Configuration de l'inscription automatique ZTNA Secure Access

Table des matières

Introduction

Ce document décrit les étapes requises pour configurer le ZTNA pour l'inscription automatique basée sur certificat.

Conditions préalables

- Client sécurisé version minimale 5.1.9.x

- Module de plateforme sécurisée (TPM) pour Windows

- Coprocesseur Secure Enclave pour les appareils Apple

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé Cisco
- Section Inscrire des périphériques sans accès sécurisé à l'aide du guide de certificat

Composants utilisés

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

- Windows 11 avec TPM version 2.0
- Client sécurisé version 5.1.10.17 avec module ZTNA et DUO activé.
- Microsoft Active Directory 2022
- Outil Openssl pour la génération de certificats

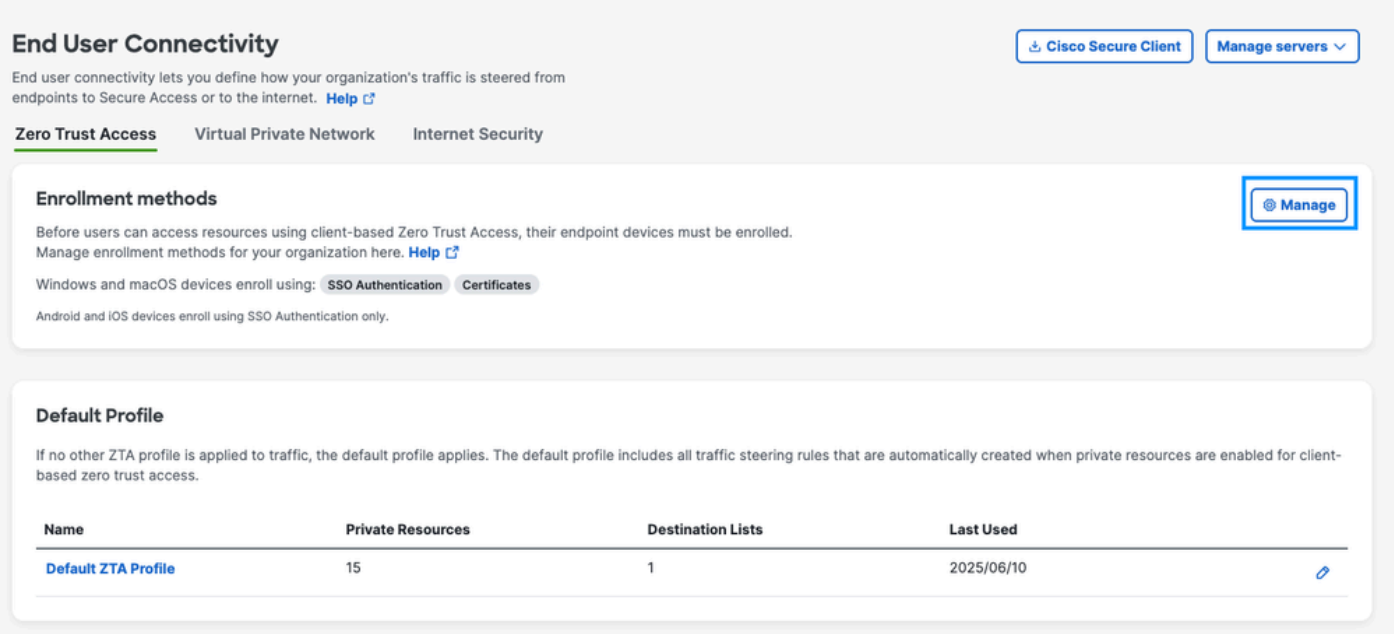
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Activation de l'inscription automatique sur le tableau de bord Secure Access

La première étape de l'activation de cette fonctionnalité consiste à activer la fonctionnalité d'inscription automatique d'accès sécurisé, qui comprend :

