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

Contents

- Introdução
- Overview
  - Usando este Guia
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
  - Licenciamento
- Parte 1 - Configurar o ISE para a 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 XE_RW - Perfil do administrador
    - IOS XE_RO - Perfil do operador
  - Configurar conjuntos de comandos TACACS+
    - CISCO_IOS XE_RW - Conjunto de comandos do administrador
    - CISCO_IOS XE_RO - Conjunto de comandos do operador
  - ConfigurarConjuntos de Políticas de Administração do Dispositivo
- Parte 2 - Configurar o Cisco IOS XE para TACACS+ sobre TLS 1.3
- Método de configuração 1 - Par de chaves gerado pelo dispositivo
  - Configuração do servidor TACACS+
  - Configuração do Trustpoint
  - TACACS e AAA com configuração TLS
- Método de configuração 2 - Par de chaves gerado pela CA
  - TACACS e AAA com configuração TLS
- Verificação

Introdução

Este documento descreve um exemplo para TACACS+ sobre TLS com Cisco Identity Services Engine (ISE) como servidor e um dispositivo Cisco IOS® XE 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 XE.
· Parte 1 - Configurar o ISE para o administrador de dispositivos
· Parte 2 - Configurar o Cisco IOS XE 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
- Software Cisco IOS XE, versão 17.15+

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.

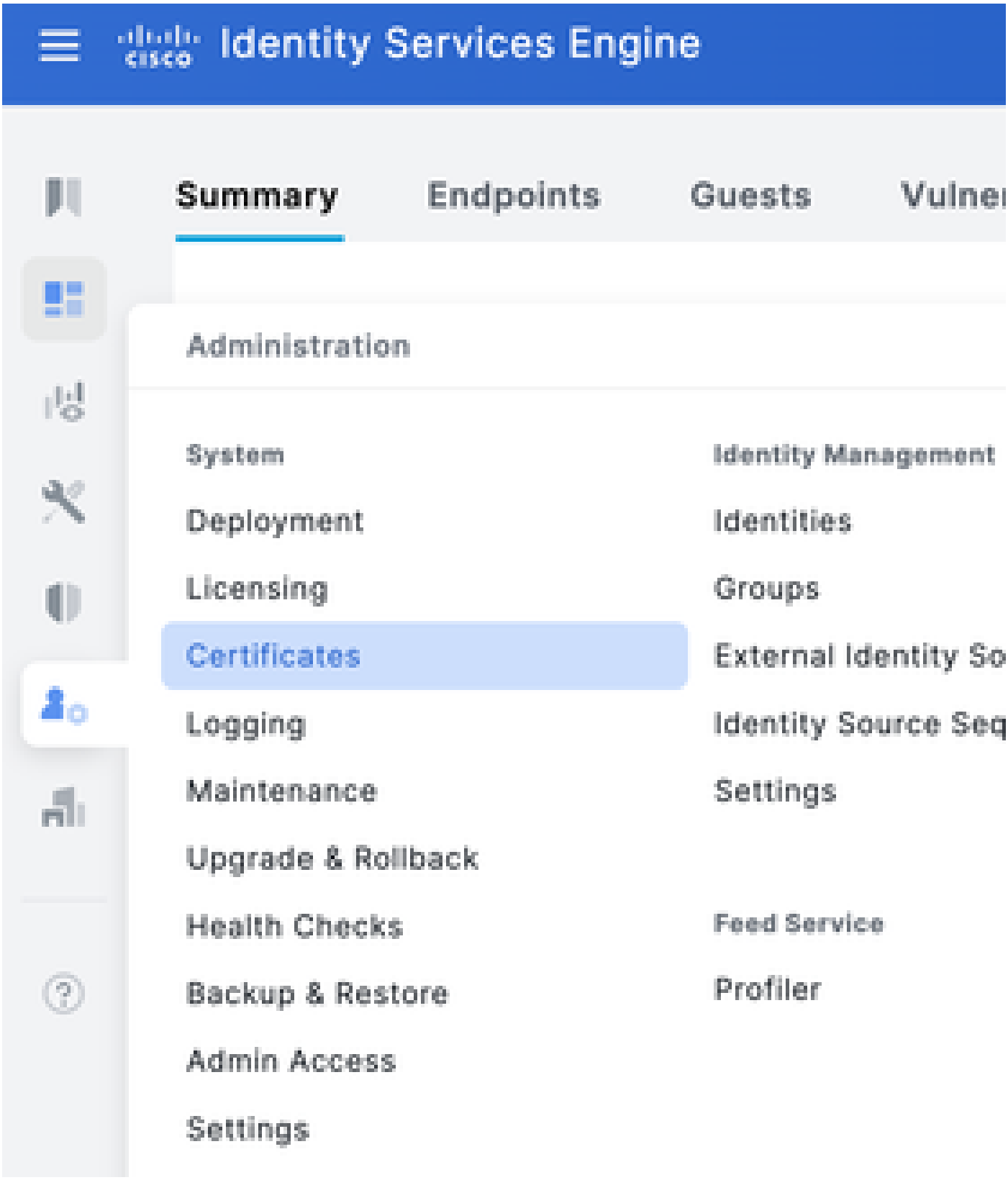
Parte 1 - Configurar o ISE para a administração de dispositivos

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).

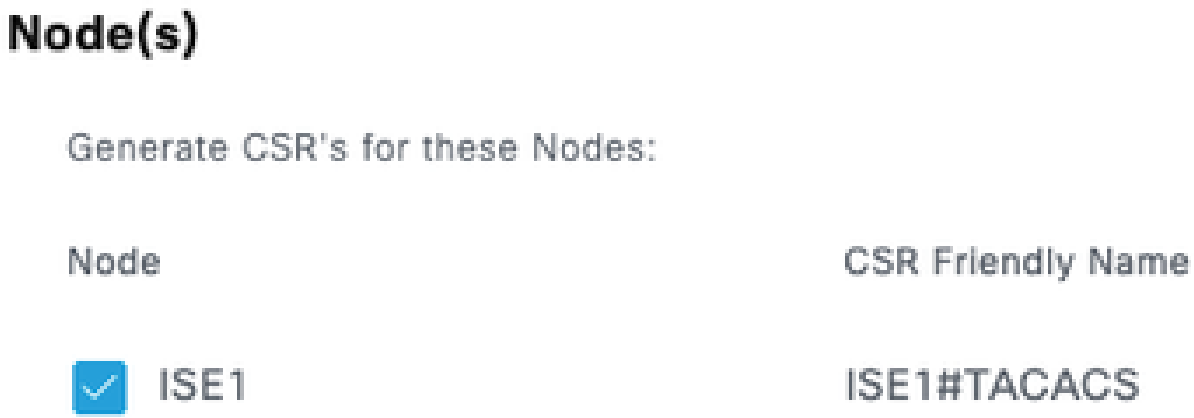
Etapa 2.Navegue até Administração > Sistema > Certificados.



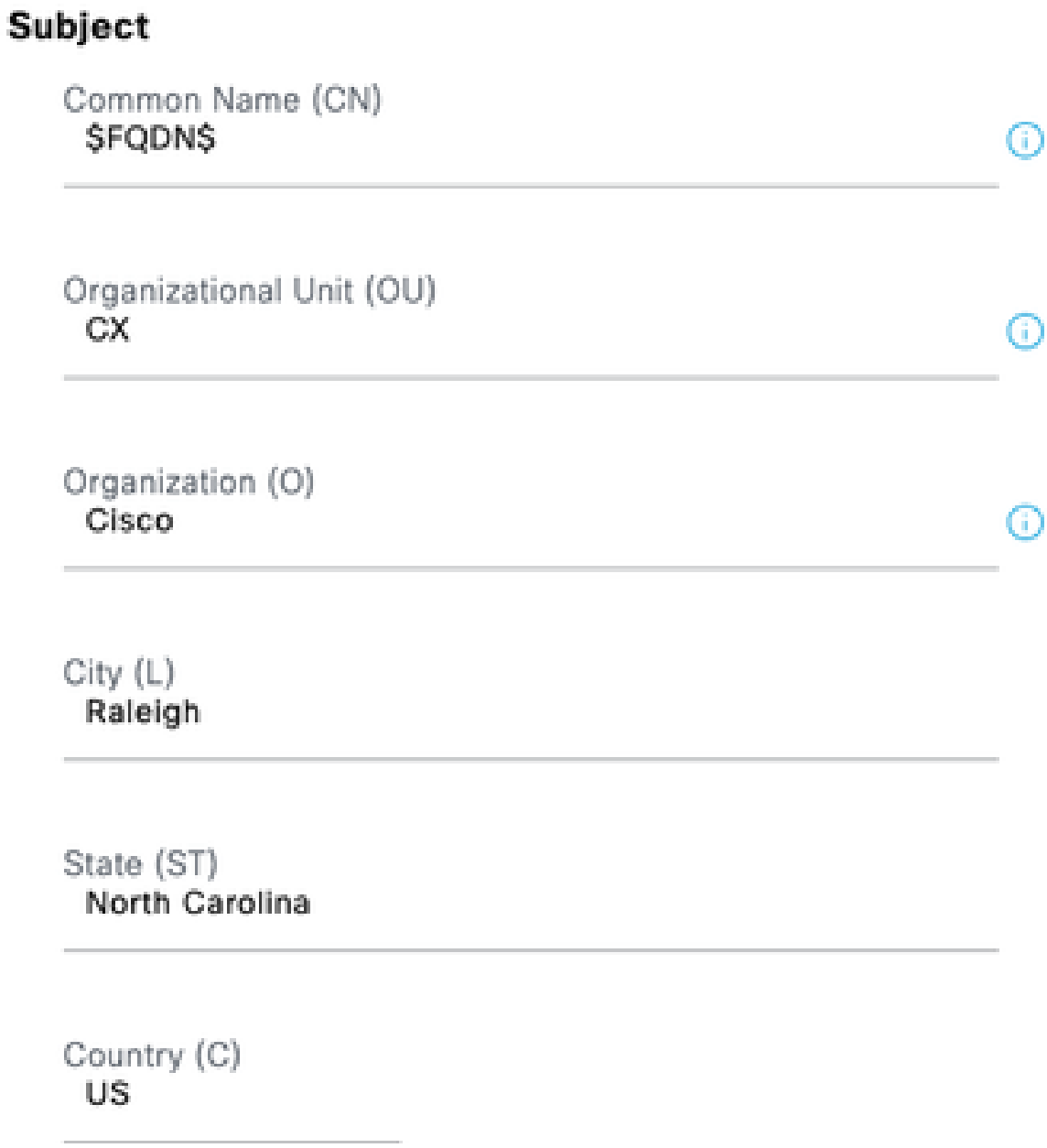
Etapa 3. Em Certificate Signing Requests, clique em Generate Certificate Signing Request.

Etapa 4.Selecione TACACS em Uso.

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

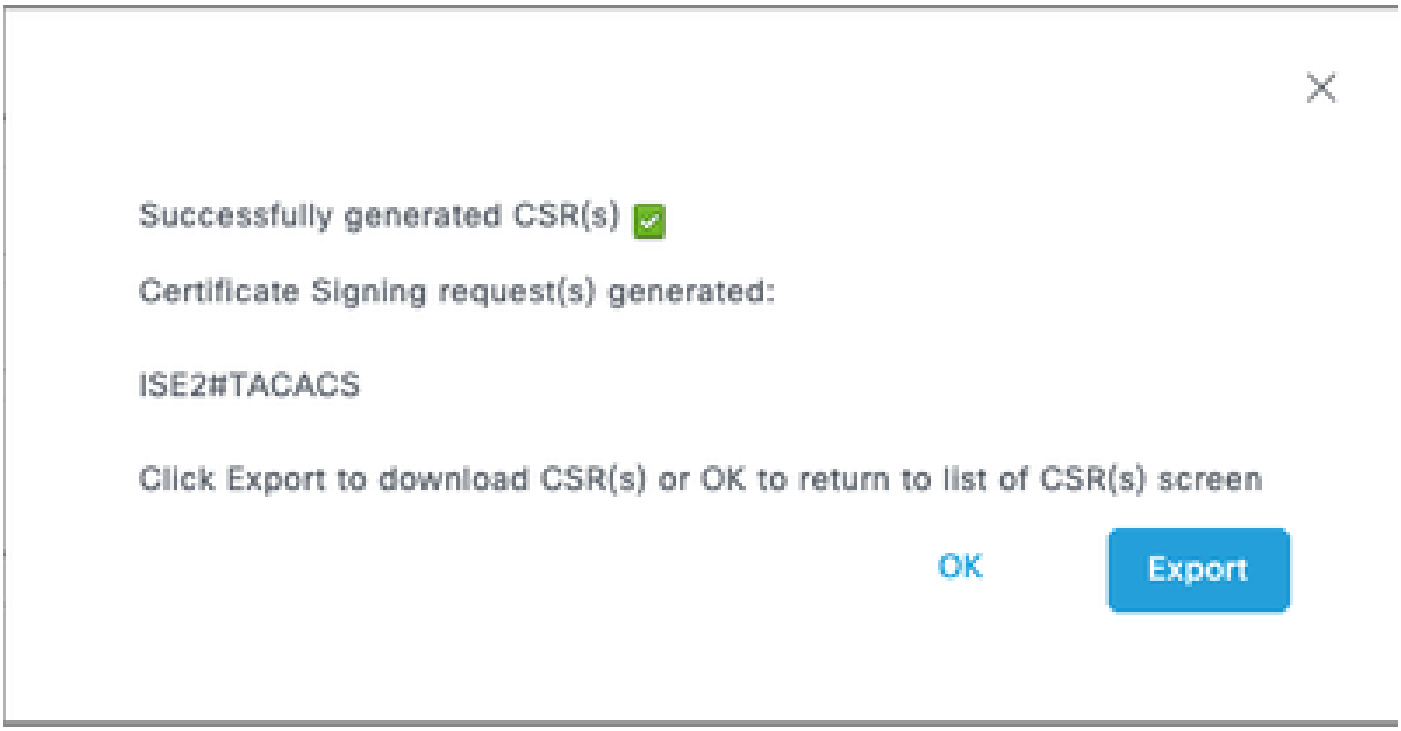


Etapa 6. Preencha os campos Assunto com as informações apropriadas.



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

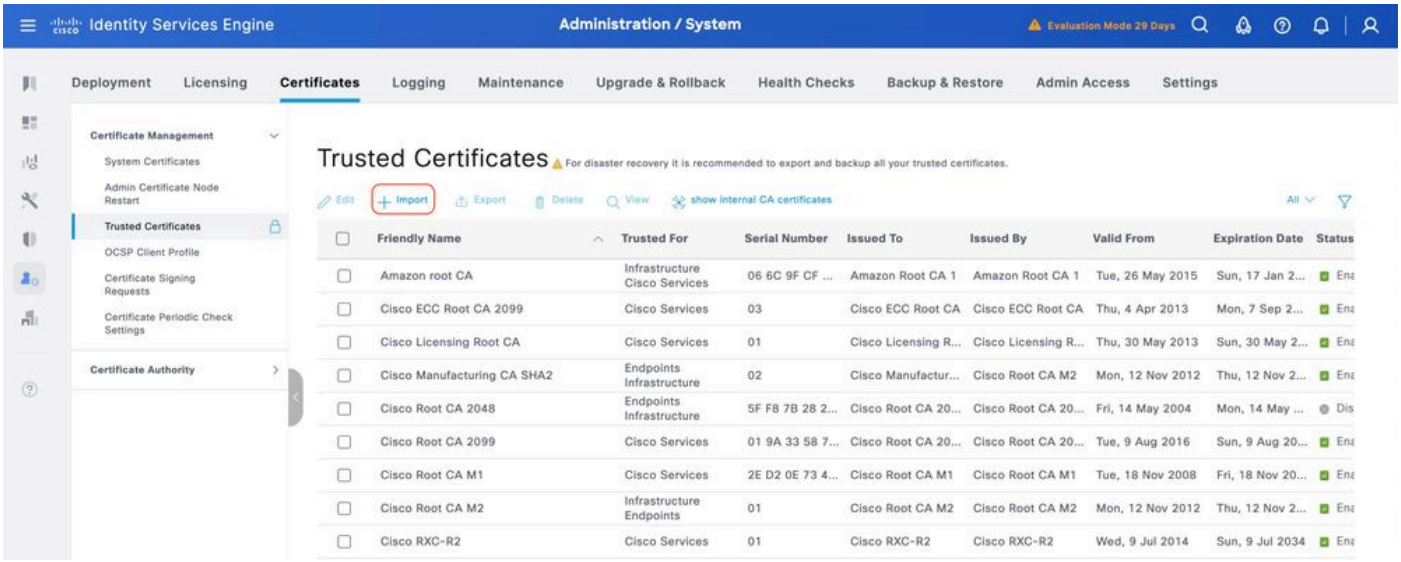
Etapa 8.Clique em Gerar e em Exportar.



