Configurar TACACS+ sobre TLS 1.3 em um dispositivo IOS XR com ISE

Contents

- Introdução
- Overview
  - Usando este Guia
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
  - Licenciamento
- Parte 1 - Configuração do ISE para Administração de Dispositivos
  - Gerar solicitação de assinatura de certificado para autenticação de servidor TACACS+
  - Carregar certificado CA raiz para autenticação de servidor TACACS+
  - Vincule a solicitação de assinatura de certificado (CSR) assinada ao ISE
  - Ativar TLS 1.3
  - Ativar a administração de dispositivos no ISE
  - Habilitar TACACS sobre TLS
  - Criar dispositivo de rede e grupos de dispositivo de rede
  - ConfigurarRepositórios de Identidade
  - Configurar perfis TACACS+
    - IOS XR_RW - Perfil do administrador
    - IOS XR_RO - Perfil do operador
  - Configurar conjuntos de comandos TACACS+
    - CISCO IOS XR RW - Conjunto de Comandos do Administrador
    - CISCO IOS XR RO - Conjunto de comandos do operador
  - ConfigurarConjuntos de Políticas de Administração do Dispositivo
- Parte 2 - Configurar o Cisco IOS XRpara TACACS+ sobre TLS 1.3
  - Configurações iniciais
  - Configurar Ponto de Confiabilidade
  - Configurar TACACS e AAA com TLS
- Renovação de certificado
- Verificação
  - Troubleshooting

Introdução

Este documento descreve um exemplo para TACACS+ sobre TLS com Cisco Identity Services Engine (ISE) como servidor e um dispositivo Cisco IOS® XR como cliente.

Overview

O protocolo TACACS+ (Terminal Access Controller Access-Control System Plus) [RFC8907] permite a administração centralizada de dispositivos para roteadores, servidores de acesso à rede e outros dispositivos em rede por meio de um ou mais servidores TACACS+. Ele fornece serviços de autenticação, autorização e auditoria (AAA - Authentication, Authorization, and Accounting), especificamente desenvolvidos para casos de uso de administração de dispositivos.

O TACACS+ sobre TLS 1.3 [RFC8446] melhora o protocolo introduzindo uma camada de transporte segura, protegendo dados altamente confidenciais. Essa integração garante confidencialidade, integridade e autenticação para a conexão e o tráfego de rede entre clientes e servidores TACACS+.

Usando este Guia

Este guia divide as atividades em duas partes para permitir que o ISE gerencie o acesso administrativo para dispositivos de rede baseados no Cisco IOS XR.
· Parte 1 - Configurar o ISE para o administrador de dispositivos
· Parte 2 - Configurar o Cisco IOS XR para TACACS+ sobre TLS

Pré-requisitos

Requisitos

Requisitos para configurar TACACS+ sobre TLS:

- Uma Autoridade de Certificação (CA) para assinar o certificado usado pelo TACACS+ sobre TLS para assinar os certificados do ISE e dos dispositivos de rede.
- O certificado raiz da Autoridade de Certificação (CA).
- Os dispositivos de rede e o ISE têm acessibilidade de DNS e podem resolver nomes de host.

Componentes Utilizados

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

- Dispositivo virtual ISE VMware, versão 3.4, patch 2
- Roteador Cisco 8201, versão 25.3.1

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.

Licenciamento

Uma licença de Administração de dispositivo permite que você use serviços TACACS+ em um nó de Serviço de política. Em uma implantação autônoma de alta disponibilidade (HA), uma licença de Administração de dispositivo permite que você use serviços TACACS+ em um único nó de Serviço de política no par HA.

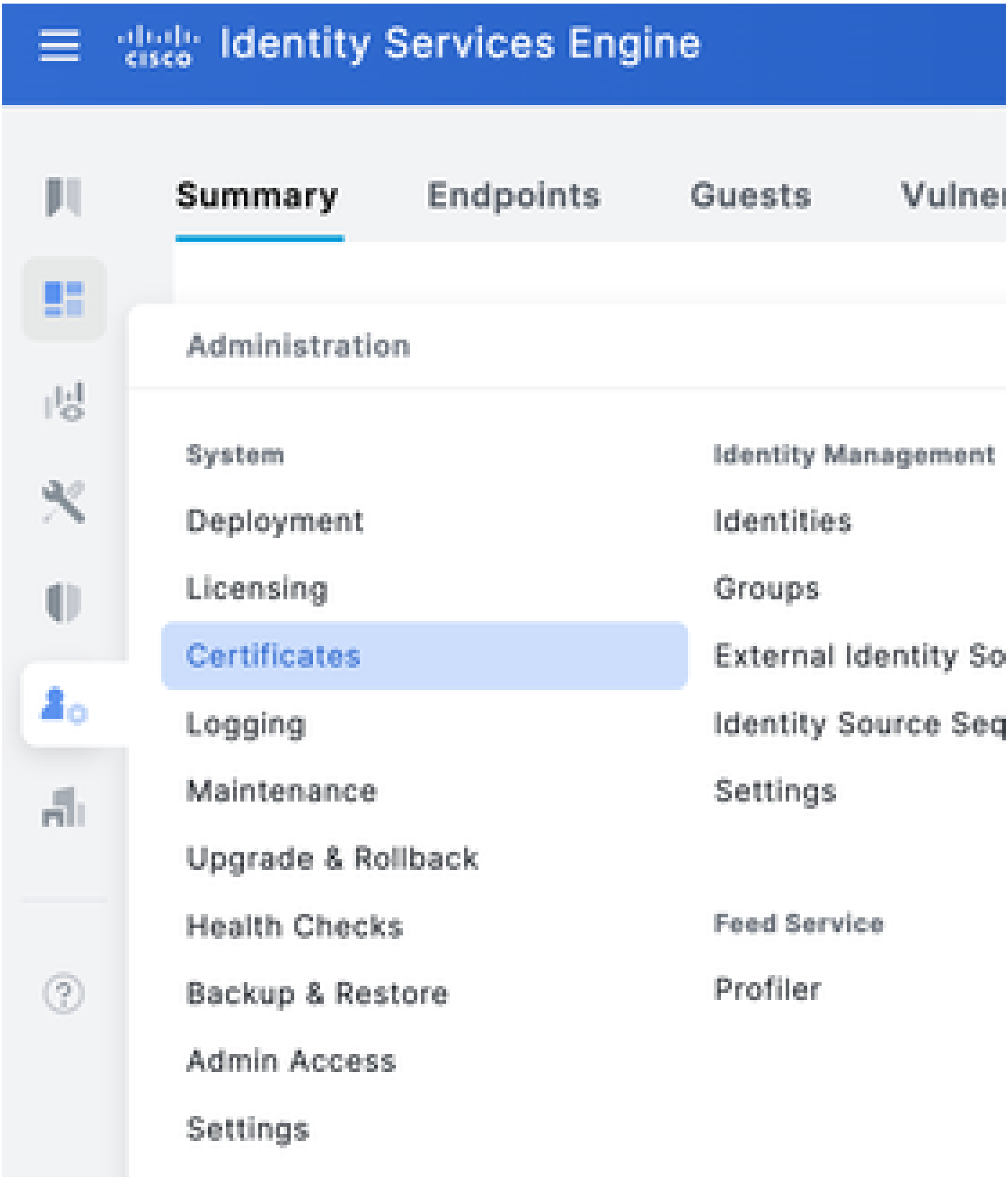
Parte 1 - Configuração do ISE para Administração de Dispositivos

Gerar solicitação de assinatura de certificado para autenticação de servidor TACACS+

Etapa 1. Faça login no portal da Web do administrador do ISE usando um dos navegadores compatíveis.

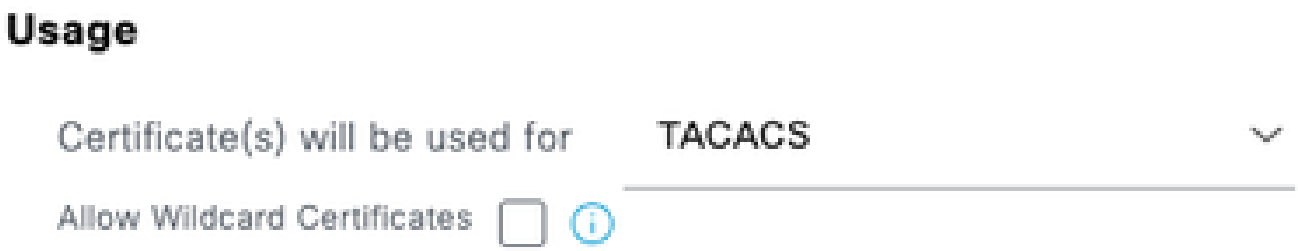
Por padrão, o ISE usa um certificado autoassinado para todos os serviços. A primeira etapa é gerar uma CSR (Certificate Signing Request, solicitação de assinatura de certificado) para que ela seja assinada por nossa CA (Certificate Authority, autoridade de certificação).

Etapa 2. Navegue até Administração > Sistema > Certificados.

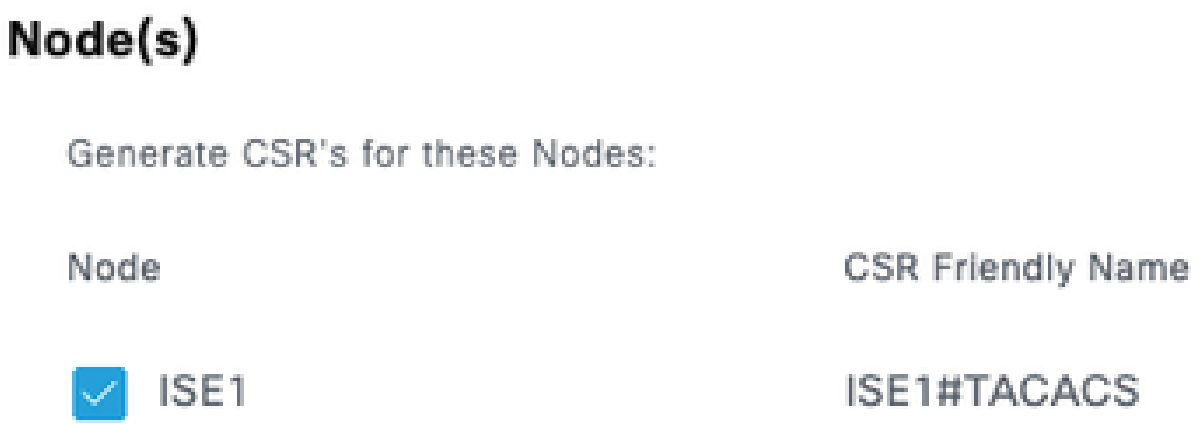


Etapa 3. Em Certificate Signing Requests, clique em Generate Certificate Signing Request.

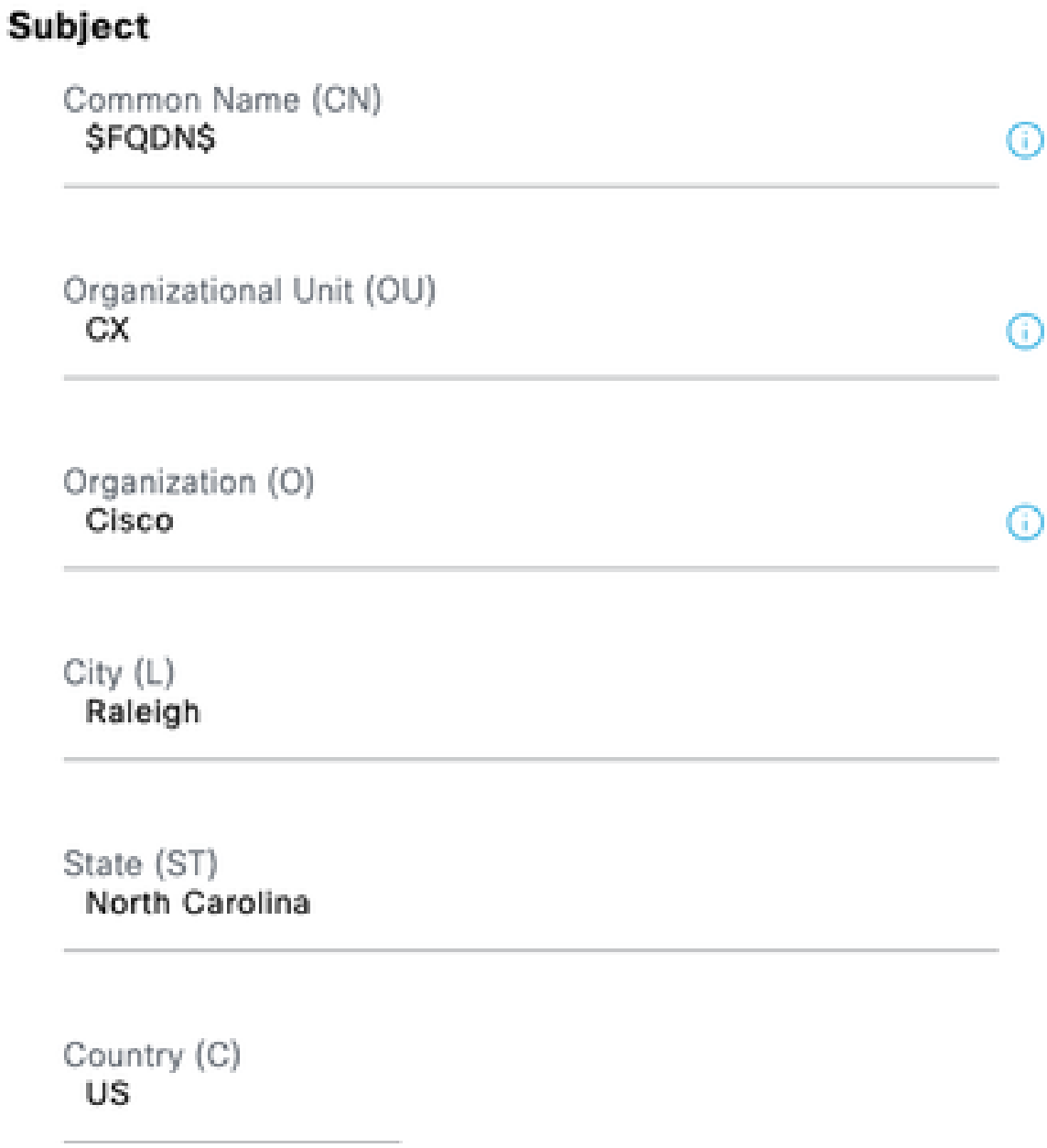
Etapa 4. SelectTACACS inUsage.



Etapa 5. Selecione as PSNs que têm o TACACS+ habilitado.

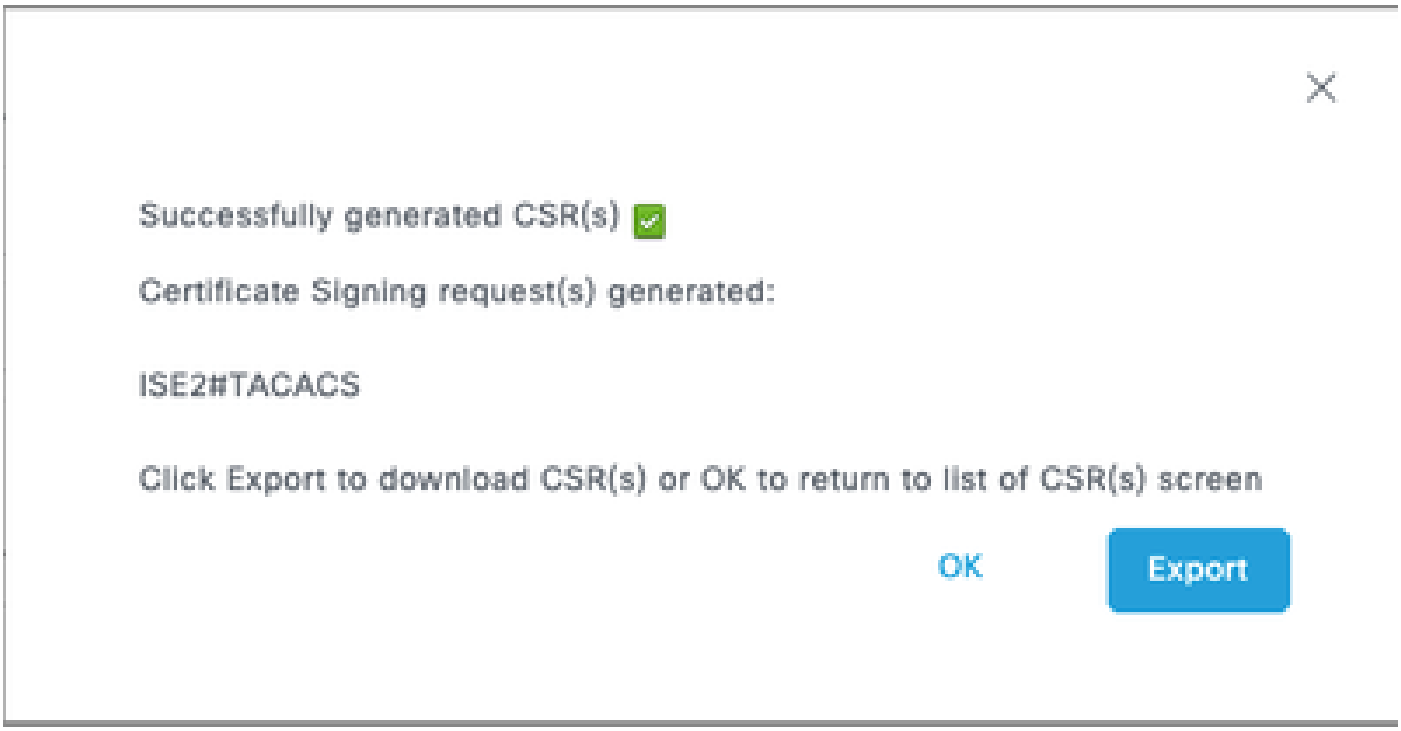


Etapa 6. Preencha os campos Assunto com as informações apropriadas.



Etapa 7. Adicione o nome DNS e o endereço IP em Nome alternativo do assunto (SAN).

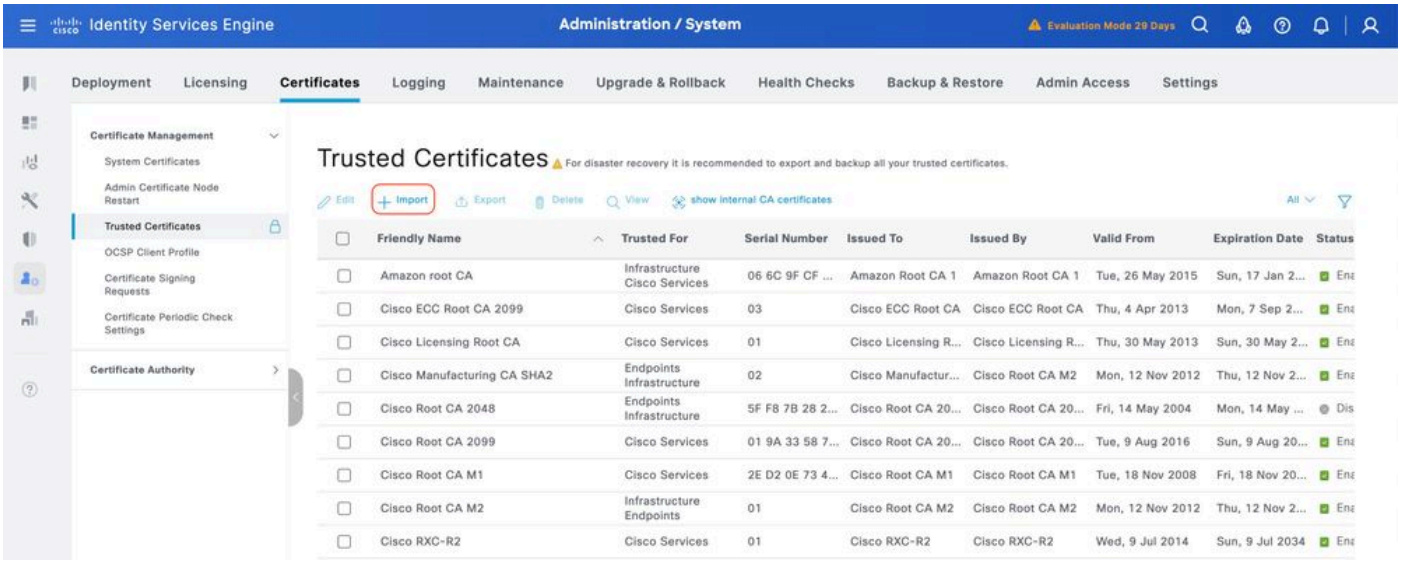
Etapa 8. Clique em Gerar e depois em Exportar.



