

보안 액세스 ZTNA 자동 등록 구성

목차

소개

이 문서에서는 인증서 기반 자동 등록을 위해 ZTNA를 구성하는 데 필요한 단계를 설명합니다.

사전 요구 사항

- Secure Client 최소 버전 5.1.9.x
- Windows용 TPM(신뢰할 수 있는 플랫폼 모듈)
- Apple 디바이스용 Secure Enclave 코프로세서

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 액세스
- [인증서 가이드 섹션을 사용하여 제로 트러스트 액세스에 디바이스 등록](#)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows 11(TPM 버전 2.0 포함)
- ZTNA 및 DUO 모듈이 활성화된 Secure Client 버전 5.1.10.17
- Microsoft Active Directory 2022
- 인증서 생성을 위한 Openssl 툴

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Secure Access Dashboard에서 자동 등록 활성화

이 기능을 활성화하는 첫 번째 단계는 다음과 같은 보안 액세스 자동 등록 기능을 활성화하는 것입니다.

1. Dashboard(대시보드) -> Connect(연결) -> End User Connectivity(최종 사용자 연결) -> Zero Trust(제로 신뢰)로 이동합니다.

2. 관리 옵션을 클릭합니다.

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

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
Default ZTA Profile	15	1	2025/06/10

3. 인증서 사용을 활성화합니다.

4. 로컬 인증 기관에서 CA 인증서를 다운로드하여 업로드합니다.

5. 등록 구성을 다운로드하고 운영 체제에 따라 디렉토리에 배치합니다.

-창: C:\ProgramData\Cisco\Cisco 보안 클라이언트\ZTA\enrollment_choices

- macOS: /opt/cisco/secureclient/zta/enrollment_choices

6. 설정이 완료되면 저장해야 합니다.

Windows and macOS devices

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

☒ **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

인증서 템플릿 및 설치

보안 액세스에는 다음과 같은 필수 인증서 필드가 필요합니다.

- 사용자 RFC-822 불만 이메일 주소 또는 UPN(User Principal Name)을 포함하는 주체 대체 이름 (SAN)

예:

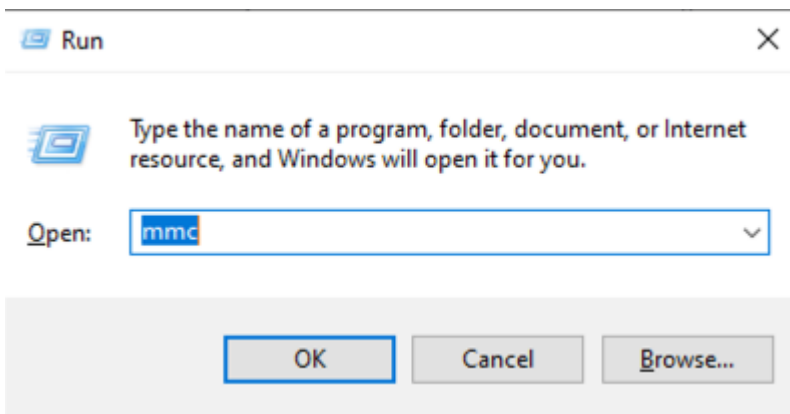
옵션 1: RFC822 호환 이메일
email.1 = username@domain.local

옵션 2: (대체): UPN(Microsoft 전용)
기타 이름:1.3.6.1.4.1.311.20.2.3;UTF8:username@domain.local

이 예에서는 Microsoft AD의 사용자 인증서 템플릿을 사용하여 인증서를 생성합니다.

