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

Inhalt

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

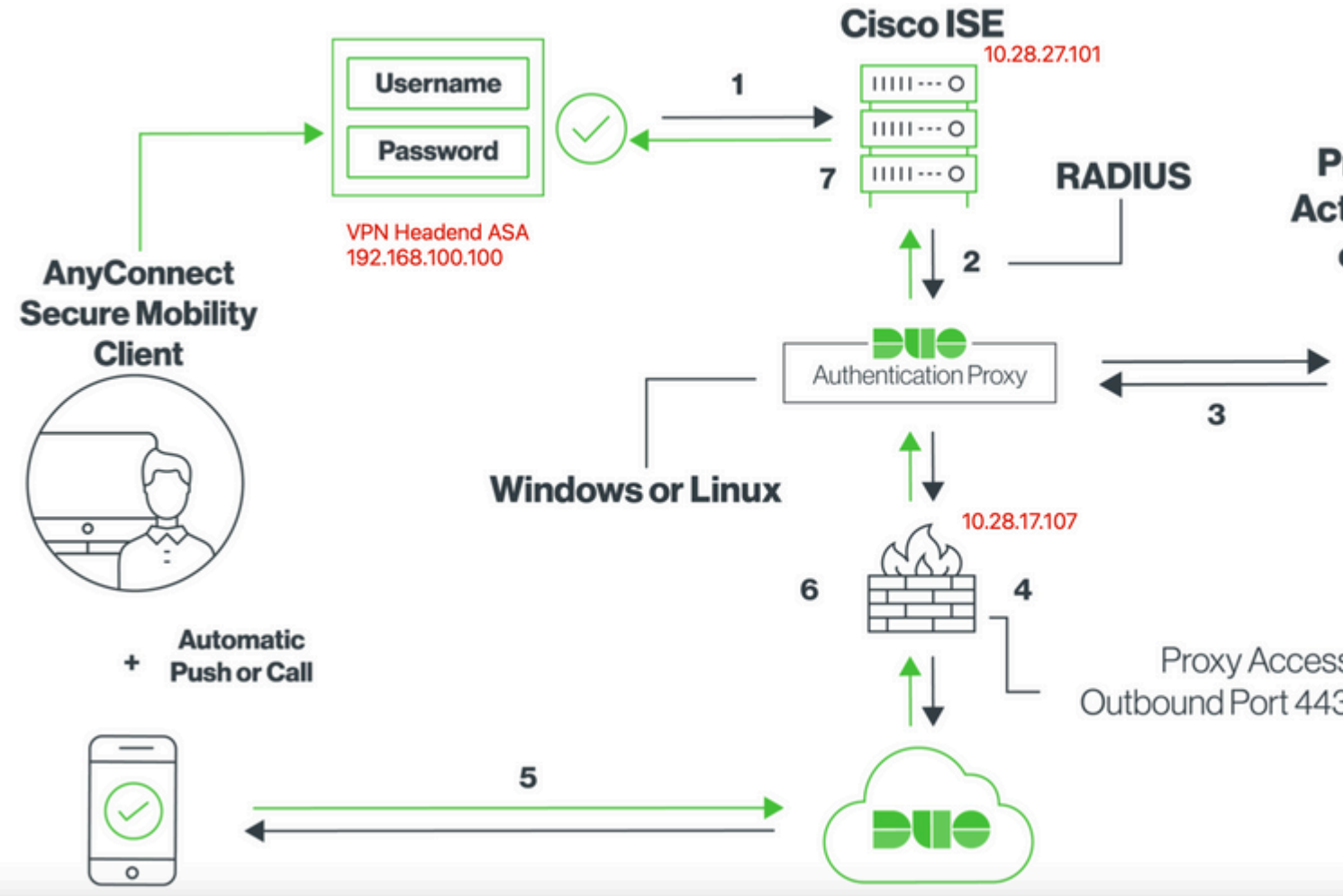
- ISE-Server 3.0
- Duo-Server
- Duo Authentifizierungsproxy-Manager

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.

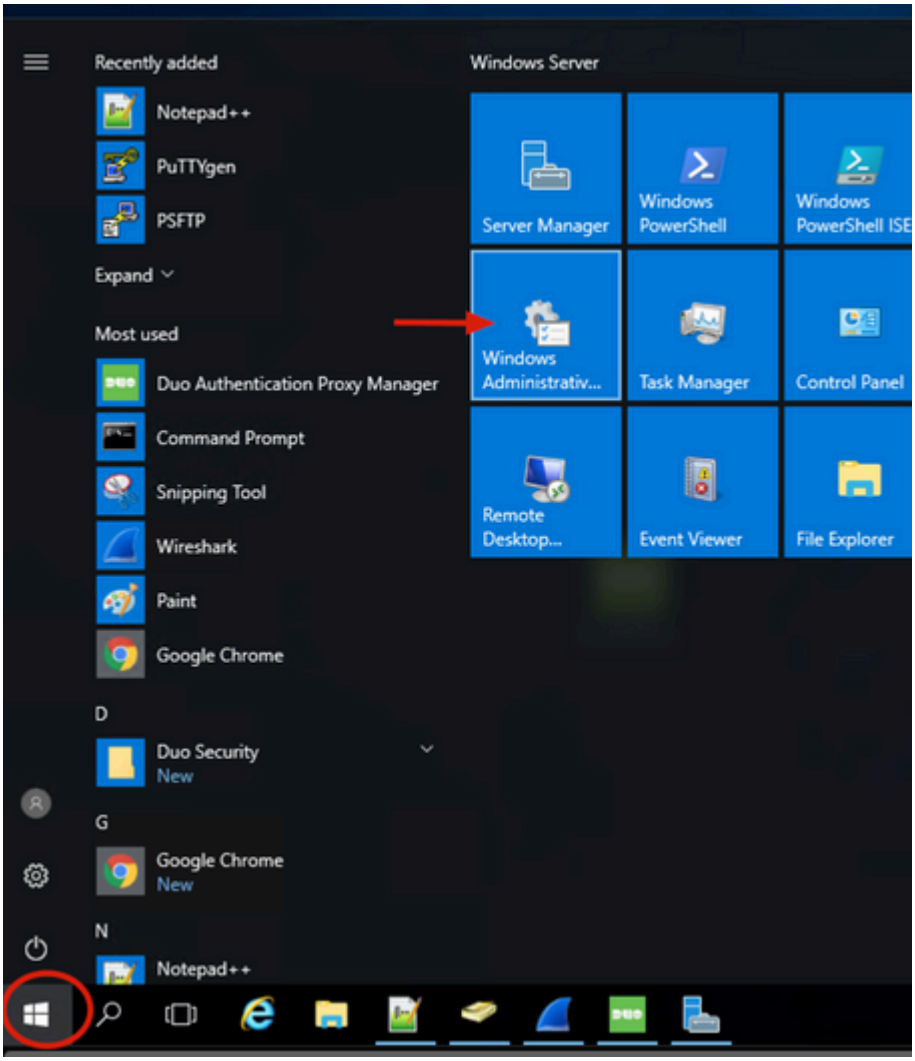
- Stammzertifizierungsstelle. Wenn LDAPS oder STARTTLS verwendet wird, ist die Stammzertifizierungsstelle zum Signieren des von LDAPS verwendeten SSL-Zertifikats erforderlich.

- 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.

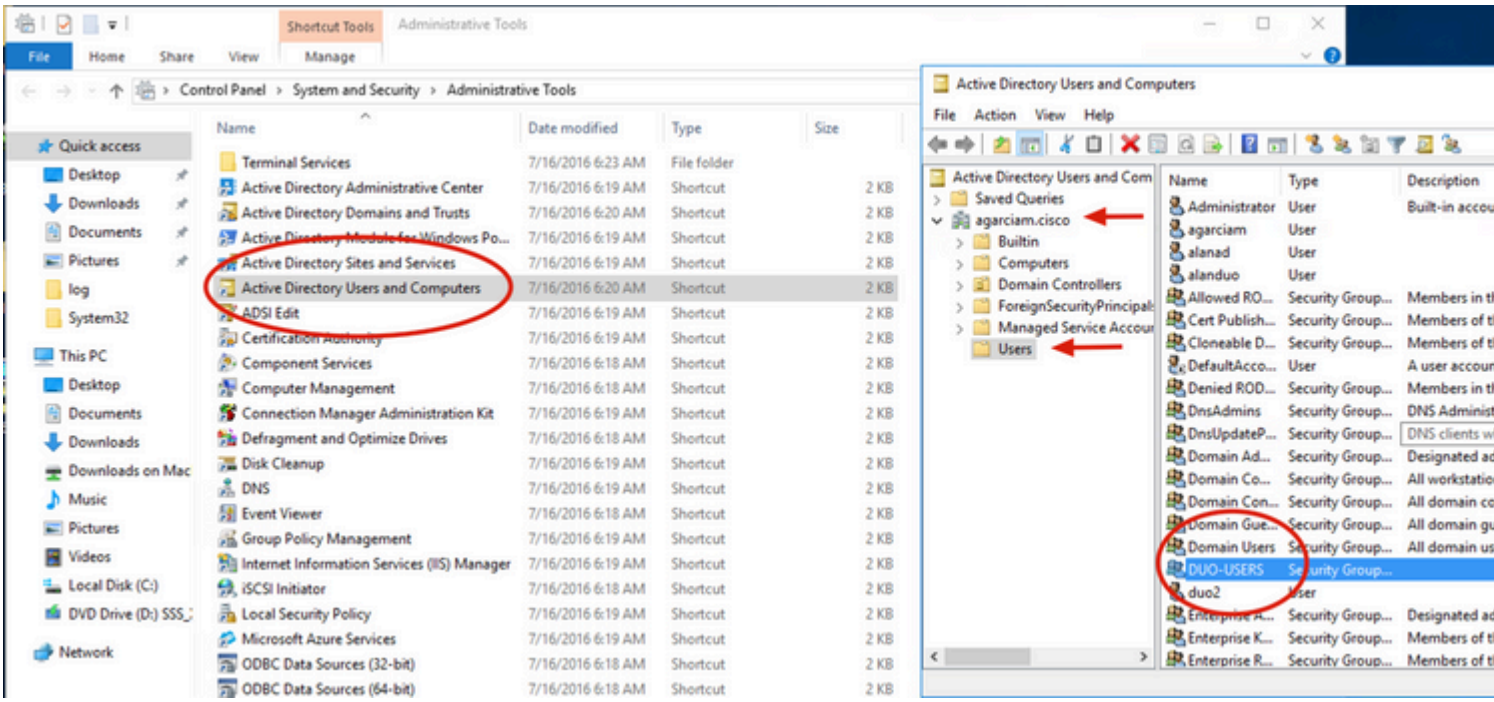
1. Um einen neuen Duo-Benutzer hinzuzufügen, navigieren Sie auf Windows Server zum **Windows**-Symbol unten links, und klicken Sie auf **Windows-Verwaltungstools,** wie im Bild dargestellt.



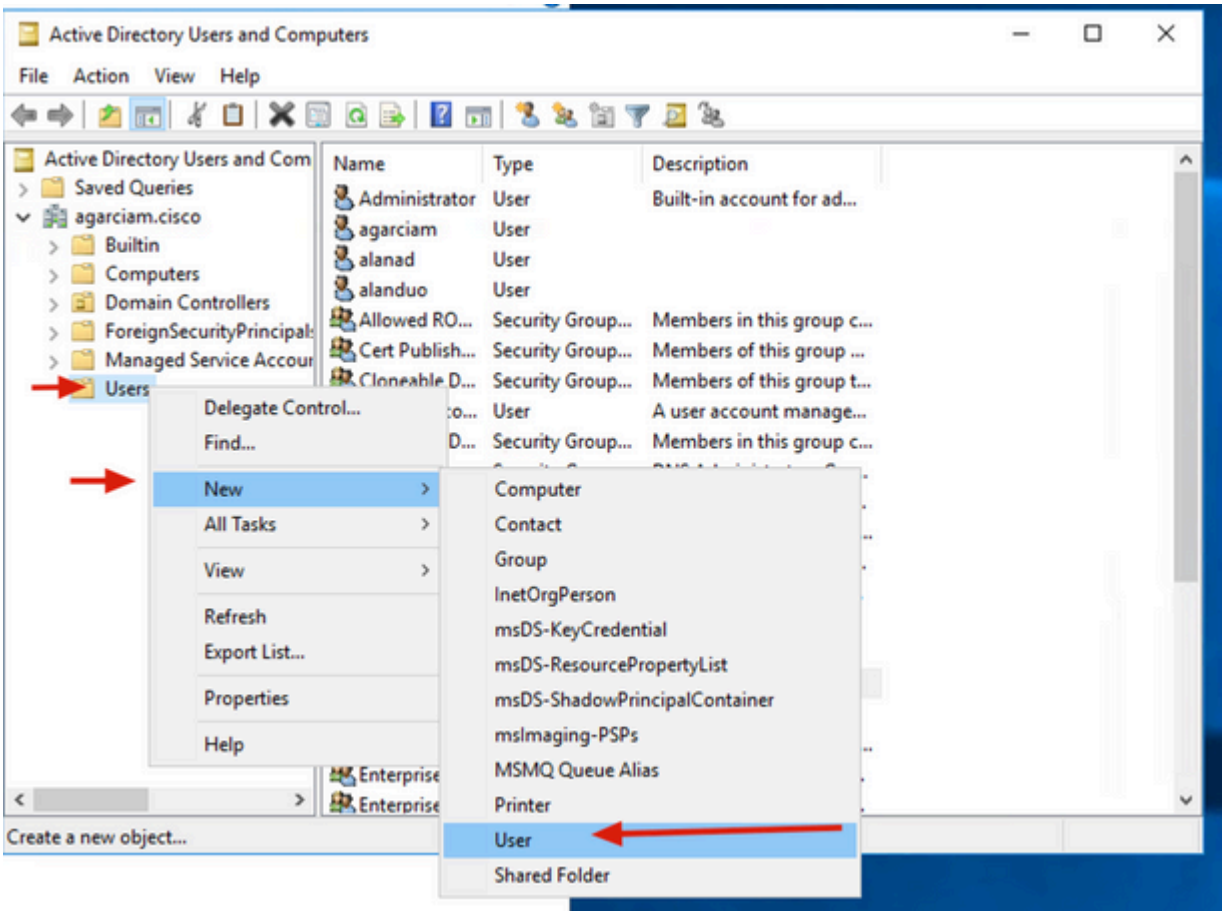
2. Navigieren Sie im Fenster Windows-Verwaltungstools zu **Active Directory-Benutzer und -Computer**.

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

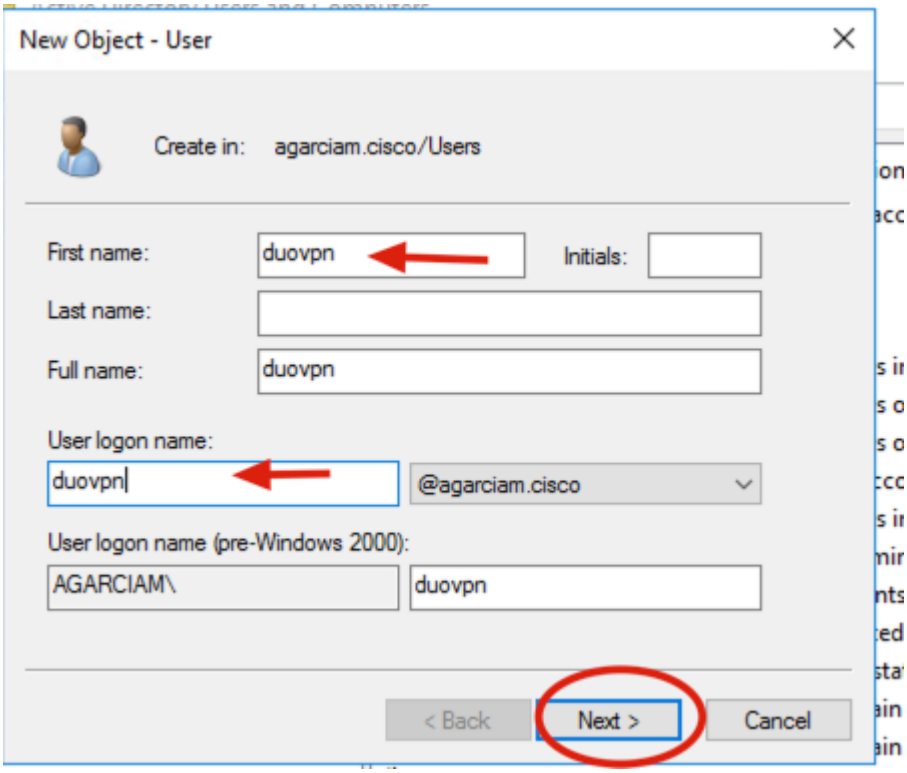
In diesem Konfigurationsbeispiel wird Duo-USERS als Zielgruppe für die sekundäre Authentifizierung verwendet.