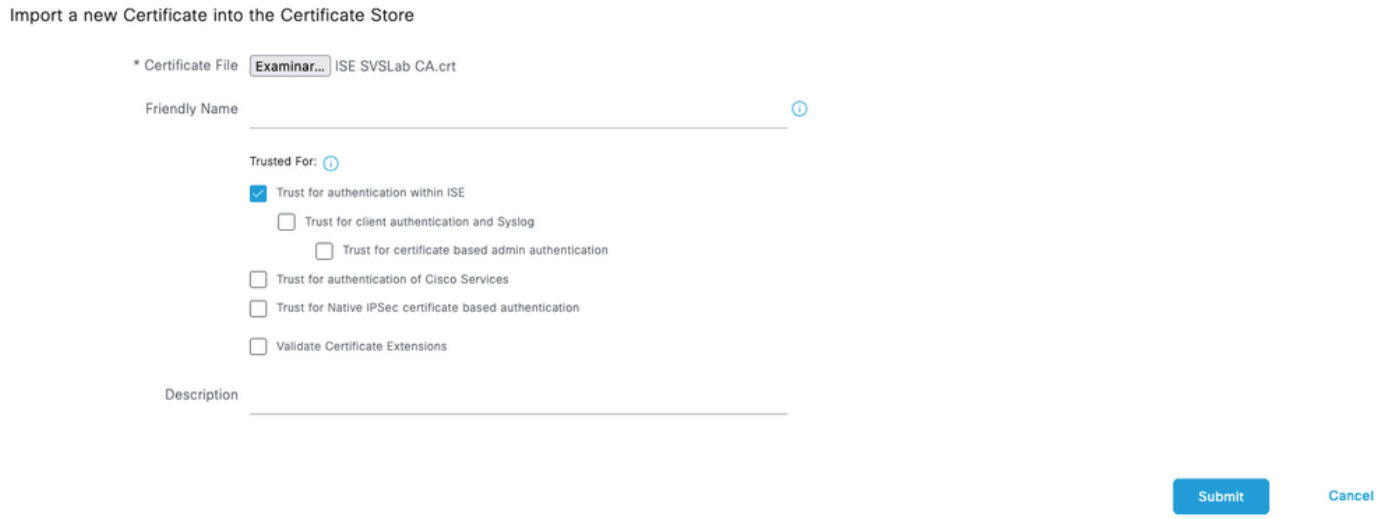
Agora, você pode ter o certificado (CRT) assinado pela Autoridade de Certificação (CA).

Carregar certificado CA raiz para autenticação de servidor TACACS+

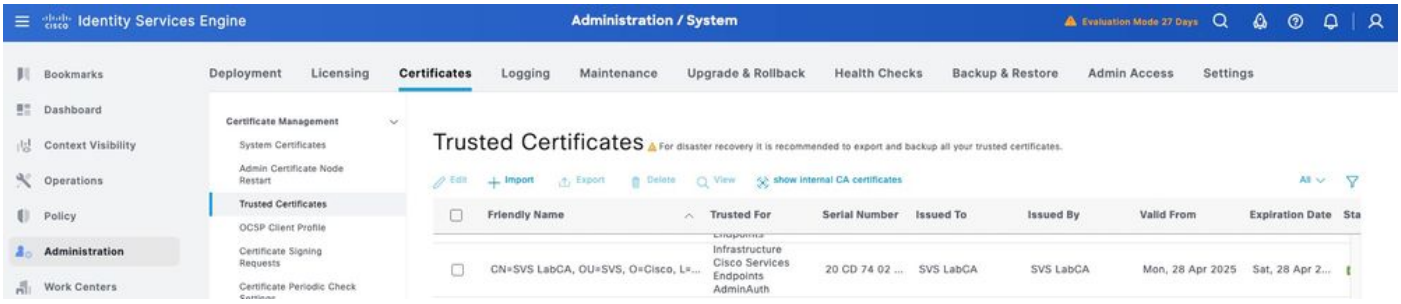
Etapa 1.Navegue até Administração > Sistema > Certificados. Em Certificados de Confiabilidade, clique em Importar.



Etapa 2. Selecione o certificado emitido pela Autoridade de Certificação (CA) que assinou sua CSR (Certificate Signing Request, Solicitação de Assinatura de Certificado) TACACS. Verifique se o comando Confiança para autenticação no ISE está ativada.



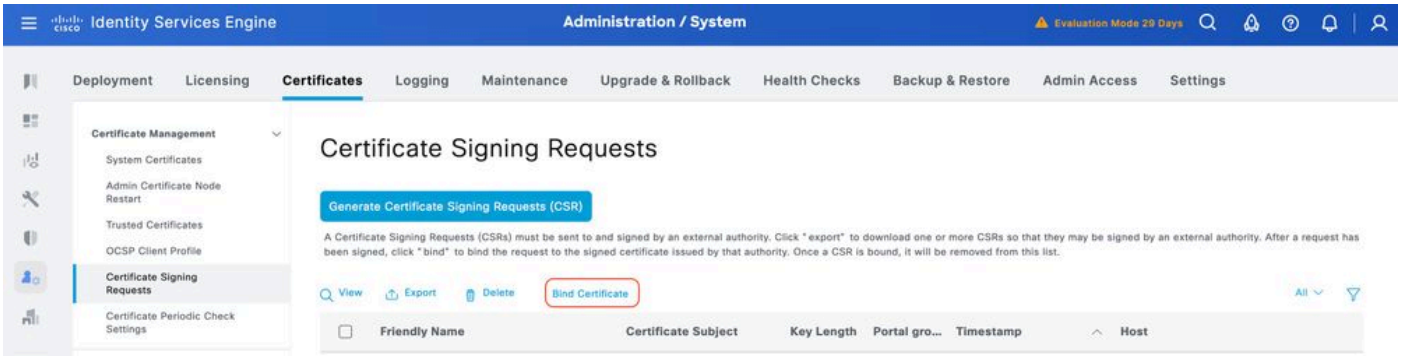
Clique em Enviar. O certificado deve aparecer agora em Certificados de Confiabilidade.



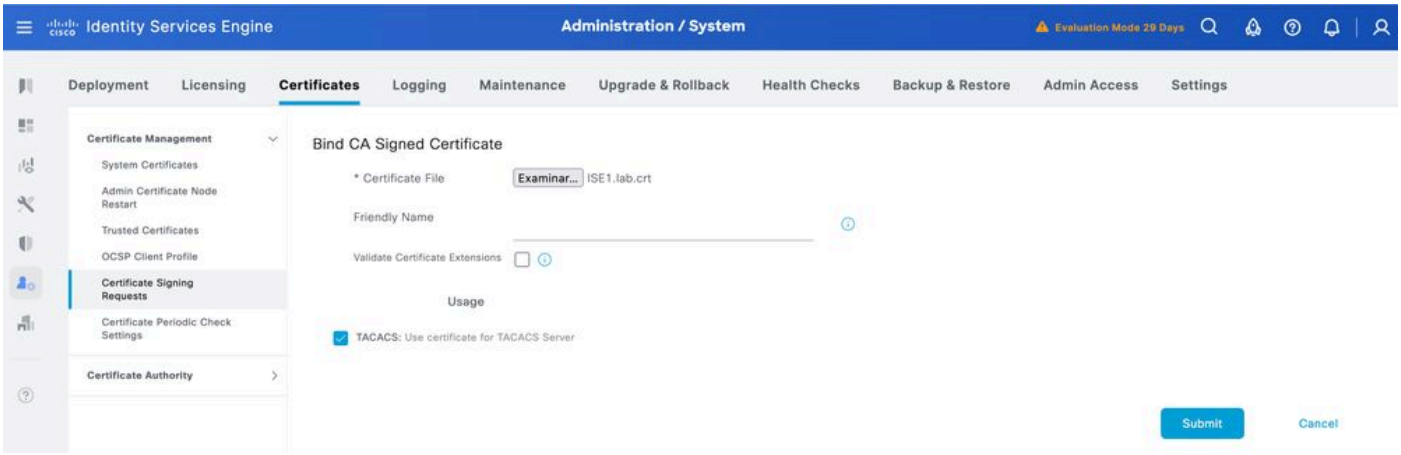
Vincule a solicitação de assinatura de certificado (CSR) assinada ao ISE

Depois que a CSR (Certificate Signing Request, Solicitação de assinatura de certificado) for assinada, você poderá instalar o certificado assinado no ISE.

Etapa 1.Navegue até Administração > Sistema > Certificados. Em Certificate Signing Requests, selecione o CSR TACACS gerado na etapa anterior e clique em Bind Certificate.

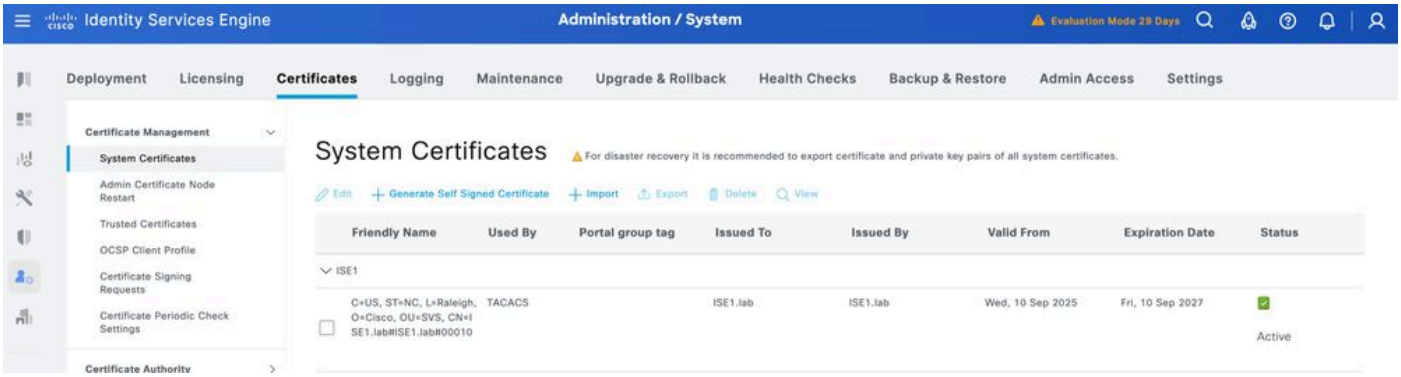


Etapa 2.Selecione o certificado assinado e certifique-se de que a caixa de seleção TACACS em Usage permaneça marcada.



Etapa 3. Clique em Enviar. Se você receber um aviso sobre a substituição do certificado existente, clique em Sim para continuar.

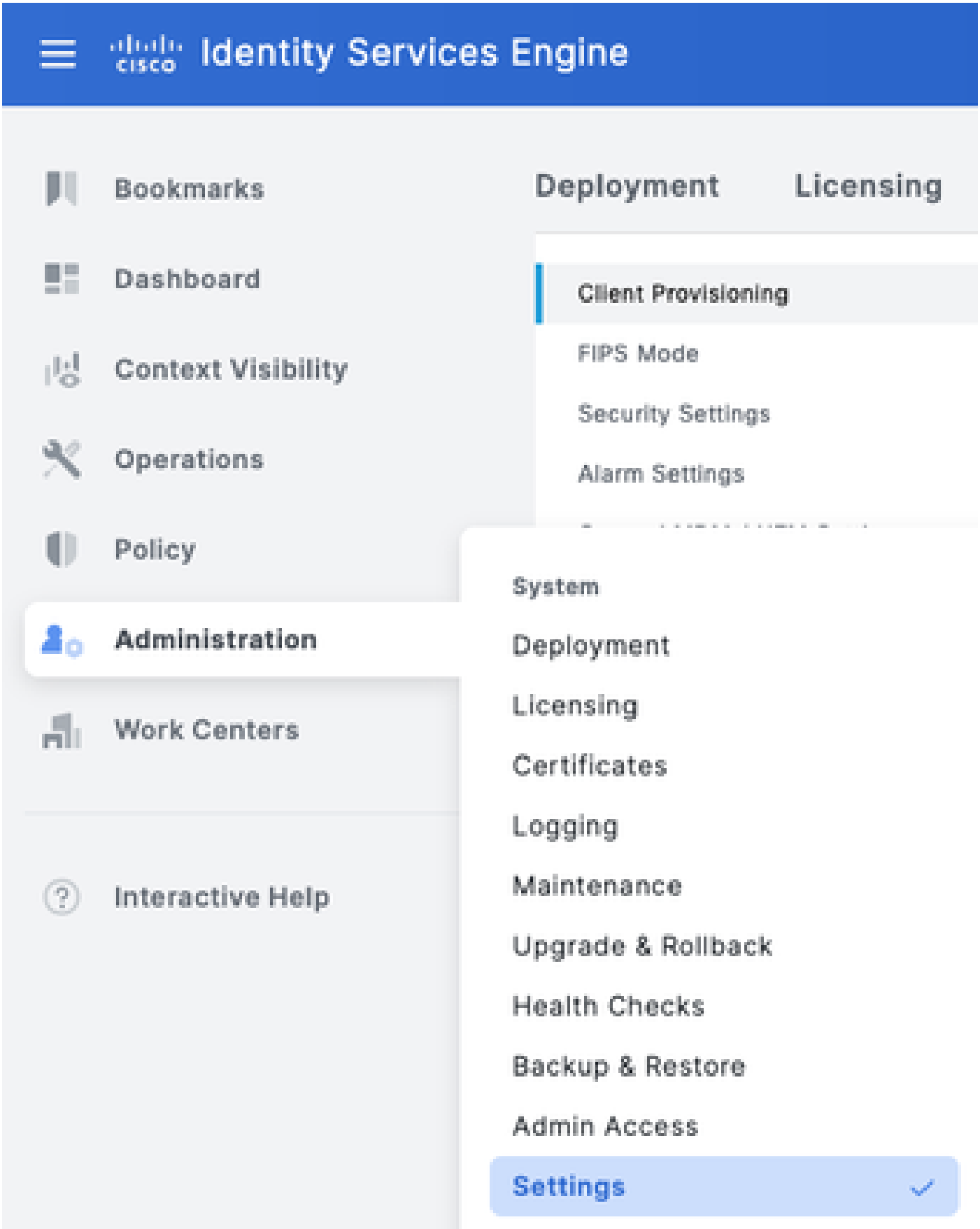
O certificado deve agora estar instalado corretamente. Você pode verificar isso em Certificados do sistema.



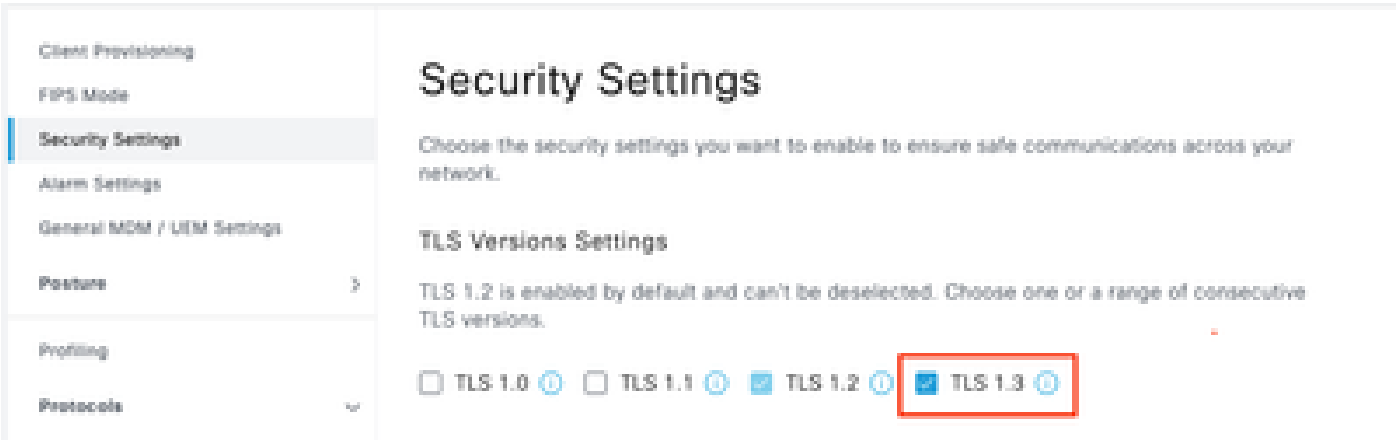
Ativar TLS 1.3

O TLS 1.3 não está habilitado por padrão no ISE 3.4.x. Ele deve ser habilitado manualmente.

Etapa 1.Navegue até Administração > Sistema > Configurações.



Etapa 2. Clique em Security Settings, marque a caixa de seleção ao lado de TLS1.3 em TLS Version Settings e clique em Save.

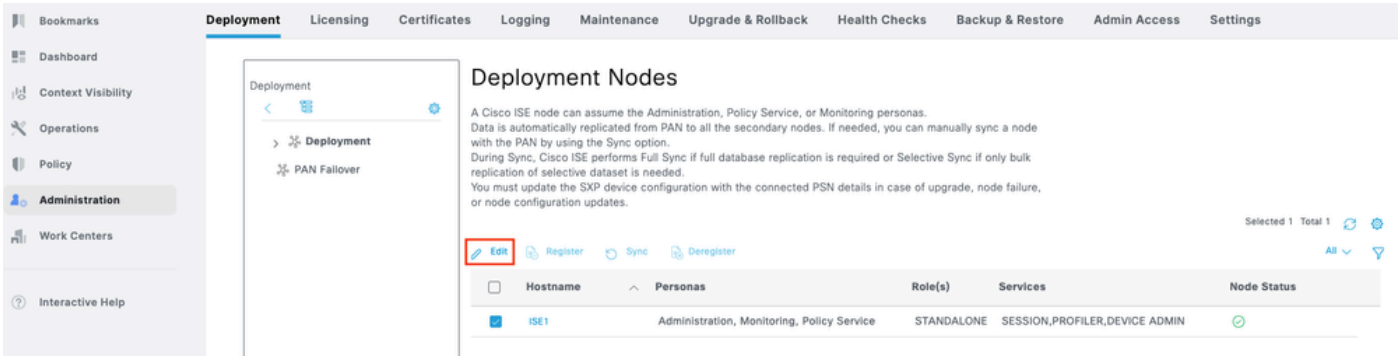


aviso: Quando você altera a versão do TLS, o servidor de aplicativos do Cisco ISE é reiniciado em todas as máquinas de implantação do Cisco ISE.

