Configurer le & Authentification par certificat Authentification DUO SAML

Table des matières

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.

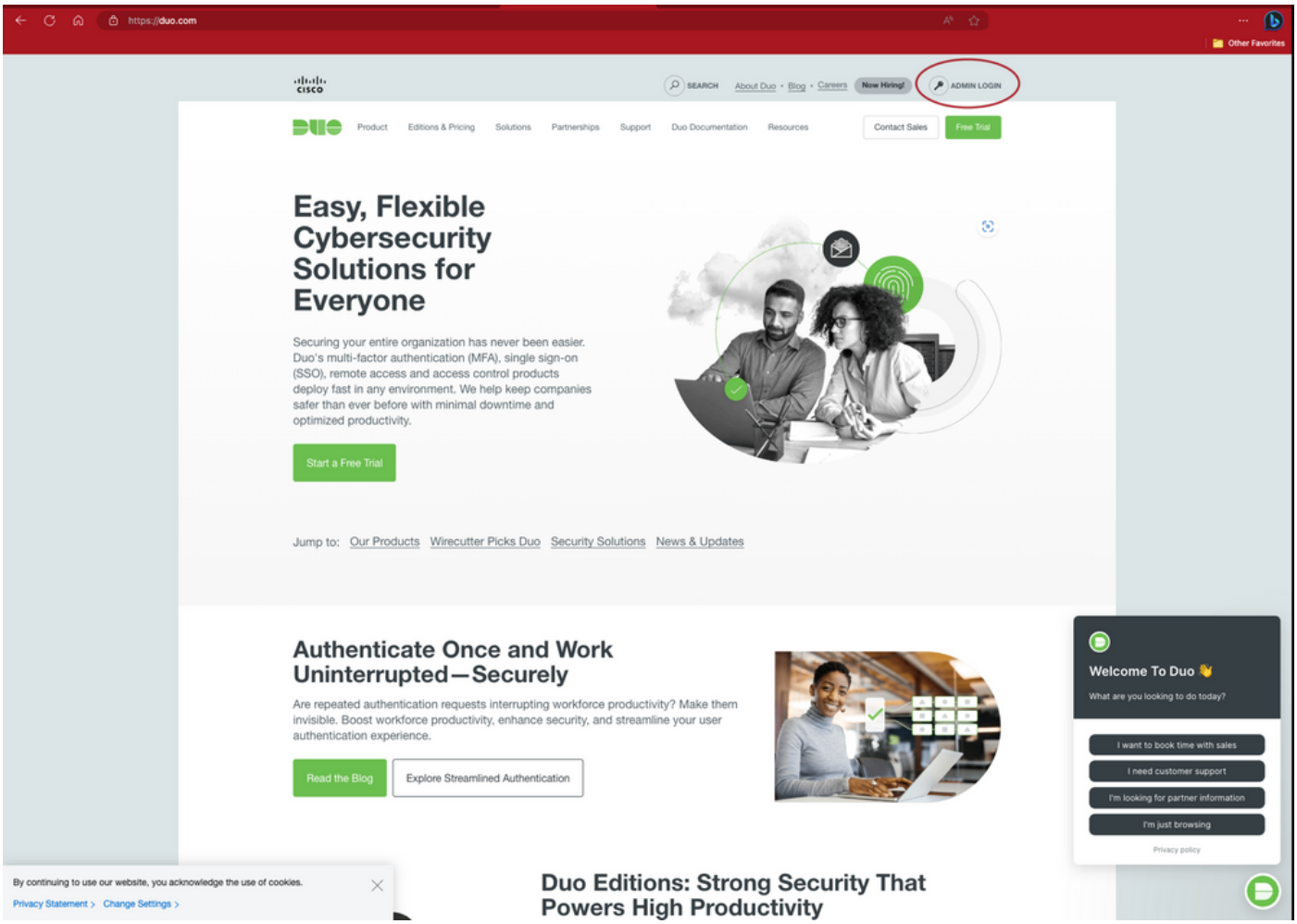
Configuration des étapes sur DUO

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

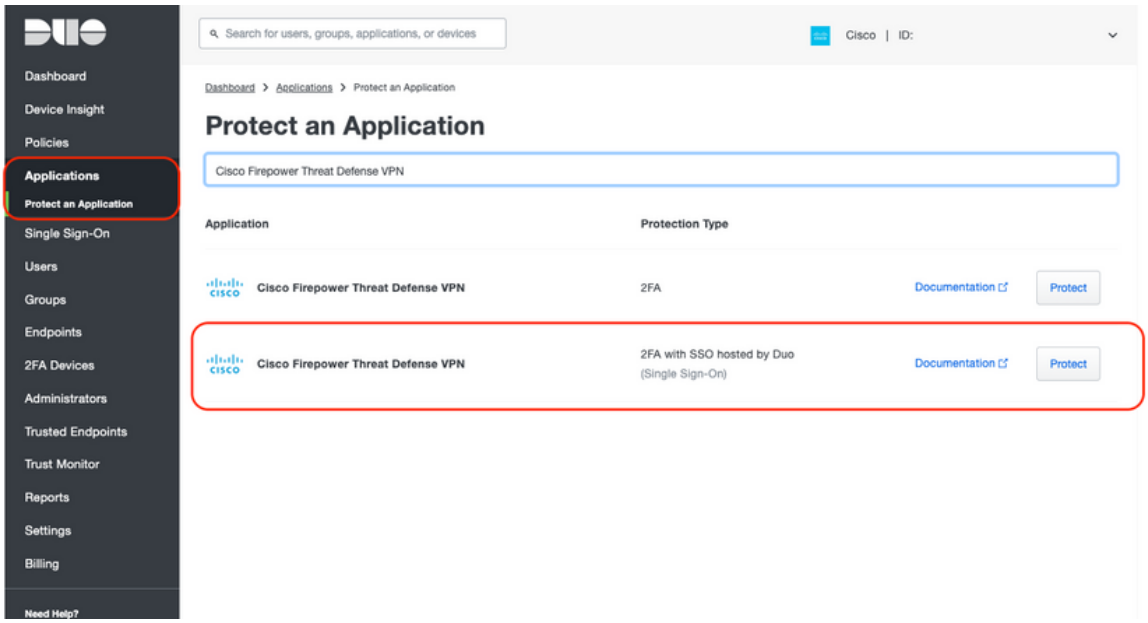
Étape 1. Connectez-vous au panneau d’administration via ce lien Cisco Duo



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

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.

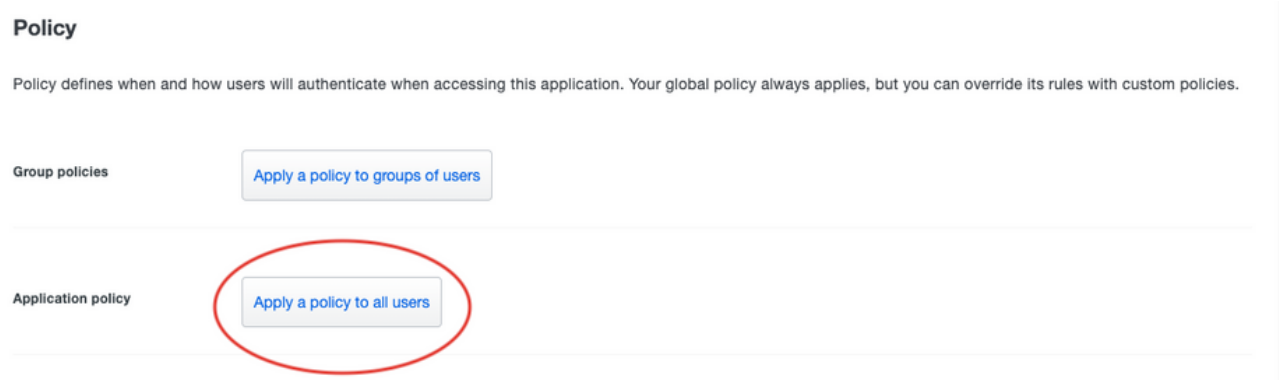
Étape 5. Renseignez les informations relatives au fournisseur de services

