

Configurar a integração Duo com o Active Directory e o ISE para autenticação de dois fatores em clientes VPN Anyconnect/Acesso Remoto

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama e cenário de rede](#)

[Processo de comunicação](#)

[Configurações do Active Directory](#)

[Configurações Duo](#)

[Configuração do proxy de autenticação Duo](#)

[Configurações do Cisco ISE](#)

[Configuração do Cisco ASA RADIUS/ISE](#)

[Configuração de VPN de acesso remoto do Cisco ASA](#)

[Teste](#)

[Troubleshooting](#)

[Depurações de trabalho](#)

Introdução

Este documento descreve a integração por push do Duo com o AD e o ISE como autenticação de dois fatores para clientes AnyConnect conectados ao ASA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN RA no ASA
- Configuração RADIUS no ASA
- ISE
- Diretório ativo
- Aplicativos Duo

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

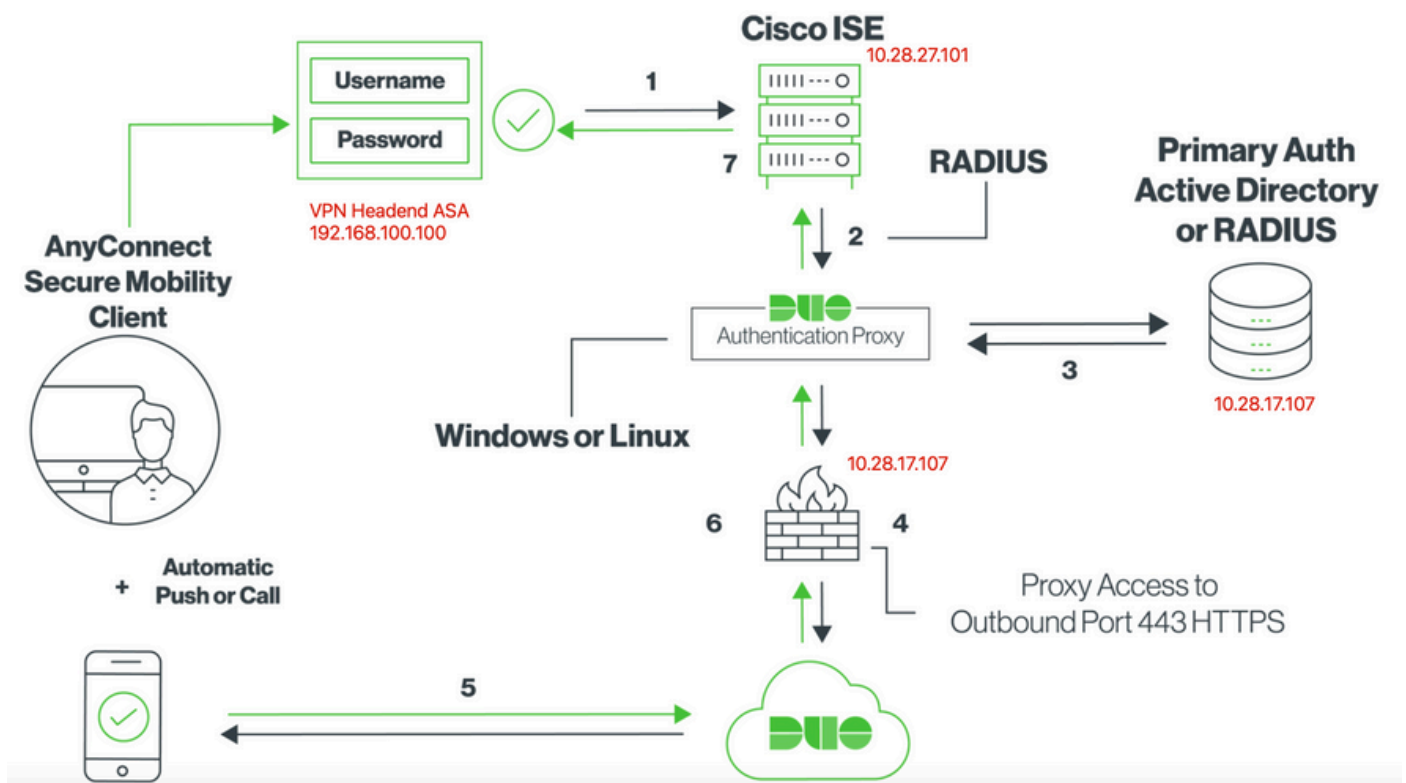
- Microsoft 2016 Server
- ASA 9.14(3)18
- Servidor ISE 3.0
- Servidor Duo
- Gerenciador de proxy de autenticação Duo

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve como configurar a integração por envio do Duo com o Active Directory (AD) e o Cisco Identity Service Engine (ISE) como autenticação de dois fatores para clientes AnyConnect que se conectam ao Cisco Adaptive Security Appliance (ASA).

Diagrama e cenário de rede



Processo de comunicação

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


1. Autenticação primária iniciada no Cisco ISE
2. O Cisco ISE envia a solicitação de autenticação para o proxy de autenticação Duo
3. A autenticação primária usa o Active Directory ou o RADIUS
4. Conexão de Proxy de Autenticação Duo estabelecida para Segurança Duo sobre a porta TCP 443
5. Autenticação secundária por meio do serviço Duo Security
6. O proxy de autenticação Duo recebe a resposta de autenticação
7. Acesso concedido ao Cisco ISE

Contas do usuário:

- Administrador do Active Directory: usado como a conta de diretório para permitir que o Proxy de Autenticação Duo se vincule ao servidor do Active Directory para autenticação primária.
- Usuário de teste do Active Directory
- Usuário de teste Duo para autenticação secundária

Configurações do Active Directory

O servidor Windows está pré-configurado com os serviços de domínio do Active Directory.

 Nota: Se o RADIUS Duo Auth Proxy Manager for executado na mesma máquina host do Active Directory, as funções NPS (Servidor de Políticas de Rede) deverão ser desinstaladas/excluídas; se ambos os serviços RADIUS forem executados, eles poderão entrar em conflito e afetar o desempenho.

Para obter a configuração do AD para autenticação e identidade de usuário em usuários de VPN de acesso remoto, alguns valores são necessários.

Todos esses detalhes devem ser criados ou coletados no Microsoft Server para que a configuração possa ser feita no servidor proxy ASA e Duo Auth.

Os principais valores são:

- Nome de domínio. Este é o nome de domínio do servidor. Neste guia de configuração, `agaricam.cisco` é o nome de domínio.
- Endereço IP/FQDN do servidor. O endereço IP ou FQDN usado para acessar o Microsoft Server. Se um FQDN for usado, um servidor DNS deverá ser configurado no ASA e no proxy Duo Auth para resolver o FQDN.

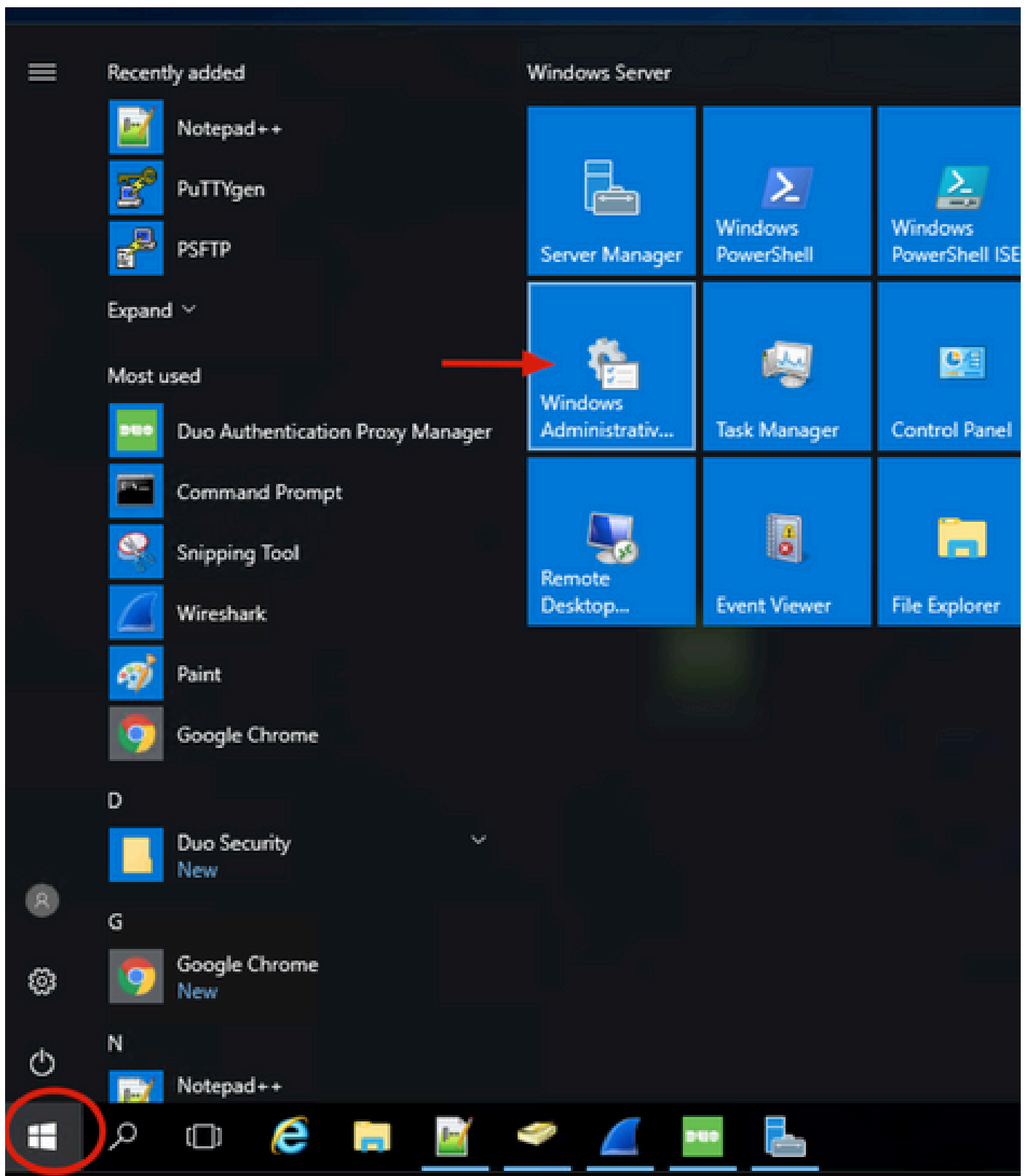
Neste guia de configuração, esse valor é `agaricam.cisco` (que é resolvido como `10.28.17.107`).

