Konfigurieren des sicheren Zugriffs für die automatische ZTNA-Registrierung

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Konfiguration des ZTNA für die zertifikatbasierte automatische Registrierung beschrieben.

Voraussetzungen

- Secure Client, Mindestversion 5.1.9.x

- Trusted Platform Module (TPM) für Windows

- Secure Enclave Coprozessor für Apple Geräte

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff von Cisco
- Registrieren von Geräten für den nicht vertrauenswürdigen Zugriff mithilfe des Zertifikatshandbuchs

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Windows 11 mit TPM Version 2.0
- Secure Client Version 5.1.10.17 mit aktiviertem ZTNA- und DUO-Modul
- Microsoft Active Directory 2022
- OpenSSL-Tool zur Erstellung von Zertifikaten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

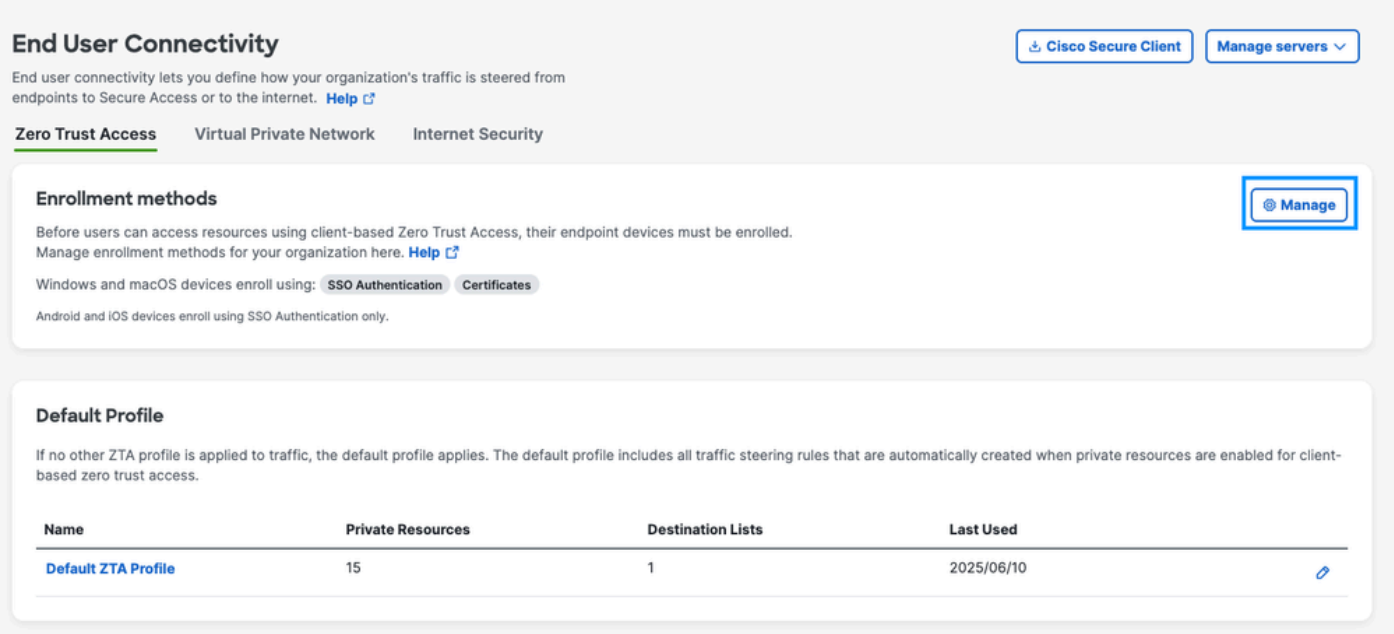
Aktivieren der automatischen Registrierung auf dem Secure

Access Dashboard

Der erste Schritt bei der Aktivierung dieser Funktion besteht in der Aktivierung der Funktion für die automatische Anmeldung bei Secure Access. Diese umfasst:

