

Konfiguration der Duo Integration mit Active Directory und ISE für die Zwei-Faktor-Authentifizierung auf AnyConnect/Remote Access VPN Clients

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdiagramm und -szenario](#)

[Kommunikationsprozess](#)

[Active Directory-Konfigurationen](#)

[Duo Konfigurationen](#)

[Duo Authentifizierungsproxy-Konfiguration](#)

[Cisco ISE-Konfigurationen](#)

[Konfiguration von Cisco ASA RADIUS/ISE](#)

[Konfiguration des Cisco ASA Remote Access VPN](#)

[Test](#)

[Fehlerbehebung](#)

[Arbeitsdebugs](#)

Einleitung

In diesem Dokument wird die Duo-Push-Integration mit AD und ISE als Zwei-Faktor-Authentifizierung für mit ASA verbundene AnyConnect-Clients beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- RA VPN-Konfiguration auf ASA
- RADIUS-Konfiguration auf ASA
- ISE
- Active Directory
- Duo-Anwendungen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Microsoft Server 2016
- ASA 9.14(3)18

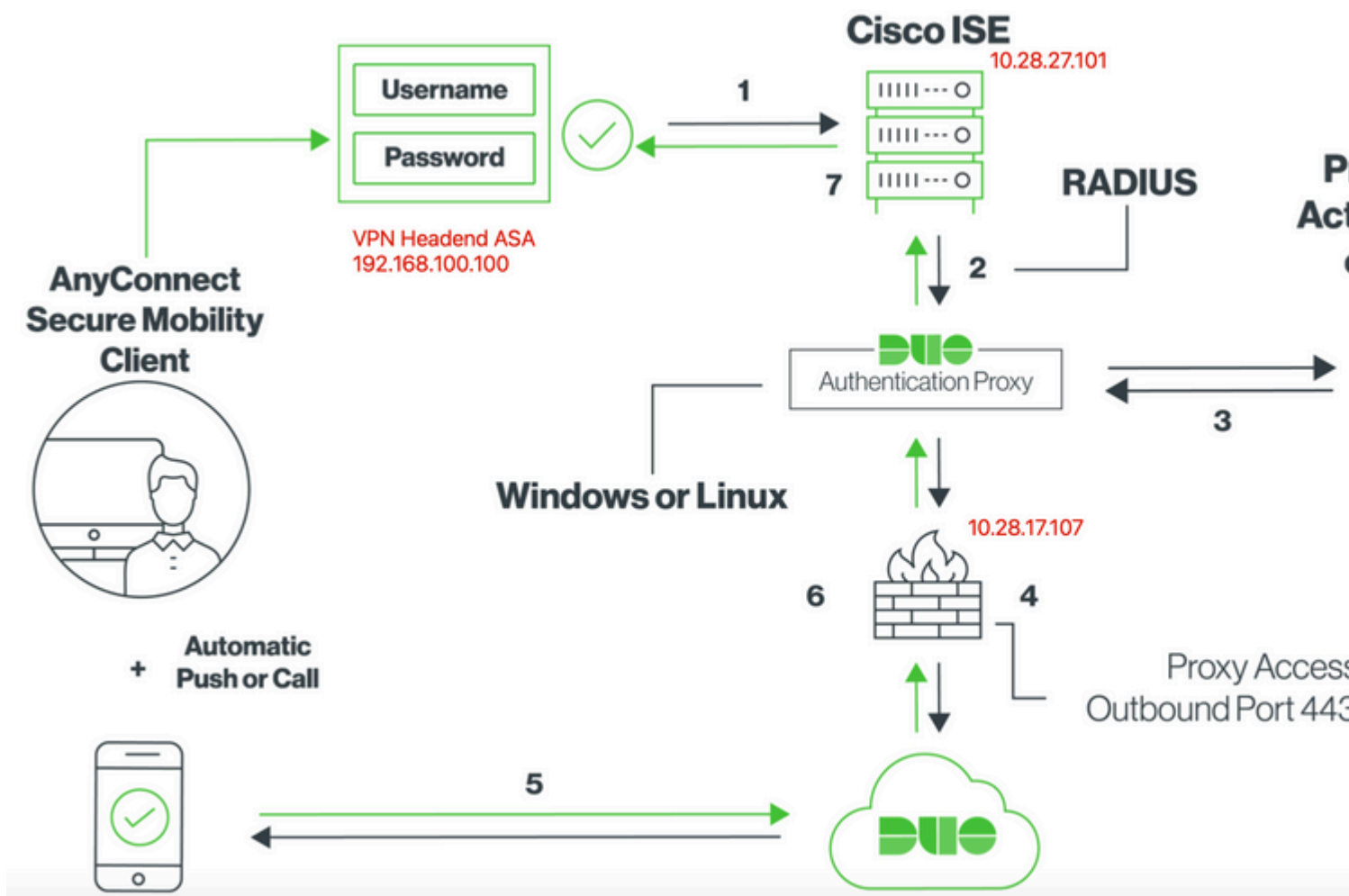
- ISE-Server 3.0
- Duo-Server
- Duo Authentifizierungsproxy-Manager

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.

Hintergrundinformationen

In diesem Dokument wird beschrieben, wie die Duo Push-Integration mit Active Directory (AD) und der Cisco Identity Service Engine (ISE) als Zwei-Faktor-Authentifizierung für AnyConnect-Clients konfiguriert wird, die eine Verbindung mit der Cisco Adaptive Security Appliance (ASA) herstellen.

Netzwerkdiagramm und -szenario



Kommunikationsprozess

<https://duo.com/docs/ciscoise-radius>

1. Primäre Authentifizierung wird auf Cisco ISE initiiert
2. Cisco ISE sendet Authentifizierungsanforderung an den Duo-Authentifizierungsproxy
3. Die primäre Authentifizierung verwendet Active Directory oder RADIUS.
4. Duo Authentication Proxy-Verbindung mit Duo Security über TCP-Port 443 hergestellt

5. Sekundäre Authentifizierung über den Dienst von Duo Security
6. Duo Authentifizierungsproxy empfängt Authentifizierungsantwort
7. Zugriff auf die Cisco ISE gewährt

Benutzerkonten:

- Active Directory-Administrator: Diese Eigenschaft dient als Verzeichniskonto, über das der Duo-Authentifizierungsproxy zur primären Authentifizierung an den Active Directory-Server gebunden werden kann.
- Active Directory-Testbenutzer
- Duo-Testbenutzer für sekundäre Authentifizierung

Active Directory-Konfigurationen

Der Windows-Server ist mit Active Directory-Domänendiensten vorkonfiguriert.

Hinweis: Wenn der RADIUS Duo-Authentifizierungsproxy-Manager auf demselben Active Directory-Hostcomputer ausgeführt wird, müssen die NPS-Rollen (Network Policy Server) deinstalliert/gelöscht werden. Wenn beide RADIUS-Dienste ausgeführt werden, können sie Konflikte verursachen und die Leistung beeinträchtigen.

Um eine AD-Konfiguration für die Authentifizierung und die Benutzeridentität von Remotezugriff-VPN-Benutzern zu erreichen, sind einige Werte erforderlich.

Alle diese Details müssen auf dem Microsoft-Server erstellt oder erfasst werden, bevor die Konfiguration auf dem ASA- und Duo Auth-Proxyserver erfolgen kann.

Die wichtigsten Werte sind:

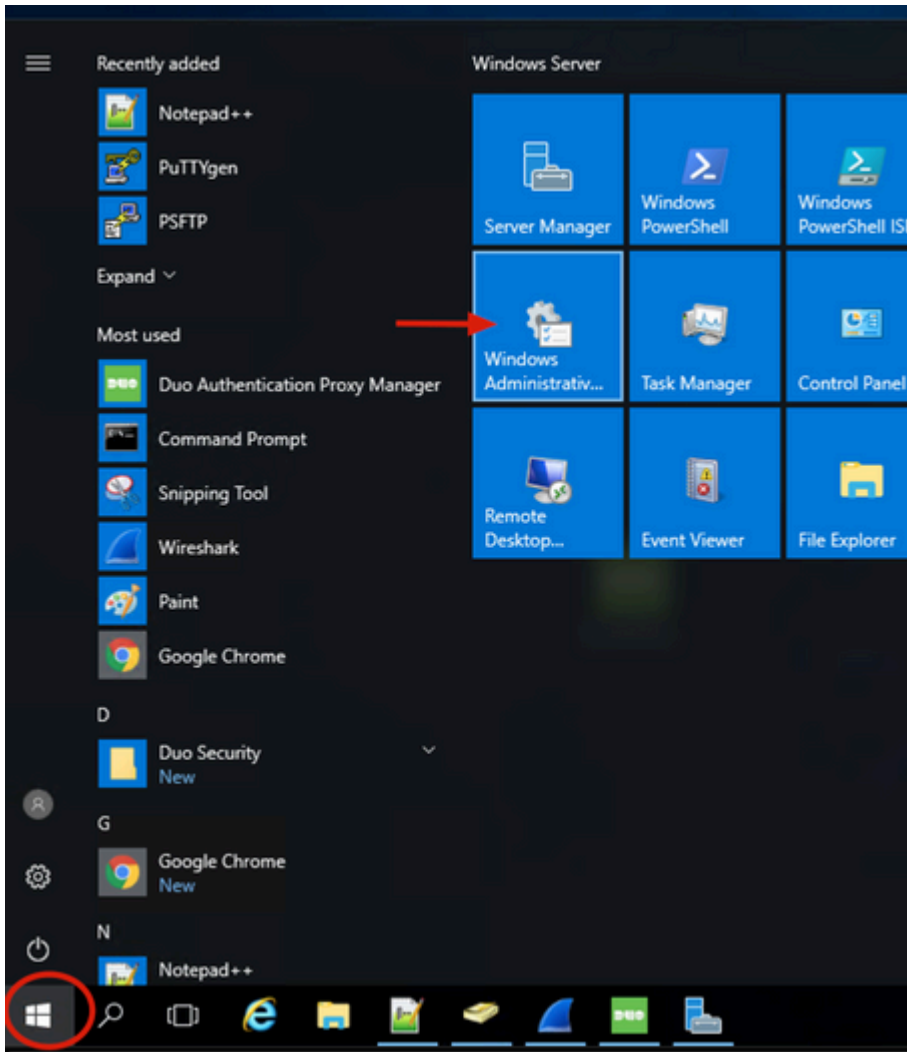
- Domänenname. Dies ist der Domänenname des Servers. In diesem Konfigurationsleitfaden ist `agarciam.cisco` der Domänenname.
- IP-/FQDN-Adresse des Servers Die IP-Adresse oder der FQDN für die Verbindung zum Microsoft-Server. Wenn ein FQDN verwendet wird, muss ein DNS-Server innerhalb des ASA- und Duo Auth-Proxys konfiguriert werden, um den FQDN aufzulösen.

In diesem Konfigurationsleitfaden lautet der Wert `agarciam.cisco` (wird zu `10.28.17.107` aufgelöst).

