

Anyconnect/リモートアクセスVPNクライアントでの2要素認証のためのActive DirectoryおよびISEとのDuo統合の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワークダイアグラムとシナリオ](#)

[通信プロセス](#)

[Active Directoryの設定](#)

[Duo構成](#)

[Duo認証プロキシの設定](#)

[Cisco ISEの設定](#)

[Cisco ASA RADIUS/ISEの設定](#)

[Cisco ASAリモートアクセスVPNの設定](#)

[テスト](#)

[トラブルシューティング](#)

[作業のデバッグ](#)

はじめに

このドキュメントでは、ASAに接続されたAnyConnectクライアントの2要素認証としてADおよびISEとDuoプッシュ統合について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 適応型セキュリティアプライアンス(ASA)でのRA VPNの設定
- ASAでのRADIUSの設定
- Identity Services Engine (ISE)
- Active Directory (AD)
- Duoアプリケーション

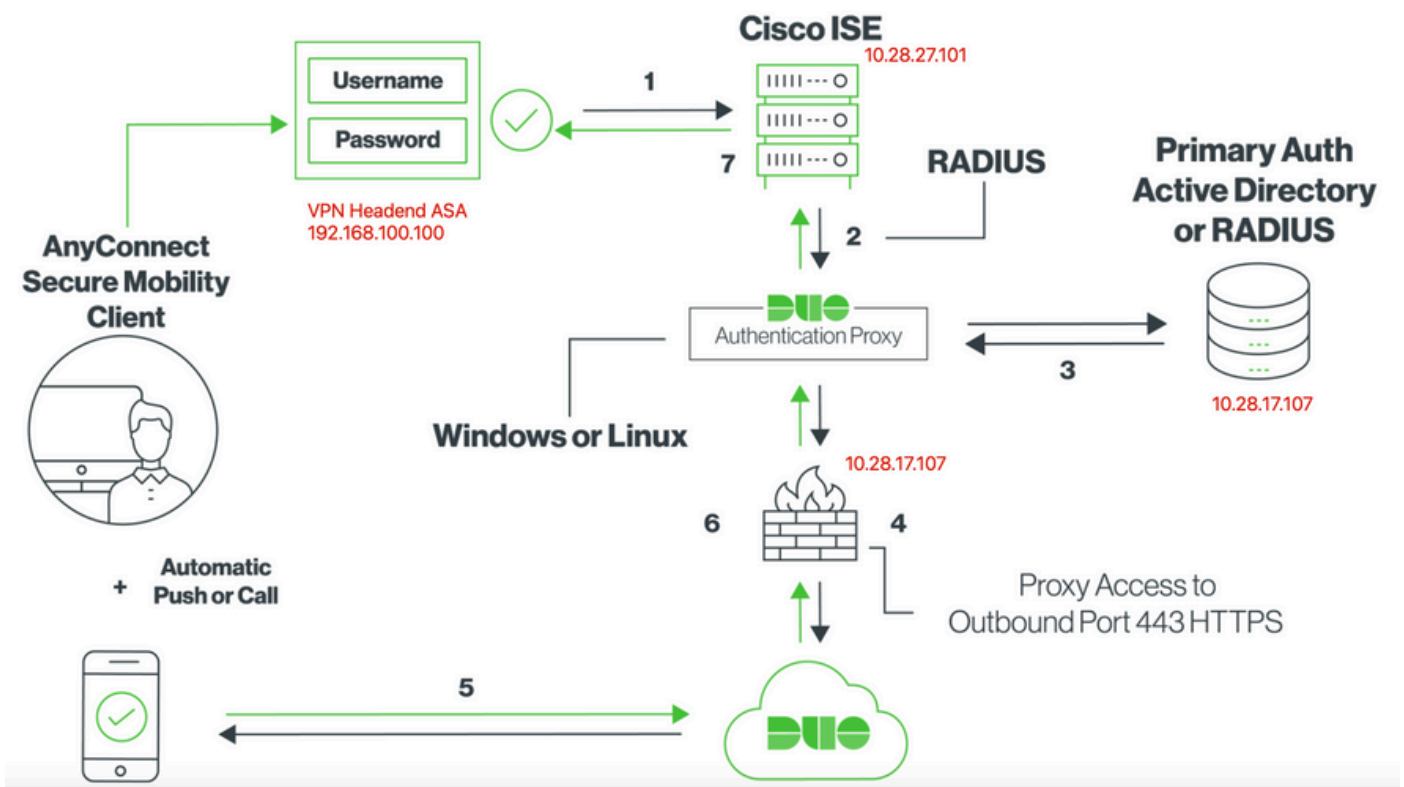
使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft 2016サーバー
- ASA 9.14(3)18
- ISEサーバ3.0
- Duoサーバ
- Duo認証プロキシマネージャ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワークダイアグラムとシナリオ



通信プロセス

[Cisco ISE用Duo 2要素RADIUS認証](#)


1. Cisco ISEに対して開始されたプライマリ認証。
2. Cisco ASAがDuo認証プロキシに認証要求を送信します。
3. プライマリ認証では、Active DirectoryまたはRADIUSを使用します。
4. TCPポート443経由でDuo SecurityへのDuo認証プロキシ接続が確立されました。
5. Duo Securityのサービスを介した二次認証。
6. Duo認証プロキシが認証応答を受信します。
7. Cisco ISEアクセスが許可されます。

ユーザアカウント:

- Active Directory Admin:Duo Auth Proxyがプライマリ認証用にActive Directoryサーバにバインドできるようにするためのディレクトリアカウントとして使用されます。
- Active Directoryテストユーザ
- セカンダリ認証のためのDuoテストユーザ

Active Directoryの設定

Windowsサーバには、Active Directoryドメインサービスが事前設定されています。

 注: RADIUS Duo Auth Proxy Managerが同じActive Directoryホストマシンで実行されている場合は、ネットワークポリシーサーバー(NPS)の役割をアンインストールまたは削除する必要があります。両方のRADIUSサービスが実行されると、競合が発生し、パフォーマンスに影響を与える可能性があります。

