配置安全访问ZTNA自动注册

目录

简介

本文档介绍为基于证书的自动注册配置ZTNA所需的步骤。

先决条件

— 安全客户端最低版本5.1.9.x

— 适用于Windows的受信任平台模块(TPM)

— 适用于Apple设备的安全群落协处理器

要求

Cisco 建议您了解以下主题：

- 思科安全访问
- 使用证书指南注册零信任访问的设备

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 具有TPM 2.0版的Windows 11
- 启用ZTNA和DUO模块的安全客户端5.1.10.17版。
- Microsoft Active Directory 2022
- 用于生成证书的Openssl工具

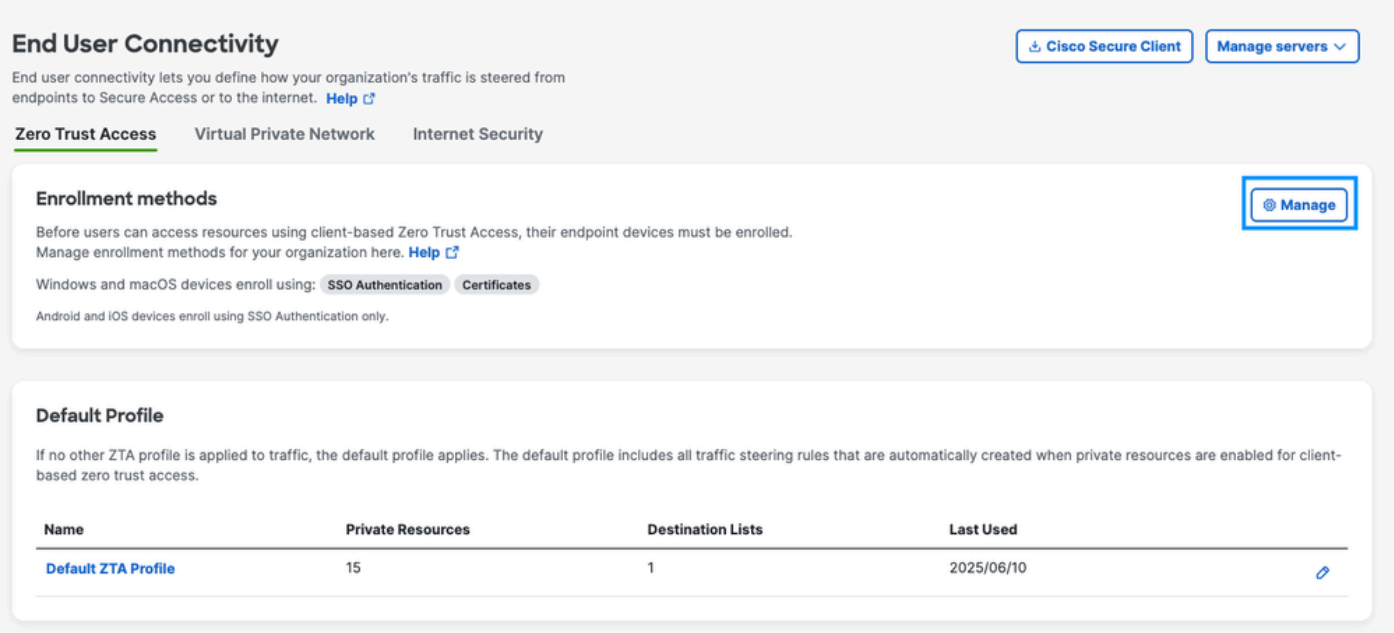
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

在安全访问控制面板上启用自动注册

启用此功能的第一步是启用安全访问自动注册功能，包括：

1.导航至“控制面板” — >“连接” — >“最终用户连接” — >“零信任”