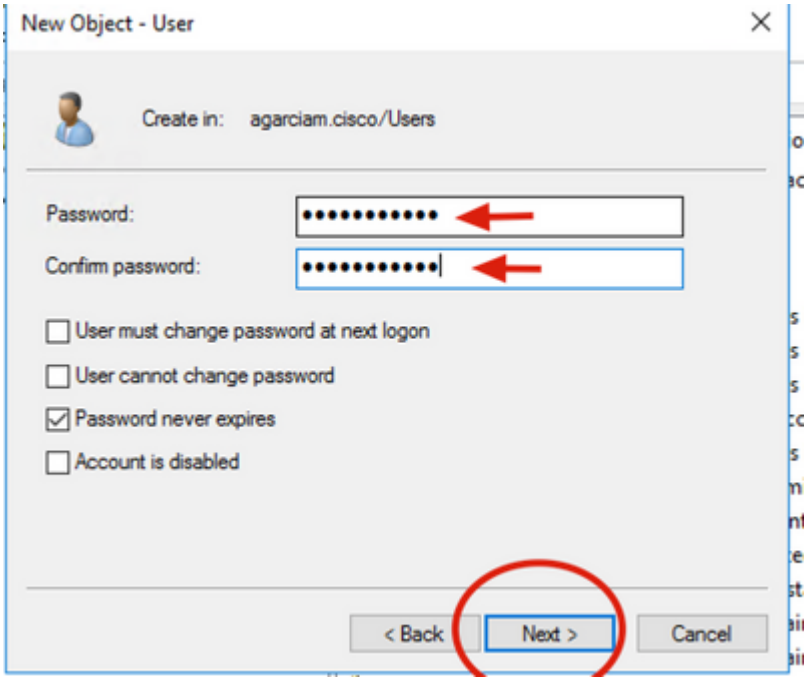
3. Klicken Sie mit der rechten Maustaste auf den Ordner **Benutzer** und wählen Sie **Neu** > **Benutzer**, wie im Bild dargestellt.



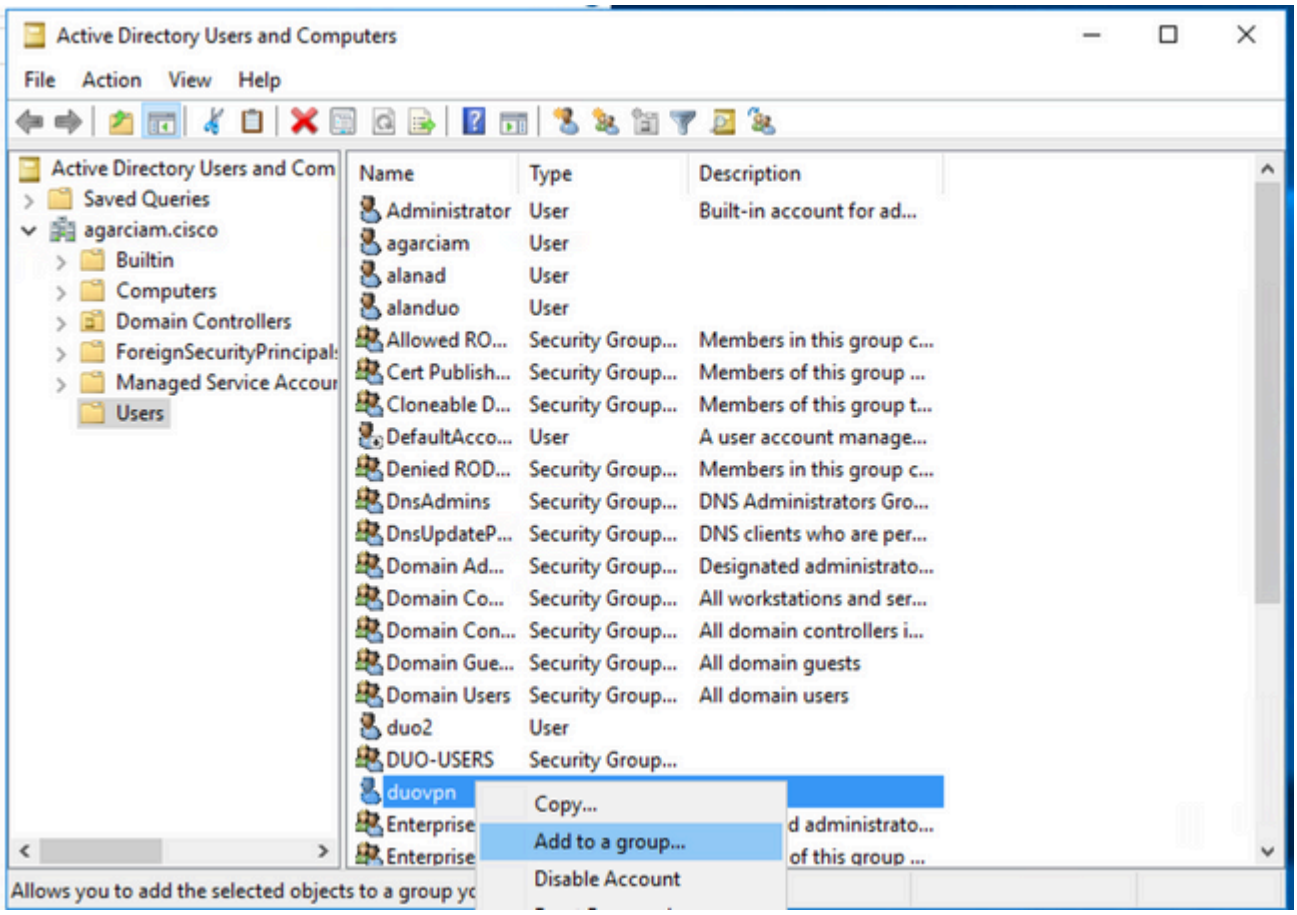
4. Geben Sie im Fenster Neues Objekt-Benutzer die Identitätsattribute für diesen neuen Benutzer an, und klicken Sie auf **Weiter**, wie im Bild dargestellt.



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

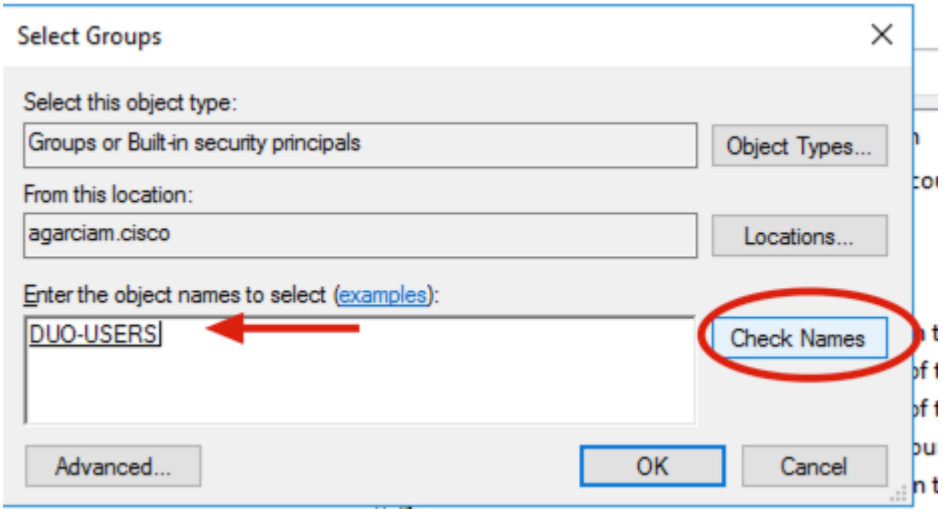


6. Weisen Sie den neuen Benutzer einer bestimmten Gruppe zu, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Zu einer Gruppe hinzufügen**, wie im Bild dargestellt.



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

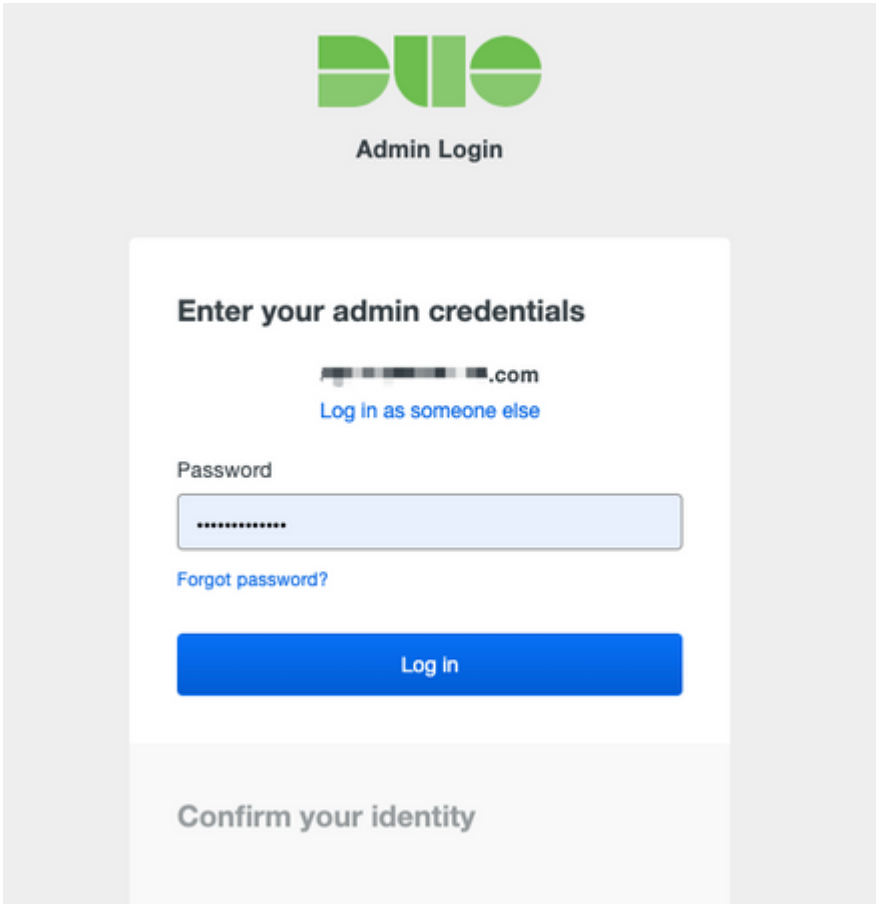
Wählen Sie dann den Namen aus, der Ihren Kriterien entspricht, und klicken Sie auf **OK**.



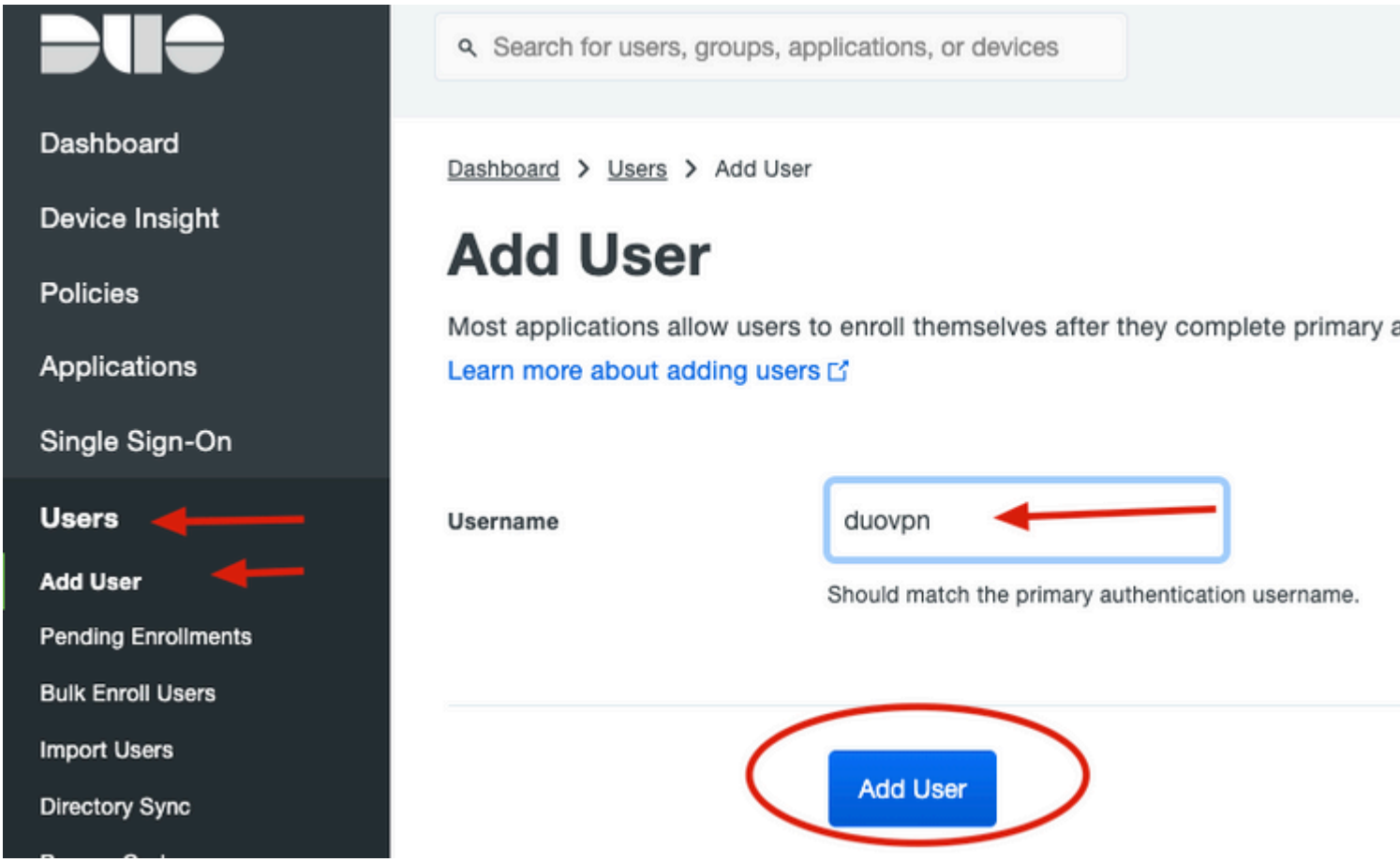
8. Dies ist der Benutzer, der in diesem Dokument als Beispiel verwendet wird.

Duo Konfigurationen

1. Melden Sie sich in Ihrem Dudo Admin Portal.



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)**.