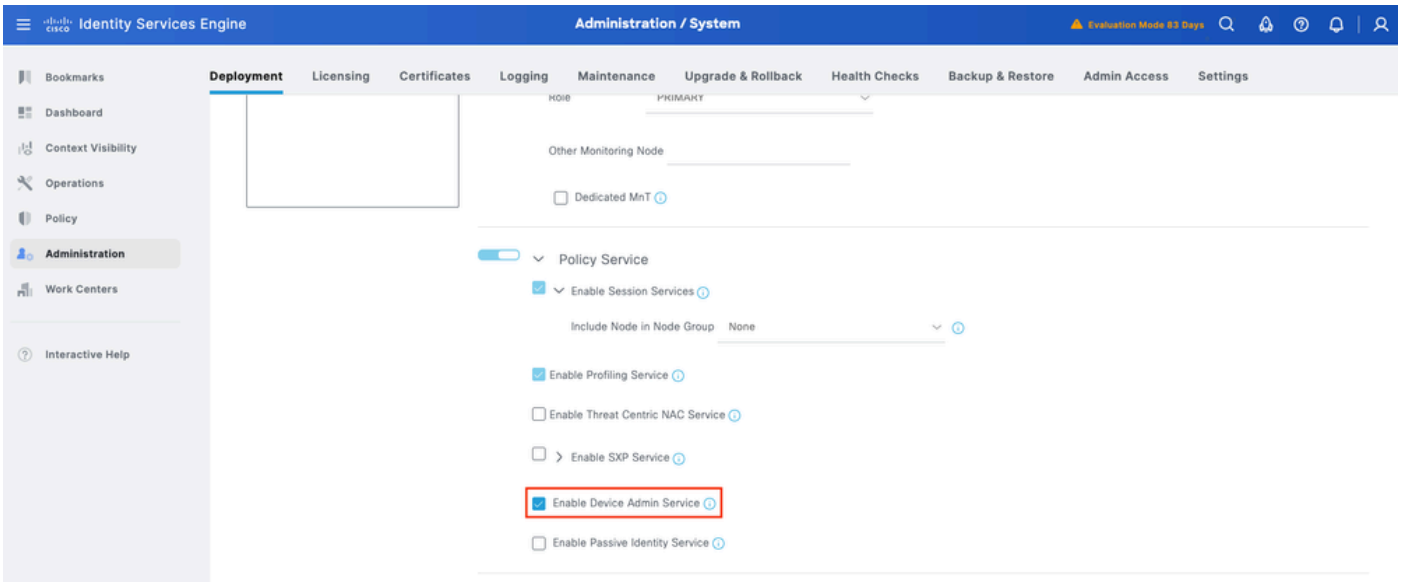
Ativar a administração de dispositivos no ISE

O serviço de Administração de dispositivo (TACACS+) não é habilitado por padrão em um nó ISE. Para ativar o TACACS+ em um nó PSN:

Etapa 1. Navegue até Administração > Sistema > Implantação. Marque a caixa de seleção ao lado do nó ISE e clique em Editar.



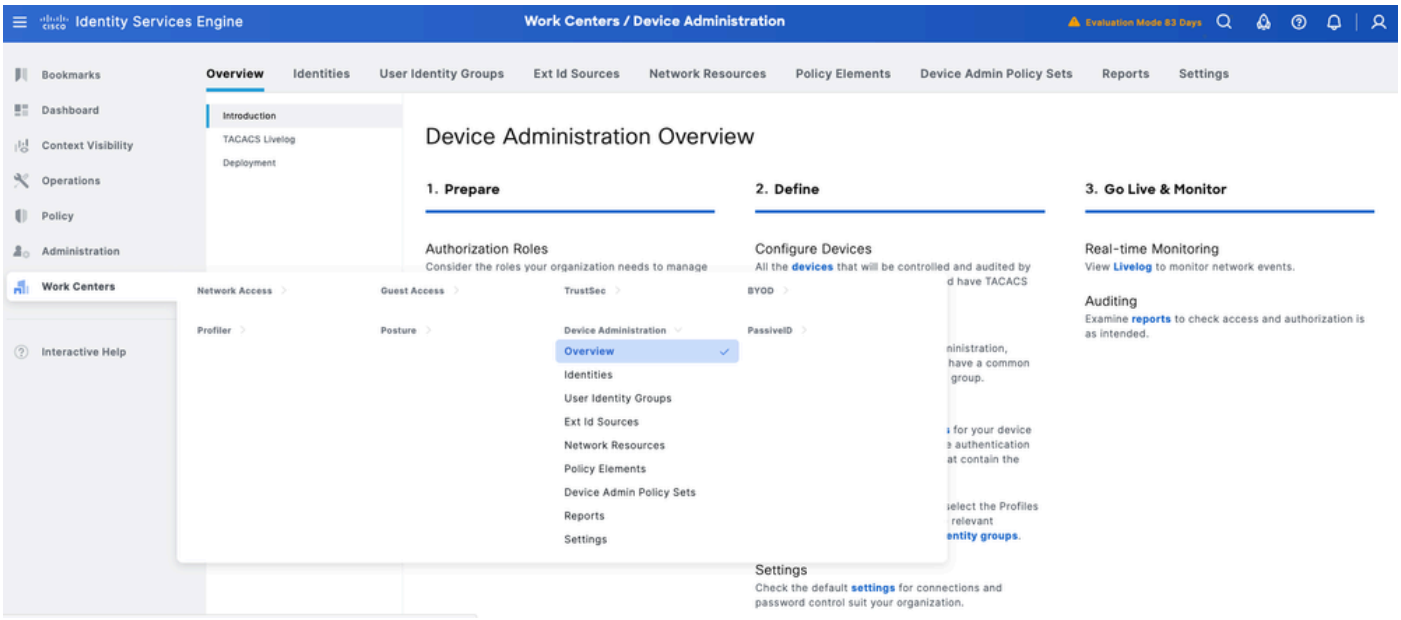
Etapa 2.Em GeneralSettings, role para baixo e marque a caixa de seleção ao lado de Enable Device Admin Service.



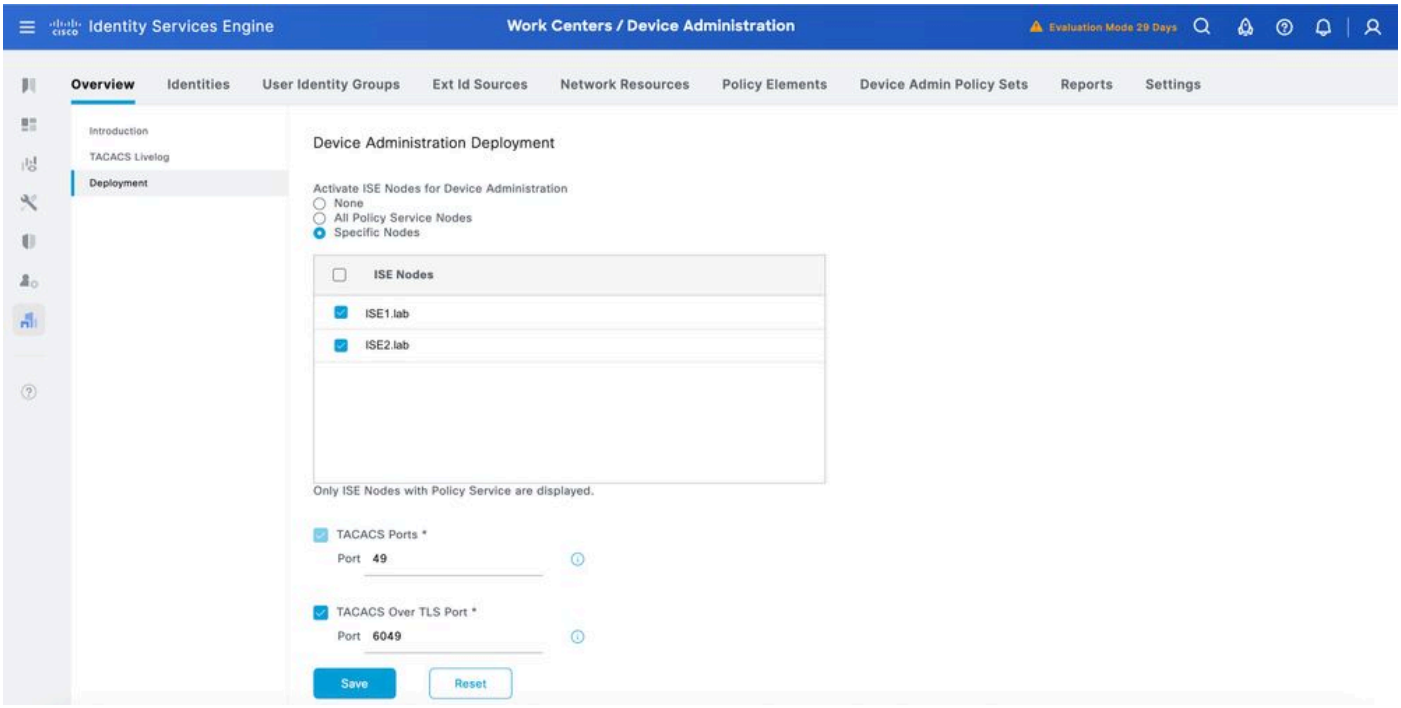
Etapa 3. Salvar a configuração. O Device Admin Service agora está habilitado no ISE.

Habilitar TACACS sobre TLS

Etapa 1.Navegue até Centros de trabalho > Administração do dispositivo > Visão geral.



Etapa 2.Clique em Deployment. Selecione os nós PSN onde deseja habilitar TACACS sobre TLS.

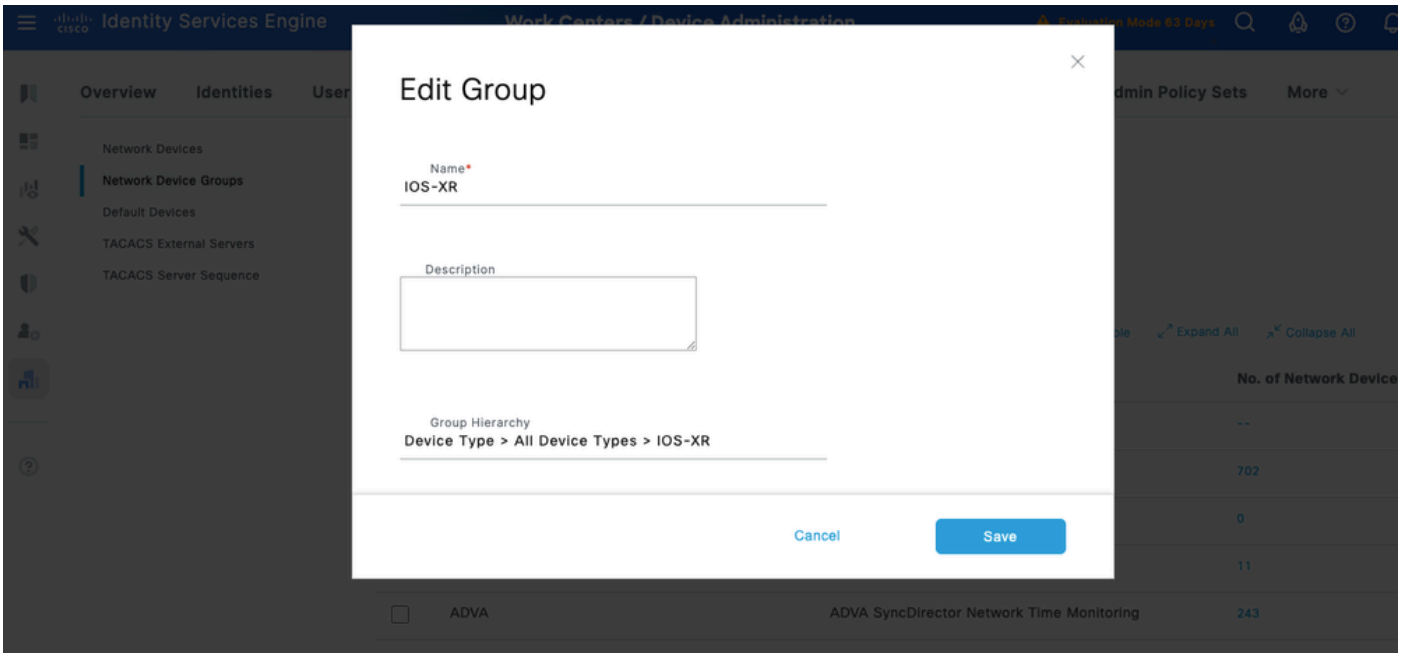


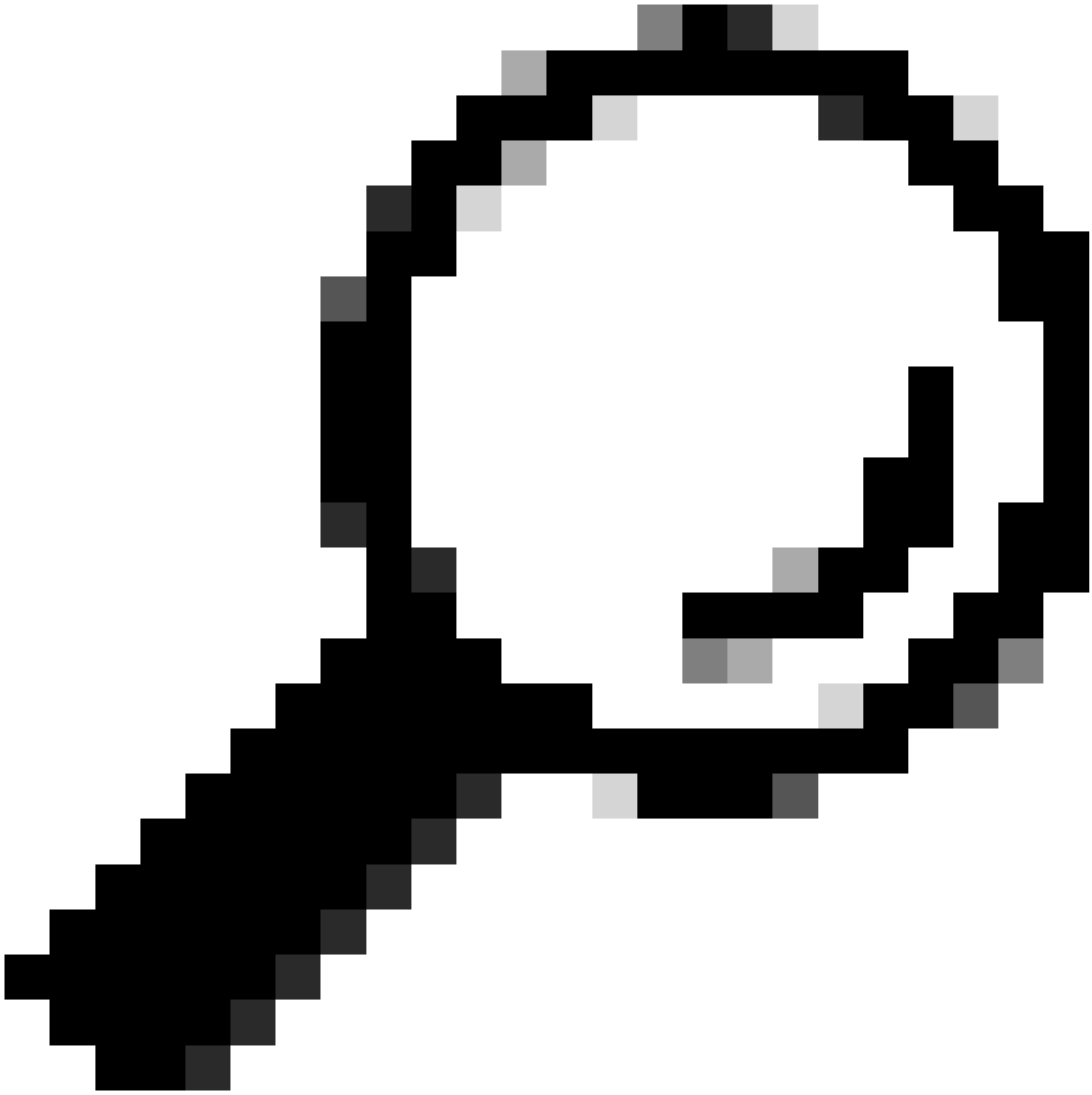
Etapa 3.Mantenha a porta padrão 6049 ou especifique uma porta TCP diferente para TACACS sobre TLS e clique em Save.

Criar dispositivo de rede e grupos de dispositivo de rede

O ISE fornece um agrupamento eficiente de dispositivos com várias hierarquias de grupos de dispositivos. Cada hierarquia representa uma classificação distinta e independente dos dispositivos de rede.

Etapa 1.Navegue até Centros de trabalho > Administração de dispositivos > Recursos de rede.Clique em Grupos de dispositivos de rede e crie um grupo com o nome IOS XR.