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

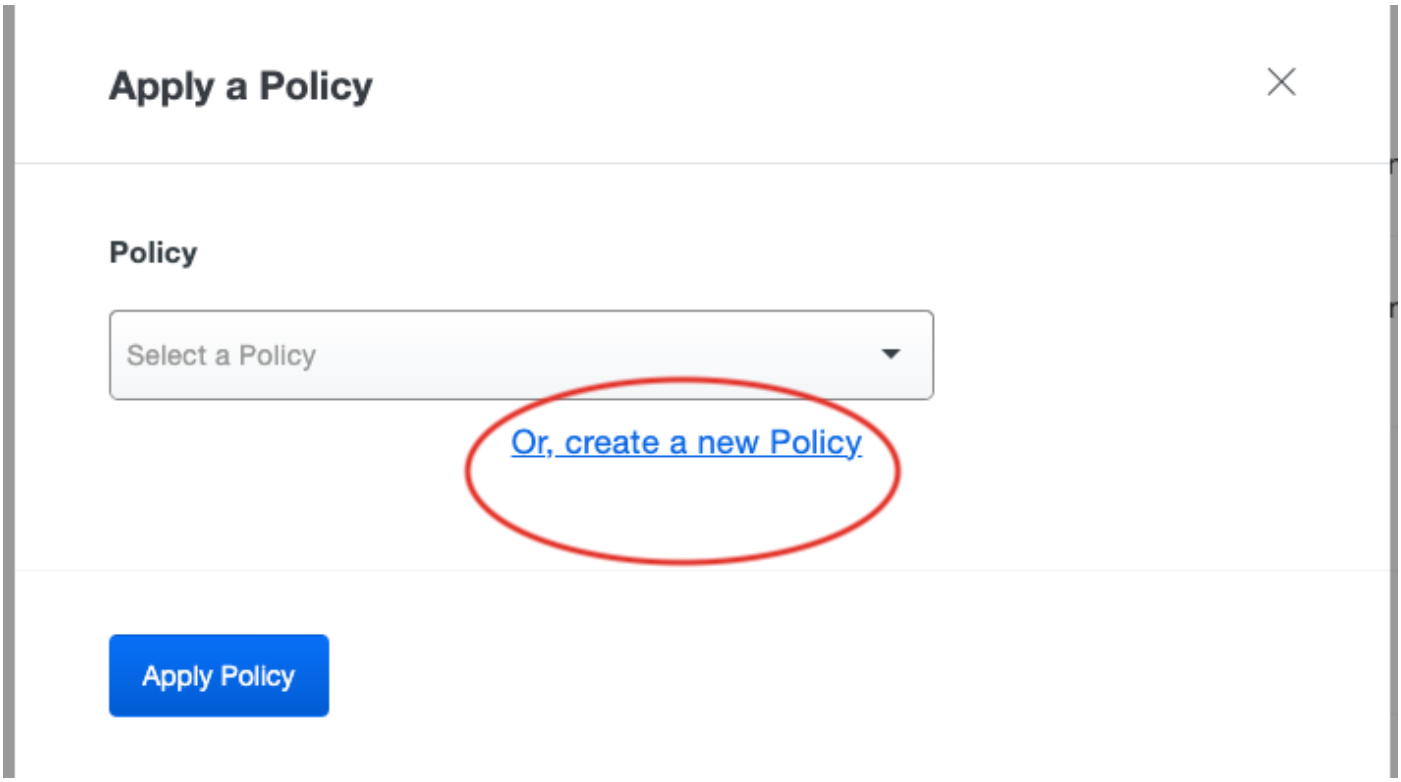
Nom du profil de connexion- Nom du groupe de tunnels

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.

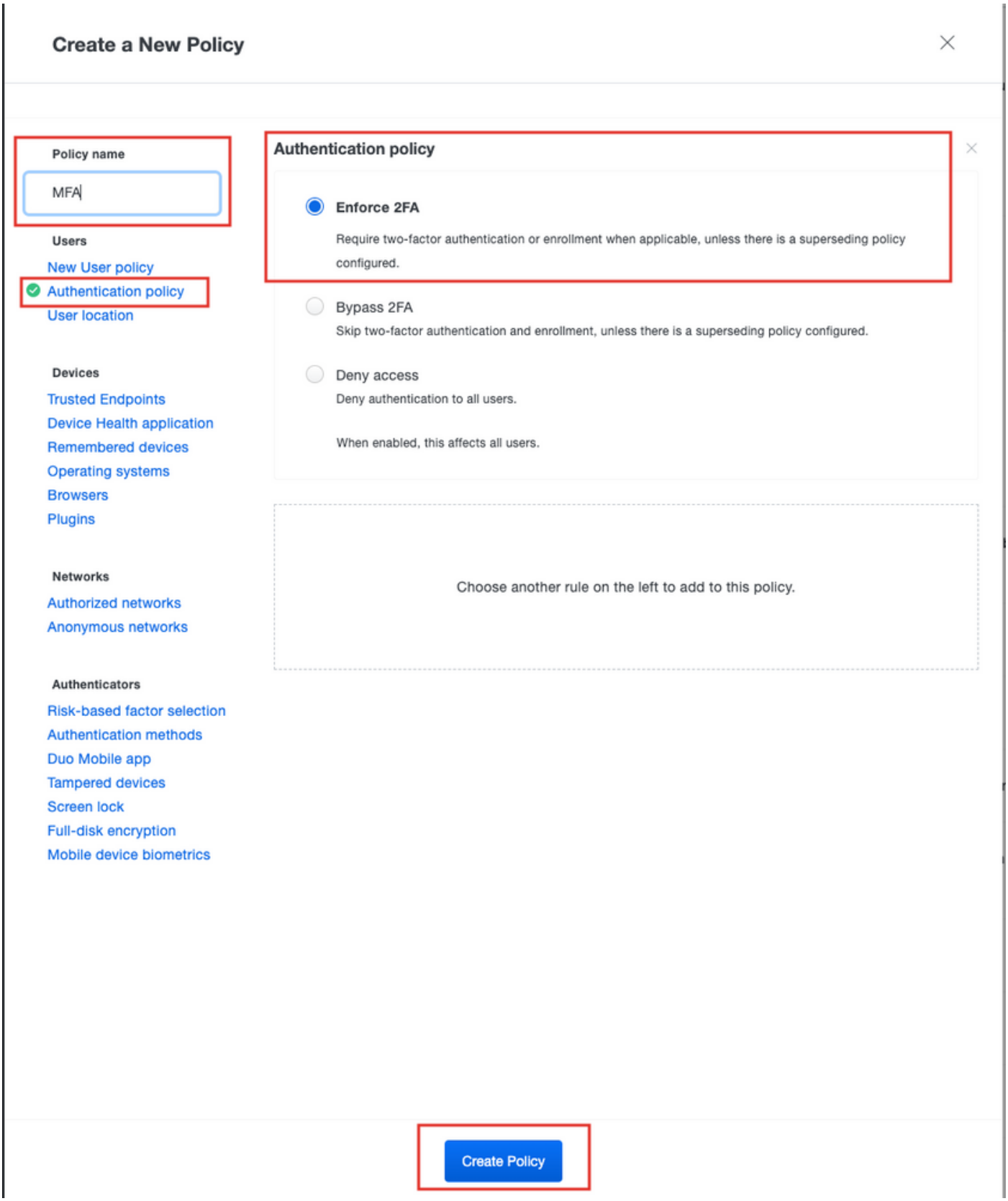


Exemple de création d'une stratégie d'application



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".



Exemple de création d'une stratégie d'application

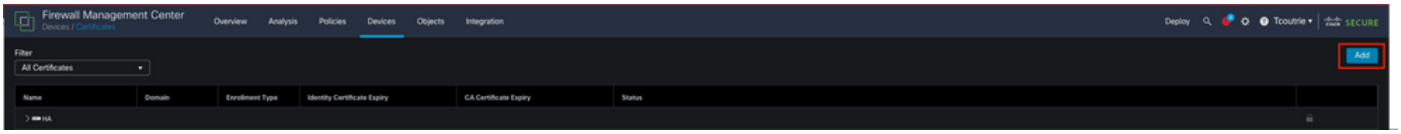
Étape 3. Appliquez la stratégie en cliquant sur « Appliquer la stratégie » dans la fenêtre suivante. puis faites défiler jusqu'en bas de la page et sélectionnez "Enregistrer" pour terminer les configurations DUO