- Porta do servidor. A porta usada pelo serviço LDAP. Por padrão, LDAP e STARTTLS usam a porta TCP 389 para LDAP, e LDAP sobre SSL (LDAPS) usa a porta TCP 636.
- CA raiz. Se LDAPS ou STARTTLS for usado, a CA raiz usada para assinar o certificado SSL usado por LDAPS será necessária.

- Nome de usuário e senha do diretório. Essa é a conta usada pelo servidor proxy Duo Auth para vincular-se ao servidor LDAP e autenticar usuários e pesquisar usuários e grupos.
- Nome distinto (DN) de base e de grupo. O DN de base é o ponto de partida para o proxy de autenticação dupla e informa ao Active Directory para iniciar a pesquisa e autenticar usuários.

Neste guia de configuração, o domínio raiz `agaricam.cisco` é usado como DN base e DN de grupo é `Duo-USERS`.

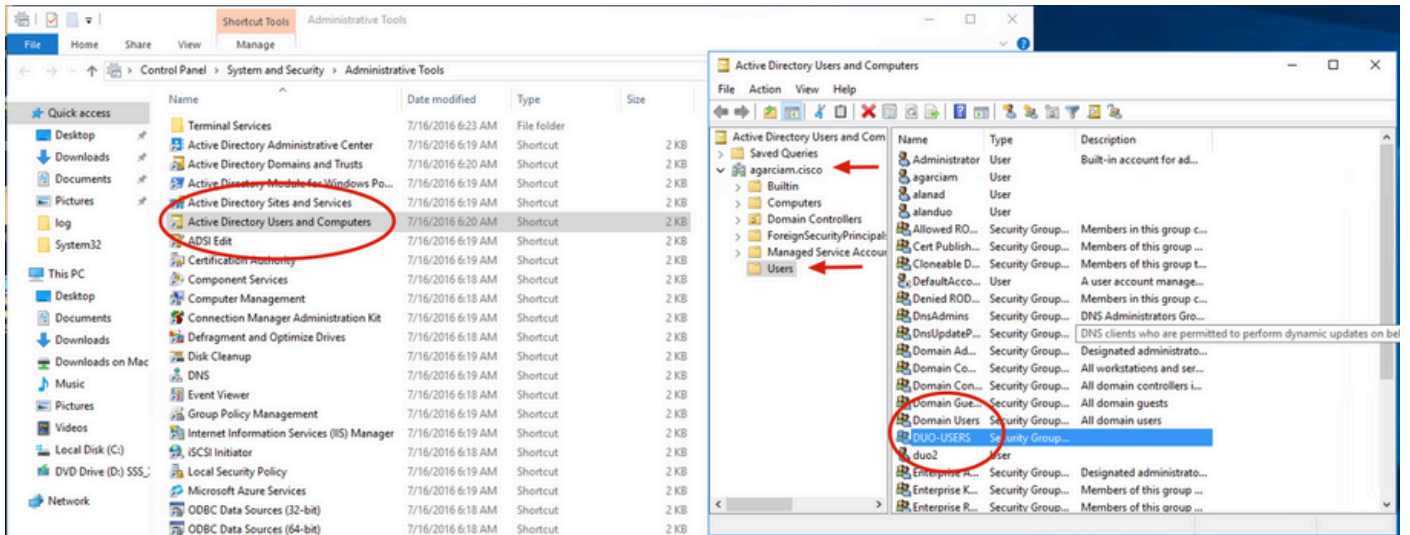
1. Para adicionar um novo usuário do Duo, no Windows Server, navegue para o ícone do Windows na parte inferior esquerda e clique em Ferramentas Administrativas do Windows, conforme mostrado na imagem.



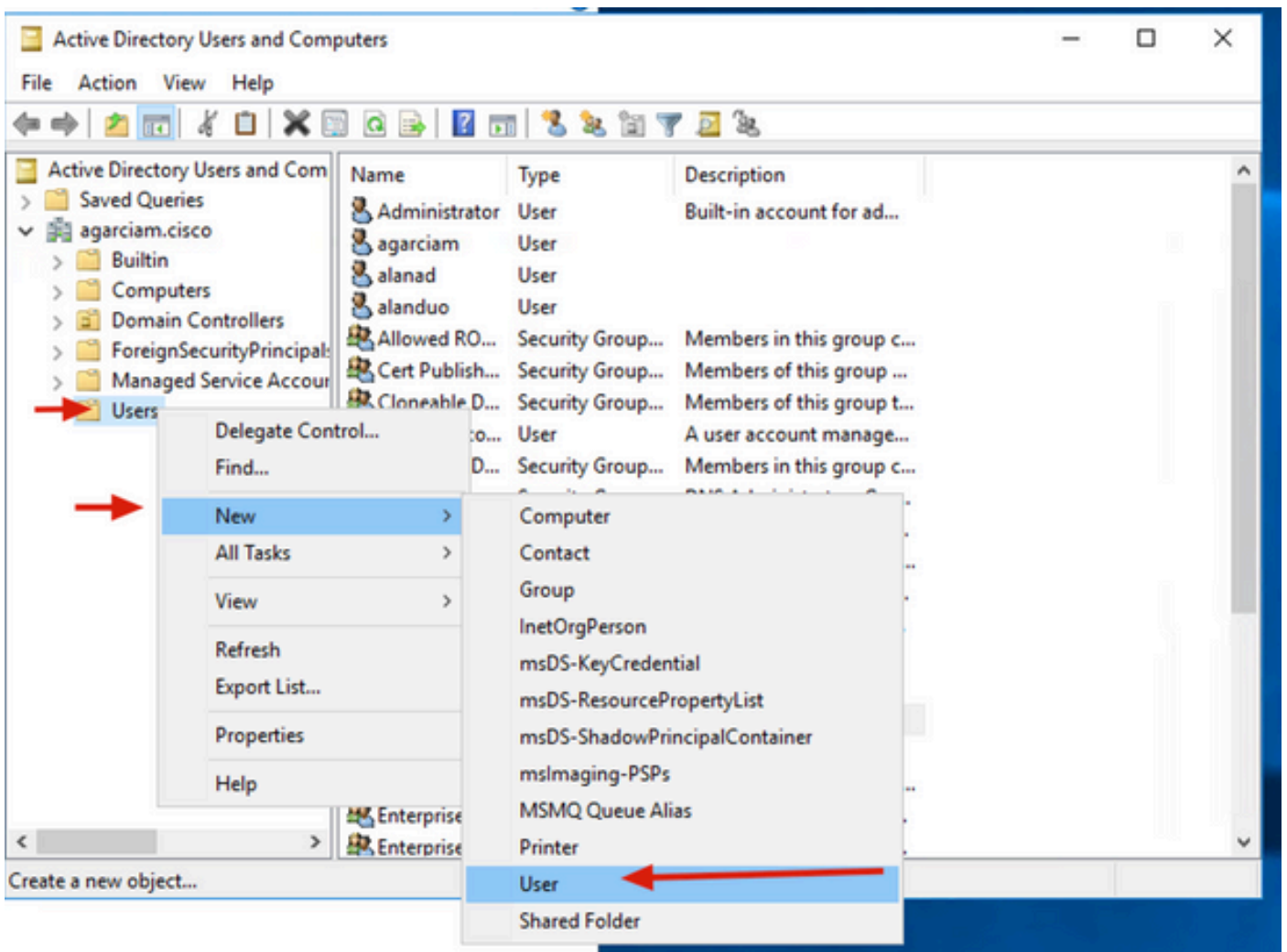
2. Na janela Ferramentas Administrativas do Windows, navegue até Usuários e Computadores do Active Directory.

