

証明書認証の設定& DUO SAML認証

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[DUOでのステップの設定](#)

[アプリケーション保護ポリシーの作成](#)

[アプリケーションポリシーの作成](#)

[FMCの設定手順](#)

[FTDへのID証明書の展開](#)

[IDP証明書のFTDへの展開](#)

[SAML SSOオブジェクトの作成](#)

[リモートアクセス仮想プライベートネットワーク\(RAVPN\)構成の作成](#)

[確認](#)

[トラブルシューティング](#)

[問題1: 証明書認証が失敗している。](#)

[問題2:SAMLの障害](#)

はじめに

このドキュメントでは、証明書ベースの認証と二重SAML認証の実装例について説明します。

前提条件

このガイドで使用するツールとデバイスは次のとおりです。

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- 内部認証局(CA)
- Cisco DUO Premierアカウント
- Cisco DUO認証プロキシ
- Cisco Secure Client(CSC)

要件

次の項目に関する知識があることが推奨されます。

- 基本的なVPN
- SSL/TLS
- 公開キーインフラストラクチャ

- FMCの経験
- Cisco Secure Client
- FTDコード7.2.0以降
- Cisco DUO認証プロキシ

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。

- シスコFTD(7.3.1)
- Cisco FMC(7.3.1)
- Cisco Secure Client(5.0.02075)
- Cisco DUO認証プロキシ(6.0.1)
- Mac OS(13.4.1)
- Active Directory

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たものです。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。

DUOでのステップの設定

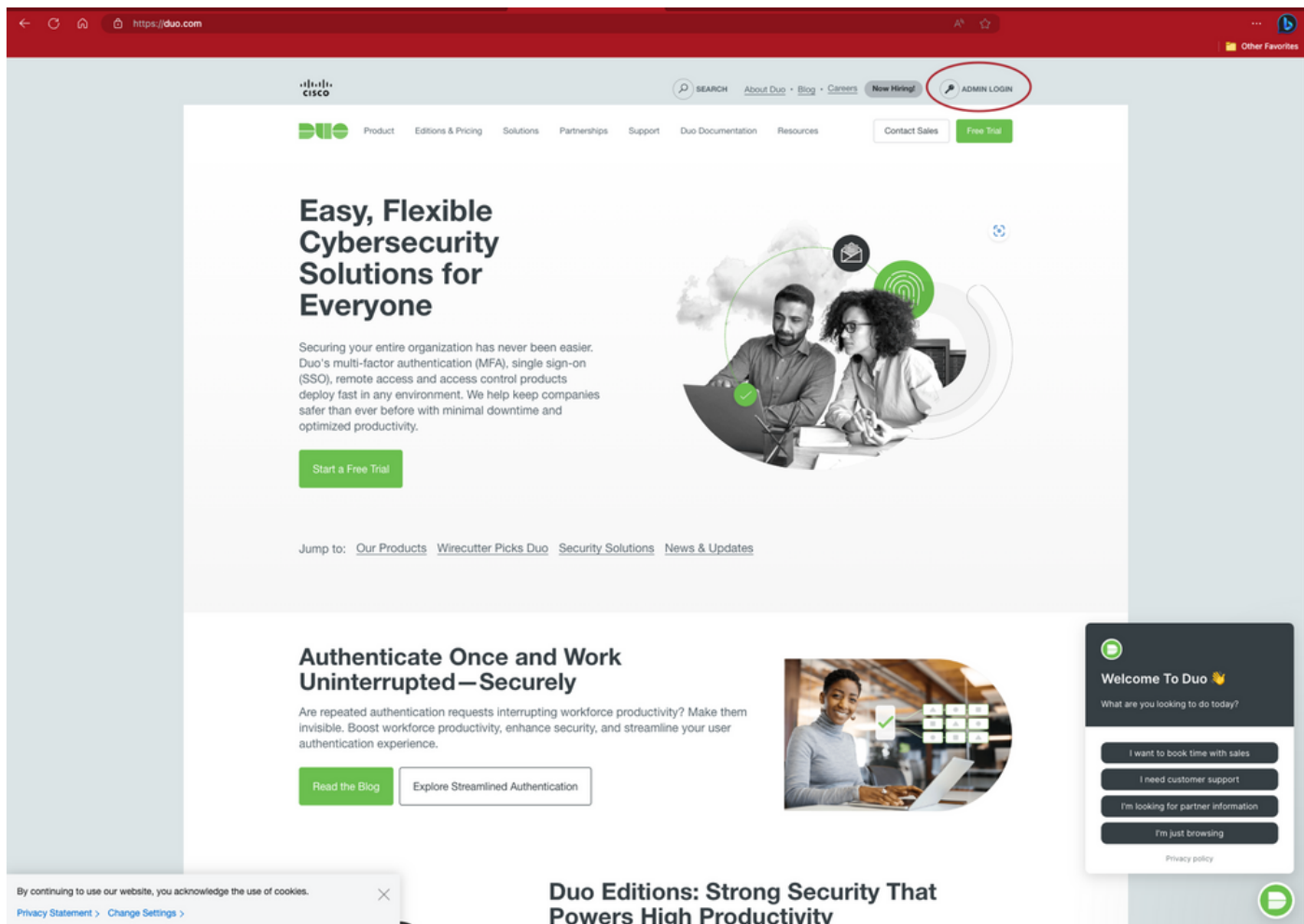
この項では、Cisco DUOシングルサインオン(SSO)を設定する手順について説明します。開始する前に、認証プロキシが実装されていることを確認してください。



