

Konfiguration der SSL VPN-Authentifizierung über FTD, ISE, DUO und Active Directory

Inhalt

[Einleitung](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[FTD-Konfigurationen](#)

[Integration eines RADIUS-Servers in das FirePOWER Management Center \(FMC\)](#)

[Konfigurieren Sie das Remote-VPN.](#)

[ISE-Konfigurationen](#)

[Integrieren Sie DUO als externen Radius-Server.](#)

[FTD als Netzwerkzugriffsg r t integrieren.](#)

[DUO-Konfigurationen](#)

[DUO-Proxy-Installation.](#)

[Integration von DUO Proxy mit ISE und DUO Cloud.](#)

[Integration von DUO mit Active Directory](#)

[Exportieren von Benutzerkonten aus Active Directory \(AD\)  ber die DUO Cloud](#)

[Registrieren Sie Benutzer in der Cisco DUO Cloud.](#)

[Verfahren zur Konfigurationsvalidierung.](#)

[H ufige Probleme.](#)

[Arbeitsszenario.](#)

[Fehler11353 Keine externen RADIUS-Server mehr; Failover kann nicht ausgef hrt werden](#)

[Die RADIUS-Sitzungen werden nicht in den ISE-Live-Protokollen angezeigt.](#)

[Zus tzliche Fehlerbehebung.](#)

Einleitung

Dieses Dokument beschreibt die Integration von SSL VPN in Firepower Threat Defense mit Cisco ISE und DUO Security f r AAA.

Anforderungen

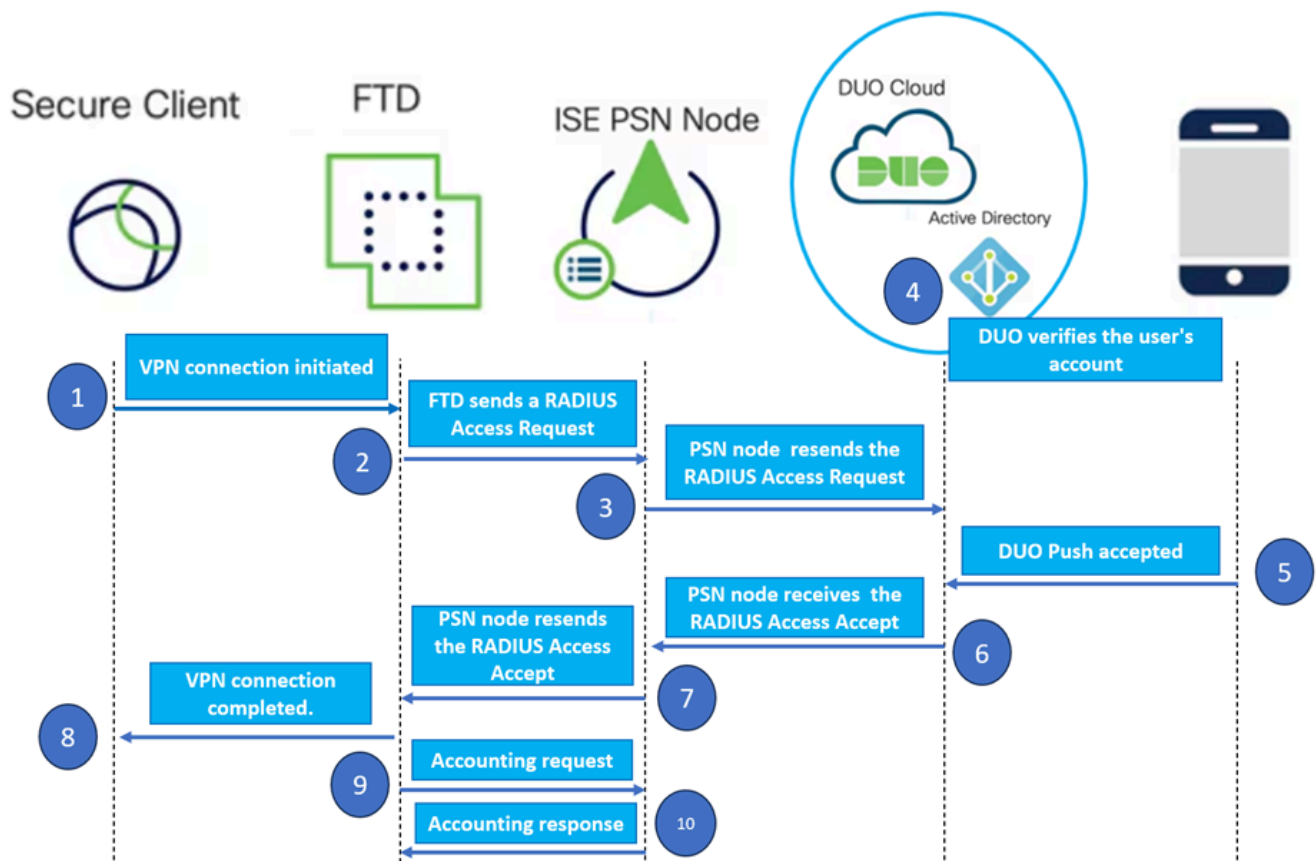
- ISE 3.0 oder h her
- FMC 7.0 oder h her
- FTD 7.0 oder h her
- DUO-Authentifizierungsproxy.
- ISE Essentials-Lizenzierung
- DUO Essentials-Lizenzierung

Verwendete Komponenten

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm



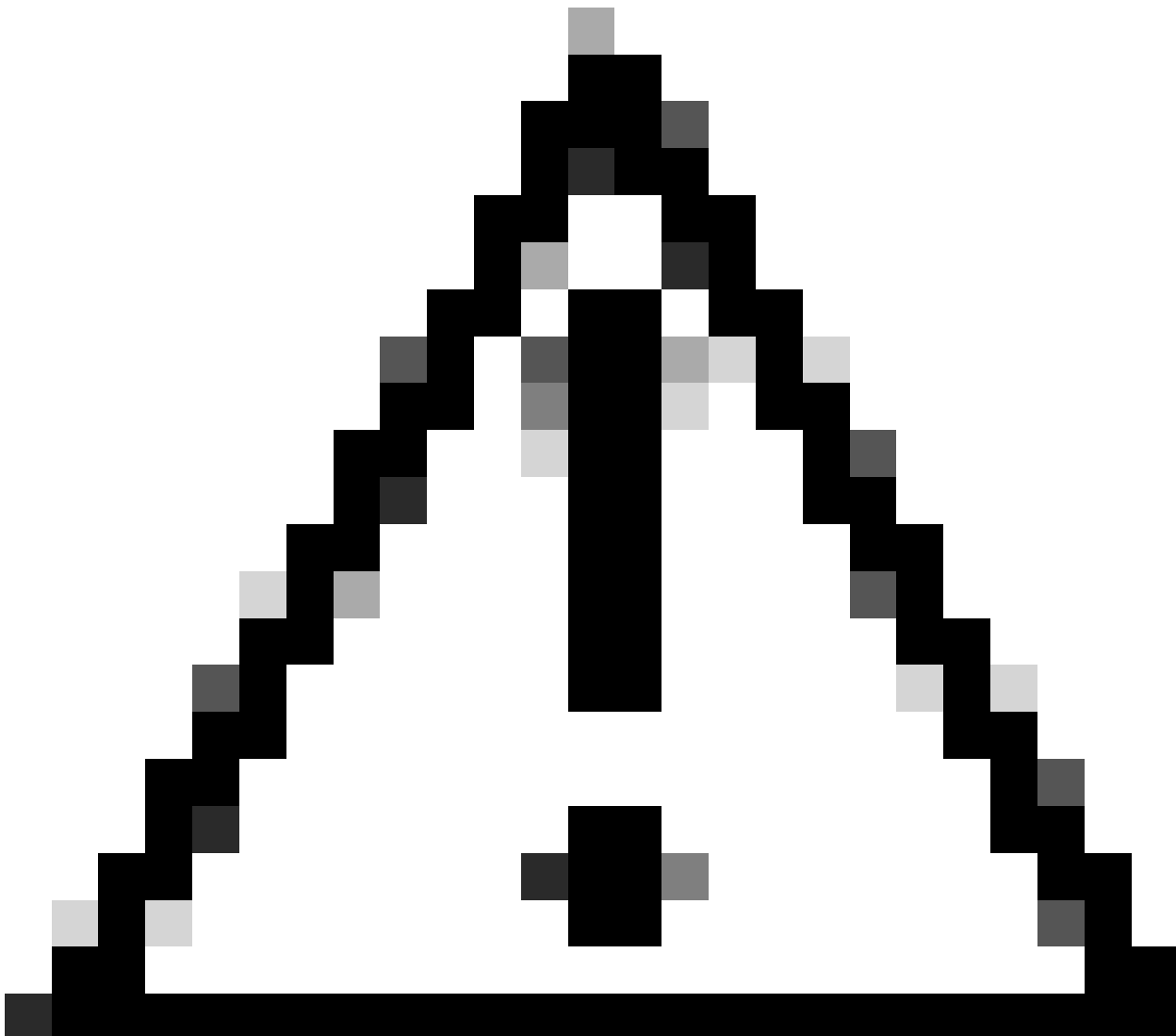
Topologie.

In unserer vorgeschlagenen Lösung ist die Cisco ISE ein wichtiger RADIUS-Server-Proxy. Anstatt Authentifizierungs- oder Autorisierungsrichtlinien direkt auszuwerten, ist die ISE so konfiguriert, dass die RADIUS-Pakete vom FTD an den DUO Authentication Proxy weitergeleitet werden.

Der DUO Authentication Proxy fungiert als dedizierter Vermittler innerhalb dieses Authentifizierungsflusses. Sie wird auf einem Windows-Server installiert und schließt die Lücke zwischen der Cisco ISE und der DUO-Cloud. Die primäre Proxy-Funktion besteht darin, Authentifizierungsanforderungen - eingekapselt in RADIUS-Pakete - an die DUO Cloud zu

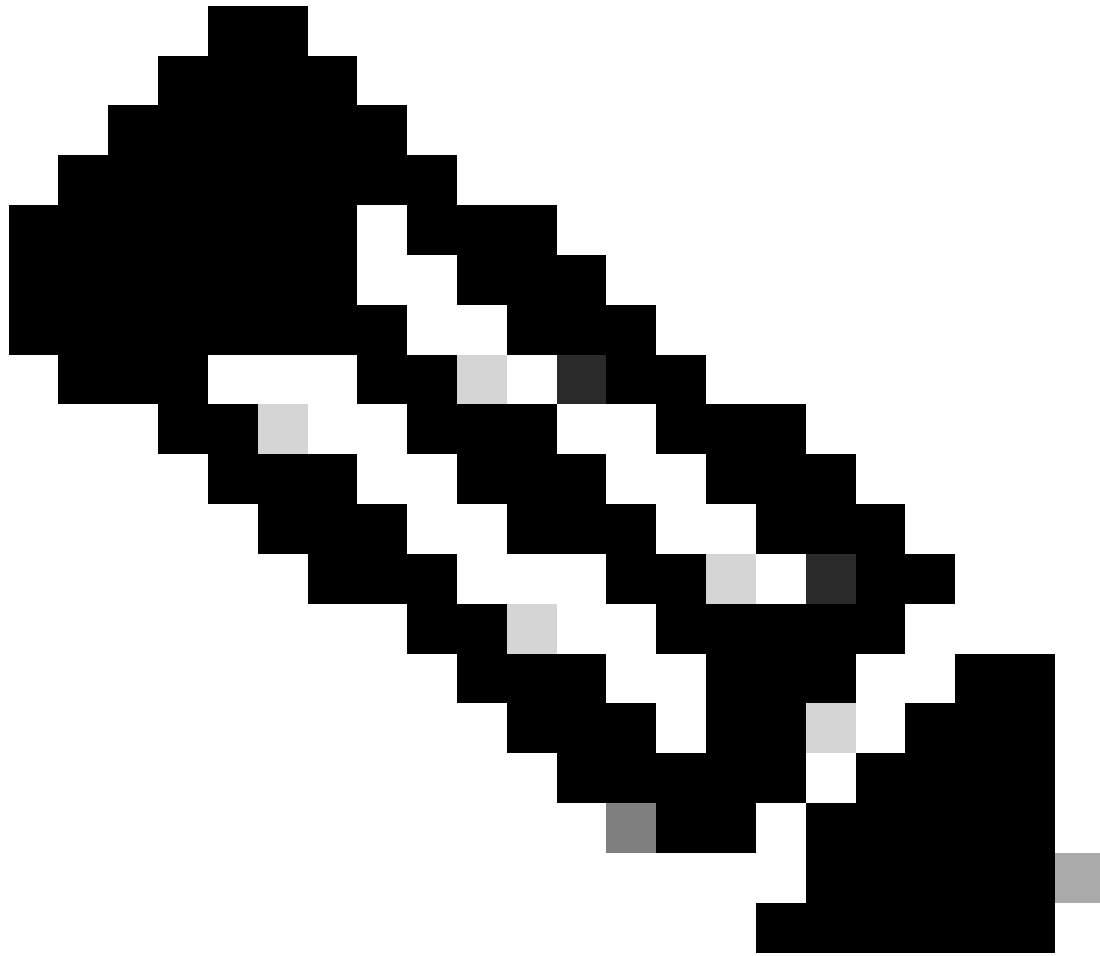
übertragen. Die DUO Cloud ermöglicht oder verweigert den Netzwerkzugriff basierend auf den Zwei-Faktor-Authentifizierungskonfigurationen.