1. Accédez à Tableau de bord -> Connexion -> Connectivité de l'utilisateur final -> Confiance zéro

2. Cliquez sur l'option Gérer.



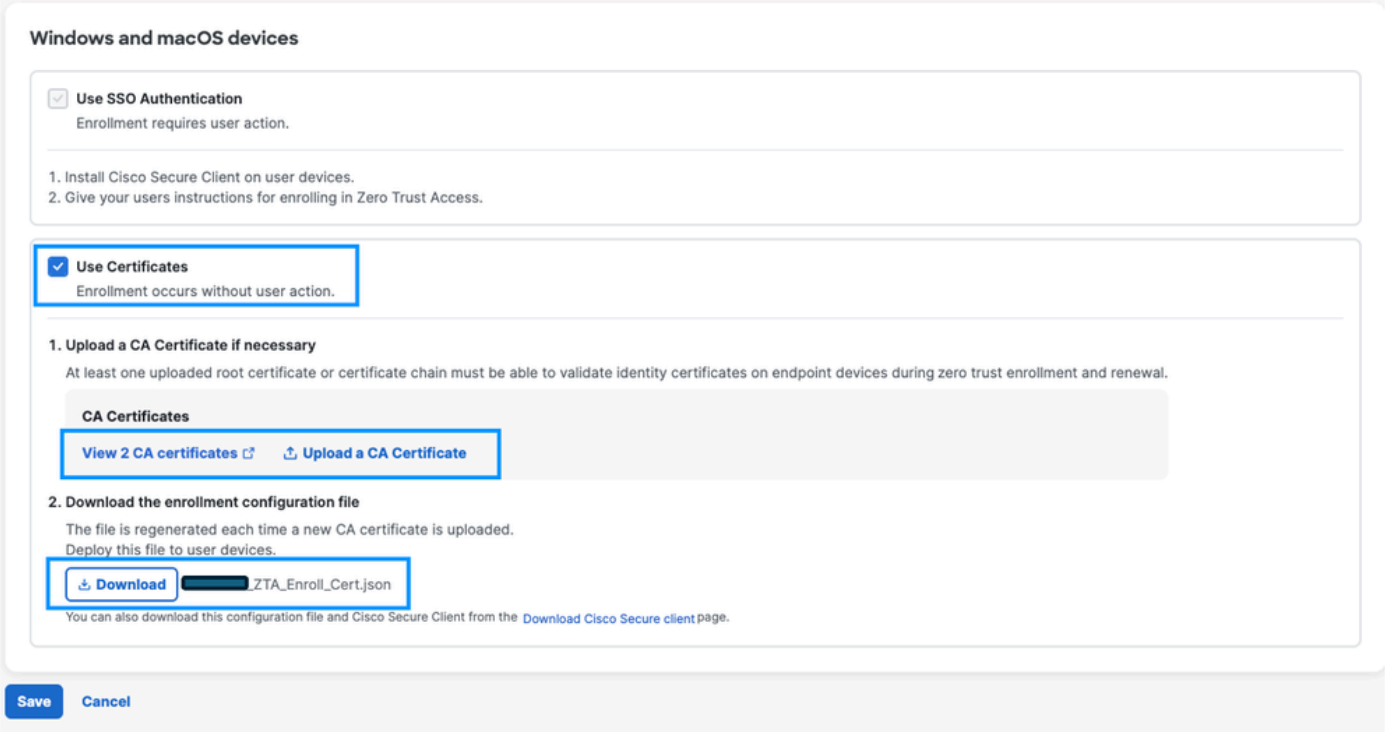
3. Activez Utiliser les certificats.

