

Configurer le & Authentification par certificat Authentification DUO SAML

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration des étapes sur DUO](#)

[Créer une stratégie de protection des applications](#)

[Créer une stratégie d'application](#)

[Étapes de configuration de FMC](#)

[Déployer le certificat d'identité sur le FTD](#)

[Déployer le certificat IDP sur le FTD](#)

[Création de l'objet SSO SAML](#)

[Créer une configuration de réseau privé virtuel d'accès à distance \(RAVPN\)](#)

[Vérifier](#)

[Dépannage](#)

[Problème 1: Échec de l'authentification du certificat.](#)

[problème 2: Échecs SAML](#)

Introduction

Ce document décrit un exemple de mise en oeuvre de l'authentification basée sur certificat et de l'authentification SAML duo.

Conditions préalables

Les outils et périphériques utilisés dans le guide sont les suivants :

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Autorité de certification interne (CA)
- Compte Cisco DUO Premier
- Proxy d'authentification Cisco DUO
- Cisco Secure Client (CSC)

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN de base,
- SSL/TLS
- Infrastructure à clé publique
- Expérience avec FMC
- Client sécurisé Cisco
- Code FTD 7.2.0 ou supérieur
- Proxy d'authentification Cisco DUO

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTD (7.3.1)
- Cisco FMC (7.3.1)
- Client sécurisé Cisco (5.0.02075)
- Proxy d'authentification Cisco DUO (6.0.1)
- Mac OS (13.4.1)
- Active Directory

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration des étapes sur DUO

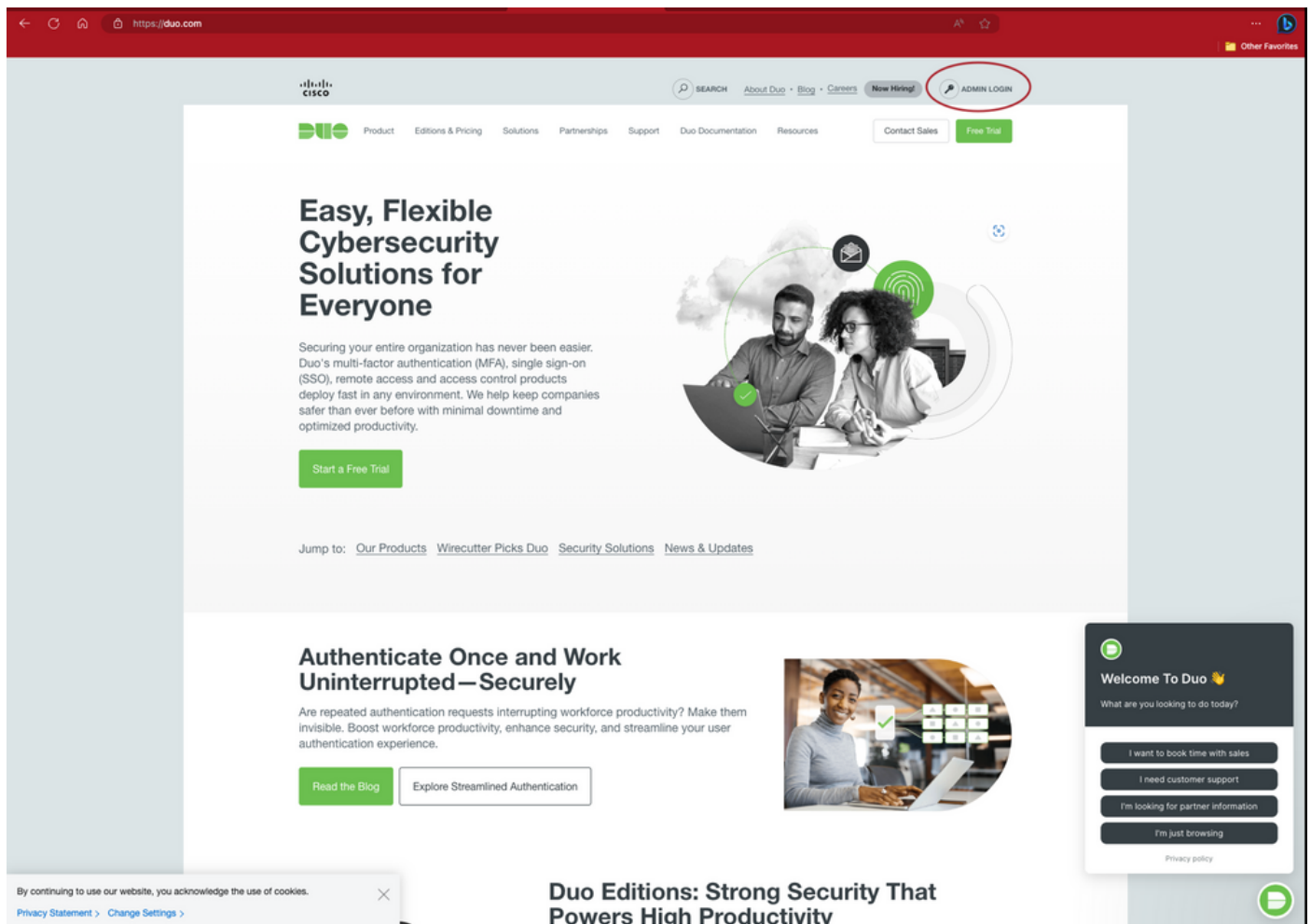
Cette section décrit les étapes de configuration de l'authentification unique (SSO) Cisco DUO. Avant de commencer, assurez-vous que le proxy d'authentification est implémenté.



