

Configurazione dell'integrazione Duo con Active Directory e ISE per l'autenticazione a due fattori su client VPN Anyconnect/Remote Access

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio e diagramma reticolare](#)

[Processo di comunicazione](#)

[Configurazioni di Active Directory](#)

[Duo](#)

[Duo Auth Proxy Configuration](#)

[Configurazioni Cisco ISE](#)

[Configurazione Cisco ASA RADIUS/ISE](#)

[Configurazione VPN di accesso remoto Cisco ASA](#)

[Test](#)

[Risoluzione dei problemi](#)

[Debug del lavoro](#)

Introduzione

In questo documento viene descritta l'integrazione push Duo con AD e ISE come autenticazione a due fattori per i client AnyConnect connessi all'appliance ASA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione VPN Autorità registrazione su ASA
- Configurazione RADIUS su ASA
- ISE
- Active Directory
- Applicazioni Duo

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

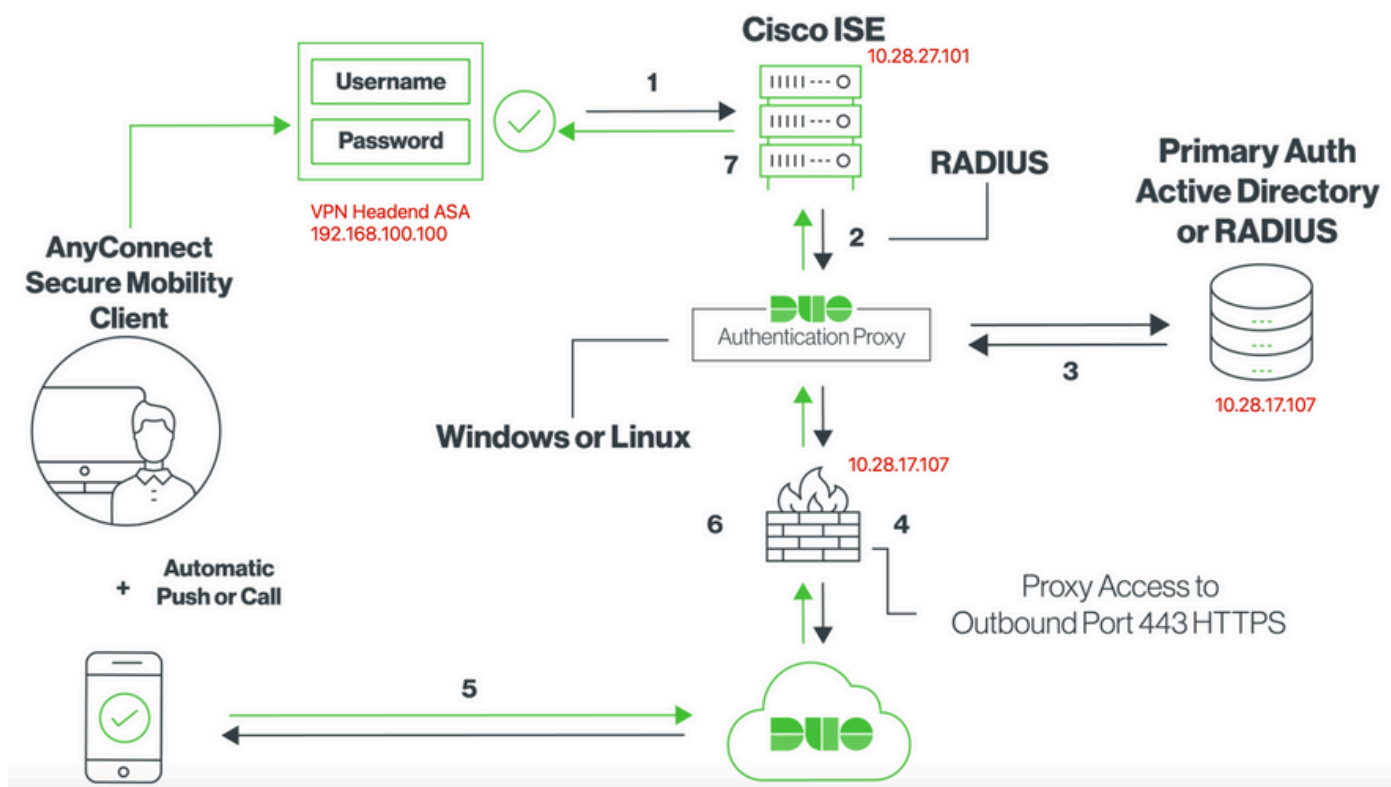
- Server Microsoft 2016
- ASA 9.14(3)18
- ISE Server 3.0
- Duo
- Duo Authentication Proxy Manager

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene descritto come configurare Duo Push Integration con Active Directory (AD) e Cisco Identity Service Engine (ISE) come autenticazione a due fattori per i client AnyConnect che si connettono a Cisco Adaptive Security Appliance (ASA).

Esempio e diagramma reticolare



Processo di comunicazione

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

1. Autenticazione primaria avviata su Cisco ISE
2. Cisco ISE invia una richiesta di autenticazione al proxy di autenticazione Duo


3. L'autenticazione primaria utilizza Active Directory o RADIUS
4. Connessione Duo Authentication Proxy stabilita a Duo Security sulla porta TCP 443
5. Autenticazione secondaria tramite il servizio Duo Security
6. Il proxy di autenticazione Duo riceve una risposta di autenticazione
7. Accesso Cisco ISE concesso

Account utente:

- Amministratore di Active Directory: questo account viene utilizzato come account di directory per consentire al proxy di autenticazione Duo di eseguire il binding al server di Active Directory per l'autenticazione primaria.
- Utente test Active Directory
- Duo test user per autenticazione secondaria

Configurazioni di Active Directory

Il server Windows è preconfigurato con Servizi di dominio Active Directory.

 Nota: se Gestione proxy di autenticazione RADIUS Duo viene eseguito sullo stesso computer host di Active Directory, è necessario disinstallare/eliminare i ruoli di Server dei criteri di rete. Se vengono eseguiti entrambi i servizi RADIUS, possono verificarsi conflitti e influire sulle prestazioni.

Per ottenere la configurazione di Active Directory per l'autenticazione e l'identità degli utenti su utenti VPN ad accesso remoto, sono necessari alcuni valori.

Tutti questi dettagli devono essere creati o raccolti sul server Microsoft prima di poter eseguire la configurazione sull'appliance ASA e sul server proxy Duo Auth.

I valori principali sono:

- Nome dominio. Nome di dominio del server. In questa guida alla configurazione, il nome di dominio è agarciam.cisco.
- Indirizzo IP/FQDN del server. Indirizzo IP o FQDN utilizzato per raggiungere il server Microsoft. Se si utilizza un FQDN, è necessario configurare un server DNS all'interno di ASA e del proxy di autenticazione Duo per risolvere l'FQDN.

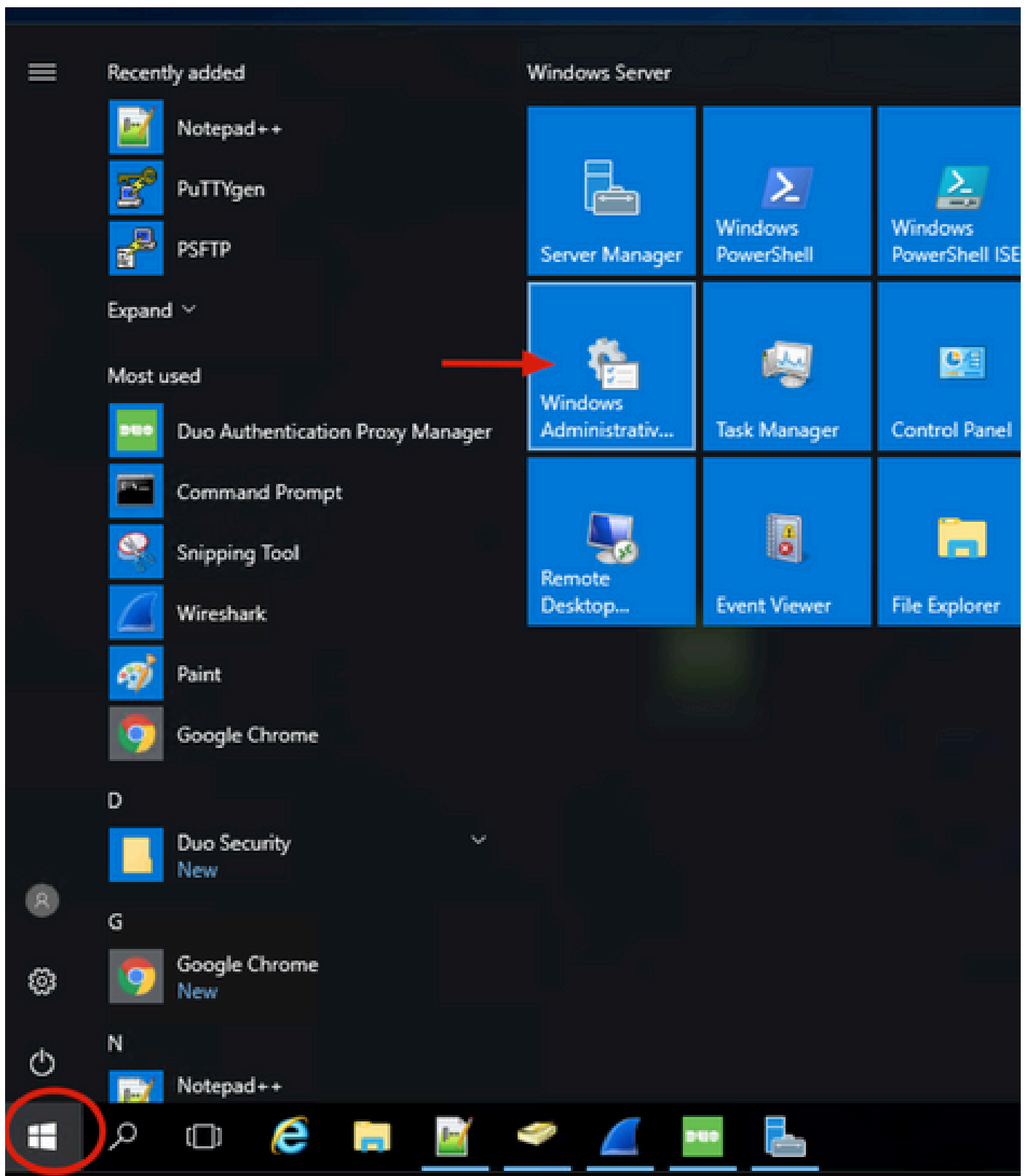
In questa guida alla configurazione, questo valore è agarciam.cisco (che si risolve in 10.28.17.107).

