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

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要素認証としてのADおよびISEとの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。

- ASAでのRA VPNの設定
- ASAでのRADIUSの設定
- ISE
- Active Directory
- 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。

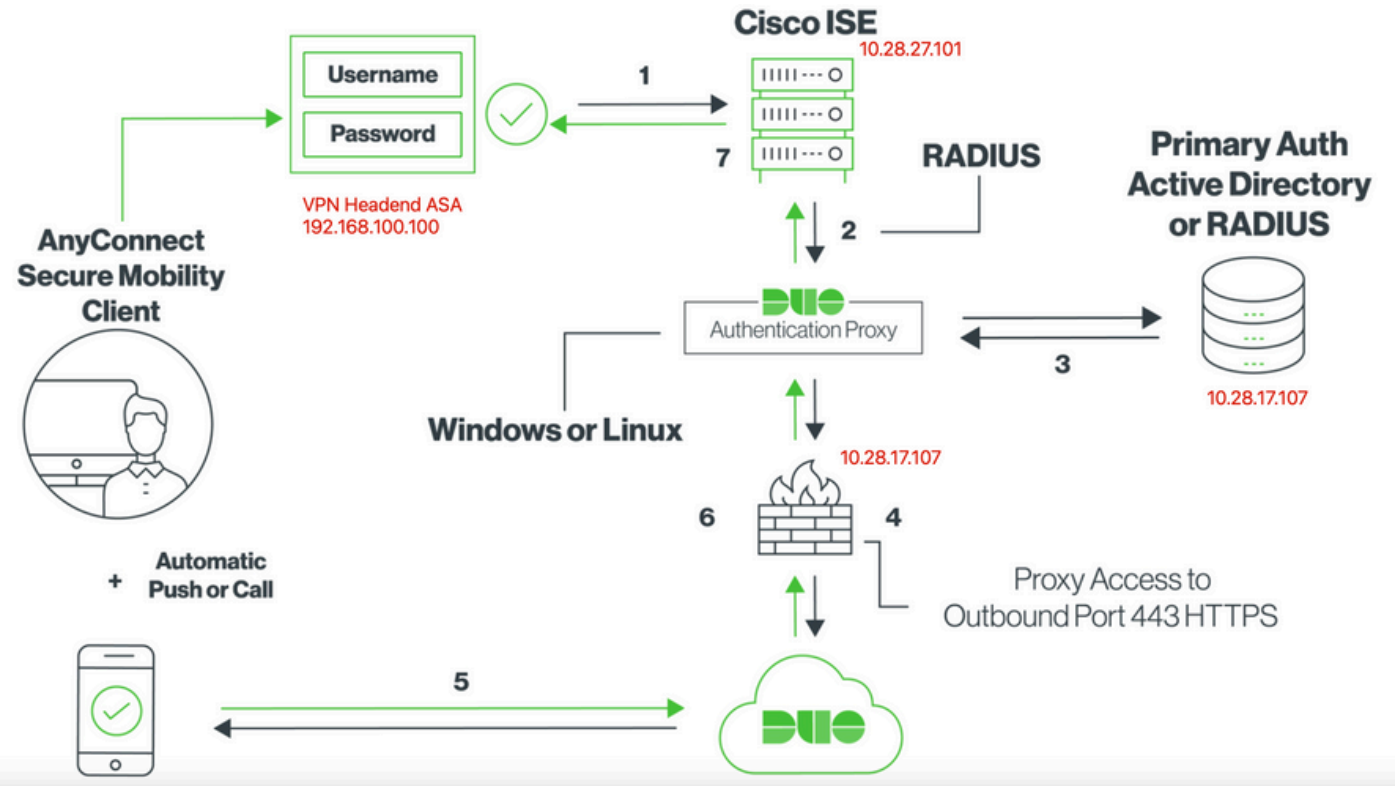
- Microsoft 2016サーバ
- ASA 9.14(3)18
- ISEサーバ3.0
- Duoサーバ
- Duo認証プロキシマネージャ

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。

背景説明

このドキュメントでは、Cisco適応型セキュリティアプライアンス(ASA)に接続するAnyConnectクライアントの2要素認証として、Active Directory(AD)およびCisco Identity Service Engine(ISE)とのDuoプッシュ統合(DUC)を設定する方法について説明します。

ネットワークダイアグラムとシナリオ



通信プロセス

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

1. Cisco ISEに対して開始されたプライマリ認証
2. Cisco ASAが認証要求をDuo認証プロキシに送信
3. プライマリ認証はActive DirectoryまたはRADIUSを使用

4. TCPポート443経由でDuo SecurityへのDuo Authentication Proxy接続が確立されました
5. Duo Securityサービスによる二次認証
6. Duo認証プロキシが認証応答を受信
7. Cisco ISEへのアクセスが許可される

ユーザアカウント:

- Active Directory Admin：これは、Duo Auth Proxyがプライマリ認証用にActive Directoryサーバにバインドすることを許可する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、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ている場合、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ユーザで認証およびユーザIDの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IP/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 Authプロキシ内で設定してFQDNを解決する必要があります。

このコンフィギュレーションガイドでは、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。

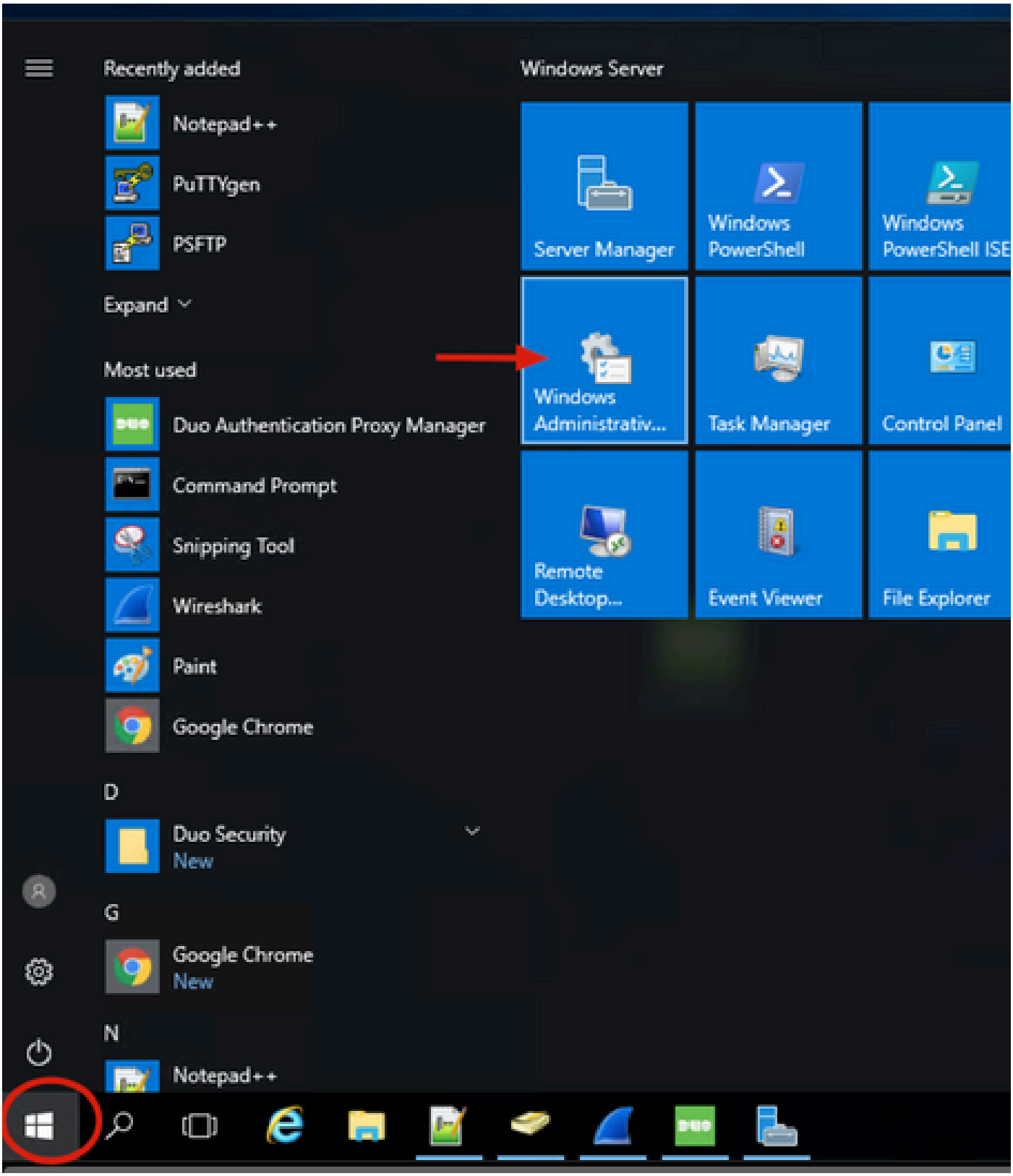
- ルートCA。LDAPSまたはSTARTTLSを使用する場合、LDAPSで使用するSSL証明書の署名に使用するルートCAが必要です。

- 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。

この設定ガイドでは、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はDuo-USERSです。

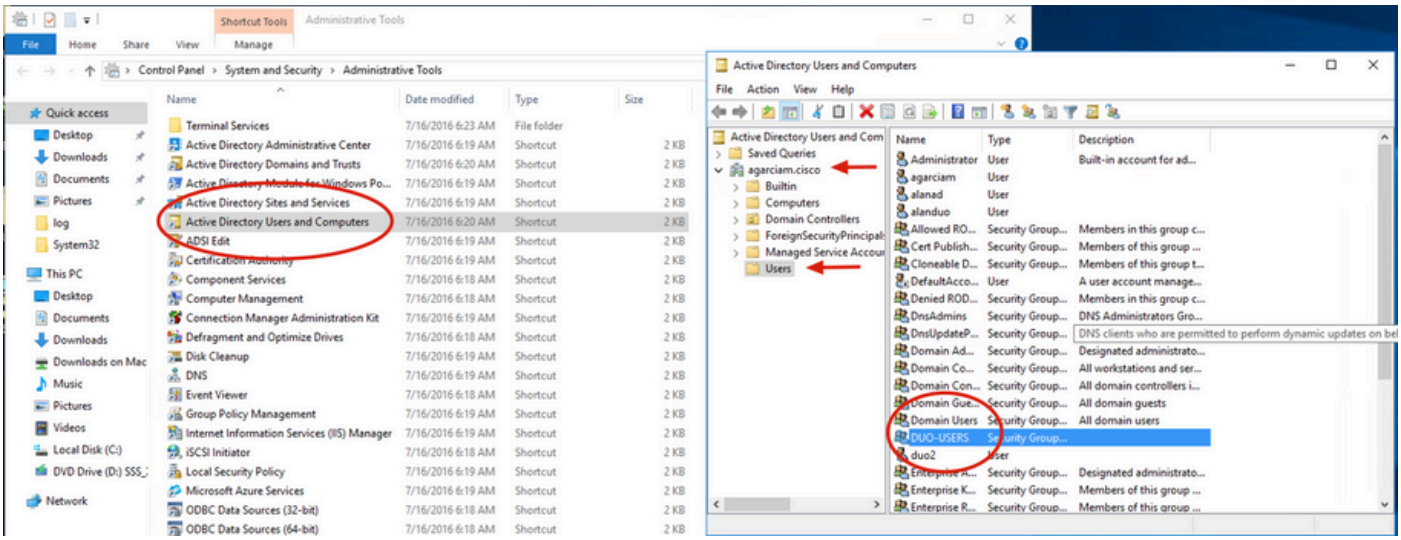
1.新しいDuoユーザを追加するには、Windows Serverで、左下のWindowsアイコンに移動し、図に示すようにWindows Administrative toolsをクリックします。