Avertissement : Si un proxy d'authentification n'a pas été implémenté, ce lien dispose du guide pour cette tâche. [Guide du proxy d'authentification DUO](#)

Créer une stratégie de protection des applications

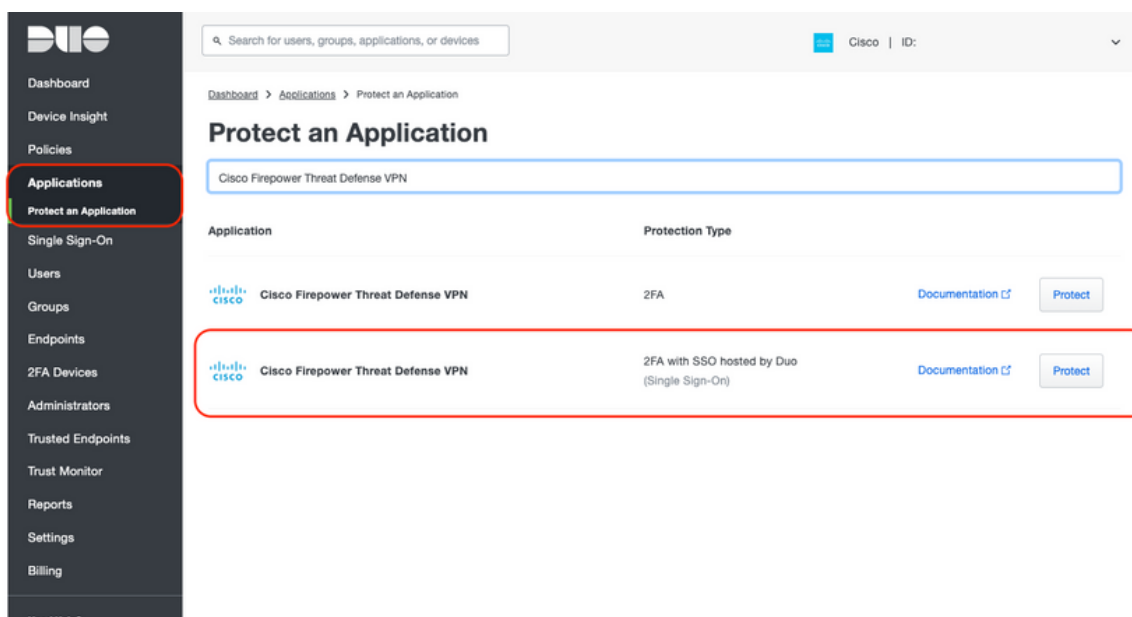
Étape 1. Connectez-vous au panneau d'administration via ce lien [Cisco Duo](#)



Page d'accueil Cisco DUO

Étape 2. Accédez à Tableau de bord > Applications > Protéger une application.

Dans la barre de recherche, saisissez « Cisco Firepower Threat Defense VPN » et sélectionnez « Protect ».



Protection d'une capture d'écran

Sélectionnez l'option avec uniquement le type de protection "2FA avec SSO hébergé par Duo".

Étape 3: Copiez ces informations d'URL sous Métadonnées.

- ID entité fournisseur d'identités
- URL SSO
- URL de déconnexion

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

Exemple d'informations à copier



Remarque : Les liens ont été omis de la capture d'écran.

Étape 4. Sélectionnez « Télécharger le certificat » pour télécharger le certificat du fournisseur d'identité sous Téléchargements.

Étape 5. Renseignez les informations relatives au fournisseur de services

URL de base Cisco Firepower : nom de domaine complet utilisé pour atteindre le FTD

Nom du profil de connexion- Nom du groupe de tunnels

Créer une stratégie d'application

Étape 1: Pour créer une stratégie d'application sous Stratégie, sélectionnez "Appliquer une stratégie à tous les utilisateurs", puis sélectionnez "Ou, créer une nouvelle stratégie" comme illustré dans l'image.

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

Exemple de création d'une stratégie d'application

Apply a Policy



Policy

Select a Policy



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

Apply Policy

Exemple de création d'une stratégie d'application

Étape 2. Sous Policy name, saisissez le nom souhaité, sélectionnez "Authentication policy" sous Users, et sélectionnez "Appliquer 2FA." Ensuite, enregistrez avec "Créer une stratégie".

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

Exemple de création d'une stratégie d'application

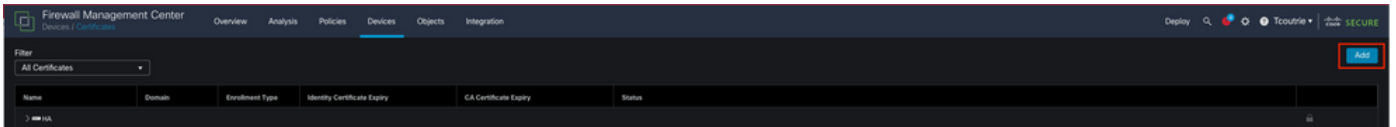
Étape 3. Appliquez la stratégie en cliquant sur « Appliquer la stratégie » dans la fenêtre suivante. puis faites défiler jusqu'en bas de la page et sélectionnez "Enregistrer" pour terminer les configurations DUO

Étapes de configuration de FMC

Déployer le certificat d'identité sur le FTD

Cette section décrit la configuration et le déploiement du certificat d'identité sur le FTD requis pour l'authentification de certificat. Avant de commencer, assurez-vous de déployer toutes les configurations.

Étape 1. Accédez à Périphériques > Certificat et choisissez Ajouter, comme illustré dans l'image.