警告：認証プロキシが実装されていない場合、このリンクがこのタスクのガイドになります。 [DUO認証プロキシガイド](#)

アプリケーション保護ポリシーの作成

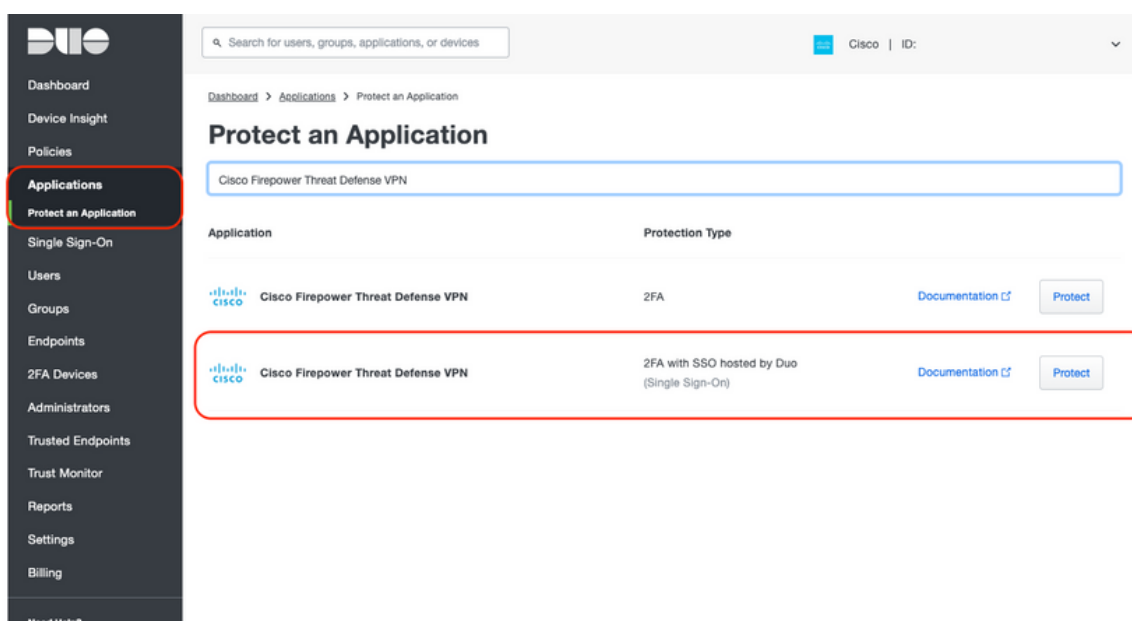
ステップ 1： [Cisco Duo](#) リンクから管理パネルにサインオンします。



Cisco DUOホームページ

ステップ 2ダッシュボード>アプリケーション>アプリケーションの保護に移動します。

検索バーで「Cisco Firepower Threat Defense VPN」と入力し、「Protect」を選択します。



アプリケーションの保護のスクリーンショット

保護タイプが「2FA with SSO hosted by Duo」のみのオプションを選択します。

ステップ3：このURL情報をメタデータの下にコピーします。

- アイデンティティプロバイダーエンティティID
- SSOのURL
- ログアウトURL

See the [Cisco ASA SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID

Copy

Sign In URL

Copy

Sign Out URL

Copy

コピーする情報の例



注：スクリーンショットのリンクが省略されています。

ステップ4「Download certificate」を選択し、Downloadsの下にあるIdentity Provider Certificateをダウンロードします。

ステップ5サービスプロバイダー情報の入力

Cisco FirepowerベースURL:FTDに到達するために使用されるFQDN

接続プロファイル名：トンネルグループ名

アプリケーションポリシーの作成

ステップ1:Policyの下にApplication Policyを作成するには、図のようにApply a policy to all usersを選択してからOr, create a new Policyを選択します。

Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies

Apply a policy to groups of users

Application policy

Apply a policy to all users

アプリケーションポリシーの作成例

Apply a Policy



Policy

Select a Policy



[Or, create a new Policy.](#)

Apply Policy

アプリケーションポリシーの作成例

ステップ 2Policy nameで目的の名前を入力し、UsersでAuthentication policyを選択して、2FAを適用」次に、「Create Policy」を使用して保存します。

Create a New Policy

Policy name

MFA

Users

New User policy

Authentication policy

User location

Devices

Trusted Endpoints

Device Health application

Remembered devices

Operating systems

Browsers

Plugins

Networks

Authorized networks

Anonymous networks

Authenticators

Risk-based factor selection

Authentication methods

Duo Mobile app

Tampered devices

Screen lock

Full-disk encryption

Mobile device biometrics

Authentication policy

Enforce 2FA

Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Bypass 2FA

Skip two-factor authentication and enrollment, unless there is a superseding policy configured.

Deny access

Deny authentication to all users.

When enabled, this affects all users.

Choose another rule on the left to add to this policy.

