Configurar TACACS de Autenticação Externa do Catalyst Center com ISE

Contents

Introdução

Este documento descreve as etapas necessárias para integrar o Cisco Identity Services Engine com o Catalyst Center para ativar a autenticação TACACS+.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso de administrador ao Cisco ISE e ao Cisco Catalyst Center.
- Compreensão básica dos conceitos de AAA (Authentication, Authorization, and Accounting).
- Conhecimento prático do protocolo TACACS+.
- Conectividade de rede entre o Catalyst Center e o servidor ISE.

Componentes Utilizados

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

- Cisco Catalyst Center versão 2.3.7.x
- Cisco Identity Services Engine (ISE) versão 3.x (ou posterior)
- Protocolo TACACS+ para autenticação de usuário externo

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.

Informações de Apoio

Essa integração permite que usuários externos façam login no Catalyst Center para acesso e gerenciamento administrativos.

Configurar

Cisco Identity Services Engine (ISE)

Licenciar e ativar os serviços TACACS+

Antes de começar com a configuração TACACS+ no ISE, você deve confirmar se a licença correta está instalada e se o recurso está habilitado.

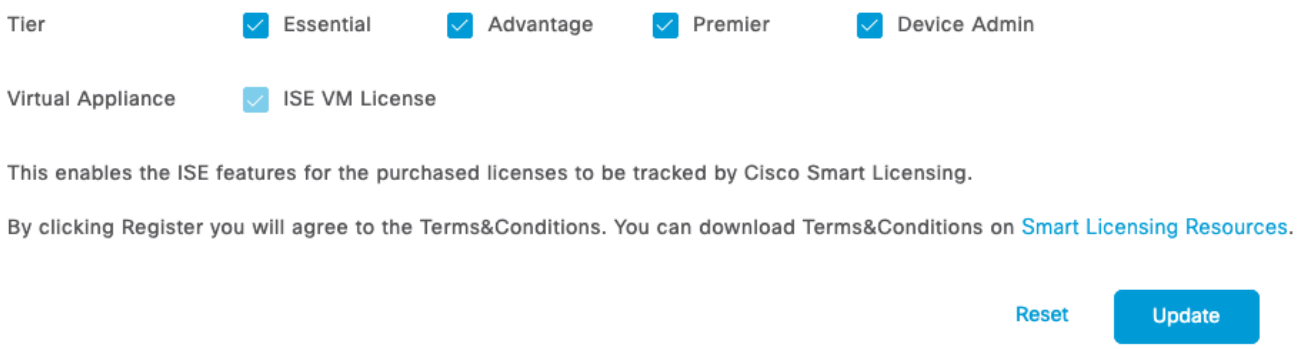
1. Verifique se você tem a licença PID L-ISE-TACACS-ND= no portal Cisco Smart Software Manager ou Cisco License Central.

Habilite a Administração de dispositivo no portal de licenciamento do ISE.

- A licença Device Admin (PID: L-ISE-TACACS-ND=) permite serviços TACACS+ em um Policy Service Node (PSN).
- Navegue até:

  Administração > Sistema > Licenciamento

- Marque a caixa Device Admin nas opções de camada.



Administrador do dispositivo

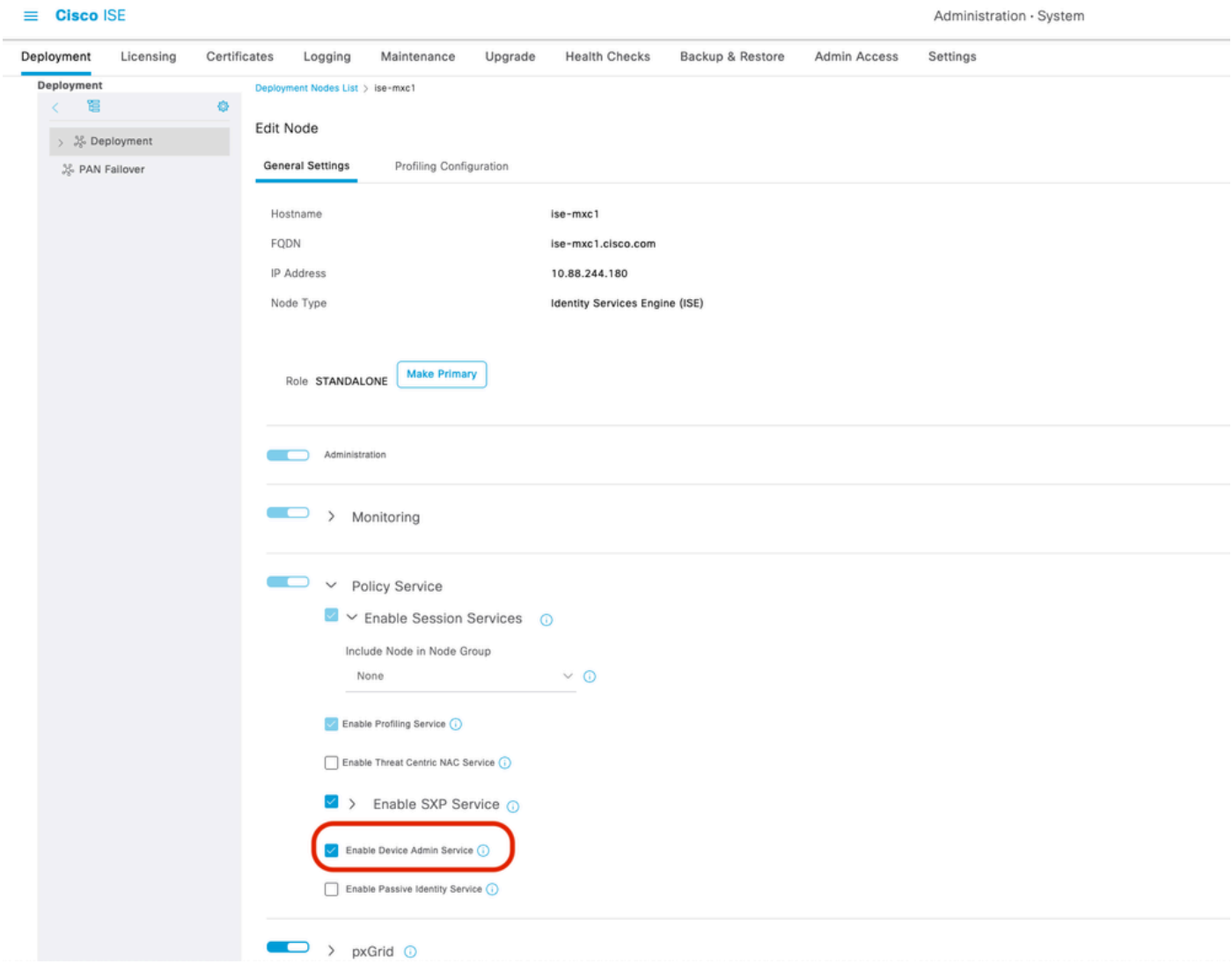
Administrador do dispositivo de licença

3. Ative o Device Admin Service no nó ISE que executa o serviço TACACS+.

- Navegue até:

  Administração > Sistema > Implantação > Selecionar o nó

- Marque a opção Enable Device Admin Service.