Étapes de configuration de FMC

Déployer le certificat d'identité sur le FTD

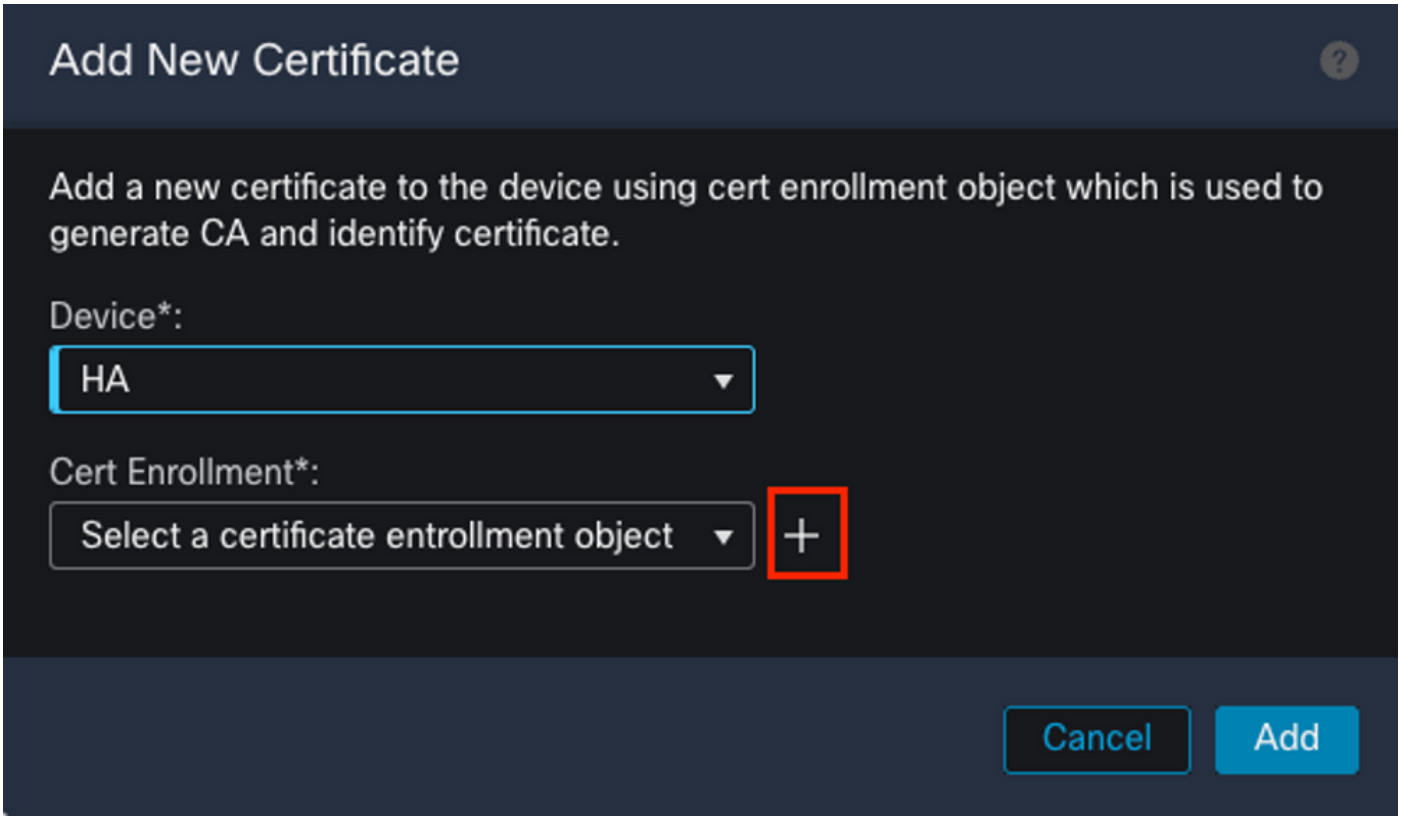
Cette section décrit la configuration et le déploiement du certificat d'identité sur le FTD requis pour l'authentification de certificat. Avant de commencer, assurez-vous de déployer toutes les configurations.

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



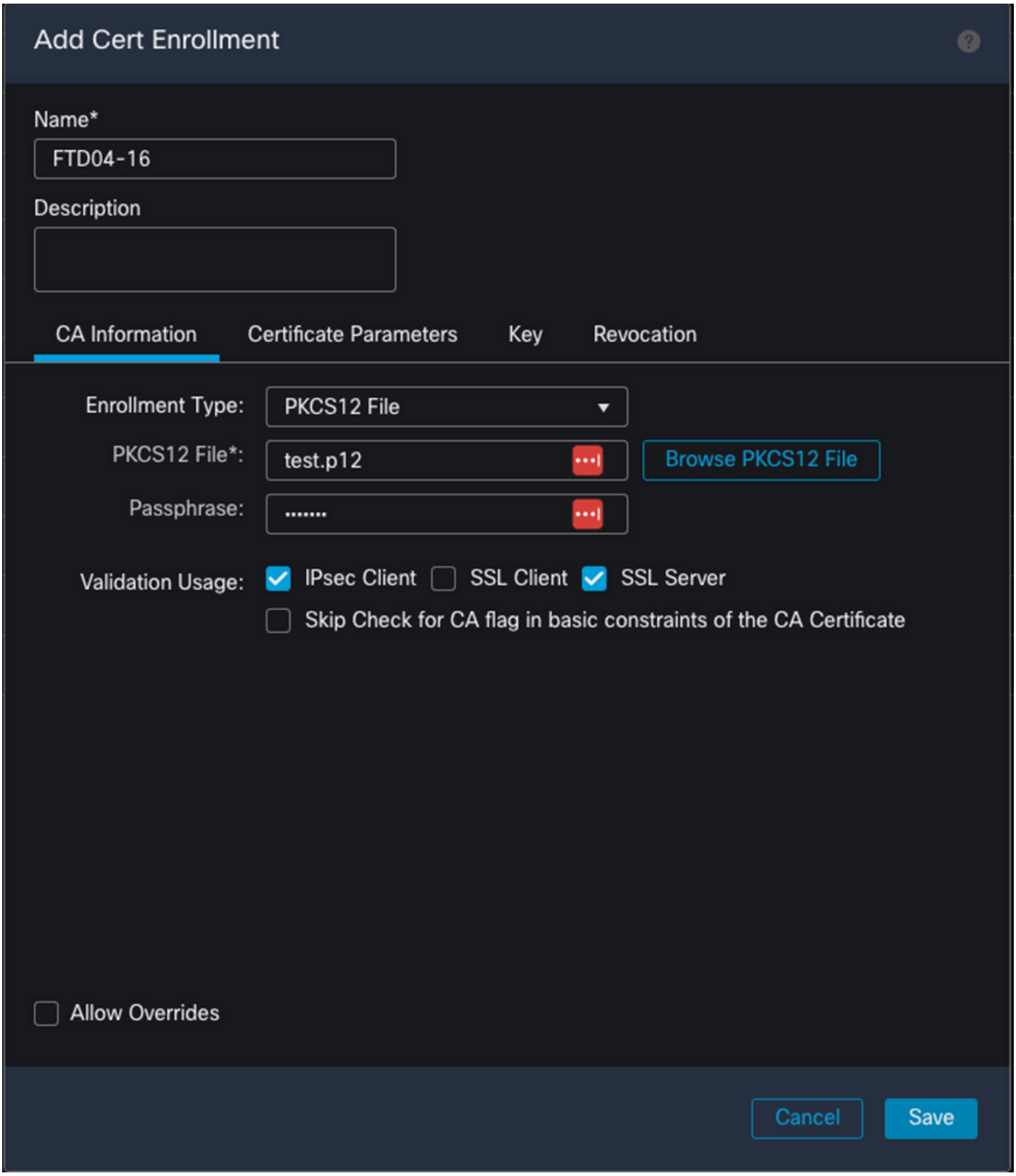
Capture d'écran des périphériques/certificats

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.



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.