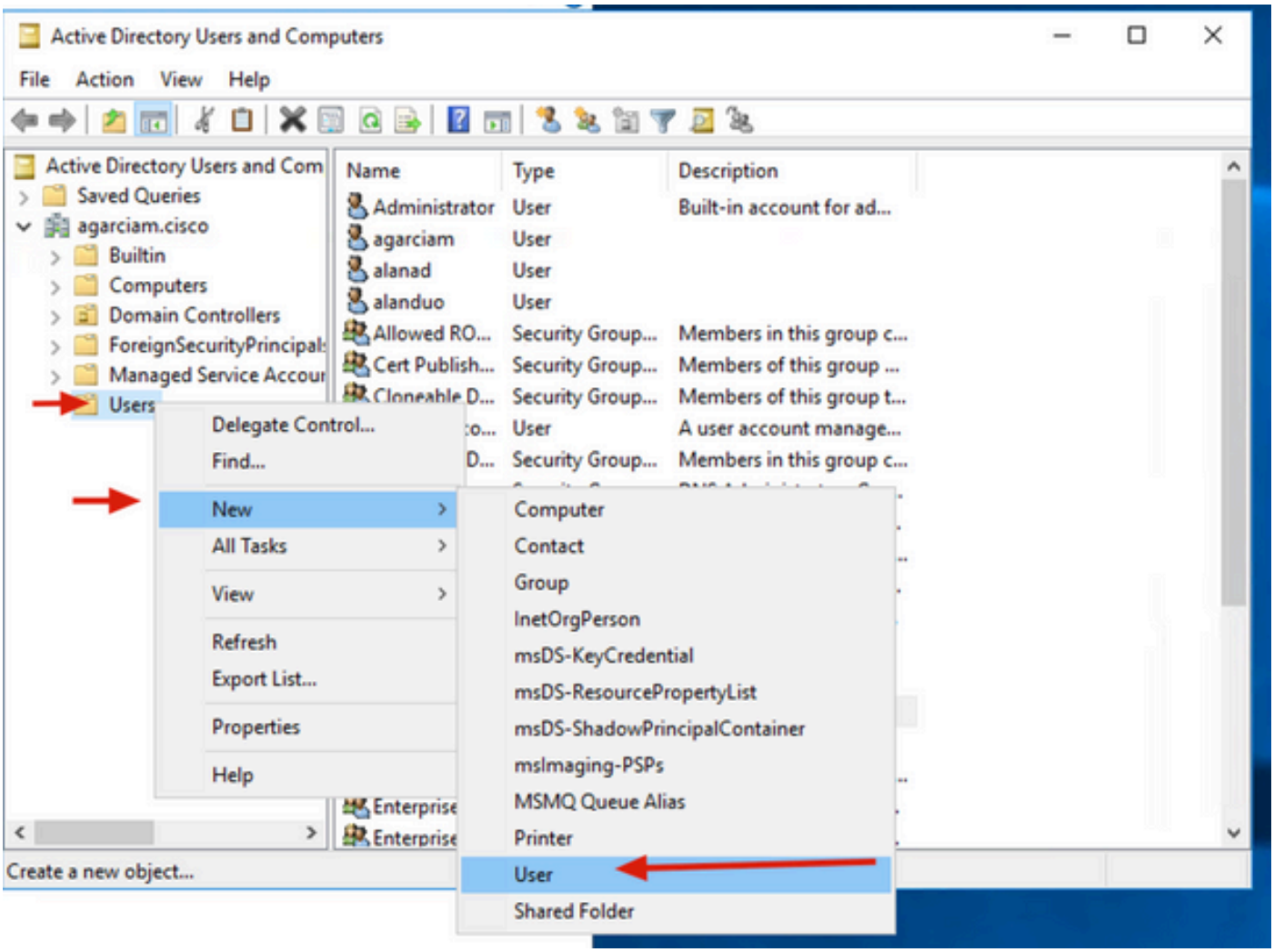
2. Windowsの管理ツールウィンドウで、Active Directory Users and Computersに移動します。

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。

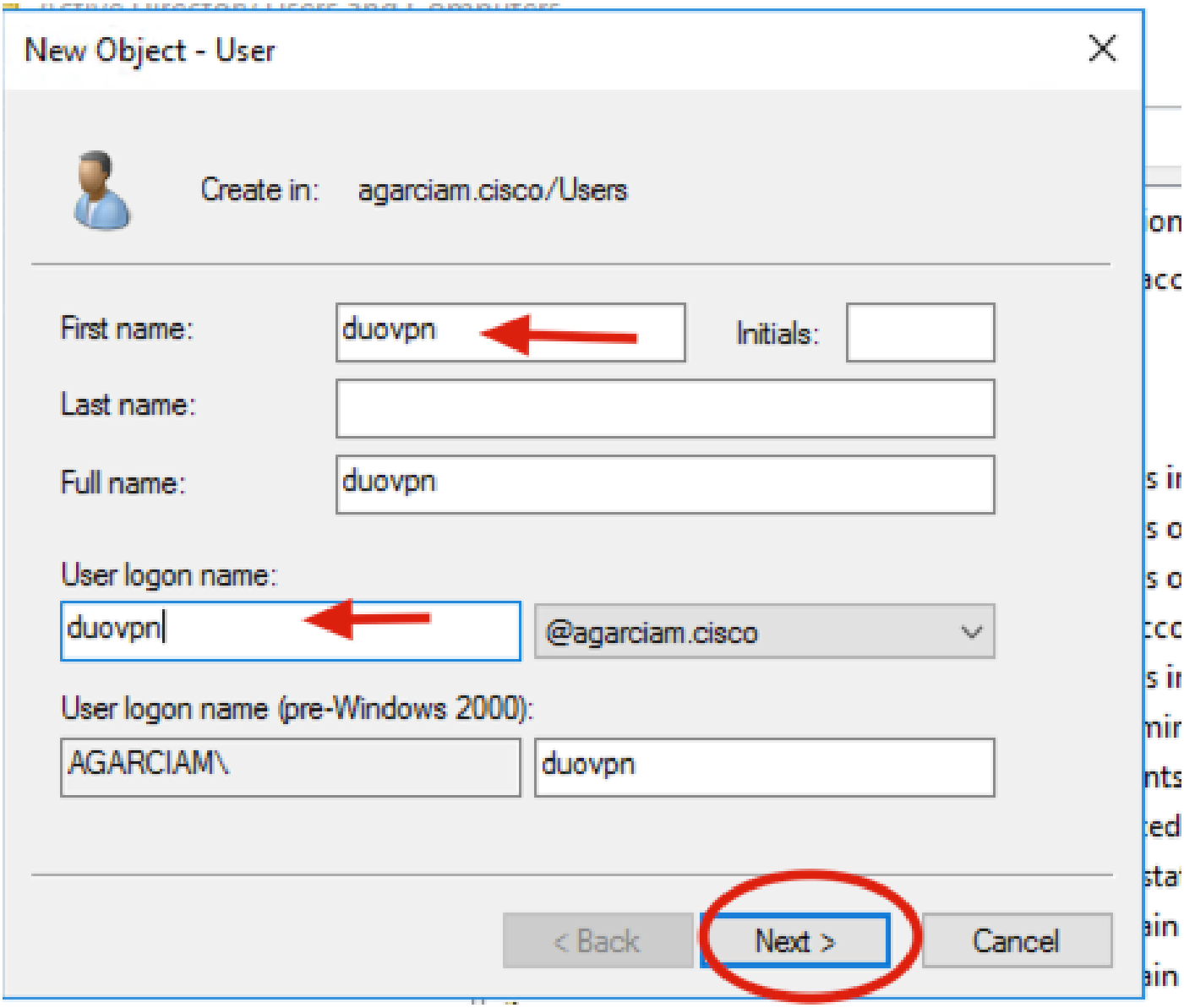
この設定例では、Duo-USERSがセカンダリ認証用のターゲットグループとして使用されています。



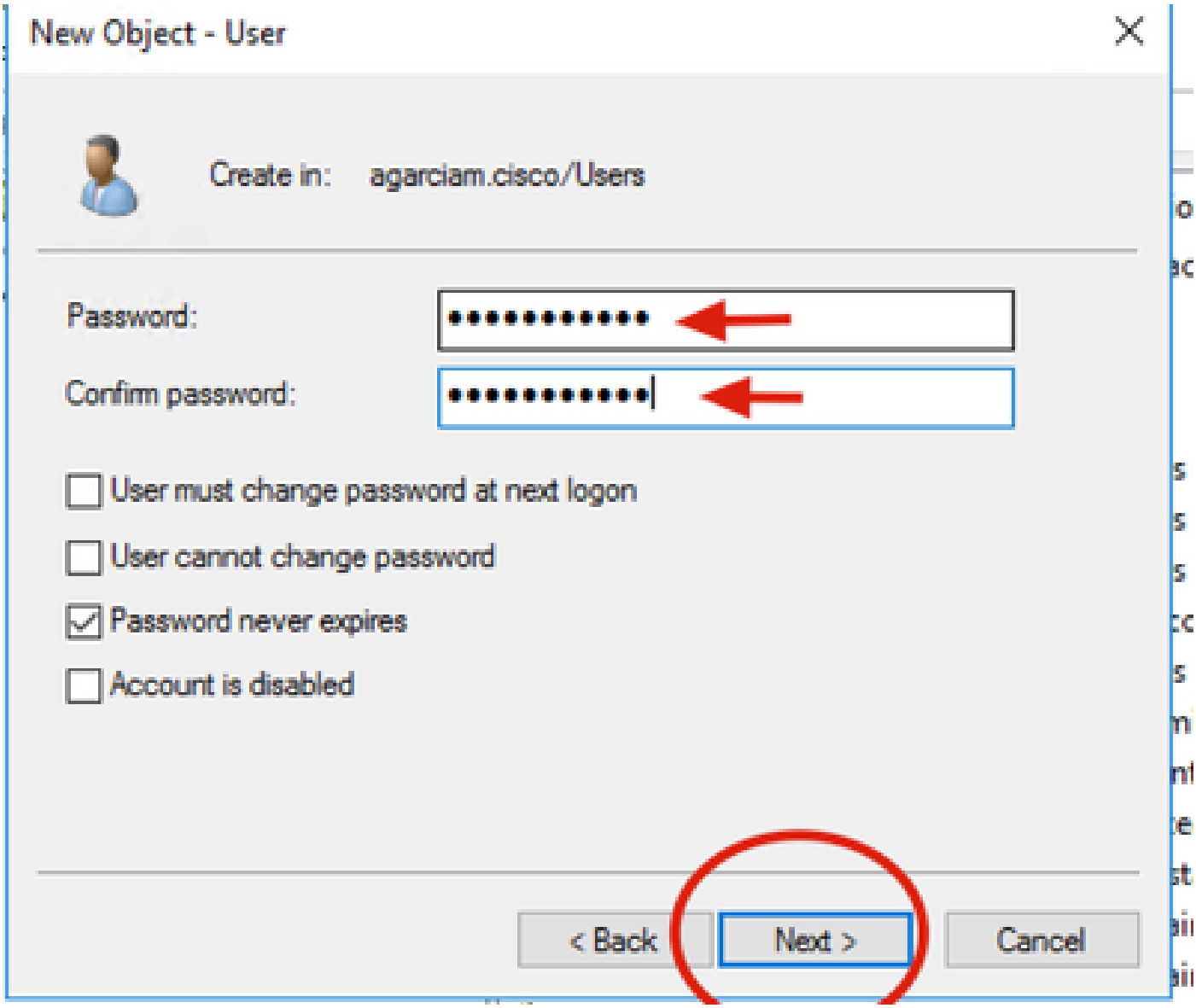
3.図に示すように、Usersフォルダを右クリックし、New > Userを選択します。