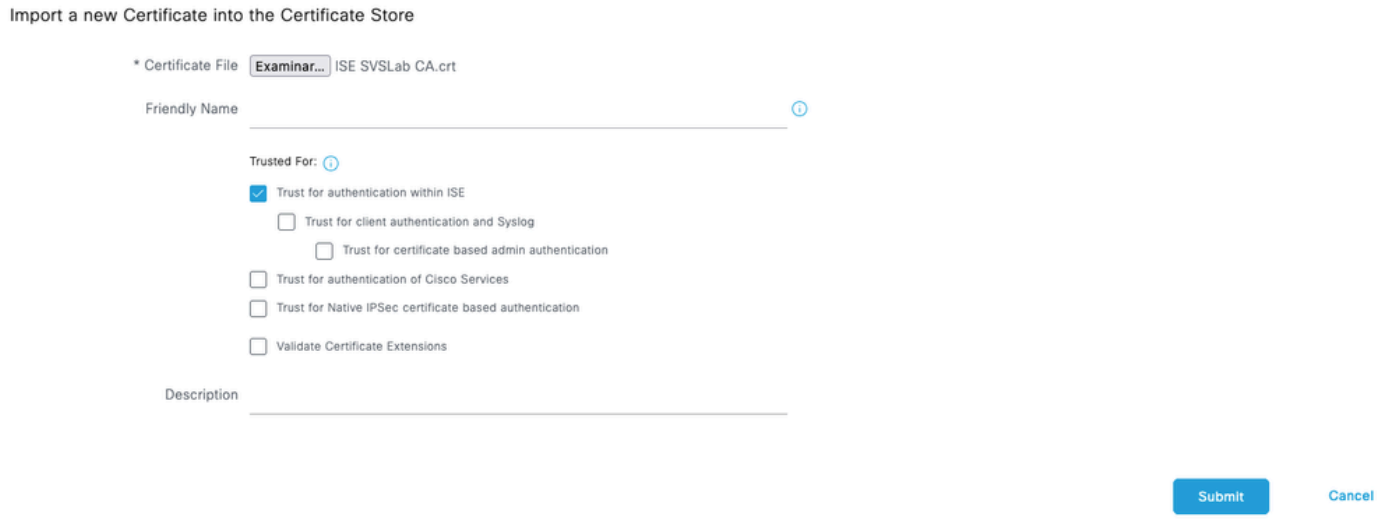
Agora, você pode ter o certificado (CRT) assinado pela suaAutoridade de Certificação (CA).

Carregar certificado CA raiz para autenticação de servidor TACACS+

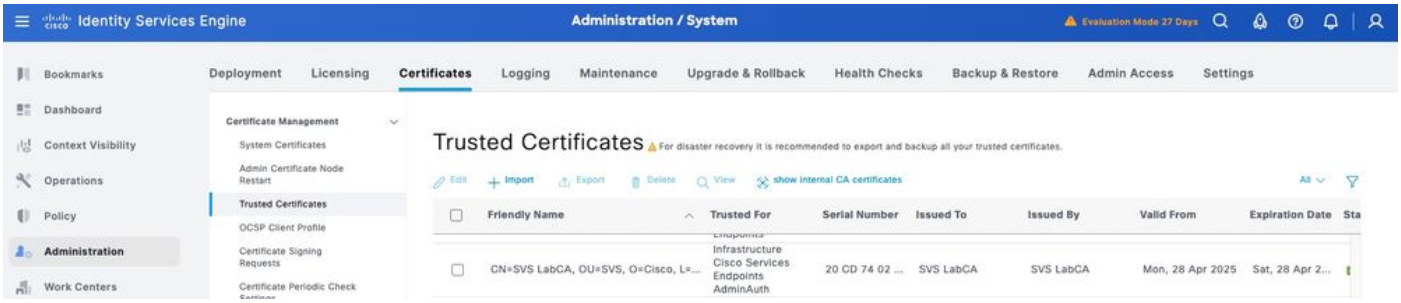
Etapa 1. Navegue até Administração > Sistema > Certificados. Em Certificados de Confiabilidade, clique em Importar.



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 comandoConfiança para autenticação no ISE está ativada.



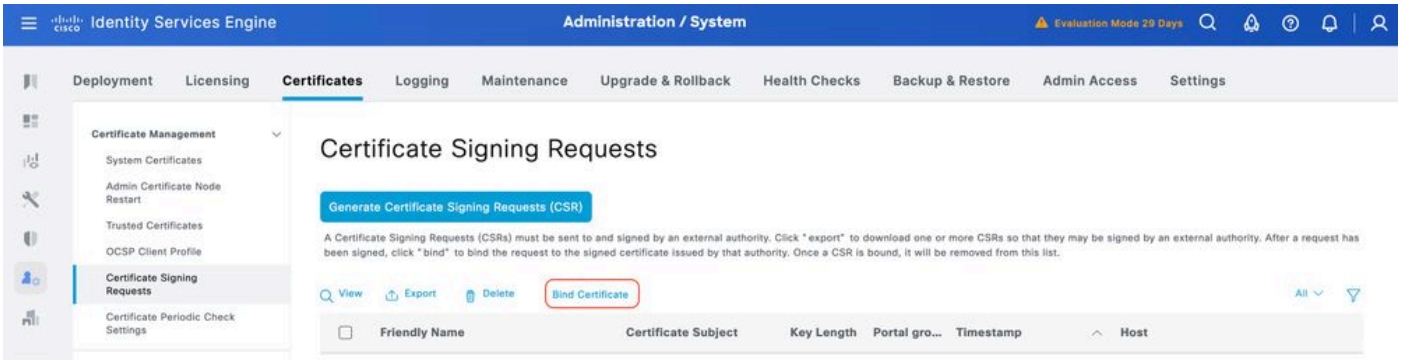
Etapa 3. Clique em Enviar. O certificado deverá aparecer agora em Certificados de Confiabilidade.



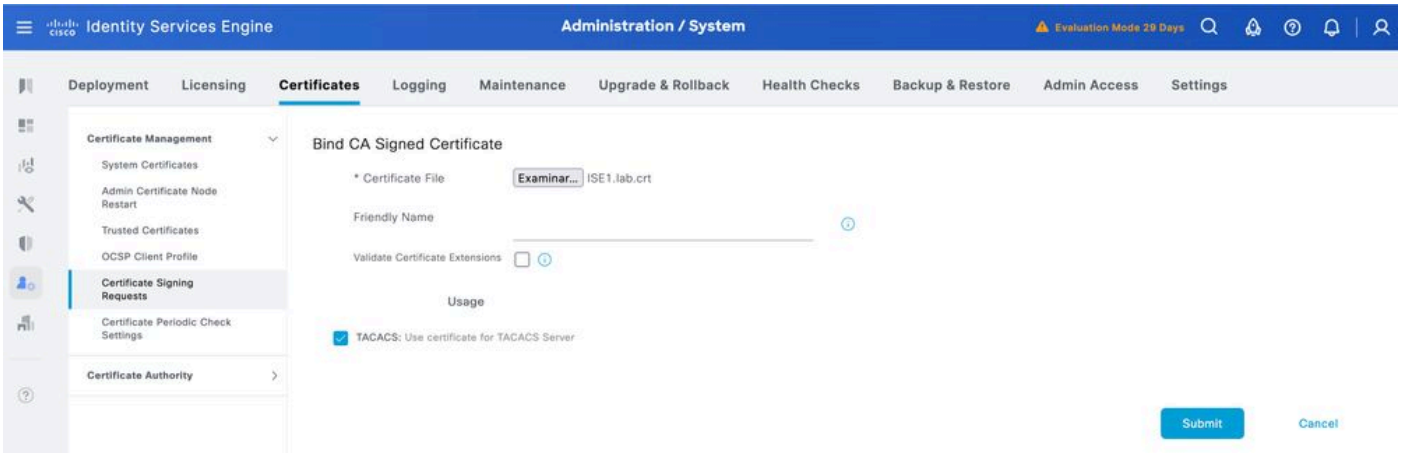
Vincule a solicitação de assinatura de certificado (CSR) assinada ao ISE

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 TACACS CSR gerado na etapa anterior e clique em Bind Certificate.

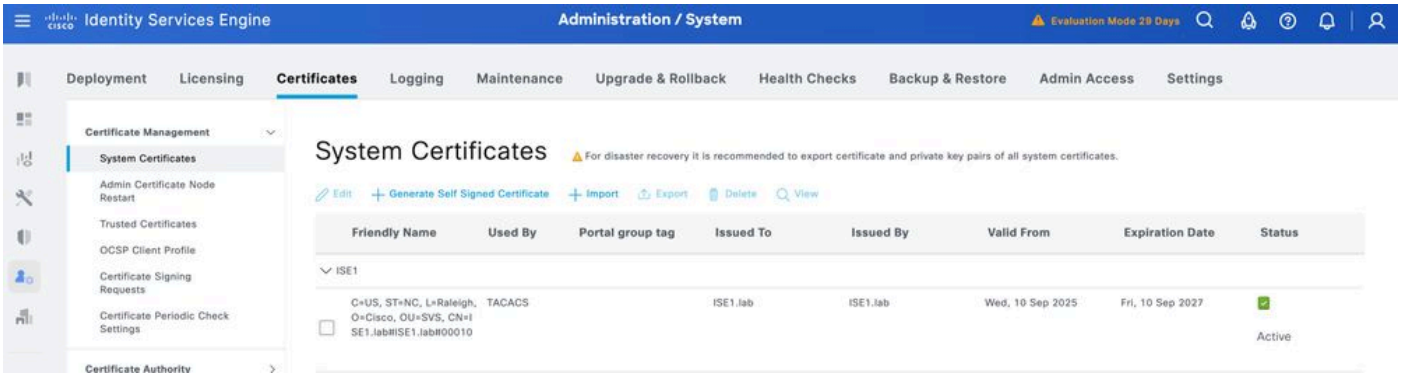


Etapa 2.Selecione o certificado assinado e certifique-se de que a caixa de seleção TACACS em Usage permaneça selecionada.



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

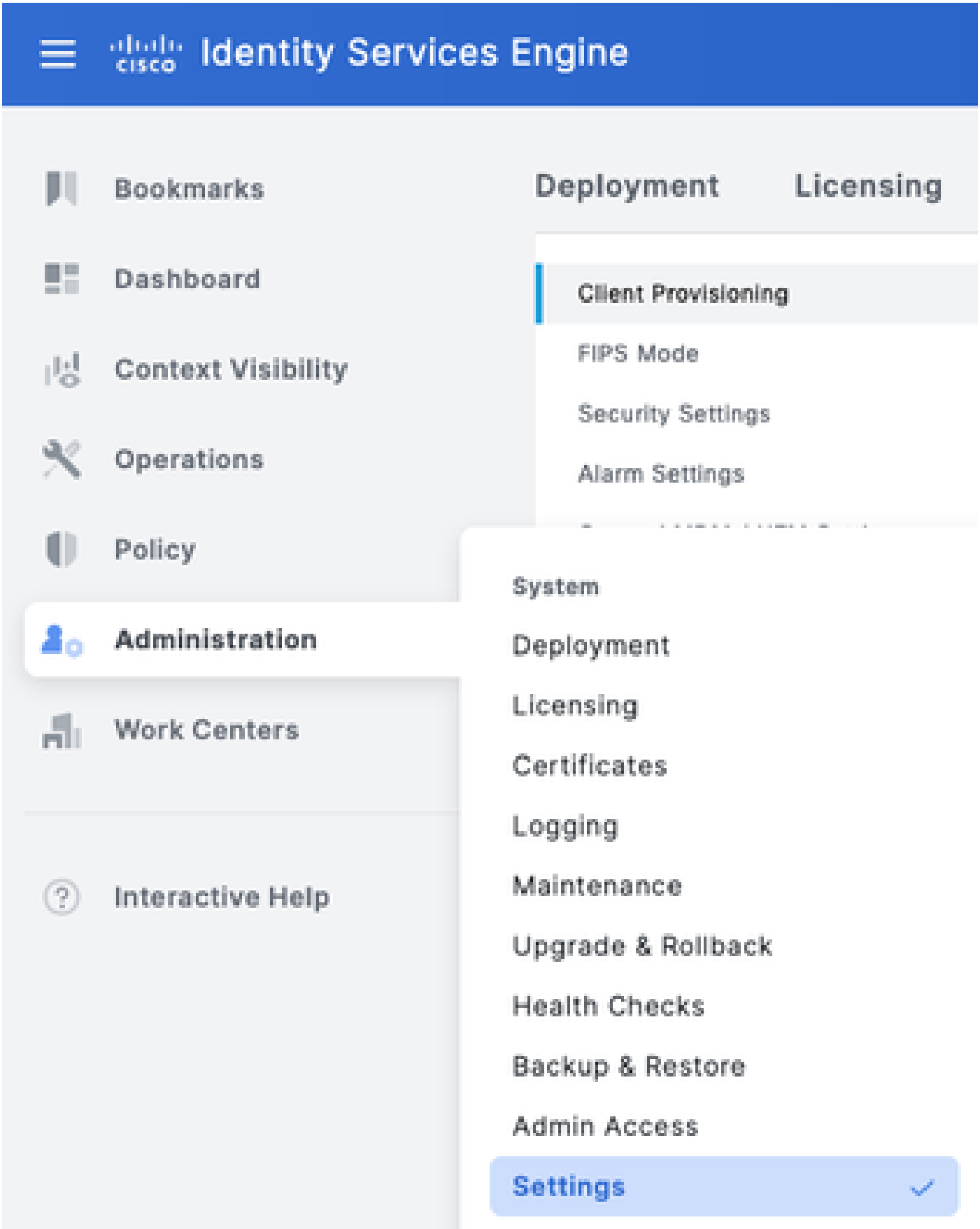
O certificado deve agora estar instalado corretamente. Você pode verificar isso em Certificados do sistema.



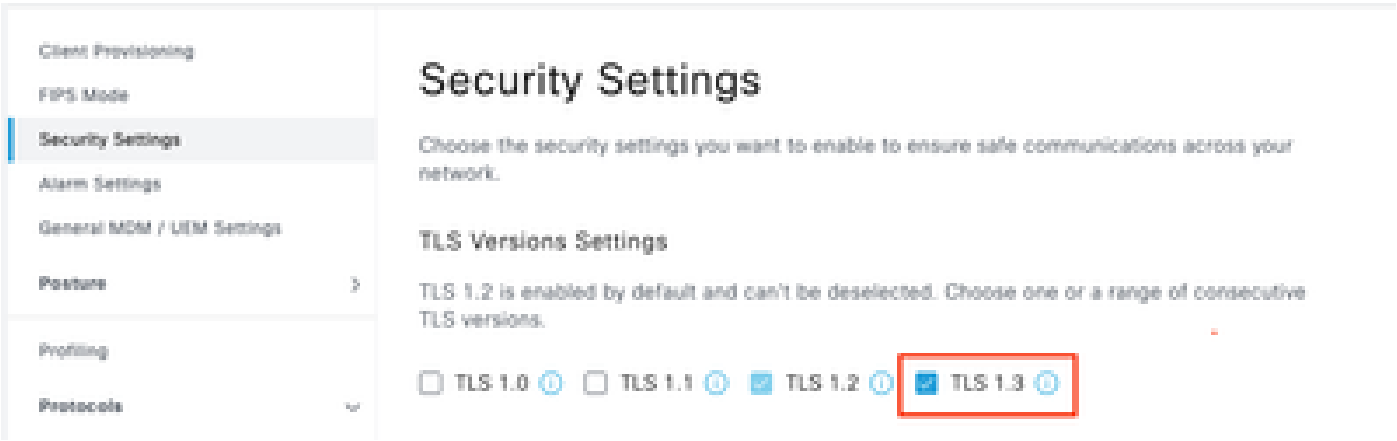
Ativar TLS 1.3

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

Etapa 1.Navegue até Administração > Sistema > Configurações.



