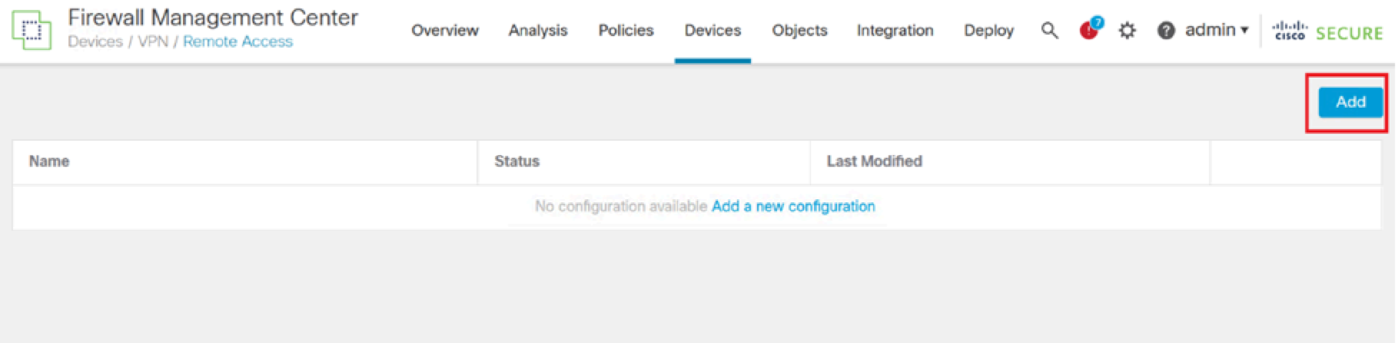
FTD_01 Ready for Deployment

Deploying AAA Server.

Configure the remote VPN.

1. Navigate to **Devices** > **VPN** > **Remote Access** in the FMC GUI to begin the VPN configuration process.

2. Click the **Add** button to create a new VPN connection profile.



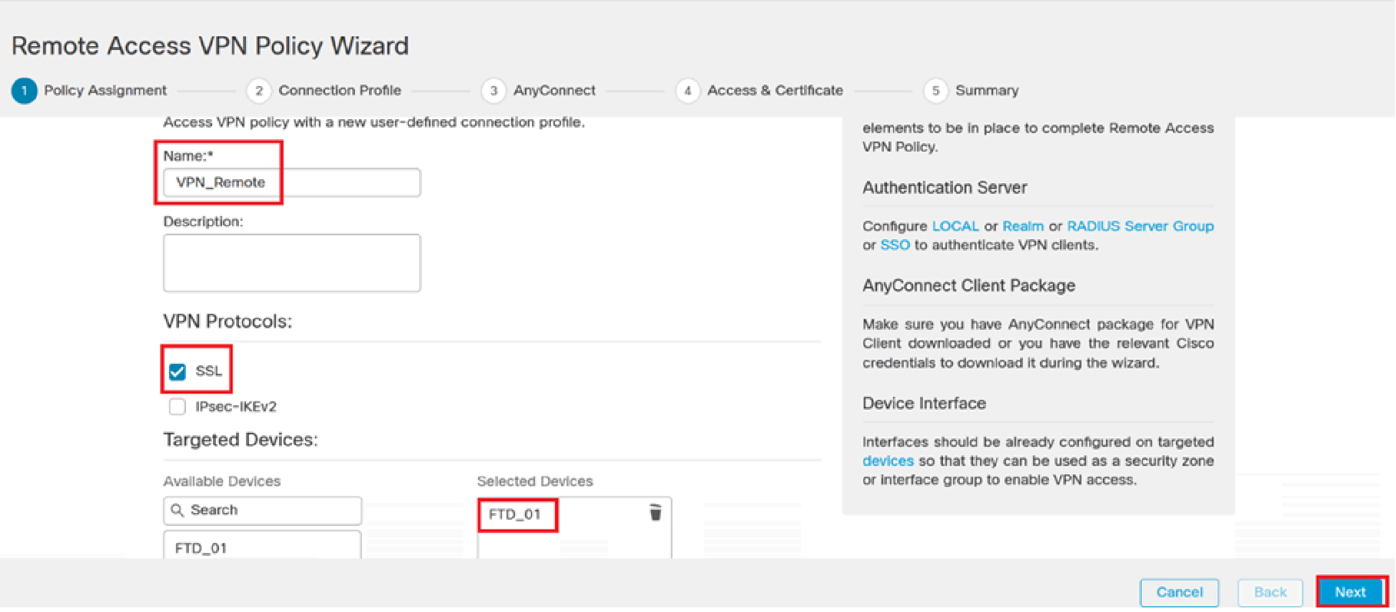
Name	Status	Last Modified
No configuration available Add a new configuration		

VPN connection profile.

3. Enter a unique and descriptive name for the VPN to help identify it within your network settings.

4. Choose the SSL option to ensure a secure connection using the SSL VPN protocol.

5. From the list of devices, select the specific FTD device.



Remote Access VPN Policy Wizard

Access VPN policy with a new user-defined connection profile.

Name:* VPN_Remote

Description:

VPN Protocols:

☑ SSL

□ IPsec-IKEv2

Targeted Devices:

Available Devices: FTD_01

Selected Devices: FTD_01

elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.

AnyConnect Client Package

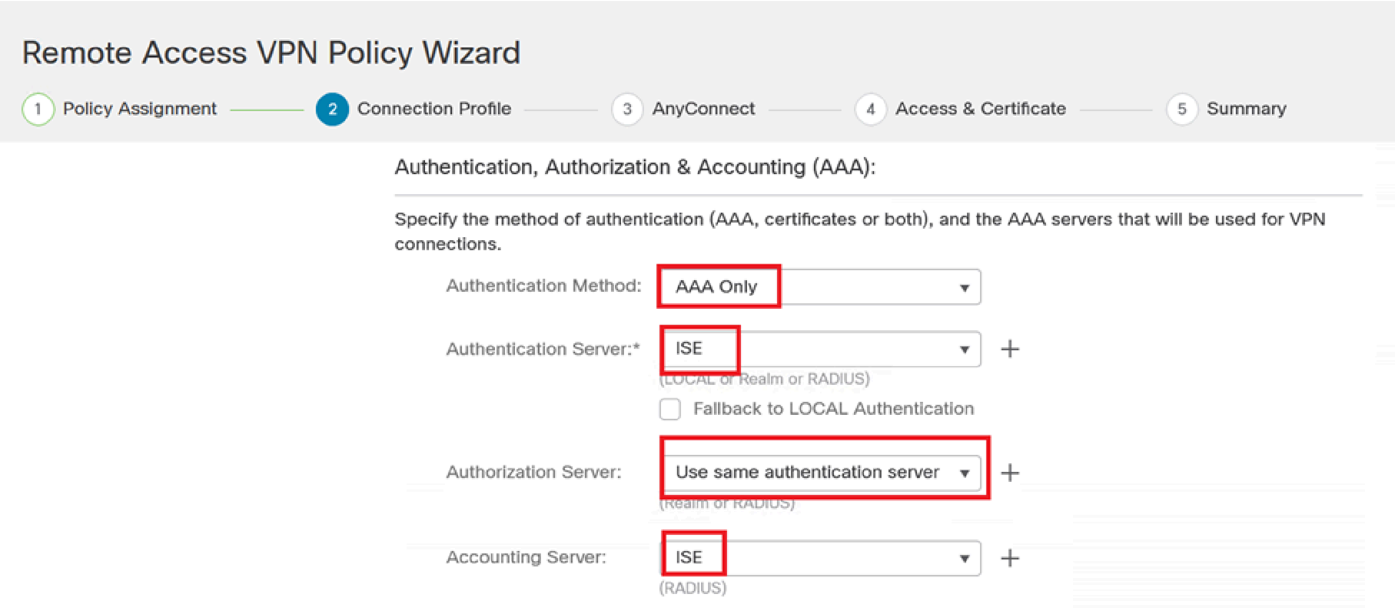
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

VPN settings.

6. Configure the AAA method to utilize the PSN node in the authentication settings.



Remote Access VPN Policy Wizard

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)

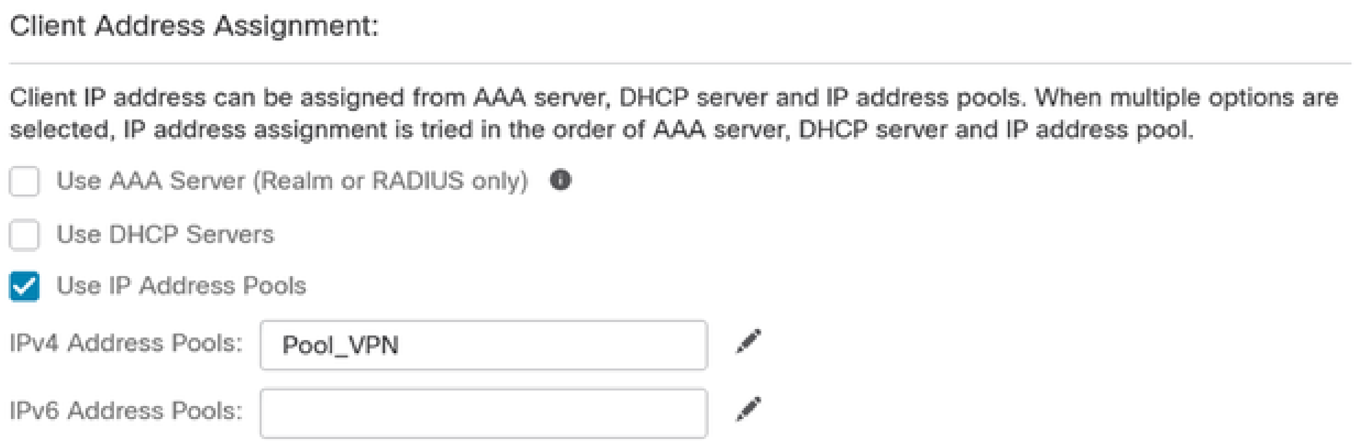
Accounting Server: ISE

(RADIUS)

Connection profile.

7. Set up dynamic IP address assignment for VPN.

Caution: For example purposes, the DHCP VPN pool was selected.



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

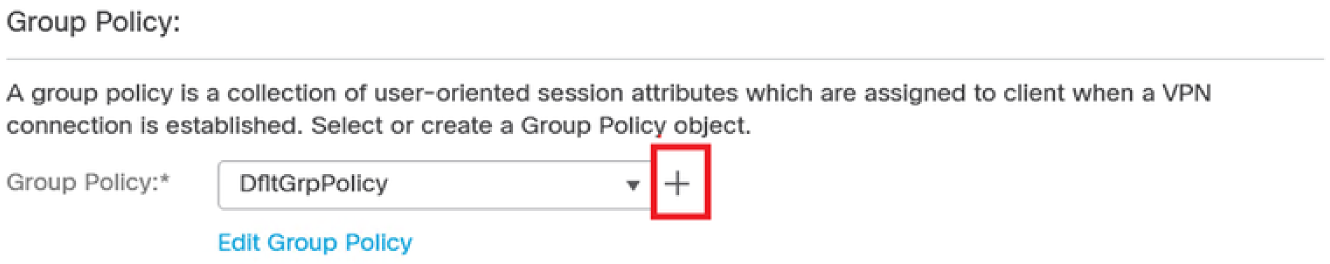
☑ Use IP Address Pools

IPv4 Address Pools: Pool_VPN

IPv6 Address Pools:

IP Address pool.

8. Proceed to create a new Group Policy.



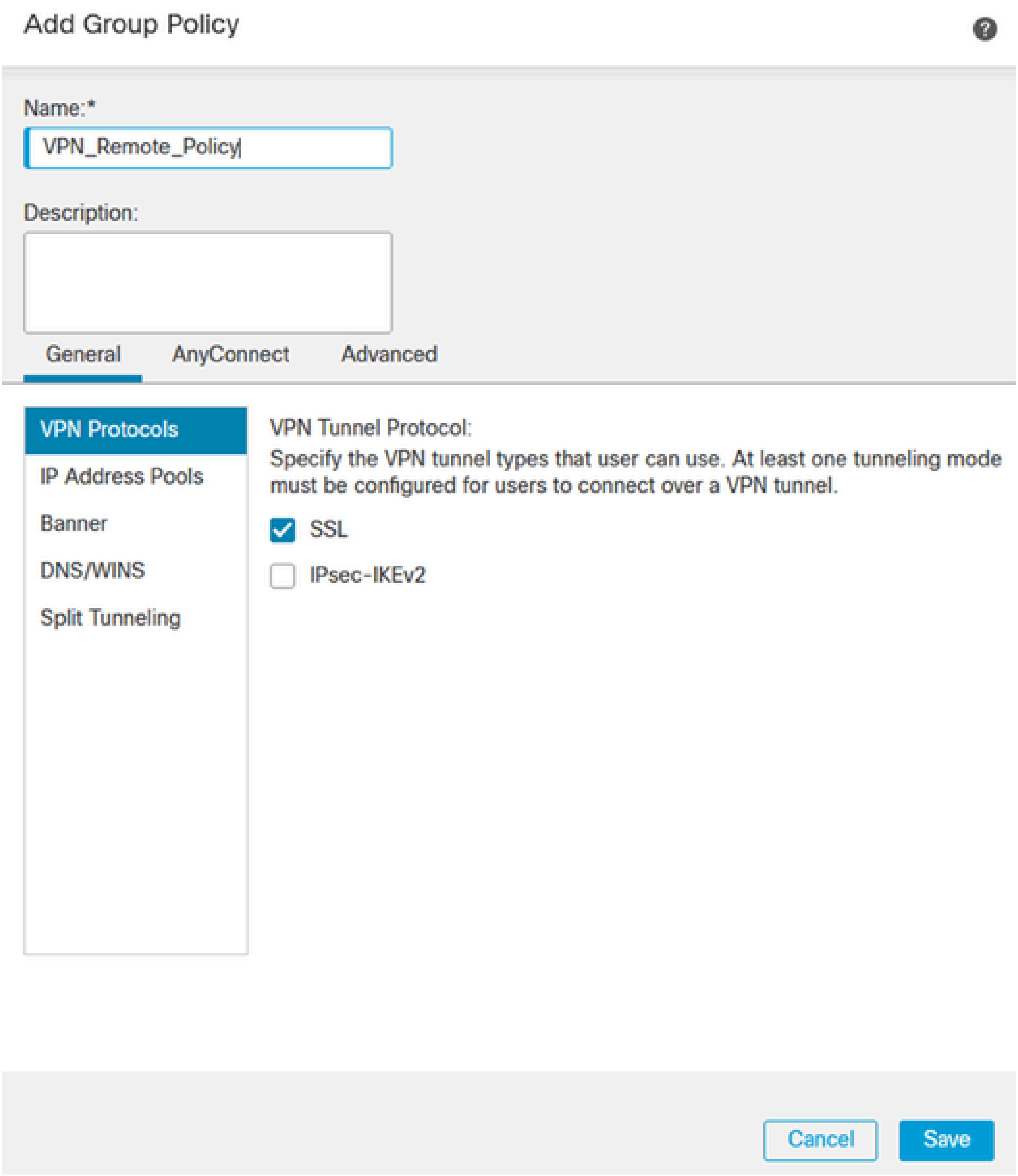
Group Policy:

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:* DfltGrpPolicy

Group policy.

9. In the **Group Policy** settings, ensure the SSL protocol is selected.



Add Group Policy

Name:* VPN_Remote_Policy

Description:

VPN Tunnel Protocol:

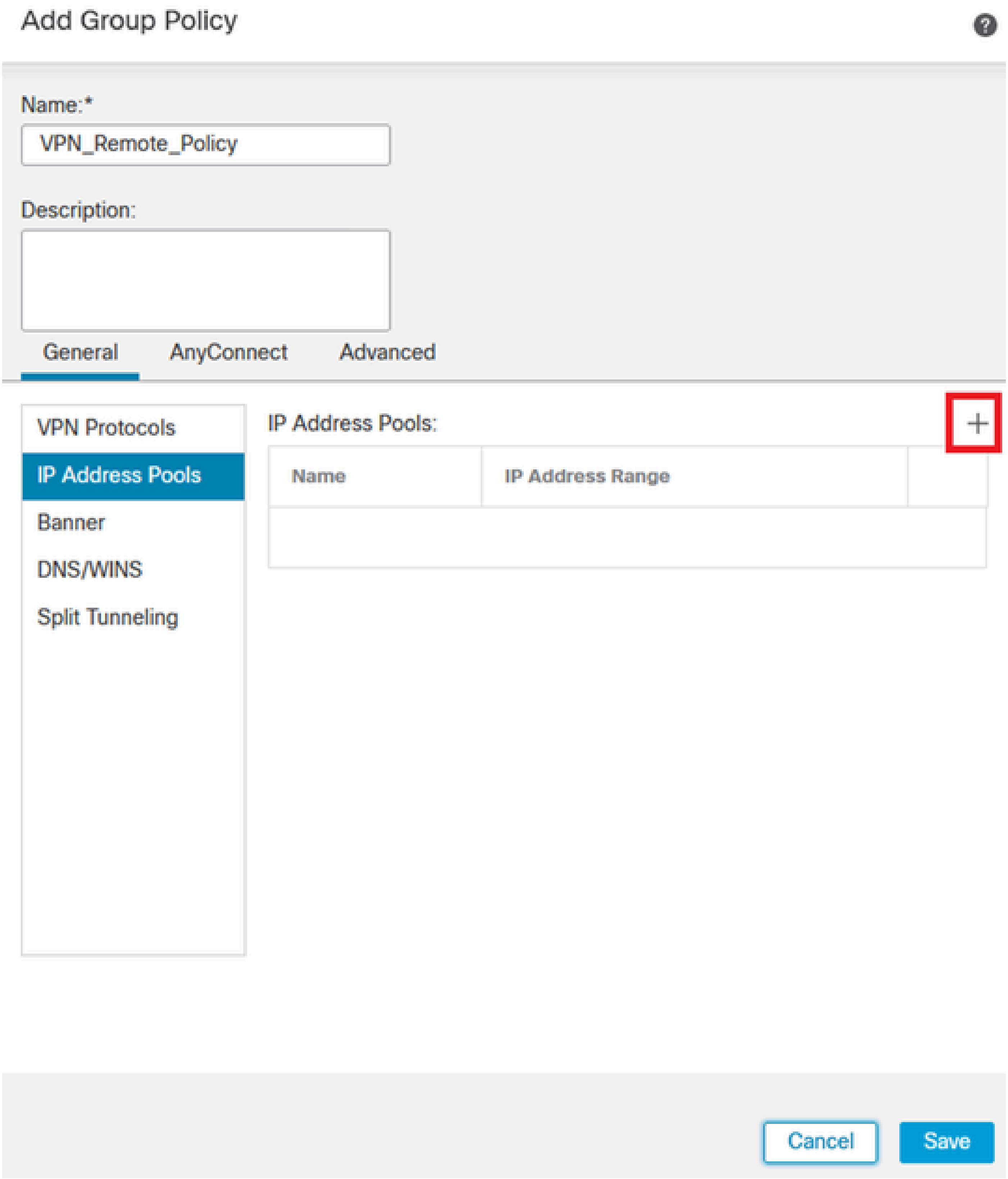
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☑ SSL

□ IPsec-IKEv2

VPN Protocols.

10. Either create a new VPN Pool or select an existing one to define the range of IP addresses available for VPN clients.