No painel Usuários e computadores do Active Directory, expanda a opção de domínio e navegue até a pasta Usuários.

Neste exemplo de configuração, Duo-USERS é usado como o grupo de destino para a autenticação secundária.





3. Clique com o botão direito do mouse na pasta Users e selecione New > User, como mostrado na imagem.



4. Na janela Novo Usuário de Objeto, especifique os atributos de identidade para este novo usuário e clique em Próximo, conforme mostrado na imagem.


New Object - User X

 Create in: `agarciam.cisco/Users`

First name:  Initials:

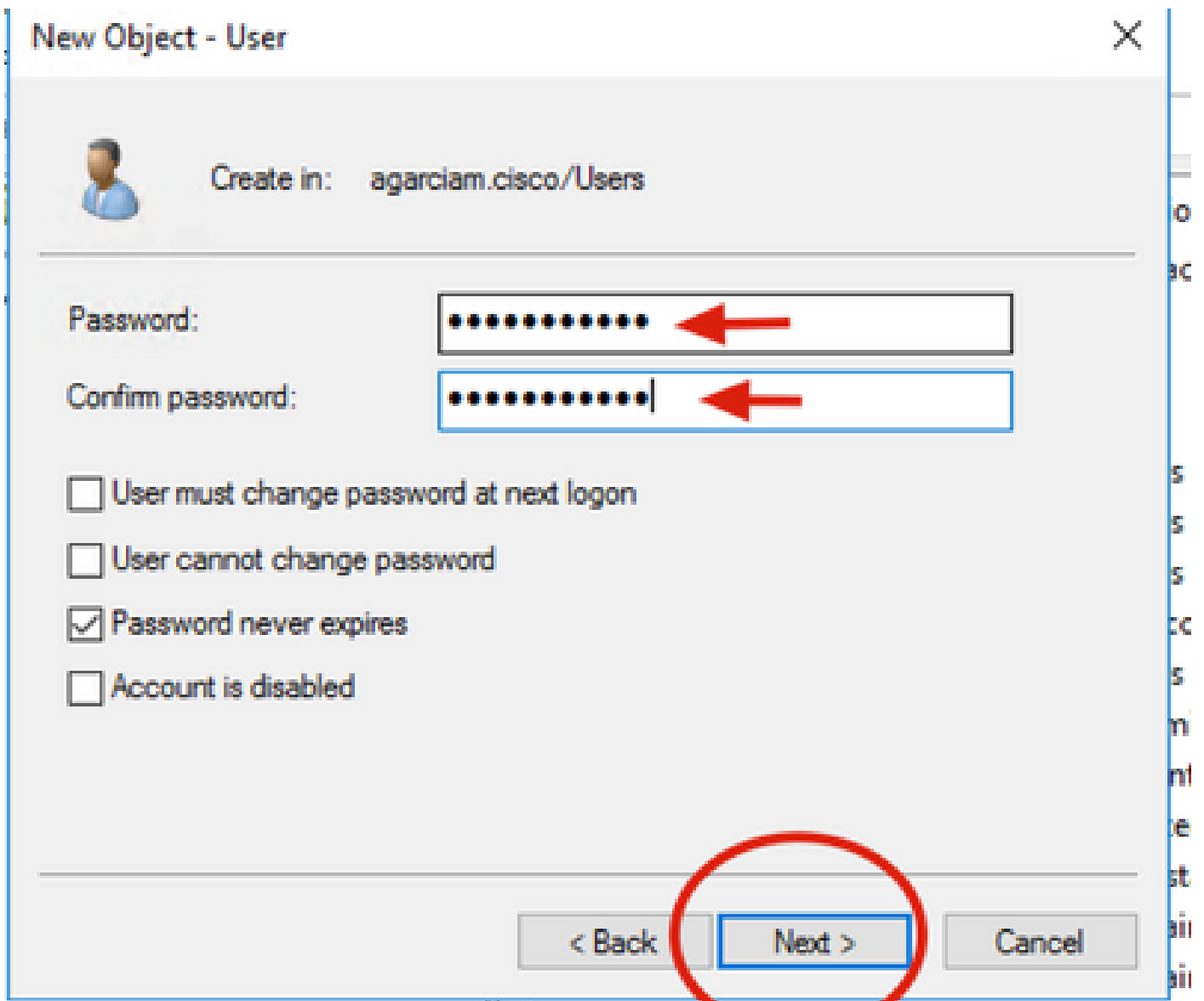
Last name:

Full name:

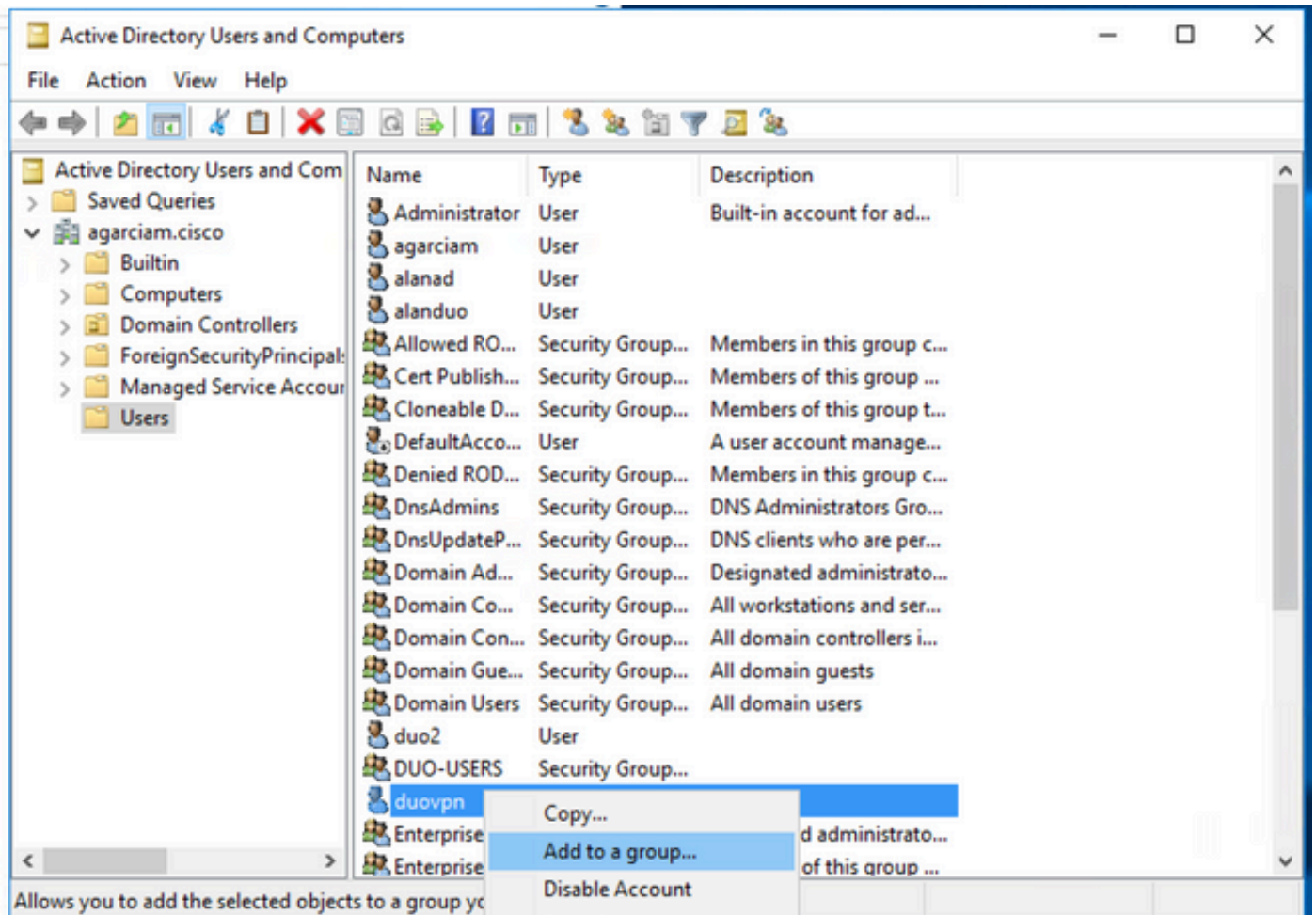
User logon name:
 