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

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 f

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

Full name test vpn user

Email [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

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

Versioning
Core Authentication Service:
D235.6
Admin Panel:
D235.6
Read Release Notes

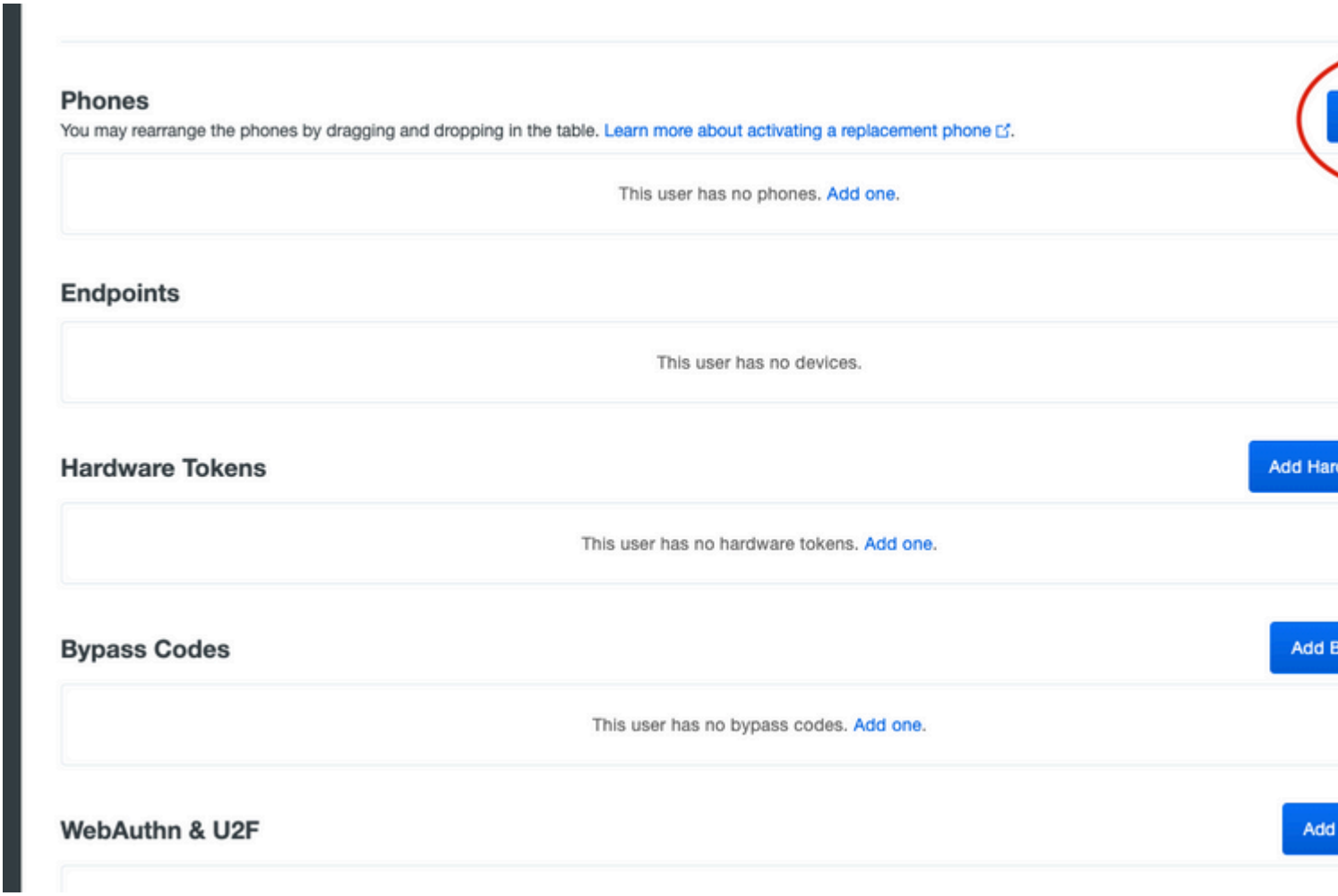
Account ID
2910-6030-53

Deployment ID
DUO63

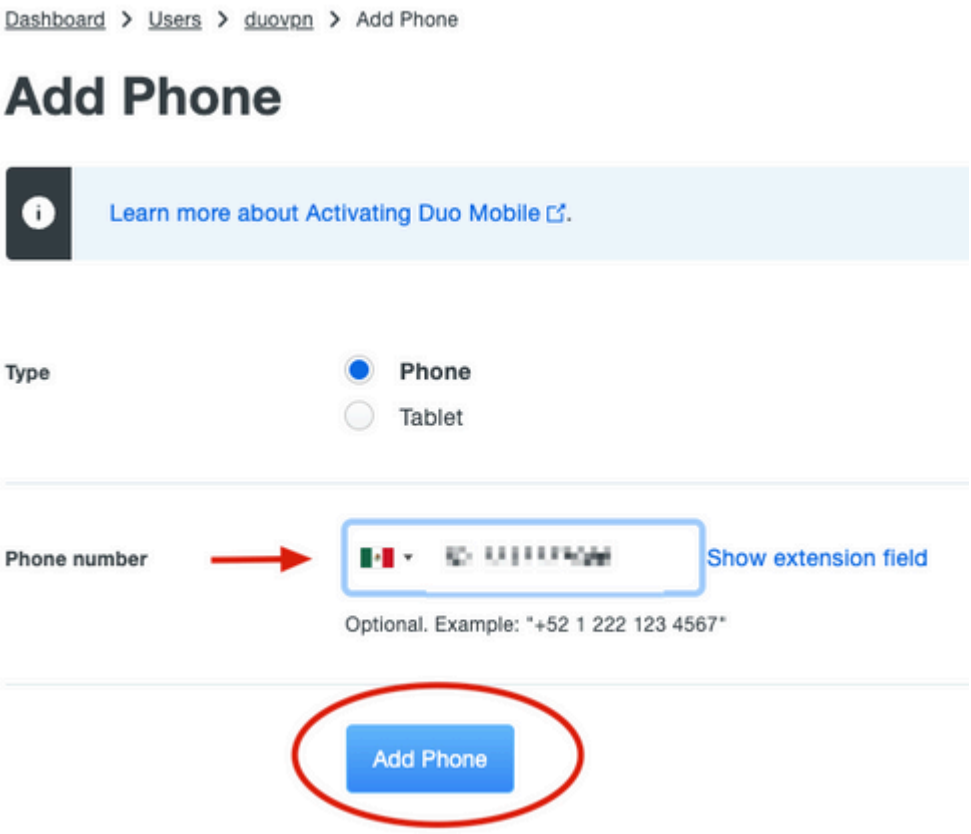
Helpful Links
Documentation
User Guide

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

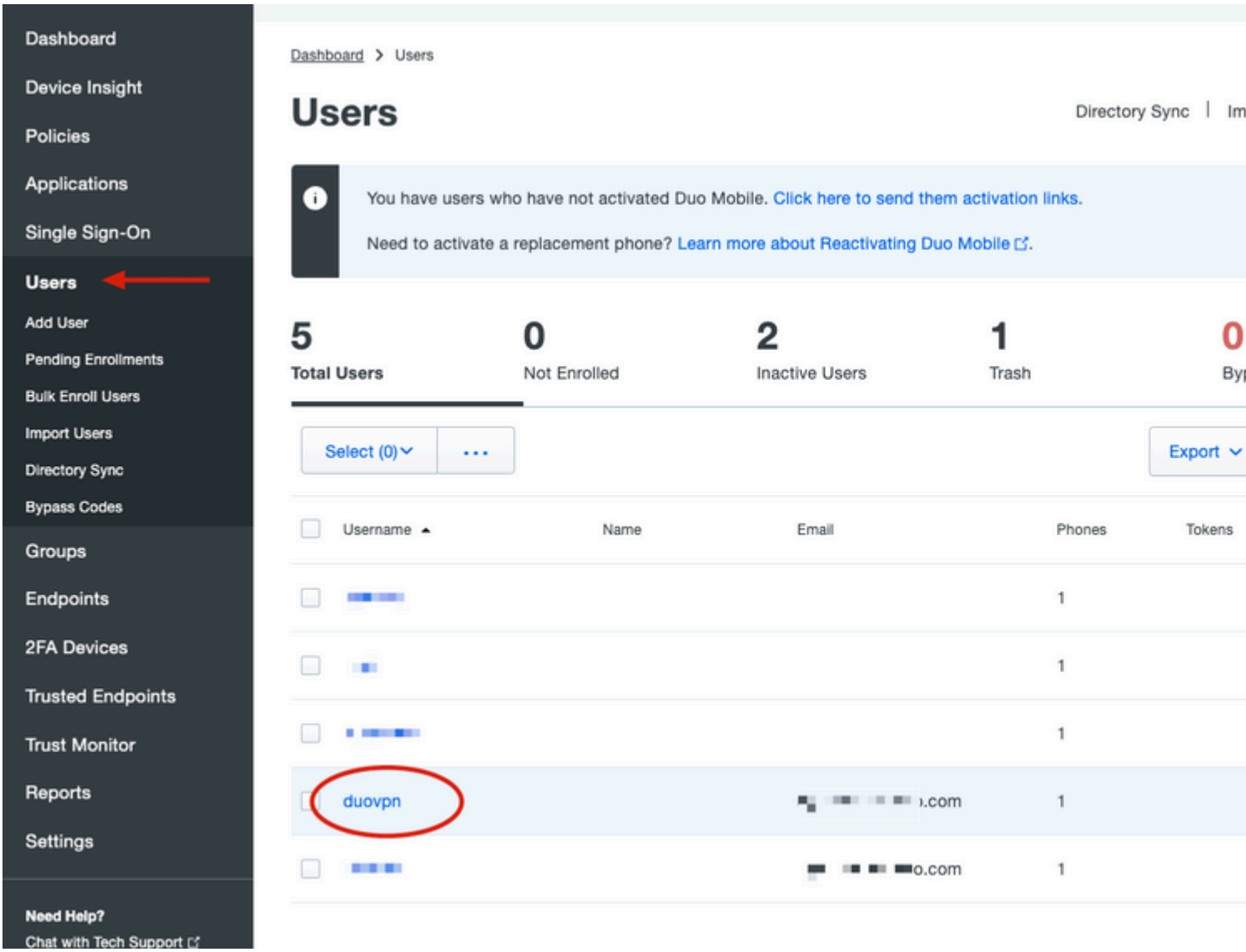
Klicken Sie auf **Telefon hinzufügen**.



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

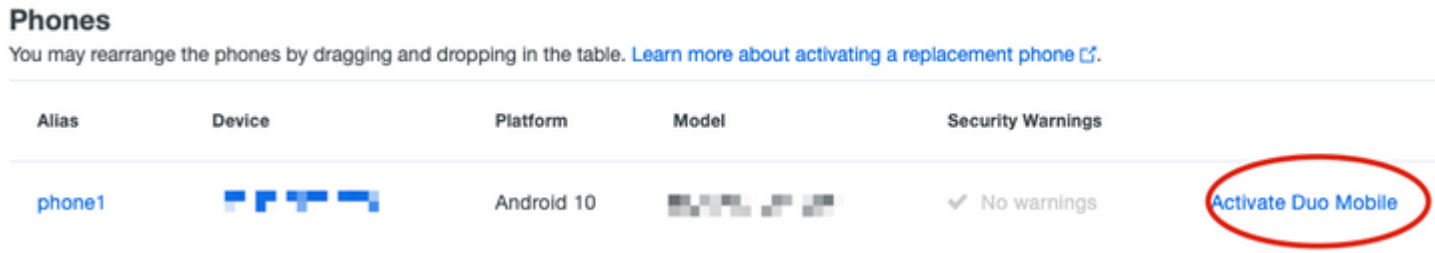


6. Navigieren Sie im linken Duo-Administrationsbereich zu **Benutzer**, und klicken Sie auf den neuen Benutzer.

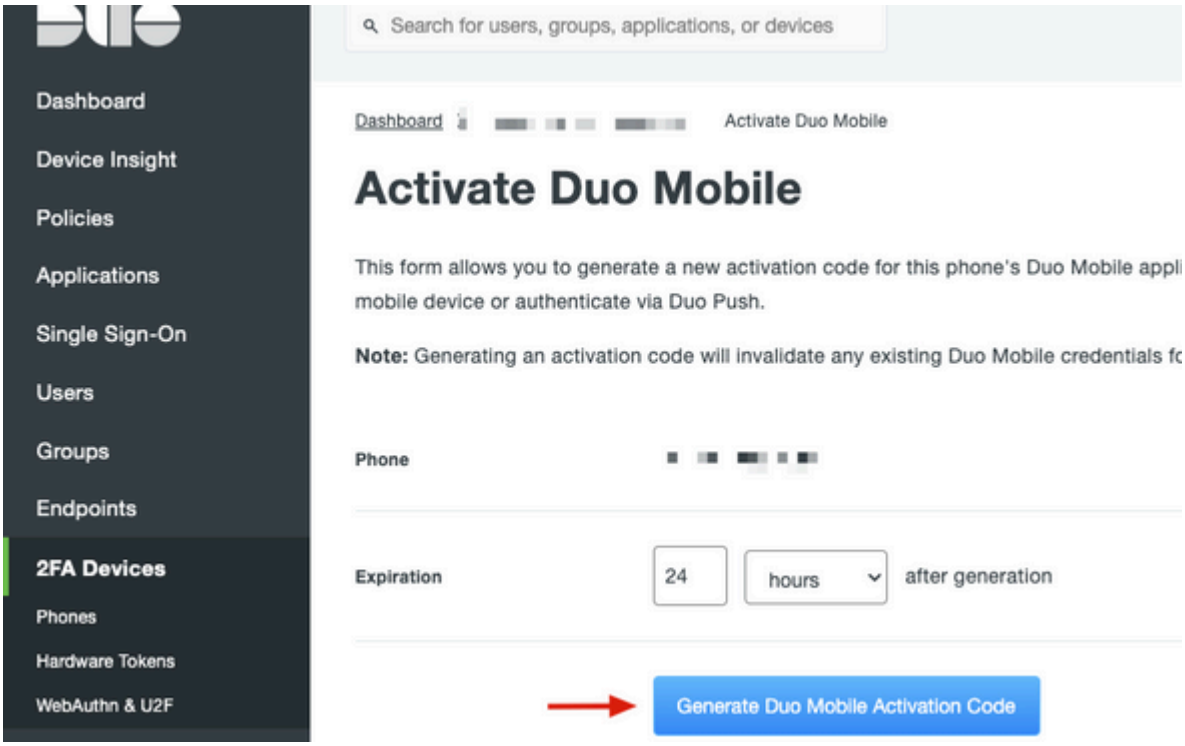


Hinweis: Falls Sie derzeit keinen Zugriff auf Ihr Telefon haben, können Sie die E-Mail-Option auswählen.

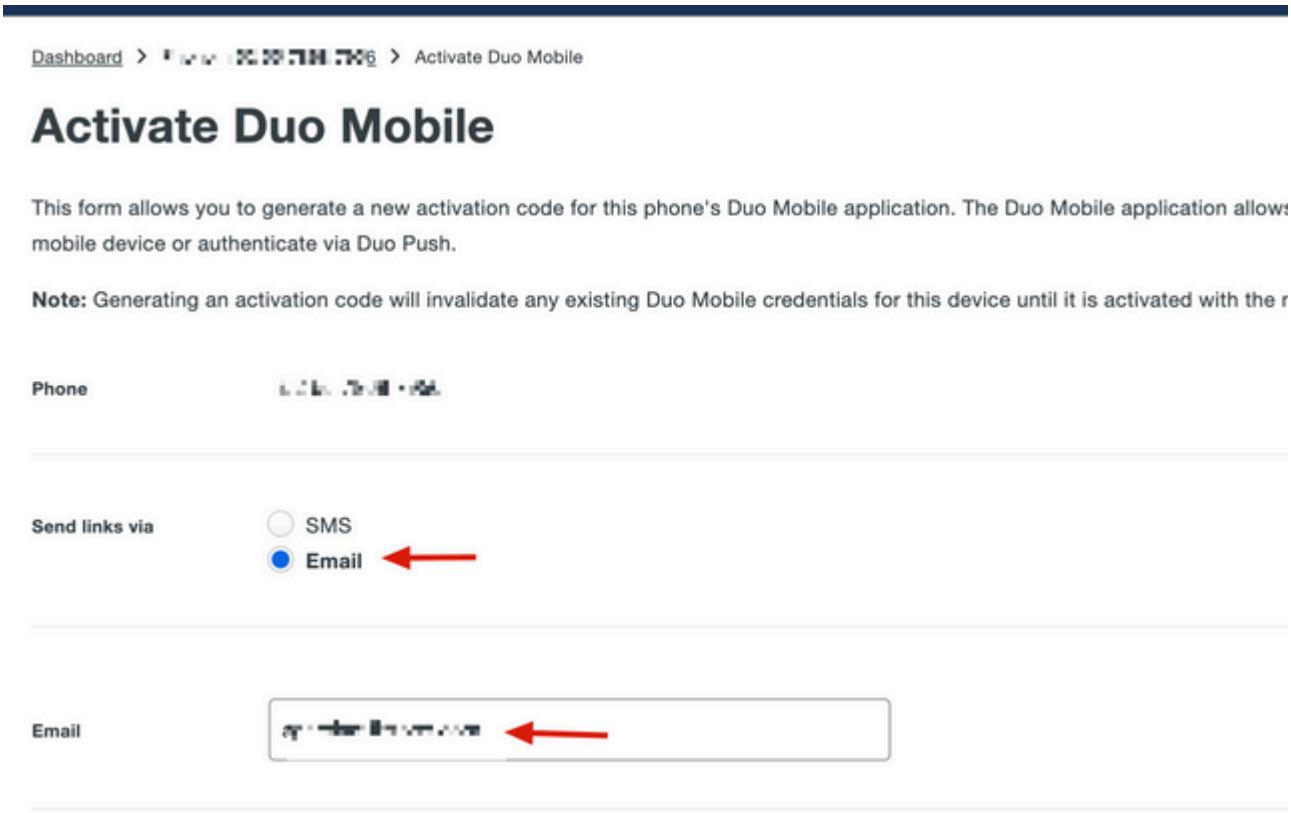
7. Navigieren Sie zum Abschnitt **Telefone**, und klicken Sie auf **Activate Duo Mobile (Duo-Mobiltelefon aktivieren)**.