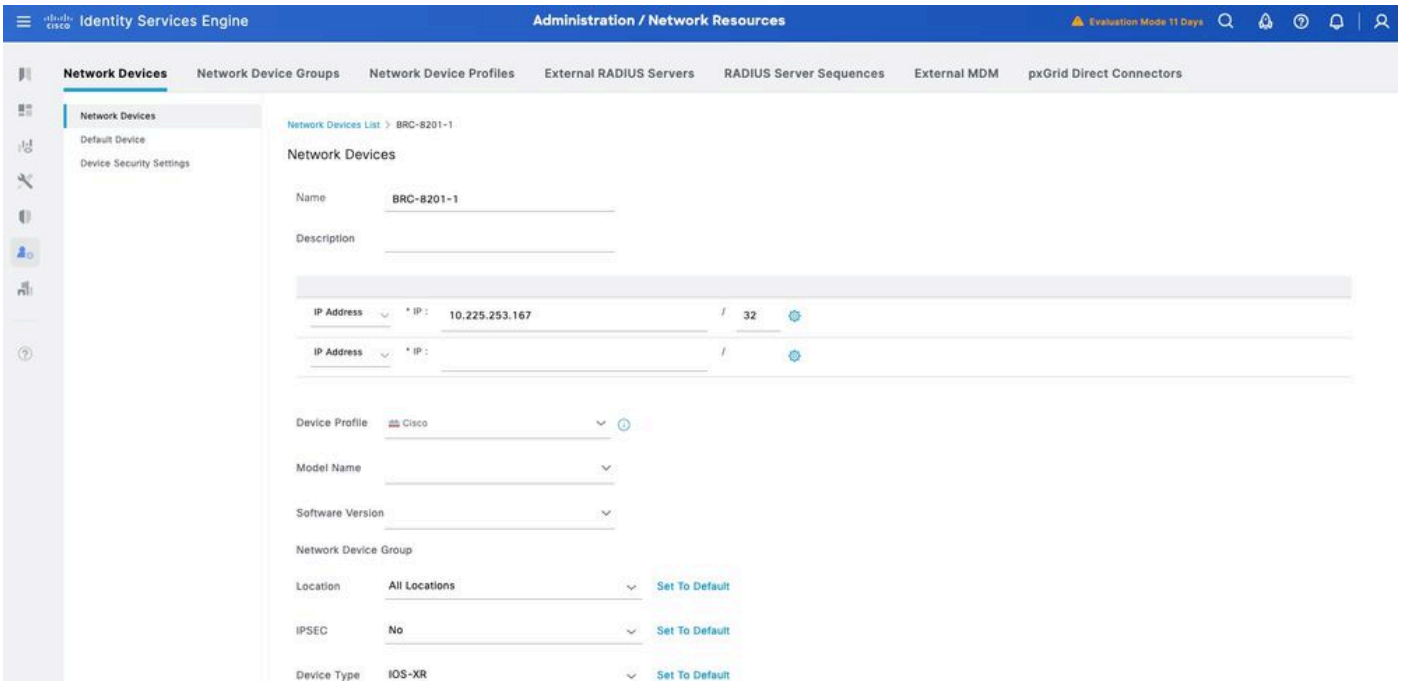

Identity Services Engine
Work Centers / Device Administration
Overview
Identities
User
Admin Policy Sets
More
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Expand All
Collapse All
No. of Network Device
Edit Group
Name*
IOS-XR
Description
Group Hierarchy
Device Type > All Device Types > IOS-XR
Cancel
Save
ADVA
ADVA SyncDirector Network Time Monitoring
243



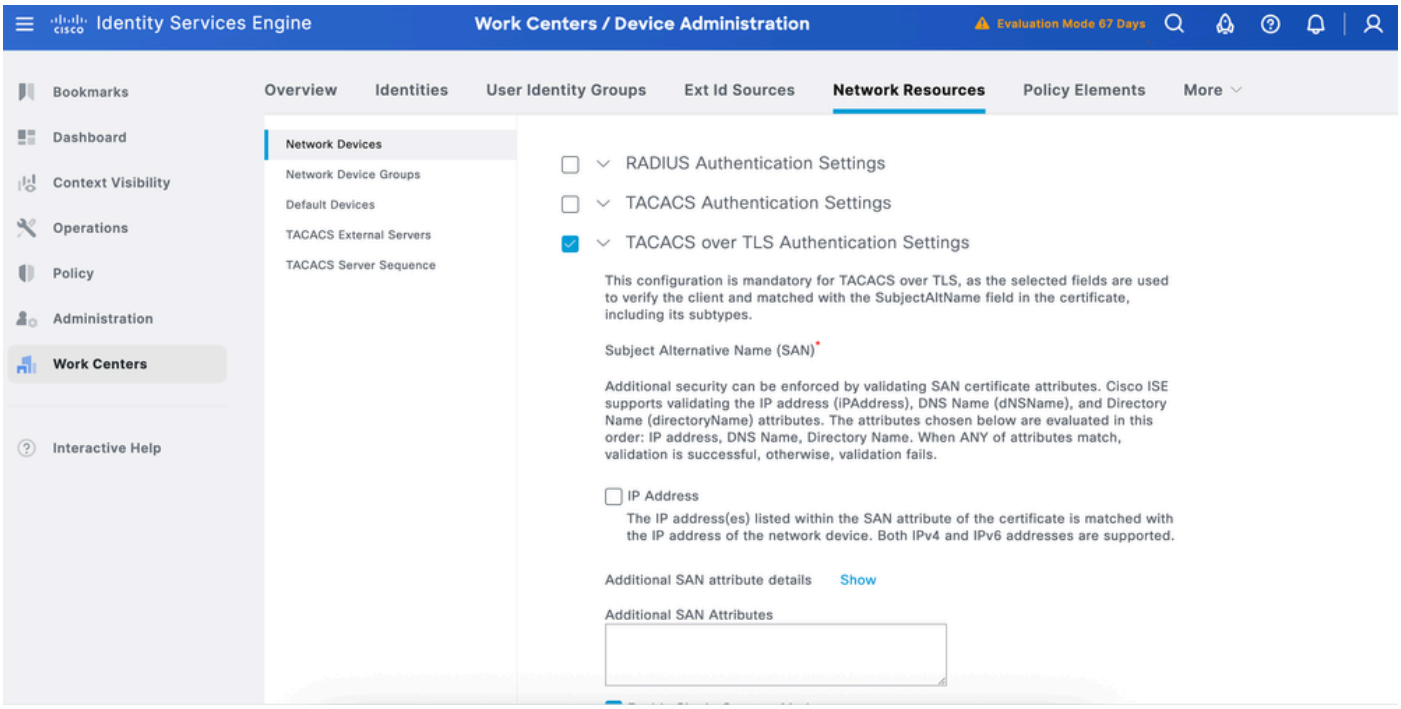
Tip: Todos os tipos de dispositivos e todos os locais são hierarquias padrão fornecidas pelo ISE. Você pode adicionar suas próprias hierarquias e definir os vários componentes na identificação de um dispositivo de rede que pode ser usado posteriormente na condição de política

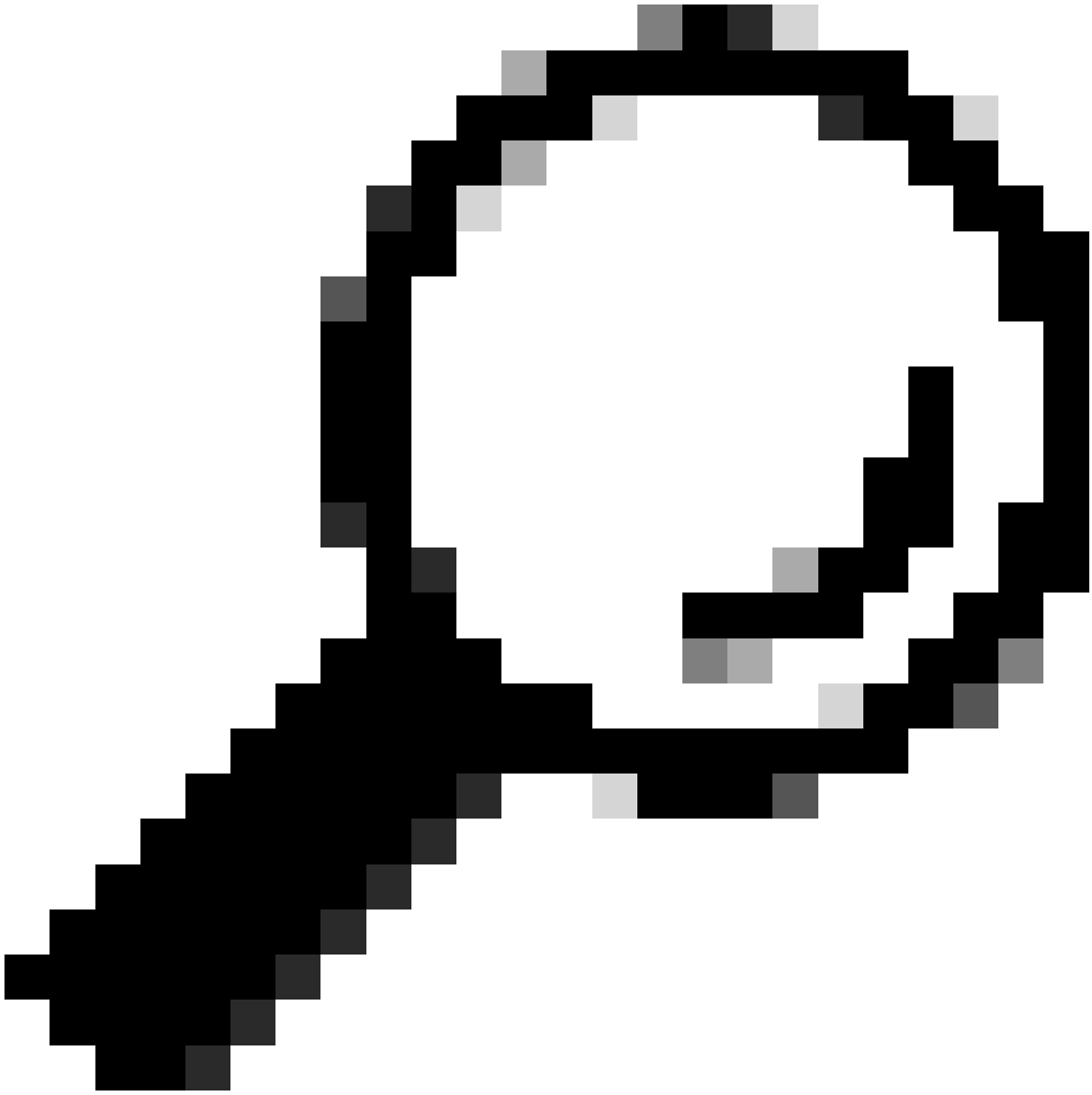
---

Etapa 2. Agora, adicione um dispositivo Cisco IOS XR como um dispositivo de rede. Navegue até Centros de trabalho > Administração de dispositivos > Recursos de rede > Dispositivos de rede. Clique em Add para adicionar um novo dispositivo de rede.



Etapa 3.Insira o endereço IP do dispositivo e certifique-se de mapear o local e o tipo de dispositivo (IOS XR) para o dispositivo. Por fim, habilite as Configurações de autenticação TACACS+ sobre TLS.



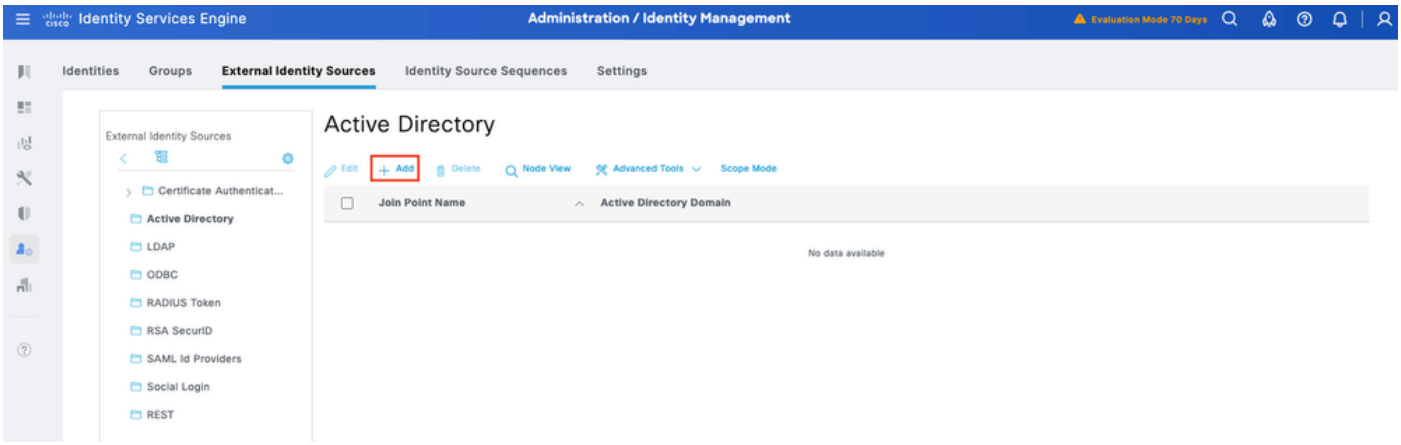


Tip: É recomendável ativar o modo de conexão única para evitar reiniciar a sessão TCP toda vez que um comando for enviado ao dispositivo.

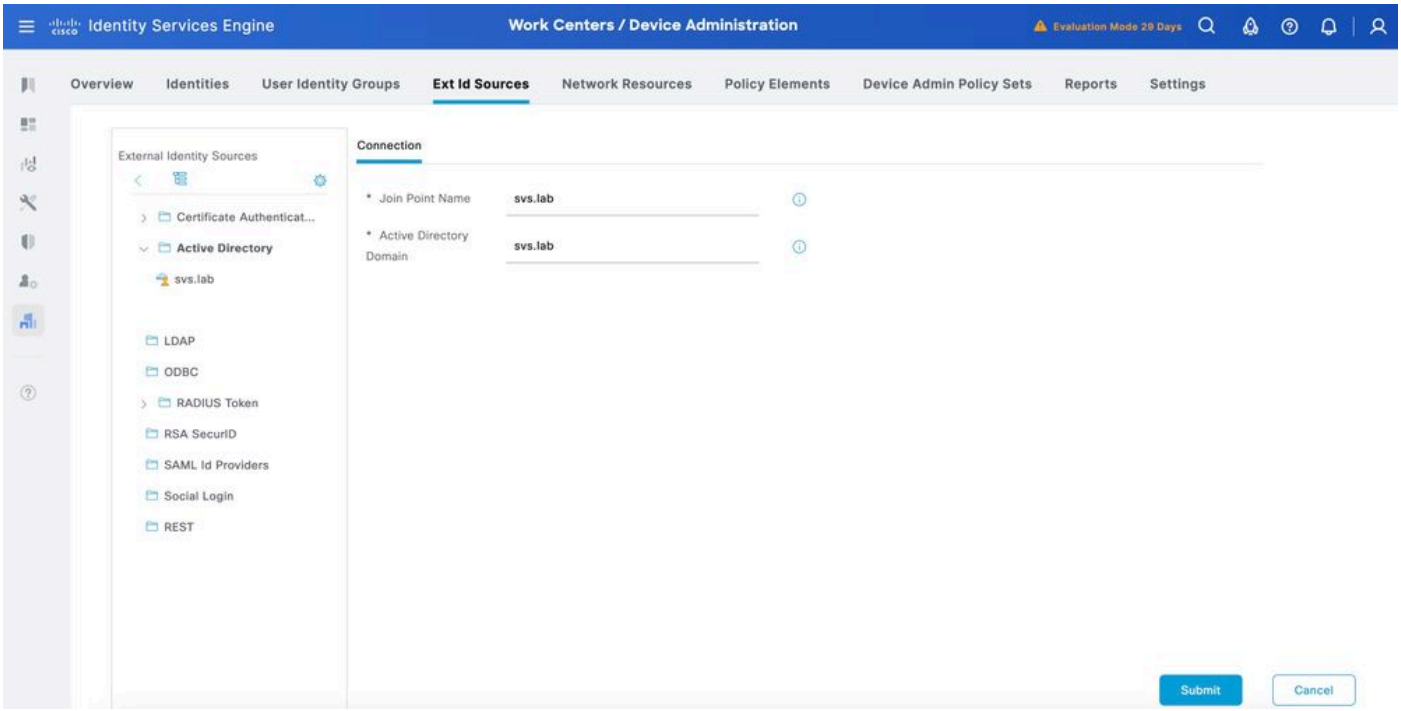
ConfigurarRepositórios de Identidade

Esta seção define um Repositório de identidades para os administradores de dispositivos, que pode ser o ISE Internal Users e qualquer External Identity Sources com suporte. Aqui usa o Ative Diretory (AD), uma fonte de identidade externa.

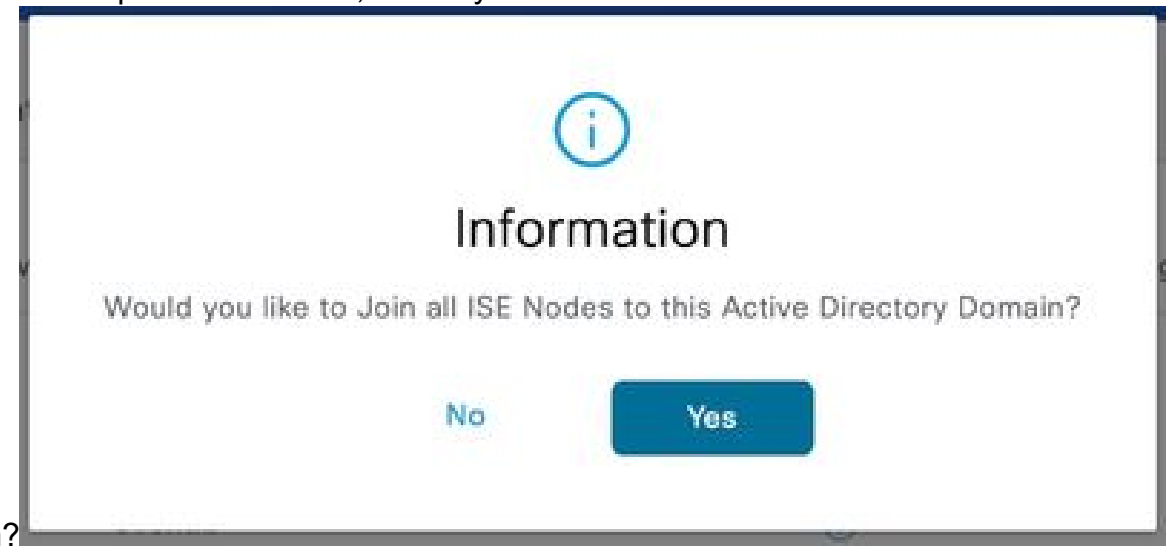
Etapa 1. Navegue até Administração > Gerenciamento de identidades > Repositórios de identidades externos > Ative Diretory. Clique em Adicionar para definir um novo ponto conjunto do AD.



Etapa 2. Especifique o nome do ponto de junção e o nome de domínio do AD e clique em Enviar.

