

Configurar RADIUS & TACACS+ para GUI & CLI Auth em WLCs 9800

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Restrições de Usuário Somente Leitura](#)

[Configurar a autenticação RADIUS para a WLC](#)

[Configurar ISE para RADIUS](#)

[Configurar TACACS+ WLC](#)

[Configuração do TACACS+ ISE](#)

[Troubleshooting](#)

[Solucionar problemas de acesso RADIUS/TACACS+ de GUI ou CLI de WLC via CLI de WLC](#)

[Solucionar problemas da GUI da WLC ou do acesso CLITACACS+ através da GUI do ISE](#)

Introdução

Este documento descreve como configurar um Catalyst 9800 para autenticação externa RADIUS ou TACACS+.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modelo de configuração Catalyst Wireless 9800
- Conceitos AAA, RADIUS e TACACS+

Componentes Utilizados

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

- C9800-CL v17.9.2
- ISE 3.2.0

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

Quando um usuário tenta acessar a CLI ou a GUI da WLC, ele é solicitado a inserir um nome de usuário e uma senha. Por padrão, essas credenciais são comparadas com o banco de dados local de usuários, que está presente no próprio dispositivo. Como alternativa, a WLC pode ser instruída a comparar as credenciais de entrada com um servidor AAA remoto: a WLC pode se comunicar com o servidor com o uso de RADIUS ou TACACS+.

Configurar

Neste exemplo, dois tipos de usuários no servidor AAA (ISE), respectivamente o `adminuser` e o `configuradoshelpdeskuser`. Esses usuários fazem parte dos grupos `admin-group` e dos `helpdesk-group` grupos, respectivamente. Espera-se que o usuário `adminuser`, parte da `admin-group`, receba acesso total à WLC. Por outro lado, o `helpdeskuser`, parte do `helpdesk-group`, deve receber somente privilégios de monitor para o WLC. Portanto, não há acesso à configuração.

Este artigo primeiro configura a WLC e o ISE para autenticação RADIUS e depois executa o mesmo para TACACS+.

Restrições de Usuário Somente Leitura

Quando TACACS+ ou RADIUS é usado para a autenticação WebUI 9800, estas restrições existem:

- Os usuários com nível de privilégio 0 existem, mas não têm acesso à GUI

-

Os usuários com níveis de privilégio de 1 a 14 podem apenas exibir a guia Monitor (isso equivale ao nível de privilégio de um usuário autenticado localmente somente leitura)

-

Usuários com nível de privilégio 15 têm acesso total

-

Usuários com nível de privilégio 15 e um conjunto de comandos que permite apenas comandos específicos não são suportados. O usuário ainda pode executar alterações de configuração por meio da WebUI

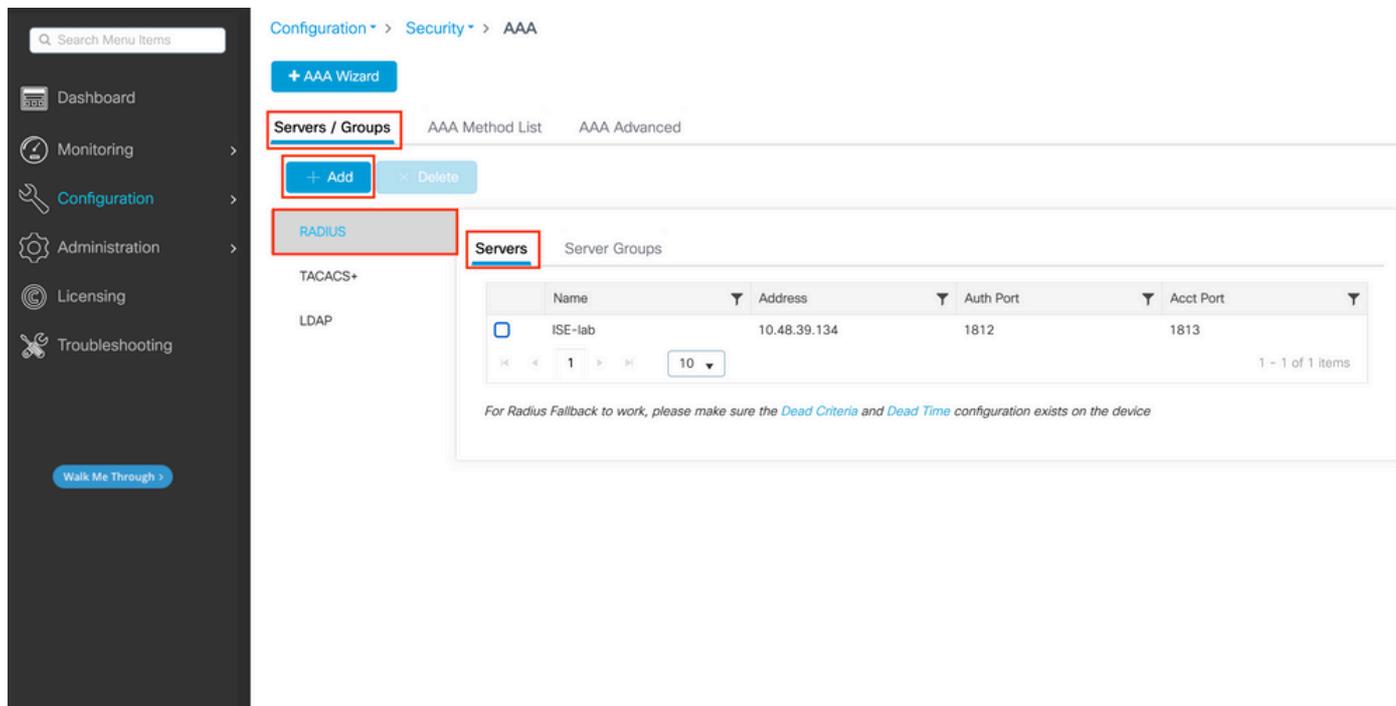
Essas considerações não podem ser alteradas nem modificadas.