Create Policy

アプリケーションポリシーの作成例

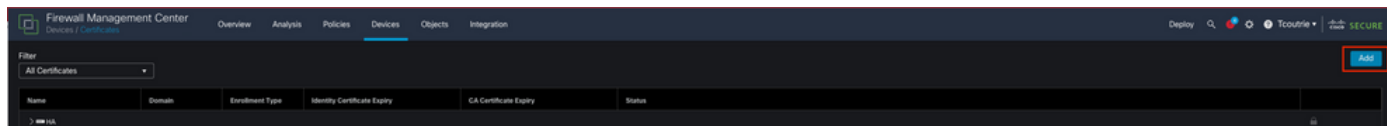
ステップ 3 次のウィンドウで「Apply Policy」をクリックしてポリシーを適用します。ページの一番下までスクロールして「Save」を選択し、DUO 構成を終了します

FMC の設定手順

FTDへのID証明書の展開

このセクションでは、証明書認証に必要なID証明書の設定とFTDへの展開について説明します。開始する前に、すべての設定を展開してください。

ステップ 1：図に示すように、Devices > Certificateに移動し、Addを選択します。



デバイス/証明書のスクリーンショット

ステップ2：デバイスドロップダウンからFTDアプライアンスを選択します。+アイコンをクリックして、新しい証明書登録方式を追加します。

A screenshot of the 'Add New Certificate' dialog box. The title is 'Add New Certificate'. Below the title, there is a description: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.' There are two dropdown menus: 'Device*' with 'HA' selected, and 'Cert Enrollment*' with 'Select a certificate enrollment object' selected. To the right of the 'Cert Enrollment*' dropdown, there is a red square button with a white '+' icon. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

新規証明書の追加のスクリーンショット

ステップ3:図に示すように、「登録タイプ」を使用して環境で証明書を取得するための推奨される方法を選択します。

Add Cert Enrollment



Name*

FTD04-16

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

PKCS12 File



PKCS12 File*:

test.p12



Browse PKCS12 File

Passphrase:

.....



Validation Usage:



IPsec Client



SSL Client



SSL Server



Skip Check for CA flag in basic constraints of the CA Certificate



Allow Overrides

Cancel

Save

新しい証明書登録ページのスクリーンショット



ヒント：次のオプションを使用できます。自己署名証明書 – 新しい証明書をローカルに生成します。SCEP - Simple Certificate Enrollment Protocol(SCEP)を使用してCAから証明書を取得します。手動 – ルートおよびID証明書を手動でインストールします。PKCS12 – ルート、ID、秘密キーを使用して暗号化された証明書バンドルをします。

IDP証明書のFTDへの展開

このセクションでは、IDP証明書の設定とFTDへの展開について説明します。開始する前に、すべての設定を展開してください。

ステップ1: Devices > Certificateの順に移動し、Addを選択します。

ステップ2: デバイスドロップダウンからFTDアプライアンスを選択します。+アイコンをクリックして、新しい証明書登録方式を追加します。

ステップ3: 証明書登録の追加ウィンドウで、図に示すように必要な情報を入力し、次に図に示すように「保存」を入力します。

- Name: オブジェクトの名前
- 登録タイプ: 手動
- チェックボックスが有効: CAのみ
- CA証明書: 証明書のPEM形式

Add Cert Enrollment

Name*

duocert

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type

Manual

☒ CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

OC957DUc7tc4
b79bVzOXuqz5ZpaJHqtXV8fLOH
eIPYblyYBwSstXB+k75VHs0Voz
AkeySJCWRQXF
ISSRGu8DpUIKzKu2zd55322+wd
fkyy/WMXUJWmSXXKnnHEsOqL
GCxmfd+5OsWlo
ICCMGa5gYgEv8EHF3Y++sFg=
-----END CERTIFICATE-----

Validation Usage:

☒ IPsec Client

☐ SSL Client

☒ SSL Server

☐ Skip Check for CA flag in basic constraints of the CA Certificate

☐ Allow Overrides

Cancel

Save

証明書登録オブジェクトの作成例



注意：必要に応じて、「CA証明書の基本的な制約におけるCAフラグのスキップチェック」を使用できます。このオプションは注意して使用してください。

ステップ4：図に示すように、「Cert Enrollment*」で新しく作成した証明書登録オブジェクトを

選択してから、「Add」を選択します。

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

HA

Cert Enrollment*:

duocert

Cert Enrollment Details:

Name:	duocert
Enrollment Type:	Manual (CA Only)
Enrollment URL:	N/A

Cancel

Add

追加された証明書登録オブジェクトとデバイスのスクリーンショット

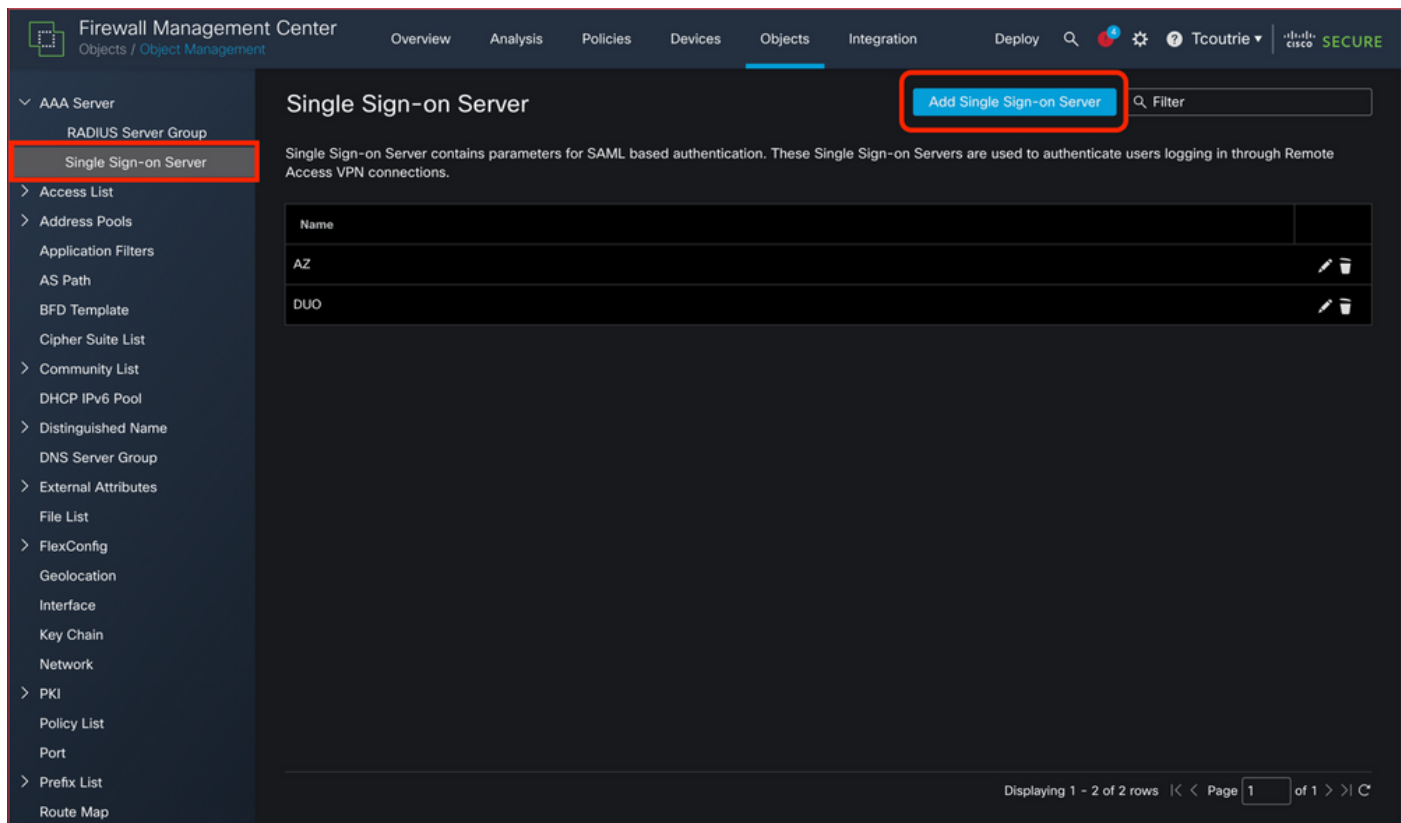


注：追加されると、証明書はただちに導入されます。

SAML SSOオブジェクトの作成

ここでは、FMC経由でSAML SSOを設定する手順について説明します。開始する前に、すべての設定を展開してください。

ステップ 1：Objects > AAA Server > Single Sign-on Serverの順に移動し、Add Single Sign-on Serverを選択します。



新しいSSOオブジェクトの作成例

ステップ 2 「Create an Application Protection Policy」で必要な情報を入力します。

になります。完了したら続行するには、「保存」を選択します。

- Name* : オブジェクトの名前
- アイデンティティプロバイダーエンティティID* : 手順3のエンティティID
- SSO URL* : 手順3からコピーしたサインインURL
- ログアウトURL : ステップ3からコピーしたログアウトURL
- ベースURL : ステップ5の「Cisco FirepowerベースURL」と同じFQDNを使用します
- アイデンティティプロバイダー証明書* : 展開されたIDP証明書
- サービスプロバイダー証明書:FTDの外部インターフェイス上の証明書

New Single Sign-on Server?

Name*

duosso

Identity Provider Entity ID*

SSO URL*

Logout URL

Base URL

https://vpn.ciscoexample.com

Identity Provider Certificate*

duocert

+

Service Provider Certificate

FTD04-16

+

Request Signature

--No Signature--

Request Timeout

Use the timeout set by the provide

seconds (1-7200)

☐ Enable IdP only accessible on Internal Network

☒ Request IdP re-authentication on Login

☐ Allow Overrides

Cancel

Save

新しいSSOオブジェクトの例



注：エンティティID、SSO URL、およびログアウトURLのリンクがスクリーンショット

から省略されています

リモートアクセス仮想プライベートネットワーク(RAVPN)構成の作成

このセクションでは、ウィザードを使用してRAVPNを設定する手順について説明します。

ステップ 1 : Devices > Remote Accessの順に移動し、Addを選択します。

ステップ 2ウィザードで、新しいRAVPN Policy Wizardの名前を入力し、図に示すように、VPN Protocols: Add the Targeted Devicesの下でSSLを選択します。完了したら「Next」を選択します。

RAVPNウィザードのステップ1

ステップ 2接続プロファイルのオプションを設定します (以下を参照)。完了したら「次へ」を選択します。

- 接続プロファイル名 : 「アプリケーション保護ポリシーの作成」のステップ5のトンネルグループ名を使用します。

認証、許可、アカウントिंग(AAA):

- Authentication Method : クライアント証明書およびSAML
- Authentication Server:* 「SAML SSOオブジェクトの作成中」に作成したSSOオブジェクトを選択します。

