

Configurar o Registro Automático ZTNA de Acesso Seguro

Contents

Introdução

Este documento descreve as etapas necessárias para configurar o ZTNA para o registro automático baseado em certificado.

Pré-requisitos

- Versão mínima do Secure Client 5.1.9.x
- Trusted Platform Module (TPM) para Windows
- Co-processador Secure Enclave para dispositivos Apple

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro da Cisco
- Seção [Registrar Dispositivos no Acesso de Confiança Zero Usando o](#) Guia de [Certificação](#)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Windows 11 com TPM versão 2.0
- Secure Client versão 5.1.10.17 com o ZTNA e o módulo DUO ativados.
- Microsoft Active Directory 2022
- Ferramenta Openssl para geração de certificados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Habilitando a Inscrição Automática no Painel de Acesso Seguro

A primeira etapa na habilitação desse recurso é habilitar o recurso de Registro Automático de

Acesso Seguro, que inclui:

1. Navegue até Dashboard -> Connect -> End User Connectivity -> Zero Trust (Painel -> Conectar -> Conectividade do usuário final -> Zero Trust)
2. Clique na opção Gerenciar.

The screenshot shows the 'End User Connectivity' dashboard. At the top, there are buttons for 'Cisco Secure Client' and 'Manage servers'. Below the header, there are tabs for 'Zero Trust Access', 'Virtual Private Network', and 'Internet Security'. The 'Zero Trust Access' tab is selected. Under this tab, there is a section for 'Enrollment methods' with a 'Manage' button. Below this, there is a section for 'Default Profile' with a table showing the default ZTA profile.

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 [Manage](#)

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.

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. Habilitar Certificados de Uso.
4. Carregue o Certificado de CA fazendo o download dele em sua Autoridade de Certificação local.
5. Baixe a Configuração de Inscrição e coloque-a nos diretórios com base no sistema operacional.
 - Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choice
 - MacOS: /opt/cisco/secureclient/zta/enrollment_choices
6. Certifique-se de salvar suas configurações quando terminar.

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](#)

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

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

Modelo e instalação do certificado

O acesso seguro requer estes campos de certificado obrigatórios:

- SAN (Nome alternativo do assunto) para incluir o endereço de e-mail de reclamação RFC-822 do usuário ou UPN (Nome principal do usuário)

Exemplo:

Opção 1: E-mail compatível com RFC822

e-mail.1 = username@domain.local

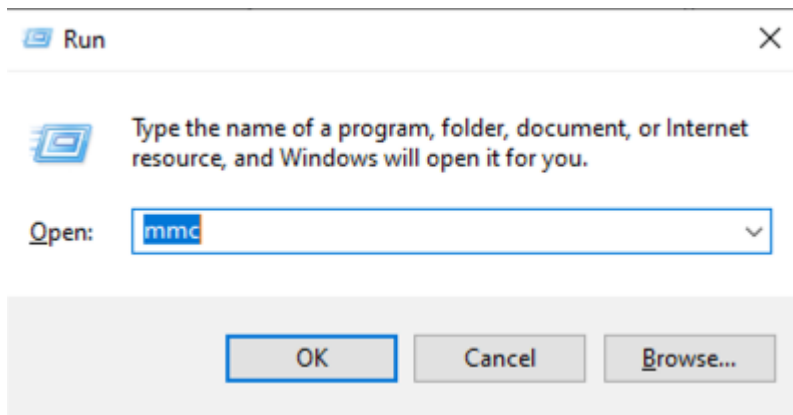
Opção 2: (alternativa): UPN (específico da Microsoft)

otherName:1.3.6.1.4.1.311.20.2.3;UTF8:username@domain.local

Neste exemplo, estamos usando o modelo de certificado do usuário no Microsoft AD para gerar o certificado.

Passo 1: Navegue até o Microsoft AD e abra o Gerenciador de Certificados

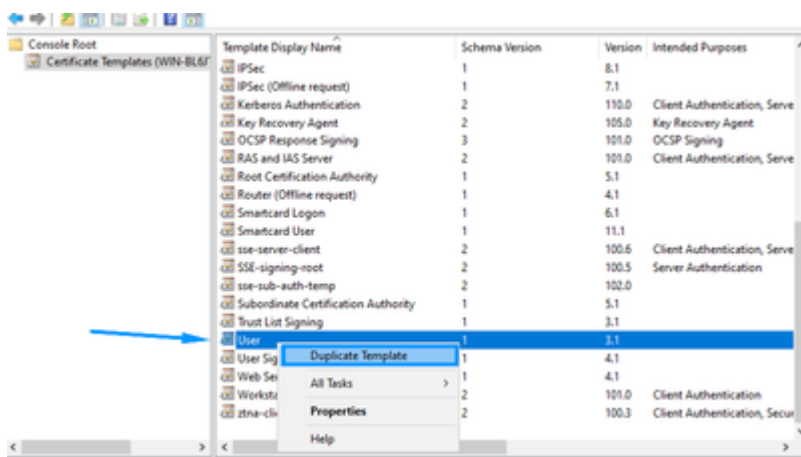
Passo 2: Abra Executar e entre no Console de Gerenciamento Microsoft (mmc)



