ACL para download em switches Catalyst 1300

Objetivo

O objetivo deste artigo é demonstrar como a lista de controle de acesso (DACL) disponível para download funciona nos switches Cisco Catalyst 1300 com Cisco Identity Service Engine (ISE).

Dispositivos aplicáveis | Versão do software

- Catalyst 1300 Series |4.1.6.54

Introdução

As ACLs dinâmicas são ACLs atribuídas a uma porta de switch com base em uma política ou em critérios, como a participação em grupos de contas de usuário, hora do dia e muito mais. Podem ser ACLs locais especificadas por ID de filtro ou ACLs para download (DACL).

As ACLs para download são ACLs dinâmicas criadas e baixadas do servidor Cisco ISE. Eles aplicam regras de controle de acesso dinamicamente com base na identidade do usuário e no tipo de dispositivo. A DACL tem a vantagem de permitir que você tenha um repositório central para ACLs, de modo que você não precisa criá-las manualmente em cada switch. Quando um usuário se conecta a um switch, ele só precisa se autenticar, e o switch fará o download das ACLs aplicáveis do servidor Cisco ISE.

Casos de uso de ACL para download

1. Usuários diferentes receberão ACLs diferentes quando se conectarem a um switch (Usuários locais do ISE).
2. Os usuários com conectividade de rede limitada podem entrar em um portal central da Web para obter acesso total à rede (Autenticação da Web Central).
3. Avançado - uso de MAC Authentication Bypass (MAB) para permitir a comunicação com o Windows Ative Diretory (AD) e alguns serviços relacionados ao conectar o servidor ISE ao AD e monitorar a autenticação do usuário. Antes do login do Windows AD, a rede só permitirá acesso a recursos muito limitados, mas a autenticação do AD baixará ACLs diferentes com base nos grupos do Windows e permitirá acesso total à rede.
4. Avançado - Os usuários recebem ACLs diferentes com base no dia da semana, hora do dia ou algum outro fator devido às políticas no servidor ISE.

Neste artigo, o primeiro caso de uso será discutido em detalhes.

Table Of Contents

- Configurar o cliente RADIUS
- Configurar a autenticação 802.1x
- Configuração do servidor Cisco ISE para ACL para download
- Configurações do cliente
- Verificação de DACL

Pré-requisitos

- Verifique se o switch Catalyst 1300 está atualizado para o firmware mais recente (o firmware do switch deve ser 4.1.6 ou superior).
- Atribua um IP estático ao switch para fins de gerenciamento.

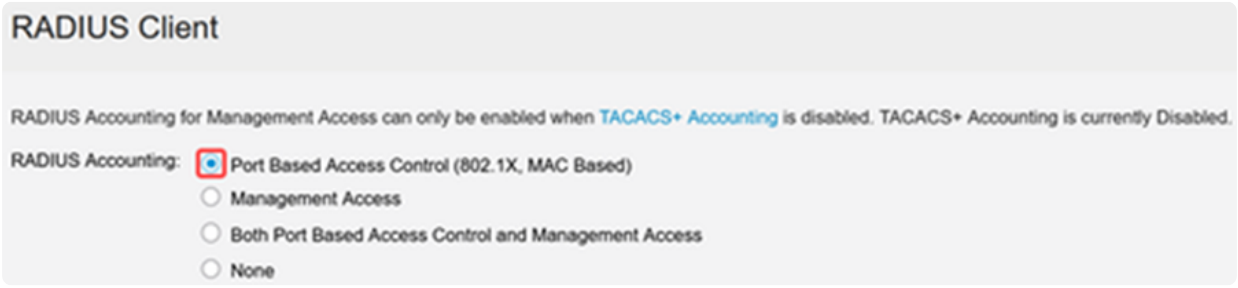
Configurar o cliente RADIUS

Passo 1

Faça login no switch Catalyst 1300 e navegue para o menu Security > RADIUS Client.

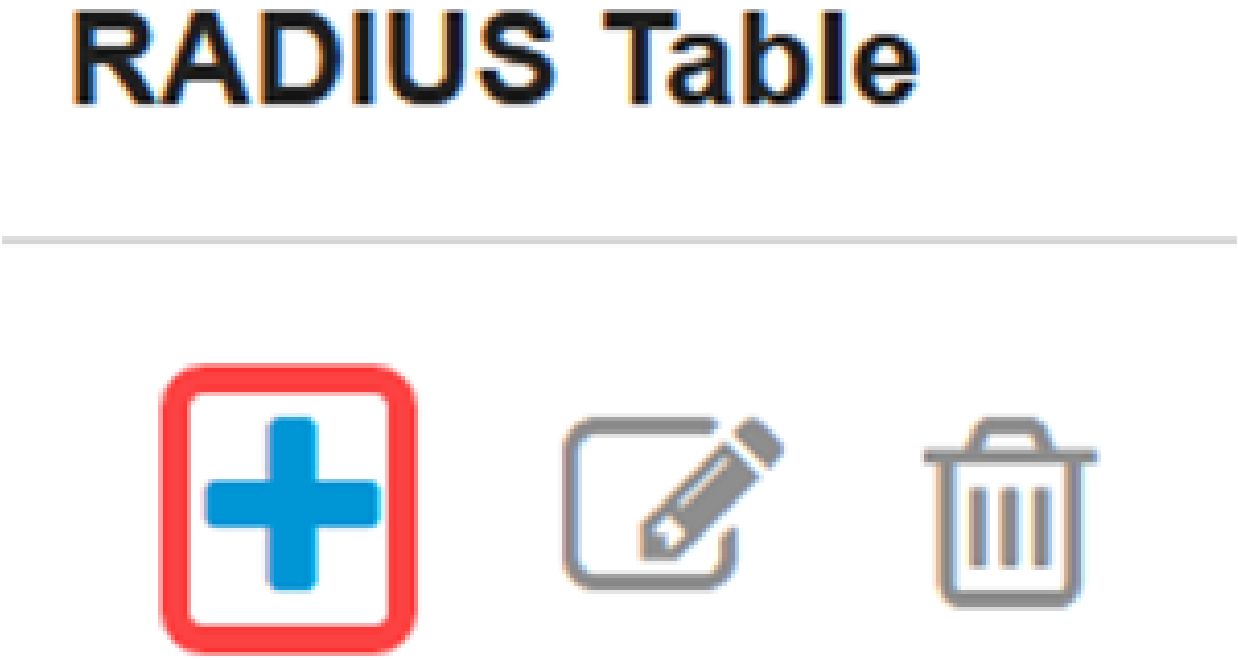
Passo 2

Para Contabilidade RADIUS, selecione a opção Controle de acesso baseado em porta.



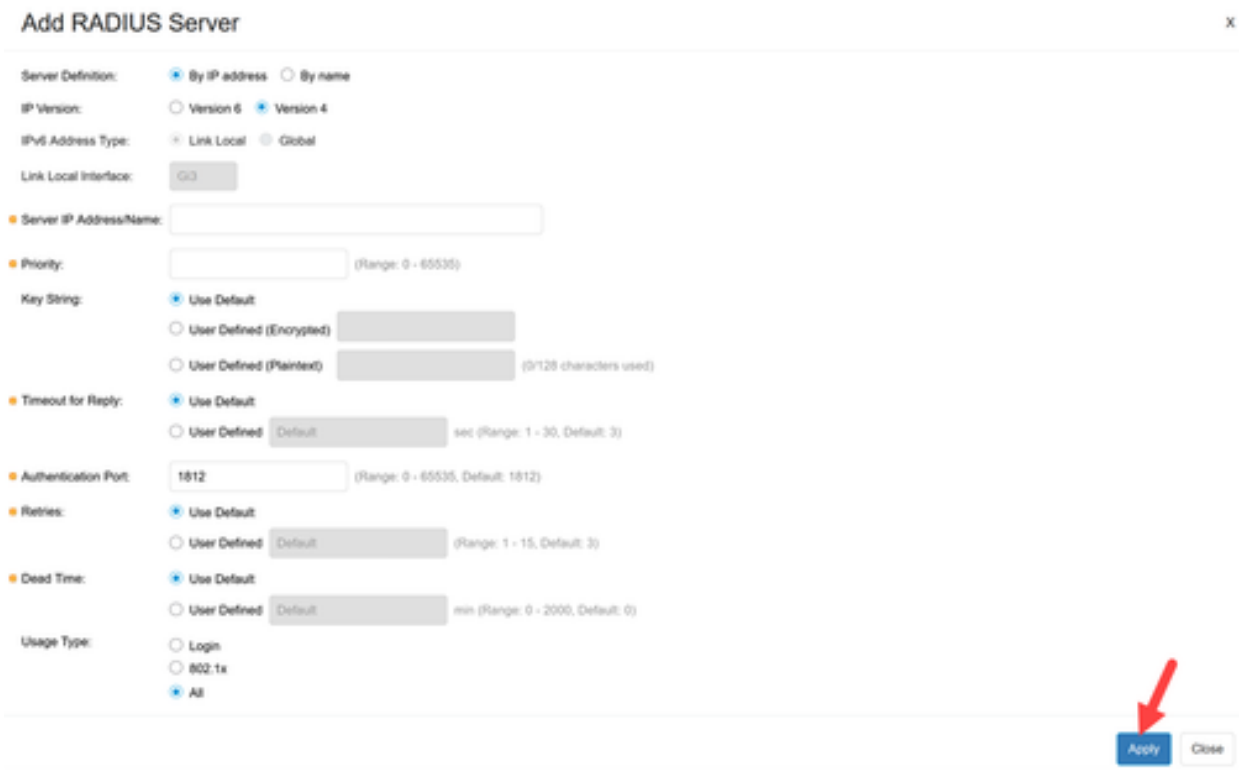
Etapa 3

Em Tabela RADIUS, clique no ícone de mais para adicionar o servidor Cisco ISE.



Passo 4

Insira os detalhes do servidor Cisco ISE e clique em Apply.



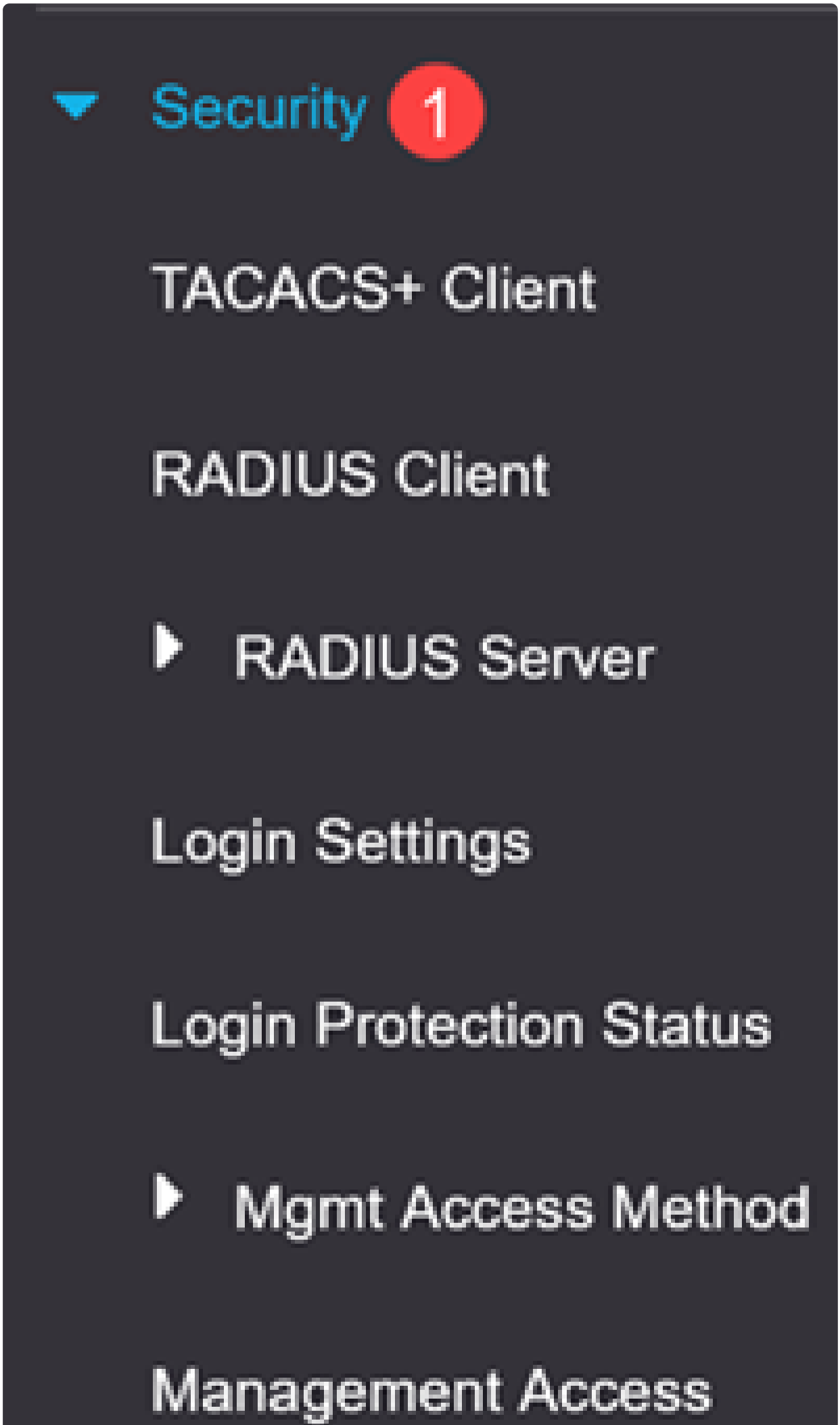
Note:

O Tipo de uso deve ser selecionado como 802.1x.