1단계: Microsoft AD로 이동하여 Certificate Manager를 엽니다

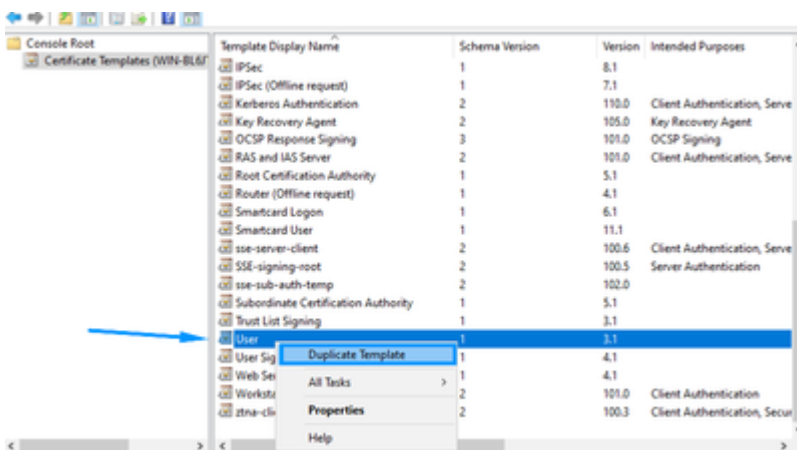
2단계: 실행을 열고 mmc(Microsoft Management Console)를 입력합니다.



3단계: File(파일)을 클릭한 다음 Snap-in 추가/제거

4단계: 인증서 템플릿 추가

5단계: 중복 사용자 인증서



6단계: 설명된 대로 설정을 구성합니다

1. 새 템플릿 이름: (General)(일반) 탭에 있는 ztna-client-enroll(ztna-client-enroll)
2. (Subject Name) 탭에서 (Supply in the request)를 선택합니다.

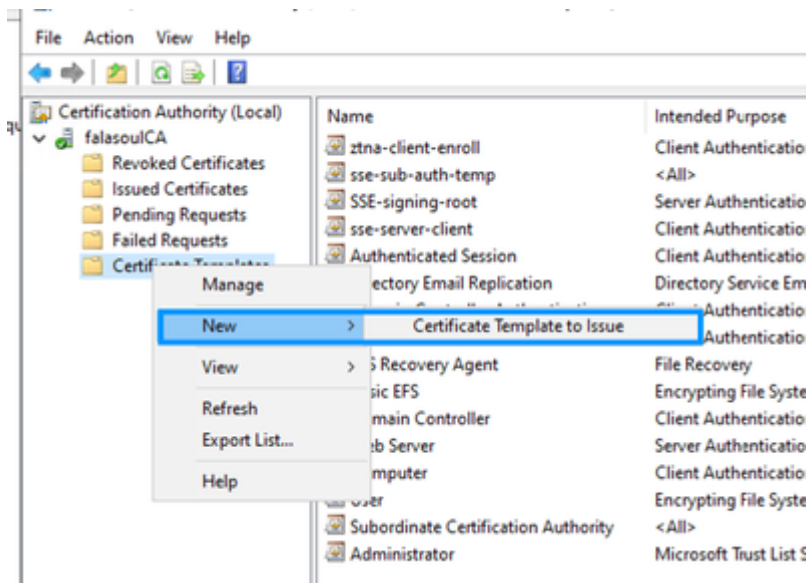


참고: 이렇게 하면 SAN(Service Alternative Name)과 같은 openssl 템플릿에서 제공하는 옵션이 수락됩니다

7단계: OK(확인)를 클릭하여 새 템플릿을 저장합니다

8단계: 다음을 수행하여 AD 템플릿 목록에 새 템플릿을 추가합니다.

1. certsrv.msc를 실행합니다
2. Certificate Templates(인증서 템플릿)를 마우스 오른쪽 버튼으로 클릭하고 New(새로 만들기) -> certificate template to issue(인증서 템플릿)를 선택합니다.
3. 새로 생성한 템플릿을 선택합니다(ztna-client-enroll).