Etapa 2.Clique em Configurações de segurança, marque a caixa de seleção ao lado de TLS1.3 em Configurações de versão de TLS e clique em Salvar.

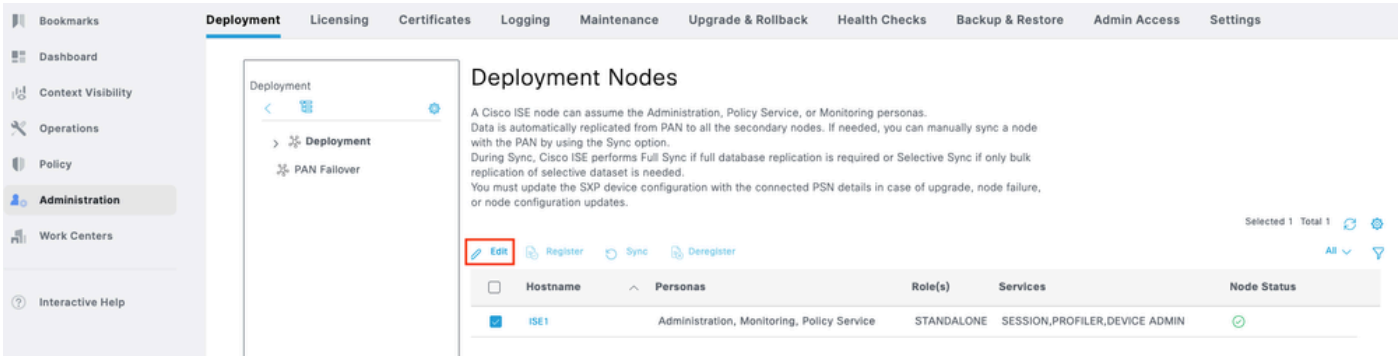


aviso: Quando você altera a versão do TLS, o servidor de aplicativos do Cisco ISE é reiniciado em todas as máquinas de implantação do Cisco ISE.

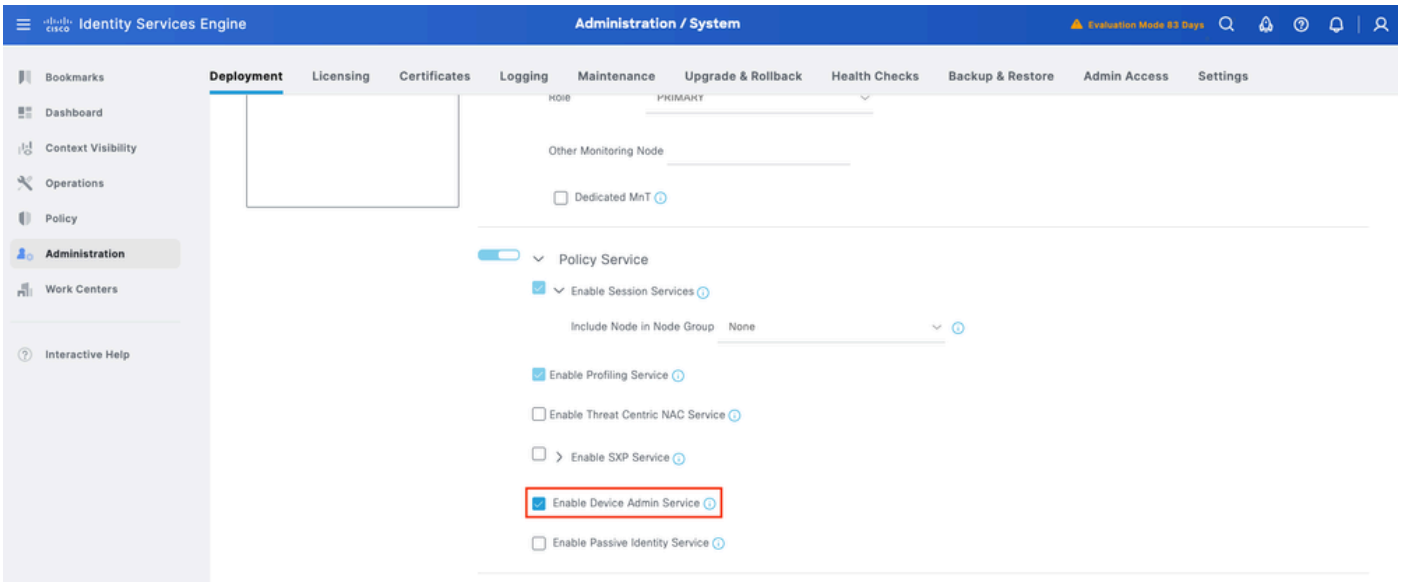
Ativar a administração de dispositivos no ISE

O serviço de Administração de dispositivo (TACACS+) não é habilitado por padrão em um nó ISE. Ative 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.



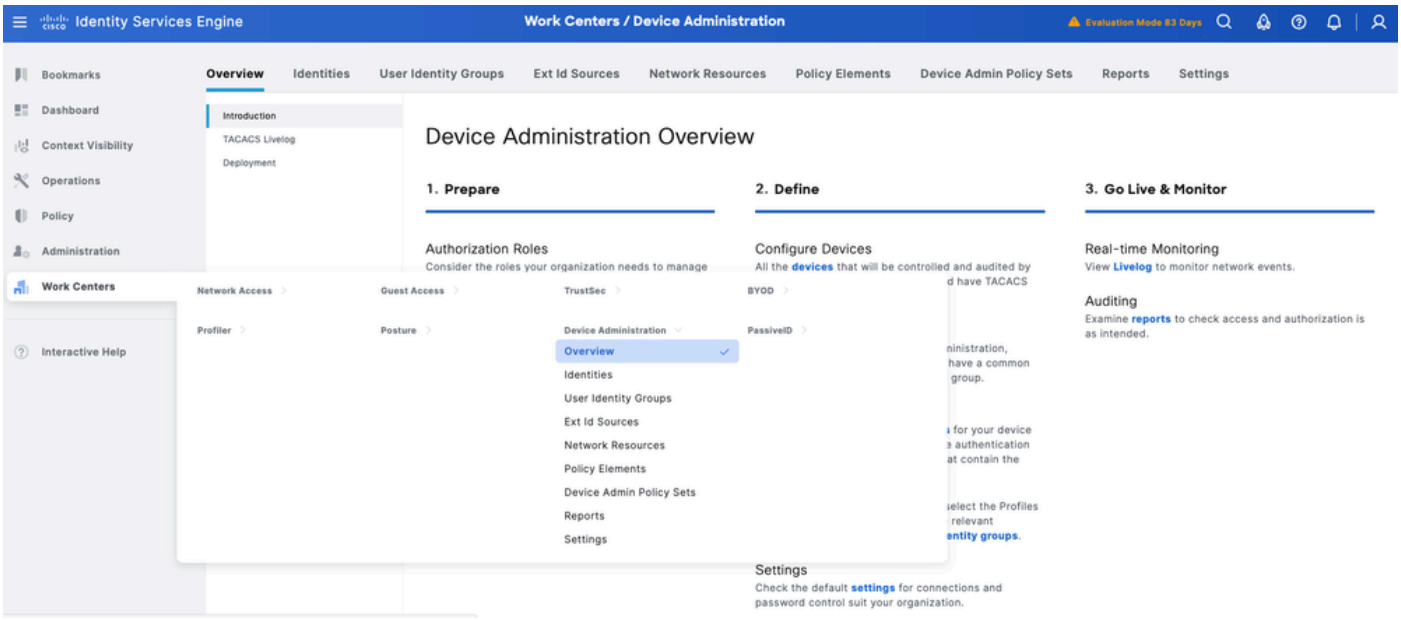
Etapa 2.Em GeneralSettings, role para baixo e selecione a caixa de seleção ao lado de Enable Device Admin Service.



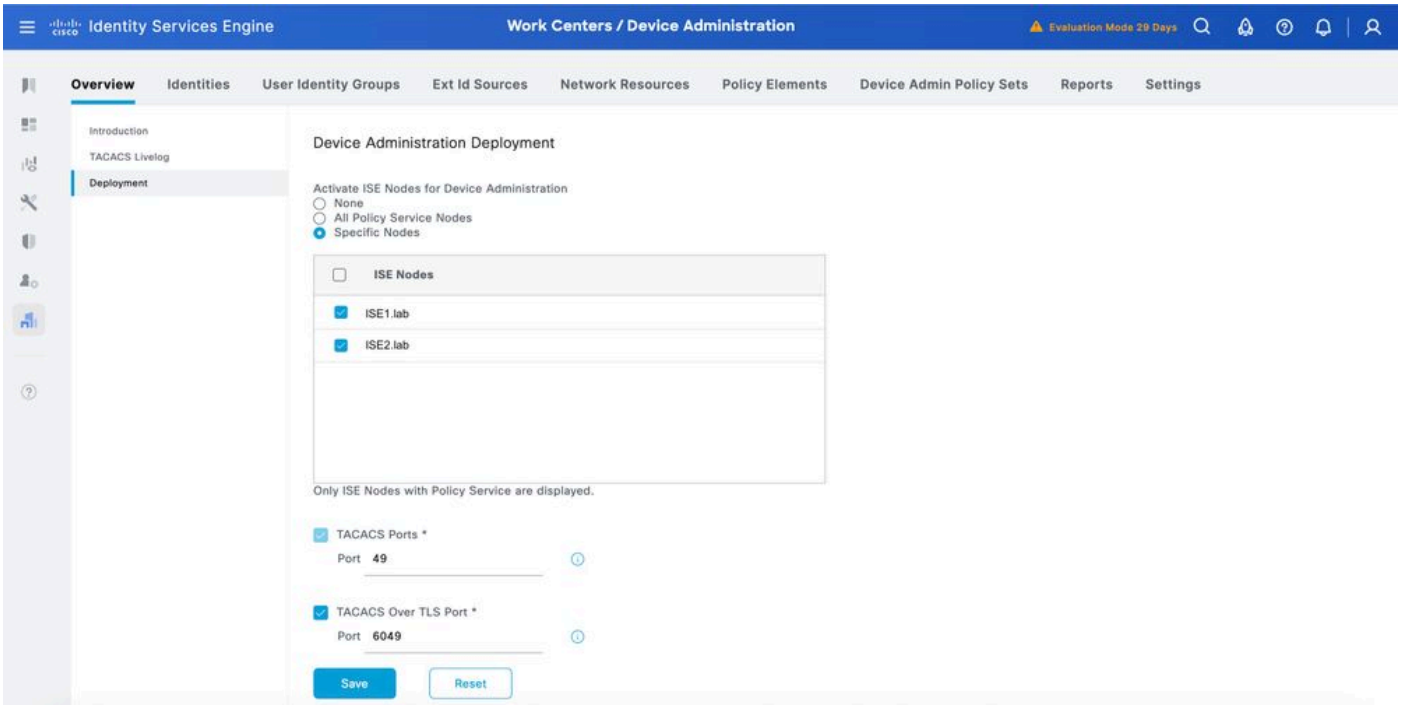
Etapa 3. Salvar a configuração. O Device Admin Service agora está habilitado no ISE.

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.

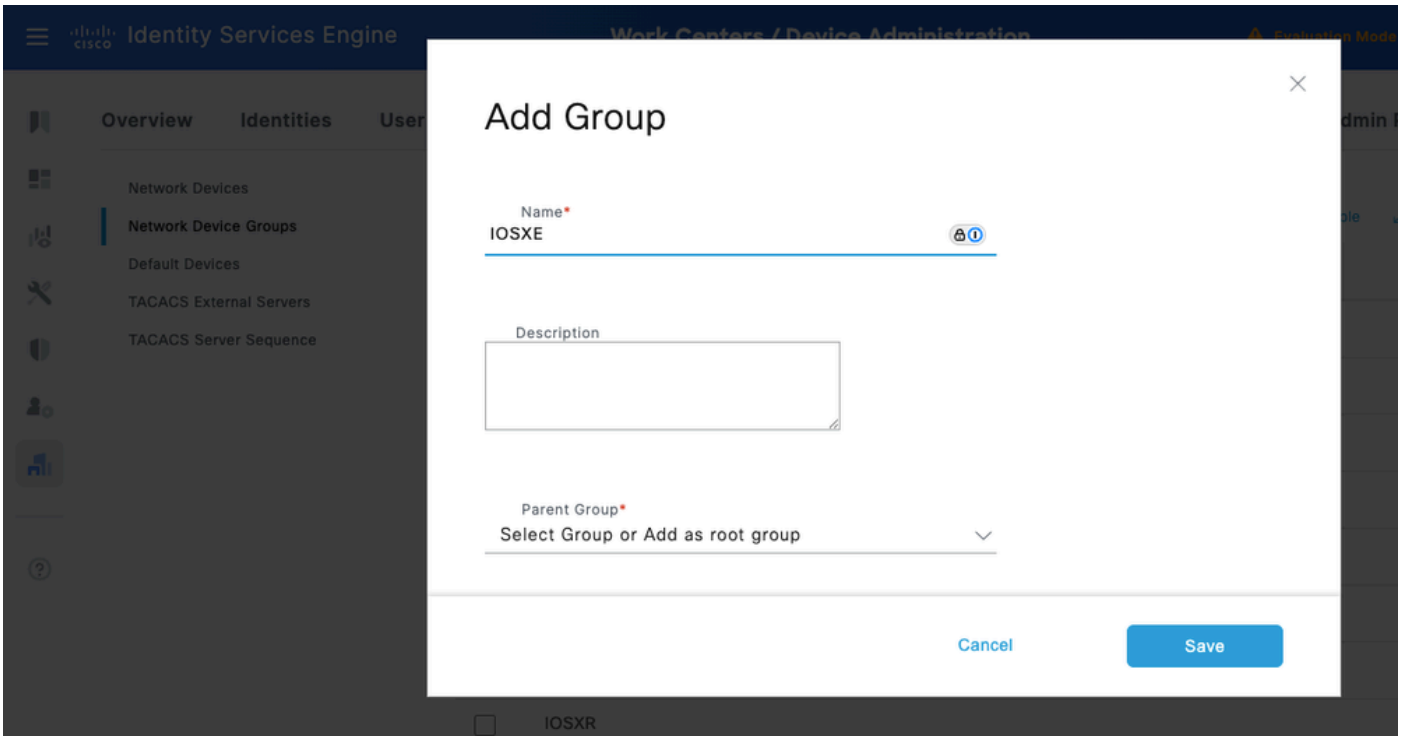


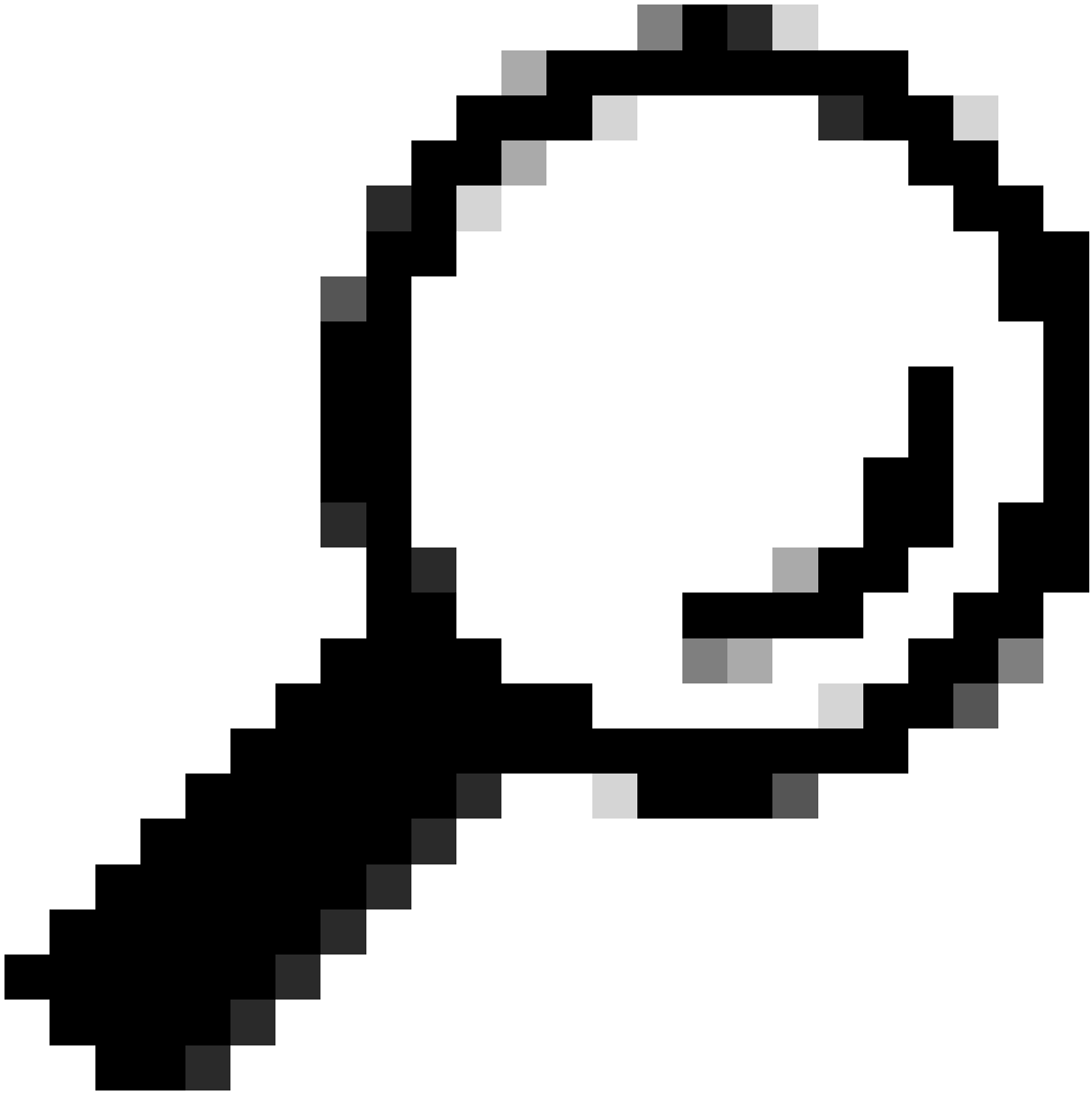
Etapa 3.Mantenha a porta padrão 6049 ou especifique uma porta TCP diferente para TACACS sobre TLS e clique em Save.