Configurar a autenticação RADIUS para a WLC

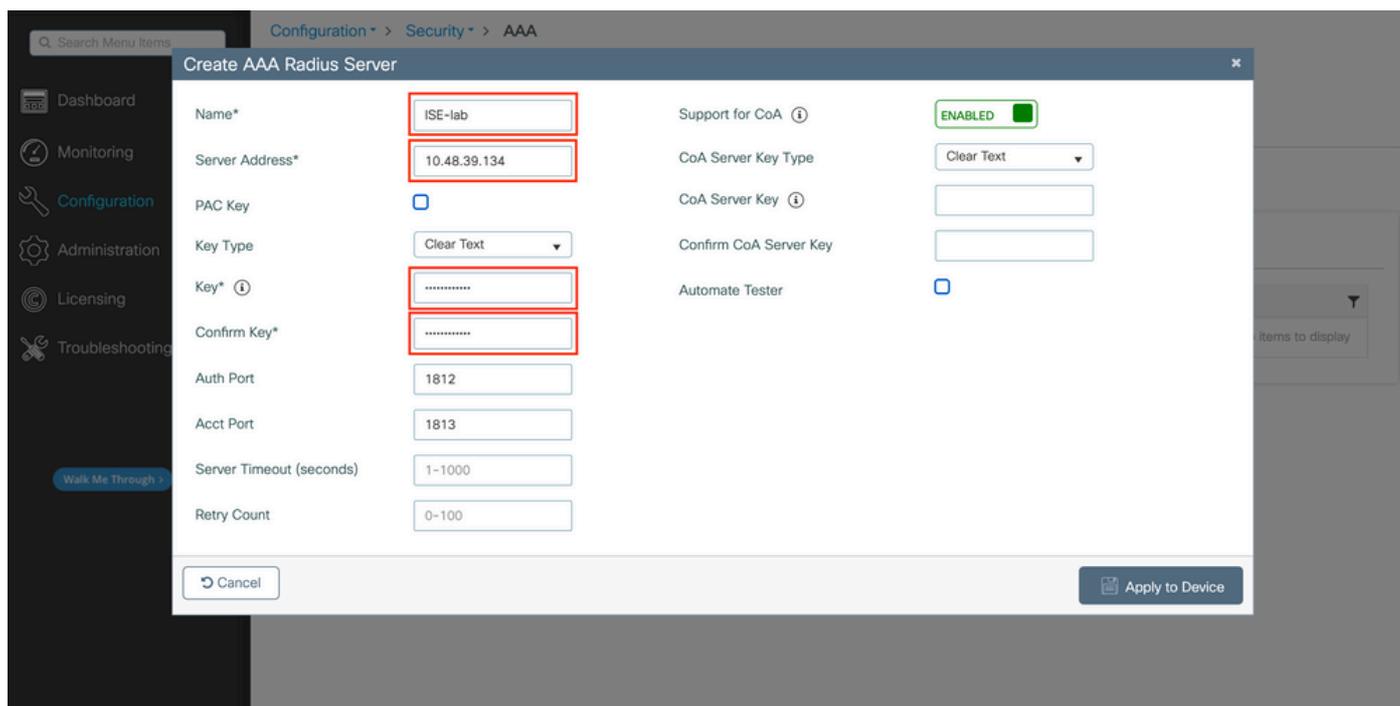
Etapa 1. Declare o servidor RADIUS.