- Server-Port Der vom LDAP-Dienst verwendete Port. Standardmäßig verwenden LDAP und STARTTLS den TCP-Port 389 für LDAP und LDAP über SSL (LDAPS) den TCP-Port 636.
- Stammzertifizierungsstelle. Wenn LDAPS oder STARTTLS verwendet wird, ist die Stammzertifizierungsstelle zum Signieren des von LDAPS verwendeten SSL-Zertifikats erforderlich.
- Benutzername und Kennwort für das Verzeichnis. Dieses Konto wird vom Duo Auth-Proxyserver verwendet, um eine Bindung zum LDAP-Server herzustellen, Benutzer zu authentifizieren und nach Benutzern und Gruppen zu suchen.
- Distinguished Name (DN) für Basis- und Gruppenname Die Basis-DN ist der Ausgangspunkt für den Duo Auth-Proxy und weist das Active Directory an, mit der Suche und Authentifizierung von Benutzern zu beginnen.

In diesem Konfigurationsleitfaden wird die Root-Domäne `agarciam.cisco` als Basis-DN und die Gruppen-DN als `Duo-USERS` verwendet.

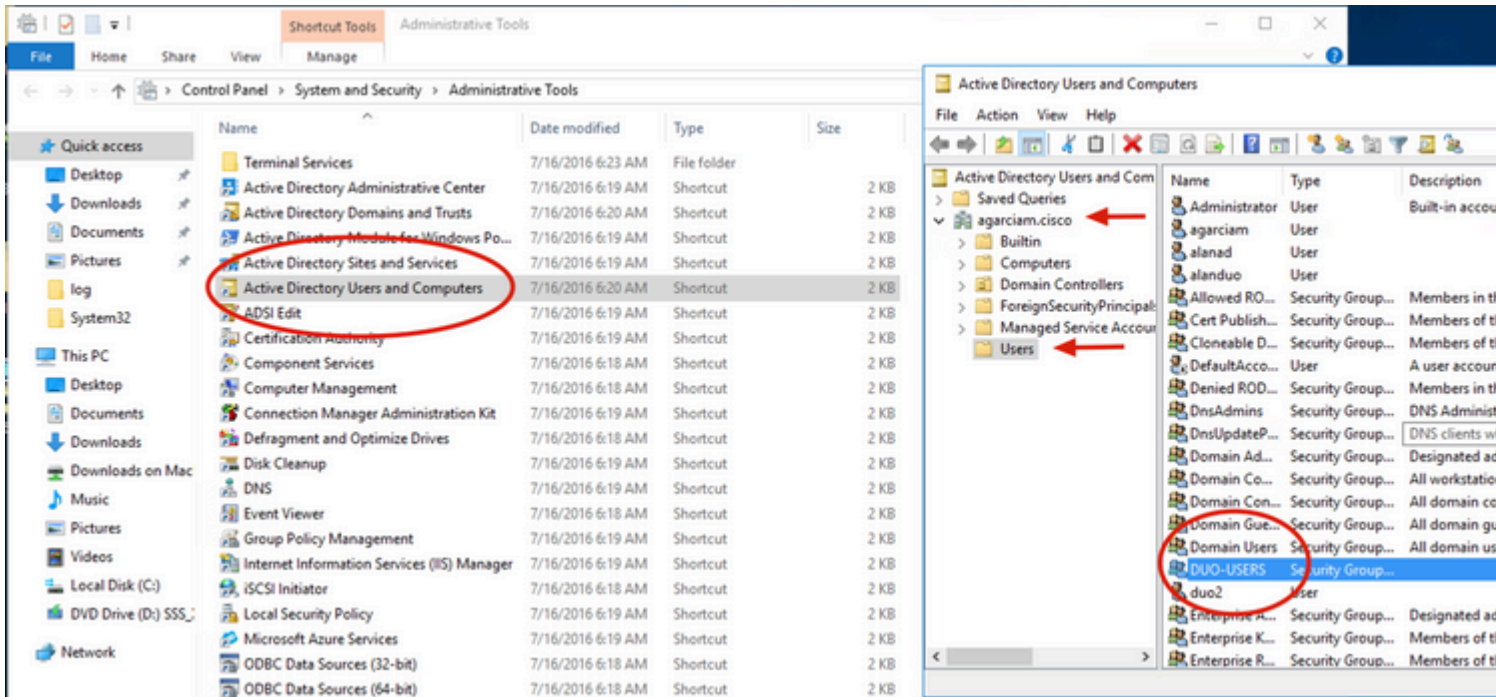
1. Um einen neuen Duo-Benutzer hinzuzufügen, navigieren Sie auf Windows Server zum **Windows**-Symbol unten links, und klicken Sie auf **Windows-Verwaltungstools**, wie im Bild dargestellt.



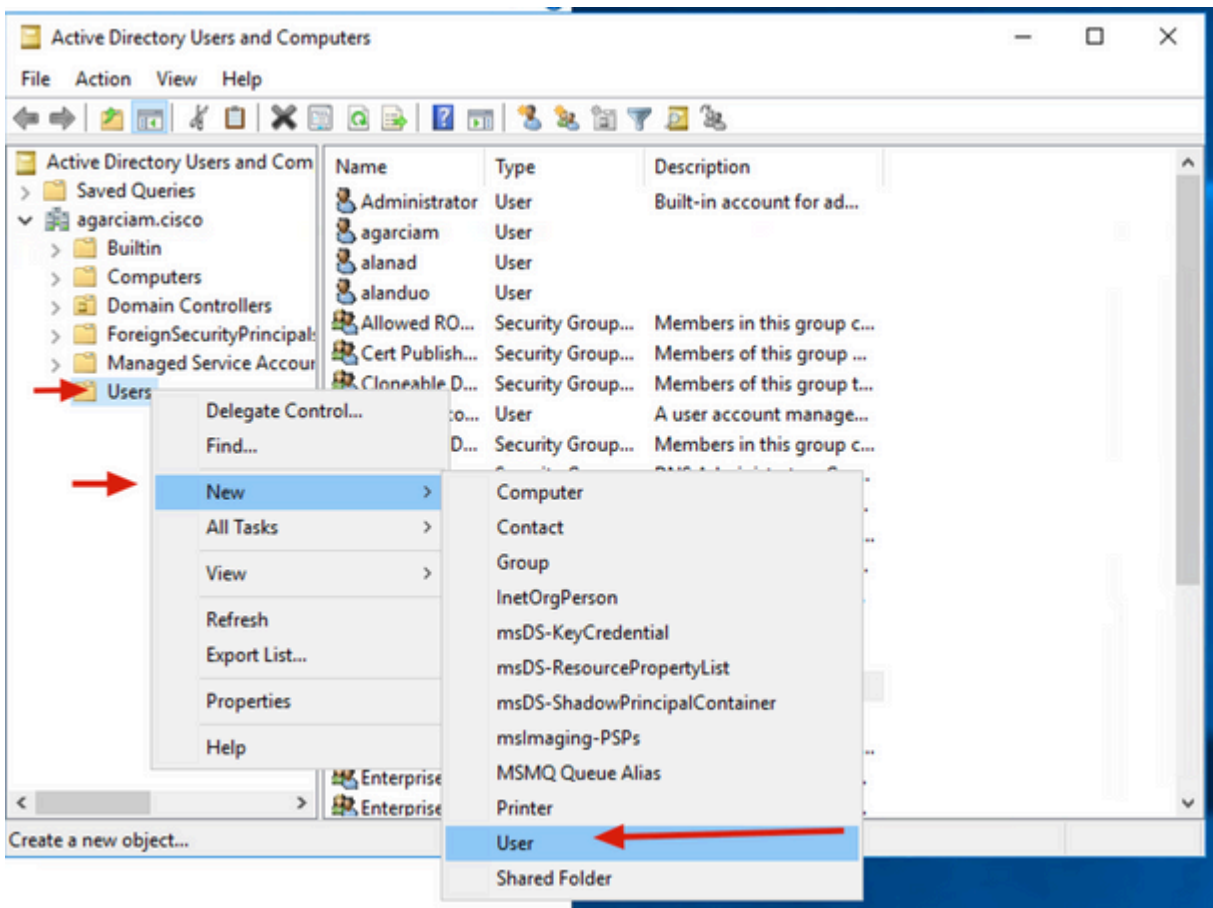
2. Navigieren Sie im Fenster Windows-Verwaltungstools zu **Active Directory-Benutzer und -Computer**.

Erweitern Sie im Bereich Active Directory-Benutzer und -Computer die Domänenoption, und navigieren Sie zum Ordner **Benutzer**.

In diesem Konfigurationsbeispiel wird Duo-USERS als Zielgruppe für die sekundäre Authentifizierung verwendet.



3. Klicken Sie mit der rechten Maustaste auf den Ordner **Benutzer** und wählen Sie **Neu > Benutzer**, wie im Bild dargestellt.



4. Geben Sie im Fenster Neues Objekt-Benutzer die Identitätsattribute für diesen neuen Benutzer an, und klicken Sie auf **Weiter**, wie im Bild dargestellt.

New Object - User

Create in: agarciam.cisco/Users

First name: duovpn Initials:

Last name:

Full name: duovpn

User logon name: duovpn @agarciam.cisco

User logon name (pre-Windows 2000): AGARCIAM\ duovpn

< Back Next > Cancel

5. Bestätigen Sie das Kennwort, und klicken Sie auf **Weiter** und dann auf **Beenden**, sobald die Benutzerinformationen überprüft wurden.

New Object - User

Create in: agarciam.cisco/Users

Password:

Confirm password:

User must change password at next logon

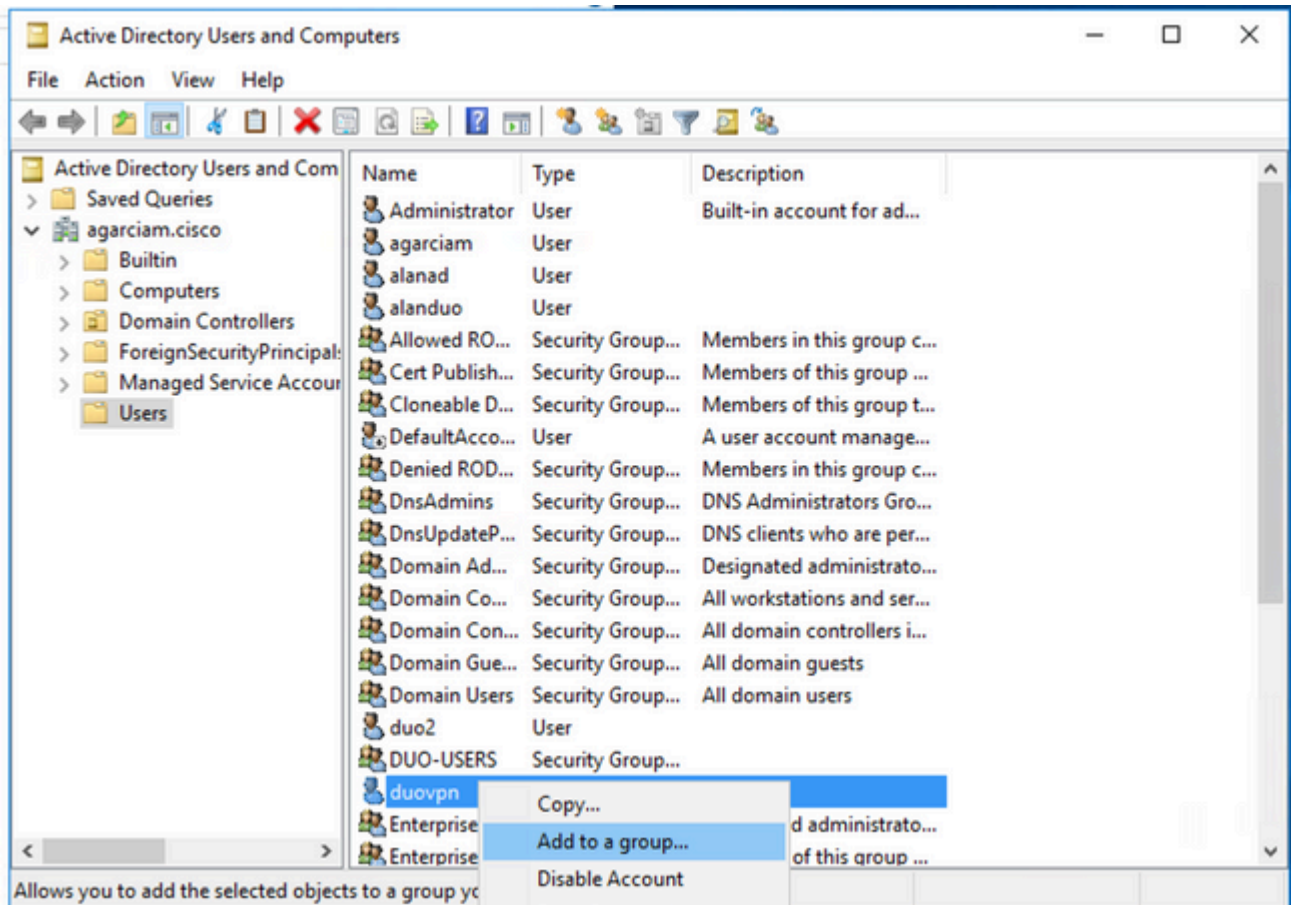
User cannot change password

Password never expires

Account is disabled

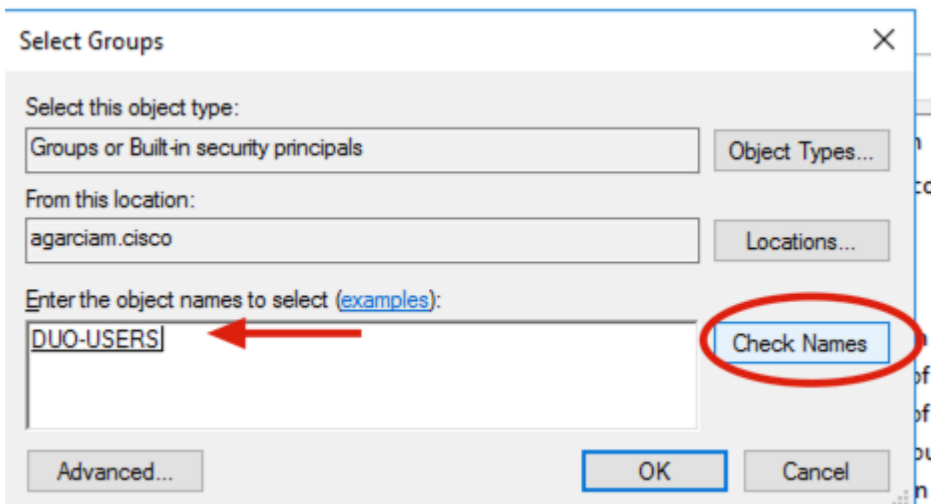
< Back Next > Cancel

6. Weisen Sie den neuen Benutzer einer bestimmten Gruppe zu, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Zu einer Gruppe hinzufügen**, wie im Bild dargestellt.



7. Geben Sie im Bereich "Gruppen auswählen" den Namen der gewünschten Gruppe ein, und klicken Sie auf **Namen überprüfen**.

Wählen Sie dann den Namen aus, der Ihren Kriterien entspricht, und klicken Sie auf **OK**.



8. Dies ist der Benutzer, der in diesem Dokument als Beispiel verwendet wird.

Duo Konfigurationen

1. Melden Sie sich in Ihrem Dudo Admin Portal.



Admin Login

Enter your admin credentials

██████████.com


[Log in as someone else](#)

Password

[Forgot password?](#)

Confirm your identity

2. Navigieren Sie auf der linken Seite zu **Users (Benutzer)**, klicken Sie auf **Add User (Benutzer hinzufügen)** und geben Sie den Namen des Benutzers ein, der mit unserem Active Domain-Benutzernamen übereinstimmt. Klicken Sie dann auf **Add User (Benutzer hinzufügen)**.



- Dashboard
- Device Insight
- Policies
- Applications
- Single Sign-On
- Users** ←
- Add User** ←
- Pending Enrollments
- Bulk Enroll Users
- Import Users
- Directory Sync

Search for users, groups, applications, or devices

[Dashboard](#) > [Users](#) > Add User

Add User

Most applications allow users to enroll themselves after they complete primary authentication. [Learn more about adding users](#)

Username

 ←

Should match the primary authentication username.

Add User

3. Füllen Sie auf dem neuen Bedienfeld alle erforderlichen Informationen aus.

Policies

Applications

Single Sign-On

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

Endpoints

2FA Devices

Trusted Endpoints

Trust Monitor

Reports

Settings

Need Help?

[Chat with Tech Support](#)

[Email Support](#)

Call us at 1-855-386-2884

Versioning

Core Authentication Service:

D235.6

Admin Panel:

D235.6

[Read Release Notes](#)

Account ID

2910-6030-53

Deployment ID

[DUO63](#)

Helpful Links

[Documentation](#)

[User Guide](#)

[Dashboard](#) > [Users](#) > duovpn

duovpn



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

Username

duovpn



Username aliases

[+ Add a username alias](#)

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number for (e.g., Username alias 1 should only be used for Employee ID).

Full name

test ypn user



Email

[redacted]@[redacted].com

Status

Active



Require multi-factor authentication (default).

Bypass

Allow users to skip two-factor authentication and log in w

Disabled

Automatically deny access

This controls the user's two-factor authentication process.

Groups

You don't have any editable groups. [Add one.](#)

Groups can be used for management, reporting, and policy. [Le](#)

Notes

: In diesem Dokument wird die Duo-Push-for-Mobile-Device-Methode verwendet, daher muss ein Telefongerät hinzugefügt werden.

Klicken Sie auf **Telefon hinzufügen**.

Phones
You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) ↗.

This user has no phones. [Add one.](#)

Endpoints

This user has no devices.

Hardware Tokens [Add Hardware Token](#)

This user has no hardware tokens. [Add one.](#)



Bypass Codes [Add Bypass Code](#)

This user has no bypass codes. [Add one.](#)

WebAuthn & U2F [Add WebAuthn & U2F](#)

5. Geben Sie die Telefonnummer des Benutzers ein, und klicken Sie auf **Telefon hinzufügen**.

Add Phone

 [Learn more about Activating Duo Mobile](#) 

Type

Phone

Tablet

Phone number  [Show extension field](#)

Optional. Example: "+52 1 222 123 4567"



6. Navigieren Sie im linken Duo-Administrationsbereich zu **Benutzer**, und klicken Sie auf den neuen Benutzer.

Dashboard > Users

Users

Directory Sync | Im

i You have users who have not activated Duo Mobile. [Click here to send them activation links.](#)
Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

5 Total Users **0** Not Enrolled **2** Inactive Users **1** Trash **0** Bypassed

Select (0) ▾ ... Export ▾

<input type="checkbox"/>	Username ▲	Name	Email	Phones	Tokens
<input type="checkbox"/>	[redacted]			1	
<input type="checkbox"/>	[redacted]			1	
<input type="checkbox"/>	[redacted]			1	
<input type="checkbox"/>	duovpn		[redacted]@i.com	1	
<input type="checkbox"/>	[redacted]		[redacted]@o.com	1	

Need Help?
Chat with Tech Support

Hinweis: Falls Sie derzeit keinen Zugriff auf Ihr Telefon haben, können Sie die E-Mail-Option auswählen.

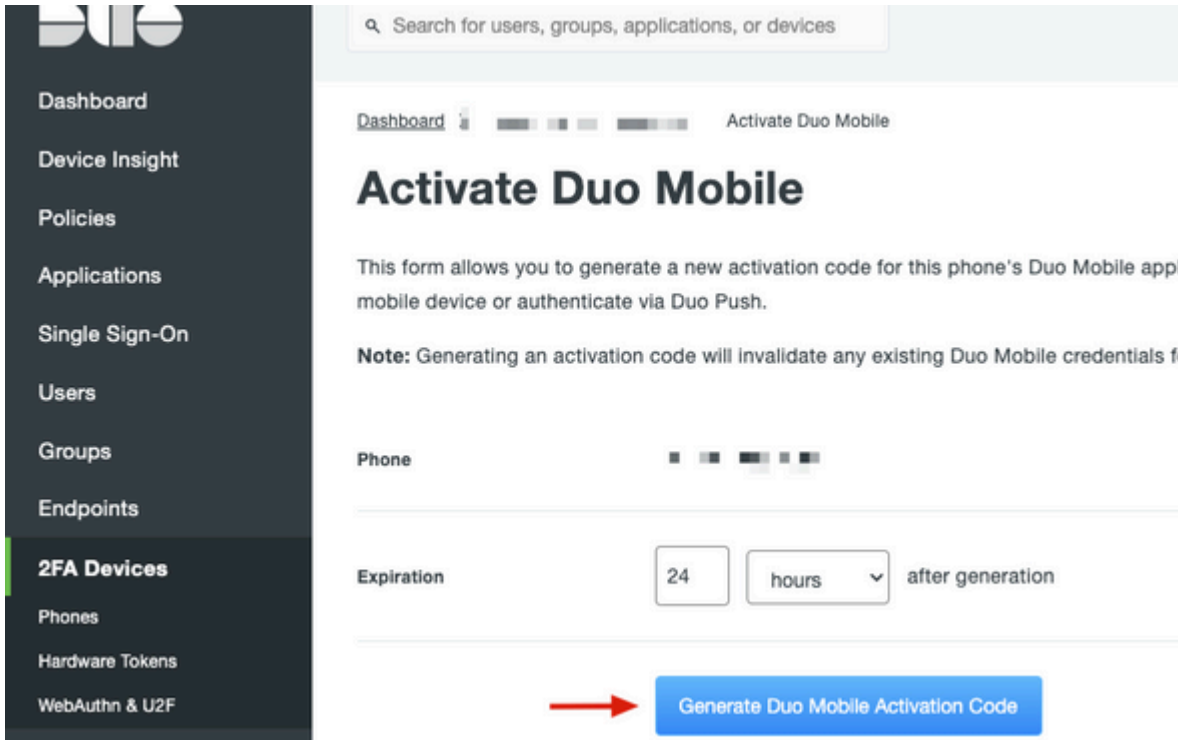
7. Navigieren Sie zum Abschnitt **Telefone**, und klicken Sie auf **Activate Duo Mobile (Duo-Mobiltelefon aktivieren)**.