Configurar a autenticação 802.1x

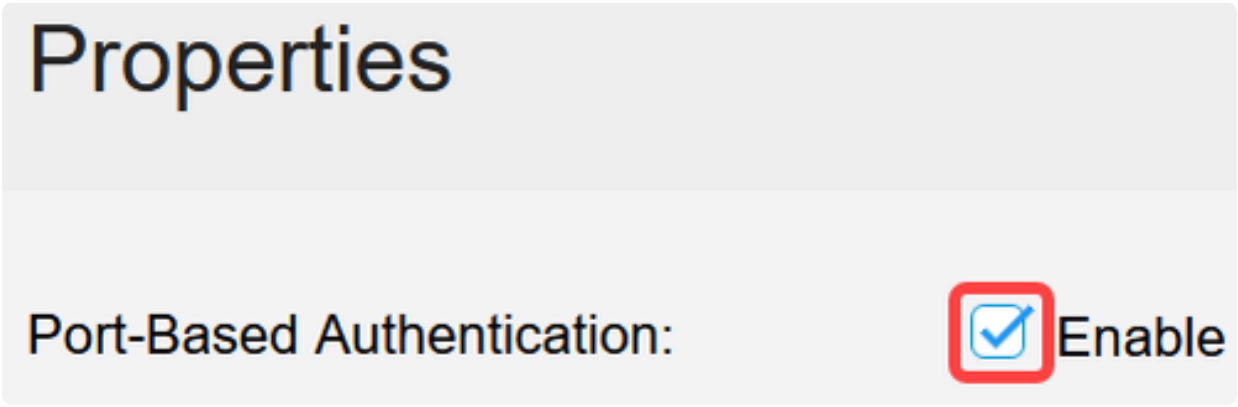
Passo 1

Navegue para o menu Security > 802.1X Authentication > Properties.


Security 1
TACACS+ Client
RADIUS Client
RADIUS Server
Login Settings
Login Protection Status
Mgmt Access Method
Management Access

Passo 2

Clique na caixa de seleção para habilitar a autenticação baseada em porta.

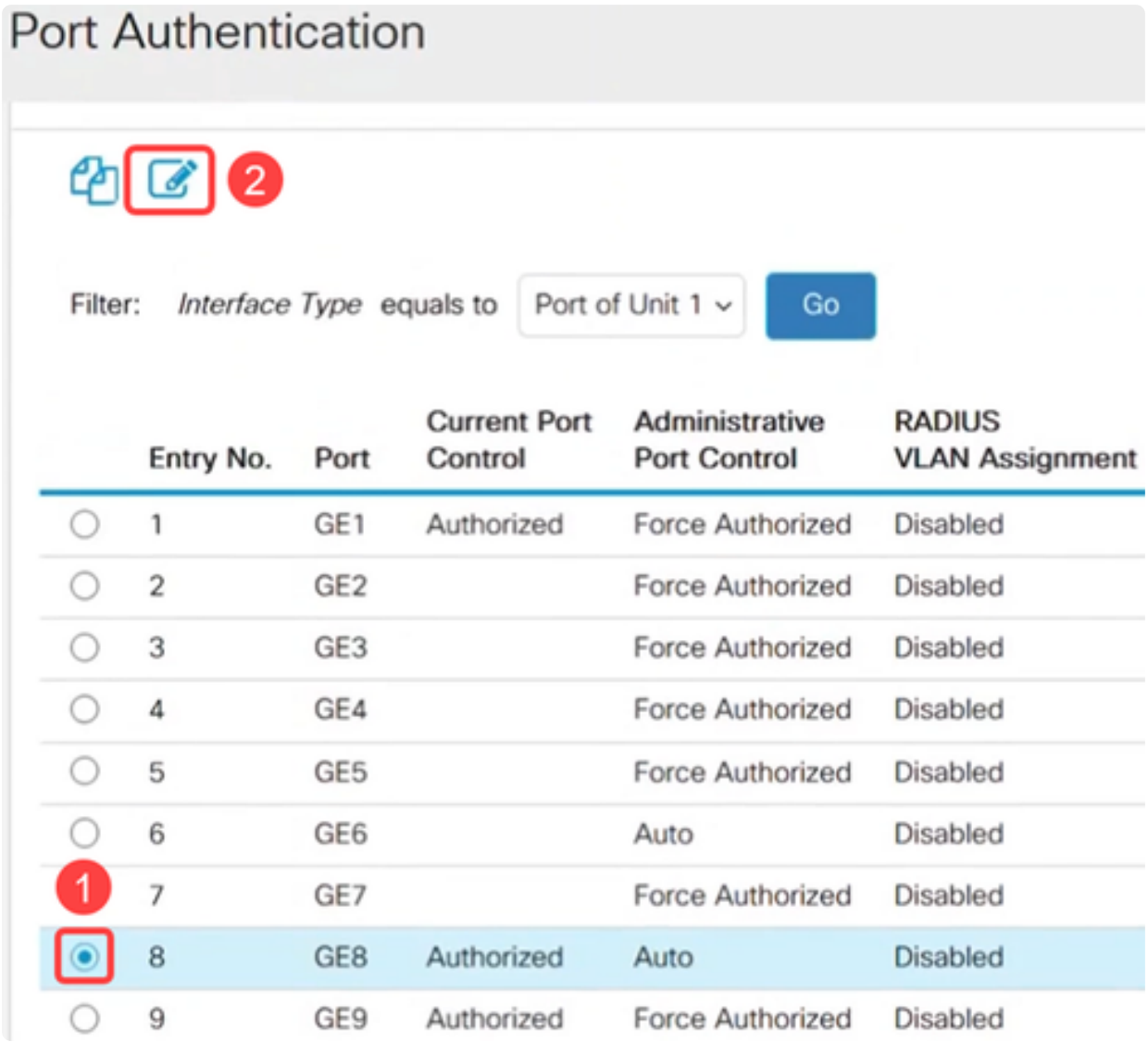


Etapa 3

Em Authentication Method, selecione RADIUS e clique em Apply.

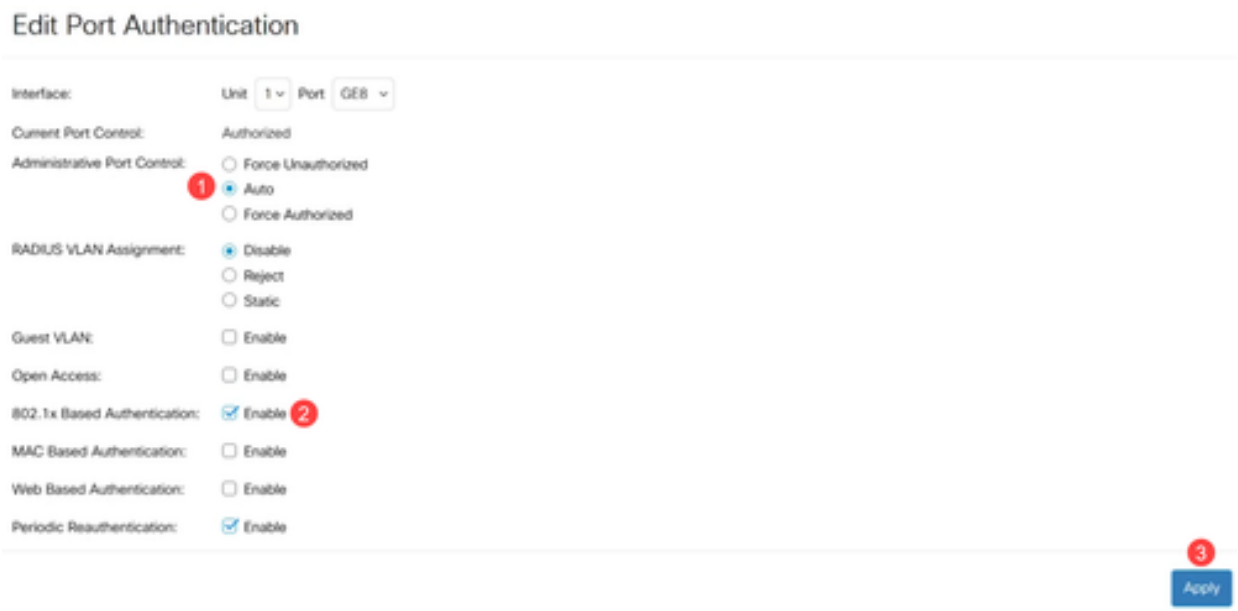
Passo 4

Vá para o menu Security > 802.1X Authentication > Port Authentication. Selecione a porta à qual o laptop está conectado e clique no ícone de edição. Neste exemplo, GE8 está selecionado.



Etapa 5

Selecione Administrative Port Control como Auto e habilite 802.1x Based Authentication. Clique em Apply.



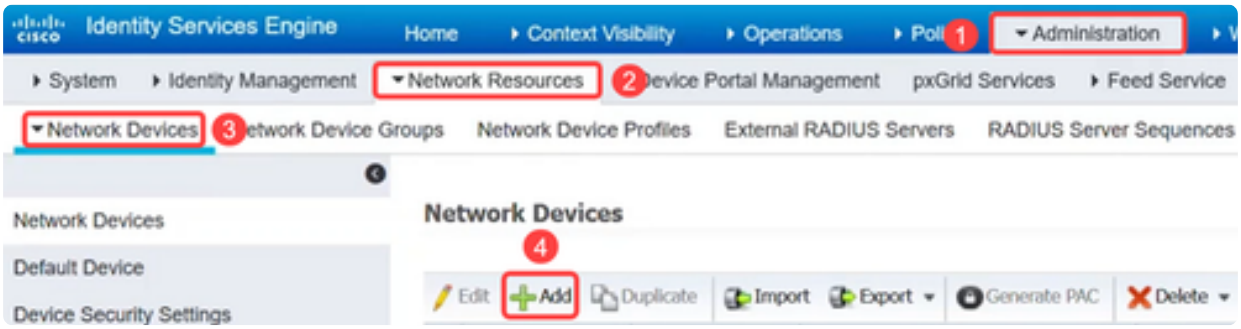
Configuração do servidor Cisco ISE para ACL para download

> **Note:**
> A configuração do ISE está além do escopo do suporte Cisco Business. Consulte o guia de administração do ISE para obter mais informações.

As configurações mostradas neste artigo são um exemplo de ACL para download para trabalhar com o switch Cisco Catalyst da série 1300.