Passo 3: Clique em Arquivo e adicione/remova Snap-in

Passo 4: Adicionar modelos de certificado

Passo 5: Duplicar certificado do usuário



Passo 6: Defina as configurações conforme descrito

1. Nome do Novo Modelo: ztna-client-enroll na guia (Geral).
2. Selecione (Suprimento na solicitação) na guia (Nome do Assunto).



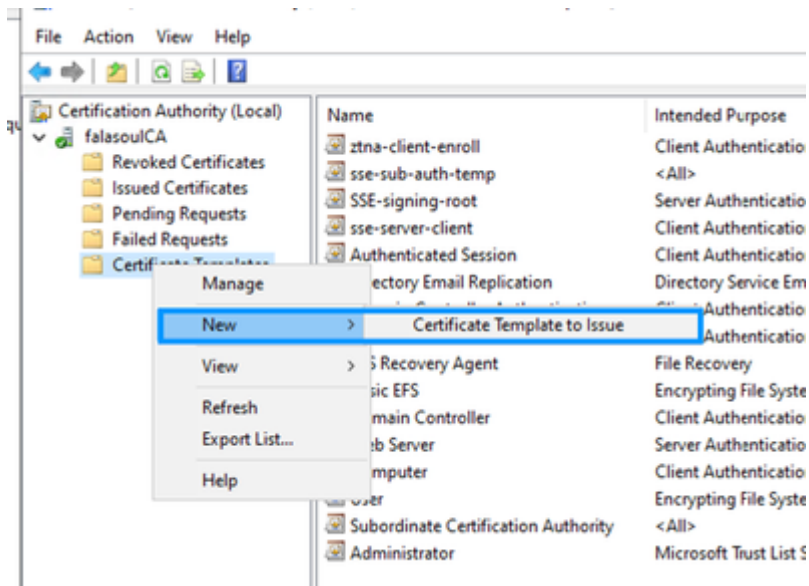
Note: Isso garante que as opções fornecidas pelo modelo openssl, como Nome Alternativo do Serviço (SAN), sejam aceitas

Passo 7: Clique em OK para salvar o novo modelo

Passo 8: Adicione o novo Modelo à lista de modelos do AD executando:

1. Execute certsrv.msc
2. clique com o botão direito do mouse em Modelos de certificado e selecione Novo -> modelo de certificado a ser emitido

3. Selecione o modelo recém-criado (ztna-client-enroll)



Criando Certificado usando Openssl

Passo 1: Criar arquivo san.cnf com conteúdo

```
[ 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
```

Passo 2: criar certificado usando o modelo

```
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
```

Assinar certificado do usuário com o Modelo CA ZTNA

Passo 1: Copie o conteúdo do arquivo user.csr

Passo 2: vá para sua autoridade local de assinatura do AD (<https://<ip-address>/certsrv/>)

Passo 3: Clique em Request a Certificate -> Advanced Certificate Request -> select ztna-client-enroll template (Solicitar um certificado -> Solicitação avançada de certificado -> selecionar modelo ztna-client-enroll)

Saved Request:

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

```
/Ks79kDXdxW44Xsnk21Q/fVnLlrv94q1Q7Ni0RBFERK
VlVlAoICCG4VTduA7Vjwd08YUDb5jpkPmYexgnLX4M
xrjxHMWU5uVAtM5dmhQ74nrxrhud60nso3rFQJA92d
TjtUDuocyYMP24V8ycu/Qso717NPW/4n1k7vhdM0Sq
7rygR1DNj5eVI89Pt6J20Do0scK5WjHi+Bx38ieSZI
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

ztna-client-enroll

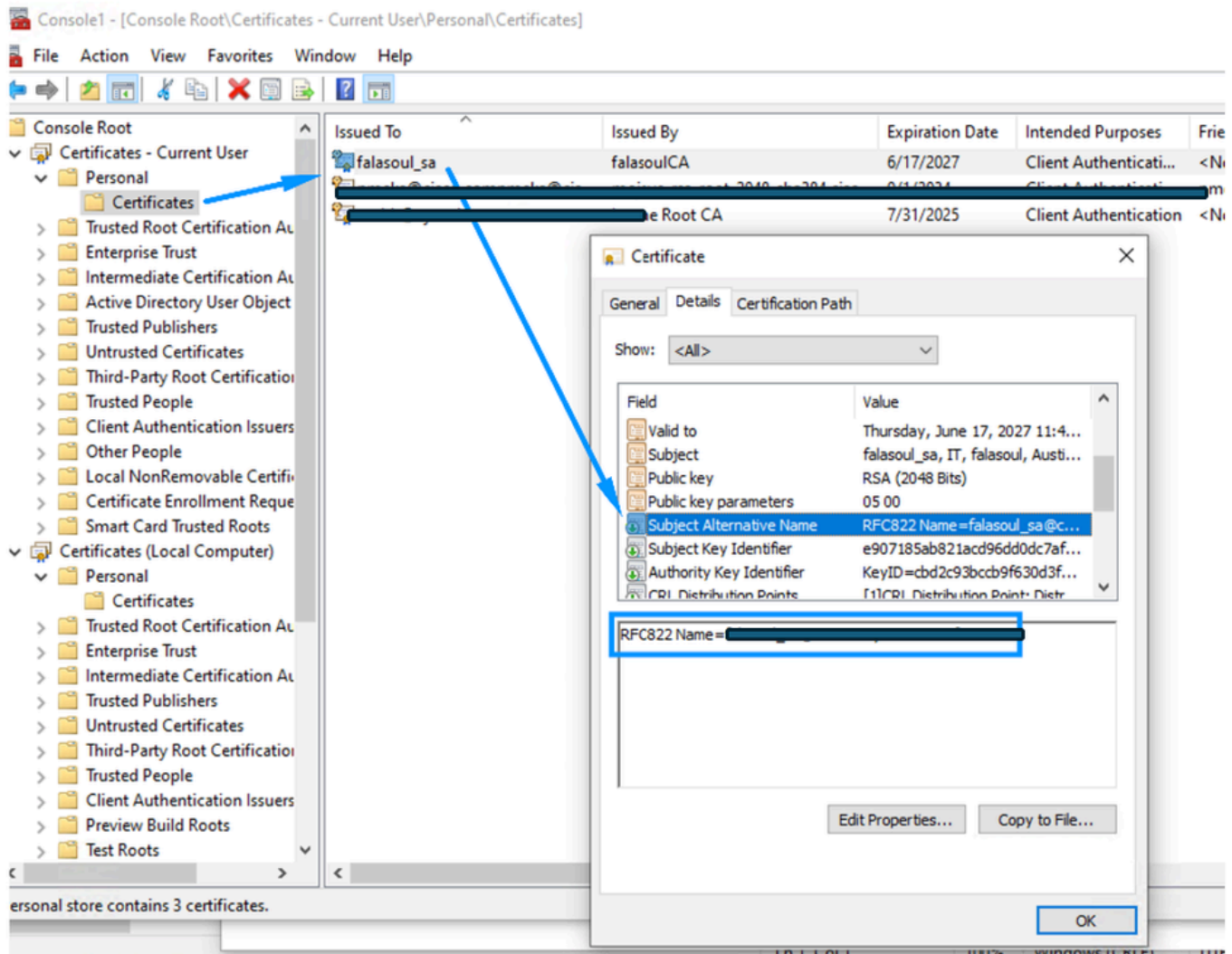
Additional Attributes:

Attributes:

Submit >

Passo 4: Baixe o certificado no formato Base64 e instale no certificado de armazenamento confiável pessoal do usuário.

Passo 5: Confirme se as informações corretas estão no certificado

