

# Configure Secure Access ZTNA Auto Enrollment

## Contents

---

## Introduction

This document describes the required steps to configure the ZTNA for Certificate based auto enrollment.

## Prerequisites

- Secure Client minimum version 5.1.9.x
- Trusted Platform Module (TPM) for Windows
- Secure Enclave coprocessor for Apple Devices

## Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Access
- [Enroll Devices in Zero Trust Access Using Certificate](#) Guide Section

## Components Used

The information in this document is based on these software and hardware versions:

- Windows 11 with TPM version 2.0
- Secure Client version 5.1.10.17 with ZTNA and DUO Module Enabled.
- Microsoft Active Directory 2022
- Openssl tool for certificate generation

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. If your network is live, ensure that you understand the potential impact of any command.

## Enabling Auto-Enrollment on Secure Access Dashboard

First step in enabling this feature is to enable the Secure Access Auto-enrollment feature which includes:

1. Navigate to Dashboard -> Connect -> End User Connectivity -> Zero Trust
2. Click on Manage option.

## End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust Access
Virtual Private Network
Internet Security

[Cisco Secure Client](#)
[Manage servers](#)

### Enrollment methods

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. [Help](#)

Windows and macOS devices enroll using: [SSO Authentication](#) [Certificates](#)

Android and iOS devices enroll using SSO Authentication only.

[Manage](#)

### Default Profile

If no other ZTA profile is applied to traffic, the default profile applies. The default profile includes all traffic steering rules that are automatically created when private resources are enabled for client-based zero trust access.

| Name                                | Private Resources | Destination Lists | Last Used  |
|-------------------------------------|-------------------|-------------------|------------|
| <a href="#">Default ZTA Profile</a> | 15                | 1                 | 2025/06/10 |

3. Enable Use Certificates.

4. Upload CA Certificate by downloading it from your local Certificate Authority.

5. Download the Enrollment Configuration and place it in the the directories based on operating system.

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment\_choices

- macOS: /opt/cisco/secureclient/zta/enrollment\_choices

6. Make sure to save your settings once completed.

### Windows and macOS devices

☒ **Use SSO Authentication**  
Enrollment requires user action.

1. Install Cisco Secure Client on user devices.  
2. Give your users instructions for enrolling in Zero Trust Access.

☒ **Use Certificates**  
Enrollment occurs without user action.

#### 1. Upload a CA Certificate if necessary

At least one uploaded root certificate or certificate chain must be able to validate identity certificates on endpoint devices during zero trust enrollment and renewal.

##### CA Certificates

[View 2 CA certificates](#)
[Upload a CA Certificate](#)

#### 2. Download the enrollment configuration file

The file is regenerated each time a new CA certificate is uploaded.  
Deploy this file to user devices.

[Download](#)
ZTA\_Enroll\_Cert.json

You can also download this configuration file and Cisco Secure Client from the [Download Cisco Secure client](#) page.

[Save](#)
[Cancel](#)

## Certificate Template and Installation

Secure Access require these mandatory Certificate Fields:

- Subject Alternative Name (SAN) to include the user RFC-822 compliant email address or User Principle Name (UPN)

Example:

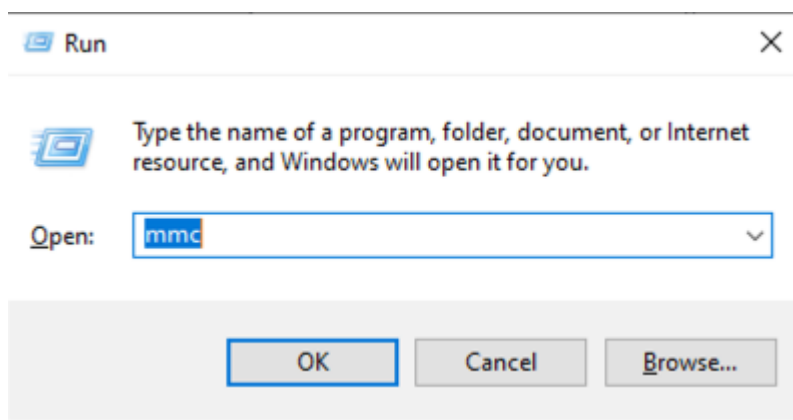
Option 1: RFC822-compliant email  
email.1 = username@domain.local

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

In this example we are using the user certificate template in Microsoft AD to generate the certificate.