Habilitar Serviço de Administração de Dispositivo

Criar usuário administrador e adicionar dispositivo de rede

1. Crie o Usuário Admin.

- Essa conta de usuário é usada para fazer login na IU do Catalyst Center através da autenticação do ISE.
- Navegue até:

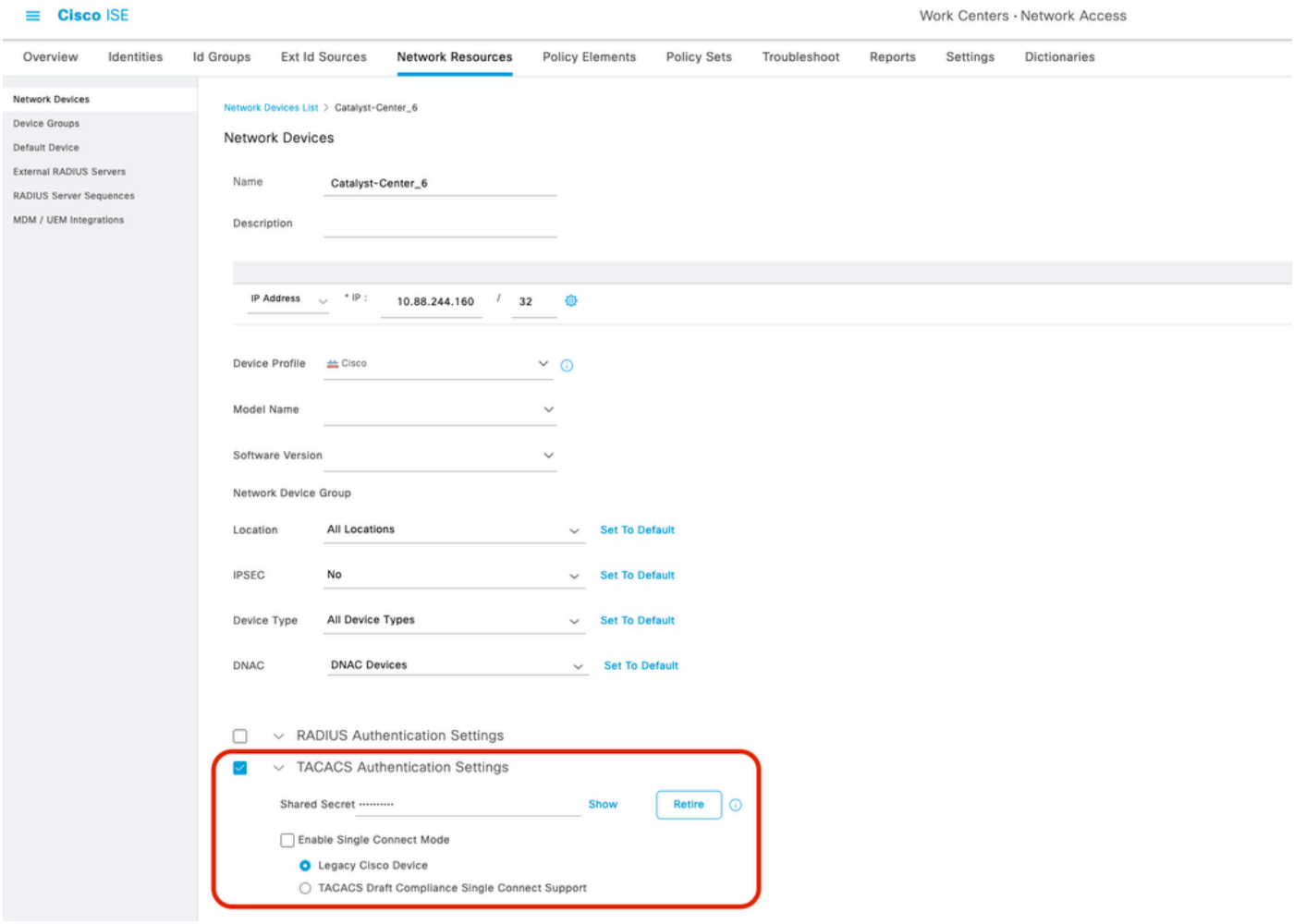
  Centros de Trabalho > Acesso à Rede > Identidades > Usuário de Acesso à Rede
- Adicione um novo usuário (por exemplo, catc-user).
- Se o usuário já existir, vá para a próxima etapa.

2. Crie o Dispositivo de Rede.

- Navegue até:

  Centros de trabalho > Acesso à rede > Identidades > Recurso de rede

- Adicione o endereço IP do Catalyst Center ou defina a sub-rede onde o IP do Catalyst Center está localizado.
- Se o dispositivo já existir, verifique se ele contém os parâmetros:
    - As configurações de autenticação TACACS estão habilitadas.
    - O segredo compartilhado está configurado e é conhecido (salve esse valor, conforme exigido posteriormente no Catalyst Center).



Configurações de autenticação TACACS

Configurar perfil TACACS+

1. Crie um novo perfil TACACS+.

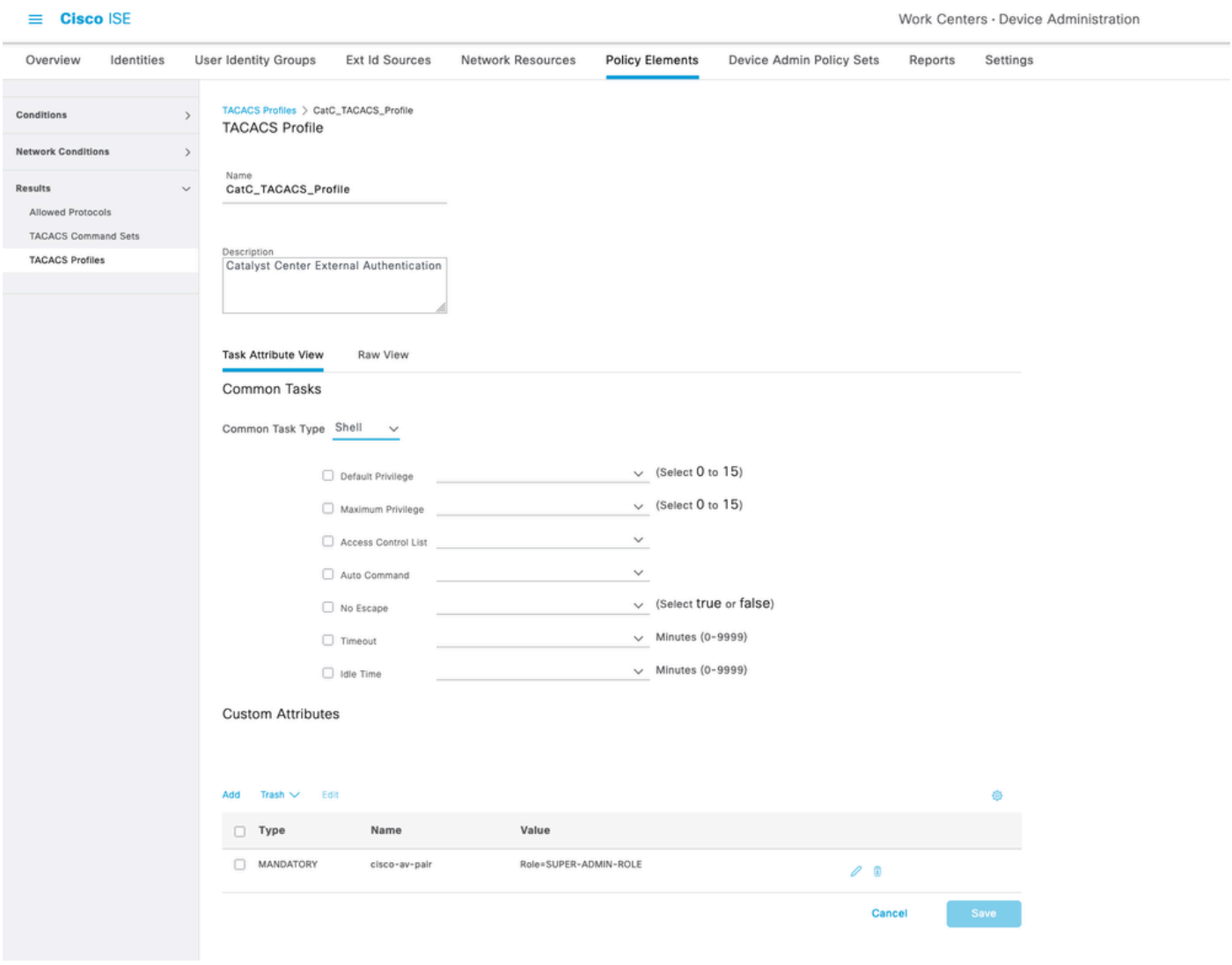
- Navegue até:

Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS

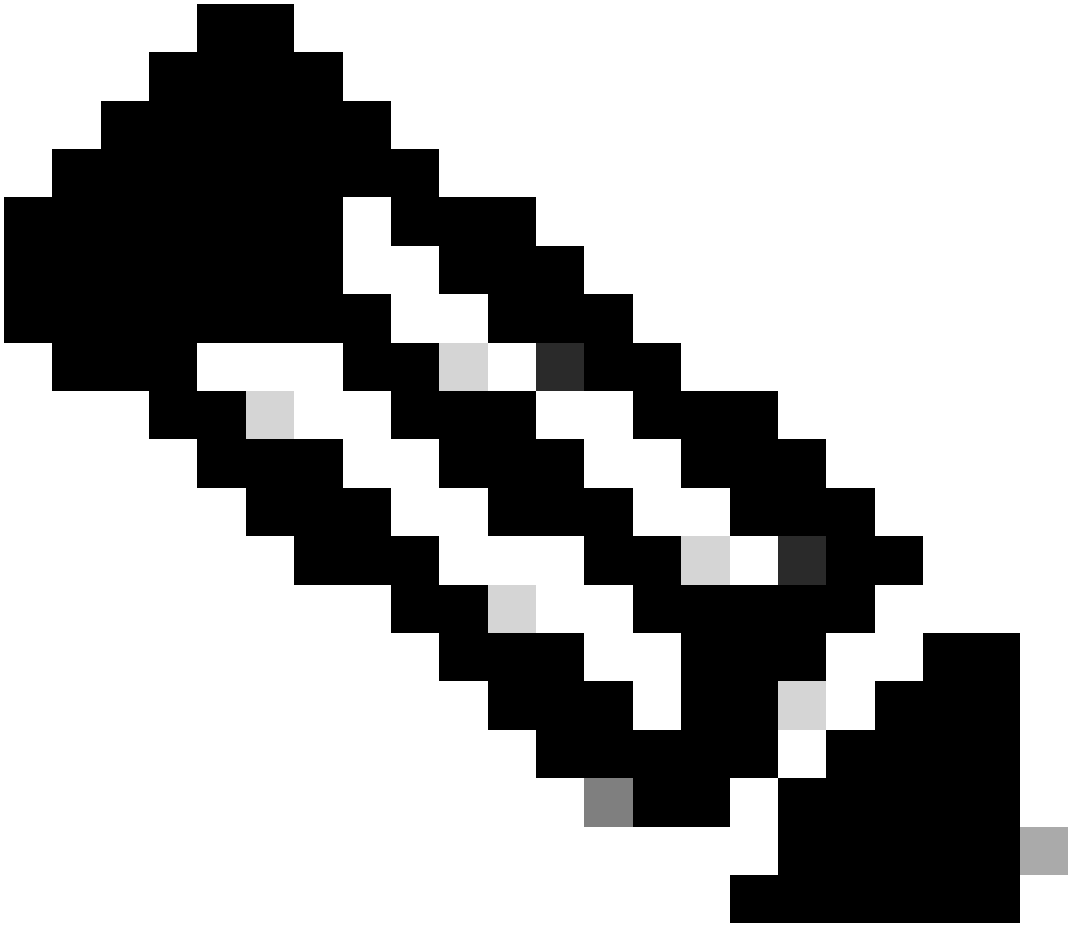
- Adicione um nome de perfil.
- Adicione um atributo personalizado da seguinte maneira:

- Digite: Obrigatório
- Nome: Cisco-av-pair
- Valor: Role=FUNÇÃO-SUPERADMIN

- Salve o perfil.



Perfil TACACS+



Note: O Cisco Catalyst Center suporta servidores externos de Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization and Accounting) para controle de acesso. Se estiver usando um servidor externo para autenticação e autorização de usuários externos, você poderá ativar a autenticação externa no Cisco Catalyst Center. A configuração de atributo AAA padrão corresponde ao atributo de perfil de usuário padrão.

O valor do atributo AAA padrão do protocolo TACACS é cisco-av-pair.

O valor do atributo AAA padrão do protocolo RADIUS é Cisco-AVPair.

A alteração só é necessária se o servidor AAA tiver um atributo personalizado no perfil do usuário. No servidor AAA, o formato do valor do atributo AAA é Role=role1. No servidor Cisco Identity Services Engine (Cisco ISE), ao configurar o perfil RADIUS ou TACACS, o usuário pode selecionar ou inserir cisco av-pair como atributo AAA.

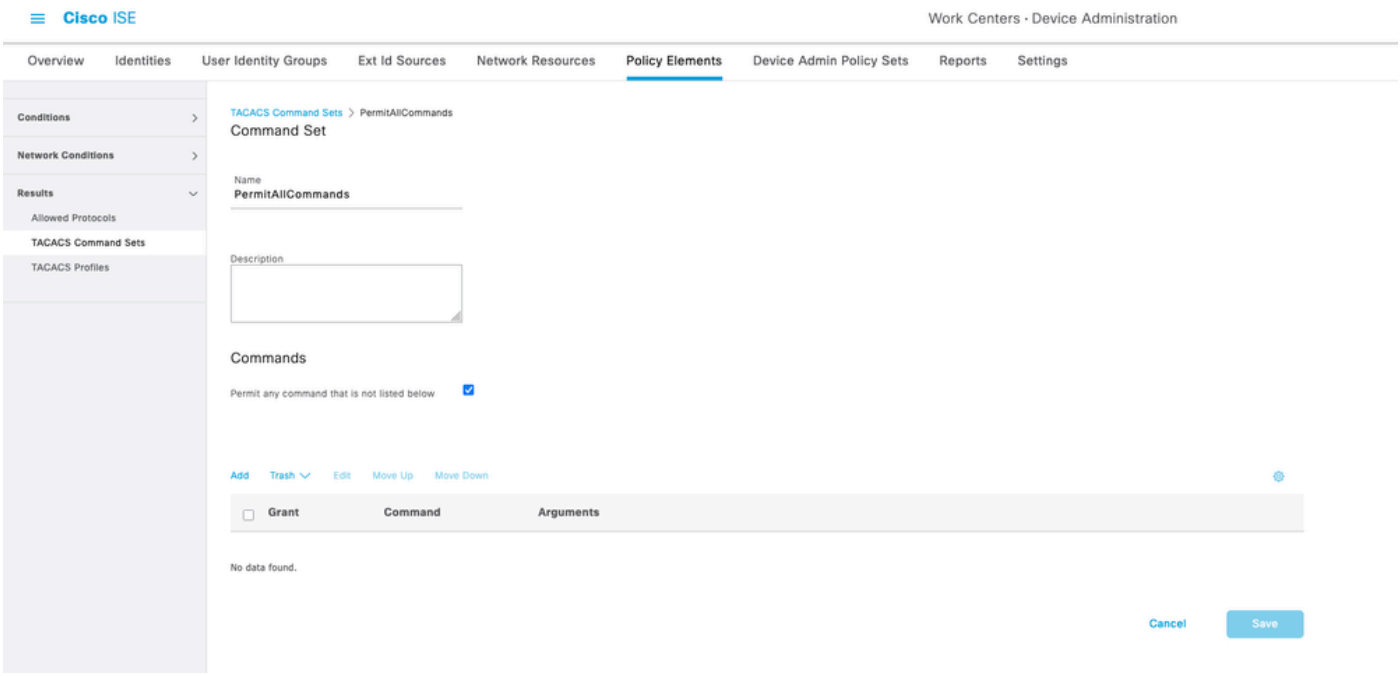
Por exemplo, você pode selecionar e configurar manualmente o atributo AAA como cisco-av-pair=Role=SUPER-ADMIN-ROLE ou Cisco-AVPair=Role=SUPER-ADMIN-ROLE.

2. Crie um Conjunto de Comandos TACACS+.

- Navegue até:

Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Conjuntos de comandos TACACS

- Adicione um nome.
- Marque a opção Permitir qualquer comando que não esteja listado abaixo.
- Salve o conjunto de comandos.