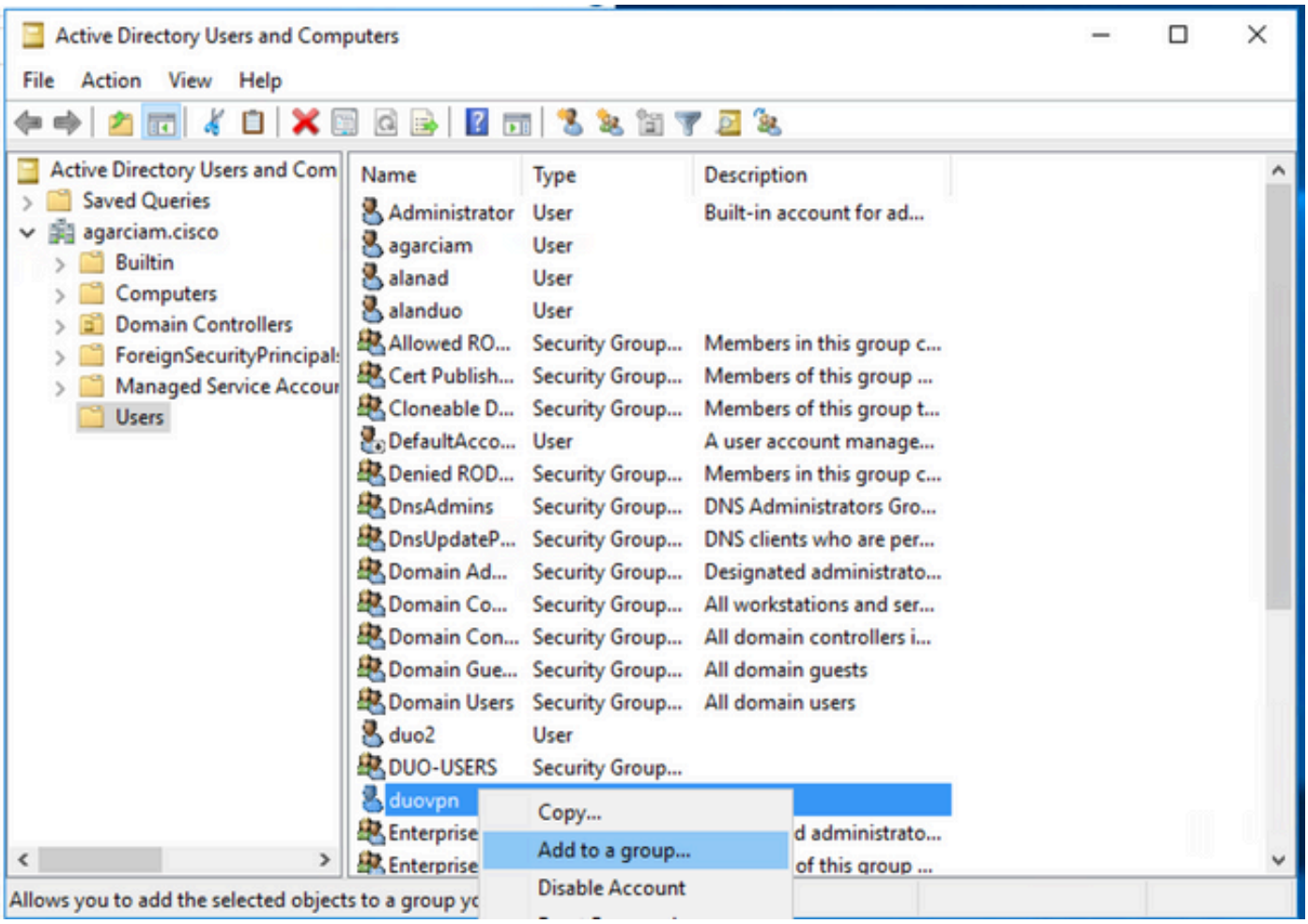
4.「新規オブジェクト・ユーザー」ウィンドウで、この新規ユーザーのID属性を指定し、図に示すように「次へ」をクリックします。