- Porta server. La porta utilizzata dal servizio LDAP. Per impostazione predefinita, LDAP e STARTTLS utilizzano la porta TCP 389 per LDAP, mentre LDAP over SSL (LDAPS) utilizza la porta TCP 636.
- CA radice. Se si utilizza LDAPS o STARTTLS, è necessaria la CA radice utilizzata per firmare il certificato SSL utilizzato da LDAPS.

- Nome utente e password della directory. Questo è l'account usato dal server proxy Duo Auth per eseguire il binding al server LDAP e autenticare gli utenti e cercare utenti e gruppi.
- Nome distinto (DN) di base e gruppo. Il DN di base è il punto di partenza per il proxy Duo Auth e indica ad Active Directory di iniziare la ricerca e l'autenticazione degli utenti.

In questa guida alla configurazione, il dominio radice agarciam.cisco viene utilizzato come DN di base e il DN gruppo è Duo-USERS.

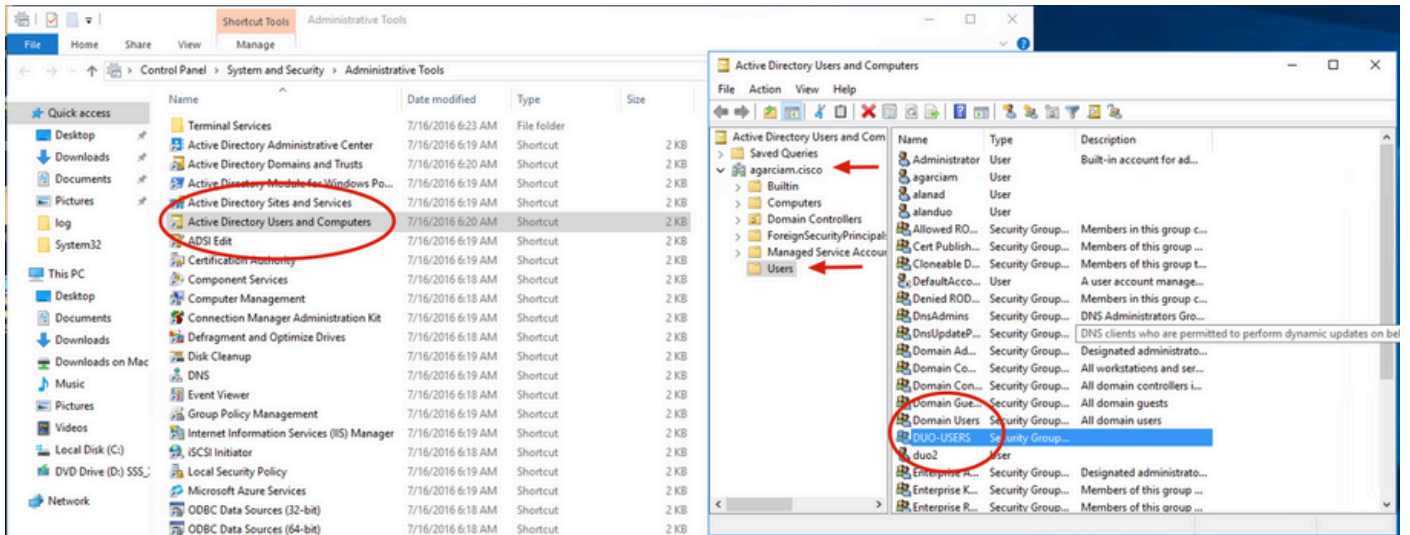
1. Per aggiungere un nuovo utente Duo, in Windows Server passare all'icona Windows in basso a sinistra e fare clic su Strumenti di amministrazione di Windows, come mostrato nell'immagine.



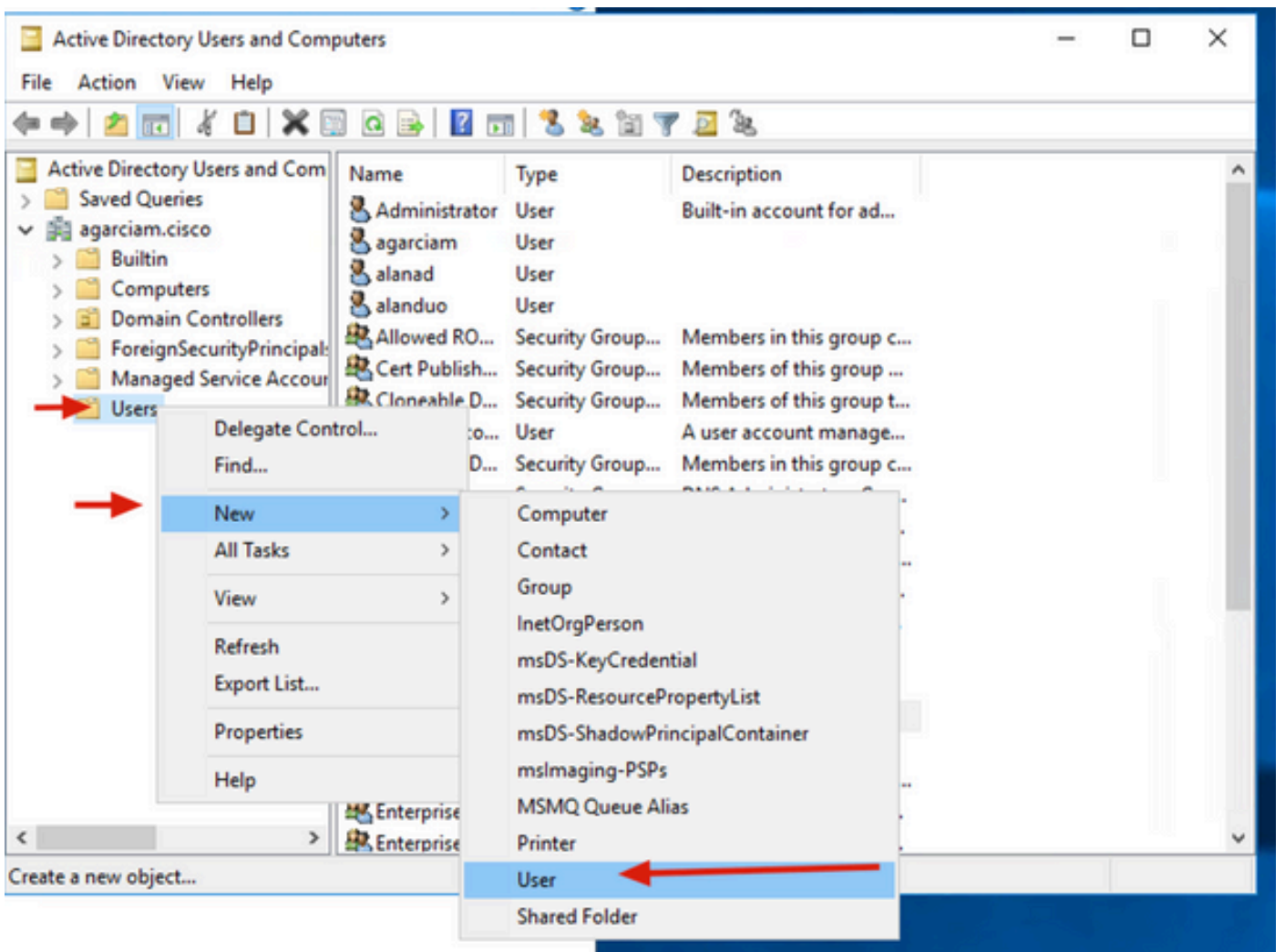
2. Nella finestra Strumenti di amministrazione di Windows passare a Utenti e computer di Active Directory.

Nel pannello Utenti e computer di Active Directory espandere l'opzione dominio e passare alla cartella Utenti.

In questo esempio di configurazione, Duo-USERS viene utilizzato come gruppo di destinazione per l'autenticazione secondaria.





3. Fare clic con il pulsante destro del mouse sulla cartella Users (Utenti) e selezionare New > User (Nuovo utente), come mostrato nell'immagine.



