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

Contents

Introduction

Requirements

Components Used

Network Diagram

Configurations

- FTD configurations.
  - Integrate a RADIUS server within the Firepower Management Center (FMC)
  - Configure the remote VPN.
- ISE configurations.
  - Integrate DUO as an External Radius Server.
  - Integrate the FTD as a Network Access Device.
- DUO configurations.
  - DUO Proxy Installation.
  - Integrate DUO Proxy with ISE and DUO Cloud.
  - Integrate DUO with Active Directory.
  - Export user accounts from Active Directory (AD) via DUO Cloud.
  - Enroll Users in the Cisco DUO Cloud.
- Configuration Validation Procedure.

Common issues.

- Working scenario.
- Error11353 No more external RADIUS servers; cant perform failover
- The RADIUS sessions do not appear in the ISE live logs.
- Additional troubleshooting.

Introduction

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

Requirements

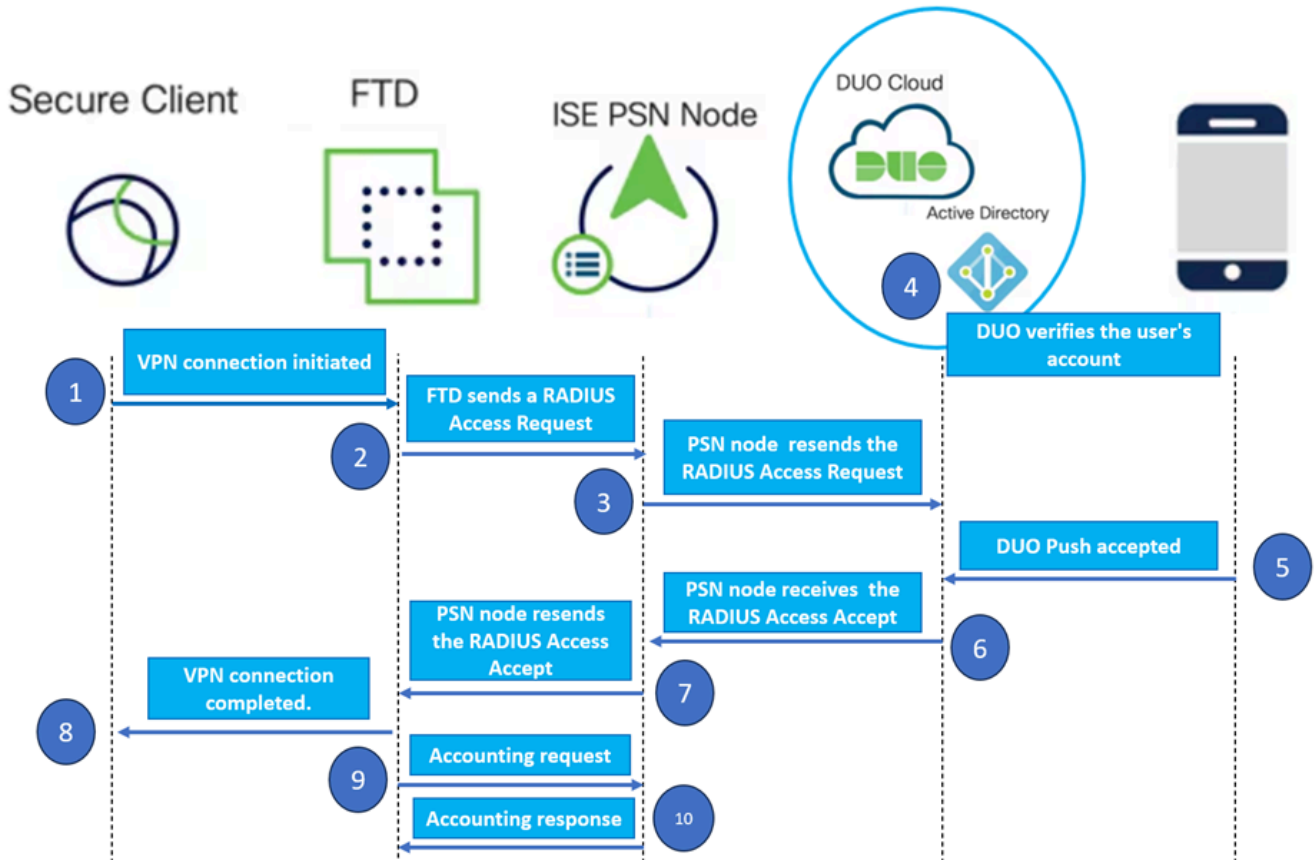
- ISE 3.0 or higher.
- FMC 7.0 or higher.
- FTD 7.0 or higher.
- DUO Authentication Proxy.
- ISE Essentials Licensing
- DUO Essentials Licensing.

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



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.

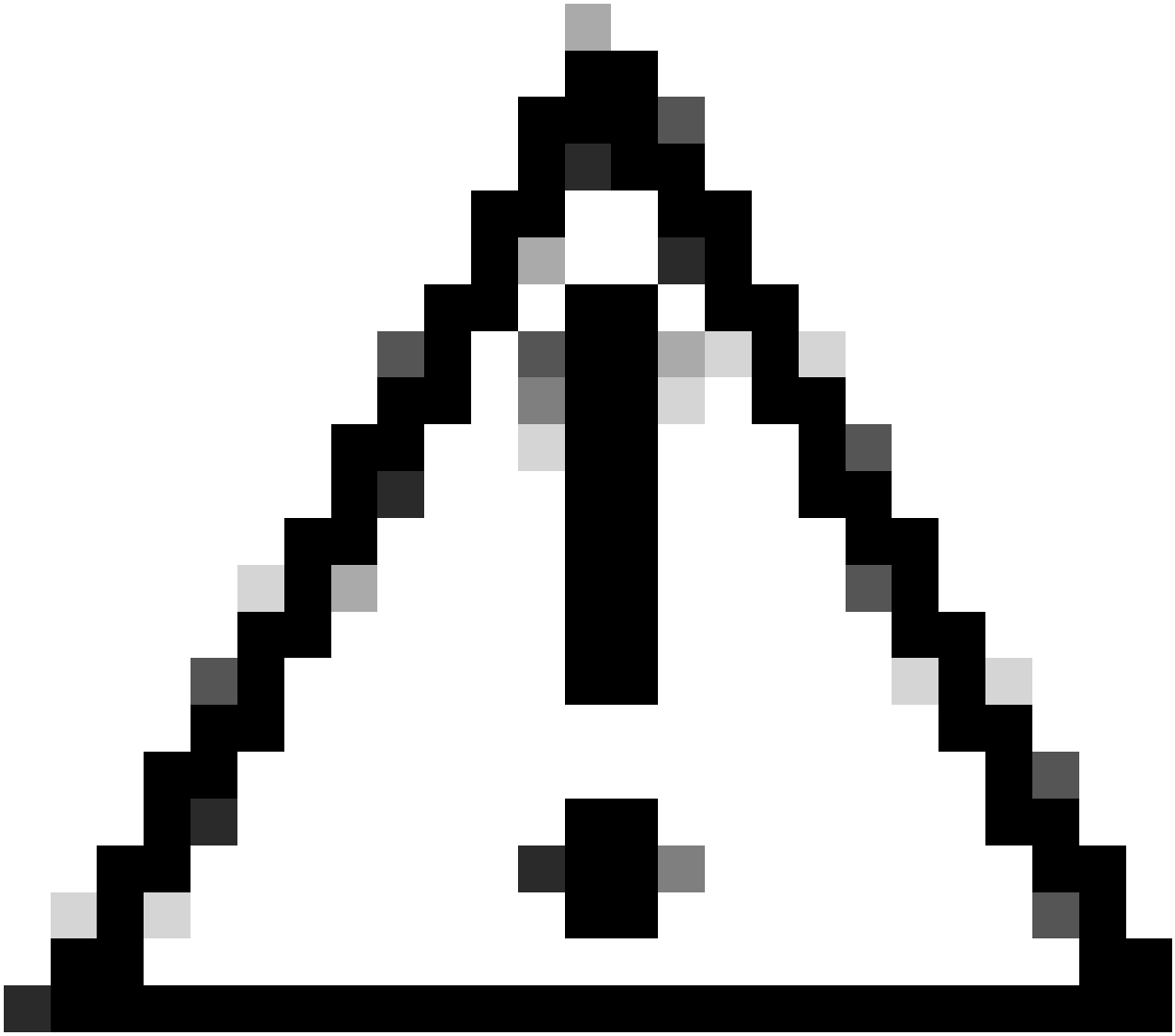
The DUO Authentication Proxy operates as a dedicated intermediary within this authentication flow. Installed on a Windows server, it bridges the gap between Cisco ISE and DUOs cloud. The proxy primary function is to transmit authentication requests – encapsulated within RADIUS packets – to the DUO Cloud. 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.

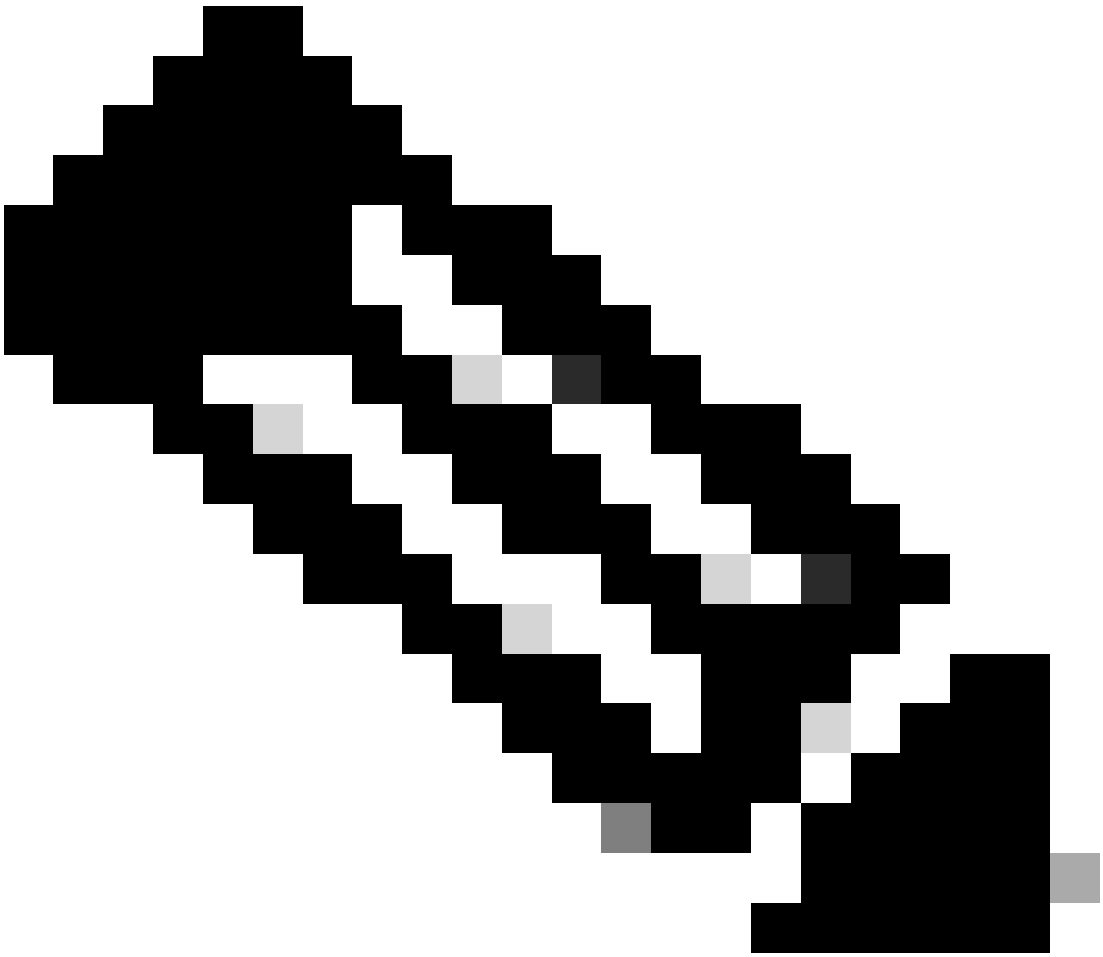
6. Once the user approves the DUO Push, the DUO Authentication Proxy Server sends a confirmation back to the PSN to indicate that the authentication request has been accepted by the user.

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

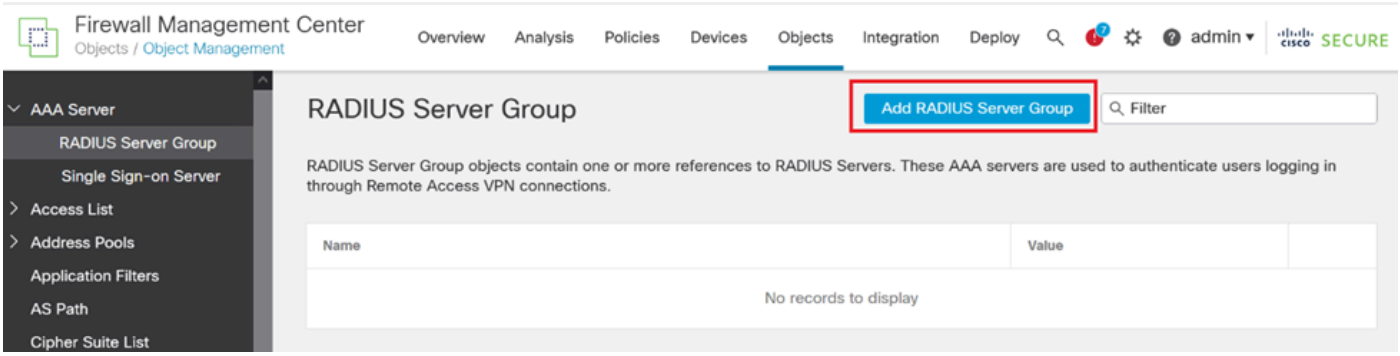
FTD configurations.

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.



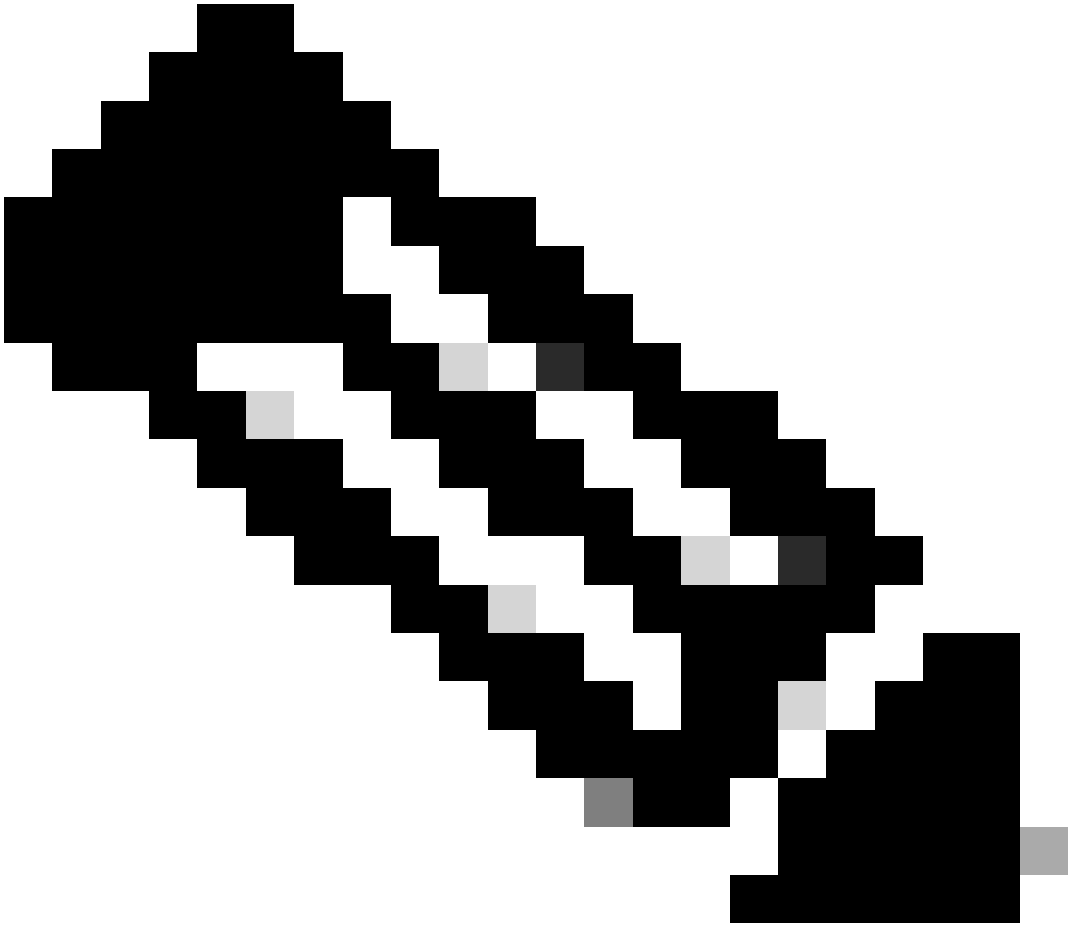
RADIUS Server Group.

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

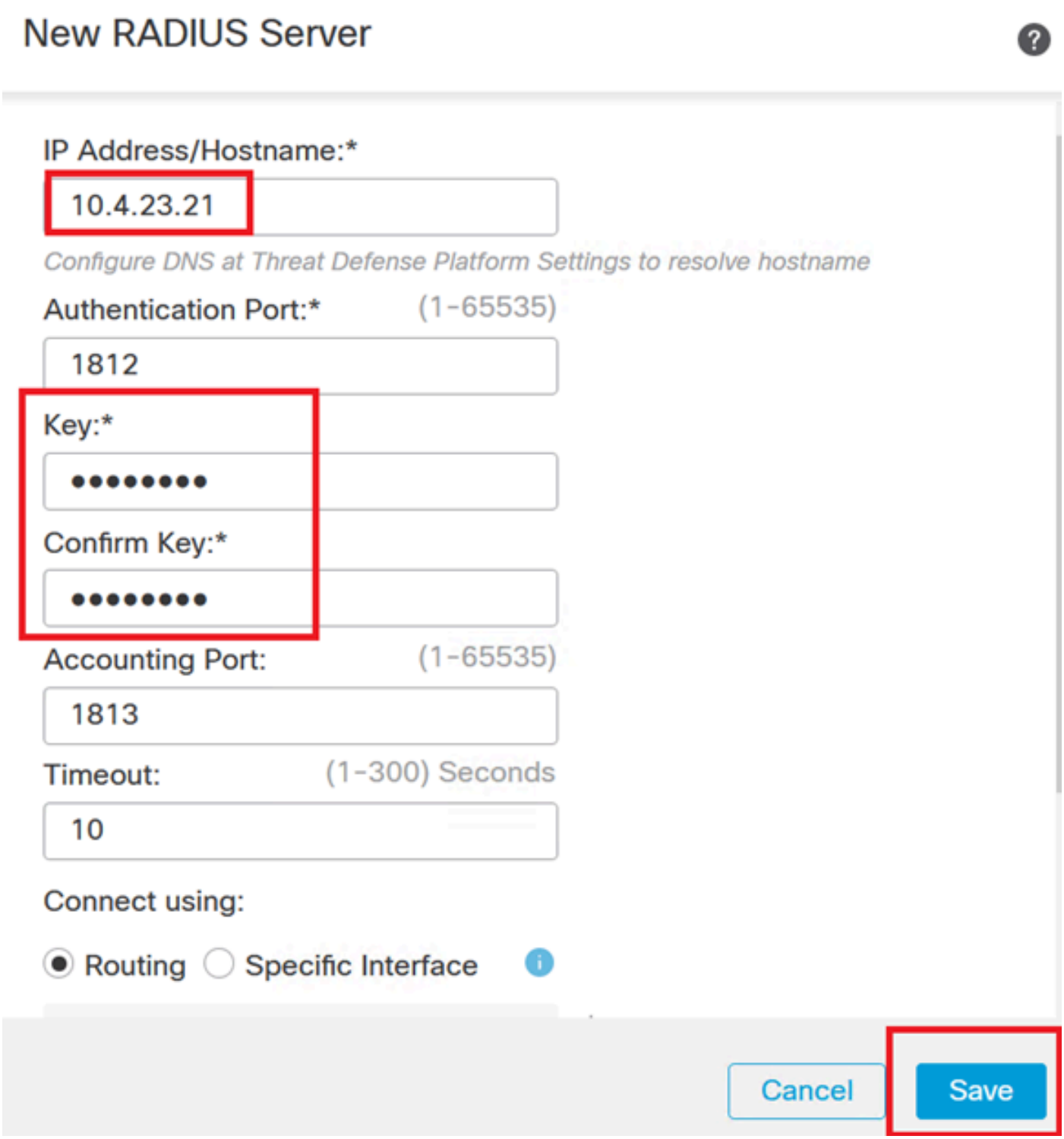
5. Proceed to add a new RADIUS Server by selecting the appropriate option within the group configuration.

RADIUS Server.