リモートアクセスVPNユーザの認証とユーザIDに対してAD設定を行うには、いくつかの値が必要です。

これらの詳細情報はすべて、ASAおよびDuo Authプロキシサーバで設定を行う前に、Microsoftサーバで作成または収集する必要があります。

主な値は次のとおりです。

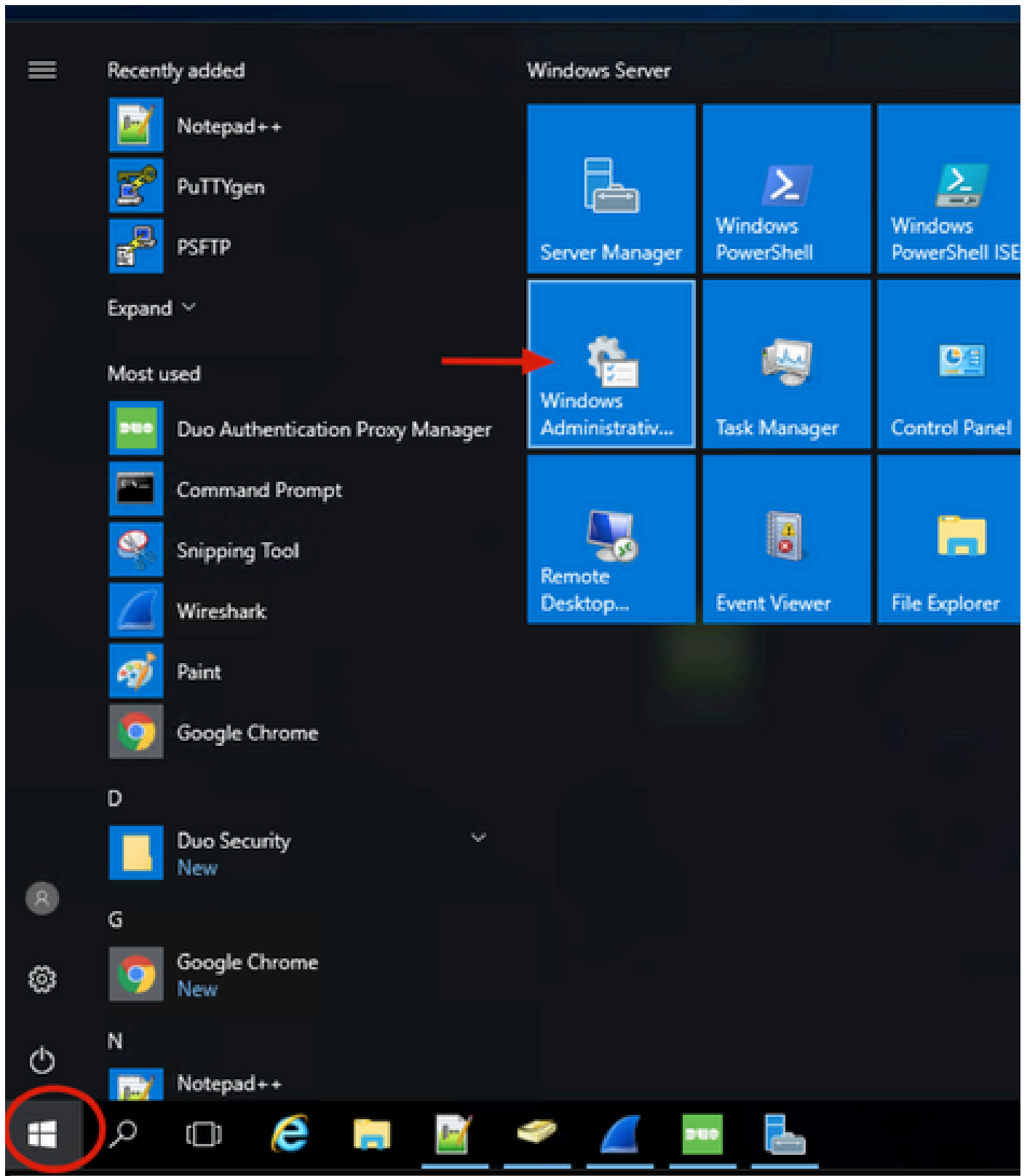
- ドメイン名.これはサーバのドメイン名です。この設定ガイドでは、agarciam.ciscoがドメイン名です。
- サーバのIP/完全修飾ドメイン名(FQDN)アドレス。Microsoftサーバに到達するために使用されるIPアドレスまたはFQDN。FQDNを使用する場合、DNSサーバはASAおよびDuo認証プロキシ内で設定してFQDNを解決する必要があります。

この設定ガイドでは、この値はagarciam.cisco (10.28.17.107に解決) です。

- サーバポート。LDAPサービスが使用するポート。デフォルトでは、LDAPおよびSTARTTLSはLDAPにTCPポート389を使用し、LDAP over SSL(LDAPS)はTCPポート636を使用します。
- ルートプロセッサ。LDAPSまたはSTARTTLSを使用する場合、LDAPSで使用するSSL証明書の署名に使用するルートCAが必要です。
- ディレクトリのユーザ名とパスワードこれは、Duo AuthプロキシサーバがLDAPサーバにバインドし、ユーザを認証し、ユーザとグループを検索するために使用するアカウントです。
- ベースおよびグループの識別名(DN)。ベースDNはDuo Authプロキシの出発点であり、ユーザの検索と認証を開始するようにActive Directoryに指示します。

このコンフィギュレーションガイドでは、ルートドメインagarciam.ciscoがベースDNとして使用され、グループDNがDuo-USERSです。

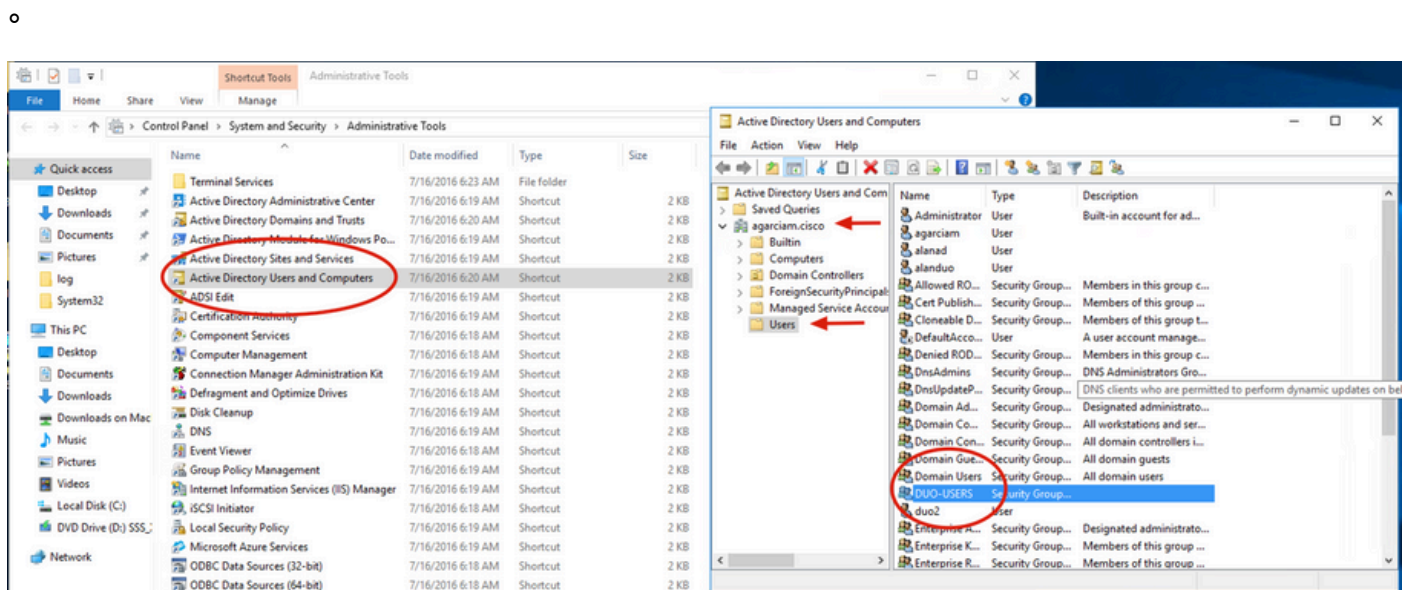
1. 新しいDuoユーザを追加するには、Windows Serverで、左下のWindowsアイコンに移動し、図のようにWindows Administrative toolsをクリックします。