1. Der Benutzer initiiert den VPN-Authentifizierungsprozess durch Eingabe seines eindeutigen Benutzernamens und Kennworts.
2. Die Firewall Threat Defense (FTD) sendet die Authentifizierungsanforderung an die Cisco Identity Services Engine (ISE).
3. Der Policy Services Node (PSN) leitet die Authentifizierungsanforderung an den DUO-Authentifizierungsproxyserver weiter. Anschließend werden die Anmeldeinformationen vom DUO Authentication Server über den DUO Cloud-Service validiert.
4. Die DUO Cloud vergleicht Benutzername und Passwort mit der synchronisierten Datenbank.



Achtung: Die Synchronisierung zwischen der DUO Cloud und den Organisationen, in denen Active Directory aktiv ist, muss aktiviert sein, damit eine aktuelle Benutzerdatenbank in der DUO Cloud verfügbar ist.

5. Nach erfolgreicher Authentifizierung initiiert die DUO Cloud einen DUO-Push an das registrierte Mobilgerät des Benutzers über eine sichere, verschlüsselte Push-Benachrichtigung. Der Benutzer muss dann den DUO-Push genehmigen, um seine Identität bestätigen und fortfahren zu können.
6. Sobald der Benutzer den DUO-Push genehmigt, sendet der DUO-Authentifizierungsproxy-Server eine Bestätigung zurück an das PSN, um anzugeben, dass die Authentifizierungsanforderung vom Benutzer akzeptiert wurde.
7. Der PSN-Knoten sendet die Bestätigung an das FTD, um mitzuteilen, dass der Benutzer authentifiziert wurde.
8. Der FTD erhält die Authentifizierungsbestätigung und stellt die VPN-Verbindung zum Endpunkt mit den entsprechenden Sicherheitsmaßnahmen her.
9. Der FTD protokolliert die Details der erfolgreichen VPN-Verbindung und überträgt die Abrechnungsdaten sicher an den ISE-Knoten zu Aufzeichnungs- und Prüfzwecken zurück.
10. Der ISE-Knoten protokolliert die Buchhaltungsinformationen in seinen Lebensläufen und stellt sicher, dass alle Datensätze sicher gespeichert werden und für zukünftige Prüfungen oder Compliance-Prüfungen zugänglich sind.



Anmerkung:

Bei der Einrichtung in diesem Leitfaden werden die folgenden Netzwerkparameter verwendet:

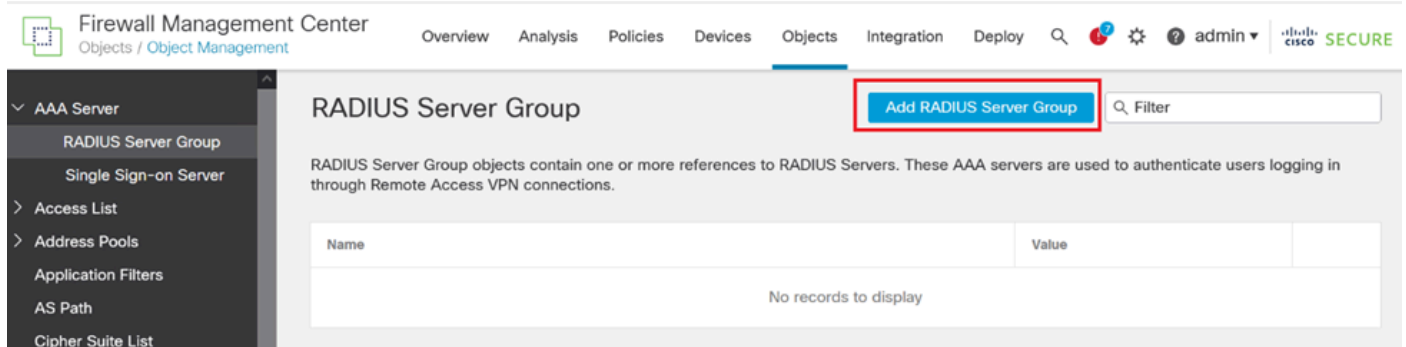
- Primäre Netzwerkserver (PNS)-Knoten-IP: 10.4.23.21
- Firepower Threat Defense (FTD) IP für Peer-VPN: 10.4.23.53
- DUO-Authentifizierungsproxy IP: 10.31.126.207
- Domänenname: testlab.local

Konfigurationen

FTD-Konfigurationen

Integration eines RADIUS-Servers in das FirePOWER Management Center (FMC)

1. Rufen Sie das FMC auf, indem Sie Ihren Webbrowser starten und die IP-Adresse des FMC eingeben, um die grafische Benutzeroberfläche (GUI) zu öffnen.
2. Navigieren Sie zum Menü Objekte, wählen Sie AAA-Server aus, und fahren Sie mit der Option RADIUS Server Group fort.
3. Klicken Sie auf die Schaltfläche RADIUS-Servergruppe hinzufügen, um eine neue Gruppe für RADIUS-Server zu erstellen.



RADIUS-Servergruppe.

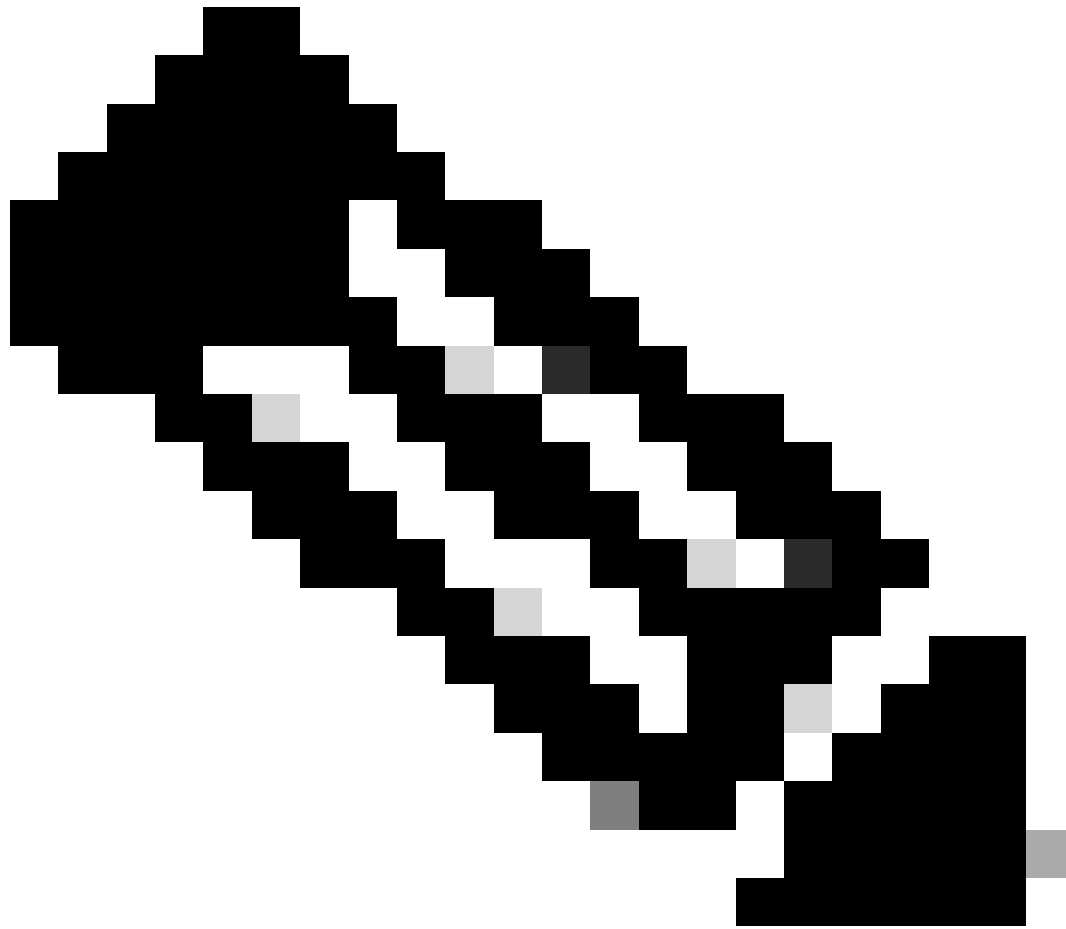
4. Geben Sie einen beschreibenden Namen für die neue AAA RADIUS-Servergruppe ein, um eine klare Identifizierung innerhalb Ihrer Netzwerkinfrastruktur sicherzustellen.
5. Fahren Sie mit dem Hinzufügen eines neuen RADIUS-Servers fort, indem Sie die entsprechende Option in der Gruppenkonfiguration auswählen.

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname	
No records to display	

RADIUS-Server.

6. Geben Sie die IP-Adresse des RADIUS-Servers ein, und geben Sie den gemeinsamen geheimen Schlüssel ein.



Hinweis: Um eine erfolgreiche RADIUS-Verbindung herzustellen, muss sichergestellt werden, dass dieser geheime Schlüssel sicher mit dem ISE-Server gemeinsam genutzt wird.

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

Neuer RADIUS-Server.

7. Klicken Sie nach der Konfiguration der RADIUS-Serverdetails auf Speichern, um die Einstellungen für die RADIUS-Servergruppe beizubehalten.

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

Servergruppendetails.

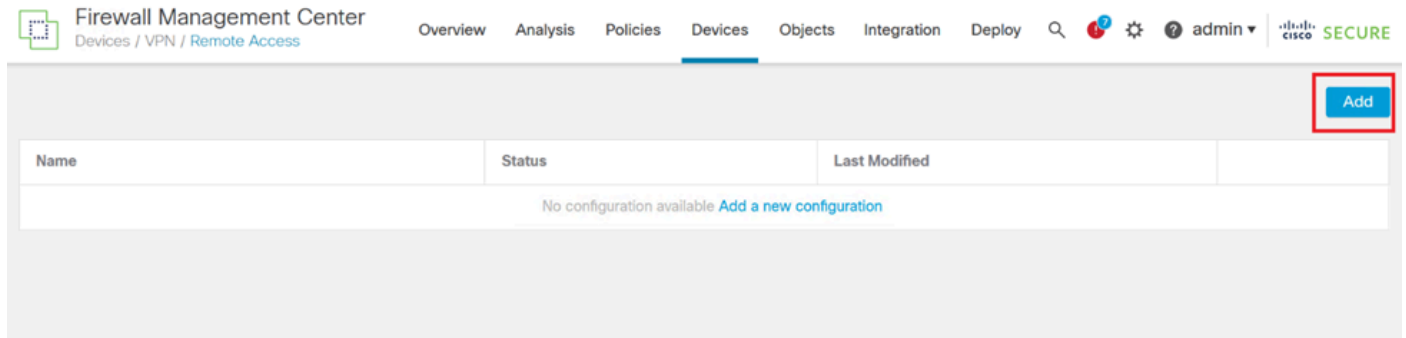
8. Um die Konfiguration des AAA-Servers im gesamten Netzwerk abzuschließen und zu implementieren, navigieren Sie zum Menü Bereitstellen, und wählen Sie dann Alle bereitstellen aus, um die Einstellungen zu übernehmen.