Openssl을 사용하여 인증서 생성

1단계: 콘텐츠로 san.cnf 파일 만들기

```
[ 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
```

2단계: 템플릿을 사용하여 인증서 생성

```
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
```

CA ZTNA 템플릿으로 사용자 인증서 서명

1단계: user.csr 파일의 내용을 복사합니다.

2단계: 로컬 AD 서명 기관(<https://<ip-address>/certsrv/>)으로 이동합니다.

3단계: Request a Certificate(인증서 요청) -> Advanced Certificate Request(고급 인증서 요청) -> select ztna-client-enroll template(ztna-client-enroll 템플릿 선택)을 클릭합니다.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
/Ks79kDXdxW44Xsnk21Q/fVnLlrv94q1Q7NiQRBFER-
KVlvAoICCG4VTduA7Vjwd08YUDb5jpkPmYexgnLX4M
xrjxHMWou5uVAtM5dmhQ74nxrhud60nso3rFQJA92d,
TjtUDuocyYMP24V8ycu/Qso717NPw/4n1k7vhdM0Sq
7rygRiDNj5eVId89Pt6J20Do0scK5WjHi+Bx38ieSZ
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

ztna-client-enroll

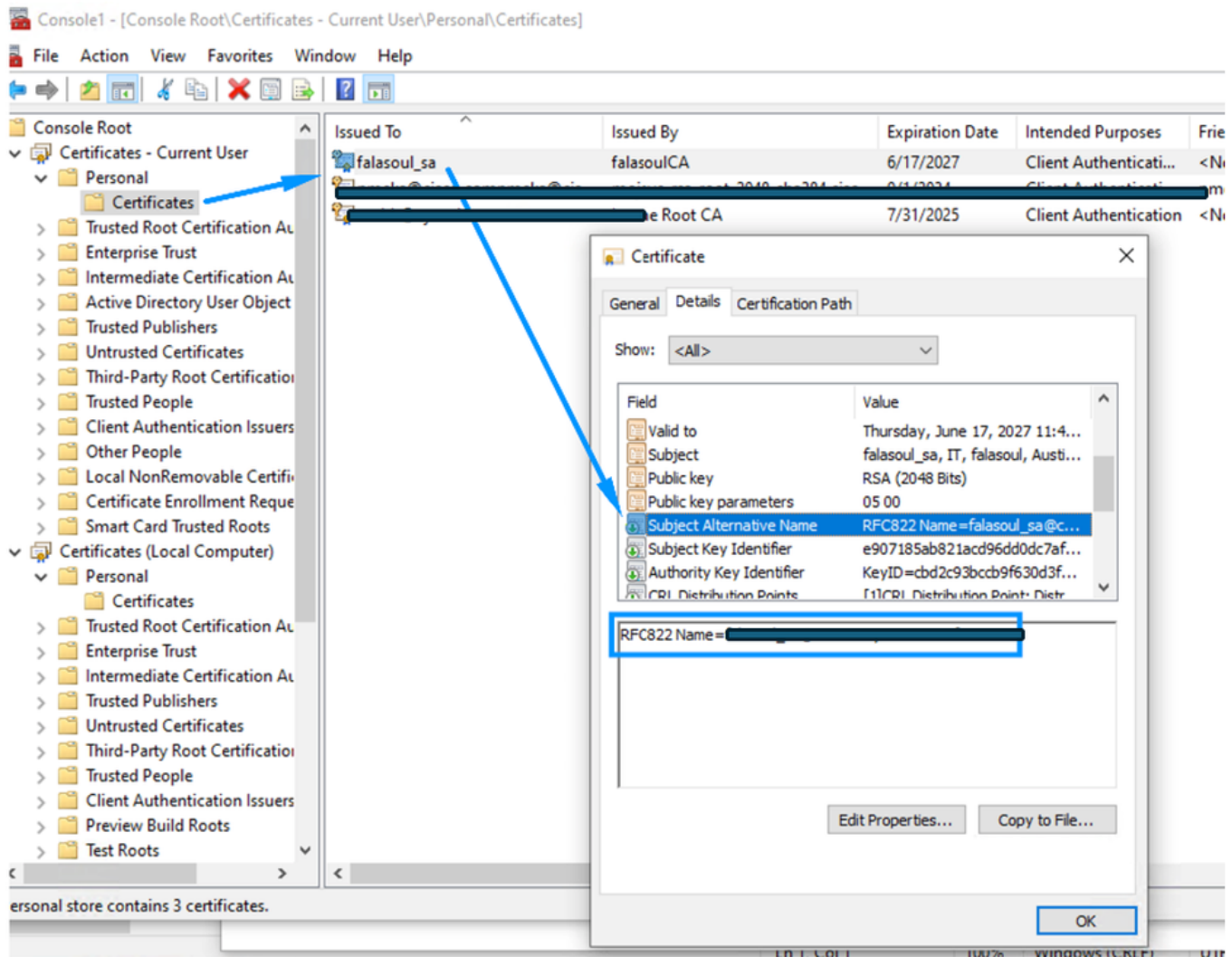
Additional Attributes:

Attributes:

Submit >

4단계: Base64 형식의 인증서를 다운로드하고 사용자 개인 신뢰 저장소 인증서에 설치합니다.

5단계: 인증서에 올바른 정보가 있는지 확인합니다.

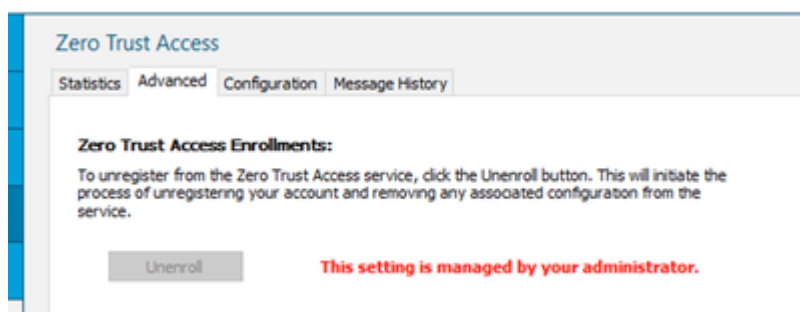


6단계: 등록을 시작하려면 ZTNA 모듈을 다시 시작하십시오.

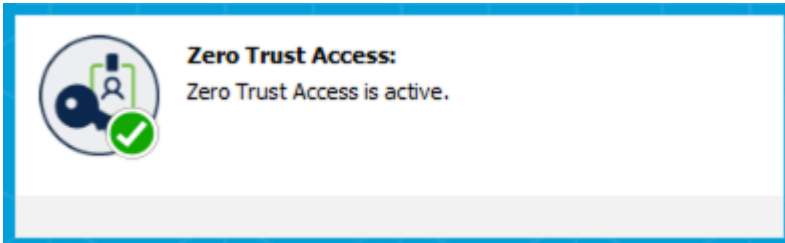
다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계: 등록 선택 파일을 구성할 때 ZTNA 모듈 메시지:



2단계: ZTNA 모듈을 처음 재시작한 후에는 ZTNA에 자동 등록되었음을 확인할 수 있습니다

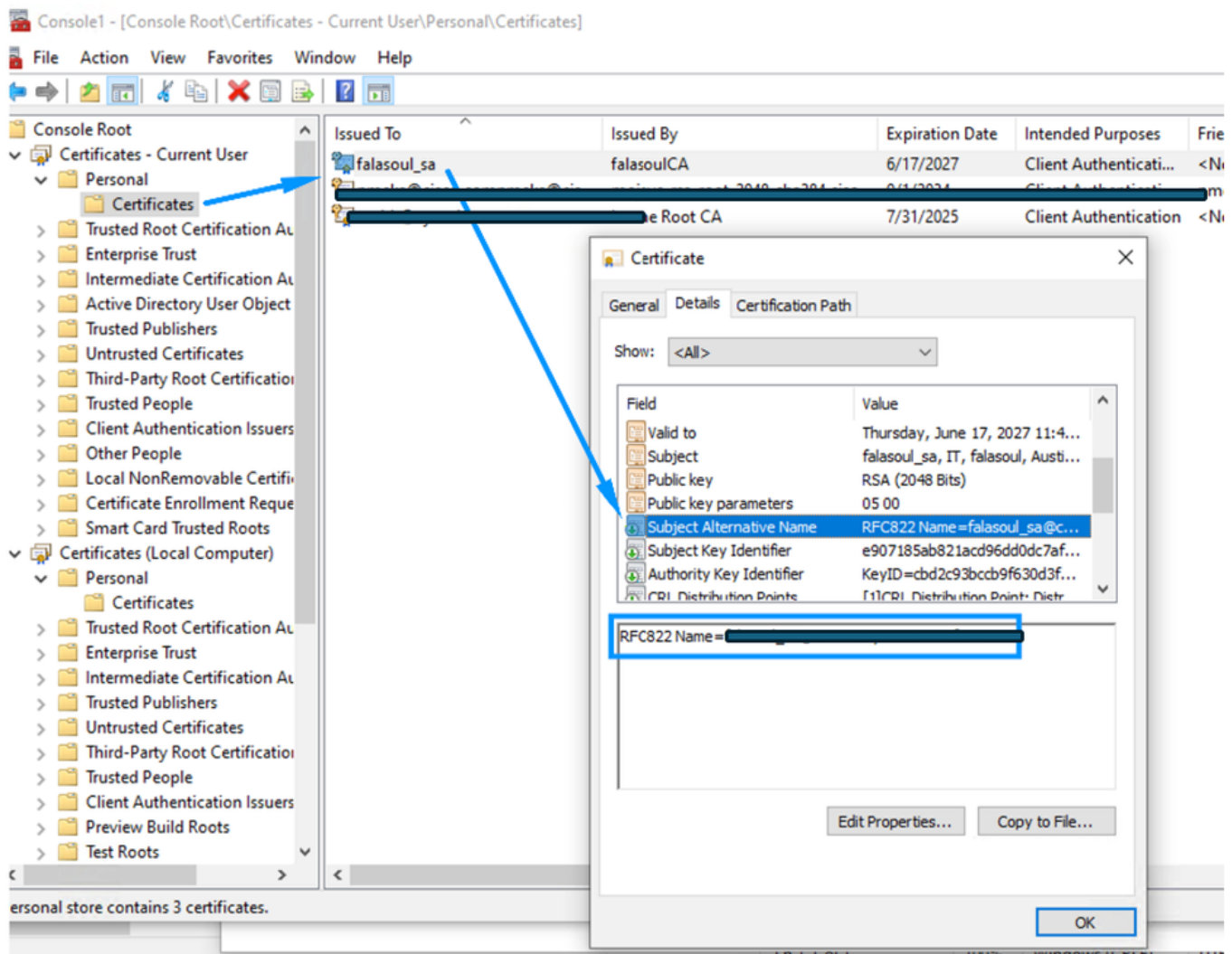


3단계: SAN 정보를 기반으로 활동 검색에 표시되는 올바른 사용자를 확인합니다.