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 XE.

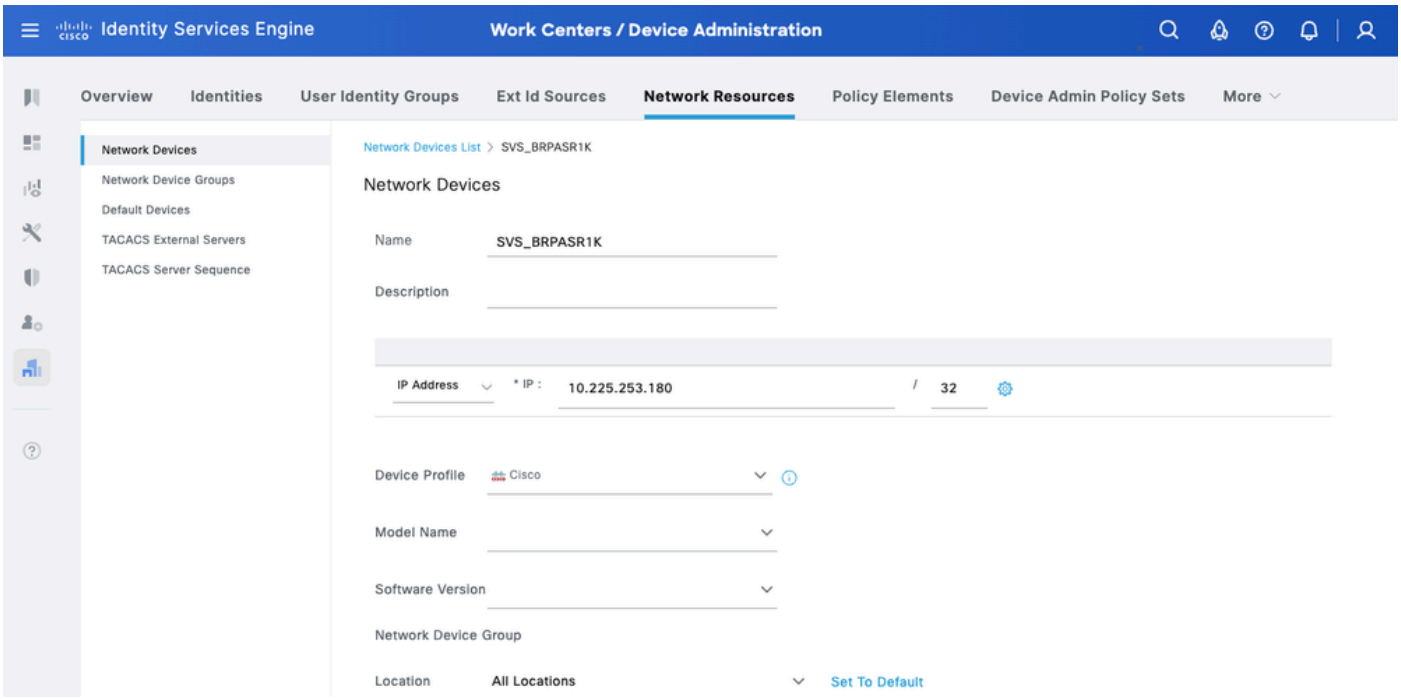

Identity Services Engine
Work Centers / Device Administration
Overview
Identities
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Add Group
Name*
IOSXE
Description
Parent Group*
Select Group or Add as root group
Cancel
Save
IOSXR



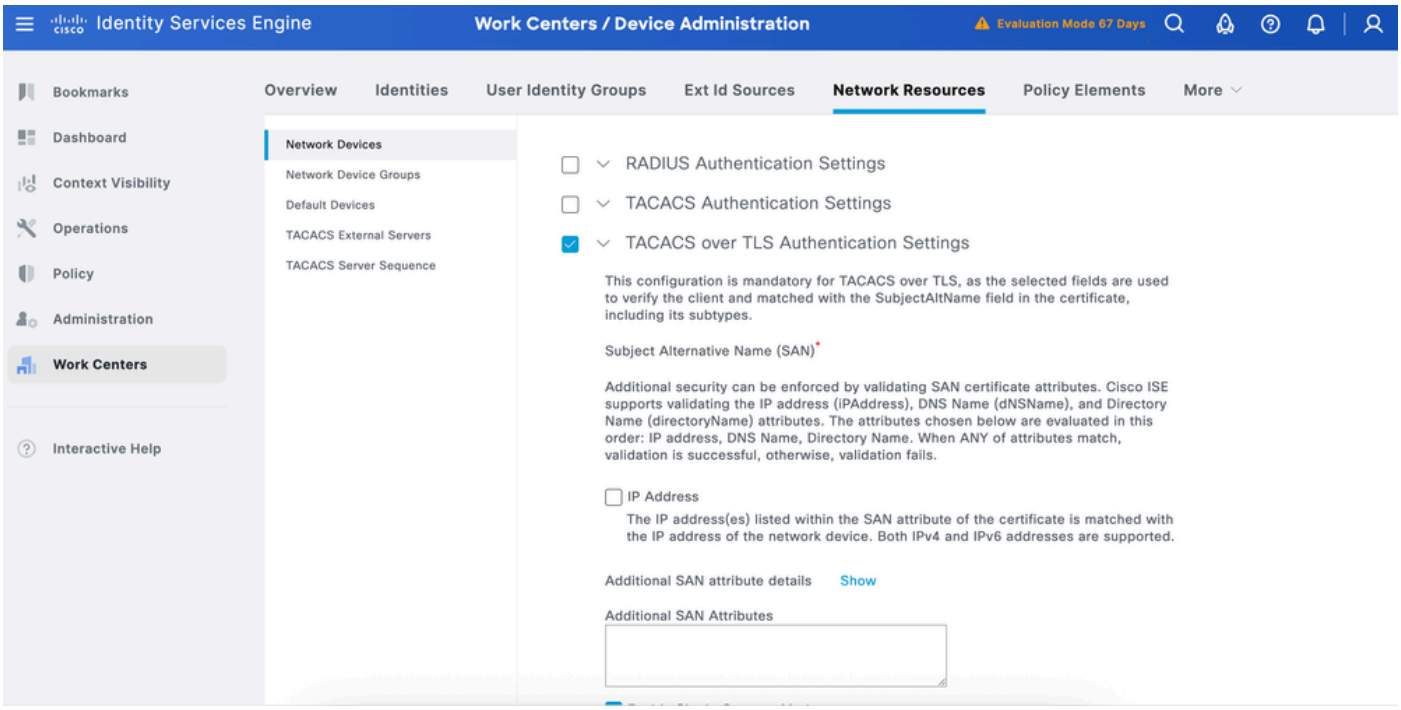
Tip: Todos os tipos de dispositivos e todos os locais são hierarquias padrão fornecidas pelo ISE. Você pode adicionar suas próprias hierarquias e definir os vários componentes na identificação de um dispositivo de rede que pode ser usado posteriormente na condição de política

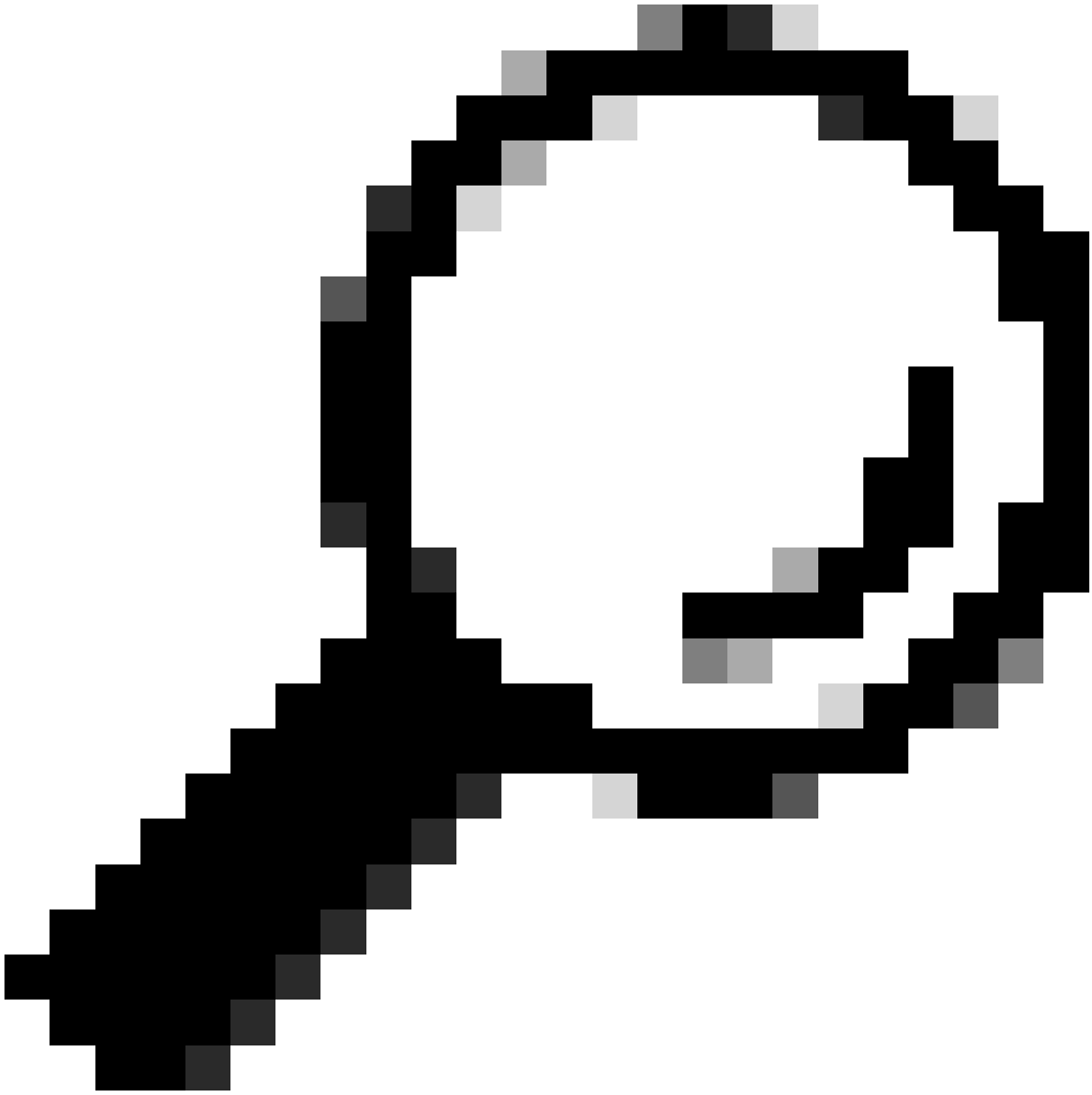
---

Etapa 2.Agora, adicione um dispositivo Cisco IOS XE 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. Para este teste, seria SVS_BRPASR1K.



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



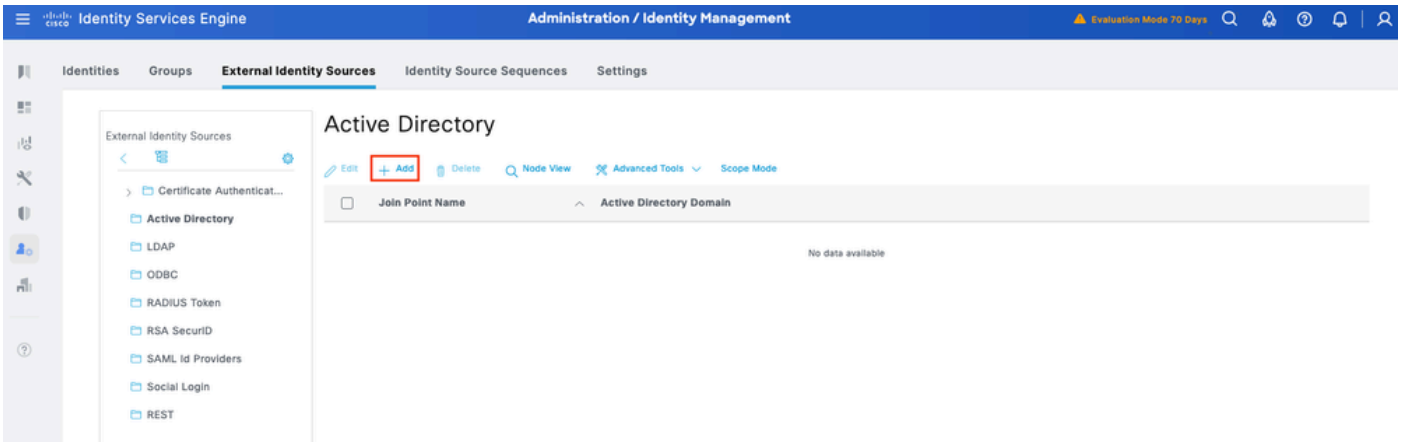


Tip: É recomendável ativar o modo de conexão única para evitar reiniciar a sessão TCP toda vez que um comando for enviado ao dispositivo.