4. Téléchargez le certificat CA depuis votre autorité de certification locale.

5. Téléchargez la configuration d'inscription et placez-la dans les répertoires en fonction du système d'exploitation.

-Fenêtres: C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choice
- macOS : /opt/cisco/secureclient/zta/enrollment_choices

6. Veillez à enregistrer vos paramètres une fois terminé.



Modèle de certificat et installation

L'accès sécurisé nécessite les champs de certificat suivants :

- Autre nom du sujet (SAN) pour inclure l'adresse e-mail de plainte RFC-822 de l'utilisateur ou le nom de principe de l'utilisateur (UPN)

Exemple :

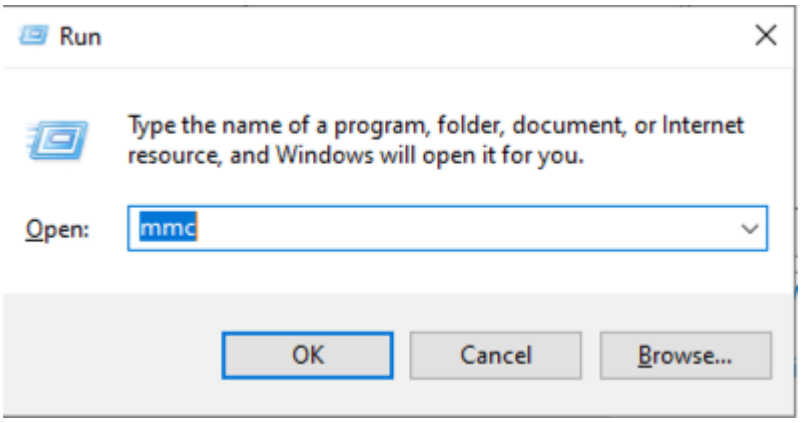
Option 1 : E-mail conforme RFC822
email.1 = username@domain.local

Option 2 : (alternative) : UPN (spécifique à Microsoft)
otherName : 1.3.6.1.4.1.311.20.2.3 ; UTF8 : username@domain.local

Dans cet exemple, nous utilisons le modèle de certificat utilisateur dans Microsoft AD pour générer le certificat.

Étape 1 : Accédez à Microsoft AD et ouvrez le Gestionnaire de certificats

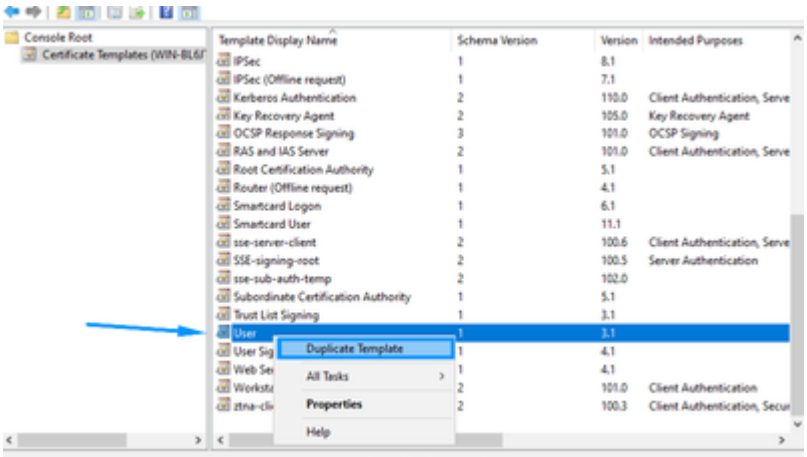
Étape 2 : Ouvrez Exécuter et accédez à Microsoft Management Console (mmc)



Étape 3 : Cliquez sur Fichier, puis ajoutez/supprimez un composant logiciel enfichable

Étape 4 : Ajouter des modèles de certificats

Étape 5 : Certificat utilisateur en double



Étape 6 : Configurez les paramètres comme décrit

1. Nouveau nom de modèle : ztna-client-enroll sous l'onglet (Général).

2. Sélectionnez (Approvisionnement dans la demande) dans l'onglet (Nom de l'objet).

Remarque : Cela garantit que les options fournies par le modèle openssl, telles que le nom alternatif de service (SAN), sont acceptées