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 + ır copy and paste it into Duo Mobile manually:

If you're not reading this from + n 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 Anleitungs-E-Mail.

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

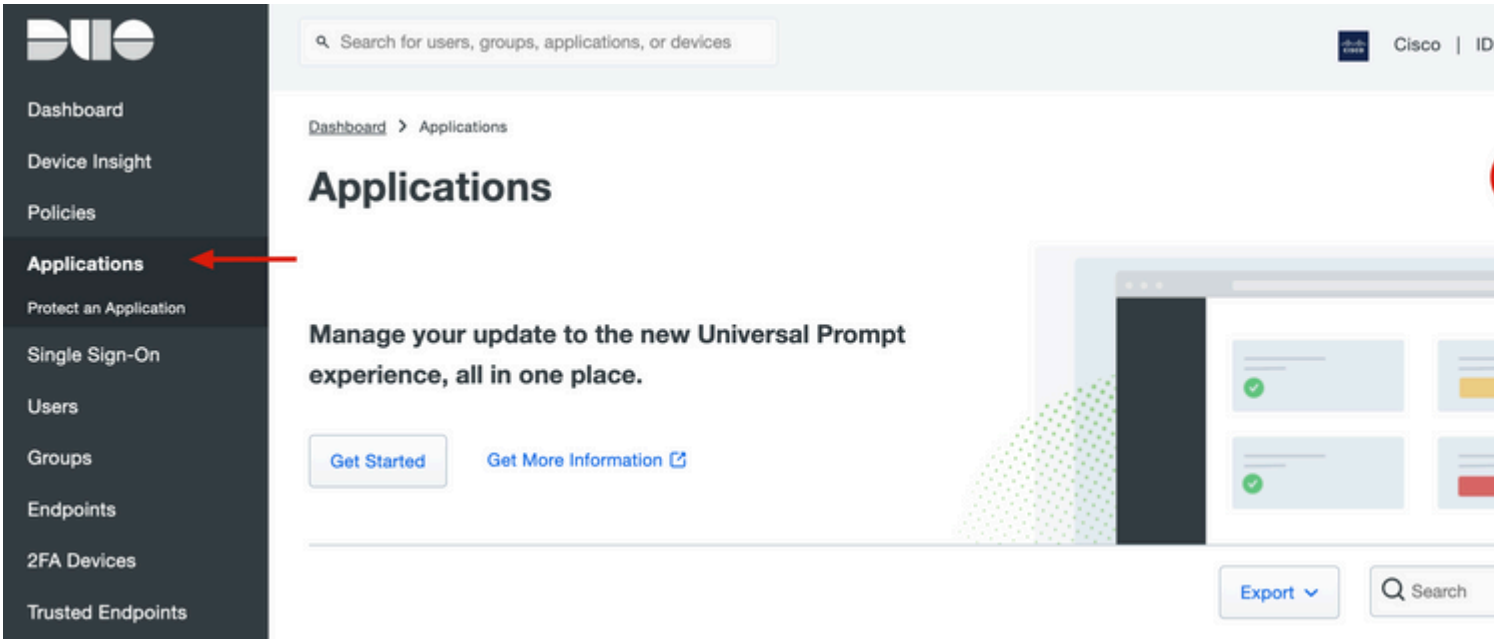
Duo Authentifizierungsproxy-Konfiguration

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

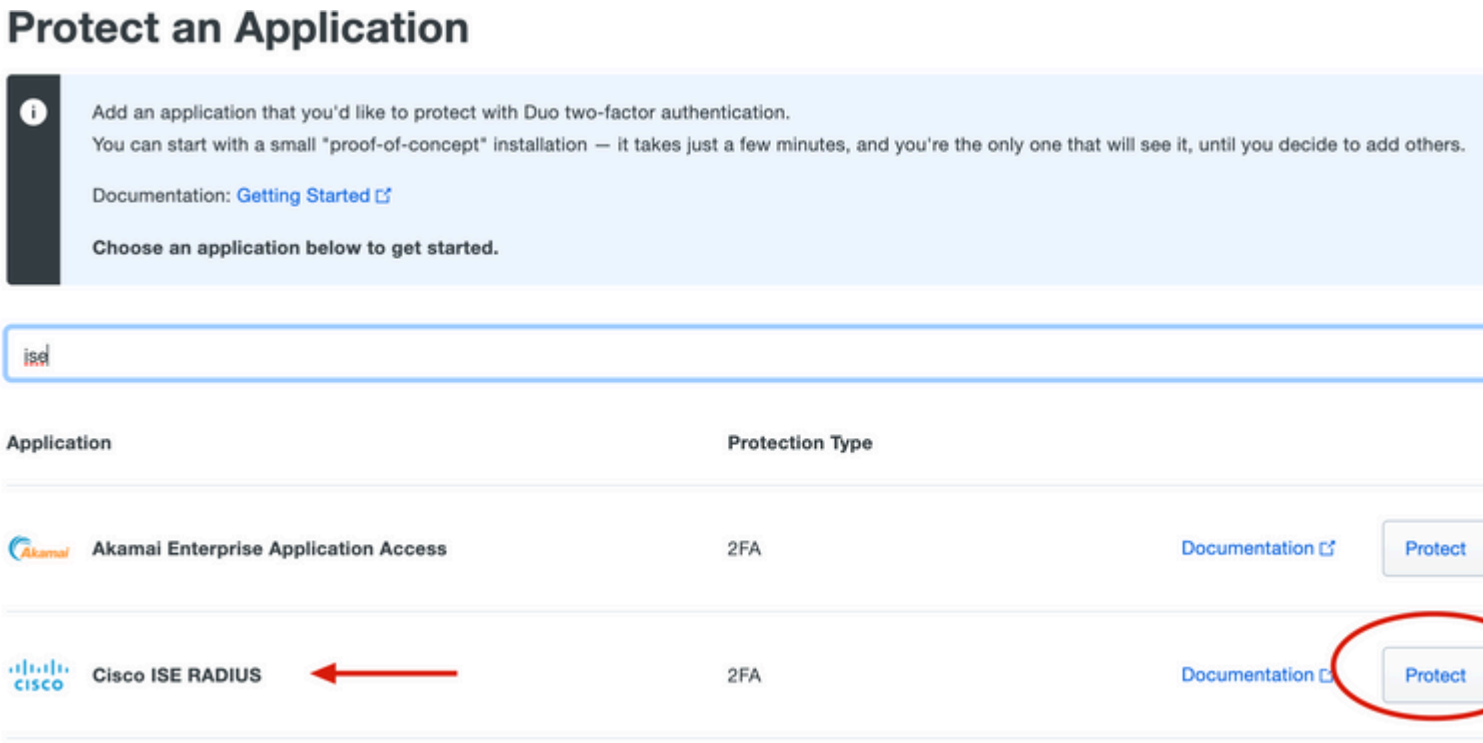
> **Hinweis**: In diesem Dokument ist der Duo Auth Proxy Manager auf demselben Windows-Server installiert, auf dem die Active Directory-Dienste gehostet werden.

---

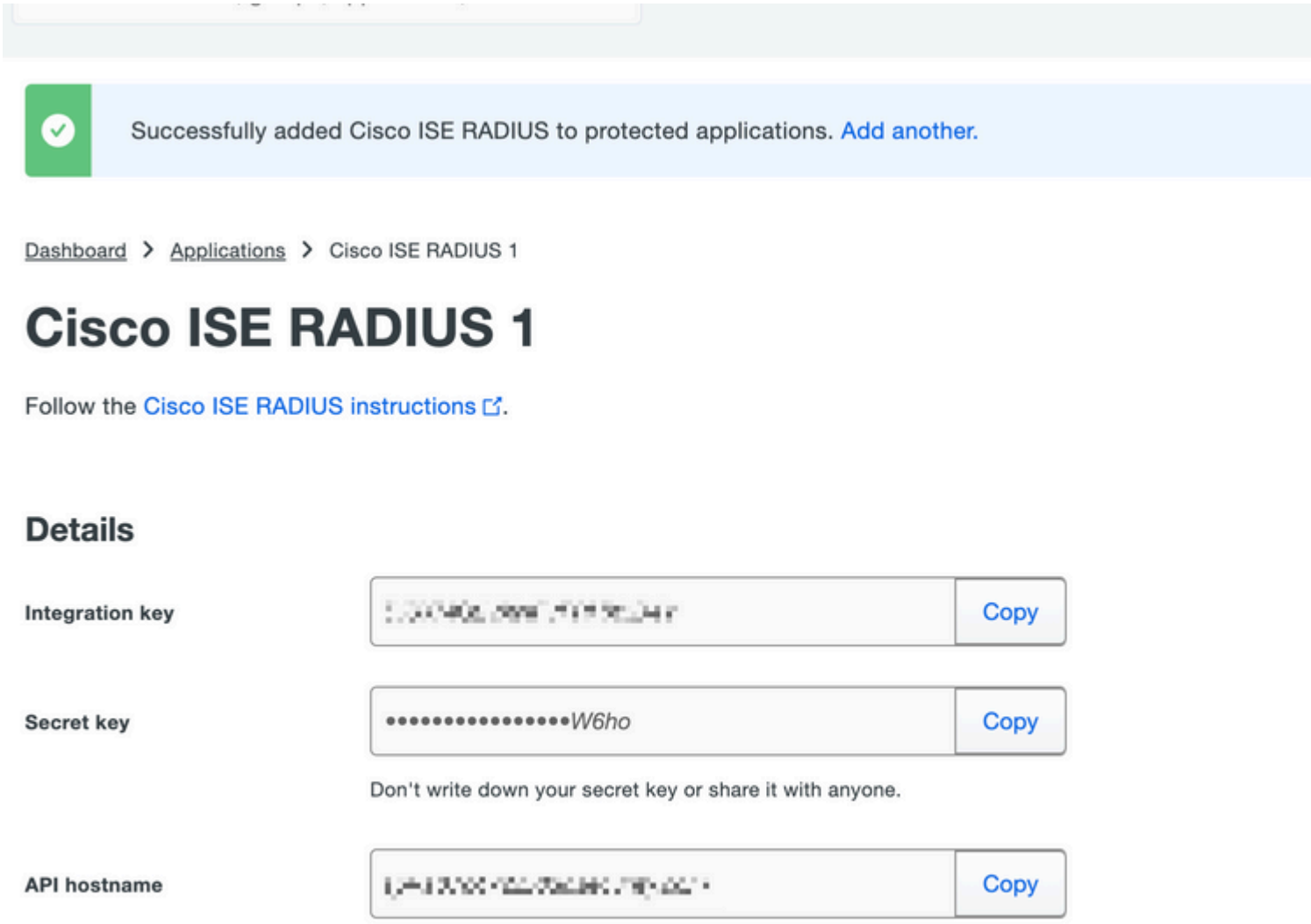
2. Navigieren Sie im Duo-Administrationsbereich zu Anwendungen**,** und klicken Sie auf **Anwendung schützen**.



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

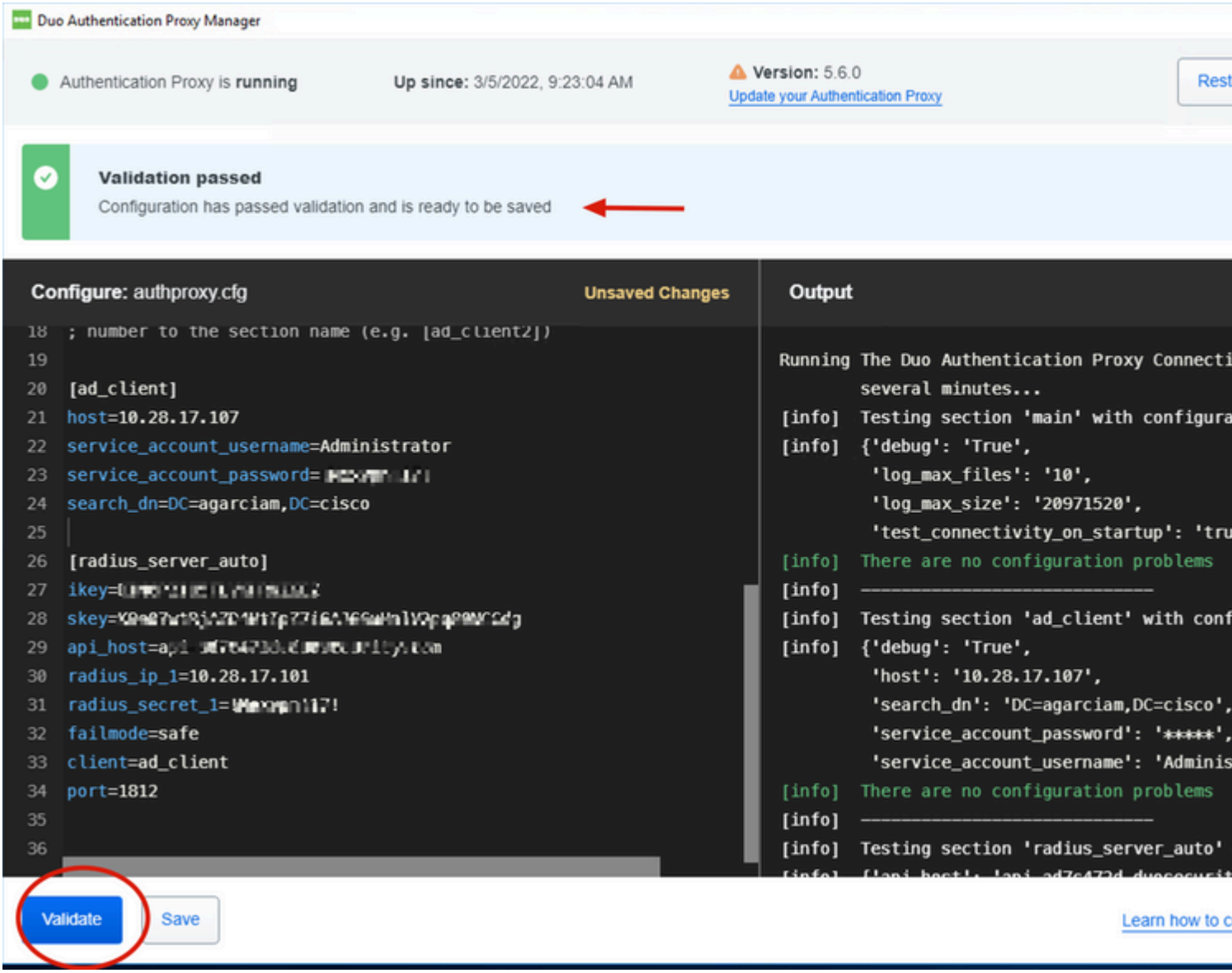


4. Kopieren Sie den Integrationsschlüssel, den Sicherheitsschlüssel und den API-Hostnamen. Sie benötigen diese Informationen für die Konfiguration des Duo-Authentifizierungsproxys.



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**.