Phones

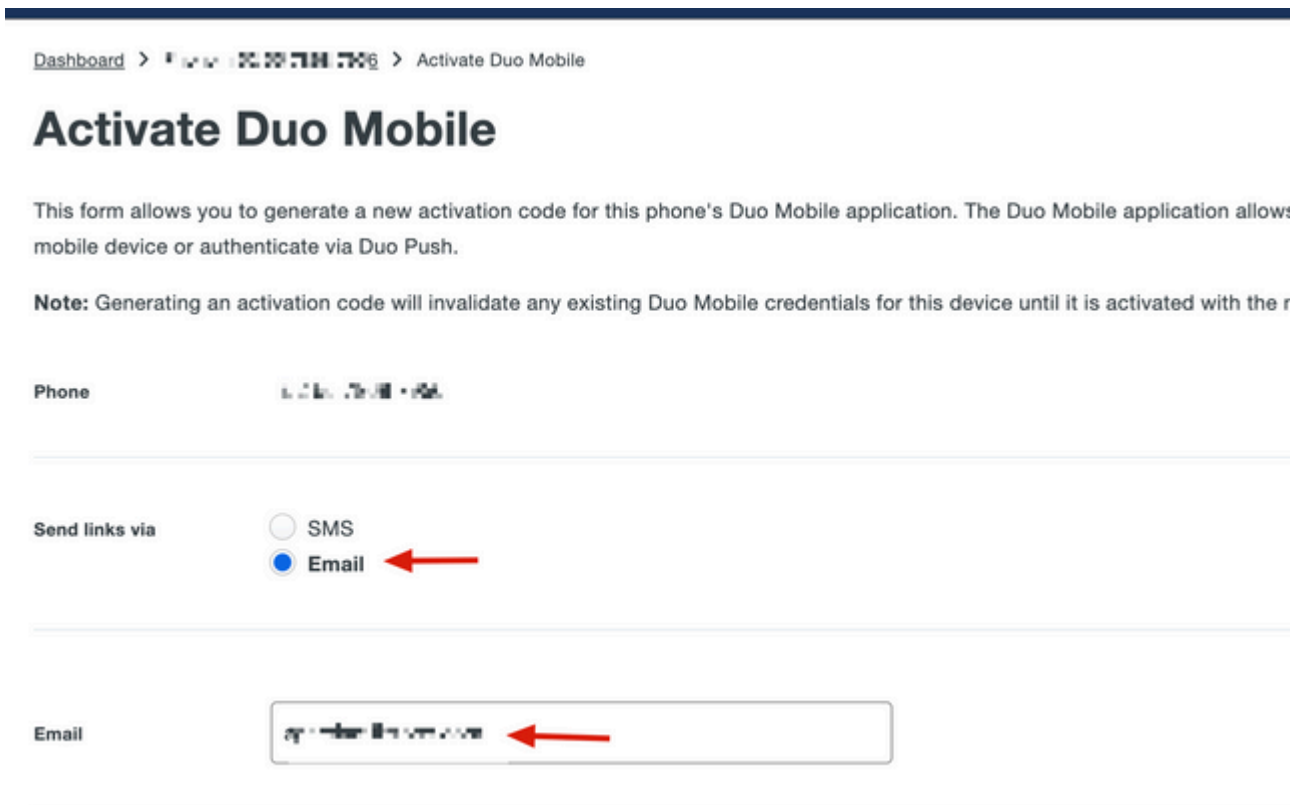
You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#).

Alias	Device	Platform	Model	Security Warnings	
phone1	[redacted]	Android 10	[redacted]	✓ No warnings	Activate Duo Mobile

8. Klicken Sie auf **Duo Mobile-Aktivierungscode generieren**.



9. Wählen Sie **E-Mail**, um die Anweisungen per E-Mail zu erhalten, geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **Anweisungen per E-Mail senden**.



10. Sie erhalten eine E-Mail mit den Anweisungen, wie im Bild gezeigt.

This is an automated email from Duo Security.

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:



Just tap this link from + [redacted] or copy and paste it into Duo Mobile manually:



If you're not reading this from + [redacted] Duo Mobile on your phone and scan this barcode:



Don't have Duo Mobile yet? Install it first:

iPhone: <https://itunes.apple.com/us/app/duo-mobile/id422663827>

Android: <https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>

11. Öffnen Sie die Duo Mobile App von Ihrem Mobilgerät und klicken Sie auf **Hinzufügen**, wählen Sie dann **QR-Code verwenden** und scannen Sie den Code aus der Anleitung-E-Mail.

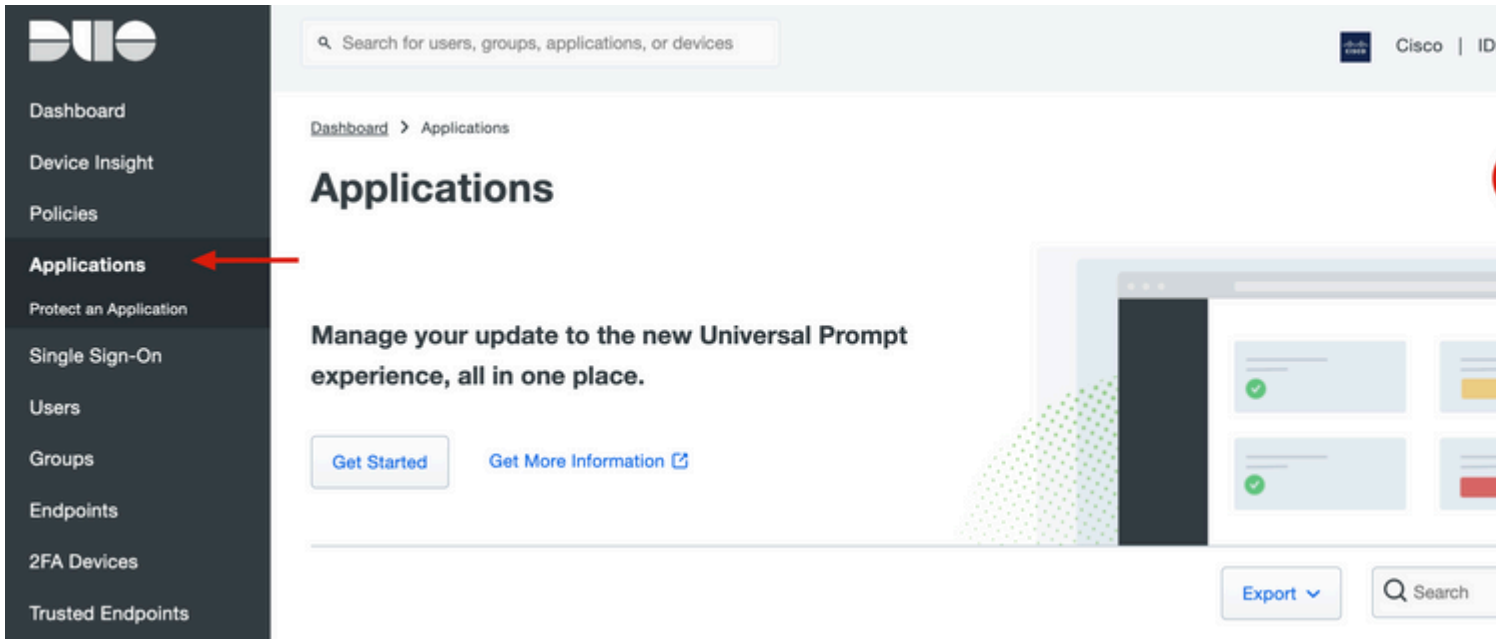
12. Neuer Benutzer wird zu Ihrer mobilen Duo-App hinzugefügt.

Duo Authentifizierungsproxy-Konfiguration

1. Laden Sie Duo Auth Proxy Manager von <https://duo.com/docs/authproxy-reference> herunter, und installieren Sie es.

Hinweis: In diesem Dokument ist der Duo Auth Proxy Manager auf demselben Windows-Server installiert, auf dem die Active Directory-Dienste gehostet werden.

2. Navigieren Sie im Duo-Administrationsbereich zu Anwendungen, und klicken Sie auf **Anwendung schützen**.



3. Suchen Sie in der Suchleiste nach Cisco ISE Radius.

Protect an Application

i 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.

isel

Application	Protection Type	Documentation	Protect
Akamai Enterprise Application Access	2FA	Documentation	Protect
Cisco ISE RADIUS	2FA	Documentation	Protect

4. Kopieren Sie den Integrationsschlüssel, den Sicherheitsschlüssel und den API-Hostnamen. Sie benötigen diese Informationen für die Konfiguration des Duo-Authentifizierungsproxys.



Successfully added Cisco ISE RADIUS to protected applications. [Add another.](#)

[Dashboard](#) > [Applications](#) > Cisco ISE RADIUS 1

Cisco ISE RADIUS 1

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

Details

Integration key

XX

[Copy](#)

Secret key

.....W6ho

[Copy](#)

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

API hostname

XX

[Copy](#)

5. Führen Sie die Anwendung Duo Authentication Proxy Manager aus, schließen Sie die Konfiguration für den Active Directory-Client und den ISE Radius-Server ab, und klicken Sie auf **Validieren**.

Hinweis: Wenn die Validierung nicht erfolgreich ist, finden Sie auf der Registerkarte debug weitere Informationen, und korrigieren Sie diese entsprechend.