User logon name (pre-Windows 2000):

5. Confirme a senha e clique em Avançar, em seguida, em Concluir quando as informações do usuário forem verificadas.

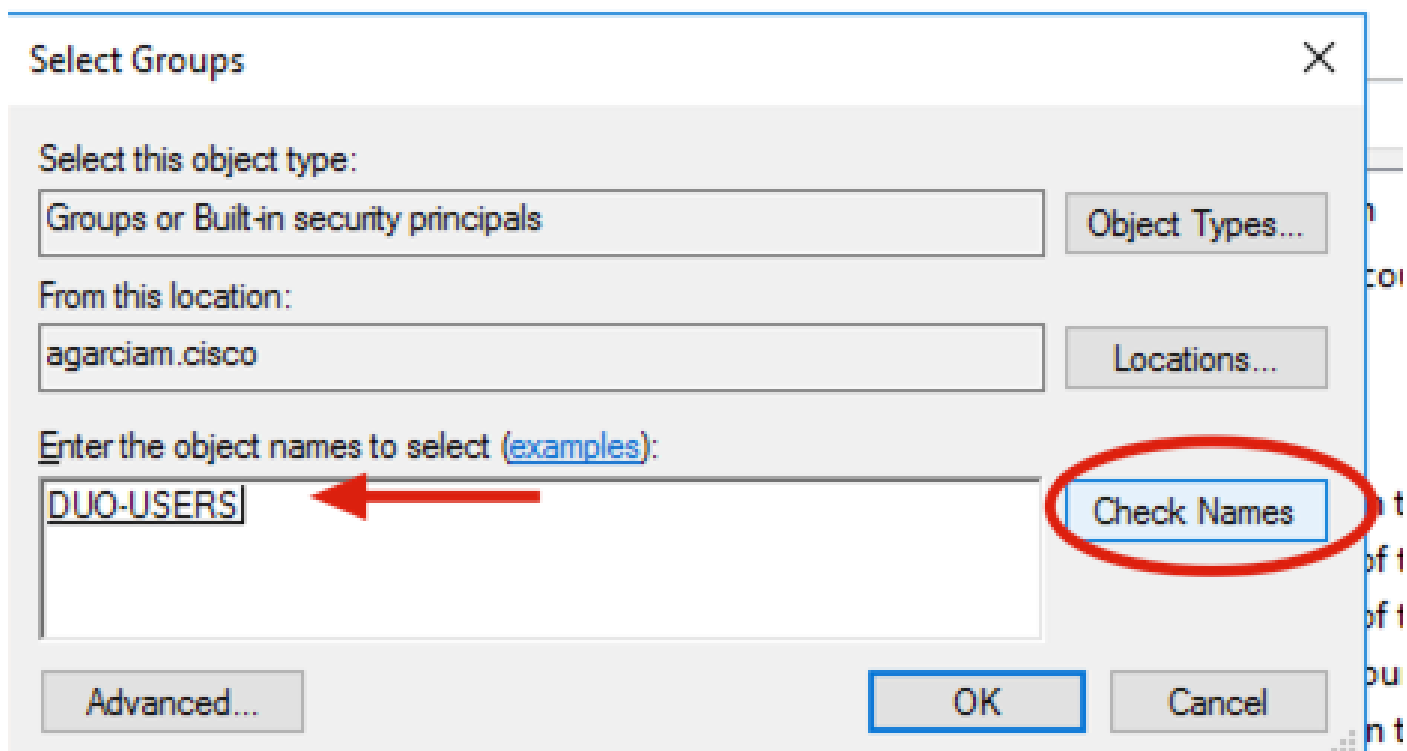


6. Atribua o novo usuário a um grupo específico, clique com o botão direito do mouse nele e selecione Adicionar a um grupo, como mostrado na imagem.



7. No painel Selecionar grupos, digite o nome do grupo desejado e clique em Verificar nomes.

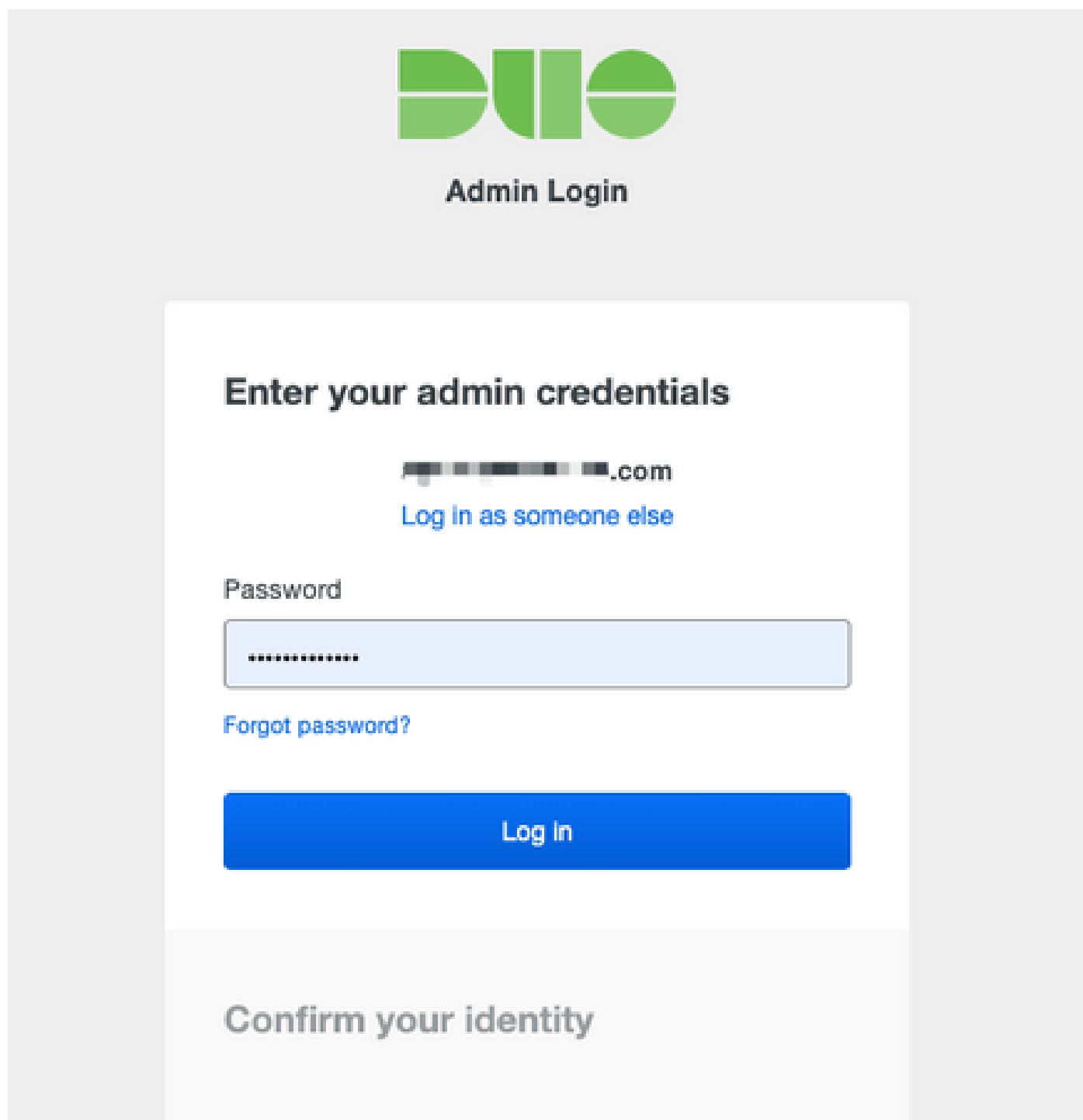
Em seguida, selecione o nome que corresponde aos seus critérios e clique em Ok.



8. Este é o usuário usado neste documento como exemplo.

Configurações Duo

1. Faça login no portal do Administrador do Dudo.



Duo

Admin Login

Enter your admin credentials

██████████@██████████.com

[Log in as someone else](#)

Password

.....

[Forgot password?](#)

Log In

Confirm your identity

2. No painel do lado esquerdo, navegue até Users, clique em Add User e digite o nome do usuário que corresponde ao seu nome de usuário do Active Domain e clique em Add User.

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. No painel do novo usuário, preencha a lacuna com todas as informações necessárias.

duovpn


 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. Em dispositivos do usuário, especifique o método de autenticação secundário.

 Nota: Neste documento, é usado o método Duo push for mobile devices, de modo que é necessário adicionar um dispositivo telefônico.

Clique em Adicionar telefone.

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. Digite o número de telefone do usuário e clique em Adicionar Telefone.