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

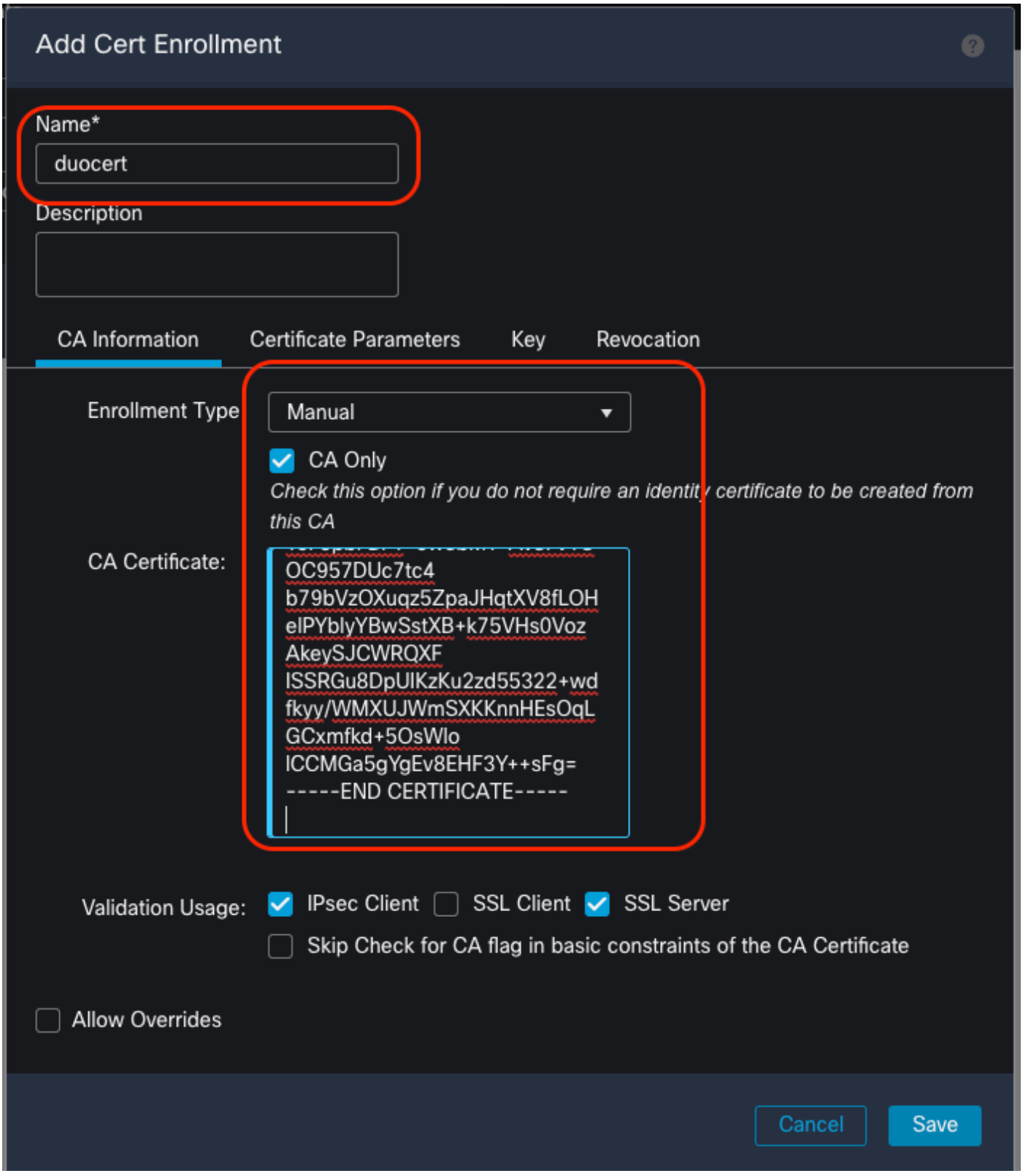
Cette section décrit la configuration et le déploiement du certificat IDP sur le FTD. Avant de commencer, assurez-vous de déployer toutes les configurations.

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.

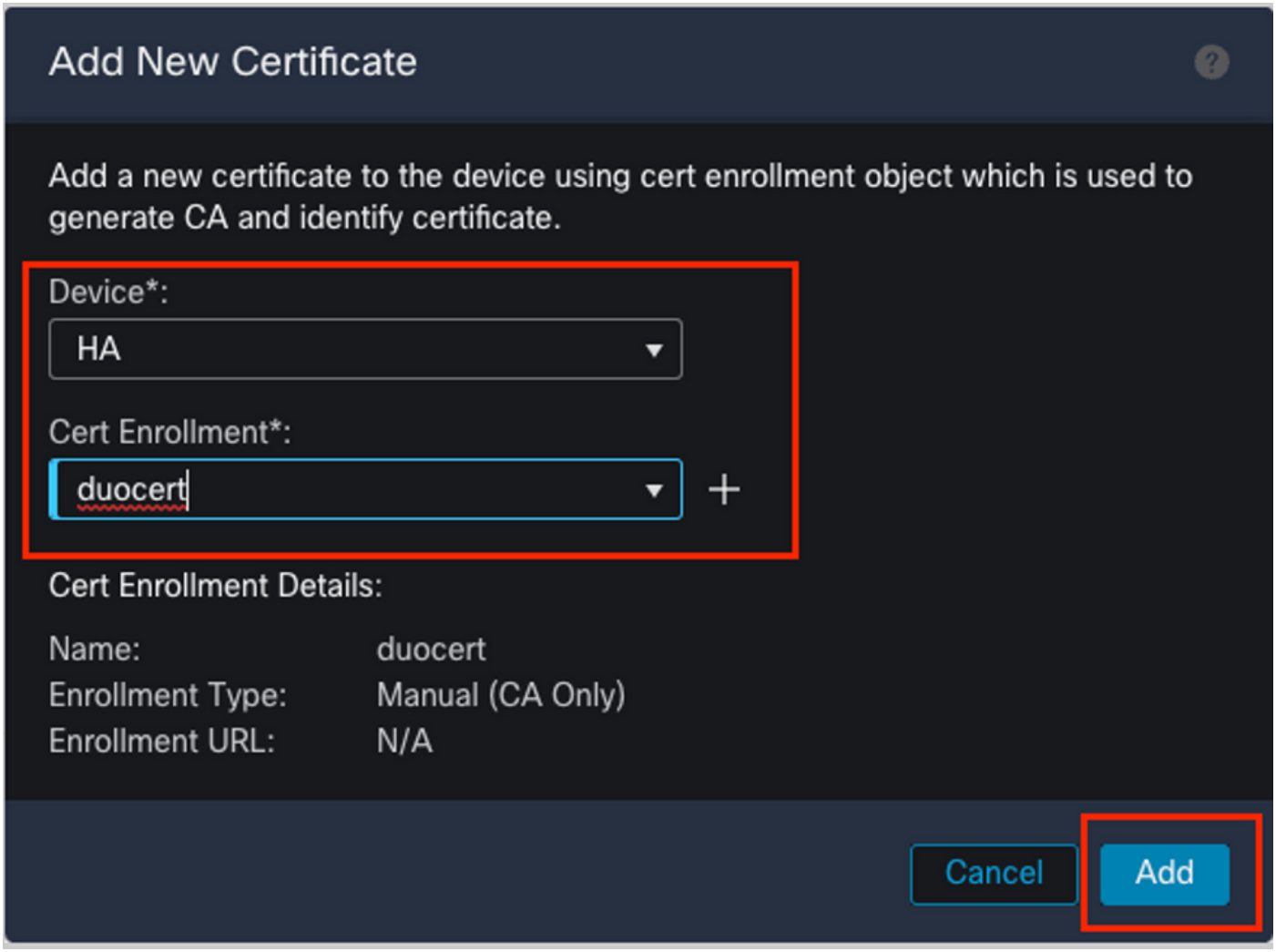
- Name : Nom de l'objet
- Type d'inscription : Manuel
- Case à cocher activée : CA uniquement
- Certificat CA : Format Pem du certificat



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.