4. Nella finestra Nuovo oggetto-utente, specificare gli attributi di identità per il nuovo utente e fare clic su Avanti, come mostrato nell'immagine.


New Object - User X

 Create in: `agarciam.cisco/Users`

First name:  Initials:

Last name:


Full name:

User logon name:
 

User logon name (pre-Windows 2000):

5. Confermare la password e fare clic su Avanti, quindi su Fine una volta verificate le informazioni sull'utente.

New Object - User X

 Create in: `agarciam.cisco/Users`

Password: ←

Confirm password: ←

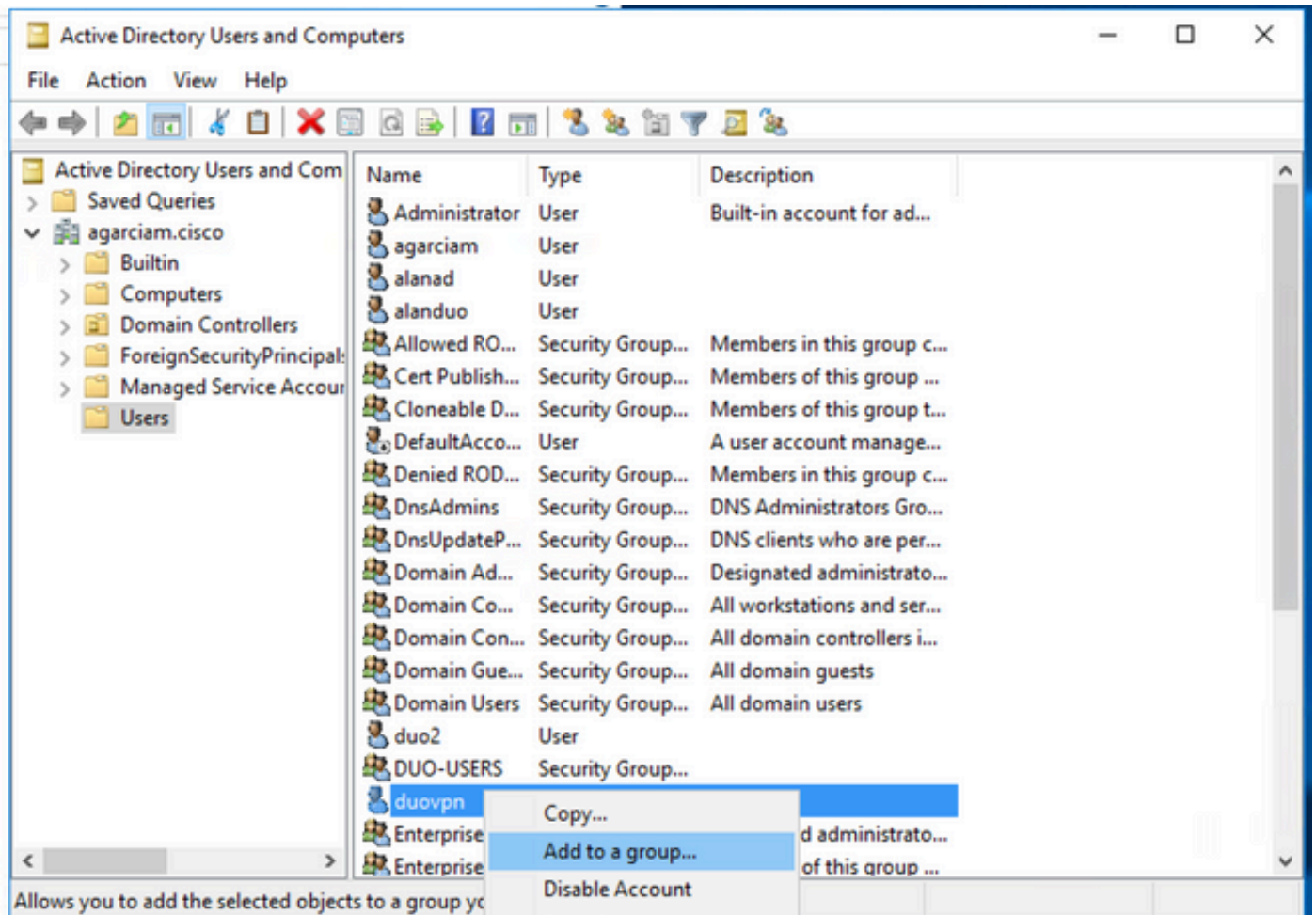
User must change password at next logon

User cannot change password

Password never expires

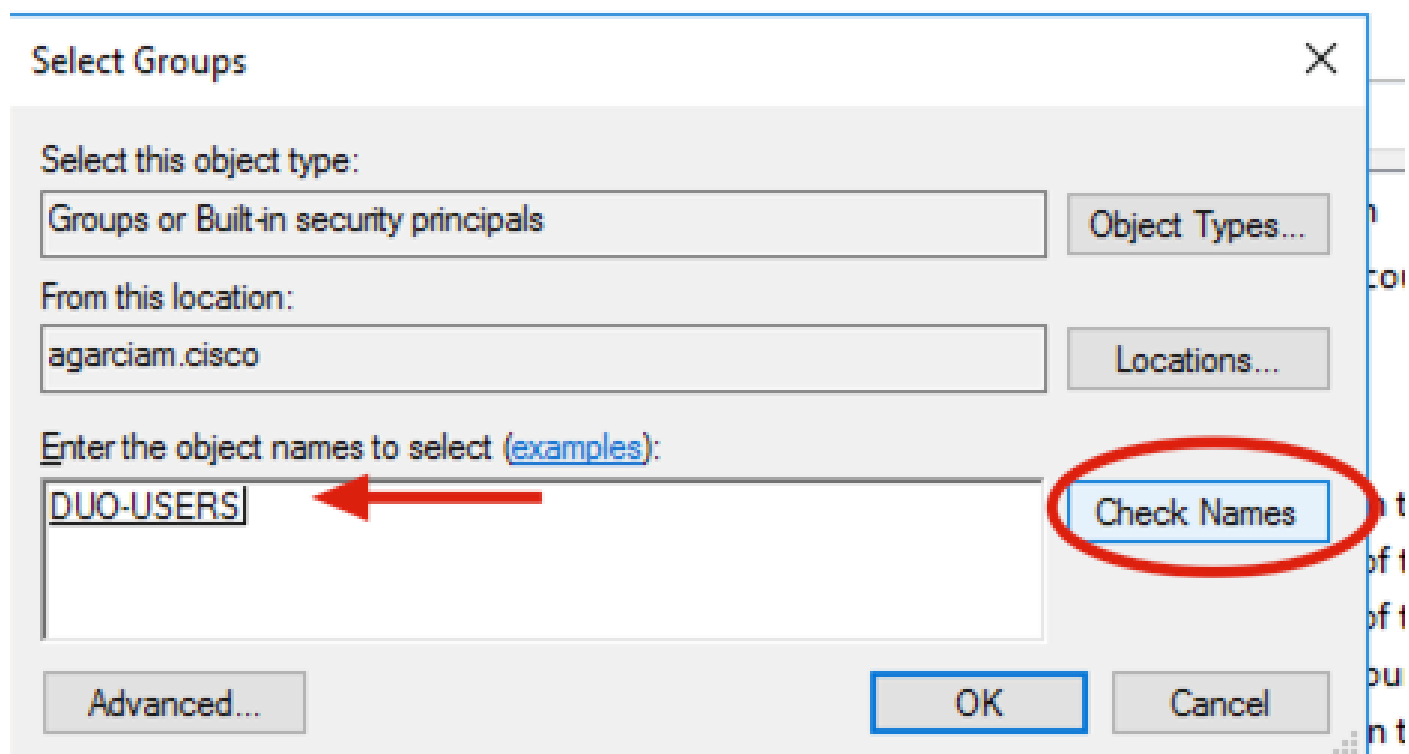
Account is disabled

6. Assegnare il nuovo utente a un gruppo specifico, fare clic con il pulsante destro del mouse e selezionare Aggiungi a un gruppo, come mostrato nell'immagine.