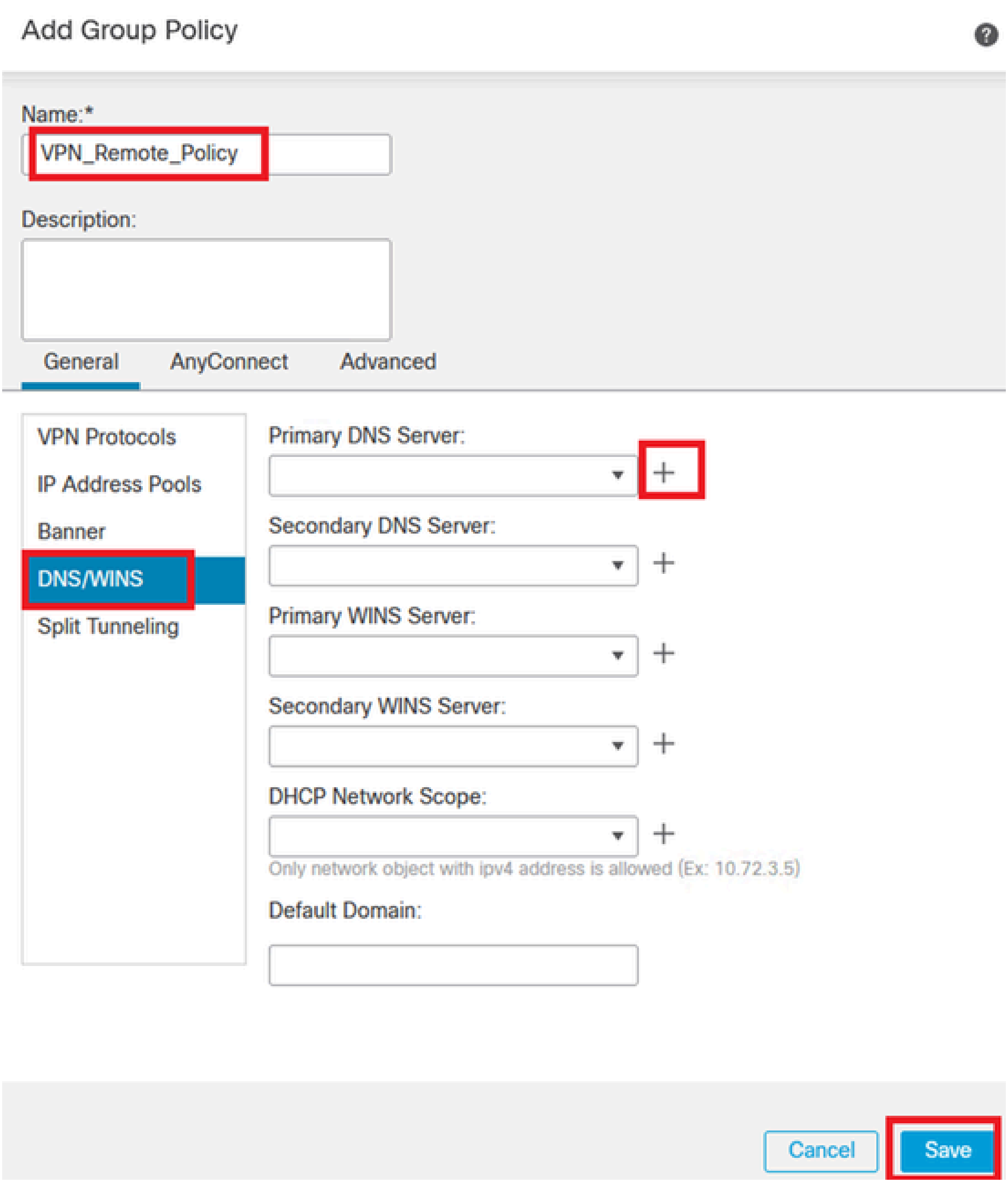
Add Group Policy

Name:* VPN_Remote_Policy

Description:

Pool VPN.

11. Specify the DNS Server details for the VPN connection.



Add Group Policy

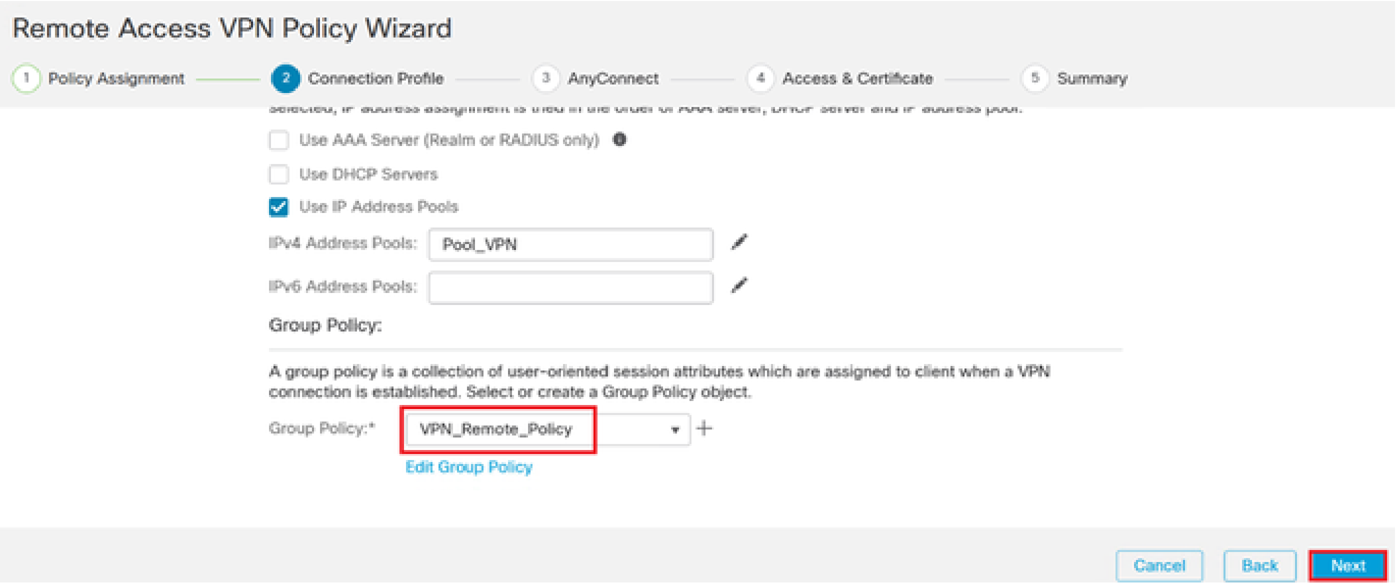
Name:* VPN_Remote_Policy

Description:

DNS Settings.

Warning: Please note that additional features such as the Banner, Split Tunneling, AnyConnect, and Advanced options are considered optional for this configuration.

12. After configuring the necessary details, click **Next** to proceed to the next phase of the setup.



Remote Access VPN Policy Wizard

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

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: Pool_VPN

IPv6 Address Pools:

Group Policy:

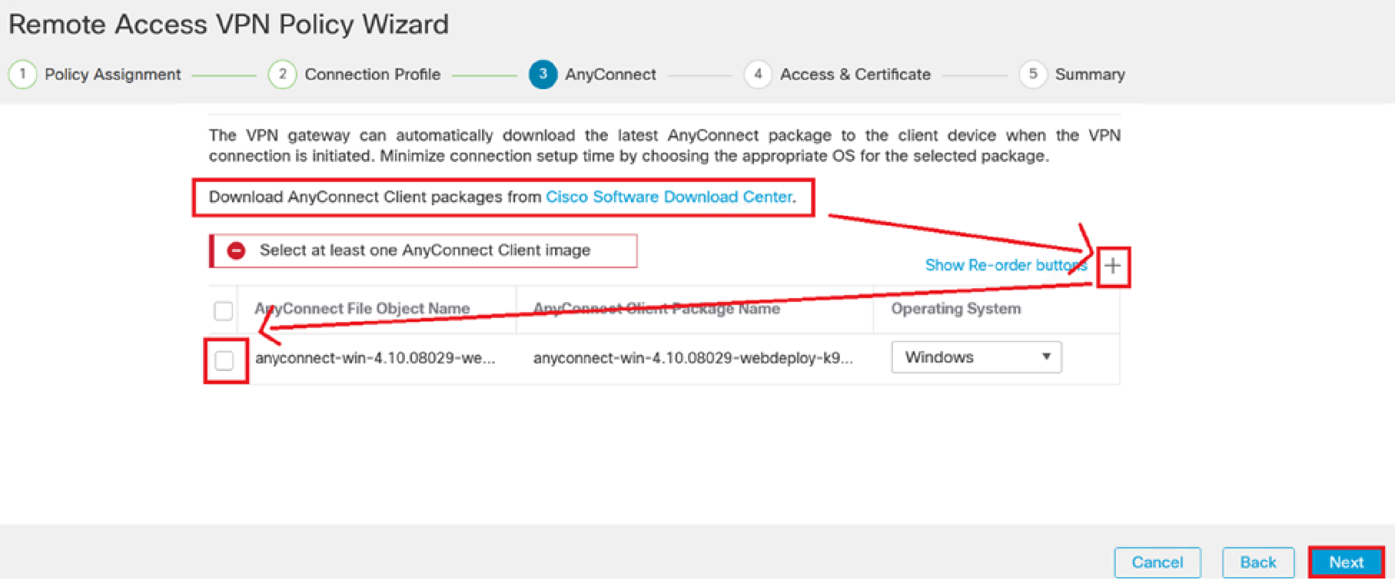
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* VPN_Remote_Policy

Edit Group Policy

Group Policy.

13. Select the appropriate AnyConnect package for the VPN users. If the required package is not listed, you have the option to add the necessary package at this stage.



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.

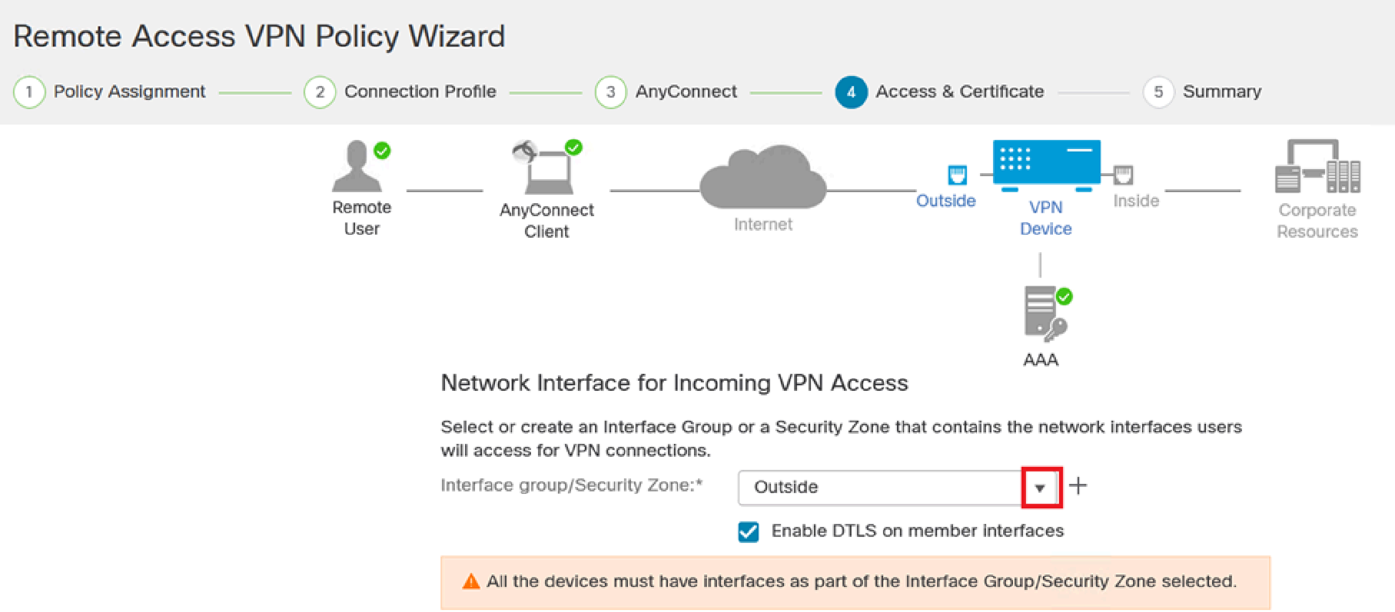
Select at least one AnyConnect Client image

Show Re-order buttons +

□	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
□	anyconnect-win-4.10.08029-we...	anyconnect-win-4.10.08029-webdeploy-k9...	Windows

Package installation.

14. Choose the network interface on the FTD device in which you want to enable the VPN remote feature.



Remote Access VPN Policy Wizard

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:* Outside

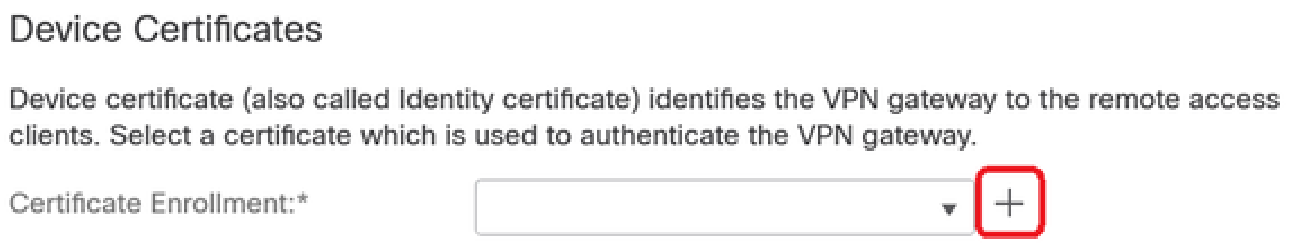
☑ Enable DTLS on member interfaces

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

VPN Interface

15. Establish a Certificate enrollment process by selecting one of the available methods to create and install the certificate on the firewall, which is crucial for secure VPN connections.

Caution: For example, a self-signed certificate was selected in this guide.

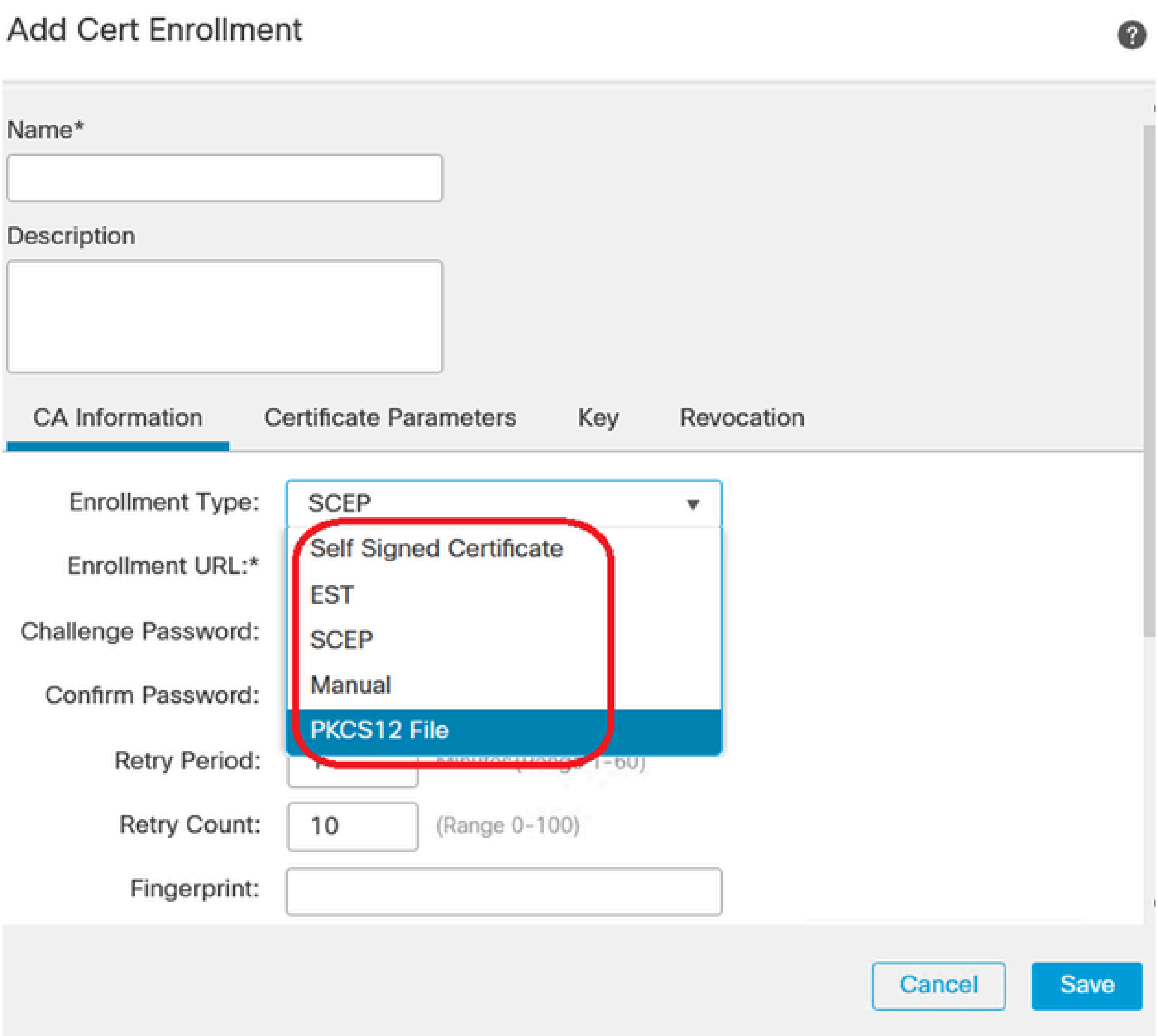


Device Certificates

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:*

Device Certificate.



Add Cert Enrollment

Name*

Description

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

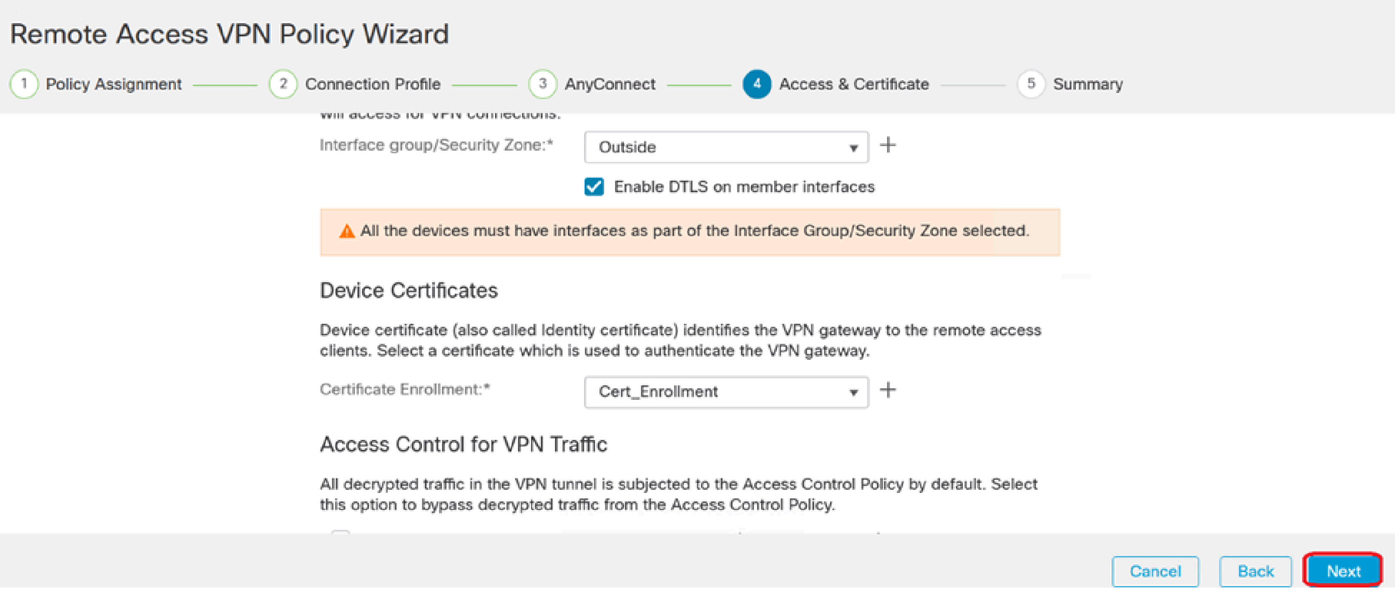
Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint:

Cert Enrollment.