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

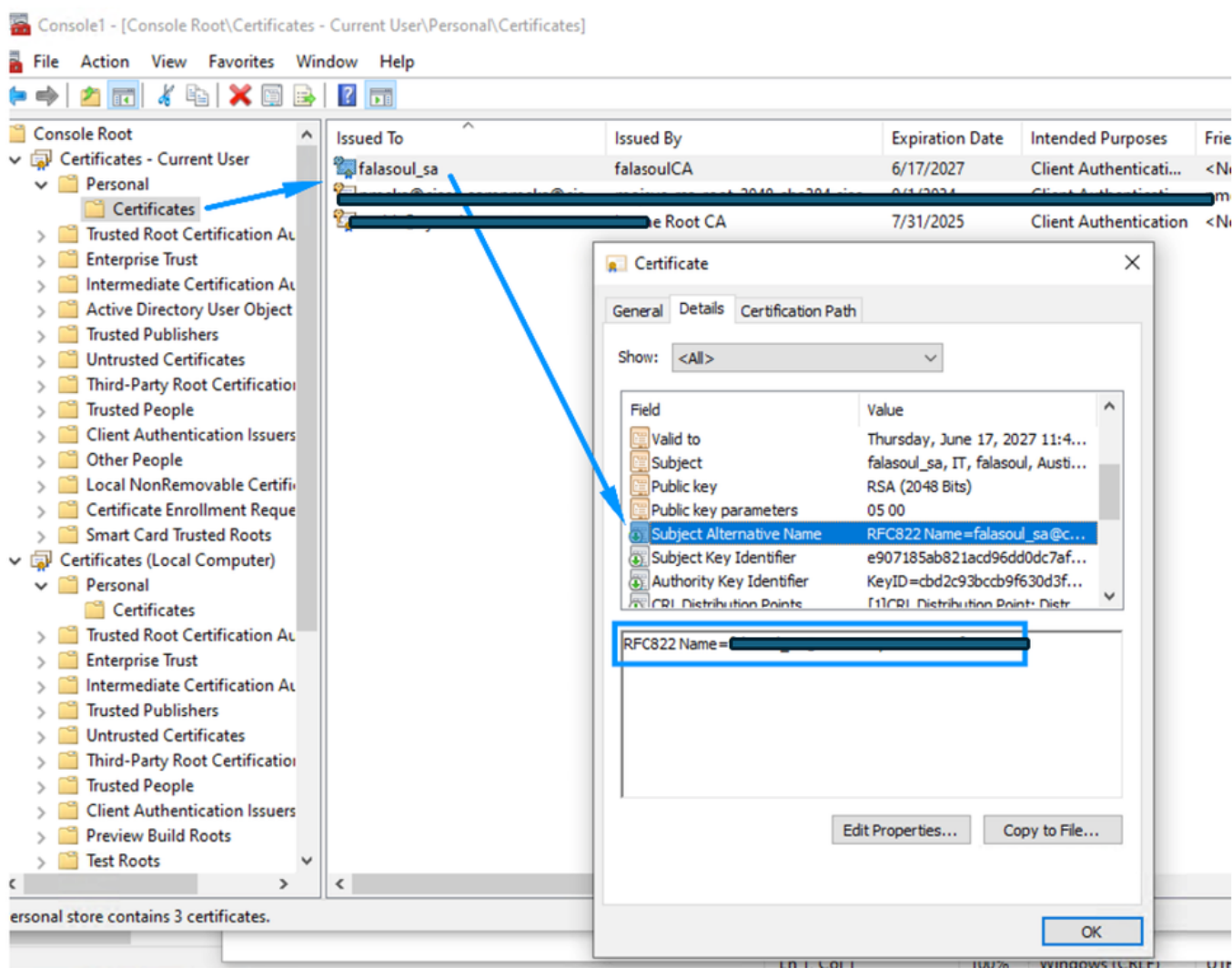
4단계: 인증서에 올바른 정보가 있는지 확인합니다.



문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

1단계: 올바른 정보가 인증서에 있으며 올바른 인증서 저장소에 설치되어 있는지 확인합니다.



2단계: DART를 사용한 인증서 요구 사항에 대해 등록이 실패하지 않는지 확인합니다.

3단계: UZTNA를 사용 중인 경우 FTD 외부 인터페이스를 올바르게 확인할 수 있는지 확인합니다.

일반 오류:

```
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 AppSocket
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::
```

관련 정보

- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.