7. Nel pannello Seleziona gruppi, digitare il nome del gruppo desiderato e fare clic su Controlla nomi.

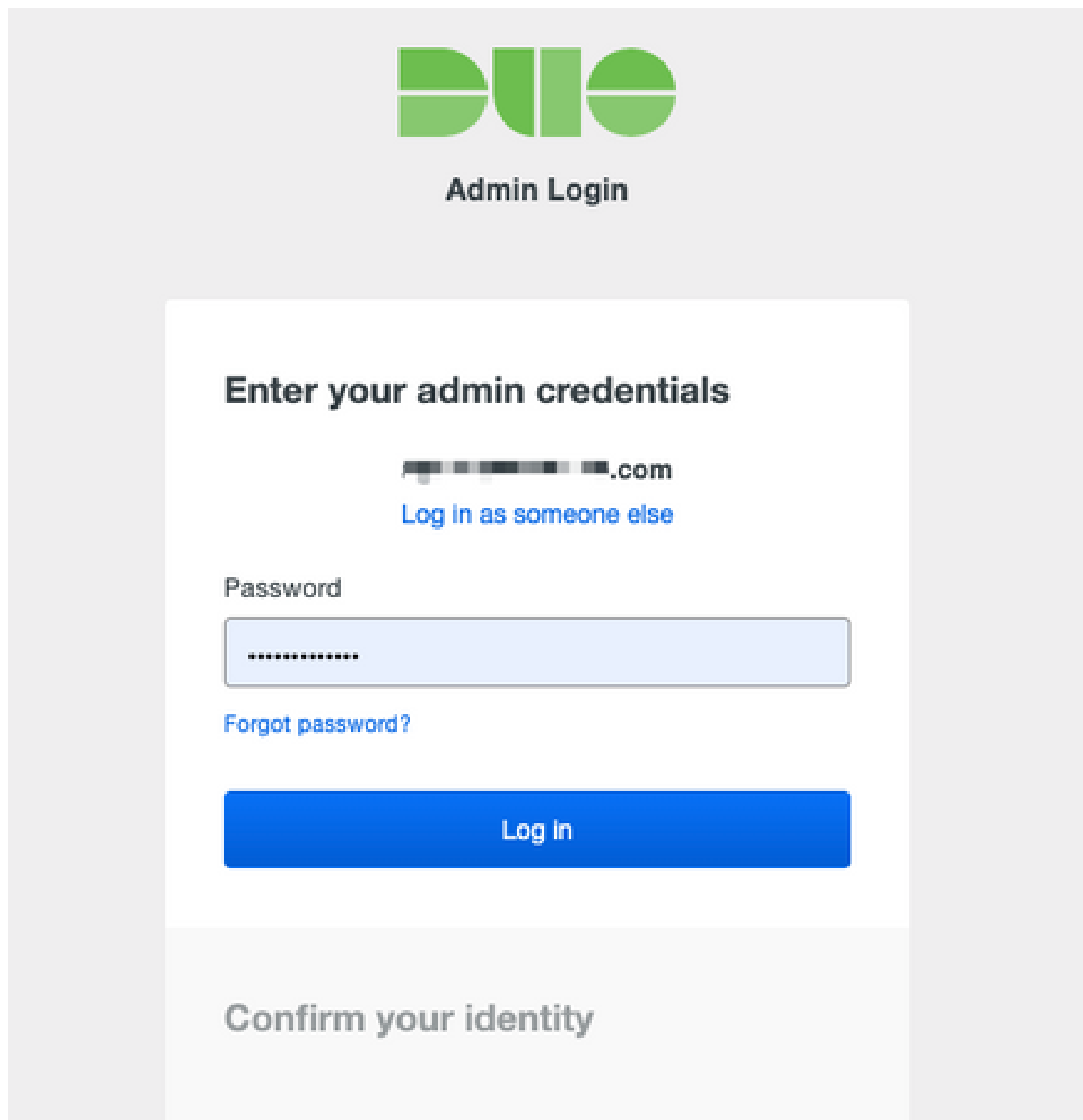
Selezionare quindi il nome che corrisponde ai criteri e fare clic su OK.



8. Utente utilizzato come esempio nel documento.

Duo

1. Accedere al portale di amministrazione Dudo.



Duo

Admin Login

Enter your admin credentials

██████████@██████████.com

[Log in as someone else](#)

Password

.....

[Forgot password?](#)

Log In

Confirm your identity

2. Nel riquadro a sinistra, passare a Utenti, fare clic su Aggiungi utente e digitare il nome dell'utente corrispondente al nome utente di Active Domain, quindi fare clic su Aggiungi utente.

DUO

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. Nel nuovo pannello utente, compilare il campo vuoto con tutte le informazioni necessarie.

duovpn

i This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.

Username ←

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).

Full name ←

Email

Status

- Active** ←
Require multi-factor authentication (default).
- Bypass**
Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.
- 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. [Learn more about groups](#)

Notes

For internal use.

4. In Periferiche utente specificare il metodo di autenticazione secondaria.

 **Nota:** in questo documento viene utilizzato il metodo Duo push per i dispositivi mobili, quindi è necessario aggiungere un dispositivo telefonico.

Fare clic su [Aggiungi telefono](#).

Phones

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

Add 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 Security Key

5. Digitare il numero di telefono dell'utente e fare clic su Aggiungi telefono.

Add Phone



[Learn more about Activating Duo Mobile](#)

Type

Phone

Tablet

Phone number



[Show extension field](#)

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



Add Phone

6. Nel pannello di sinistra Duo Admin, passare a Users e fare clic sul nuovo utente.

Dashboard > Users

Users


Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

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** Bypass Users **0** Locked Out

Select (0) ... [Export](#) Search

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/>	duovpn		...@...i.com	1		Active	Mar 8, 2022 6:50 PM
<input type="checkbox"/>				1		Active	Mar 5, 2022 7:04 PM
<input type="checkbox"/>				1		Active	Never authenticated
<input type="checkbox"/>	duovpn		...@...o.com	1		Active	Mar 5, 2022 7:16 PM




 Nota: se al momento non hai accesso al telefono, puoi selezionare l'opzione email.

7. Passare alla sezione Telefoni e fare clic su Attiva Duo Mobile.

Phones

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

[Add Phone](#)

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

8. Fare clic su Generate Duo Mobile Activation Code.

9. Seleziona Email per ricevere le istruzioni via email, digita il tuo indirizzo email e fai clic su Send Instructions by email (Invia istruzioni per posta elettronica).

10. Si riceve un messaggio di posta elettronica contenente le istruzioni, come illustrato nell'immagine.

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. Aprire Duo Mobile App dal dispositivo mobile e fare clic su Aggiungi, quindi selezionare Usa codice QR e digitalizzare il codice dall'e-mail di istruzioni.

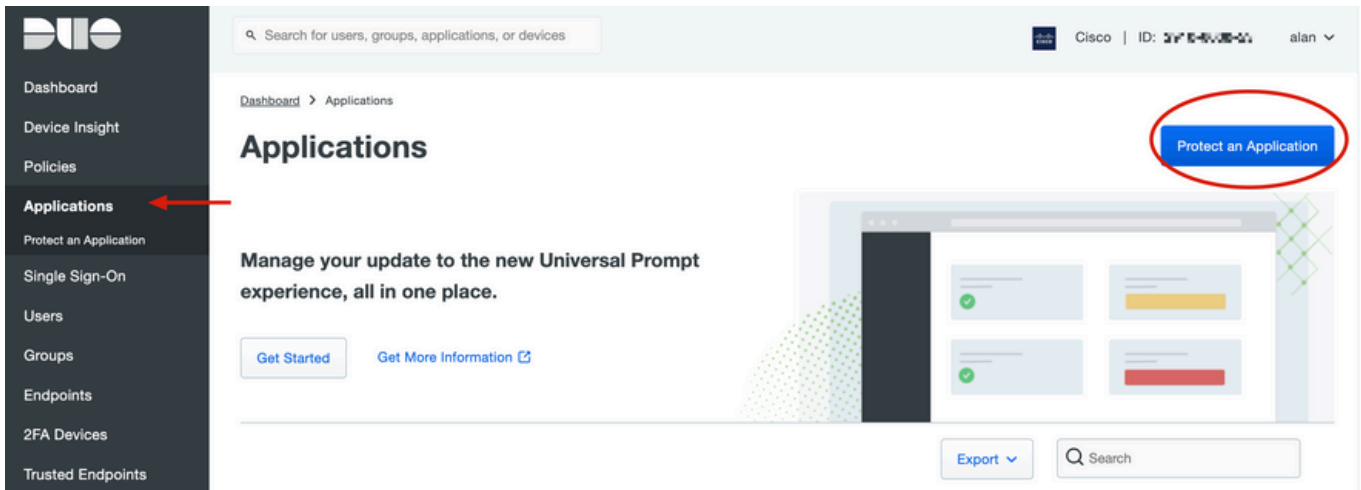
12. Il nuovo utente viene aggiunto alla tua Duo Mobile App.

Duo Auth Proxy Configuration

1. Scaricare e installare Duo Auth Proxy Manager da <https://duo.com/docs/authproxy-reference>.

 Nota: in questo documento Duo Auth Proxy Manager è installato sullo stesso Windows Server che ospita i servizi Active Directory.