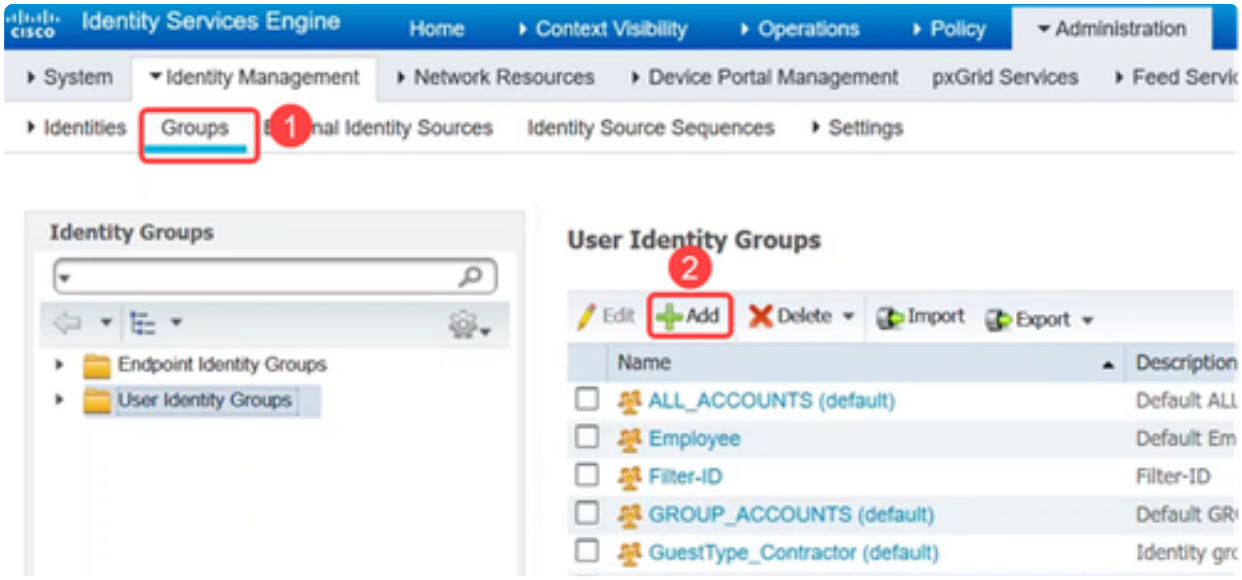
Passo 1

Faça login no servidor Cisco ISE, navegue até Administração > Recursos de rede > Dispositivos de rede e adicione o dispositivo do switch Catalyst.



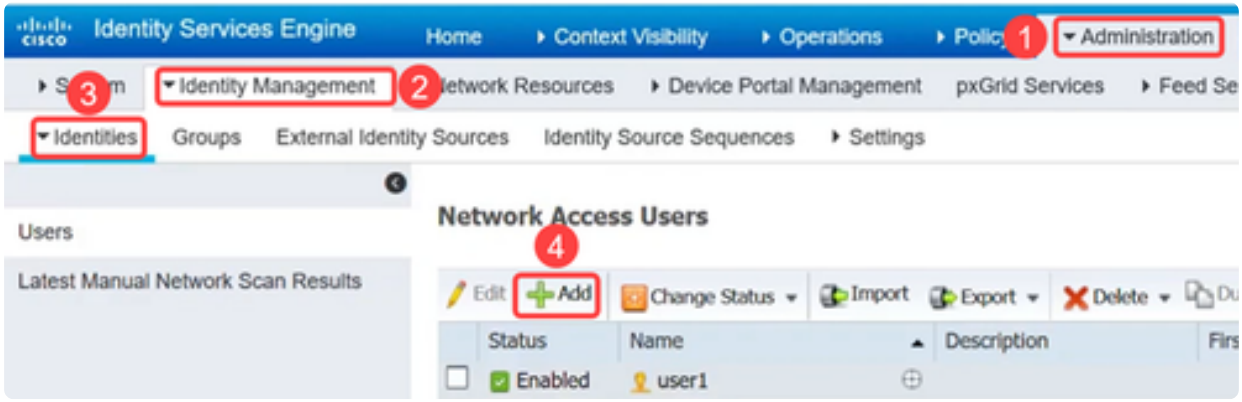
Passo 2

Para criar Grupos de identidade de usuário, navegue até a guia Grupos e adicione os Grupos de identidade de usuário.



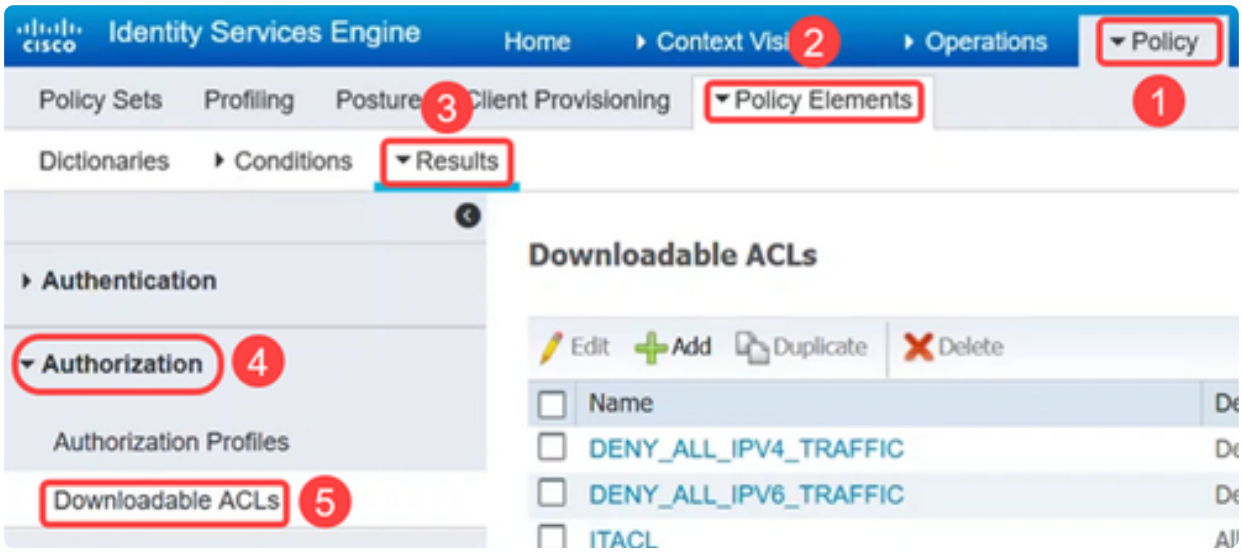
Etapa 3

Vá para o menu Administração > Gerenciamento de identidades > Identidades para definir os usuários e mapear os usuários para os grupos.



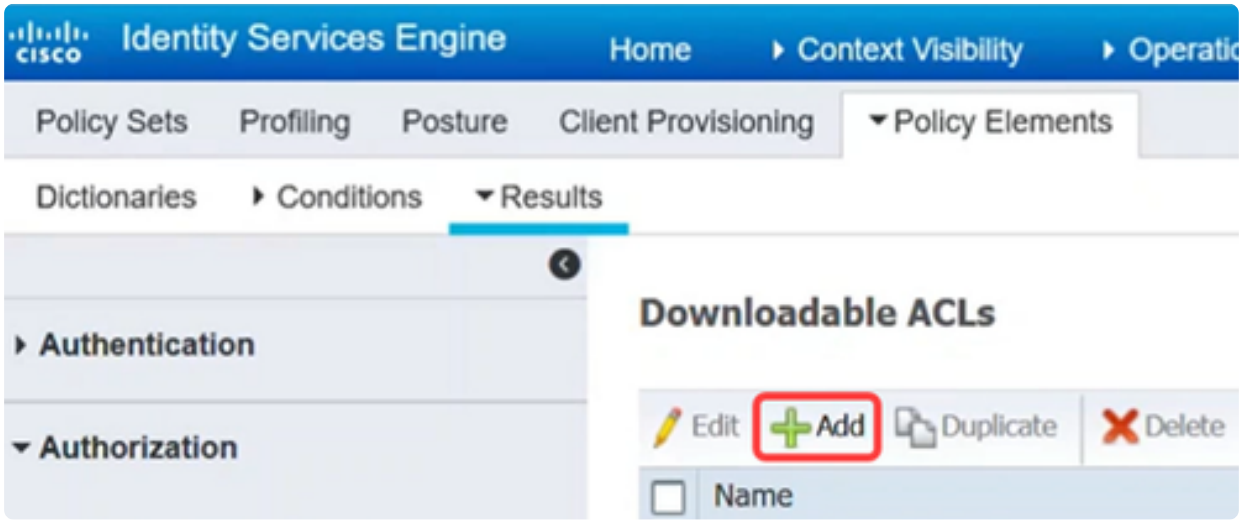
Passo 4

Navegue até o menu Política > Elementos de política > Resultados. Em Authorization, clique em Downloadable ACLs.



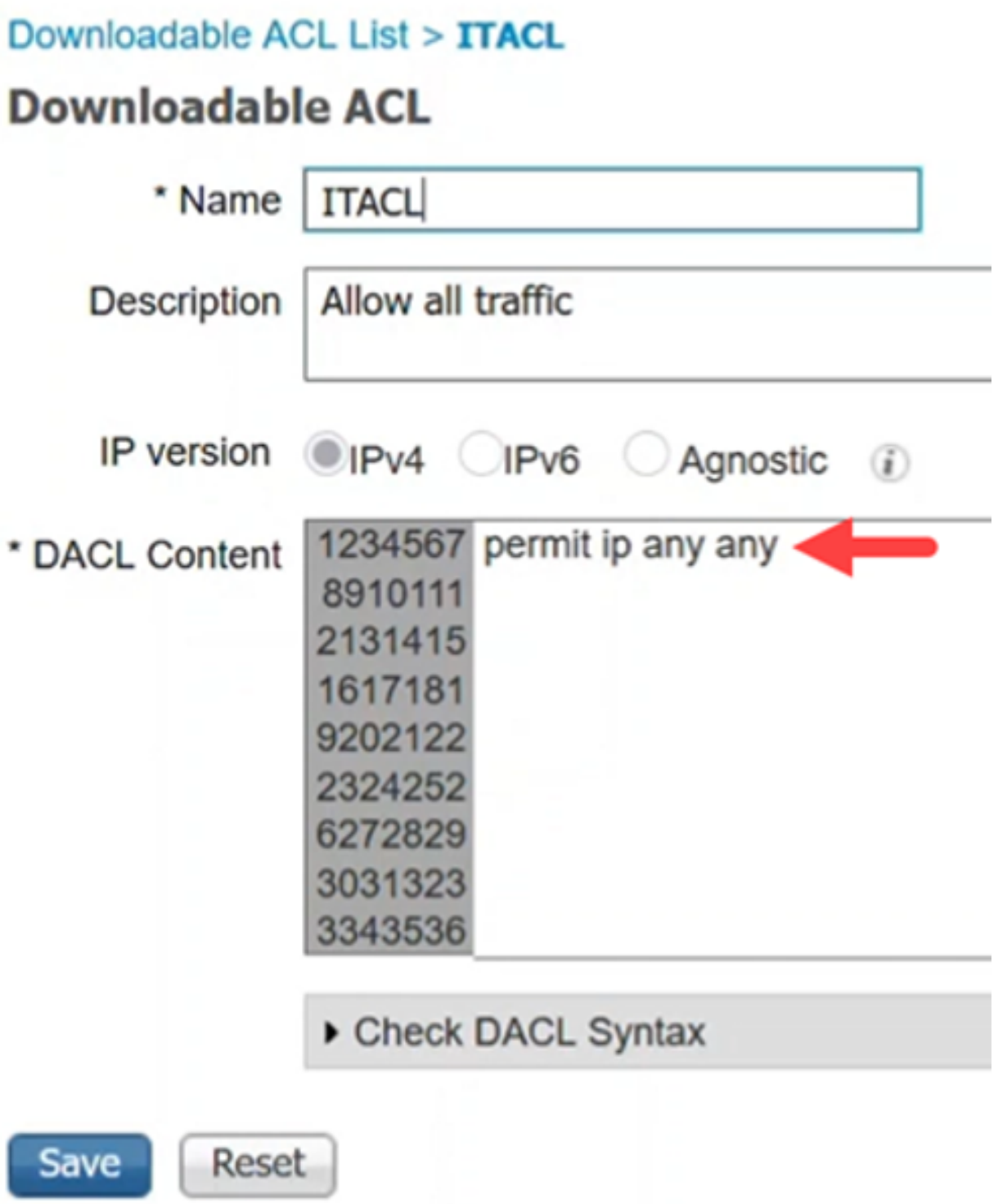
Etapa 5

Clique no ícone Add para criar a ACL para download.



Etapa 6

Configure o Nome, a Descrição, selecione a versão IP e insira as entradas de controle de acesso (ACEs) que formarão a ACL para download no campo DACL Content. Click Save.