1. Navigieren Sie zu Dashboard -> Verbinden -> Endbenutzerverbindung -> Zero Trust

2. Klicken Sie auf die Option Verwalten.



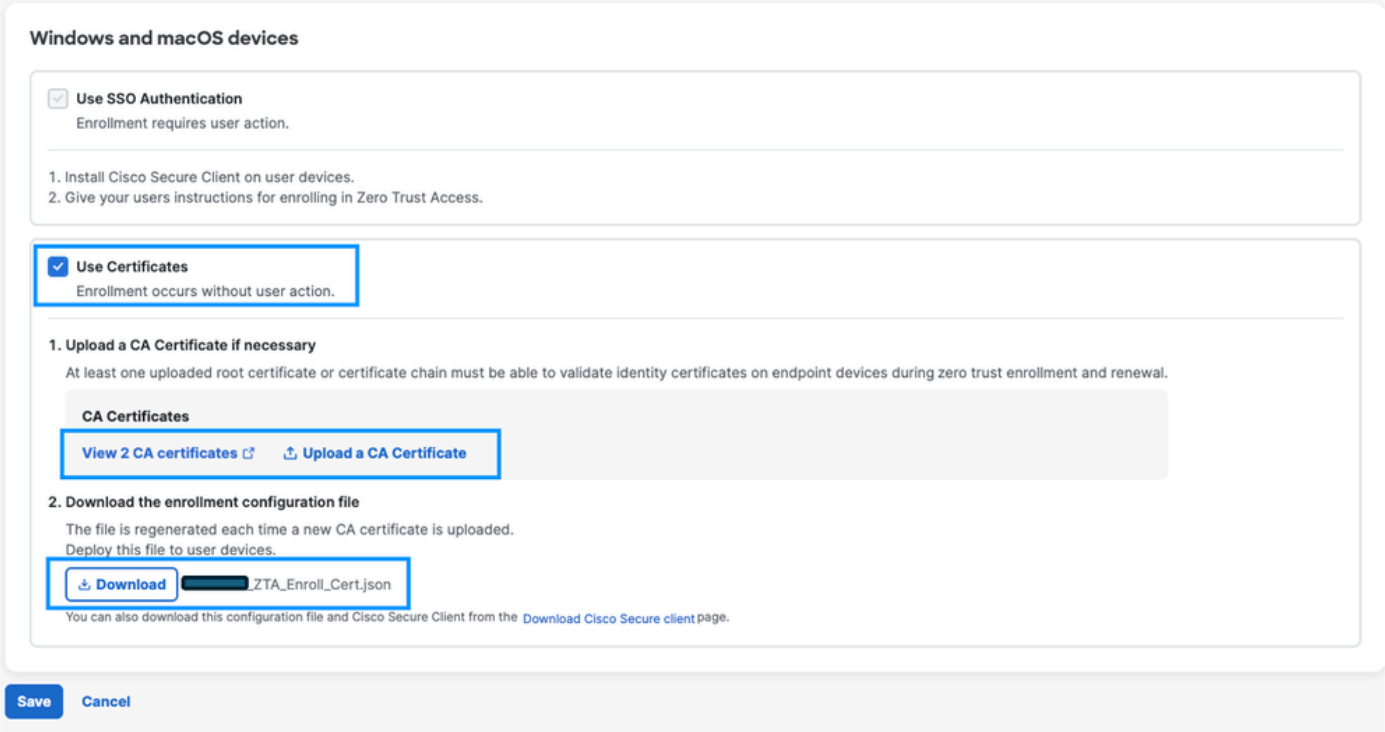
3. Aktivieren Sie die Option "Zertifikate verwenden".

4. Laden Sie das Zertifizierungsstellenzertifikat hoch, indem Sie es von Ihrer lokalen Zertifizierungsstelle herunterladen.

5. Laden Sie die Registrierungskonfiguration herunter, und speichern Sie sie je nach Betriebssystem in den Verzeichnissen.