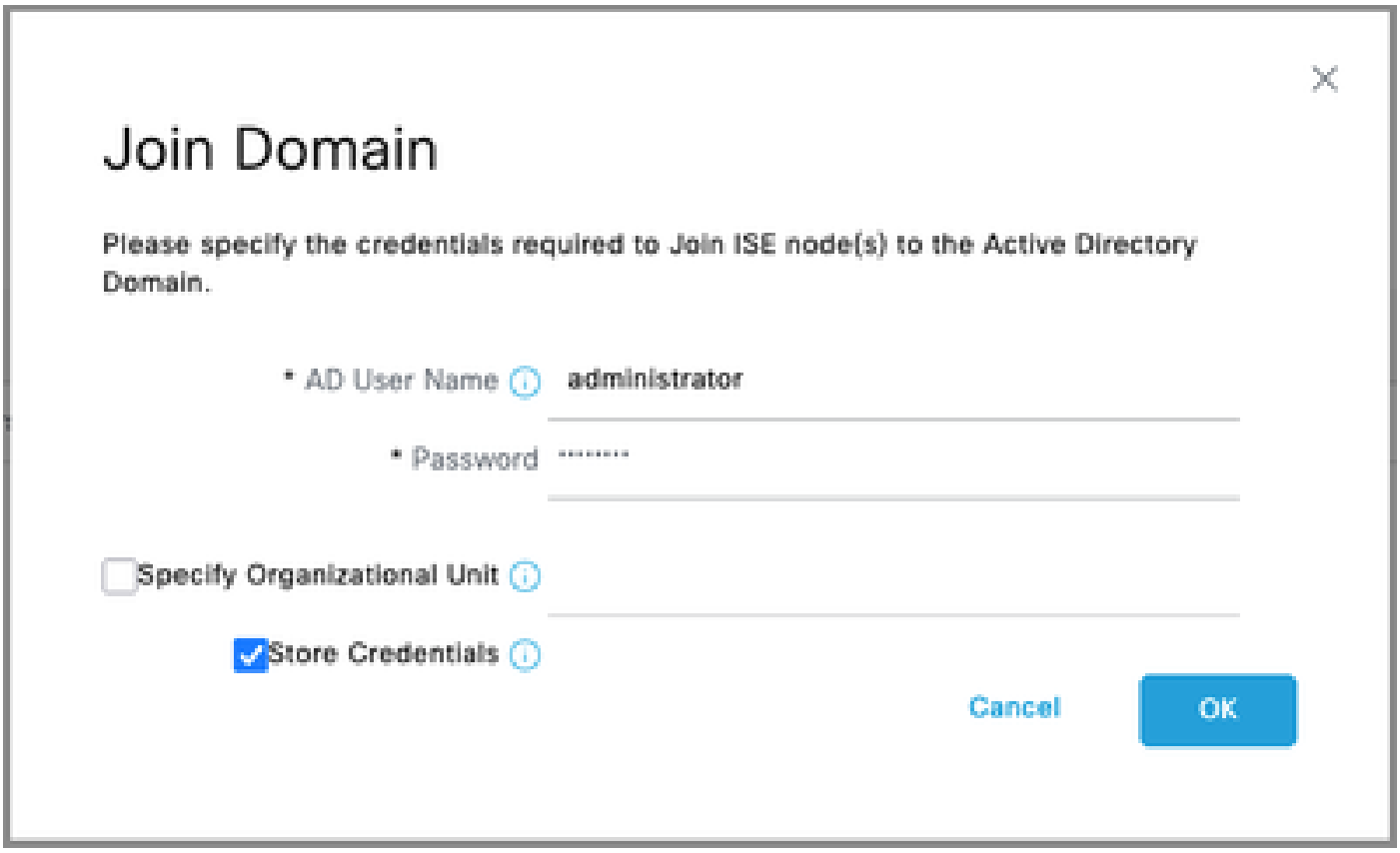


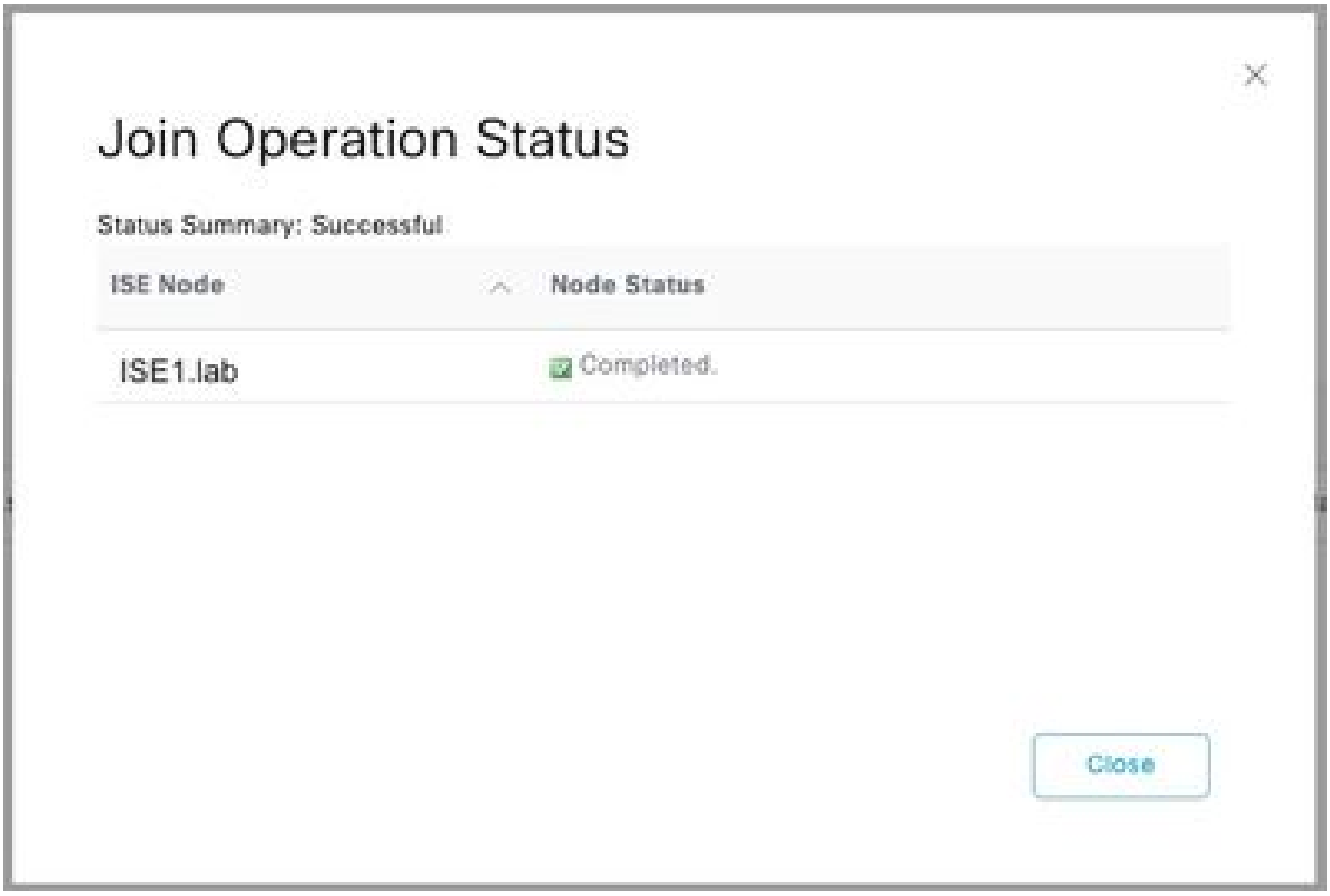
Etapa 3.Clique em Yes quando solicitado, Would you like to Join all ISE Nodes to this Ative Diretory Domain?



Etapa 4.Insira as credenciais com privilégios de associação do AD e Ingresse no ISE para o AD.

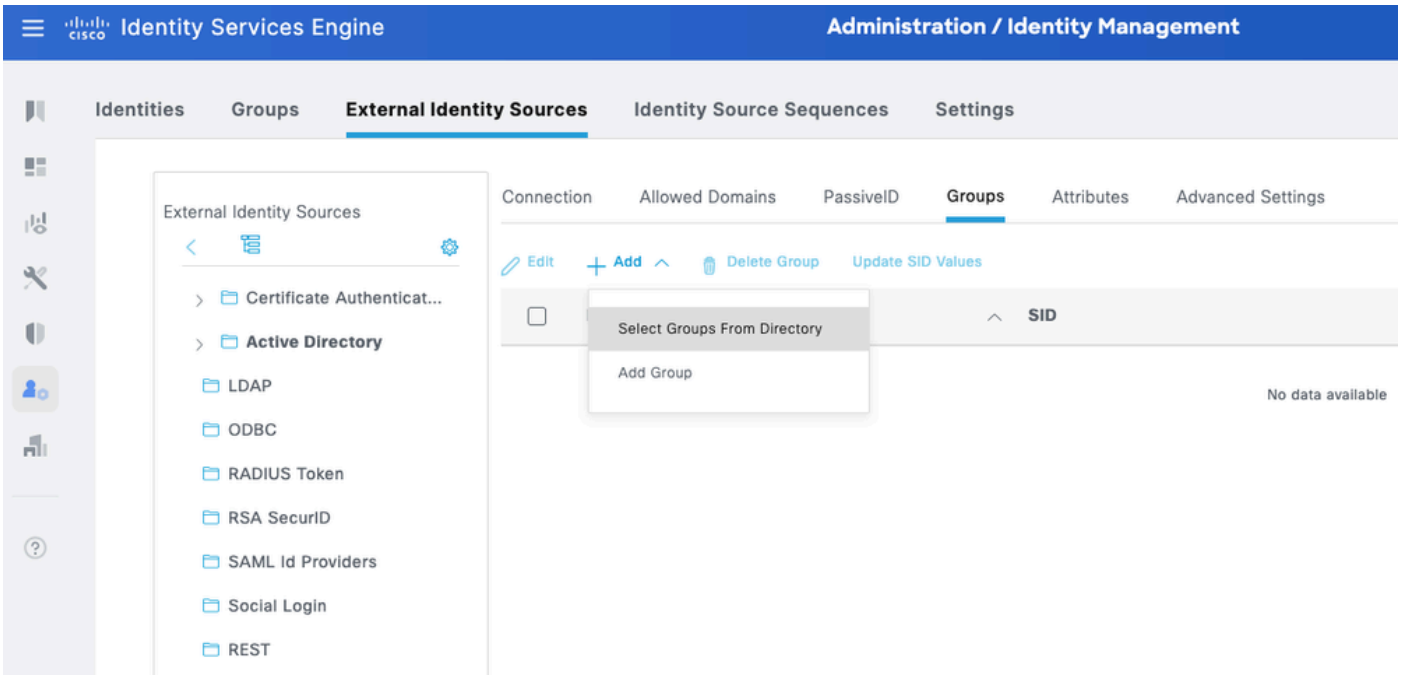
Verifique o Status para verificar se ele está operacional.

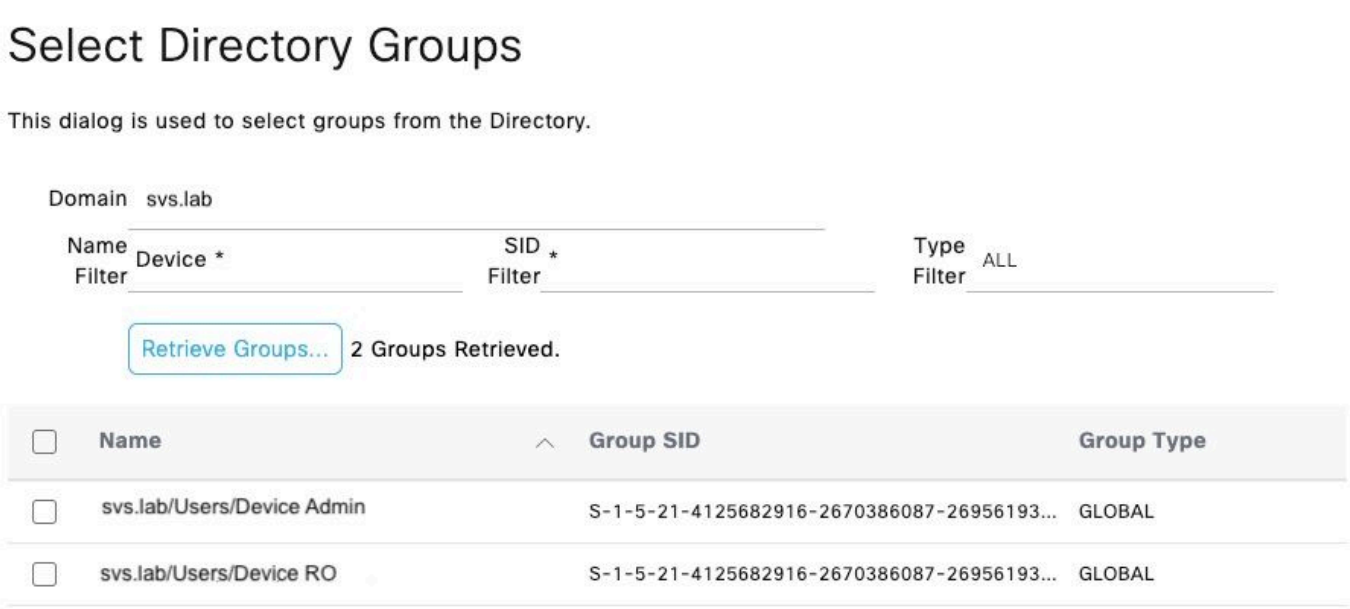


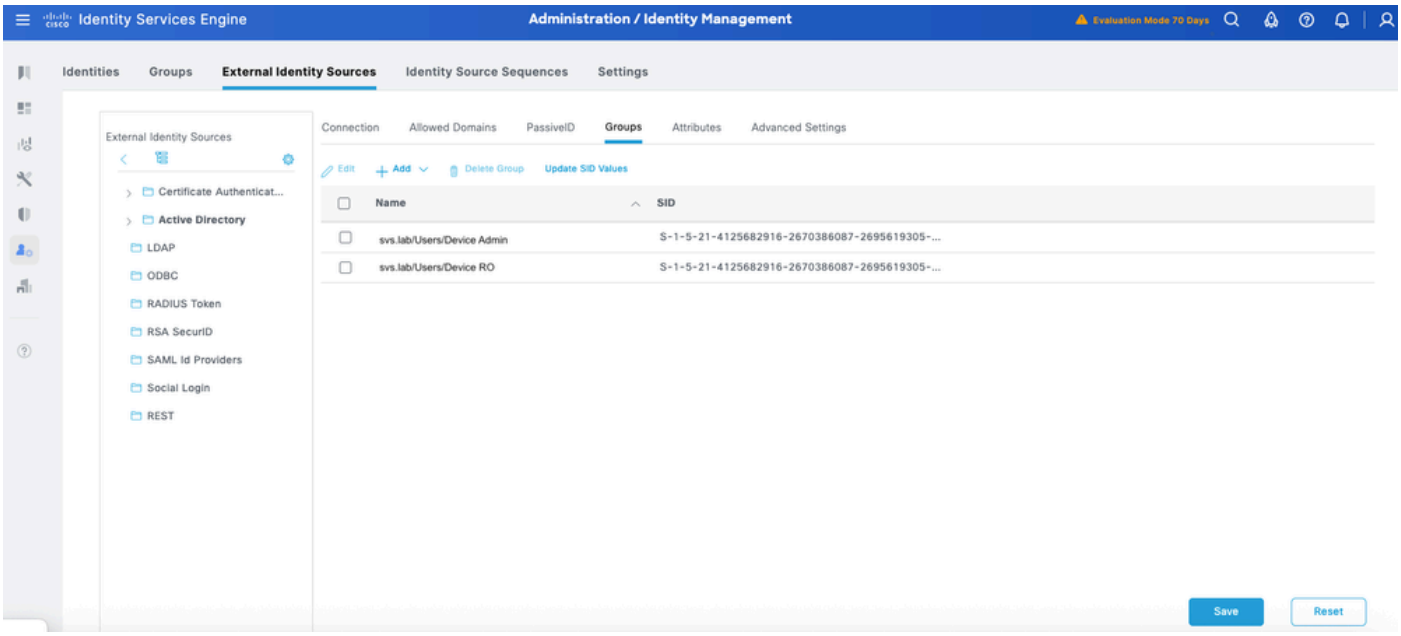


Etapa 5.Navegue até a guia Groups e clique em Add para obter todos os grupos necessários com

base nos quais os usuários estão autorizados para o acesso ao dispositivo. Este exemplo mostra os grupos usados na Diretiva de autorização.







Configurar perfis TACACS+

Mapeie os perfis TACACS+ para funções de usuário nos dispositivos Cisco IOS XR. Neste exemplo, eles são definidos:

- Administrador do sistema raiz - Essa é a função com maior privilégio no dispositivo. O usuário com a função de administrador do sistema raiz tem acesso administrativo total a todos os comandos do sistema e recursos de configuração.
- Operador -Essa função destina-se a usuários que precisam de acesso somente leitura ao sistema para fins de monitoramento e solução de problemas.

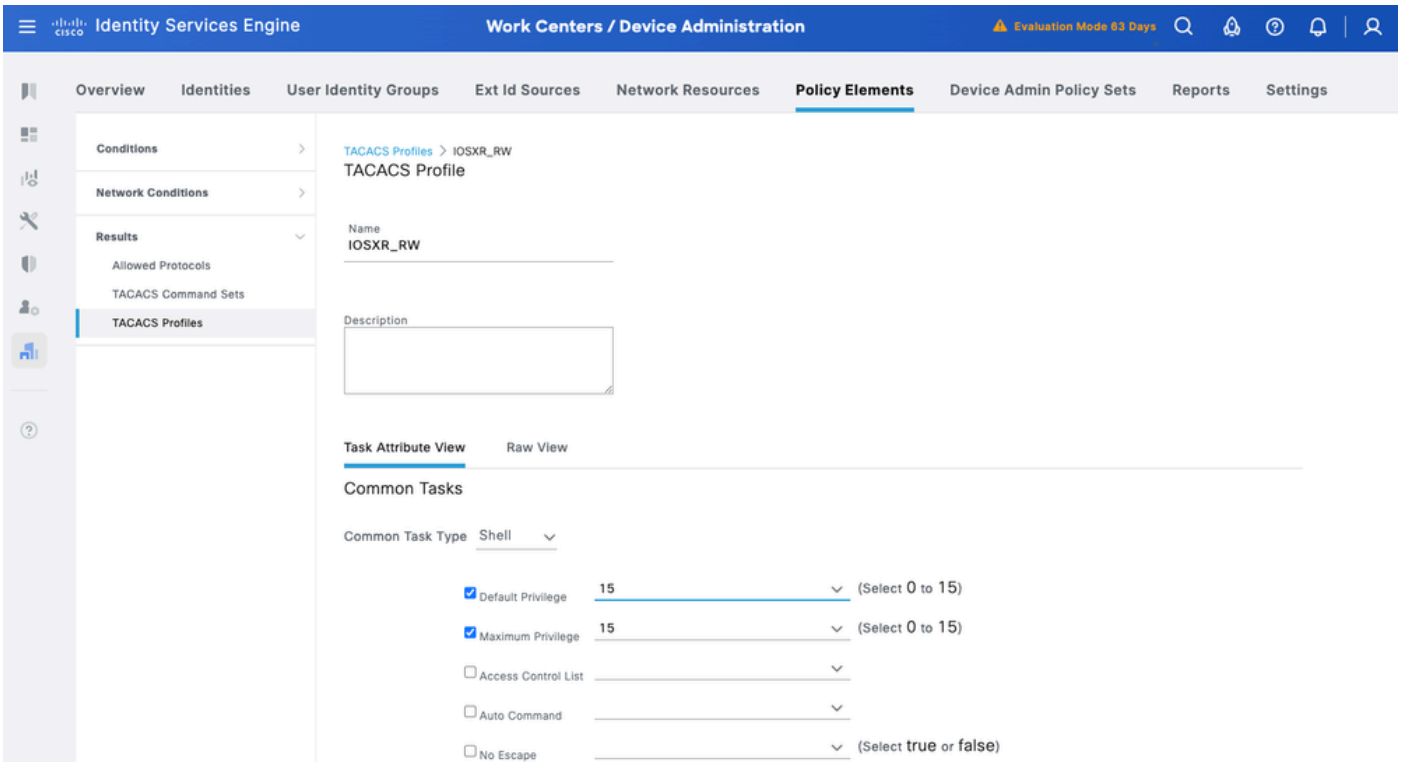
Defina dois perfis TACACS+: IOSXR_RW e IOSXR_RO.

IOS XR_RW - Perfil do administrador

Etapa 1. Navegue até Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS. Adicione um novo Perfil TACACS e nomeie-o como IOSXR_RW.

Etapa 2. Verifique e defina o Privilégio Padrão e o Privilégio Máximo como 15.

Etapa 3. Confirme a configuração e salve.