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

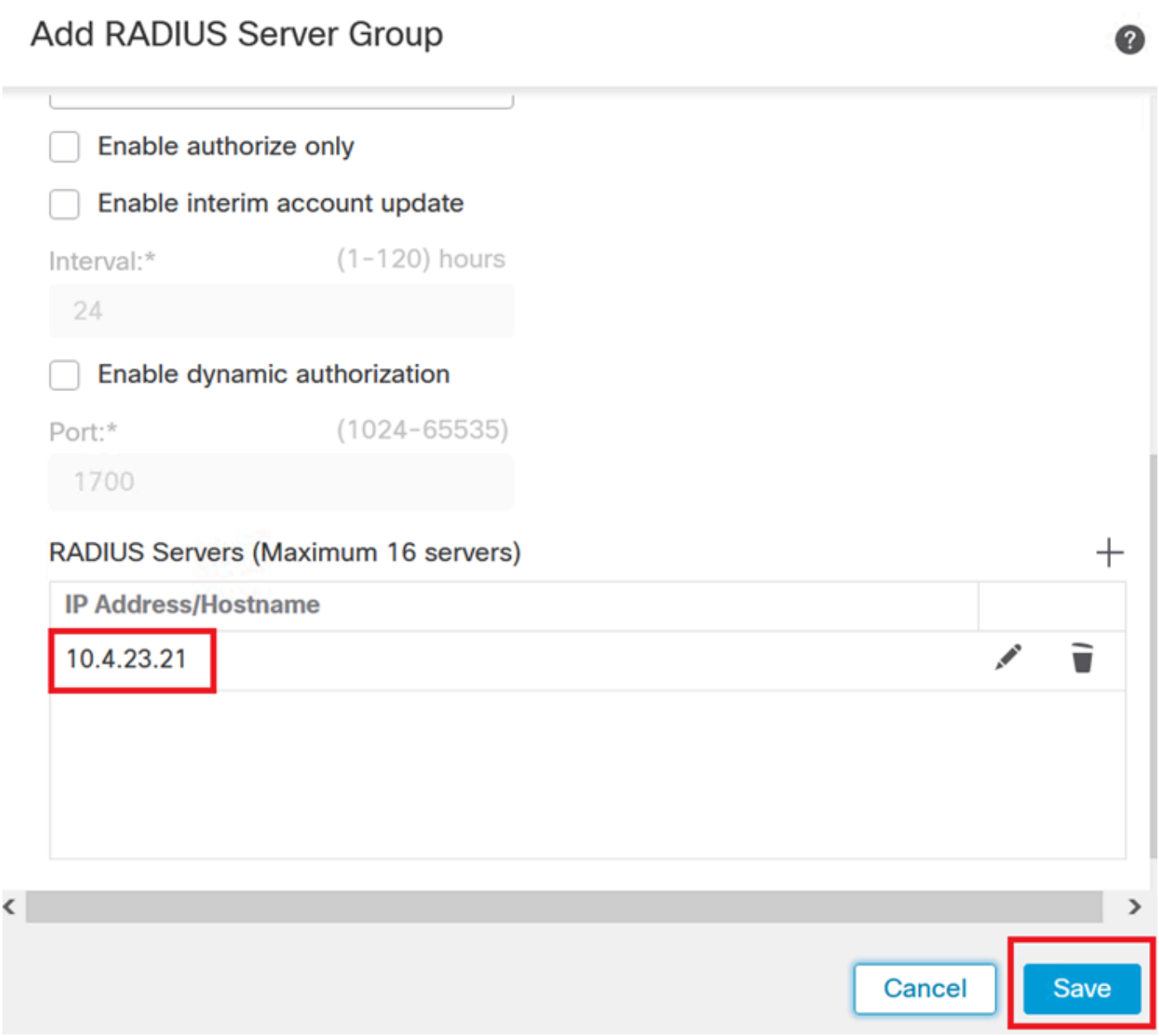


Note: It is essential to ensure that this secret key is securely shared with the ISE Server to establish a successful RADIUS connection.



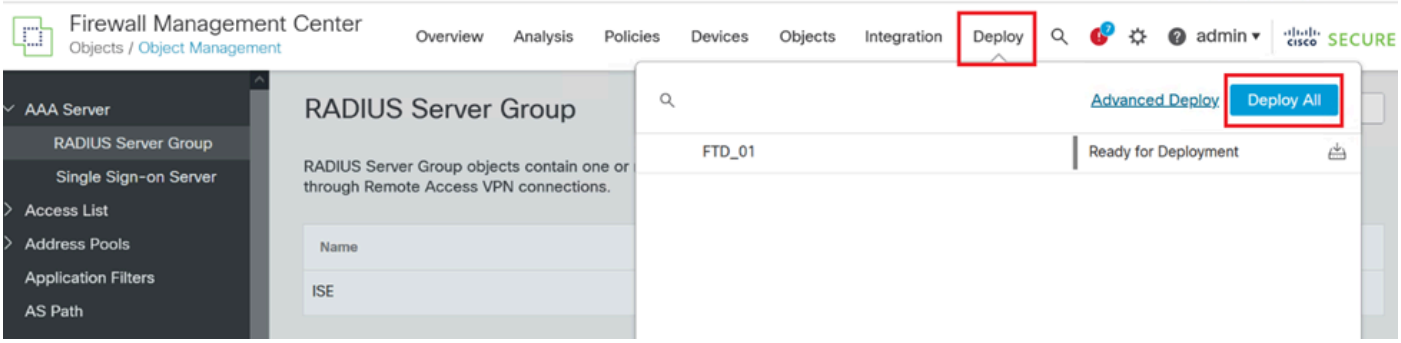
New RADIUS Server.

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



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.

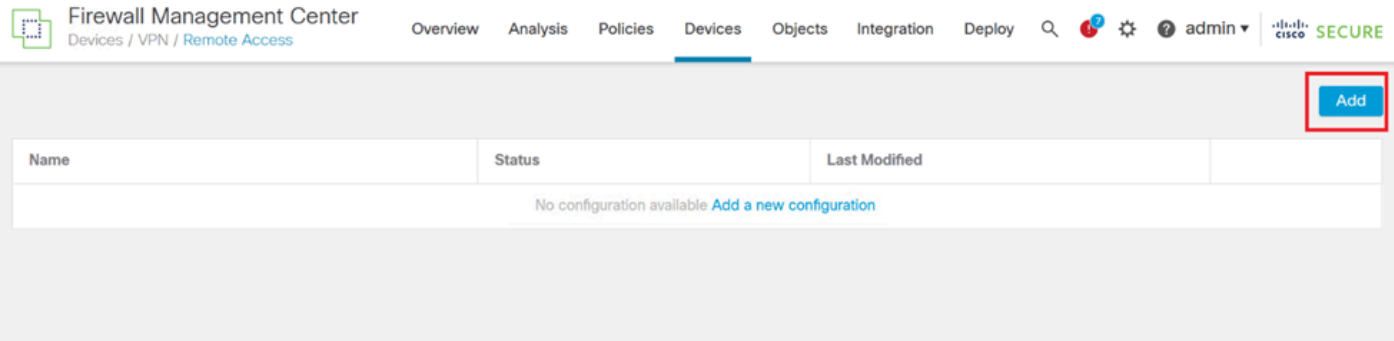


Deploying AAA Server.

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.

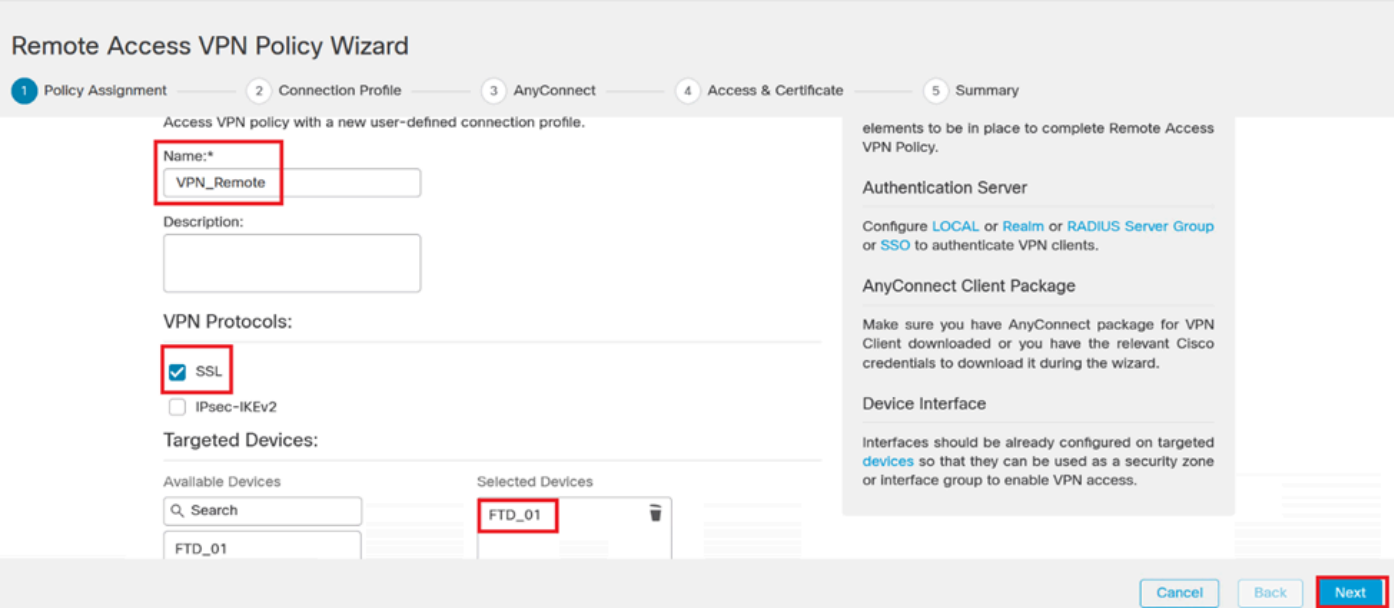


VPN connection profile.

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

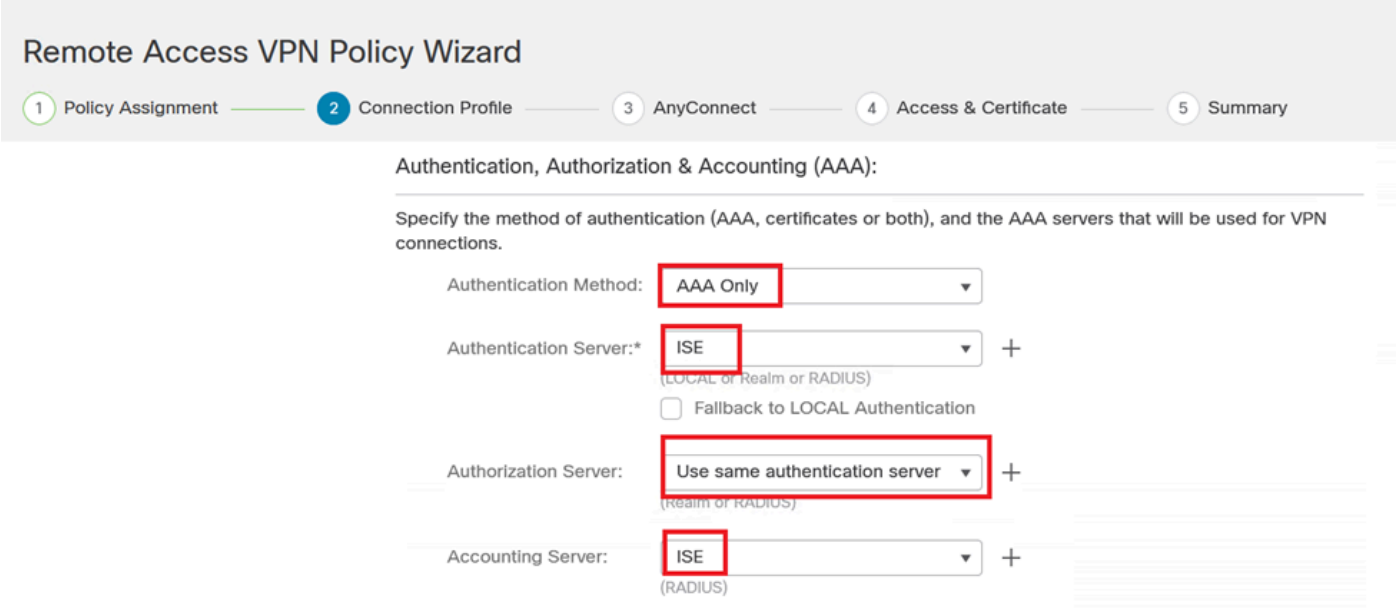
4. Choose the SSL option to ensure a secure connection using the SSL VPN protocol.

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



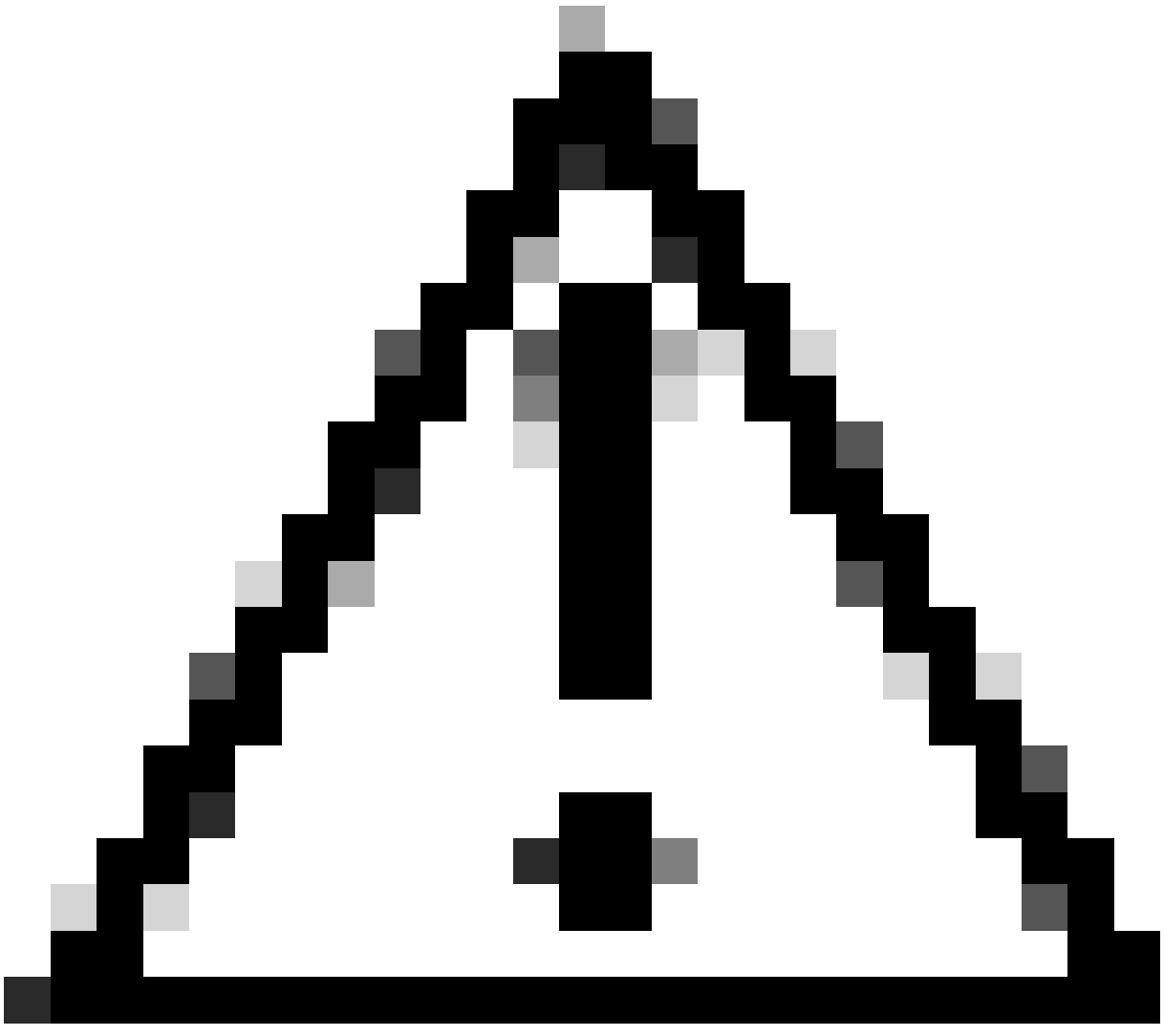
VPN settings.

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

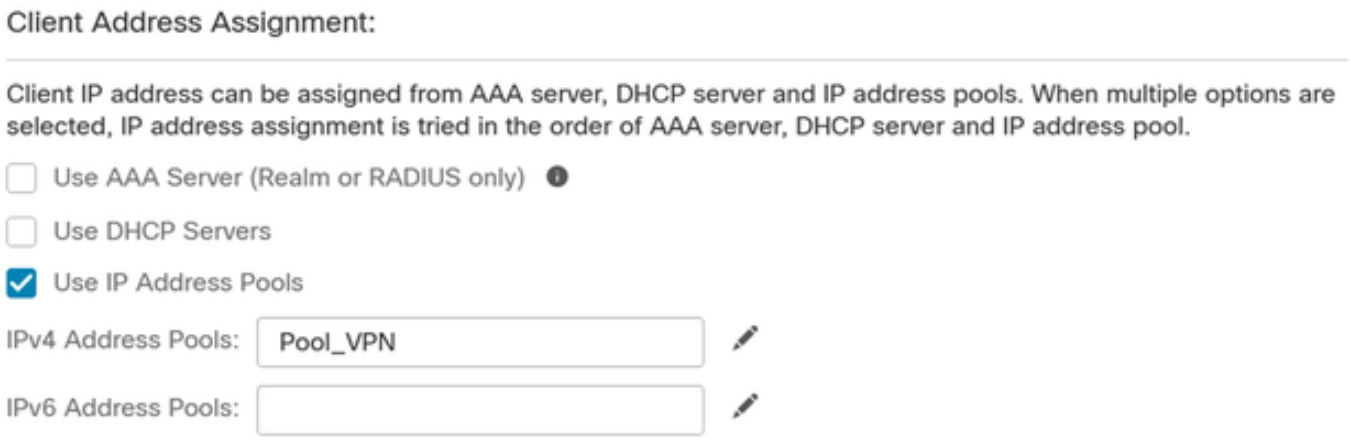


Connection profile.

7. Set up dynamic IP address assignment for VPN.

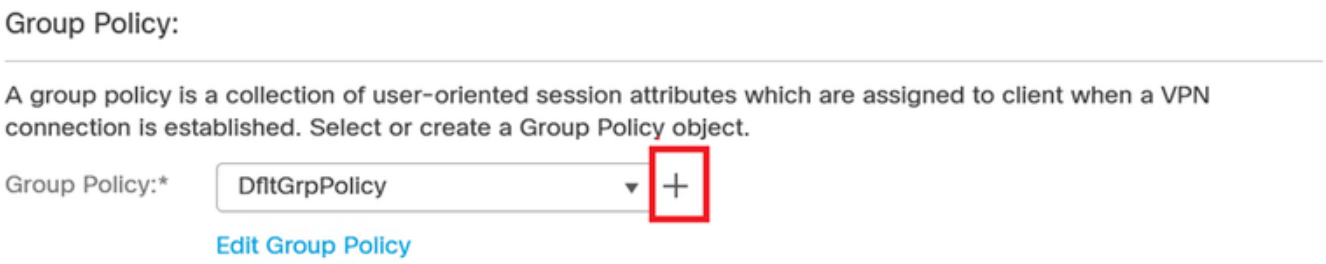


Caution: For example purposes, the DHCP VPN pool was selected.



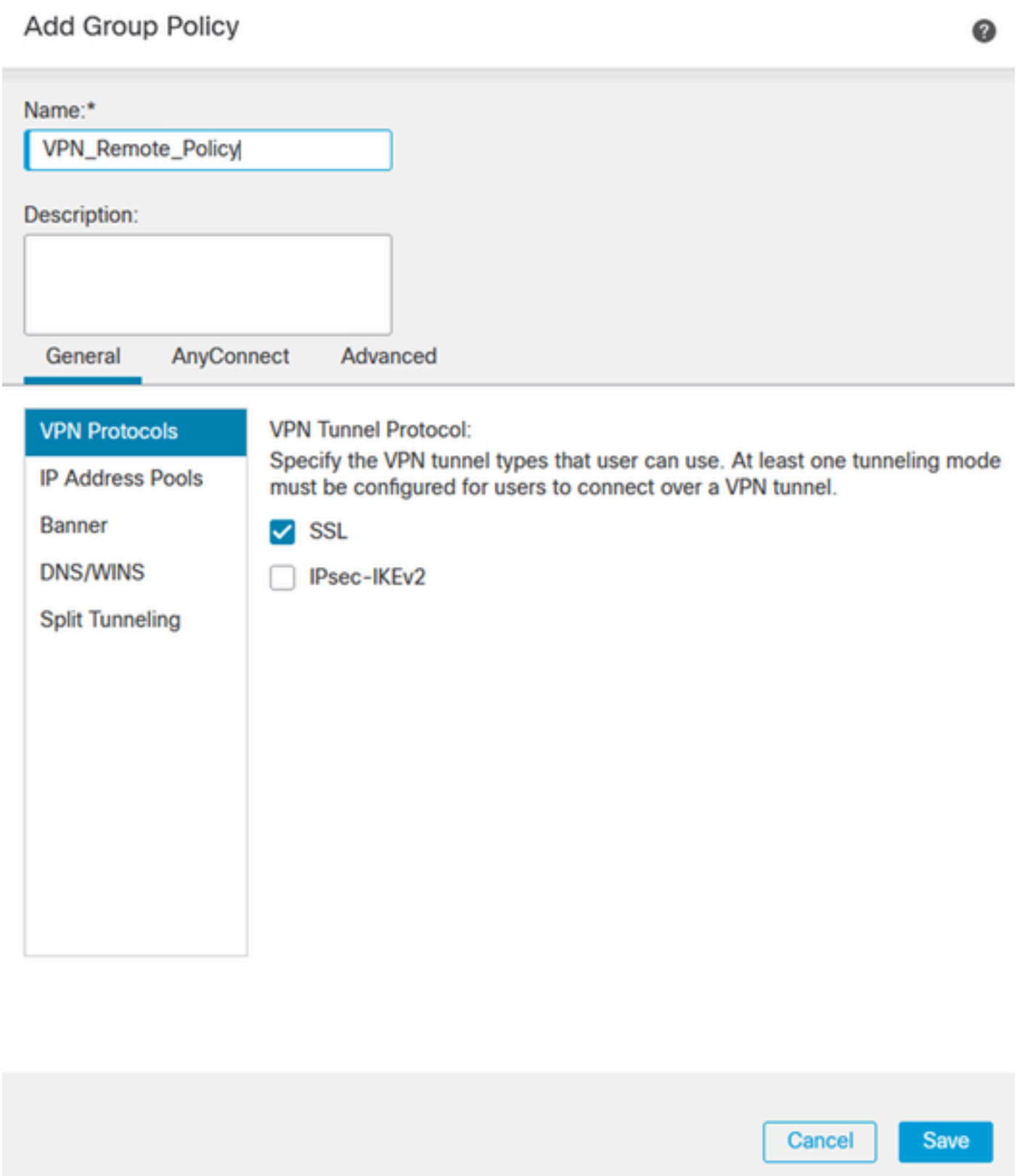
IP Address pool.