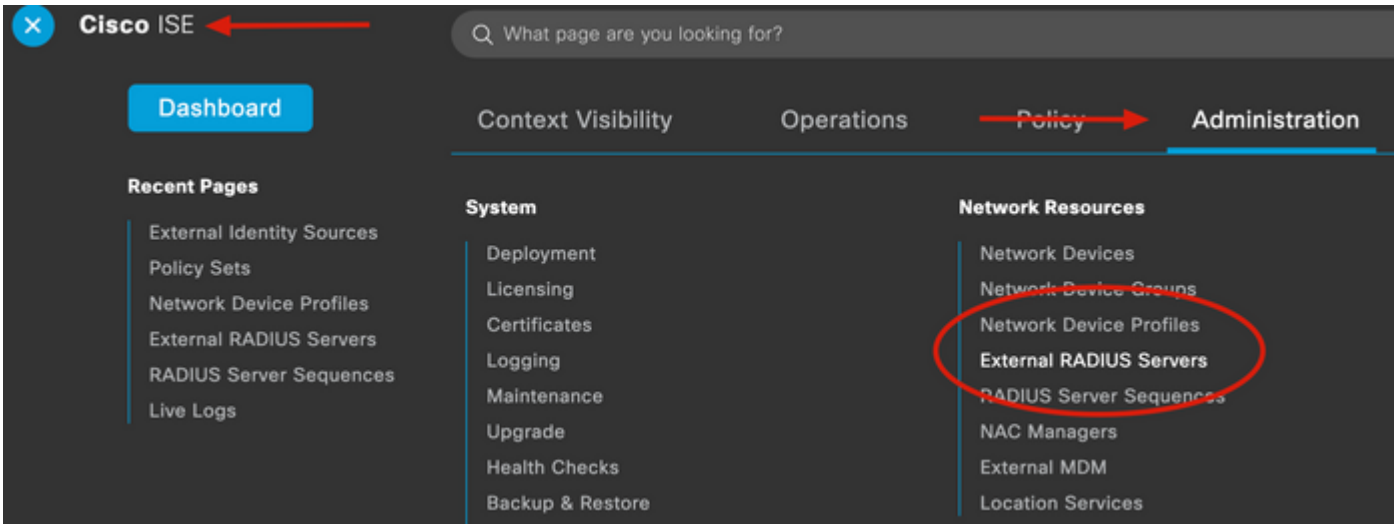
> **Hinweis**: Wenn die Validierung nicht erfolgreich ist, finden Sie auf der Registerkarte debug weitere Informationen, und korrigieren Sie diese entsprechend.



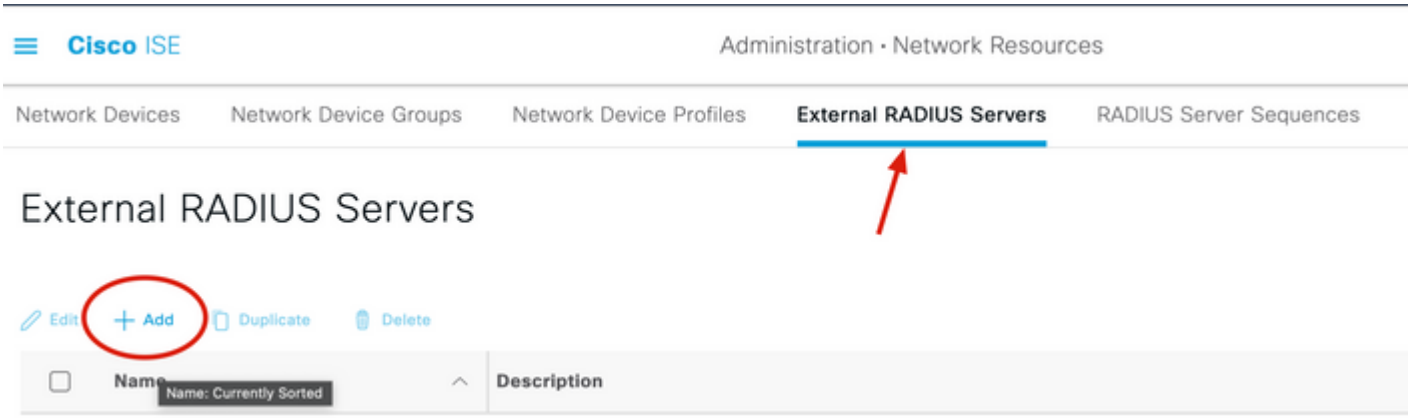
Cisco ISE-Konfigurationen

1. Melden Sie sich beim ISE-Administratorportal an.

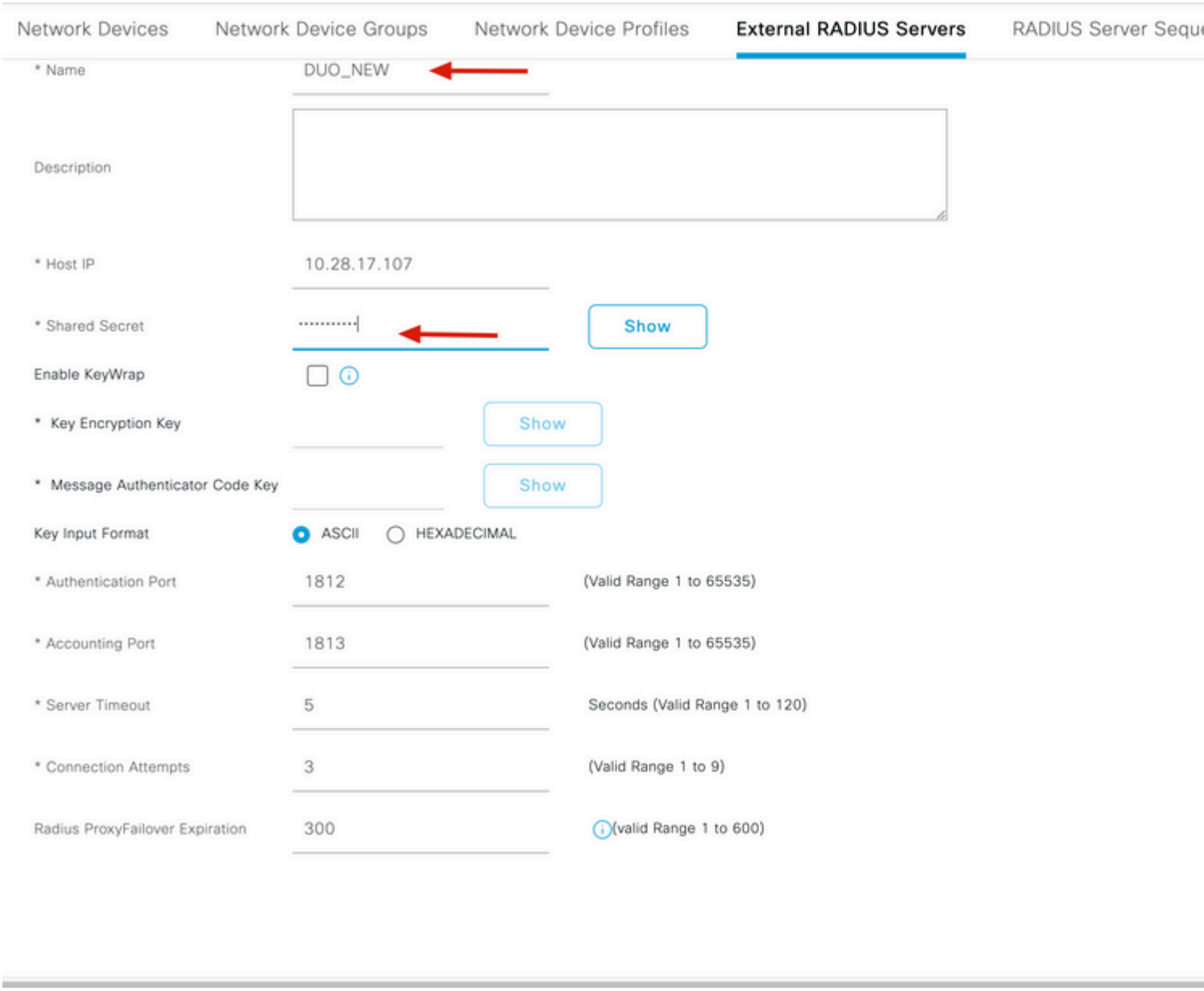
2. Erweitern Sie die Registerkarte Cisco ISE, und navigieren Sie zu **Administration**, klicken Sie dann auf **Network Resources (Netzwerkressourcen)**, und klicken Sie auf **External RADIUS Servers (Externe RADIUS-Server)**.



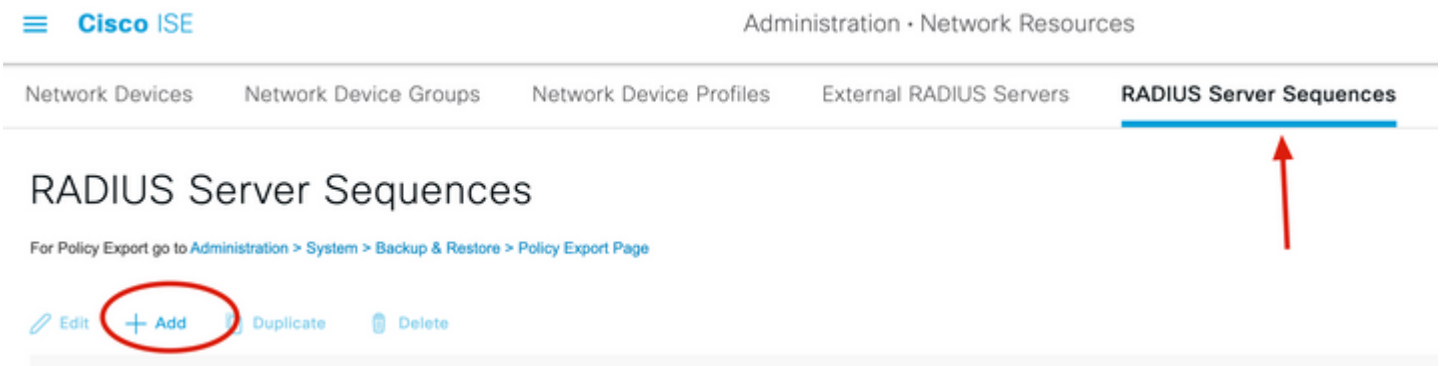
3. Klicken Sie auf der Registerkarte **"Externe RADIUS-Server**" auf **Hinzufügen**.



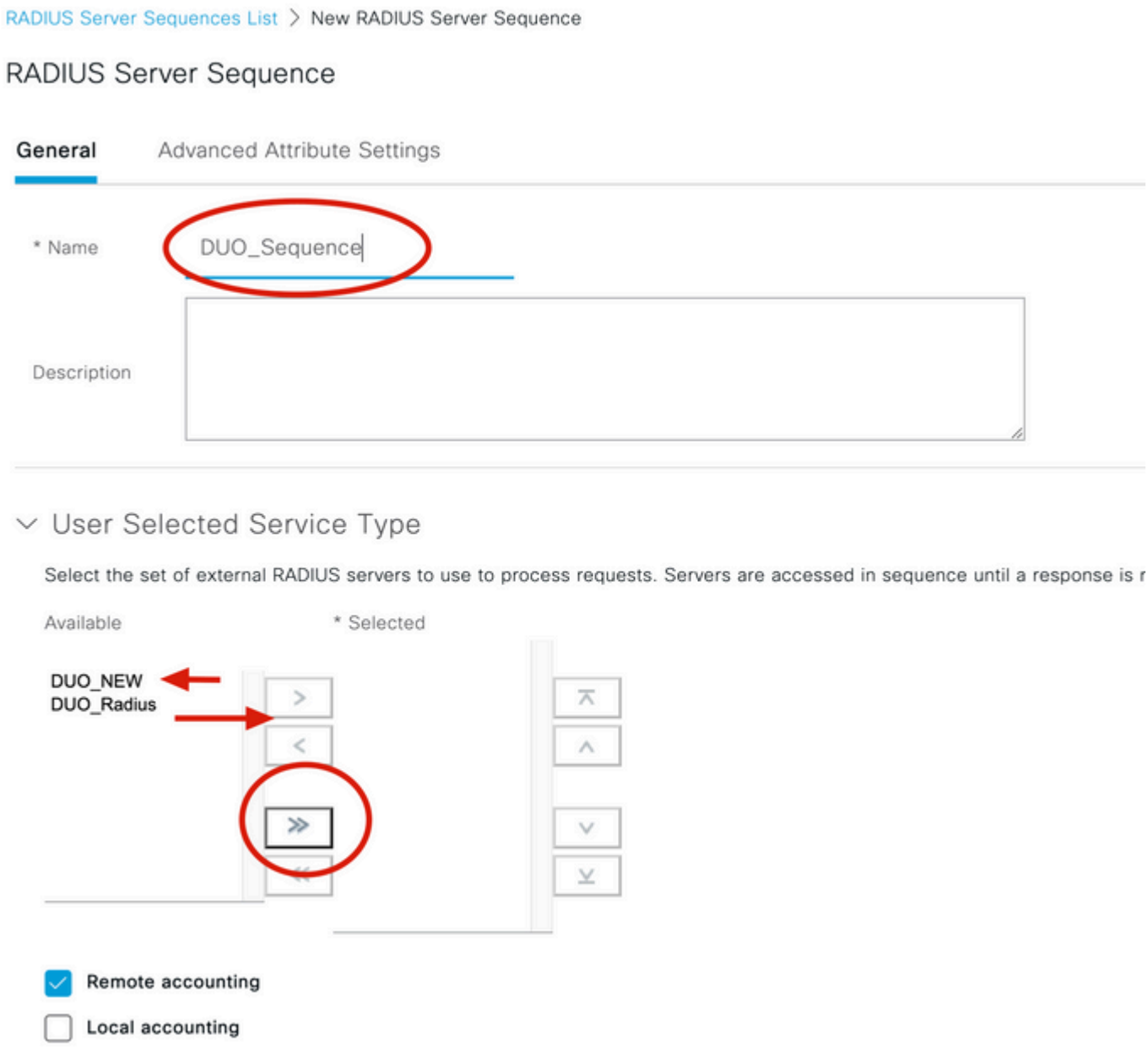
4. Füllen Sie die Lücke mit der RADIUS-Konfiguration aus, die im Duo Authentication Proxy Manager verwendet wird, und klicken Sie auf **Submit (Senden)**.



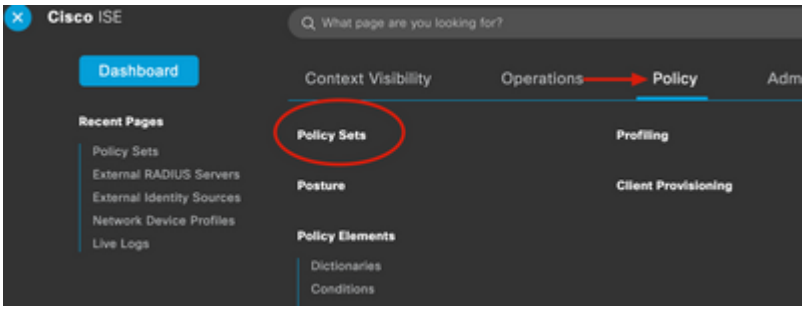
5. Navigieren Sie zur Registerkarte **RADIUS Server Sequences** (**RADIUS-Serversequenzen**), und klicken Sie auf **Add (Hinzufügen)**.