Capture d'écran des périphériques/certificats

Étape 2: Sélectionnez le dispositif FTD dans la liste déroulante des périphériques. Cliquez sur l'icône + pour ajouter une nouvelle méthode d'inscription de certificat.

A screenshot of the 'Add New Certificate' dialog box. The title 'Add New Certificate' is at the top. Below it, a message states: '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. A red box highlights a '+' button to the right of the 'Cert Enrollment*' dropdown. At the bottom right, there are 'Cancel' and 'Add' buttons.

Capture d'écran Ajouter un nouveau certificat

Étape 3 : choisissez l'option qui est la méthode préférée pour obtenir des certificats dans l'environnement via le "Type d'inscription", comme indiqué dans l'image.

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

Capture d'écran de la nouvelle page d'inscription



Conseil : Les options disponibles sont les suivantes : Certificat auto-signé - Générez un nouveau certificat localement, SCEP - Utilisez le protocole d'inscription de certificat simple pour obtenir un certificat auprès d'une autorité de certification, Manuel - Installez manuellement le certificat racine et le certificat d'identité, PKCS12 - Téléchargez le lot de

certificats chiffrés avec la racine, l'identité et la clé privée.

Déployer le certificat IDP sur le FTD

Cette section décrit la configuration et le déploiement du certificat IDP sur le FTD. Avant de commencer, assurez-vous de déployer toutes les configurations.

Étape 1: Accédez à Devices > Certificate et choisissez Add."

Étape 2: Sélectionnez le dispositif FTD dans la liste déroulante des périphériques. Cliquez sur l'icône + pour ajouter une nouvelle méthode d'inscription de certificat.

Étape 3 : Dans la fenêtre d'ajout d'inscription de certificat, saisissez les informations requises comme indiqué dans l'image, puis "Enregistrer" comme indiqué dans l'image.

- Name : Nom de l'objet
- Type d'inscription : Manuel
- Case à cocher activée : CA uniquement
- Certificat CA : Format Pem du certificat

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

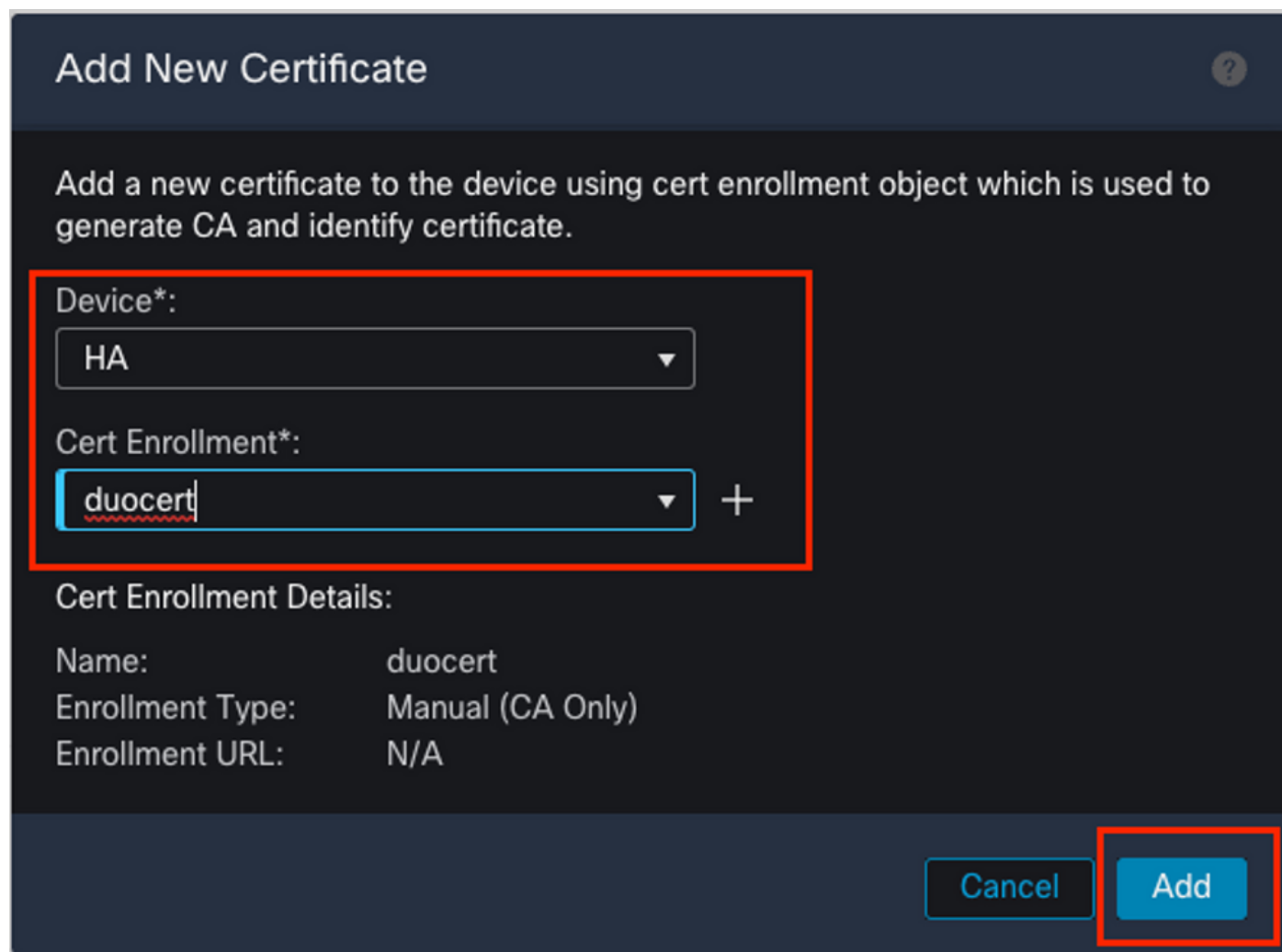
Save

Exemple de création d'un objet d'inscription de certificat



Mise en garde : L'indicateur « Ignorer la vérification de l'autorité de certification dans les contraintes de base du certificat d'autorité de certification » peut être utilisé si nécessaire. Utilisez cette option avec prudence.