The screenshot shows the 'Firewall Management Center' interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Deploy'. The 'Deploy' menu is highlighted with a red box. Below the navigation bar, the left sidebar shows a tree view with 'AAA Server' expanded, and 'RADIUS Server Group' selected. The main content area displays the 'RADIUS Server Group' configuration page, which includes a search bar, a table with one entry 'FTD_01' in 'Ready for Deployment' status, and two buttons: 'Advanced Deploy' and 'Deploy All'. The 'Deploy All' button is highlighted with a red box.

Bereitstellen des AAA-Servers.

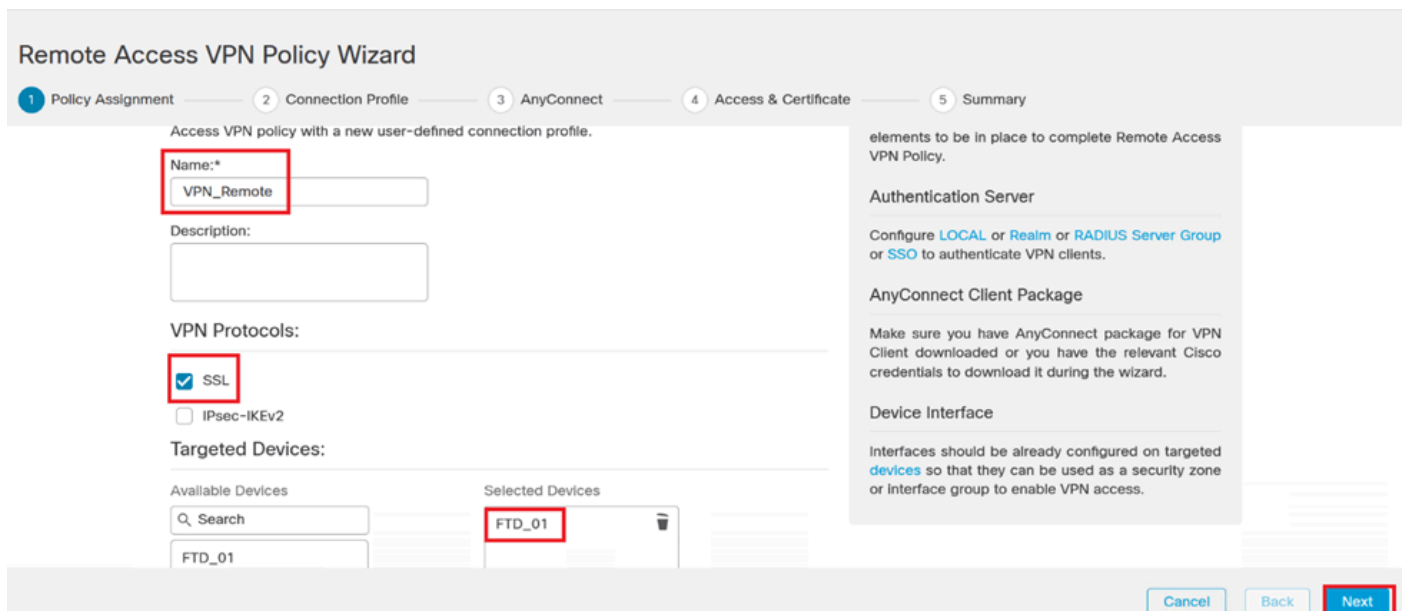
Konfigurieren Sie das Remote-VPN.

1. Navigieren Sie in der FMC-GUI zu Devices > VPN > Remote Access, um den VPN-Konfigurationsprozess zu starten.
2. Klicken Sie auf die Schaltfläche Hinzufügen, um ein neues VPN-Verbindungsprofil zu erstellen.



VPN-Verbindungsprofil.

3. Geben Sie einen eindeutigen beschreibenden Namen für das VPN ein, um es in Ihren Netzwerkeinstellungen einfacher zu identifizieren.
4. Wählen Sie die SSL-Option, um eine sichere Verbindung über das SSL VPN-Protokoll sicherzustellen.
5. Wählen Sie aus der Geräteliste das jeweilige FTD-Gerät aus.



VPN-Einstellungen.

6. Konfigurieren Sie die AAA-Methode, um den PSN-Knoten in den Authentifizierungseinstellungen zu verwenden.

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** ▼ +

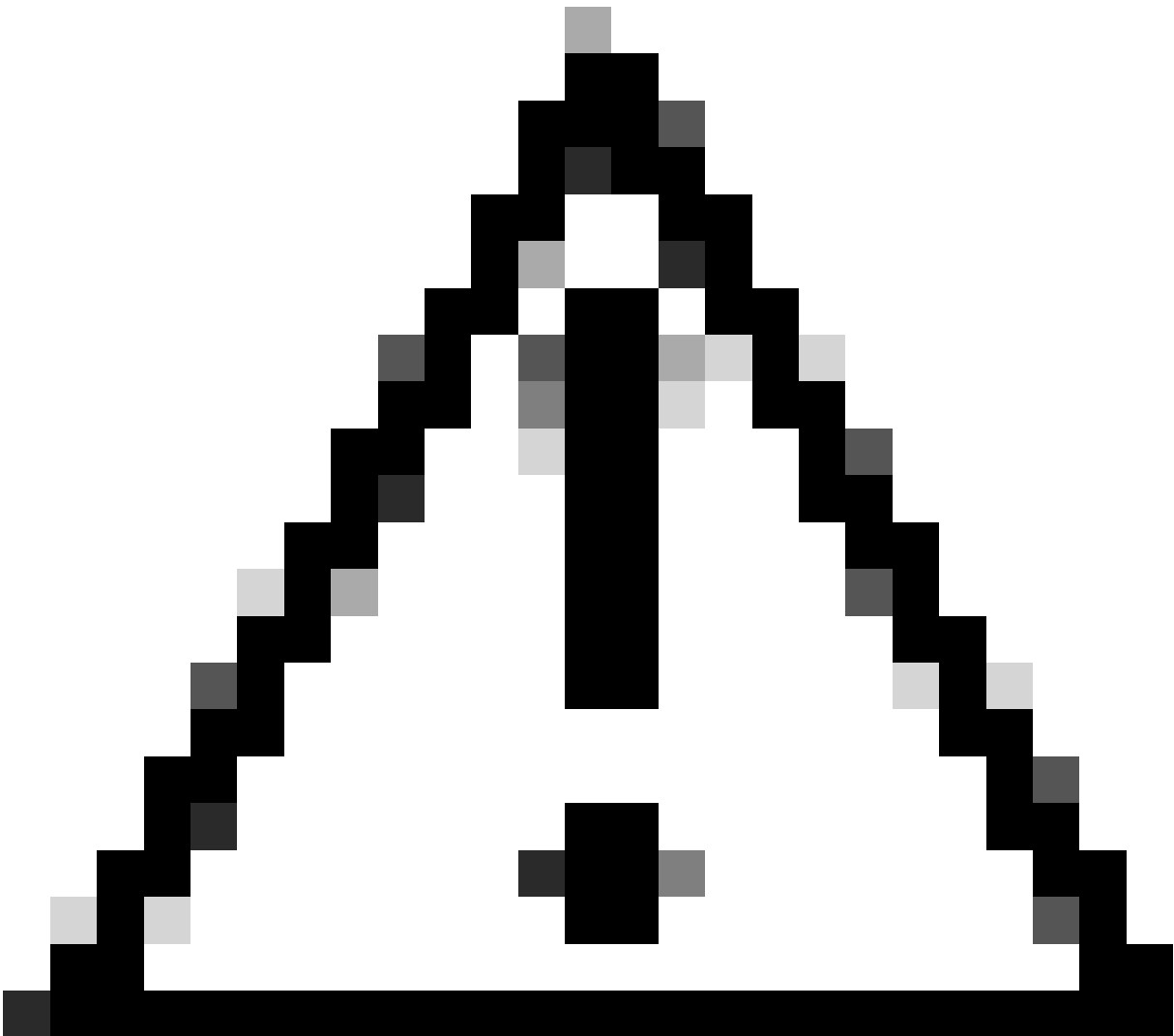
(realm or RADIUS)

Accounting Server: **ISE** ▼ +

(RADIUS)

Verbindungsprofil.

7. Richten Sie eine dynamische IP-Adresszuweisung für VPN ein.



Vorsicht: Zu diesem Beispiel wurde der DHCP-VPN-Pool ausgewählt.

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-Adresspool.

8. Fahren Sie mit dem Erstellen einer neuen Gruppenrichtlinie fort.

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](#)

Gruppenrichtlinie.

9. Stellen Sie in den Gruppenrichtlinieneinstellungen sicher, dass das SSL-Protokoll ausgewählt ist.

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-Protokolle.

10. Erstellen Sie entweder einen neuen VPN-Pool, oder wählen Sie einen vorhandenen Pool aus, um den Bereich der für VPN-Clients verfügbaren IP-Adressen zu definieren.

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

Cancel

Save

VPN-Pool.

11. Geben Sie die DNS-Serverdetails für die VPN-Verbindung an.

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-Einstellungen.



Warnung: Beachten Sie, dass zusätzliche Funktionen wie Banner, Split Tunneling, AnyConnect und Advanced für diese Konfiguration als optional gelten.

12. Nachdem Sie die erforderlichen Details konfiguriert haben, klicken Sie auf Weiter, um mit der nächsten Phase der Einrichtung fortzufahren.

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

Gruppenrichtlinie.

13. Wählen Sie das entsprechende AnyConnect-Paket für die VPN-Benutzer aus. Wenn das erforderliche Paket nicht aufgeführt ist, können Sie das erforderliche Paket zu diesem Zeitpunkt hinzufügen.

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

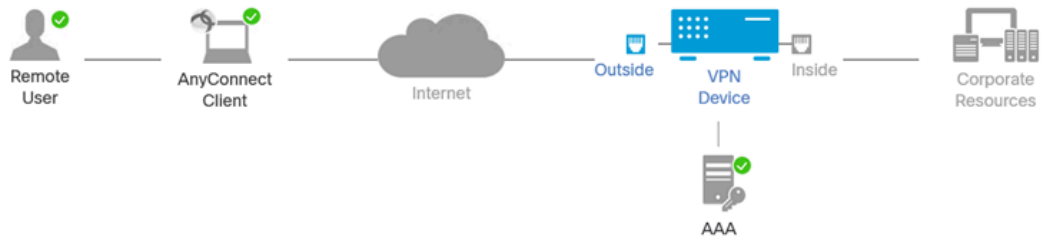
Next

Paketinstallation.

14. Wählen Sie die Netzwerkschnittstelle auf dem FTD-Gerät, in der Sie die VPN-Remote-Funktion aktivieren möchten.

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.