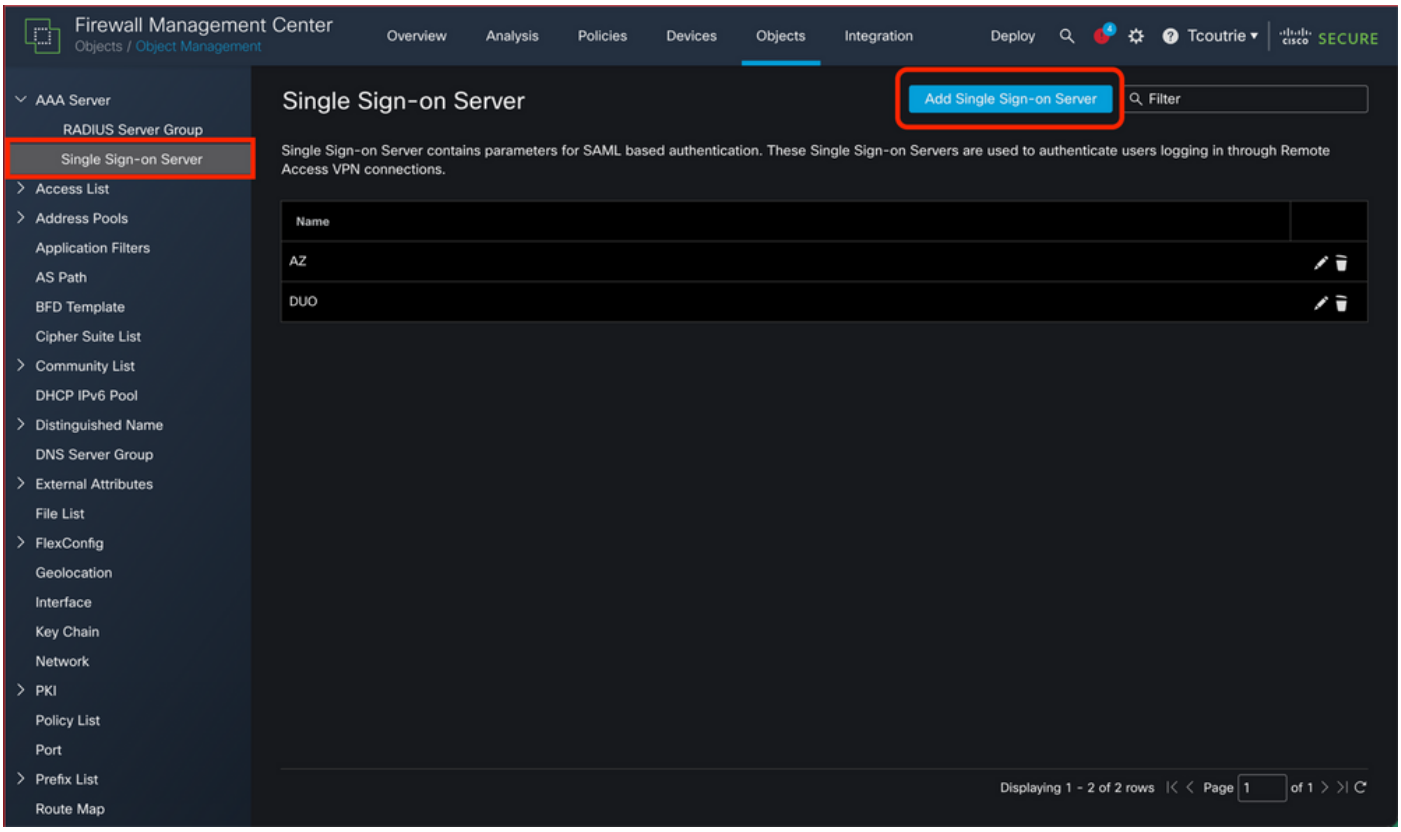
Capture d'écran de l'objet et du périphérique d'inscription

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".

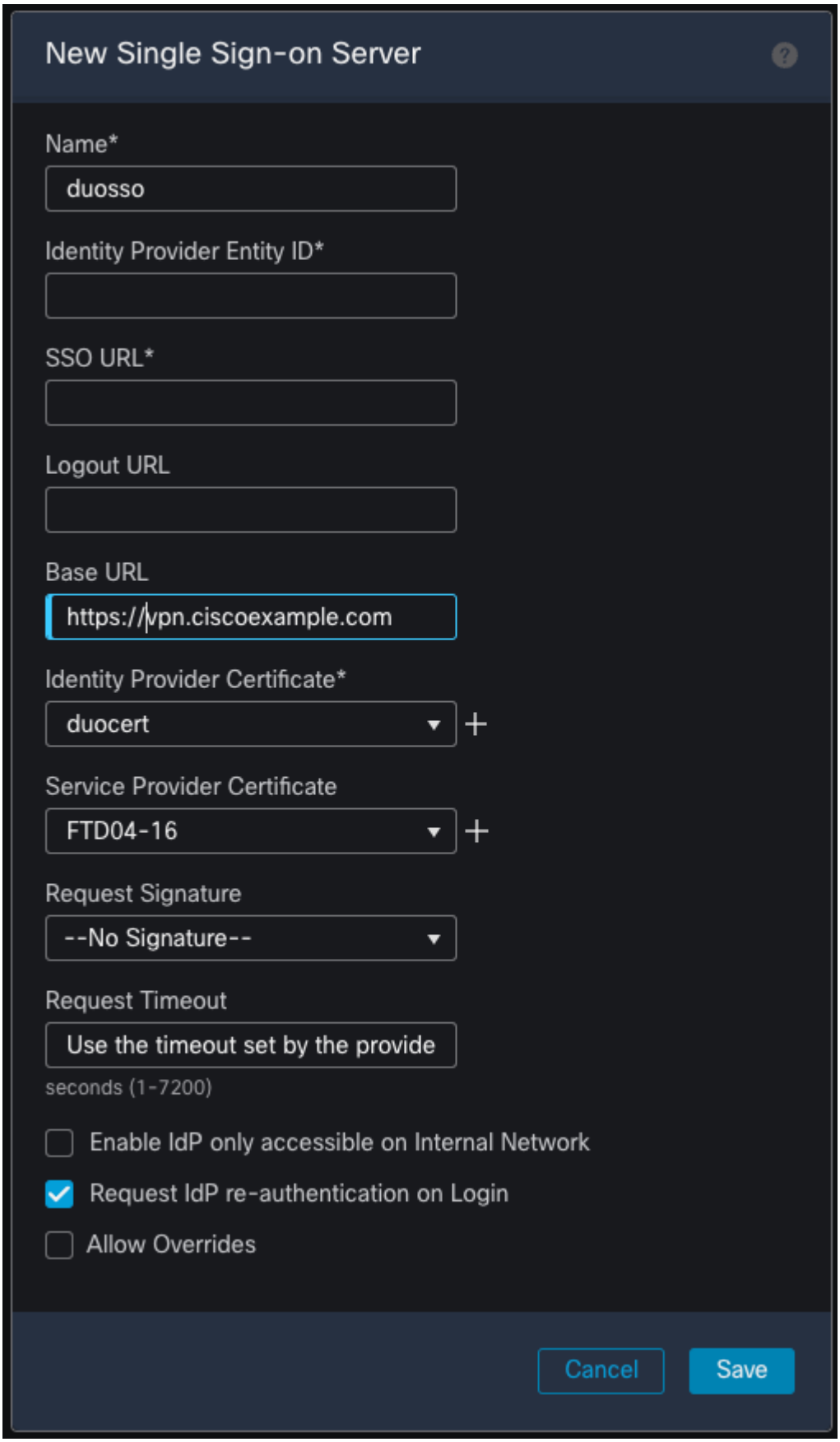


exemple de création d'un objet SSO

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



Exemple de nouvel objet SSO.

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

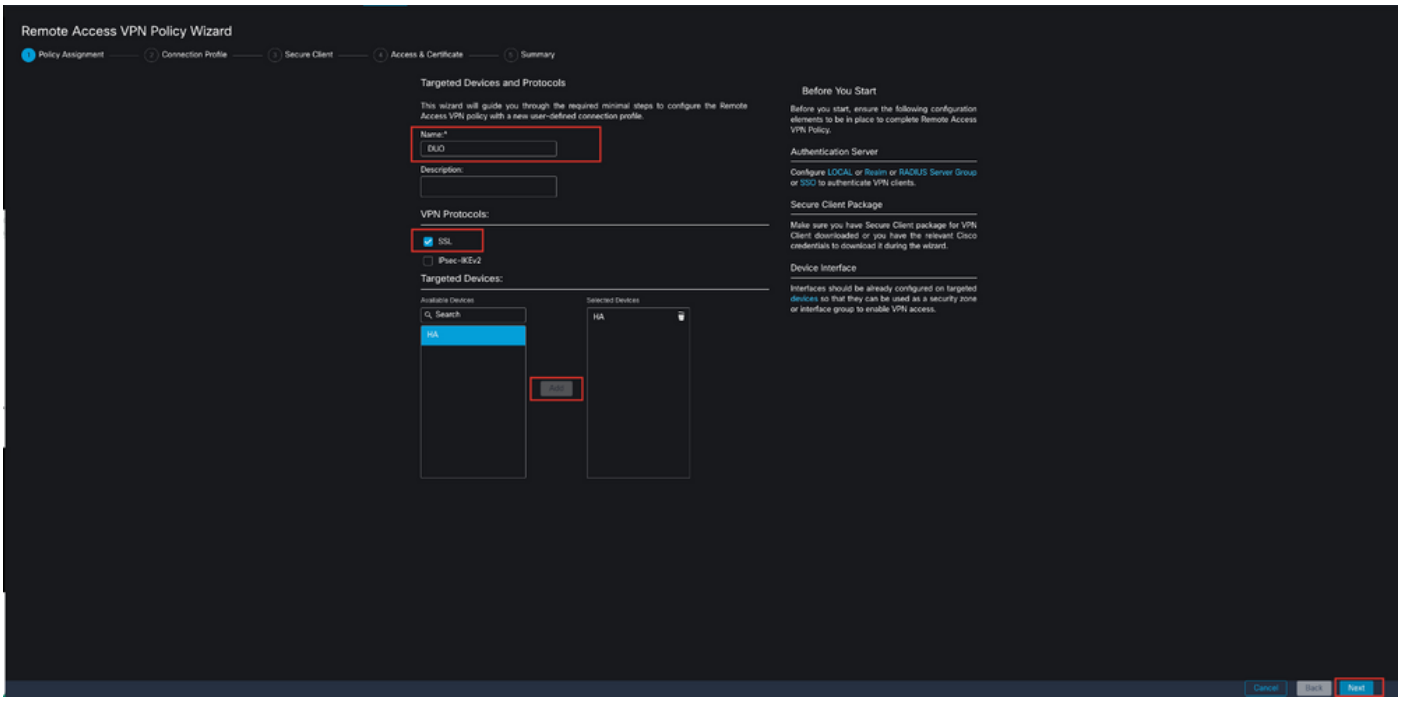
capture d'écran

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.