8. Proceed to create a new Group Policy.



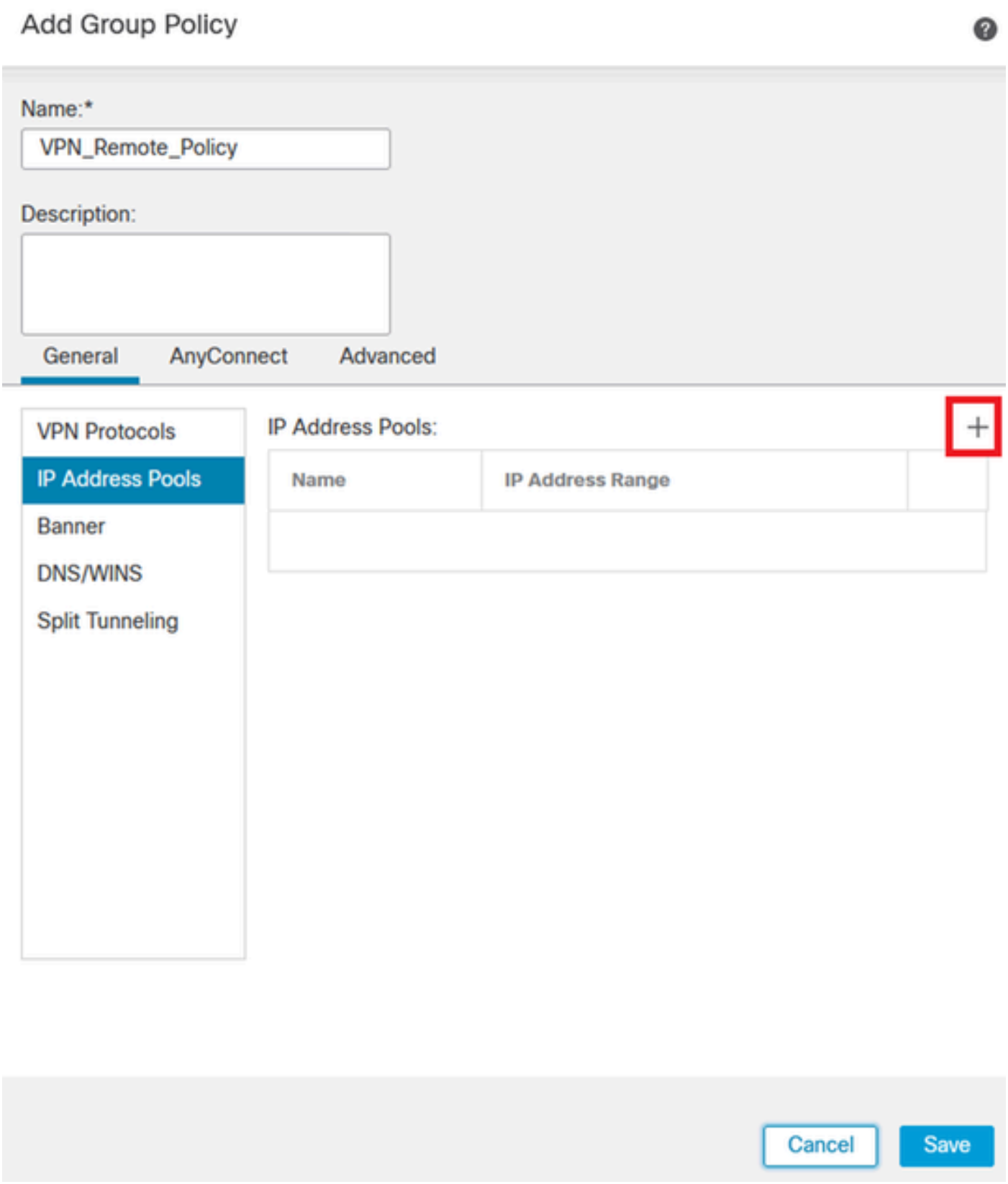
Group policy.

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



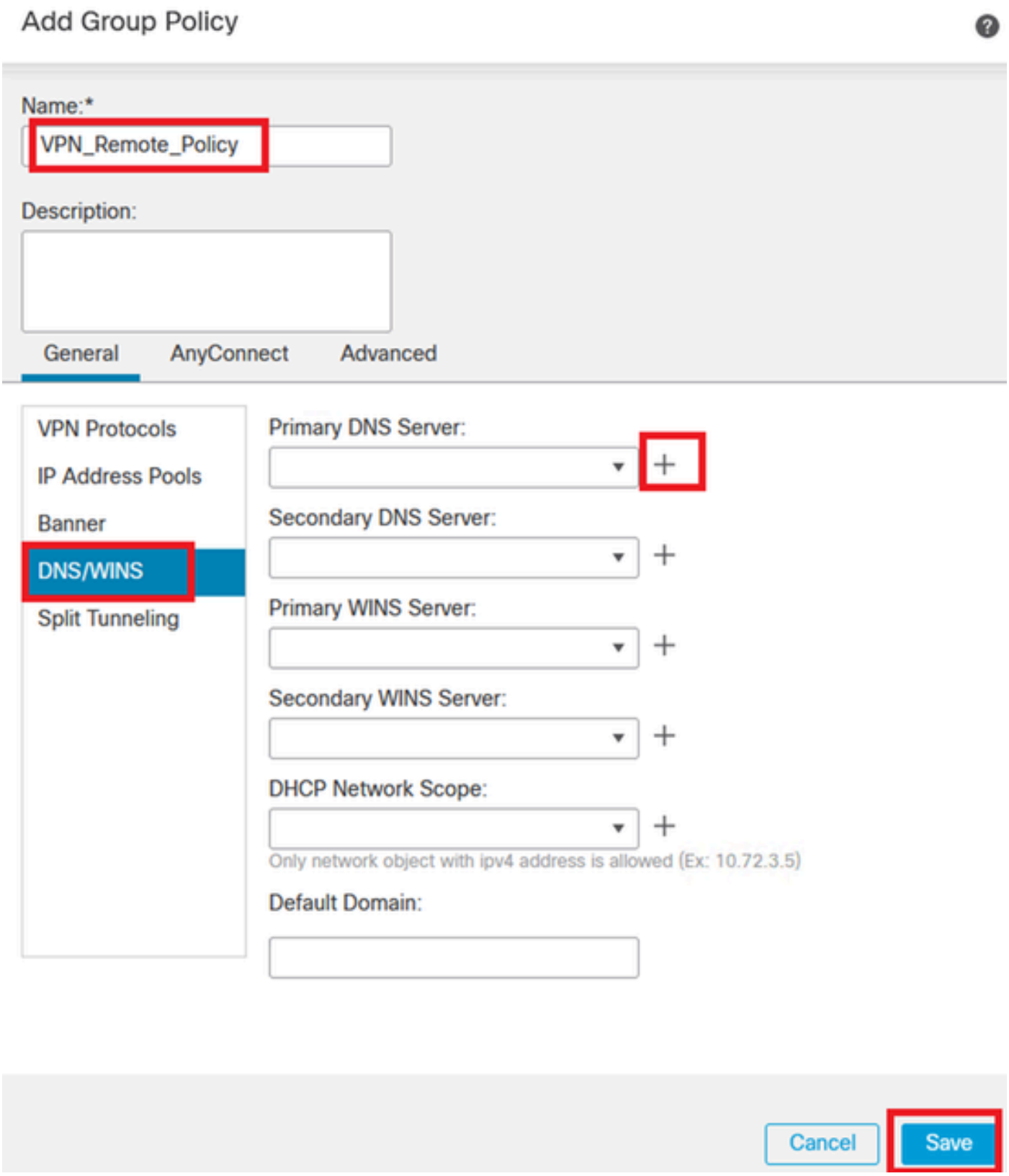
VPN Protocols.

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

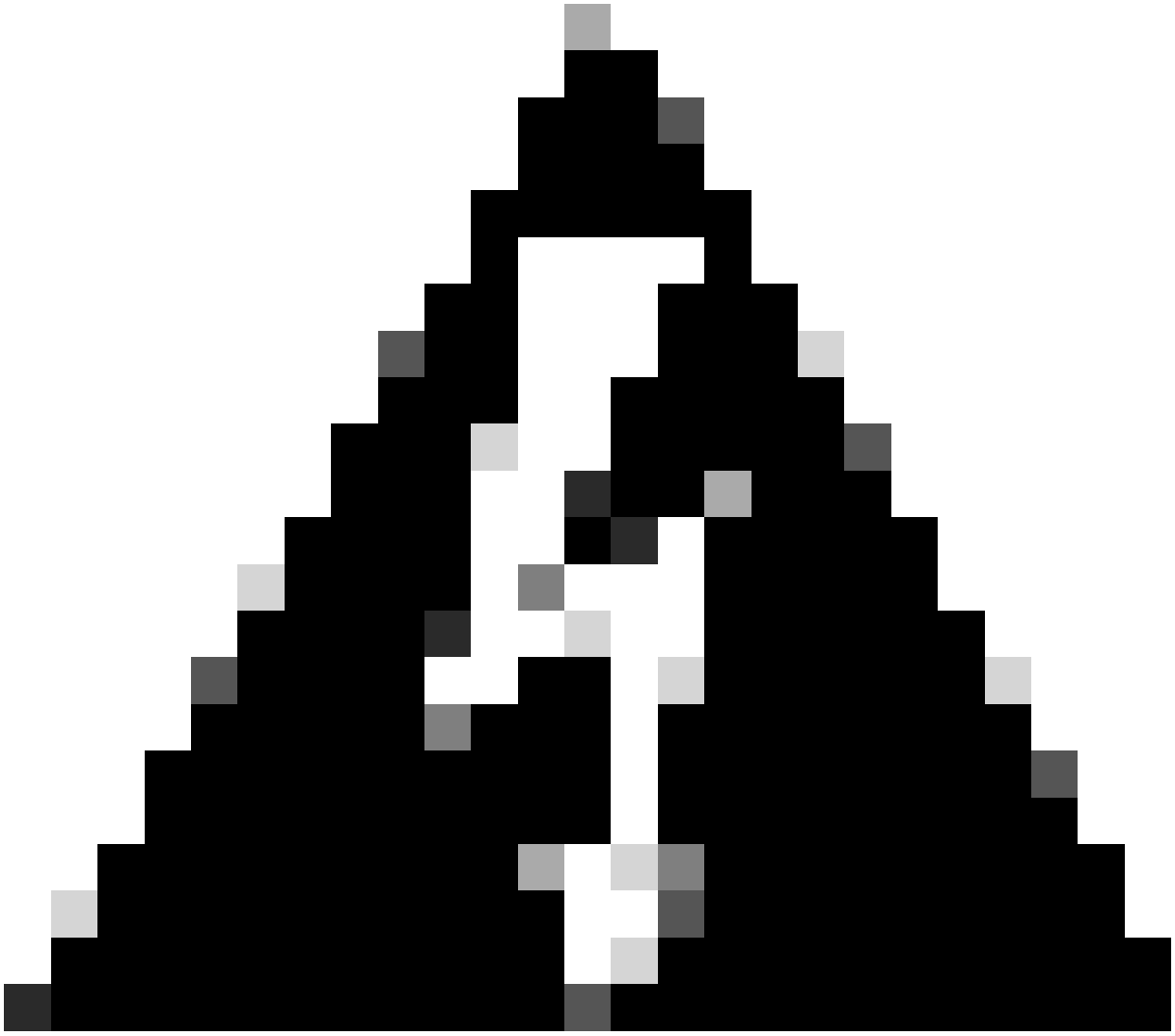


Pool VPN.

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

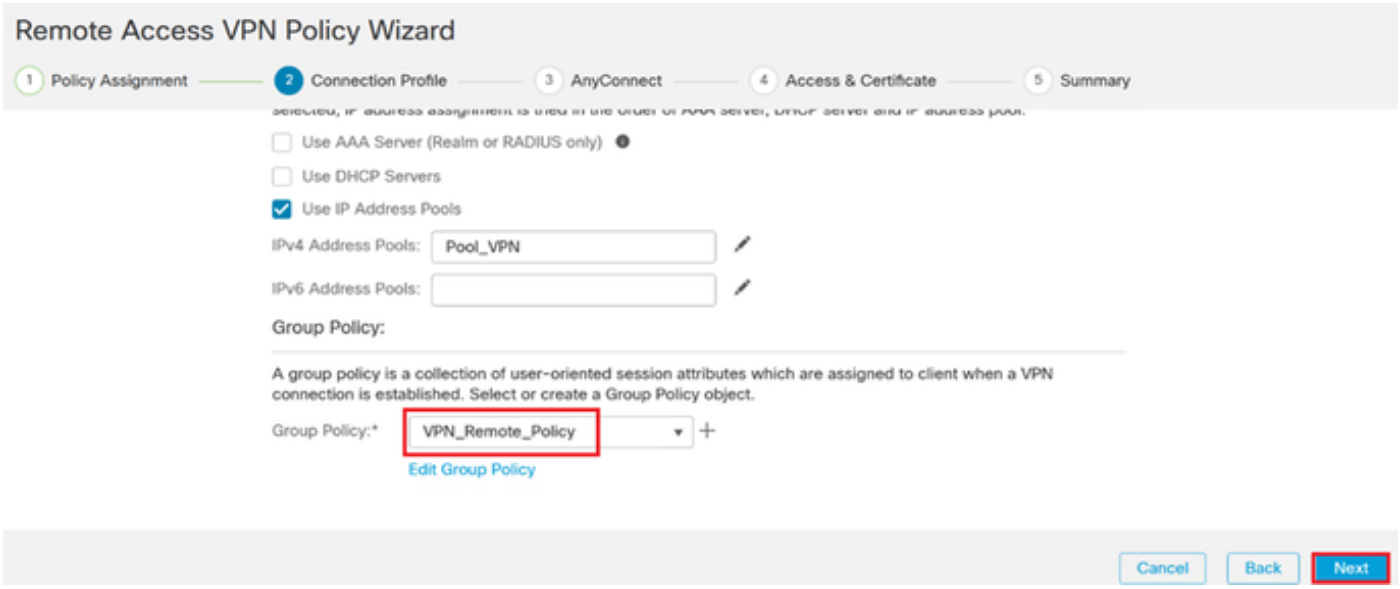


DNS Settings.



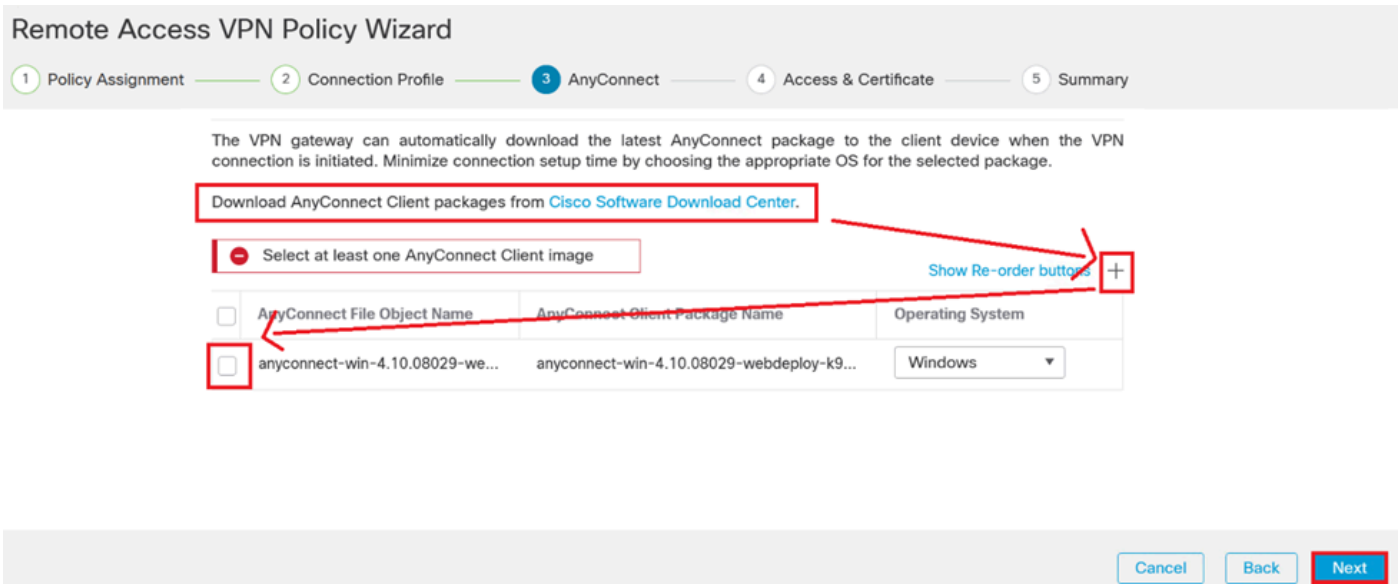
Warning: Please note that additional features such as the Banner, Split Tunneling, AnyConnect, and Advanced options are considered optional for this configuration.

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



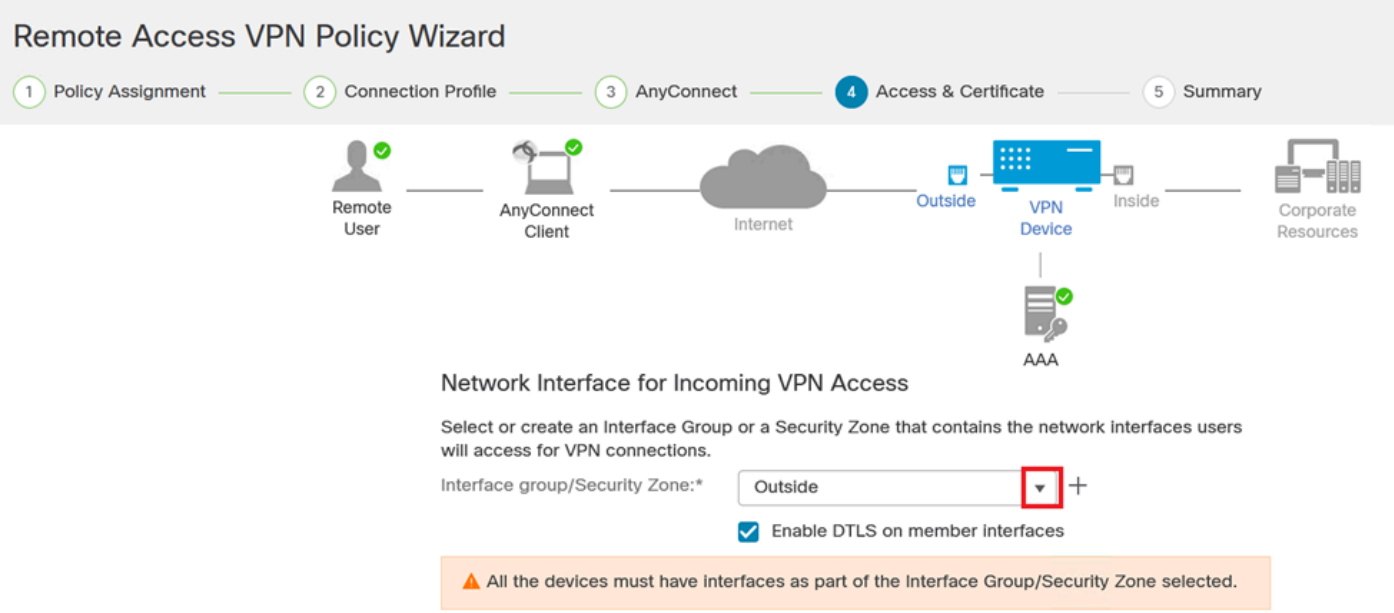
Group Policy.

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.



Package installation.

