

配置安全訪問ZTNA自動註冊

目錄

簡介

本文檔介紹為基於證書的自動註冊配置ZTNA所需的步驟。

必要條件

- 安全客戶端最低版本5.1.9.x
- 適用於Windows的受信任平台模組(TPM)
- 適用於Apple裝置的安全群落協處理器

需求

思科建議您瞭解以下主題：

- Cisco Secure Access
- [「使用證書指南註冊零信任訪問中的裝置」](#) 部分

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- TPM版本2.0的Windows 11
- 啟用ZTNA和DUO模組的安全客戶端版本5.1.10.17。
- Microsoft Active Directory 2022
- 用於生成證書的Openssl工具

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

在Secure Access控制面板上啟用自動註冊

啟用此功能的第一步是啟用安全訪問自動註冊功能，包括：

1. 導航到控制面板 — >連線 — >終端使用者連線 — >零信任
2. 按一下管理選項。

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](#)

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

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.啟用「使用證書」。

4.從本地證書頒發機構下載CA證書，以上載該證書。

5.下載註冊配置，並將其放在基於作業系統的目錄中。

-Windows:C:\ProgramData\Cisco\Cisco安全客戶端\ZTA\enrollment_choices

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

6.確保在完成之後儲存設定。

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](#)

證書模板和安裝

安全訪問需要以下必填的證書欄位：

— 主題備用名稱(SAN)，包括使用者RFC-822投訴電子郵件地址或使用者主體名稱(UPN)

範例：

選項 1:符合RFC822標準的電子郵件

email.1 = username@domain.local

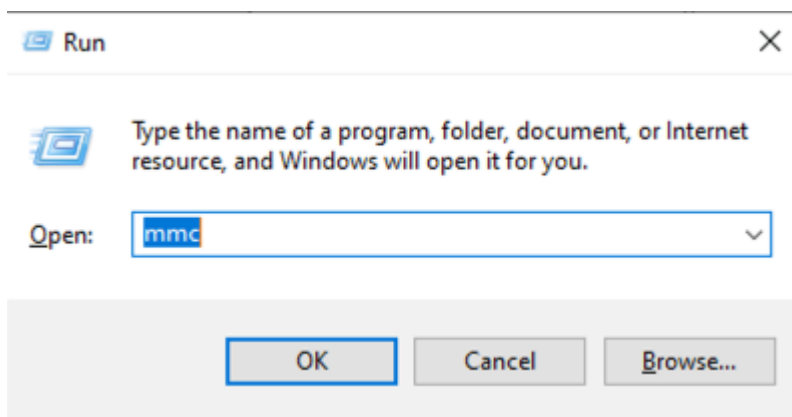
選項 2: (備選)：UPN (特定於Microsoft)

otherName:1.3.6.1.4.1.311.20.2.3;UTF8:username@domain.local

在本示例中，我們使用Microsoft AD中的使用者證書模板生成證書。

步驟 1:導航到Microsoft AD並開啟證書管理器

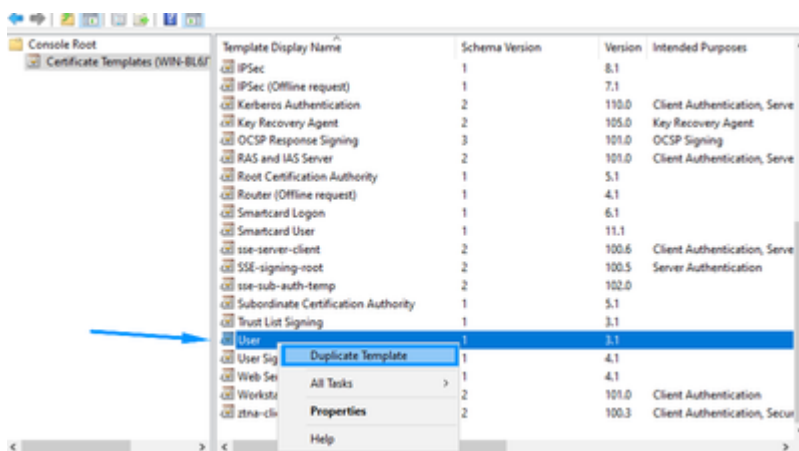
步驟 2:開啟「運行」並輸入Microsoft Management Console(mmc)