5.パスワードを確認してNextをクリックし、ユーザ情報が確認されたらFinishをクリックします。

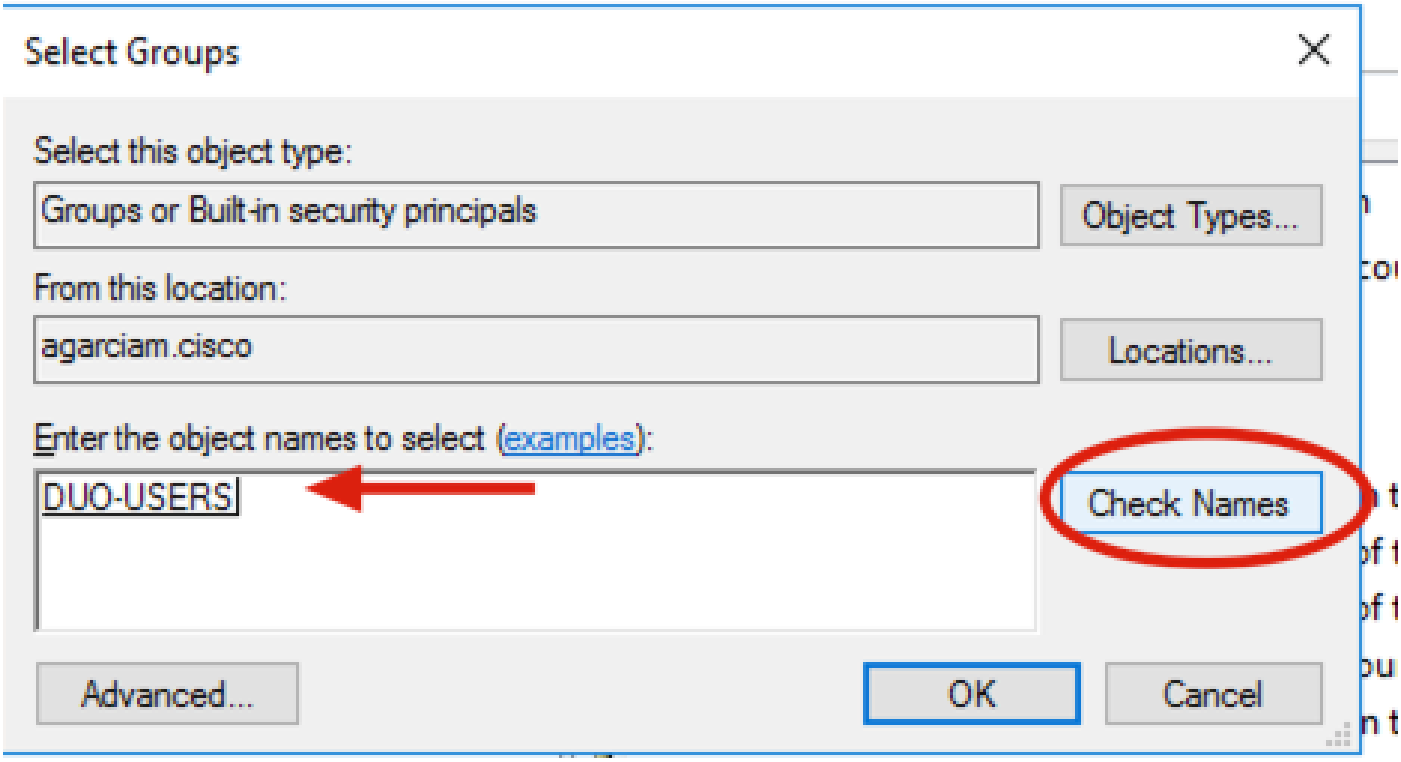


6.図に示すように、新しいユーザを特定のグループに割り当て、それを右クリックしてAdd to a groupを選択します。



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、「名前の確認」をクリックします。

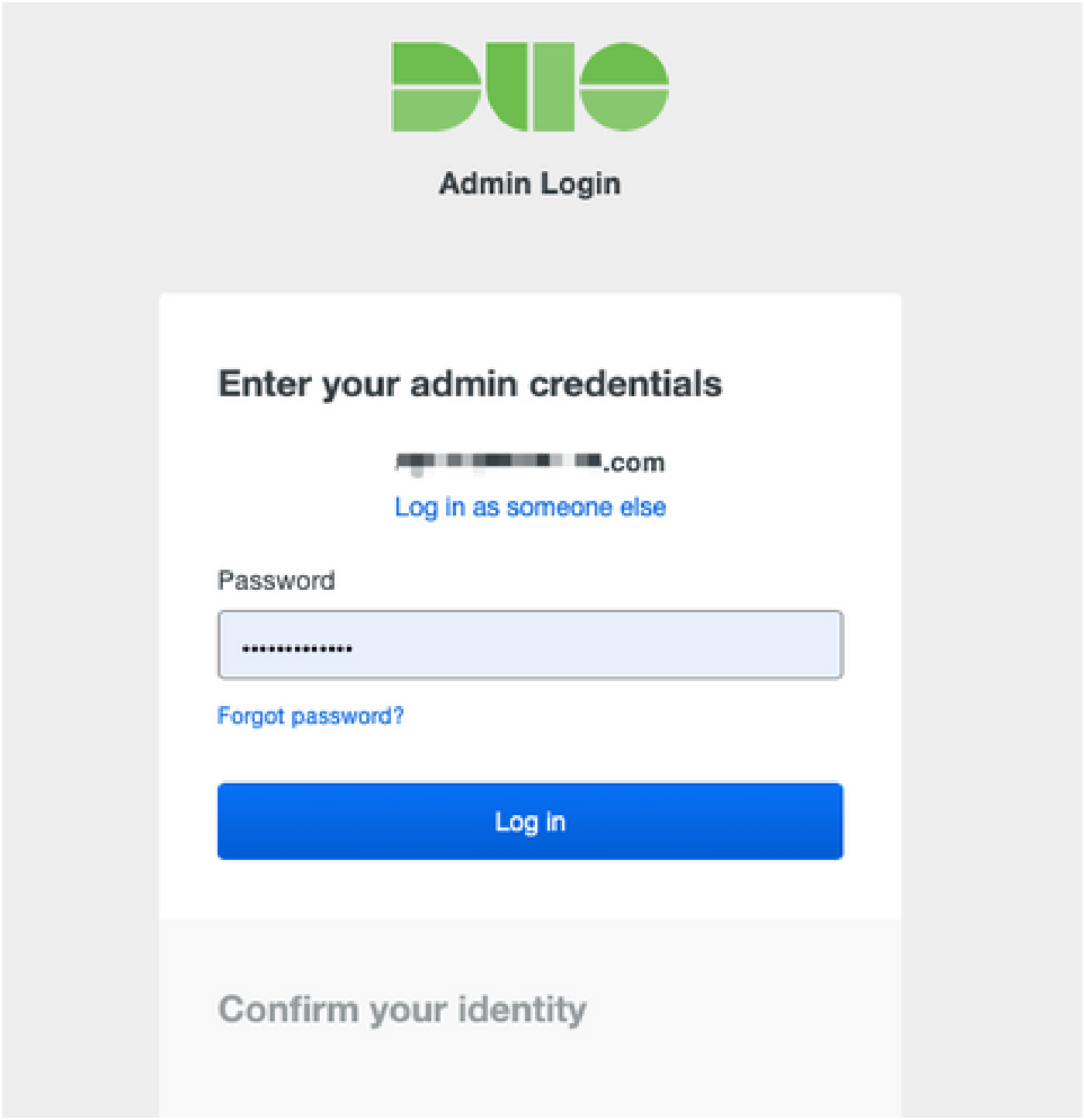
次に、条件に一致する名前を選択して、OKをクリックします。



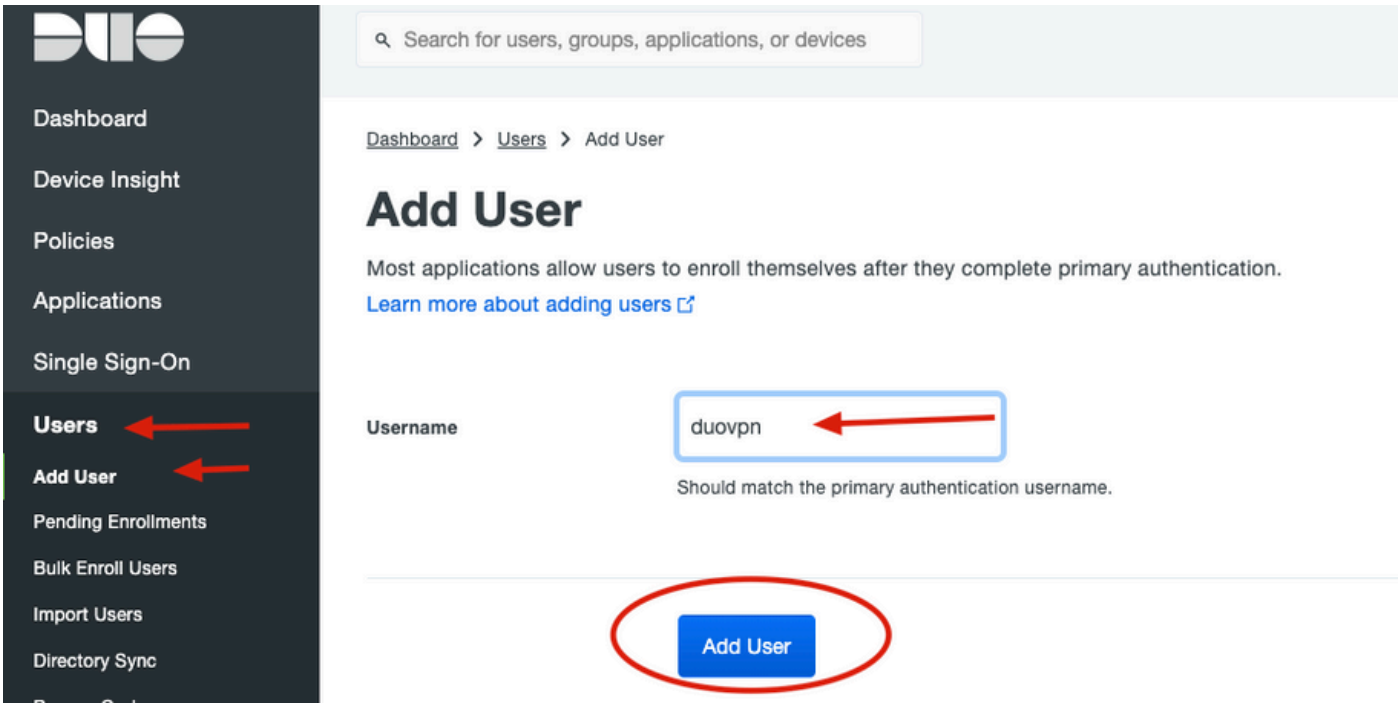
8.これは、このドキュメントで例として使用されているユーザです。

Duo構成

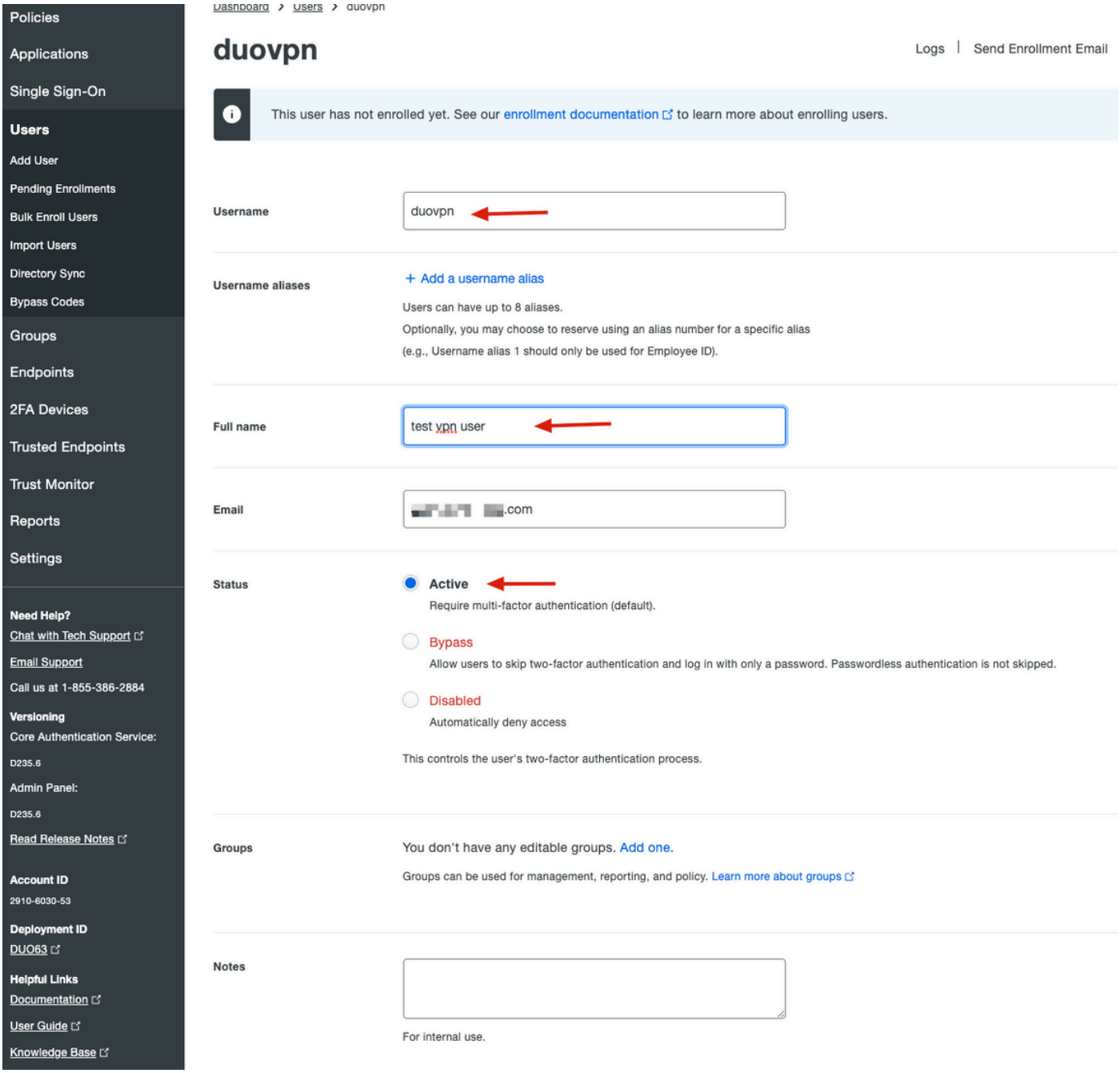
1. Dudo Adminポータルにログインします。



2.左側のパネルで、Usersに移動し、Add Userをクリックして、Active Domainの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。