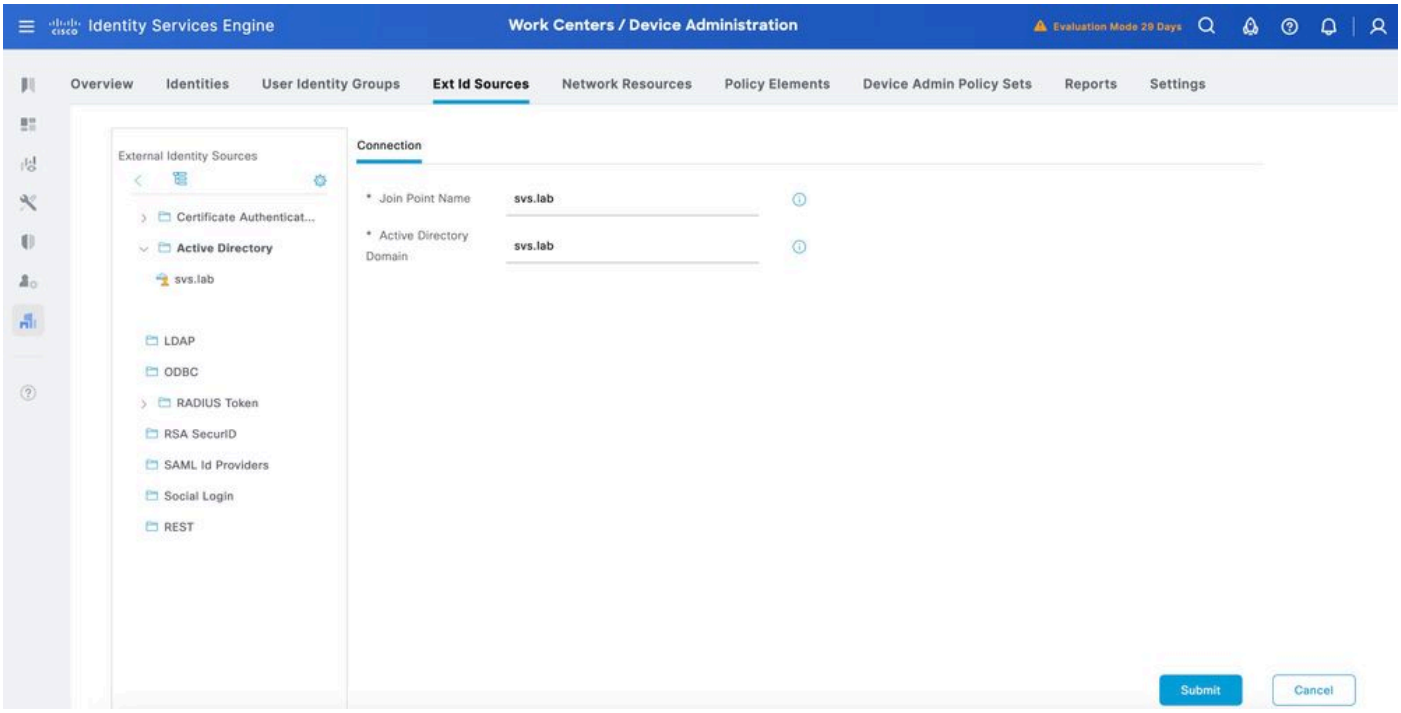
ConfigurarRepositórios de Identidade

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.

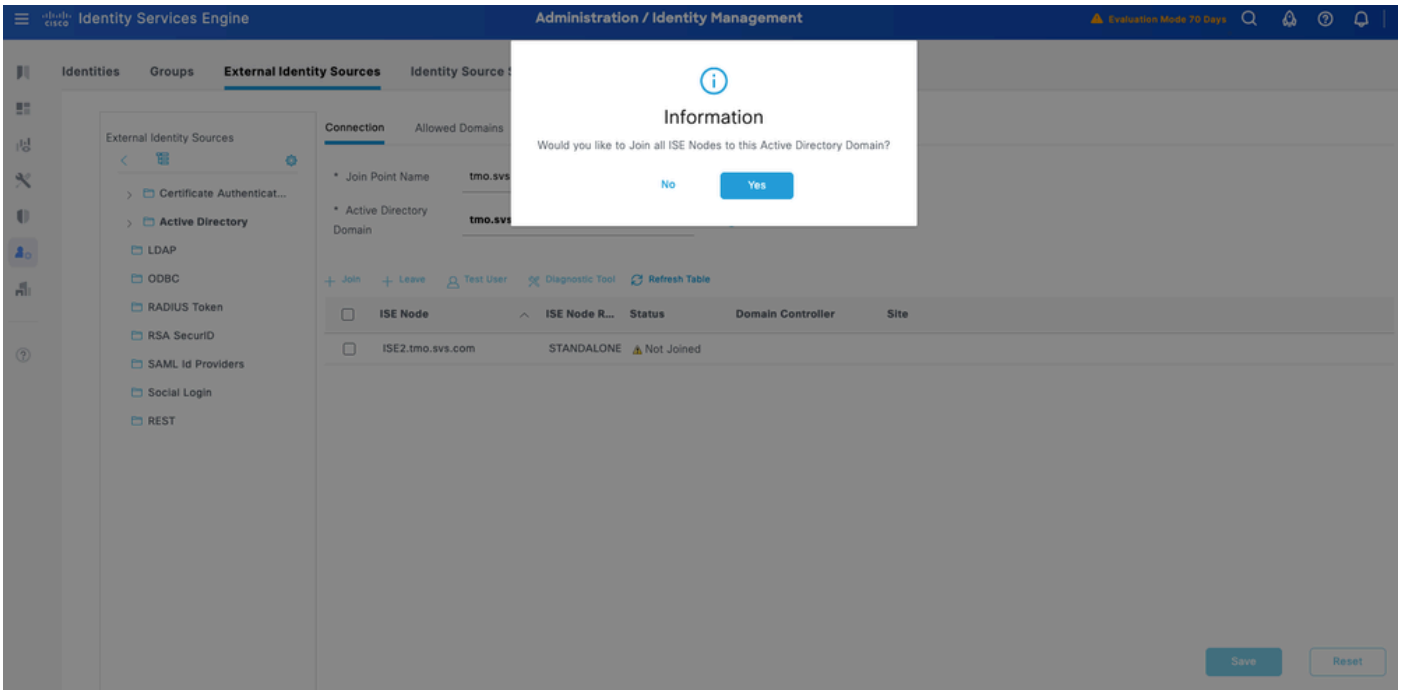
Etapa 1. Navegue até Administração > Gerenciamento de identidades > Repositórios de identidades externos > Ative Diretory. Clique em Adicionar para definir um novo ponto conjunto do AD.



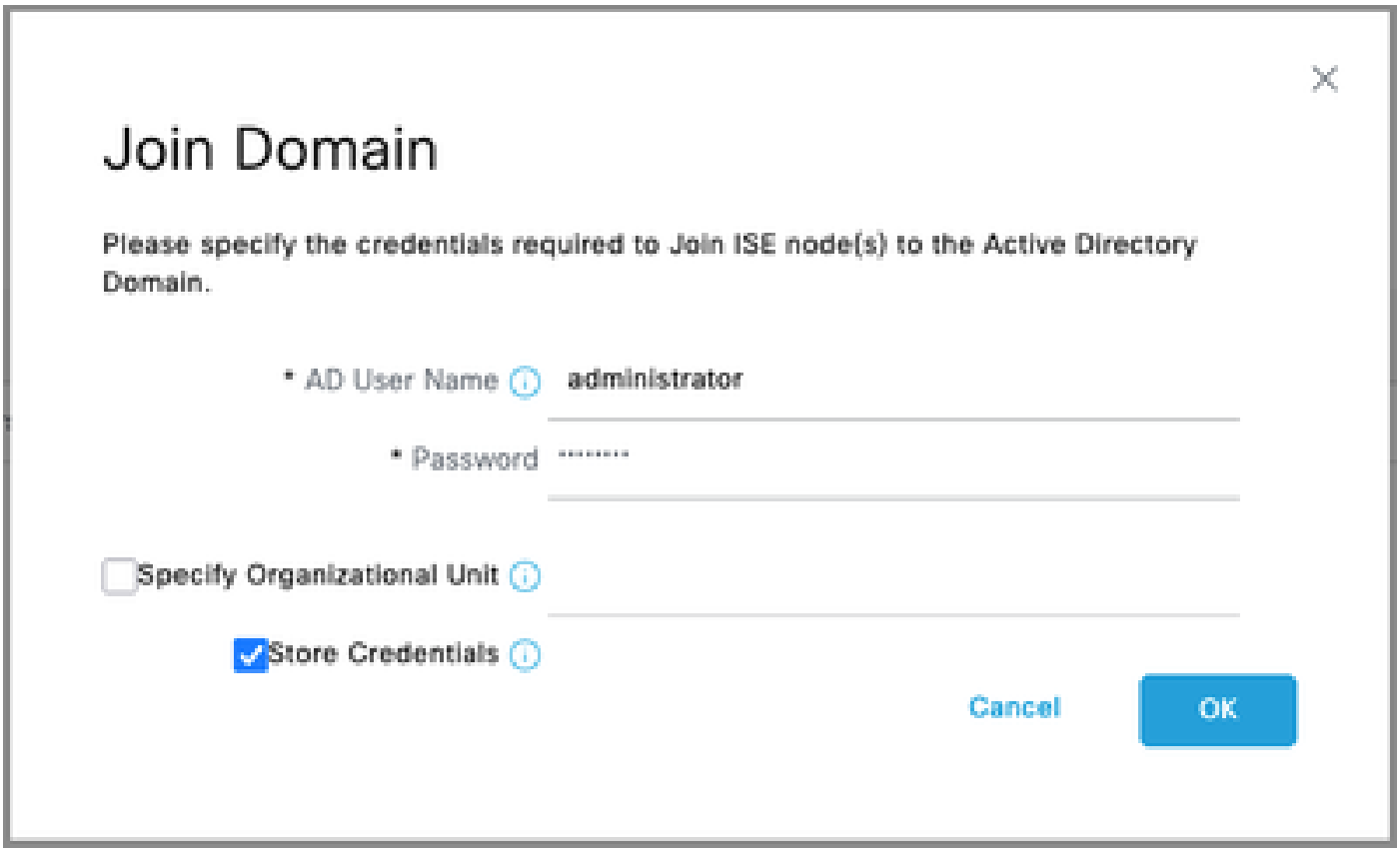
Etapa 2. Especifique o nome do ponto de junção e o nome de domínio do AD e clique em Enviar.

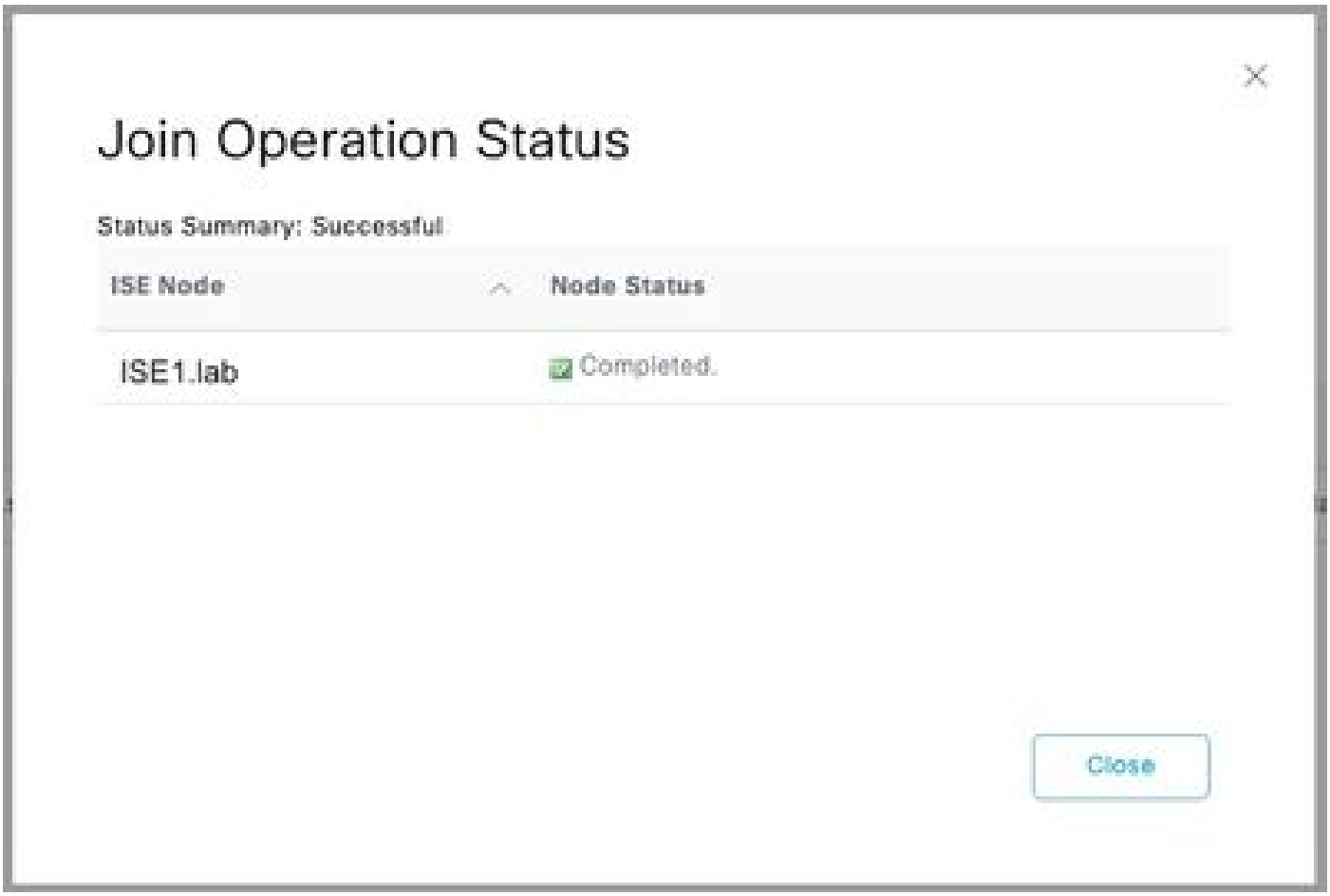


Etapa 3. Clique em Sim quando solicitado Deseja unir todos os nós do ISE a este domínio do Ative Diretory?

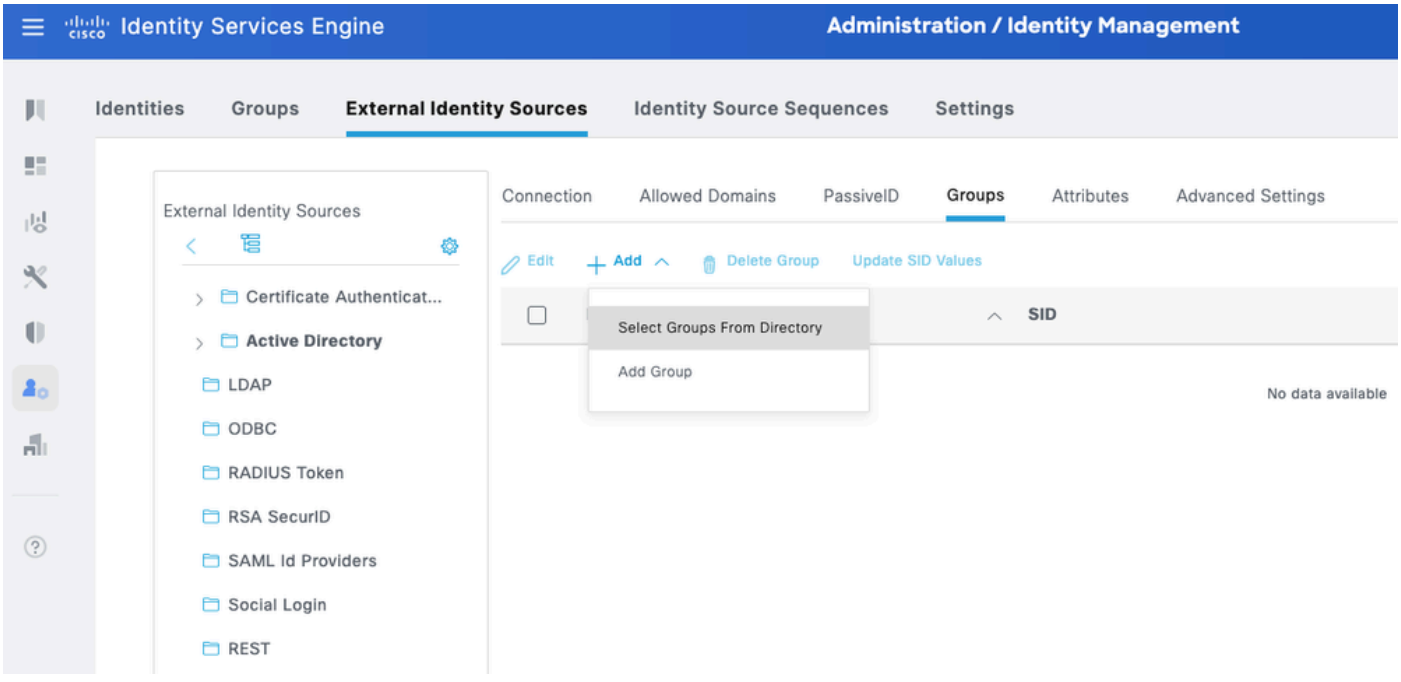


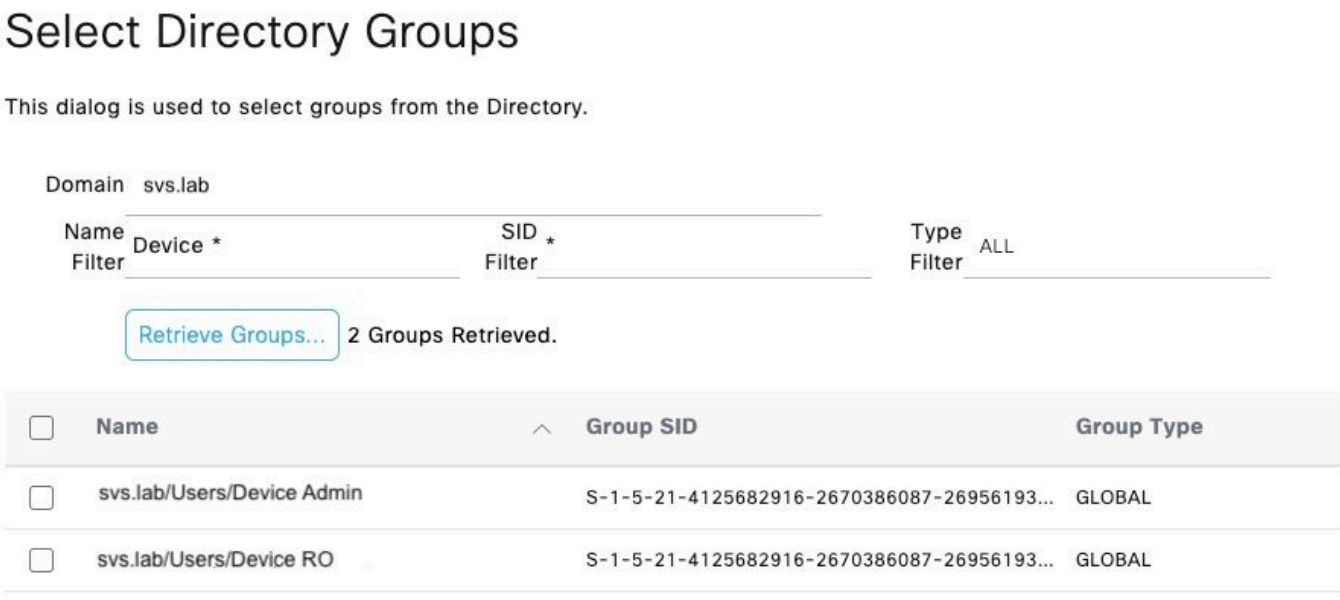
Etapa 4. Insira as credenciais com privilégios de ingresso no AD e Ingresse no ISE para o AD. Verifique o Status para verificar se ele está operacional.