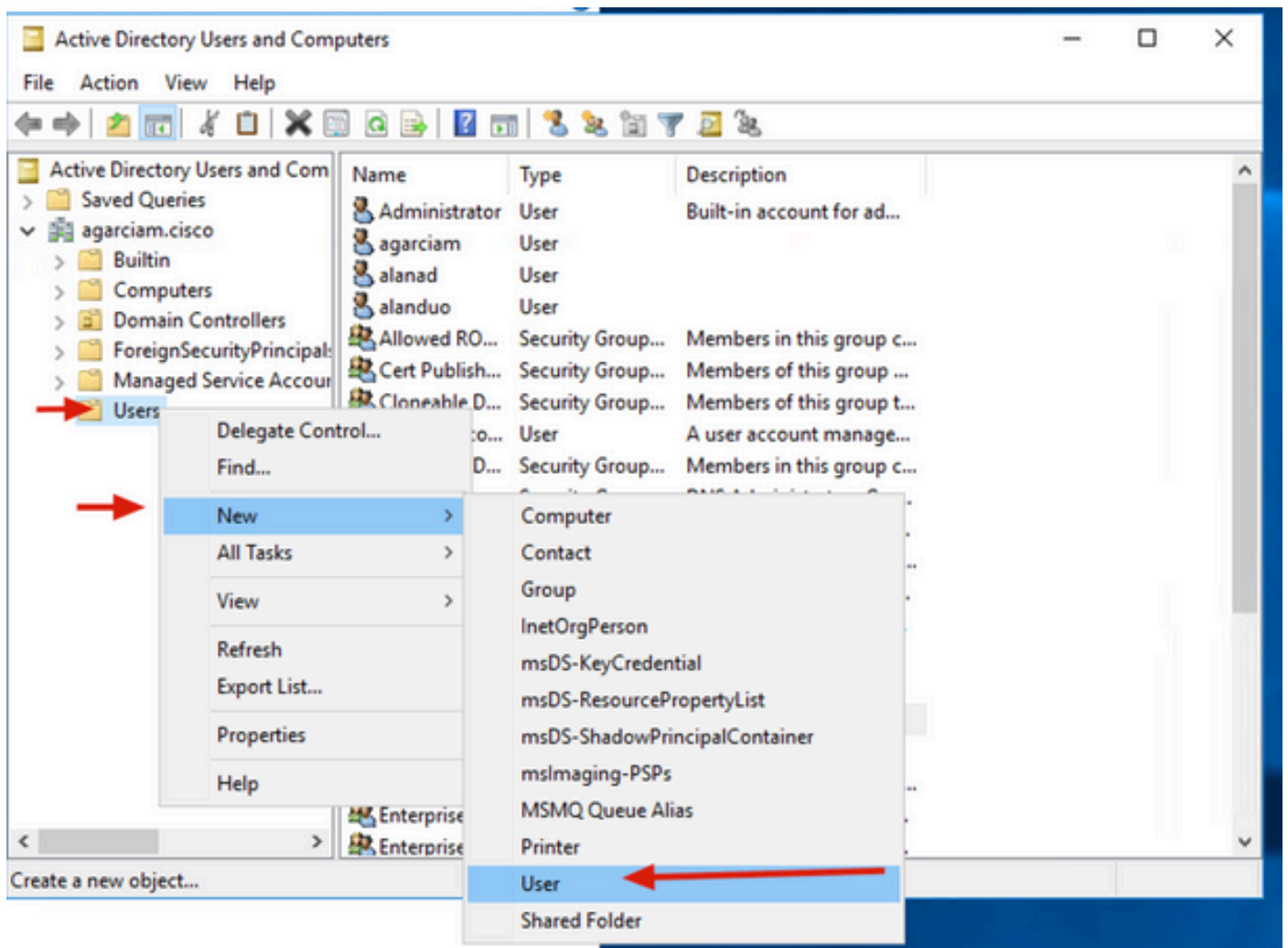
2. Windowsの管理ツールウィンドウで、Active Directoryユーザとコンピュータに移動します。

Active Directory Users and Computersパネルで、domainオプションを展開し、Usersフォルダに移動します。

この設定例では、セカンダリ認証のターゲットグループとしてDuo-USERSが使用されています。



3. 図に示すように、Usersフォルダを右クリックし、New > Userの順に選択します。



4. 「新規オブジェクト - ユーザー」ウィンドウで、図に示すように、この新規ユーザーのID属性を指定し、「次へ」をクリックします。

New Object - User

Create in: agarciam.cisco/Users

First name: ← Initials:

Last name:

Full name:


User logon name: ← @agarciam.cisco

User logon name (pre-Windows 2000):