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



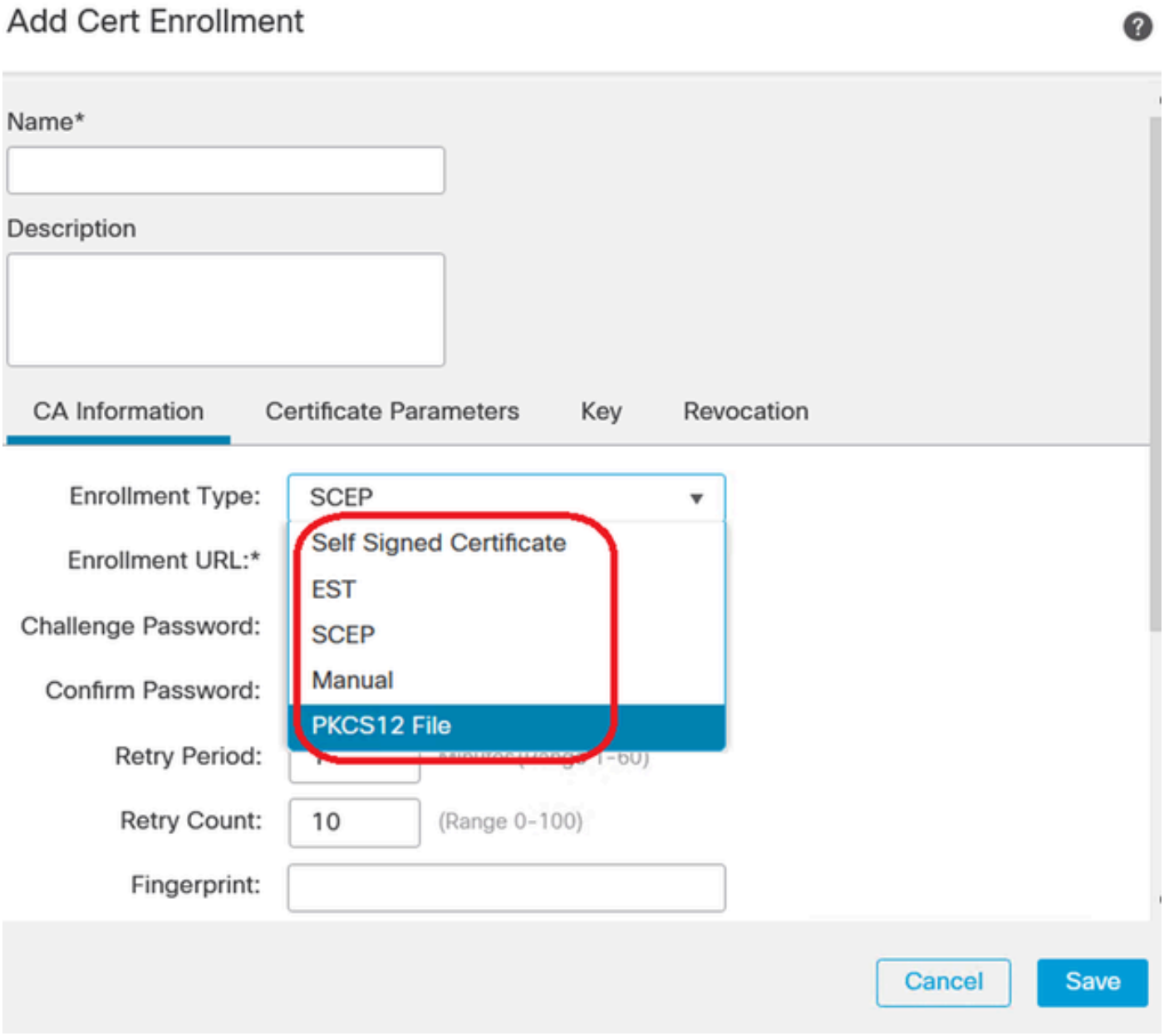
VPN Interface

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.

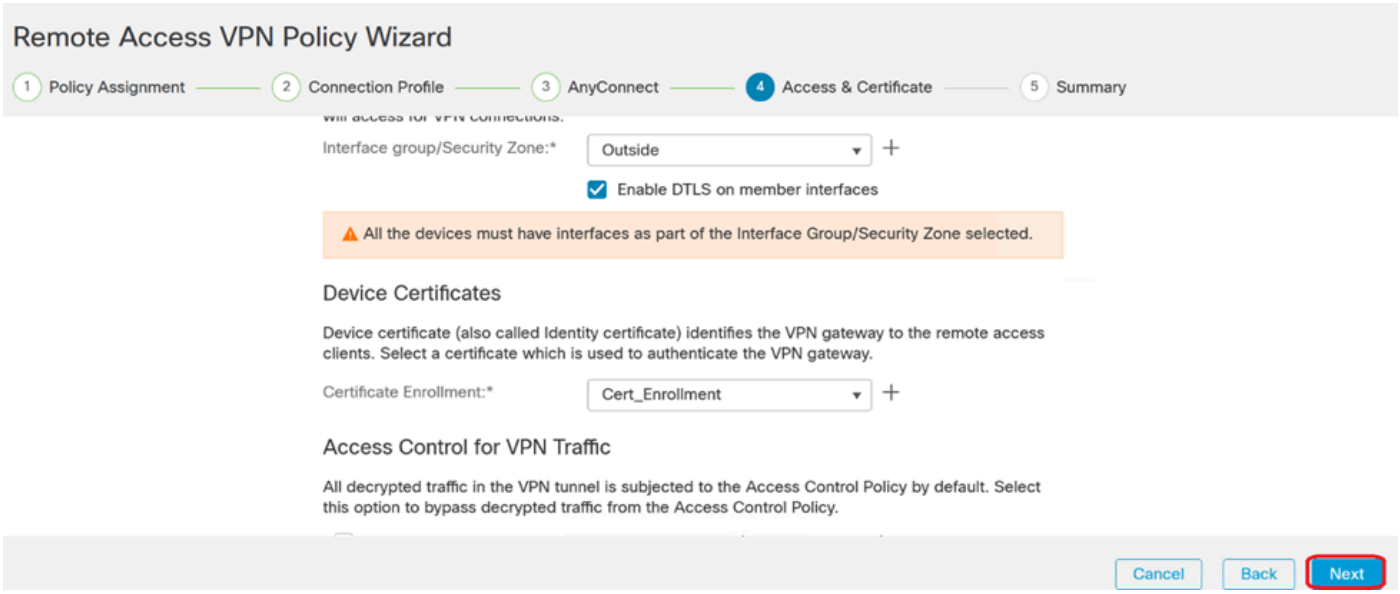


Device Certificate.



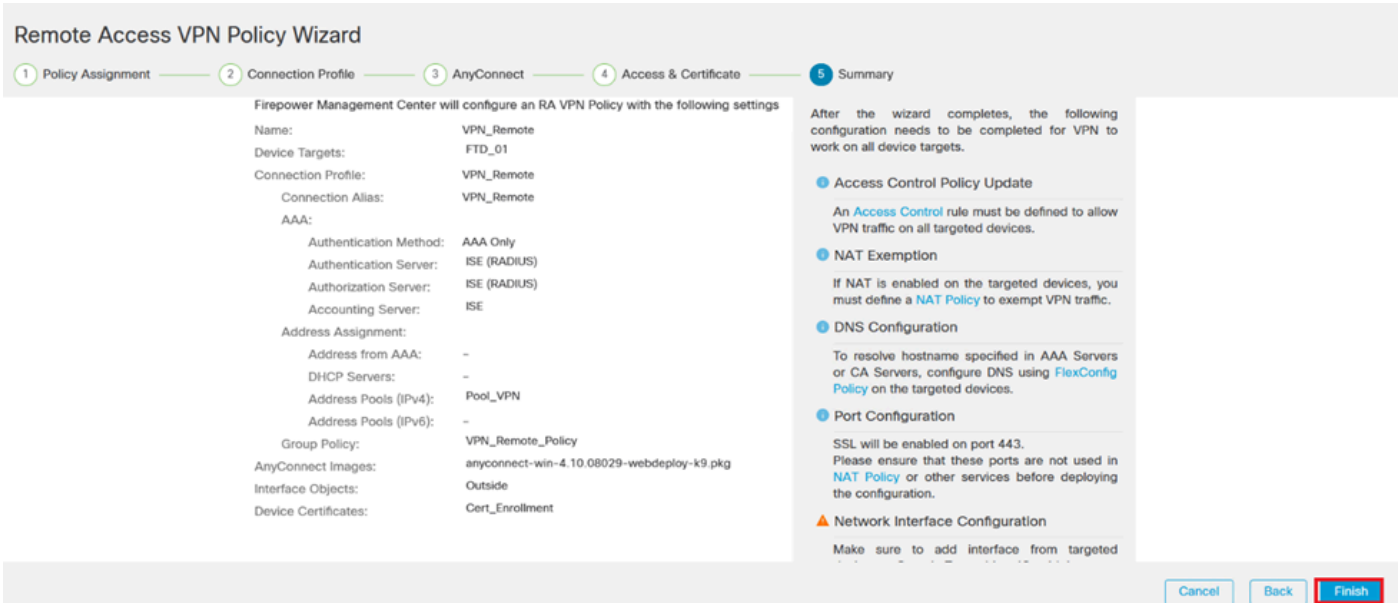
Cert Enrollment.

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



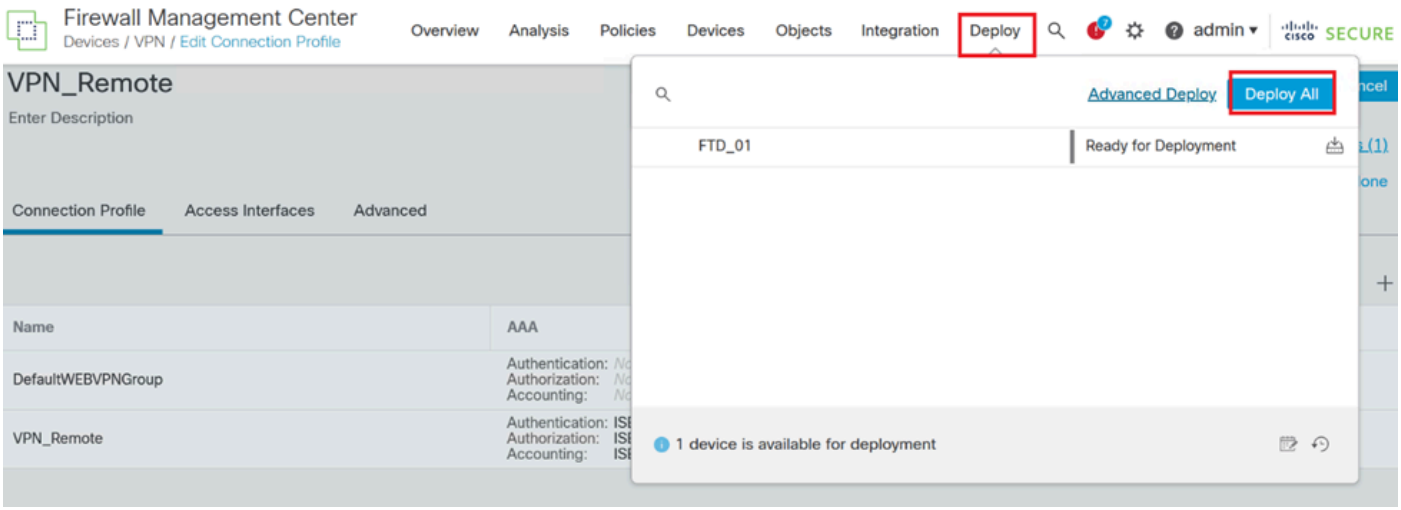
Summary of Access & services

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



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.



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.

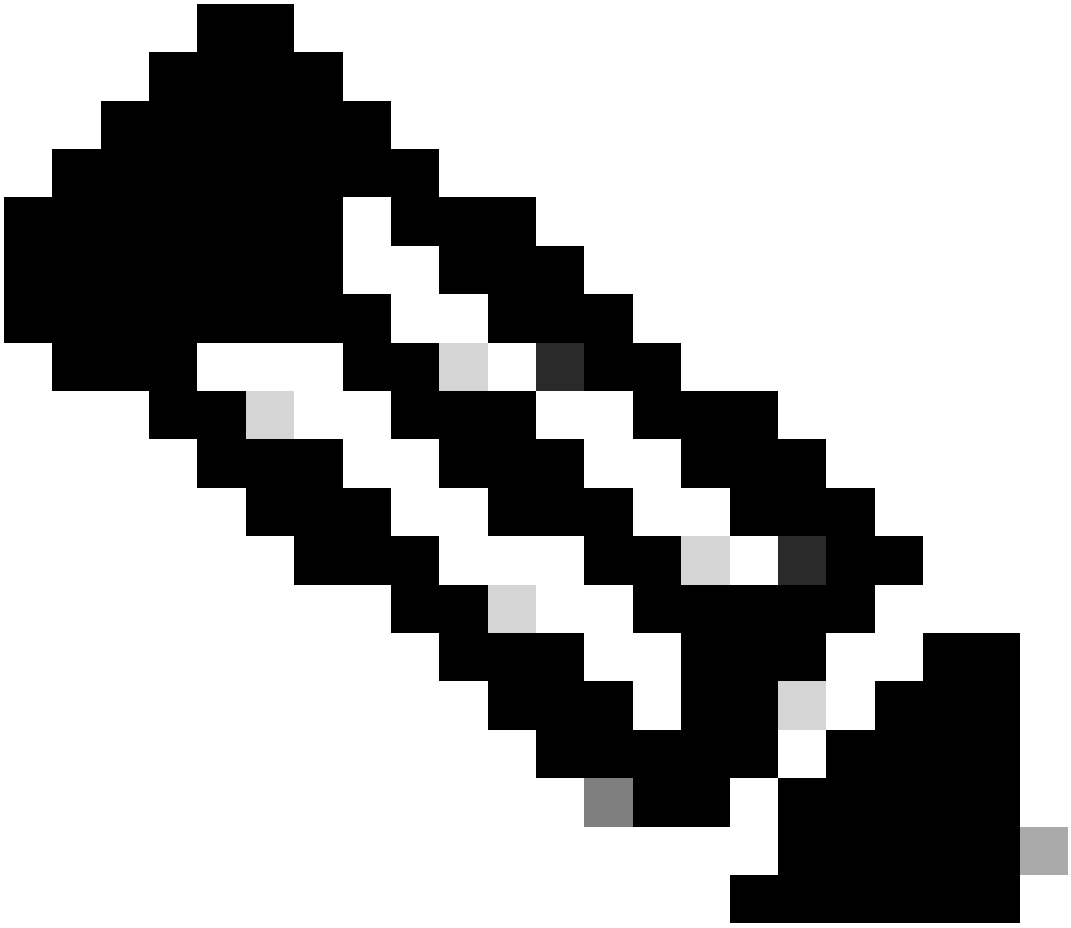


External Radius Servers

3. Enter a name for the Proxy DUO Server.

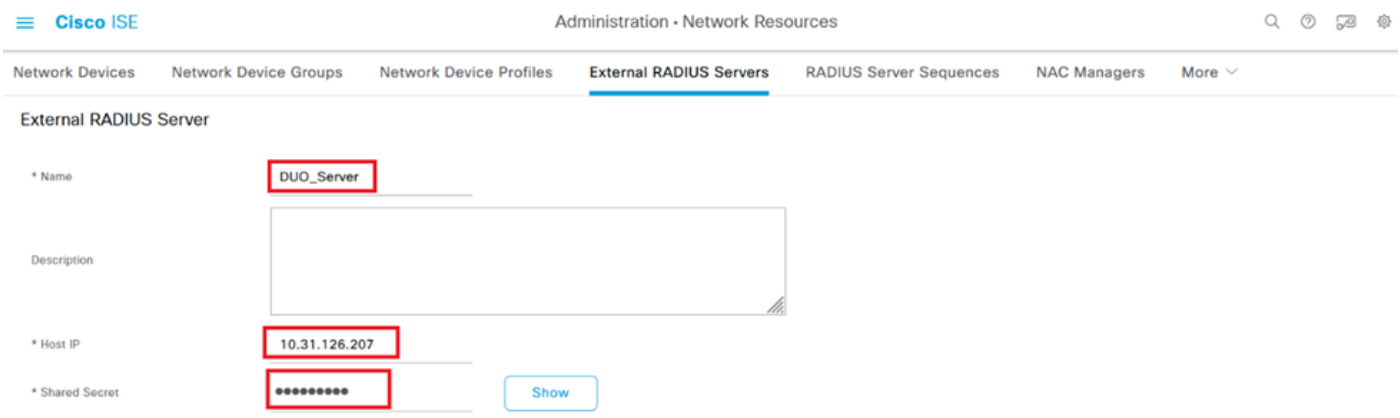
4. Input the correct IP address for the Proxy DUO Server to ensure proper communication between the ISE and the DUO server.

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.

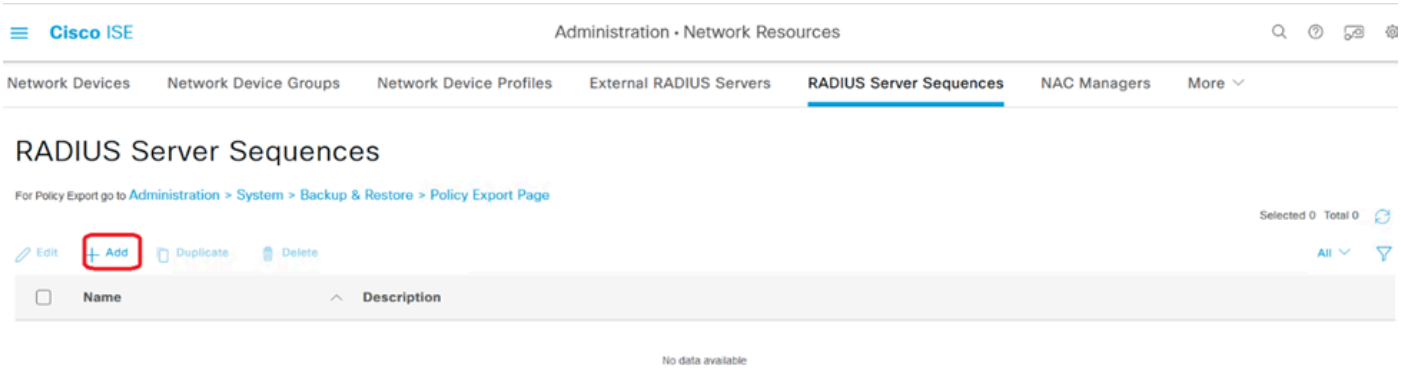
6. Once all the details are correctly entered, click **Submit** to save the new Proxy DUO Server configuration.



External RADIUS Servers

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

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

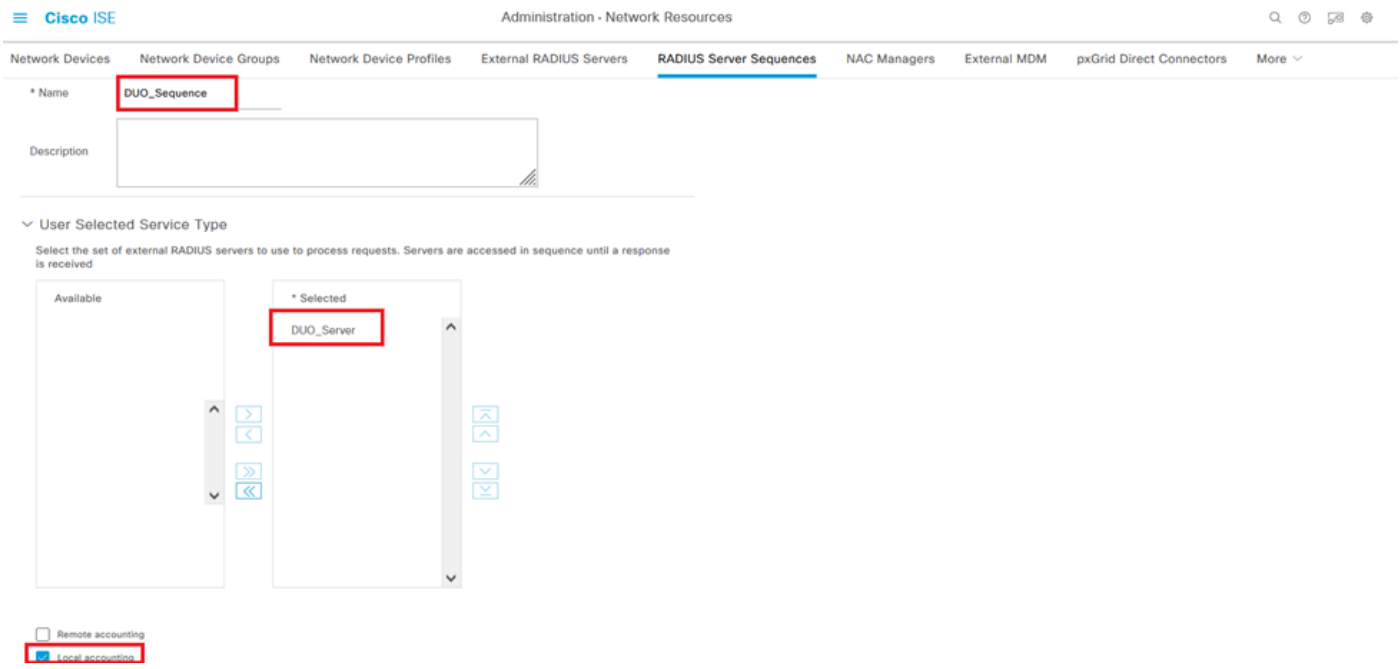


RADIUS Server Sequences

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.

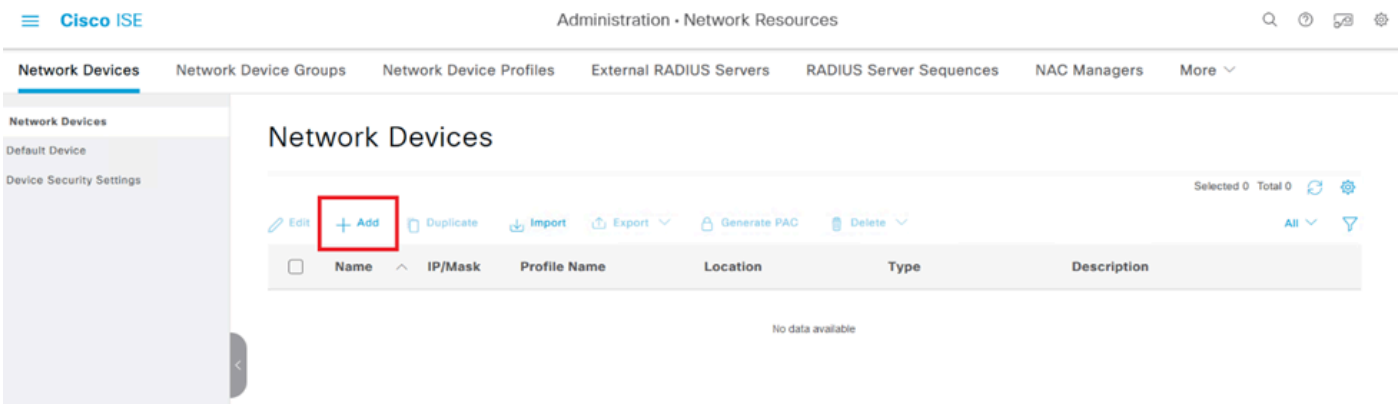


Radius Server Sequences configuration.