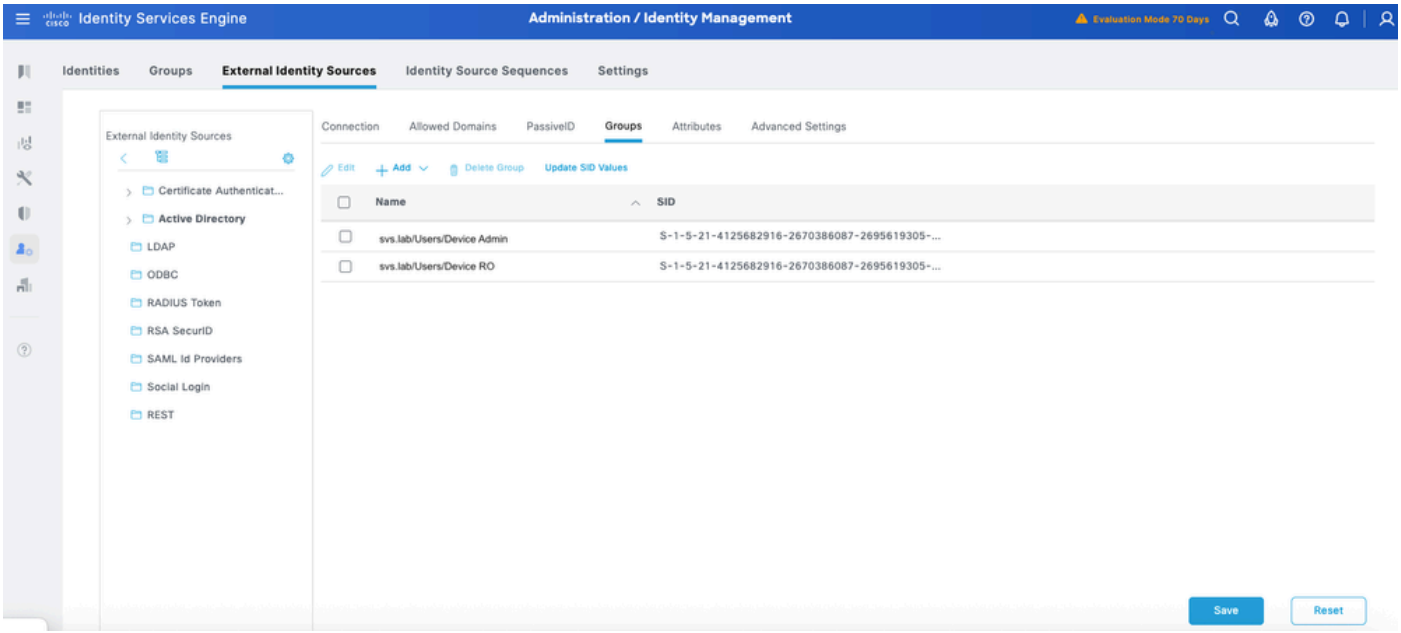




Etapa 5. Navegue até a guia Grupos e clique em Adicionar para obter todos os grupos necessários com base nos quais os usuários estão autorizados para o acesso ao dispositivo. Este exemplo mostra os grupos usados na Diretiva de Autorização neste guia







Configurar perfis TACACS+

Você vai mapear os Perfis TACACS+ para as duas principais funções de usuário nos dispositivos Cisco IOS XE:

- 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.

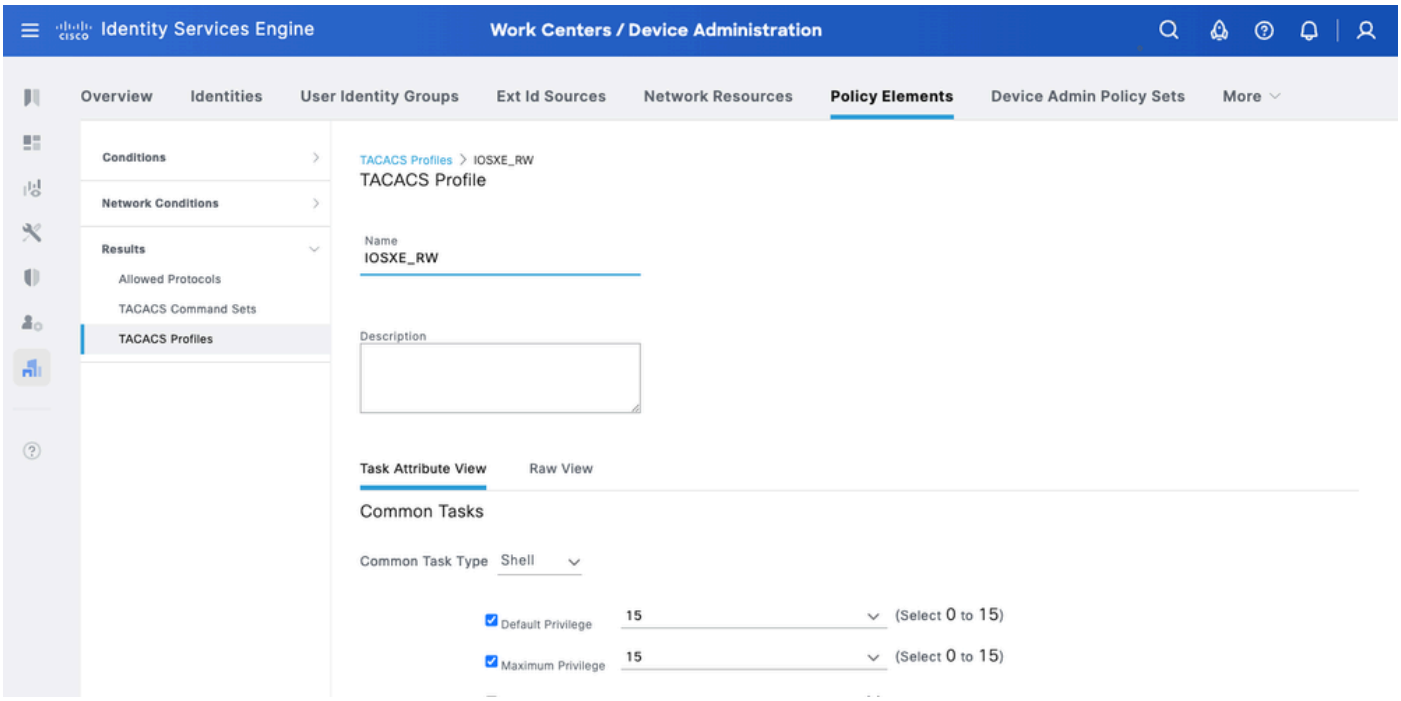
Eles são definidos como dois perfis TACACS+: IOS XE_RW e IOSXR_RO.

IOS XE_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 IOS XE_RW.

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

Etapa 3.Confirme a configuração e salve.

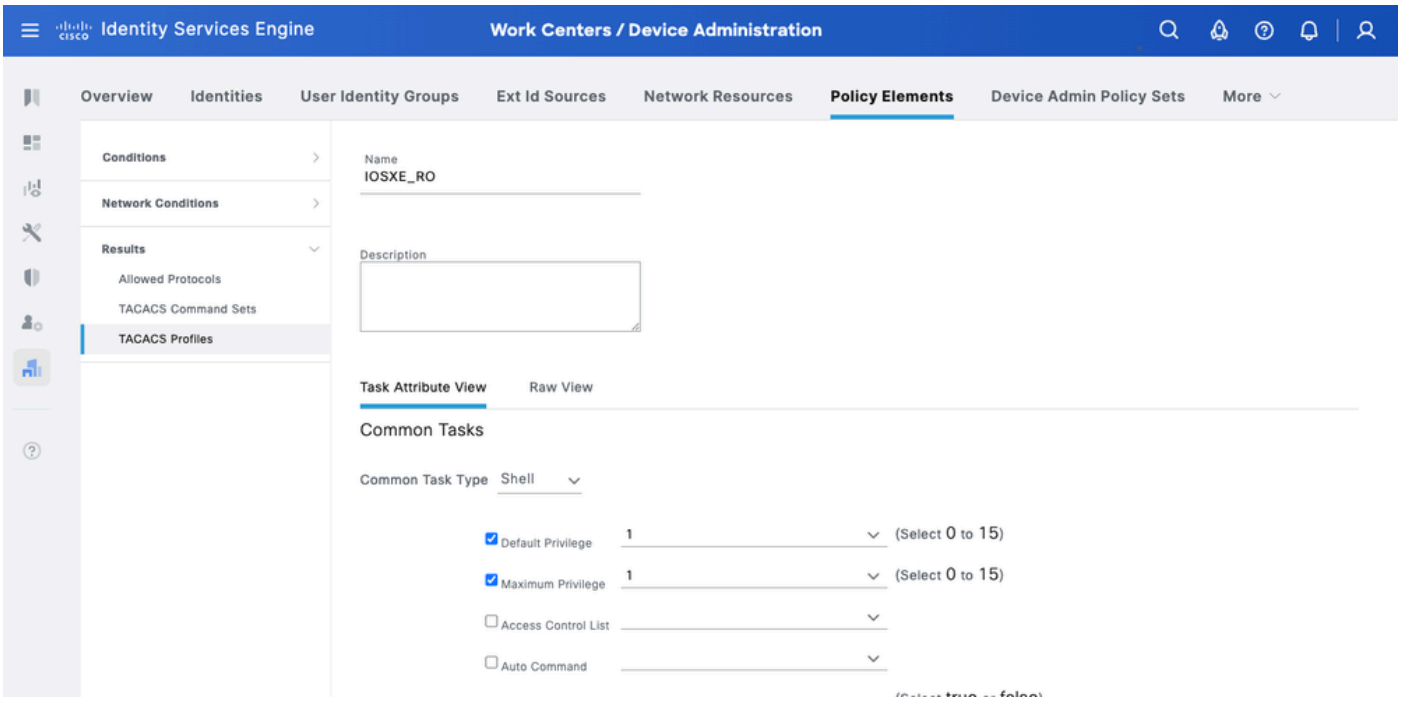


IOS XE_RO - Perfil do operador

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 IOS XE_RO.

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

Etapa 3.Confirme a configuração e salve.



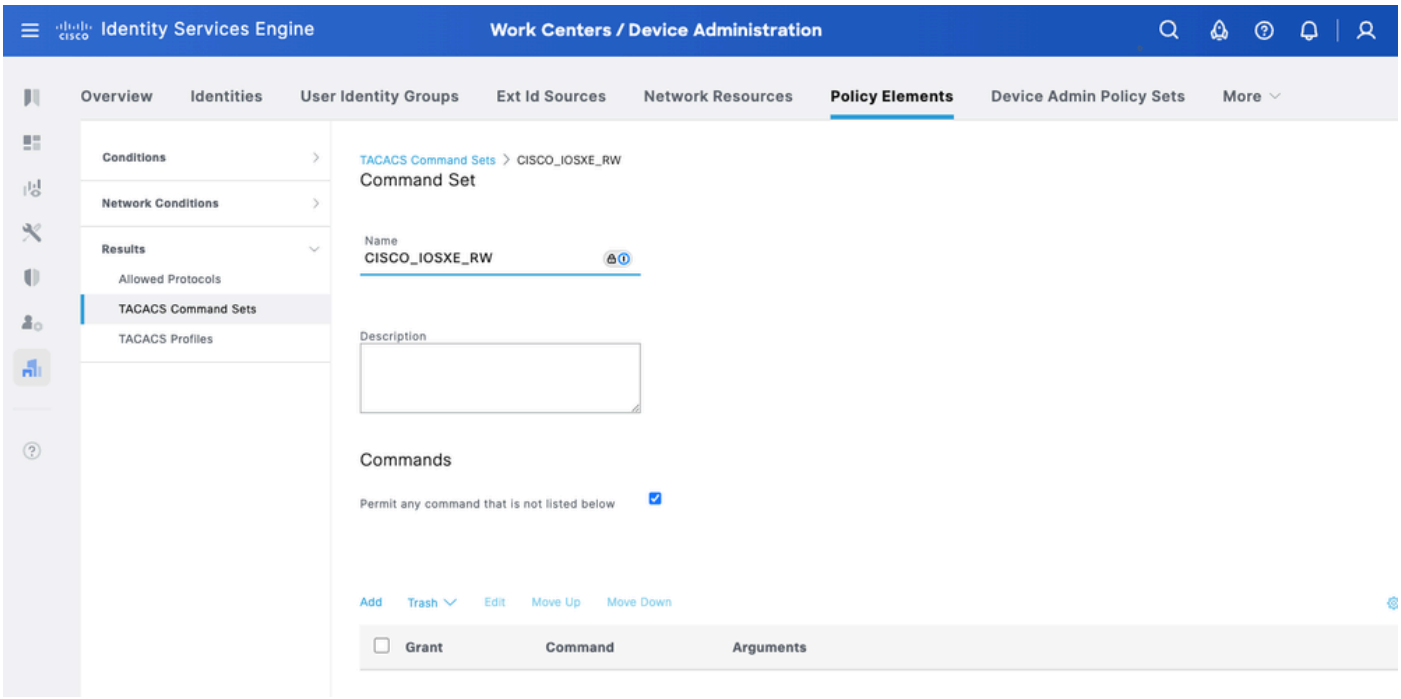
Configurar conjuntos de comandos TACACS+

eles são definidos como dois conjuntos de comandos TACACS+: CISCO_IOS XE_RW e CISCO_IOS XE_RO.

CISCO_IOS XE_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 como CISCO_IOS XE_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.