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

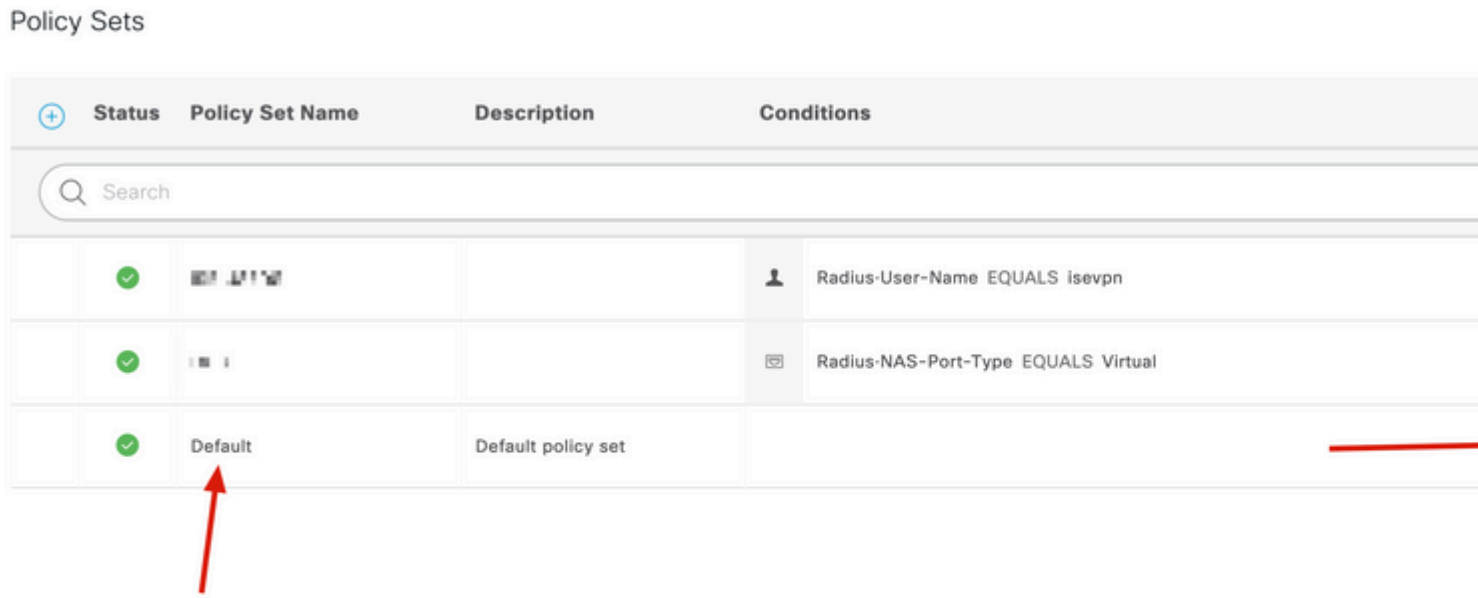


7. Navigieren Sie vom Dashboard-Menü zu **Policy** und klicken Sie auf **Policy Sets**.



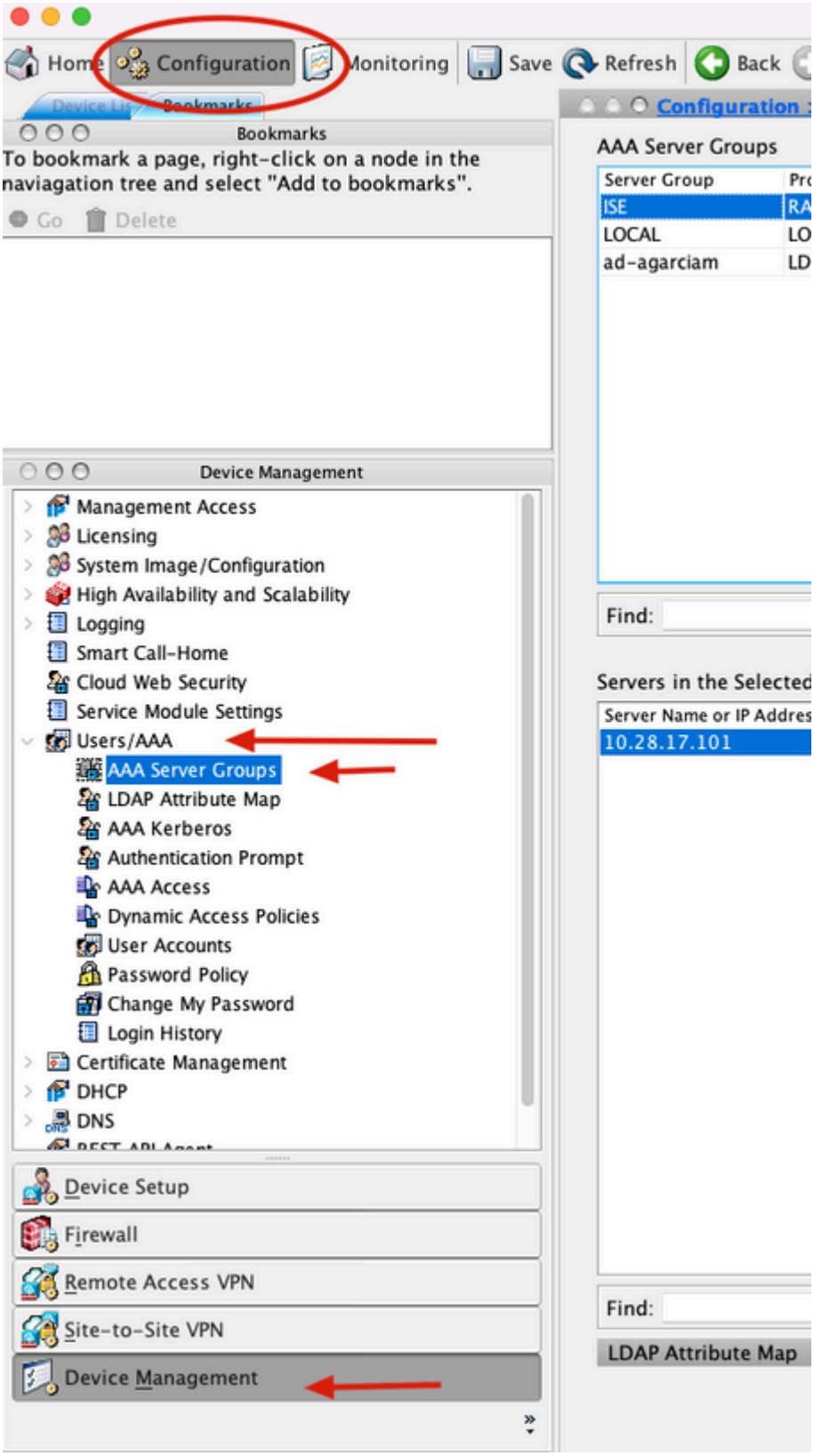
8. Weisen Sie die RADIUS-Sequenz der Standardrichtlinie zu.

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

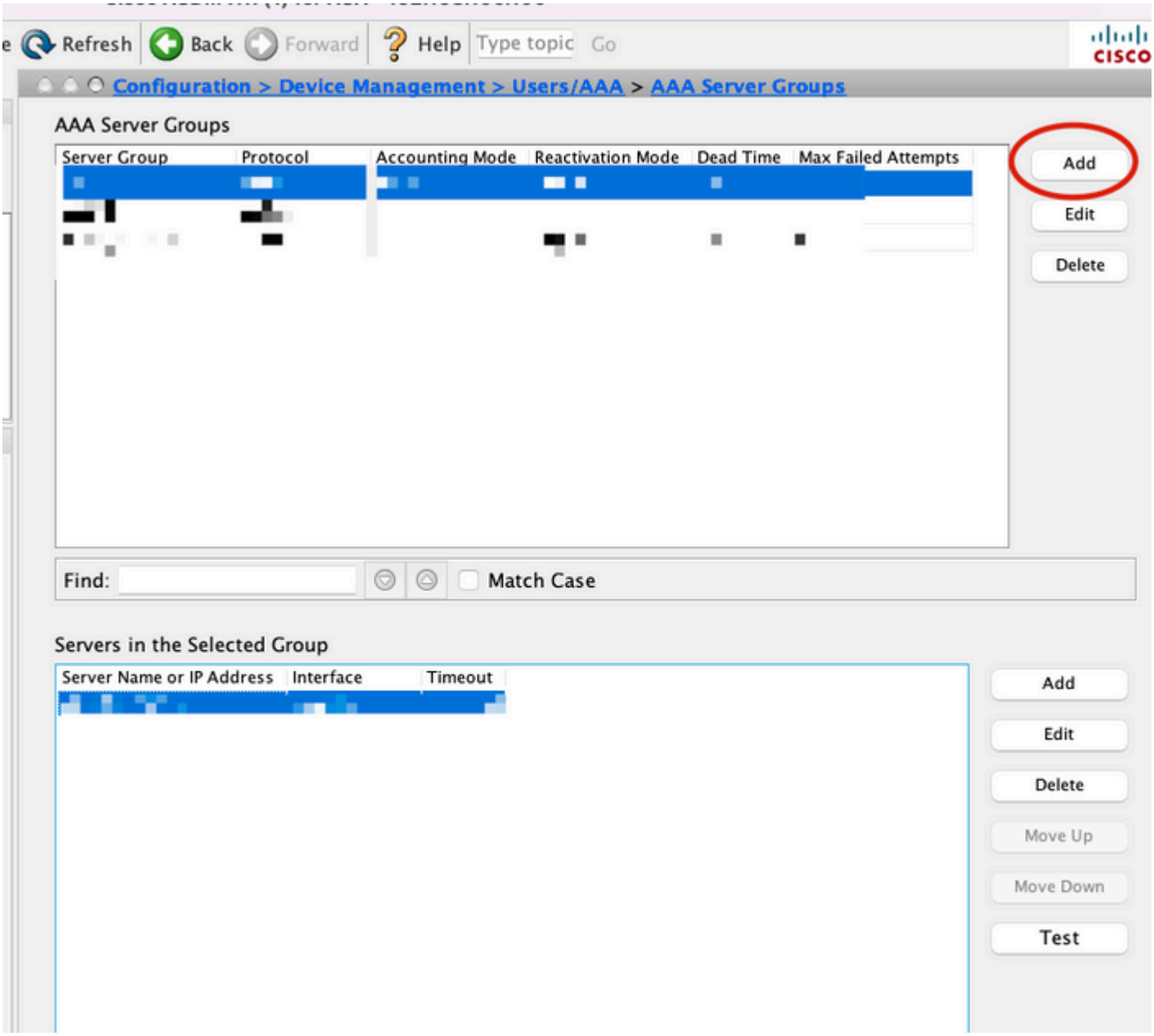


Konfiguration von Cisco ASA RADIUS/ISE

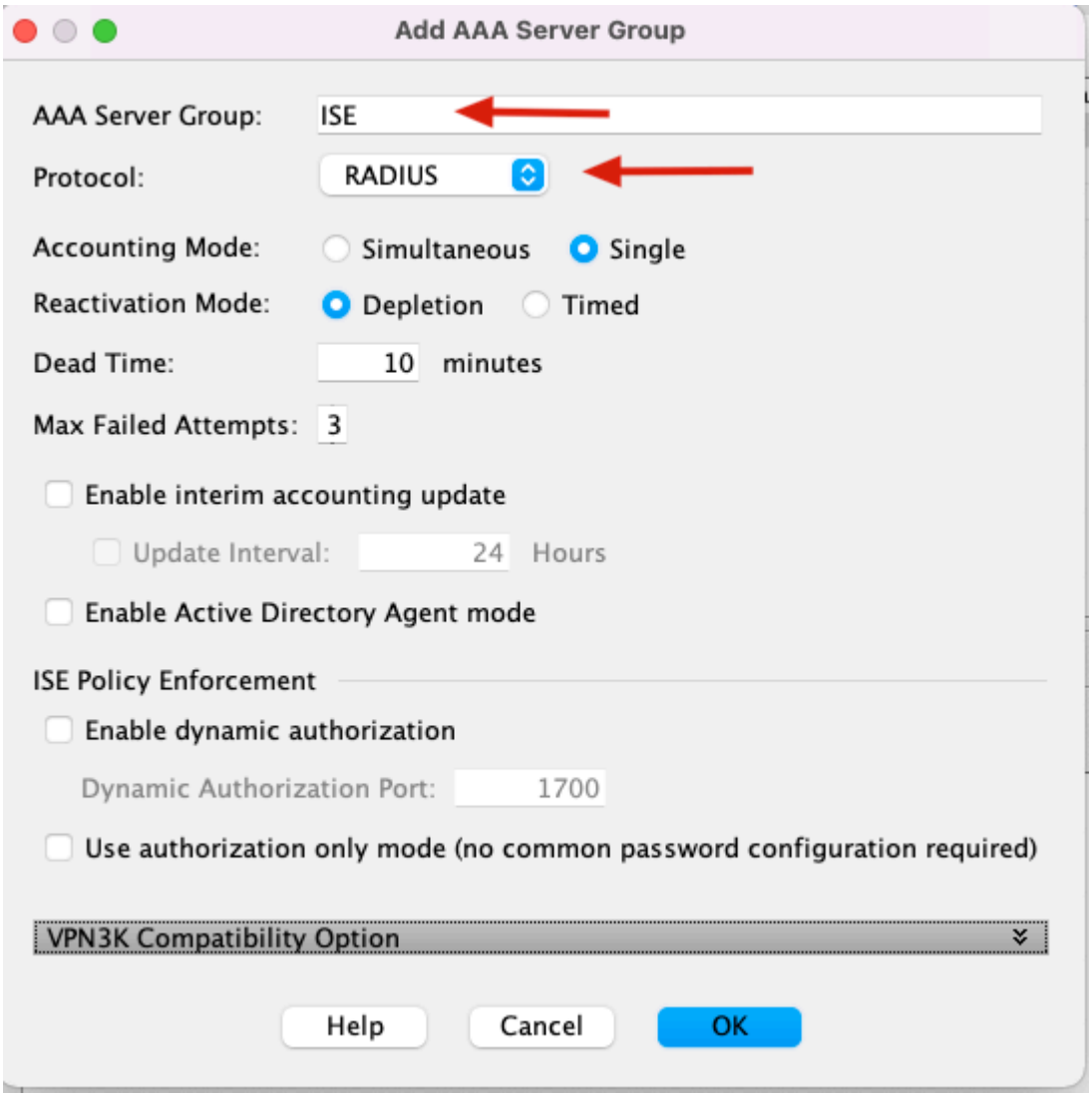
1. Konfigurieren Sie den ISE RADIUS-Server unter AAA-Servergruppen. Navigieren Sie zu **Konfiguration,** klicken Sie dann auf **Geräteverwaltung,** und erweitern Sie den Abschnitt **Benutzer/AAA,** und wählen Sie **AAA-Servergruppen aus**.



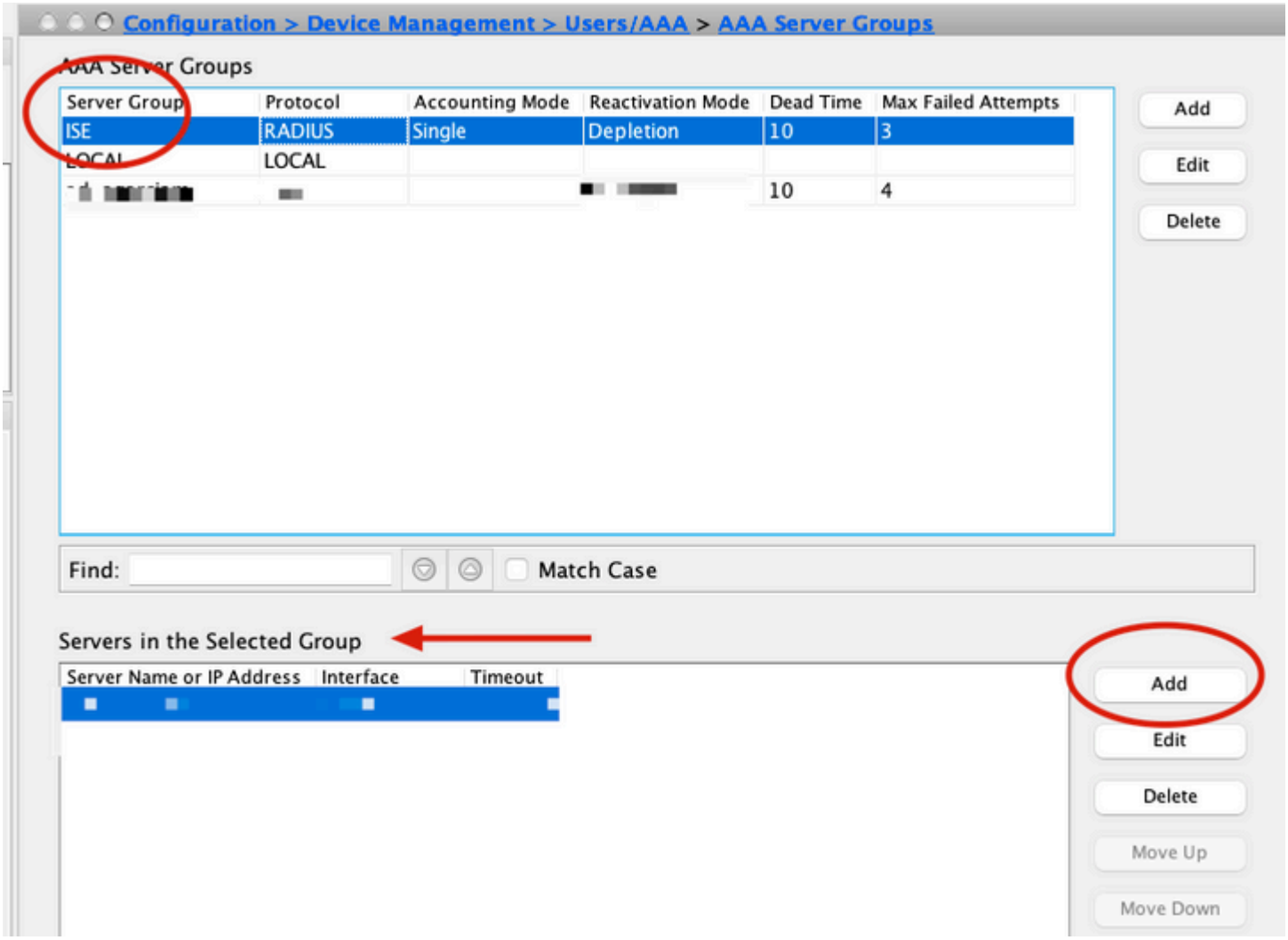
2. Klicken Sie im Bereich **AAA-Servergruppen** auf **Hinzufügen**.