16. Click **Next** once the certificate enrollment is configured.



will access for VPN connections.

Interface group/Security Zone:* Outside ▾ +

☑ 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.

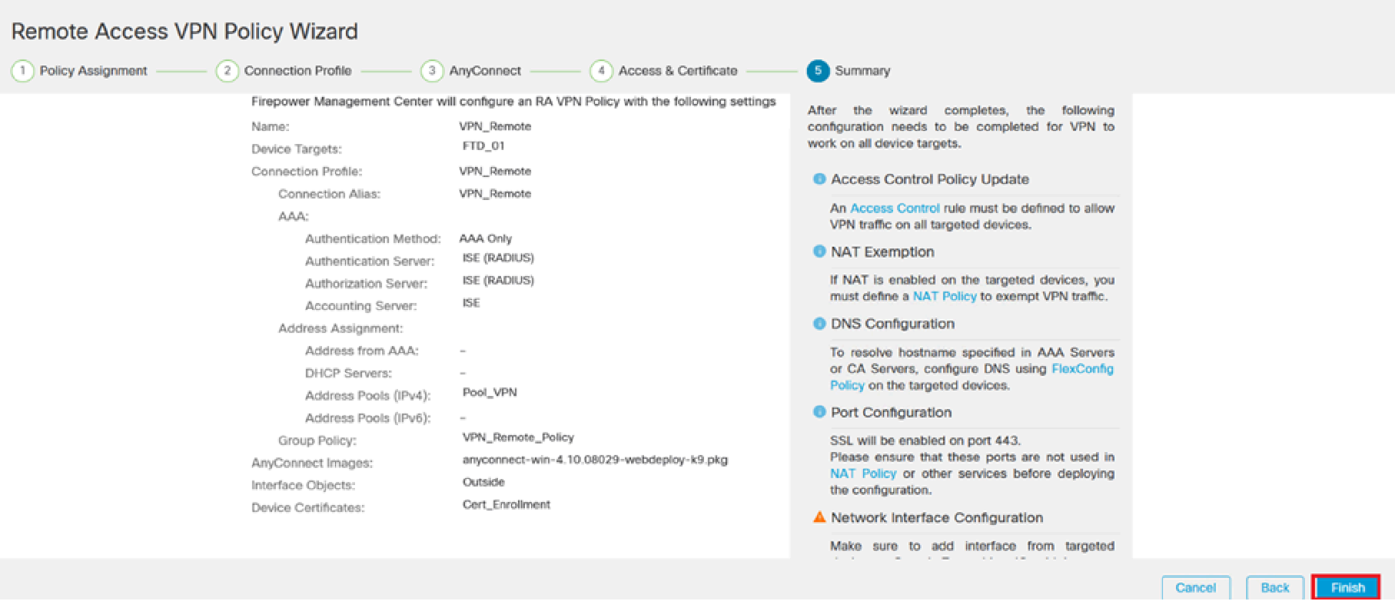
Certificate Enrollment:* Cert_Enrollment ▾ +

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.

Summary of Access & services

17. Review the summary of all your configurations to ensure they are accurate and reflect your intended setup.



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.

Access Control Policy Update

An Access Control rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption

If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.

DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.

Port Configuration

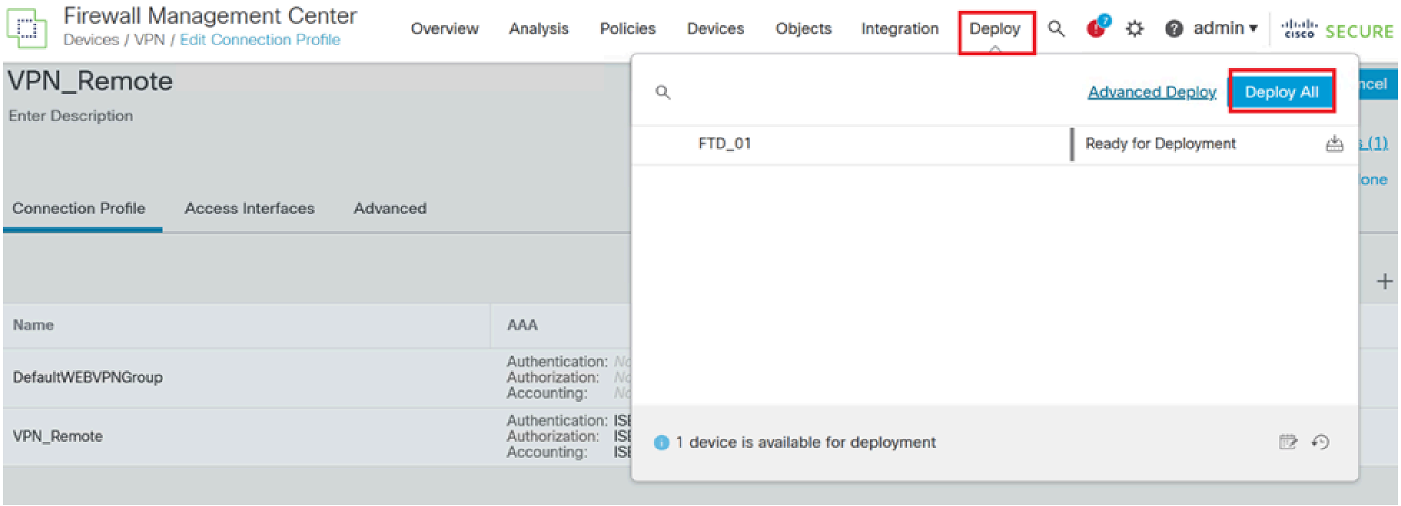
SSL will be enabled on port 443.
Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

⚠ Network Interface Configuration

Make sure to add interface from targeted

Summary of VPN settings.

18. To apply and activate the VPN remote access configuration, navigate to **Deploy** > **Deploy All** and execute the deployment to the selected FTD device.



Name	AAA
DefaultWEBVPNGroup	Authentication: No Authorization: No Accounting: No
VPN_Remote	Authentication: ISE Authorization: ISE Accounting: ISE

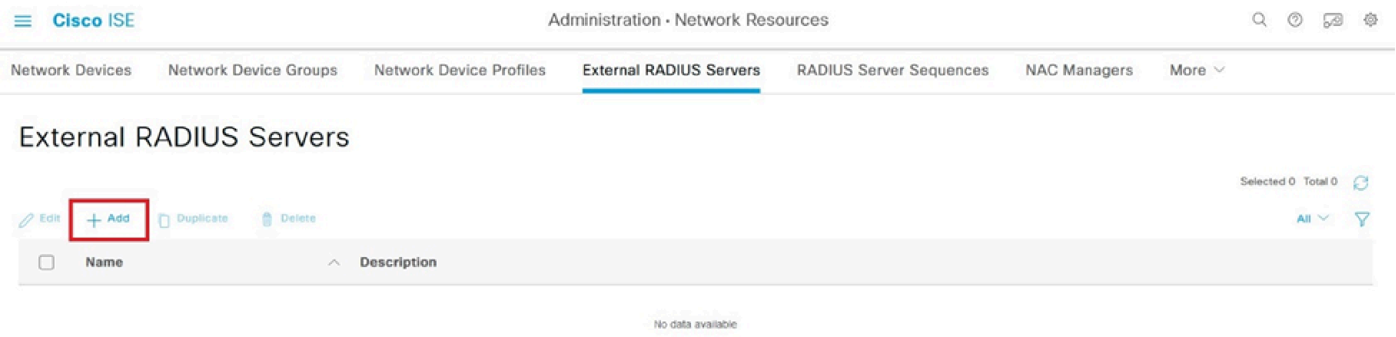
Deploying VPN Settings.

ISE configurations.

Integrate DUO as an External Radius Server.

1. Navigate to **Administration** > **Network Resources** > **External RADIUS Servers** in the Cisco ISE administrative interface.

2. Click the **Add** button to configure a new external RADIUS server.



External Radius Servers

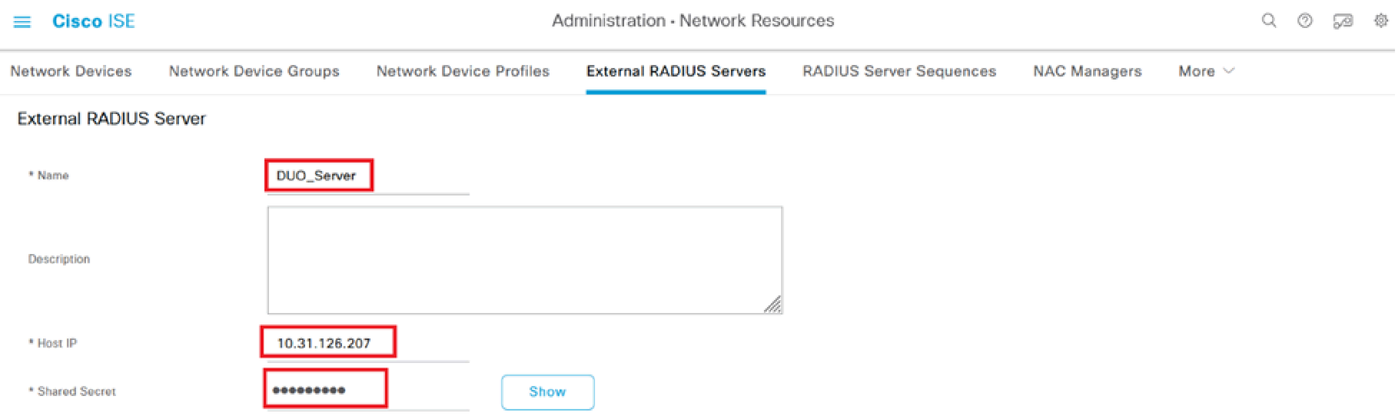
3. Enter a name for the Proxy DUO Server.

4. Input the correct IP address for the Proxy DUO Server to ensure proper communication between the ISE and the DUO server.

5. Set the shared secret key.

Note: This shared secret key must be configured into the Proxy DUO Server to establish a RADIUS connection successfully.

6. Once all the details are correctly entered, click **Submit** to save the new Proxy DUO Server configuration.



External RADIUS Server

* Name: DUO_Server

Description:

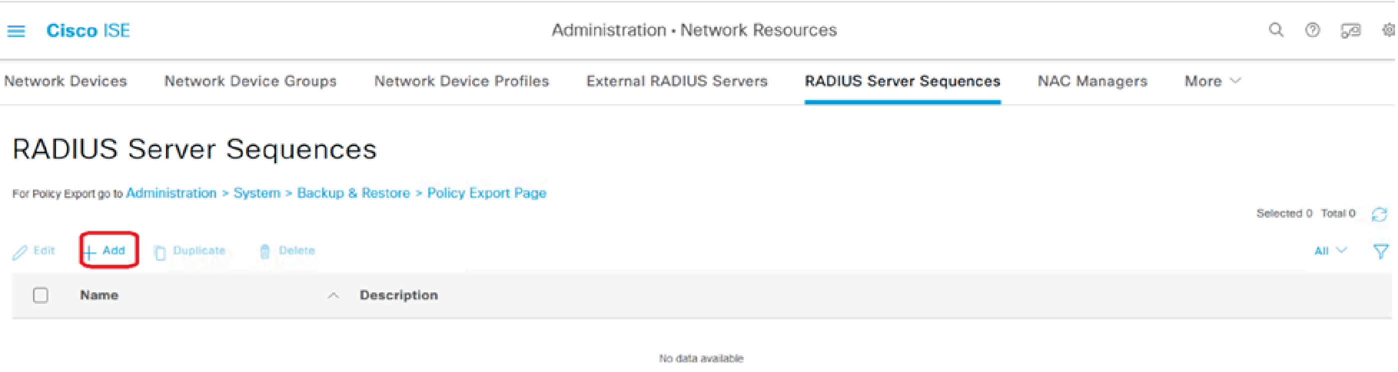
* Host IP: 10.31.126.207

* Shared Secret: •••••••••

External RADIUS Servers

7. Proceed to **Administration > RADIUS Server Sequences**.

8. Click **Add** to create a new RADIUS server sequence.



RADIUS Server Sequences

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

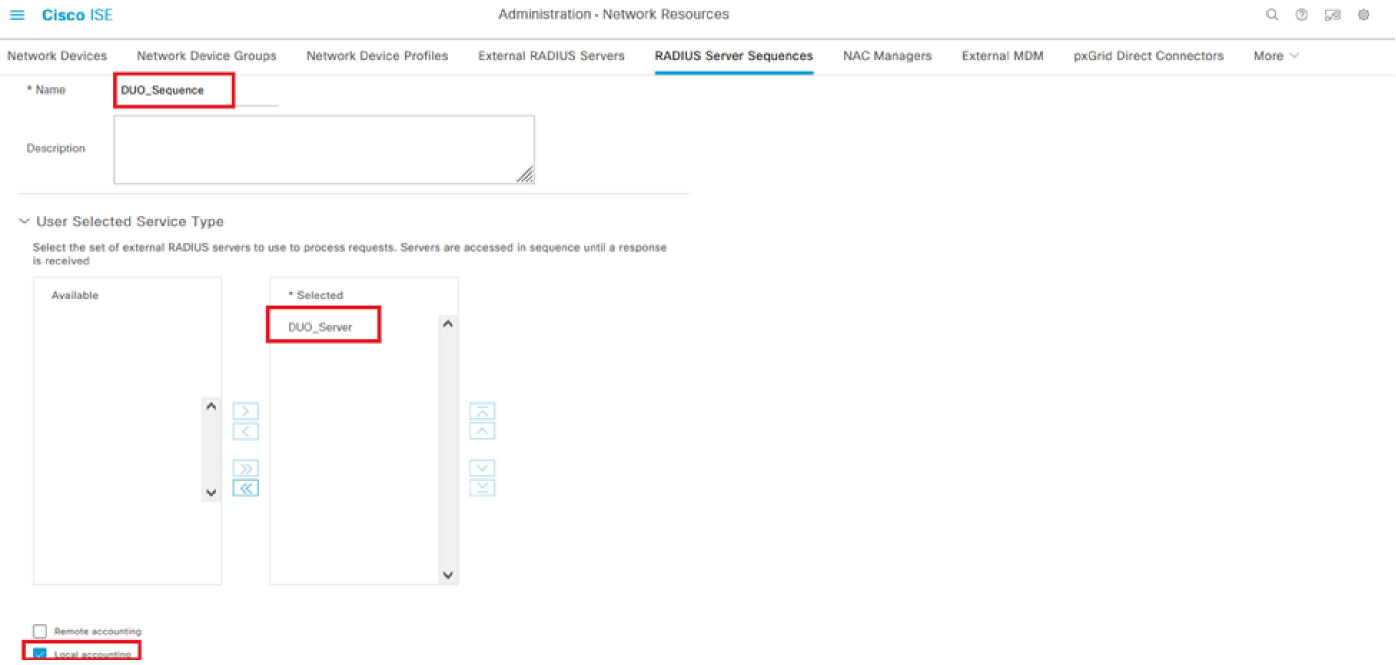
No data available

RADIUS Server Sequences

9. Provide a distinct name for the RADIUS Server Sequence for easy identification.

10. Locate the previously configured DUO RADIUS Server, referred to as **DUO_Server** in this guide, and move it to the selected list on the right to include it in the sequence.

11. Click **Submit** to finalize and save the **RADIUS Server Sequence** configuration.



* Name: DUO_Sequence

Description

User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is received

* Selected: DUO_Server

☐ Remote accounting

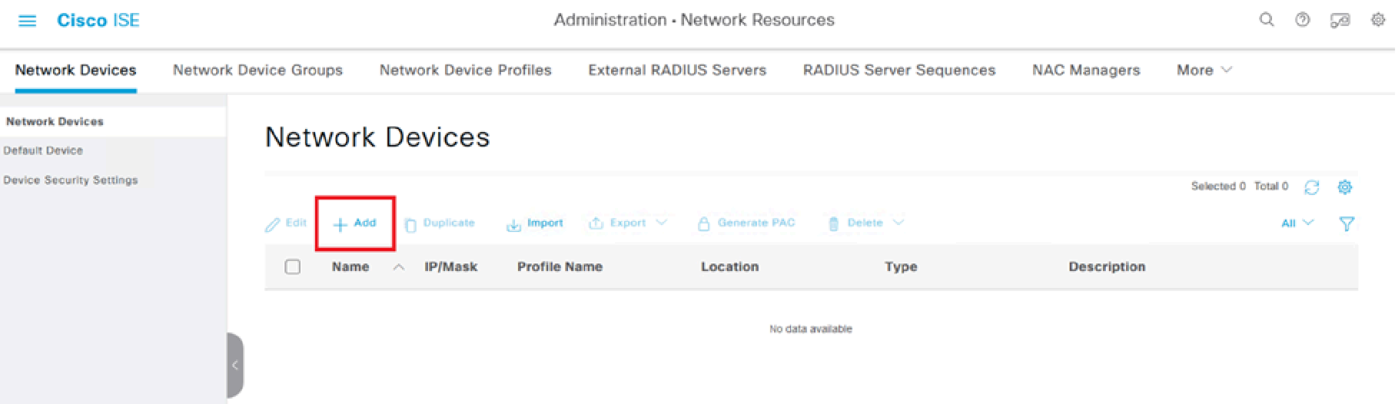
☑ Local accounting

Radius Server Sequences configuration.

Integrate the FTD as a Network Access Device.

1. Navigate to the **Administration** section in your system interface, and from there, select **Network Resources** to access the configuration area for network devices.

2. Once in the **Network Resources** section, locate and click the **Add** button to initiate the process of adding a new Network Access Device.