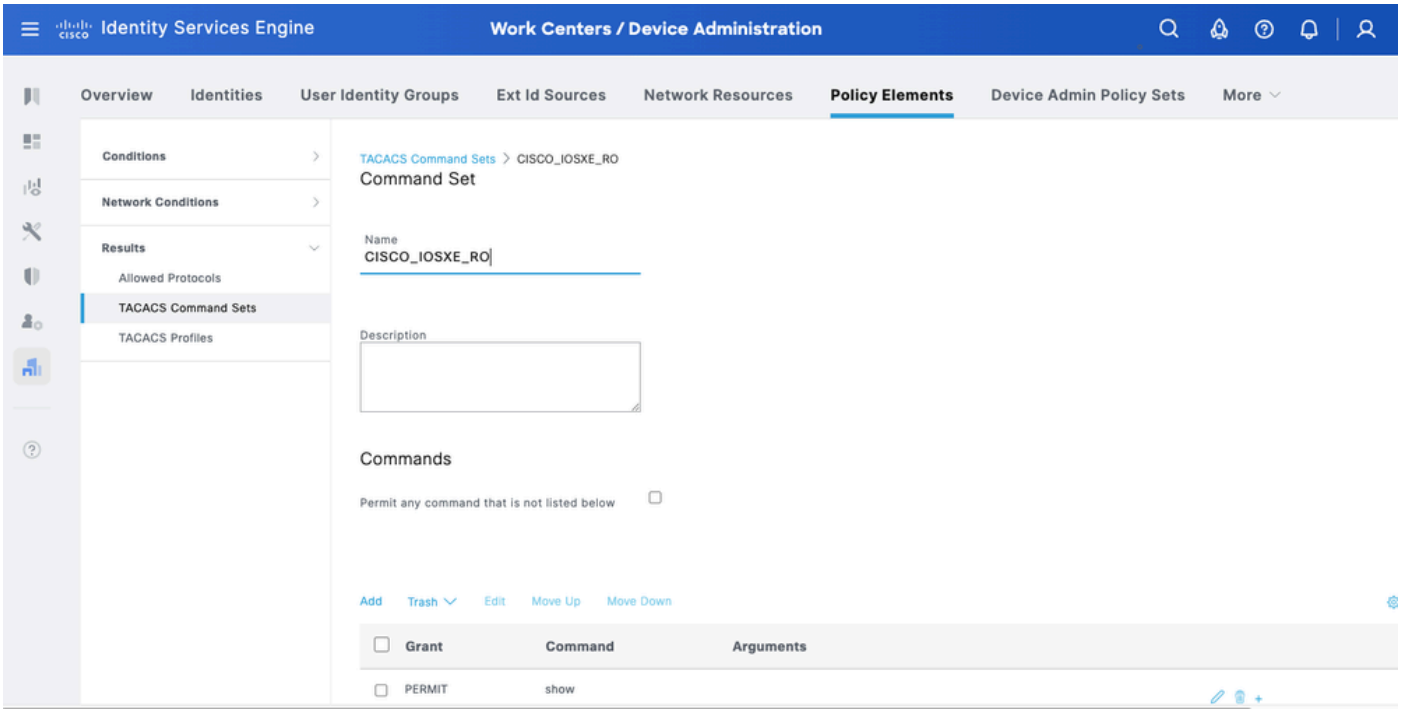
CISCO_IOS XE_RO - Conjunto de comandos do operador

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_IOS XE_RO.

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

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

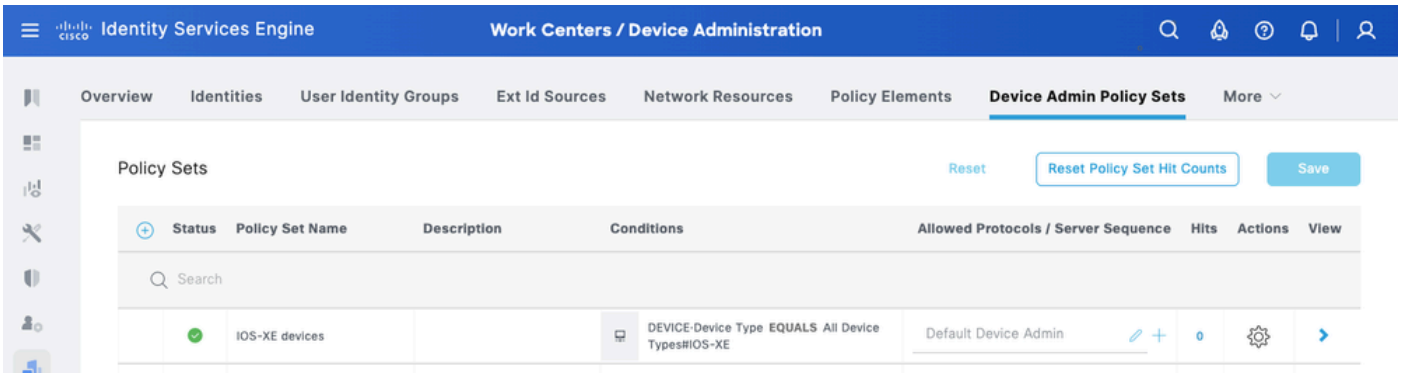
Etapa 4. Confirme os dados e clique em Salvar.



ConfigurarConjuntos de Políticas de Administração do Dispositivo

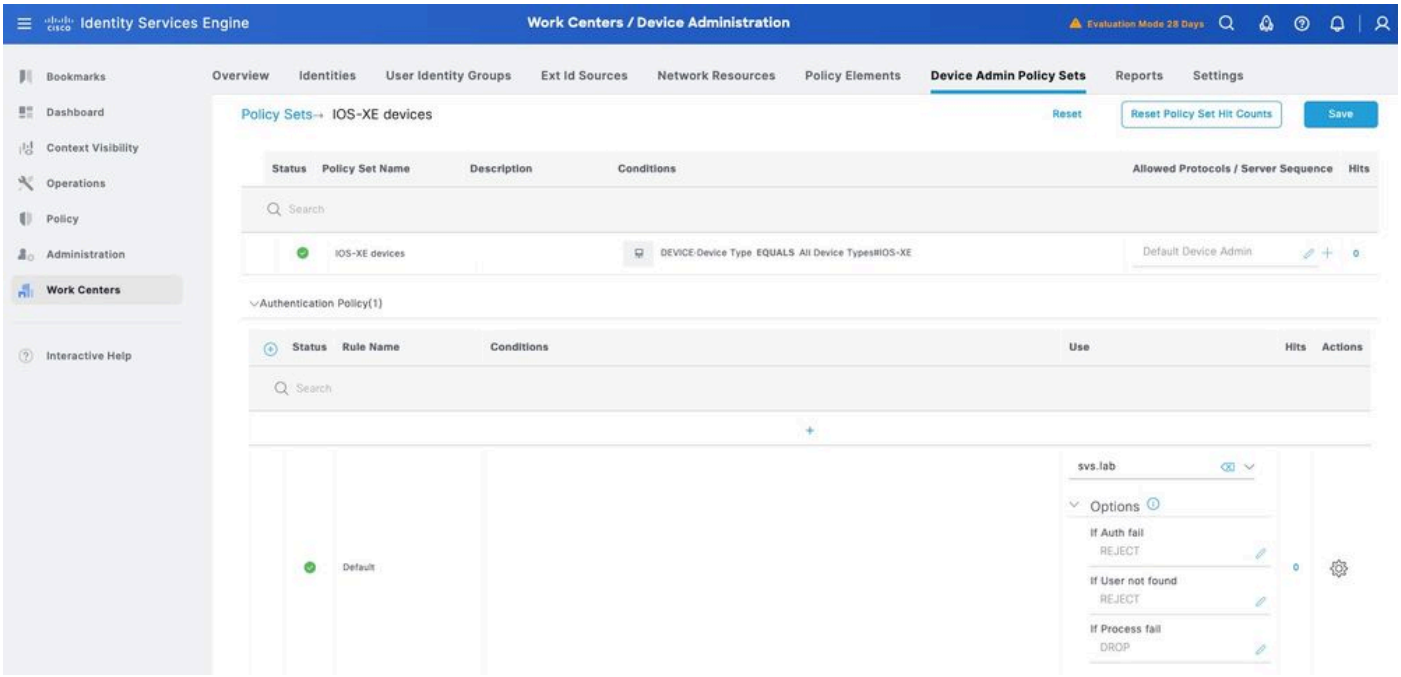
Os conjuntos de políticas são ativados por padrão para a Administração de dispositivos. Os conjuntos de políticas podem dividir as políticas com base nos tipos de dispositivo para facilitar a aplicação de perfis TACACS.

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



Etapa 2.Clique em Save e clique na seta para a direita para configurar esse Policy Set.

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.



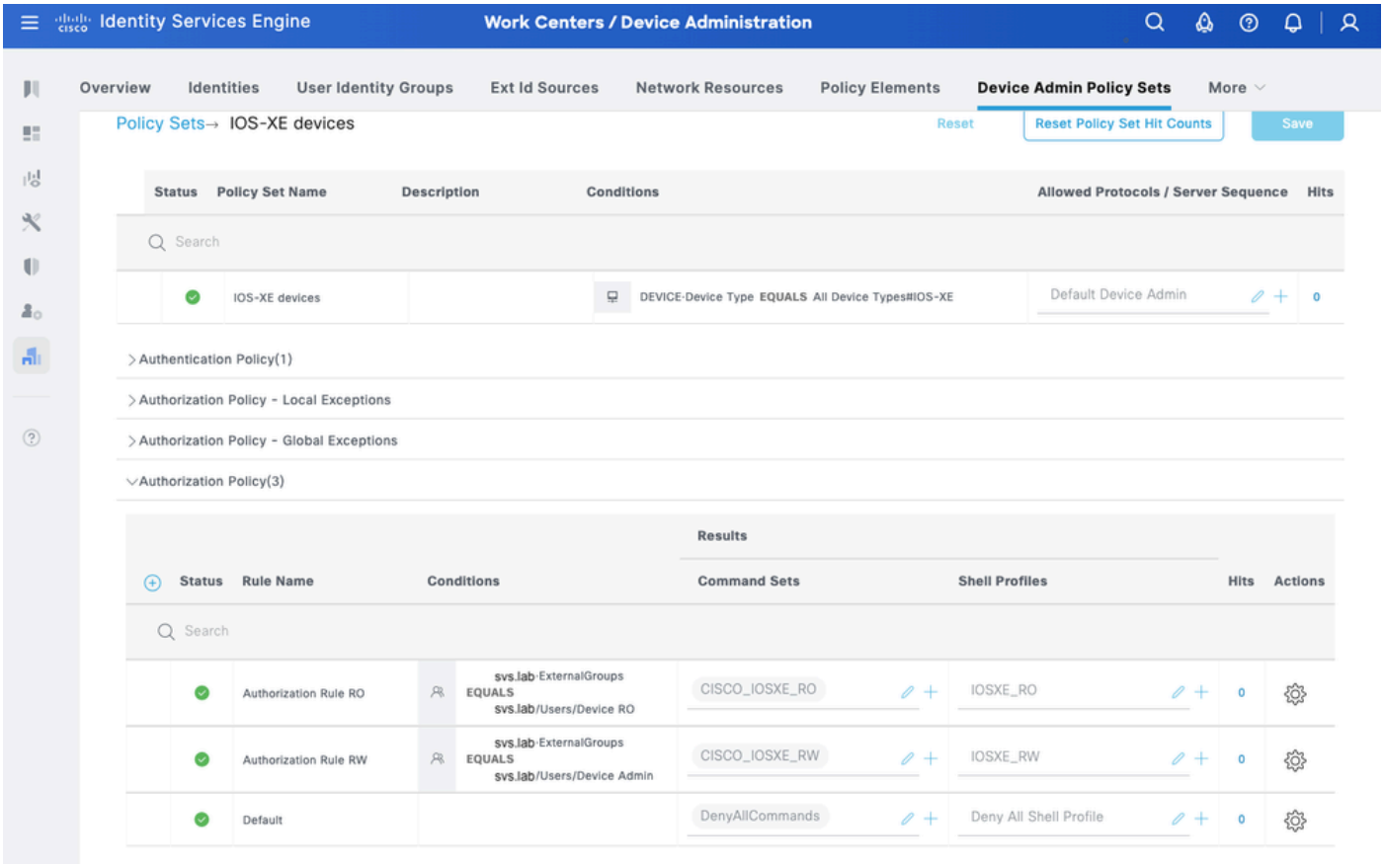
Etapa 4. Definir a Política de Autorização.

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

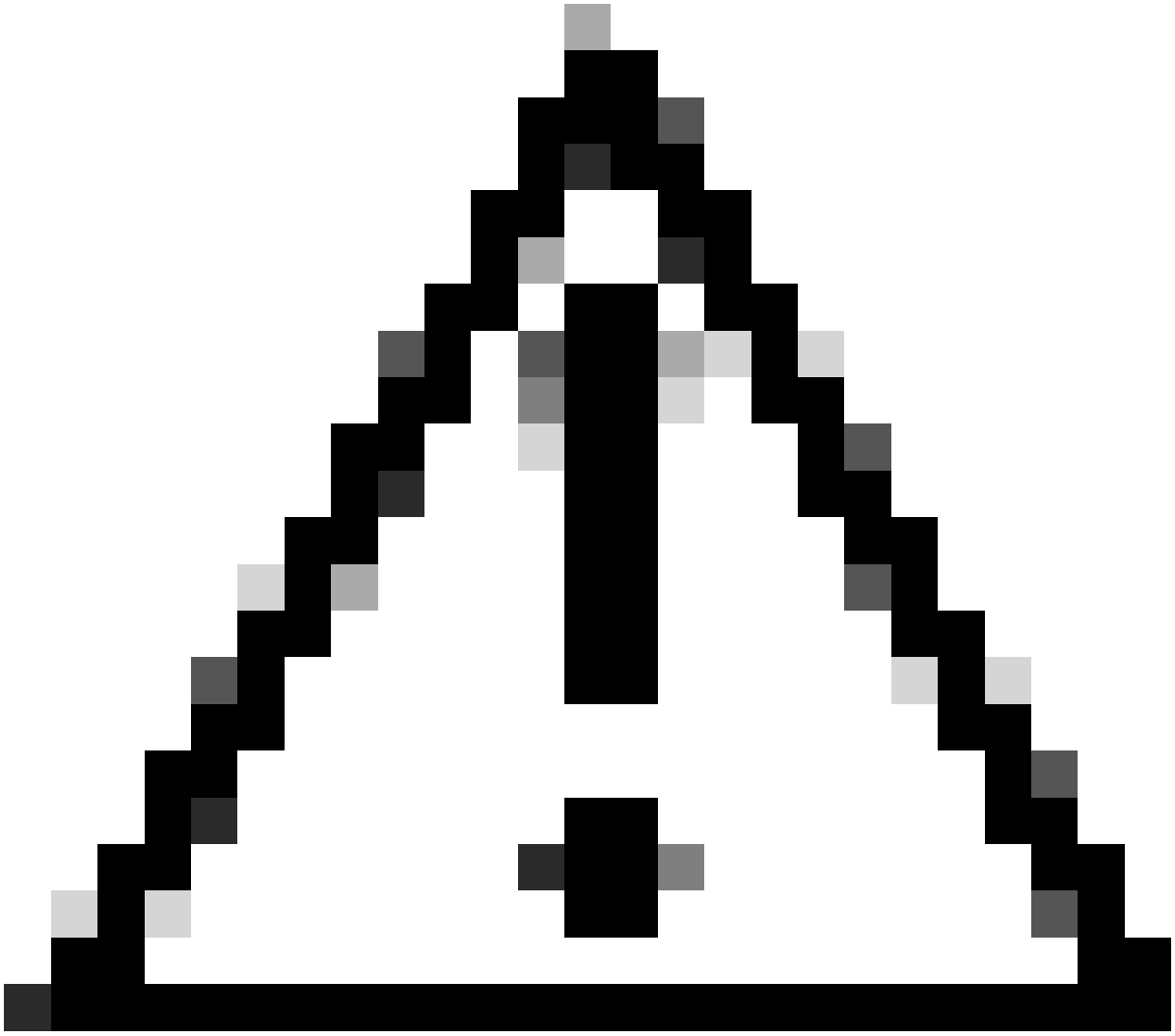
Por exemplo:

Os usuários do grupo AD Device RO recebem o conjunto de comandos CISCO_IOSXR_RO e o perfil do shell IOSXR_RO .