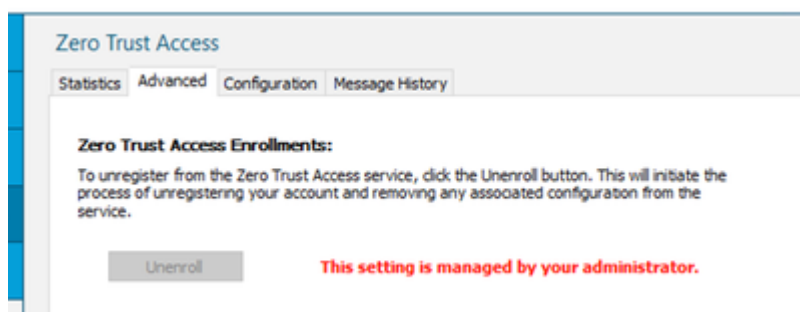


Passo 6: Reinicie o módulo ZTNA para iniciar a inscrição

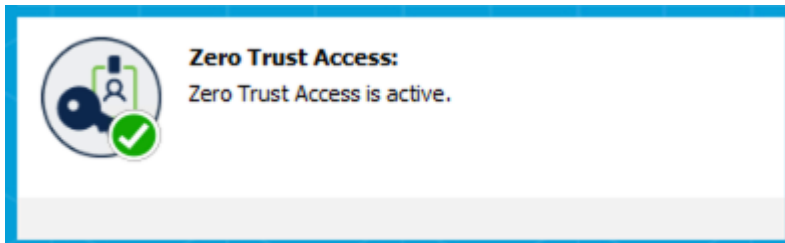
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Passo 1: Mensagem do Módulo ZTNA ao configurar o arquivo de opções de registro:



Passo 2: Após reiniciar o ZTNA Module pela primeira vez você pode ver que você está inscrito automaticamente no ZTNA

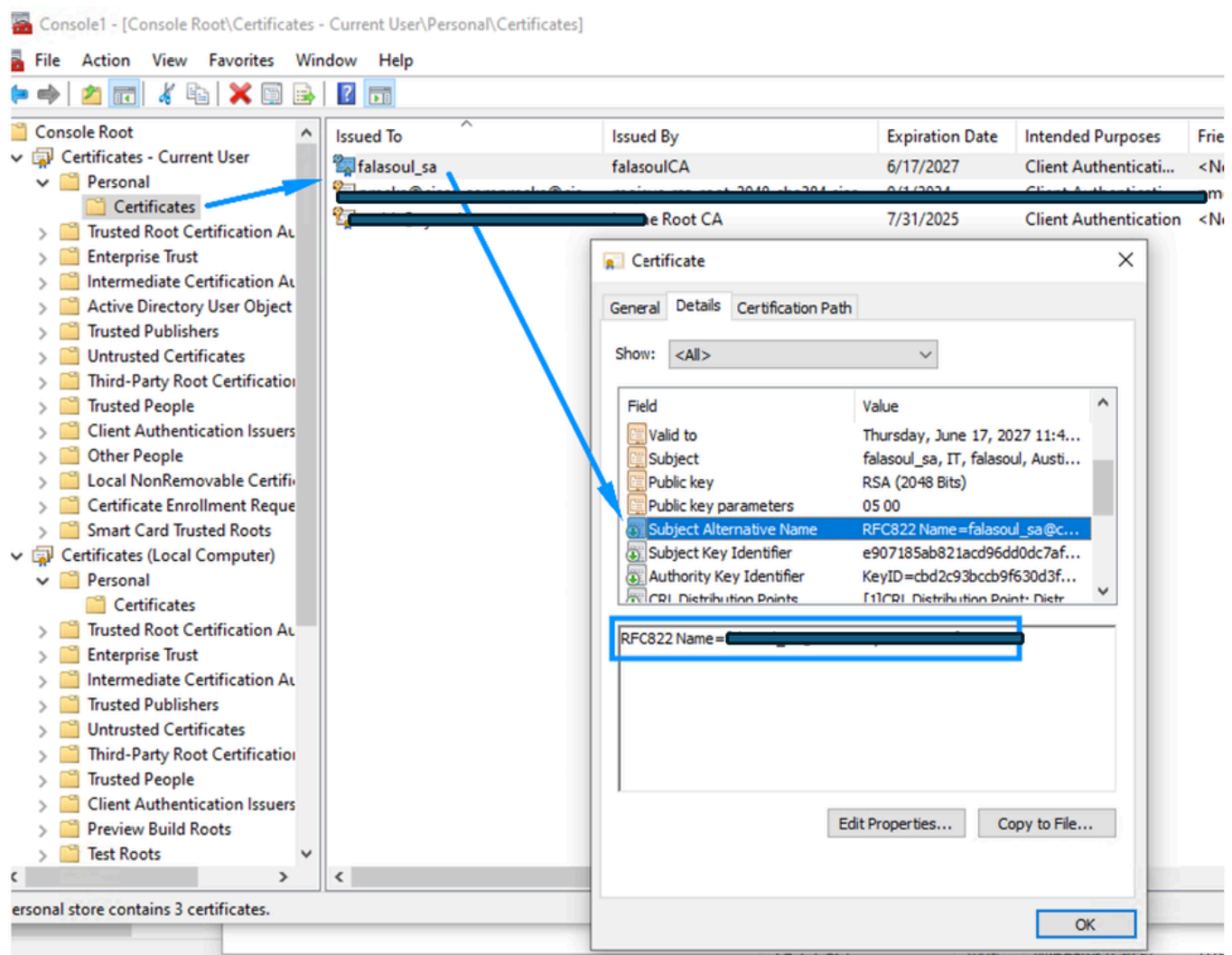


Passo 3: Verificar se o usuário correto aparece na pesquisa de atividades com base nas informações de SAN

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