□	Name	IP/Mask	Profile Name	Location	Type	Description

No data available

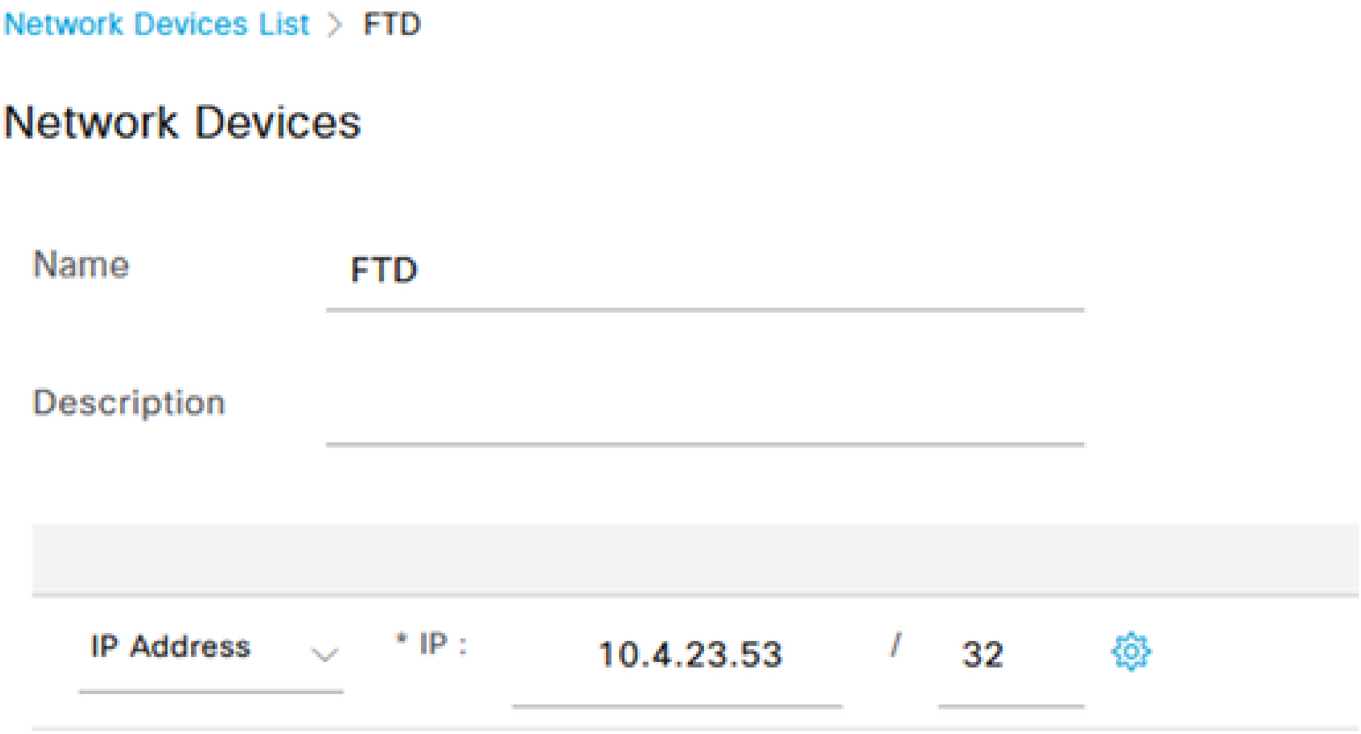
Network Access Devices.

3. In the provided fields, enter the Network Access Device name to dentify the device within your network.

4. Proceed to specify the IP Address of the FTD (Firepower Threat Defense) device.

5. Input the key that was previously established during the FMC (Firepower Management Center) setup. This key is essential for secure communication between devices.

6. Complete the process by clicking the **Submit** button.

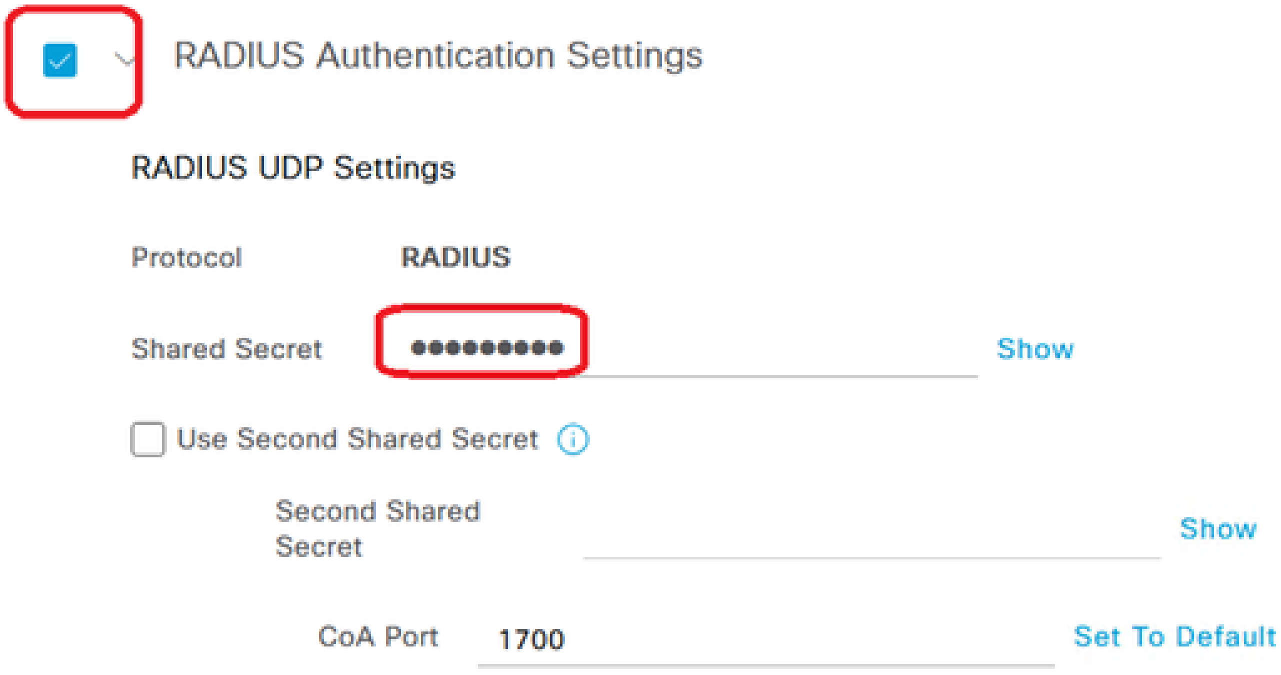


Name FTD

Description

IP Address * IP : 10.4.23.53 / 32

Adding FTD as NAD.



☑ 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 settings

DUO configurations.

DUO Proxy Installation.

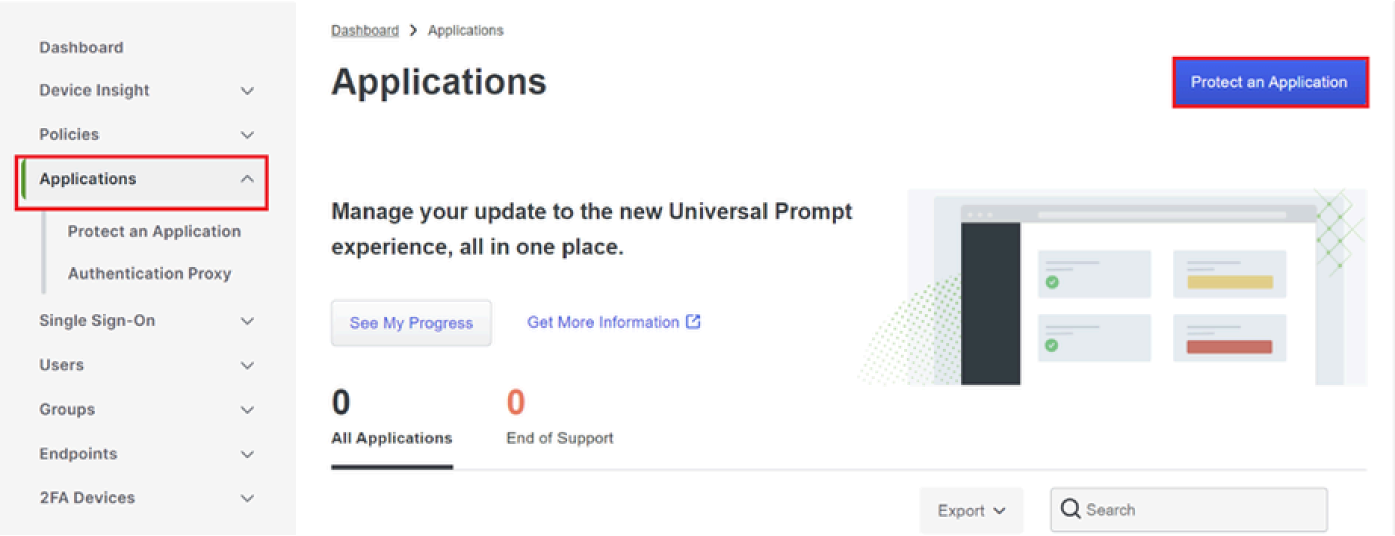
Access the **DUO Proxy Download and Installation Guide** by clicking on the next link:

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

Integrate DUO Proxy with ISE and DUO Cloud.

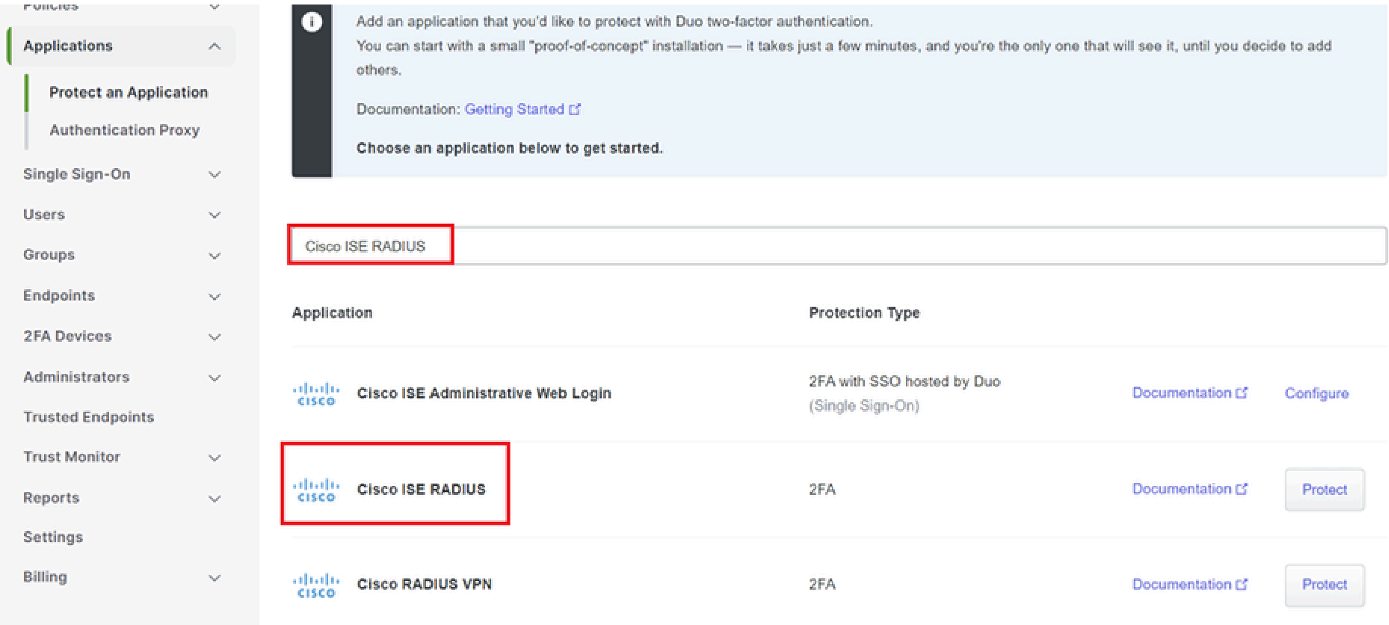
1. Log in to the DUO Security website at https://duo.com/ using your credentials.

2. Navigate to the **Applications** section and select **Protect** an application to proceed.



DUO Applications

3. Search for the "**Cisco ISE RADIUS**" option in the list and click **Protect** to add it to your applications.



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.

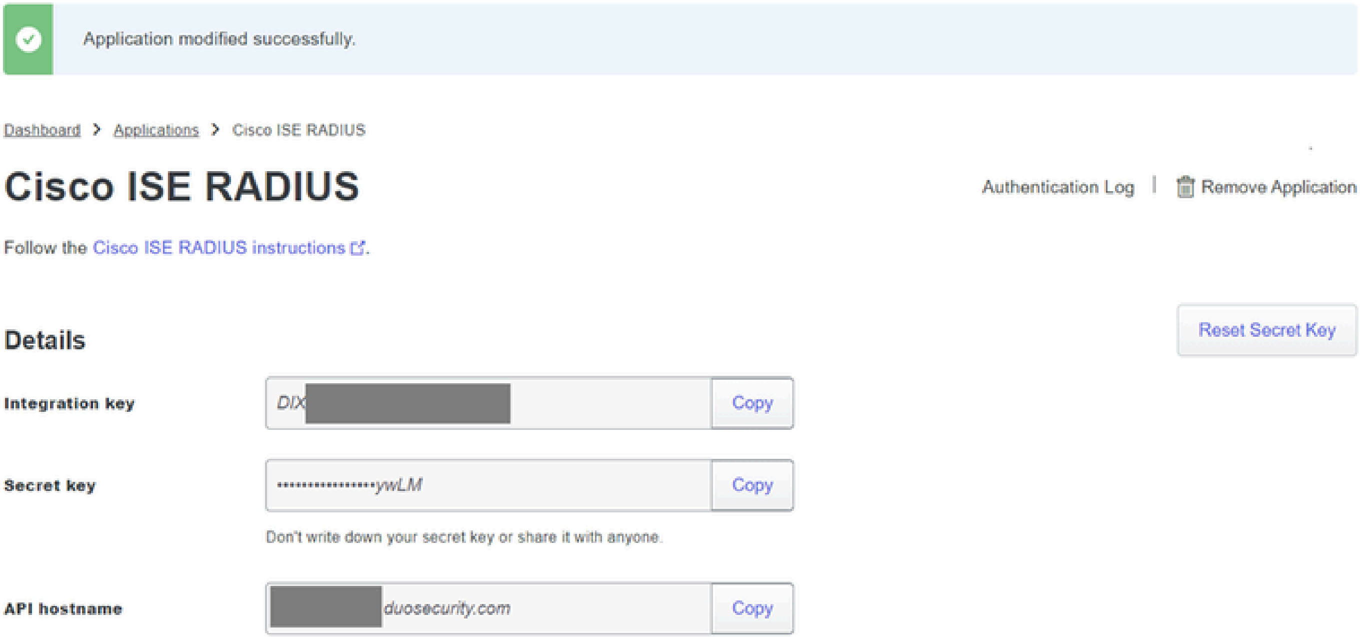
Cisco ISE RADIUS

Application	Protection Type		
Cisco ISE Administrative Web Login	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Configure
Cisco ISE RADIUS	2FA	Documentation	Protect
Cisco RADIUS VPN	2FA	Documentation	Protect

ISE RADIUS option

4. Upon successful addition, you are going to see the details of the DUO application. Scroll down and click **Save**.

5. Copy the provided integration key, secret key, and API hostname; these are crucial for the upcoming steps.


Application modified successfully.

Dashboard > Applications > Cisco ISE RADIUS

Cisco ISE RADIUS

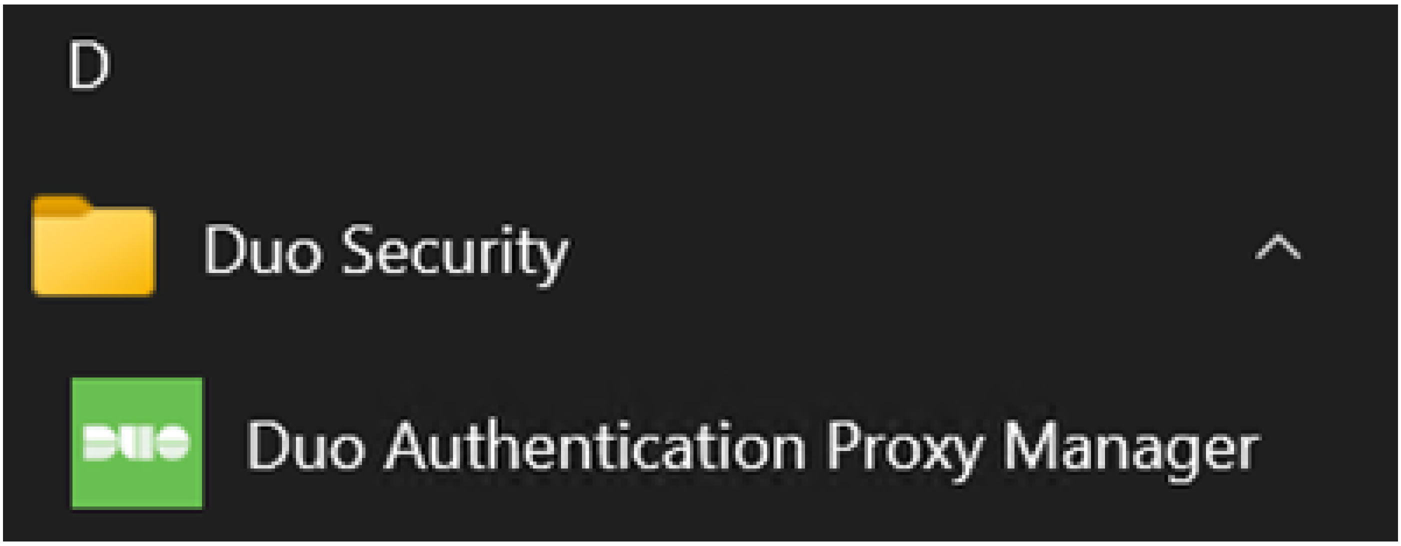
Follow the Cisco ISE RADIUS instructions.

Details

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 Server details

6. Launch the **DUO Proxy Manager** on your system to continue with the setup.



DUO Proxy Manager

7. (Optional) If your DUO Proxy Server requires a proxy configuration to connect to the DUO Cloud, input the next parameters:

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

Caution: Ensure that you replace and with your actual proxy details.

8. Now, utilize the information you copied earlier to complete the integration configuration.

```
[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
```

Tip: The line client=ad_client is an indication that the DUO Proxy authenticates using an Active Directory account. Ensure this information is correct to complete the synchronization with the Active Directory.

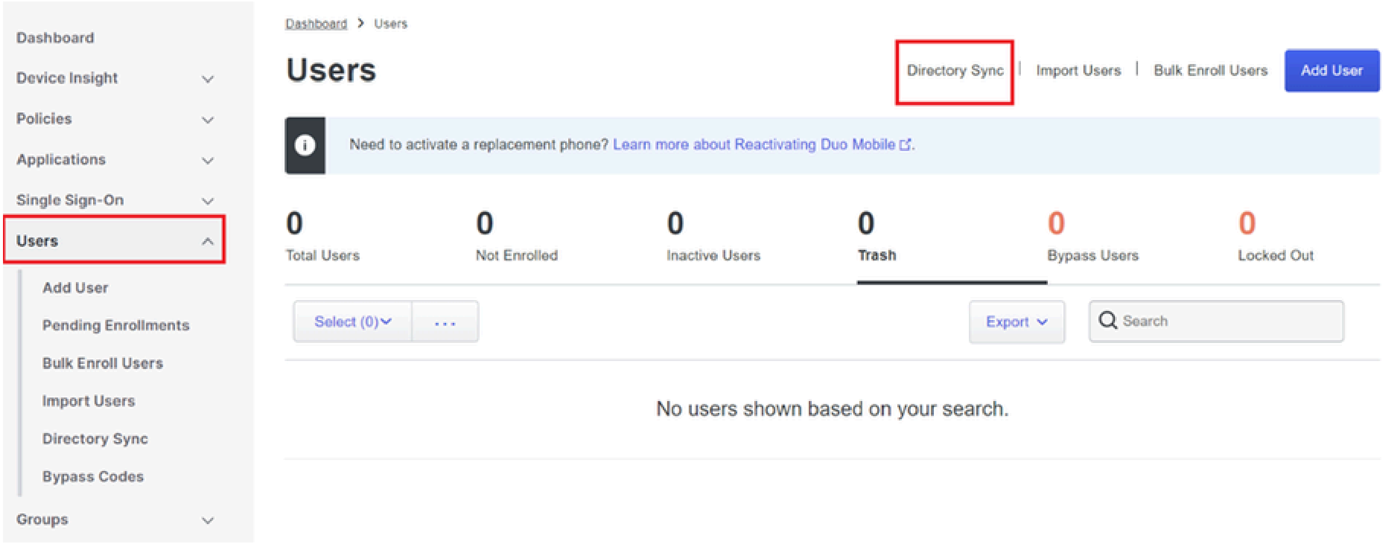
Integrate DUO with Active Directory.