Conjuntos de comandos TACACS

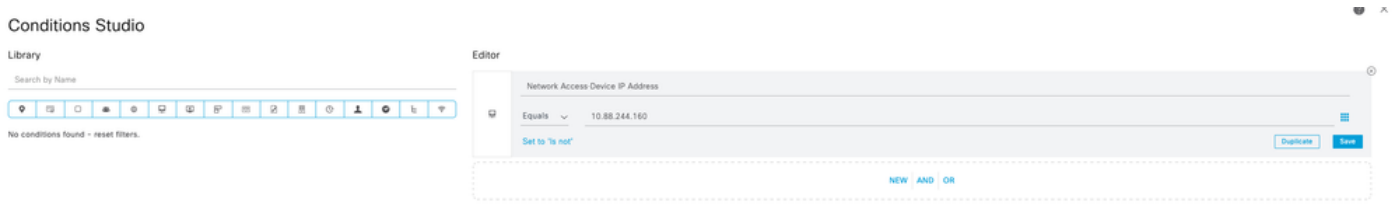
Configurar políticas TACACS+

1. Crie um Novo Conjunto de Políticas TACACS+.

- Navegue até:

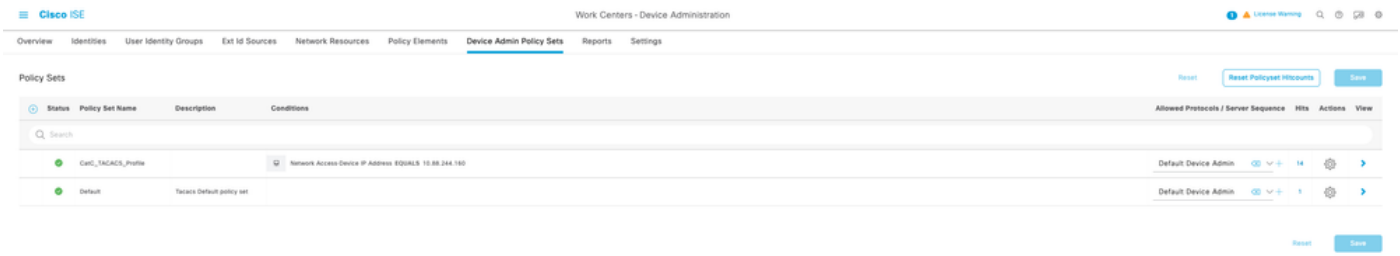
Centros de Trabalho > Administração de Dispositivos > Conjunto de Políticas de Administração de Dispositivos

- Adicione um nome para o conjunto de políticas.
- Configure a condição.
    - Neste exemplo, a condição corresponde ao endereço IP do Catalyst Center.



Endereço IP do Catalyst Center

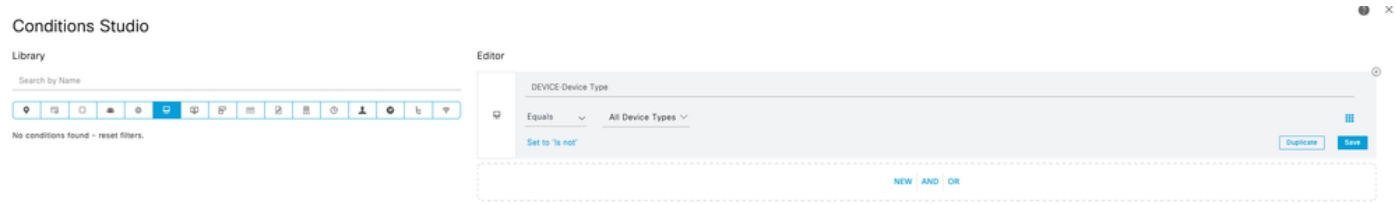
1.3 Em Allowed Protocols / Server Sequence, selecione Default Device Admin.



Selecionar administrador de dispositivo padrão

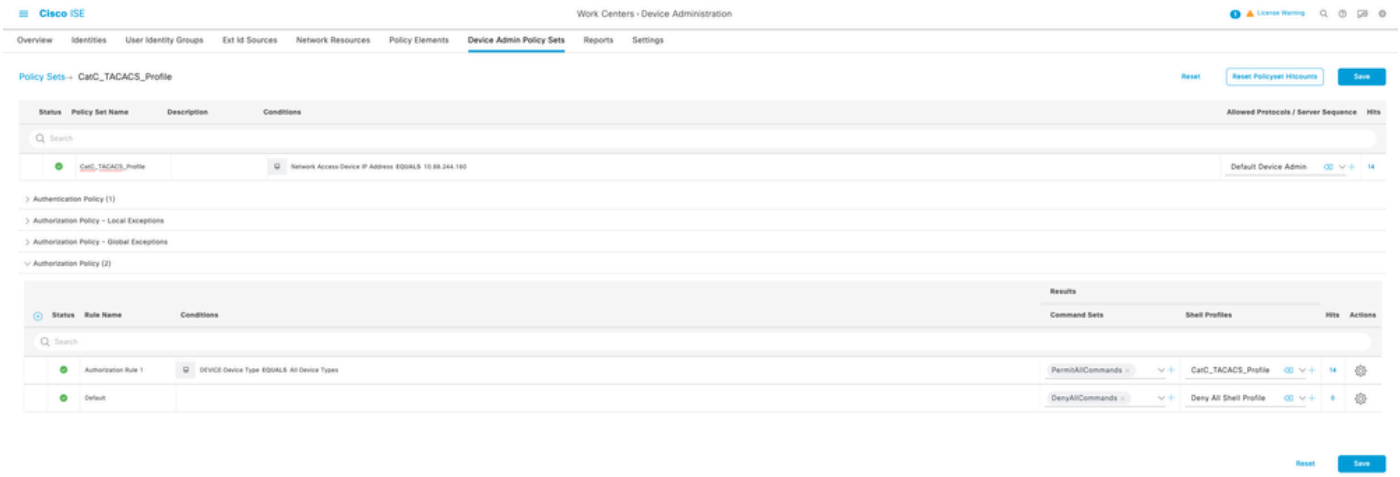
2. Configure o Conjunto de Políticas.

- Clique na seta (>) à direita para expandir e configurar o conjunto de políticas.
- Adicione uma nova Regra em Política de Autorização.
- Configure a nova regra da seguinte maneira:
  - Nome: Insira um nome de regra descritivo.
  - Condição: Para este exemplo, a condição correspondeu a Todos os tipos de dispositivo.



Todos os tipos de dispositivo

- Conjunto de comandos: Selecione o conjunto de comandos TACACS+ criado anteriormente.
- Perfil do Shell: Selecione o Perfil TACACS+ criado anteriormente.