Da GUI:

Primeiro, crie o servidor ISE RADIUS no WLC. Isso pode ser feito a partir da guia Servers/Groups > RADIUS > Servers da página da GUI WLC acessível no <https://<WLC-IP>/webui/#/aaa>, ou se você navegar para [Configuration > Security > AAA](#), como mostrado nesta imagem.



Para adicionar um servidor RADIUS na WLC, clique no botão Add (Adicionar) emoldurado em vermelho na imagem. Isso abre a janela pop-up descrita na captura de tela.



Nessa janela pop-up, você deve fornecer:

- O nome do servidor (observe que ele não precisa corresponder ao nome do sistema ISE)
- O endereço IP do servidor
- O segredo compartilhado entre a WLC e o servidor RADIUS

Outros parâmetros podem ser configurados, como as portas usadas para autenticação e contabilização, mas eles não são obrigatórios e são deixados como padrão para esta documentação.

Do CLI:

```
<#root>
```

```
WLC-9800(config)#radius server
```

```
ISE-1ab
```

```
WLC-9800(config-radius-server)#address ipv4
```

```
10.48.39.134
```

```
auth-port 1812 acct-port 1813
```

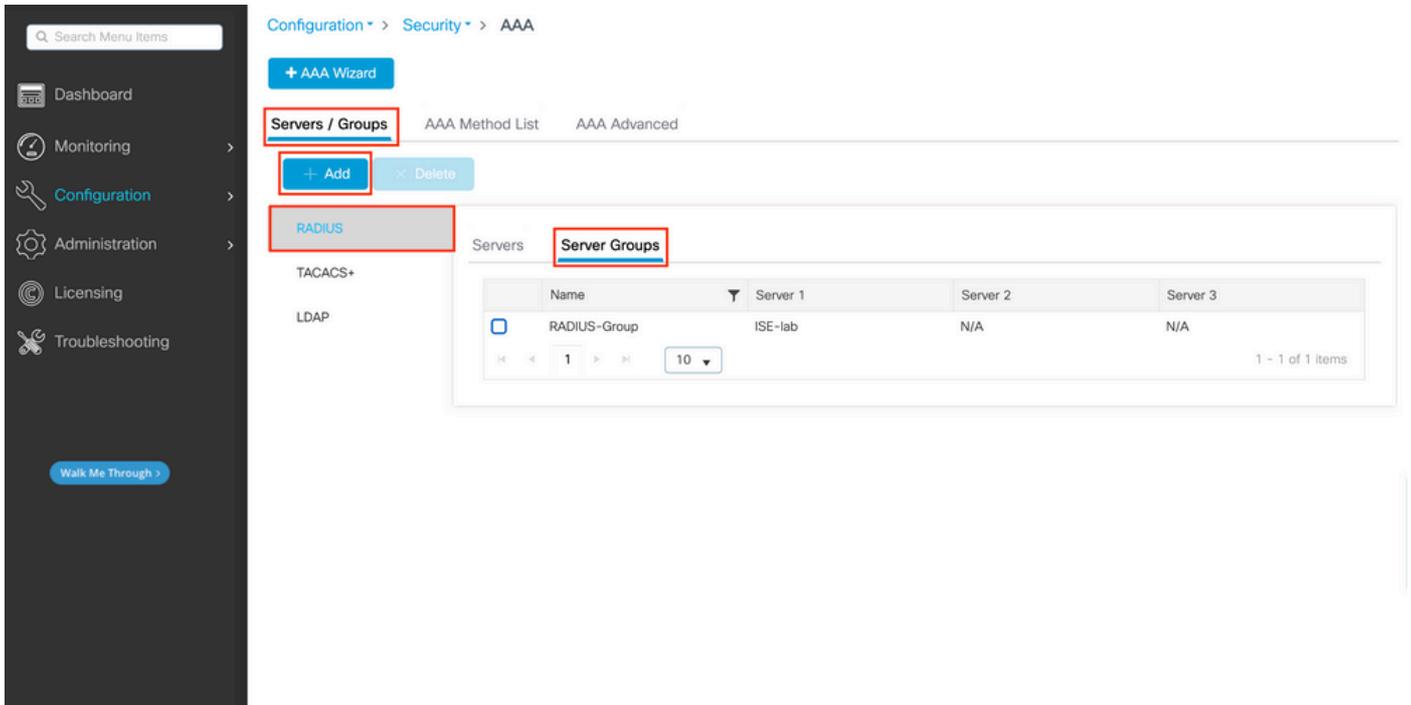
```
WLC-9800(config-radius-server)#key
```

```
Cisco123
```