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

6. Speichern Sie Ihre Einstellungen, sobald Sie fertig sind.



Zertifikatvorlage und Installation

Für den sicheren Zugriff müssen folgende Zertifikatfelder ausgefüllt werden:

- Betreff Alternativer Name (SAN) mit der RFC-822-Beschwerde-E-Mail-Adresse oder dem Benutzerprinzipalnamen (UPN)

Beispiel:

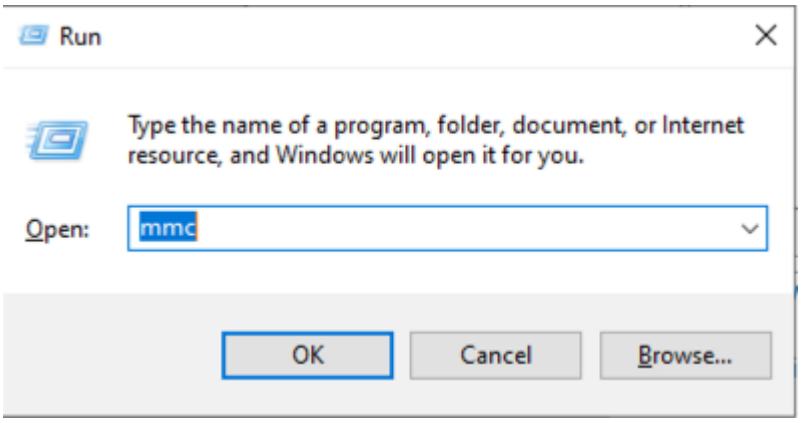
Option 1: RFC822-konforme E-Mail
email.1 = username@domain.local

Option 2: (alternativ): UPN (Microsoft-spezifisch)
SonstigeName:1.3.6.1.4.1.311.20.2.3;UTF8:username@domain.local

In diesem Beispiel wird die Benutzerzertifikatvorlage in Microsoft AD zum Generieren des Zertifikats verwendet.

Schritt 1: Navigieren Sie zu Microsoft AD, und öffnen Sie den Zertifikats-Manager.

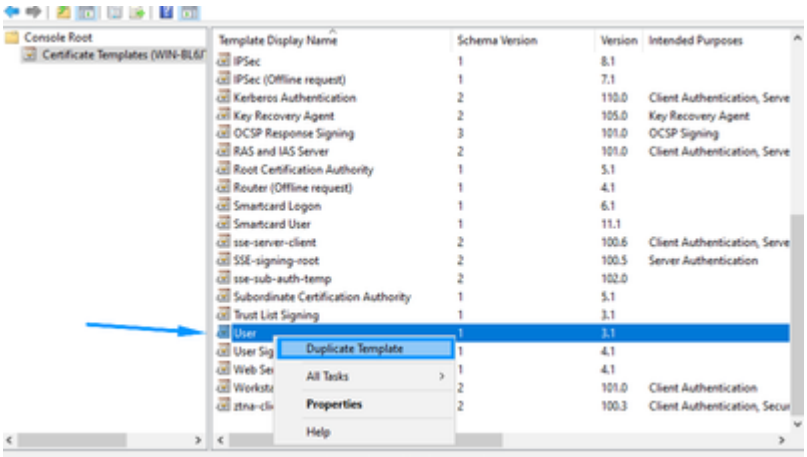
Phase 2: Öffnen Sie Ausführen, und rufen Sie Microsoft Management Console (mmc) auf.



Schritt 3: Klicken Sie auf Datei und fügen Sie Snap-In hinzu bzw. entfernen Sie Snap-In.

Schritt 4: Zertifikatvorlagen hinzufügen

Schritt 5: Benutzerzertifikat kopieren



Schritt 6: Konfigurieren Sie die Einstellungen wie beschrieben.

1. Name der neuen Vorlage: ztna-client-enroll under (Allgemein) tab.

2. Wählen Sie (im Antrag angeben) auf der Registerkarte (Betreffname).

Anmerkung: Dadurch wird sichergestellt, dass die von der openssl-Vorlage bereitgestellten Optionen wie Service Alternative Name (SAN) akzeptiert werden.