Étape 4: Sélectionnez l'objet d'inscription de certificat nouvellement créé sous "Inscription de certificat:" puis sélectionnez "Ajouter" comme indiqué dans l'image.



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

Capture d'écran de l'objet et du périphérique d'inscription

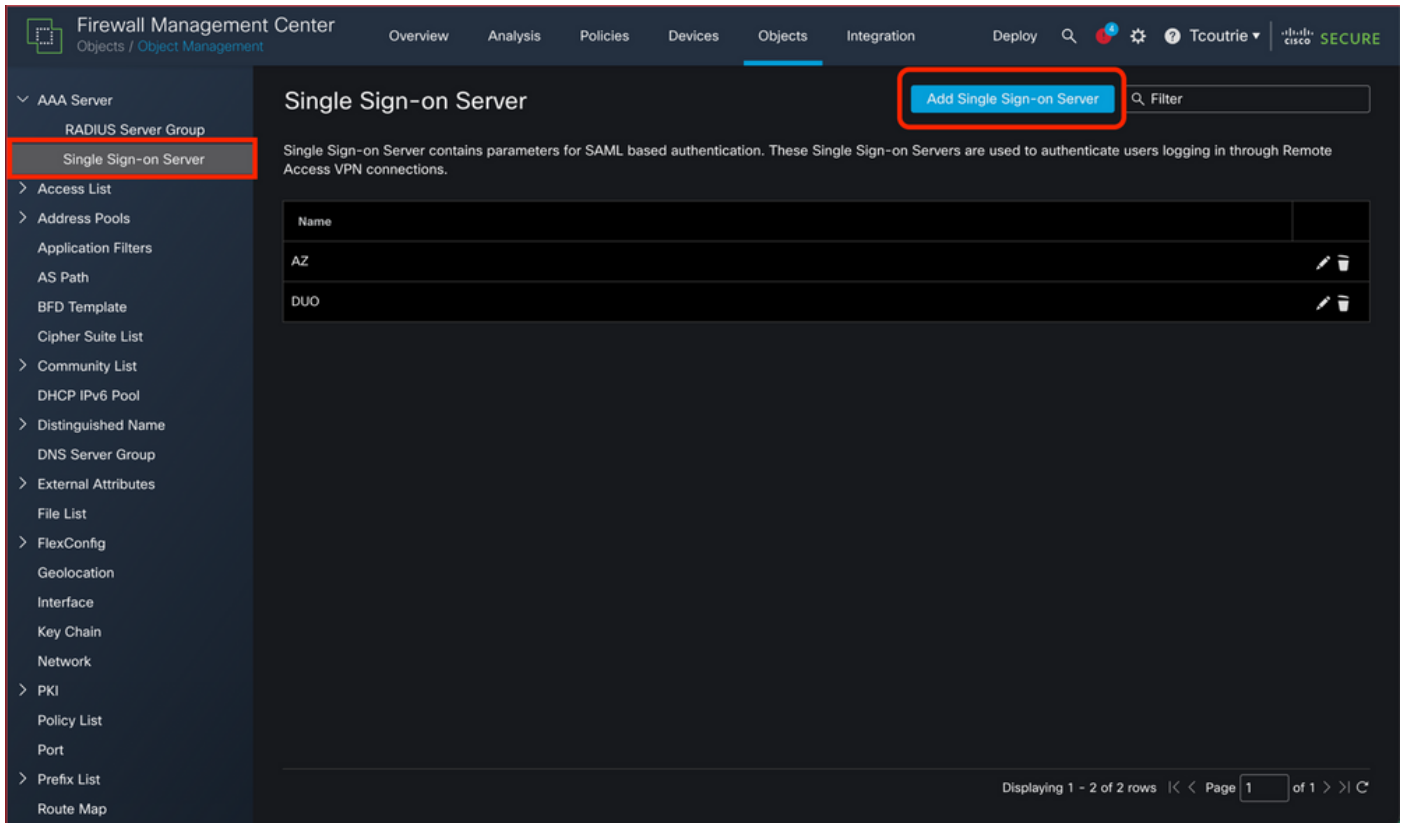


Remarque : Une fois ajouté, le certificat déploie immédiatement.

Création de l'objet SSO SAML

Cette section décrit les étapes de configuration de l'authentification unique SAML via FMC. Avant de commencer, assurez-vous de déployer toutes les configurations.

Étape 1. Accédez à Objects > AAA Server > Single Sign-on Server et sélectionnez "Add Single Sign-on Server".



exemple de création d'un objet SSO

Étape 2. Entrez les informations requises à partir de « Créer une stratégie de protection des applications »

". Pour continuer une fois terminé, sélectionnez "Enregistrer".