2.单击“管理”选项。



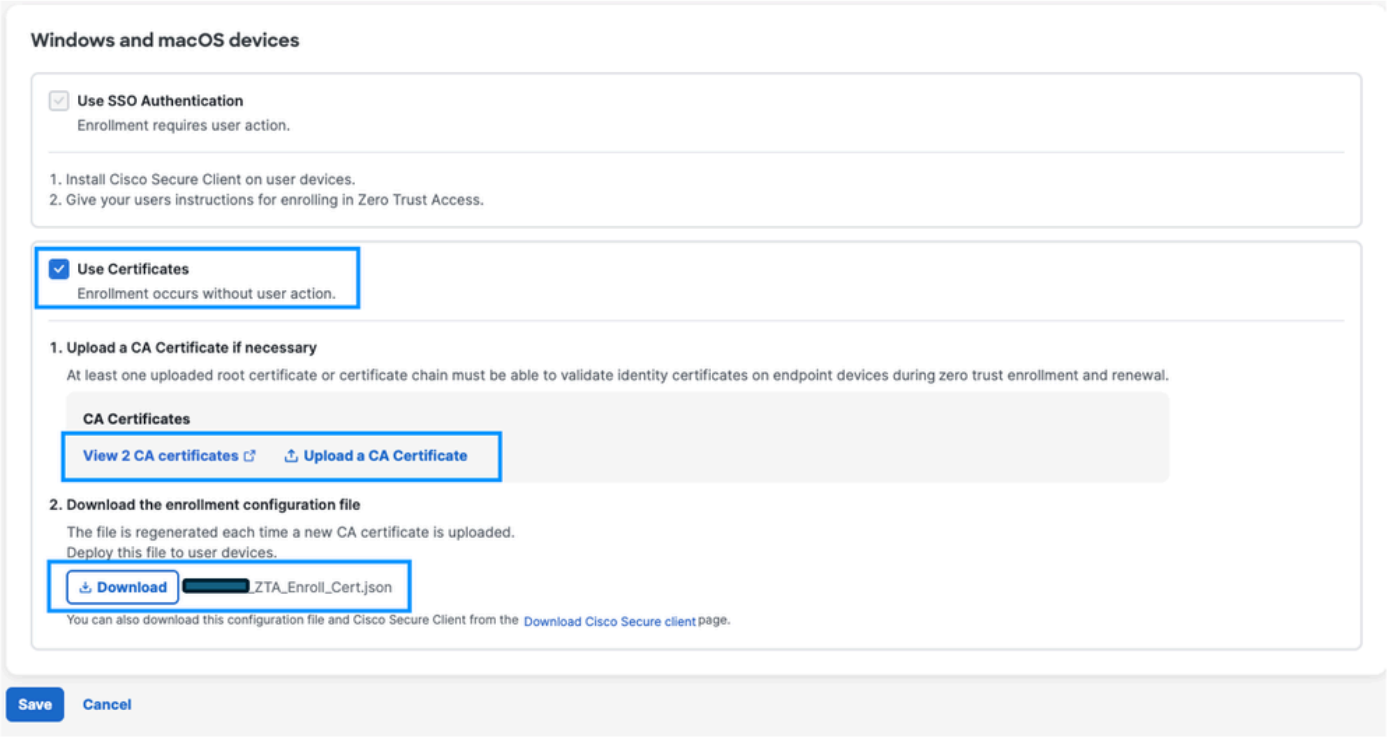
3.启用使用证书。

4.通过从本地证书颁发机构下载CA证书来上传CA证书。

5.下载注册配置，并将其放在基于操作系统的目录中。

-Windows 窗口版本:C:\ProgramData\Cisco\Cisco安全客户端\ZTA\enrollment_choices
- macOS:/opt/cisco/secureclient/zta/enrollment_choices

6.确保完成之后保存设置。



证书模板和安装

安全访问需要以下必填的证书字段：

— 主题备用名称(SAN)，包括用户RFC-822投诉电子邮件地址或用户主体名称(UPN)

示例：

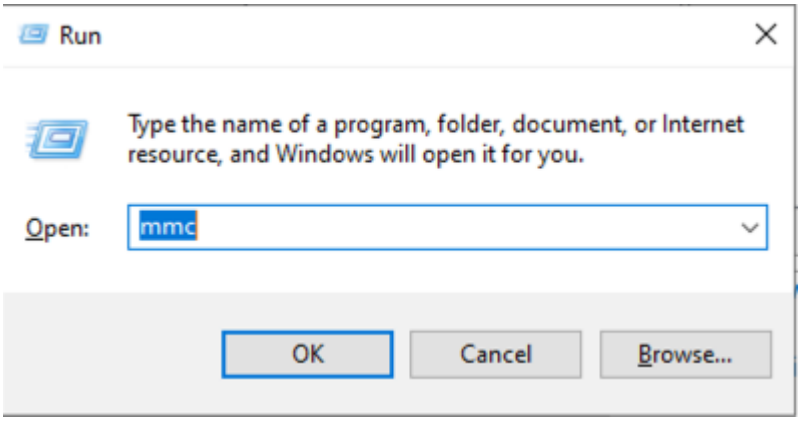
选项 1：符合RFC822的电子邮件
email.1 = username@domain.local