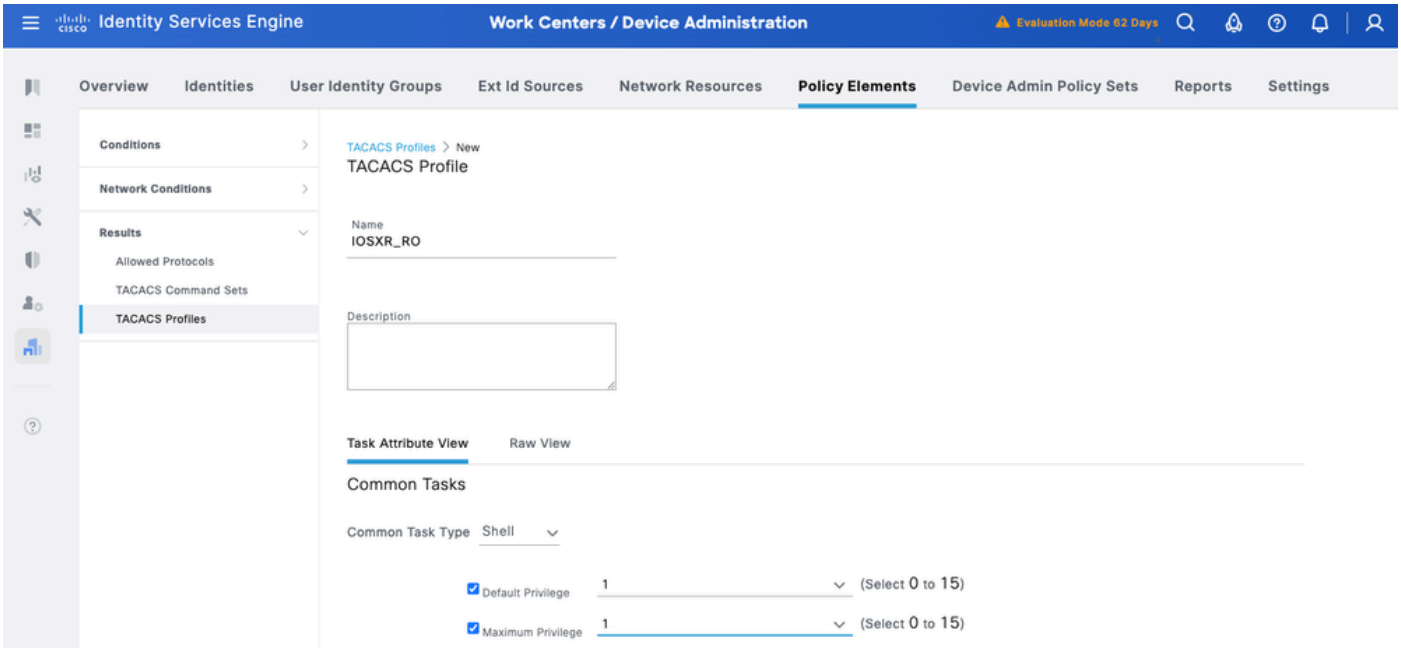


IOS XR_RO - Perfil do operador

Etapa 1. Navegue até Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS. Adicione um novo Perfil TACACS e nomeie-o como IOSXR_RO.

Etapa 2. Verifique e defina o Privilégio Padrão e o Privilégio Máximo como 1.

Etapa 3.Confirme a configuração e salve.



Configurar conjuntos de comandos TACACS+

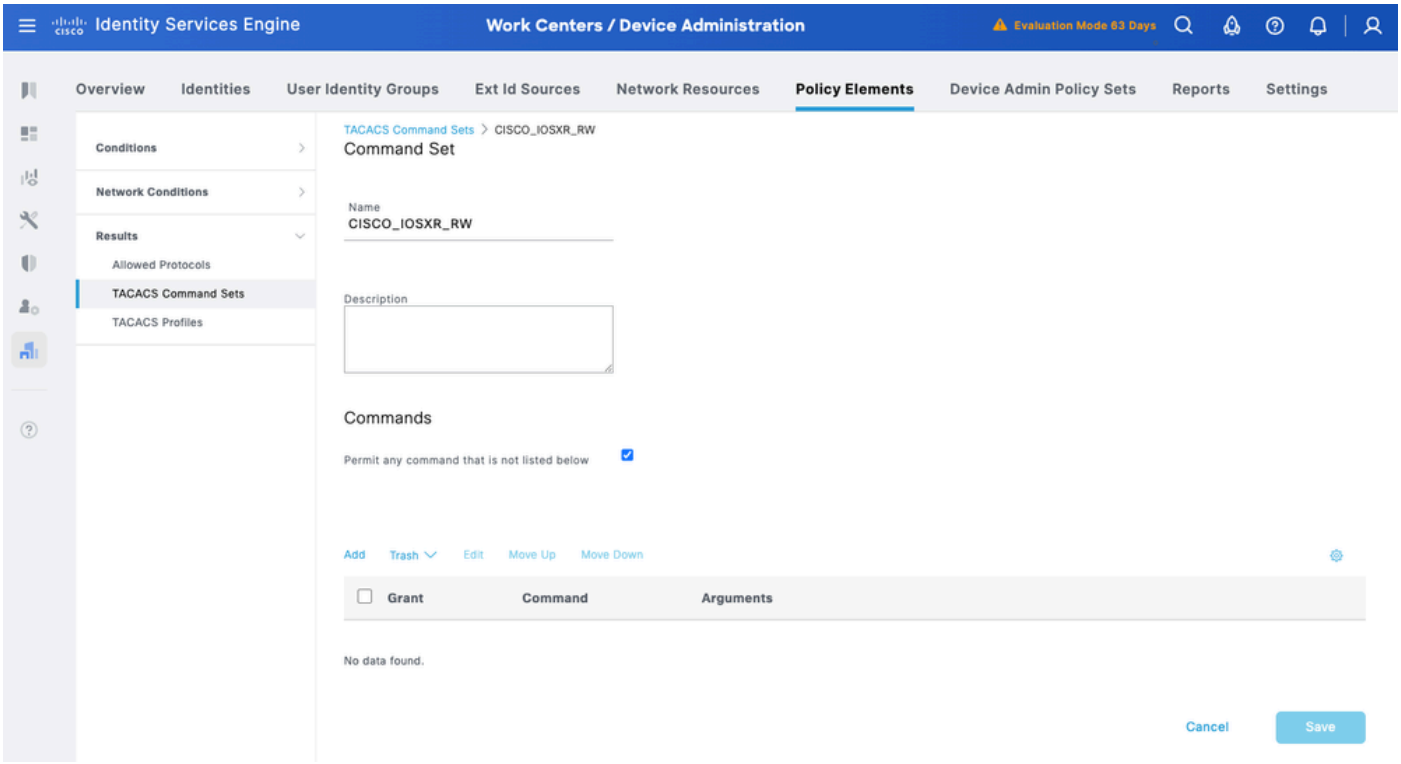
Defina os conjuntos de comandos TACACS+: Neste exemplo, eles são definidos como

CISCO_IOSXR_RW e CISCO_IOSXR_RO.

CISCO IOS XR RW - Conjunto de Comandos do Administrador

Etapa 1. Navegue até Centros de Trabalho > Administração de Dispositivo > Elementos de Política > Resultados > Conjuntos de Comandos TACACS. Adicione um novo Conjunto de Comandos TACACS e nomeie-o CISCO_IOSXR_RW.

Etapa 2. Marque a caixa de seleção Permitir qualquer comando que não esteja listado abaixo (isso permite qualquer comando para a função de administrador) e clique em Salvar.



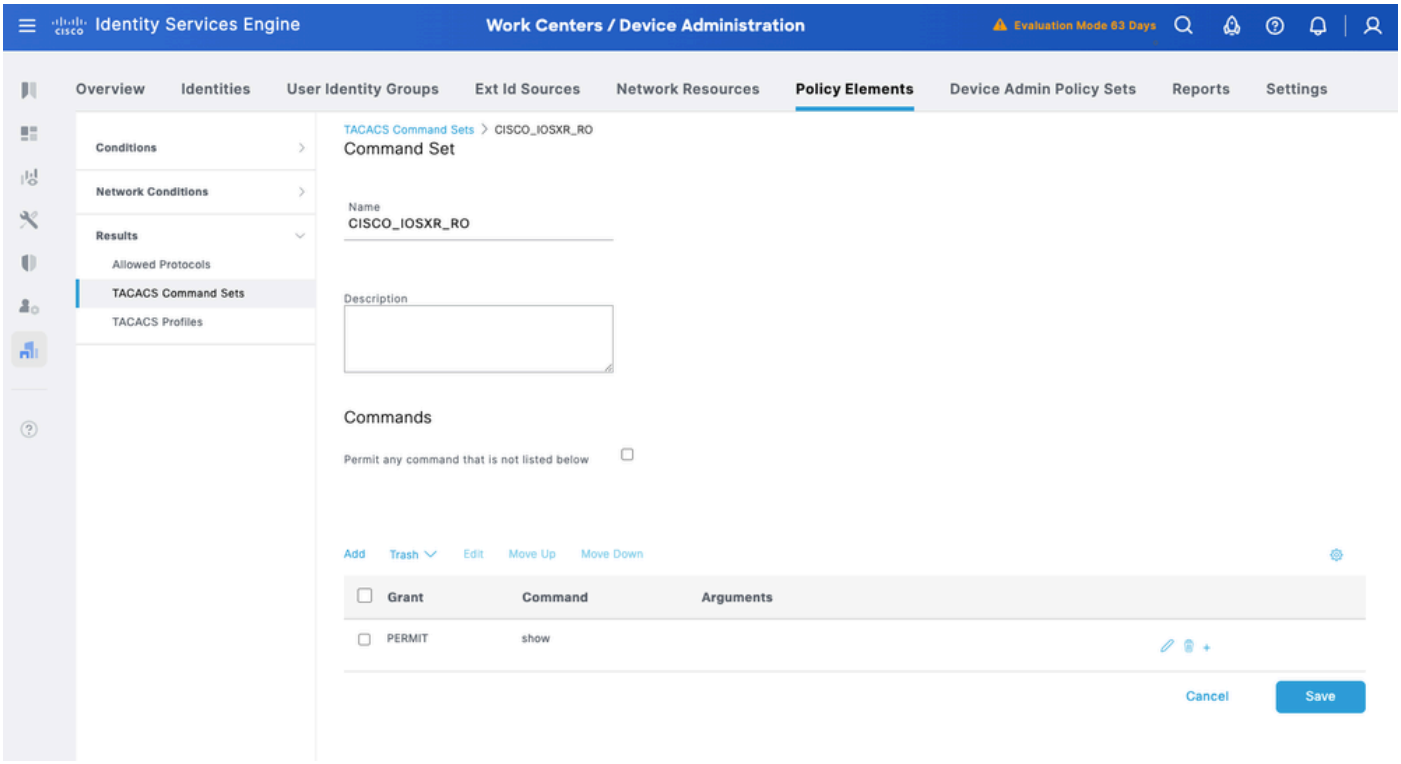
CISCO IOS XR RO - Conjunto de comandos do operador

Etapa 1. Na interface do usuário do ISE, navegue até Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Conjuntos de comandos TACACS. Adicione um novo Conjunto de comandos TACACS e nomeie-o CISCO_IOSXR_RO.

Etapa 2. Na seção Comandos, adicione um novo comando.

Etapa 3. Selecione Permit na lista drop-down da coluna Grant e digite show na coluna Command; e clique na seta verificar.

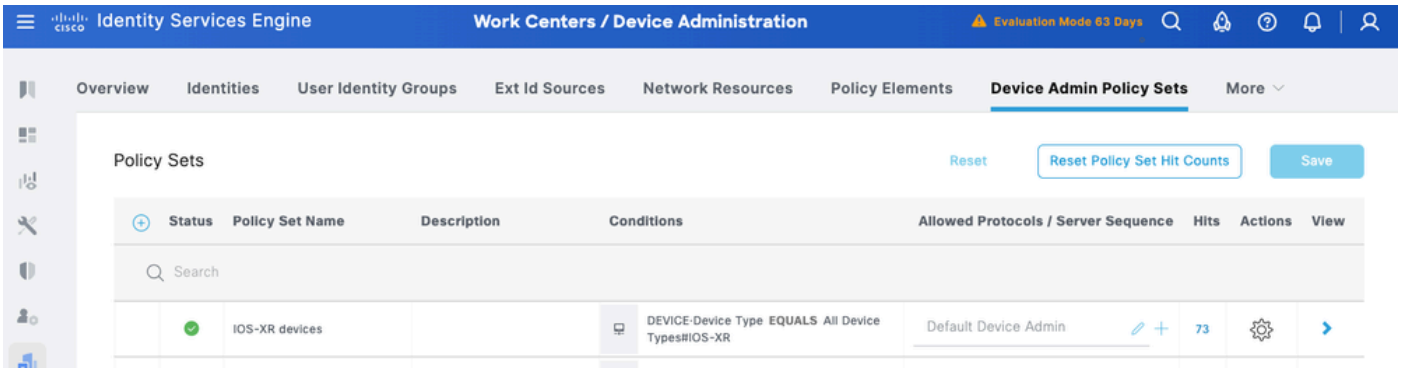
Etapa 4. Confirme os dados e clique em Salvar.



ConfigurarConjuntos de Políticas de Administração do Dispositivo

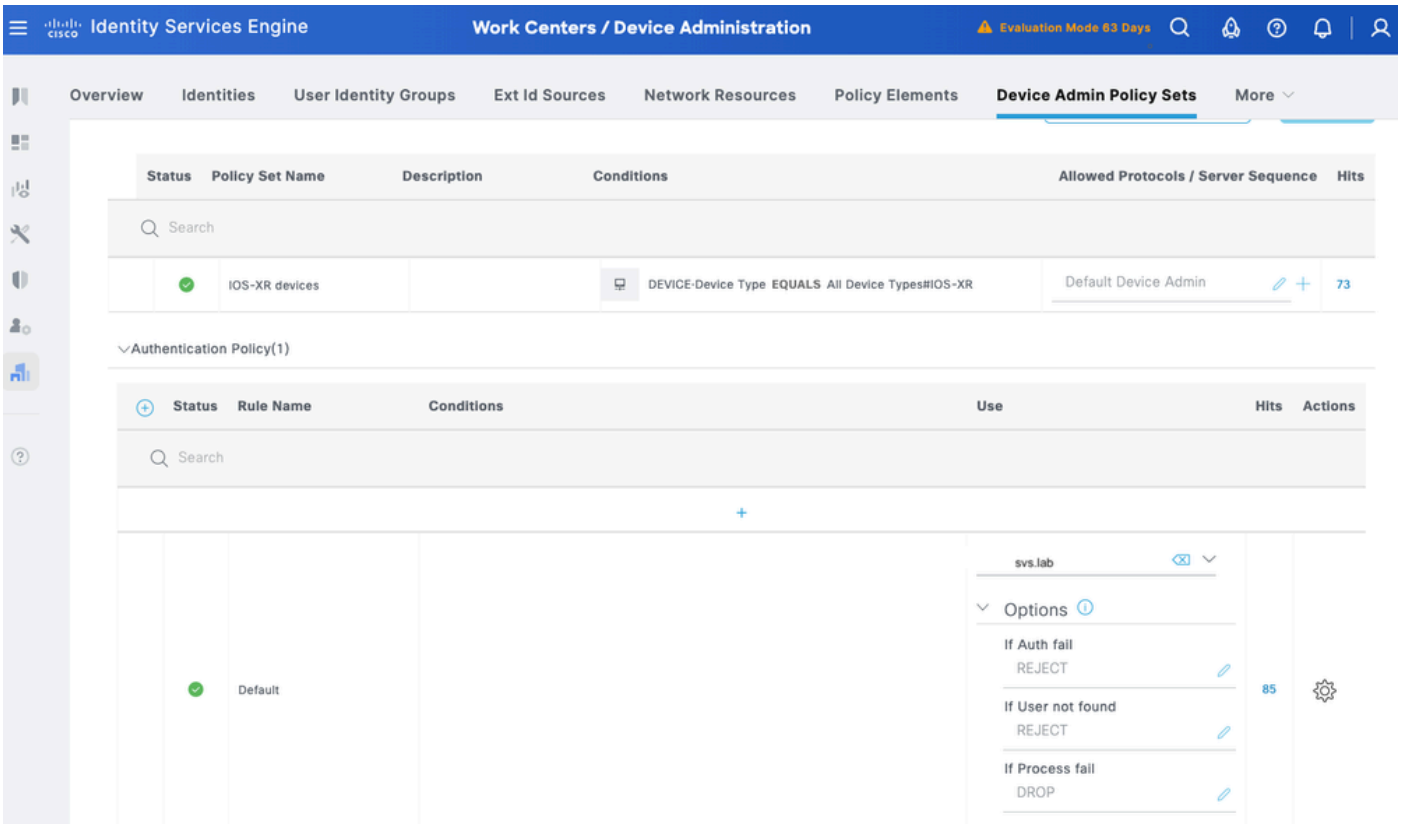
Os conjuntos de políticas são ativados por padrão para a Administração de dispositivos. Os conjuntos de políticas podem dividir as políticas com base nos tipos de dispositivo para facilitar a aplicação de perfis TACACS.

Etapa 1.Navegue até Centros de trabalho > Administração de dispositivos > Conjuntos de diretivas de administração de dispositivos. Adicione um novo conjunto de políticas de dispositivos IOS XR. Sob condição, especifique DEVICE:Device Type EQUALS All Device Types#IOS XR. Em Allowed Protocols, selecione Default Device Admin.



Etapa 2. Clique em Salvar e clique na seta para a direita para configurar esse Conjunto de políticas.

Etapa 3. Crie a Política de Autenticação. Para a autenticação, use o AD como o ID Store. Deixe as opções padrão em If Auth fail, If User not found e If Process fail.

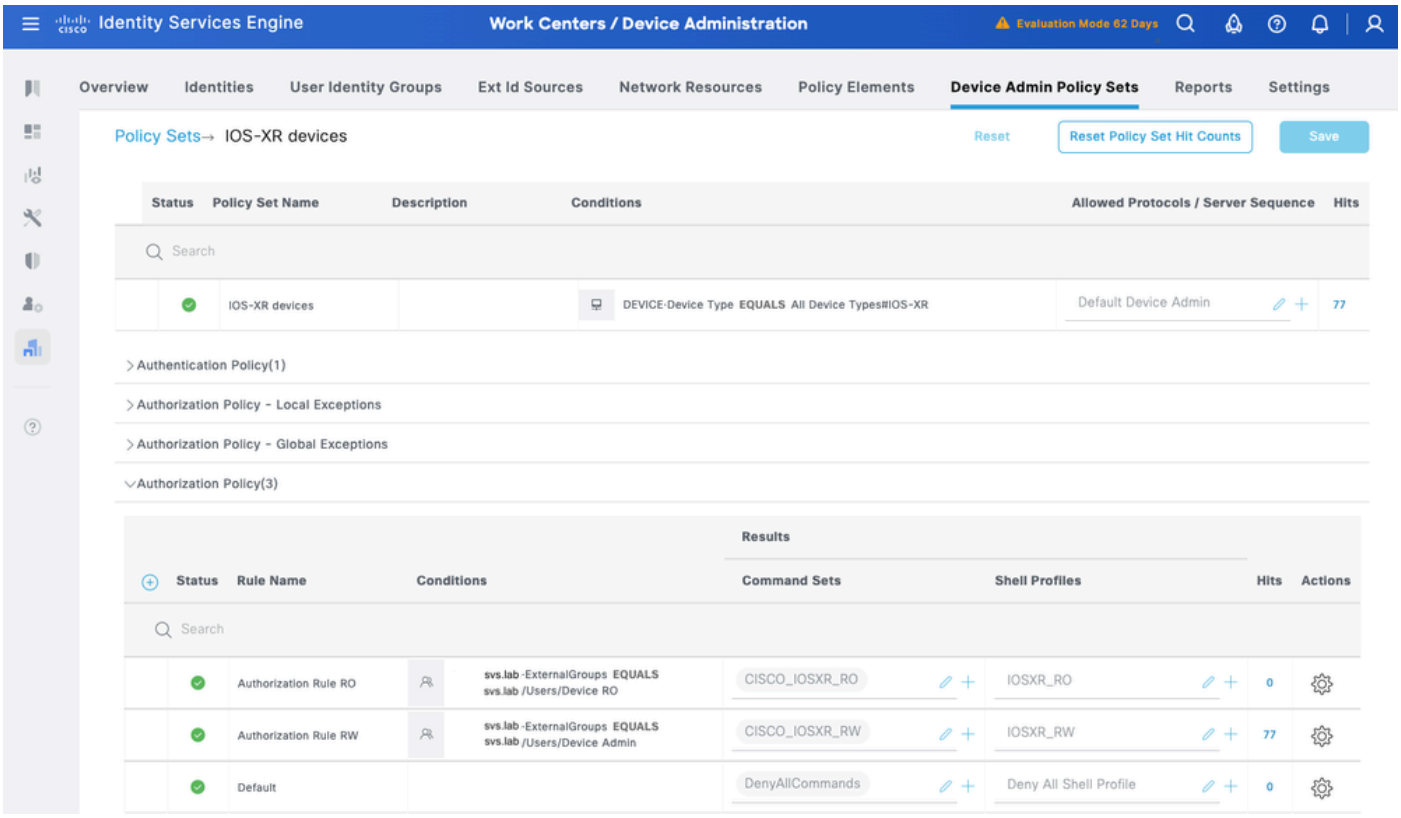


Etapa 4. Defina a Política de Autorização.