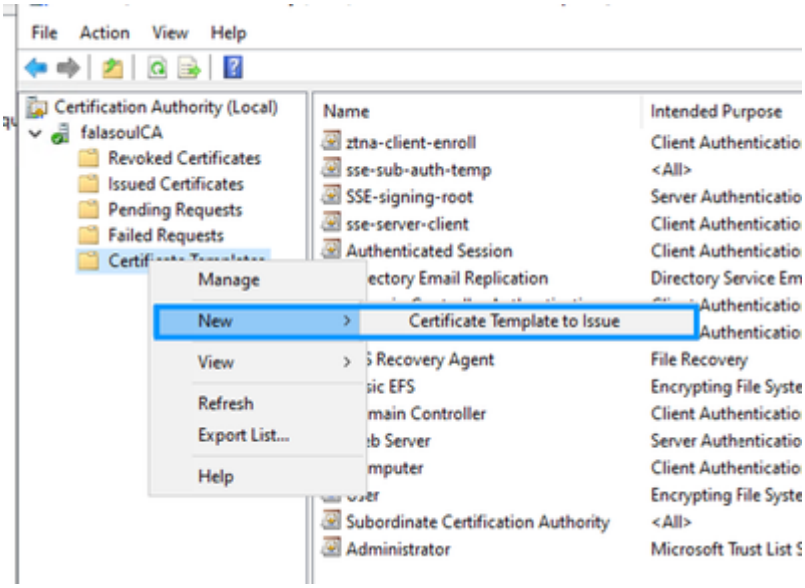
Schritt 7: Klicken Sie auf OK, um die neue Vorlage zu speichern

Schritt 8: Fügen Sie der Liste der AD-Vorlagen die neue Vorlage hinzu, indem Sie wie folgt vorgehen:

1. Führen Sie certsrv.msc

2. Klicken Sie mit der rechten Maustaste auf Zertifikatvorlagen, und wählen Sie Neu -> Zertifikatvorlage aus, die ausgestellt werden soll

3. Wählen Sie Ihre neu erstellte Vorlage (ztna-client-enroll)



Erstellen eines Zertifikats mit OpenSSL

Schritt 1: san.cnf-Datei mit Inhalt erstellen

```
[ 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
```

Phase 2: Zertifikat mithilfe der Vorlage erstellen

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

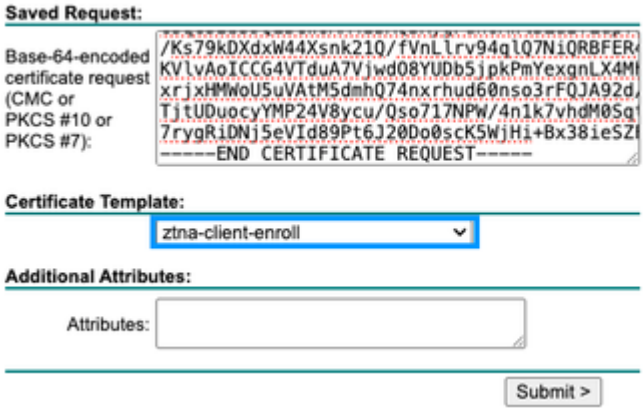
```
openssl req -new -key user.key -out user.csr
openssl req -new -key user.key -out user.csr -config san.cnf
```

Benutzerzertifikat mit CA ZTNA-Vorlage signieren

Schritt 1: Kopieren Sie den Inhalt der Datei user.csr.