选项 2：（备选）：UPN（特定于Microsoft）
otherName:1.3.6.1.4.1.311.20.2.3;UTF8:username@domain.local

在本示例中，我们使用Microsoft AD中的用户证书模板生成证书。

步骤 1：导航到Microsoft AD并打开证书管理器

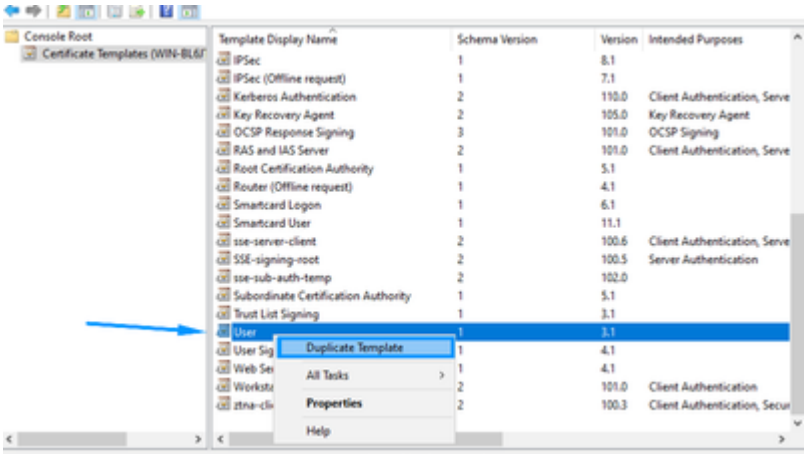
步骤 2：打开运行并输入Microsoft管理控制台(mmc)



步骤 3：单击“文件”，然后添加/删除管理单元

步骤 4：添加证书模板

步骤 5：复制用户证书



步骤 6：按所述配置设置

1.新模板名称：ztna-client-enroll under(General)选项卡。

2.在（主题名称）标签中选择（在请求中提供）。

注意：这样可以确保接受openssl模板提供的选项，例如服务备用名称(SAN)

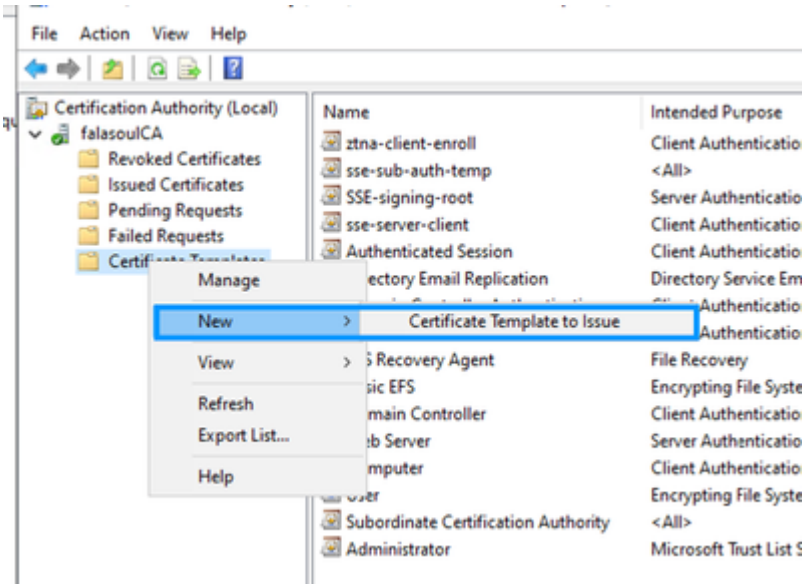
步骤 7：点击OK以保存新模板

步骤 8::通过执行以下操作将新模板添加到AD模板列表：

1.运行certsrv.msc

2.右键点击Certificate Templates（证书模板），然后选择New -> certificate template to issue（新建 — >证书模板）