步驟 3:按一下「檔案」，然後新增/刪除管理單元

步驟 4:新增證書模板

步驟 5:重複的使用者證書



步驟 6:按所述配置設定

1.新模板名稱：ztna-client-enroll下的(General)頁籤。

2.在 (主題名稱) 標籤中選擇 (在請求中提供) 。



附註：這可確保接受openssl模板提供的選項，例如服務替代名稱(SAN)

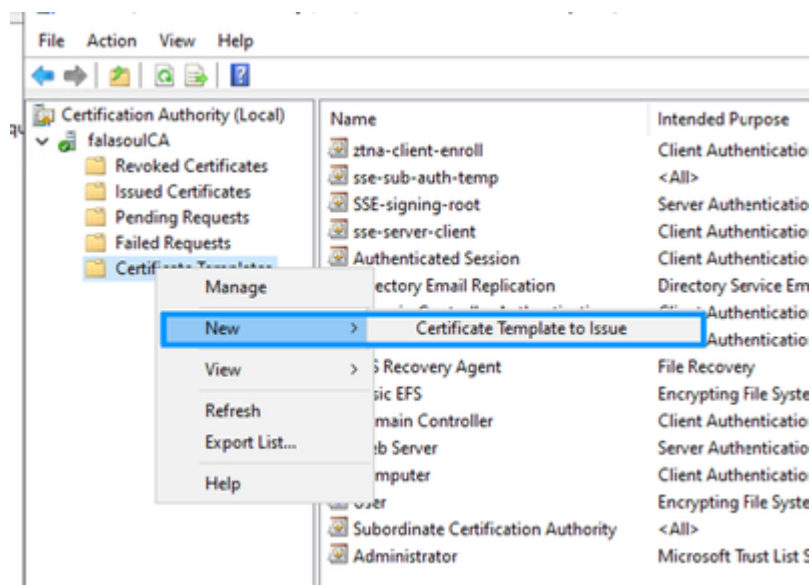
步驟 7:按一下「確定」(OK)儲存新模板

步驟 8:通過以下操作將新模板新增到AD模板清單：

1.運行certsrv.msc

2.按一下右鍵「證書模板」，然後選擇「新建」—>要頒發的證書模板

3.選擇新建立的模板(ztna-client-enroll)



使用Openssl建立憑證

步驟 1:建立包含內容的san.cnf檔案

```
[ 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
```

步驟 2:使用模板建立證書

```
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
```

使用CA ZTNA模板簽署使用者證書

步驟 1:複製檔案user.csr的內容

步驟 2:轉到您的本地AD簽名授權(<https://<ip-address>/certsrv/>)

步驟 3:點選Request a Certificate -> Advanced Certificate Request -> select ztna-client-enroll template

Saved Request:

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

```
/Ks79kDXdxW44Xsnk21Q/fVnLlrv94q1Q7NiQRBFER-
KVlvAoICCG4VTduA7Vjwd08YUDb5jpkPmYexqnLX4M
xrixHMWou5uVatM5dmhQ74nxrhud60nso3rFQJA92d
TjtUDuocyYMP24V8ycu/Qso717NPw/4n1k7vhdM0Sq
7rygRiDNj5eVId89Pt6J20Do0scK5WjHi+Bx38ieSZ
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

ztna-client-enroll

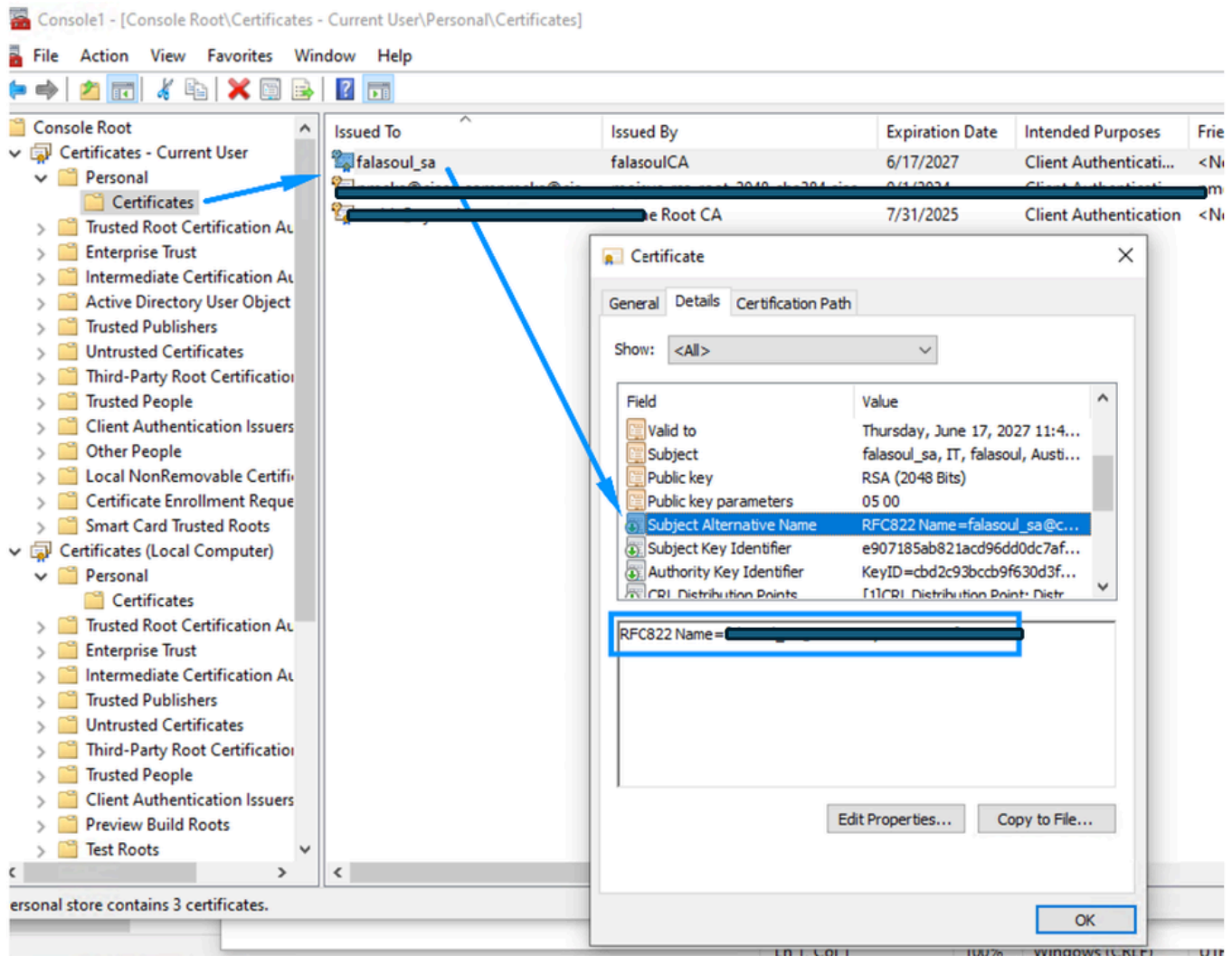