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.



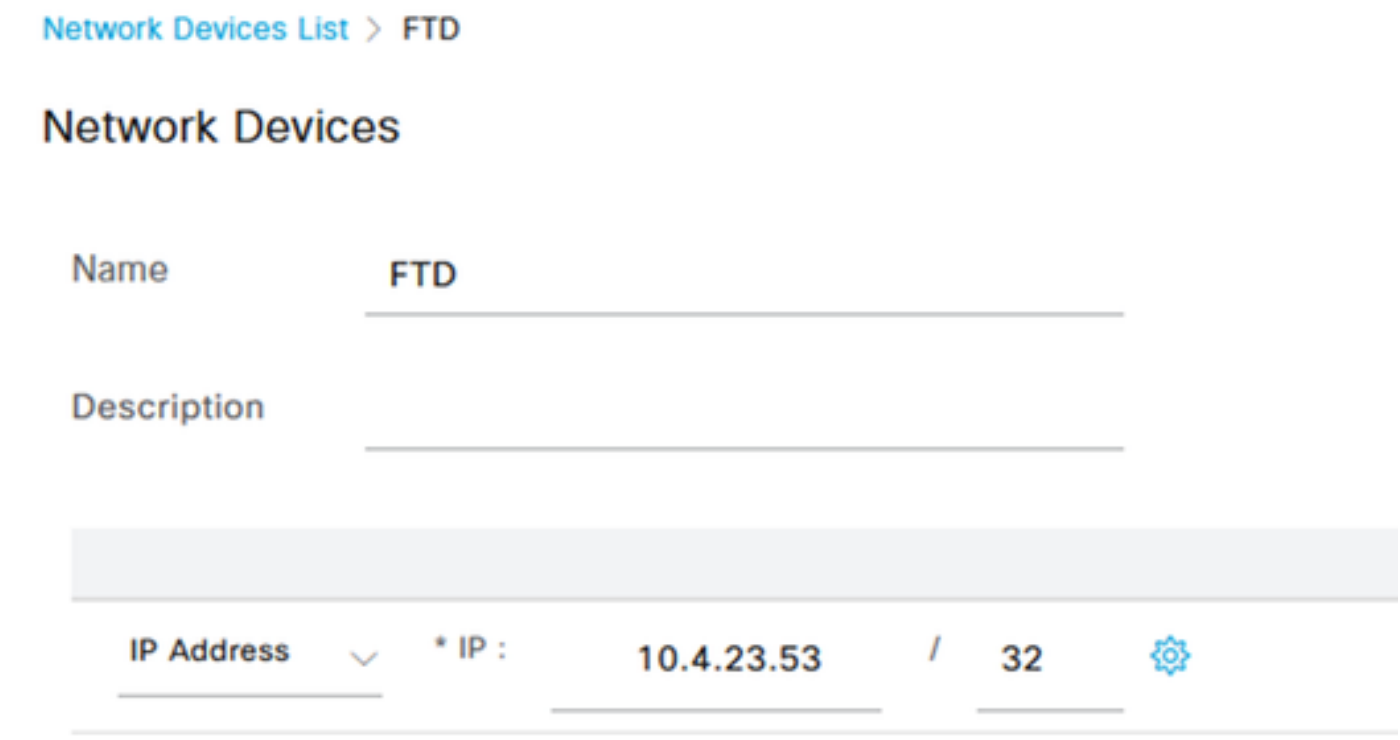
Network Access Devices.

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

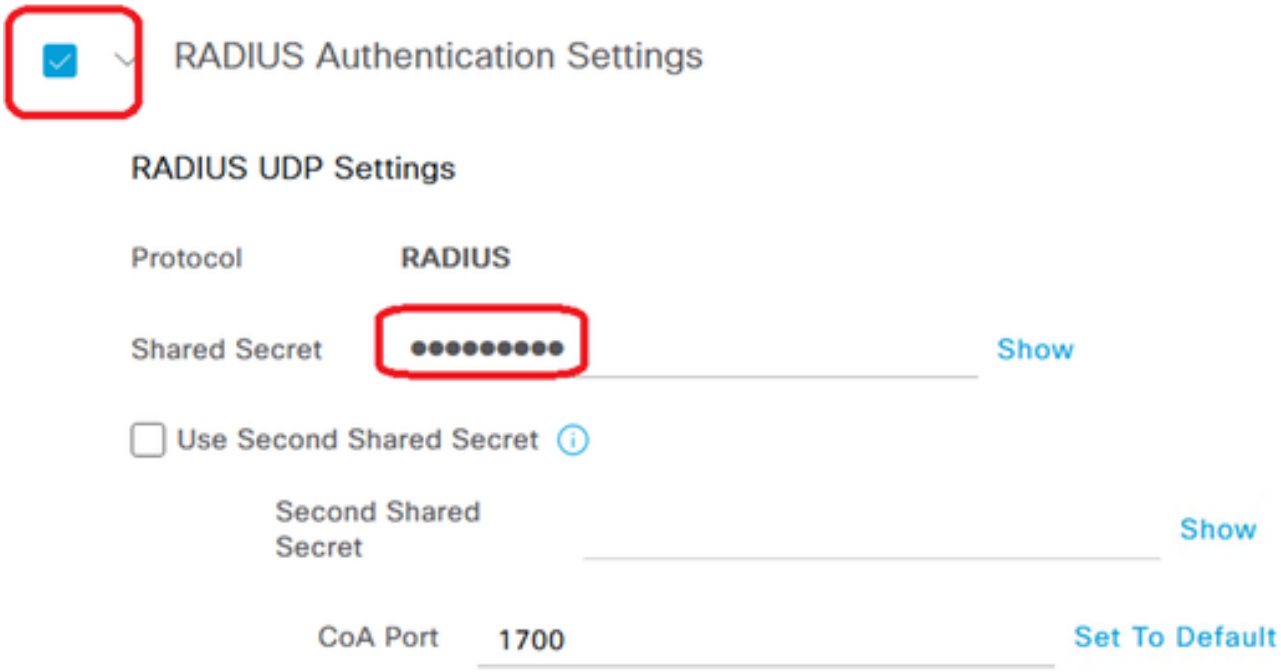
4. Proceed to specify the IP Address of the FTD (Firepower Threat Defense) device.

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.



Adding FTD as NAD.



RADIUS settings

DUO configurations.

DUO Proxy Installation.

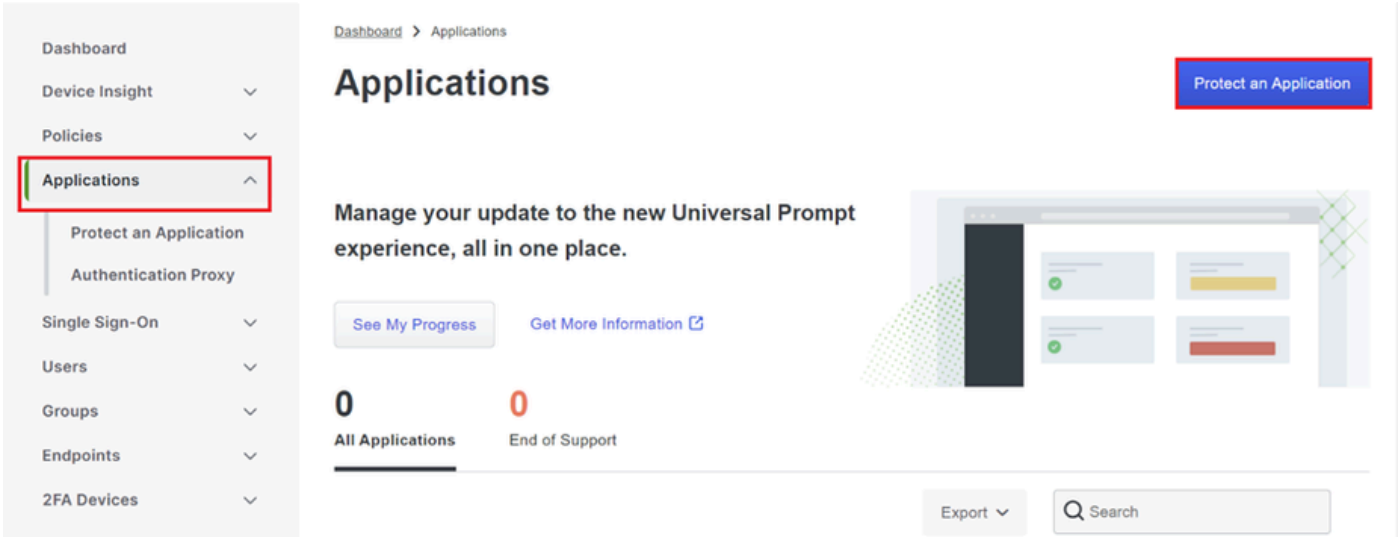
Access the **DUO Proxy Download and Installation Guide** by clicking on the next link:

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

Integrate DUO Proxy with ISE and DUO Cloud.

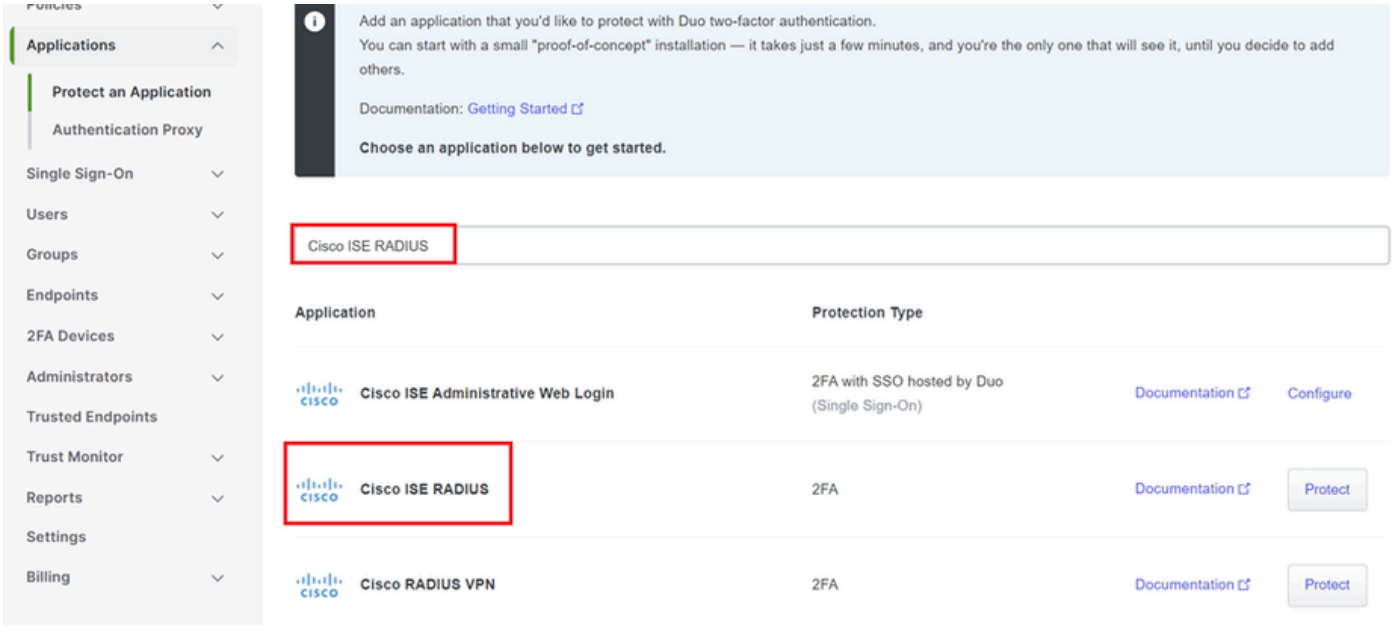
1. Log in to the DUO Security website at https://duo.com/ using your credentials.

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



DUO Applications

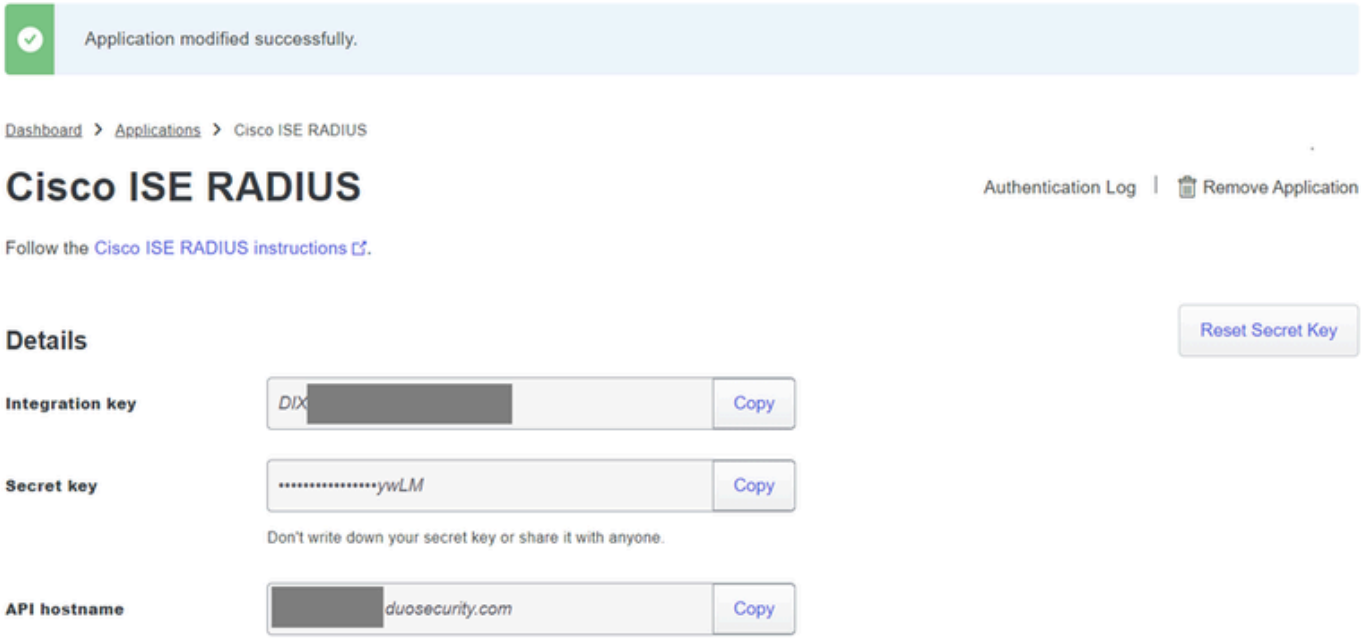
3. Search for the "**Cisco ISE RADIUS**" option in the list and click **Protect** to add it to your applications.



ISE RADIUS option

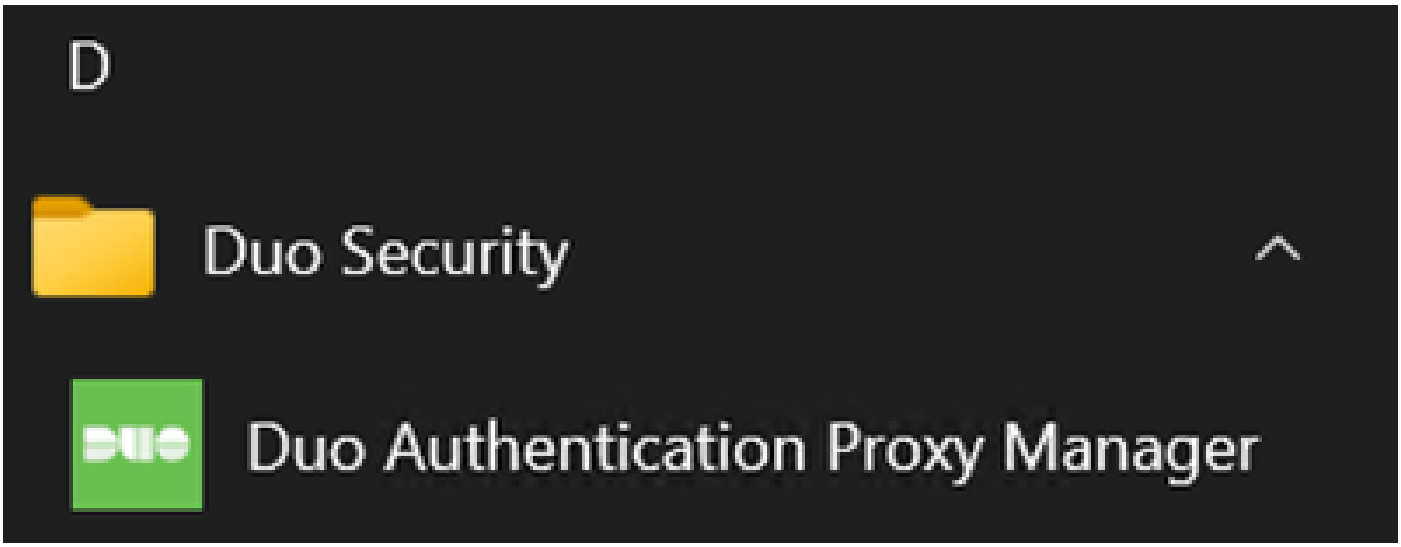
4. Upon successful addition, you are going to see the details of the DUO application. Scroll down and click **Save**.

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



ISE Server details

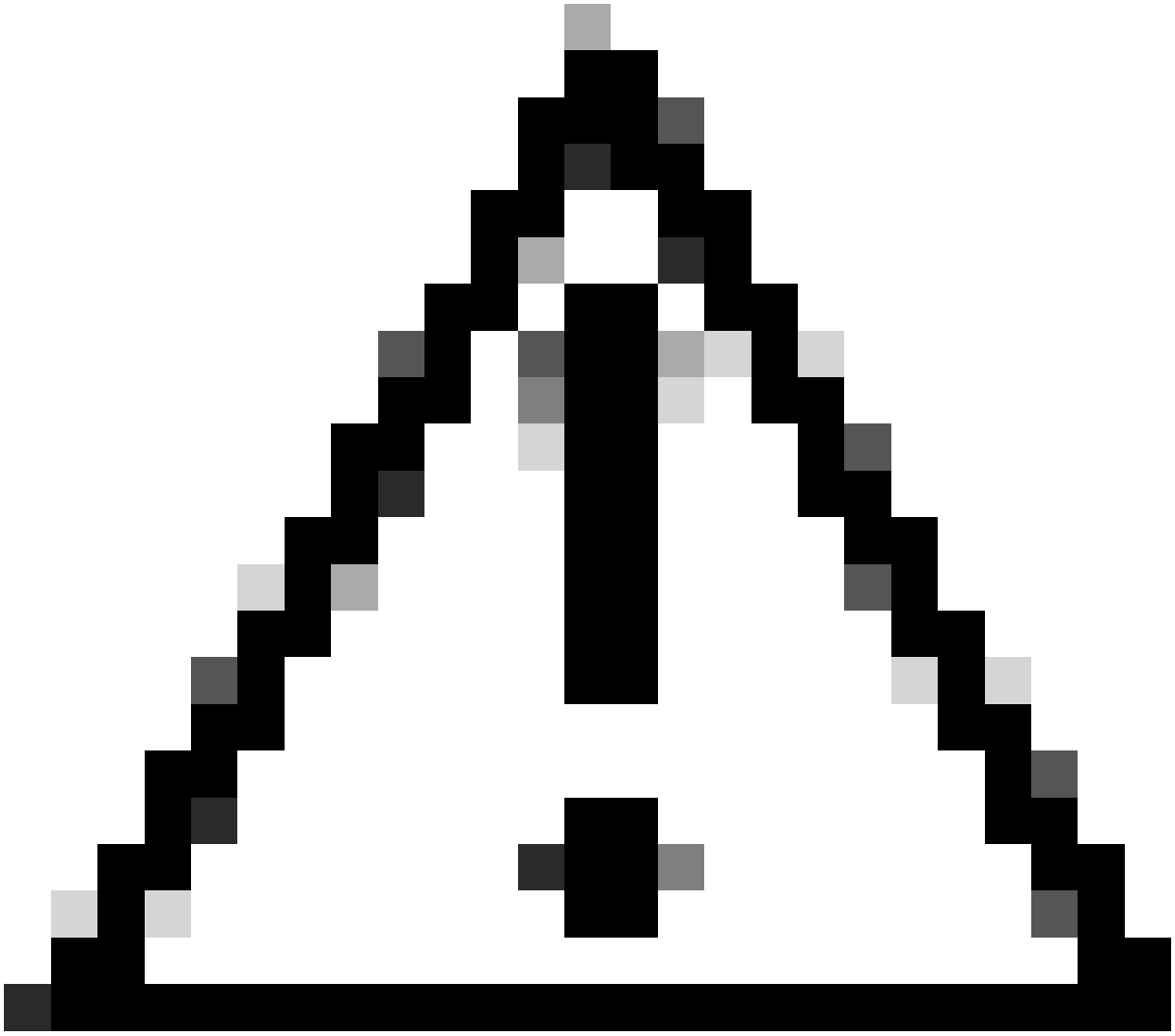
6. Launch the **DUO Proxy Manager** on your system to continue with the setup.