- Nom* : Nom de l'objet
- ID d'entité du fournisseur d'identités* : ID d'entité de l'étape 3
- URL SSO* : URL de connexion copiée à partir de l'étape 3
- URL de déconnexion : URL de déconnexion copiée à partir de l'étape 3
- URL de base : Utilisez le même nom de domaine complet que « URL de base Cisco Firepower » à l'étape 5
- Certificat du fournisseur d'identité* : Certificat IDP déployé
- Certificat du fournisseur de services : Certificat sur l'interface externe du FTD

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

Exemple de nouvel objet SSO.



Remarque : Les liens ID d'entité, URL SSO et URL de déconnexion ont été omis de la

Créer une configuration de réseau privé virtuel d'accès à distance (RAVPN)

Cette section décrit les étapes à suivre pour configurer RAVPN à l'aide de l'assistant.

Étape 1. Accédez à Périphériques > Accès à distance Sélectionnez "Ajouter".

Étape 2. Dans l'assistant, entrez le nom du nouvel assistant de stratégie RAVPN, sélectionnez SSL sous VPN Protocols : Add the Targeted Devices, comme indiqué dans l'image. Sélectionnez "Next" une fois terminé.

The screenshot shows the 'Remote Access VPN Policy Wizard' with the 'Access & Certificate' step selected. The 'Targeted Devices and Protocols' section contains the following fields and options:

- Name:** A text field containing 'DLO'.
- Description:** An empty text field.
- VPN Protocols:** A section with two radio buttons: 'SSL' (selected) and 'IPsec-IKEv2'.
- Targeted Devices:** A section with two columns: 'Available Devices' and 'Selected Devices'. In 'Available Devices', 'HA' is selected. In 'Selected Devices', 'HA' is listed.

On the right side, there is a 'Before You Start' section with instructions for configuration. At the bottom right, there are 'Cancel', 'Back', and 'Next' buttons, with 'Next' being highlighted.

Étape 1 de l'assistant RAVPN

Étape 2. Pour le profil de connexion, définissez les options (indiquées ici) : Sélectionnez "Suivant" une fois terminé.

- Nom du profil de connexion : Utilisez le nom du groupe de tunnels à l'étape 5 de "Créer une stratégie de protection d'application".

Authentification, autorisation et comptabilité (AAA) :

- Méthode d'authentification : Certificat client et SAML
- Authentication Server : * sélectionnez l'objet SSO créé lors de la création de l'objet SSO SAML.

Affectation d'adresses client :

- Utiliser le serveur AAA (domaine ou RADIUS uniquement) - Radius ou LDAP
- Utiliser les serveurs DHCP - Serveur DHCP

- Utiliser les pools d'adresses IP - Pool local sur le FTD

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy Tcoutrie

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 DHCP Servers:

☐ Use IP Address Pools

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:

[Edit Group Policy](#)

Cancel Back **Next**

Étape 2 de l'assistant RAVPN



Conseil : Pour ces travaux pratiques, un serveur DHCP est utilisé.

Étape 3. Sélectionnez le « + » pour télécharger une image Web du client sécurisé Cisco à déployer. Cochez ensuite la case de l'image CSC à déployer. Comme l'illustre l'image. Sélectionnez "Suivant" une fois terminé.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy Tcoutrie

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-...	cisco-secure-client-macos-5.0.02075-...	Mac OS
☒ cisco-secure-client-win-5.0.02075-...	cisco-secure-client-win-5.0.02075-...	Windows