Step 1: Navigate to Microsoft AD and open Certificate Manager

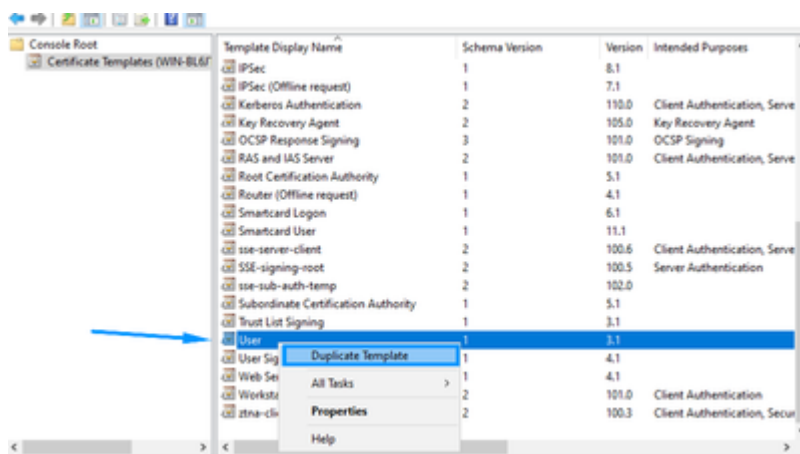
Step 2: Open Run and enter Microsoft Management Console (mmc)



Step 3: Click on File then add/remove Snap-in

Step 4: Add certificate Templates

Step 5: Duplicate User Certificate



Step 6: Configure the settings as described

1. New Template name: ztna-client-enroll under (General) tab.
2. Select (Supply in the request) in (Subject Name) tab.

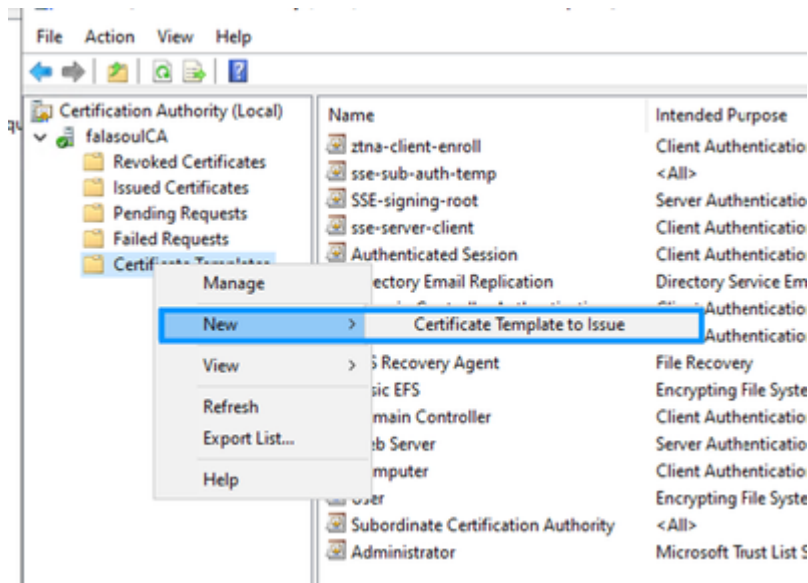


**Note:** This insure that the options provided by the openssl template such as Service Alternative Name (SAN) are accepted

Step 7: Click on OK to save the new template

Step 8: Add the new Template to the AD template list by doing:

1. Run certsrv.msc
2. right click on Certificate Templates and select New -> certificate template to issue
3. Select your newly created template (ztna-client-enroll)



## Creating Certificate using Openssl

Step 1: Create san.cnf file with content

```
[ 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
```

Step 2: create certificate using the template

```
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
```

## Sign user certificate with CA ZTNA Template

Step 1: Copy the content of the file user.csr

Step 2: go to your local AD signing authority (<https://<ip-address>/certsrv/>)

Step 3: Click on Request a Certificate -> Advanced Certificate Request -> select ztna-client-enroll template