---

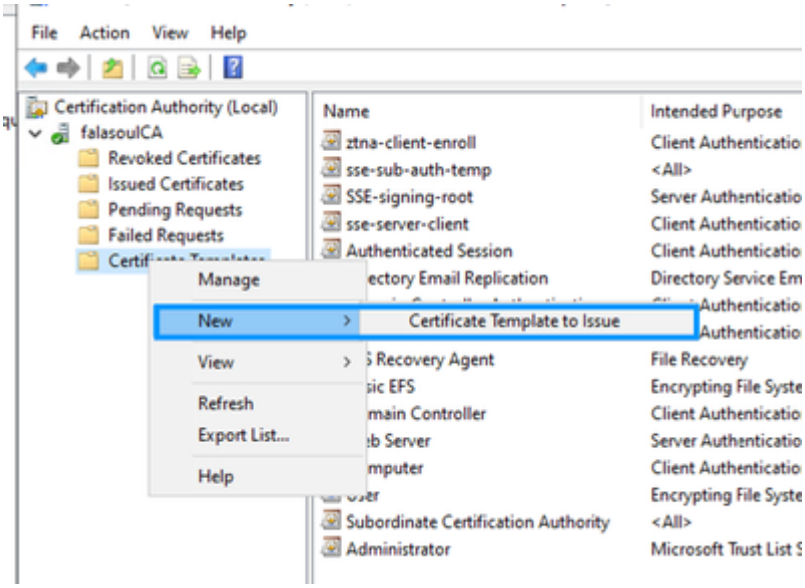
Étape 7 : Cliquez sur OK pour enregistrer le nouveau modèle

Étape 8 : Ajoutez le nouveau modèle à la liste des modèles AD en procédant comme suit :

1. Exécutez certsrv.msc

2. cliquez avec le bouton droit sur Modèles de certificat et sélectionnez Nouveau -> modèle de certificat à émettre

3. Sélectionnez votre nouveau modèle (ztna-client-enroll)



Création de certificat avec Openssl

Étape 1 : Créer un fichier san.cnf avec un contenu

```
[ req ]
default_bits       = 2048
prompt             = no
default_md         = sha256
distinguished_name = dn
req_extensions     = req_ext

[ dn ]
C  = US
ST = Texas
L  = Austin
O  = exampleusername
OU = IT
CN = exampleusername

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
# Option 1: RFC822-compliant email
email.1 = user@domain.local

# Option 2 (alternative): UPN (Microsoft-specific)
#otherName:1.3.6.1.4.1.311.20.2.3;UTF8:user@domain.local
```

Étape 2 : créer un certificat en utilisant le modèle

```
openssl genrsa -out user.key 2048
```

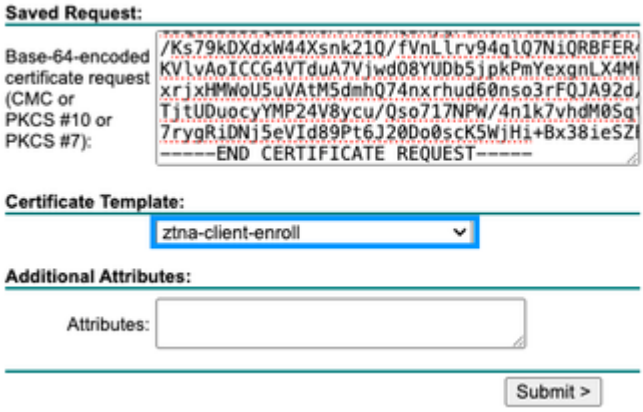
```
openssl req -new -key user.key -out user.csr
openssl req -new -key user.key -out user.csr -config san.cnf
```