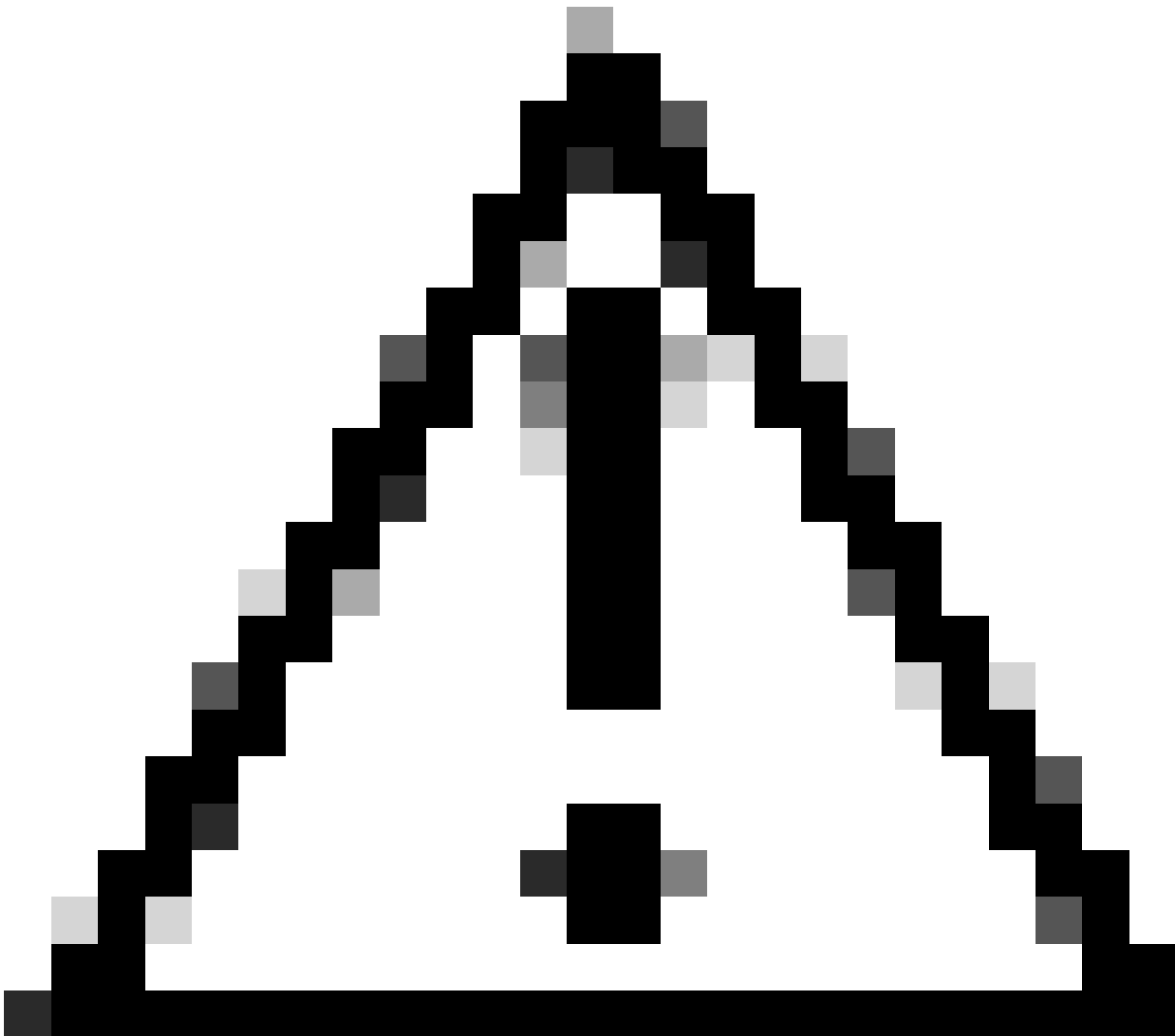
Interface group/Security Zone:* +

Enable DTLS on member interfaces

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

VPN-Schnittstelle

15. Richten Sie einen Zertifikatregistrierungsprozess ein, indem Sie eine der verfügbaren Methoden zum Erstellen und Installieren des Zertifikats auf der Firewall auswählen, was für sichere VPN-Verbindungen entscheidend ist.



Vorsicht: In diesem Leitfaden wurde z. B. ein selbstsigniertes Zertifikat ausgewählt.

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:*

Gerätezertifikat.

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

Zertifikatregistrierung.

16. Klicken Sie nach der Konfiguration der Zertifikatregistrierung auf Weiter.

Remote Access VPN Policy Wizard

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

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.

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.

Übersicht Zugriff und Services

17. Überprüfen Sie die Zusammenfassung aller Konfigurationen, um sicherzustellen, dass sie korrekt sind und der beabsichtigten Konfiguration entsprechen.

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.

- 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

Zusammenfassung der VPN-Einstellungen

18. Um die VPN-Remotezugriffskonfiguration anzuwenden und zu aktivieren, navigieren Sie zu Deploy > Deploy All (Bereitstellen > Alle bereitstellen) und führen Sie die Bereitstellung für das ausgewählte FTD-Gerät aus.

Bereitstellen der VPN-Einstellungen

ISE-Konfigurationen

Integrieren Sie DUO als externen Radius-Server.

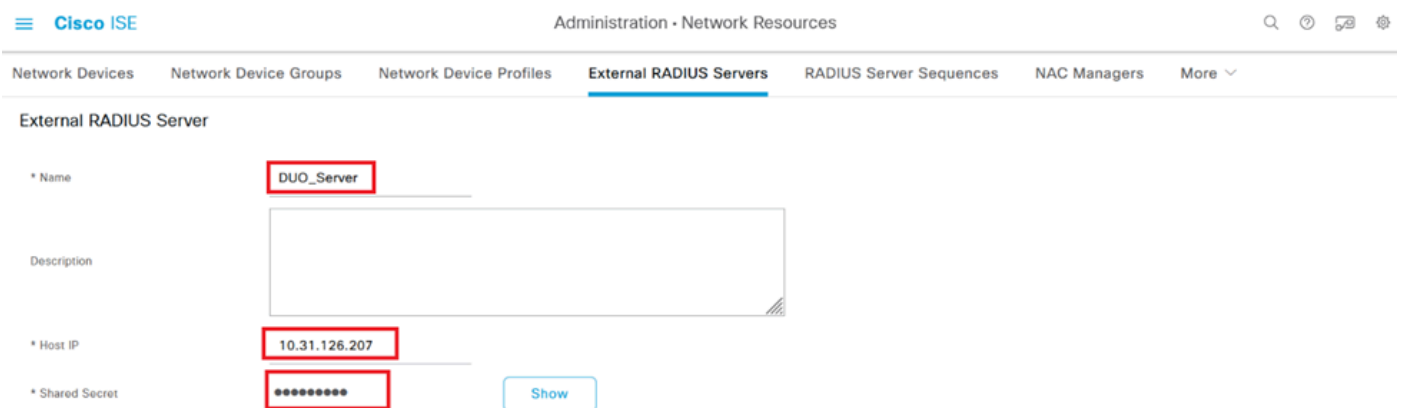
1. Navigieren Sie in der Cisco ISE-Administrationsoberfläche zu Administration > Network Resources > External RADIUS Servers.
2. Klicken Sie auf die Schaltfläche Hinzufügen, um einen neuen externen RADIUS-Server zu konfigurieren.

Externe Radius-Server

3. Geben Sie einen Namen für den Proxy DUO-Server ein.
4. Geben Sie die richtige IP-Adresse für den Proxy-DUO-Server ein, um eine ordnungsgemäße Kommunikation zwischen der ISE und dem DUO-Server sicherzustellen.
5. Legen Sie den gemeinsamen geheimen Schlüssel fest.

Hinweis: Dieser gemeinsame geheime Schlüssel muss für den Proxy DUO-Server konfiguriert werden, damit eine RADIUS-Verbindung erfolgreich hergestellt werden kann.

6. Wenn Sie alle Details korrekt eingegeben haben, klicken Sie auf **Senden**, um die neue Proxy DUO Server-Konfiguration zu speichern.



The screenshot shows the Cisco ISE Administration interface for configuring an External RADIUS Server. The breadcrumb trail is "Administration > Network Resources > External RADIUS Servers". The "External RADIUS Server" configuration form has the following fields:

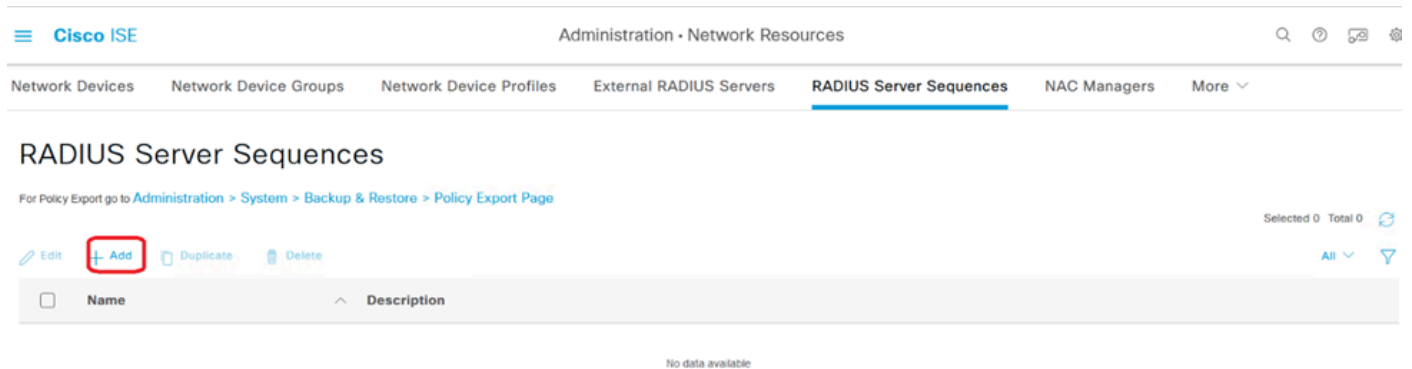
- * Name: DUO_Server
- Description: (Empty text area)
- * Host IP: 10.31.126.207
- * Shared Secret: (Masked with asterisks)

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

Externe RADIUS-Server

7. Fahren Sie mit Administration > RADIUS Server Sequences fort.

8. Klicken Sie auf Hinzufügen, um eine neue RADIUS-Serversequenz zu erstellen.

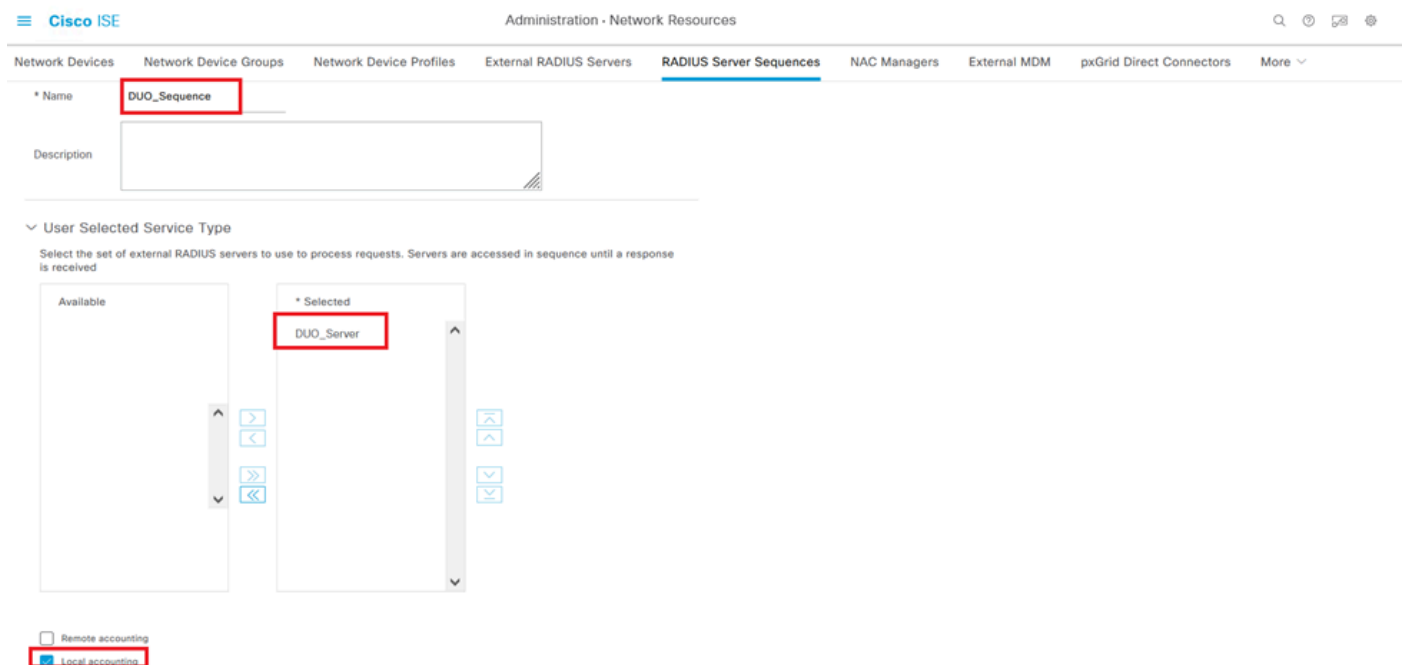


RADIUS-Serversequenzen

9. Geben Sie einen eindeutigen Namen für die RADIUS-Serversequenz an, um eine einfache Identifizierung zu ermöglichen.

10. Suchen Sie den zuvor konfigurierten DUO RADIUS-Server, der in diesem Handbuch als DUO_Server bezeichnet wird, und verschieben Sie ihn in die ausgewählte Liste auf der rechten Seite, um ihn in die Sequenz aufzunehmen.