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

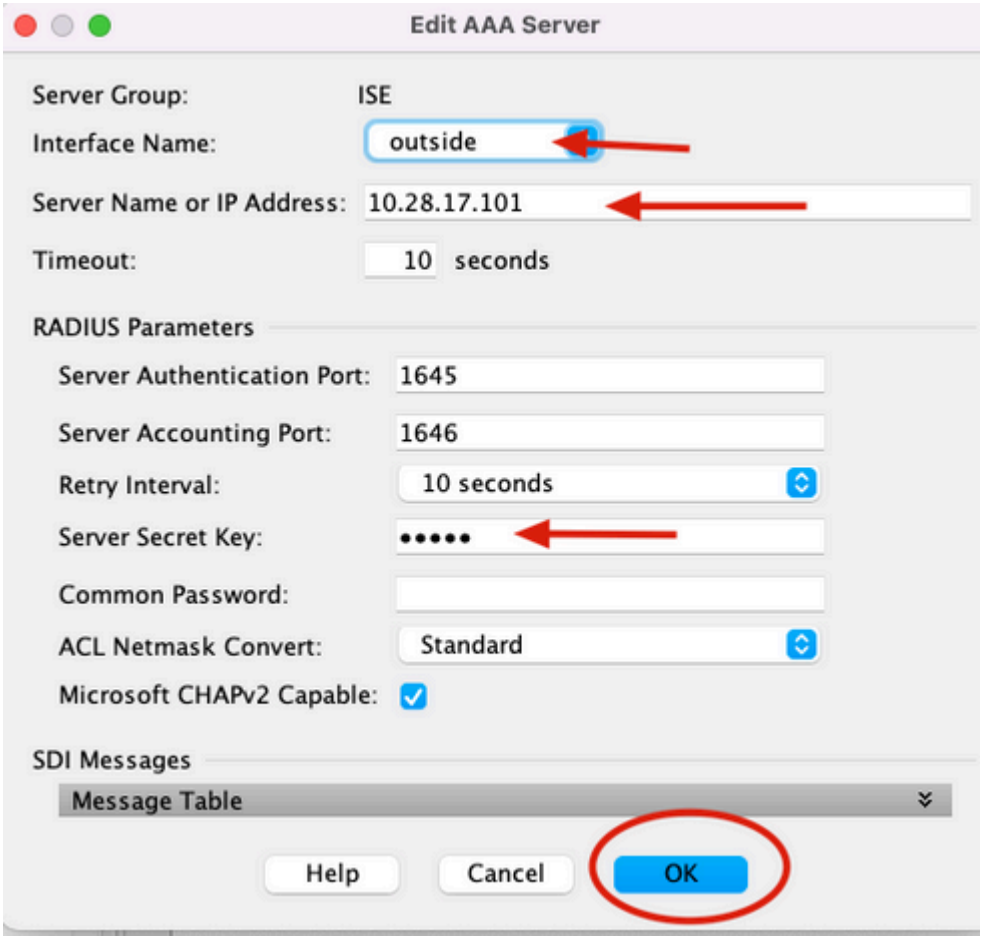


5. Wählen Sie Ihre neue Servergruppe aus, und klicken Sie unter **Server im** Bereich **Ausgewählte Gruppe** auf **Hinzufügen**, wie im Bild gezeigt.



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
```

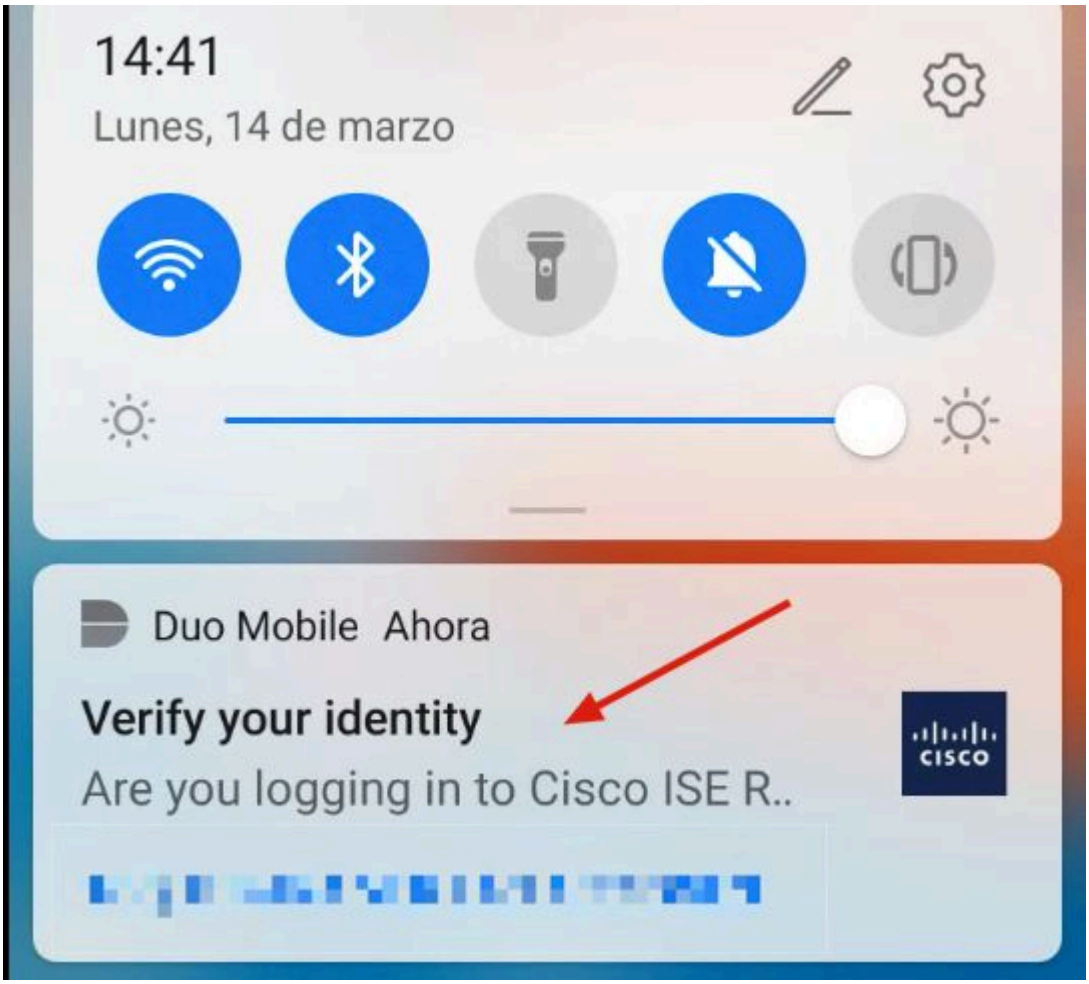
```
 default-group-policy DUO
tunnel-group ISE-users webvpn-attributes
 group-alias ISE enable
 dns-group DNS-CISCO
```

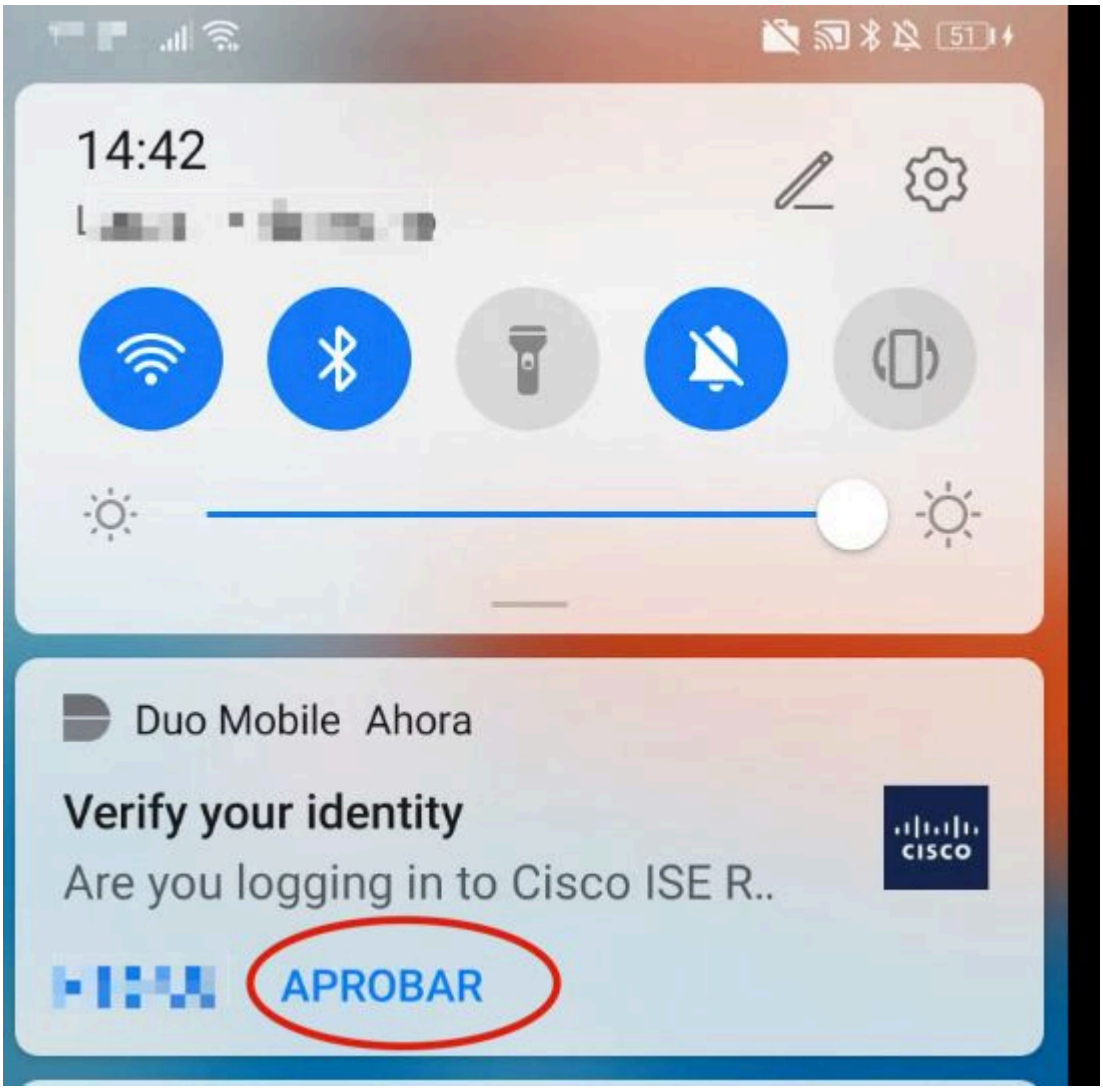
Test

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**.

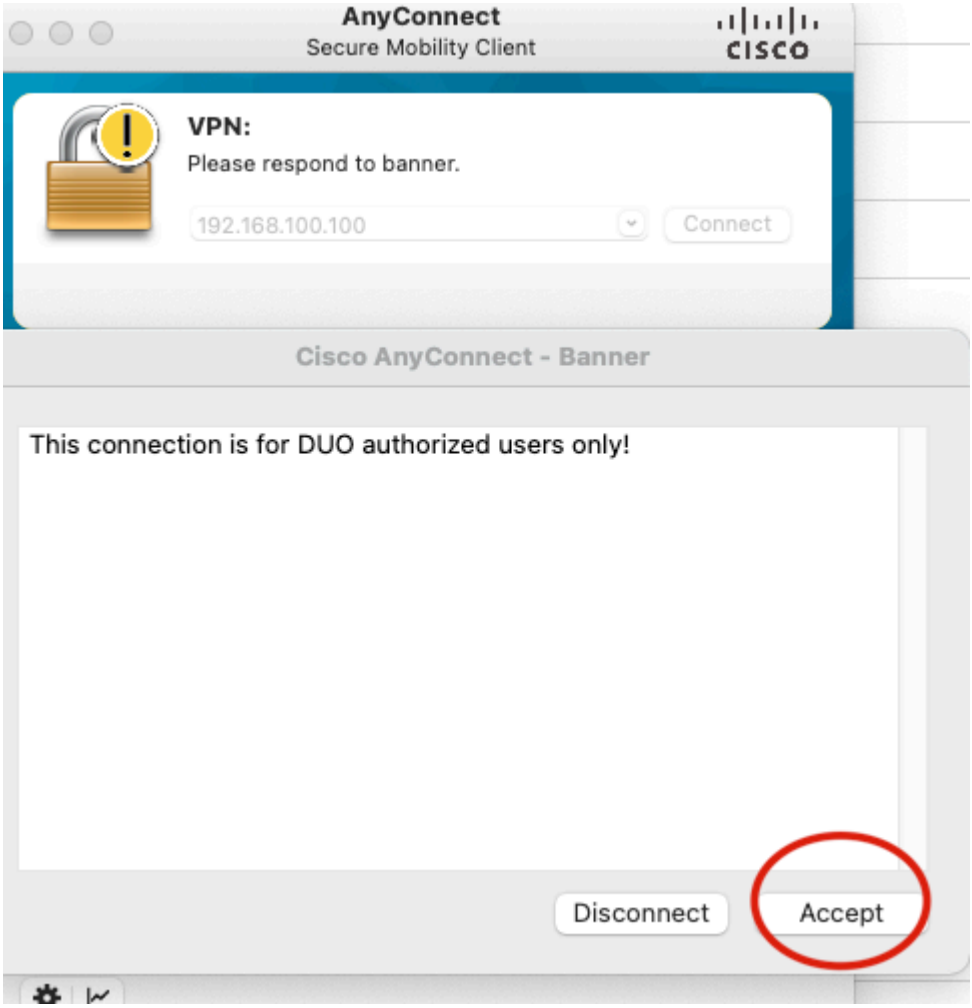
2. Sie haben eine Duo-Push-Benachrichtigung auf dem angegebenen Duo Mobilgerät erhalten.

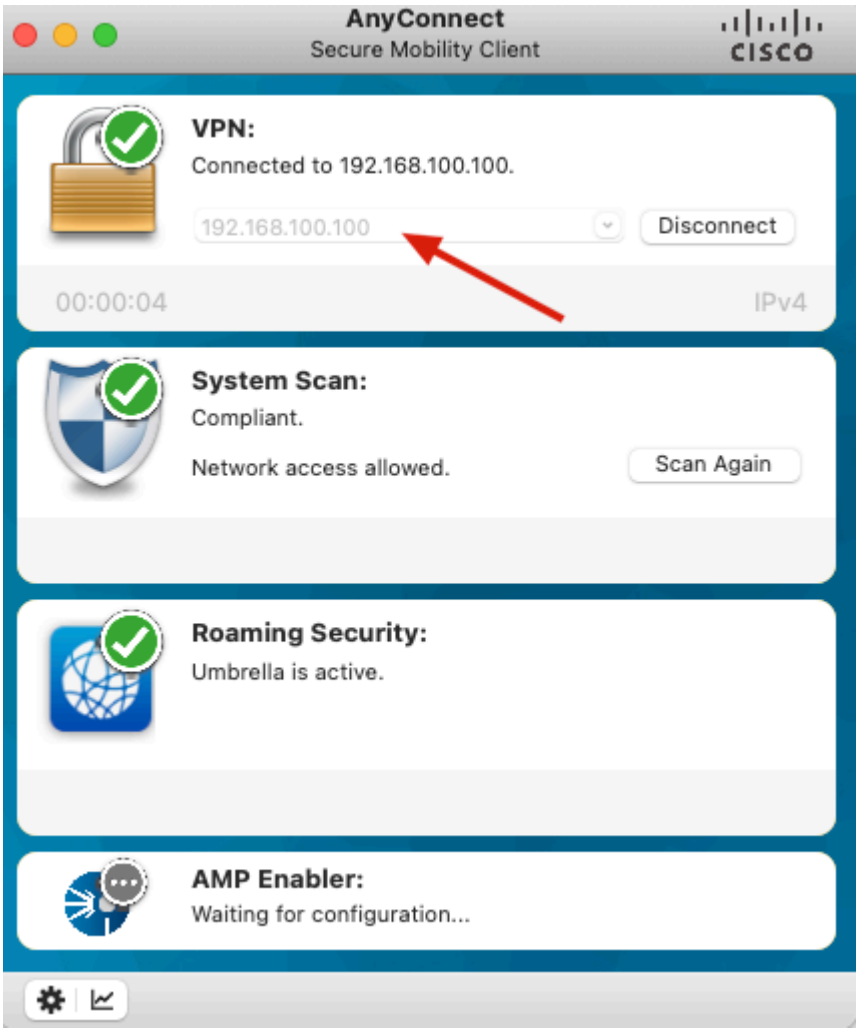
3. Öffnen Sie die Duo Mobile App-Benachrichtigung, und klicken Sie auf **Genehmigen**.


14:41
Lunes, 14 de marzo
Duo Mobile Ahora
Verify your identity
Are you logging in to Cisco ISE R..
cisco



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


AnyConnect
Secure Mobility Client
CISCO
VPN:
Please respond to banner.
192.168.100.100
Connect
Cisco AnyConnect - Banner
This connection is for DUO authorized users only!
Disconnect
Accept



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': '[redacted]',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': '[redacted]',
         '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': '[redacted]',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': '[redacted]',
         '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
```

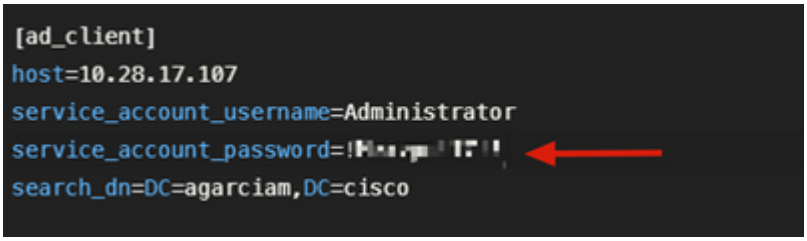
1. Verbindungsprobleme, falsche IP, nicht auflösbarer FQDN/Hostname in der Active Directory-Konfiguration.