2. Nel pannello Duo Admin, passare ad Applicazioni e fare clic su Proteggi un'applicazione.



3. Sulla barra di ricerca, cerca Cisco ISE Radius.

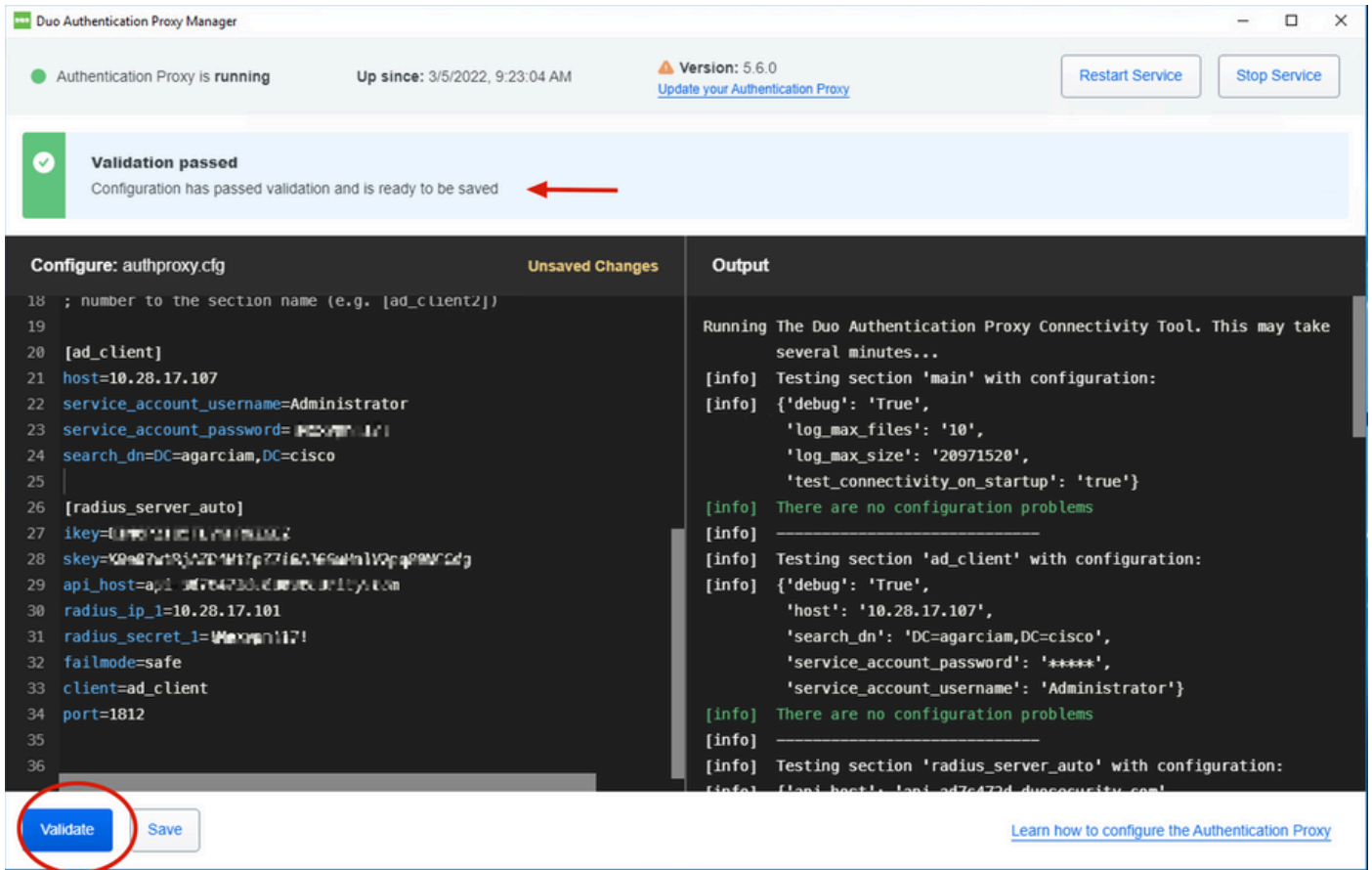
Protect an Application

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](#)

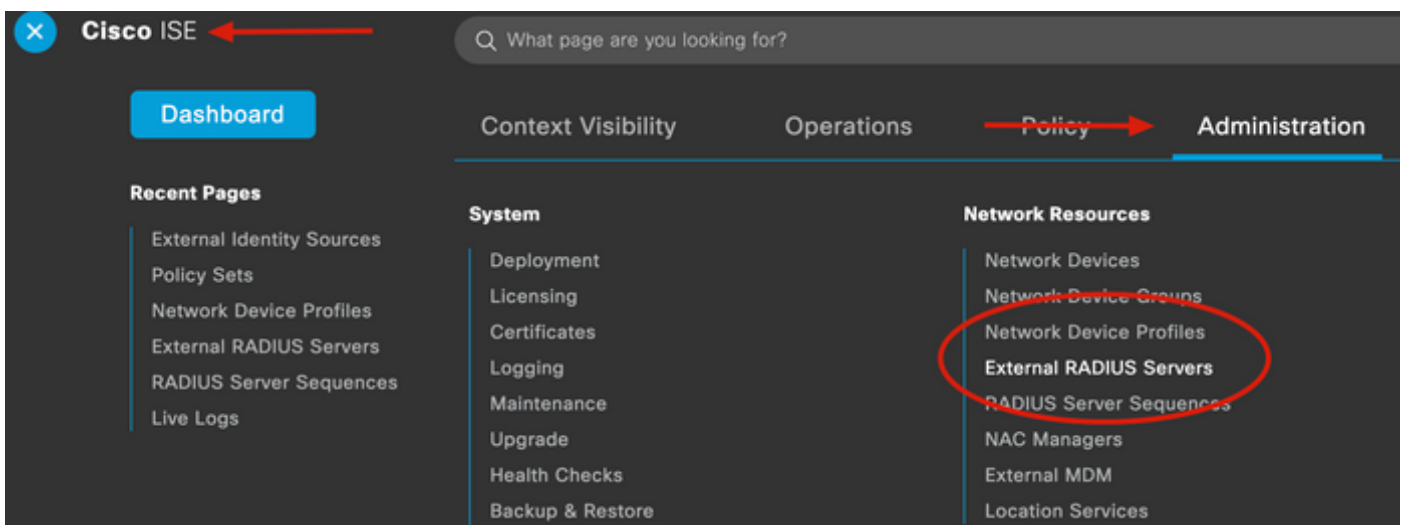
Choose an application below to get started.

4. Copiare la chiave di integrazione, la chiave segreta e il nome host dell'API. Queste informazioni sono necessarie per la configurazione del proxy di autenticazione Duo.



Configurazioni Cisco ISE

1. Accedere al portale di amministrazione di ISE.
2. Espandere la scheda Cisco ISE e passare ad Amministrazione, quindi fare clic su Risorse di rete e selezionare Server RADIUS esterni.



3. Nella scheda Server Radius esterni, fare clic su Aggiungi.

External RADIUS Servers

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

Name Name: Currently Sorted [^](#) **Description**

4. Compilare il campo vuoto con la configurazione RADIUS utilizzata in Duo Authentication Proxy Manager e fare clic su Invia.

* Name

Description

* Host IP

* Shared Secret [Show](#)

Enable KeyWrap

* Key Encryption Key [Show](#)

* Message Authenticator Code Key [Show](#)

Key Input Format ASCII HEXADECIMAL

* Authentication Port (Valid Range 1 to 65535)

* Accounting Port (Valid Range 1 to 65535)

* Server Timeout Seconds (Valid Range 1 to 120)

* Connection Attempts (Valid Range 1 to 9)

Radius ProxyFailover Expiration (Valid Range 1 to 600)

[Submit](#)

5. Passare alla scheda Sequenze server RADIUS e fare clic su Aggiungi.

RADIUS Server Sequences

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

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

6. Specificare il nome della sequenza e assegnare il nuovo server esterno RADIUS, quindi fare clic su Invia.

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

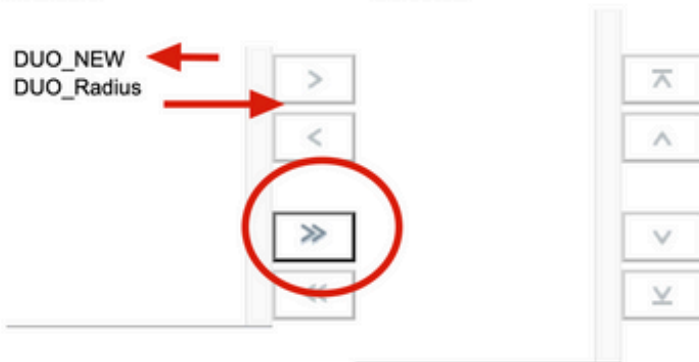
∨ User Selected Service Type

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

Available

* Selected

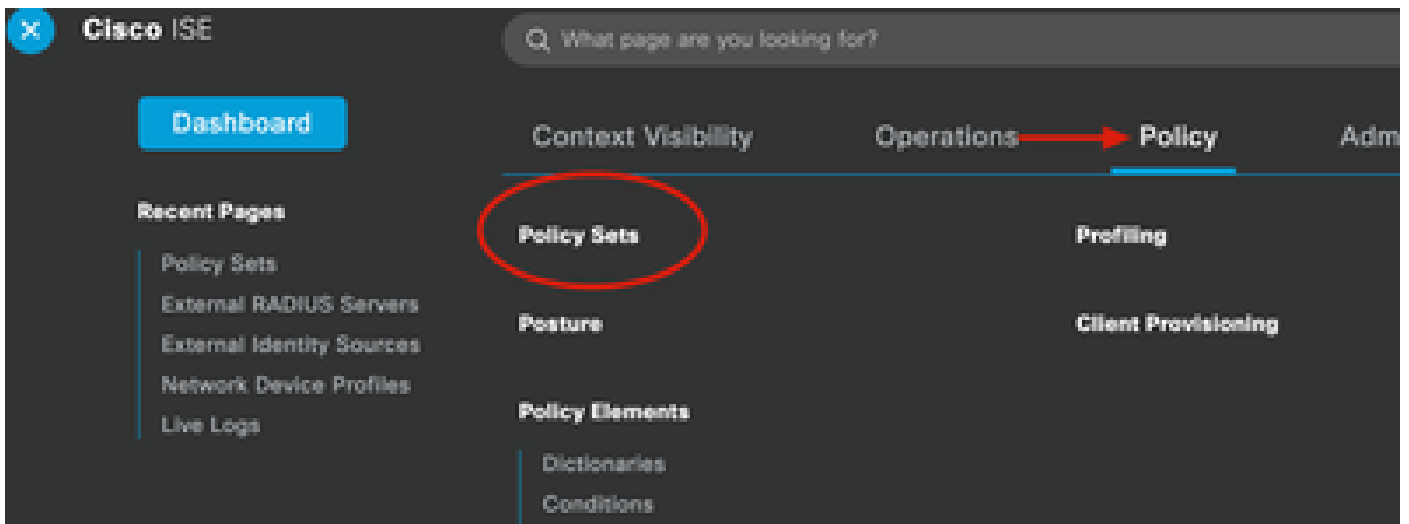
DUO_NEW
DUO_Radius




Remote accounting

Local accounting

7. Passare dal menu del dashboard a Criterio e fare clic su Set di criteri.



8. Assegnate la sequenza RADIUS al criterio di default.

 Nota: in questo documento viene applicata la sequenza Duo a tutte le connessioni, quindi viene utilizzato il criterio predefinito. L'assegnazione dei criteri può variare in base ai requisiti.