クライアントアドレス割り当て :

- AAAサーバを使用 (レルムまたはRADIUSのみ) :RADIUSまたはLDAP
- DHCPサーバの使用:DHCPサーバ

- IPアドレスプールの使用:FTDのローカルプール

Firewall Management Center
Devices / VPN / Setup Wizard

Remote Access VPN Policy Wizard

Policy Assignment — Connection Profile — Secure Client — Access & Certificate — Summary

Connection Profile Name:

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Authentication Server:

SAML Login Experience: ☒ VPN client embedded browser ☐ Default OS Browser

☐ Allow connection only if username from certificate and SAML are the same

☐ Use username from client certificate for Authorization

Username From Certificate:

Primary Field:

Secondary Field:

Authorization Server:

Accounting Server:

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

☐ Use AAA Server (Realm or RADIUS only) ☒ Use DHCP Servers ☐ Use IP Address Pools

Use DHCP Servers:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:

Cancel Back Next

RAVPNウィザードのステップ2



ヒント：この実習では、DHCPサーバを使用します。

ステップ 3+を選択し、導入するCisco Secure ClientのWeb導入イメージをアップロードします。次に、展開するCSCイメージのチェックボックスを選択します。図に示すように。完了したら「Next」を選択します。

Firewall Management Center
Devices / VPN / Setup Wizard

Remote Access VPN Policy Wizard

Policy Assignment — Connection Profile — Secure Client — Access & Certificate — Summary

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from Cisco Software Download Center.

Secure Client File Object Name	Secure Client Package Name	Operating System
☒ cisco-secure-client-macos-5.0.02075-web...	cisco-secure-client-macos-5.0.02075-web...	Mac OS
☒ cisco-secure-client-win-5.0.02075-web...	cisco-secure-client-win-5.0.02075-web...	Windows