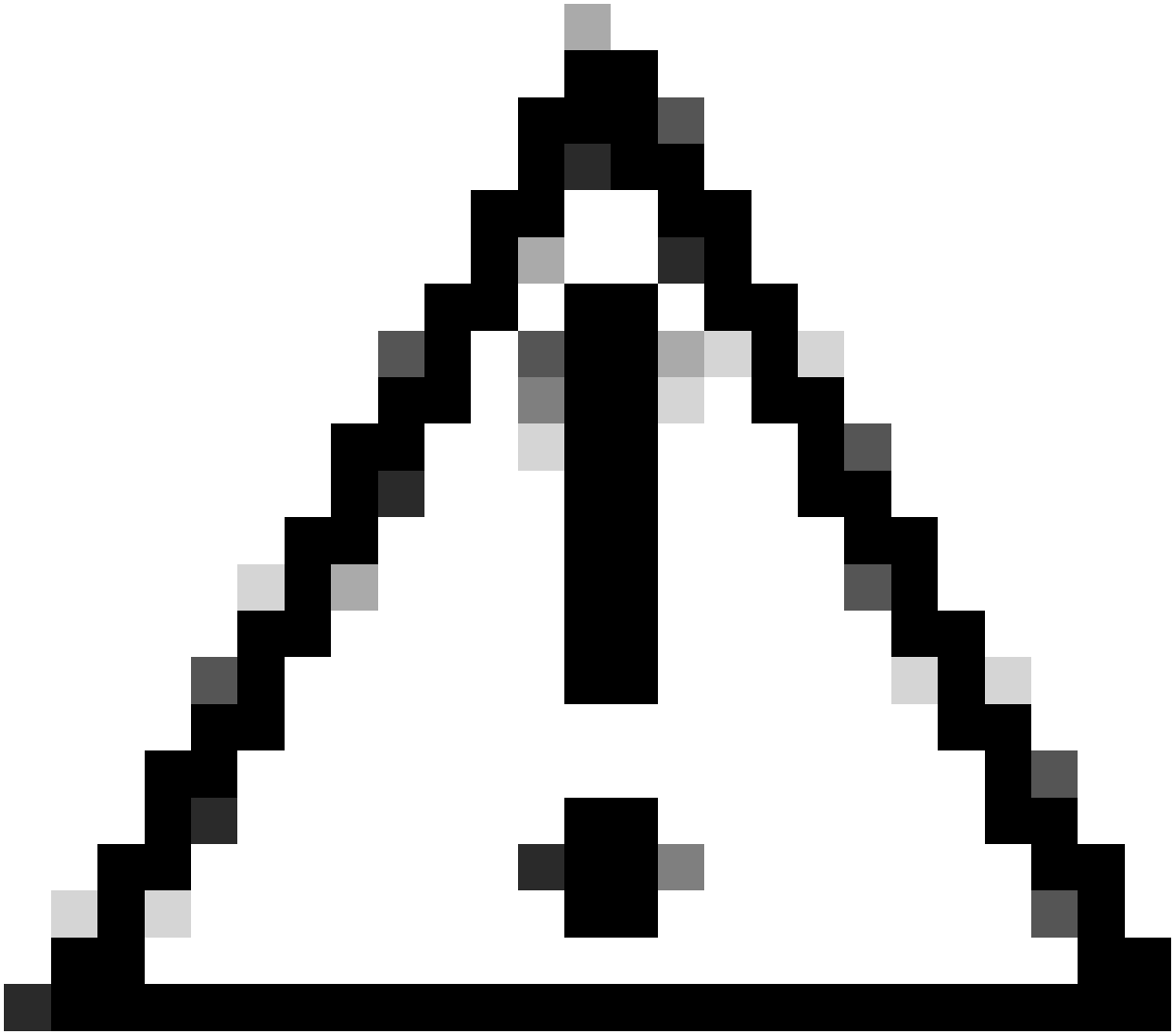
Crie a política de autorização com base nos grupos de usuários no Ative Diretory (AD).

Por exemplo:

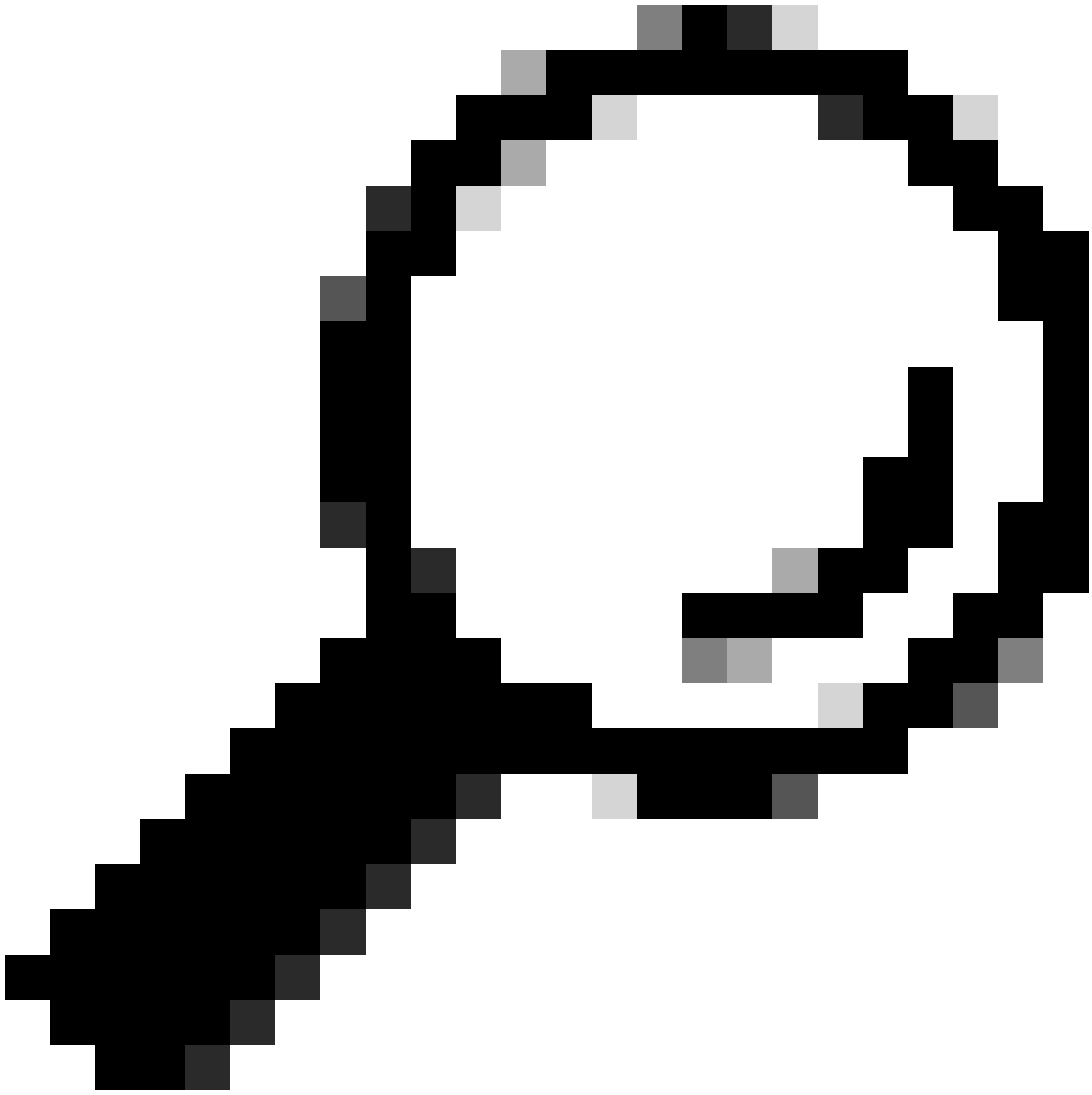
- Os usuários do grupo AD Device RO recebem o conjunto de comandos CISCO_IOSXR_RO e o perfil do shell IOSXR_RO .
- Os usuários do grupo AD Device Admin recebem o conjunto de comandos CISCO_IOSXR_RW e o perfil do IOSXR_RW Shell.



Parte 2 - Configurar o Cisco IOS XR para TACACS+ sobre TLS 1.3



Caution: Verifique se a conexão do console pode ser alcançada e se está funcionando corretamente.



Tip: É recomendável configurar um usuário temporário e alterar os métodos de autenticação e autorização AAA para usar credenciais locais em vez de TACACS ao fazer alterações de configuração, para evitar ser bloqueado fora do dispositivo.

Configurações iniciais

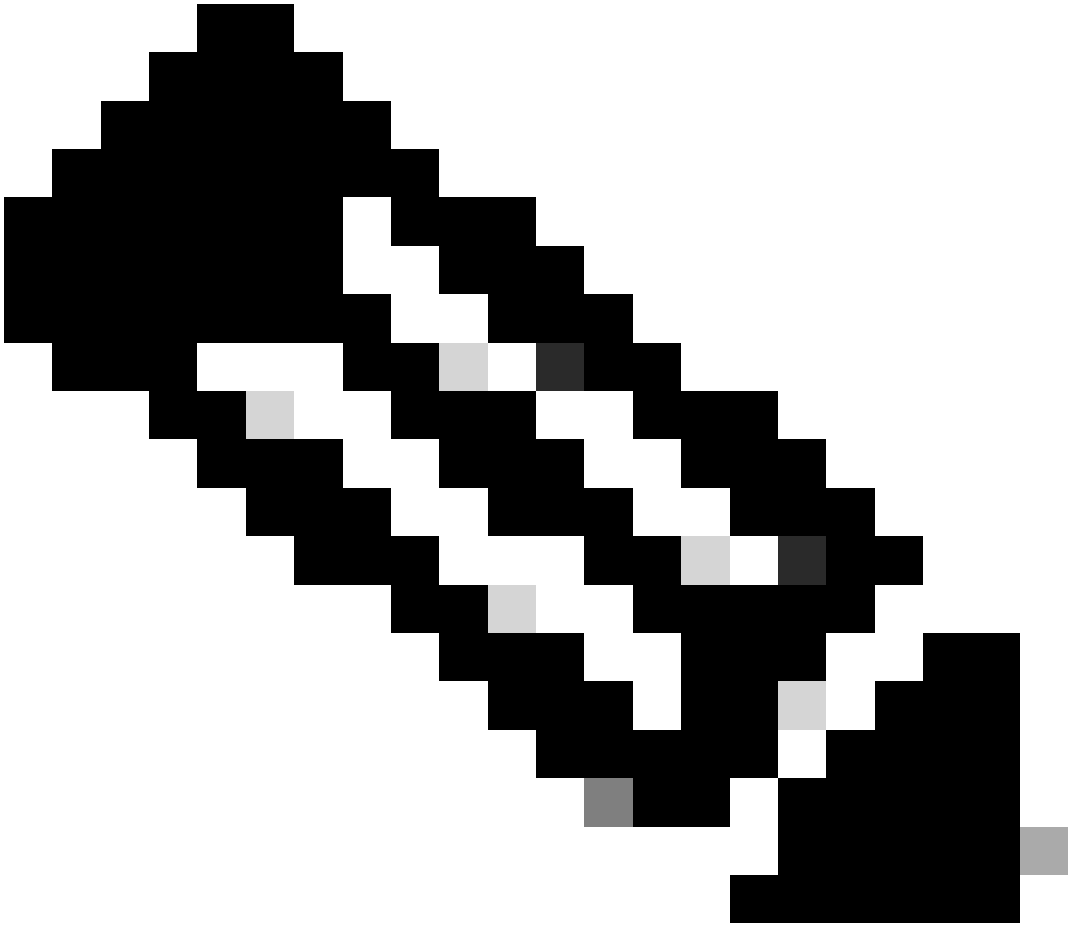
Etapa 1. Verifique se o servidor de nomes (DNS) está configurado e se o roteador consegue resolver com êxito os Nomes de Domínio Frequentemente Qualificados (FQDNs), especialmente o FQDN do servidor ISE.

```
domain vrf mgmt name svs.lab
domain vrf mgmt name-server 10.225.253.247
no domain vrf mgmt lookup disable
```

```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Etapa 2. Limpe todos os pontos de confiança e certificados antigos/não usados. Verifique se não há pontos de confiança e certificados antigos presentes. Se você vir entradas antigas, remova-as/limpe-as.

```
show crypto ca trustpoint
show crypto ca certificates

(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



Note: Você pode criar manualmente um novo par de chaves RSA e anexá-lo sob o ponto confiável. Se você não criar um, o par de chaves padrão será usado. A definição do par de chaves ECC sob o ponto de confiança não é suportada atualmente.

Configurar Ponto de Confiabilidade

Etapa 1. Configuração do par de chaves (opcional).

<#root>

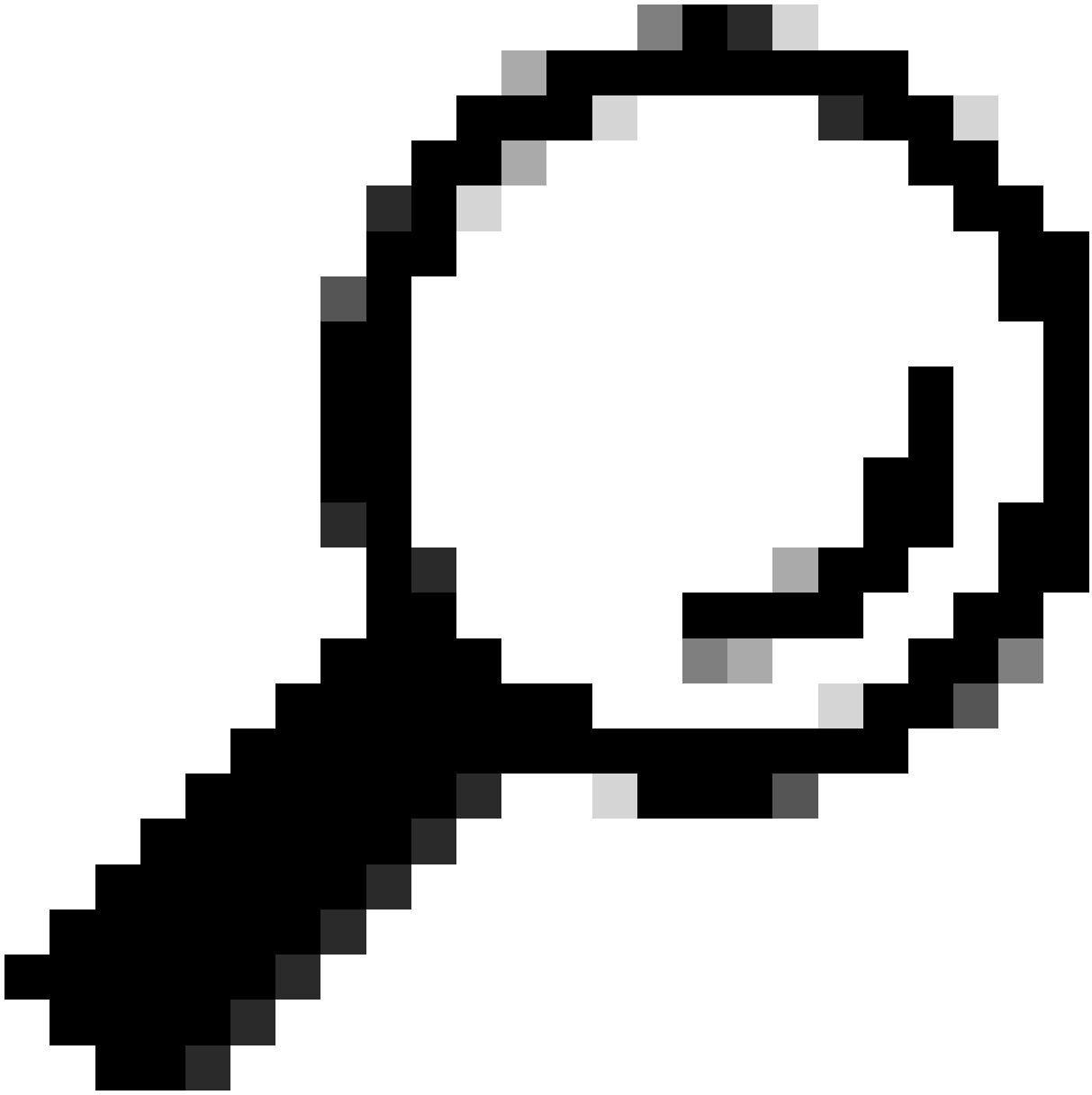
RP/0/RP0/CPU0:BRC-8201-1(config)#

crypto key generate rsa

4096

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint


RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair
```

Etapa 2. Crie um ponto confiável.

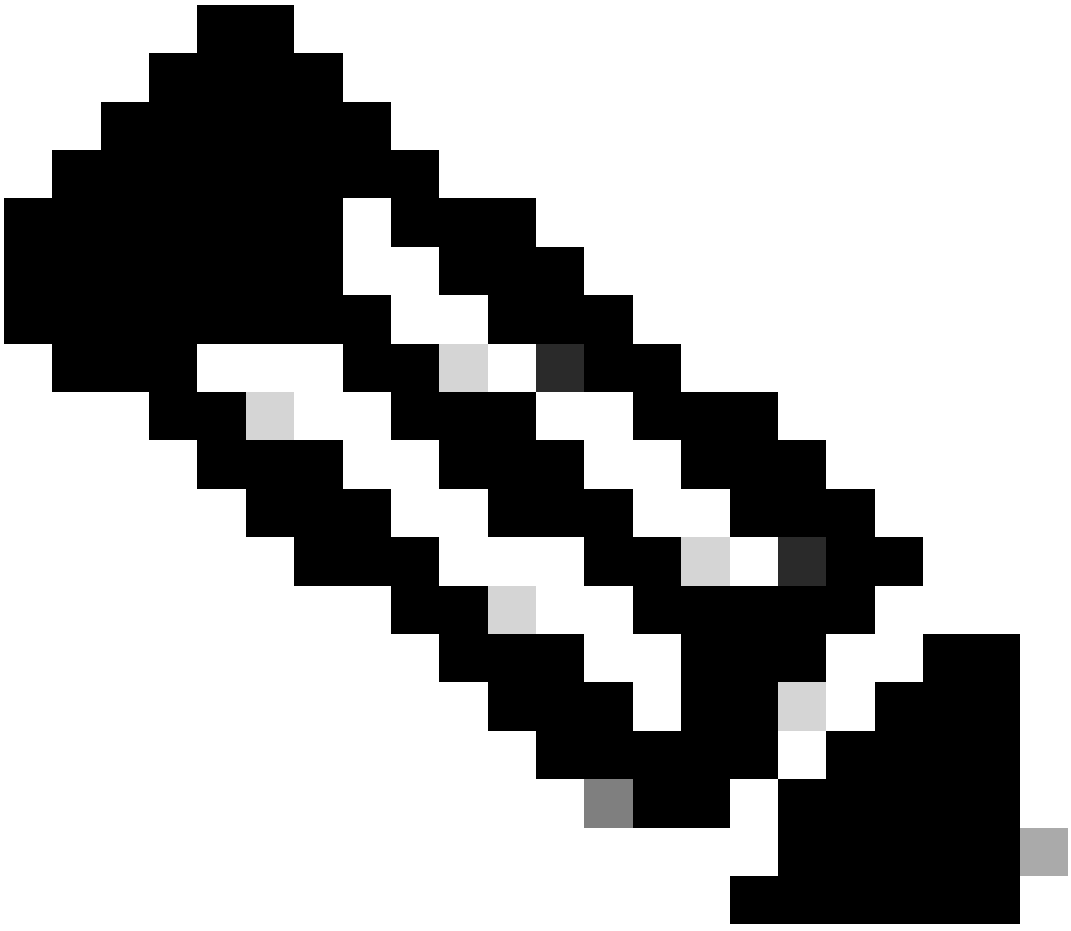


Tip: A configuração DNS para o nome alternativo do requerente é opcional (se estiver sendo habilitada no ISE), mas recomendada.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint svs

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
vrf mgmt

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
crl optional
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
enrollment url terminal
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair svs-4096

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
commit
```



Note: Se você precisar usar vírgula em O ou OU, você pode usar uma barra invertida (\) antes da vírgula. Por exemplo: O=Cisco Systems\, Inc.