Policy Sets Reset [Reset Policyset Hitcount](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
			Radius-User-Name EQUALS isevpn	Default Network Access	3
			Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence	22
	Default	Default policy set		Default Network Access	0

Allowed Protocols

- Default Network Access
- Proxy Sequence
- DUO_NEW
- DUO_Sequence**

Configurazione Cisco ASA RADIUS/ISE

1. Configurare il server ISE RADIUS in gruppi di server AAA, passare a Configurazione, quindi fare clic su Gestione dispositivi ed espandere la sezione Utenti/AAA, quindi selezionare Gruppi di server AAA.

Bookmarks

To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".

Go Delete

Configuration

AAA Server Groups

Server Group	Pro
ISE	RA
LOCAL	LO
ad-agarciam	LD

Device Management


- > Management Access
- > Licensing
- > System Image/Configuration
- > High Availability and Scalability
- > Logging
- Smart Call-Home
- Cloud Web Security
- Service Module Settings
- Users/AAA
 - AAA Server Groups
 - LDAP Attribute Map
 - AAA Kerberos
 - Authentication Prompt
 - AAA Access
 - Dynamic Access Policies
 - User Accounts
 - Password Policy
 - Change My Password
 - Login History
- > Certificate Management
- > DHCP
- > DNS
- REST API Agent

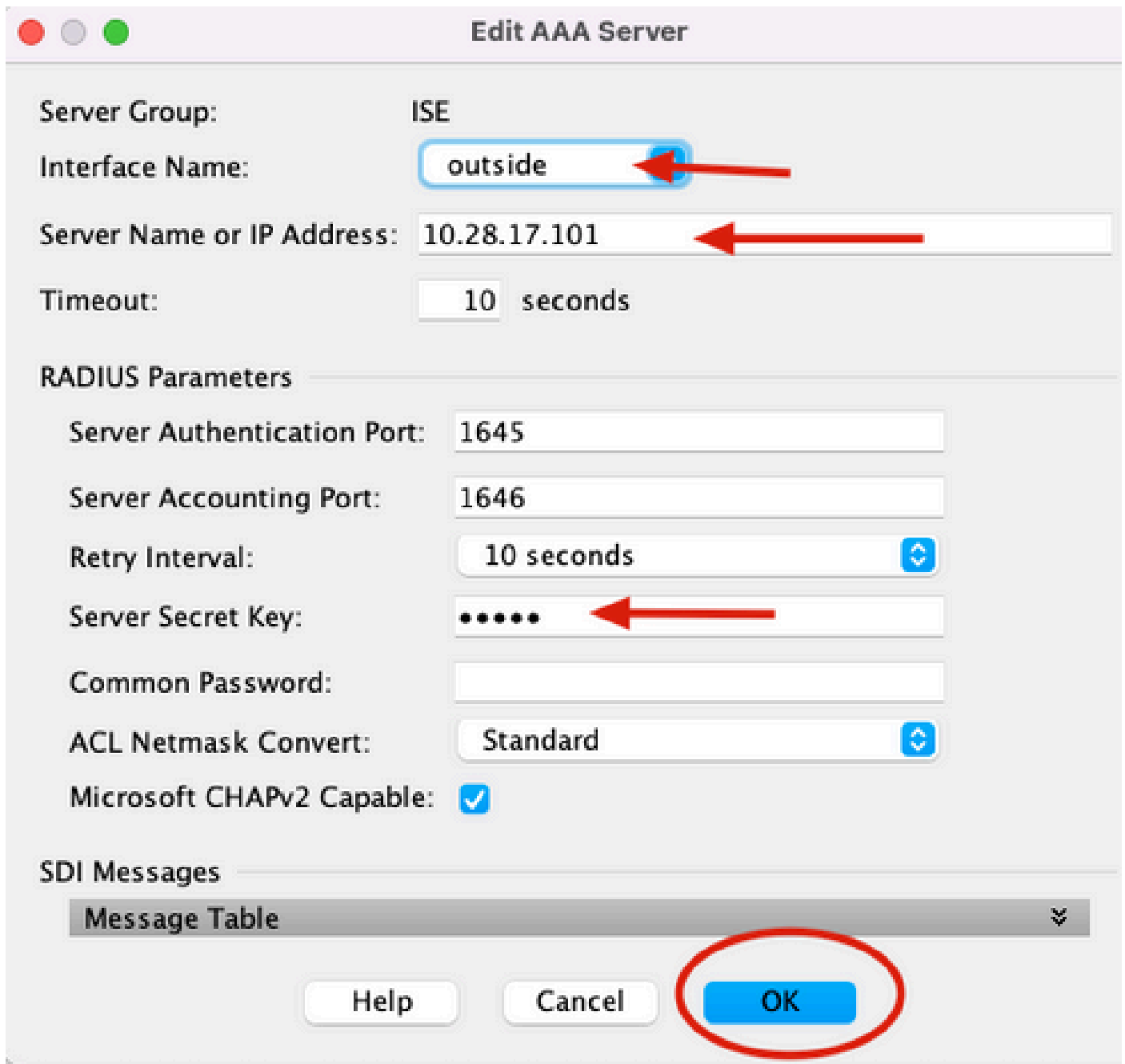
Find:

Servers in the Selected

Server Name or IP Address
10.28.17.101

, selezionare il nome dell'interfaccia, specificare l'indirizzo IP del server ISE e digitare la chiave segreta RADIUS, quindi fare clic su Ok.

 Nota: tutte queste informazioni devono corrispondere a quelle specificate in Duo Authentication Proxy Manager.



Edit AAA Server

Server Group: ISE

Interface Name: outside

Server Name or IP Address: 10.28.17.101

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: *****

Common Password:

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

Message Table

Help Cancel **OK**

Configurazione CLI.