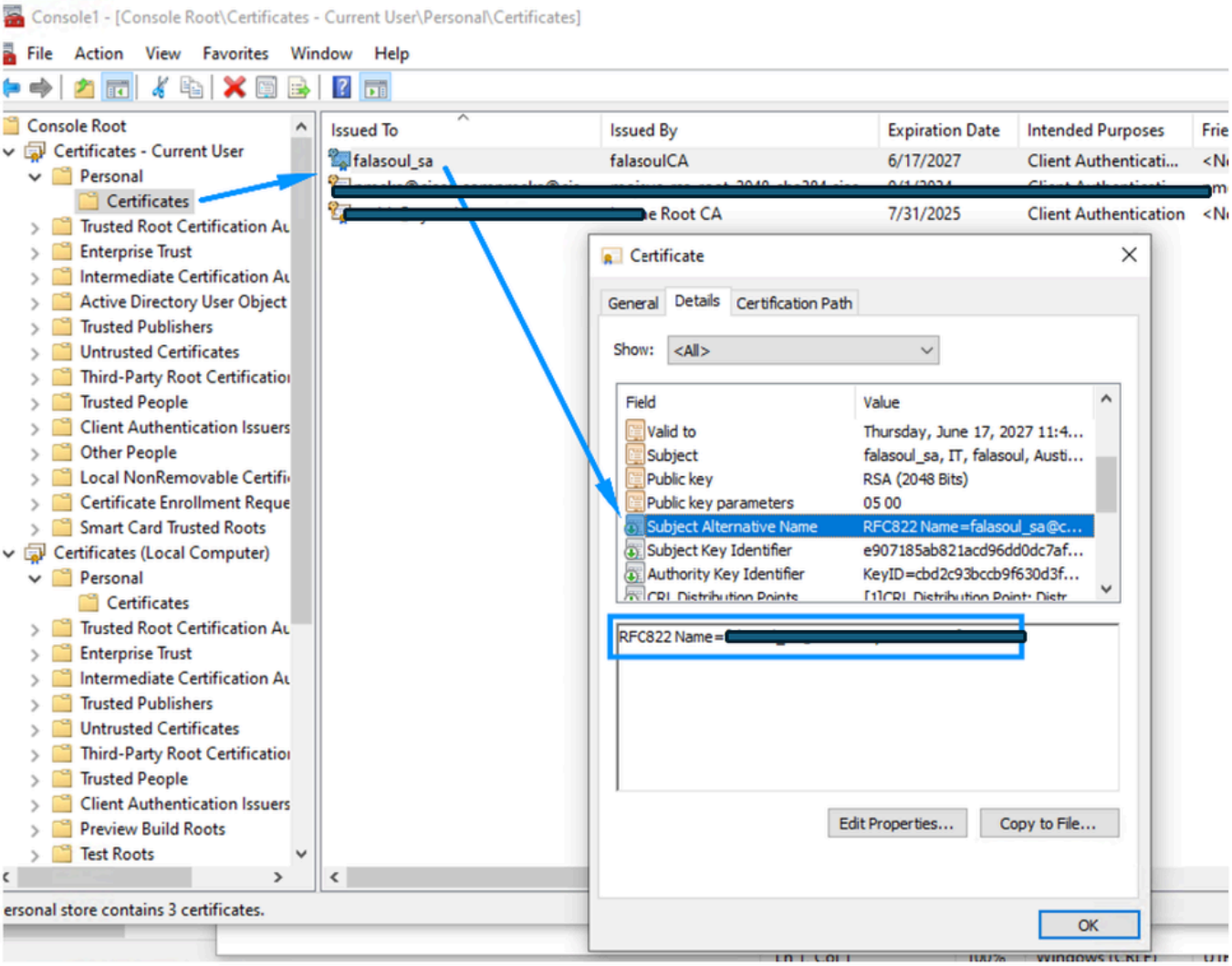
Phase 2: wenden Sie sich an Ihre lokale AD-Signierungsstelle (https:http://<ip-address>/certsrv/).

Schritt 3: Klicken Sie auf Zertifikat anfordern -> Erweiterte Zertifikatanforderung -> wählen Sie die Vorlage ztna-client-enroll aus.



Schritt 4: Laden Sie das Zertifikat im Base64-Format herunter, und installieren Sie es im persönlichen Zertifikat des vertrauenswürdigen Speichers des Benutzers.