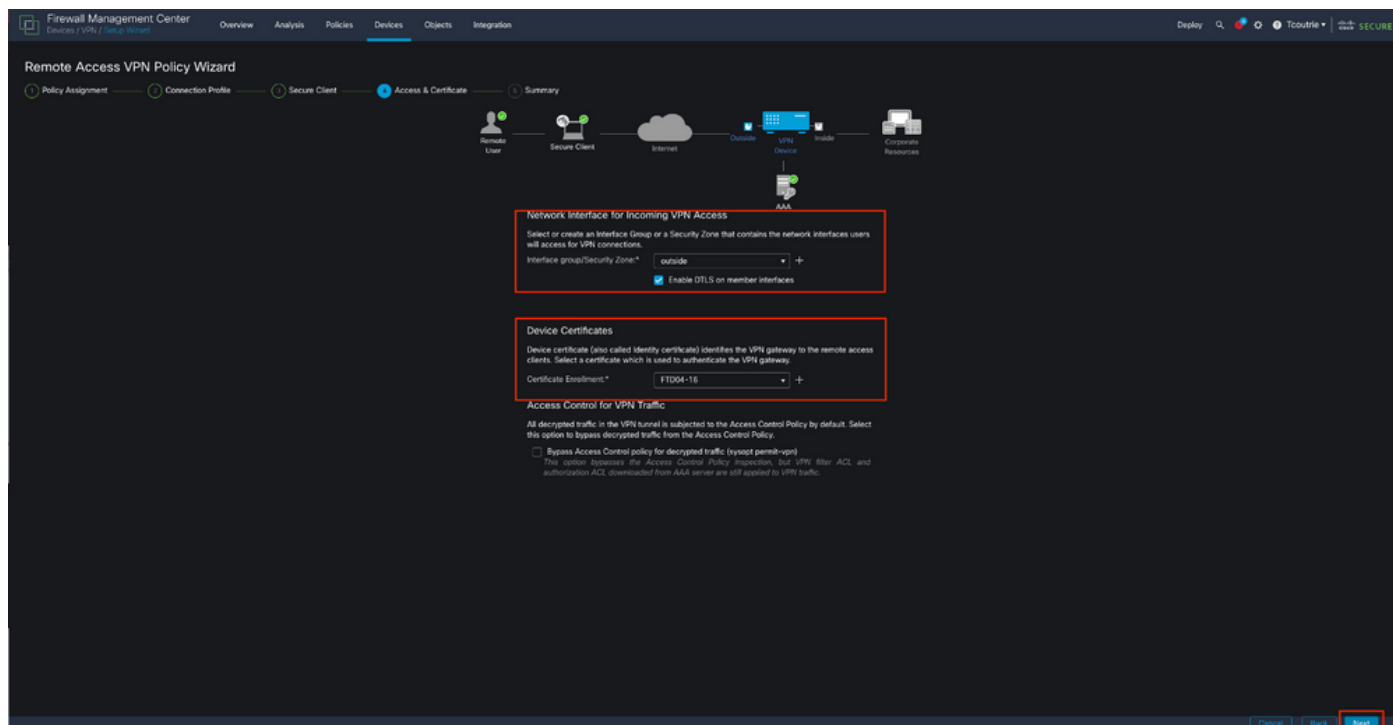
Cancel Back Next

ステップ3 RAVPNウィザード

ステップ4次のオブジェクトを設定します (図を参照)。完了したら、「Next」を選択します。

インターフェイスグループ/セキュリティゾーン：*:外部インターフェイス

「Certificate Enrollment:*」:このガイドの「FTDへのID証明書の展開」の部分で作成されたID証明書

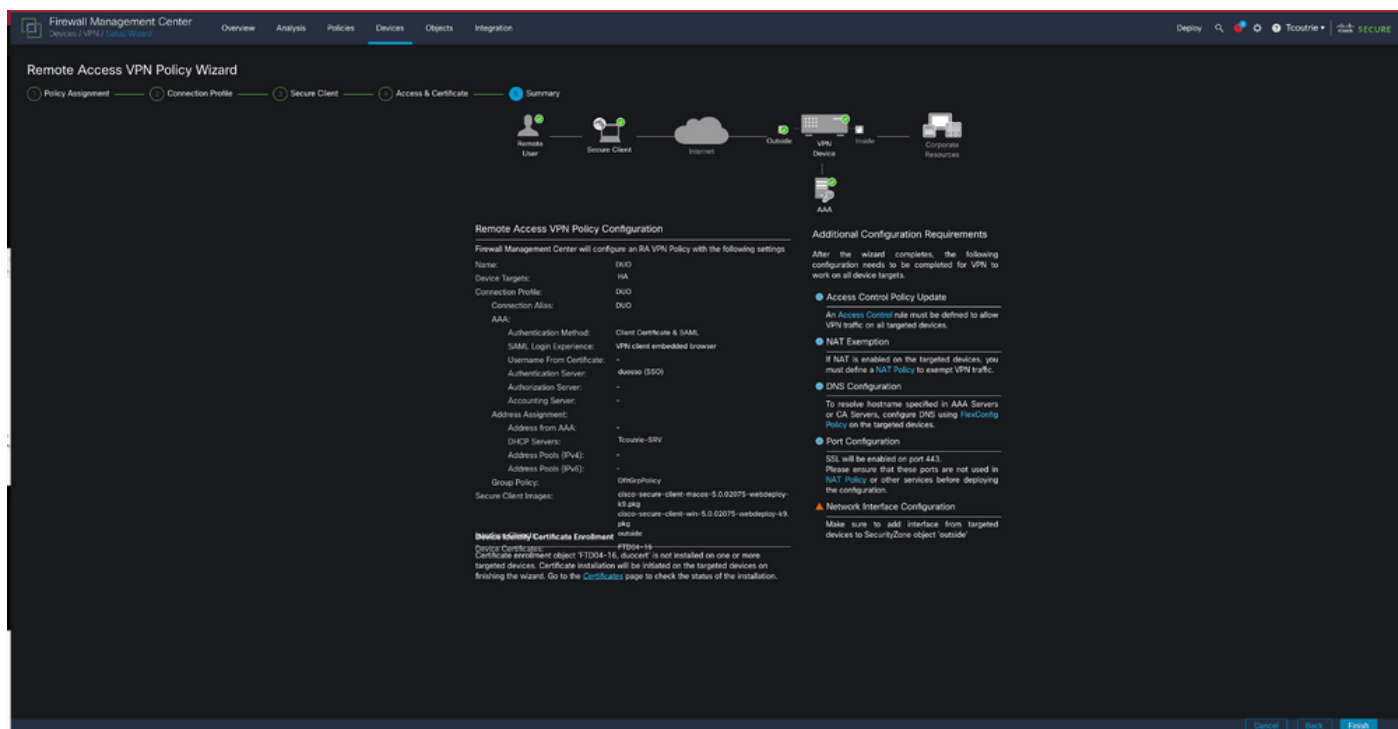


RAVPNウィザードのステップ4