Conjunto de comandos TACACS+

Cisco Catalyst Center

Configurar o servidor ISE / AAA

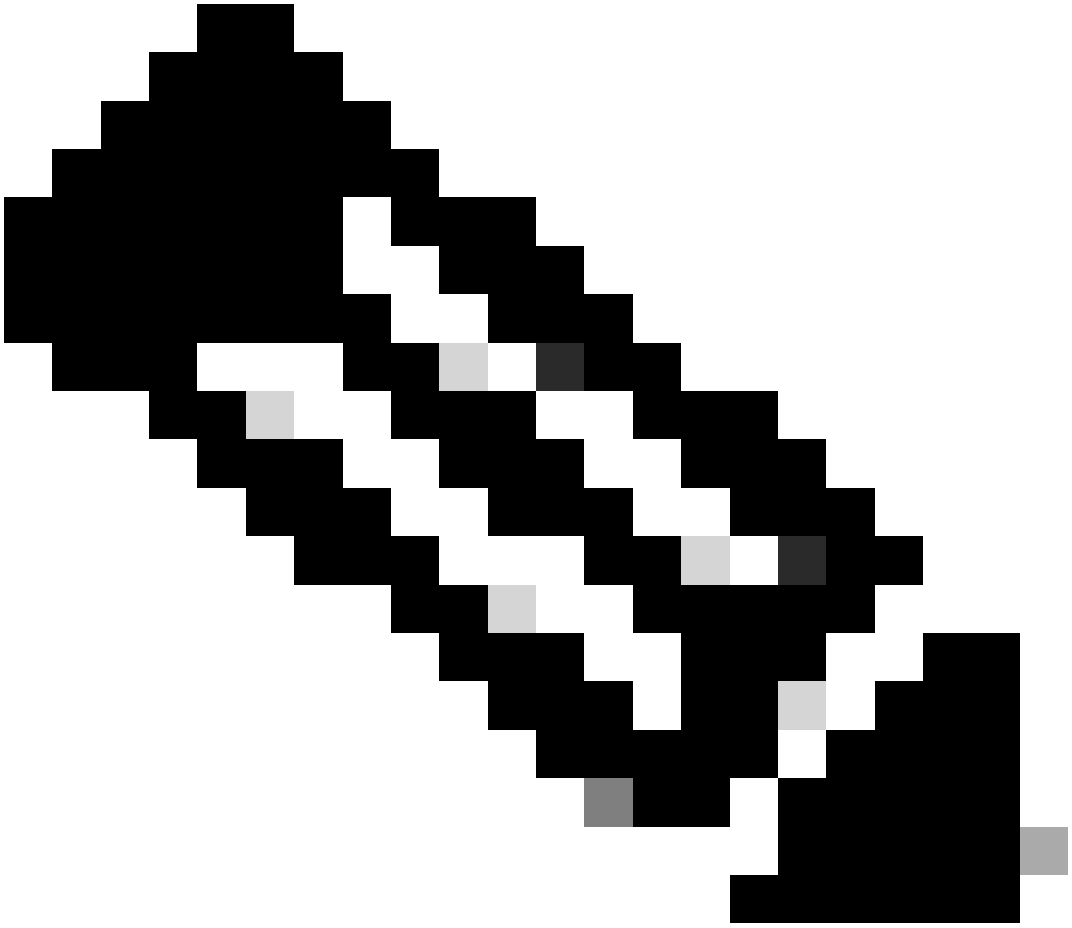
1. Faça login na interface da Web do Catalyst Center.

- Navegue até:

Menu principal > Sistema > Configurações > Serviços externos > Servidores de autenticação e política

2. Adicione um novo servidor. Você pode selecionar ISE ou AAA.

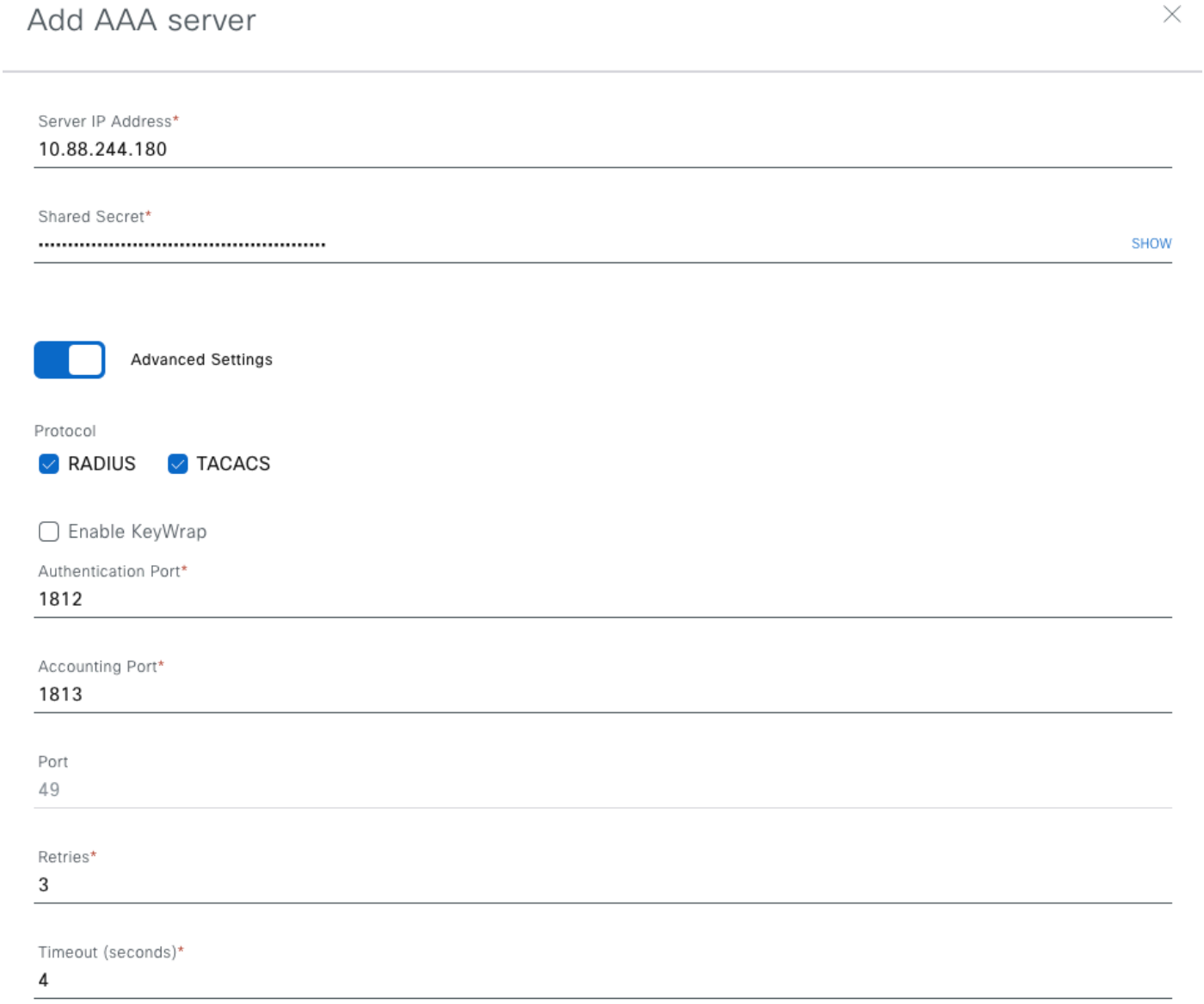
- Para esta demonstração, a opção AAA server é usada.



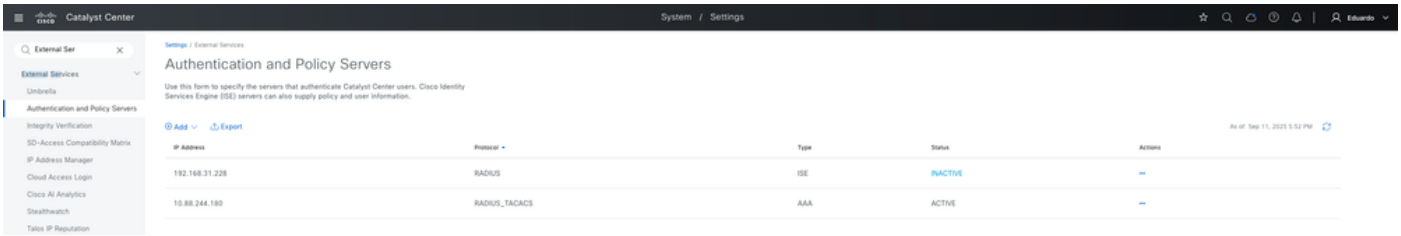
Note: Um cluster do Catalyst Center pode ter apenas um cluster do ISE configurado.

3. Configure estas opções e salve:

- Insira o endereço IP do servidor AAA.
- Adicione o segredo compartilhado (o mesmo segredo configurado no recurso de rede do Cisco ISE).
- Alterne Advanced Settings para On.
- Marque a opção TACACS.