Schritt 5: Bestätigen, dass die richtigen Informationen im Zertifikat vorhanden sind

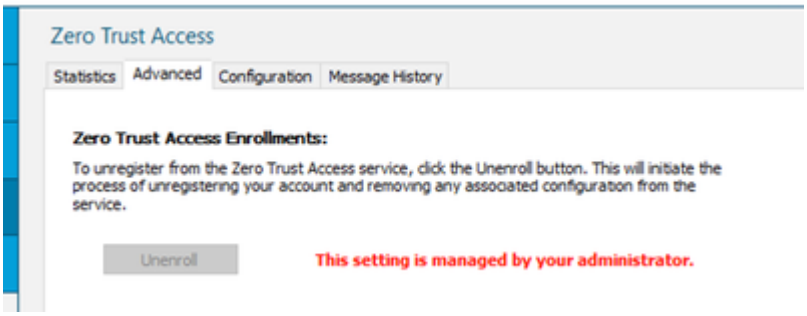


Schritt 6: Starten Sie Ihr ZTNA-Modul neu, damit die Registrierung beginnt.

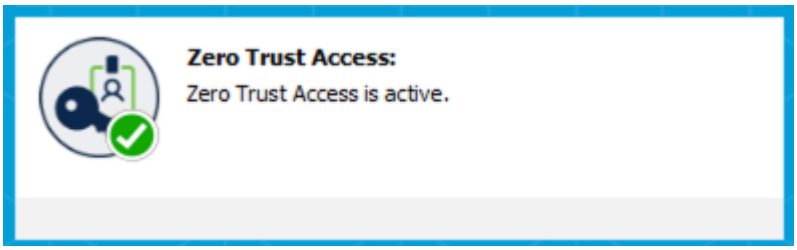
Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

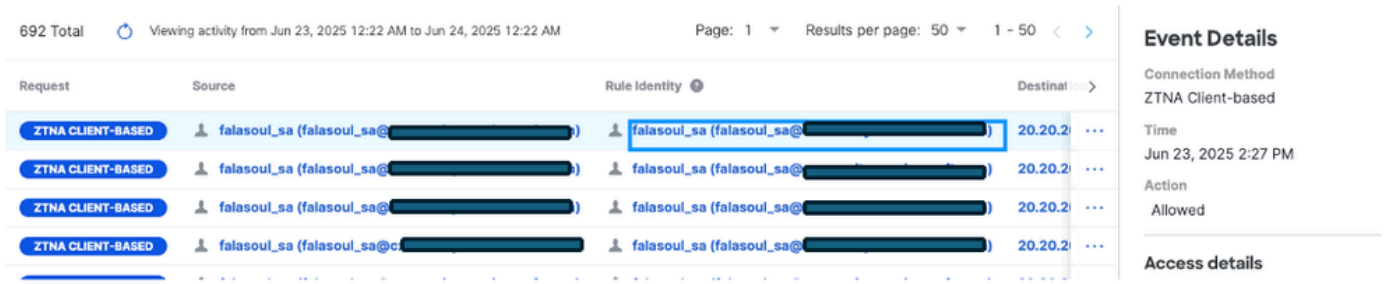
Schritt 1: Meldung des ZTNA-Moduls beim Konfigurieren der Registrierungsauswahldatei:



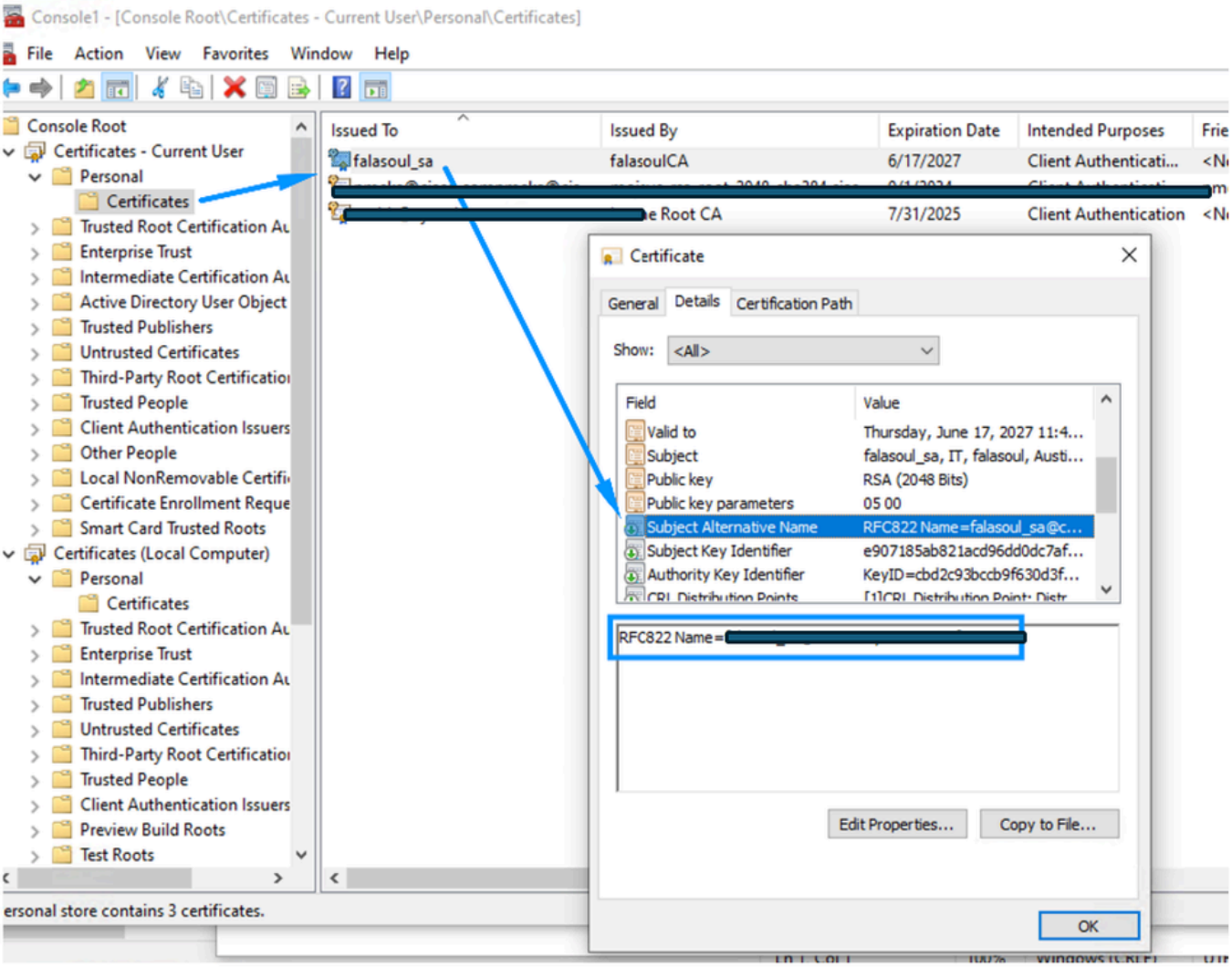
Phase 2: Nachdem Sie das ZTNA-Modul zum ersten Mal neu gestartet haben, können Sie sehen, dass Sie sich automatisch für das ZTNA-Modul angemeldet haben.



Schritt 3: Überprüfen Sie, ob der richtige Benutzer bei der Aktivitätssuche anhand der SAN-Informationen angezeigt wird.