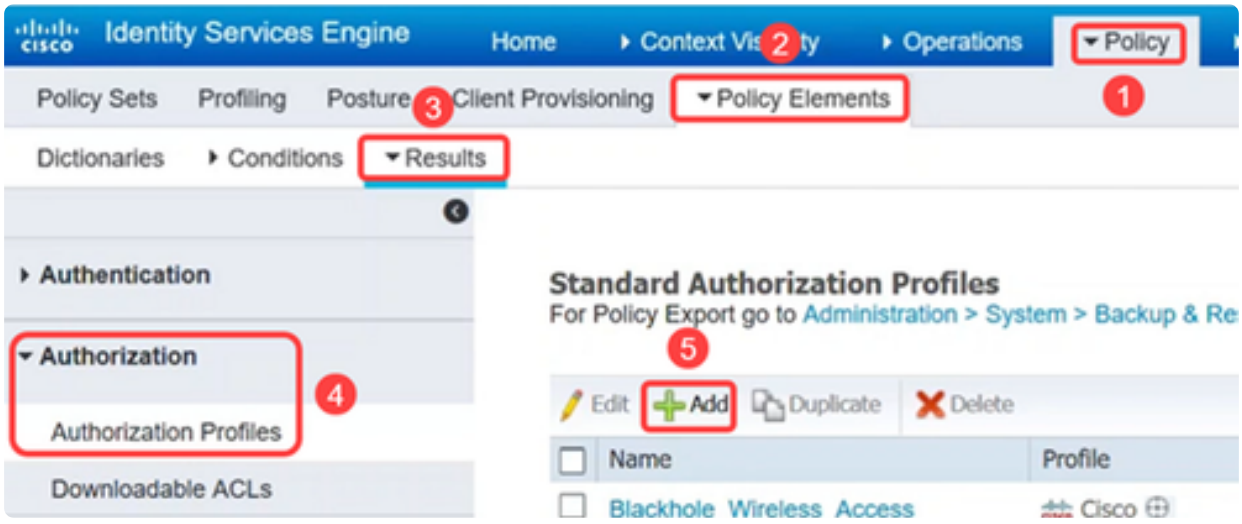
Note:

Somente ACLs IP são suportadas, e a origem deve ser ANY. Para ACL no ISE, somente IPv4 é suportado agora. Se uma ACL for inserida com outra origem, embora a sintaxe possa ser boa no que diz respeito ao ISE, ela falhará quando aplicada ao switch.

Etapa 7

Crie perfis de autorização que serão usados para associar logicamente sua DACL e outras políticas dentro dos conjuntos de políticas do ISE.

Para fazer isso, navegue para Política > Elementos de política > Resultados > Autorização > Perfis de autorização e clique em Adicionar.

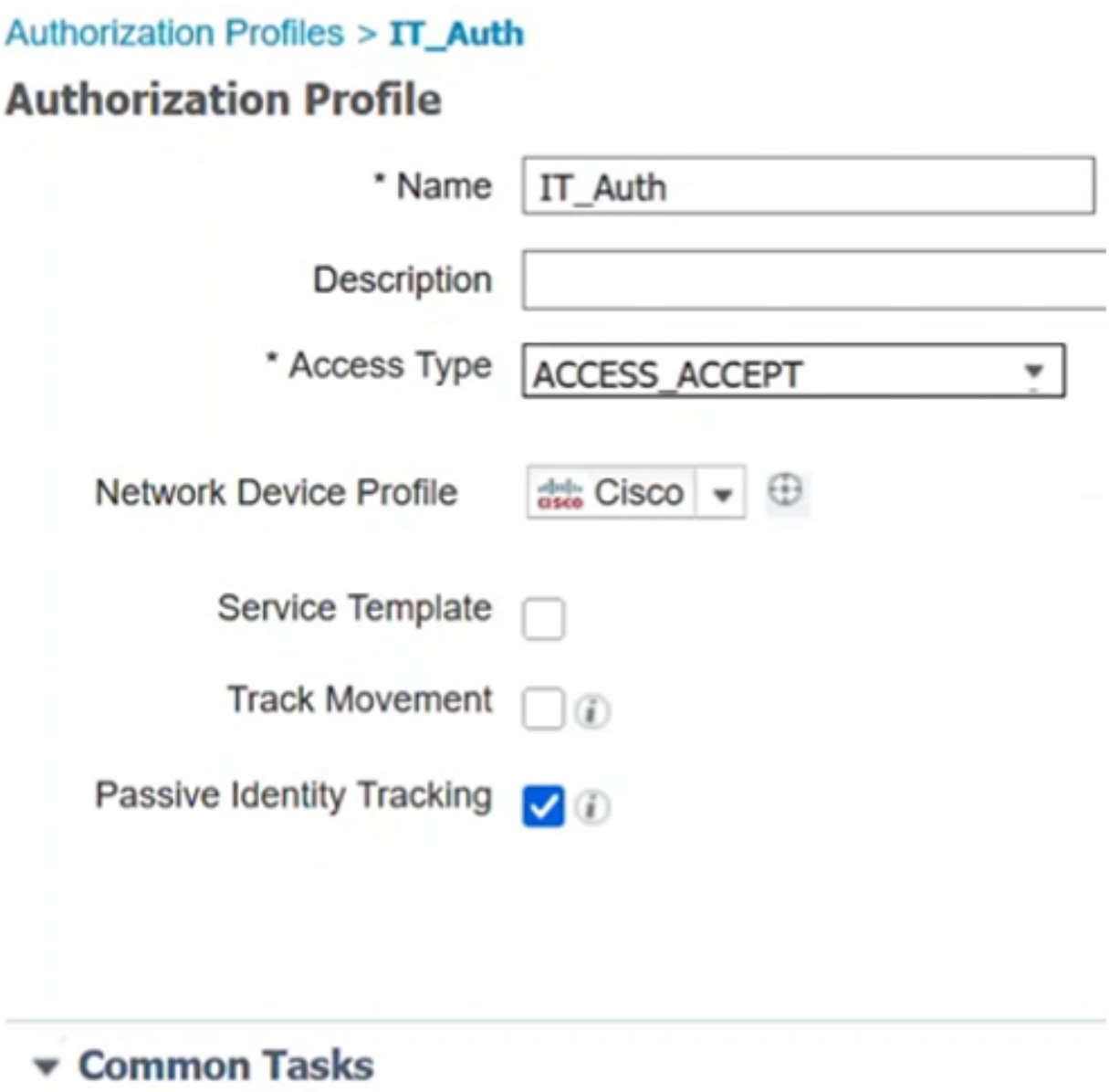


Passo 8

Na página Authorization Profile, configure o seguinte:

- Nome
- Descrição
- Tipo de acesso - deve ser definido como ACCESS_ACCEPT. Se definido como ACCESS_REJECT, ele rejeitará a autenticação.
- Network Device Profile - (Perfil do dispositivo de rede) deve ser selecionado como Cisco.
- Rastreamento passivo de identidade - talvez seja necessário habilitar para alguns cenários de autenticação. É necessário para cenários EasyConnect_PassiveID vinculados ao AD.
- Tarefas comuns - Esta seção tem muitas opções. Para este exemplo, o Nome da DACL é configurado.

Click Save.



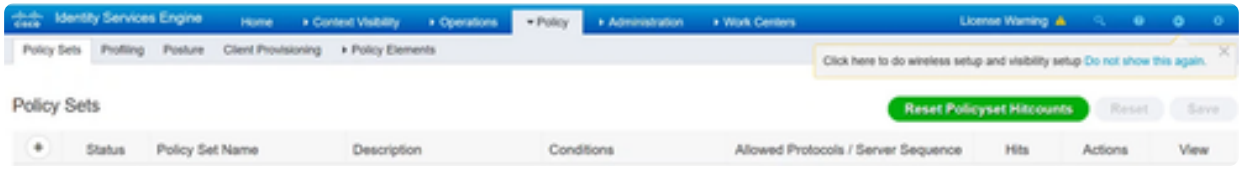
Passo 9

Para configurar conjuntos de políticas que são agrupamentos lógicos de políticas de autenticação e autorização, clique no menu Policy > Policy Sets.

Você pode exibir o seguinte ao examinar uma lista de conjuntos de políticas:

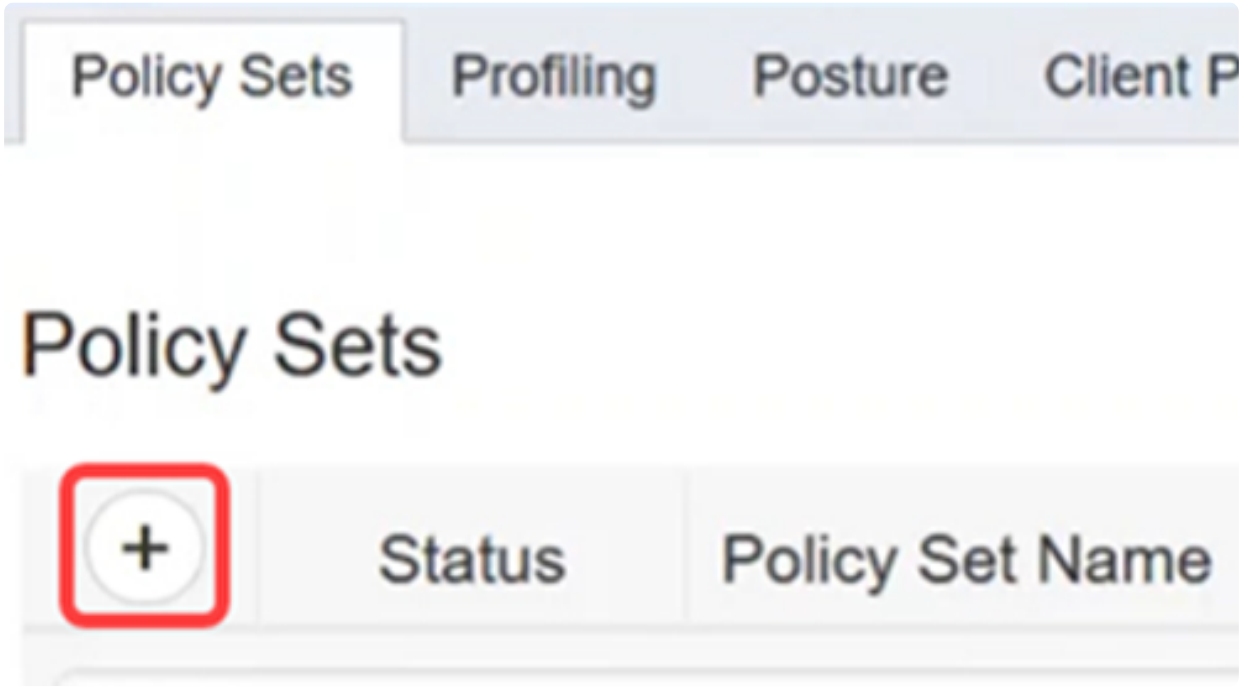
- Status - Uma marca de seleção verde indica habilitado, um círculo branco vazio indica desabilitado e um ícone de olho é para uma configuração somente de monitor.
- Nome do conjunto de políticas e Descrição - são autoexplicativos
- Condições - defina onde o conjunto de políticas se aplica.
- Protocolos permitidos/sequência de servidor - define controles mais avançados.
- Ocorrências - mostra o número de vezes que o conjunto de políticas foi usado.
- Ações - permitem alterar a ordem na qual os conjuntos de políticas podem ser aplicados, copiar um conjunto de políticas existente ou excluir um conjunto de políticas existente.

- Exibir - permite editar os detalhes do conjunto de políticas.