Servidores de autenticação e política



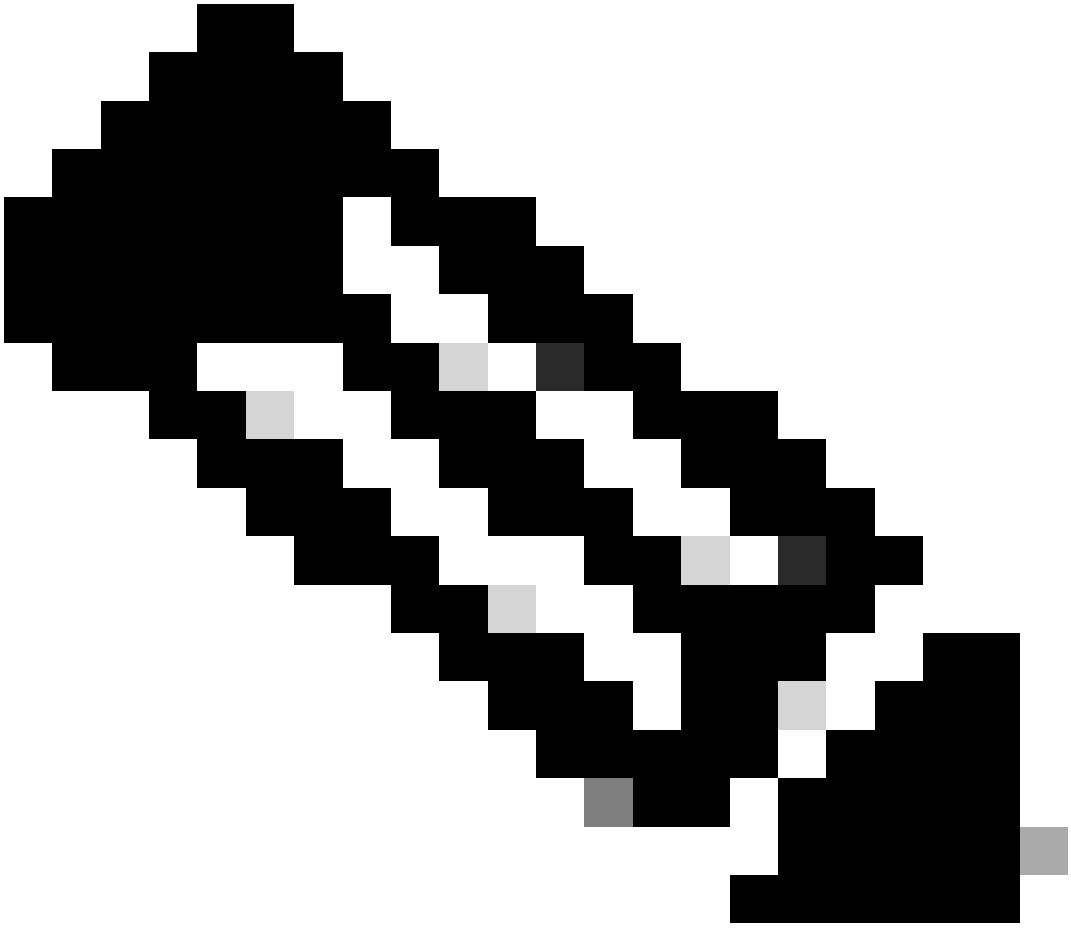
Configurações avançadas

Ative e configure a autenticação externa.

1. Navegue até a página Autenticação Externa:

    Menu principal > Sistema > Usuário e função > Autenticação externa

2. Adicione o atributo AAA cisco-av-pair e clique em Update para salvar as alterações.



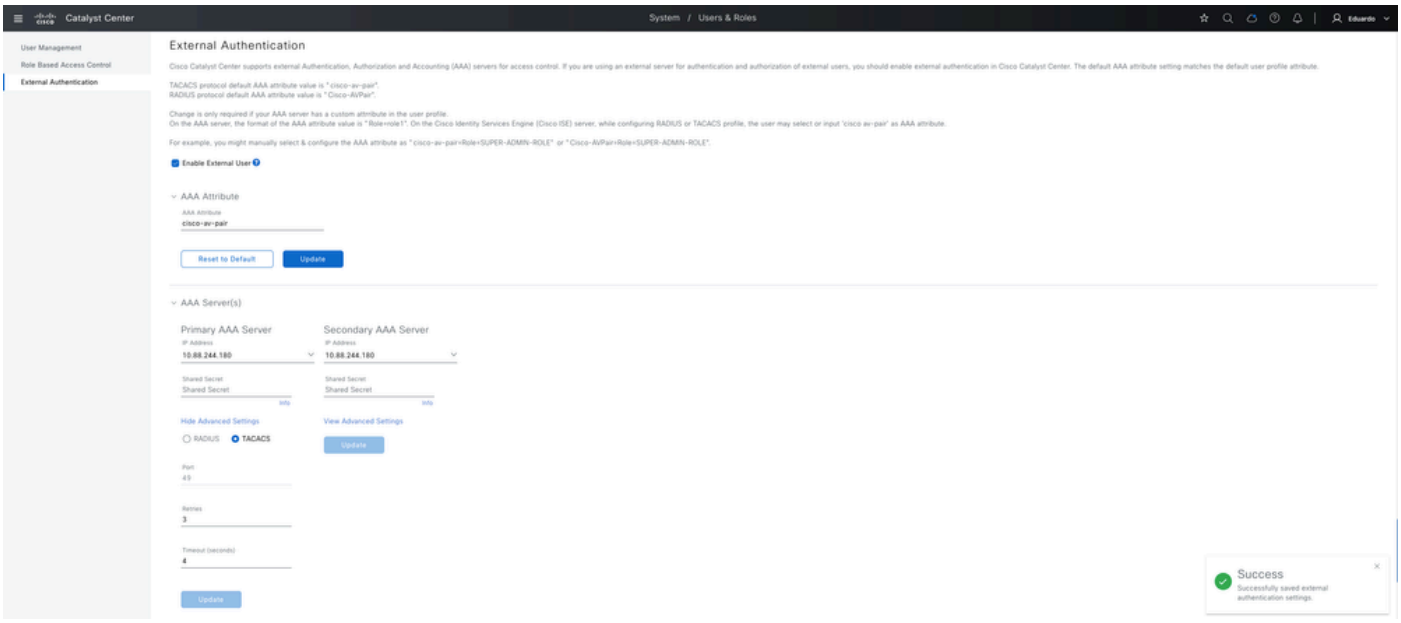
Note: Esta etapa não é obrigatória, pois o atributo padrão para TACACS+ já é cisco-av-pair, mas é considerado uma prática recomendada para configurá-lo explicitamente.

3. Em Primary AAA Server, selecione o servidor AAA configurado anteriormente.

- Clique em Exibir configurações avançadas para exibir opções adicionais.
- Selecione a opção TACACS+.
- Insira o segredo compartilhado configurado no recurso de rede do Cisco ISE.
- Clique em Atualizar para salvar as alterações.

4. Ative a caixa de seleção Usuário externo.

- Esta ação salva automaticamente a configuração.



Autenticação externa

Verificar

1. Abra uma nova sessão do navegador ou use o Modo incógnito e faça login na página da Web do Catalyst Center com a conta de usuário configurada no Cisco ISE.