DUO Proxy Manager

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

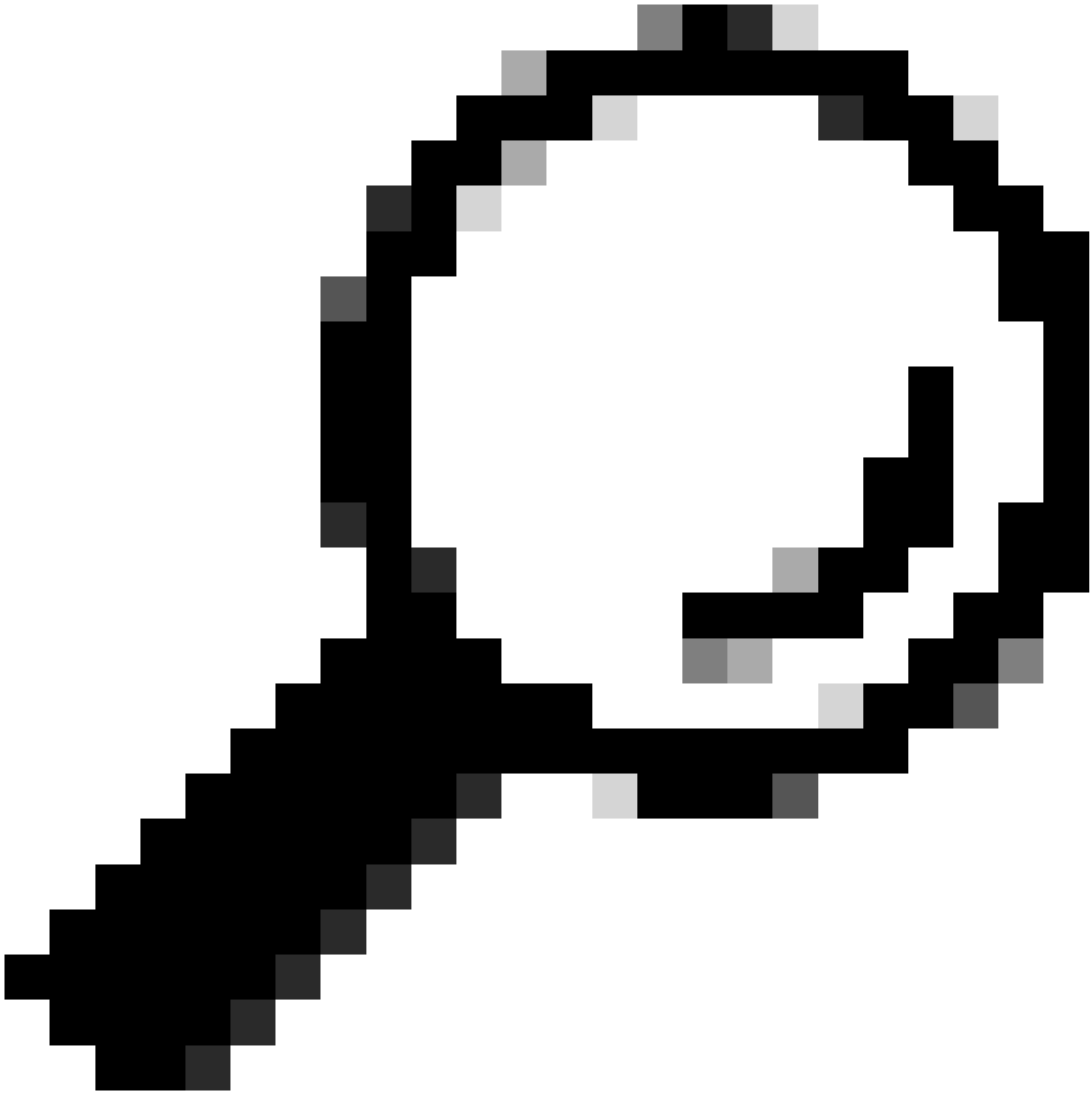
```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```



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.

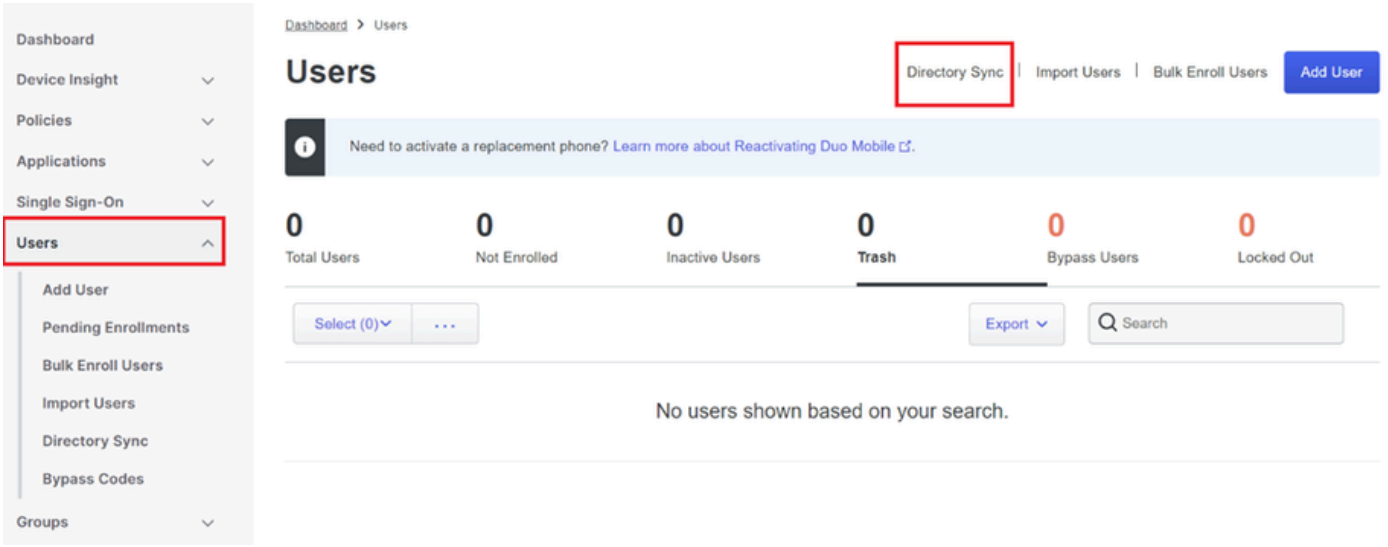
Integrate DUO with Active Directory.

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>
```

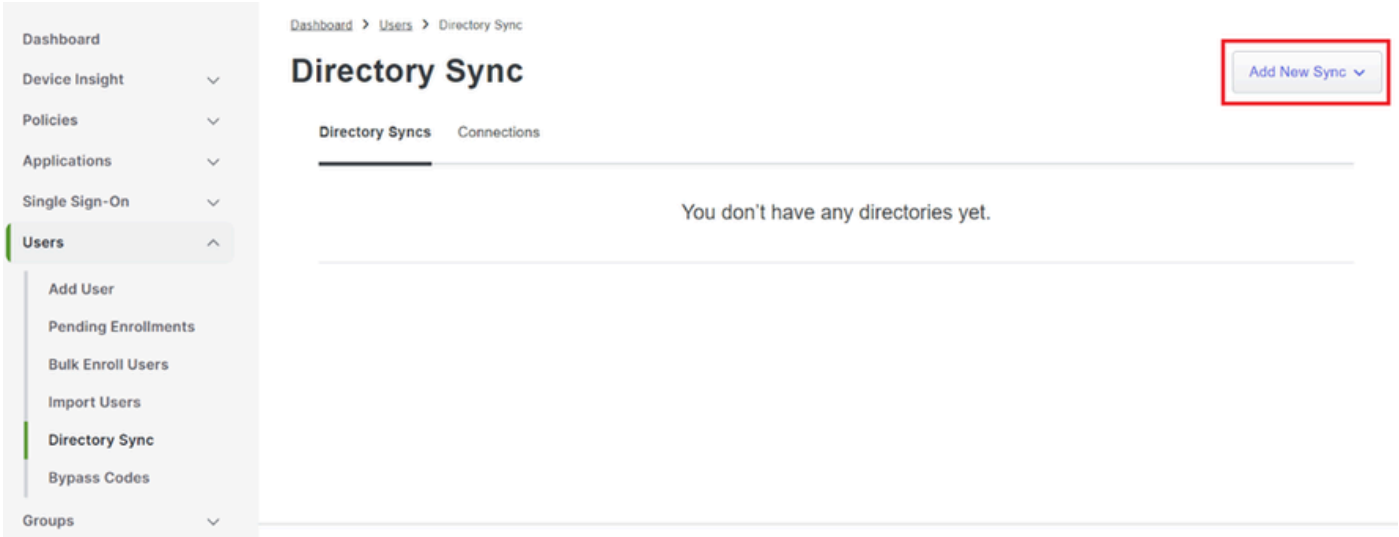
2. Join your Active Directory with DUO cloud services. Log in to https://duo.com/.

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



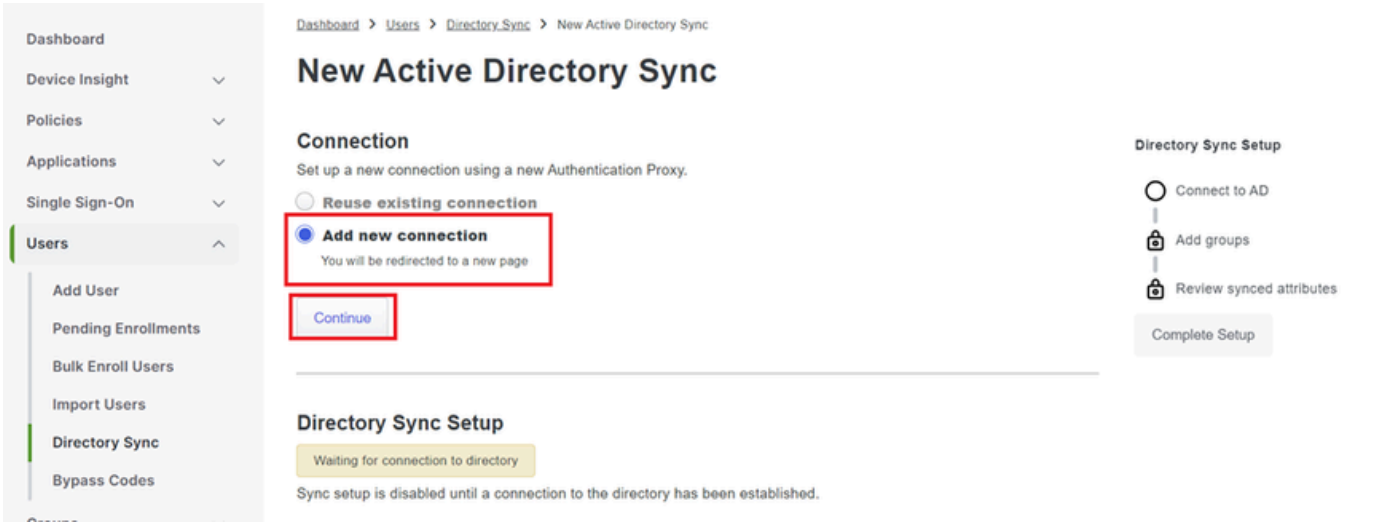
Directory Sync

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



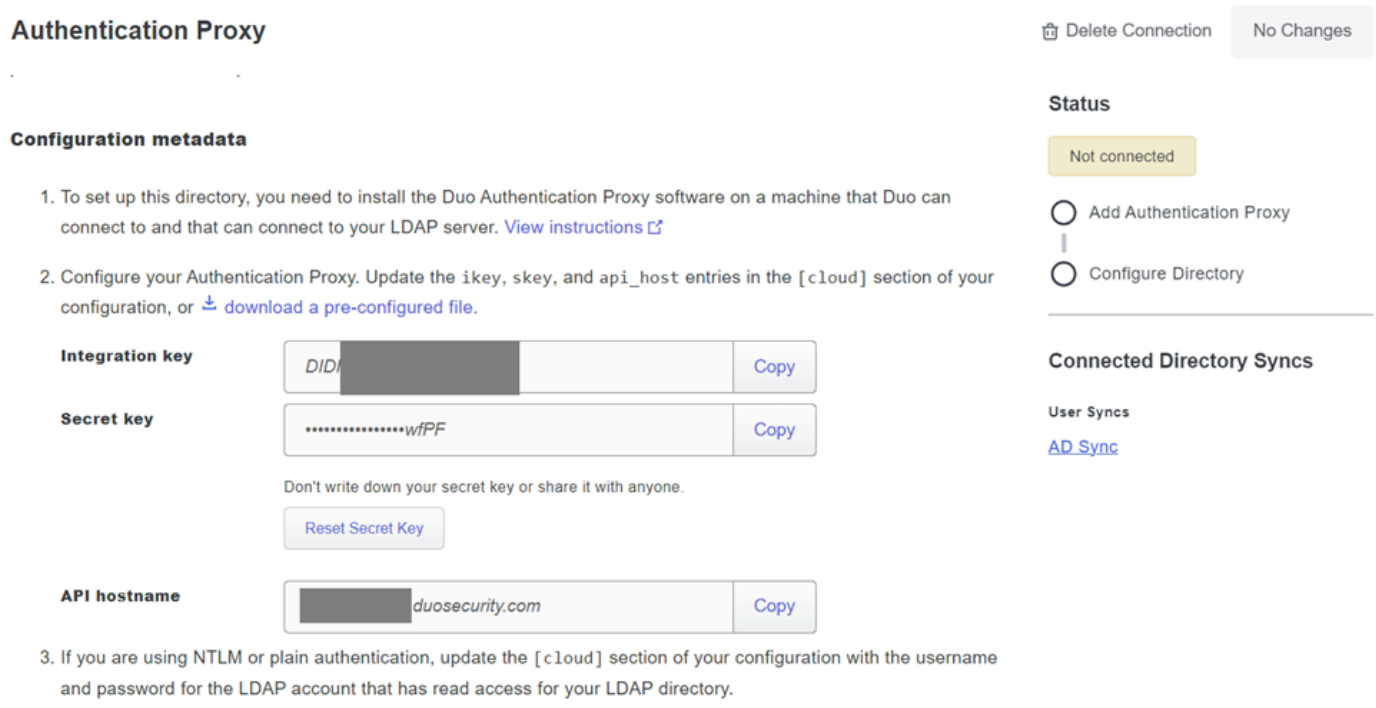
Add New Sync

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



Adding new Active Directory

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

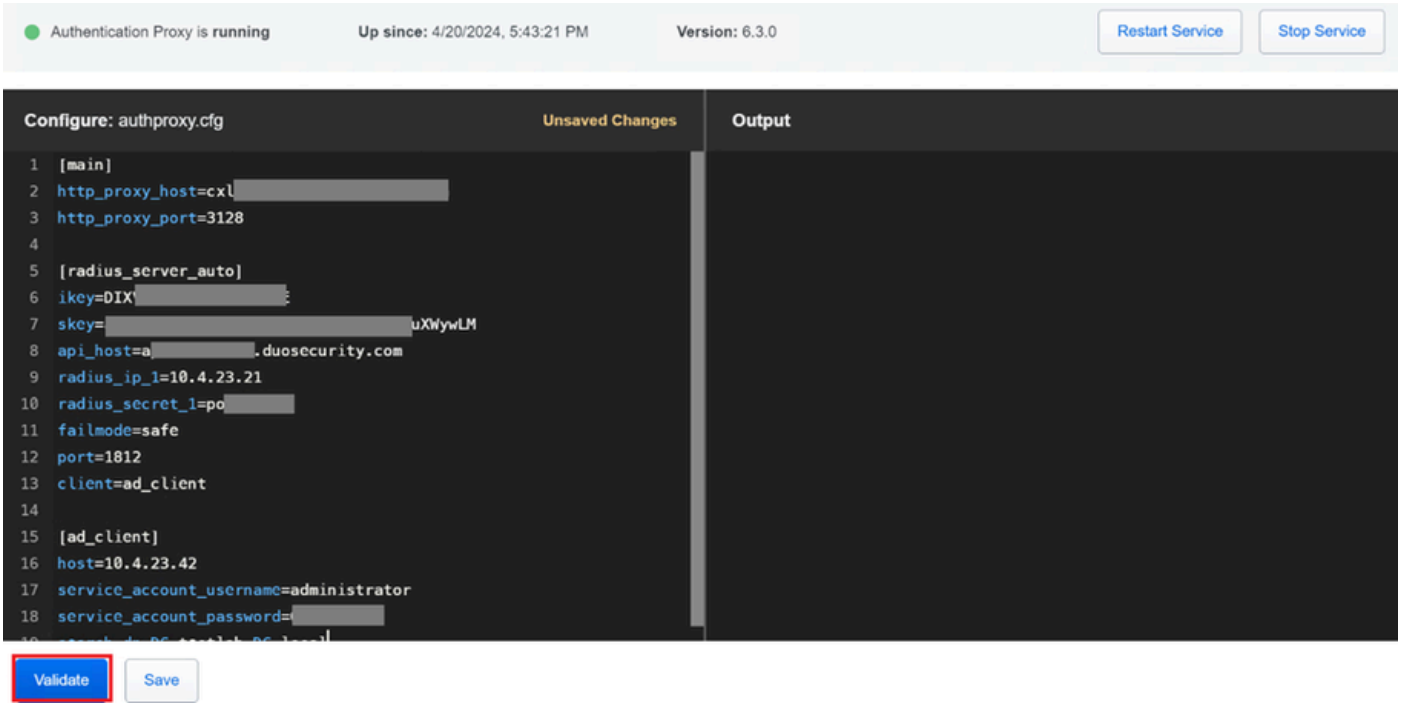


Authentication Proxy details

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:

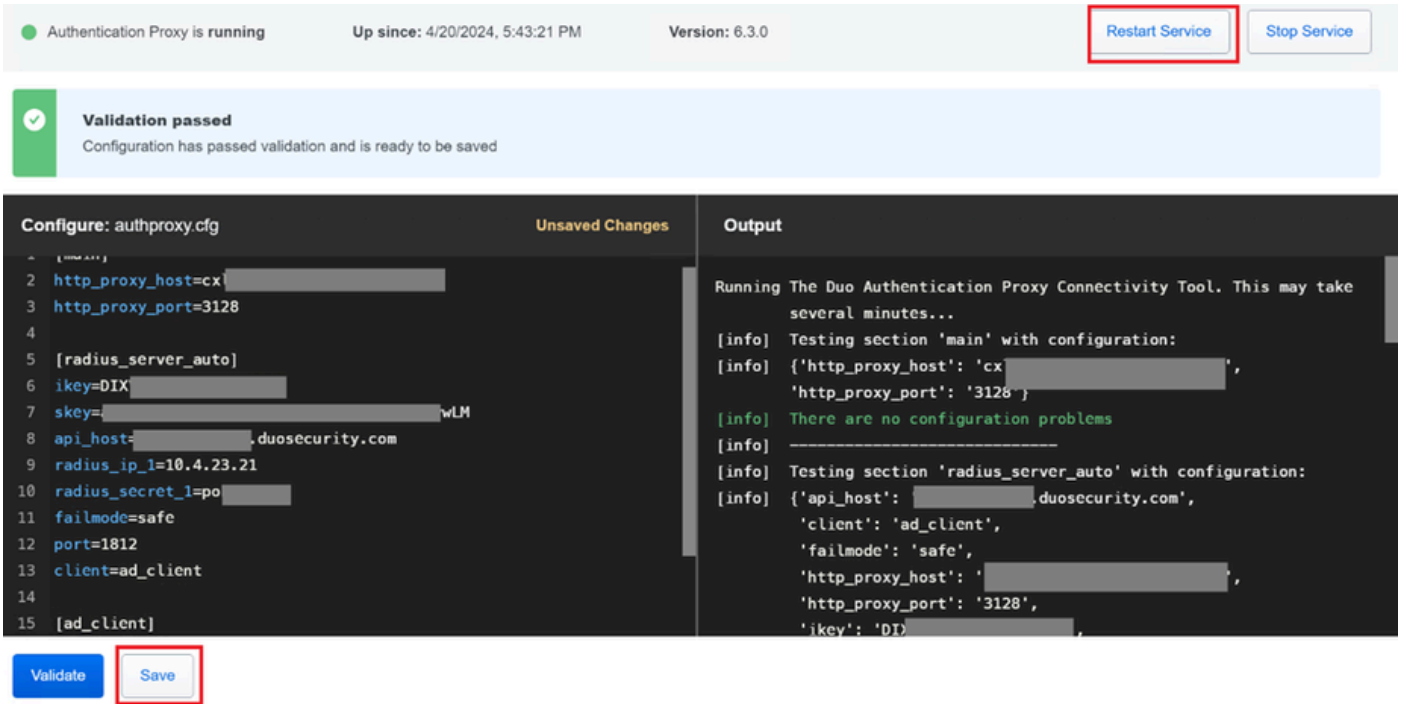
```
[cloud]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
service_account_username=<your domain>\<service_account_username>
service_account_password=<service_account_password>
```

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



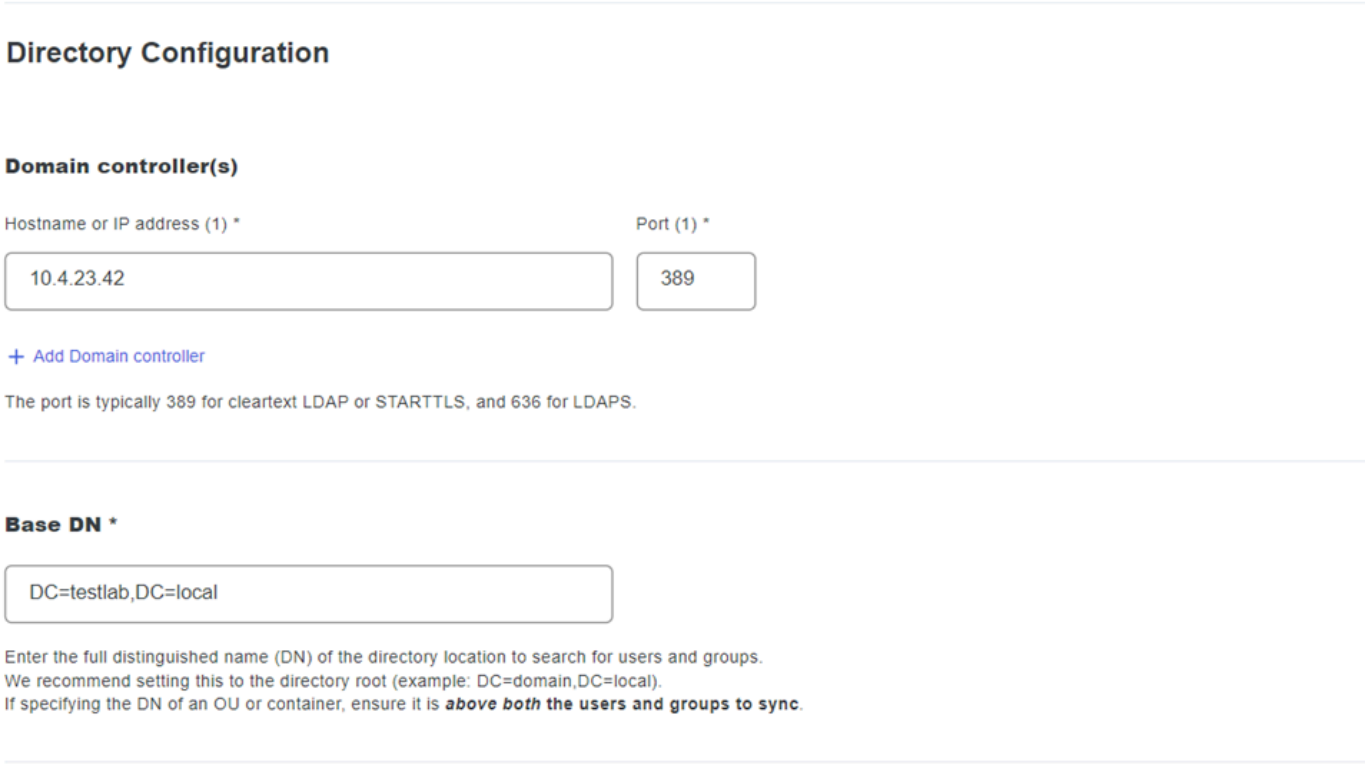
Configuration of Proxy DUO.