**Saved Request:**

|                                                                               |                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Base-64-encoded<br>certificate request<br>(CMC or<br>PKCS #10 or<br>PKCS #7): | /Ks79kDXdxW44Xsnk21Q/fVnLlrv94qlQ7NiQRBFER-<br>KVlvAoICCG4VTduA7Vjwd08YUDb5jpkPmYexqnLX4M<br>xrjxHMWolU5uVatM5dmhQ74nrxrhud60nso3rFQJA92d<br>TjtUDuocyYMP24V8ycu/Qso717NPw/4n1k7vhdM0Sq<br>7rygRiDNj5eVI89Pt6J20Do0scK5WiHi+Bx38ieSZ<br>-----END CERTIFICATE REQUEST----- |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Certificate Template:**

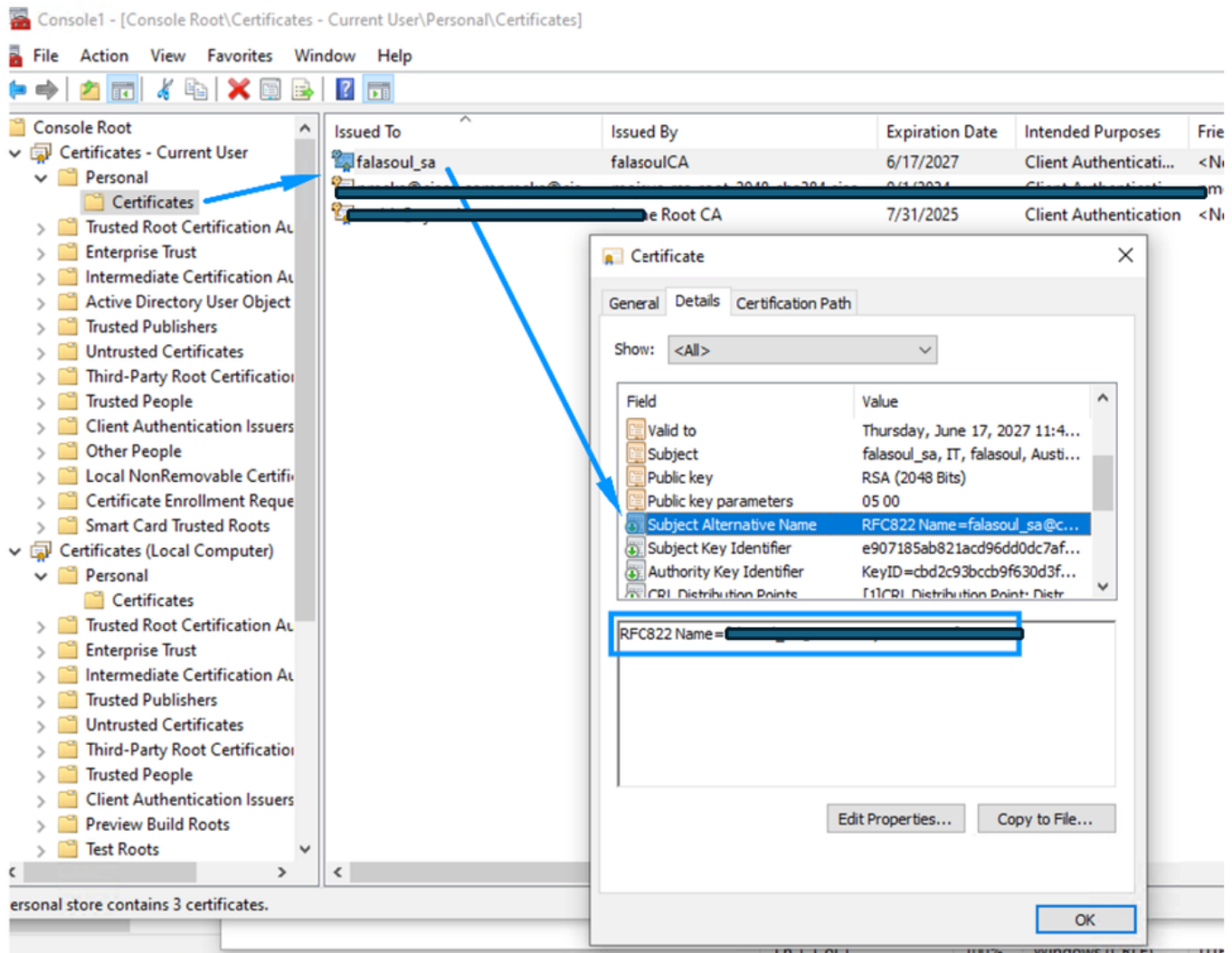
ztna-client-enroll

**Additional Attributes:**

Attributes:

Step 4: Download the certificate in Base64 format and install in the user personal trusted store certificate.