< Back **Next >** Cancel

5. パスワードを確認して、Nextをクリックし、ユーザ情報を確認したらFinishをクリックします。

New Object - User ×

 Create in: agarciam.cisco/Users

Password: ←

Confirm password: ←

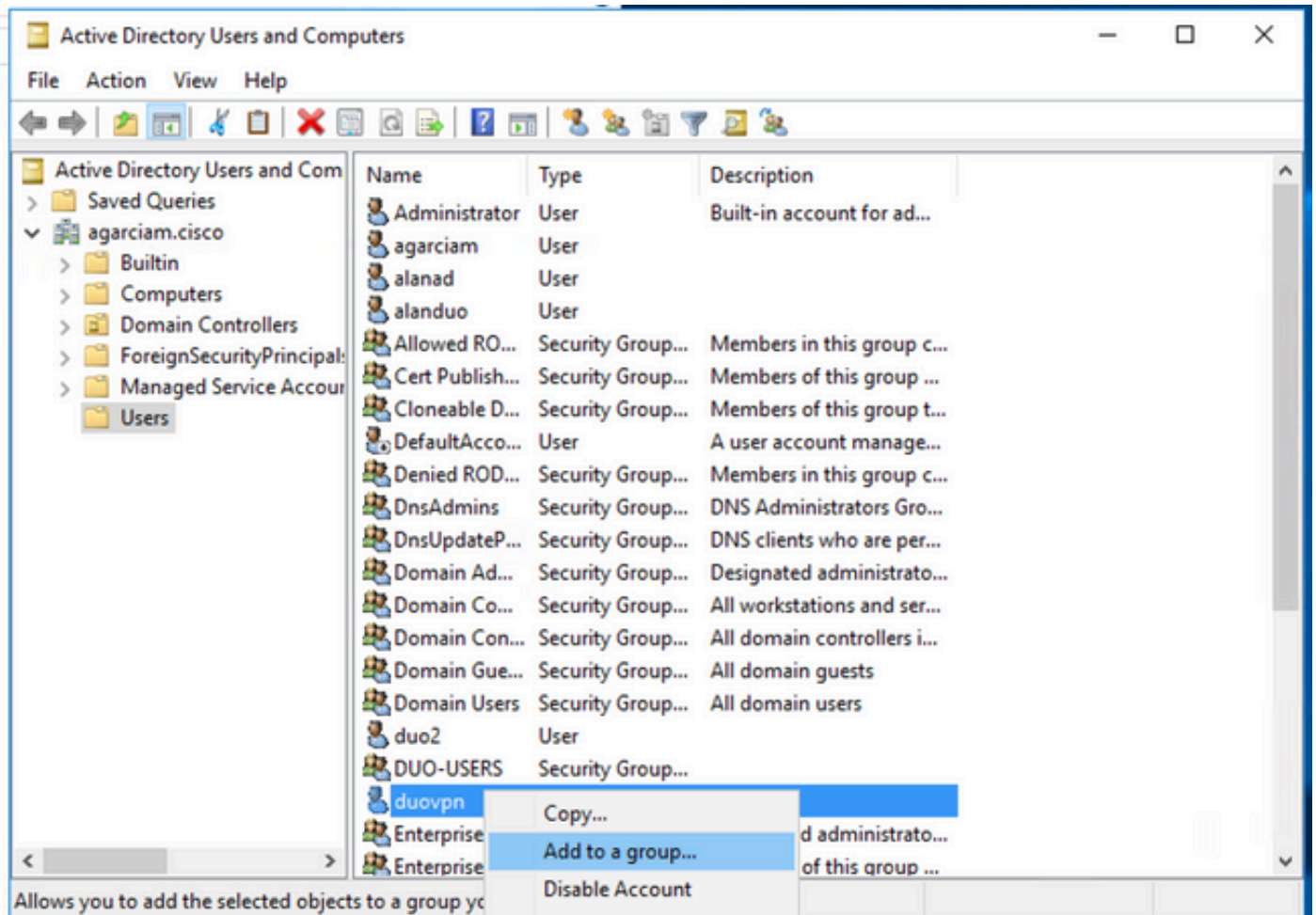
User must change password at next logon

User cannot change password

Password never expires

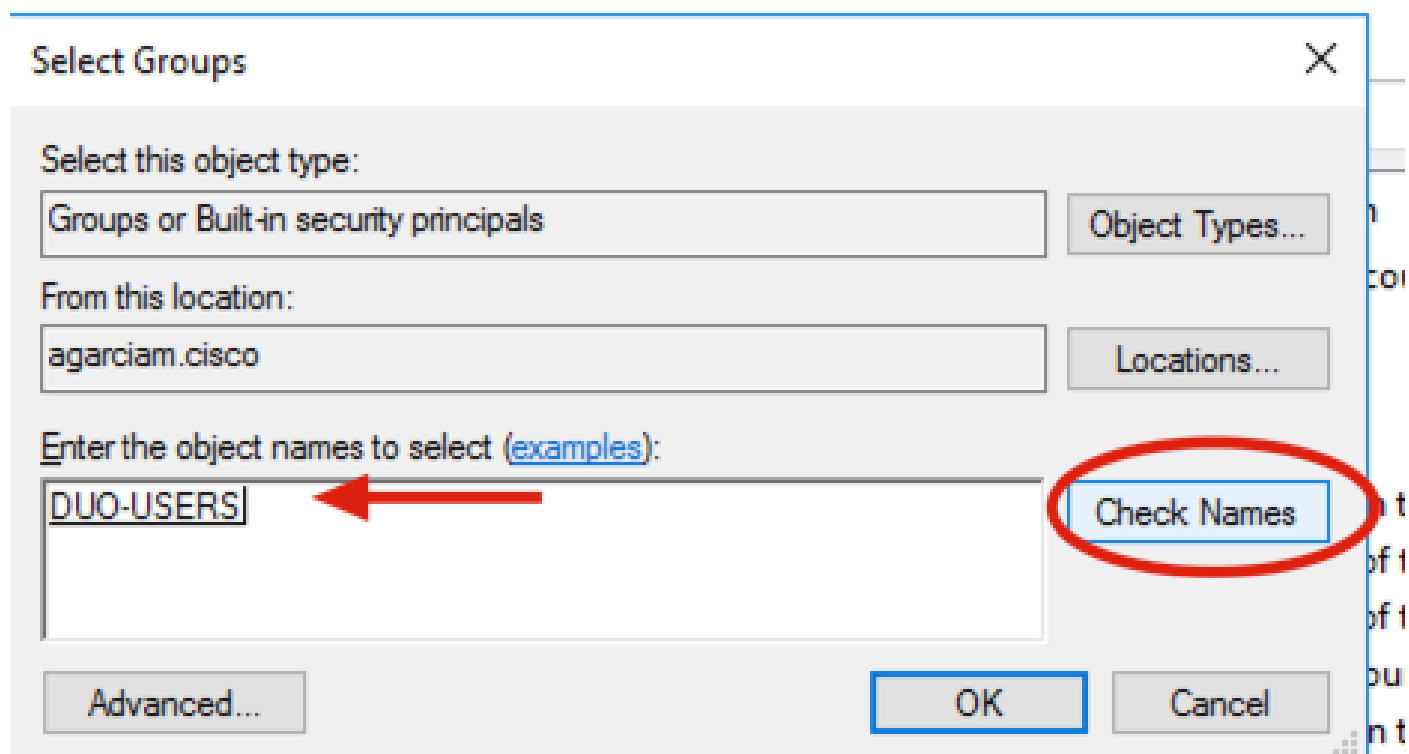
Account is disabled

6. 図に示すように、新しいユーザを特定のグループに割り当て、それを右クリックして、Add to a groupを選択します。



7. 「グループの選択」パネルで、目的のグループの名前を入力し、「名前のチェック」をクリックします。

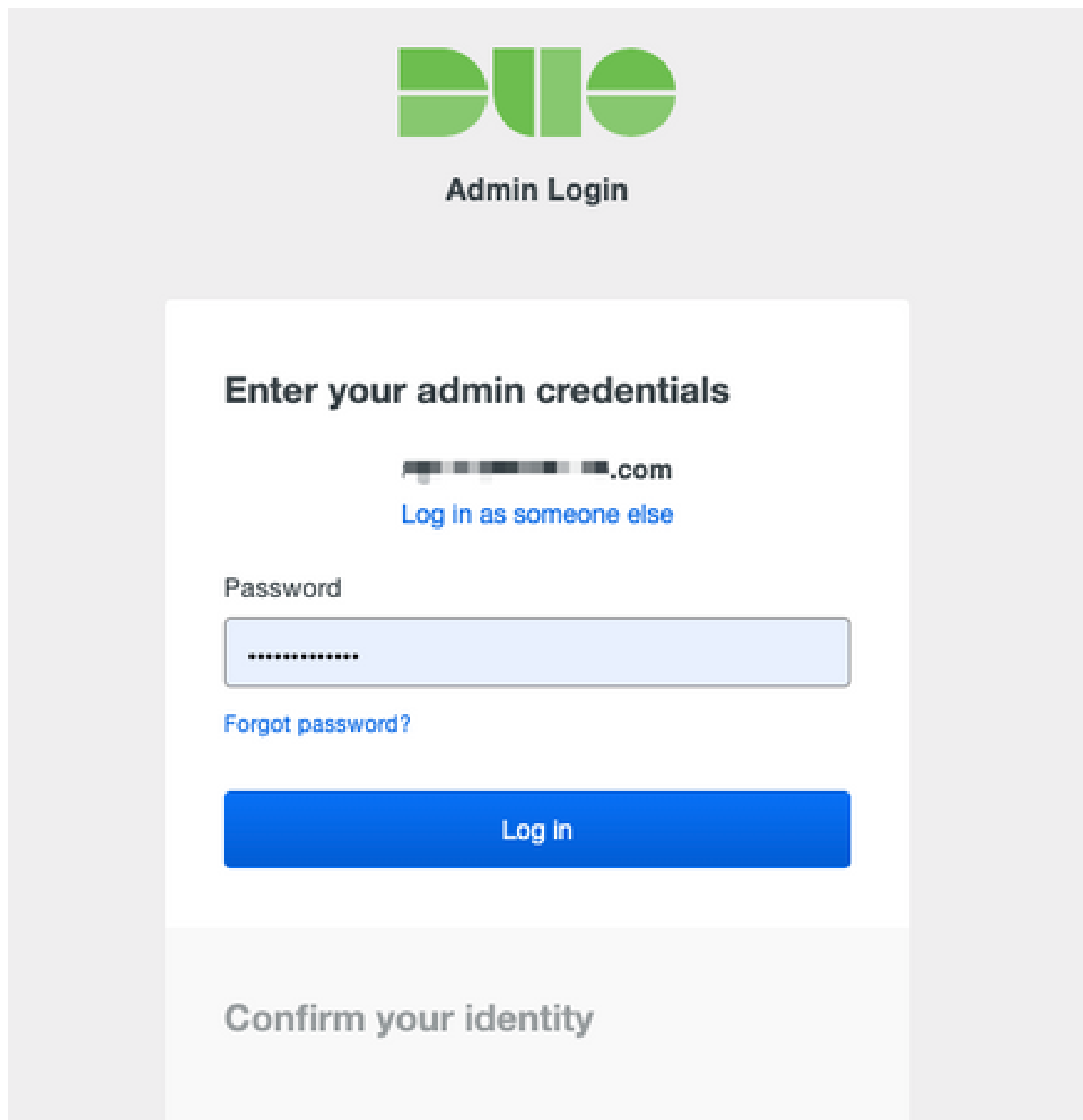
次に、条件に一致する名前を選択して、OKをクリックします。



8. これは、このドキュメントで例として使用されているユーザです。

Duo構成

1. Duo Adminポータルにログインします。



Admin Login

Enter your admin credentials

██████████@██████████.com
[Log in as someone else](#)

Password

.....

[Forgot password?](#)

Log In

Confirm your identity

2. 左側のパネルで、Usersに移動し、Add Userをクリックして、Active Domainユーザ名に一致するユーザの名前を入力し、Add Userをクリックします。

Dashboard

Device Insight

Policies

Applications

Single Sign-On

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Search for users, groups, applications, or devices

Dashboard > Users > Add User

Add User

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

Username:

Should match the primary authentication username.

Add User

3. 新しいユーザパネルで、必要な情報をすべて入力します。

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** **Bypass** **Disabled**
Require multi-factor authentication (default).
Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.
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. ユーザー・デバイスの下で、セカンダリ認証方法を指定します。

 注：このドキュメントでは、モバイルデバイス用のDuoプッシュ方式が使用されているため、電話デバイスを追加する必要があります。

Add Phoneをクリックします。

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. ユーザーの電話番号を入力し、電話の追加をクリックします。

Add Phone



[Learn more about Activating Duo Mobile](#)

Type

Phone

Tablet

Phone number



[Show extension field](#)

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



6. 左側のDuo AdminパネルでUsersに移動し、新しいユーザをクリックします。

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"/>				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		...@... .com	1		Active	Never authenticated
<input type="checkbox"/>			...@... o.com	1		Active	Mar 5, 2022 7:16 PM