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



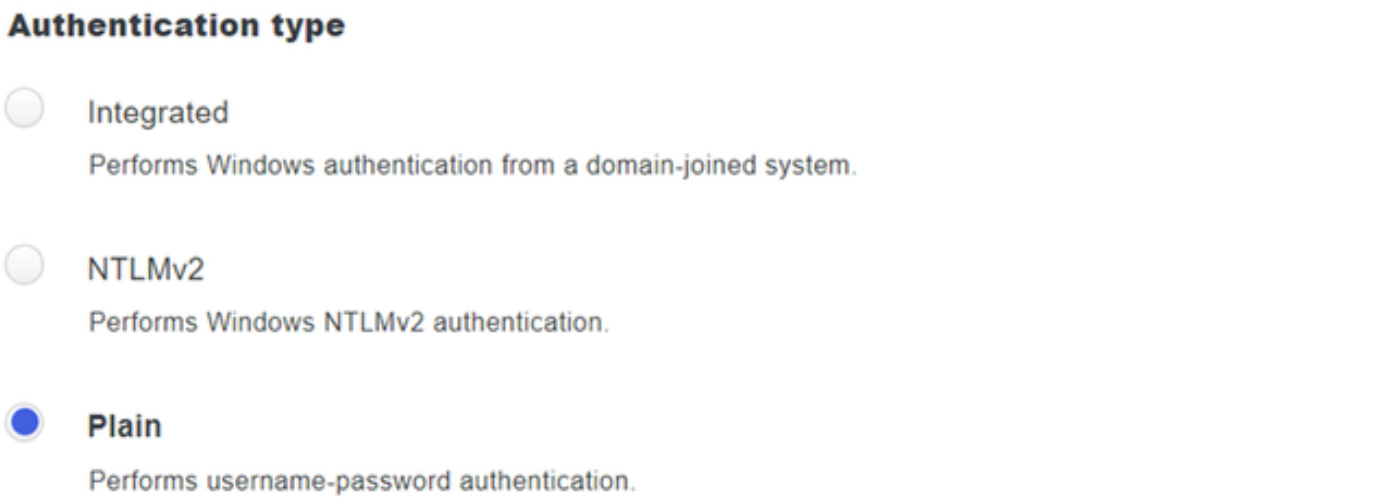
Restart Service option.

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



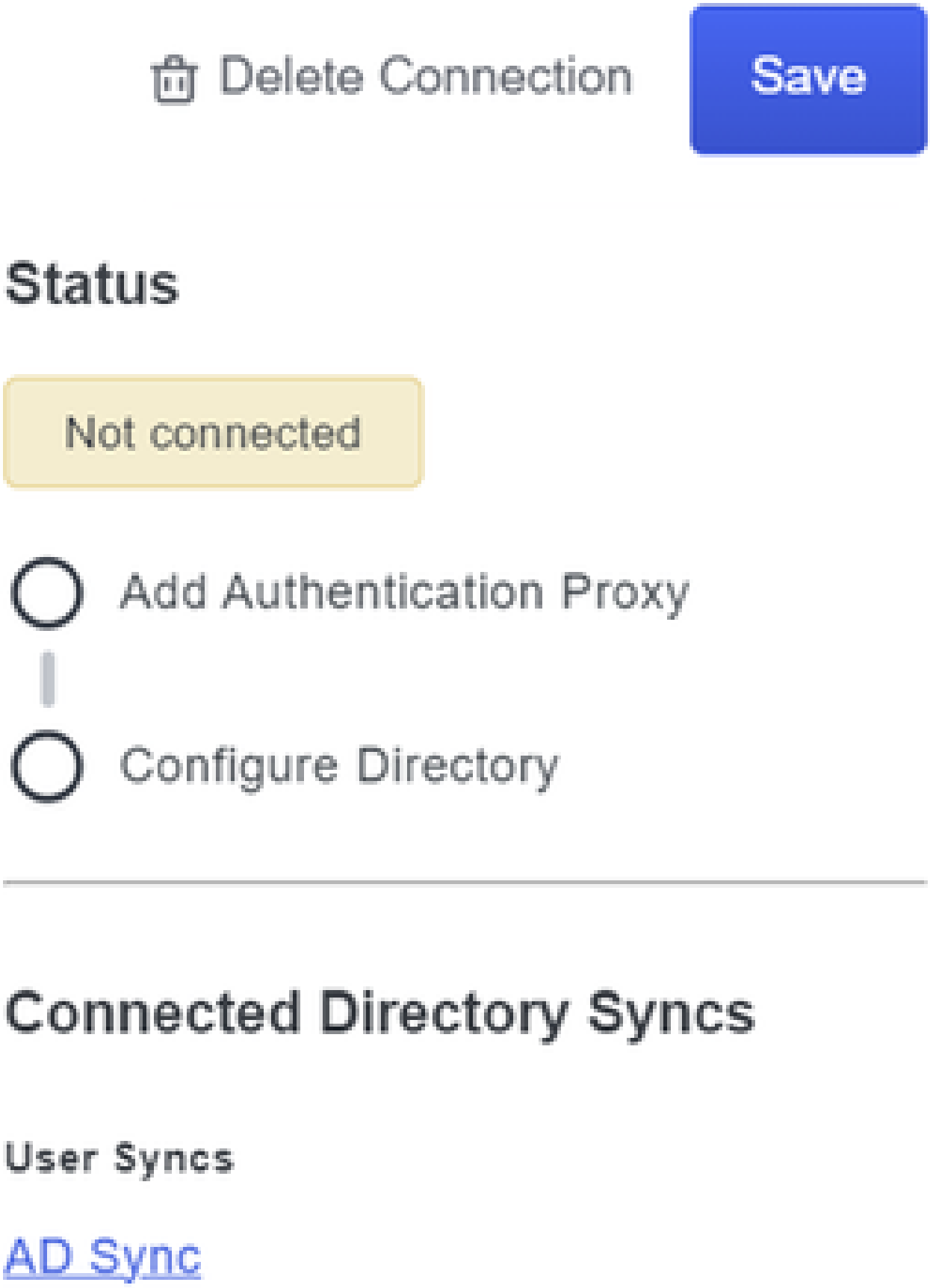
Directory settings.

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



Authentication type.

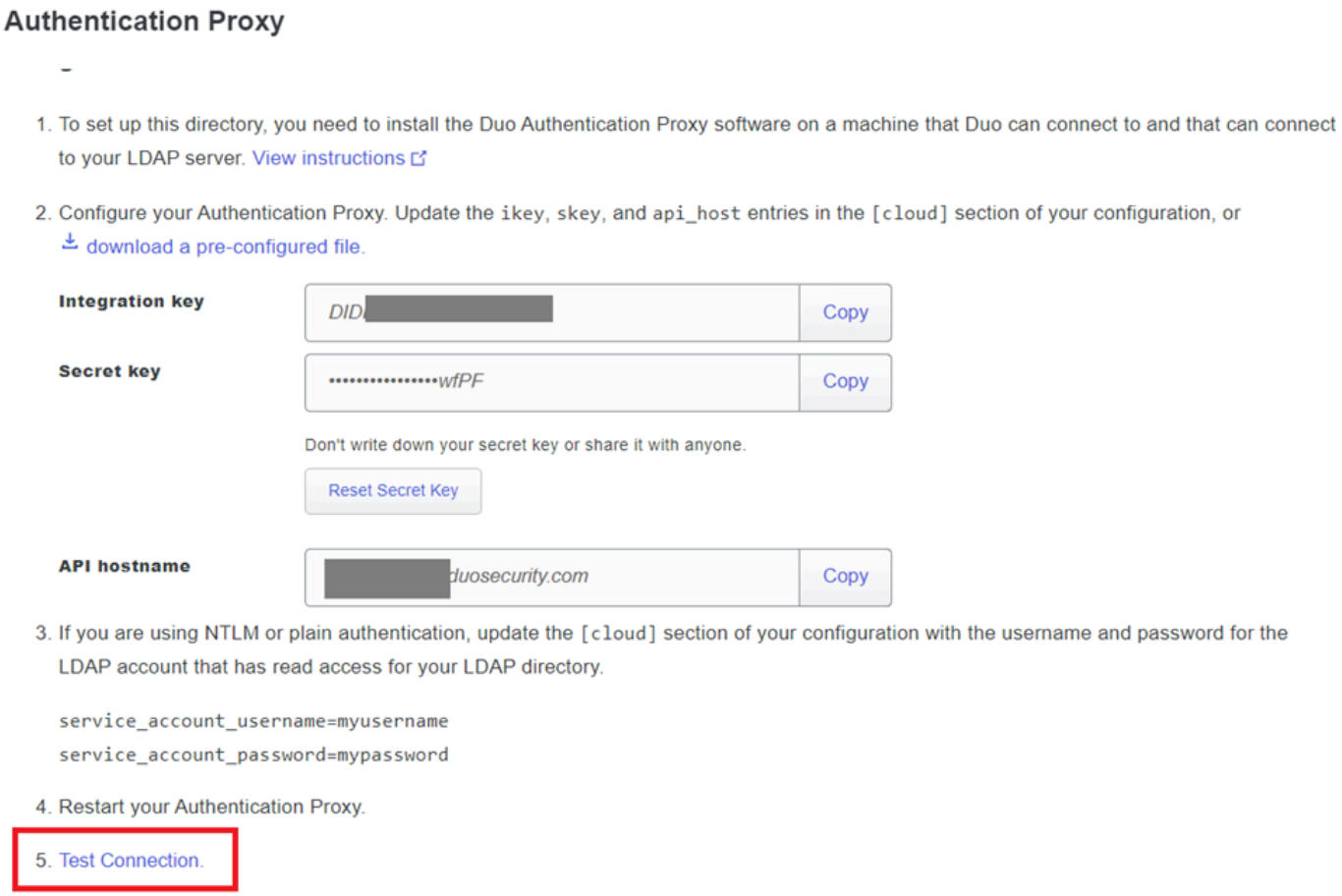
12. Save your new settings to ensure the configuration is updated.



Save option

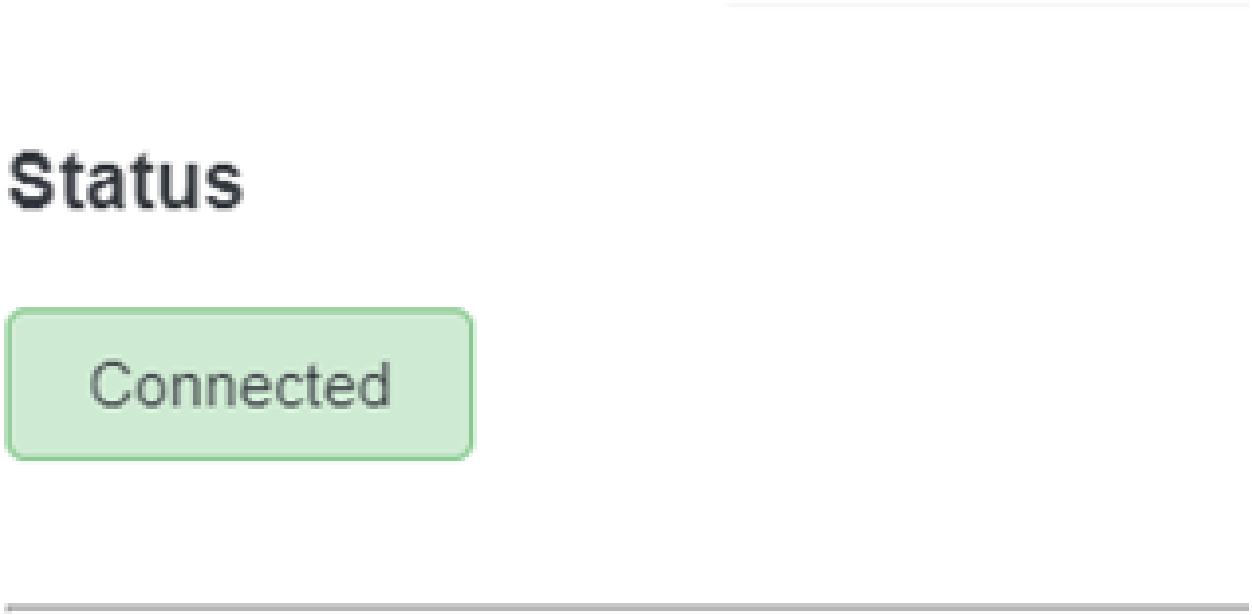
13. Utilize the "**test connection**" feature to verify that the DUO Cloud service can communicate with your

Active Directory.



Test connection option.

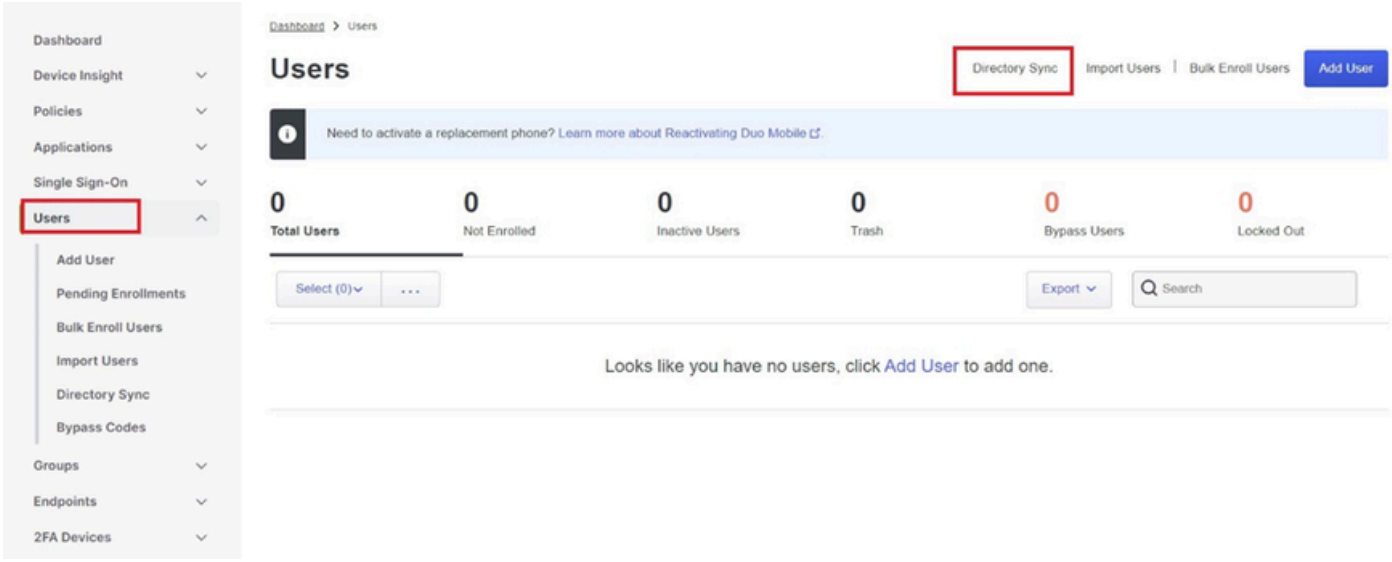
14. Confirm that the Active Directory status displays as "**Connected**," indicating a successful integration.



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.

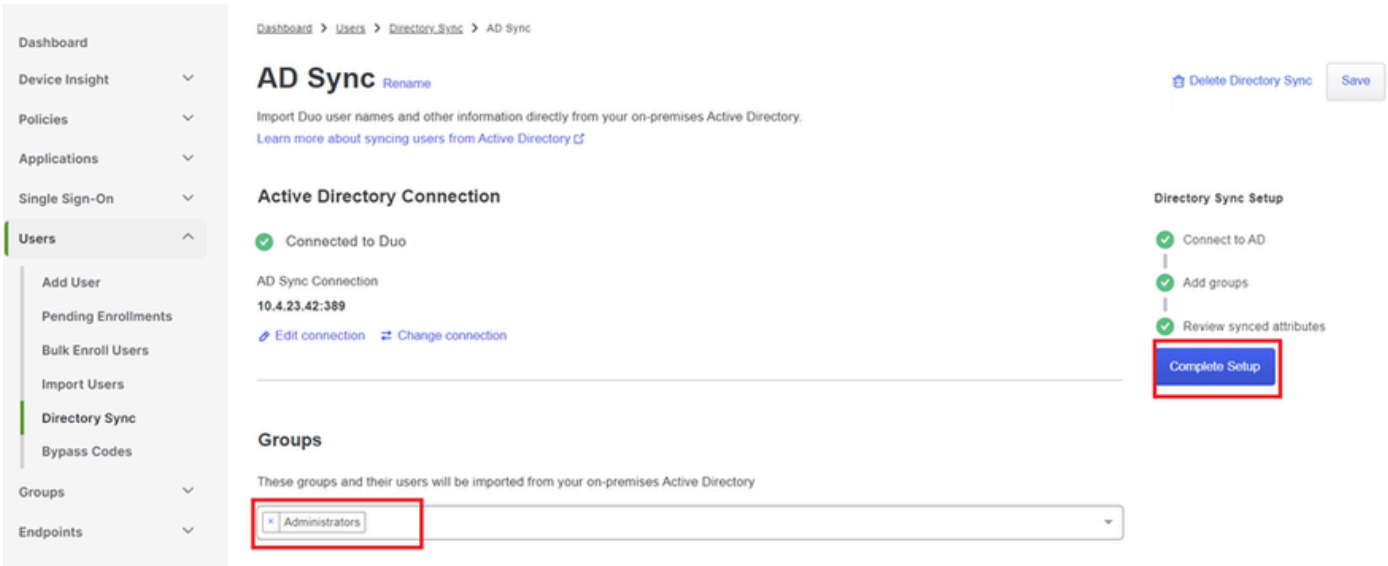


User list.

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

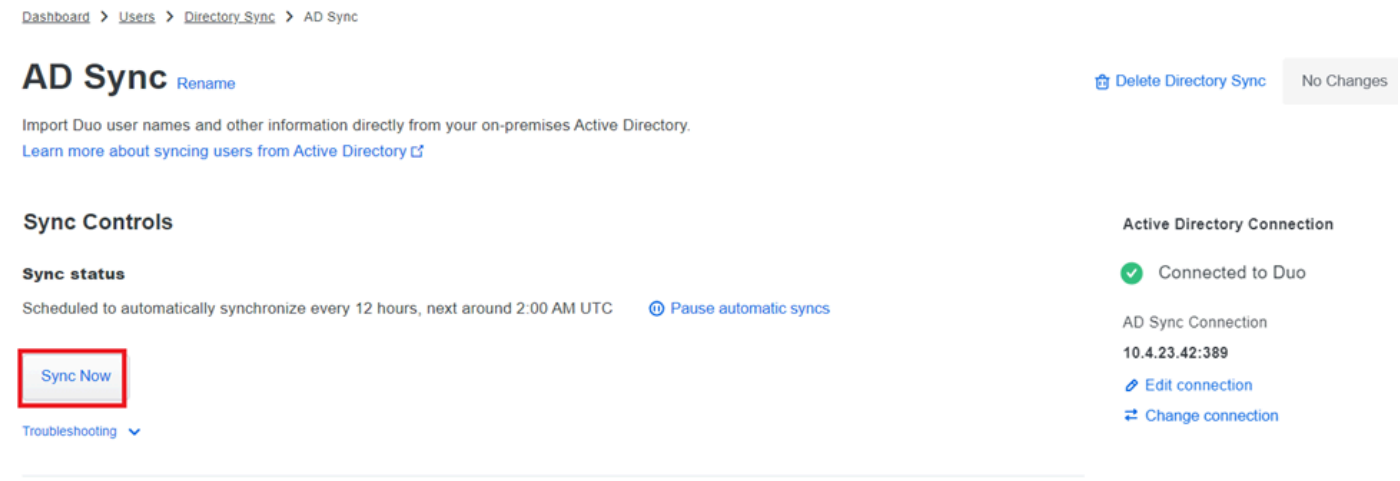
3. Within the configuration settings, identify and choose the specific groups within Active Directory that you wish to synchronize with the Duo Cloud. Consider using the filtering options for your selection.