Signer le certificat utilisateur avec le modèle CA ZTNA

Étape 1 : Copiez le contenu du fichier user.csr

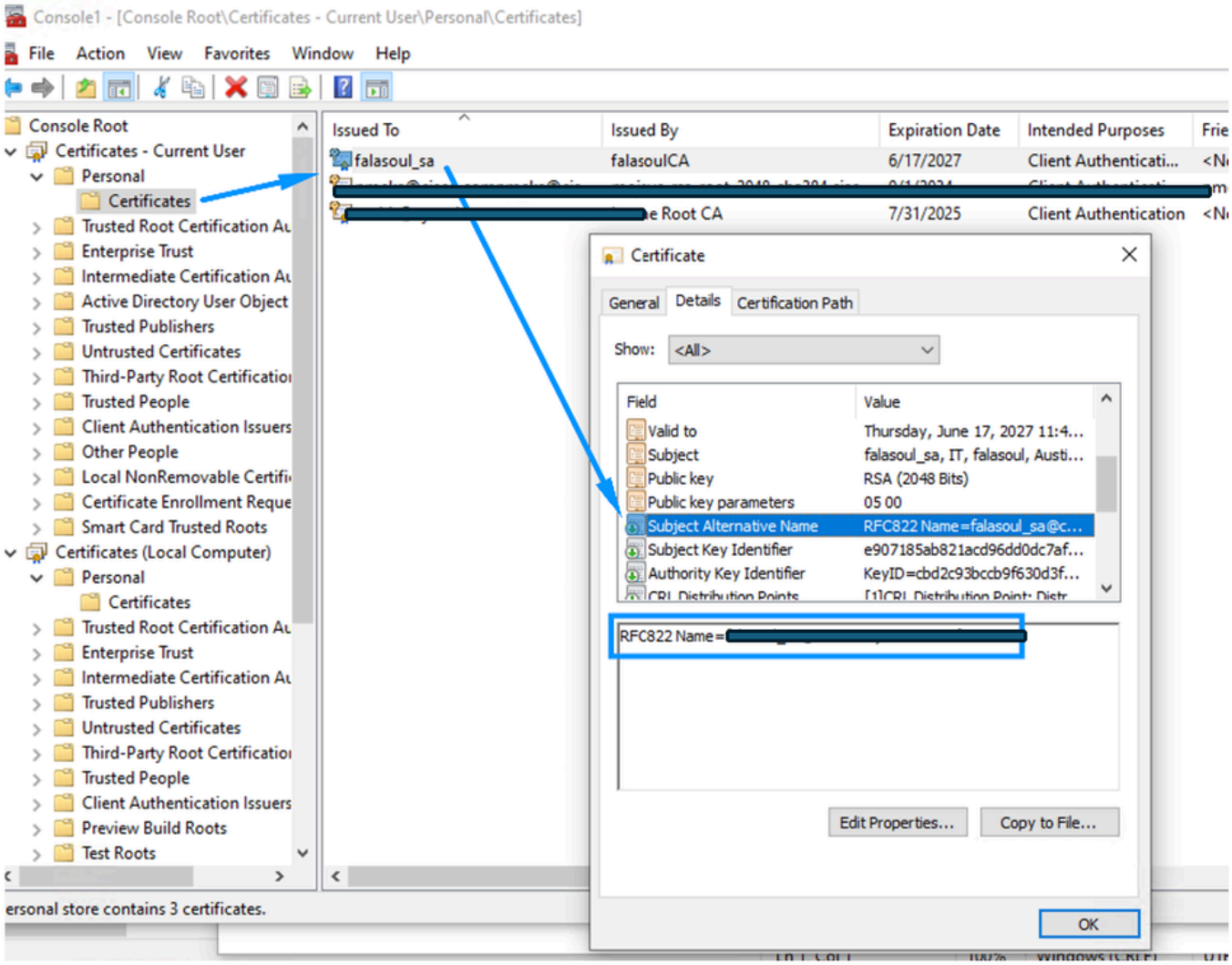
Étape 2 : accédez à votre autorité de signature AD locale (https:http://<adresse-ip>/certsrv/)

Étape 3 : Cliquez sur Request a Certificate -> Advanced Certificate Request -> sélectionnez le modèle ztna-client-enroll



Étape 4 : Téléchargez le certificat au format Base64 et installez-le dans le certificat du magasin de confiance personnel de l'utilisateur.