11. Klicken Sie auf Senden, um die RADIUS-Serversequenzkonfiguration abzuschließen und zu speichern.

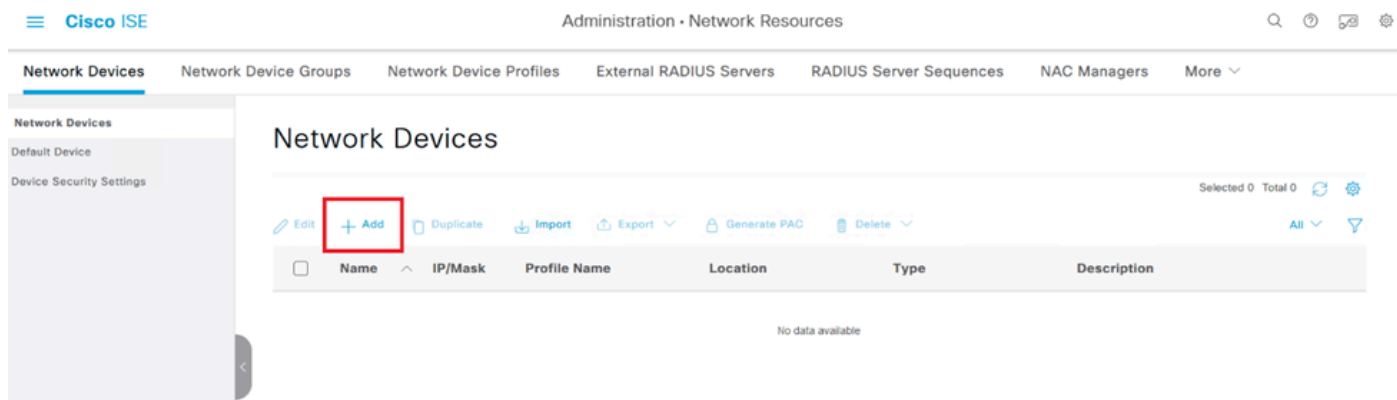


Radius-Serversequenzkonfiguration.

FTD als Netzwerkzugriffsgesetz integrieren.

1. Navigieren Sie zum Abschnitt Administration in Ihrer Systemschnittstelle, und wählen Sie von dort Network Resources (Netzwerkressourcen) aus, um auf den Konfigurationsbereich für Netzwerkgeräte zuzugreifen.

2. Sobald Sie sich im Abschnitt "Netzwerkressourcen" befinden, suchen Sie nach der Schaltfläche Hinzufügen, und klicken Sie auf diese Schaltfläche, um das Hinzufügen eines neuen Netzwerkzugriffsgeräts zu initiieren.



Netzwerkzugriffsgeräte.

3. Geben Sie in die angezeigten Felder den Namen des Netzwerkzugriffsgeräts ein, um das Gerät in Ihrem Netzwerk zu identifizieren.

4. Fahren Sie mit der Angabe der IP-Adresse des FTD-Geräts (Firepower Threat Defense) fort.

5. Geben Sie den Schlüssel ein, der zuvor während der Einrichtung des FMC (FirePOWER MANAGEMENT CENTER) eingerichtet wurde. Dieser Schlüssel ist für die sichere Kommunikation zwischen Geräten unerlässlich.

6. Schließen Sie den Prozess durch Klicken auf die Schaltfläche Senden ab.

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

Network Devices

Name

FTD

Description

IP Address

* IP :

10.4.23.53

/

32



FTD wird als NAD hinzugefügt.



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-Einstellungen

DUO-Konfigurationen

DUO-Proxy-Installation.

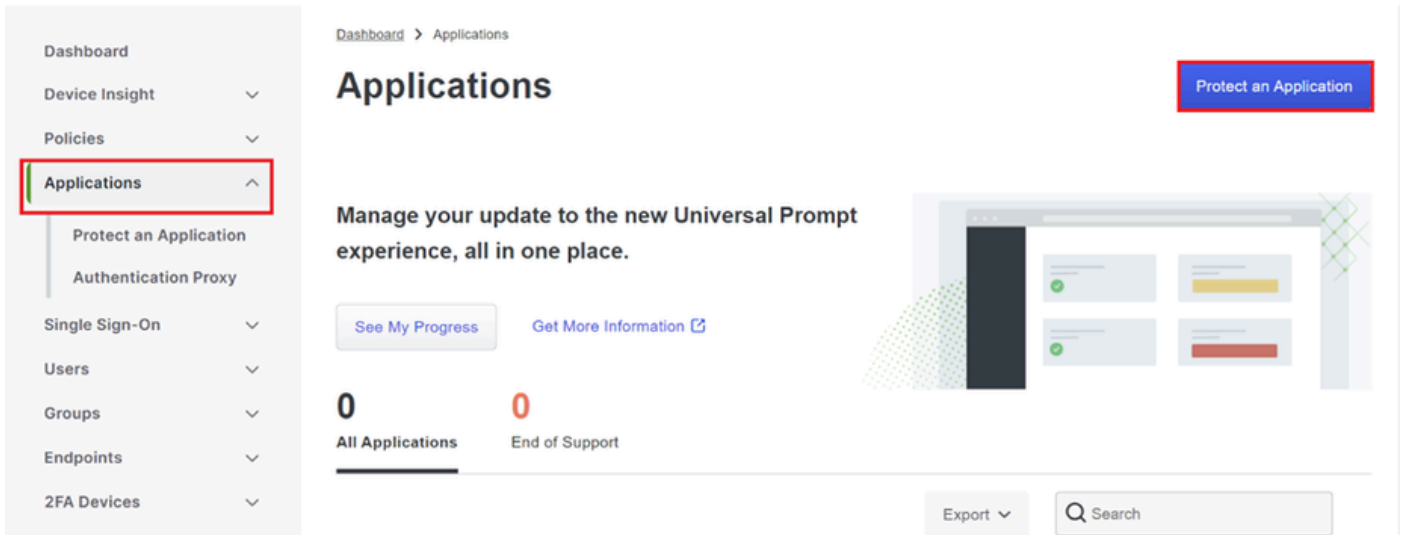
Rufen Sie den DUO Proxy Download- und Installationshandbuch auf, indem Sie auf den nächsten Link klicken:

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

Integration von DUO Proxy mit ISE und DUO Cloud.

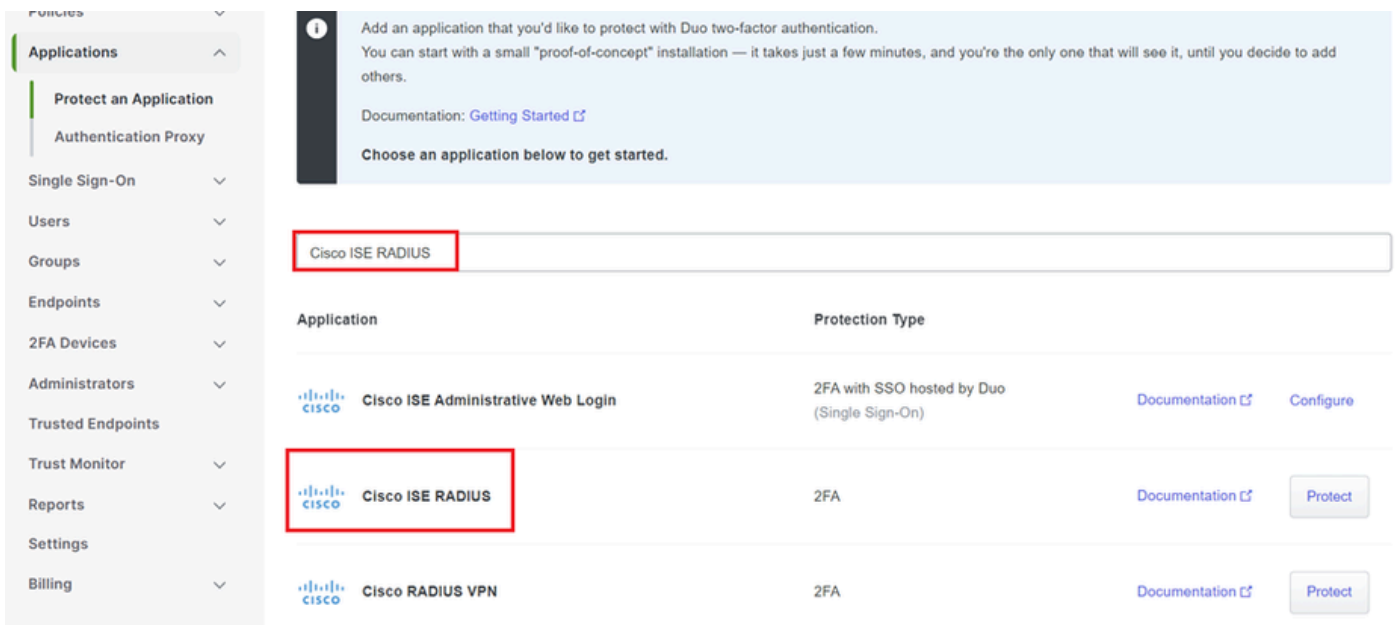
1. Melden Sie sich mit Ihren Anmeldeinformationen auf der DUO Security-Website unter <https://duo.com/> an.

2. Navigieren Sie zum Abschnitt "Anwendungen", und wählen Sie "Anwendung schützen" aus, um fortzufahren.



DUO-Anwendungen

3. Suchen Sie in der Liste nach der Option "Cisco ISE RADIUS", und klicken Sie auf Schützen, um sie Ihren Anwendungen hinzuzufügen.



ISE RADIUS-Option

4. Nach dem erfolgreichen Hinzufügen, werden Sie die Details der DUO-Anwendung zu sehen. Blättern Sie nach unten, und klicken Sie auf Speichern.

5. Kopieren Sie den bereitgestellten Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen. Diese sind für die nächsten Schritte von entscheidender Bedeutung.

✓ Application modified successfully.

Dashboard > Applications > Cisco ISE RADIUS

Cisco ISE RADIUS

Authentication Log | Remove Application

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

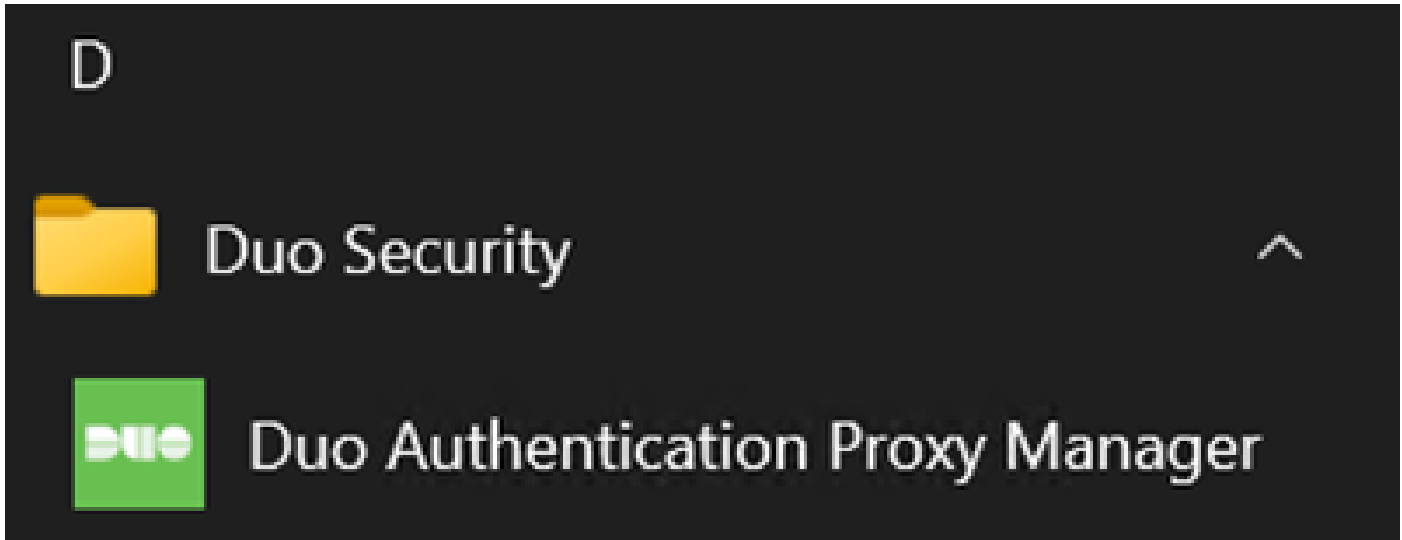
Details

Reset Secret Key

Integration key	DIX [REDACTED]	Copy
Secret keyywLM	Copy
Don't write down your secret key or share it with anyone.		
API hostname	[REDACTED] duosecurity.com	Copy