Duo Authentication Proxy Manager

Authentication Proxy is **running** Up since: 3/5/2022, 9:23:04 AM Version: 5.6.0 [Update your Authentication Proxy](#)

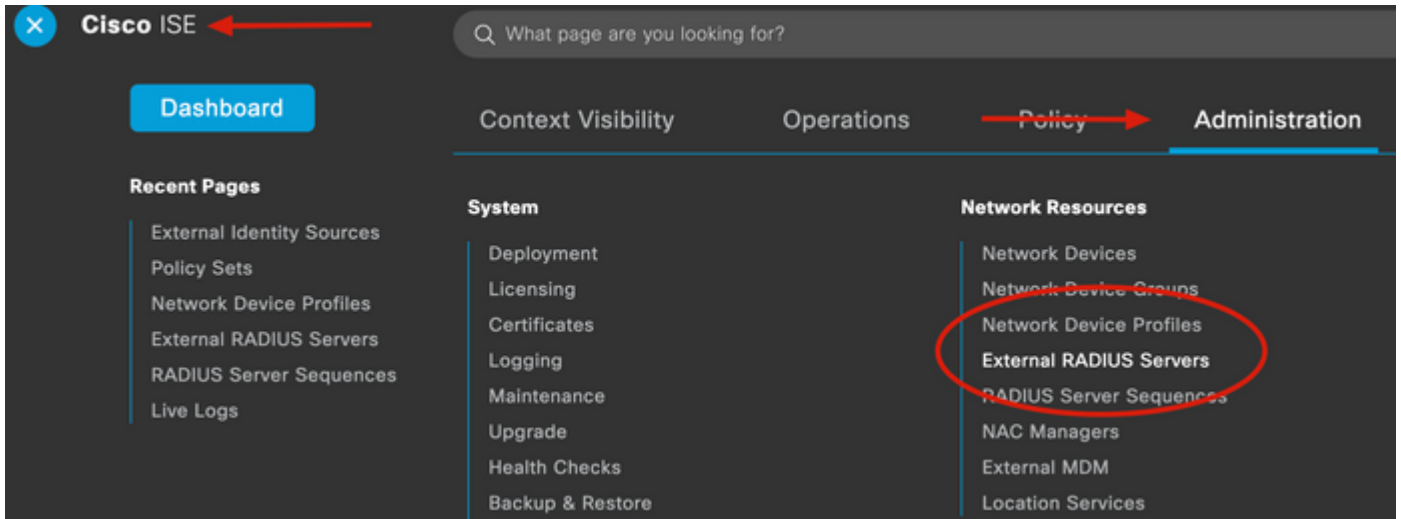
Validation passed
Configuration has passed validation and is ready to be saved ←

Configure: authproxy.cfg	Unsaved Changes	Output
<pre>18 ; number to the section name (e.g. [ad_client2]) 19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Administrator 23 service_account_password= 24 search_dn=DC=agarciam,DC=cisco 25 26 [radius_server_auto] 27 ikey= 28 skey= 29 api_host=api- 30 radius_ip_1=10.28.17.101 31 radius_secret_1= 32 failmode=safe 33 client=ad_client 34 port=1812 35 36</pre>		<pre>Running The Duo Authentication Proxy Connecting to the server... several minutes... [info] Testing section 'main' with configuration... [info] {'debug': 'True', 'log_max_files': '10', 'log_max_size': '20971520', 'test_connectivity_on_startup': 'true'} [info] There are no configuration problems [info] ----- [info] Testing section 'ad_client' with configuration... [info] {'debug': 'True', 'host': '10.28.17.107', 'search_dn': 'DC=agarciam,DC=cisco', 'service_account_password': '*****', 'service_account_username': 'Administrator'} [info] There are no configuration problems [info] ----- [info] Testing section 'radius_server_auto' with configuration... [info] {'api_host': 'api-10.28.17.101', 'radius_ip_1': '10.28.17.101', 'radius_secret_1': '*****', 'skey': '*****', 'ikey': '*****'}</pre>

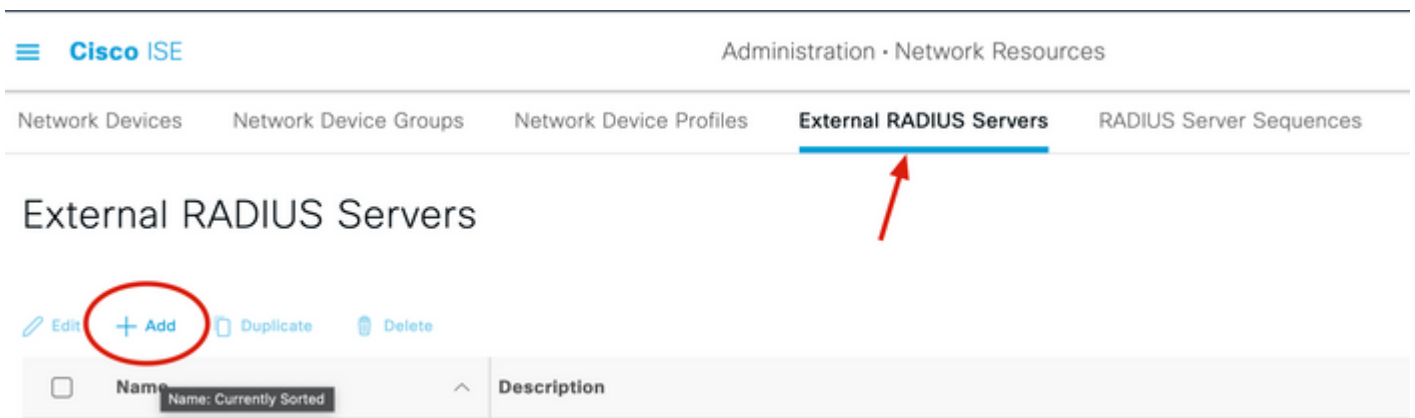
Validate Save [Learn how to configure](#)

Cisco ISE-Konfigurationen

1. Melden Sie sich beim ISE-Administratorportal an.
2. Erweitern Sie die Registerkarte Cisco ISE, und navigieren Sie zu **Administration**, klicken Sie dann auf **Network Resources (Netzwerkressourcen)**, und klicken Sie auf **External RADIUS Servers (Externe RADIUS-Server)**.



3. Klicken Sie auf der Registerkarte "Externe RADIUS-Server" auf **Hinzufügen**.



4. Füllen Sie die Lücke mit der RADIUS-Konfiguration aus, die im Duo Authentication Proxy Manager verwendet wird, und klicken Sie auf **Submit (Senden)**.

Network Devices Network Device Groups Network Device Profiles **External RADIUS Servers** RADIUS Server Sequences

* Name: DUO_NEW

Description: [Empty text area]

* Host IP: 10.28.17.107

* Shared Secret: | Show

Enable KeyWrap: ⓘ

* Key Encryption Key: Show

* Message Authenticator Code Key: Show

Key Input Format: ASCII HEXADECIMAL

* Authentication Port: 1812 (Valid Range 1 to 65535)

* Accounting Port: 1813 (Valid Range 1 to 65535)

* Server Timeout: 5 Seconds (Valid Range 1 to 120)

* Connection Attempts: 3 (Valid Range 1 to 9)

Radius ProxyFailover Expiration: 300 ⓘ (valid Range 1 to 600)

5. Navigieren Sie zur Registerkarte **RADIUS Server Sequences (RADIUS-Serversequenzen)**, und klicken Sie auf **Add (Hinzufügen)**.

Cisco ISE Administration · Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers **RADIUS Server Sequences**

RADIUS Server Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

[Edit](#) **+ Add** [Duplicate](#) [Delete](#)

6. Geben Sie den Namen der Sequenz an, und weisen Sie den neuen RADIUS External Server zu. Klicken Sie auf **Submit (Senden)**.

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

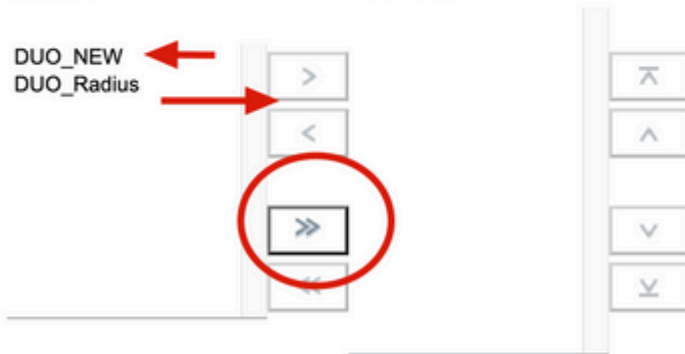
✓ User Selected Service Type

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

Available

* Selected

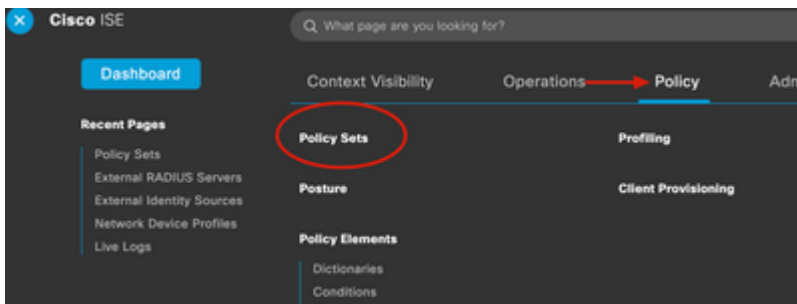
DUO_NEW
DUO_Radius



Remote accounting

Local accounting

7. Navigieren Sie vom Dashboard-Menü zu **Policy** und klicken Sie auf **Policy Sets**.




8. Weisen Sie die RADIUS-Sequenz der Standardrichtlinie zu.

Hinweis: In diesem Dokument wird die Duo-Sequenz auf alle Verbindungen angewendet, sodass die Standardrichtlinie verwendet wird. Die Richtlinienzuweisung kann je nach Anforderungen variieren.

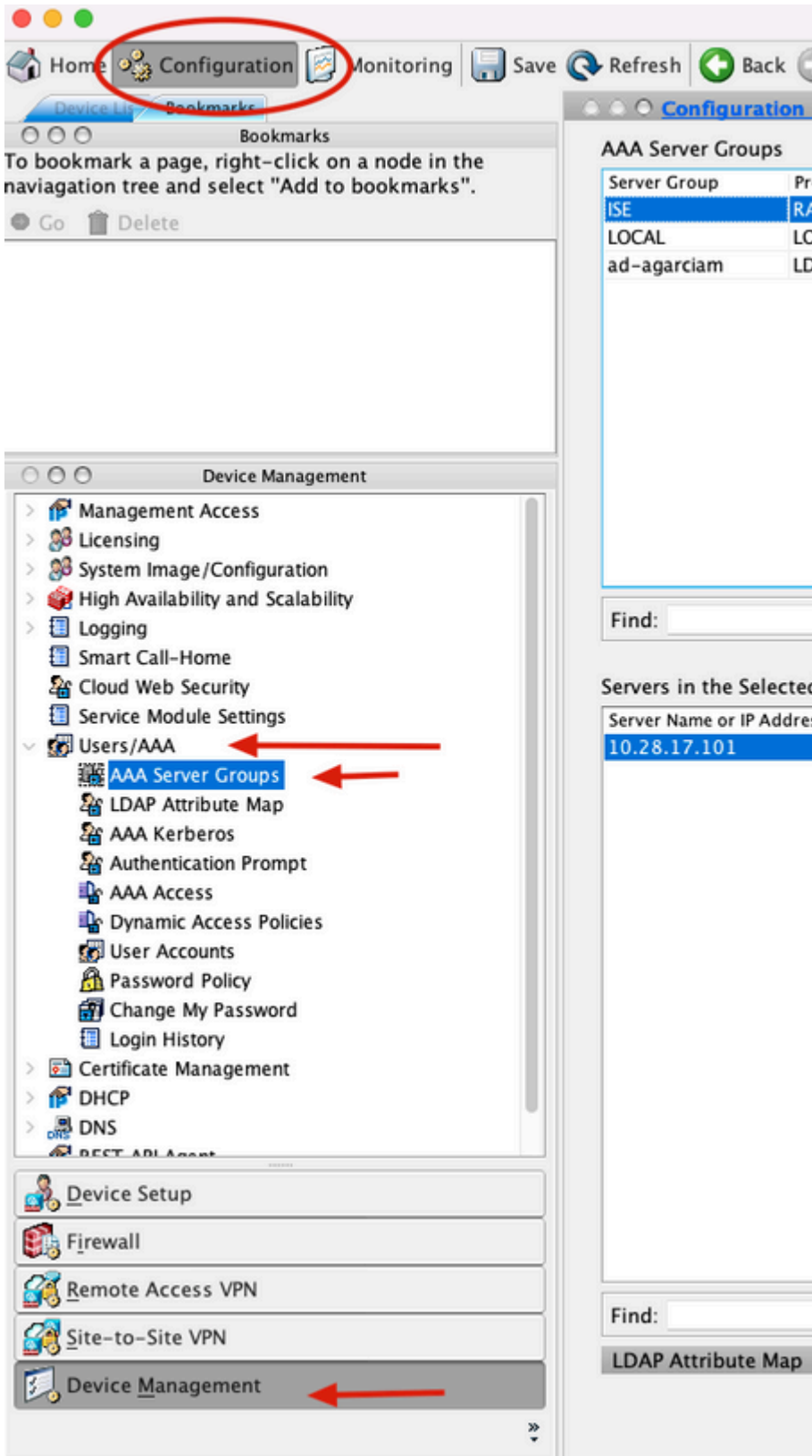
Policy Sets

Status	Policy Set Name	Description	Conditions
✓			Radius-User-Name EQUALS isevpn
✓			Radius-NAS-Port-Type EQUALS Virtual
✓	Default	Default policy set	