1. Integrate the DUO Authentication Proxy with your Active Directory.

```
[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. Join your Active Directory with DUO cloud services. Log in to https://duo.com/.

3. Navigate to "**Users**" and select "**Directory Sync**" to manage synchronization settings.

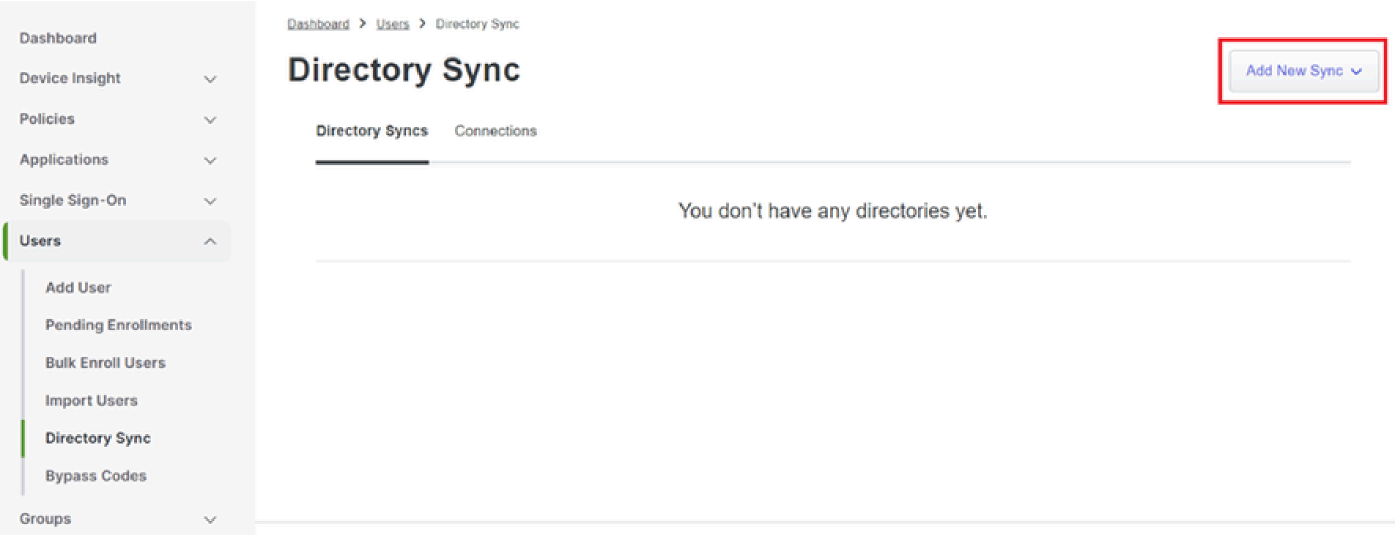


Need to activate a replacement phone? Learn more about Reactivating Duo Mobile.

No users shown based on your search.

Directory Sync

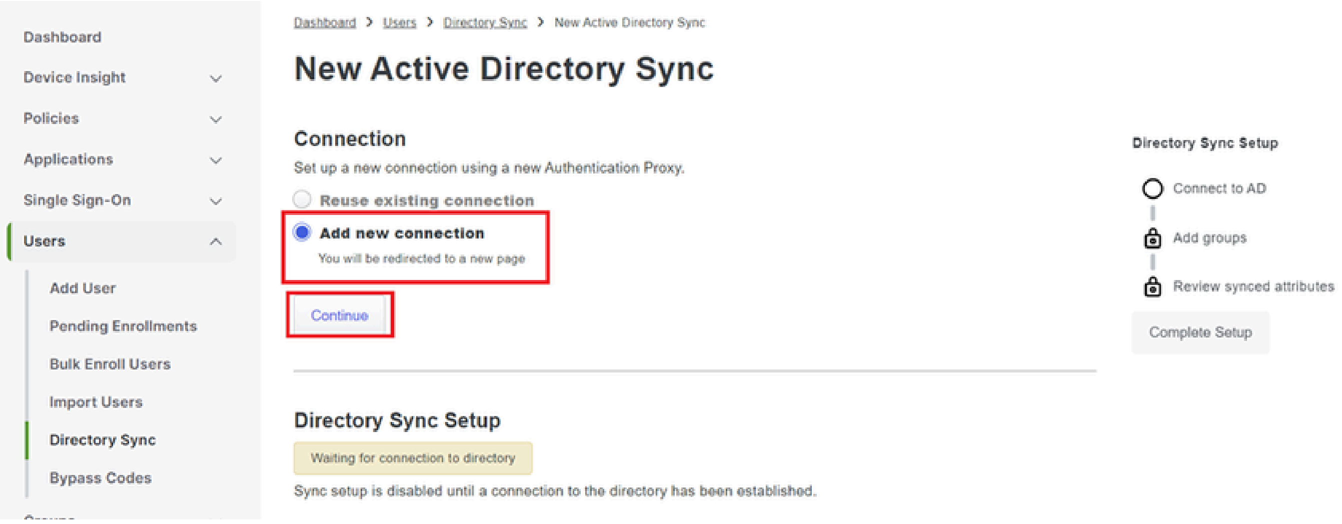
4. Click "**Add New Sync**" and choose "**Active Directory**" from the options provided.



You don't have any directories yet.

Add New Sync

5. Select **Add new connection** and click **Continue**.



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

Continue

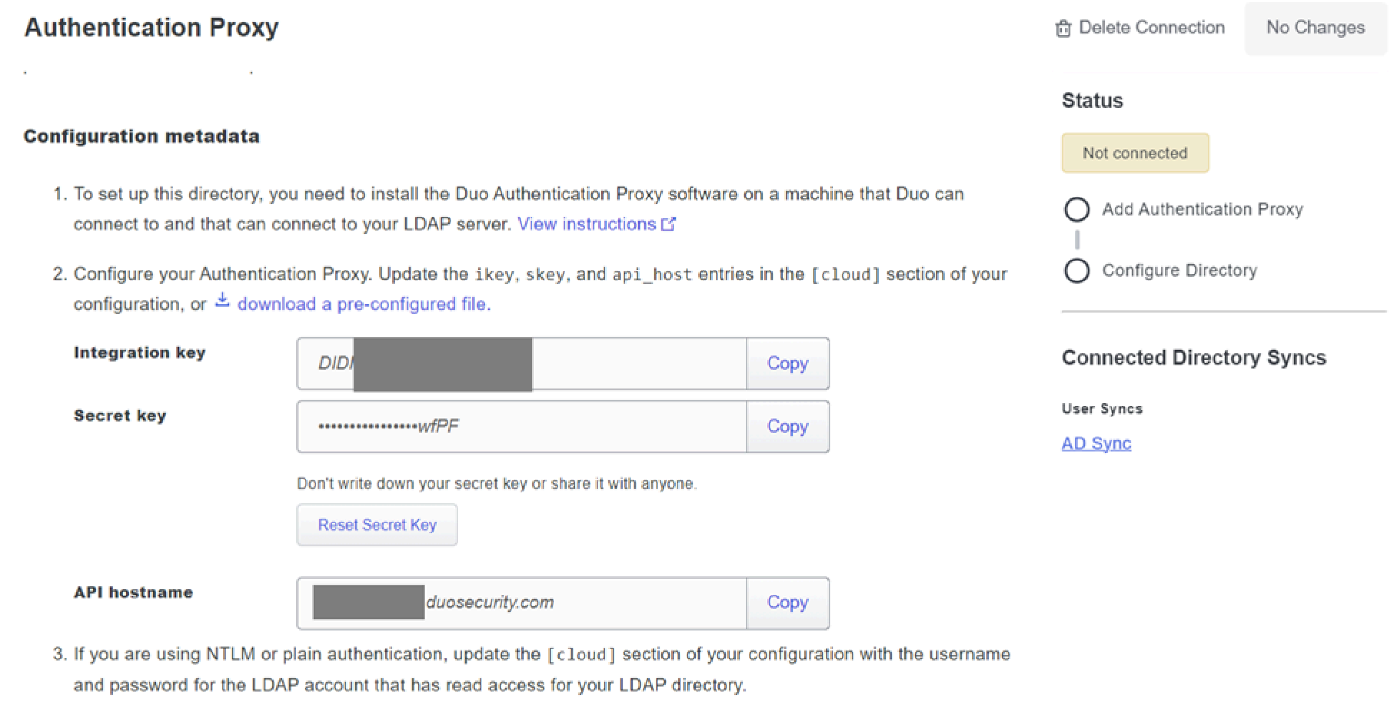
Directory Sync Setup

Waiting for connection to directory

Sync setup is disabled until a connection to the directory has been established.

Adding new Active Directory

6. Copy the generated integration key, secret key, and API hostname.



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	DIDI[redacted]	Copy
Secret key	•••••••••••••••••wfPF	Copy

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

Reset Secret Key

API hostname	[redacted]duosecurity.com	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.

Status

Not connected

○ Add Authentication Proxy

○ Configure Directory

Connected Directory Syncs

User Syncs

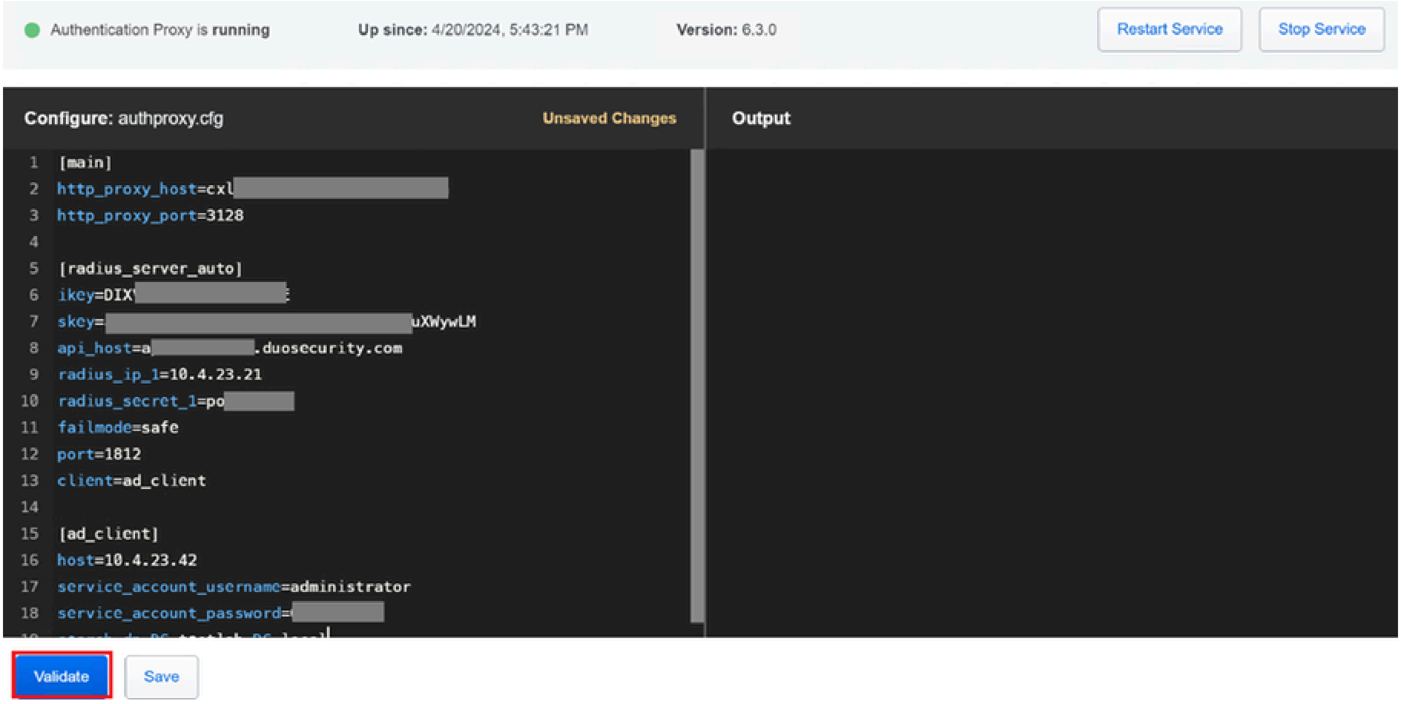
AD Sync

Authentication Proxy details

7. Return to the DUO Authentication Proxy configuration and configure the [cloud] section with the new parameters youve obtained, as well as the service account credentials for an Active Directory administrator:

```
[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>
```

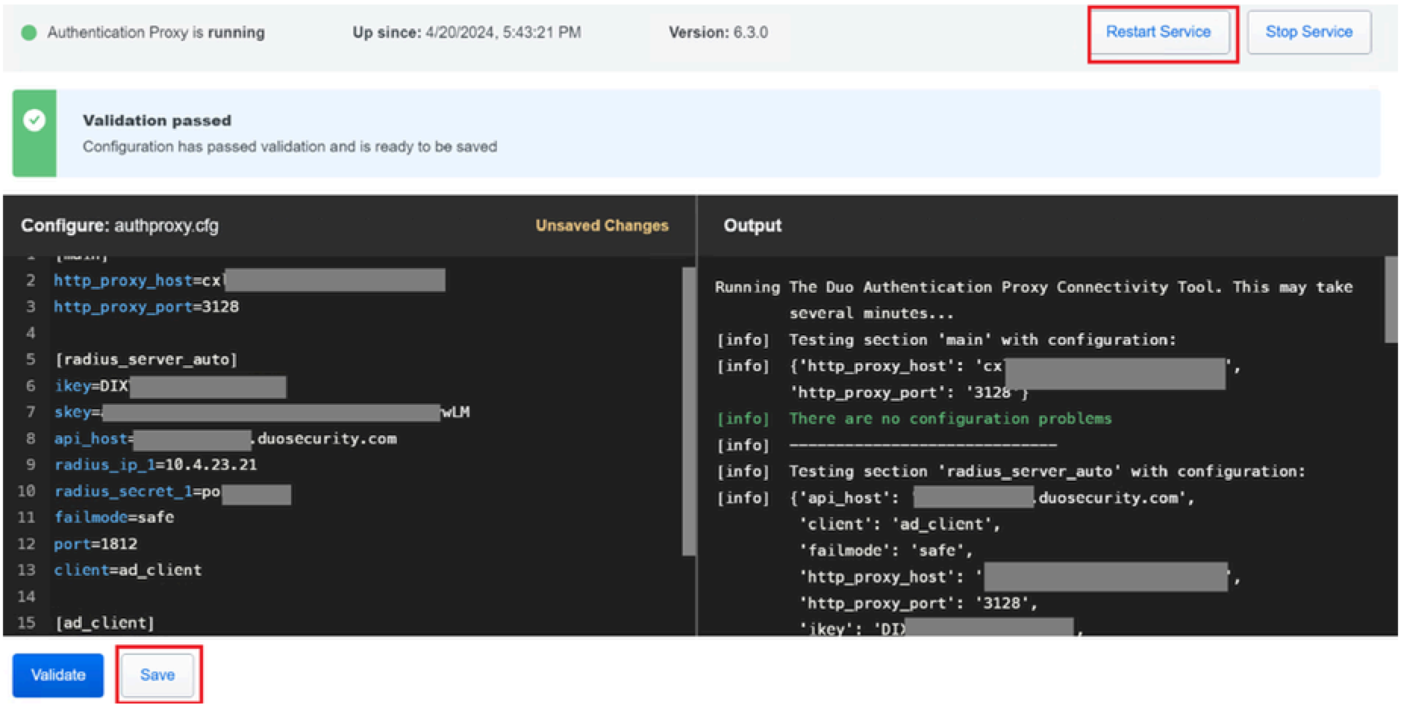
8. Validate your configuration by selecting the "**validate**" option to ensure all settings are correct.



```
[main]
http_proxy_host=cxl[redacted]
http_proxy_port=3128

[radius_server_auto]
ikey=DIX[redacted]
skey=[redacted]uXWywLM
api_host=a[redacted].duosecurity.com
radius_ip_1=10.4.23.21
radius_secret_1=po[redacted]
failmode=safe
port=1812
client=ad_client

[ad_client]
host=10.4.23.42
service_account_username=administrator
service_account_password=[redacted]
```

Configuration of Proxy DUO.

9. After validation, save your configuration and restart the DUO Authentication Proxy service to apply changes.



Validation passed

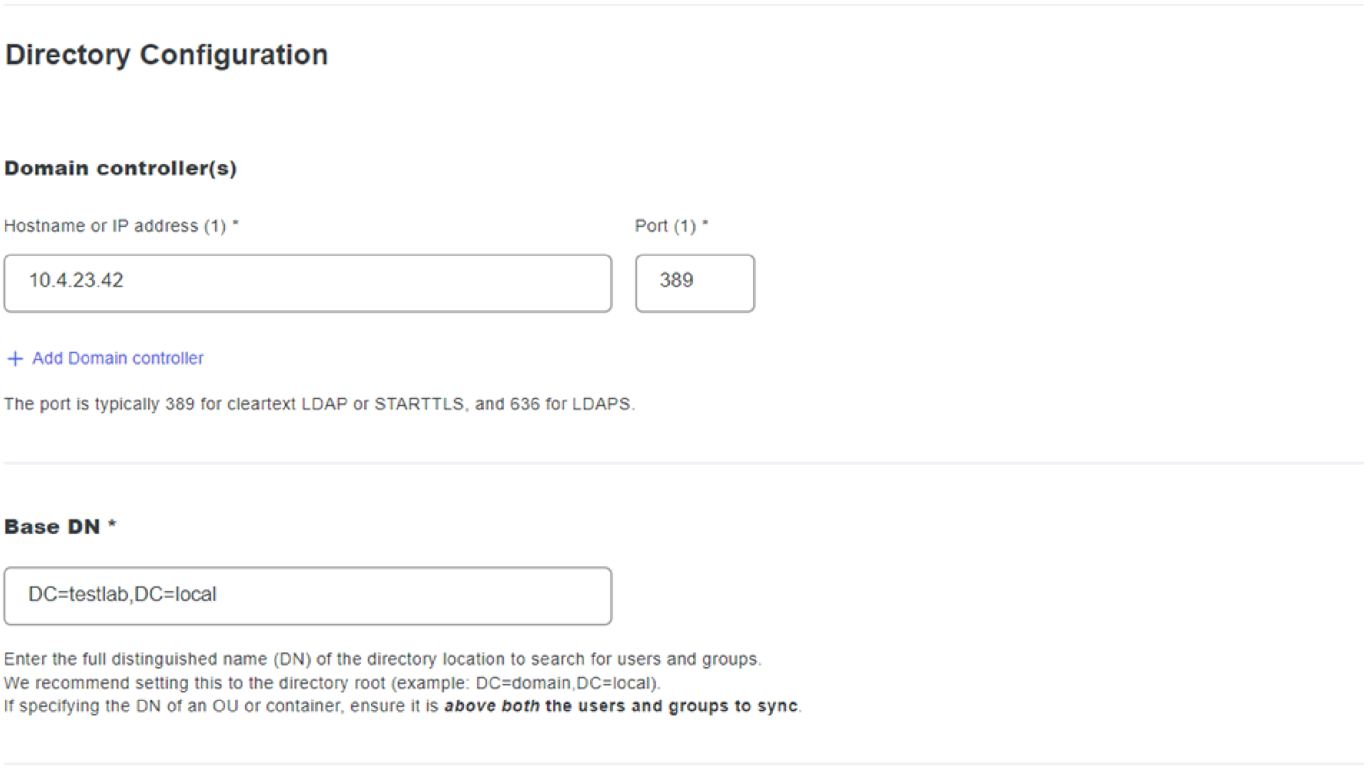
Configuration has passed validation and is ready to be saved