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".

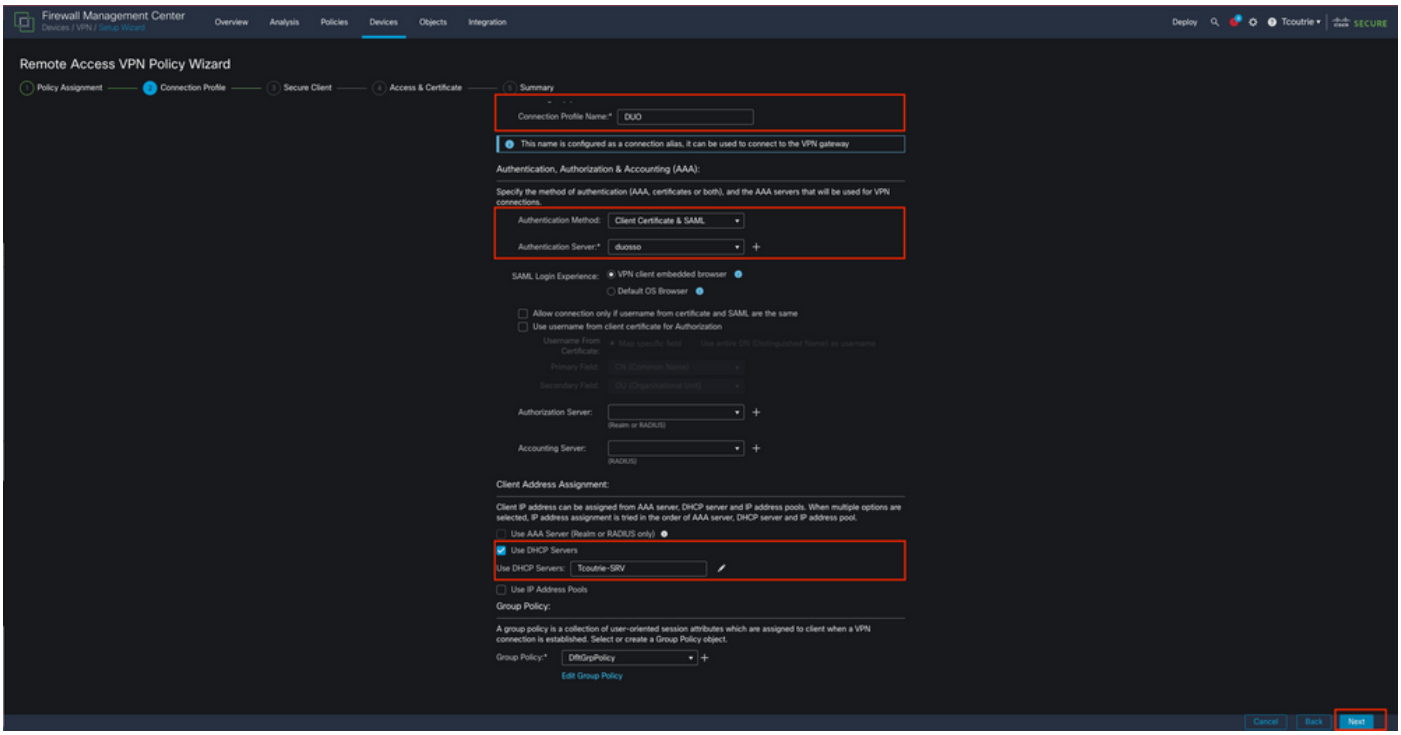
Authentification, autorisation et comptabilité (AAA) :

- 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

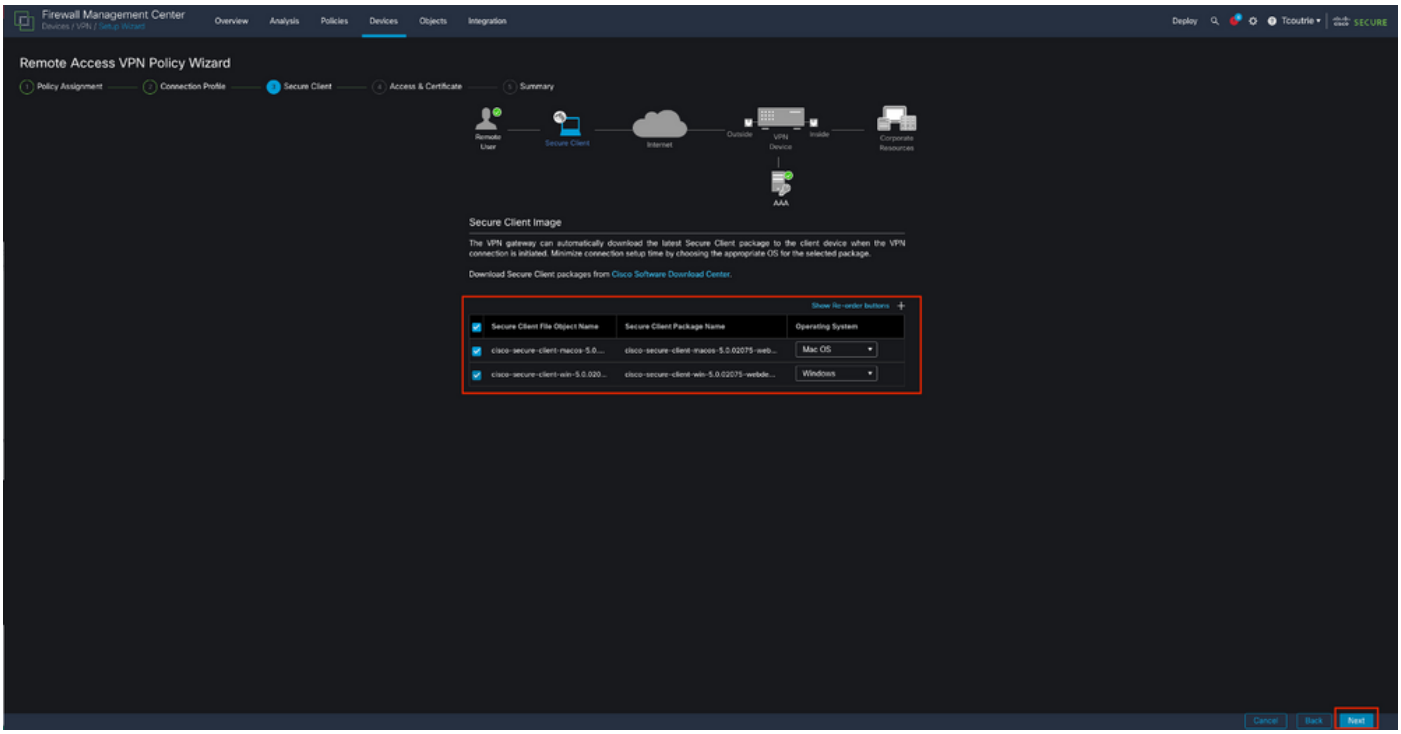
- Utiliser les pools d'adresses IP - Pool local sur le FTD



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.