Add Phone



[Learn more about Activating Duo Mobile](#)

Type

Phone

Tablet

Phone number



[Show extension field](#)

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



6. No painel Admin do Duo à esquerda, navegue até Usuários e clique no novo usuário.

Dashboard > Users


Users

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

5 Total Users **0** Not Enrolled **2** Inactive Users **1** Trash **0** Bypass Users **0** Locked Out

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




| <input type="checkbox"/> | Username | Name | Email | Phones | Tokens | Status | Last Login |
|--------------------------|----------|------|--------------|--------|--------|--------|---------------------|
| <input type="checkbox"/> | duovpn | | ...@... .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"/> | | | | 1 | | Active | Never authenticated |
| <input type="checkbox"/> | | | | 1 | | Active | Mar 5, 2022 7:16 PM |

 Nota: Caso não tenha acesso ao seu telefone no momento, você pode selecionar a opção de e-mail.

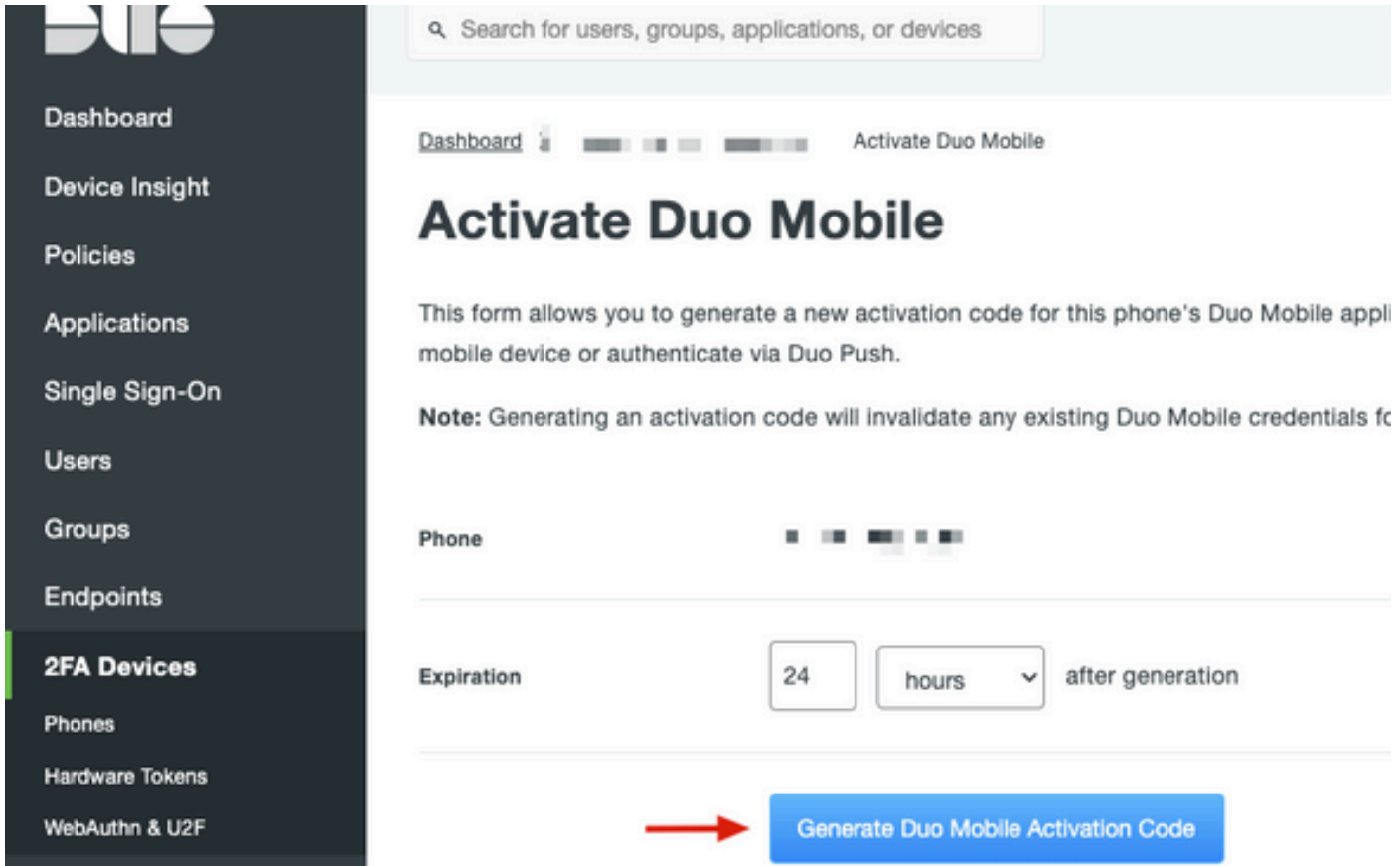
7. Navegue até a seção Telefones e clique em Ativate Duo Mobile.

Phones

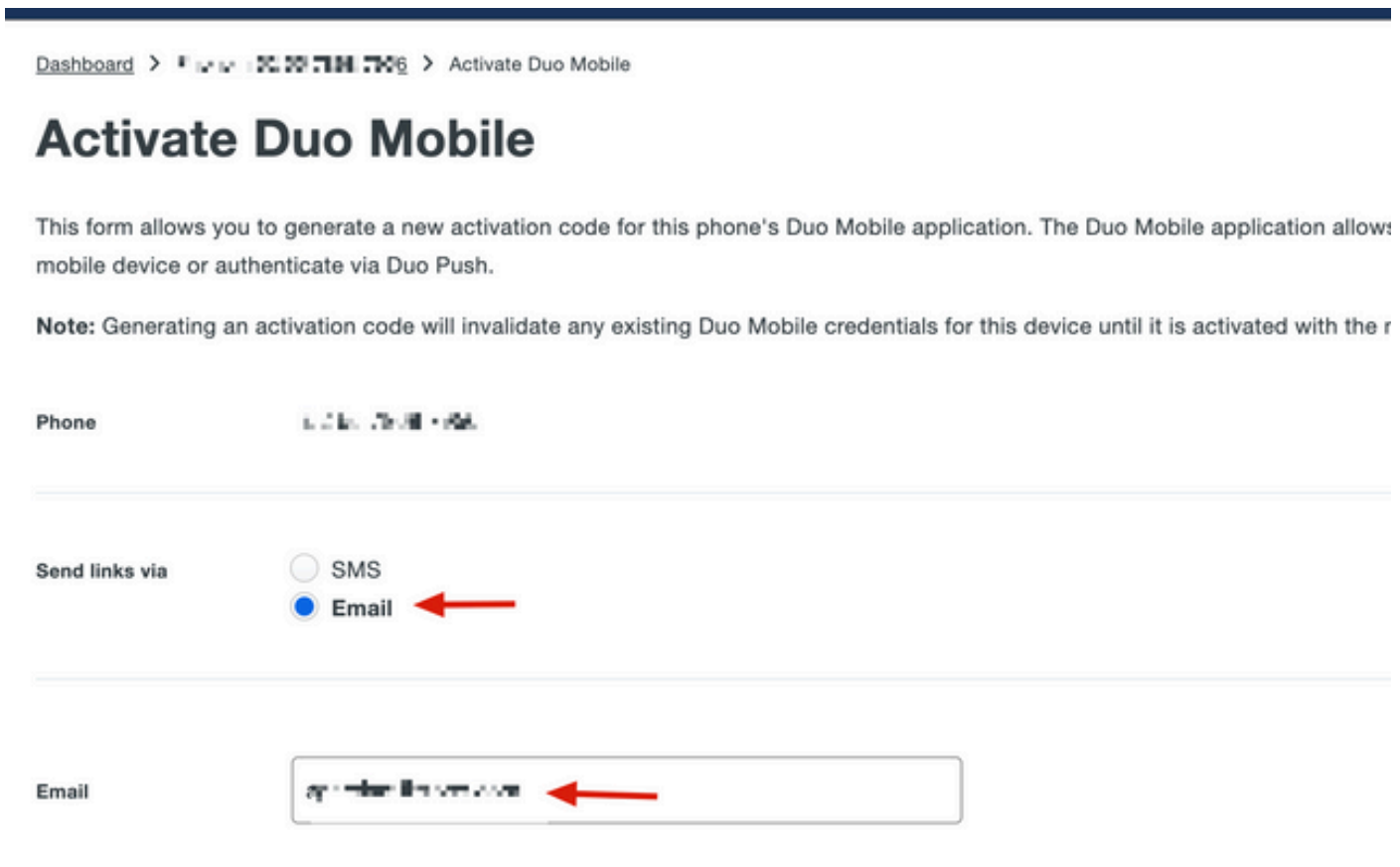
You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) [Add Phone](#)

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

8. Clique em Gerar Código de Ativação Móvel Duo.



9. Selecione Email para receber as instruções por e-mail, digite seu endereço de e-mail e clique em Enviar Instruções por e-mail.