4. Click **Complete Setup**.



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.



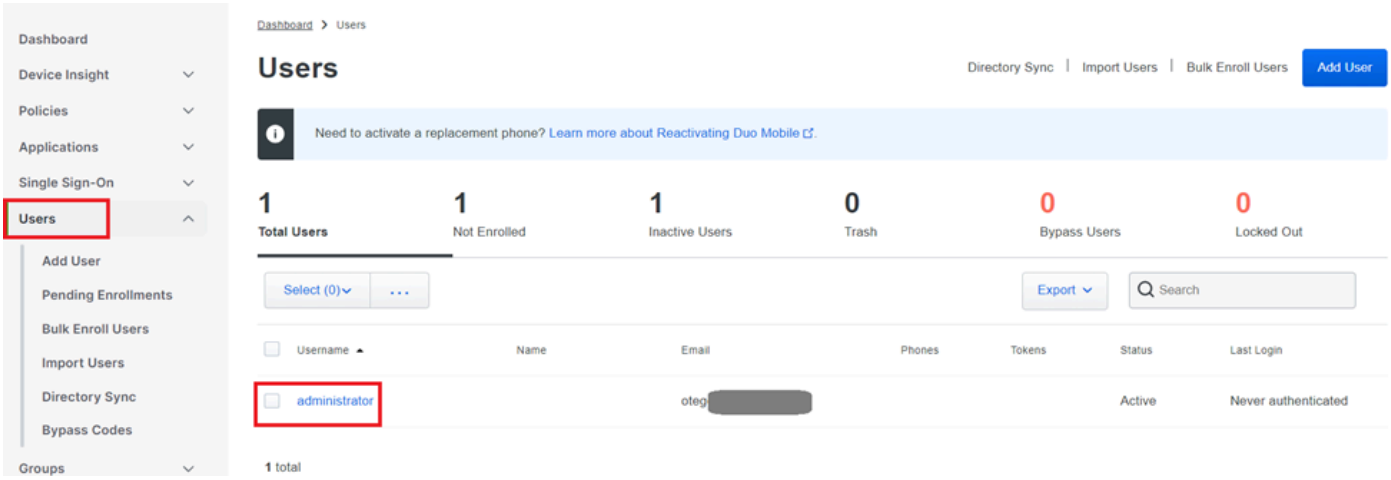
Starting Synchronization

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.

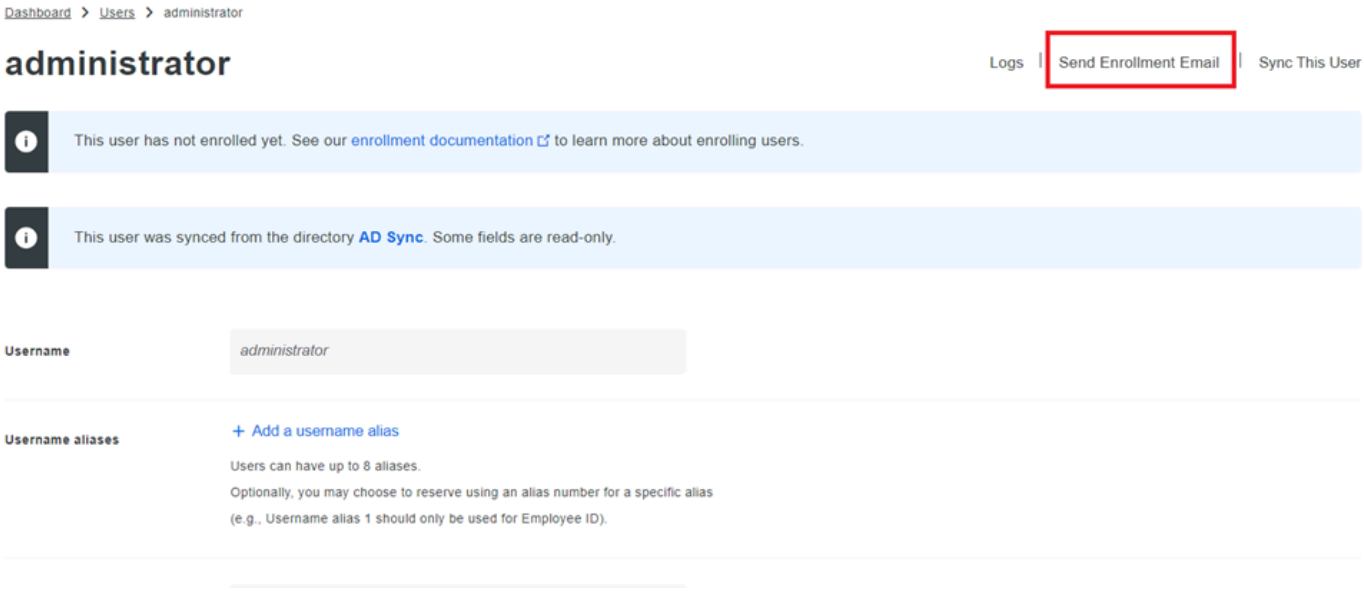
1. Navigate to the **Users** section in the **Cisco Cloud** dashboard.

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



User account list.

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



Enrollment via email.

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

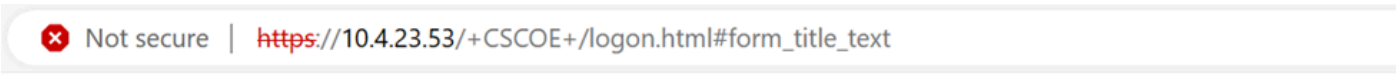
For additional details regarding the enrollment process, please refer to these resources:

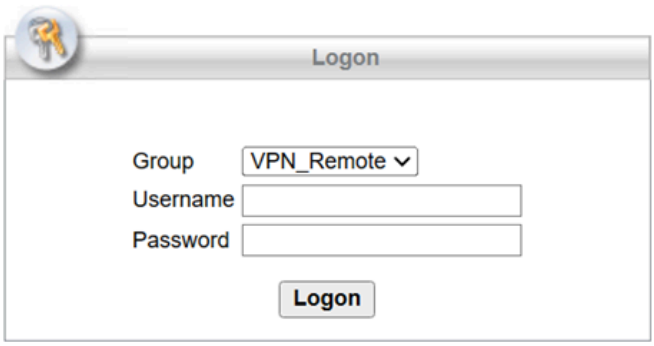
- Universal Enrollment Guide: https://guide.duo.com/universal-enrollment
- Traditional Enrollment Guide: https://guide.duo.com/traditional-enrollment

Configuration Validation Procedure.

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

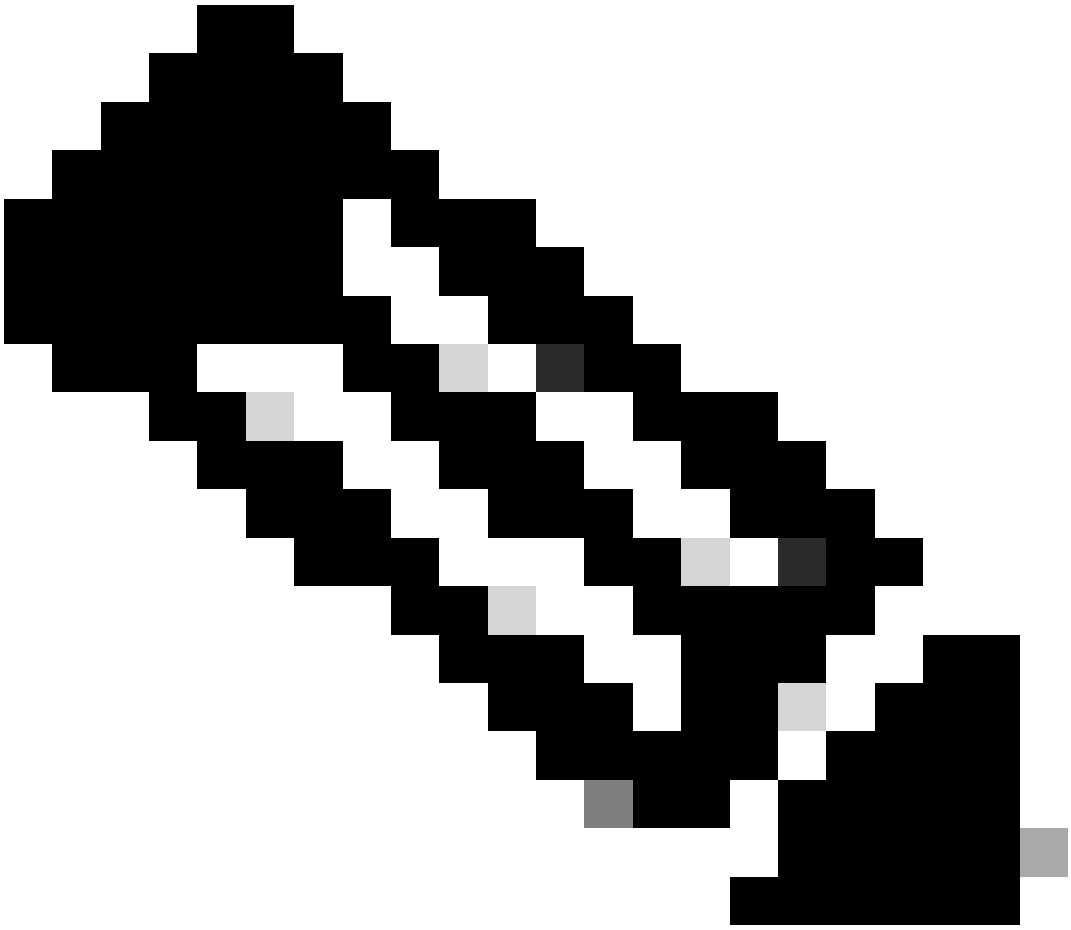
1. Launch a web browser and enter the IP address of the Firepower Threat Defense (FTD) device to access the VPN interface.





VPN Logon.

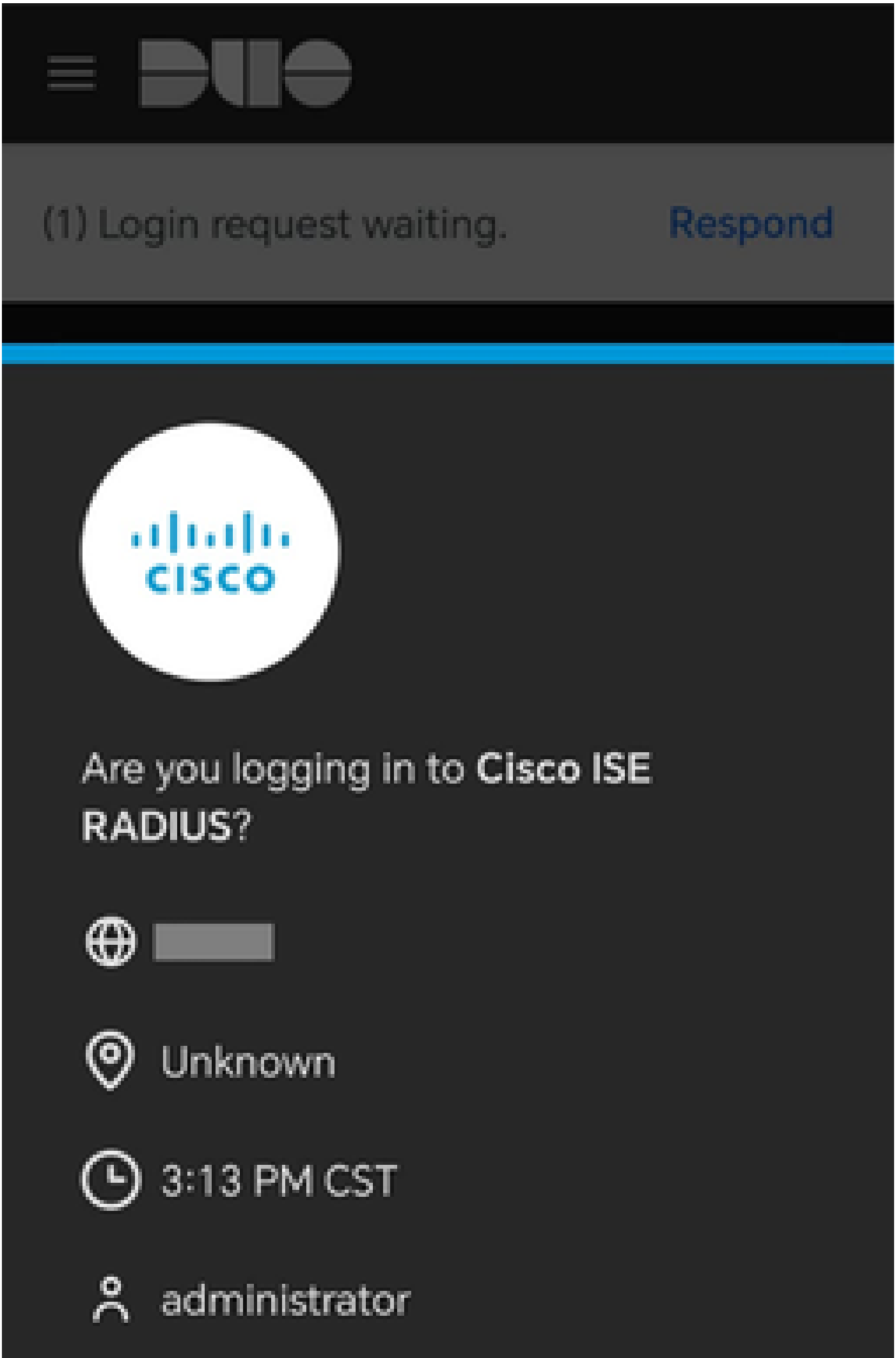
2. Input your username and password when prompted.



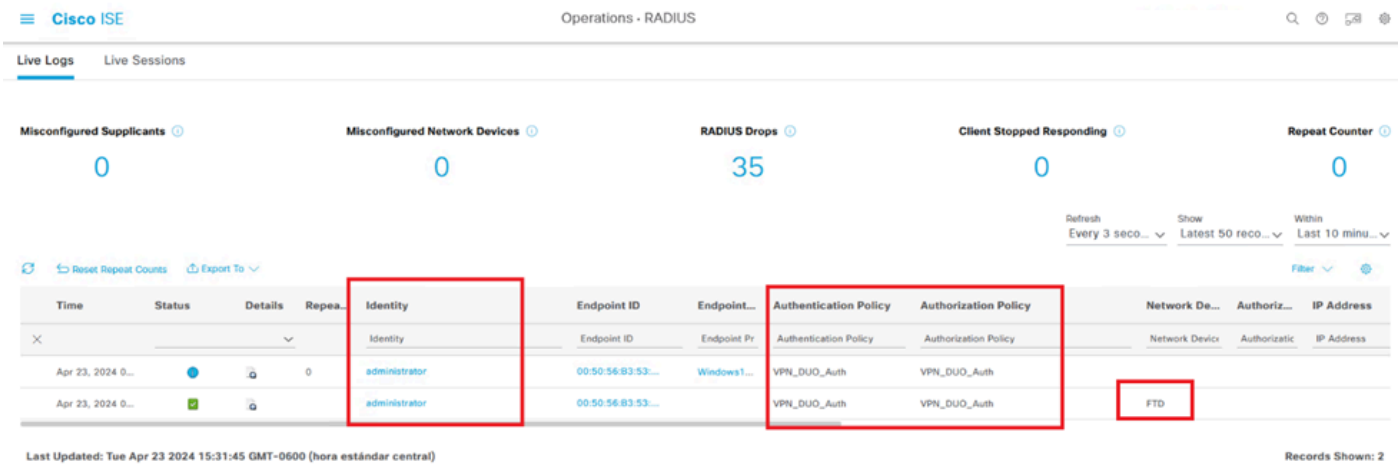
Note: The credentials are part of the Active Directory accounts.

---

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

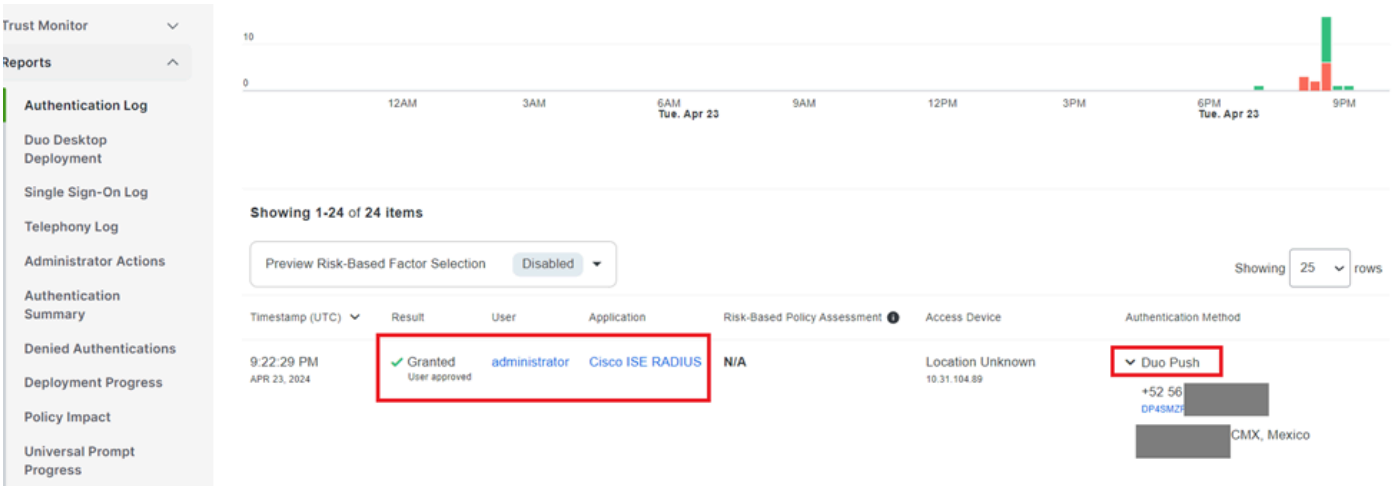

(1) Login request waiting.
Respond
Are you logging in to Cisco ISE RADIUS?
Unknown
3:13 PM CST
administrator

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



ISE Livelogs.

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



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

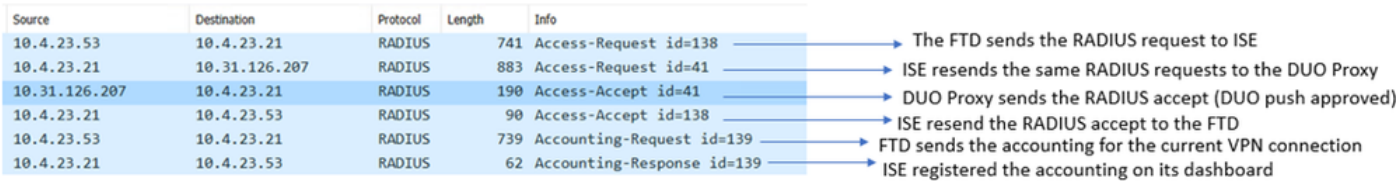
mdm-tlv=device-platform=win,
mdm-tlv=device-mac=00-50-56-b3-53-d6,
mdm-tlv=device-type=VMware, Inc. VMware7,1,
mdm-tlv=device-platform-version=10.0.19045 ,
mdm-tlv=device-public-mac=00-50-56-b3-53-d6,
mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.08029,
mdm-tlv=device-uid-
global=4CEBE2C21A8B81F490AC91086452CF3592593437,
mdm-tlv=device-
uid=3C5C68FF5FD3B6FA9D364DDB90E2B0BFA7E44B0EAAA
CA383D5A8CE0964A799DD,
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...

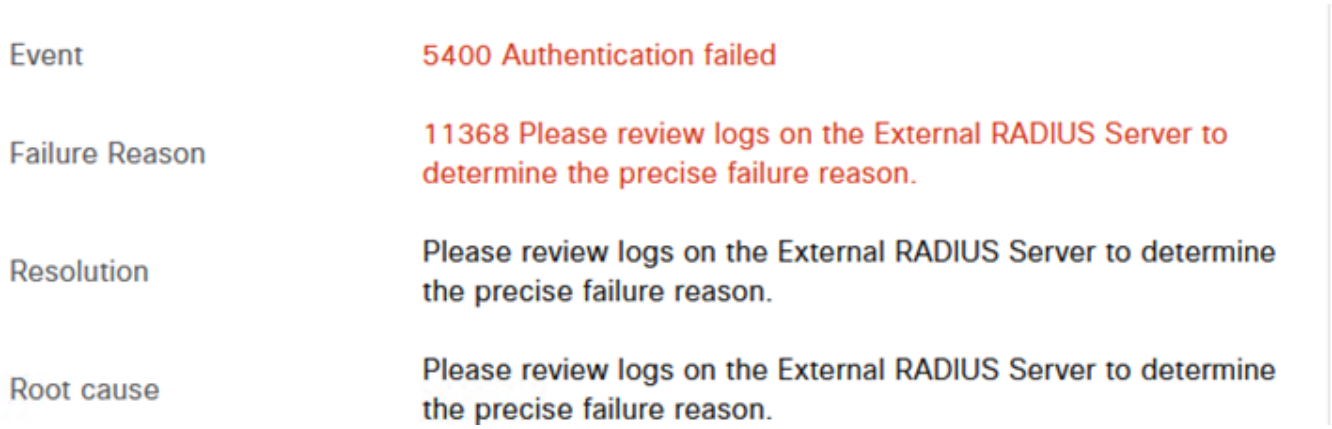
Result Successfully.

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



ISE packet capture.

Error11368 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=xxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxx
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=xxxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxx
service_account_username=<your domain\username>
service_account_password=xxxxxxxxxxxxx
```