 注：現時点で電話へのアクセス権がない場合は、電子メールオプションを選択できます。

7. Phonesセクションに移動し、Activate Duo Mobileをクリックします。

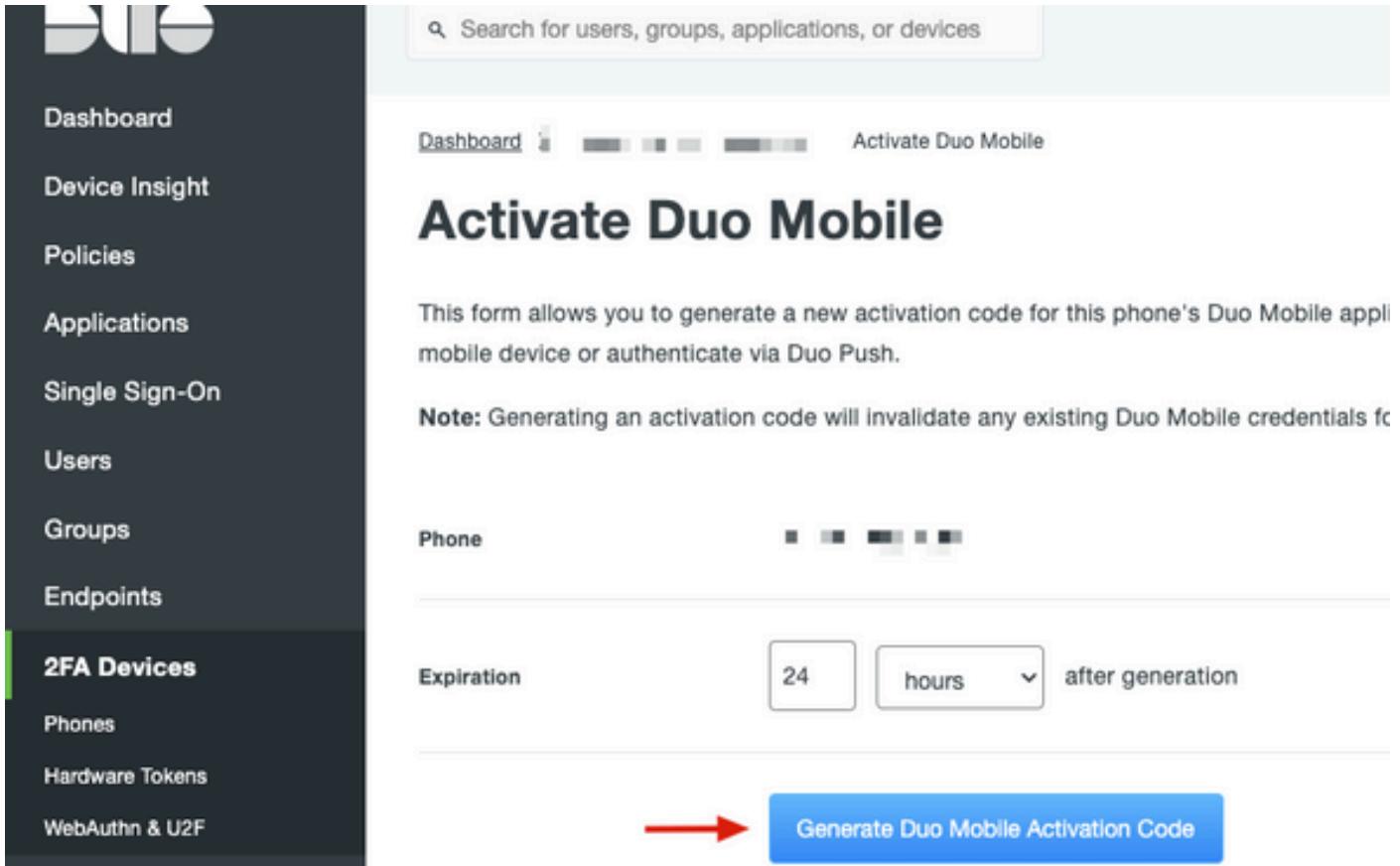
Phones

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

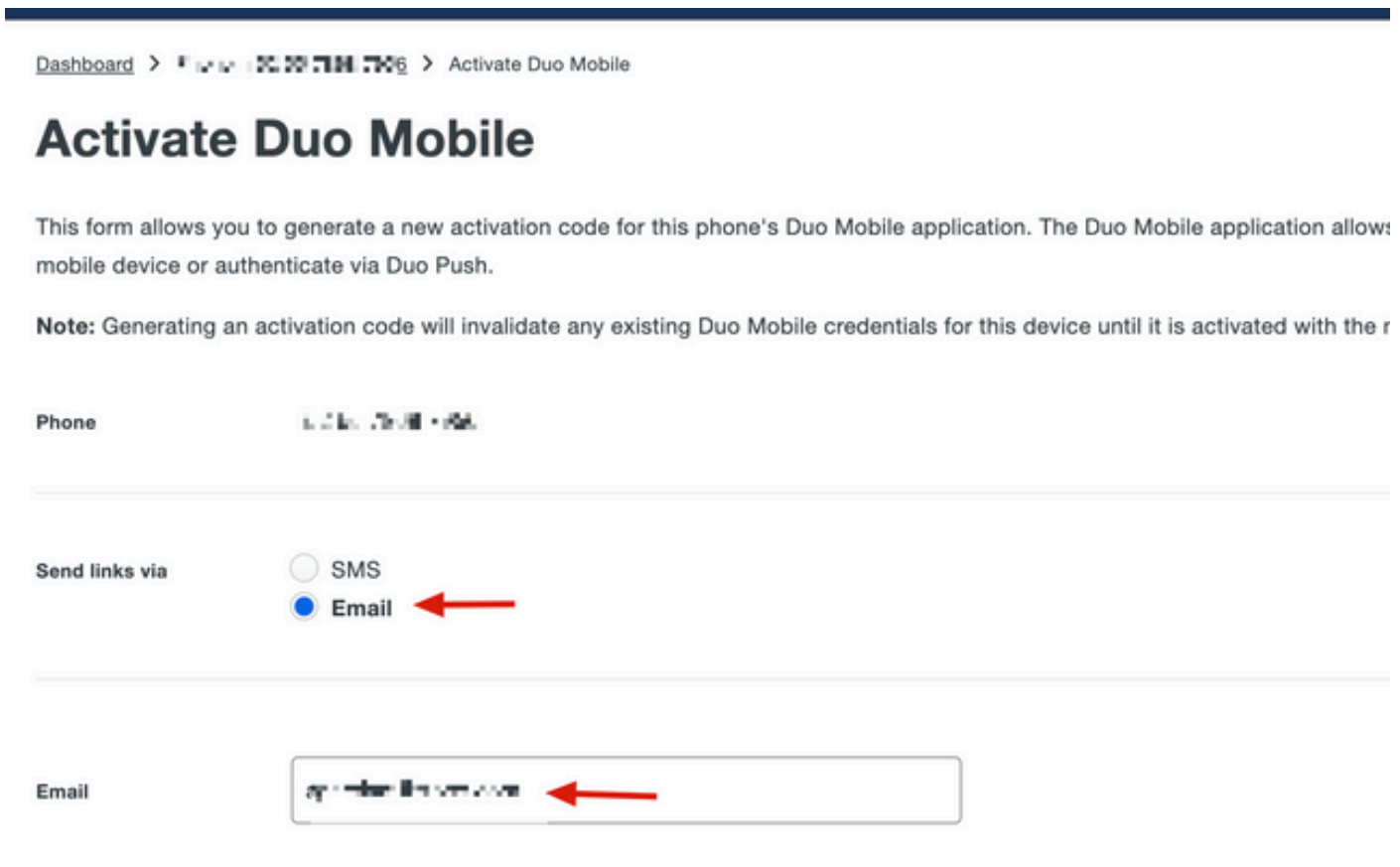
[Add Phone](#)

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

8. [Duo Mobile Activation Codeの生成]をクリックします。



9. 「Email」を選択して指示を電子メールで受け取り、電子メールアドレスを入力して「Send Instructions by email」をクリックします。



10. 図に示すように、手順が記載された電子メールを受信します。

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. 携帯端末からDuoモバイルアプリを開き、追加をクリックし、QRコードを使用を選択し、手順メールからコードをスキャンします。