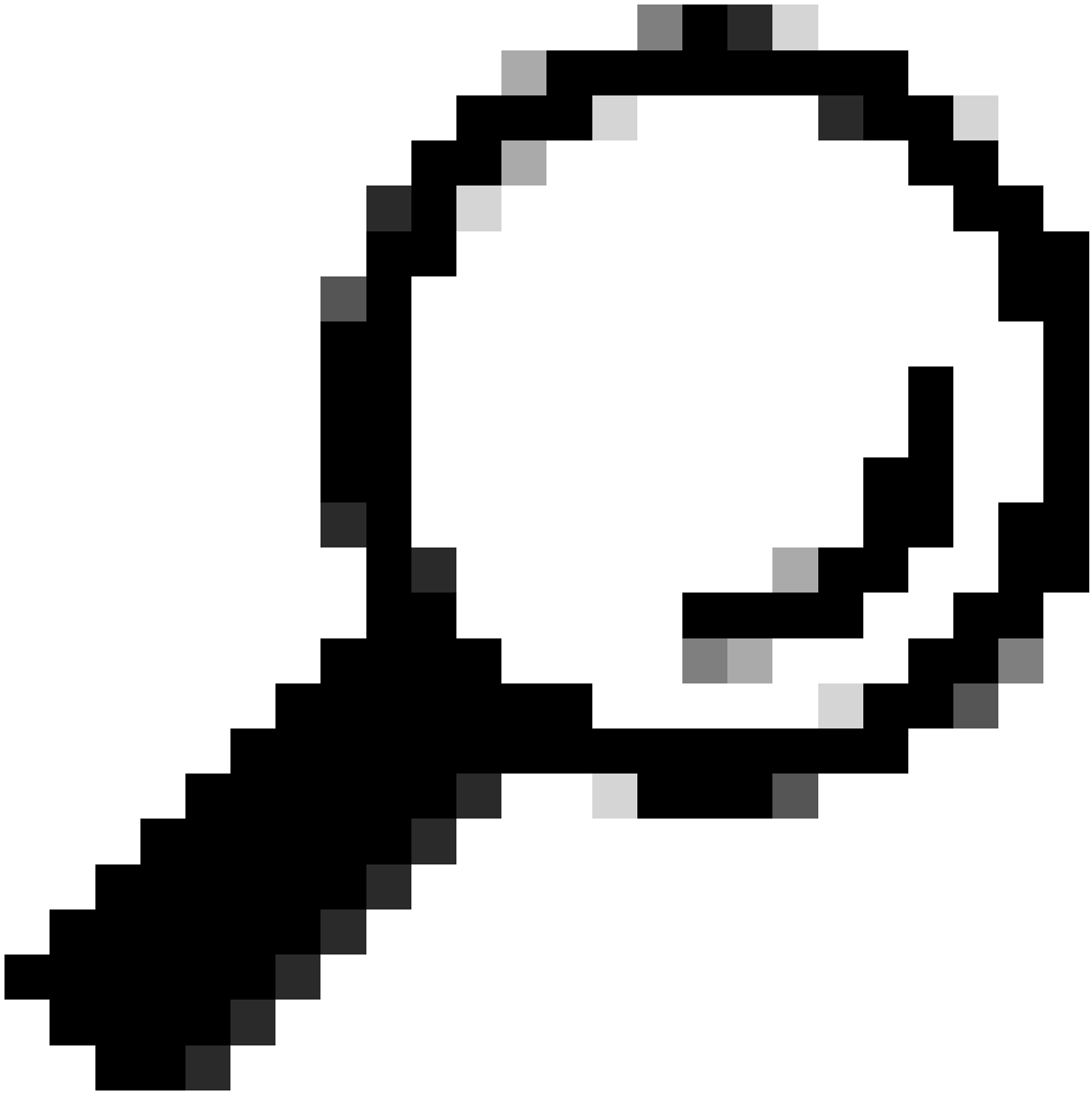
Os usuários do grupo AD Device Admin recebem o conjunto de comandos CISCO_IOSXR_RW e o perfil do shell IOSXR_RW .



Parte 2 - Configurar o Cisco IOS XE 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.

Método de configuração 1 - Par de chaves gerado pelo dispositivo

Configuração do servidor TACACS+

Etapa 1Configure o nome de domínio e gere um par de chaves usado para o ponto de confiança do roteador.

```
ip domain name svs.lab

crypto key generate ec keysize 256 label svs-256ec-key
```

Configuração do Trustpoint

Etapa 1 Crie o ponto de confiança do roteador e associe o par de chaves.

```
crypto pki trustpoint svs_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svs-256ec-key
```

Etapa 2. Autentique o ponto de confiança instalando o certificado CA.

<#root>

```
cat9k(config)#
```

crypto pki authenticate svs_cat9k

```
Enter the base 64 encoded CA certificate.

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+t3c1sNbN2AtFi4cJovTA01xh6OI4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
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
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==

-----END CERTIFICATE-----

Certificate has the following attributes:
   Fingerprint MD5: D9C4O4B2 ECO8A26O EC3539E7 F54ED17D
   Fingerprint SHA1: OEB181E9 5A3ED78O 3BC5A8O5 9A854A95 C83AC737

% Do you accept this certificate? [yes/no]:

yes


Trustpoint CA certificate accepted.
% Certificate successfully imported

cat9k(config)#
```

Etapa 3. Gerar CSR (Certificate Signing Request, solicitação de assinatura de certificado).

<#root>

```
cat9k(config)#

crypto pki enroll svs_cat9k


% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
% The subject name in the certificate will include: cat9k.svs.lab
Display Certificate Request to terminal? [yes/no]:

yes


Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIBfDCCASMCAQAwgYQxGjAYBgNVBAMTEWNhdDlrLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxCzAJBgNVBAgT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2FOOWsudG1vLnN2cy5j
b20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrtl4ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREEFTATghFjYXQ5ay5ObW8uc3ZzLmNvbTAL
```

```
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTwM3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
```

no

```
cat9k(config)#
```

Etapa 4. Importar certificado assinado pela CA.

<#root>

```
cat9k(config)#
```

crypto pki import svs_cat9k certificate

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIID8zCCAdugAwIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTE0MTUxMjAwWhcNMjYwNTE0MTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ2lzY28x
DDAKBgNVBAcTA1JUUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTAlVTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay5ObW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABOlgTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFyOrLiyjxXmLpFcO3uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2Vy
dGlmaWNhdGUwHAYDVR0RBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUAA4ICAQBObgKVykeyVC9UsvuuOAUsGaZHGwy2H9Yd
m5vIaui6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHLtifPayxv9juDuOZRx+wYR2PIQ5eLv1bafg7K8E82sqOCfOtcPr
Oc0NU8UCxqObdOgu4XsdBN1+wcWFqeQSDLmP7nxvhOOm/LXwCWUHwgVioOAuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
lxCSoLtYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqf4mGh/AO8T4iXfWDWfNezh7ZxMsCSCK/ZRlELZ2hj6OfzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVrPitwN3ZbO9poZyWiRLTnBsb42xNaWiL9bjQznAOiTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+4lOTMawDgGiEv7iaiJ6xWc95EC+AdmOx3FvBXMtIM9qr7WwHW6
3C2hVYHJH254elV5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#
```

TACACS e AAA com configuração TLS

Etapa 1. Crie o servidor TACACS e grupos AAA, associe o ponto de confiança do cliente (roteador).

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Etapa 2. Configurar métodos AAA.

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

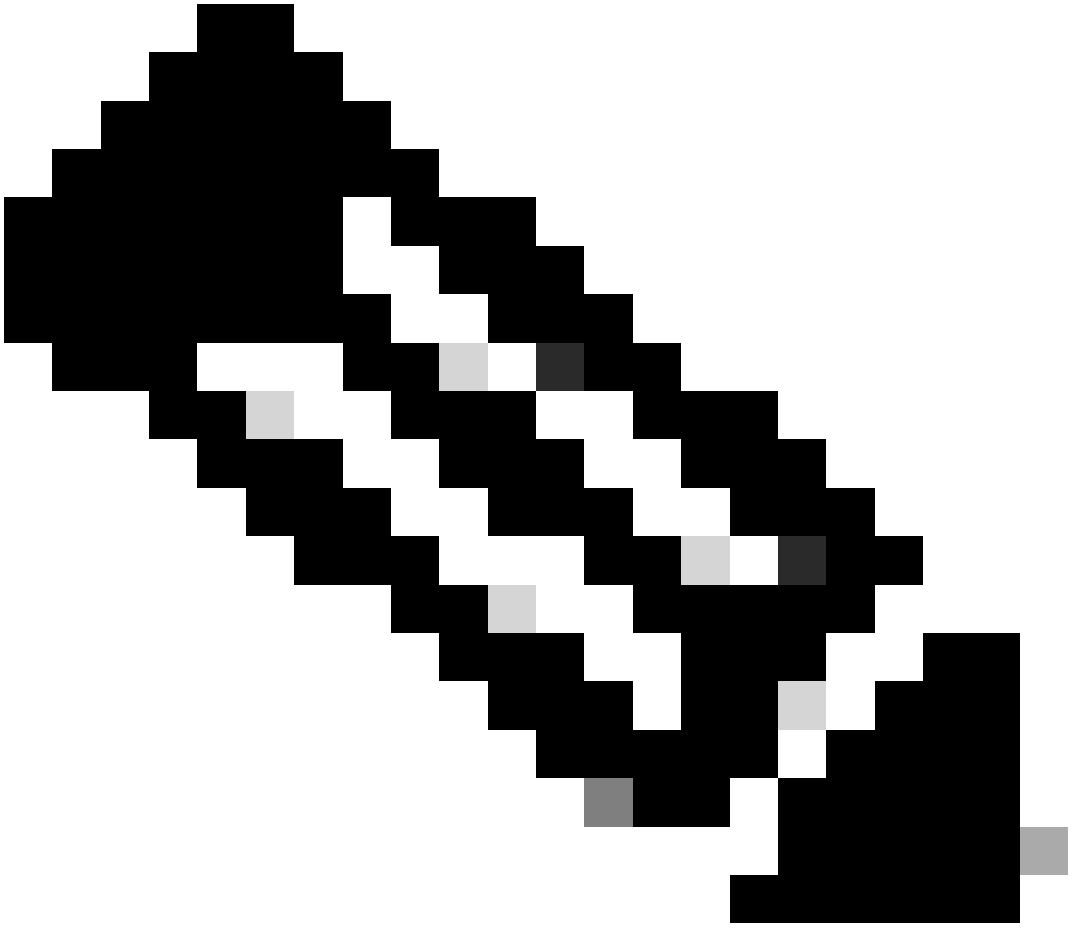
Método de configuração 2 - Par de chaves gerado pela CA

Se você estiver importando as chaves, bem como os certificados de dispositivo e CA diretamente em um formato PKCS#12 em vez do método CSR, poderá usar esse método.

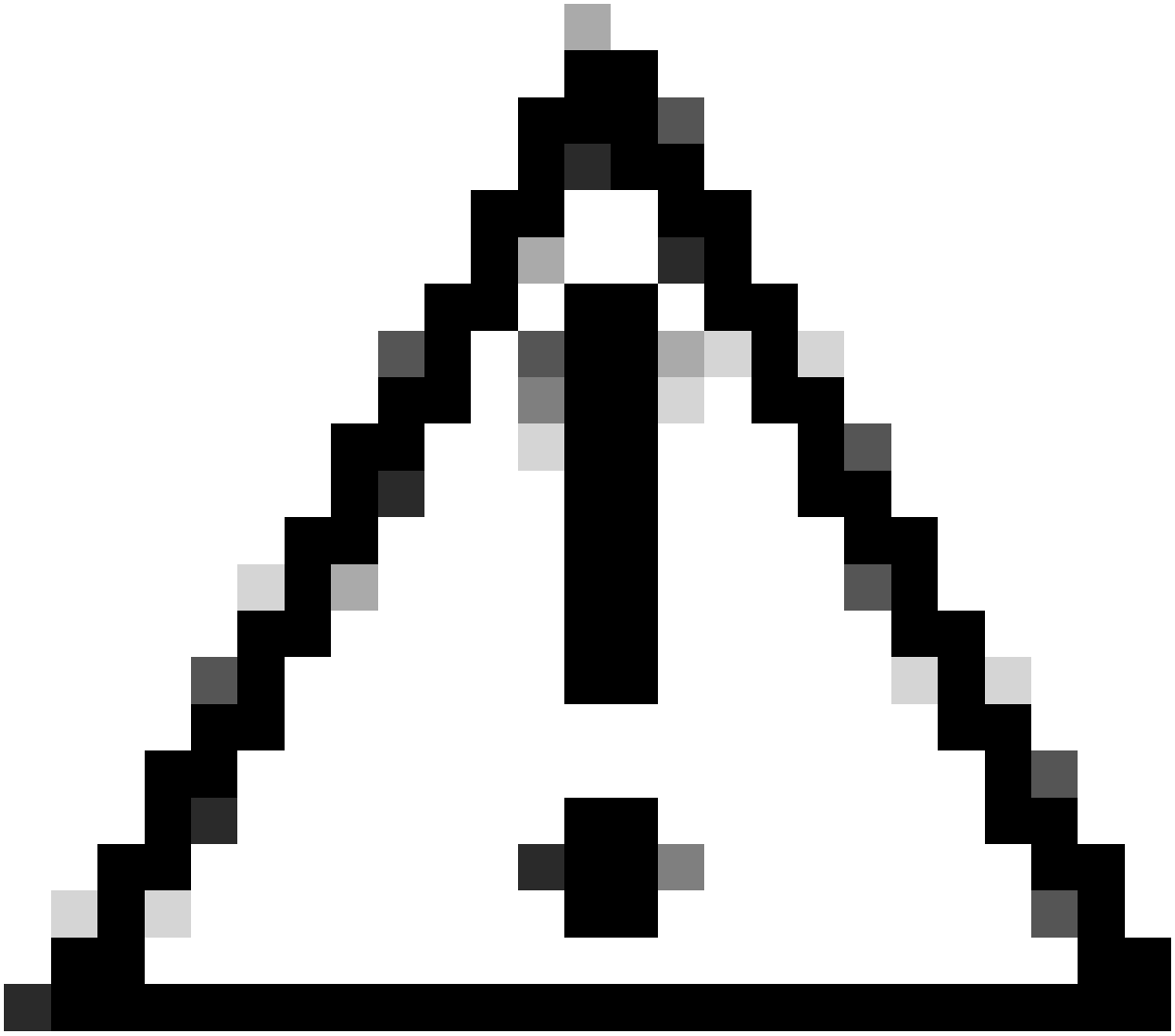
Etapa 1. Crie o ponto de confiança do cliente.

```
cat9k(config)#crypto pki trustpoint svs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

Etapa 2. Copie o arquivo PKCS#12 no bootflash.



Note: Certifique-se de que o arquivo PKCS#12 contenha a cadeia completa de certificados e a chave privada como arquivo criptografado.



Caution: As chaves no PKCS#12 importado devem ser de RSA (Por exemplo: RSA 2048), não ECC.

<#root>

cat9k#

copy sftp bootflash: vrf Mgmt-vrf

```
Address or name of remote host [10.225.253.247]?
Source username [svs-user]?
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx
Destination filename [cat9k-25jun17.pfx]?
Password:
!
2960 bytes copied in 3.022 secs (979 bytes/sec)
```

Etapa 3. Importe o arquivo PKCS#12 usando o comando import.

<#root>

```
cat9k#

crypto pki import svs_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

 password C1sco.123
% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx
CRYPTO_PKI: Imported PKCS12 file successfully.
cat9k#

cat9k#

show crypto pki certificates svs_cat9k_25jun17


Certificate
  Status: Available
  Certificate Serial Number (hex): 586OBF33A2O33365
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    Name: cat9k.svs.lab
    e=pkalkur@cisco.com
    cn=cat9k.svs.lab
    ou=svs
    o=cisco
    l=rtp
    st=nc
    c=us
  Validity Date:
    start date: 17:56:00 UTC Jun 17 2025
    end   date: 17:56:00 UTC Jun 17 2026
  Associated Trustpoints: svs_cat9k_25jun17

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 2OCD74O2C4DA37F5
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Validity Date:
    start date: 17:05:00 UTC Apr 28 2025
    end   date: 17:05:00 UTC Apr 28 2035
  Associated Trustpoints: svs_cat9k_25jun17 svs_cat9k
```

```
  Storage: nvram:SVSLabCA#37F5CA.cer
```

TACACS e AAA com configuração TLS

Etapa 1. Crie o servidor TACACS e grupos AAA, associe o ponto de confiança do cliente (roteador).

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Etapa 2. Configurar métodos AAA.

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

Verificação

Verificar a configuração.

```
show tacacs
show crypto pki certificates <>
show crypto pki trustpoints <>
```

Depuração para AAA e TACACS+.

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure

! Below debugs will be needed only if there is any issue with SSL Handshake
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

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.