Additional Attributes:

Attributes:

Submit >

步驟 4:下載Base64格式的證書，然後安裝在使用者個人信任儲存證書中。

步驟 5:確認證書中存在正確的資訊

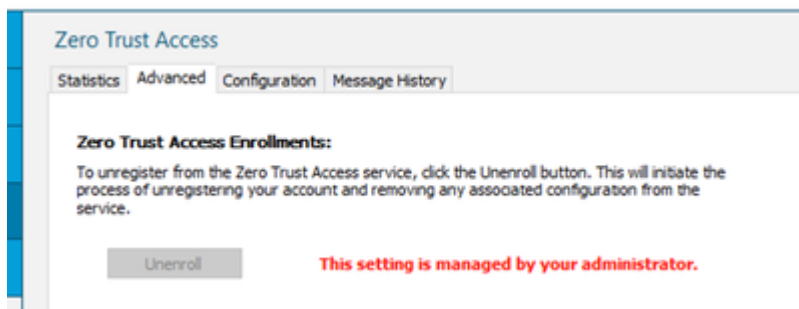


步驟 6:重新啟動ZTNA模組以開始註冊

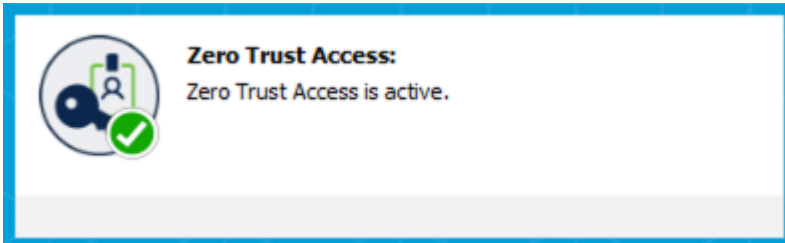
驗證

使用本節內容，確認您的組態是否正常運作。

步驟 1:配置註冊選擇檔案時出現ZTNA模組消息：



步驟 2:首次重新啟動ZTNA模組後，您可以看到您已自動註冊到ZTNA

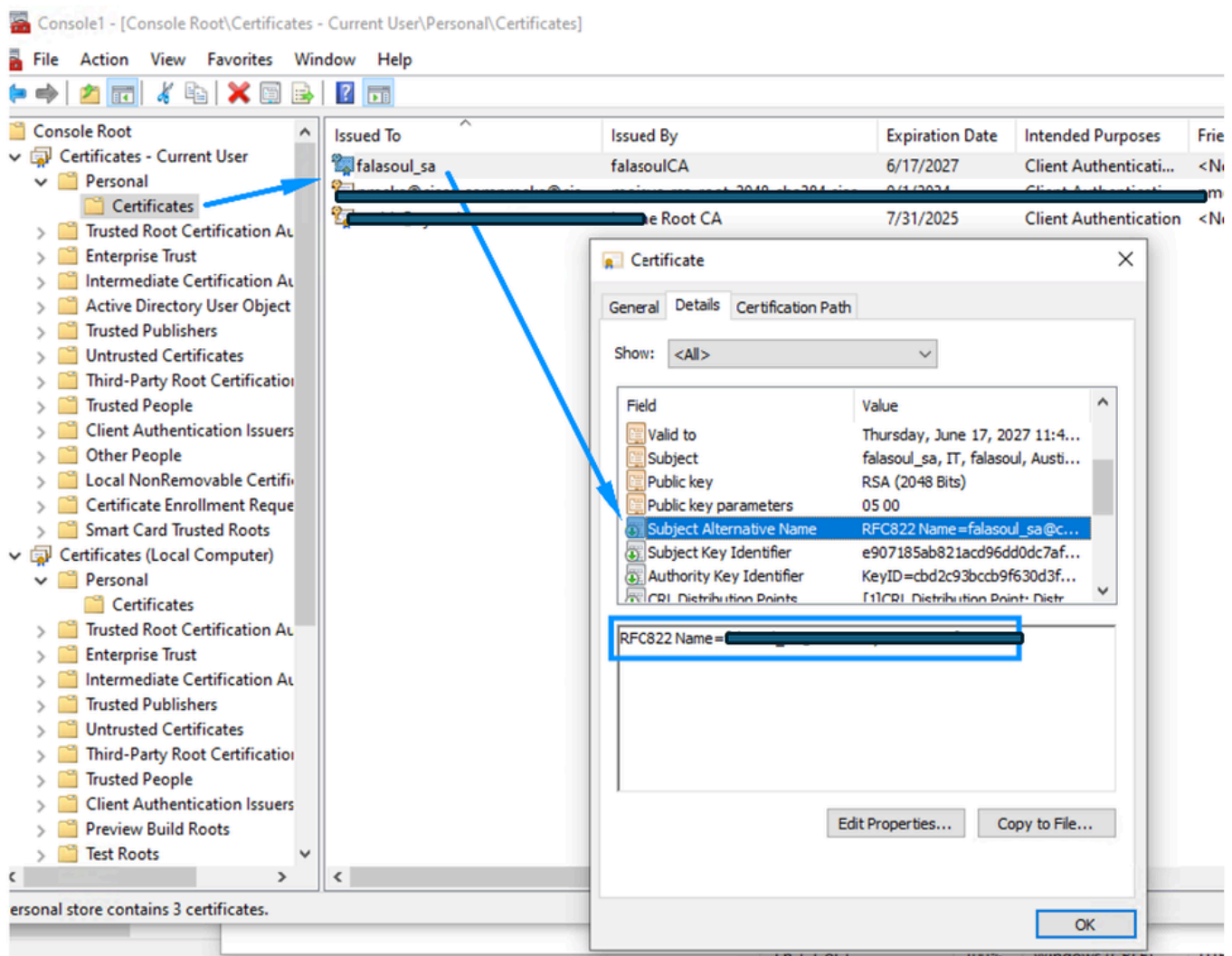


步驟 3:根據SAN資訊驗證活動搜尋中顯示的正確使用者