Etapa 3. Autentique o ponto de confiança instalando o certificado CA.

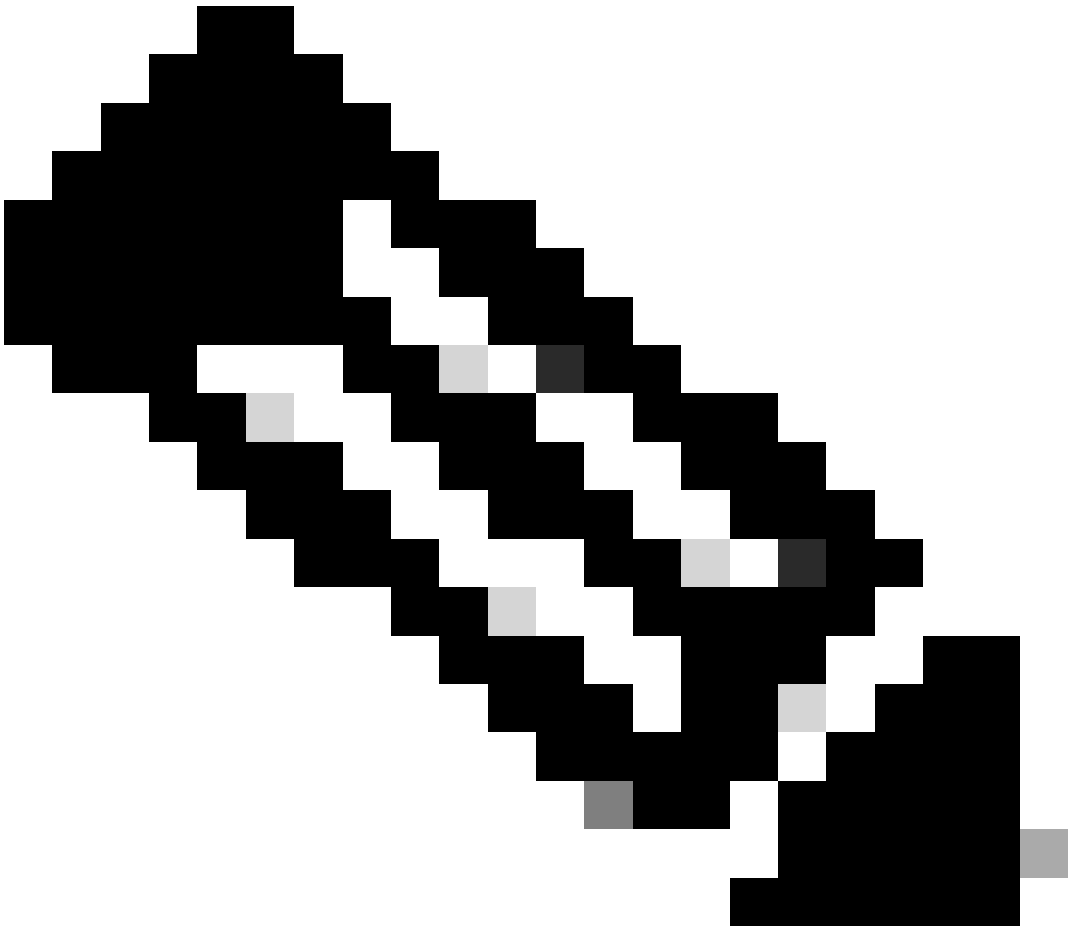
<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#

crypto ca authenticate svs



Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMA0GCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----

quit


   Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5
   Subject:
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
   Issued By :
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
   Validity Start : 17:05:00 UTC Mon Apr 28 2025
   Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
   SHA1 Fingerprint:
      0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
```

yes

```
RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated
```



Note: Se você tiver um sistema de Autoridade de Certificação Subordinada, será necessário importar os certificados de Autoridade de Certificação Raiz e Sub CA. Use o mesmo comando com Sub CA na parte superior e Root CA na parte inferior.

Etapa 4. Gerar CSR (Certificate Signing Request, solicitação de assinatura de certificado).

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca enroll svs

```
Fri May 9 14:52:44.030 UTC
% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
```

Password:

Re-enter Password:

```
% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167
% The subject name in the certificate will include: BRC-8201-1.svs.lab
% Include the router serial number in the subject name? [yes/no]:
```

yes

```
% The serial number in the certificate will be: 4090843b
% Include an IP address in the subject name? [yes/no]:
```

yes

```
Enter IP Address[]
```

10.225.253.167

```
Fingerprint: 36354532 38324335 43434136 42333545
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQH
DANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANTVlMxFzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtrloDH9iOZxPvEDARwN0t4WrPEjaQclZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaiMGqETnO0LKpwmtx10IqXL7UYMHHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRWMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkWkwI0cb1X2HgtbVQdCXTAwJDmr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAaCBiTAYBgkqhkiG
9w0BCQcxCxMJQzFzY28uMTIzMG0GCSqGSIb3DQEJDjFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBBXOeWF5ZUz7O1GFjuQHBBDgYb+3lhFOxbYm9psIWfv1uwjkKoL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswjlYpO+IxkUM971Ejwg2rj+jABDR7I8SU
O6YO6mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTIljdgVxB+XyzOFJMckIO5US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f9OA+fdg2zYtOME
Z6VAw64cY+YF6iLbYv7c4lizO5Zj2NJbUKpeqijkFAkY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZNOO
```

```
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

Etapa 5. Importar certificado assinado pela CA.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca import svs certificate

```
Fri May 9 15:00:35.426 UTC


Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA5MTQ1NzAwWhcNMjYwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDEOMAwGA1UECgwFQ2lzY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOdO2uW
gMf2I5nE+8QMBHA3S3has8SNpByVlQDprHoLGr/QmVCJR/b55C/7ispmoBnXEOGJ
qIwaoROc7QsqnCa3HXQipcvtRgwcfAX29EgjnbOiaRYDxrrdbHrpSQTFpeh5dp/k
eQuioO7rxfzdTss+8x7WwzC+artGbLYMC7fQcH8l9iVAIeZNUXPczl8G3zrHHi3W
fFMVT/iVFYwLvdROvlhOokuMykFPaOOTemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTAjRxvVfYeC1tVBOJdMDAkOavY73N3ZkJrl6dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAYb4QgENBBEWD3hjYSBjZXJOaWZpY2FO
ZTAOBgNVHQ8BAf8EBAMCBaAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUF
BwMCMAkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjI1LjI1My4xNjeHBArh/acw
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+ojO121O6WxedDQ8VduObBtrnOH+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTZrQ93tb9mMTZg7exqN89ZU
VlXoB2UOTri5Kl0/+izEGgyNq42/ytAP8YOO7HR/2jf7gfhoRvwcR5QNOEHv4o6l
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV8lRGXxxgyt1mwNmb7EiAc8lodRcgyp7FNh3
F/k9cMMMr5lM4Ysvoltx1k9AeLjzb2syv5/fG6QuOZdWwTaaQhOY2h/cVDiV97wg
ODlmEfdSv6QrxQSujZr22RzVyKKHltuiV2B74pthUuGRBtfHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDplrf1ZIrPmv3ZPP7woTB22yWzydOuse+5IalbOw7OtwN4t/IIw
8CJu6HfnDXLDPZOjsC8steffrSlopwGccp3j6aZKPFz+I/Purb44a9WxEWa2TA7H
+rloynBcGMetOHxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF537Ow+uNHoK8Bdt8mqadUT4OoUSqY8ArVOBomO5tzbemreVPmQAZ/IahZ7TqKo
3dGNonTAfFTESM1iujQ81iRKsikDHySnwcCM2nilCKZrhVq5IB8NK6jKRJZOeQAX
vMt1
-----END CERTIFICATE-----
```

quit

```
Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792
```

Verifique se o certificado de identidade do roteador está registrado.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

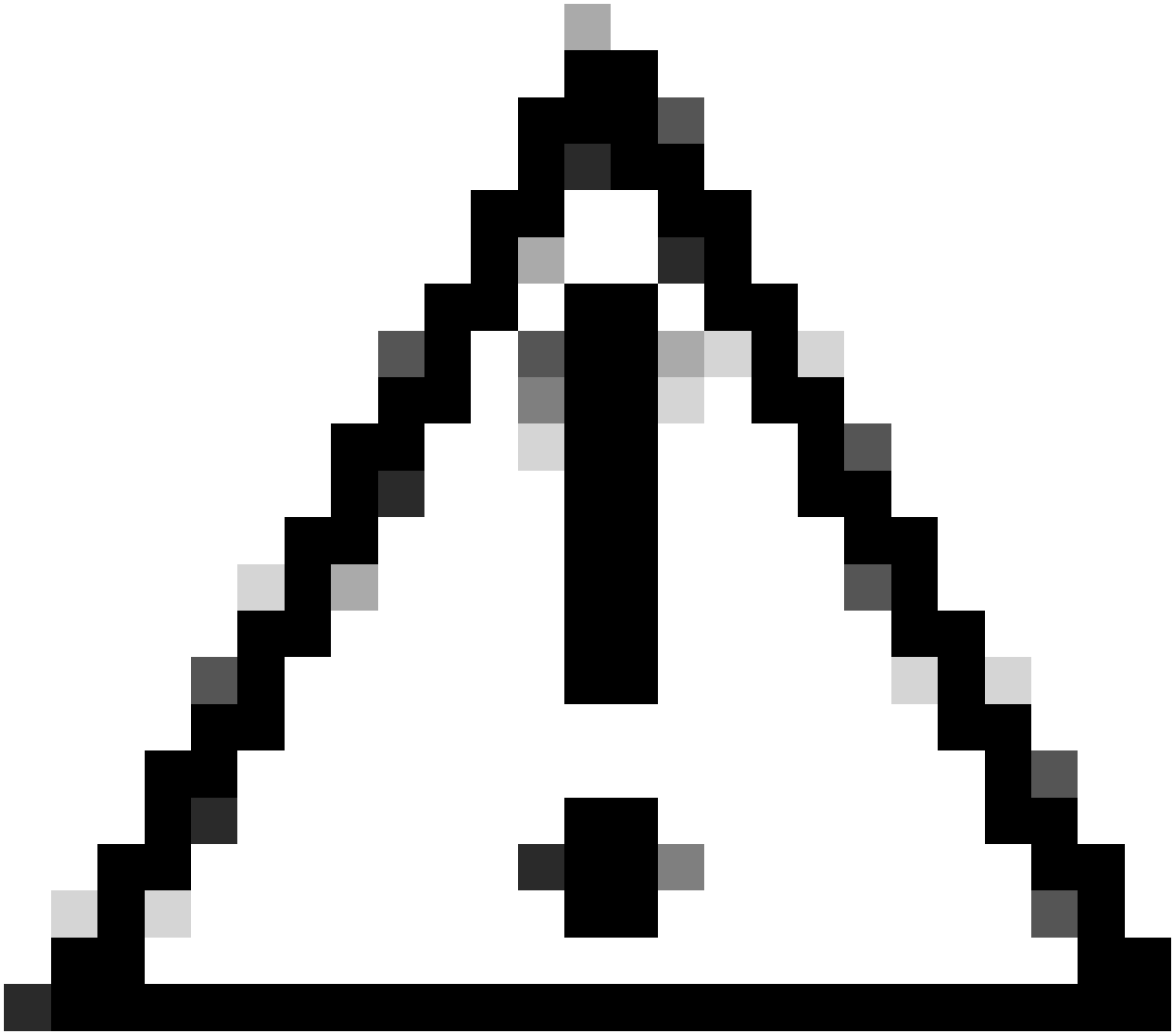
show crypto ca trustpoint svs detail

```
Trustpoint        :svs-new
================================================================
KeyPair Label: the_default
CRL:optional
enrollment: terminal
subject name: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1#
```

show crypto ca certificates svs

```
Wed May 14 14:55:58.173 UTC

Trustpoint       : svs-new
================================================
CA certificate
  Serial Number  : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
  Subject:
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
         0EB181E95A3ED7803BC5A8059A854A95C83AC737
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
  Subject:
        serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
         AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svs
```

Configurar TACACS e AAA com TLS



Caution: Execute as alterações de configuração através do console com credenciais locais.

Etapa 1. Configurar o servidor TACACS+.

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
  key 7 072C705F4D0648574453

aaa group server tacacs+ tacacs2
 server 10.225.253.209
 vrf mgmt
```

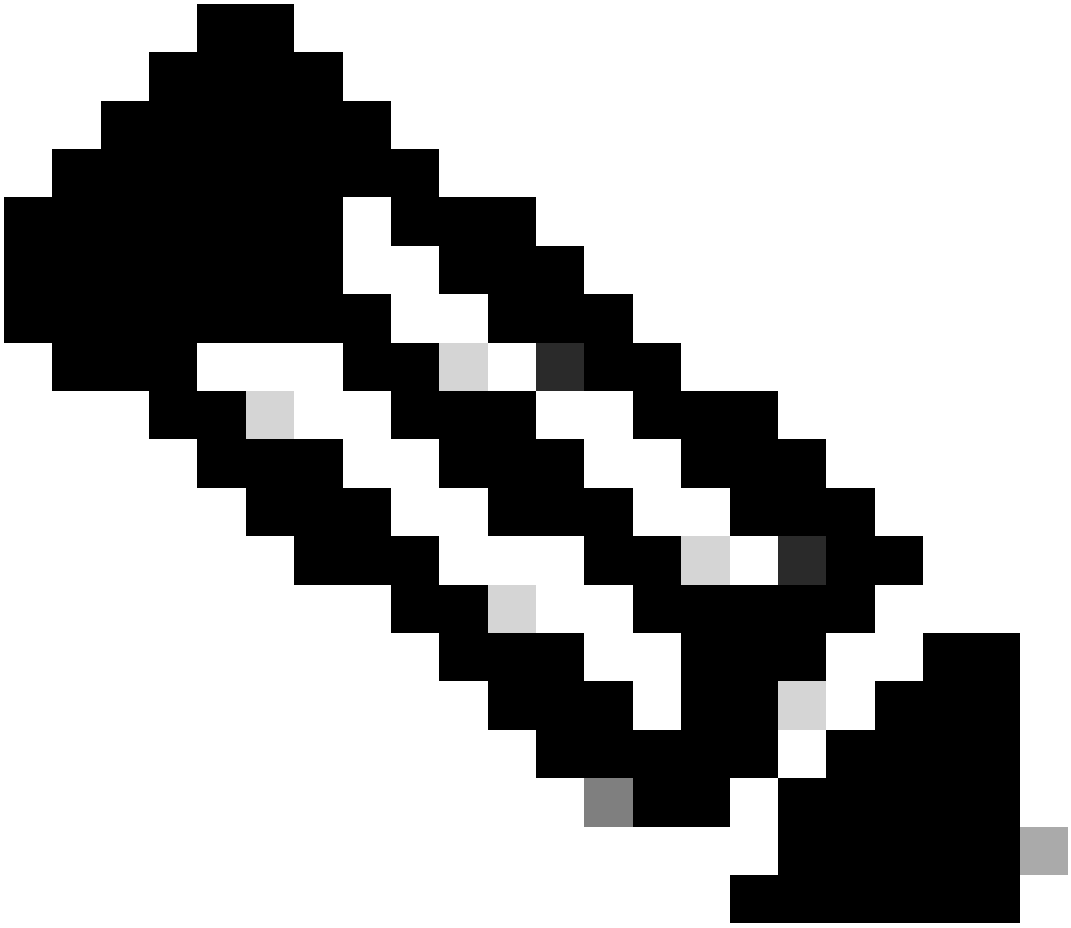
Etapa 2. Configure o grupo AAA.

```
aaa group server tacacs+ tac_tls_sc
 vrf mgmt
 server-private 10.225.253.209 port 6049
  timeout 10
  tls
   trustpoint svs
  !
  single-connection
```

Etapa 2. Configure o AAA.

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

Renovação de certificado



Note: O ponto de confiança não precisa ser removido da configuração TACACS+ durante a renovação.

Etapa 1. Verificar as datas atuais de validade do certificado.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svs-new
Thu Aug 14 15:13:37.465 UTC

Trustpoint : svs-new
==================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030
```

```
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5GvOAZM

  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 16:38:36 UTC Wed Jul 30 2025
  Validity End : 16:38:35 UTC Thu Jul 30 2026
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        B562F3CF507CE7F97893F28BC896794CFF6995C1
Associated Trustpoint: svs-new
```

Etapa 2. Excluir o certificado de ponto confiável existente.

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
Thu Aug 14 15:25:26.286 UTC
certificates cleared for trustpoint KF_TP
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database update
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:25:37.270 UTC
RP/0/RP0/CPU0:BRC-8201-1#
```

Etapa 3. Autentique novamente e registre o ponto de confiança conforme descrito nas etapas em Configuração do ponto de confiança.

Etapa 4. Verificar se as datas de validade do certificado estão atualizadas.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:31:28.309 UTC
```

```
Trustpoint : KF_TP
================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5GvOAZM
  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 15:17:29 UTC Thu Aug 14 2025
  Validity End : 15:17:28 UTC Fri Aug 14 2026

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE
Associated Trustpoint: KF_TP
```

Verificação

Verificar a configuração.

```
show crypto ca certificates [detail]
show crypto ca trustpoint detail
show tacacs details
```

Depuração para TACACS+

```
debug tacacs tls
```

Depurar TLS

```
debug ssl error
debug ssl events
```

Teste o usuário remoto antes de configurar a autenticação AAA.

<#root>

test aaa group tacacs2

```
user has been authenticated
```

Troubleshooting

Limpando os certificados (isso exclui todos os certificados associados a um ponto de confiança).

```
clear crypto ca certificate <trustpoint name>
```

Reinicialização do processo TACACS (se necessário)

```
process restart tacacsd
```

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.