 ヒント：まだ作成されていない場合は、「+」を選択して新しい証明書登録オブジェクトを追加します。

ステップ6要約

すべての情報を確認します。すべてが正しければ、「Finish」に進みます。



概要ページ

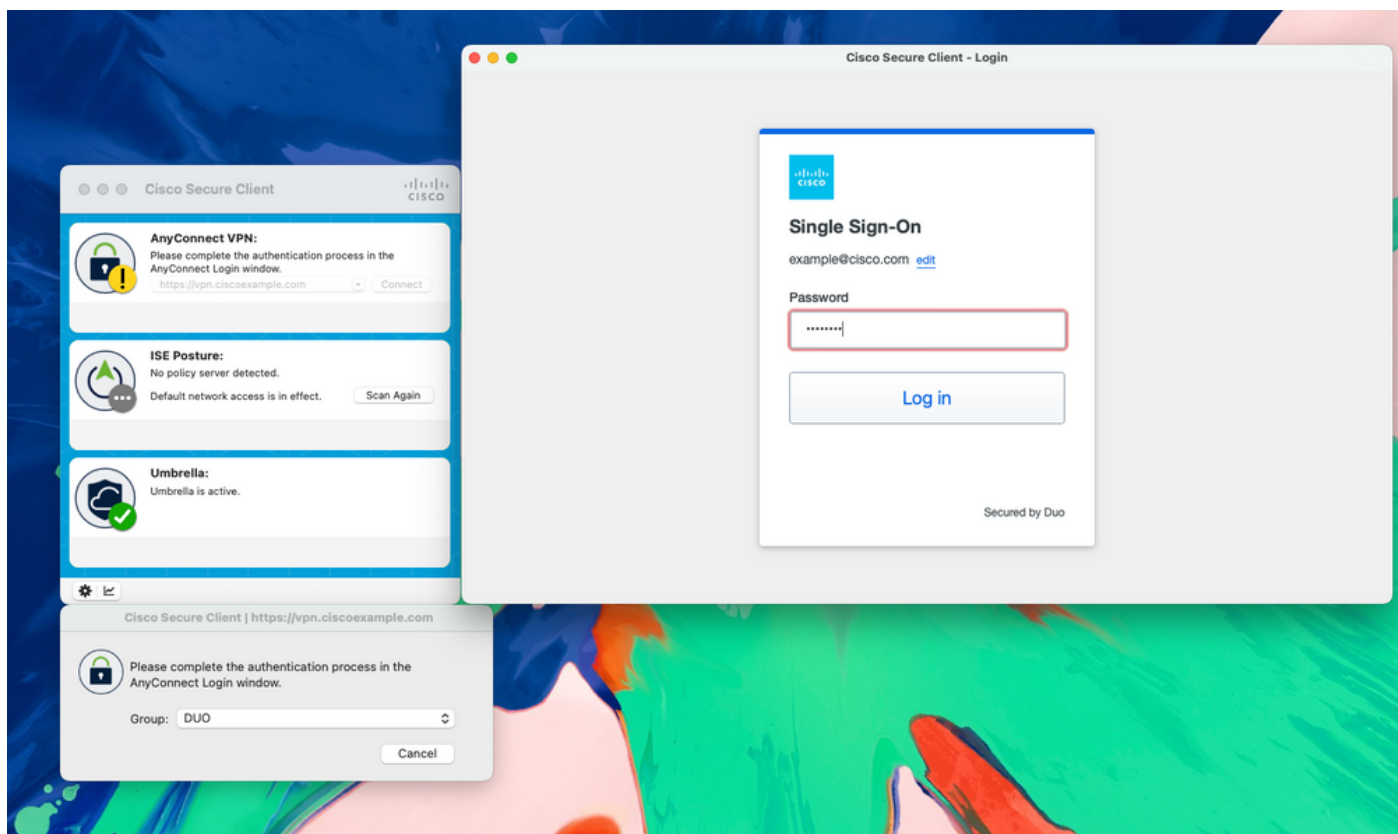
ステップ 7新しく追加した設定を展開します。

確認

この項では、接続が正常に試行されたかどうかを確認する方法について説明します。

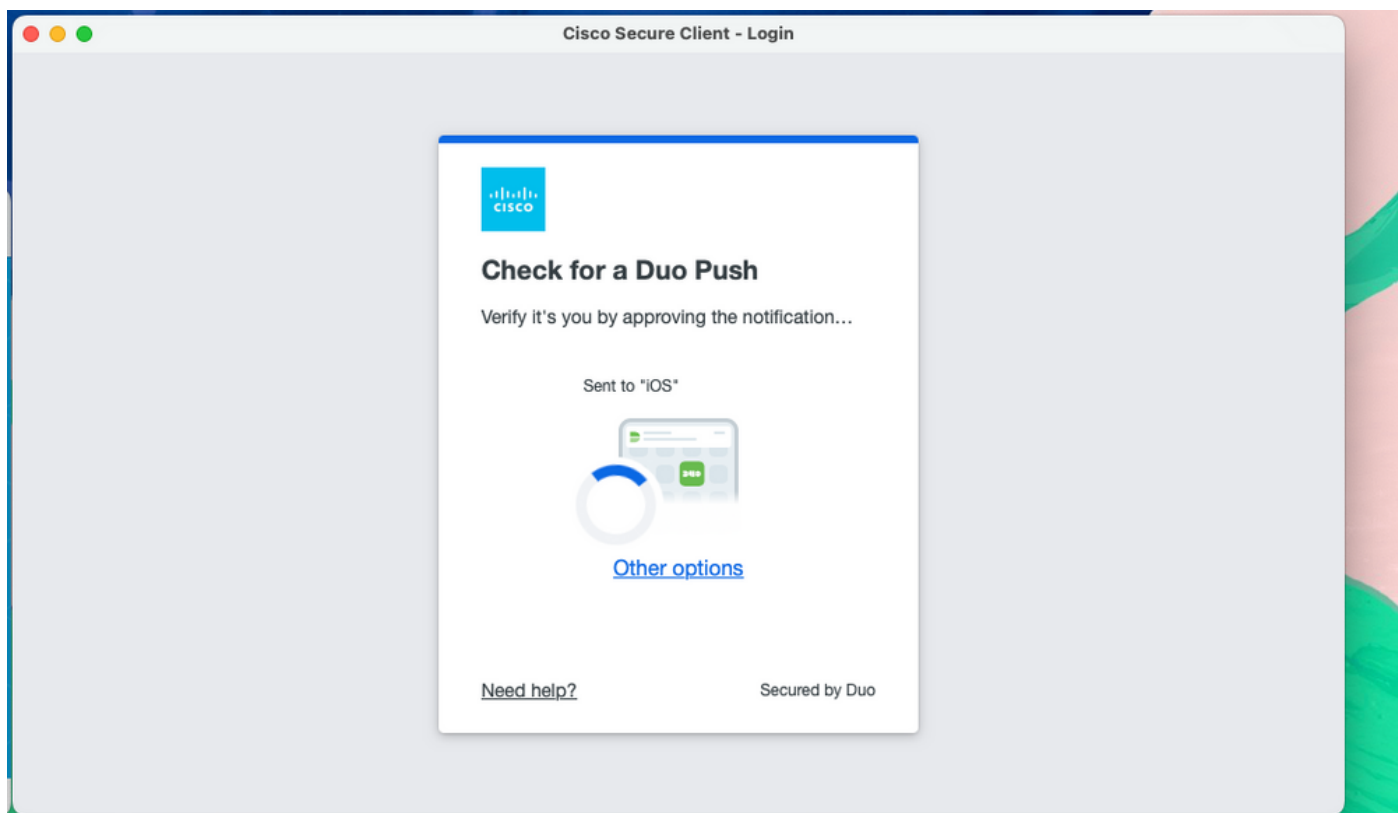
Cisco Secure Clientを開き、FTDのFQDNを入力して接続します。