```
http_proxy_host=cx[redacted]
http_proxy_port=3128

[radius_server_auto]
ikey=DIX[redacted]
skey=[redacted]wLM
api_host=[redacted].duosecurity.com
radius_ip_1=10.4.23.21
radius_secret_1=po[redacted]
failmode=safe
port=1812
client=ad_client

[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],
```

Restart Service option.

10. Back in the DUO administration dashboard, enter the IP Address of your Active Directory server along with the Base DN for user synchronization.



Directory Configuration

Domain controller(s)

Hostname or IP address (1) *: 10.4.23.42

Port (1) *: 389

+ Add Domain controller

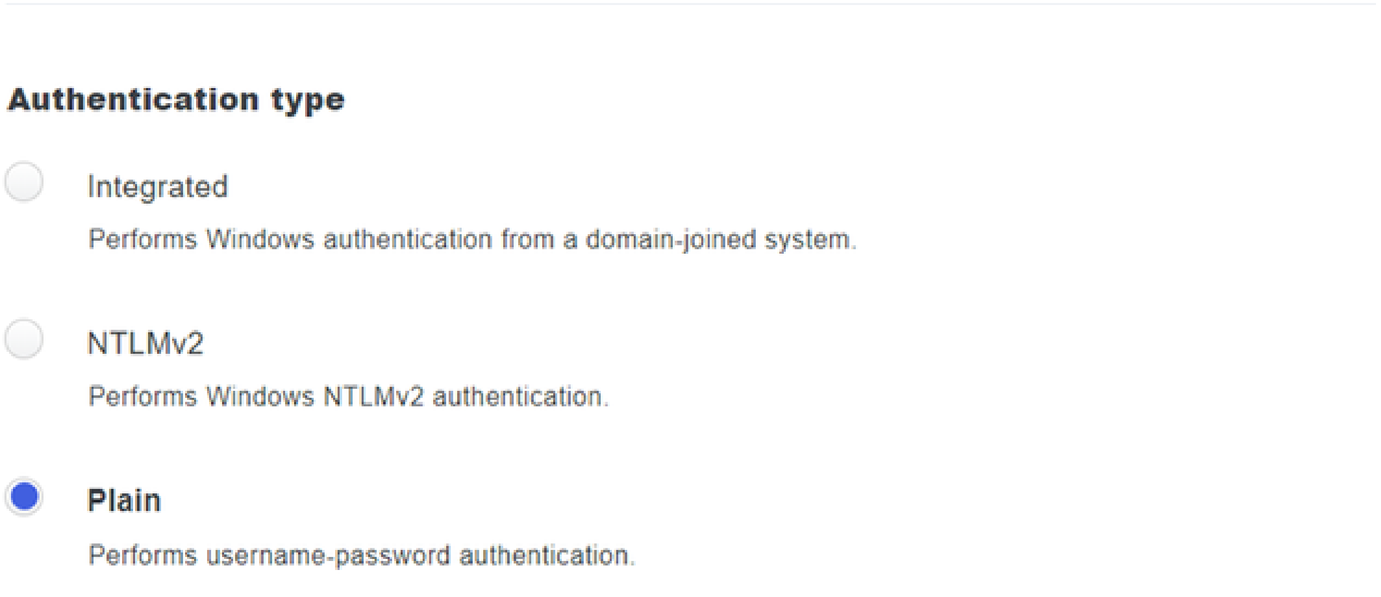
The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

Base DN *: DC=testlab,DC=local

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**.

Directory settings.

11. Select the **Plain** option to configure the system for non-NTLMv2 authentication.



Authentication type

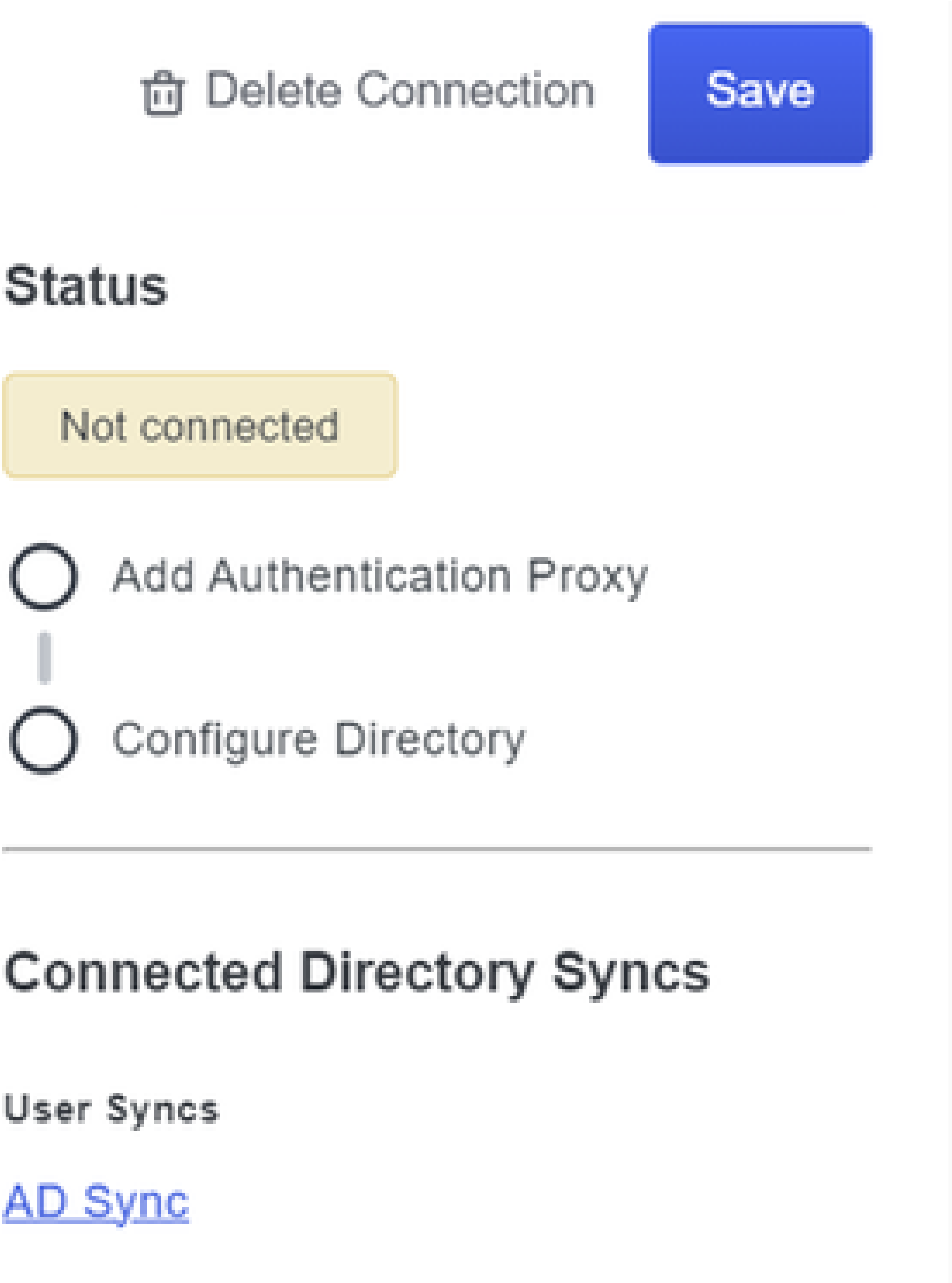
○ Integrated
Performs Windows authentication from a domain-joined system.

○ NTLMv2
Performs Windows NTLMv2 authentication.

● Plain
Performs username-password authentication.

Authentication type.

12. Save your new settings to ensure the configuration is updated.



Status

Not connected

○ Add Authentication Proxy

○ Configure Directory

Connected Directory Syncs

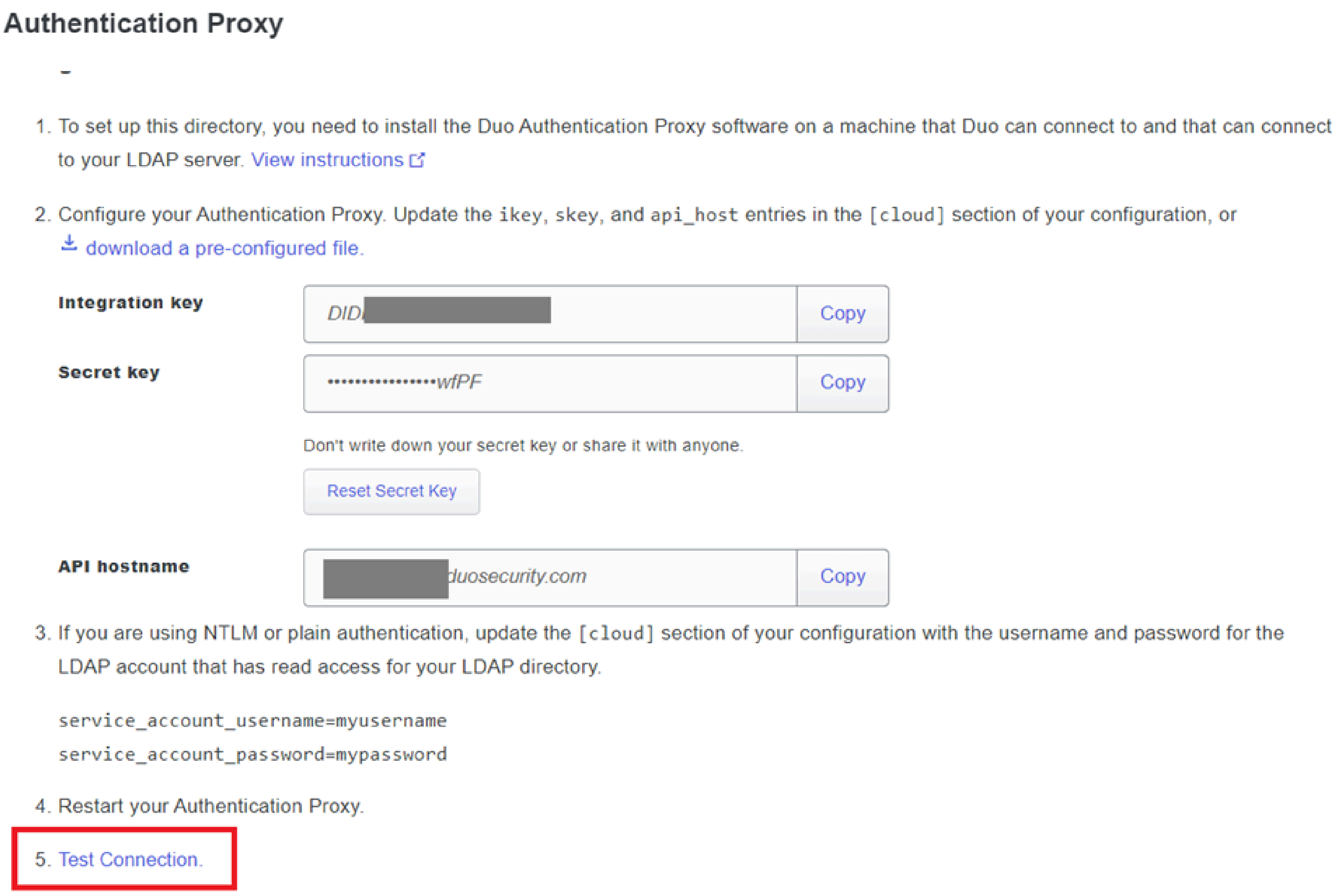
User Syncs

AD Sync

Save option

13. Utilize the "**test connection**" feature to verify that the DUO Cloud service can communicate with your

Active Directory.



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	DID[redacted]	Copy
Secret key	••••••••••••••••wfPF	Copy
	Don't write down your secret key or share it with anyone. Reset Secret Key	
API hostname	[redacted]duosecurity.com	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.

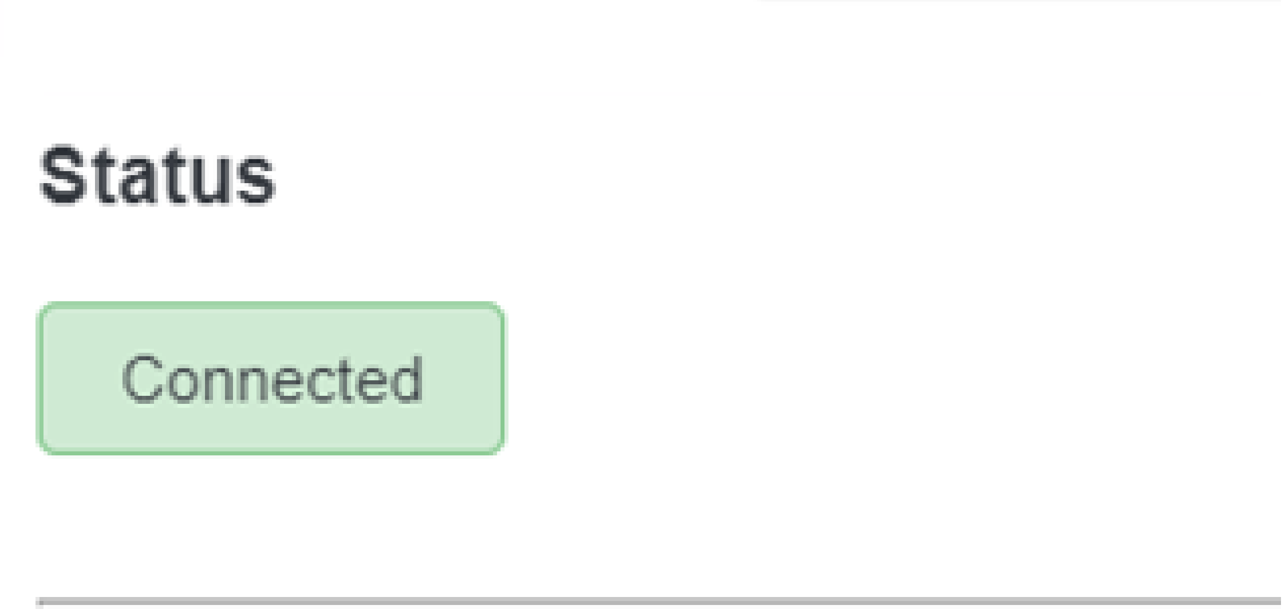
```
service_account_username=myusername
service_account_password=mypassword
```

4. Restart your Authentication Proxy.

5. Test Connection.

Test connection option.

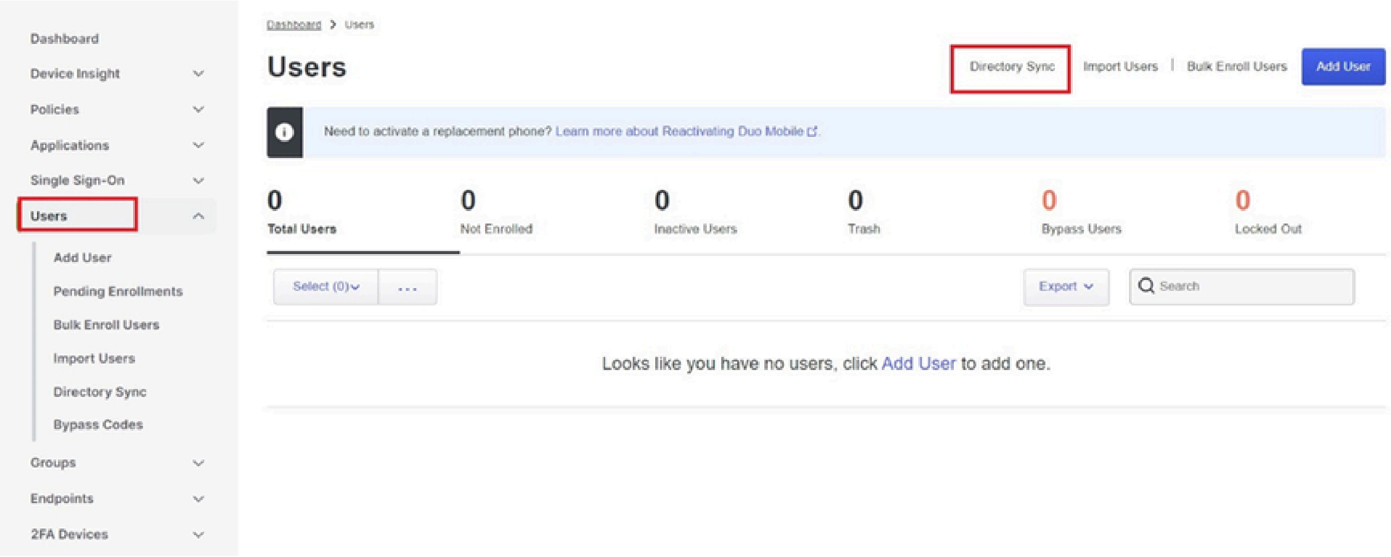
14. Confirm that the Active Directory status displays as "**Connected**," indicating a successful integration.



Status successfull.

Export user accounts from Active Directory (AD) via DUO Cloud.

1. Navigate to **Users > Directory Sync** within the Duo Admin Panel to locate the settings related to directory synchronization with Active Directory.



Need to activate a replacement phone? Learn more about Reactivating Duo Mobile

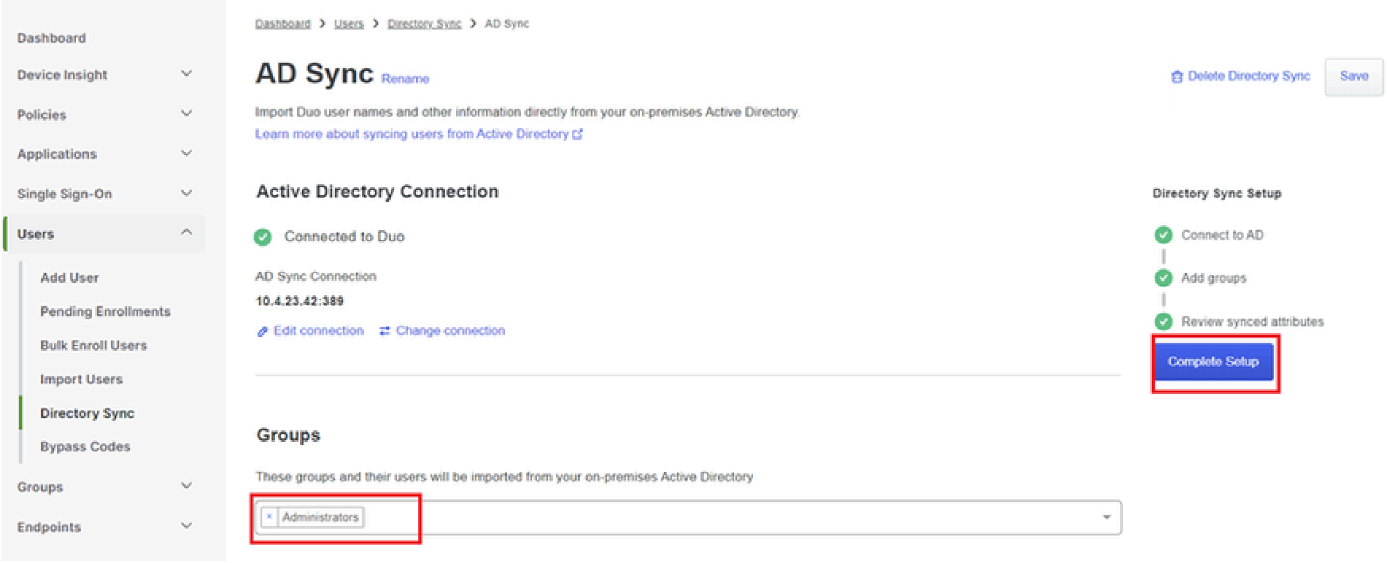
Looks like you have no users, click Add User to add one.

User list.

2. Select the Active Directory configuration you wish to manage.

3. Within the configuration settings, identify and choose the specific groups within Active Directory that you wish to synchronize with the Duo Cloud. Consider using the filtering options for your selection.

4. Click **Complete Setup**.



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

Active Directory Connection

Connected to Duo

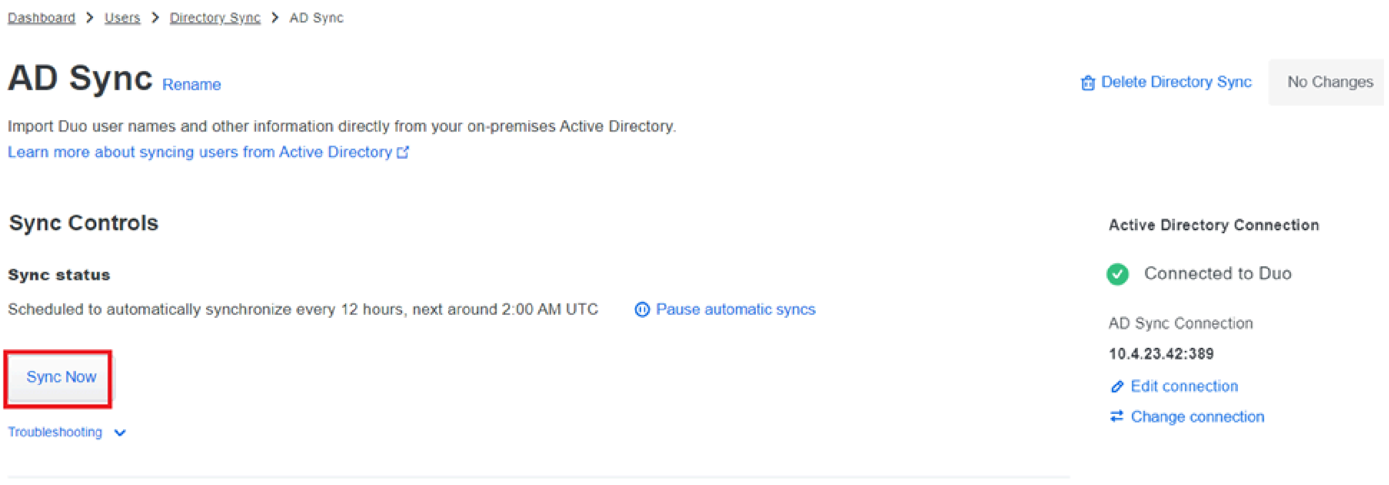
AD Sync Connection
10.4.23.42:389

Groups

These groups and their users will be imported from your on-premises Active Directory

AD Sync.

5. To initiate the synchronization immediately, click **Sync Now**. This exports the user accounts from the specified groups in Active Directory to the Duo Cloud, allowing them to be managed within the Duo Security environment.



Dashboard > Users > Directory Sync > AD Sync

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

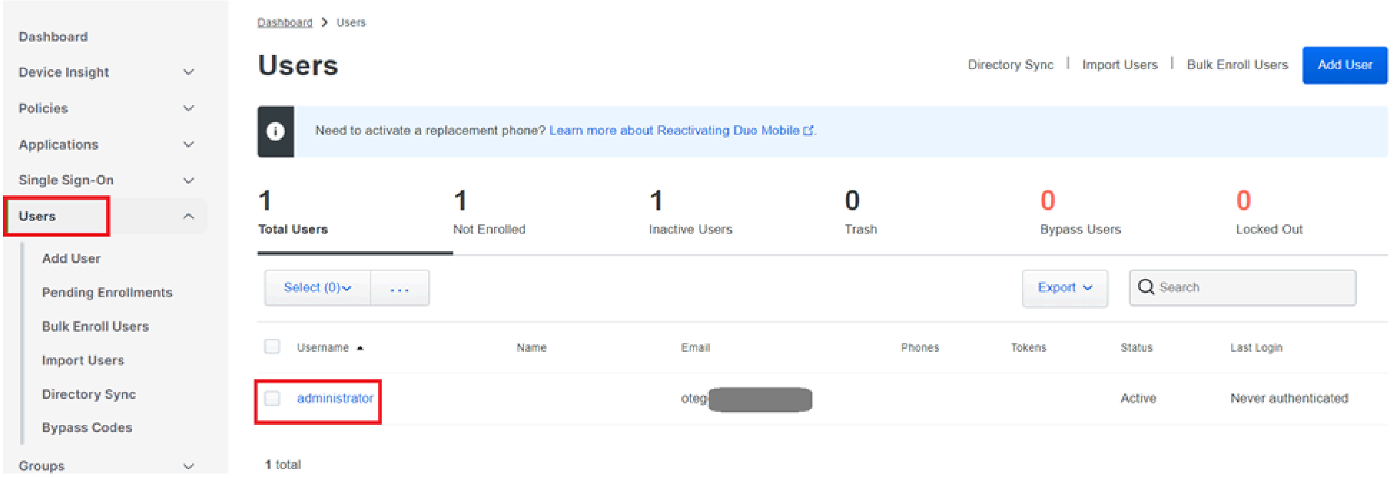
Starting Synchronization

Enroll Users in the Cisco DUO Cloud.

User enrollment enables identity verification through various methods, such as code access, DUO push, SMS codes, and tokens.

1. Navigate to the **Users** section in the **Cisco Cloud** dashboard.

2. Locate and select the account of the user you wish to enroll.



Dashboard > Users

Users

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

Need to activate a replacement phone? Learn more about Reactivating Duo Mobile.

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

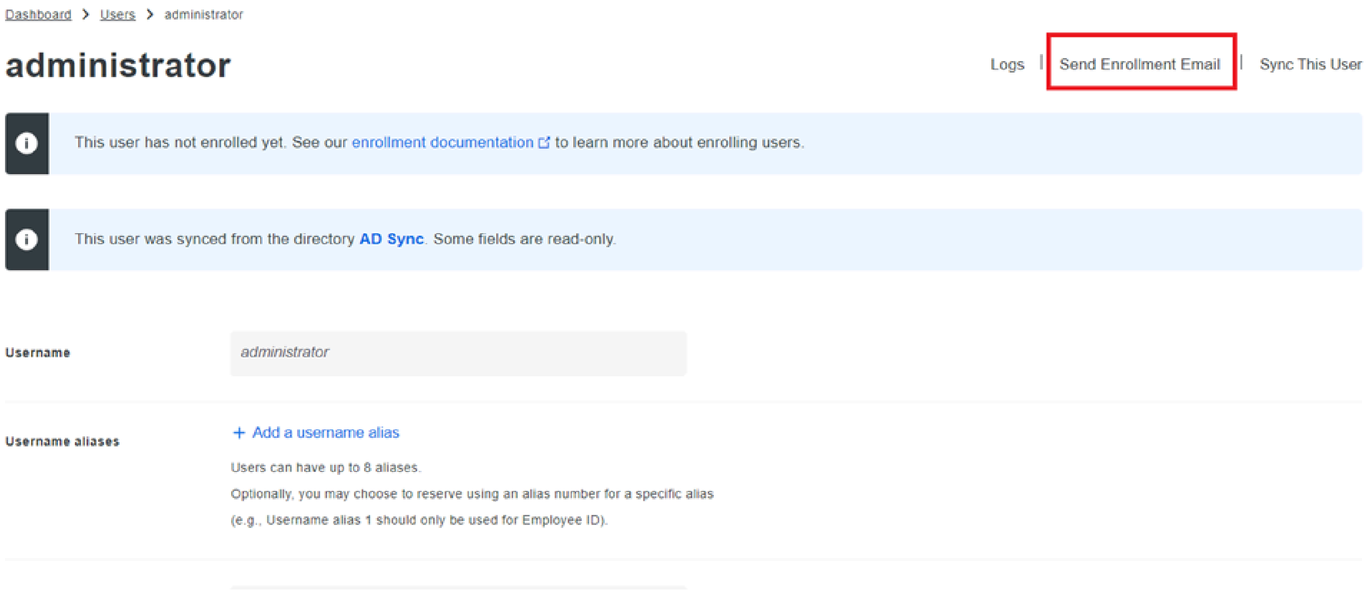
Select (0) | ... | Export | Search

Username	Name	Email	Phones	Tokens	Status	Last Login
administrator		oteg[redacted]			Active	Never authenticated

1 total

User account list.

3. Click the **Send Enrollment Email** button to initiate the enrollment process.



Dashboard > Users > administrator

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).

Enrollment via email.