Konfiguration von Cisco ASA RADIUS/ISE

1. Konfigurieren Sie den ISE RADIUS-Server unter AAA-Servergruppen. Navigieren Sie zu **Konfiguration**, klicken Sie dann auf **Geräteverwaltung**, und erweitern Sie den Abschnitt **Benutzer/AAA**, und wählen Sie **AAA-Servergruppen** aus.



2. Klicken Sie im Bereich AAA-Servergruppen auf **Hinzufügen**.

The screenshot shows the Cisco configuration interface for AAA Server Groups. The breadcrumb navigation is Configuration > Device Management > Users/AAA > AAA Server Groups. The main area displays a table with columns: Server Group, Protocol, Accounting Mode, Reactivation Mode, Dead Time, and Max Failed Attempts. The 'Add' button is circled in red. Below the table is a search bar with a 'Find:' input, a 'Match Case' checkbox, and navigation arrows. The bottom section is titled 'Servers in the Selected Group' and contains a table with columns: Server Name or IP Address, Interface, and Timeout. To the right of this table are buttons for Add, Edit, Delete, Move Up, Move Down, and Test.

3. Wählen Sie den Namen der Servergruppe aus, und geben Sie **RADIUS** als Protokoll an, das verwendet werden soll. Klicken Sie anschließend auf **OK**.

Add AAA Server Group

AAA Server Group: ISE

Protocol: RADIUS

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

Enable interim accounting update
 Update Interval: 24 Hours

Enable Active Directory Agent mode

ISE Policy Enforcement

Enable dynamic authorization
Dynamic Authorization Port: 1700

Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

Help Cancel OK

5. Wählen Sie Ihre neue Servergruppe aus, und klicken Sie unter **Server im Bereich Ausgewählte Gruppe** auf **Hinzufügen**, wie im Bild gezeigt.

Configuration > Device Management > Users/AAA > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ISE	RADIUS	Single	Depletion	10	3
LOCAL	LOCAL			10	4

Find: Match Case

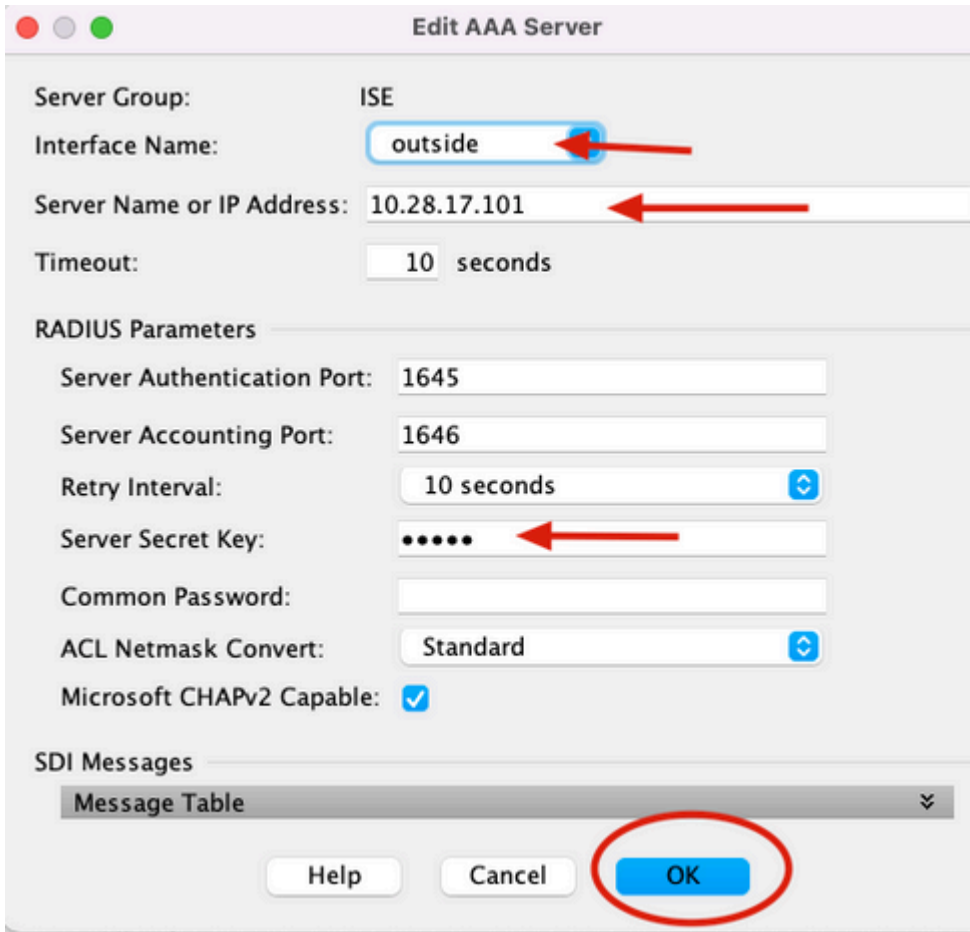
Servers in the Selected Group

Server Name or IP Address	Interface	Timeout

Buttons: Add, Edit, Delete, Move Up, Move Down

6. Wählen Sie im Fenster **AAA-Server bearbeiten** den Schnittstellennamen aus, geben Sie die IP-Adresse des ISE-Servers an, geben Sie den RADIUS-Geheimschlüssel ein, und klicken Sie auf **OK**.

Hinweis: Alle diese Informationen müssen mit den Informationen übereinstimmen, die auf dem Duo Authentifizierungsproxy-Manager angegeben sind.



CLI-Konfiguration.

```

aaa-server ISE protocol radius
dynamic-authorization
aaa-server ISE (outside) host 10.28.17.101
key *****

```

Konfiguration des Cisco ASA Remote Access VPN

```
ip local pool agarciam-pool 192.168.17.1-192.168.17.100 mask 255.255.255.0
```

```

group-policy DUO internal
group-policy DUO attributes
banner value This connection is for DUO authorized users only!
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split-agarciam
address-pools value agarciam-pool

```

```

tunnel-group ISE-users type remote-access
tunnel-group ISE-users general-attributes
address-pool agarciam-pool
authentication-server-group ISE

```

```
default-group-policy DUO
tunnel-group ISE-users webvpn-attributes
group-alias ISE enable
dns-group DNS-CISCO
```

Test

1. Öffnen Sie **AnyConnect** App auf Ihrem PC-Gerät. Geben Sie den Hostnamen des VPN ASA-Headends an, melden Sie sich mit dem Benutzer an, der für die sekundäre Duo-Authentifizierung erstellt wurde, und klicken Sie auf **OK**.



2. Sie haben eine Duo-Push-Benachrichtigung auf dem angegebenen Duo Mobilgerät erhalten.

3. Öffnen Sie die Duo Mobile App-Benachrichtigung, und klicken Sie auf **Genehmigen**.