SSOページでクレデンシャルを入力します。



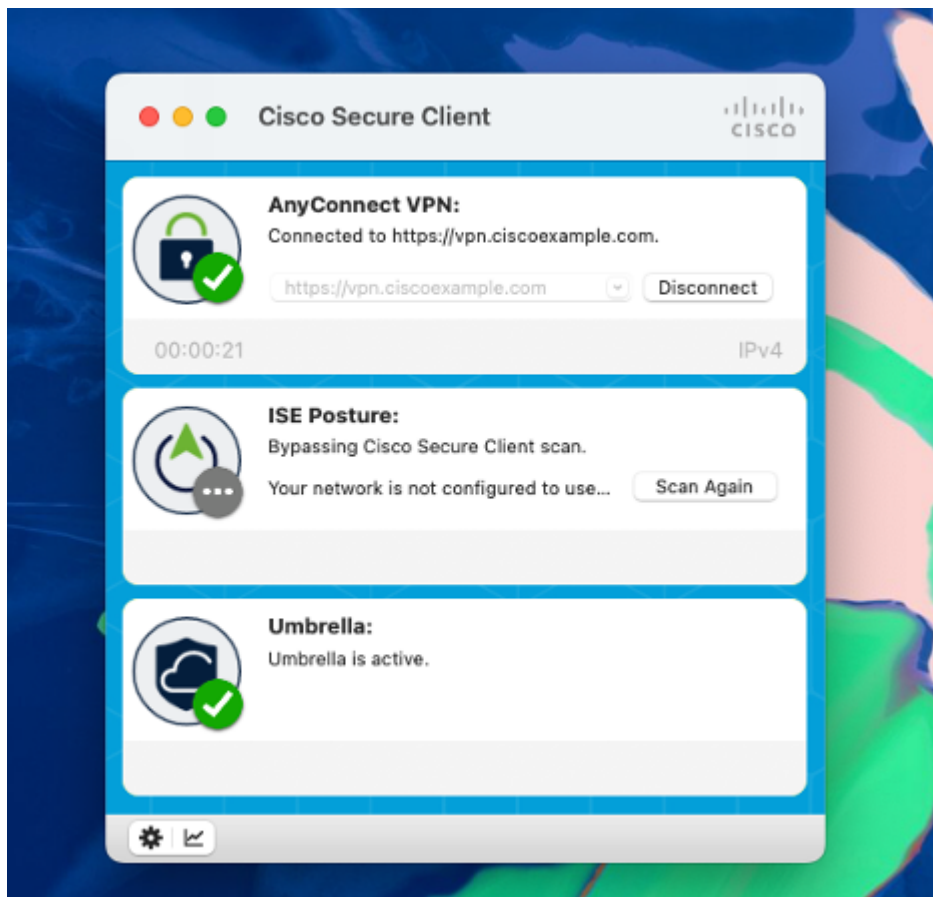
Cisco Secure Client経由のSSOページ

登録済みデバイスへのDUOプッシュを受け入れます。



DUOプッシュ

接続に成功しました。



FTDに接続

show vpn-sessiondb detail anyconnectコマンドを使用して、FTDの接続を確認します。

```

tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username      :                               Index      : 1916
Assigned IP   :                               Public IP    :
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx      : 390964                        Bytes Rx     : 124114
Pkts Tx       : 1216                          Pkts Rx      : 1223
Pkts Tx Drop  : 0                            Pkts Rx Drop : 0
Group Policy  :                               Tunnel Group :
Login Time    : 23:54:41 UTC Tue Jul 18 2023
Duration      : 0h:11m:28s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                          VLAN         : none
Audt Sess ID  : 0a7aa95d0077c00064b72641
Security Grp  : none                          Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID     : 1916.1
Public IP     :
Encryption    : none                        Hashing       : none
TCP Src Port  : 53859                       TCP Dst Port  : 443
Auth Mode     : Certificate and SAML
Idle Time Out: 30 Minutes                   Idle TO Left  : 18 Minutes
Client OS     : mac-intel

```

出力例から一部の情報が省略されています

トラブルシューティング

これらは、実装後に発生する可能性のある問題です。

問題1：証明書認証が失敗している。

ルート証明書がFTDにインストールされていることを確認します。

次のデバッグを使用します。

```
debug crypto ca 14
```

```
debug aaa shim 128
```

```
debug aaa common 128
```

問題2:SAMLの障害

トラブルシューティングのために、次のデバッグをイネーブルにできます。

```
debug aaa shim 128
```

debug aaa common 128

debug webvpn anyconnect 128

debug webvpn saml 255

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。