ISE-Serverdetails

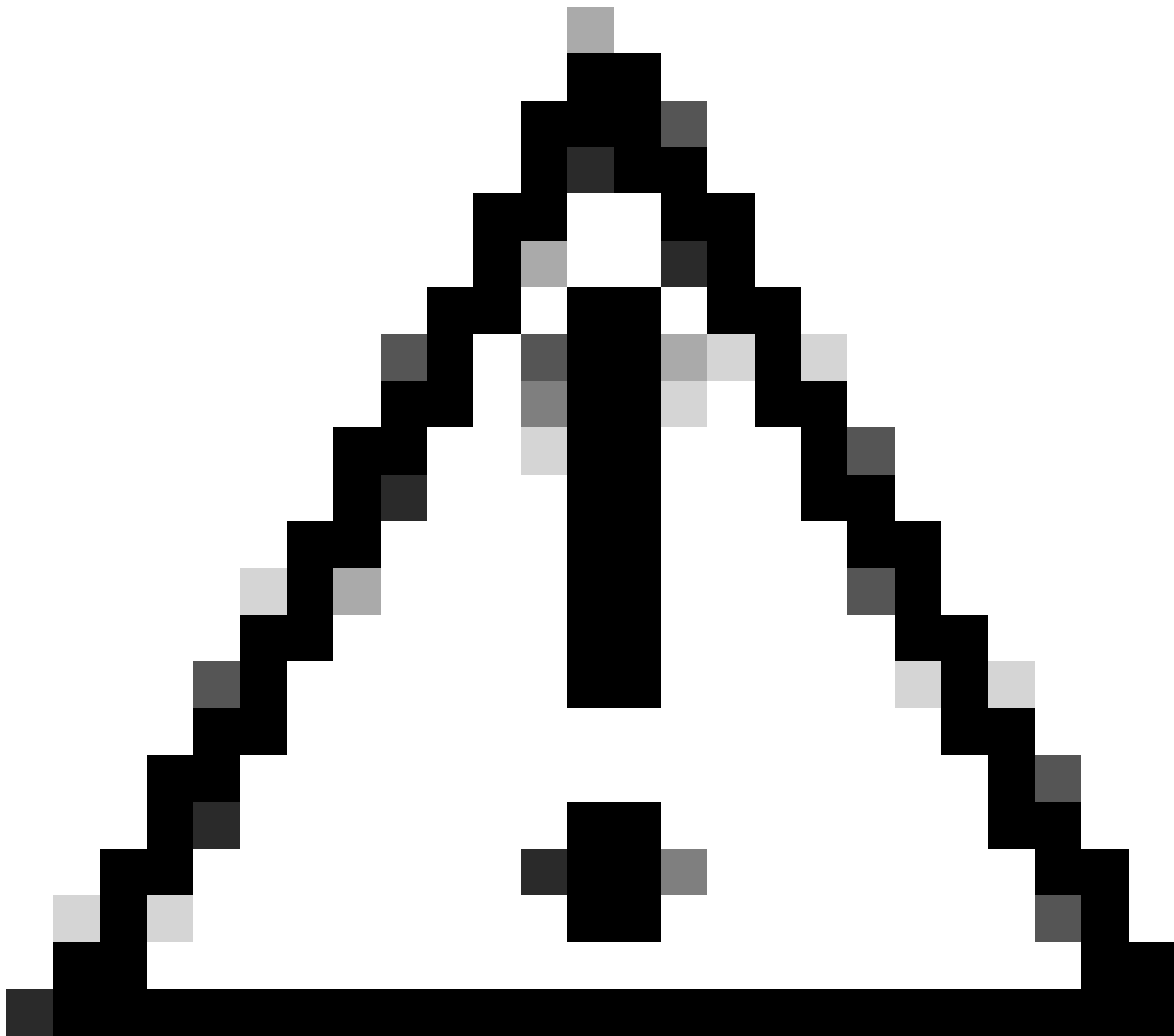
6. Starten Sie den DUO Proxy Manager auf Ihrem System, um mit dem Setup fortzufahren.



DUO-Proxy-Manager

7. (Optional) Wenn Ihr DUO Proxy Server eine Proxy-Konfiguration benötigt, um eine Verbindung zur DUO Cloud herzustellen, geben Sie die folgenden Parameter ein:

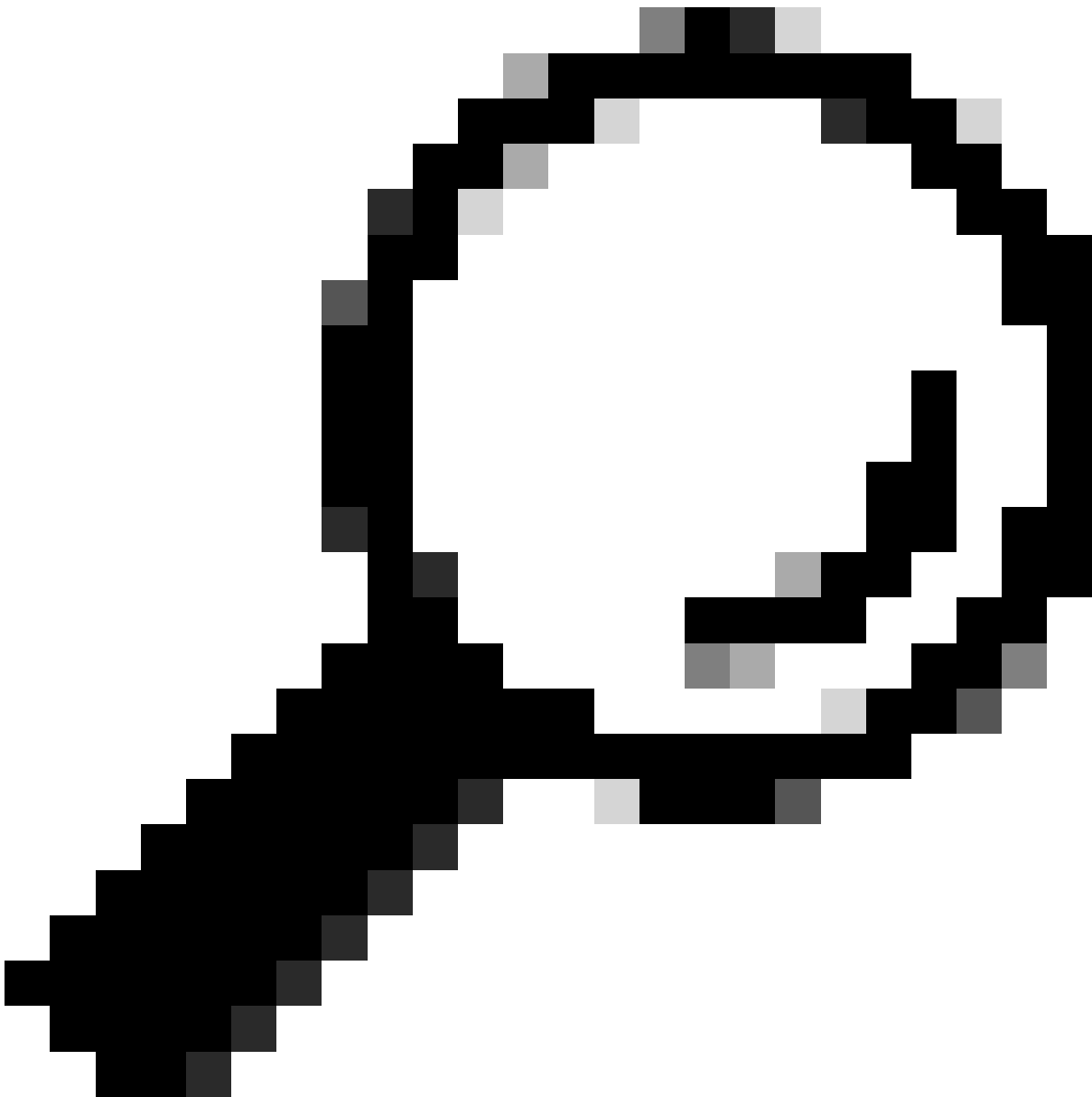
```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```



Vorsicht: Stellen Sie sicher, dass Sie und mit Ihren tatsächlichen Proxy-Details ersetzen.

8. Verwenden Sie jetzt die zuvor kopierten Informationen, um die Integrationskonfiguration abzuschließen.

```
[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
```



Tipp: Die Zeile `client=ad_client` gibt an, dass sich der DUO-Proxy über ein Active Directory-Konto authentifiziert. Stellen Sie sicher, dass diese Informationen richtig sind, um die Synchronisierung mit Active Directory abzuschließen.

Integration von DUO mit Active Directory

1. Integrieren Sie den DUO-Authentifizierungsproxy in Ihr 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. Treten Sie Ihrem Active Directory mit DUO Cloud-Services bei. Melden Sie sich bei <https://duo.com/an>.

3. Navigieren Sie zu "Benutzer", und wählen Sie "Verzeichnissynchronisierung", um die Synchronisierungseinstellungen zu verwalten.

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

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

No users shown based on your search.

Verzeichnissynchronisierung

4. Klicken Sie auf "Neue Synchronisierung hinzufügen" und wählen Sie "Active Directory" aus den bereitgestellten Optionen.

Dashboard > Users > Directory Sync

Directory Sync | Add New Sync

Directory Syncs | Connections

You don't have any directories yet.

Neue Synchronisierung hinzufügen

5. Wählen Sie Neue Verbindung hinzufügen und klicken Sie auf Weiter.

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

[Continue](#)

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

[Complete Setup](#)

Hinzufügen eines neuen Active Directory

6. Kopieren Sie den generierten Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen.

Authentication Proxy

[Delete Connection](#) [No Changes](#)

Configuration metadata

- 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](#)
- 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](#)

- 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](#)

Details zum Authentifizierungsproxy

7. Kehren Sie zur Konfiguration des DUO-Authentifizierungsproxys zurück, und konfigurieren Sie den Abschnitt `[cloud]` mit den neuen Parametern, die Sie erhalten haben, sowie den Anmeldeinformationen für das Dienstkonto eines Active Directory-Administrators:

```
[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. Validieren Sie Ihre Konfiguration, indem Sie die Option "validieren" auswählen, um sicherzustellen, dass alle Einstellungen korrekt sind.

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]uXWYwLM
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

Konfiguration von Proxy DUO.

9. Speichern Sie nach der Validierung Ihre Konfiguration, und starten Sie den DUO-Authentifizierungsproxy-Dienst neu, um die Änderungen zu übernehmen.