10. Você receberá um e-mail com as instruções, conforme mostrado na imagem.

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. Abra o Duo Mobile App a partir do seu dispositivo móvel e clique em Adicionar, selecione Usar código QR e digitalize o código a partir do e-mail de instruções.

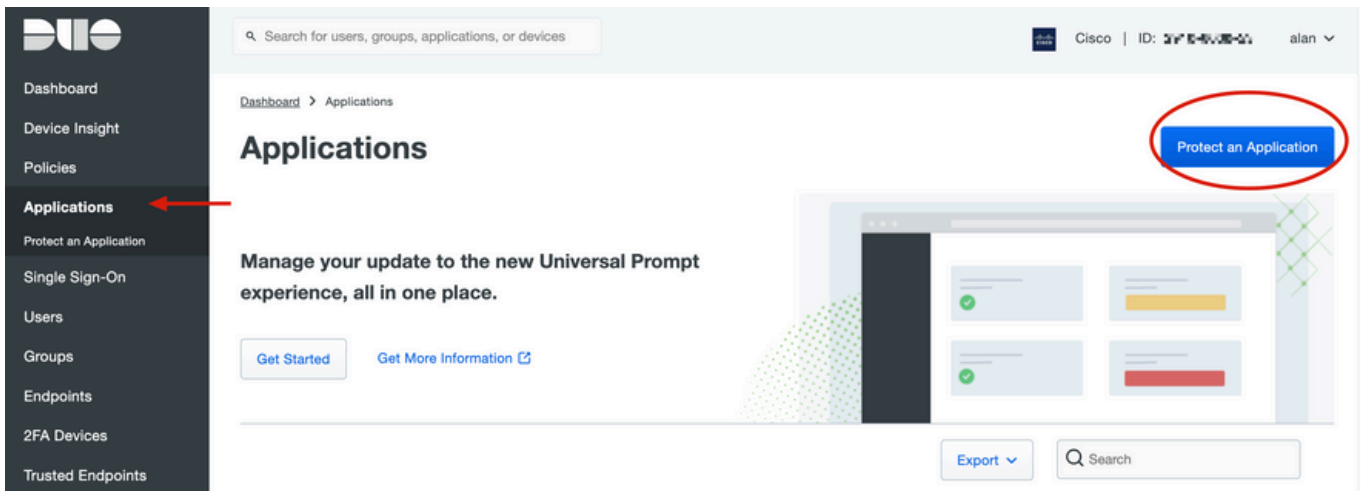
12. O novo usuário é adicionado ao seu aplicativo móvel Duo.

Configuração do proxy de autenticação Duo

1. Baixe e instale o Duo Auth Proxy Manager em <https://duo.com/docs/authproxy-reference>.

 Nota: Neste documento, o Duo Auth Proxy Manager está instalado no mesmo Windows Server que hospeda os serviços do Ative Directory.

2. No Painel de administração do Duo, navegue para Aplicativos e clique em Proteger um aplicativo.



3. Na barra de pesquisa, procure por 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. Copie a Chave de integração, a Chave de segurança e o Nome de host da API. Essas informações são necessárias para a configuração do Proxy de autenticação Duo.



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

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

[Copy](#)

Secret key

.....W6ho

[Copy](#)

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

API hostname

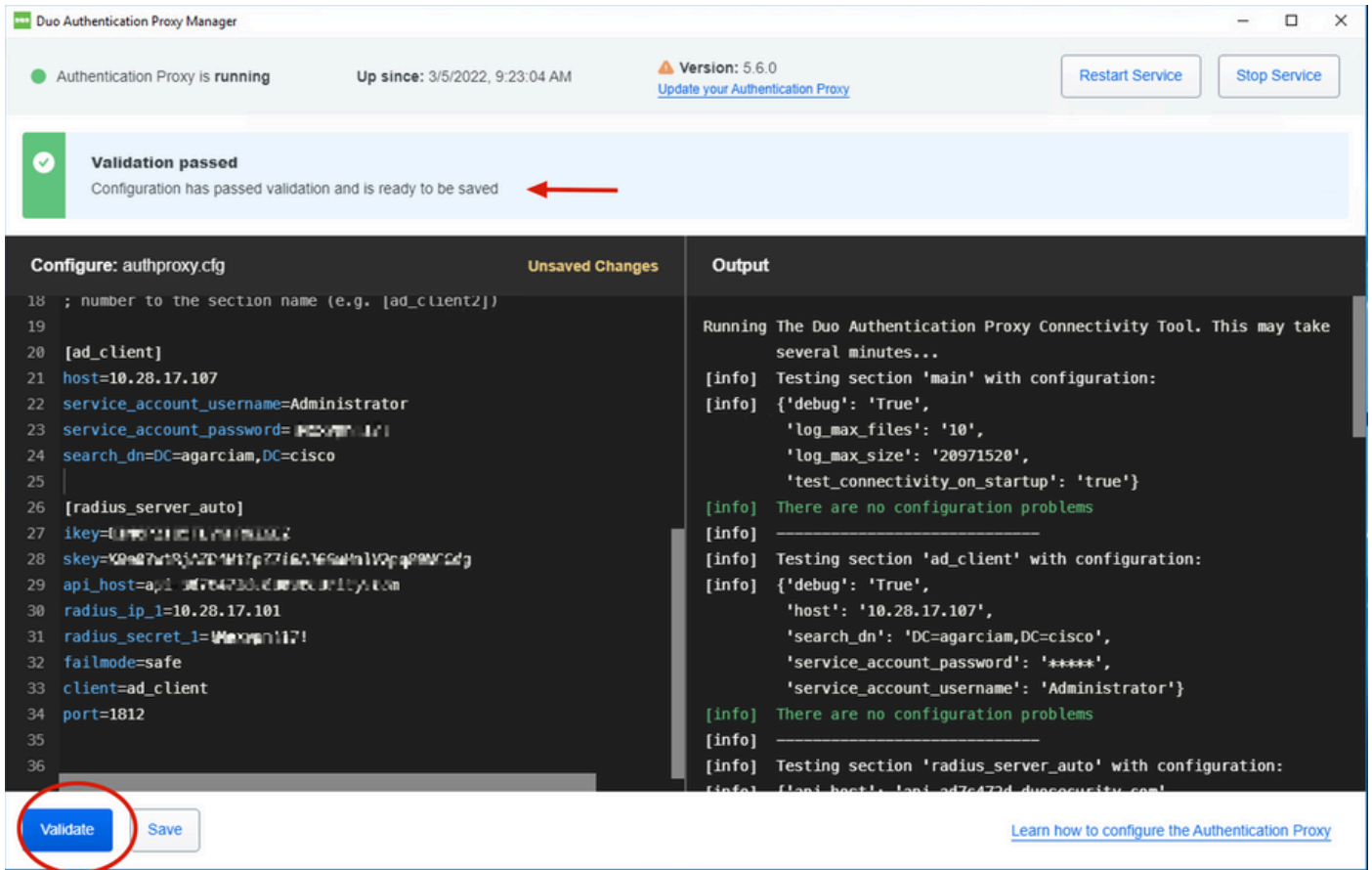
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

[Copy](#)

5. Execute o aplicativo Duo Authentication Proxy Manager e conclua a configuração do cliente do Active Directory e do ISE Radius Server e clique em Validate.

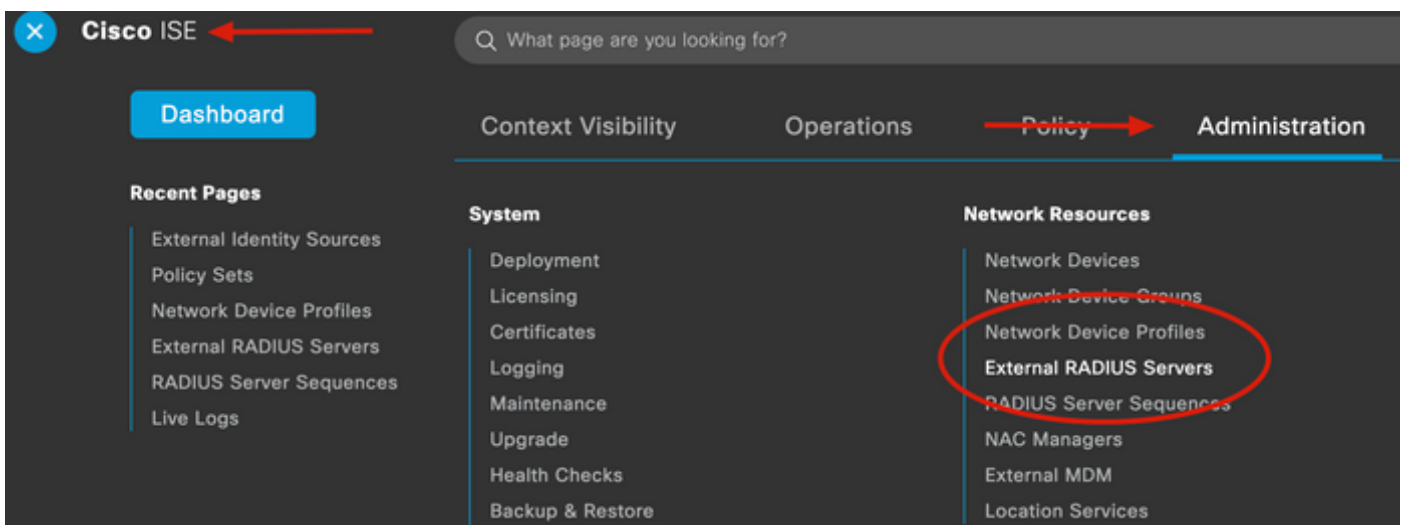


Observação: se a validação não for bem-sucedida, consulte a guia debug para obter detalhes e corrija-a de acordo.