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

Configurazione VPN di accesso remoto Cisco ASA

```
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. Apri l'app Anyconnect sul tuo dispositivo PC. Specificare il nome host dell'headend VPN ASA e accedere con l'utente creato per l'autenticazione secondaria Duo, quindi fare clic su OK.



2. È stata ricevuta una notifica di push Duo sul dispositivo mobile Duo dell'utente specificato.
3. Aprire la notifica di Duo Mobile App e fare clic su Approva.

14:41

Lunes, 14 de marzo

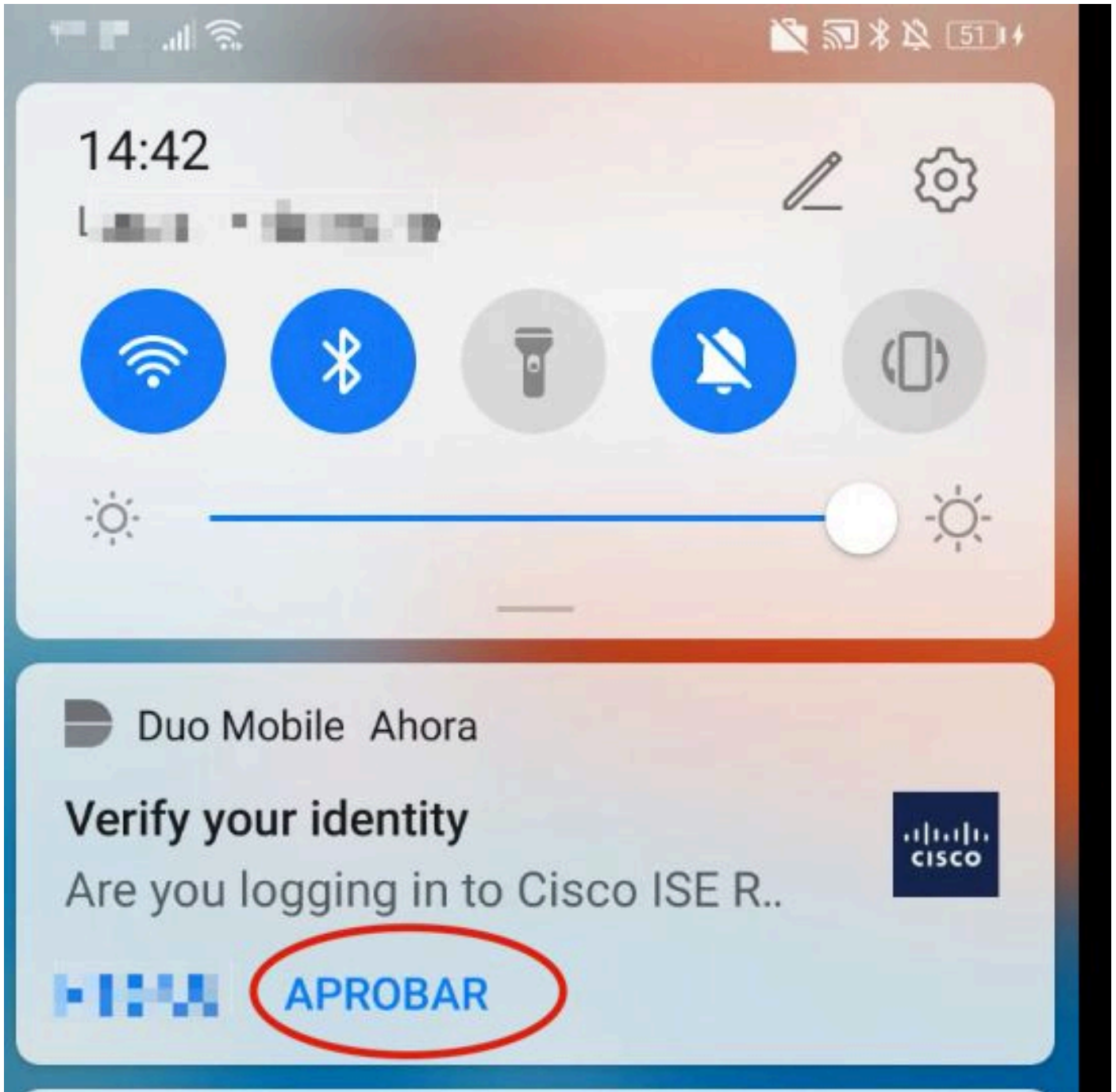


Duo Mobile Ahora

Verify your identity

Are you logging in to Cisco ISE R..





4. Accettare il banner e stabilire la connessione.



VPN:

Please respond to banner.

192.168.100.100



Connect

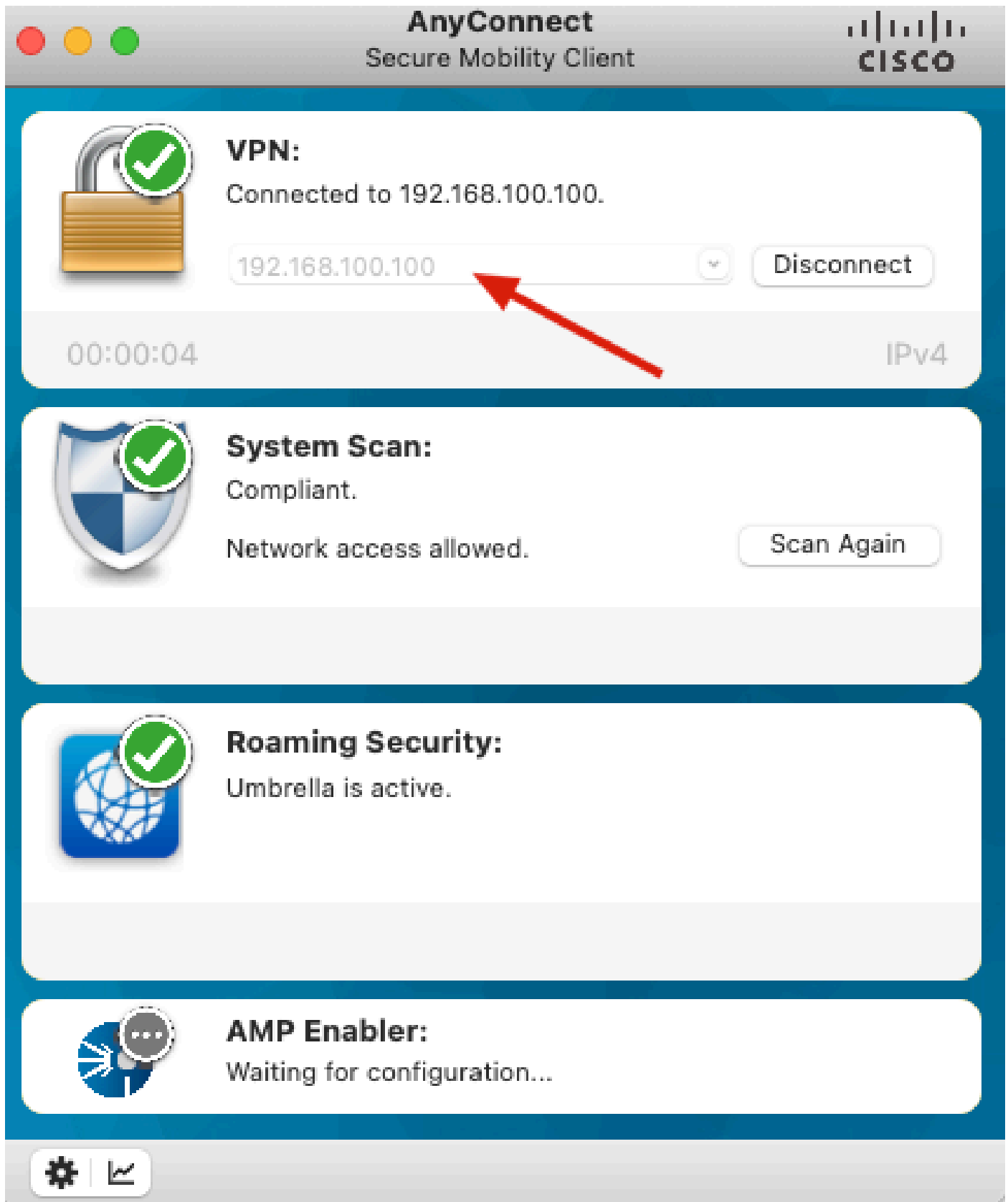
Cisco AnyConnect - Banner

This connection is for DUO authorized users only!

Disconnect

Accept






Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Duo Authentication Proxy viene fornito con uno strumento di debug che visualizza i motivi dell'errore.

Debug del lavoro

 Nota: le informazioni successive sono memorizzate in C:\Program Files\Duo Proxy di autenticazione di sicurezza\log\connectivity_tool.log.

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': 'api.10.28.17.101',
      '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': 'sal-adsrv01.ad.cisco.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. Problemi di connettività, IP errato, FQDN/nome host non risolvibile nella configurazione di Active Directory.

```
[ad_client]
```

```
host=10.28.17.106
```



```
service_account_username=Administrator
```

```
service_account_password=!H...p...17!!
```

```
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. Password errata per l'utente Administrator in Active Directory.

```
[ad_client]
```

```
host=10.28.17.107
```

```
service_account_username=Administrator
```

```
service_account_password=!H...p...17!!
```



```
search_dn=DC=agarciam,DC=cisco
```

Debug

```
[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. Dominio di base errato.

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!P@ssw0rd!
search_dn=DC=agarciam,DC=ciscoo ←
```

Debug

```
[info] The Auth Proxy was able to bind as Administrator.
[error] The Auth Proxy got an error searching the LDAP DN DC=agarciam,DC=ciscoo.
[debug] Exception: referral: 0000202B: RefErr: DSID-031007F9, data 0, 1 access points
        ref 1: 'agarciam.ciscoo'
```

4. Valore RADIUS chiave errato.

The screenshot shows a network traffic capture in Wireshark. The top pane shows a list of packets, with two RADIUS packets highlighted. The bottom pane shows the details of the selected packet (No. 1511, Time 6020.521457, Source 10.28.17.101, Destination 10.28.17.107, Protocol RADIUS, Length 877). The details pane shows the RADIUS protocol structure, including the Code (Access-Request), Packet identifier (0x1f), Length (835), Authenticator, and Attribute Value Pairs (AVPs). The AVP t=User-Name(1) l=8 val=duovpn is highlighted with a red arrow.