Étape 5 : Confirmer que les bonnes informations existent dans le certificat

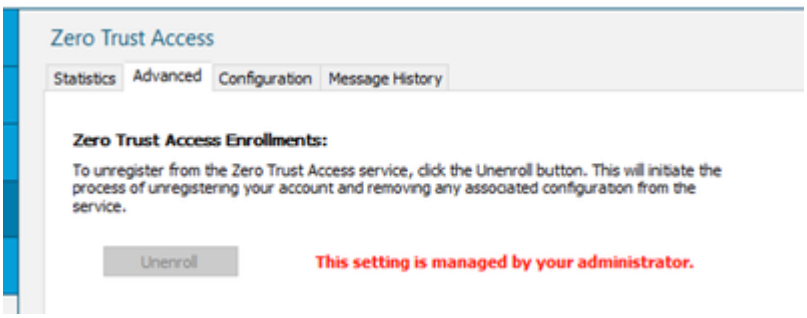


Étape 6 : Redémarrez votre module ZTNA pour que l'inscription démarre

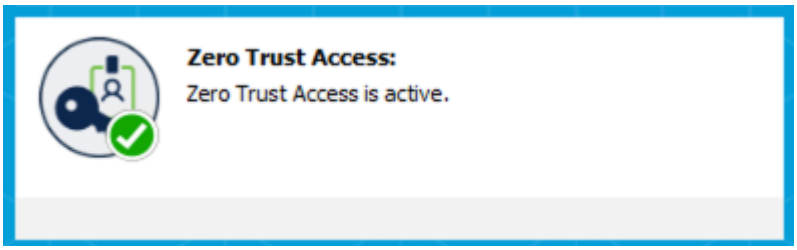
Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

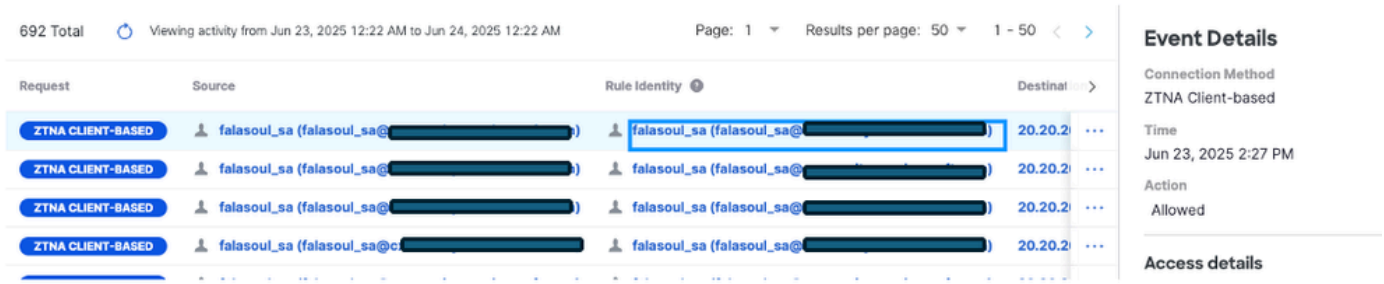
Étape 1 : Message du module ZTNA lors de la configuration du fichier de choix d'inscription :