14:41

Lunes, 14 de marzo

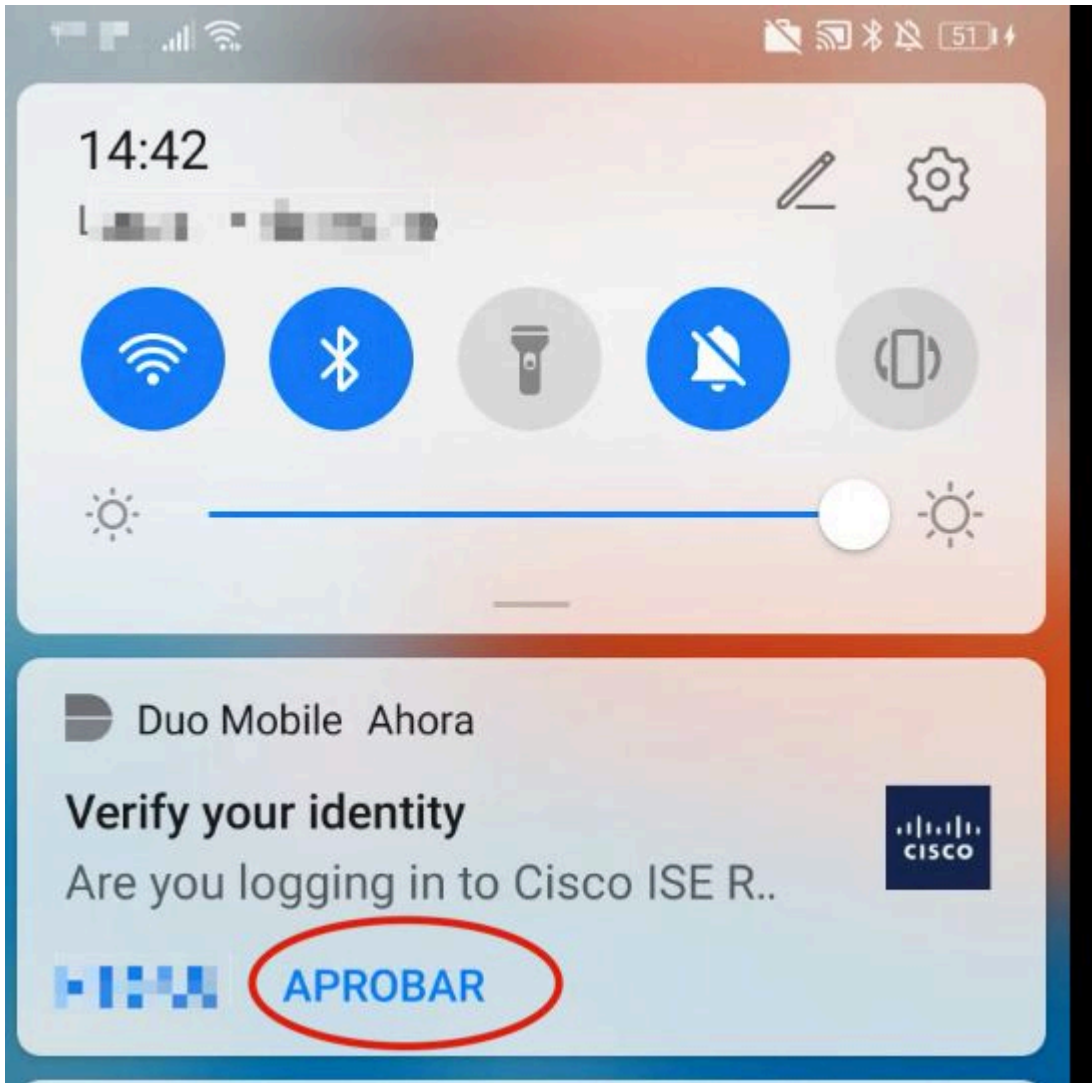


Duo Mobile Ahora

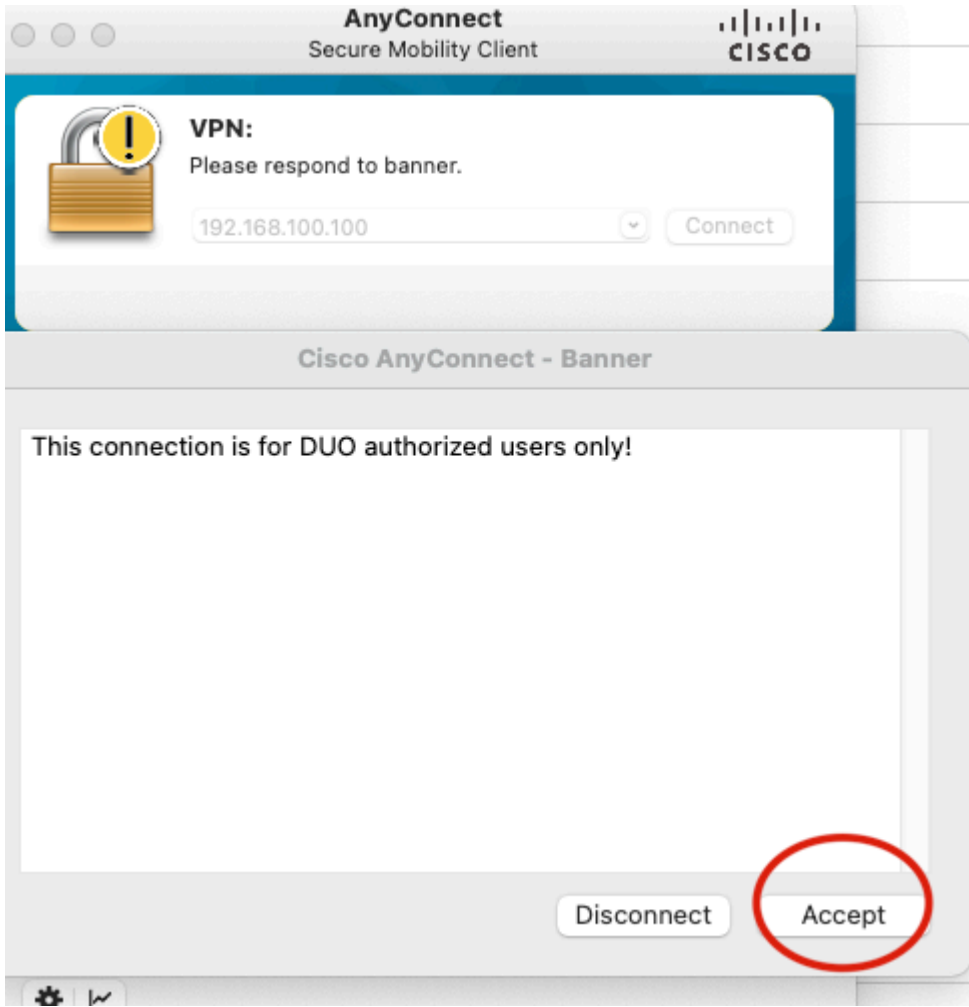
Verify your identity

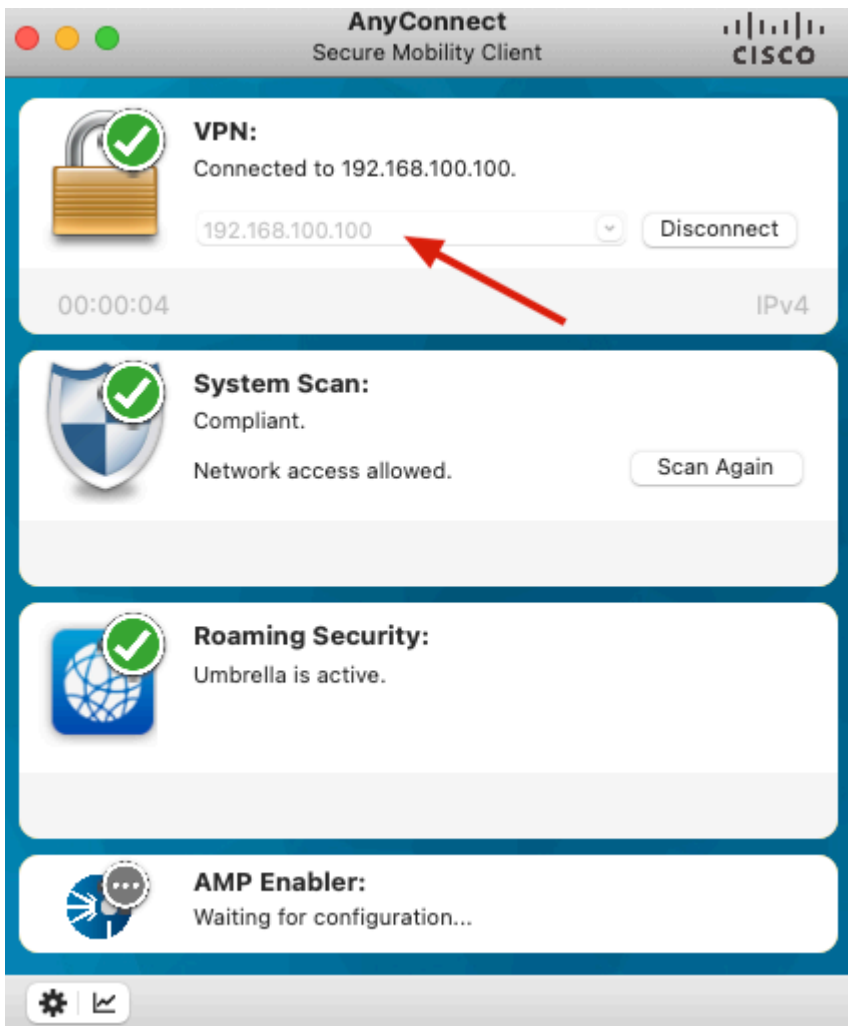
Are you logging in to Cisco ISE R..





4. Akzeptieren Sie den Banner und die Verbindung wird hergestellt.





Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Der Duo Authentifizierungsproxy wird mit einem Debug-Tool geliefert, das Fehler- und Fehlerursachen anzeigt.

Arbeitsdebugs

Hinweis: Die nächsten Informationen werden unter C:\Program Files\Duo Security Authentication Proxy\log\connectivity_tool.log gespeichert.

Output

Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes...

[info] Testing section 'main' with configuration:

```
[info] {'debug': 'True',  
       'log_max_files': '10',  
       'log_max_size': '20971520',  
       'test_connectivity_on_startup': 'true'}
```

[info] There are no configuration problems

[info] -----

[info] Testing section 'ad_client' with configuration:

```
[info] {'debug': 'True',  
       'host': '10.28.17.107',  
       'search_dn': 'DC=agarciam,DC=cisco',  
       'service_account_password': '****',  
       'service_account_username': 'Administrator'}
```

[info] There are no configuration problems

[info] -----

[info] Testing section 'radius_server_auto' with configuration:

```
[info] {'api_host': '10.28.17.107',  
       'client': 'ad_client',  
       'debug': 'True',  
       'failmode': 'safe',  
       'ikey': 'XXXXXXXXXXXXXXXXXXXX',  
       'port': '1812',  
       'radius_ip_1': '10.28.17.101',  
       'radius_secret_1': '****',  
       'skey': '****[40]'}
```

[info] There are no configuration problems

[info] Testing section 'main' with configuration:

```
[info] {'debug': 'True',  
       'log_max_files': '10',  
       'log_max_size': '20971520',  
       'test_connectivity_on_startup': 'true'}
```

[info] There are no connectivity problems with the section.

```

[info] There are no connectivity problems with the section.
[info] -----
[info] Testing section 'ad_client' with configuration:
[info] {'debug': 'True',
       'host': '10.28.17.107',
       'search_dn': 'DC=agarciam,DC=cisco',
       'service_account_password': '*****',
       'service_account_username': 'Administrator'}
[info] The LDAP Client section has no connectivity issues.
[info] -----
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': 'radius-server-auto.radiusserver.com',
       'client': 'ad_client',
       'debug': 'True',
       'failmode': 'safe',
       'ikey': 'XXXXXXXXXXXXXXXXXXXX',
       'port': '1812',
       'radius_ip_1': '10.28.17.101',
       'radius_secret_1': '*****',
       'skey': '*****[40]'}
[info] The RADIUS Server has no connectivity problems.
[info] -----
[info] SUMMARY
[info] No issues detected

```

1. Verbindungsprobleme, falsche IP, nicht auflösbarer FQDN/Hostname in der Active Directory-Konfiguration.

```

[ad_client]
host=10.28.17.106
service_account_username=Administrator
service_account_password=XXXXXXXXXX
search_dn=DC=agarciam,DC=cisco

```

```

Output

'host': '10.28.17.106',
'search_dn': 'DC=agarciam,DC=cisco',
'service_account_password': '*****',
'service_account_username': 'Administrator'}
[warn] The LDAP Client section has connectivity problems.
[warn] The LDAP host clear connection to 10.28.17.106:389 has
connectivity problems.
[error] The Auth Proxy was not able to establish a connection to 10
.28.17.106:389.