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]
```

Validate Save

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]'}

Option "Service neu starten".

10. Geben Sie im DUO-Verwaltungs-Dashboard die IP-Adresse des Active Directory-Servers zusammen mit der Basis-DN für die Benutzersynchronisierung ein.

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**.

Verzeichniseinstellungen

11. Wählen Sie die Option Plain (Einfach), um das System für eine Nicht-NTLMv2-Authentifizierung zu konfigurieren.

Authentication type

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

Authentifizierungstyp.

12. Speichern Sie Ihre neuen Einstellungen, um sicherzustellen, dass die Konfiguration aktualisiert wird.

 Delete Connection

Save

Status

Not connected

Add Authentication Proxy



Configure Directory

Connected Directory Syncs

User Syncs

[AD Sync](#)

Speicheroption

13. Verwenden Sie die "Testverbindung"-Funktion, um sicherzustellen, dass der DUO Cloud-

Service mit Ihrem Active Directory kommunizieren kann.

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 `key`, `secret_key`, 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](#).

Verbindungsoption testen.

14. Bestätigen Sie, dass der Active Directory-Status als "Verbunden" angezeigt wird, was auf eine erfolgreiche Integration hinweist.

Status

Connected

Status erfolgreich.

Exportieren von Benutzerkonten aus Active Directory (AD) über die DUO Cloud

1. Navigieren Sie zu Users > Directory Sync (Benutzer > Verzeichnissynchronisierung) im Duo Admin-Bereich, um nach den Einstellungen zu suchen, die sich auf die Verzeichnissynchronisierung mit Active Directory beziehen.

Benutzerliste.

2. Wählen Sie die Active Directory-Konfiguration, die Sie verwalten möchten.

3. Identifizieren Sie in den Konfigurationseinstellungen die Gruppen in Active Directory, die Sie mit der Duo Cloud synchronisieren möchten, und wählen Sie diese aus. Verwenden Sie die Filteroptionen für Ihre Auswahl.

4. Klicken Sie auf Setup abschließen.

AD-Synchronisierung.

5. Um die Synchronisierung sofort zu starten, klicken Sie auf Jetzt synchronisieren. Dadurch werden die Benutzerkonten der angegebenen Gruppen in Active Directory in die Duo Cloud

exportiert, sodass sie in der Duo Sicherheitsumgebung verwaltet werden können.

[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](#)

Starten der Synchronisierung

Registrieren Sie Benutzer in der Cisco DUO Cloud.

Die Registrierung von Benutzern ermöglicht die Identitätsüberprüfung mithilfe verschiedener Methoden, z. B. Codezugriff, DUO-Push, SMS-Codes und Token.

1. Navigieren Sie zum Abschnitt Benutzer im Cisco Cloud-Dashboard.
2. Suchen Sie das Konto des Benutzers, den Sie registrieren möchten, und wählen Sie es aus.

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

Select (0) ▾ ... [Export](#) ▾

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

1 total

Benutzerkontenliste.

3. Klicken Sie auf die Schaltfläche E-Mail-Anmeldung senden, um den Anmeldeprozess zu starten.

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).

Anmeldung per E-Mail.

4. Überprüfen Sie den E-Mail-Posteingang, und öffnen Sie die Einladung zur Registrierung, um den Authentifizierungsprozess abzuschließen.

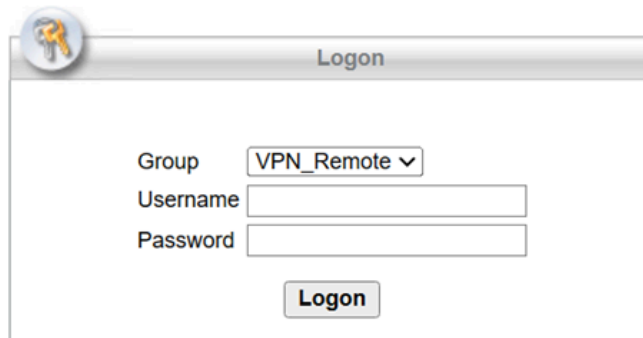
Weitere Informationen zum Registrierungsprozess finden Sie in den folgenden Ressourcen:

- Leitfaden zur allgemeinen Anmeldung: <https://guide.duo.com/universal-enrollment>
- Leitfaden zur Registrierung: <https://guide.duo.com/traditional-enrollment>

Verfahren zur Konfigurationsvalidierung.

Validieren Sie die folgenden Schritte, um sicherzustellen, dass Ihre Konfigurationen korrekt und betriebsbereit sind:

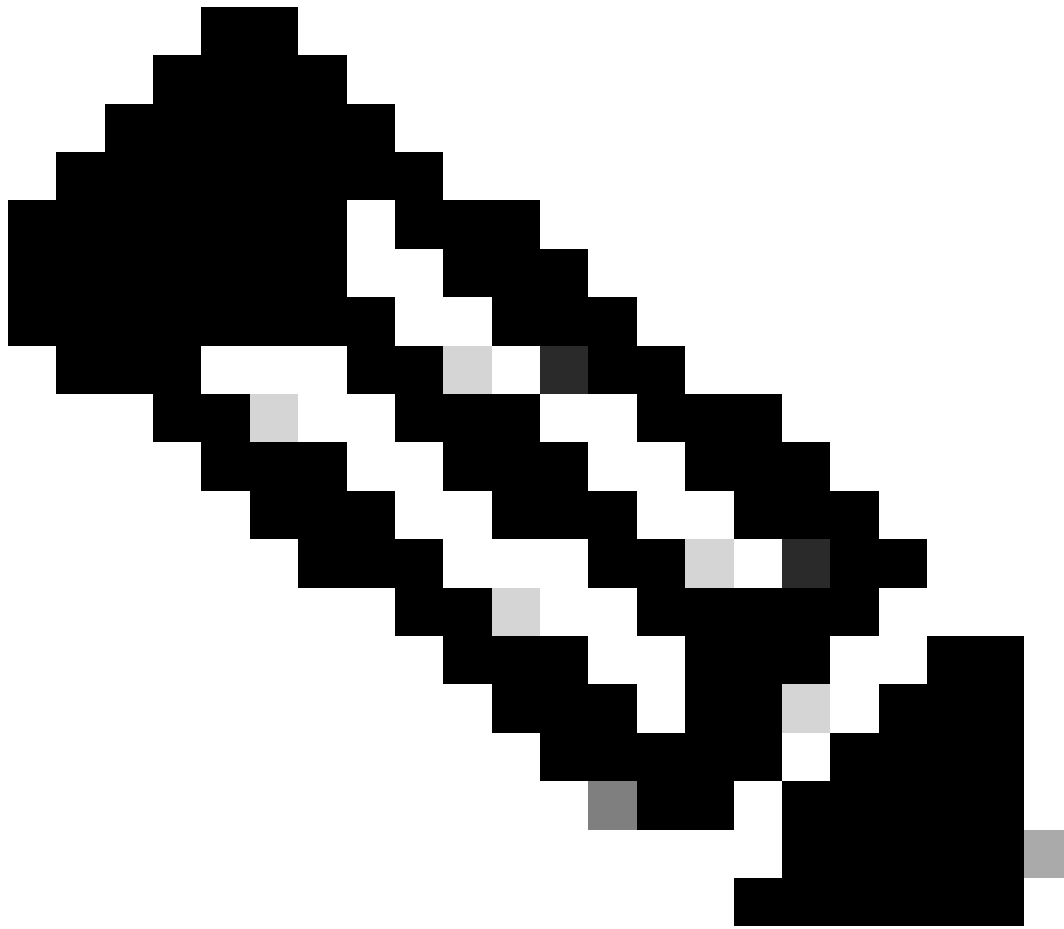
1. Starten Sie einen Webbrowser, und geben Sie die IP-Adresse des Firepower Threat Defense (FTD)-Geräts ein, um auf die VPN-Schnittstelle zuzugreifen.



The image shows a web browser window titled "Logon". The window has a grey header bar with a key icon on the left and the text "Logon" on the right. Below the header, there are three input fields: a dropdown menu for "Group" with "VPN_Remote" selected, a text box for "Username", and a text box for "Password". Below these fields is a "Logon" button.

VPN-Anmeldung.

2. Geben Sie auf Aufforderung Ihren Benutzernamen und Ihr Kennwort ein.



Hinweis: Die Anmeldeinformationen gehören zu den Active Directory-Konten.

3. Wenn Sie eine DUO-Push-Benachrichtigung erhalten, genehmigen Sie diese mithilfe der DUO Mobile-Software, um den Validierungsprozess fortzusetzen.

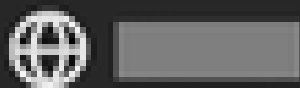


(1) Login request waiting.

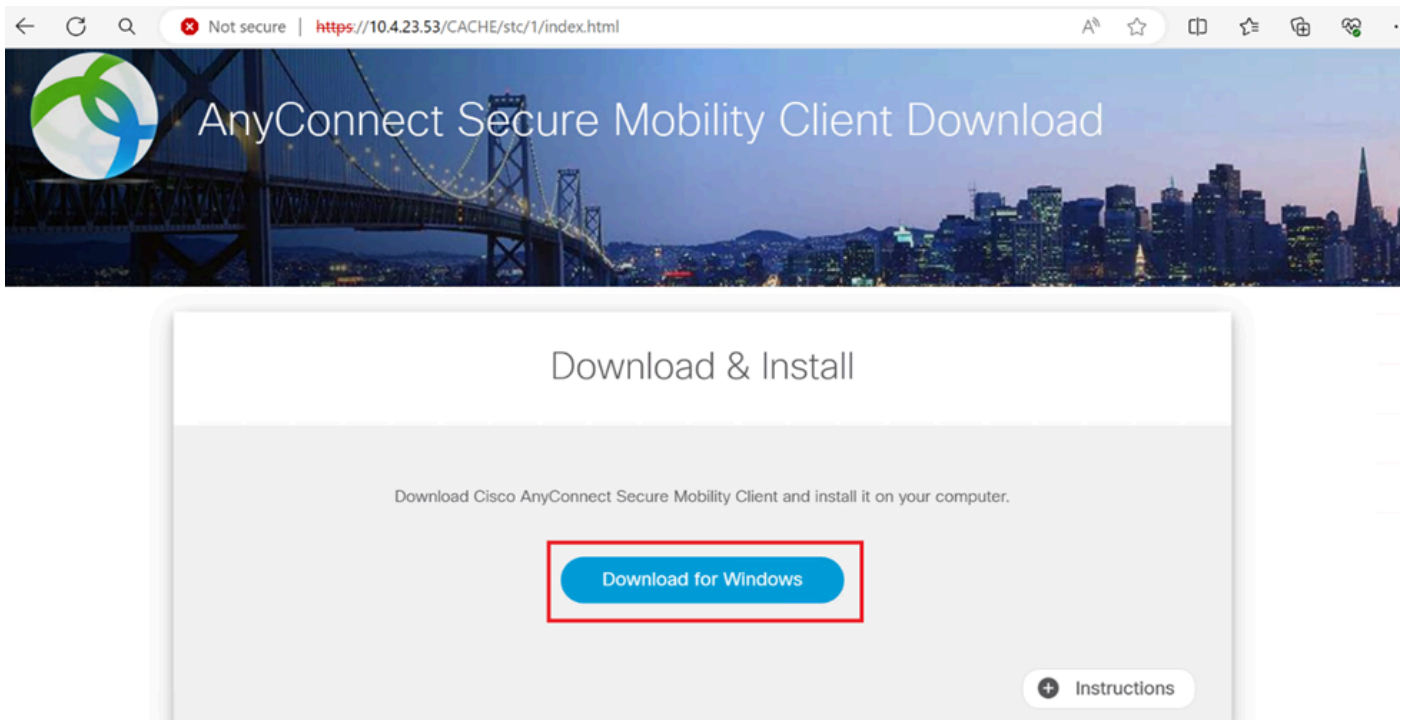
[Respond](#)



Are you logging in to Cisco ISE
RADIUS?



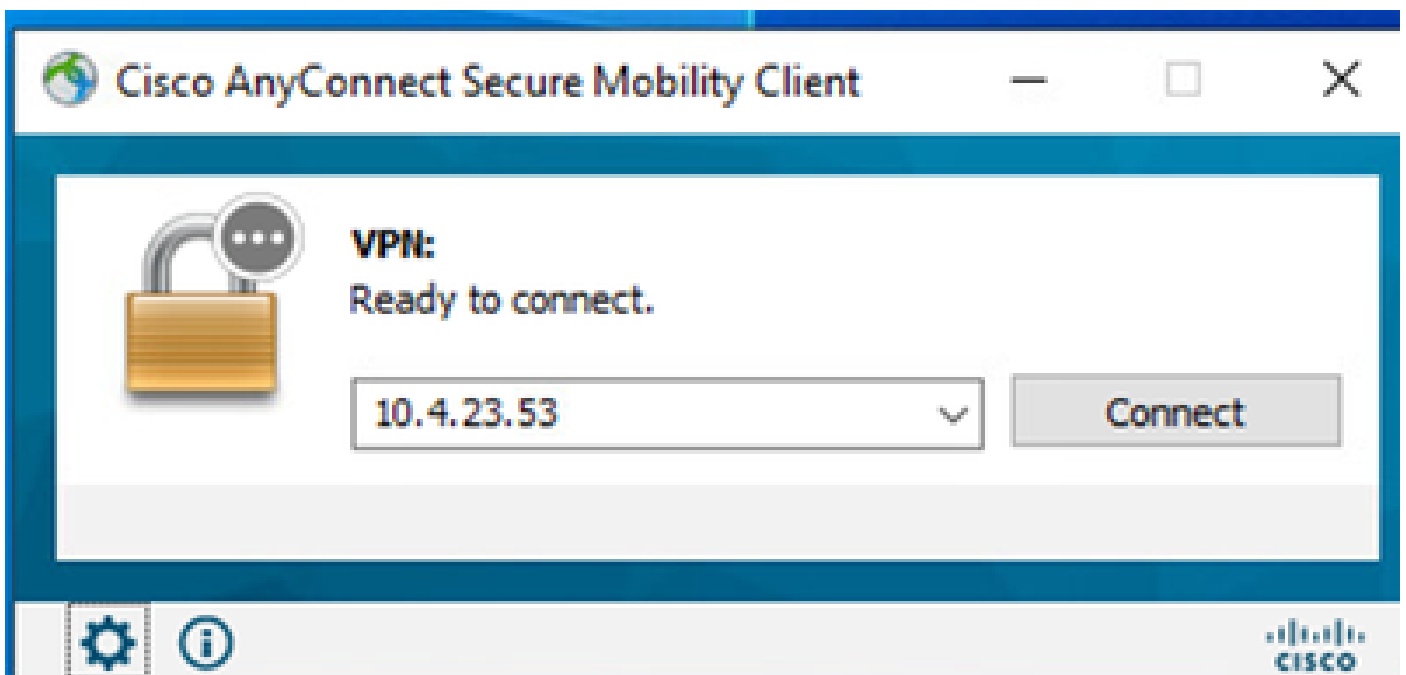
Suchen Sie nach dem für Windows-Systeme geeigneten Cisco AnyConnect VPN Client Package, und laden Sie es herunter.



Herunterladen und installieren

5. Führen Sie die heruntergeladene AnyConnect-Installationsdatei aus, und fahren Sie fort, um die Anweisungen des Installationsprogramms auf Ihrem Windows-Gerät auszuführen.

6. Öffnen Sie die Cisco AnyConnect Secure Mobility Client-Software. Stellen Sie eine Verbindung zum VPN her, indem Sie die IP-Adresse des FTD-Geräts eingeben.



AnyConnect-Software.

7. Geben Sie auf Aufforderung Ihre VPN-Zugangsdaten ein, und autorisieren Sie die DUO-Push-