3.选择新创建的模板(ztna-client-enroll)



使用Openssl创建证书

步骤 1：创建包含内容的san.cnf文件

```
[ 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
```

步骤 2：使用模板创建证书

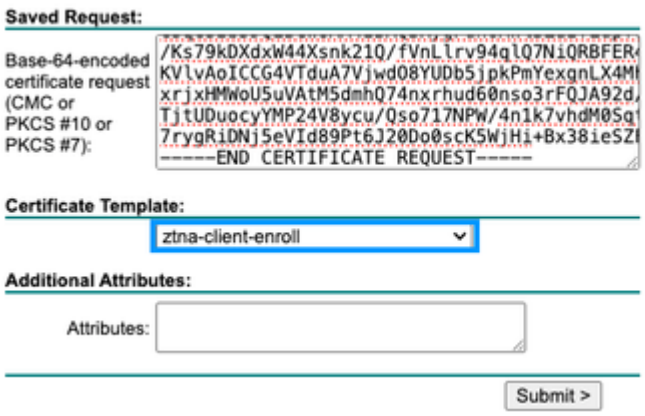
```
openssl genrsa -out user.key 2048
openssl req -new -key user.key -out user.csr
openssl req -new -key user.key -out user.csr -config san.cnf
```

使用CA ZTNA模板签署用户证书

步骤 1：复制文件user.csr的内容

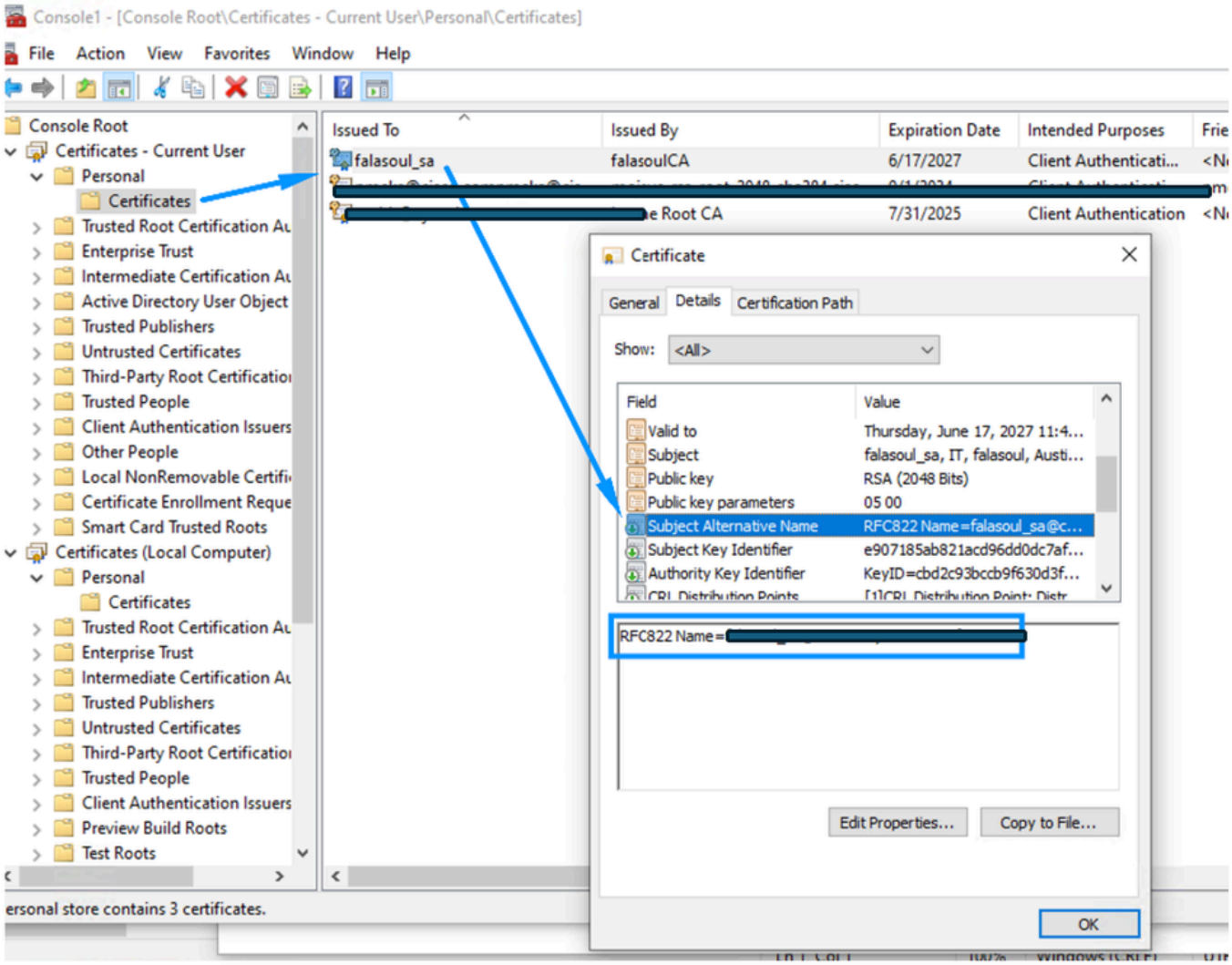
步骤 2：转到您的本地AD签名颁发机构(https:http://<ip-address>/certsrv/)