2. No Catalyst Center, confirme se o login foi bem-sucedido.

Login Configurar o TACACS de Autenticação Externa do Catalyst Center com ISE

3. No Cisco ISE, valide os registros:

   Operações > TACACS > Live Logs

- Status de autenticação: Aprovado
- Status da autorização: Aprovado

Logs ao vivo

4. Em Detalhes da autorização, compare com a próxima saída :

    - Texto da mensagem: Administração do dispositivo: Autorização de sessão bem-sucedida
    - Todos os atributos de resposta: cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

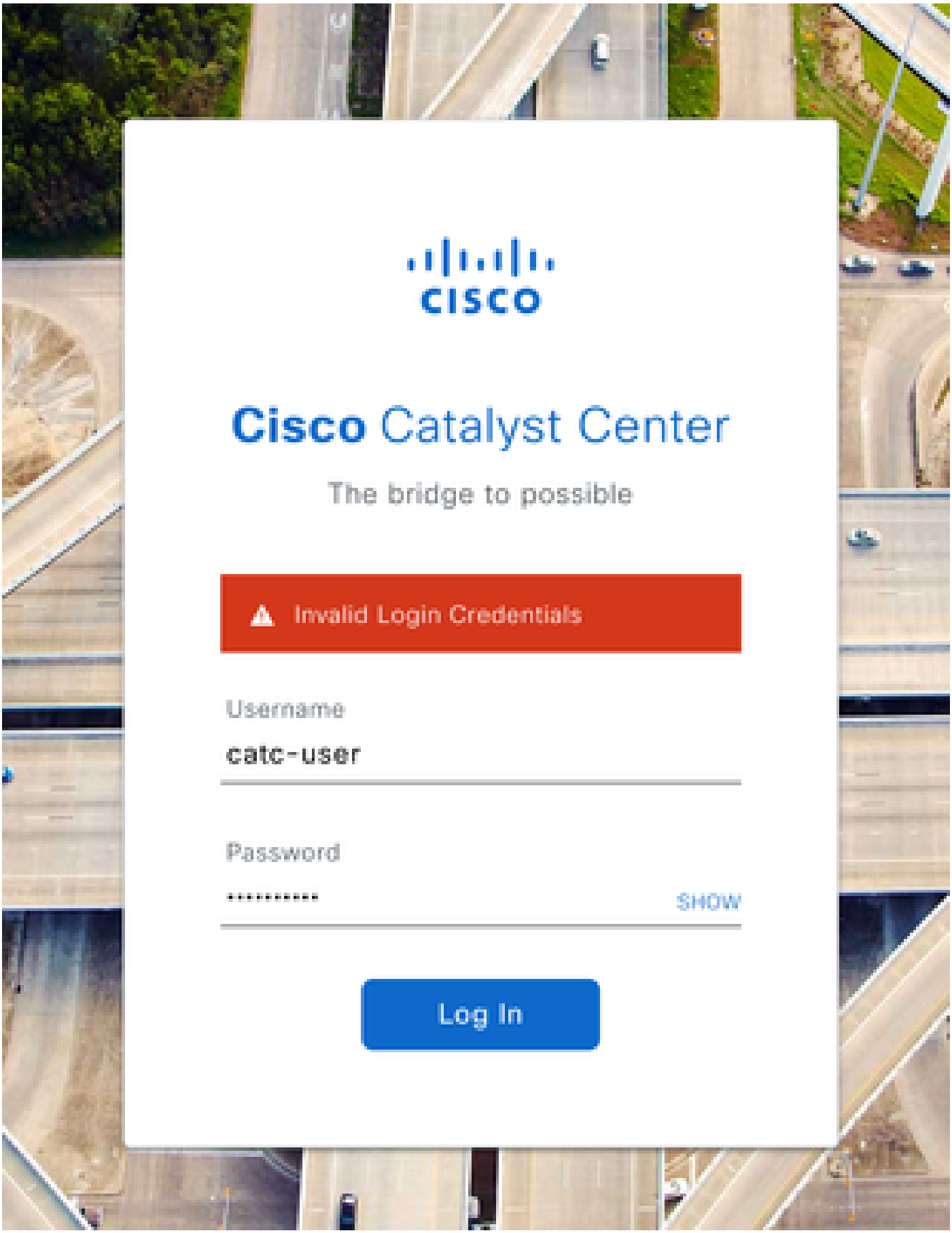
cisco-av-pair=Função=SUPER-ADMIN-ROLE

Troubleshooting

Aqui estão alguns problemas comuns que você pode encontrar durante a integração e como identificá-los:

1. Configuração Incorreta do Atributo

Sintoma no Catalyst Center: credenciais de login inválidas



Erro de configuração de atributo

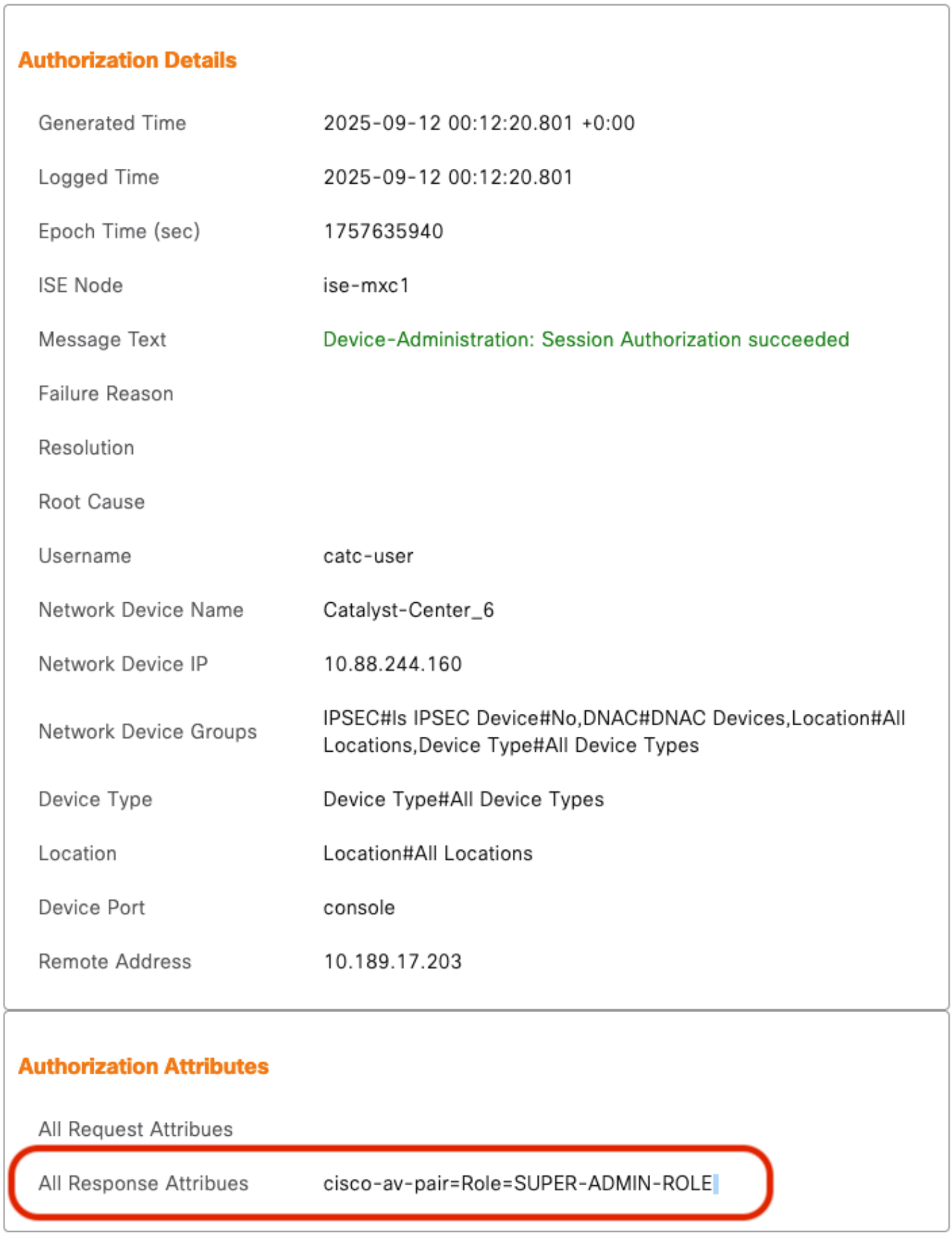
- Sintoma no Cisco ISE (registros TACACS):

- Autenticação: Aprovado
- Autorização: Aprovado

Erro de configuração de atributo

- Possíveis causas:
  - Existe um espaço no valor do atributo.