Configurações do Cisco ISE

1. Faça login no portal do administrador do ISE.
2. Expanda a guia Cisco ISE e navegue até Administration, clique em Network Resources e clique em External RADIUS Servers.



3. Na guia External Radius Servers, clique em Add.

External RADIUS Servers

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

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

4. Preencha a lacuna com a configuração RADIUS usada no Duo Authentication Proxy Manager e clique em Submit.

* 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. Navegue até a guia RADIUS Server Sequences e clique em Add.

RADIUS Server Sequences

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

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

6. Especifique o nome da sequência e atribua o novo servidor Externo RADIUS, clique em Enviar.

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

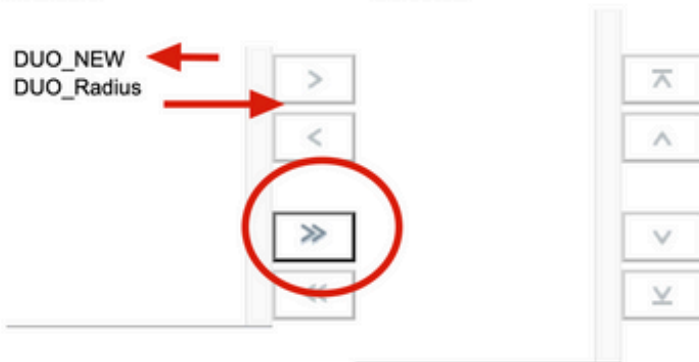
User Selected Service Type

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

Available

* Selected

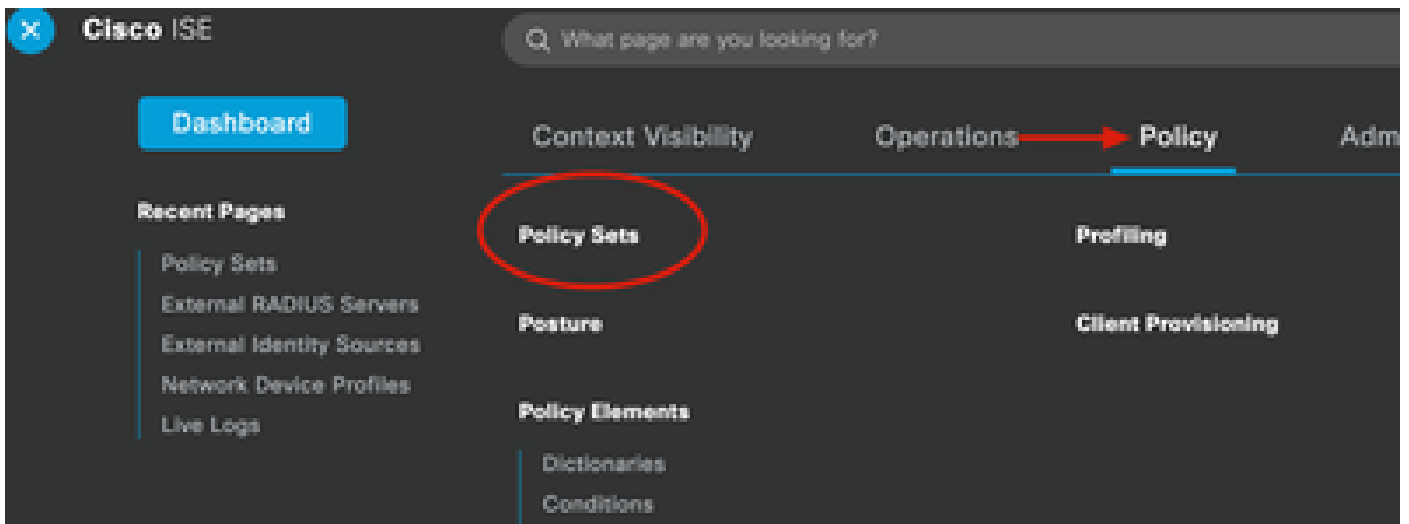
DUO_NEW
DUO_Radius




Remote accounting

Local accounting

7. Navegue do menu Pannel para Política e clique em Conjuntos de Políticas.





8. Atribua a Sequência RADIUS à política default.

 Nota: Neste documento, a sequência Duo para todas as conexões é aplicada, de modo que a política Padrão é usada. A atribuição de políticas pode variar de acordo com os requisitos.

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 |





EQ |

Allowed Protocols

- Default Network Access

Proxy Sequence

- DUO_NEW
- DUO_Sequence**

[Reset](#)

Configuração do Cisco ASA RADIUS/ISE

1. Configure o ISE RADIUS Server em grupos de servidores AAA, navegue para Configuration, clique em Device Management e expanda a seção Users/AAA, selecione AAA Server Groups.

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

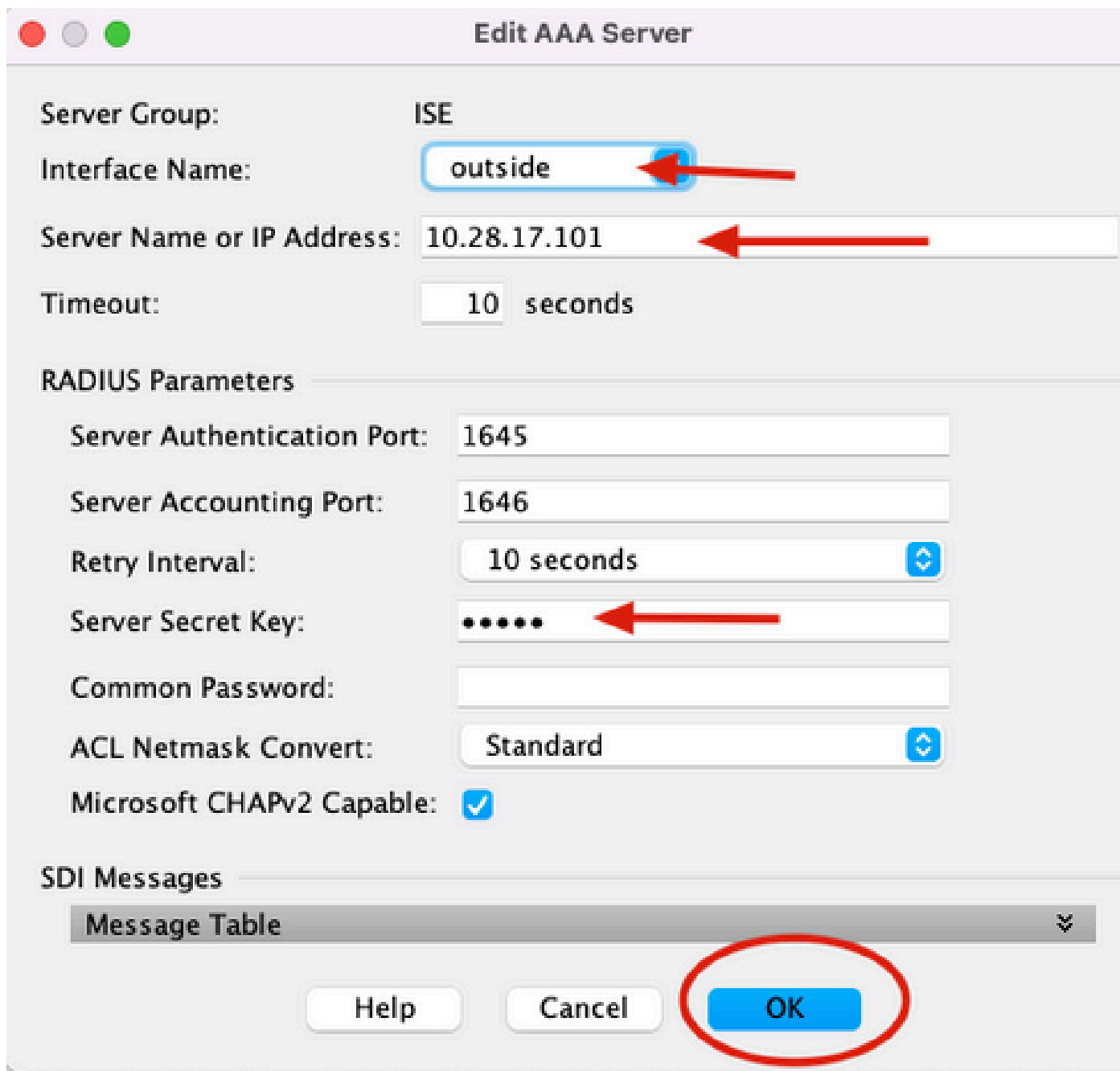
Find:

Servers in the Selected

| Server Name or IP Address |
|---------------------------|
| 10.28.17.101 |

, selecione o nome da interface, especifique o endereço IP do ISE Server e digite a chave secreta RADIUS e clique em Ok.