步骤 3：点击Request a Certificate -> Advanced Certificate Request -> select ztna-client-enroll template



步骤 4：下载Base64格式的证书并安装到用户个人信任库证书中。

步骤 5：确认证书中存在正确的信息

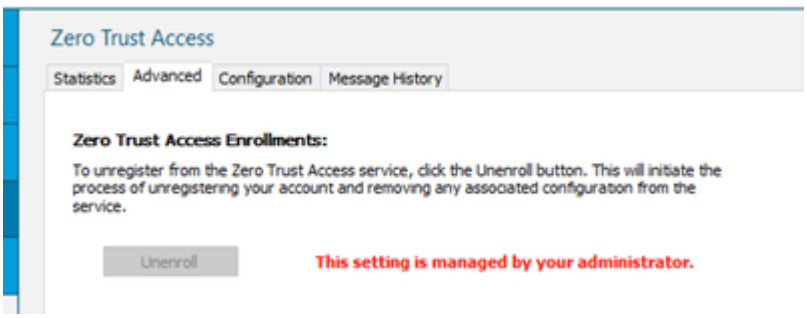


步骤 6：重新启动ZTNA模块以开始注册

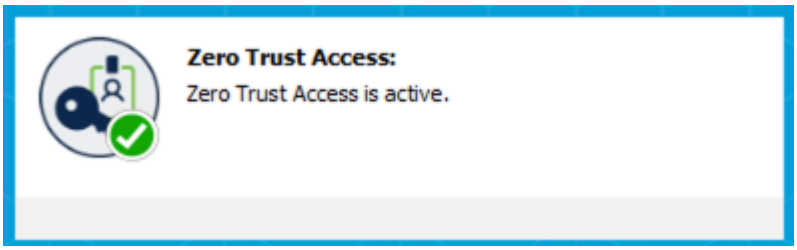