```

2. Falsches Kennwort für Administratorbenutzer in Active Directory.

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!@#%&'()* ←
search_dn=DC=agarciam,DC=cisco
```

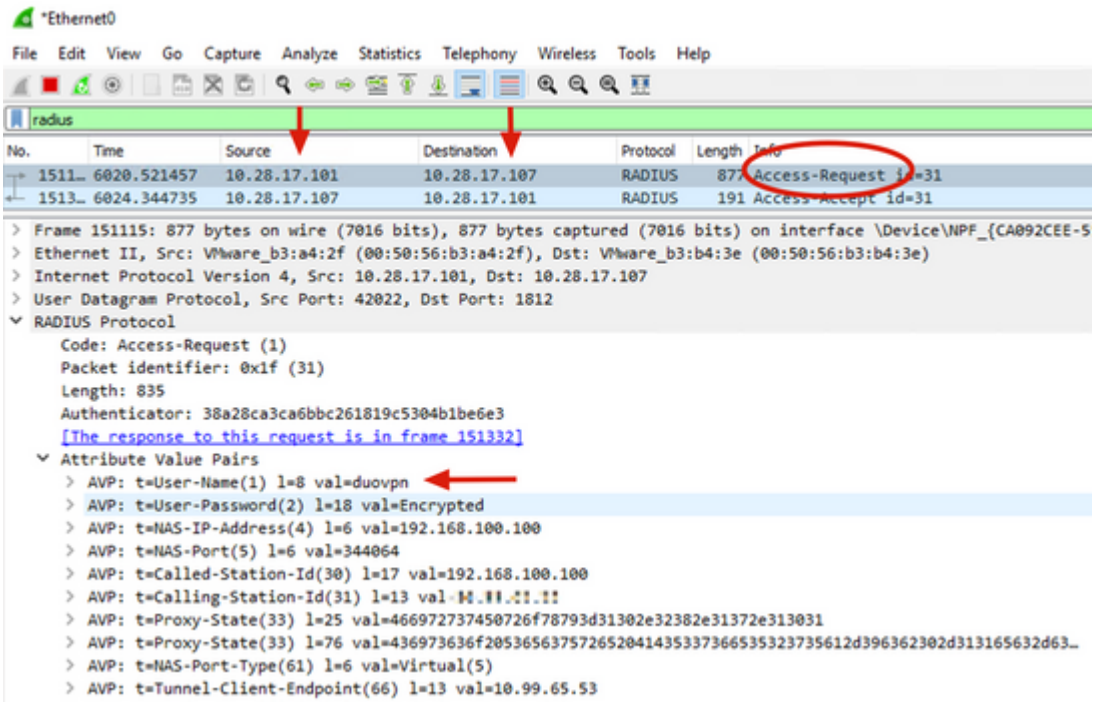
Debuggen.

```
[info] The Auth Proxy was able to establish a connection to 10.28.17.107:389.
[info] The Auth Proxy was able to establish an LDAP connection to 10.28.17.107:389.
[error] The Auth Proxy was unable to bind as Administrator.
[error] Please ensure that the provided service account credentials are correct.
[debug] Exception: invalidCredentials: 8009030C: LdapErr: DSID -0C090516, comment: AcceptSecurityContext error, data 52e, v3839
[warn] The Auth Proxy did not run the search check because of the problem(s) with the bind check. Resolve that issue and rerun the tester.
```

3. Falsche Basisdomäne

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!@#%&'()*
search_dn=DC=agarciam,DC=ciscoo ←
```

Debuggen.

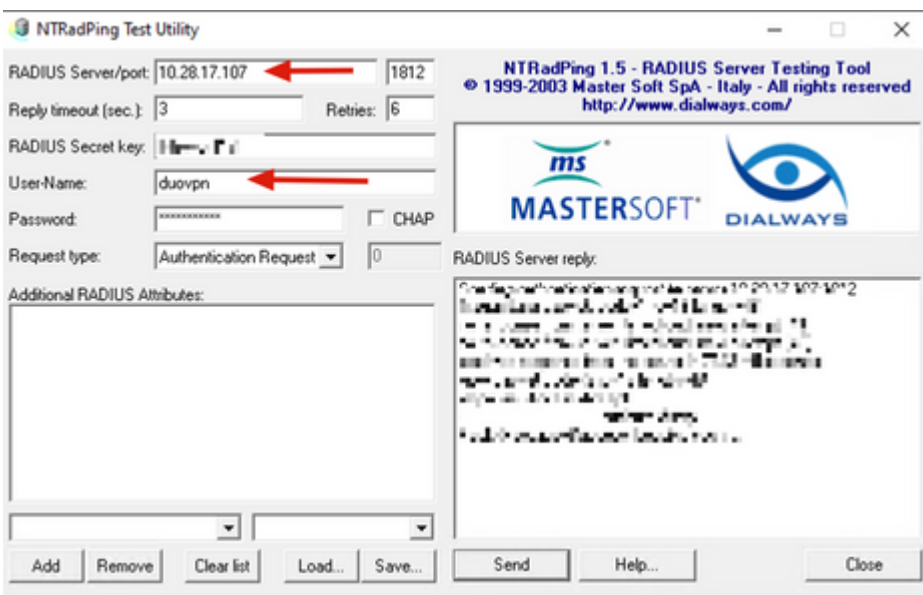


6. Um zu bestätigen, dass der Duo Authentication Proxy-Server funktioniert, stellt Duo das Tool [NTRadPing](#) zur Verfügung, um Access-Request-Pakete und die Antwort mit Duo zu simulieren.

6.1 Installieren Sie NTRadPing auf einem anderen PC, und generieren Sie Datenverkehr.

Hinweis: In diesem Beispiel wird der Windows-Computer 10.28.17.3 verwendet.

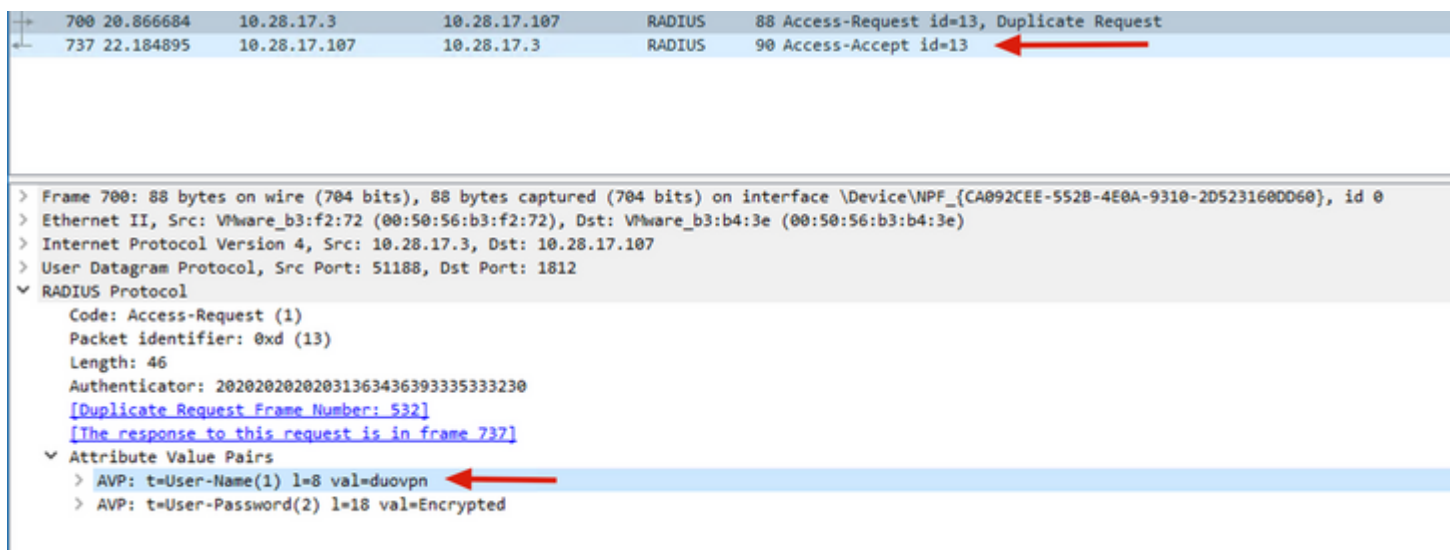
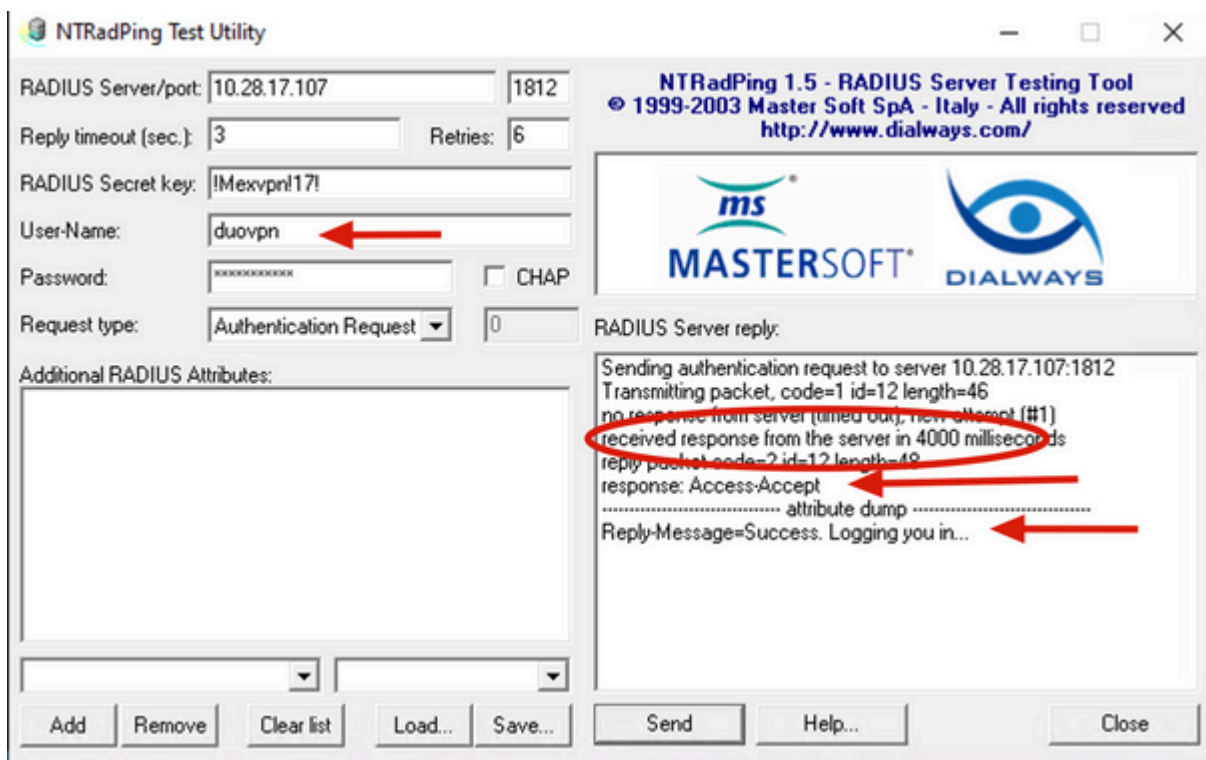
6.2 Konfigurieren Sie die Attribute, die in der ISE Radius-Konfiguration verwendet werden.



6.3 Konfigurieren Sie den Duo Authentication Proxy Manager wie folgt.

```
[radius_server_auto]
ikey=
skey=Jac3...X02
api_host=api...
radius_ip_1=10.28.17.101
radius_secret_1=!Mexv...!
radius_ip_2=10.28.17.3
radius_secret_2=!Me...
```

6.4. Navigieren Sie zu Ihrem NTRadPing-Tool, und klicken Sie auf **Senden**. Sie erhalten eine Duo-Push-Benachrichtigung auf dem zugewiesenen Mobilgerät.



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.