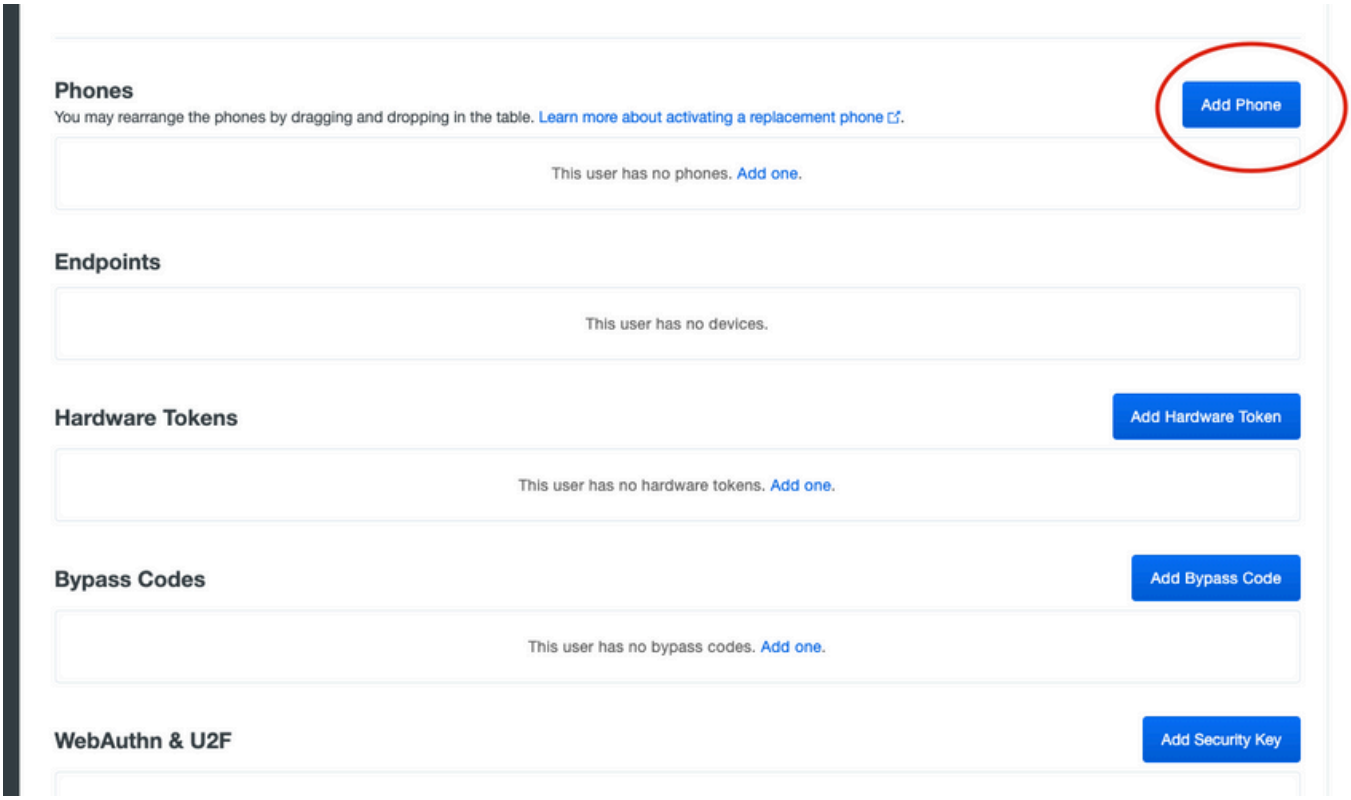
3.新しいユーザパネルで、ブランクに必要なすべての情報を入力します。



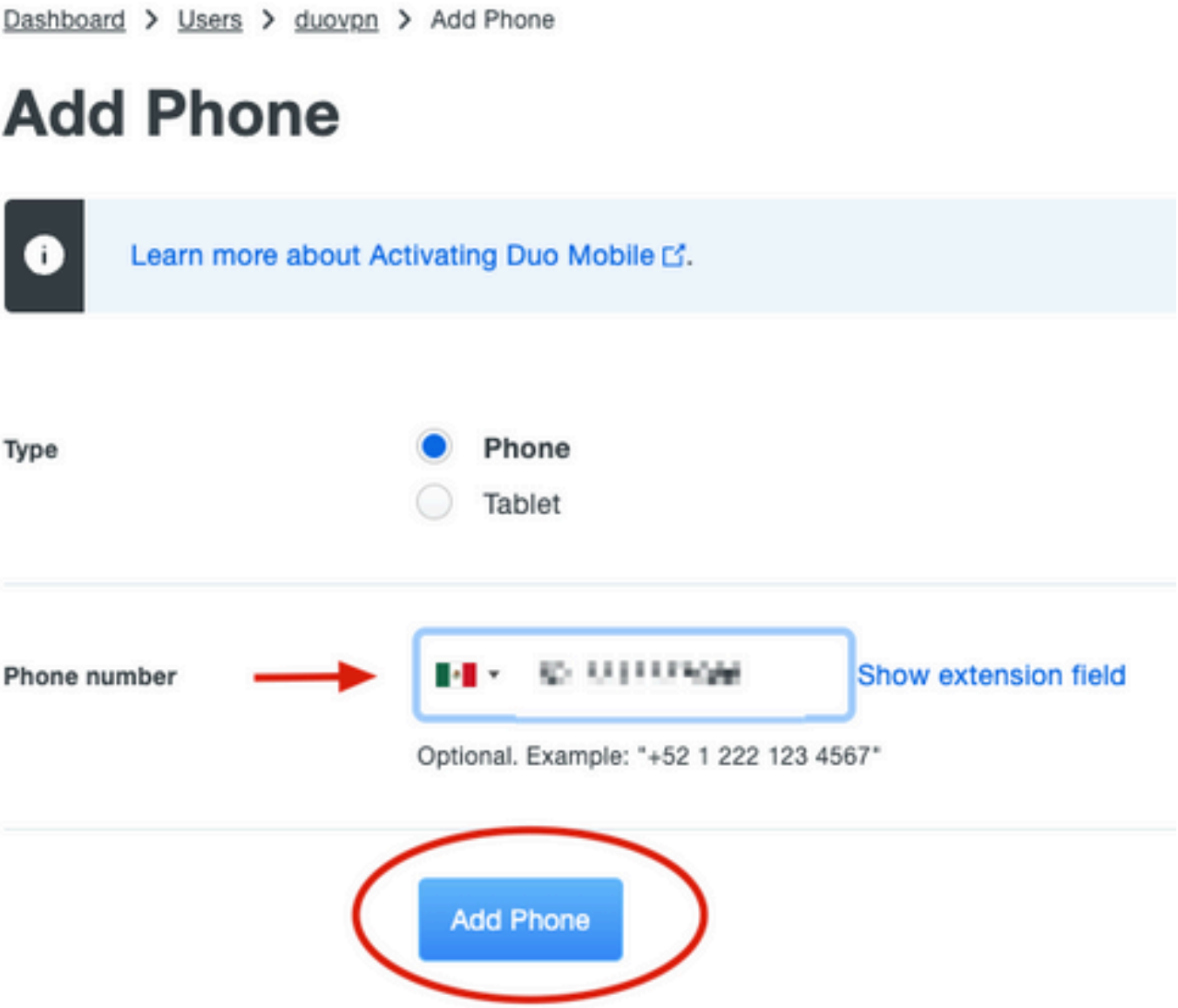
4.ユーザデバイスの下で、セカンダリ認証方式を指定します。

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。

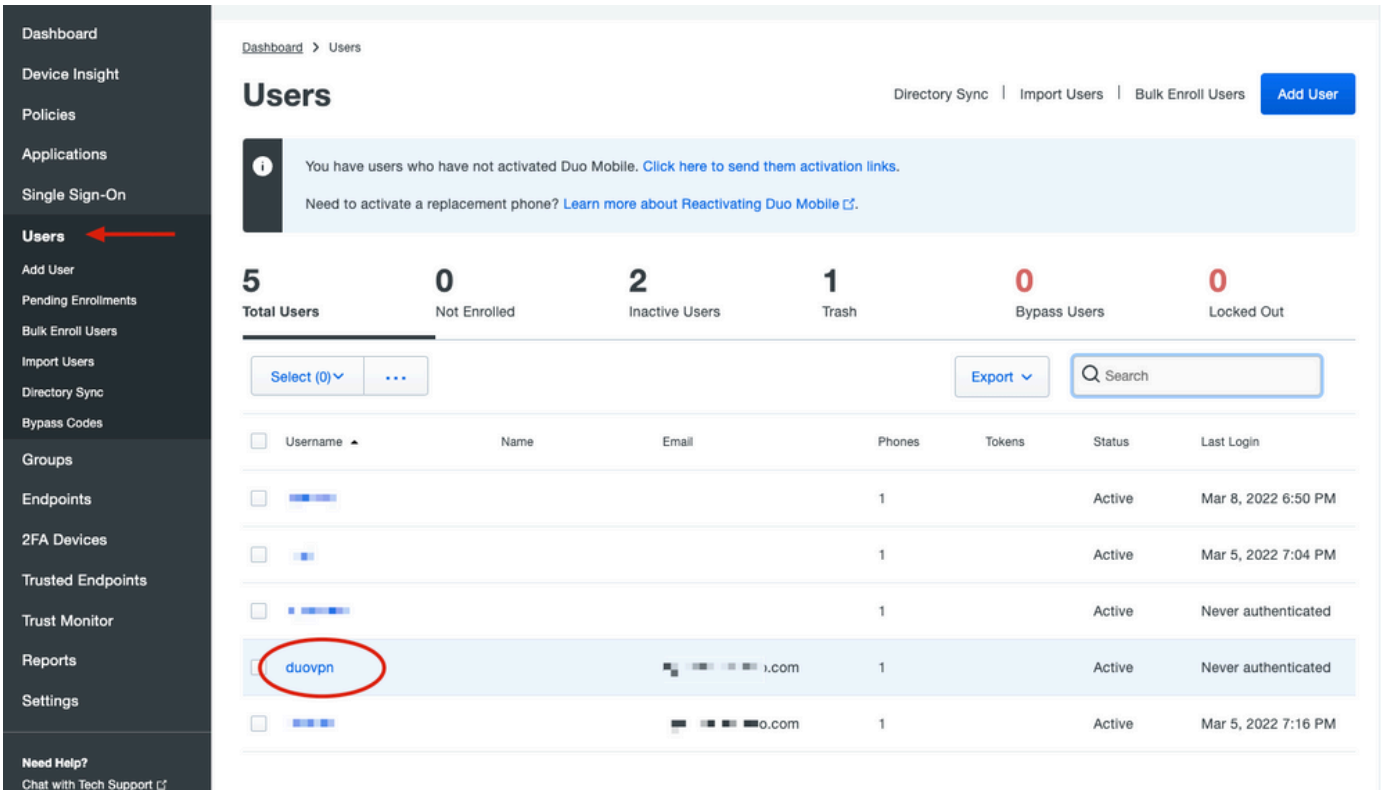
Add Phoneをクリックします。



5.ユーザの電話番号を入力し、Add Phoneをクリックします。

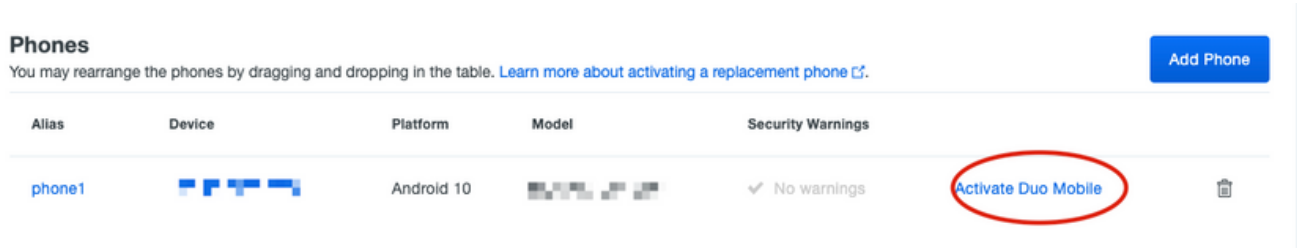


6.左側のDuo Adminパネルで、Usersに移動し、新しいユーザをクリックします。

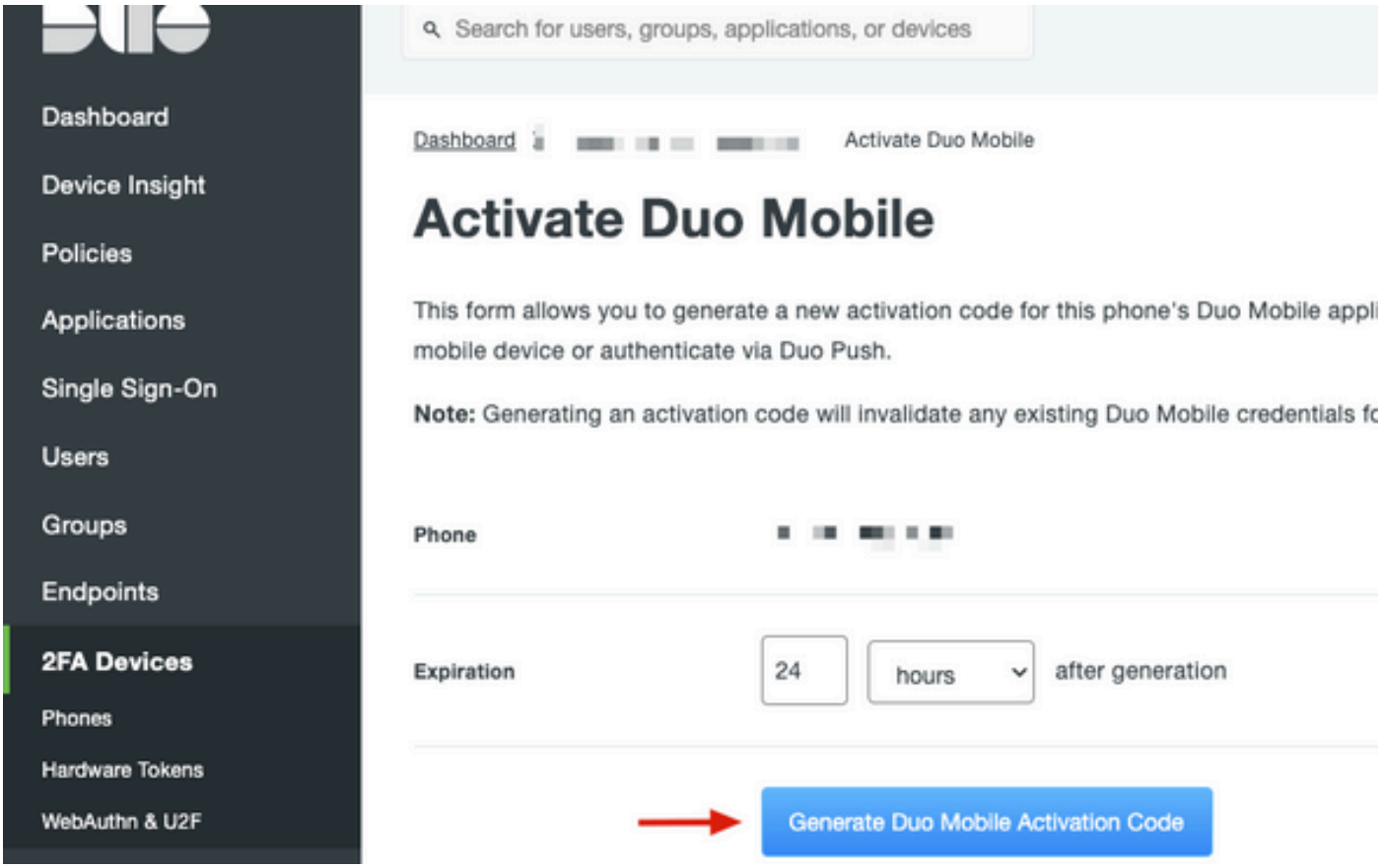


注：現時点で電話へのアクセス権がない場合は、電子メールオプションを選択できます。

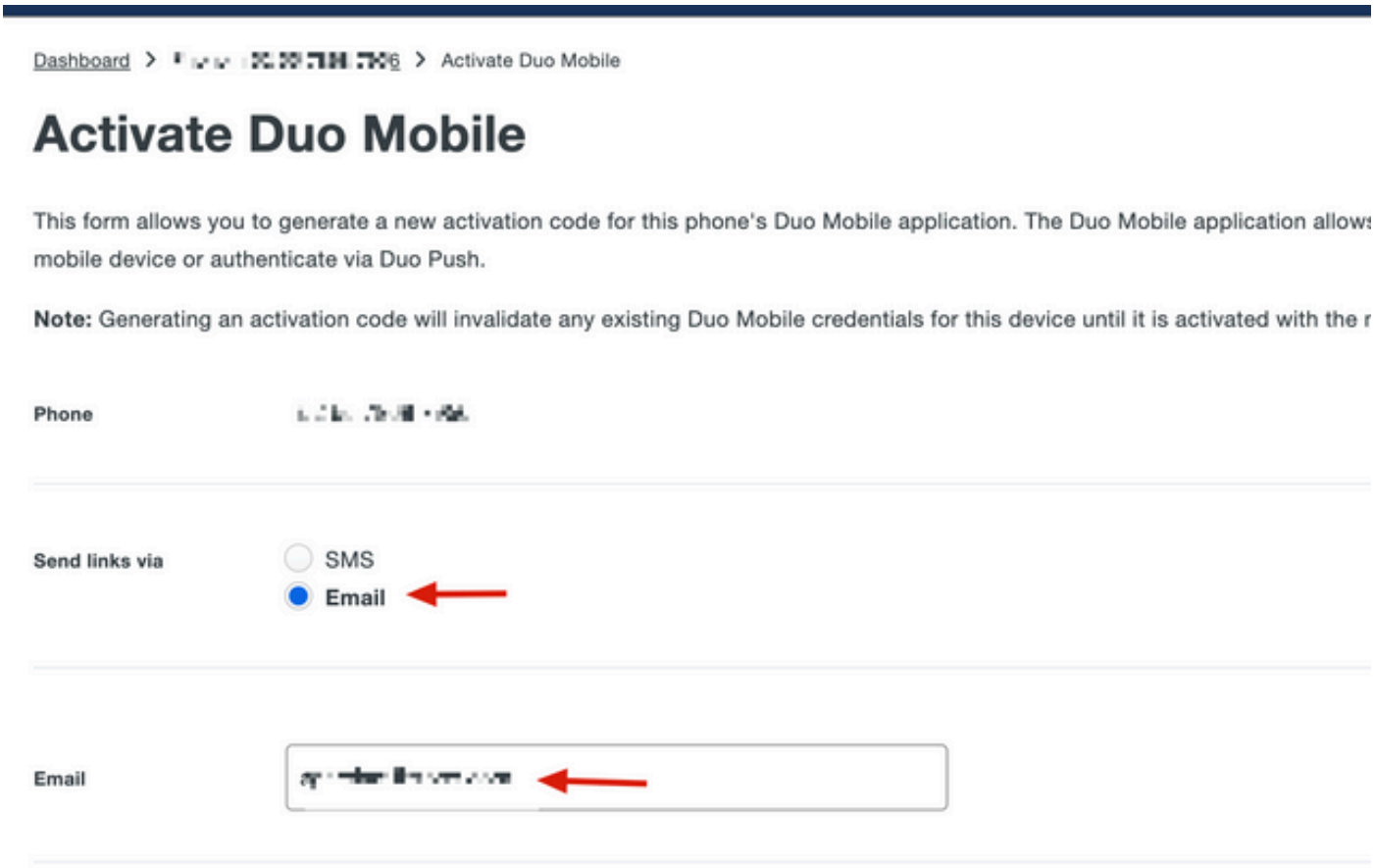
7.Phonesセクションに移動し、Activate Duo Mobileをクリックします。