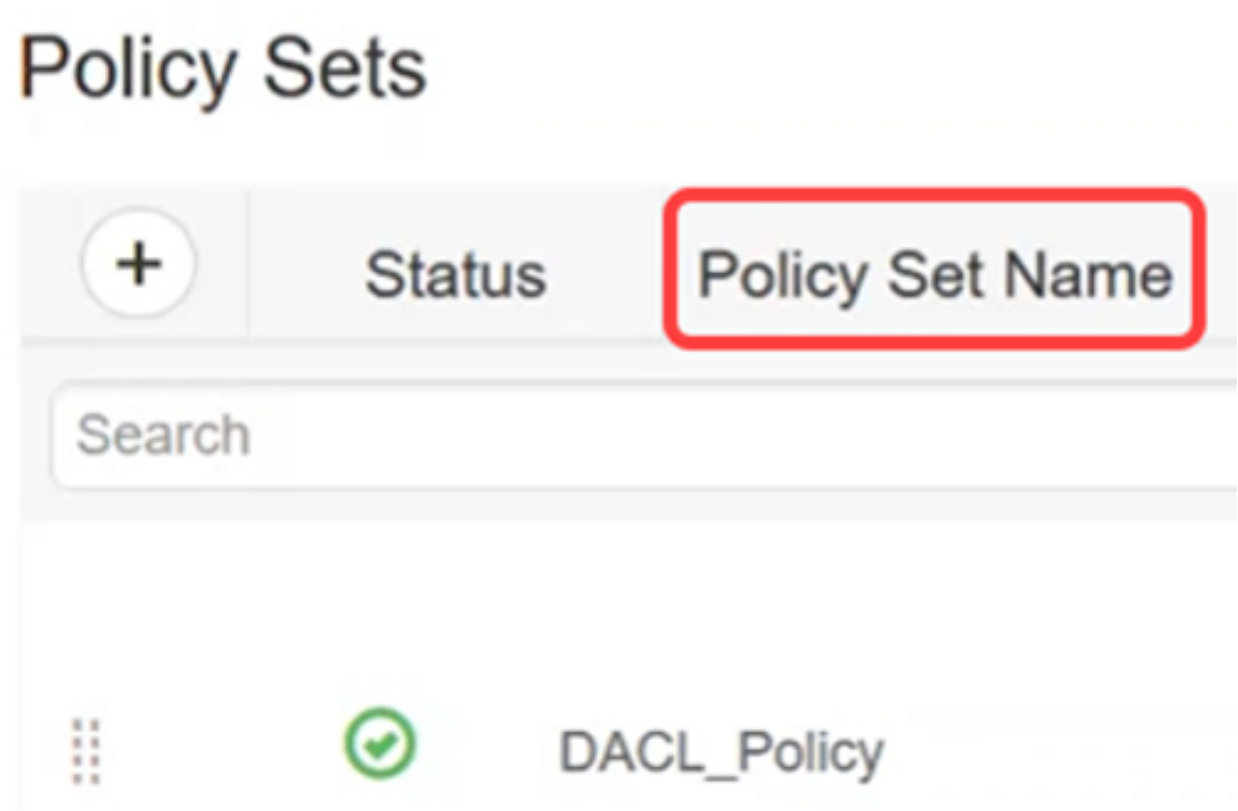
Passo 10

Para criar um conjunto de políticas, clique no botão add.



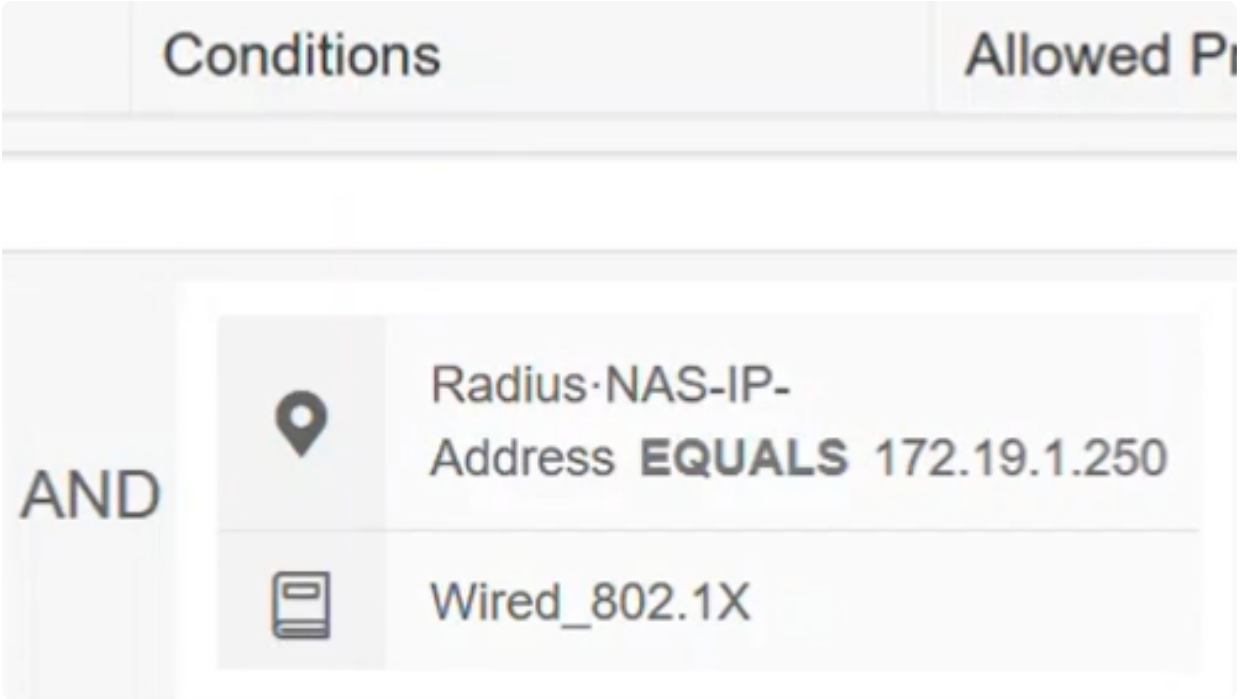
Passo 11

Defina um Nome do conjunto de políticas.



Etapa 12

Em Condições, clique no botão adicionar. Isso abre o Estúdio de Condições, onde você pode definir onde esse perfil de autenticação será usado. Neste exemplo, ele foi aplicado ao Radius-NAS-IP-Address (o switch), que é o tráfego 172.19.1.250 e wired_802.1x.

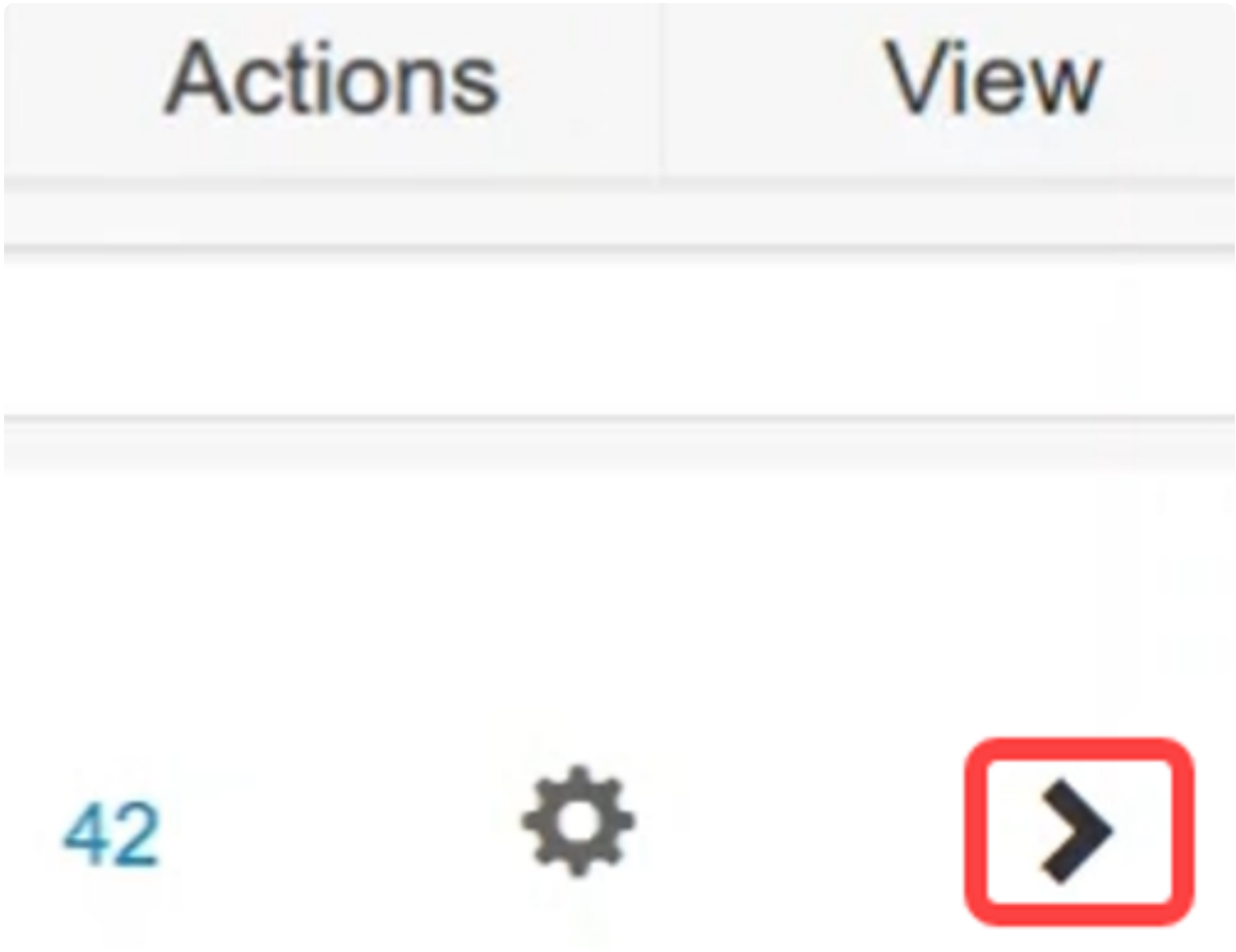


Passo 13

Configure os protocolos permitidos para o acesso padrão à rede e clique em Salvar.

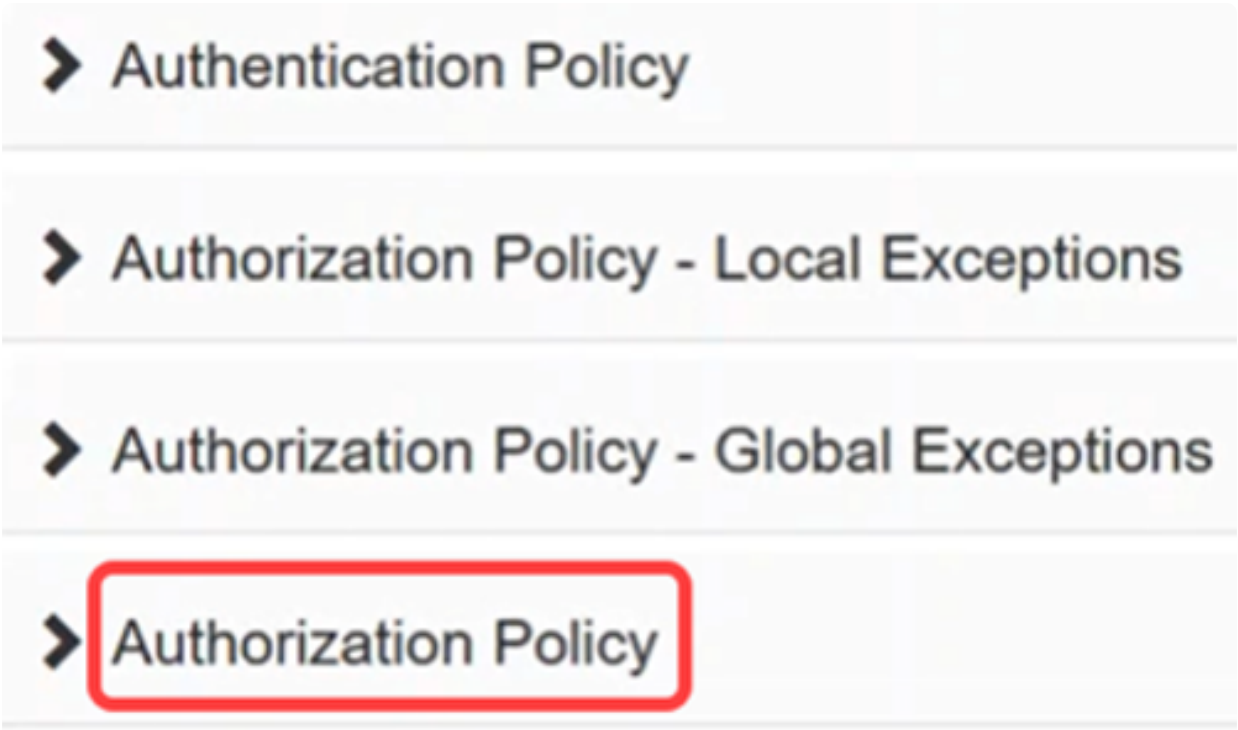
Passo 14

Em View, clique no ícone de seta para configurar as políticas de autenticação e autorização com base na configuração e nos requisitos da sua rede ou você pode escolher as configurações padrão. Neste exemplo, clique em Política de autorização.