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

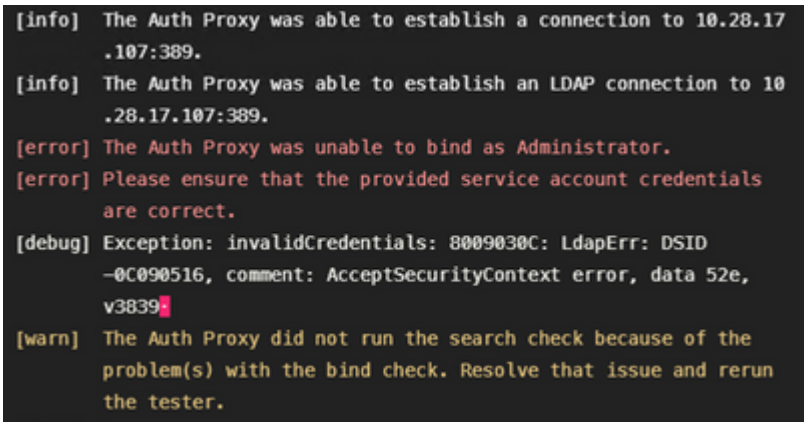
Output

```
        '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.
```

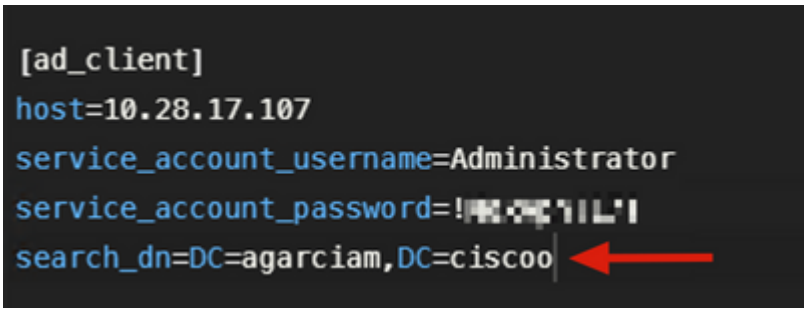
2. Falsches Kennwort für Administratorbenutzer in Active Directory.



Debuggen.



3. Falsche Basisdomäne



Debuggen.

```
[info]  The Auth Proxy was able to bind as A
[error] The Auth Proxy got an error searchin
        ,DC=ciscoo.
[debug] Exception: referral: 0000202B: RefEr
        1 access points
                ref 1: 'agarciam.ciscoo'
```

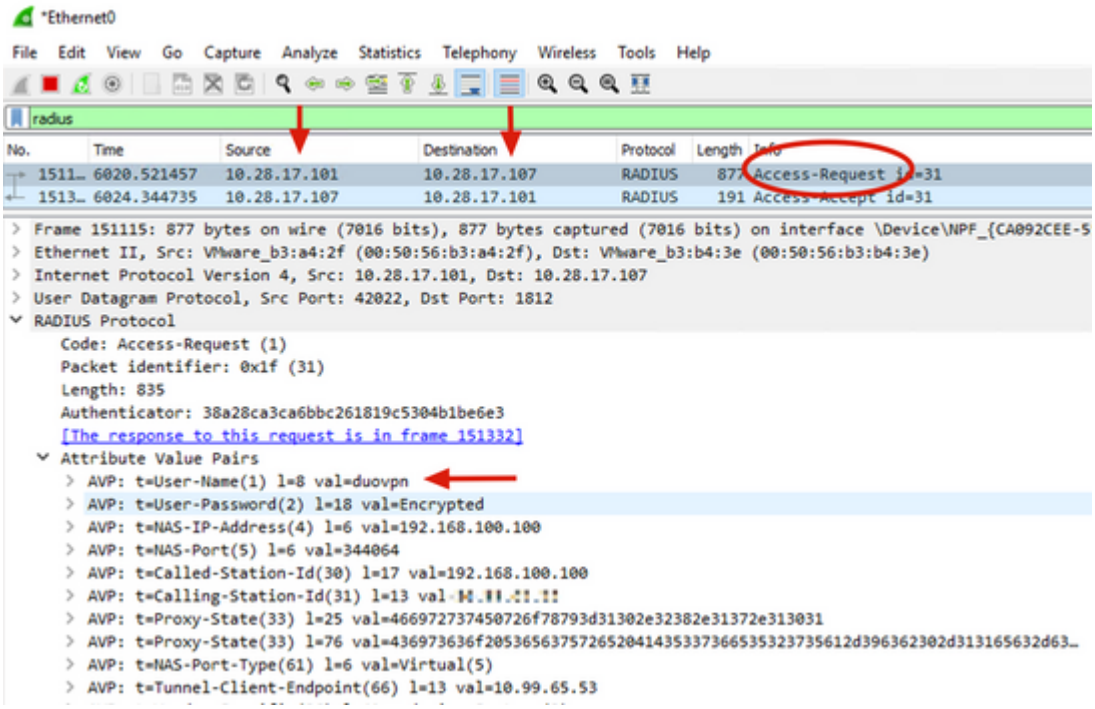
4. Falscher wichtiger RADIUS-Wert.

```
[radius_server_auto]
ikey=[redacted]XHRNZ6EZ1
skey=[redacted]
api_host=[redacted]ity.com
radius_ip_1=10.28.17.101
radius_secret_1=!Mexvpn!17!
failmode=safe
client=ad_client
port=1812
```

Fehlerbehebung

```
[error] The ikey value provided is invalid.
[info]  ----------------------------
[info]  SUMMARY
[warn]  Checks for external connectivity were not run. Please fix the
        configuration and try again.
```

5. Überprüfen Sie, ob der ISE-Server Access-Request-Pakete sendet.

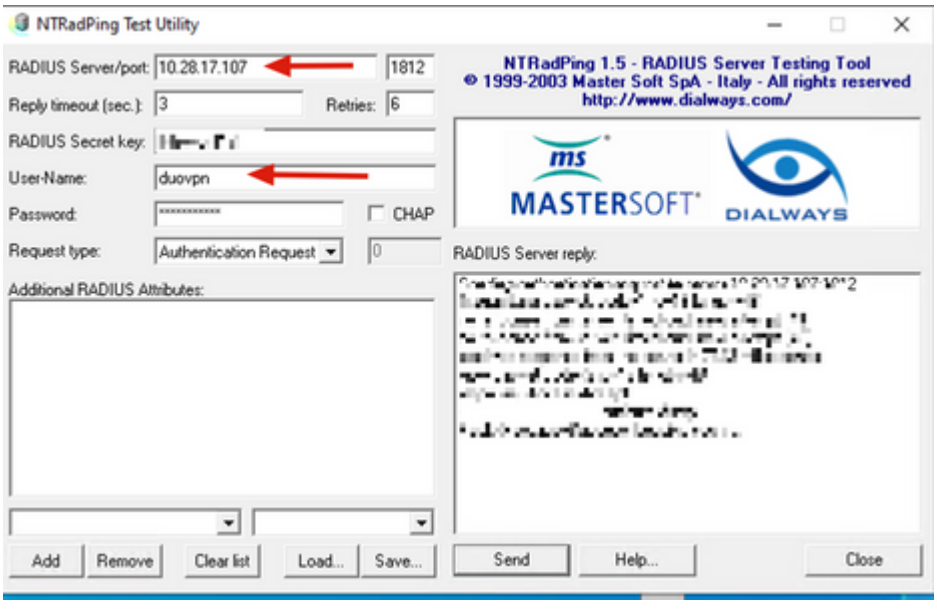


6. Um zu bestätigen, dass der Duo Authentication Proxy-Server funktioniert, stellt Duo das Tool NTRadPing zur Verfügung, um Access-Request-Pakete und die Antwort mit Duo zu simulieren.

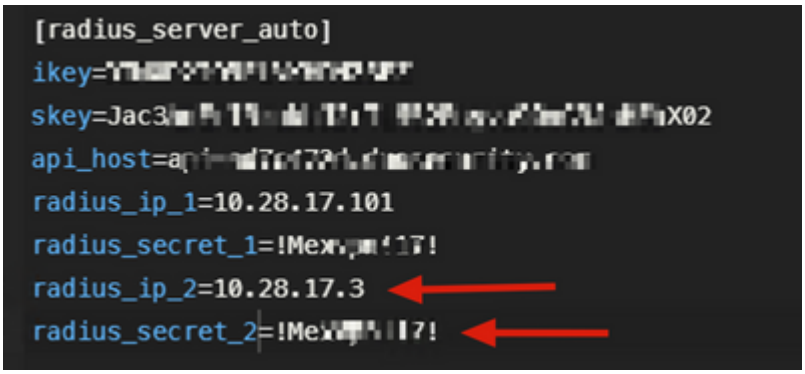
6.1 Installieren Sie NTRadPing auf einem anderen PC, und generieren Sie Datenverkehr.

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

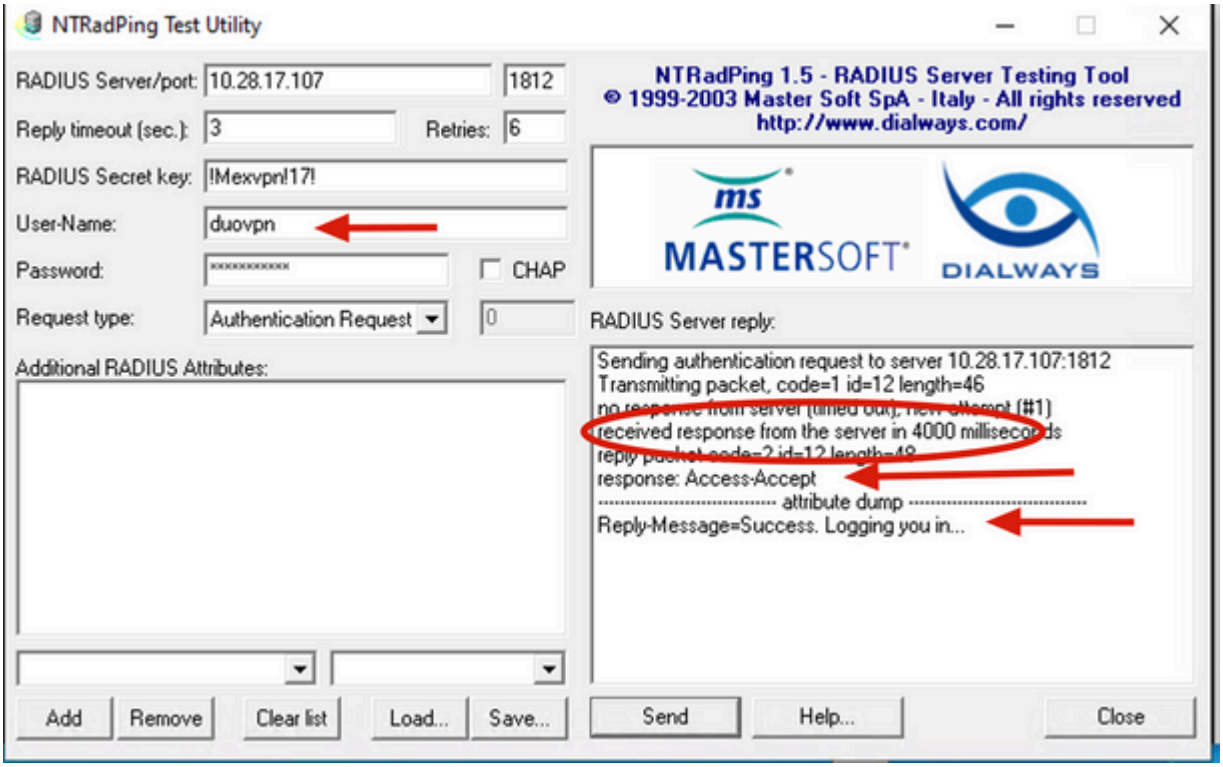
6.2 Konfigurieren Sie die Attribute, die in der ISE Radius-Konfiguration verwendet werden.

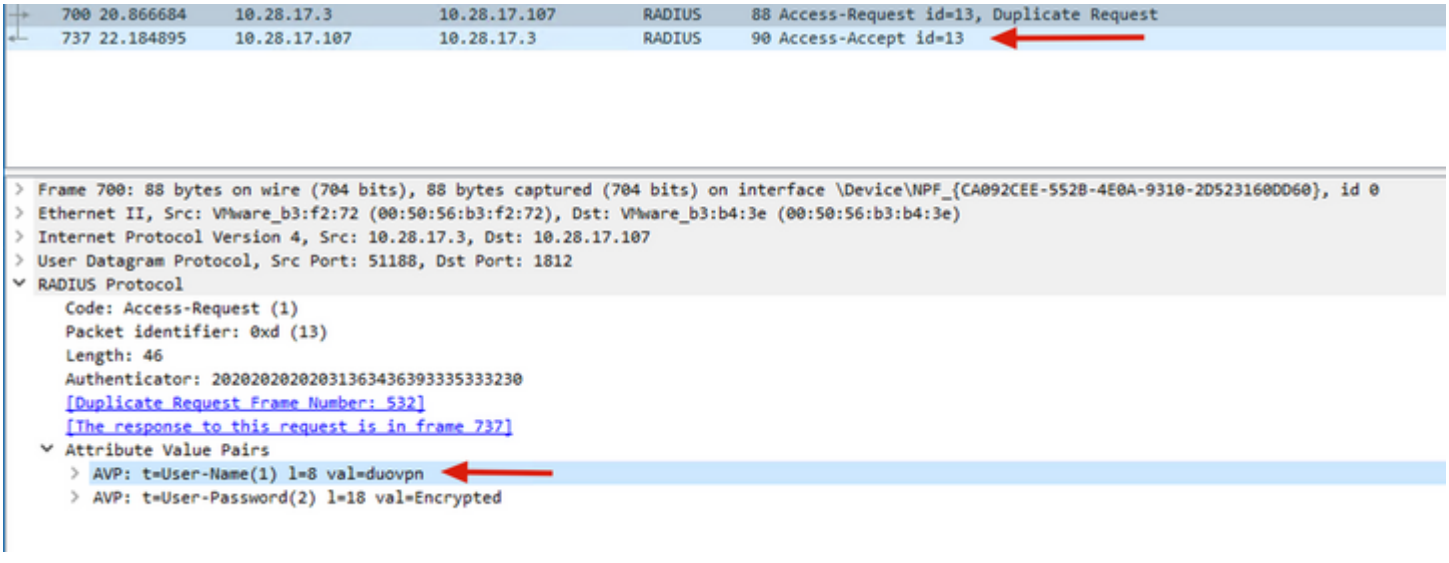


6.3 Konfigurieren Sie den Duo Authentication Proxy Manager wie folgt.



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.