12. Duoモバイルアプリに新しいユーザーが追加されました。

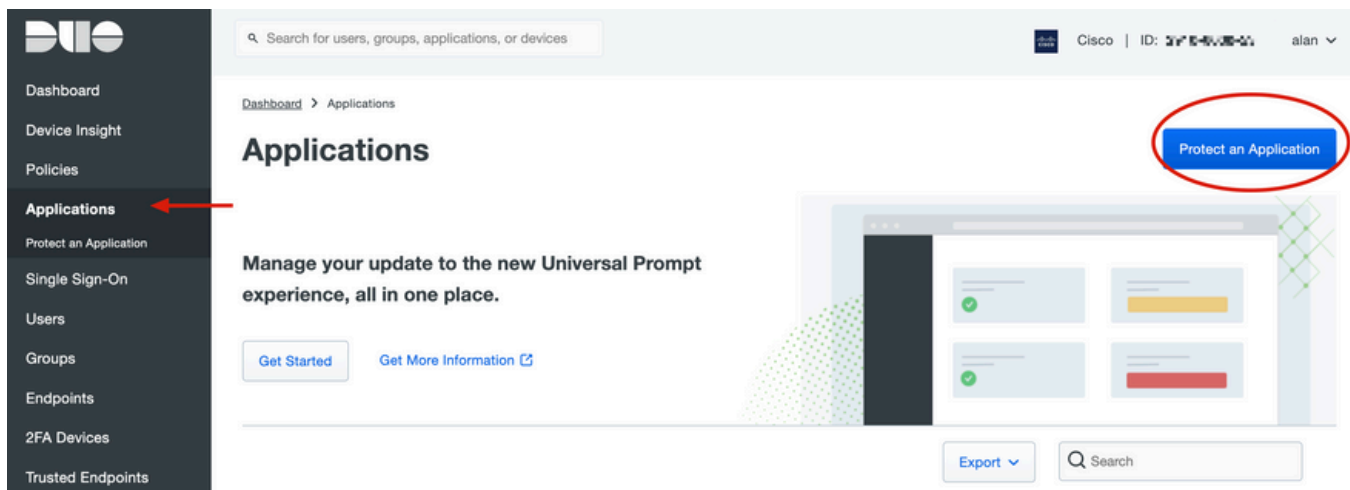
Duo認証プロキシの設定

1. [Cisco Duo Authentication](#)からDuo Auth Proxy Managerをダウンロードしてインストールします

。

 注：このドキュメントでは、Duo Auth Proxy Managerは、Active Directory(AD)サービスをホストする同じWindowsサーバにインストールされています。

2. Duo Admin PanelでApplicationsに移動し、Protect an Applicationをクリックします。






3. 検索バーで、Cisco ISE Radiusを探します。

Protect an Application

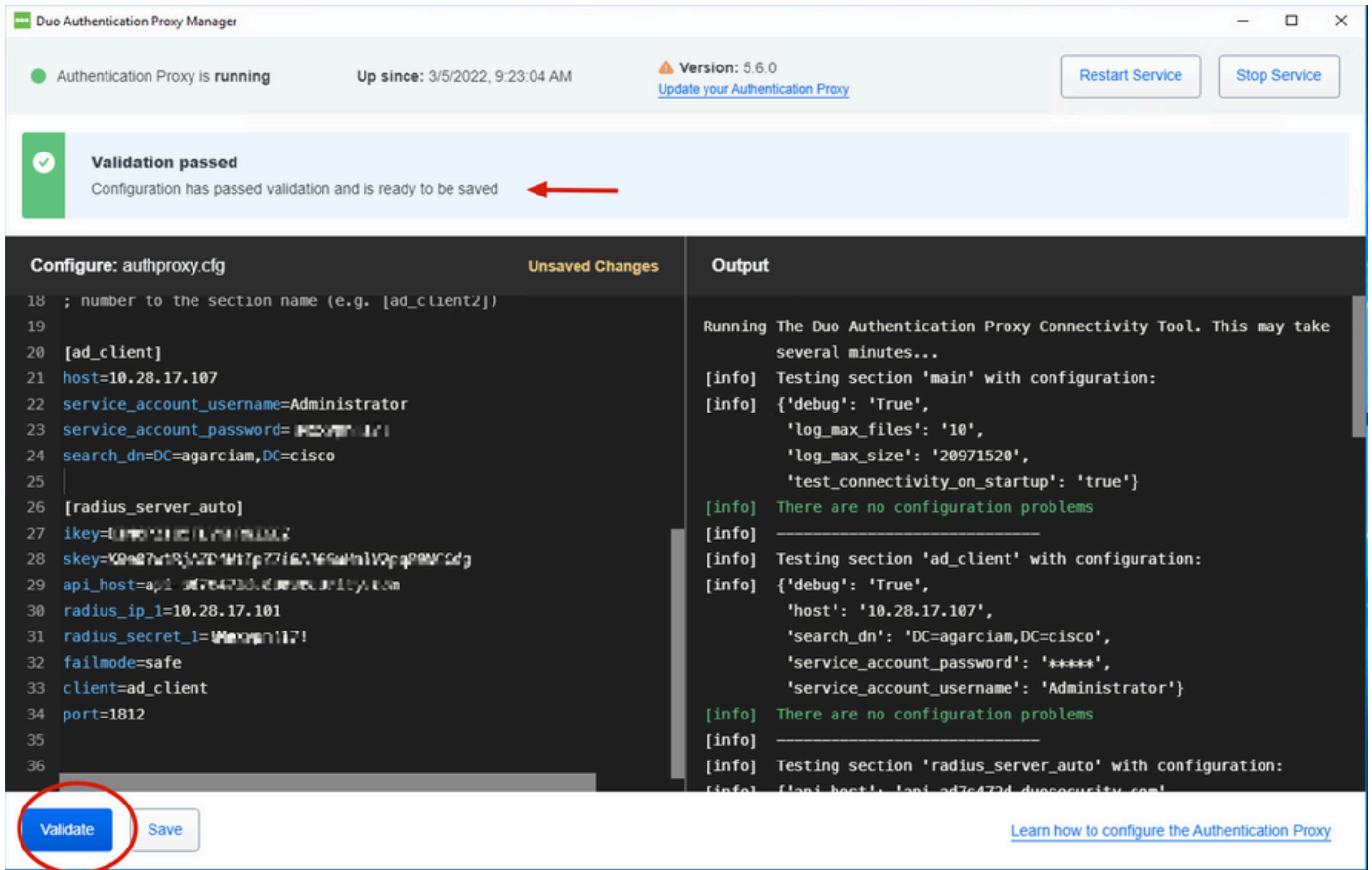
i Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

Documentation: [Getting Started](#)

Choose an application below to get started.