8. Generate Duo Mobile Activation Codeをクリックします。



9. [電子メール] を選択して電子メールで指示を受信し、電子メールアドレスを入力して、[電子メールで指示を送信] 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 + ›r 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.モバイルデバイスからDuoモバイルアプリを開き、追加をクリックしてからQRコードを使用を選択し、指示メールからコードをスキャンします。

12.新しいユーザーがDuoモバイルアプリに追加されます。

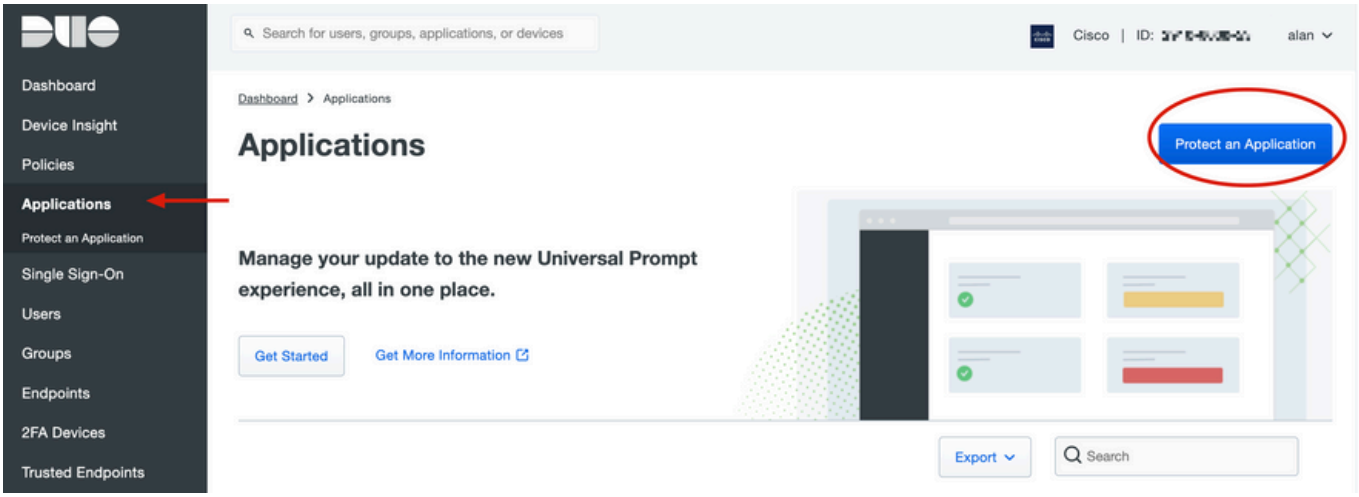
Duo認証プロキシの設定

1.https://duo.com/docs/authproxy-referenceからDuo Auth Proxy Managerをダウンロードしてインストールします。

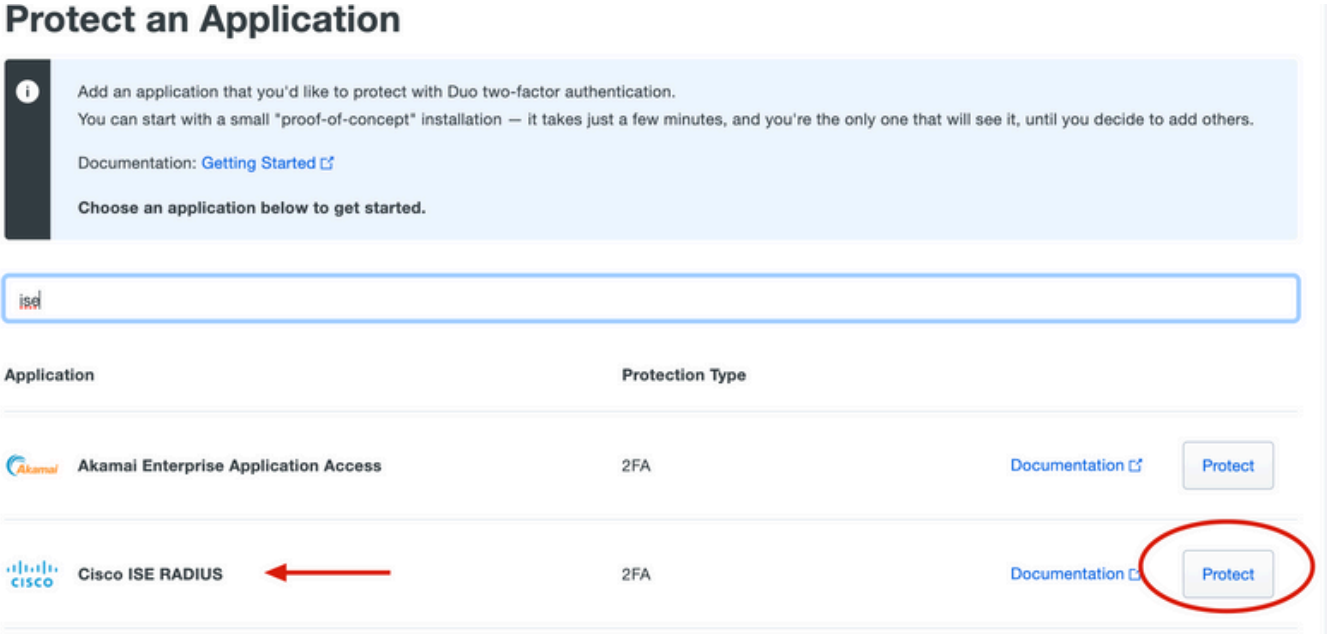
注：このドキュメントでは、Duo Auth Proxy Managerは、Active Directoryサービスをホストする同じWindowsサーバにインストールされています。

---

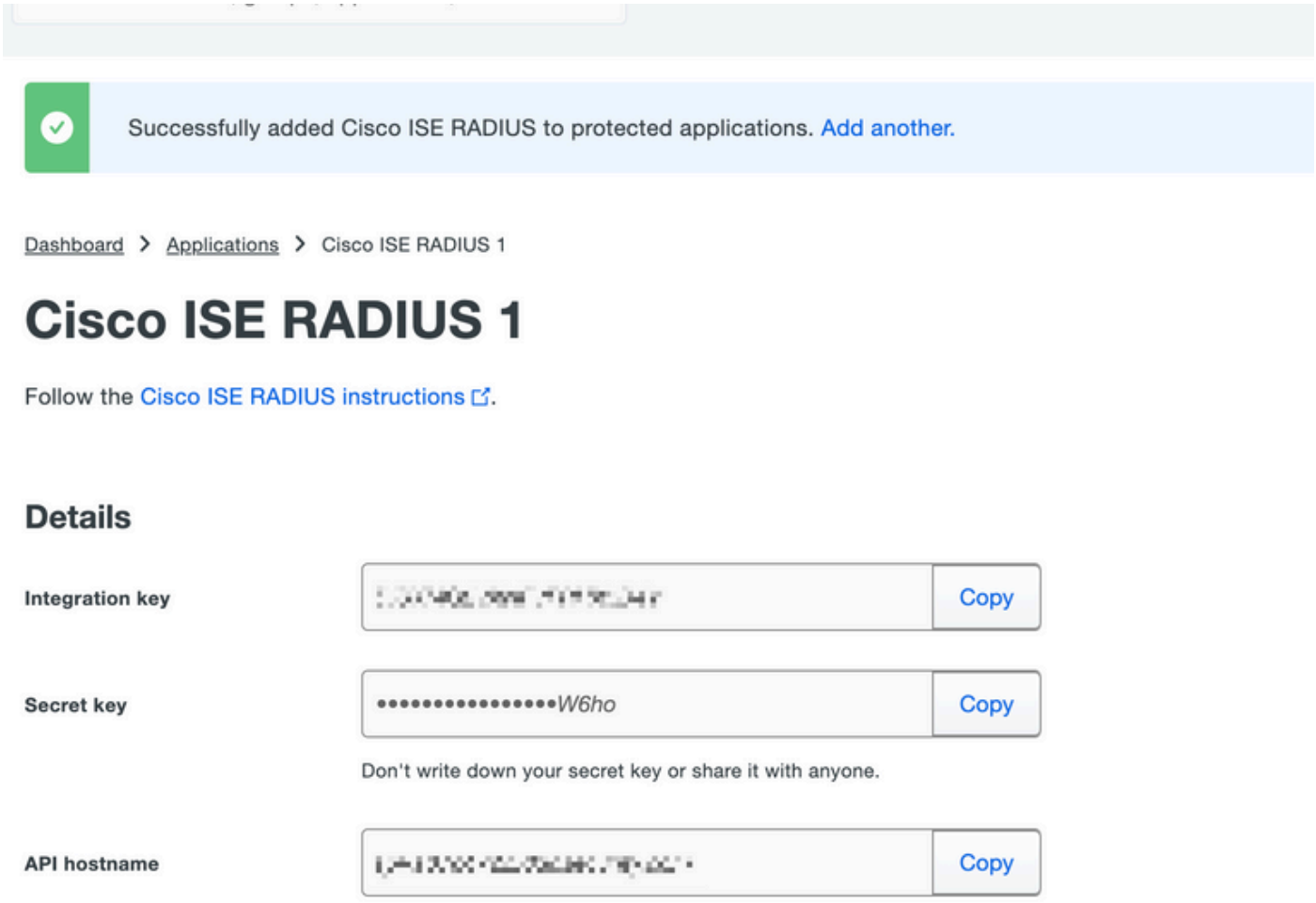
2. Duo AdminパネルでApplicationsに移動し、Protect an Applicationをクリックします。