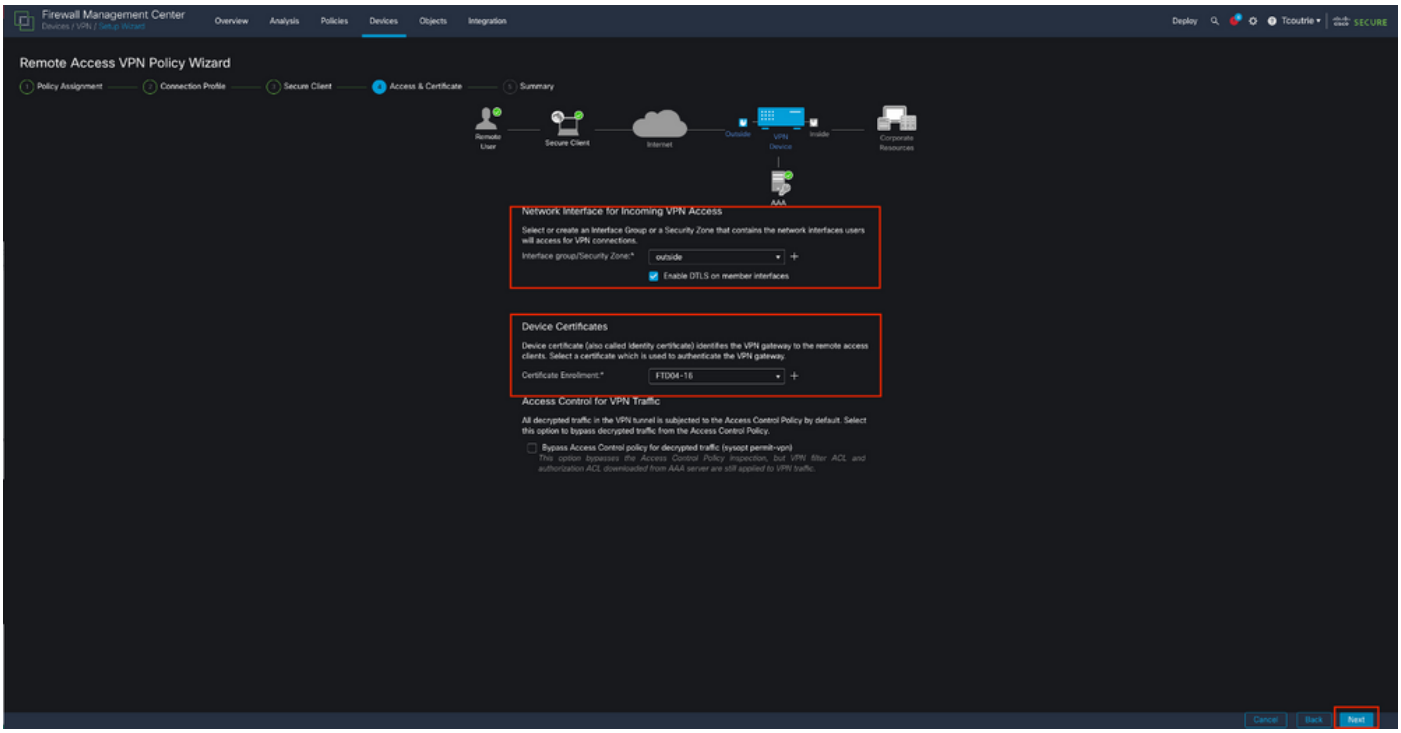


Étape 3 Assistant RAVPN

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

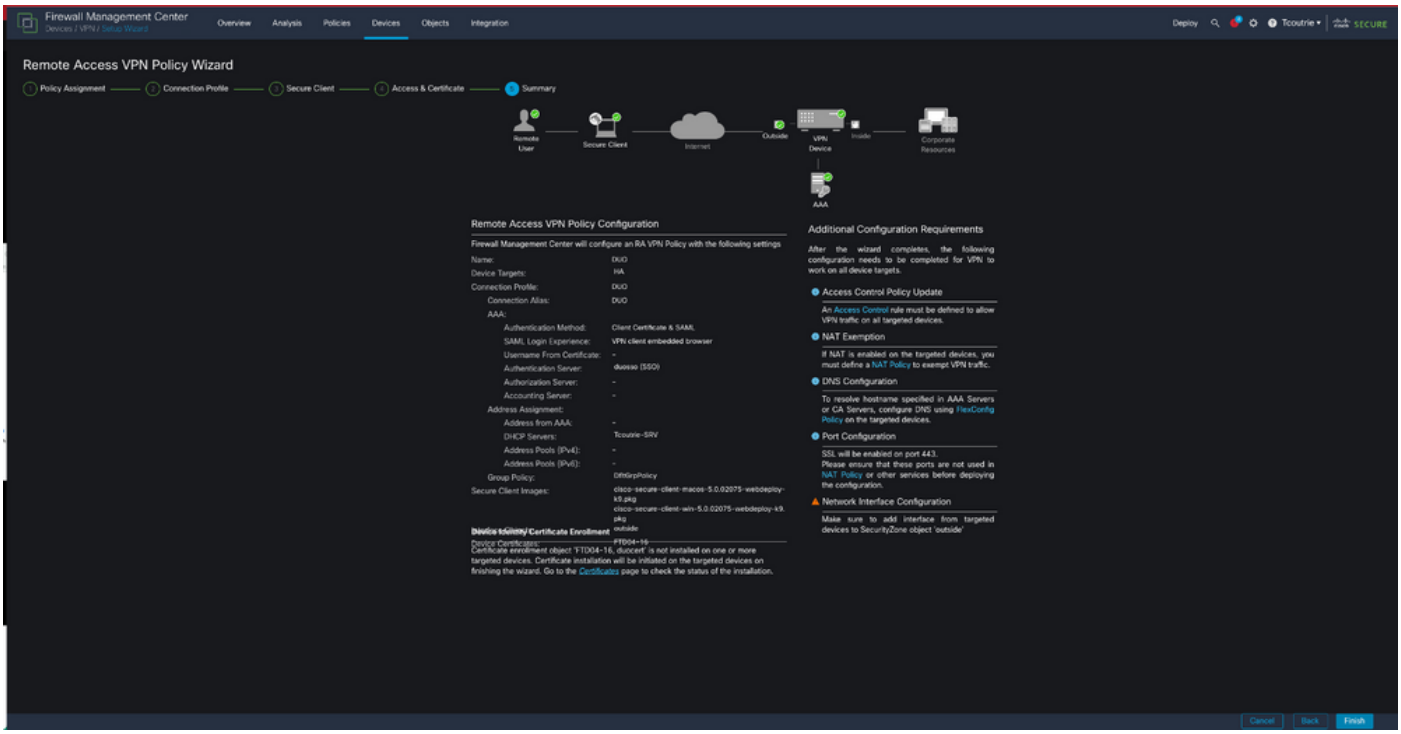


Étape 4 de l'assistant RAVPN

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

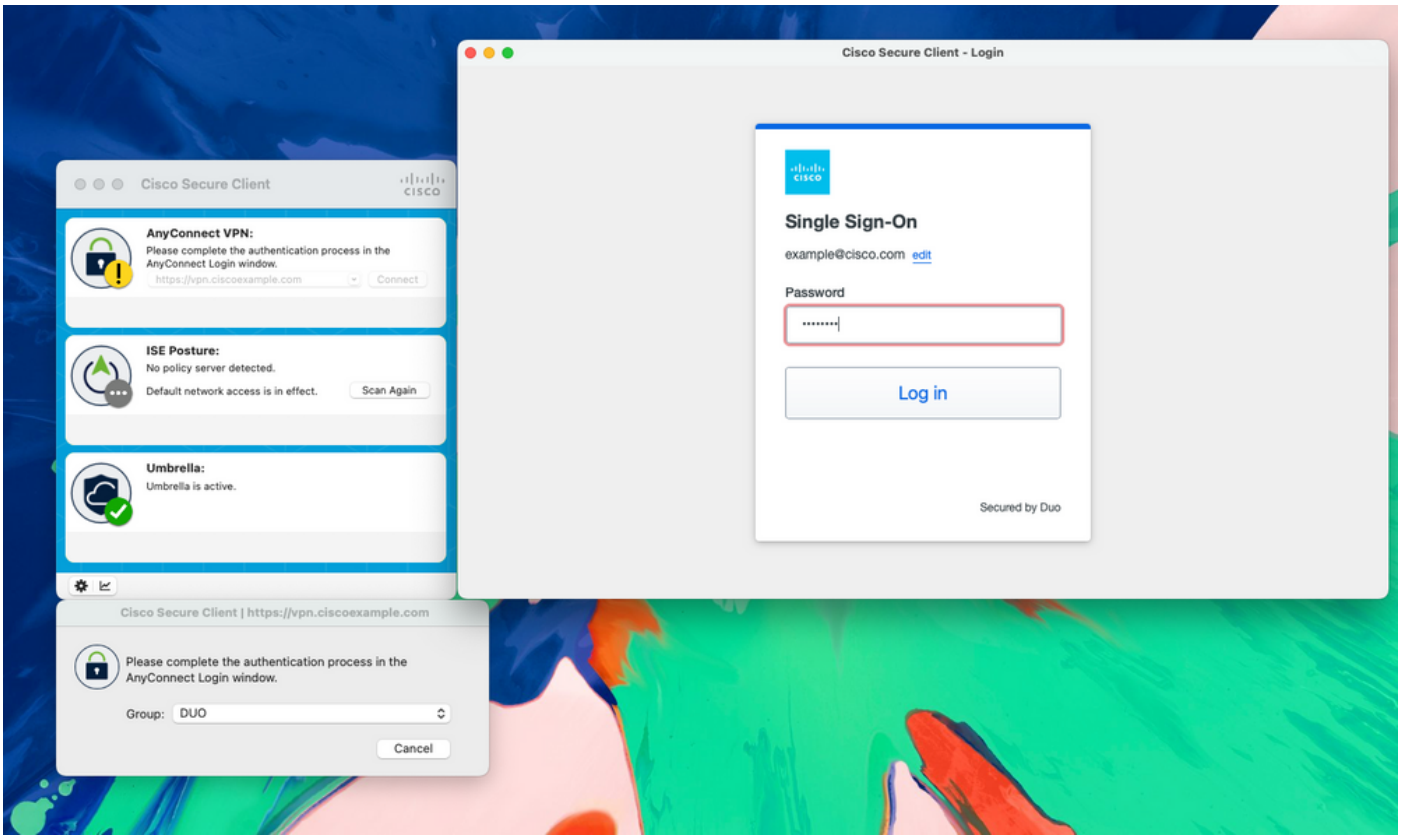
Étape 7. Déployez les configurations nouvellement ajoutées.