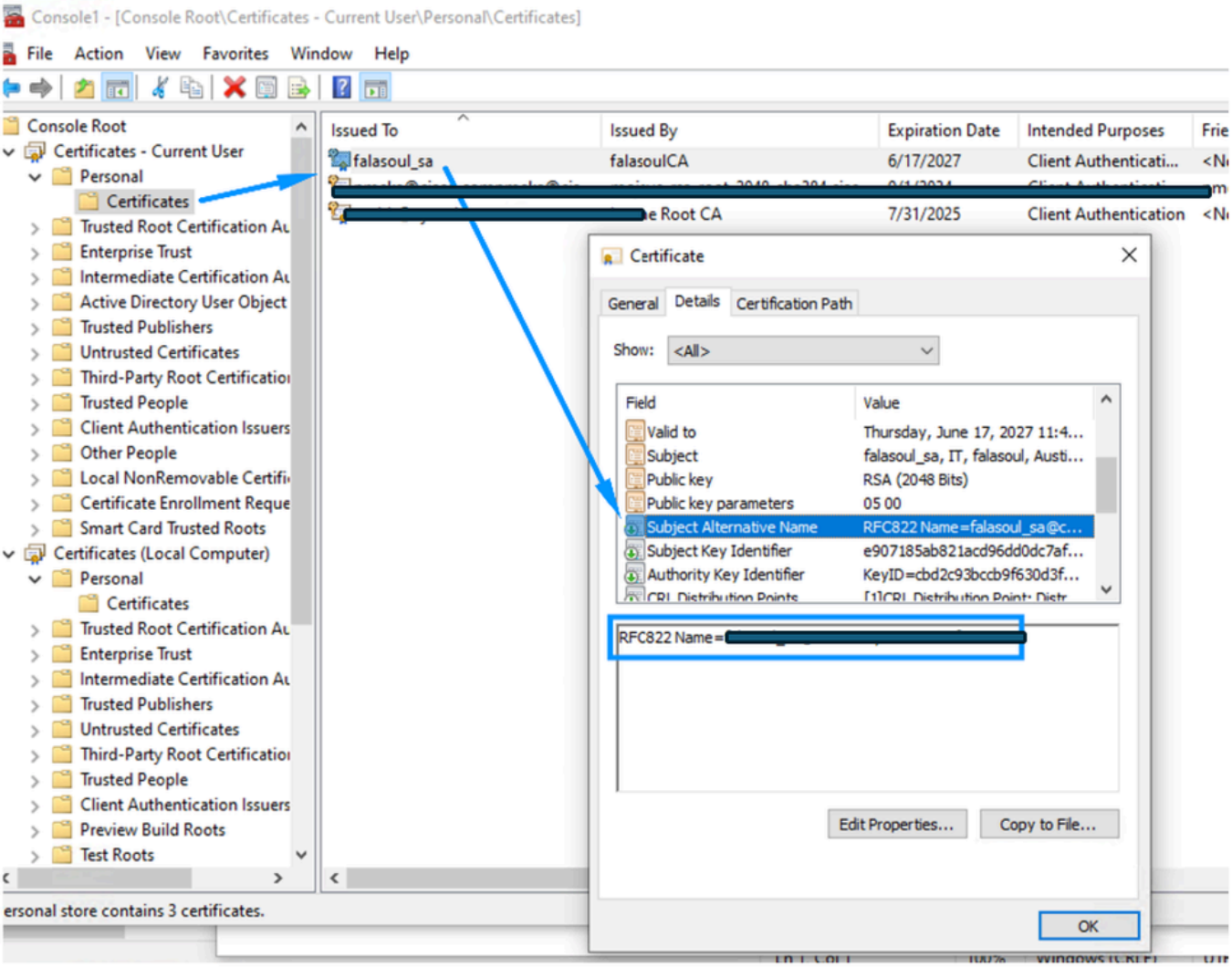
Étape 2 : Après avoir redémarré le module ZTNA pour la première fois, vous pouvez voir que vous êtes inscrit automatiquement dans ZTNA



Étape 3 : Vérifier l'utilisateur approprié dans la recherche d'activité en fonction des informations du SAN