4. Check the email inbox and open the enrollment invitation to complete the authentication process.

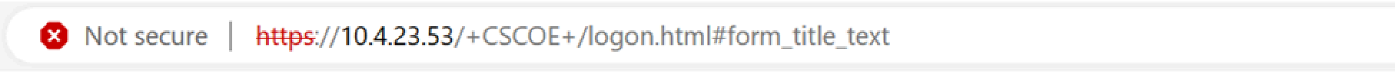
For additional details regarding the enrollment process, please refer to these resources:

- Universal Enrollment Guide: https://guide.duo.com/universal-enrollment
- Traditional Enrollment Guide: https://guide.duo.com/traditional-enrollment

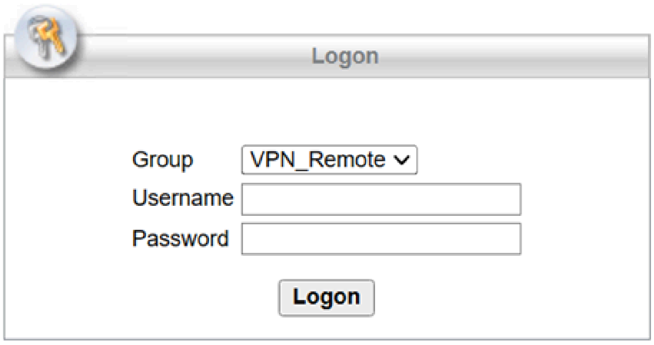
Configuration Validation Procedure.

To ensure that your configurations are accurate and operational, validate the next steps:

1. Launch a web browser and enter the IP address of the Firepower Threat Defense (FTD) device to access the VPN interface.



Not secure | ~~https~~://10.4.23.53/+CSCOE+/logon.html#form_title_text



Logon

Group: VPN_Remote

Username:

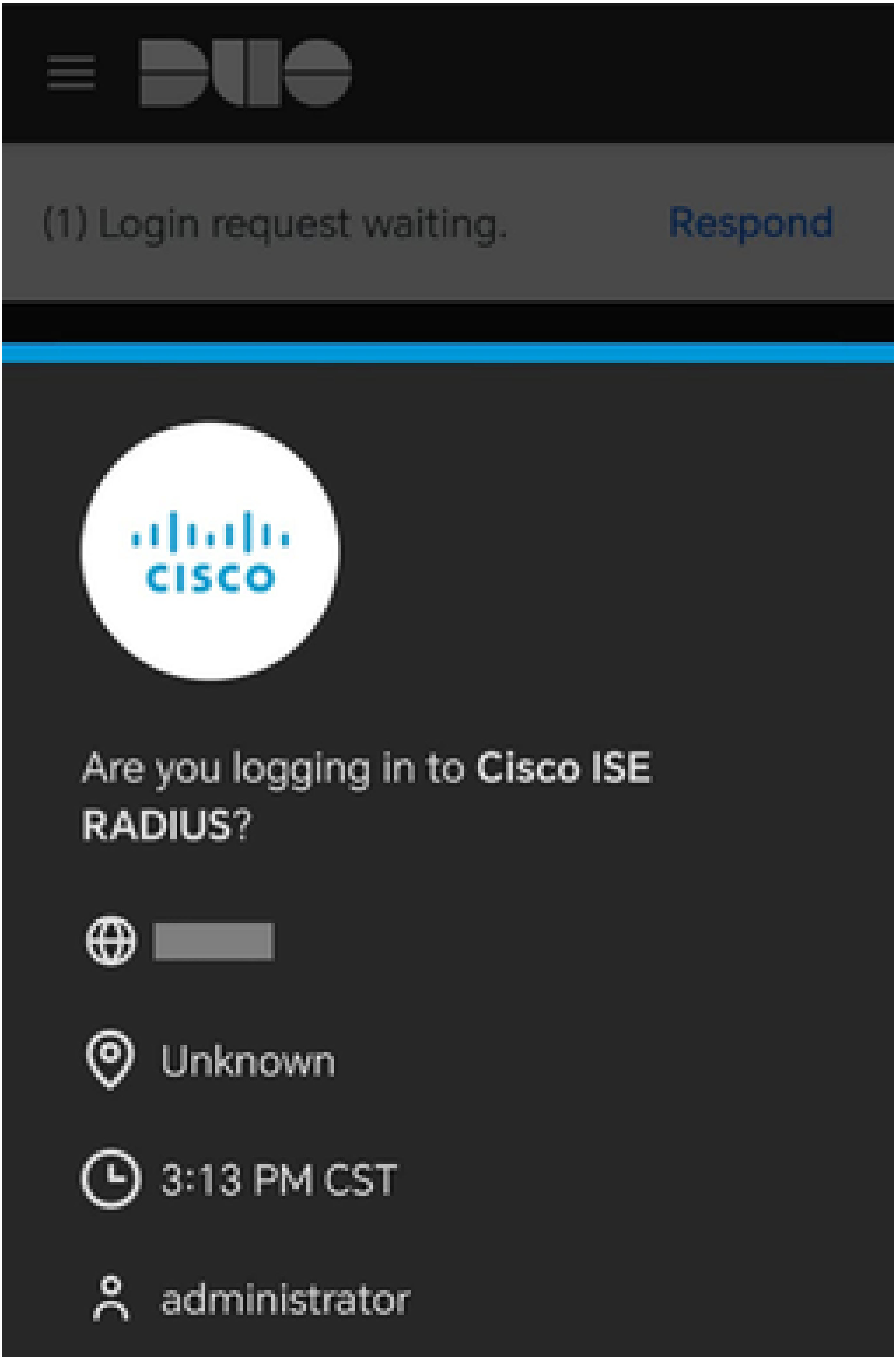
Password:

VPN Logon.

2. Input your username and password when prompted.

Note: The credentials are part of the Active Directory accounts.

3. When you receive a DUO Push notification, approve it using the DUO Mobile Software to proceed with the validation process.



(1) Login request waiting. Respond

Are you logging in to **Cisco ISE RADIUS**?

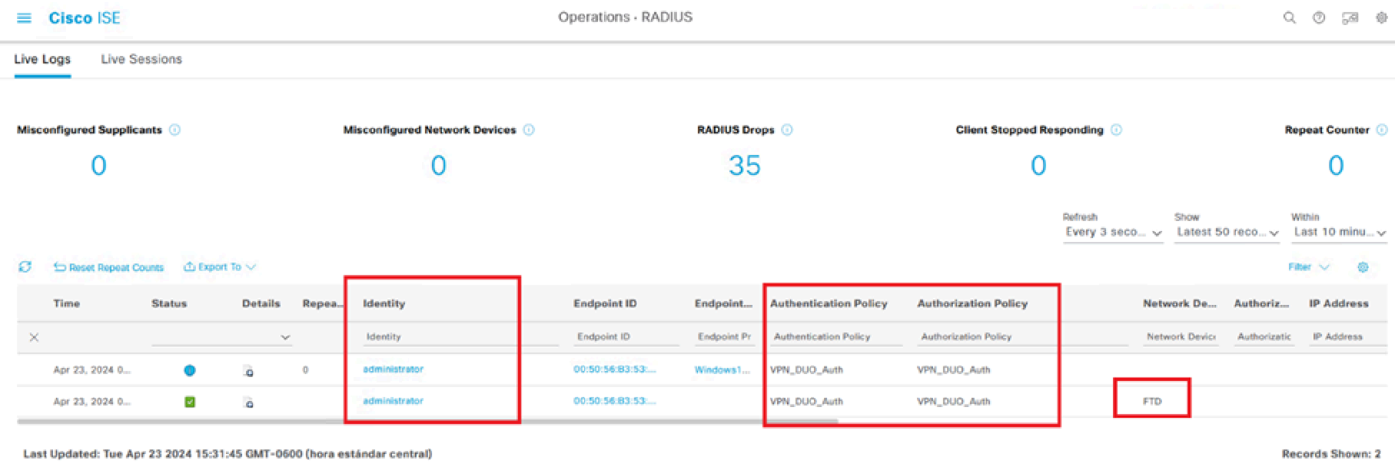
[redacted]

Unknown

3:13 PM CST

administrator

to monitor real-time activity and verify proper connectivity, access the live logs in the Cisco Identity Services Engine (ISE).



Cisco ISE — Operations · RADIUS

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	35	0	0

Refresh: Every 3 seco... Show: Latest 50 reco... Within: Last 10 minu...

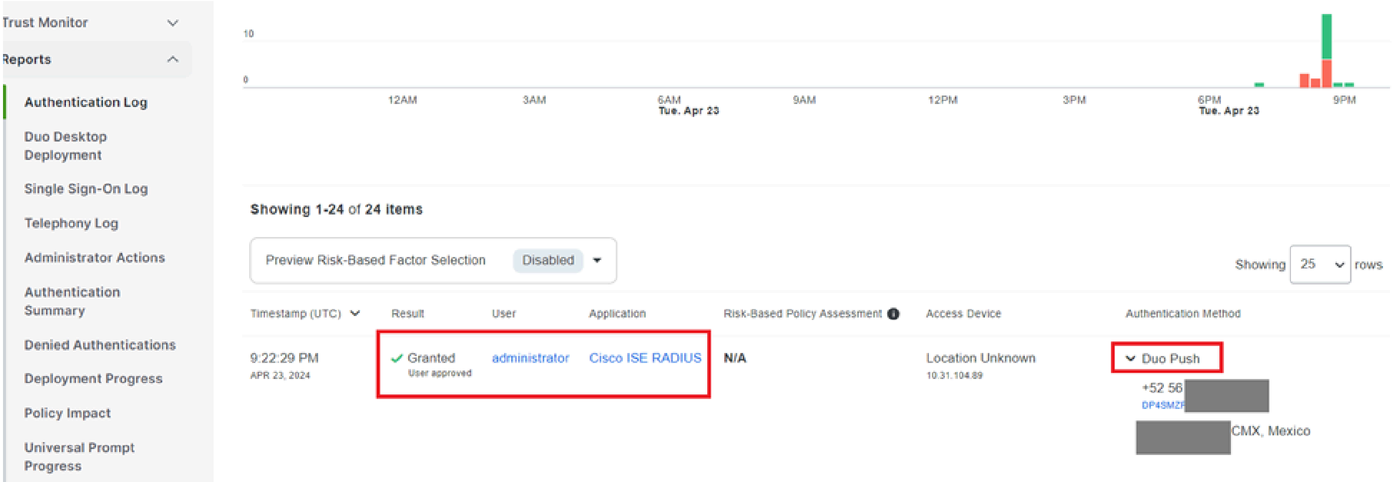
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Network De...	Authoriz...	IP Address
×				Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Network Devic	Authorizatic	IP Address
Apr 23, 2024 0...	●		0	administrator	00:50:56:83:53:...	Windows1...	VPN_DUO_Auth	VPN_DUO_Auth			
Apr 23, 2024 0...	✓			administrator	00:50:56:83:53:...		VPN_DUO_Auth	VPN_DUO_Auth	FTD		

Last Updated: Tue Apr 23 2024 15:31:45 GMT-0600 (hora estándar central)

Records Shown: 2

ISE Livelogs.

9. Go to **Reports** > **Authentication** logs to review the authentication logs in the DUO Admin Panel to confirm successful verifications.



Showing 1-24 of **24 items**

Preview Risk-Based Factor Selection: Disabled

Showing 25 rows

Timestamp (UTC)	Result	User	Application	Risk-Based Policy Assessment	Access Device	Authentication Method
9:22:29 PM APR 23, 2024	✓ Granted User approved	administrator	Cisco ISE RADIUS	N/A	Location Unknown 10.31.104.89	Duo Push +52 56 [redacted] DP4SMZ [redacted] CMX, Mexico

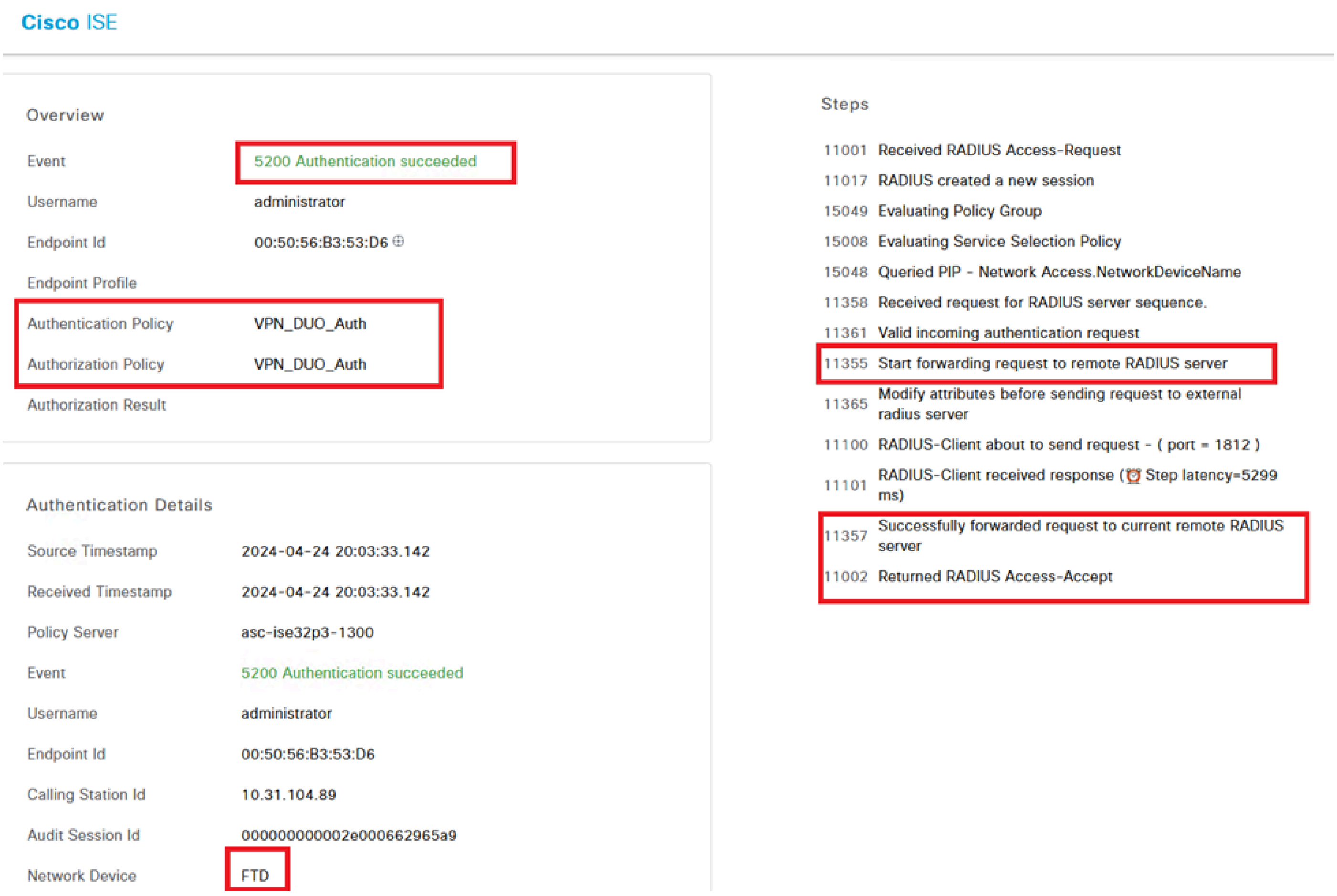
Authentication logs.

Common issues.

Working scenario.

Before you explore specific errors related to this integration, it is crucial to understand the overall working scenario.

In the ISE livelogs we can confirm that ISE forwarded the RADIUS packets to the DUO Proxy, and once the user accepted the DUO Push, the RADIUS Access Accept was received from the DUO Proxy Server.



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6 ⊕
Endpoint Profile	
Authentication Policy	VPN_DUO_Auth
Authorization Policy	VPN_DUO_Auth
Authorization Result	

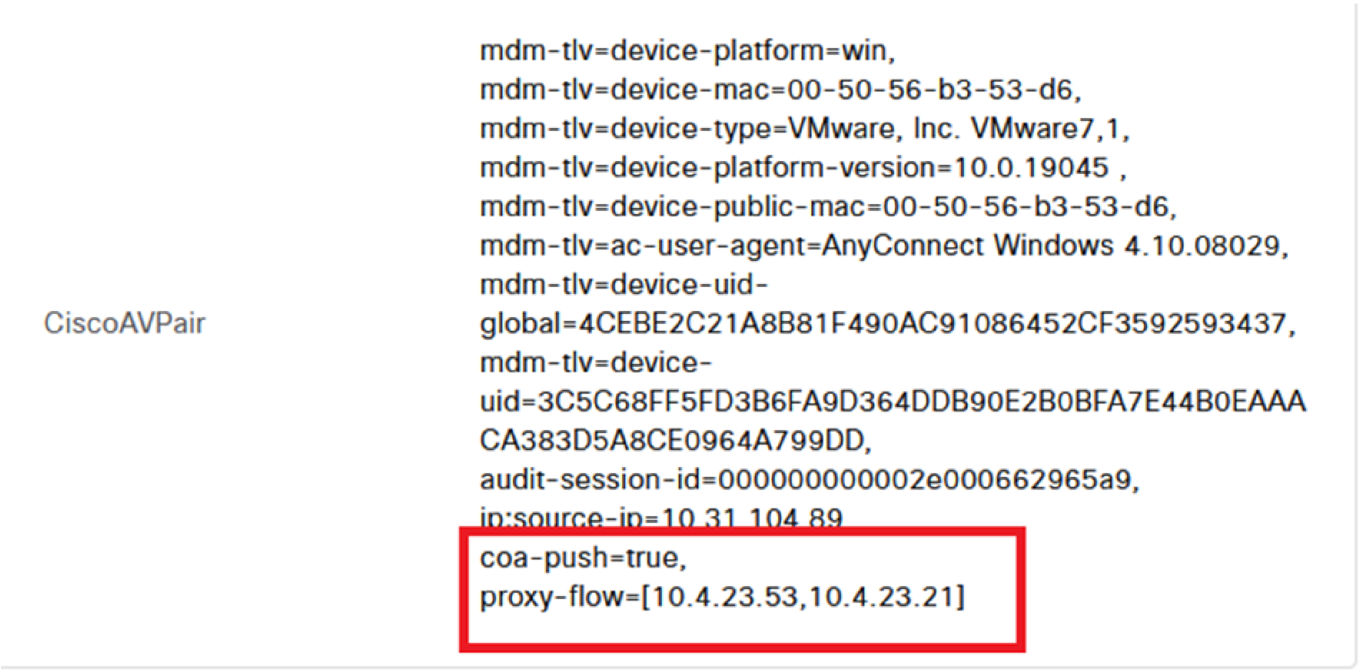
Authentication Details

Source Timestamp	2024-04-24 20:03:33.142
Received Timestamp	2024-04-24 20:03:33.142
Policy Server	asc-ise32p3-1300
Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Calling Station Id	10.31.104.89
Audit Session Id	000000000002e000662965a9
Network Device	FTD

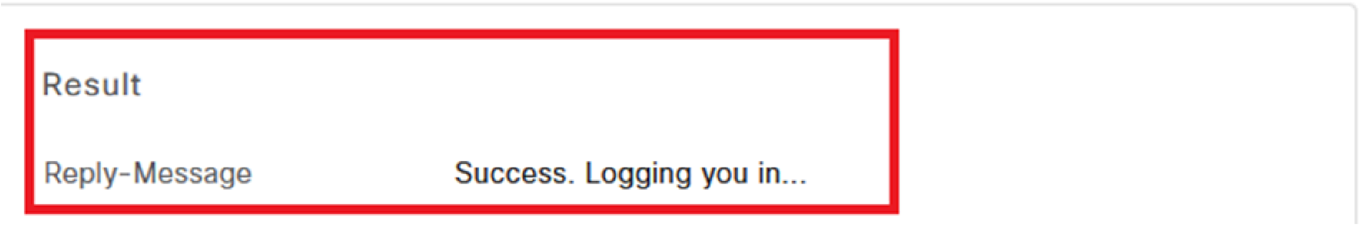
Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Network Access.NetworkDeviceName
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response (⏰ Step latency=5299 ms)
11357	Successfully forwarded request to current remote RADIUS server
11002	Returned RADIUS Access-Accept

Success authentication.



CiscoAVPair	mdm-tlv=device-platform=win, mdm-tlv=device-mac=00-50-56-b3-53-d6, mdm-tlv=device-type=VMware, Inc. VMware7,1, mdm-tlv=device-platform-version=10.0.19045 , mdm-tlv=device-public-mac=00-50-56-b3-53-d6, mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.08029, mdm-tlv=device-uid-global=4CEBE2C21A8B81F490AC91086452CF3592593437, mdm-tlv=device-uid=3C5C68FF5FD3B6FA9D364DDB90E2B0BFA7E44B0EAAACA383D5A8CE0964A799DD, audit-session-id=000000000002e000662965a9, ip:source-ip=10.31.104.89, coa-push=true, proxy-flow=[10.4.23.53,10.4.23.21]

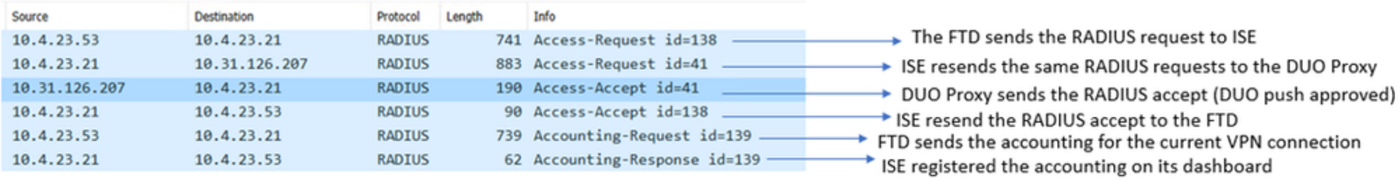


Result

Reply-Message	Success. Logging you in...

Result Successfully.

A packet capture from the ISE side shows the next information:



Source	Destination	Protocol	Length	Info
10.4.23.53	10.4.23.21	RADIUS	741	Access-Request id=138
10.4.23.21	10.31.126.207	RADIUS	883	Access-Request id=41
10.31.126.207	10.4.23.21	RADIUS	190	Access-Accept id=41
10.4.23.21	10.4.23.53	RADIUS	90	Access-Accept id=138
10.4.23.53	10.4.23.21	RADIUS	739	Accounting-Request id=139
10.4.23.21	10.4.23.53	RADIUS	62	Accounting-Response id=139

The FTD sends the RADIUS request to ISE

ISE resends the same RADIUS requests to the DUO Proxy

DUO Proxy sends the RADIUS accept (DUO push approved)

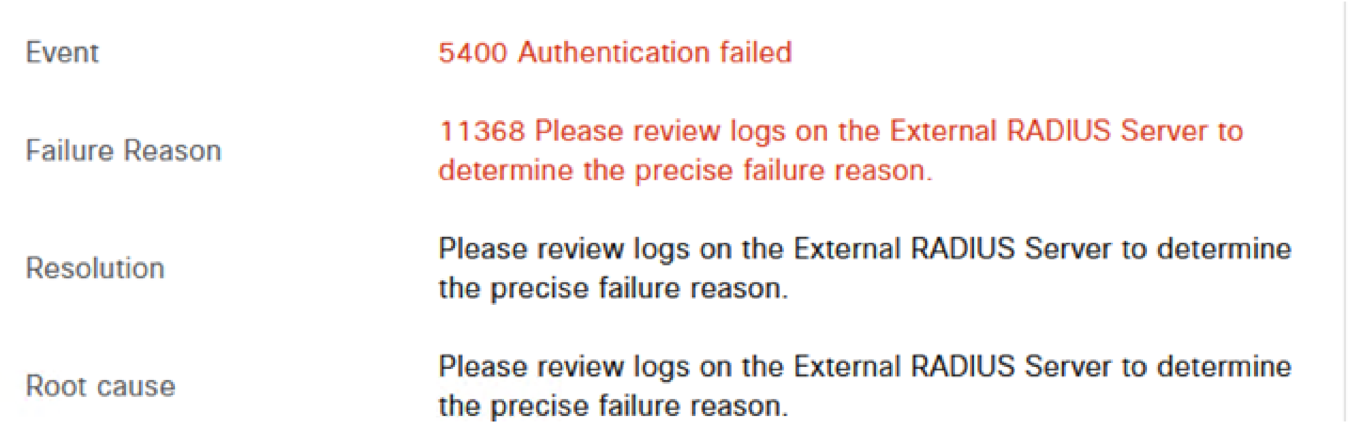
ISE resend the RADIUS accept to the FTD

FTD sends the accounting for the current VPN connection

ISE registered the accounting on its dashboard

ISE packet capture.

Error11368 Please review logs on the External RADIUS Server to determine the precise failure reason.



Event	5400 Authentication failed
Failure Reason	11368 Please review logs on the External RADIUS Server to determine the precise failure reason.
Resolution	Please review logs on the External RADIUS Server to determine the precise failure reason.
Root cause	Please review logs on the External RADIUS Server to determine the precise failure reason.

Error 11368.

Troubleshooting:

- Verify that the RADIUS shared secret key in ISE is the same as the configured key in the FMC.

1. Open the ISE GUI.

2. **Administration** > **Network Resources** > **Network Devices**.

3. Choose the DUO Proxy Server.

4. Next to the shared secret, click "**Show**" to see the key in plain text format.

5. Open the FMC GUI.

6. **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group**.

7. Choose the ISE Server.

8. Reenter the secret key.

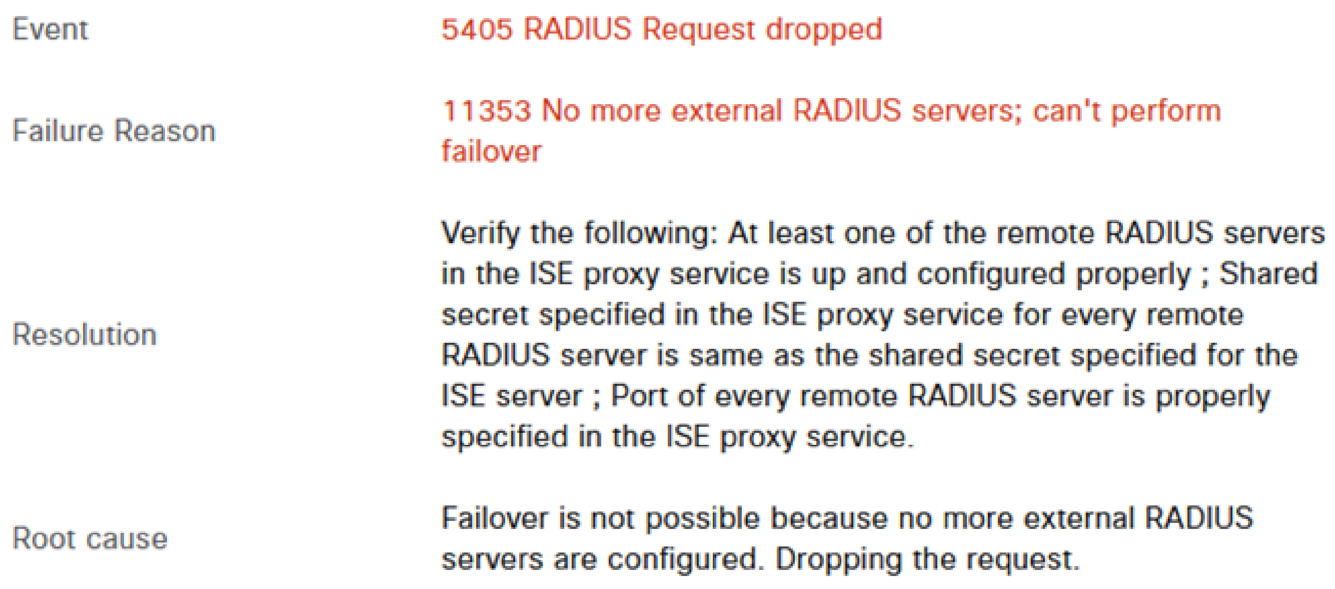
- Verify the Active Directory integration in DUO.

1. Open the DUO Authentication Proxy Manager.

2. Confirm the user and password under the [ad_client] section.

3. Click validate to confirm the current credentials are correct.

Error 11353 No more external RADIUS servers; cant perform failover



Event	5405 RADIUS Request dropped
Failure Reason	11353 No more external RADIUS servers; can't perform failover
Resolution	Verify the following: At least one of the remote RADIUS servers in the ISE proxy service is up and configured properly ; Shared secret specified in the ISE proxy service for every remote RADIUS server is same as the shared secret specified for the ISE server ; Port of every remote RADIUS server is properly specified in the ISE proxy service.
Root cause	Failover is not possible because no more external RADIUS servers are configured. Dropping the request.

Error 11353.

Troubleshooting:

- Verify that the RADIUS shared secret key in ISE is the same as the configured key in the DUO Proxy Server.

1. Open the ISE GUI.

2. **Administration** > **Network Resources** > **Network Devices**.

3. Choose the DUO Proxy Server.

4. Next to the shared secret, click "**Show**" to see the key in plain text format.

5. Open the DUO Authentication Proxy Manager.

6. Verify the [radius_server_auto] section and compare the shared secret key.

The RADIUS sessions do not appear in the ISE live logs.

Troubleshooting:

- Verify the DUO configuration.

1. Open the DUO Authentication Proxy Manager.

2. Verify the ISE IP address in the [radius_server_auto] section

- Verify the FMC configuration.

1. Open the FMC GUI.

2. Go to **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group**.

3. Choose the ISE Server.

4. Verify the ISE IP address.

- Take a packet capture in ISE to confirm the reception of the RADIUS packets.

1. Go to **Operations** > **Troubleshoot** > **Diagnostic Tools** > **TCP Dump**

Additional troubleshooting.

- Enable the next components in the PSN as debug:

Policy-engine

Prrt-JNI

runtime-AAA

For further troubleshooting in DUO Authentication Proxy Manager check the next link:

https://help.duo.com/s/article/1126?language=en_US

DUO Template.

You can use the next template to complete the configuration into your DUO Proxy Server.

```
[main]    <--- OPTIONAL
http_proxy_host=<Proxy IP address or FQDN>
http_proxy_port=<Proxy port>
[radius_server_auto]
ikey=xxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxx
radius_ip_1=<PSN IP Address>
radius_secret_1=xxxxxxxxx
failmode=safe
port=1812
client=ad_client

[ad_client]
host=<AD IP Address>
service_account_username=xxxxxxxx
service_account_password=xxxxxxxxxx
search_dn=DC=xxxxxx,DC=xxxx

[cloud]
ikey=xxxxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxx
service_account_username=<your domain\username>
service_account_password=xxxxxxxxxxxxx
```