Step 5: Confirm the right information exists in the certificate

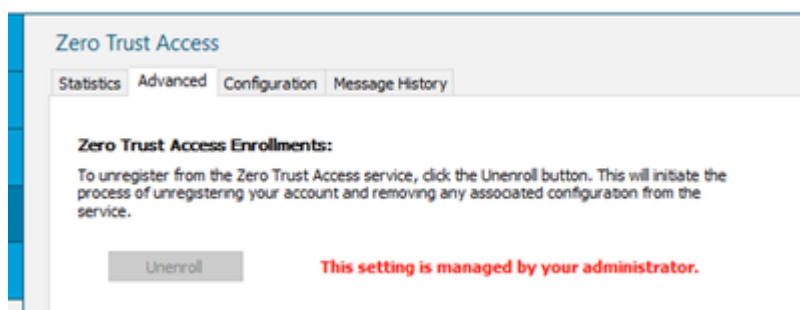


Step 6: Restart your ZTNA Module for the enrollment to start

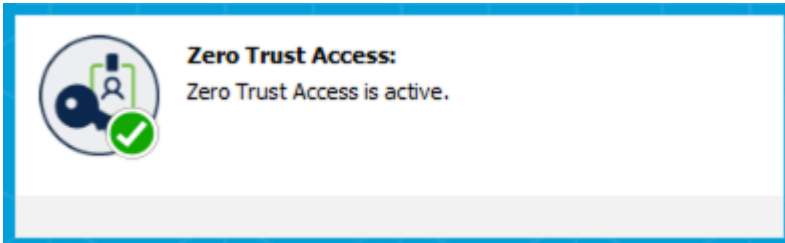
## Verify

Use this section to confirm that your configuration works properly.

Step 1: ZTNA Module message when configuring the enrollment choices file:



Step 2: After restarting the ZTNA Module for the first time you can see that you are auto-enrolled into ZTNA