No.	Time	Source	Destination	Protocol	Length	Info
1511	6020.521457	10.28.17.101	10.28.17.107	RADIUS	877	Access-Request id=31
1513	6024.344735	10.28.17.107	10.28.17.101	RADIUS	191	Access-Accept id=31

```

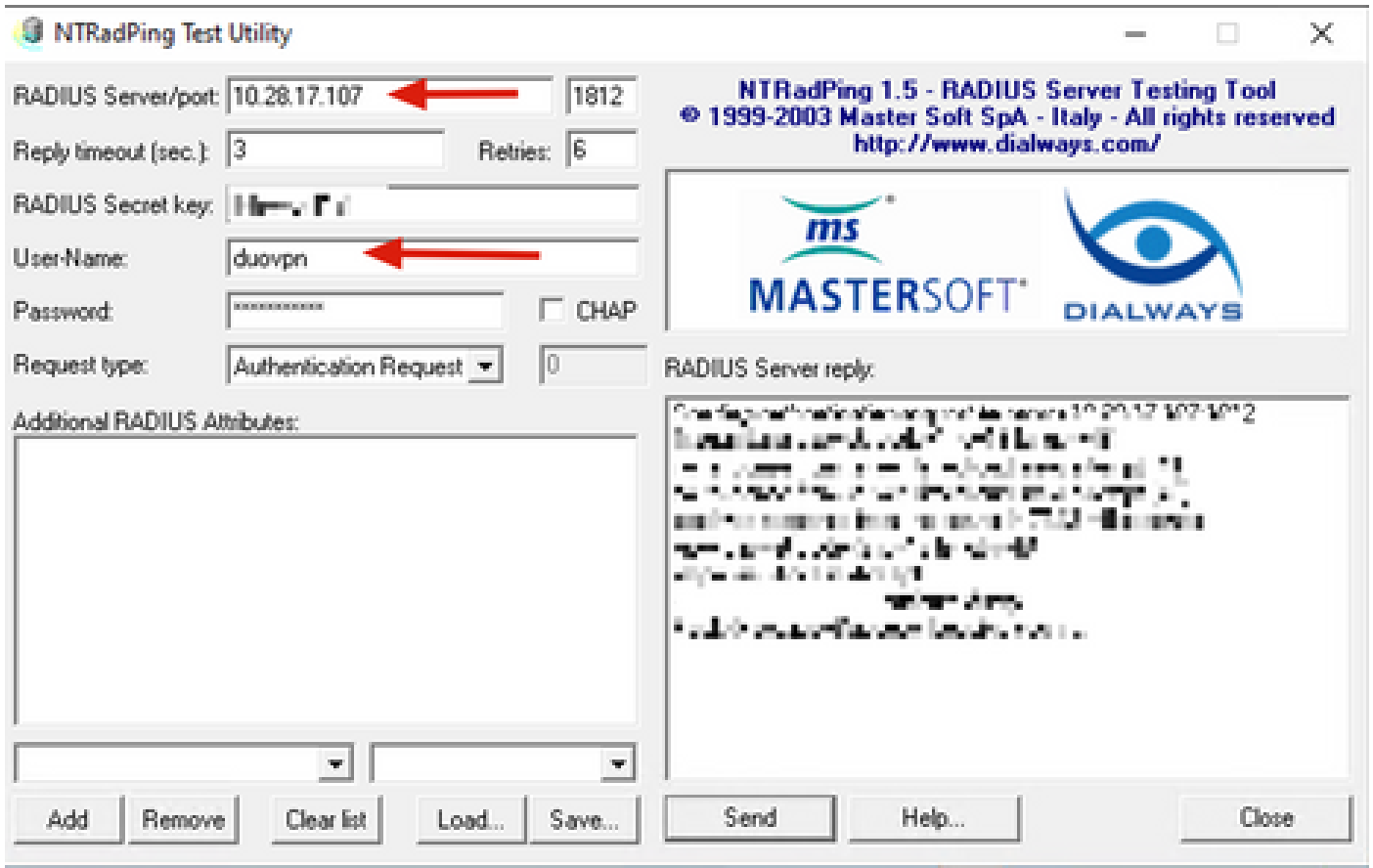
> Frame 151115: 877 bytes on wire (7016 bits), 877 bytes captured (7016 bits) on interface \Device\NPF_{CA092CEE-5...
> Ethernet II, Src: VMware_b3:a4:2f (00:50:56:b3:a4:2f), Dst: VMware_b3:b4:3e (00:50:56:b3:b4:3e)
> Internet Protocol Version 4, Src: 10.28.17.101, Dst: 10.28.17.107
> User Datagram Protocol, Src Port: 42022, Dst Port: 1812
v RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x1f (31)
  Length: 835
  Authenticator: 38a28ca3ca6bbc261819c5304b1be6e3
  [The response to this request is in frame 151332]
  Attribute Value Pairs
    > AVP: t=User-Name(1) l=8 val=duovpn
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=NAS-IP-Address(4) l=6 val=192.168.100.100
    > AVP: t=NAS-Port(5) l=6 val=344064
    > AVP: t=Called-Station-Id(30) l=17 val=192.168.100.100
    > AVP: t=Calling-Station-Id(31) l=13 val=M.##.!!.!
    > AVP: t=Proxy-State(33) l=25 val=466972737450726f78793d31302e32382e31372e313031
    > AVP: t=Proxy-State(33) l=76 val=436973636f205365637572652041435337366535323735612d396362302d313165632d63...
    > AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)
    > AVP: t=Tunnel-Client-Endpoint(66) l=13 val=10.99.65.53
  
```

6. Per verificare il corretto funzionamento del server proxy di autenticazione Duo, Duo fornisce lo strumento [NTRadPing](#) per simulare i pacchetti di richiesta di accesso e la risposta con Duo.

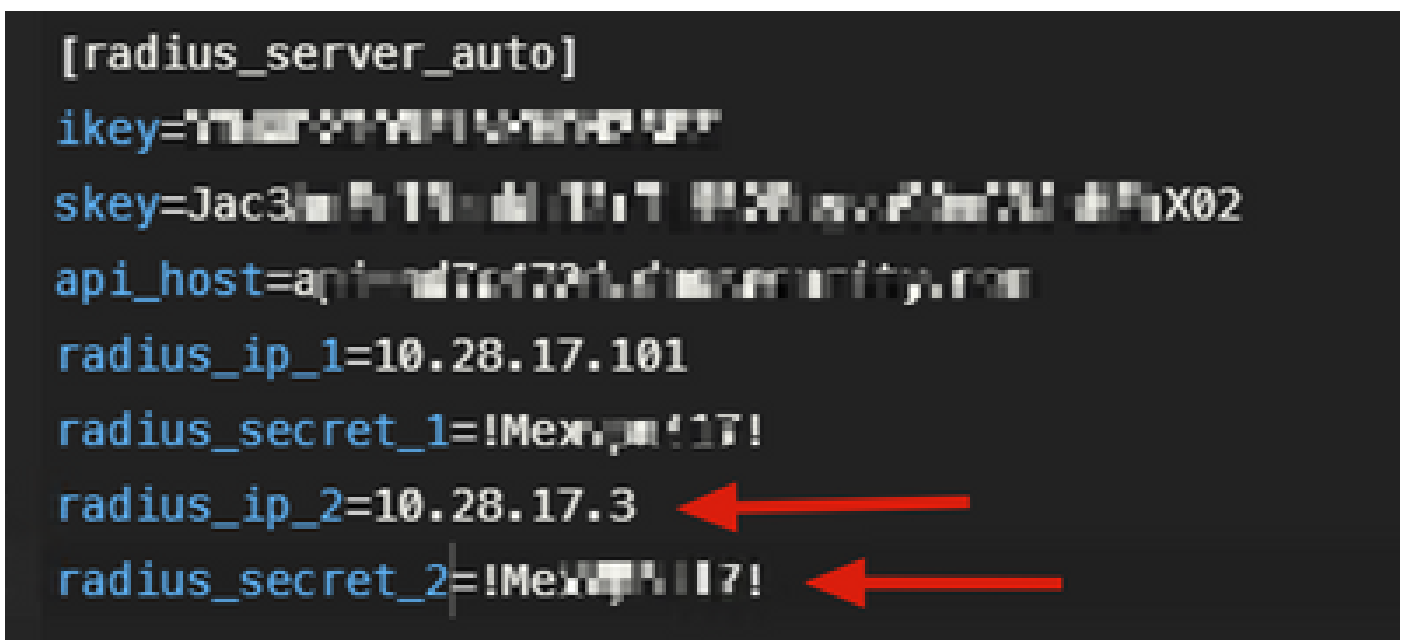
6.1 Installare NTRadPing su un PC diverso e generare traffico.

Nota: nell'esempio viene utilizzato il computer Windows 10.28.17.3.

6.2 Eseguire la configurazione con gli attributi utilizzati nella configurazione ISE Radius.



6.3 Configurare Duo Authentication Proxy Manager come segue.



6.4. Passare allo strumento NTRadPing e fare clic su Invia. Si riceve una notifica push Duo sul dispositivo mobile assegnato.

NTRadPing Test Utility

RADIUS Server/port: 10.28.17.107 1812

Reply timeout (sec.): 3 Retries: 6

RADIUS Secret key: !Mexvpr!17!

User-Name: duovpn ←



Password: ██████████ CHAP

Request type: Authentication Request 0

Additional RADIUS Attributes:

Buttons: Add Remove Clear list Load... Save... Send Help... Close

NTRadPing 1.5 - RADIUS Server Testing Tool
 © 1999-2003 Master Soft SpA - Italy - All rights reserved
<http://www.dialways.com/>

RADIUS Server reply:

```

Sending authentication request to server 10.28.17.107:1812
Transmitting packet, code=1 id=12 length=46
no response from server (timed out), new attempt (#1)
received response from the server in 4000 milliseconds
reply packet code=2 id=12 length=49
response: Access-Accept ←
..... attribute dump .....
Reply-Message=Success. Logging you in... ←
    
```

700	20.866684	10.28.17.3	10.28.17.107	RADIUS	88 Access-Request id=13, Duplicate Request
737	22.184895	10.28.17.107	10.28.17.3	RADIUS	90 Access-Accept id=13 ←

```

> Frame 700: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{CA092CEE-552B-4E0A-9310-2D5231600D60}, id 0
> Ethernet II, Src: VMware_b3:f2:72 (00:50:56:b3:f2:72), Dst: VMware_b3:b4:3e (00:50:56:b3:b4:3e)
> Internet Protocol Version 4, Src: 10.28.17.3, Dst: 10.28.17.107
> User Datagram Protocol, Src Port: 51188, Dst Port: 1812
v RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0xd (13)
  Length: 46
  Authenticator: 202020202031363436393335333230
  [Duplicate Request Frame Number: 532]
  [The response to this request is in frame 737]
v Attribute Value Pairs
  > AVP: t=User-Name(1) l=8 val=duovpn ←
  > AVP: t=User-Password(2) l=18 val=Encrypted
    
```


Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).