验证

使用本部分可确认配置能否正常运行。

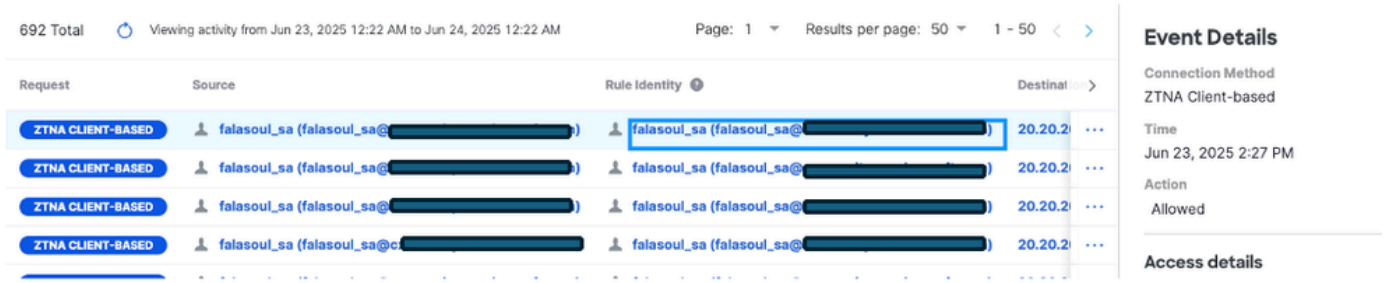
步骤 1：配置注册选择文件时的ZTNA模块消息：



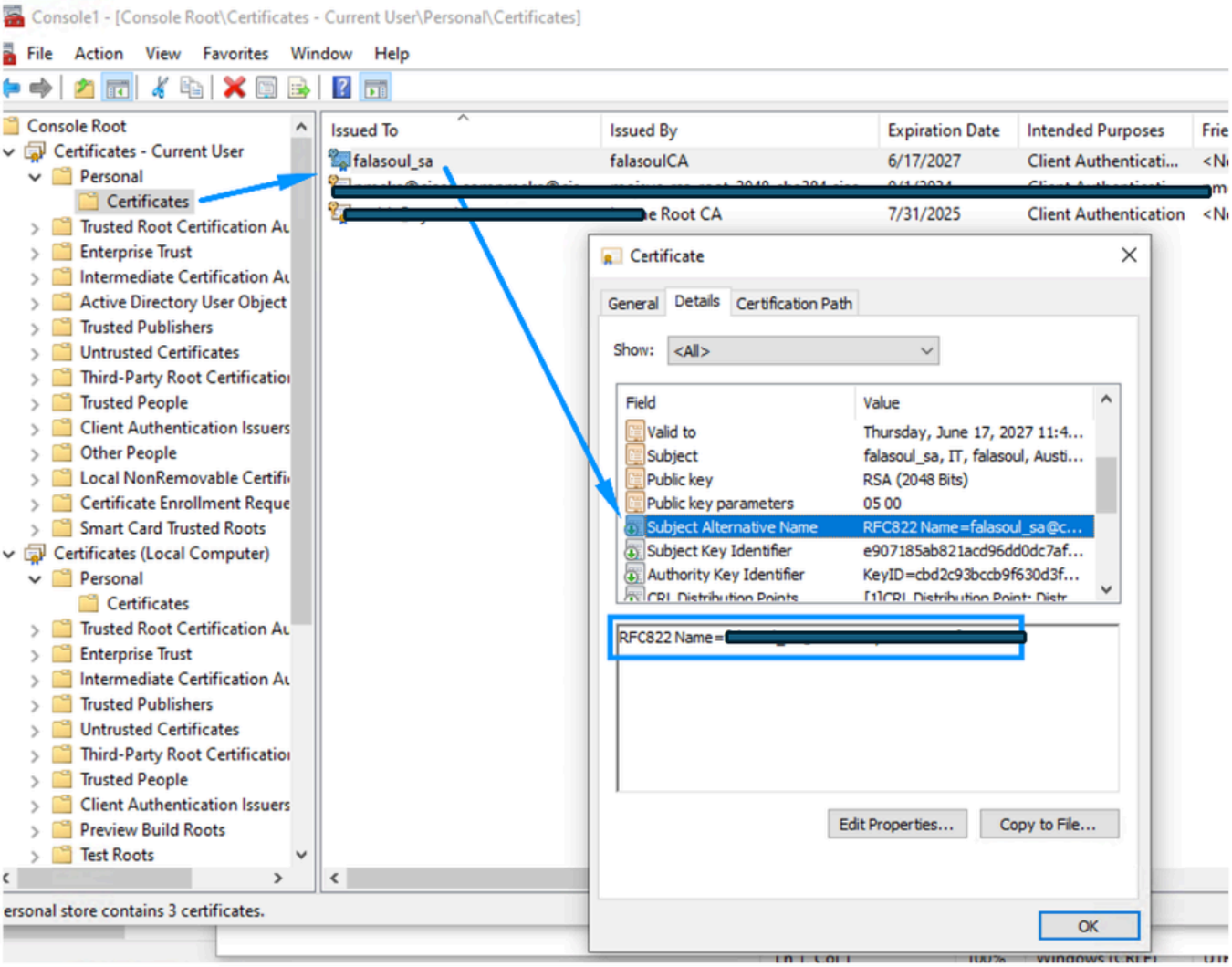
步骤 2：首次重新启动ZTNA模块后，您可以看到您已自动注册到ZTNA



步骤 3：根据SAN信息检验活动搜索中显示的正确用户



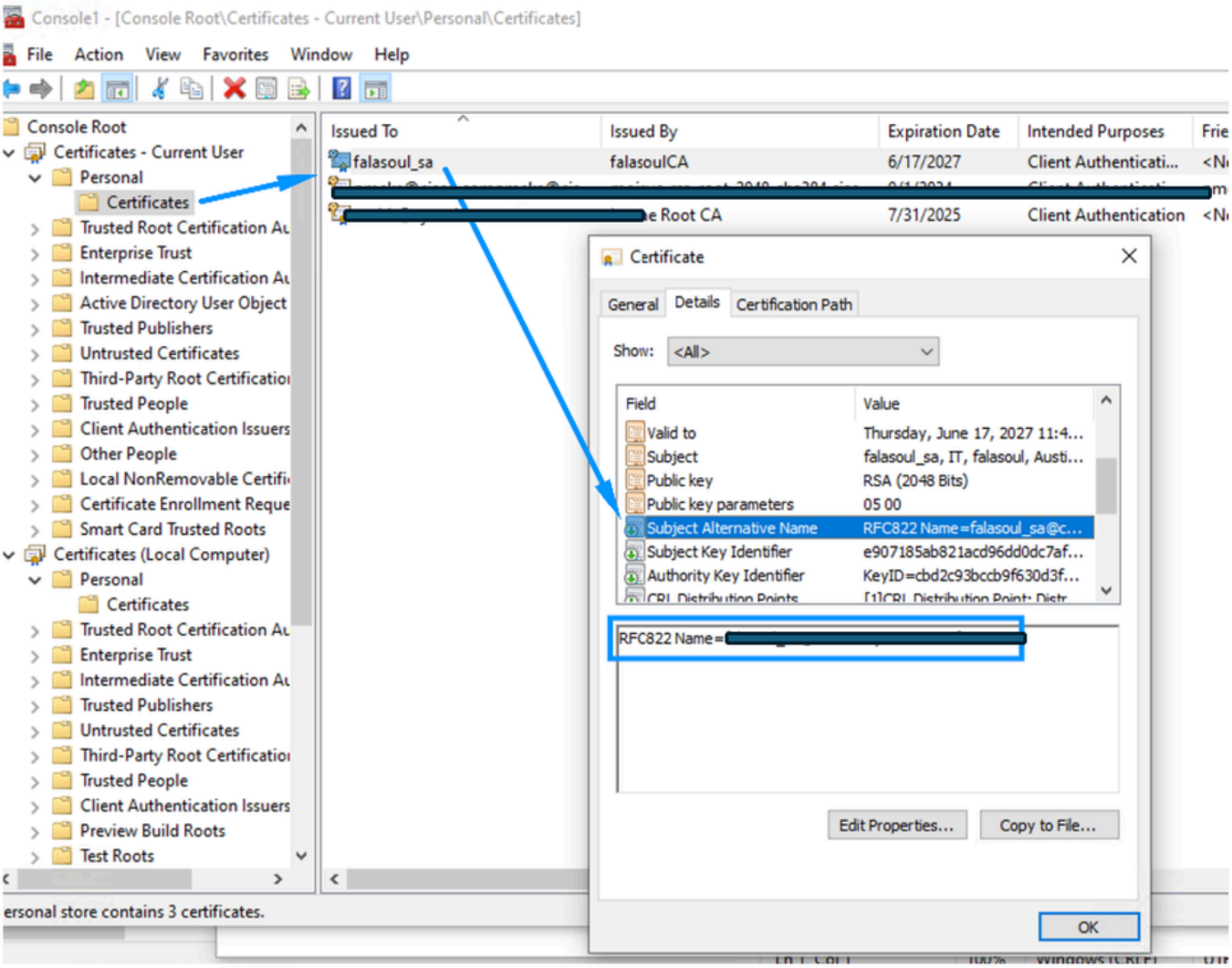
步骤 4：确认证书中存在正确的信息



故障排除

本部分提供的信息可用于对配置进行故障排除。

步骤 1： 确认证书中存在正确的信息，且已将其安装在正确的证书存储中。



步骤 2：使用DART确认注册未因证书要求而失败

步骤 3：如果使用UZTNA，请确认您能够正确解析FTD外部接口。

常见错误：

```
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::
```

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。