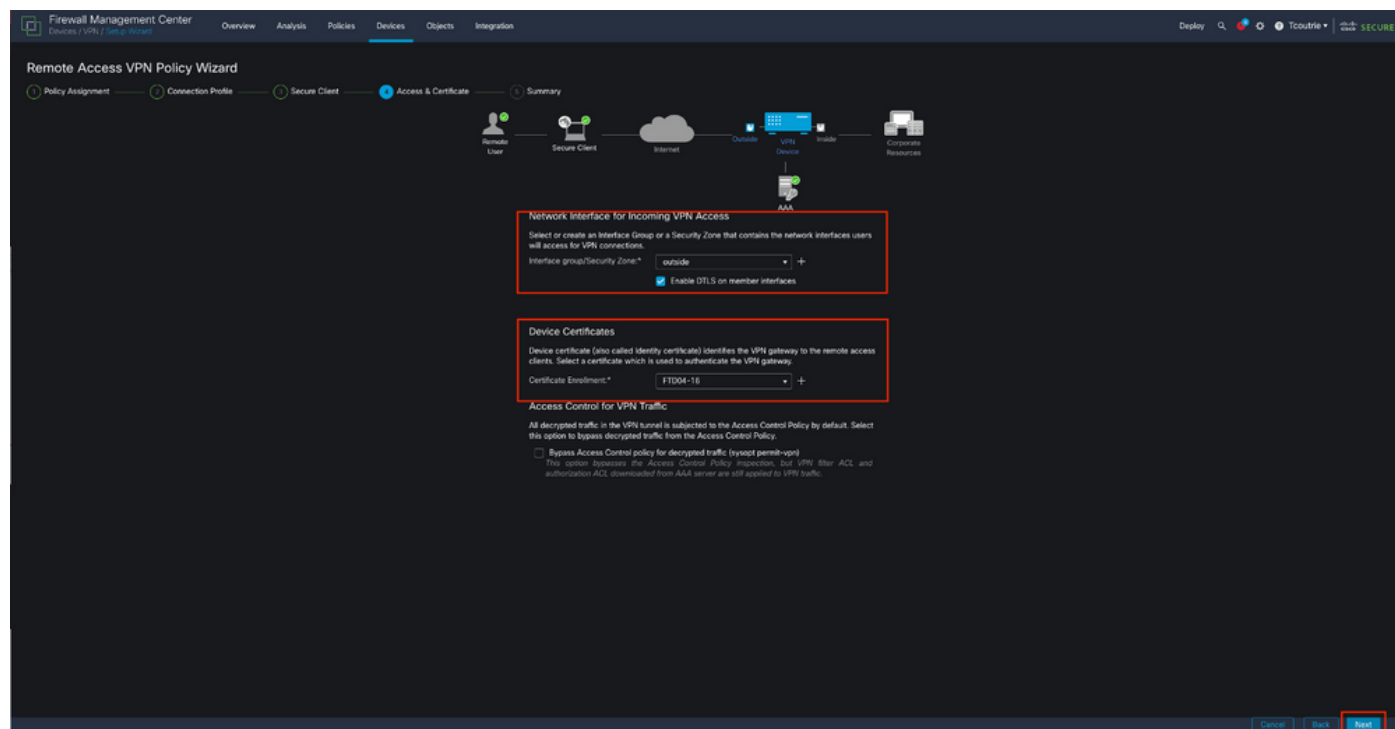
Cancel Back **Next**

Étape 3 Assistant RAVPN

Étape 4. Définir ces objets (comme on le voit dans l'image) : Sélectionnez "Suivant" une fois terminé.

Groupe d'interfaces/Zone de sécurité : * : Interface externe

"Inscription de certificat : *" : Certificat d'identité créé pendant la partie « Déployer le certificat d'identité sur le FTD » de ce guide



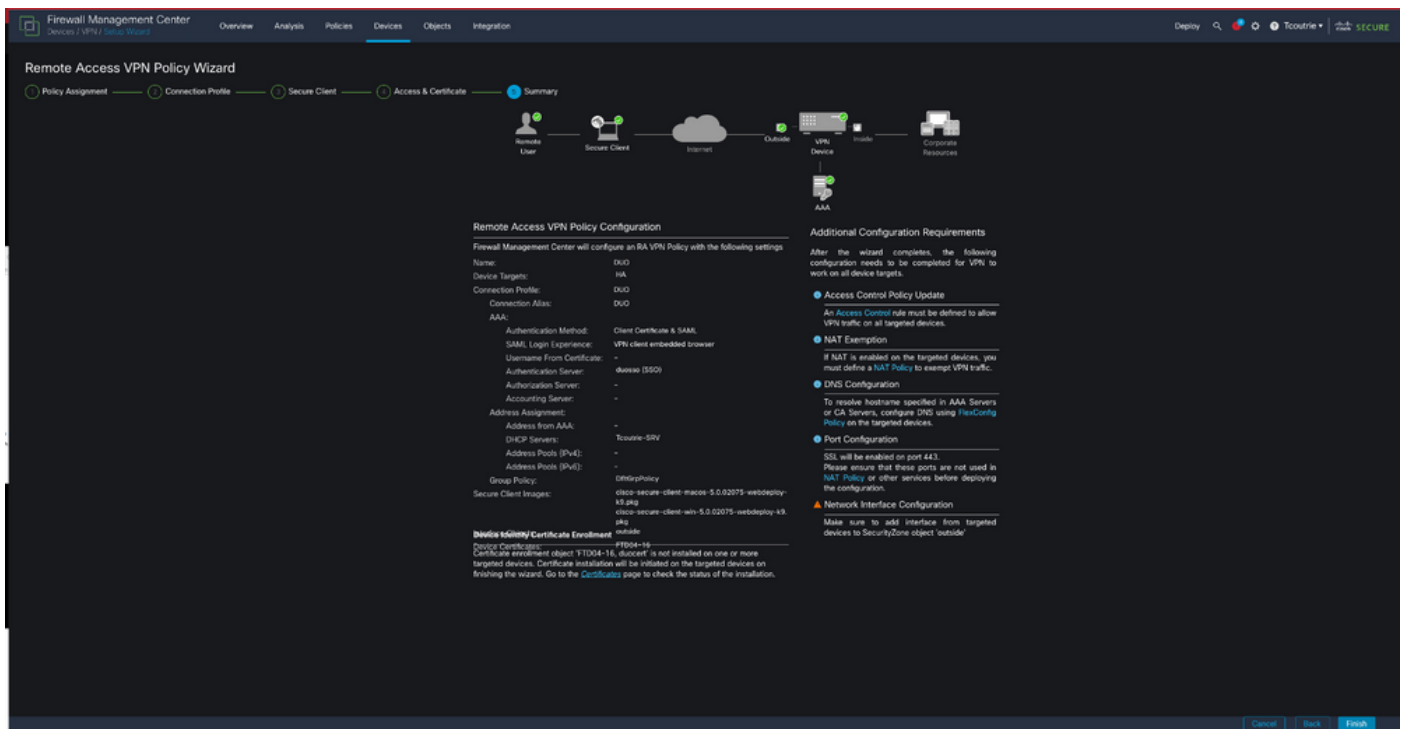
Étape 4 de l'assistant RAVPN



Conseil : Si ce n'est pas le cas, ajoutez un nouvel objet d'inscription de certificat en sélectionnant le « + ».

Étape 6. Résumé

Vérifiez toutes les informations. Si tout est correct, passez à l'étape 'Terminer'.