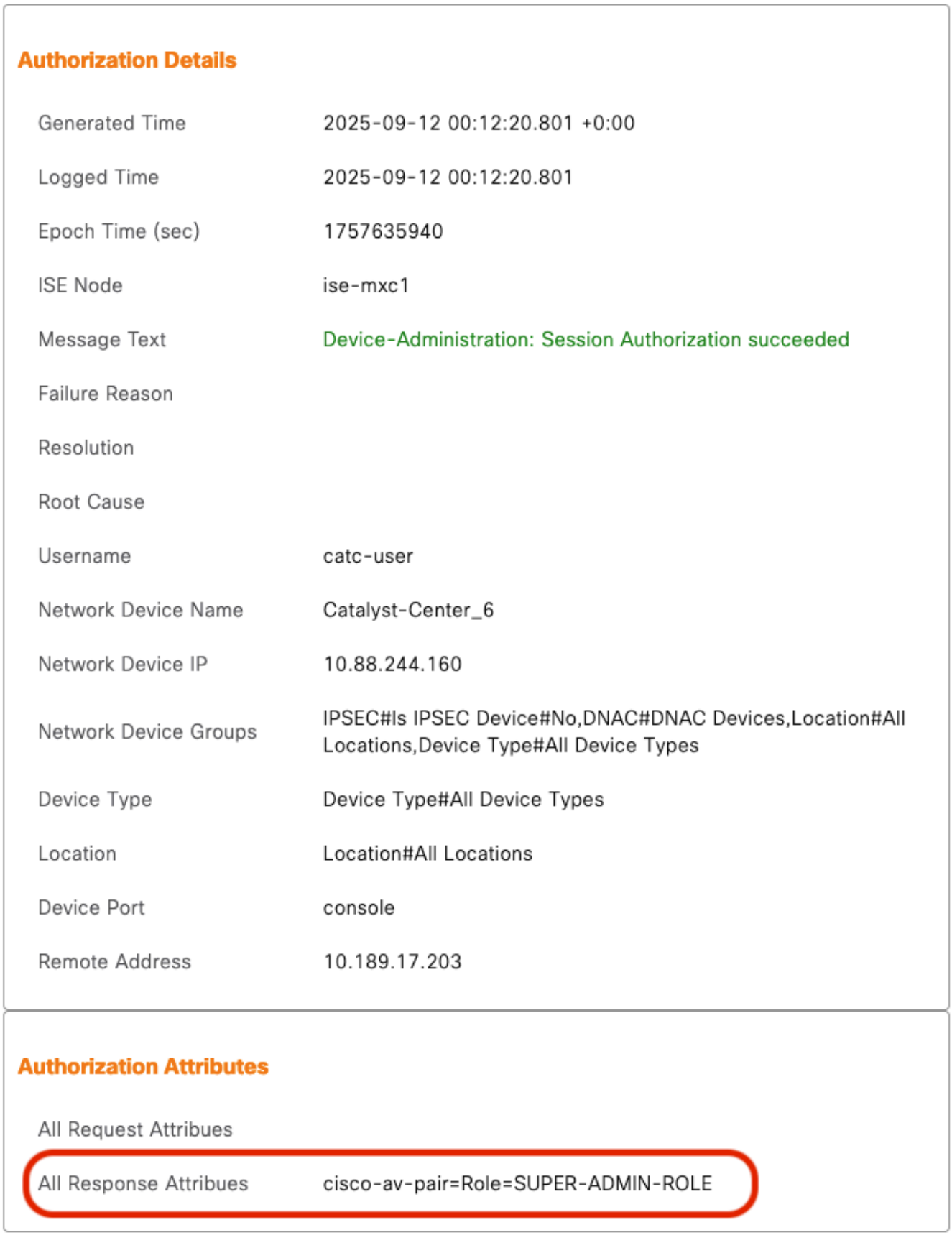
Exemplo:



Erro de configuração de atributo

- O atributo está configurado incorretamente, a palavra-chave Role= está ausente.

  Exemplo:



Erro de configuração de atributo

2. Incompatibilidade de Segredo Compartilhado

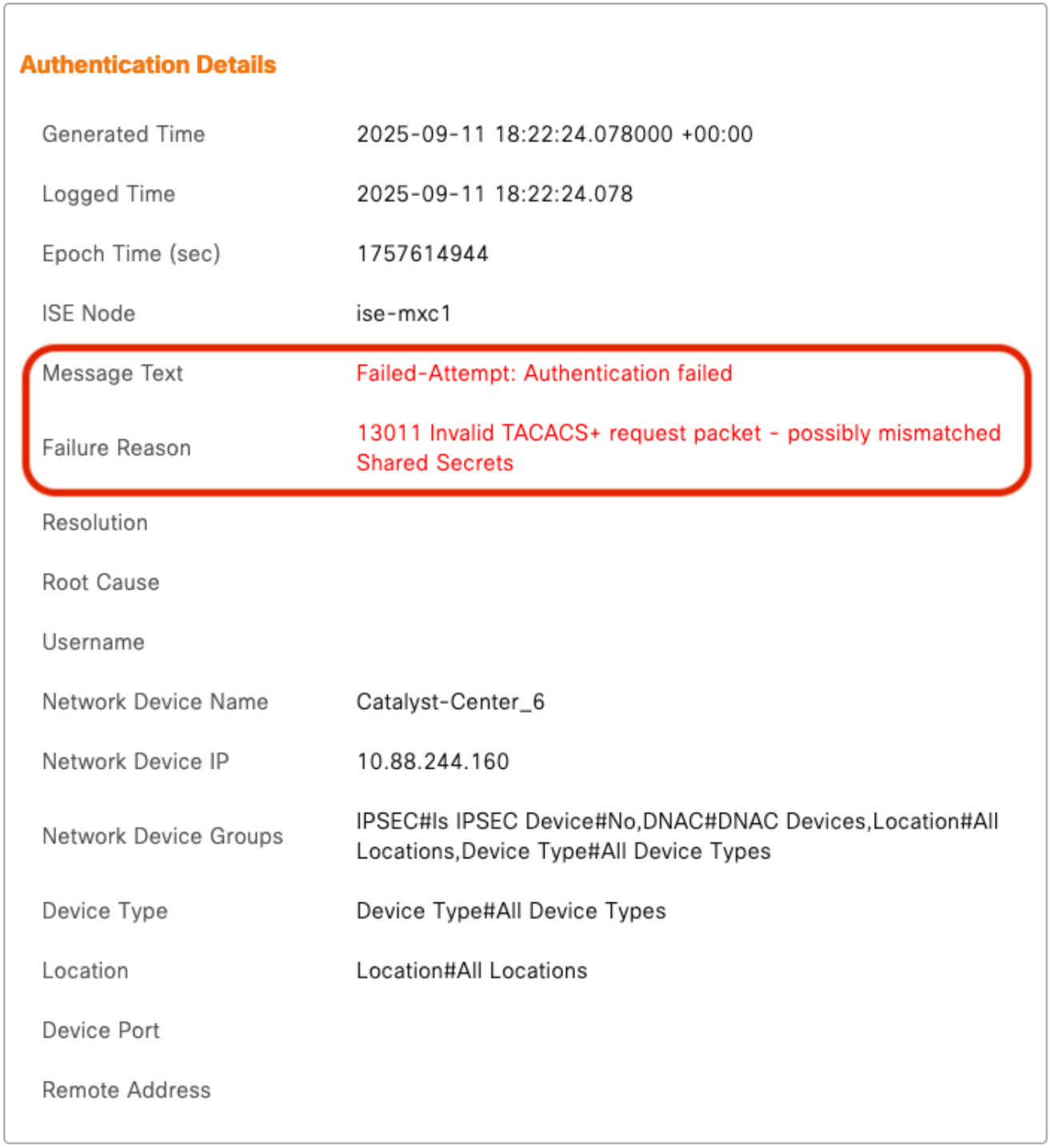
- Sintoma: Os pacotes de autenticação falham entre o Catalyst Center e o Cisco ISE.

- Possível causa: O segredo compartilhado configurado no recurso de rede do ISE não corresponde ao configurado na página Catalyst Center > Autenticação externa.

Como verificar:

- Verifique a configuração de recurso de rede no ISE.
- Compare o Shared Secret com a configuração em Catalyst Center > External Authentication.

Exemplo:



Authentication Details

Generated Time	2025-09-11 18:22:24.078000 +00:00
Logged Time	2025-09-11 18:22:24.078
Epoch Time (sec)	1757614944
ISE Node	ise-mxc1
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Resolution	
Root Cause	
Username	
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	
Remote Address	

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.