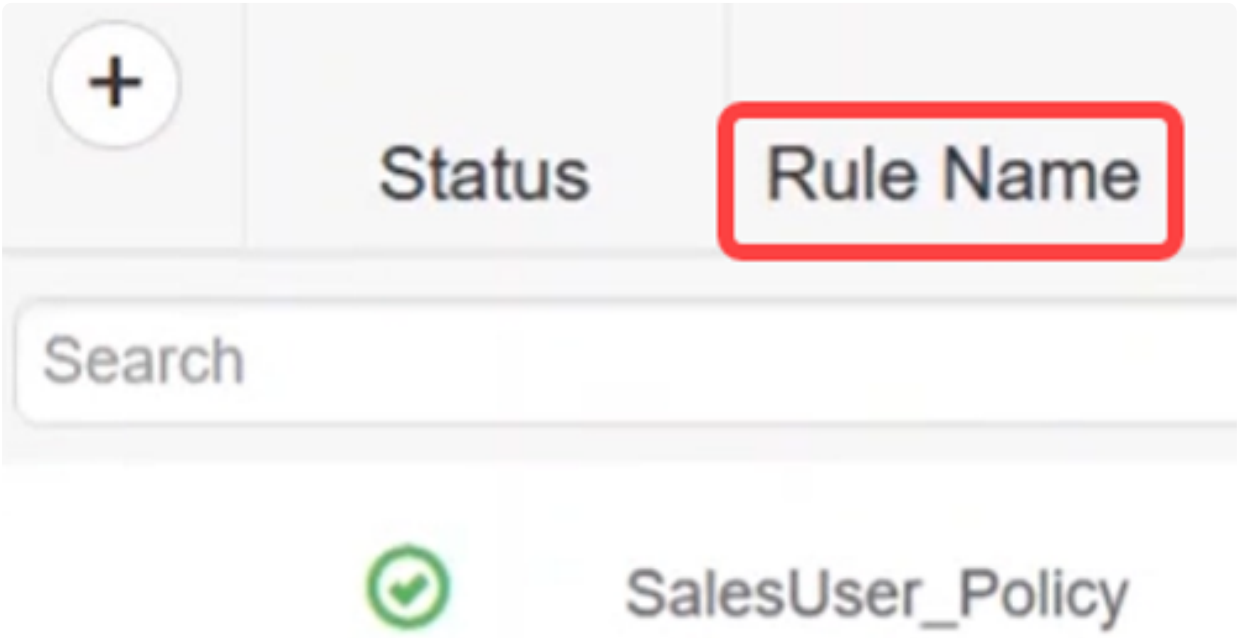
Etapa 15

Clique no ícone do sinal de mais para adicionar uma regra.



Passo 16

Insira o Nome da regra.



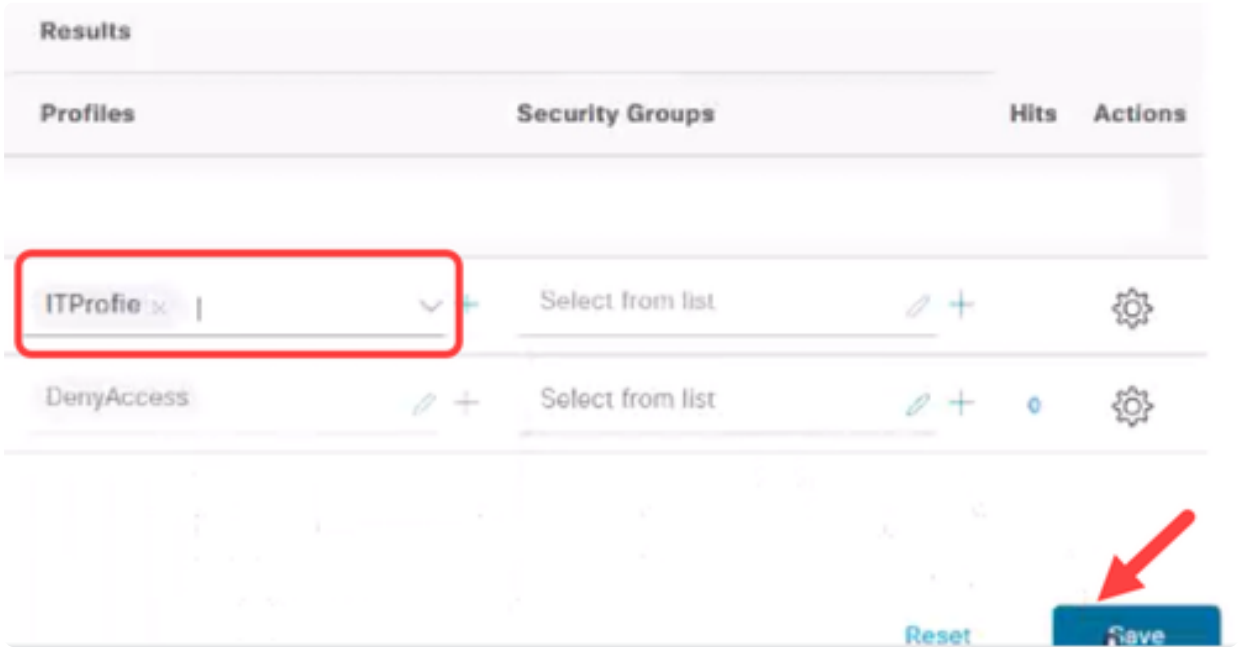
Etapa 17

Em Condições, clique no ícone do sinal de mais e selecione o grupo de identidade.

Clique em Usar.

Etapa 18

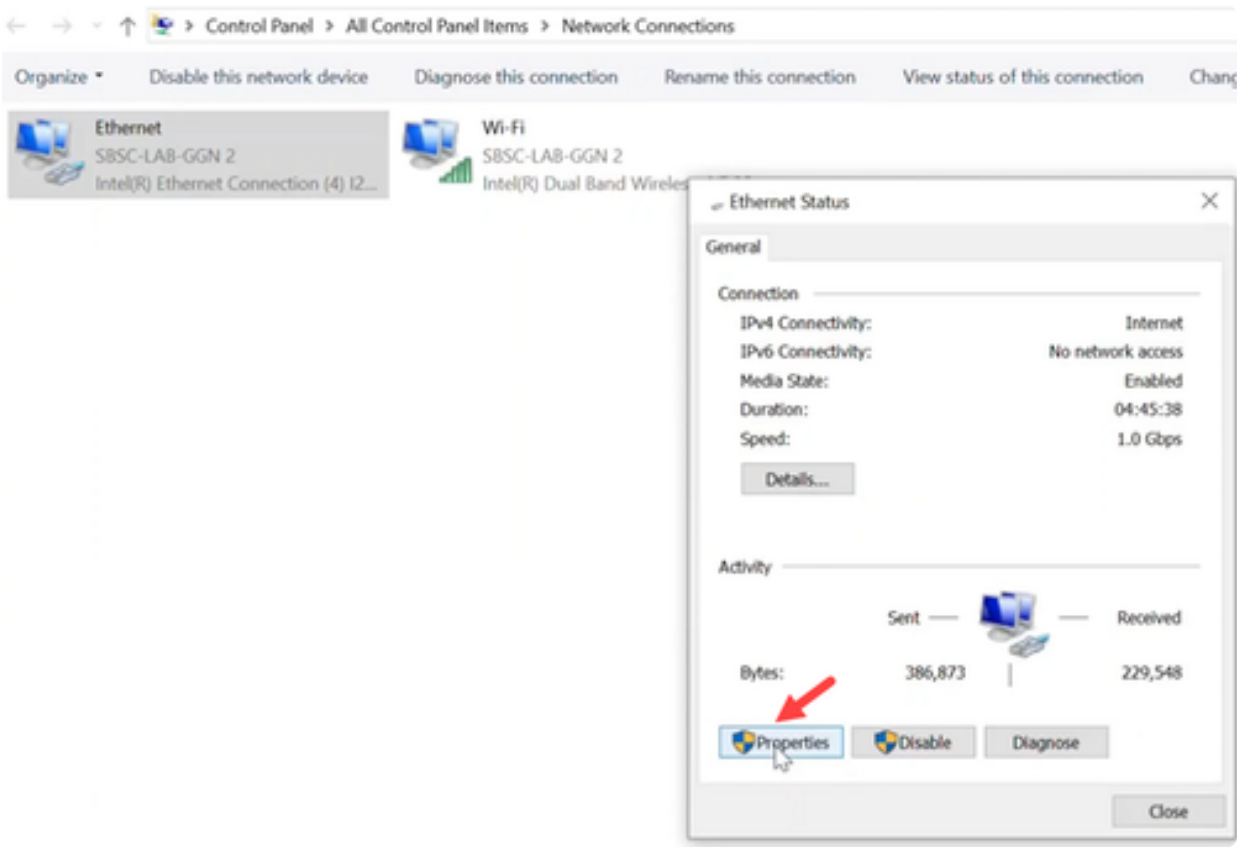
Aplique o perfil necessário e clique em Save.



Configurações do cliente

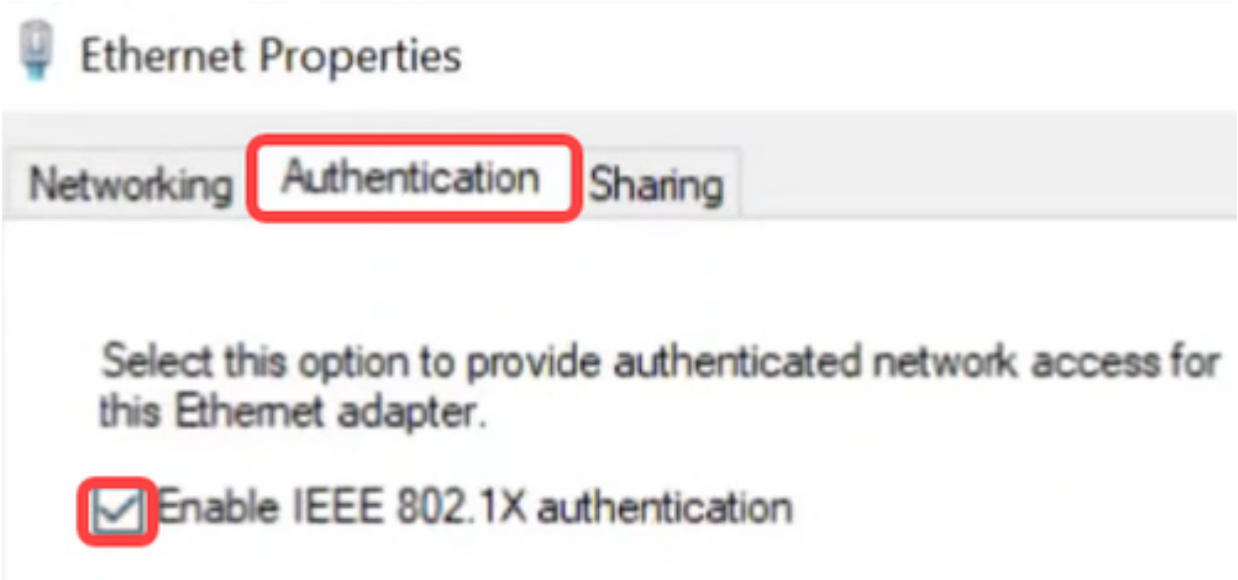
Passo 1

No laptop do cliente, navegue para Conexões de rede > Ethernet e clique em Propriedades.