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

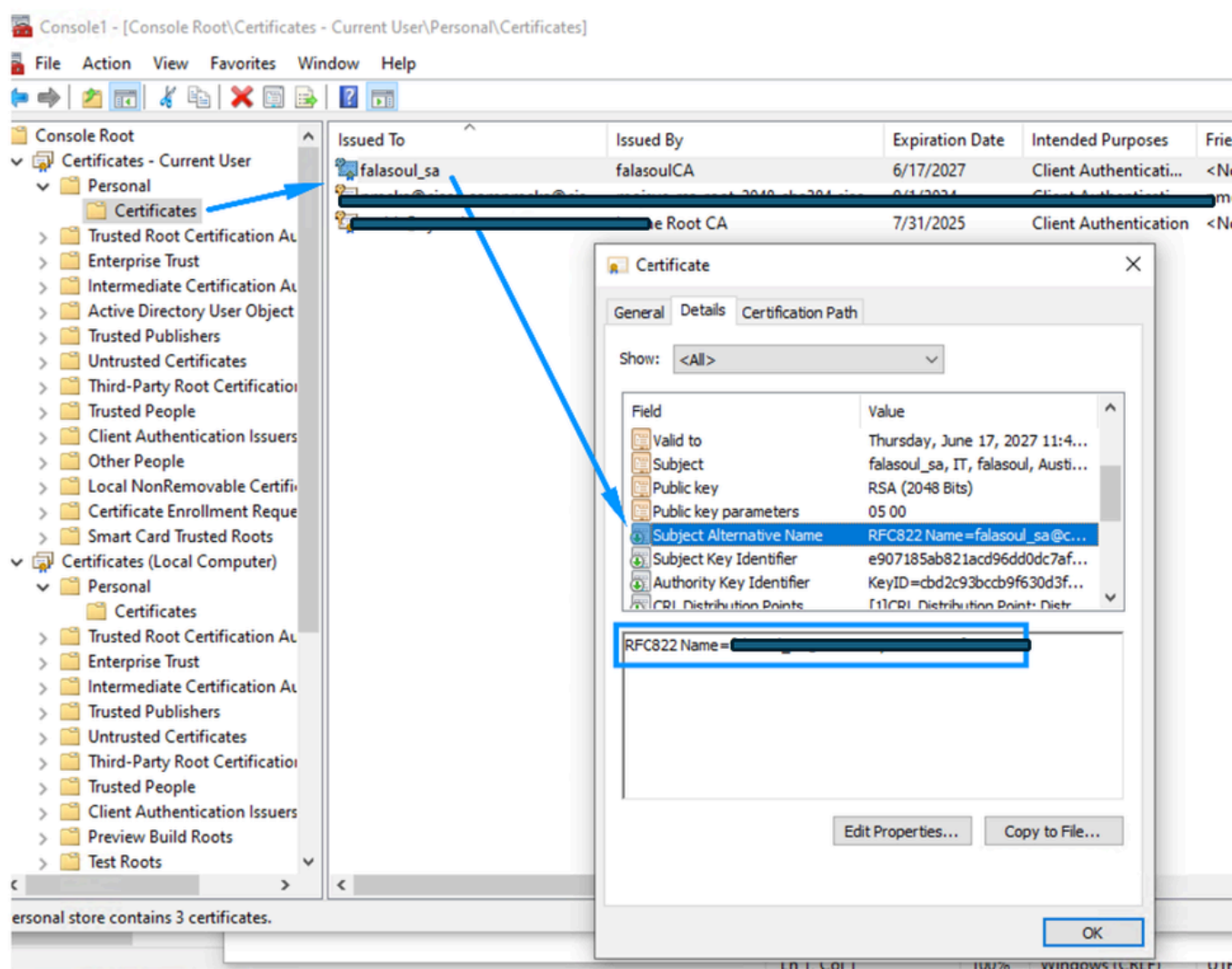
步驟 4:確認證書中存在正確的資訊



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

步驟 1: 確認證書中存在正確的資訊，並將其安裝在正確的證書儲存中。



步驟 2: 使用DART確認註冊未因證書要求而失敗

步驟 3: 確認使用UZTNA時能夠正確解析FTD外部介面。

常見錯誤：

```
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::
```

相關資訊

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。