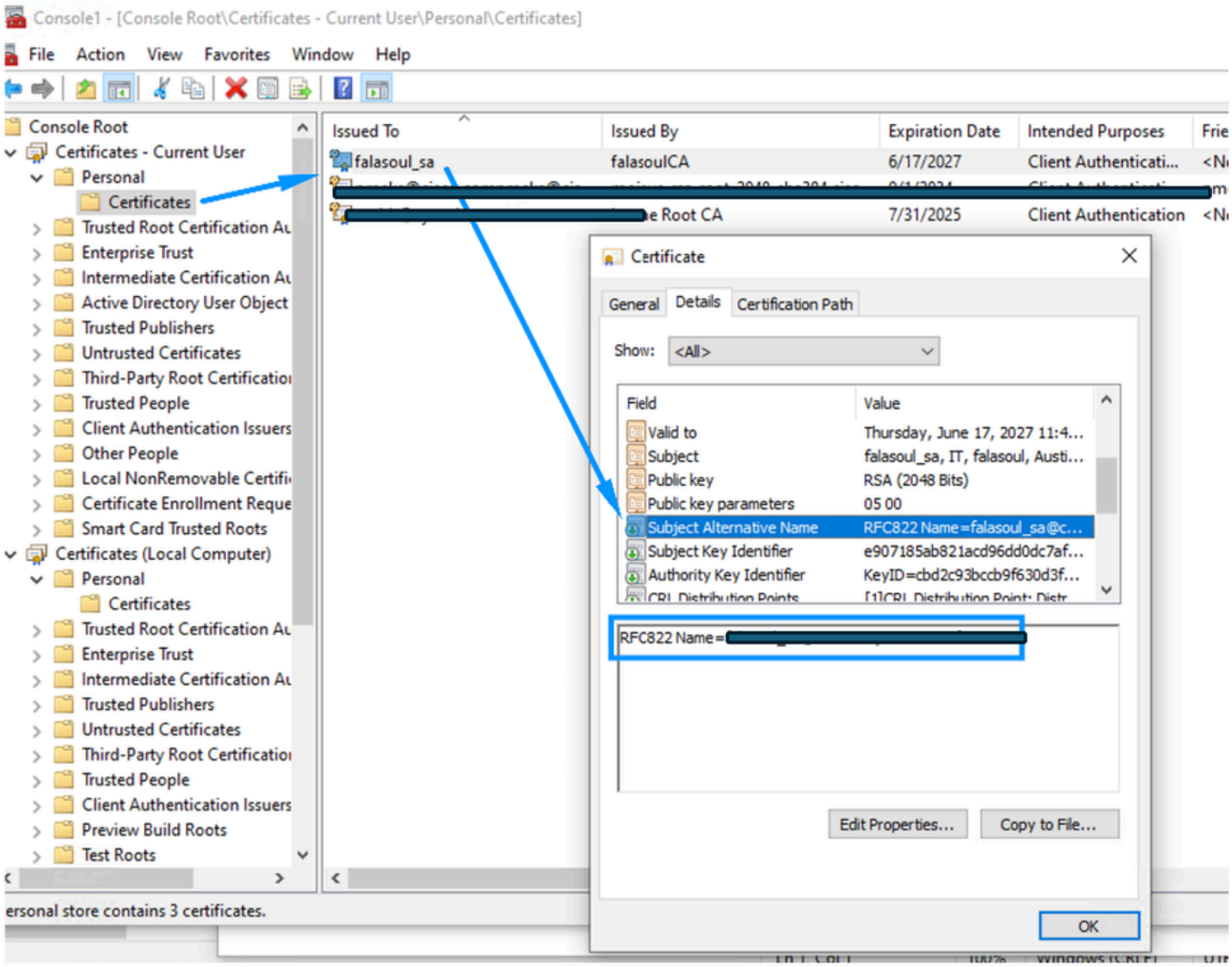
Étape 4 : Confirmer que les bonnes informations existent dans le certificat



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Étape 1 : Vérifiez que les bonnes informations existent dans le certificat et qu'elles sont installées dans le magasin de certificats approprié.



Étape 2 : Confirmez que l'inscription n'échoue pas sur les exigences de certificat à l'aide du DART

Étape 3 : Vérifiez que vous êtes en mesure de résoudre correctement votre interface externe FTD si UZTNA est utilisé.

erreur courante :

```
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] T/ AppSocketTransport.cpp:231 AppSocke
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] I/ TcpTransport.cpp:114 TcpTransport::
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x00000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.610238 csc_zta_agent[0x00001638, 0x00000e58] T/ TcpTransport.cpp:150 TcpTransport::
2025-06-16 05:44:45.610238 csc_zta_agent[0x00001638, 0x00000e58] E/ TcpTransport.cpp:166 TcpTransport::
```

Informations connexes

- Assistance et documentation techniques - Cisco Systems

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.