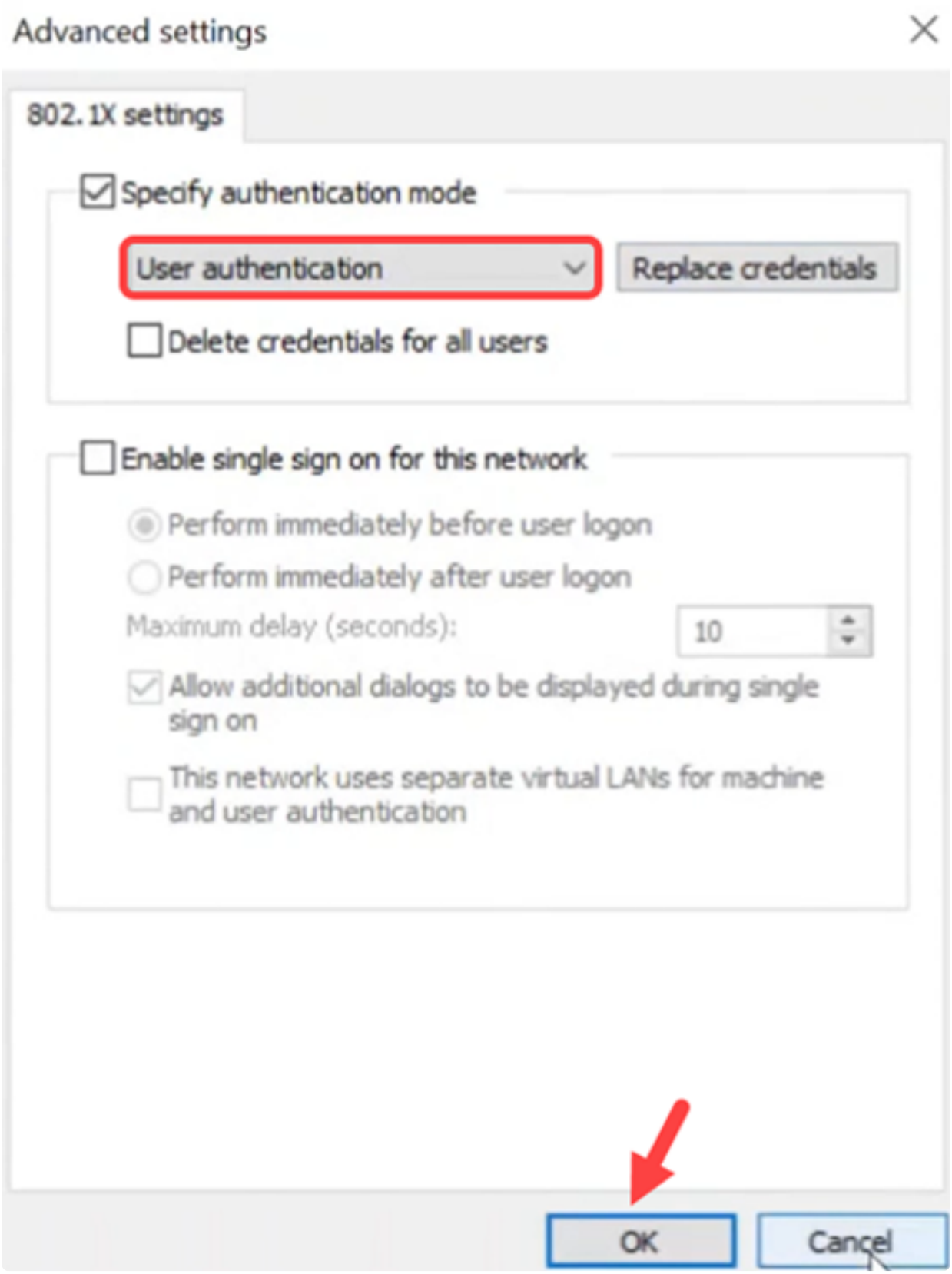
Passo 2

Clique na guia Authentication e verifique se a autenticação 802.1X está habilitada.



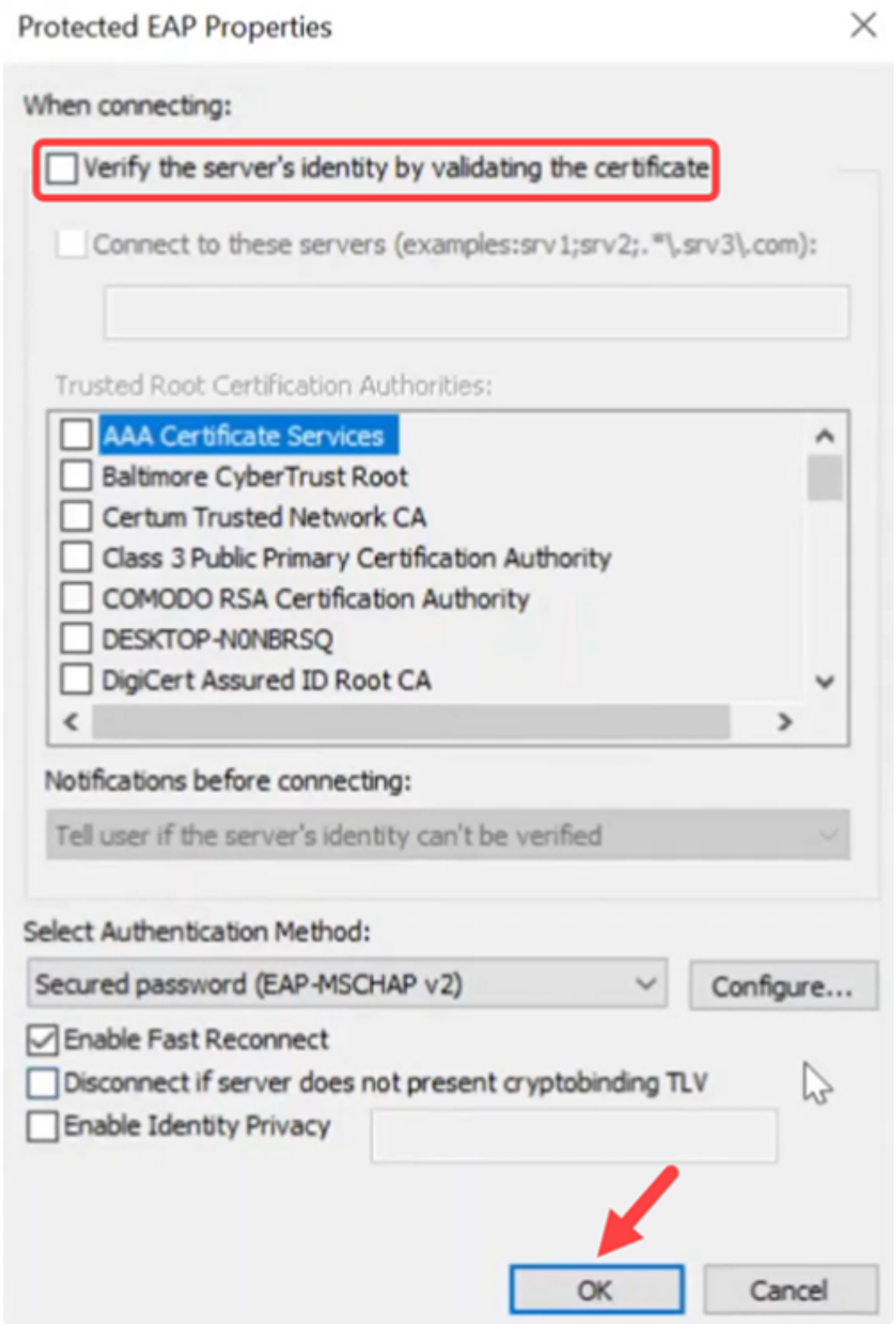
Etapa 3

Em Additional Settings, selecione User authentication como modo de autenticação. Clique em Salvar credenciais e depois em OK.



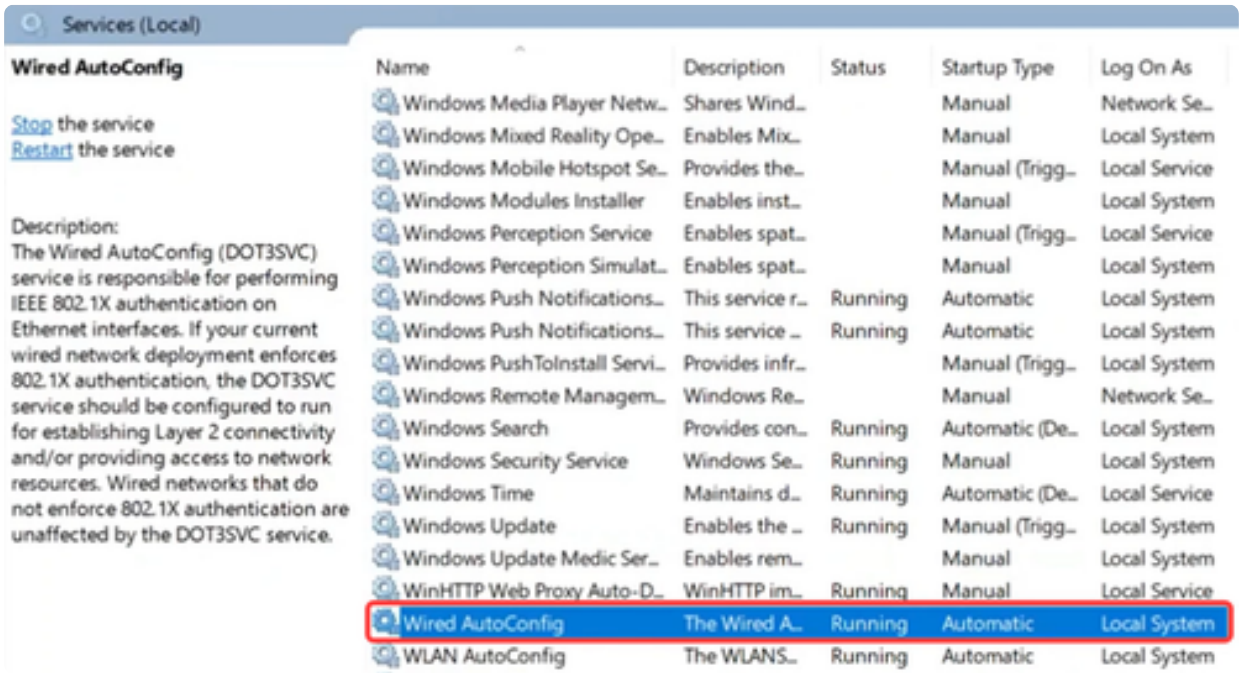
Passo 4

Clique em Settings e certifique-se de que a caixa ao lado de Verify the server’s identity by validating the certificate esteja desmarcada. Click OK.


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AAA Certificate Services
Baltimore CyberTrust Root
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DESKTOP-N0NBRSQ
DigiCert Assured ID Root CA
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

Etapa 5

Em Services, habilite Wired AutoConfig .

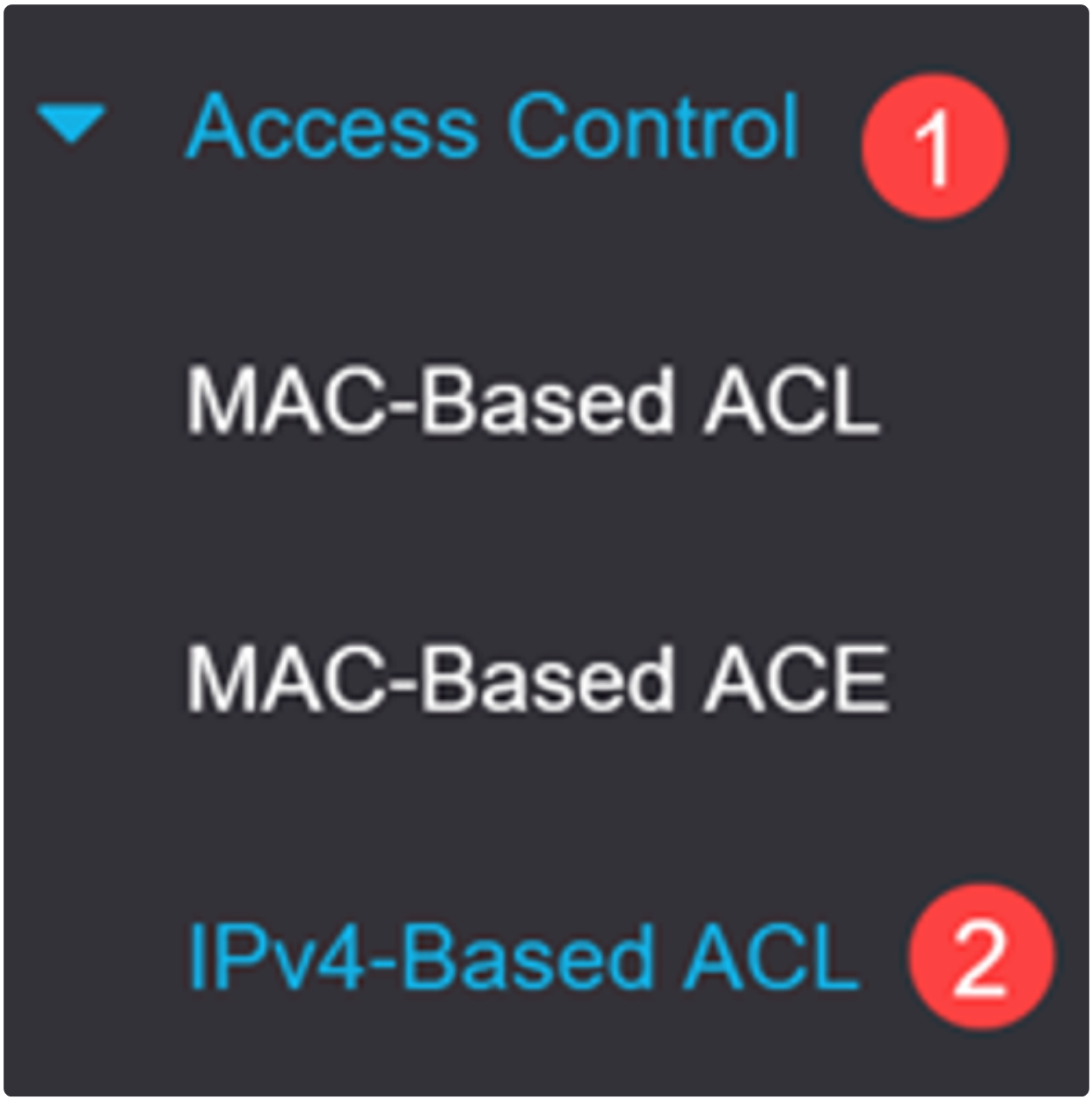


Verificação de DACL

Depois que o usuário for autenticado, você poderá verificar a ACL que pode ser obtida por download.