 Observação: todas essas informações devem corresponder àquelas especificadas no 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**

Configuração de CLI.

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

Configuração de VPN de acesso remoto do 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
```

Teste

1. Abra o aplicativo Anyconnect em seu dispositivo de PC. Especifique o nome de host do VPN ASA Headend e faça login com o usuário criado para a autenticação secundária Duo e clique em OK.



2. Você recebeu uma notificação por push Duo no dispositivo móvel Duo do usuário especificado.
3. Abra a notificação do aplicativo móvel Duo e clique em Aprovar.

14:41

Lunes, 14 de marzo

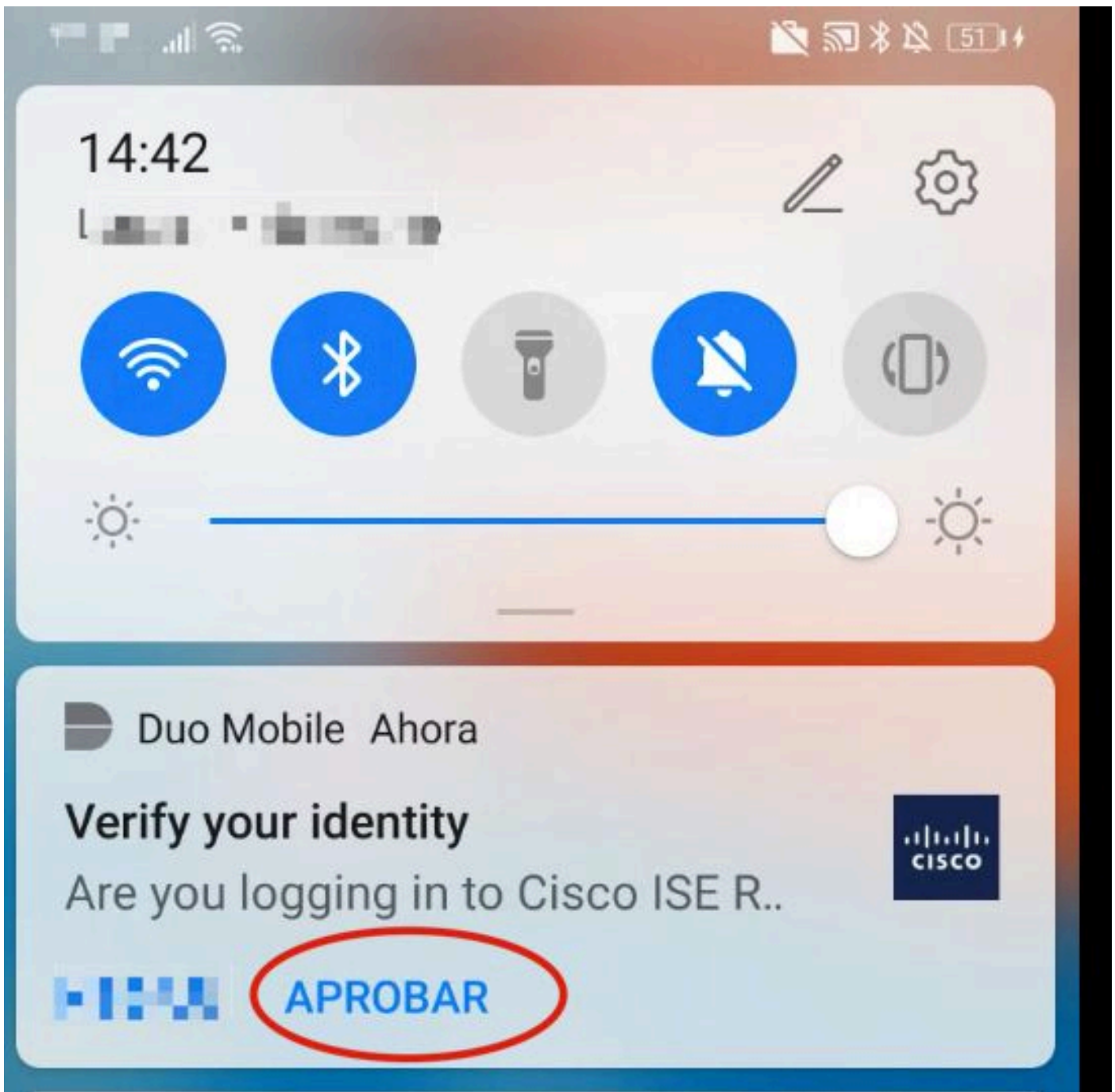


Duo Mobile Ahora

Verify your identity

Are you logging in to Cisco ISE R..





4. Aceite o banner e a conexão será estabelecida.



VPN:

Please respond to banner.

192.168.100.100



Connect

Cisco AnyConnect - Banner

This connection is for DUO authorized users only!

Disconnect

Accept



AnyConnect
Secure Mobility Client

CISCO

VPN:
Connected to 192.168.100.100.



192.168.100.100

00:00:04 IPv4

System Scan:
Compliant.
Network access allowed.

Roaming Security:
Umbrella is active.

AMP Enabler:
Waiting for configuration...


Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

O Duo Authentication Proxy é fornecido com uma ferramenta de depuração que exibe os motivos

de erros e falhas.

Depurações de trabalho

 Nota:As próximas informações são armazenadas em C:\Program Files\Duo Security Authentication Proxy\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_host',  
      '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-adv-01.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. Problemas de conectividade, IP incorreto, FQDN/Nome de Host não resolvível na configuração do Active Directory.

```
[ad_client]
```

```
host=10.28.17.106
```



```
service_account_username=Administrator
```

```
service_account_password=!H...@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. Senha incorreta para usuário Administrator no Ative Directory.

```
[ad_client]
```

```
host=10.28.17.107
```

```
service_account_username=Administrator
```

```
service_account_password=!H...@17!!
```

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



Debugs.

```
[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. Domínio Base Incorreto.

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!@#%&'*()_~:;{}|'"/\>[
search_dn=DC=agarciam,DC=ciscoo ←
```

Debugs.

```
[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. Valor de RADIUS ikey errado.

```
[radius_server_auto]
ikey=UJN5P21059LVXHRNZ6EZ1
skey=Ja2XmF4141LLP3P3Thp3d44U3d3X0z
api_host=api.10.28.17.101
radius_ip_1=10.28.17.101
radius_secret_1=!Mexvpn!17!
failmode=safe
client=ad_client
port=1812
```

Debugs

```
[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. Verifique se o Servidor ISE envia pacotes de Solicitação de Acesso.

*Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

radius

| 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

▼ 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. Para confirmar o funcionamento do servidor de Proxy de Autenticação Duo, Duo fornece a ferramenta [NTRadPing](#) para simular pacotes de solicitação de acesso e resposta com Duo.

6.1 Instale o NTRadPing em um PC diferente e gere tráfego.

Nota:Neste exemplo, a máquina com Windows 10.28.17.3 é usada.

6.2 Configure com os atributos usados na configuração do ISE Radius.

NTRadPing Test Utility

RADIUS Server/port: 10.28.17.107 | 1812

Reply timeout (sec.): 3 | Retries: 6

RADIUS Secret key: [Masked]

User-Name: duovpn

Password: [Masked] CHAP

Request type: Authentication Request | 0

Additional RADIUS Attributes:

[Empty text area]

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/>

MASTEROSOFT | **DIALWAYS**

RADIUS Server reply:

One RADIUS notification from server 10.28.17.101:2
 ...

6.3 Configure o Duo Authentication Proxy Manager da seguinte maneira:

```

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

6.4. Navegue até a ferramenta NTRadPing e clique em Send. Você recebe uma notificação por push Duo no dispositivo móvel atribuído.

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:

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: 20202020202031363436393335333230
  [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
    
```


Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.