Page Résumé

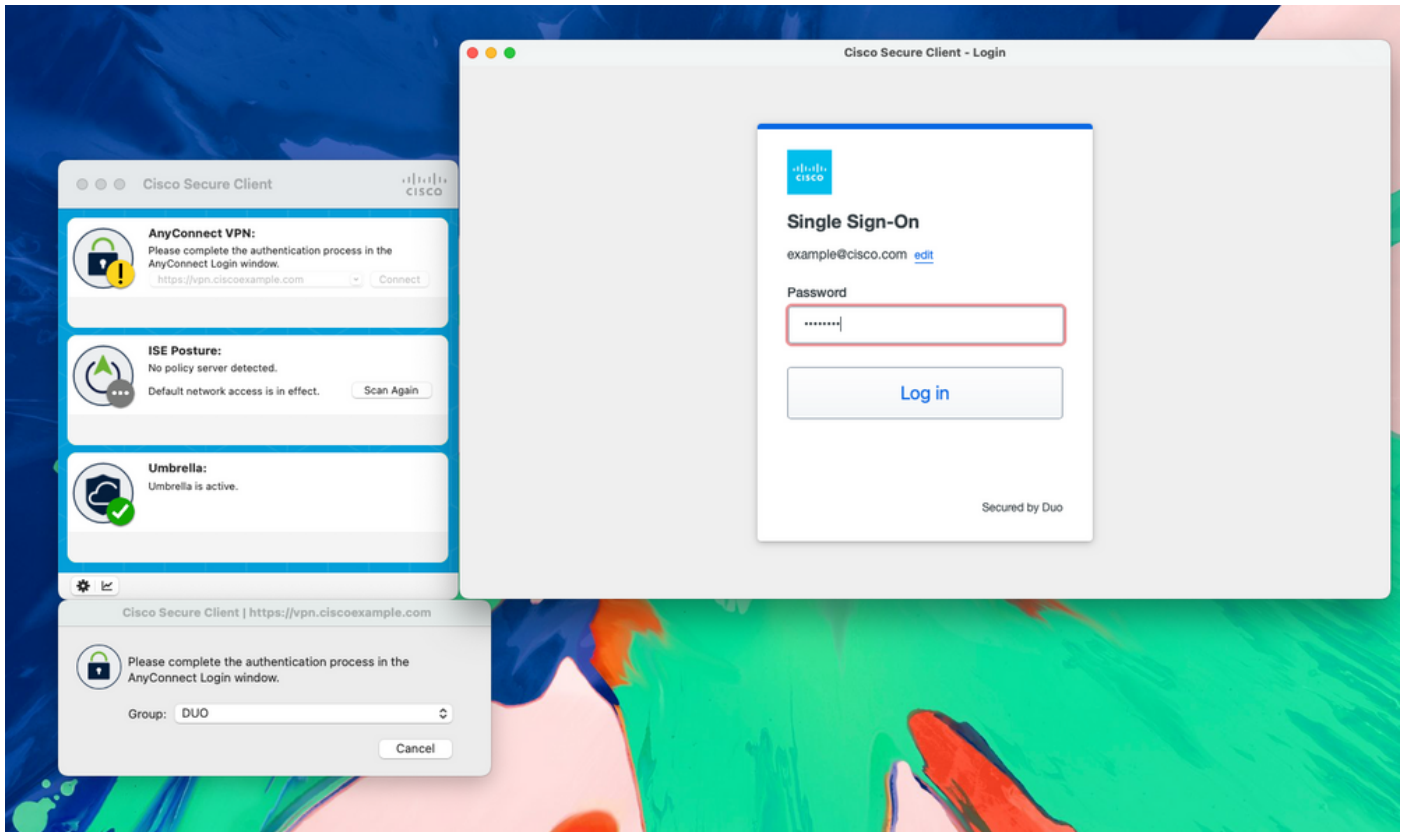
Étape 7. Déployez les configurations nouvellement ajoutées.

Vérifier

Cette section décrit la vérification d'une tentative de connexion réussie.

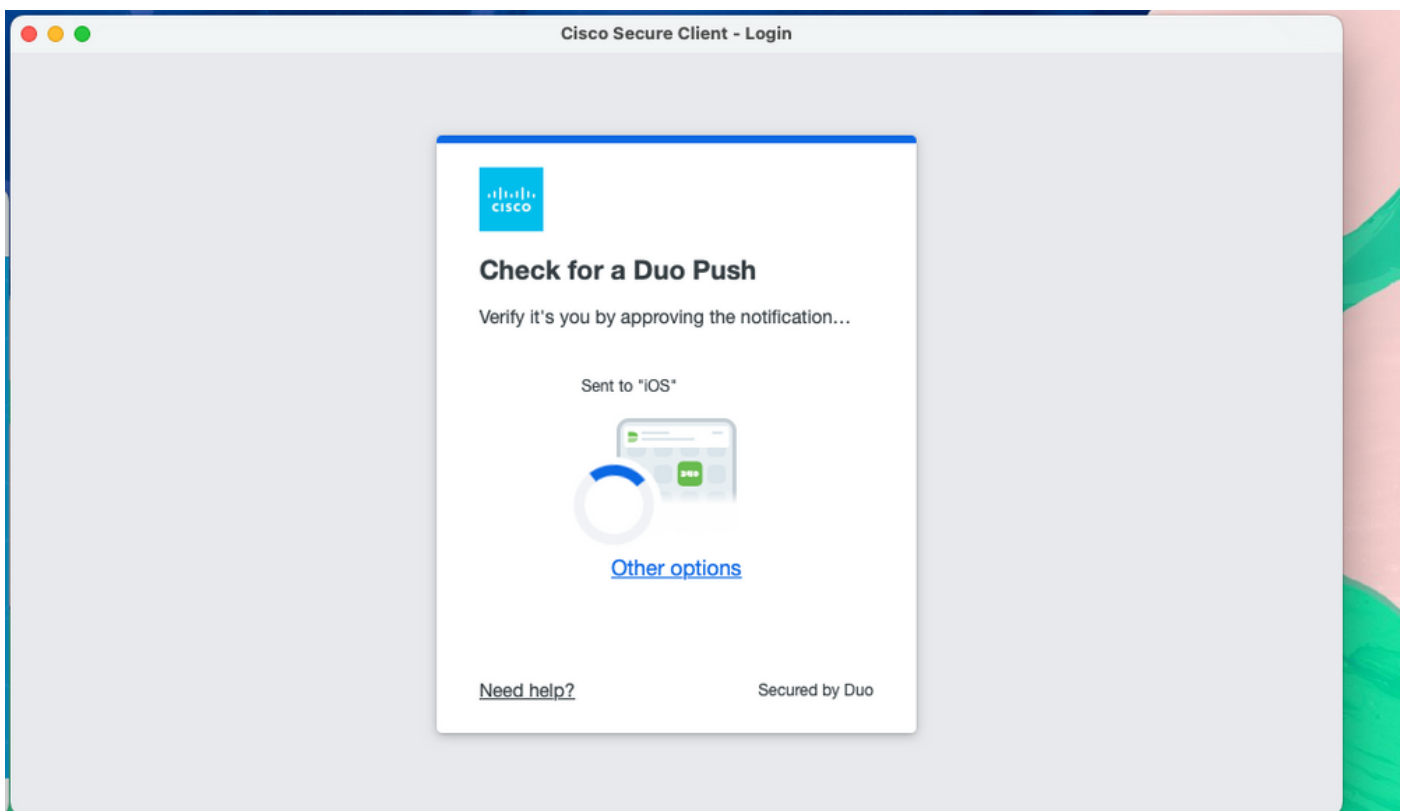
Ouvrez Cisco Secure Client, saisissez le nom de domaine complet du FTD et connectez-vous.