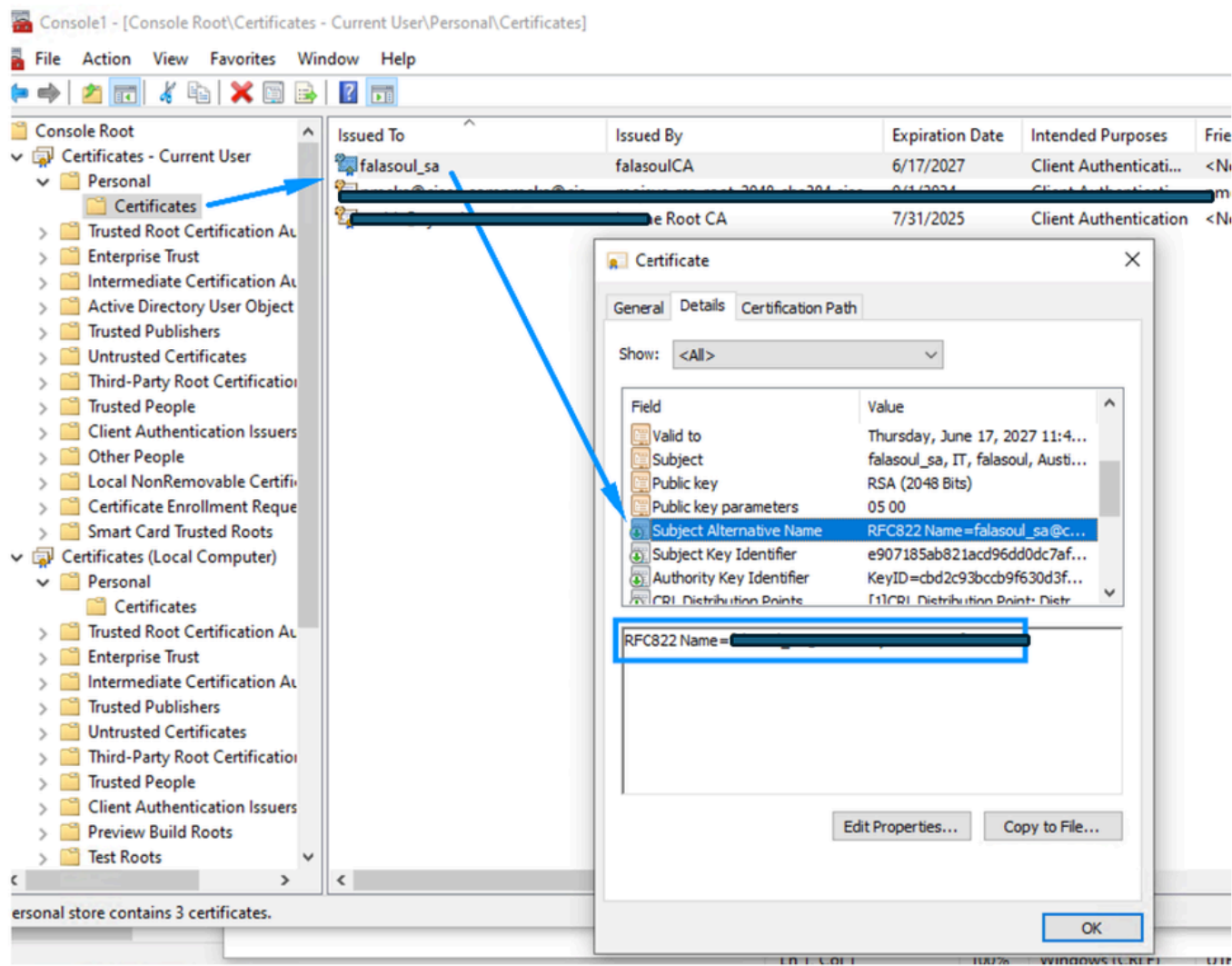
Passo 4: Confirme se as informações corretas estão no certificado



Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Passo 1: Confirme se as informações corretas existem no certificado e se estão instaladas no armazenamento de certificados correto.



Passo 2: Confirme se a inscrição não está falhando nos requisitos de certificado usando o DART

Passo 3: Confirme se você é capaz de resolver sua interface externa FTD corretamente se UZTNA está sendo usado.

erro comum:

```
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:::

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.