3.検索バーで、Cisco ISE Radiusを探します。

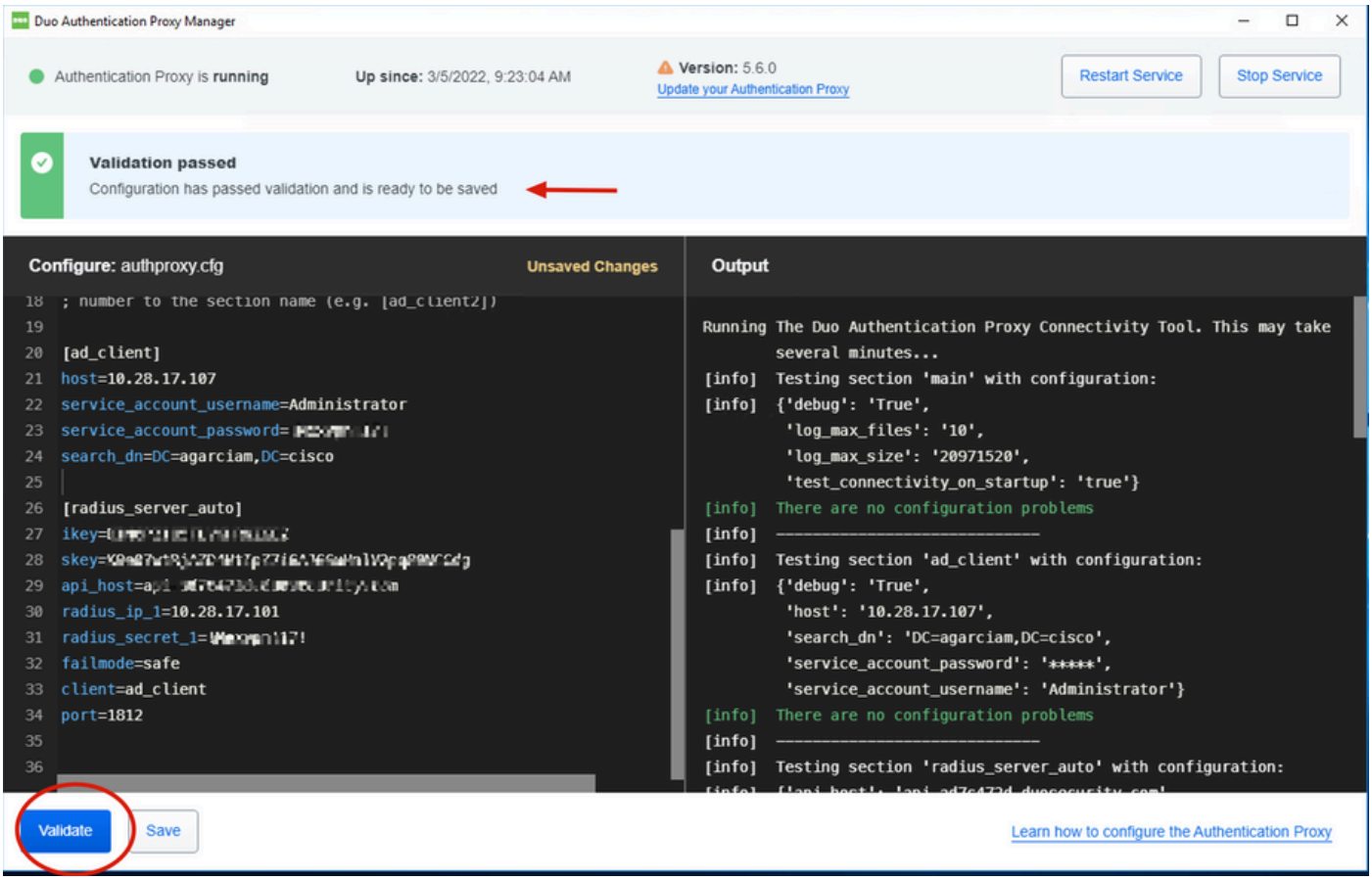


4.統合キー、秘密キー、およびAPIホスト名をコピーします。この情報は、Duo Authentication Proxy設定に必要です。



5. Duo Authentication Proxy Managerアプリケーションを実行し、Active DirectoryクライアントとISE Radiusサーバの両方の設定を完了して、Validateをクリックします。

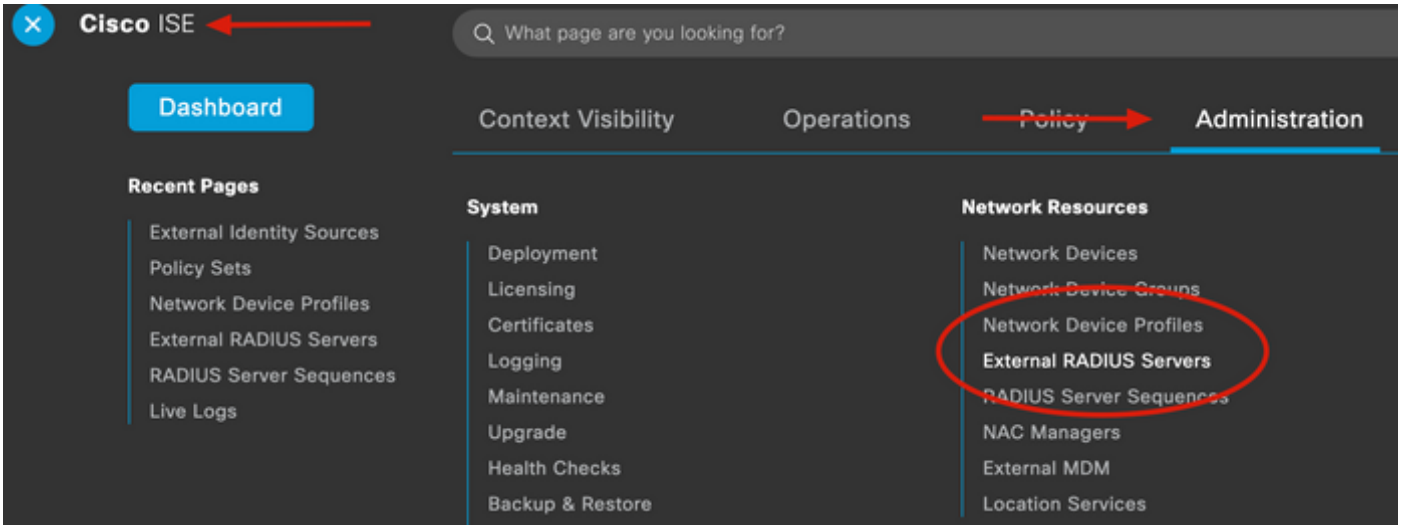
注：検証が失敗した場合は、「デバッグ」タブで詳細を参照し、適宜修正してください。



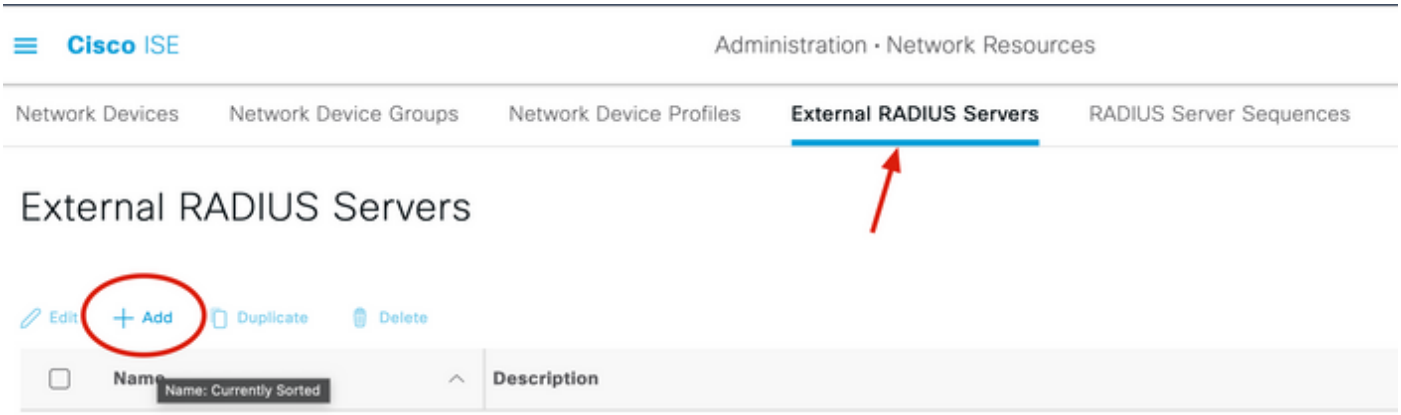
Cisco ISEの設定

1. ISE管理ポータルにログインします。

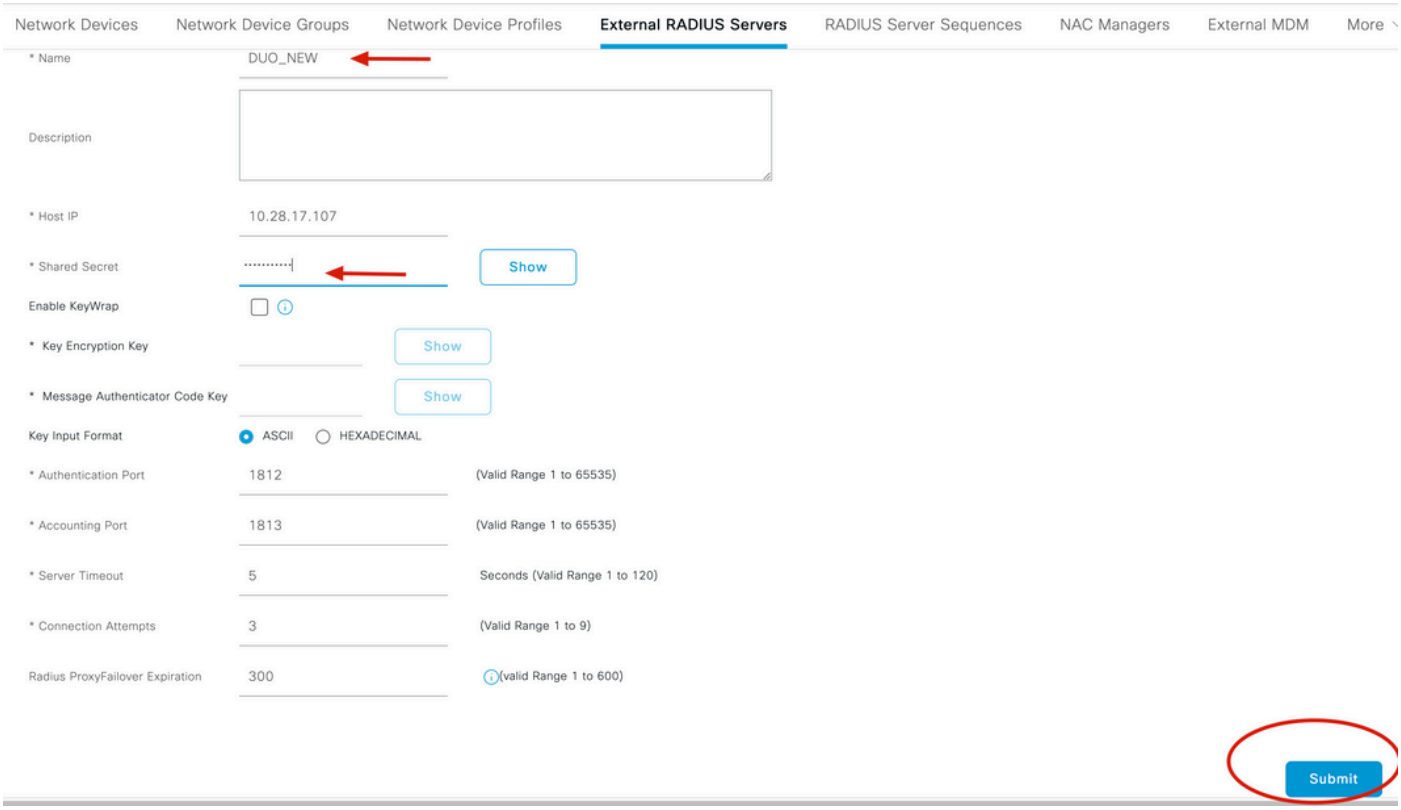
2. Cisco ISEタブを展開し、Administrationに移動して、Network Resourcesをクリックし、External RADIUS Serversをクリックします。



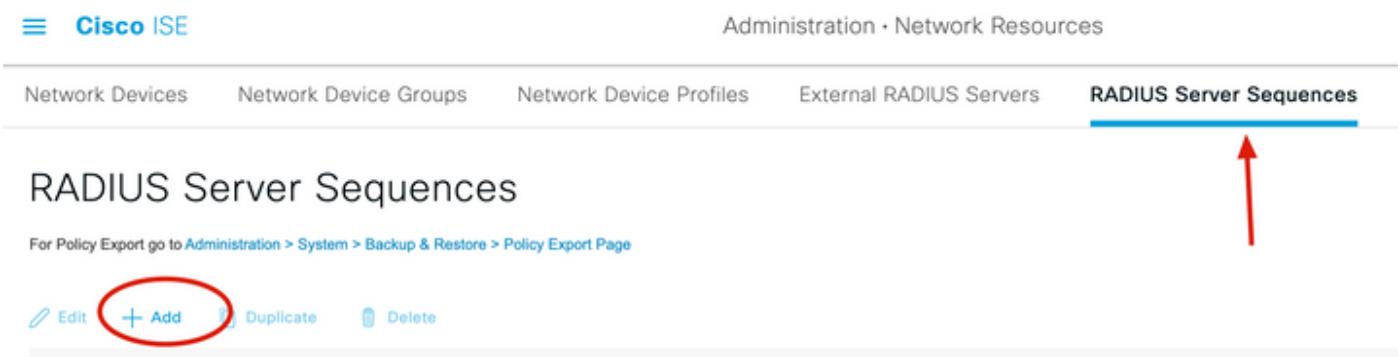
3. External Radius Serversタブで、Addをクリックします。