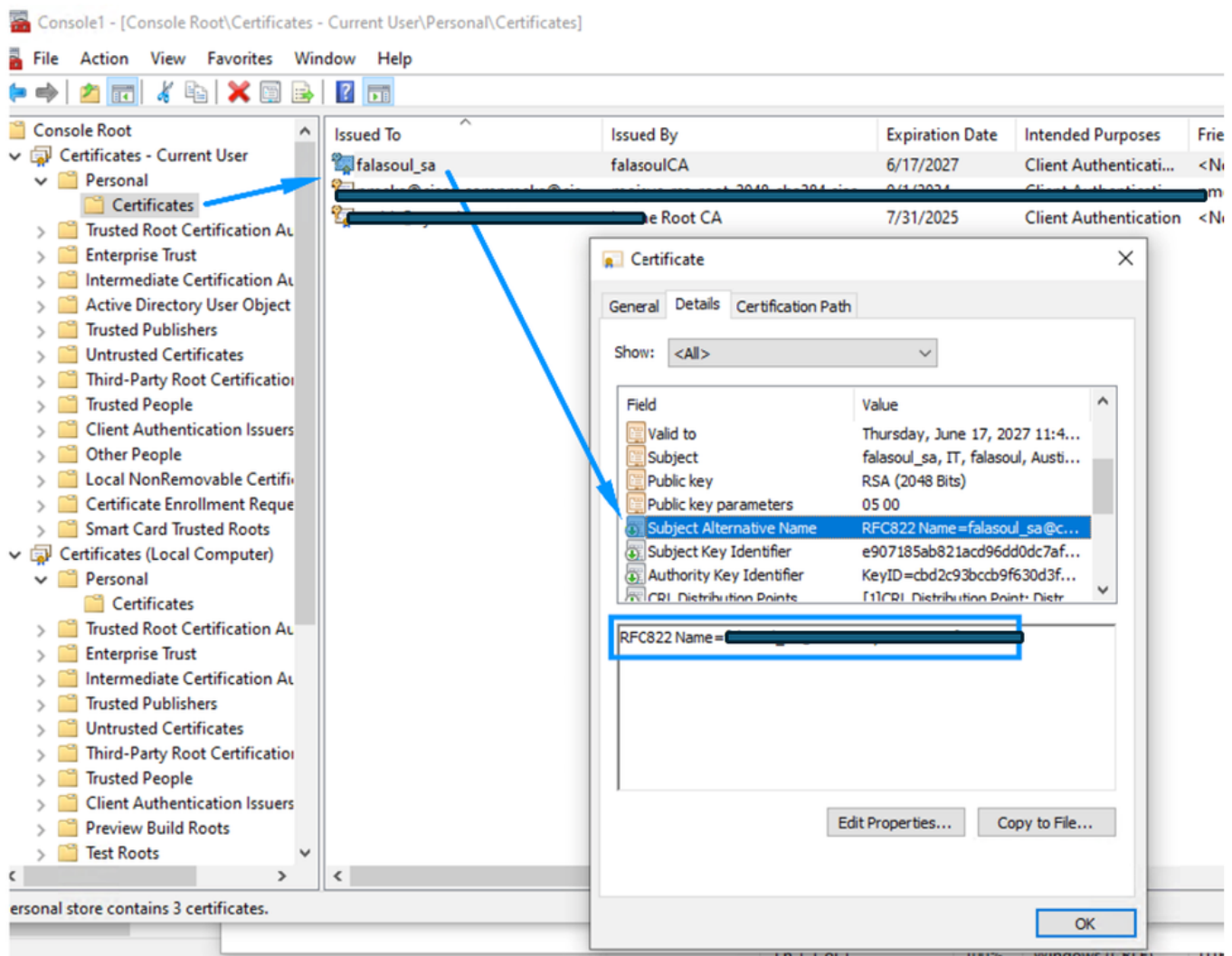


Step 3: Verify the right user showing up in activity search based on the SAN information

| 692 Total         | Viewing activity from Jun 23, 2025 12:22 AM to Jun 24, 2025 12:22 AM | Page: 1                       | Results per page: 50 | 1 - 50 |
|-------------------|----------------------------------------------------------------------|-------------------------------|----------------------|--------|
| Request           | Source                                                               | Rule Identity                 | Destination          |        |
| ZTNA CLIENT-BASED | falasoul_sa (falasoul_sa@...)                                        | falasoul_sa (falasoul_sa@...) | 20.20.2...           | ...    |
| ZTNA CLIENT-BASED | falasoul_sa (falasoul_sa@...)                                        | falasoul_sa (falasoul_sa@...) | 20.20.2...           | ...    |
| ZTNA CLIENT-BASED | falasoul_sa (falasoul_sa@...)                                        | falasoul_sa (falasoul_sa@...) | 20.20.2...           | ...    |
| ZTNA CLIENT-BASED | falasoul_sa (falasoul_sa@c...)                                       | falasoul_sa (falasoul_sa@...) | 20.20.2...           | ...    |

**Event Details**  
Connection Method  
ZTNA Client-based  
Time  
Jun 23, 2025 2:27 PM  
Action  
Allowed  
**Access details**