Benachrichtigung erneut, um Ihre Verbindung zu authentifizieren.



(1) Login request waiting.

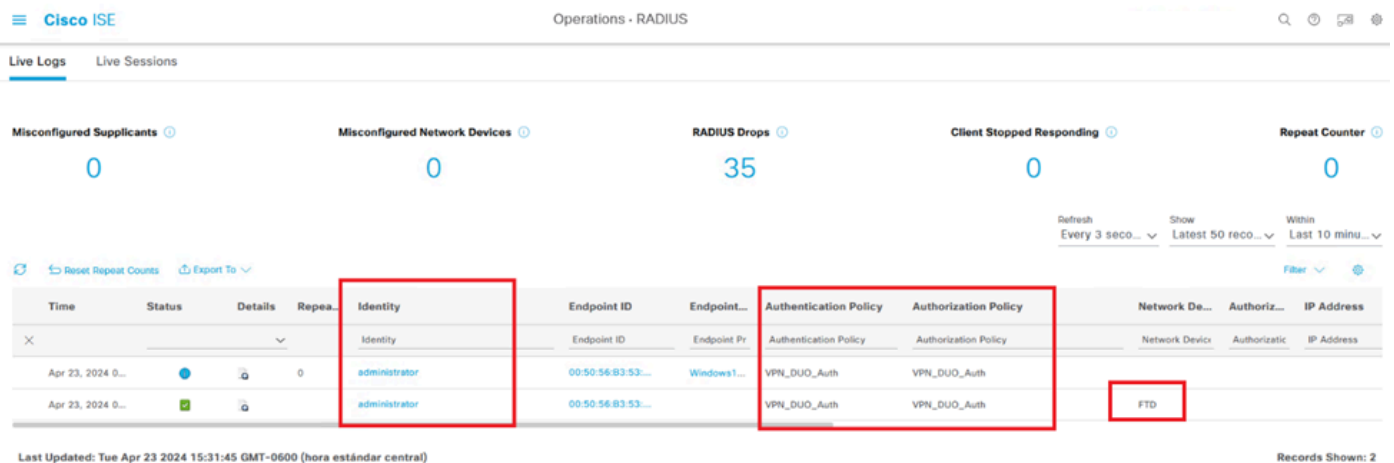
[Respond](#)



Are you logging in to Cisco ISE
RADIUS?

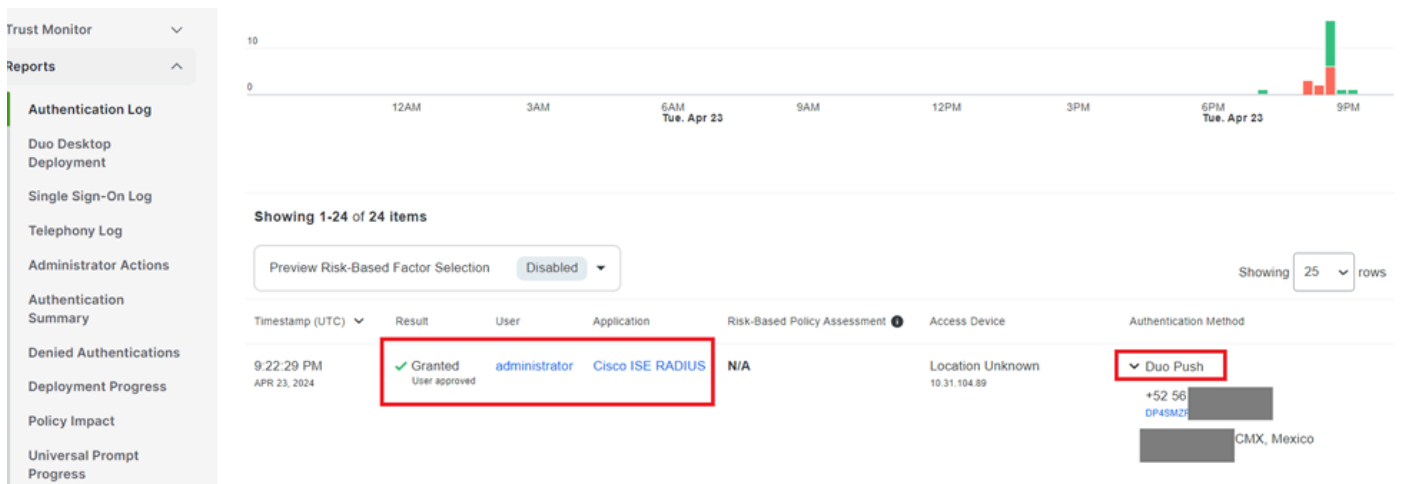


um die Echtzeitaktivität zu überwachen und die ordnungsgemäße Verbindung zu überprüfen, und greifen Sie auf die Live-Protokolle in der Cisco Identity Services Engine (ISE) zu.



ISE-Livelogs.

9. Gehen Sie zu Reports > Authentication logs, um die Authentifizierungsprotokolle im DUO Admin Panel zu überprüfen, um erfolgreiche Verifizierungen zu bestätigen.



Authentifizierungsprotokolle

Häufige Probleme.

Arbeitsszenario.

Bevor Sie sich mit bestimmten Fehlern im Zusammenhang mit dieser Integration befassen, ist es wichtig, das allgemeine Arbeitsszenario zu verstehen.

In den ISE-Livelogs können wir bestätigen, dass die ISE die RADIUS-Pakete an den DUO-Proxy weitergeleitet hat. Sobald der Benutzer den DUO-Push akzeptiert hat, wurde der RADIUS Access Accept vom DUO-Proxy-Server empfangen.

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

Authentifizierung erfolgreich durchführen.

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...

Ergebnis erfolgreich.

Eine Paketerfassung von der ISE-Seite zeigt die nächsten Informationen an:

Source	Destination	Protocol	Length	Info	
10.4.23.53	10.4.23.21	RADIUS	741	Access-Request id=138	→ The FTD sends the RADIUS request to ISE
10.4.23.21	10.31.126.207	RADIUS	883	Access-Request id=41	→ ISE resends the same RADIUS requests to the DUO Proxy
10.31.126.207	10.4.23.21	RADIUS	190	Access-Accept id=41	→ DUO Proxy sends the RADIUS accept (DUO push approved)
10.4.23.21	10.4.23.53	RADIUS	90	Access-Accept id=138	→ ISE resend the RADIUS accept to the FTD
10.4.23.53	10.4.23.21	RADIUS	739	Accounting-Request id=139	→ FTD sends the accounting for the current VPN connection
10.4.23.21	10.4.23.53	RADIUS	62	Accounting-Response id=139	→ ISE registered the accounting on its dashboard

ISE-Paketerfassung

Fehler11368 Überprüfen Sie die Protokolle auf dem externen RADIUS-Server, um den genauen Grund für den Fehler zu ermitteln.

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.

Fehler 11368.

Fehlerbehebung:

- Vergewissern Sie sich, dass der gemeinsame geheime RADIUS-Schlüssel in der ISE mit dem konfigurierten Schlüssel im FMC übereinstimmt.

1. Öffnen Sie die ISE-GUI.
 2. Administration > Network Resources > Network Devices.
 3. Wählen Sie den DUO-Proxy-Server.
 4. Klicken Sie neben dem gemeinsamen geheimen Schlüssel auf "Anzeigen", um den Schlüssel im Nur-Text-Format anzuzeigen.
 5. Öffnen Sie die FMC-GUI.
 6. Objekte > Objektverwaltung > AAA-Server > RADIUS-Servergruppe.
 7. Wählen Sie den ISE-Server aus.
 8. Geben Sie den geheimen Schlüssel erneut ein.
- Überprüfen der Active Directory-Integration in DUO

1. Öffnen Sie den DUO Authentication Proxy Manager.
2. Bestätigen Sie den Benutzer und das Kennwort im Abschnitt [ad_client].
3. Klicken Sie auf Validieren, um zu bestätigen, dass die aktuellen Anmeldeinformationen korrekt sind.

Fehler 1353 Keine externen RADIUS-Server mehr; Failover kann nicht durchgeführt werden

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.

Fehler 11353.

Fehlerbehebung:

- Vergewissern Sie sich, dass der gemeinsame geheime RADIUS-Schlüssel in der ISE mit dem konfigurierten Schlüssel im DUO-Proxy-Server übereinstimmt.

1. Öffnen Sie die ISE-GUI.
2. Administration > Network Resources > Network Devices.
3. Wählen Sie den DUO-Proxy-Server.
4. Klicken Sie neben dem gemeinsamen geheimen Schlüssel auf "Anzeigen", um den Schlüssel im Nur-Text-Format anzuzeigen.
5. Öffnen Sie den DUO Authentication Proxy Manager.
6. Überprüfen Sie den Abschnitt [radius_server_auto], und vergleichen Sie den gemeinsamen geheimen Schlüssel.

Die RADIUS-Sitzungen werden nicht in den ISE-Live-Protokollen angezeigt.

Fehlerbehebung:

- Überprüfen der DUO-Konfiguration

1. Öffnen Sie den DUO Authentication Proxy Manager.

2. Überprüfen Sie die ISE-IP-Adresse im Abschnitt [radius_server_auto].

- Überprüfen der FMC-Konfiguration

1. Öffnen Sie die FMC-GUI.

2. Gehen Sie zu Objekte > Objektverwaltung > AAA-Server > RADIUS-Servergruppe.

3. Wählen Sie den ISE-Server aus.

4. Überprüfen der ISE-IP-Adresse

- Nehmen Sie eine Paketerfassung in der ISE vor, um den Empfang der RADIUS-Pakete zu bestätigen.

1. Gehen Sie zu Operationen > Fehlerbehebung > Diagnosetools > TCP-Dump

Zusätzliche Fehlerbehebung.

- Aktivieren Sie die nächsten Komponenten im PSN als Debugging:

Policy-Engine

Port-JNI

Laufzeit-AAA

Weitere Fehlerbehebungen im DUO Authentication Proxy Manager finden Sie über den folgenden Link:

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

DUO-Vorlage.

Mit der nächsten Vorlage können Sie die Konfiguration Ihres DUO-Proxy-Servers abschließen.

```
[main] <--- OPTIONAL
http_proxy_host=<Proxy IP address or FQDN>
http_proxy_port=<Proxy port>
[radius_server_auto]
ikey=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxxxxxxx
radius_ip_1=<PSN IP Address>
radius_secret_1=xxxxxxxxxx
failmode=safe
```

port=1812
client=ad_client

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

[cloud]
ikey=xxxxxxxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxxxx
service_account_username=<your domain\username>
service_account_password=xxxxxxxxxxxxx

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.