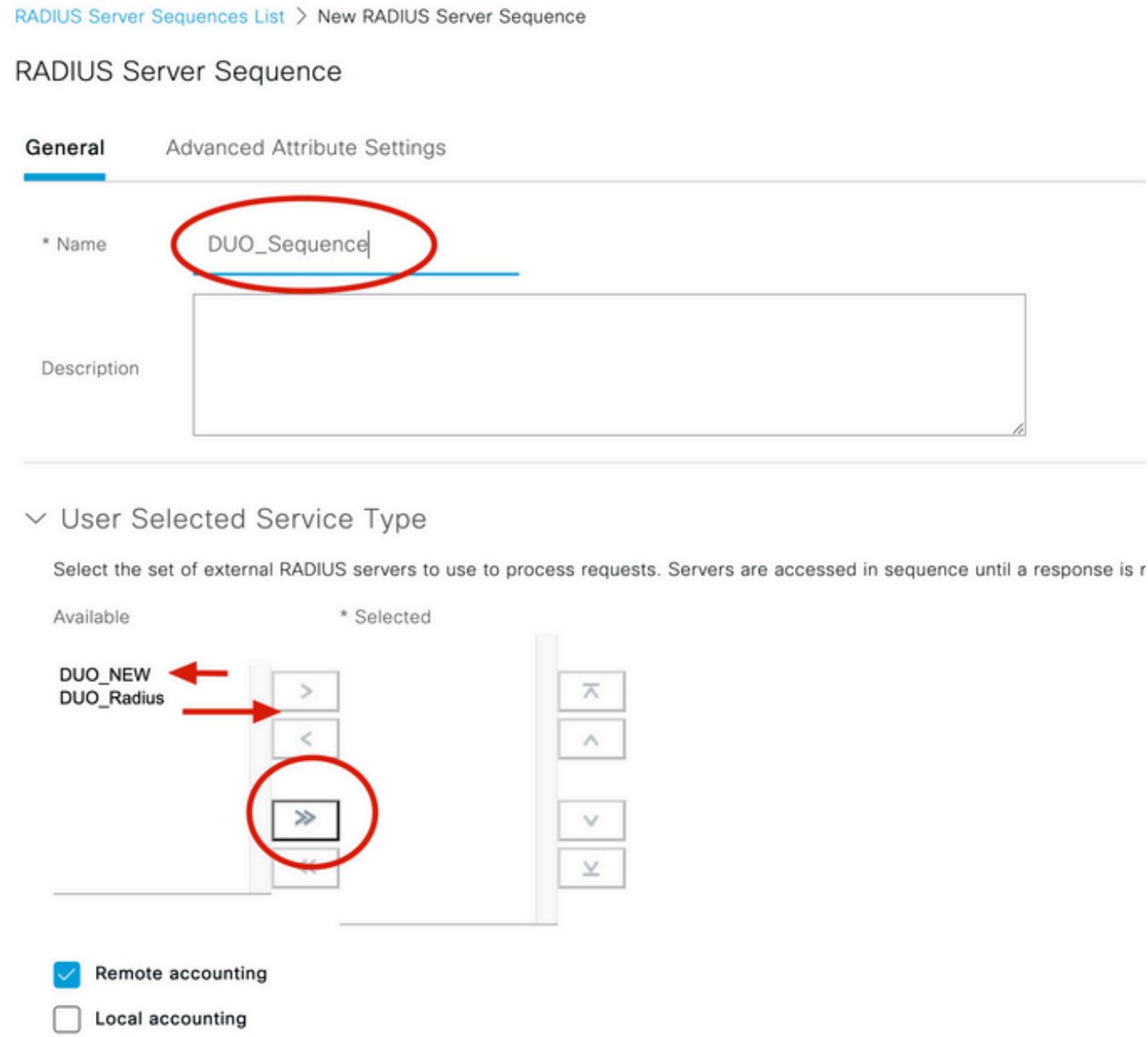
4. Duo Authentication Proxy Managerで使用されているRADIUS設定の空欄を埋め、Submitをクリックします。



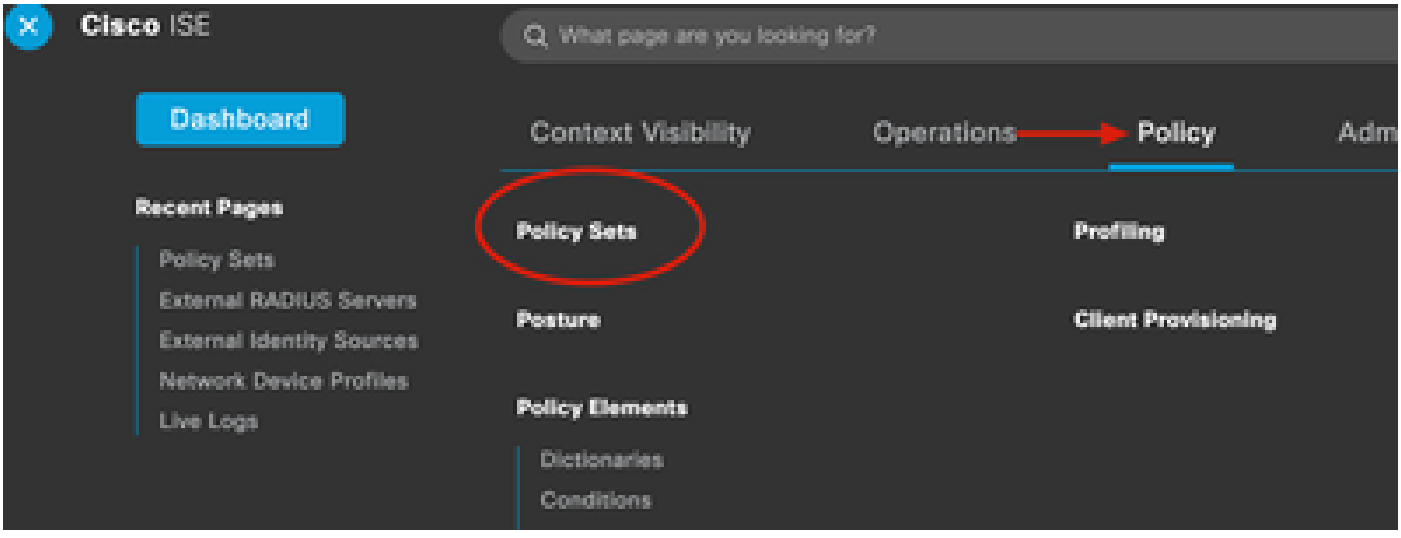
5. RADIUS Server Sequencesタブに移動し、Addをクリックします。



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。

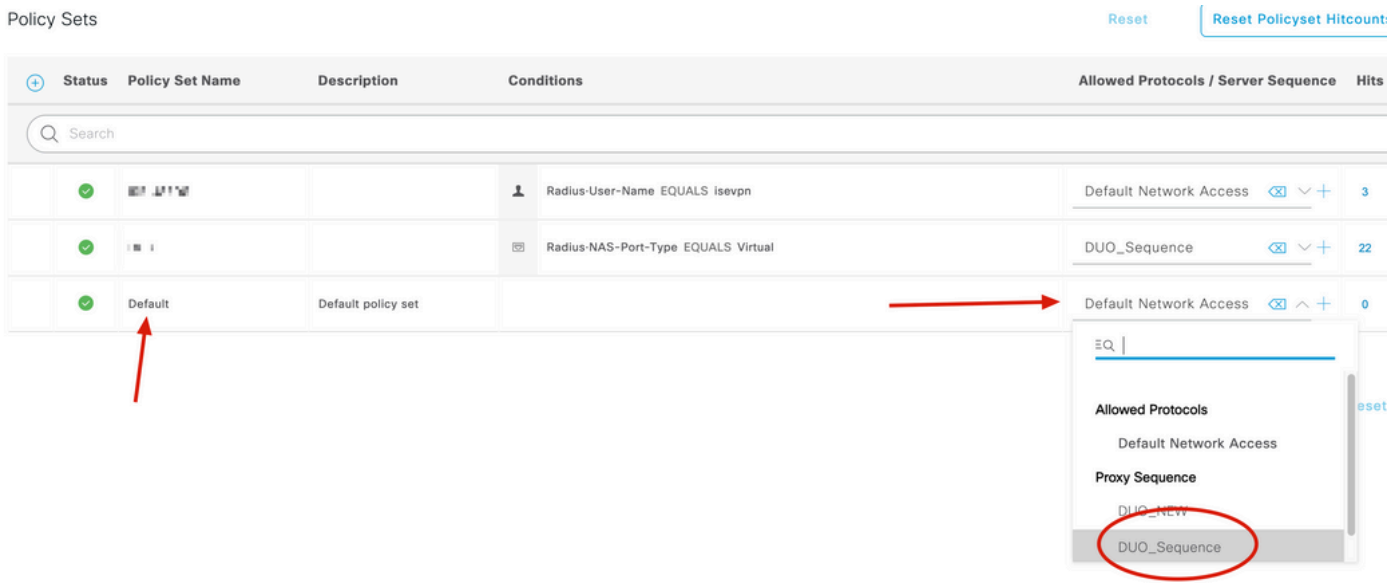


7.ダッシュボードメニューからPolicyに移動し、Policy Setsをクリックします。



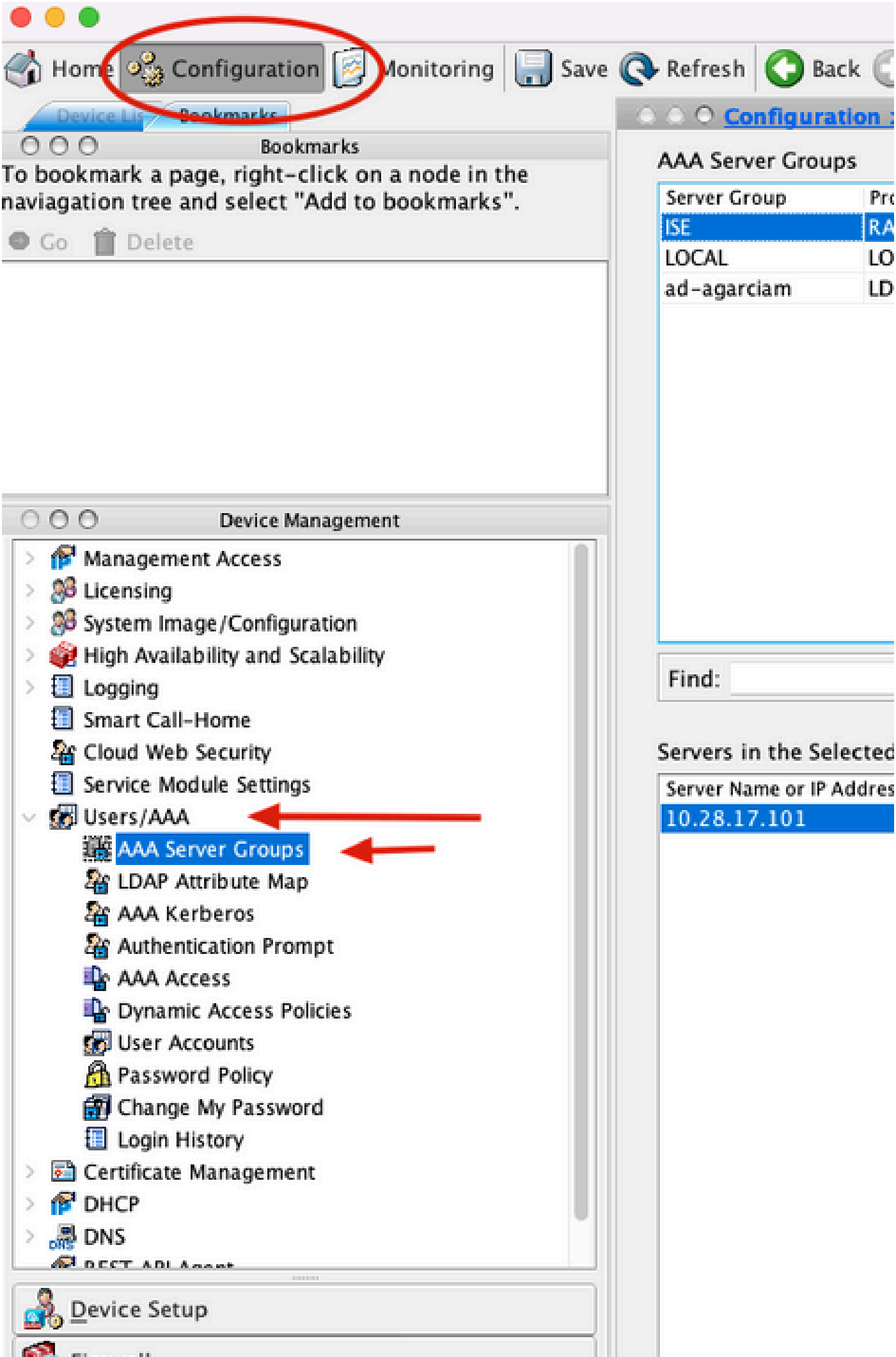
8. RADIUSシーケンスをデフォルトポリシーに割り当てます。

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ているため、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。



Cisco ASA RADIUS/ISEの設定

1. AAA Server groupsの下でISE RADIUS Serverを設定し、Configurationに移動して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。


Home
Configuration
Monitoring
Save
Refresh
Back
Bookmarks
To bookmark a page, right-click on a node in the naviagation tree and select "Add to bookmarks".
Go
Delete
Configuration
AAA Server Groups
Server Group
ISE
LOCAL
ad-agarciam
Find:
Servers in the Selected
Server Name or IP Addres
10.28.17.101
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
Device Setup

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。