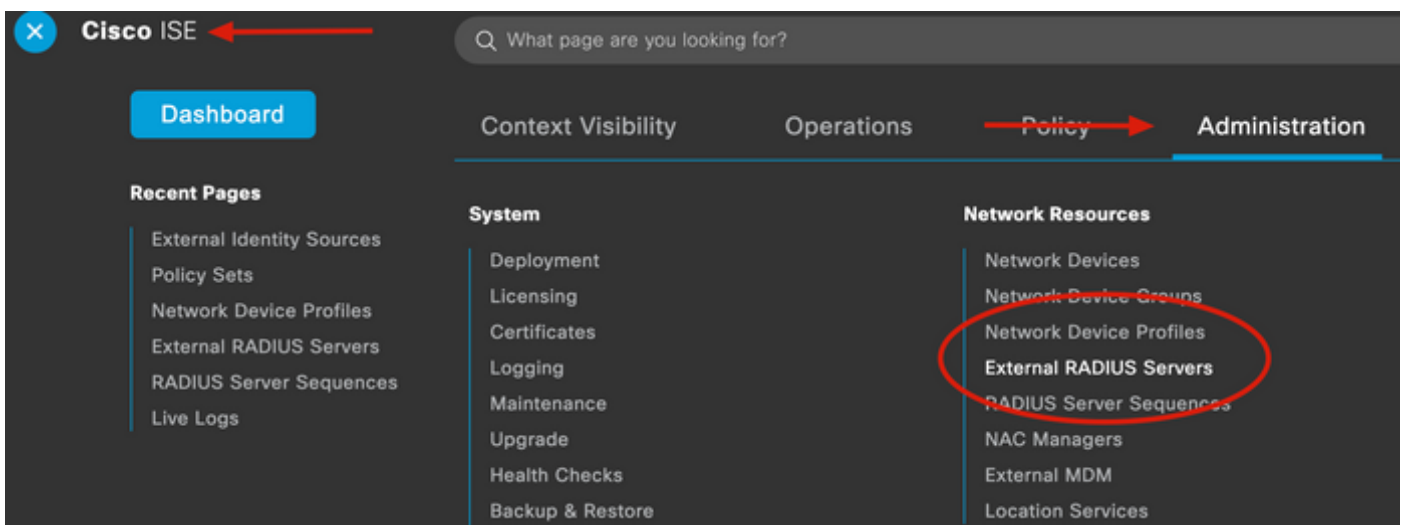
Application	Protection Type	
 Akamai Enterprise Application Access	2FA	Documentation Protect
 Cisco ISE RADIUS 	2FA	Documentation Protect

4. 統合キー、秘密キー、およびAPIホスト名をコピーします。この情報は、Duo認証プロキシの設定に必要です。



Cisco ISEの設定

1. ISE管理ポータルにログインします。
2. Cisco ISEタブを展開し、Administrationに移動し、Network Resourcesをクリックし、External RADIUS Serversをクリックします。



3. External Radius Serversタブで、Addをクリックします。

External RADIUS Servers

Edit **+ Add** Duplicate Delete

Name: Currently Sorted Description

4. Duo Authentication Proxy Managerで使用されているRADIUS設定の空欄を埋め、Submitをクリックします。

* Name DUO_NEW

Description

* Host IP 10.28.17.107

* Shared Secret Show

Enable KeyWrap

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ASCII HEXADECIMAL

* Authentication Port 1812 (Valid Range 1 to 65535)

* Accounting Port 1813 (Valid Range 1 to 65535)

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

* Connection Attempts 3 (Valid Range 1 to 9)

Radius ProxyFailover Expiration 300 (Valid Range 1 to 600)

Submit

5. RADIUS Server Sequencesタブに移動し、Addをクリックします。

RADIUS Server Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)Edit **+ Add** Duplicate Delete

6. シーケンスの名前を指定して新しいRADIUS外部サーバを割り当て、Submitをクリックします。

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

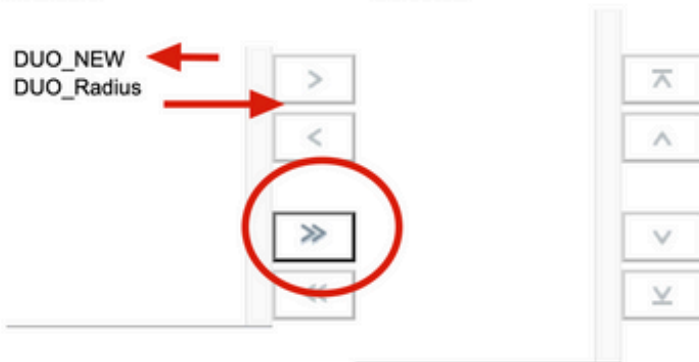
▼ User Selected Service Type

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

Available

* Selected

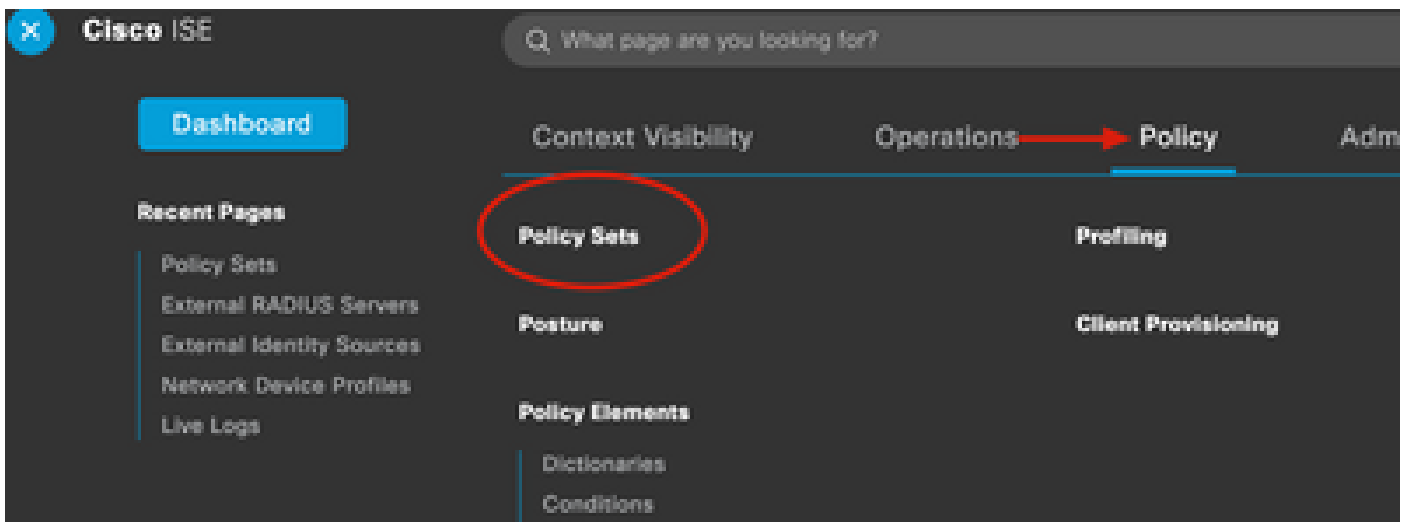
DUO_NEW
DUO_Radius




Remote accounting

Local accounting

7. 「ダッシュボード」メニューから「ポリシー」にナビゲートし、「ポリシー・セット」をクリックします。




8. RADIUSシーケンスをデフォルトポリシーに割り当てます。

 注：このドキュメントでは、すべての接続にDuoシーケンスが適用されるため、デフォルトポリシーが使用されます。ポリシーの割り当ては、要件によって異なります。

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



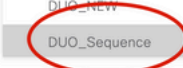
EQ |


Allowed Protocols

- Default Network Access

Proxy Sequence

- DUO_NEW
- DUO_Sequence**





Cisco ASA RADIUS/ISEの設定

1. AAAサーバグループでISE RADIUSサーバを設定するには、Configurationに移動し、Device Managementをクリックし、Users/AAAセクションを展開して、AAA Server Groupsを選択します。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。