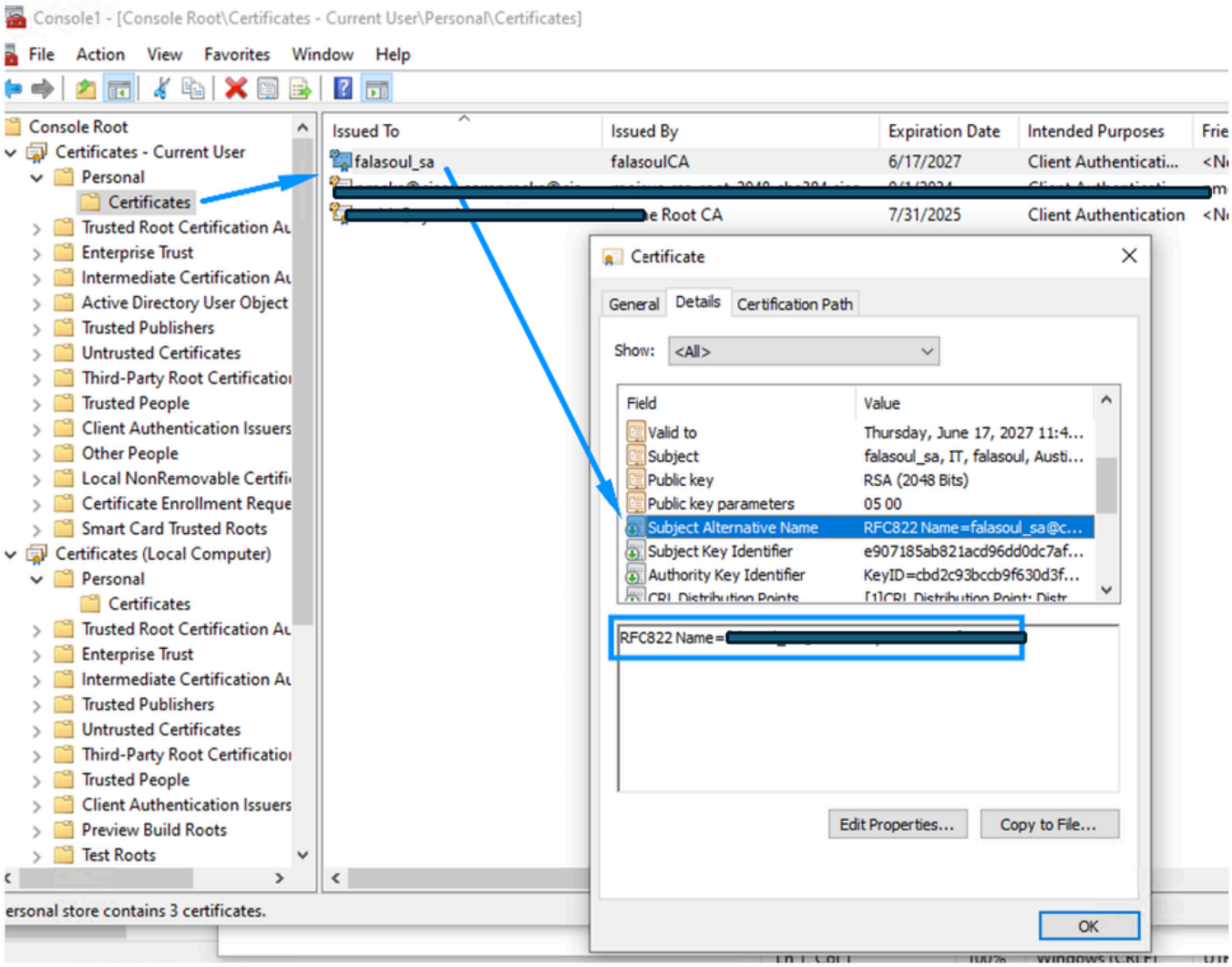
Schritt 4: Bestätigen, dass die richtigen Informationen im Zertifikat vorhanden sind



Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Schritt 1: Bestätigen Sie, dass die richtigen Informationen im Zertifikat vorhanden sind und dass das Zertifikat im richtigen Zertifikatspeicher installiert ist.



Phase 2: Bestätigen Sie, dass die Registrierung für die Zertifikatanforderungen mit DART nicht fehlschlägt.

Schritt 3: Vergewissern Sie sich, dass Sie Ihre externe FTD-Schnittstelle ordnungsgemäß auflösen können, wenn UZTNA verwendet wird.

Häufiger Fehler:

```
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::
```

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.