Saisissez les informations d'identification sur la page SSO.



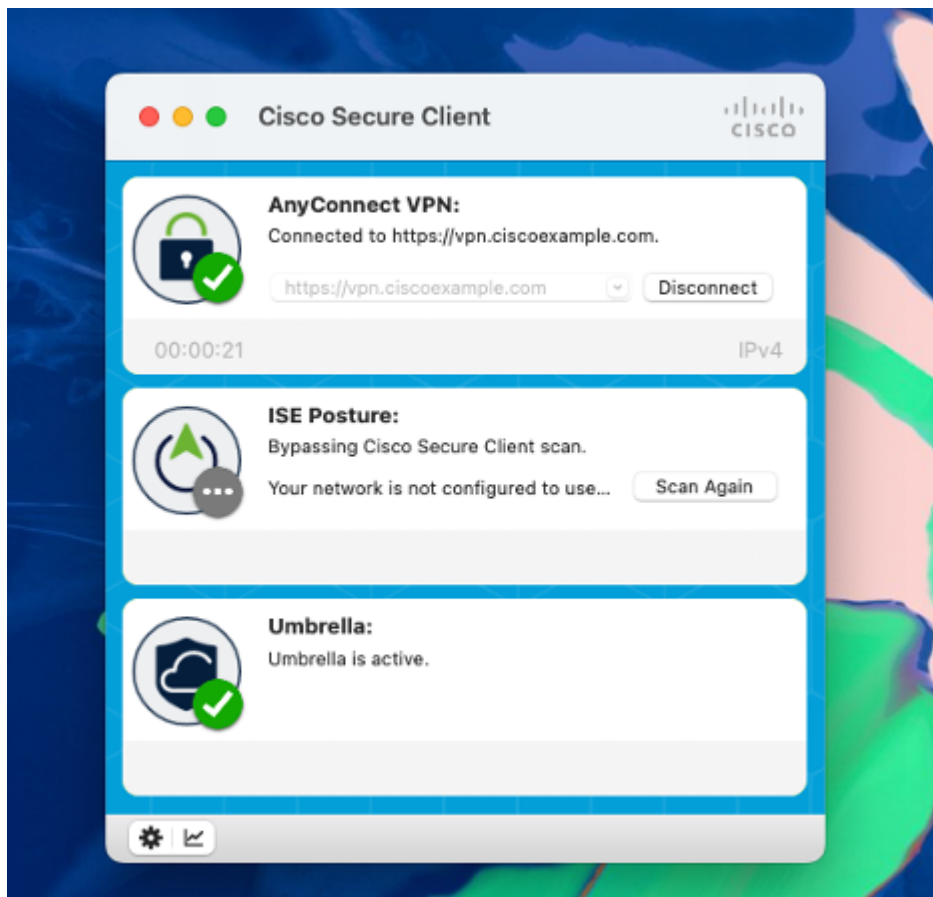
Page SSO via Cisco Secure Client

Acceptez la transmission DUO vers le périphérique enregistré.



push DUO

Connexion réussie.



Connecté à FTD

Vérifiez la connexion sur le FTD à l'aide de la commande : `show vpn-sessiondb detail anyconnect`

```

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

```

Certaines informations ont été omises dans l'exemple de sortie

Dépannage

Il s'agit de problèmes potentiels qui surviennent après la mise en oeuvre.

Problème 1: Échec de l'authentification du certificat.

Assurez-vous que le certificat racine est installé sur le FTD ;

utilisez ces débogages :

debug crypto ca 14

debug aaa shim 128

debug aaa common 128

problème 2: Échecs SAML

Ces débogages peuvent être activés pour le dépannage :

debug aaa shim 128

debug aaa common 128

debug webvpn anyconnect 128

debug webvpn saml 255

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.