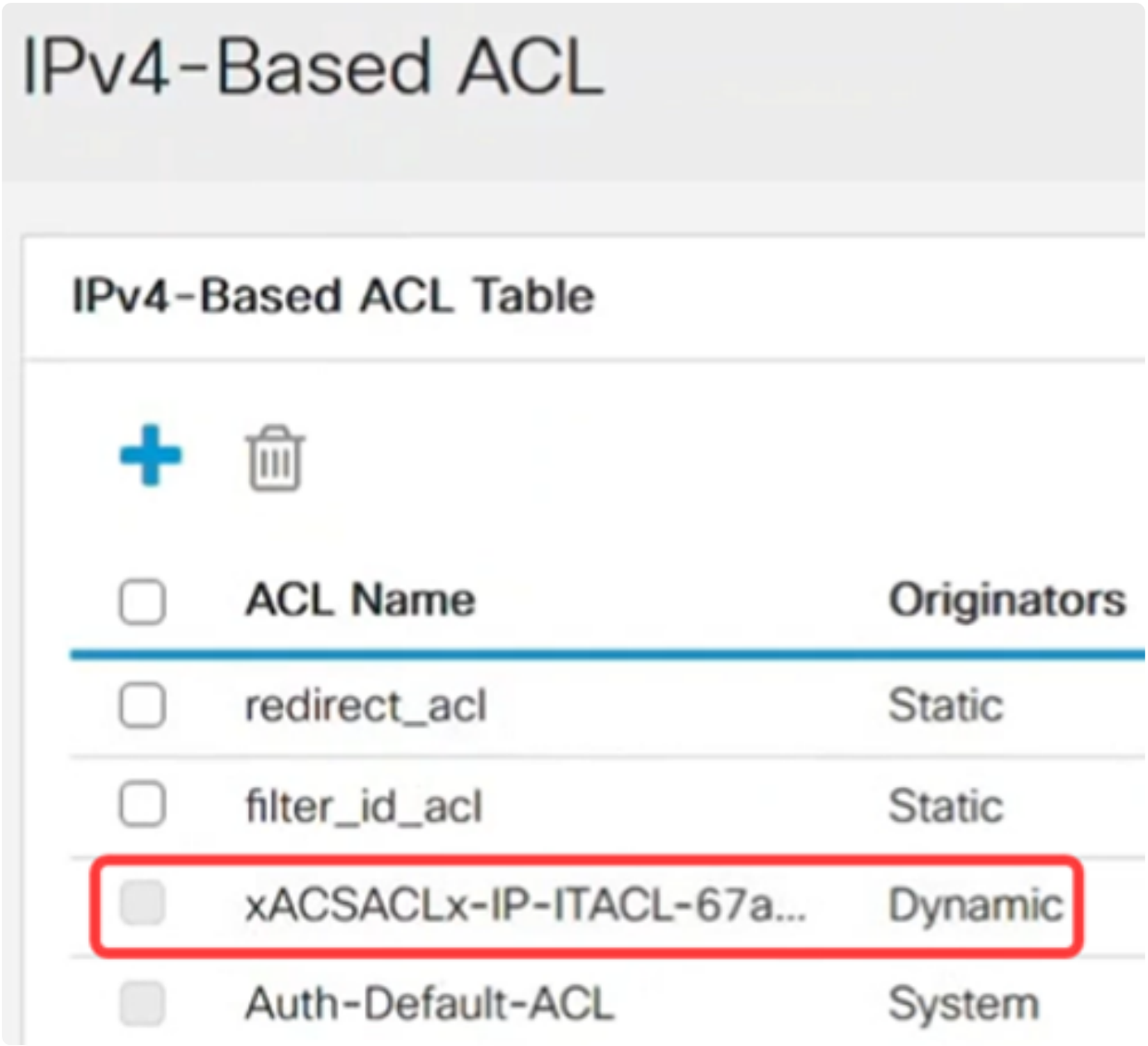
Passo 1

Faça login no switch Catalyst 1300 e navegue para o menu Controle de acesso > ACL baseada em IPv4.



Passo 2

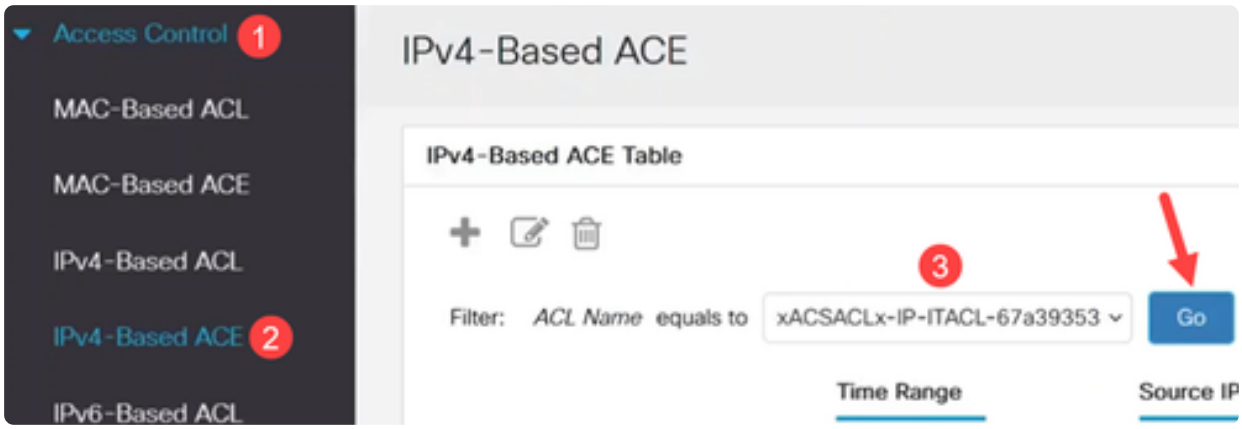
A tabela ACL baseada em IPv4 exibirá a ACL baixada.



Note:
As ACLs para download não podem ser editadas.

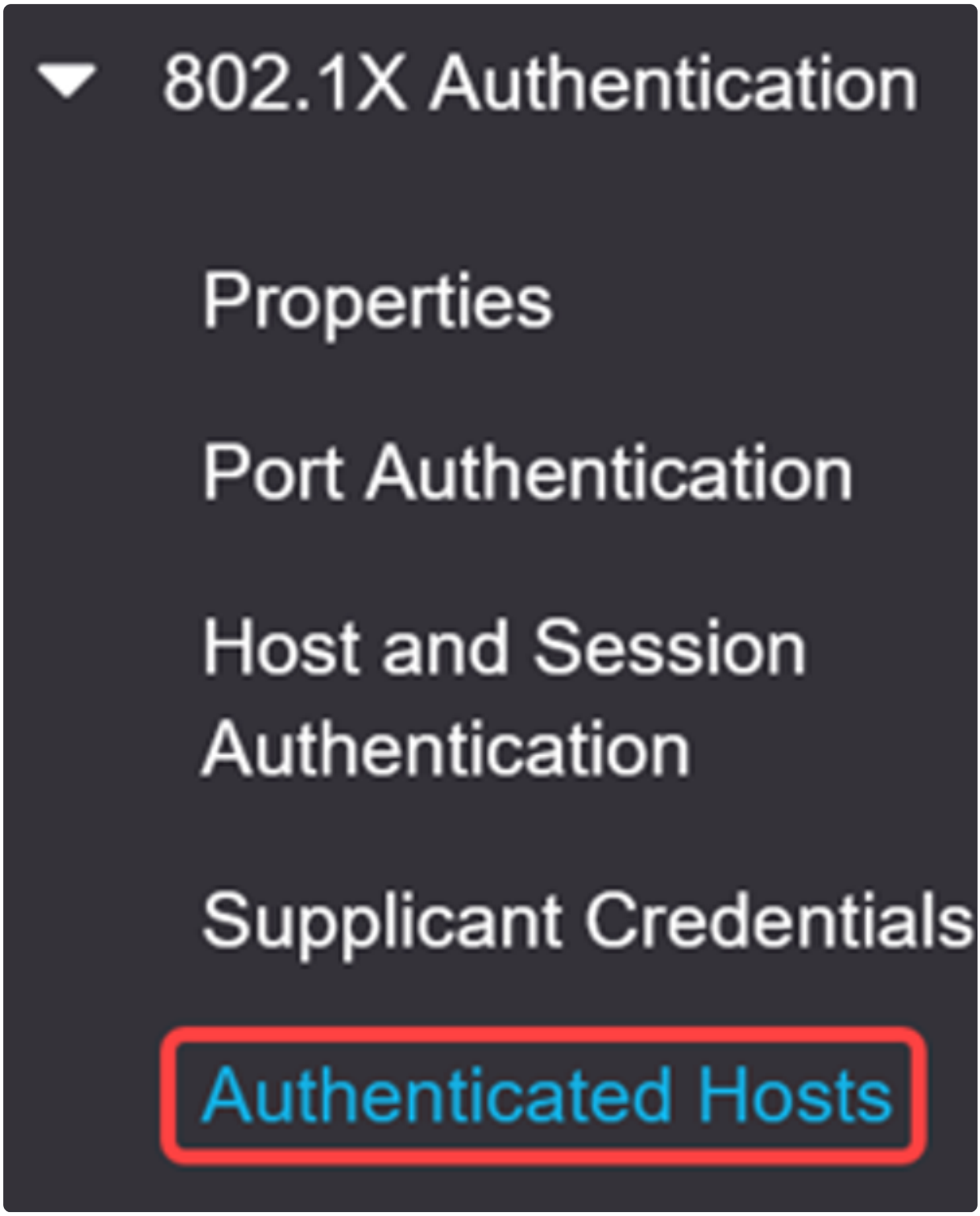
Etapa 3

Outra maneira de verificar é navegar paraACE baseada em IPv4, selecionar a ACL que pode ser baixada no menu suspenso Nome da ACL e clicar em Ir. As regras que foram configuradas no ISE serão exibidas.



Passo 4

Navegue para o menu Security > 802.1 Authentication > Authenticated Hosts. Você pode verificar os usuários autenticados. Clique em Authenticated Sessions para ver mais detalhes.



Etapa 5

Na CLI, execute o comando show ip access-lists interface seguido pelo ID da interface.

Neste exemplo, as ACLs e ACEs aplicadas ao Gigabit Ethernet 3 podem ser vistas.

```
switch4a7d55#show ip access-lists interface ge1/0/3
ip access-list extended xACSACLx-IP-SalesACL-6760399d
    deny    ip any host 192.168.251.10 ace-priority 1
    permit  ip any any ace-priority 2
ip access-list extended Auth-Default-ACL
    permit  udp any any any domain ace-priority 20
    permit  tcp any any any domain ace-priority 40
    permit  udp any bootps any any ace-priority 60
    permit  udp any any any bootpc ace-priority 80
    permit  udp any bootpc any any ace-priority 100
    deny    ip any any ace-priority 120
```

Etapa 6

Você também pode ver as configurações relacionadas à conexão do ISE e aos downloads da ACL usando o comando

show dot1x sessions interface <ID> detailed. Você pode exibir o status, o estado da autenticação 802.1x e as ACLs baixadas.

```
switch4a7d55#show dot1x sessions interface ge1/0/3 detailed

          Interface: gi1/0/3
        MAC Address: e4:          :31
       IPv4 Address: 192.168.251.11
          User-Name: user5
             Status: Authorized
     Oper host mode: multi-host
    Session timeout: N/A
     Session Uptime: 196 sec
  Common Session ID: 14FBA8C00500032222C35D9E
    Acct Session ID: 0x05000322
 Server Policies:
            ACS ACL: xACSACLx-IP-SalesACL-6760399d

 Method status list:
    Method                  State
    802.1x                  Authentication success
```

Conclusão

Pronto! Agora você sabe como a ACL para download funciona nos switches Cisco Catalyst 1300 com o Cisco ISE.

Para obter mais informações, consulte o Guia de Administração do Catalyst 1300 e a Página de Suporte do Cisco Catalyst 1300 Series.

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.