Vérifier

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

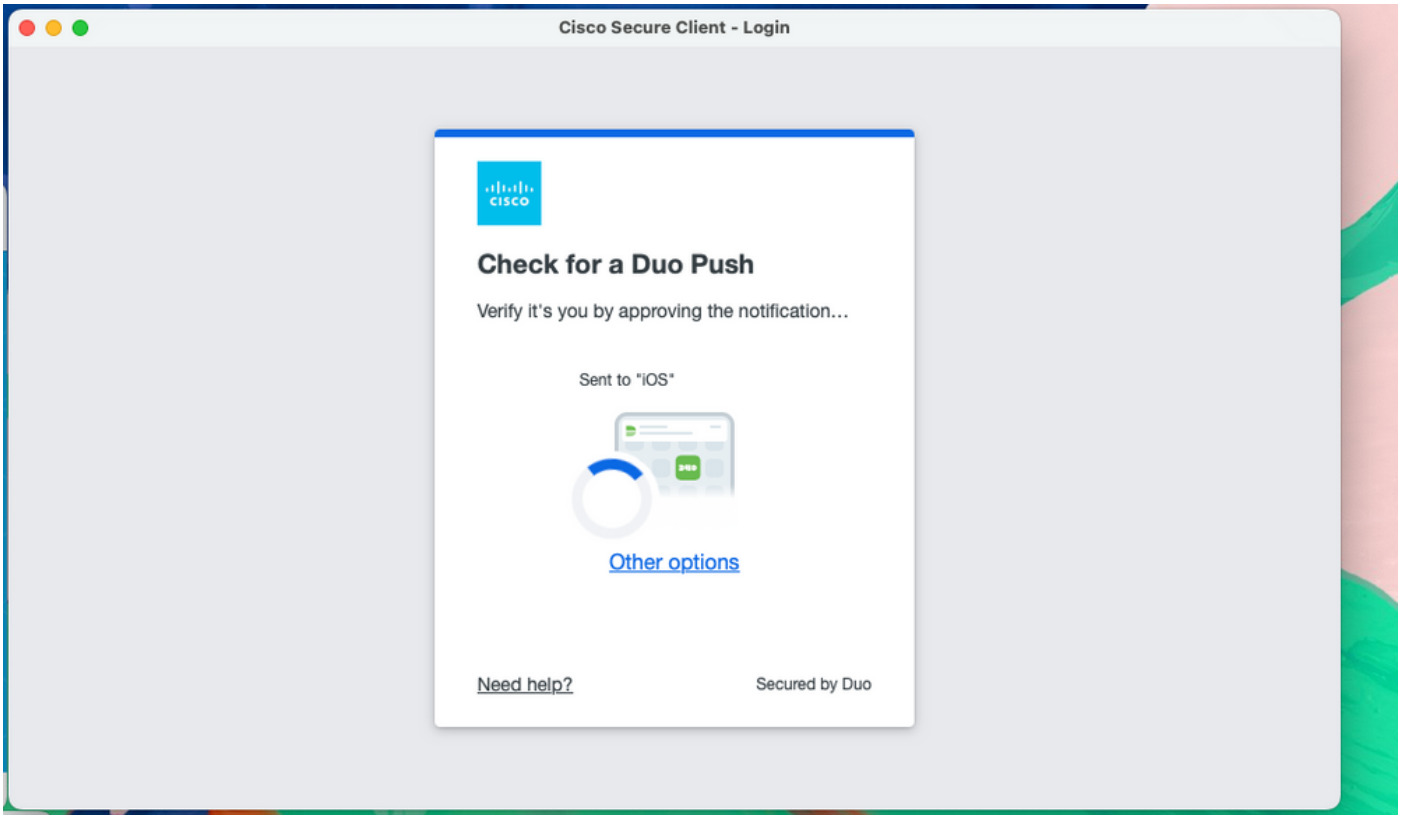
Ouvrez Cisco Secure Client, saisissez le nom de domaine complet du FTD et connectez-vous.

Saisissez les informations d'identification sur la page SSO.



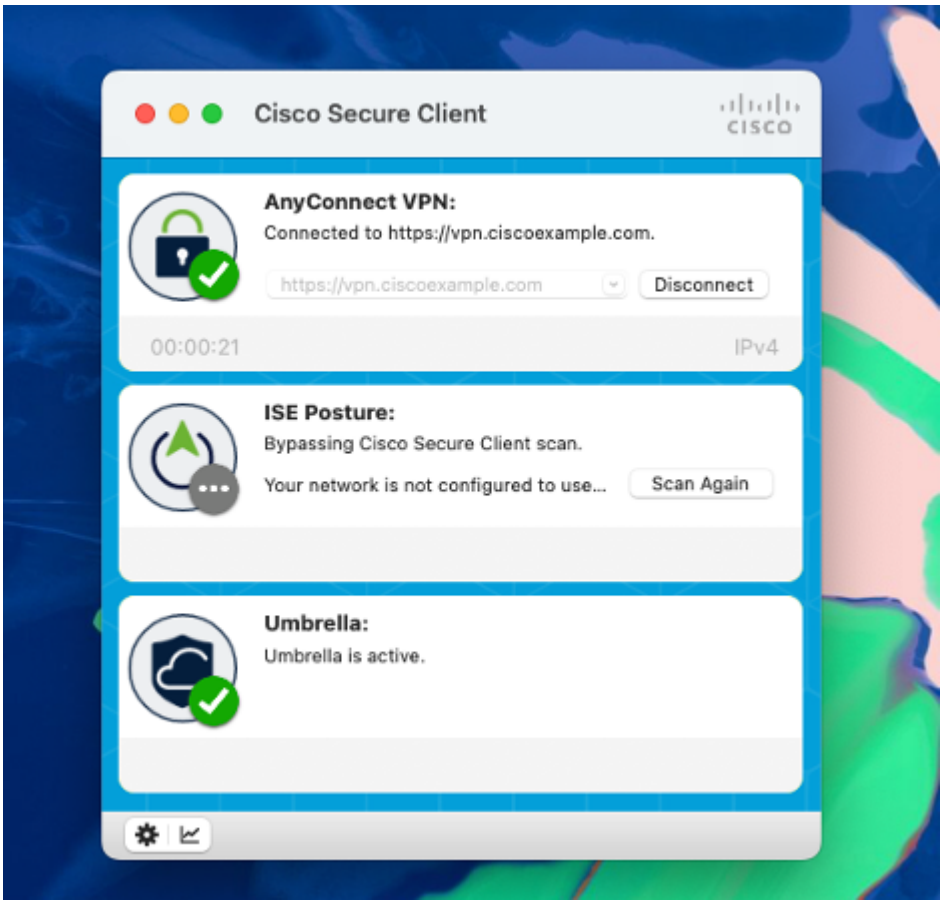
Page SSO via Cisco Secure Client

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.