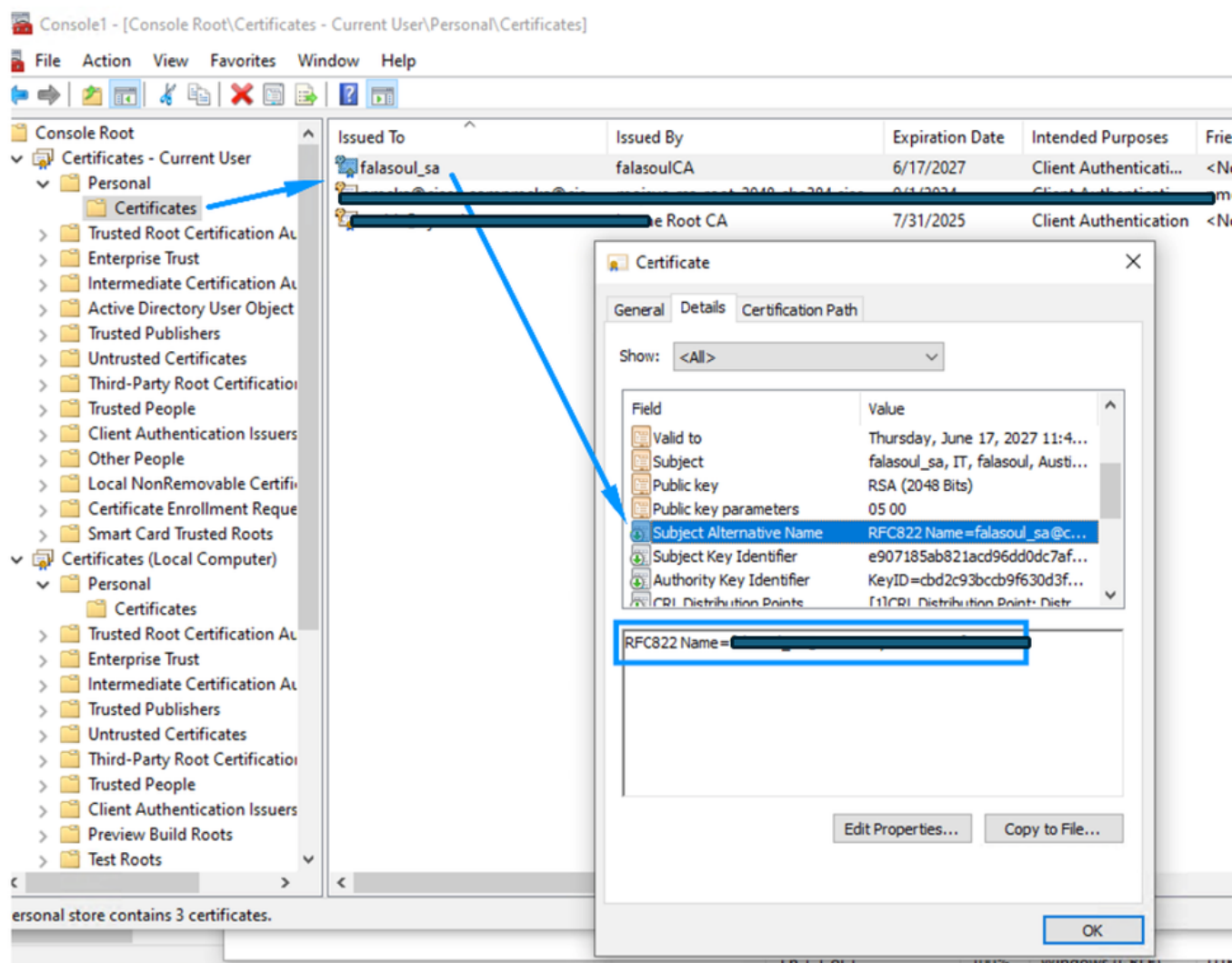
Step 4: Confirm the right information exists in the certificate



## Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Step 1: Confirm the right information exists in the certificate and its installed in the right certificate store.



Step 2: Confirm that enrollment is not failing on certificate requirements using DART

Step 3: Confirm you are able to resolve your FTD outside interface properly if UZTNA is being used.

**common error:**

```
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x000000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x000000e58] T/ AppSocketTransport.cpp:231 AppSocket
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x000000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x000000e58] I/ TcpTransport.cpp:114 TcpTransport::
2025-06-16 05:44:45.609237 csc_zta_agent[0x00001638, 0x000000e58] T/ NetworkTransportStateTracker.cpp:11
2025-06-16 05:44:45.610238 csc_zta_agent[0x00001638, 0x000000e58] T/ TcpTransport.cpp:150 TcpTransport::
2025-06-16 05:44:45.610238 csc_zta_agent[0x00001638, 0x000000e58] E/ TcpTransport.cpp:166 TcpTransport::
```

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)