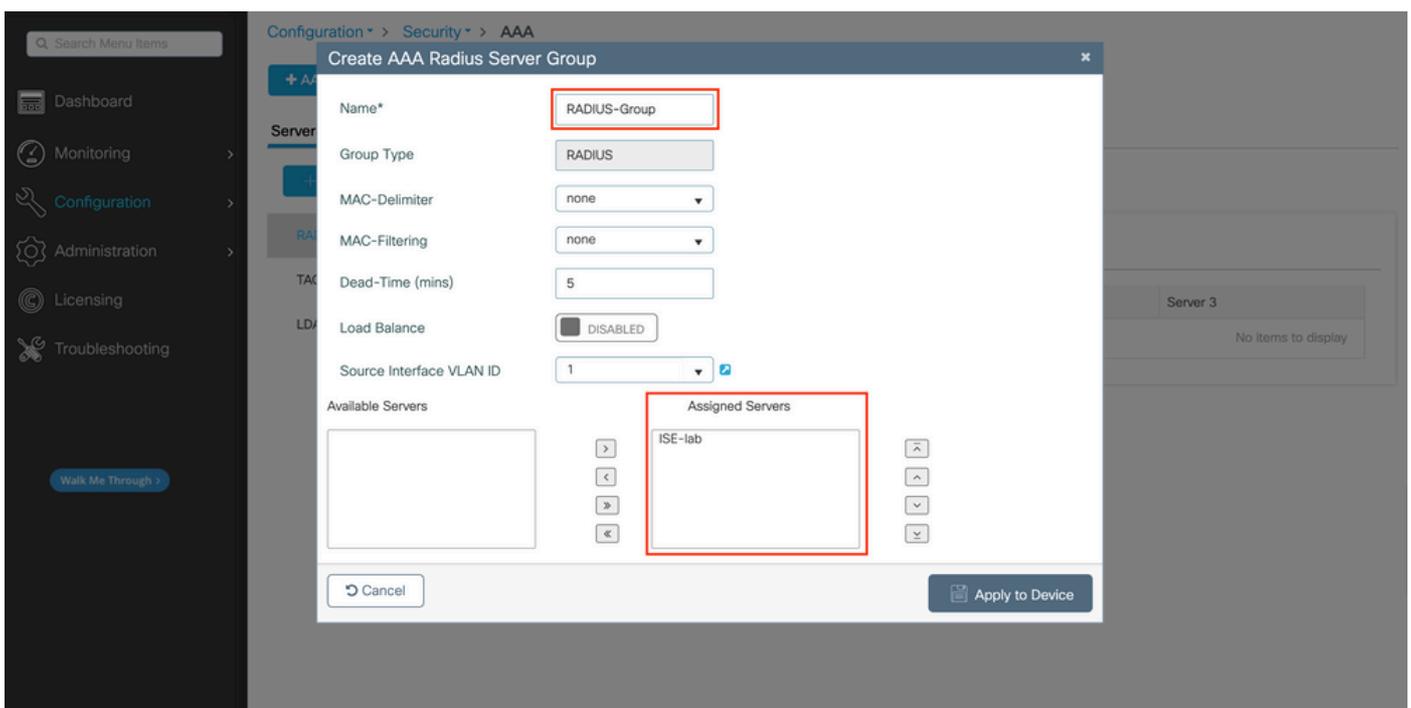
Etapa 2. Mapeie o servidor RADIUS para um grupo de servidores.

Da GUI:

Caso você tenha vários servidores RADIUS que possam ser usados para autenticação, é recomendável mapear todos esses servidores para o mesmo grupo de servidores. A WLC cuida do balanceamento de carga de diferentes autenticações entre os servidores no grupo de servidores. Os grupos de servidores RADIUS são configurados na guia Servers/Groups > RADIUS > Server Groups na mesma página da GUI que a mencionada na Etapa 1, como mostrado na imagem.



Quanto à criação do servidor, uma janela pop-up aparece quando você clica no botão Adicionar (enquadrado na imagem anterior), que é descrito aqui.



No pop-up, forneça um nome para o grupo e mova os servidores desejados para a lista Servidores Atribuídos.

Do CLI:

<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

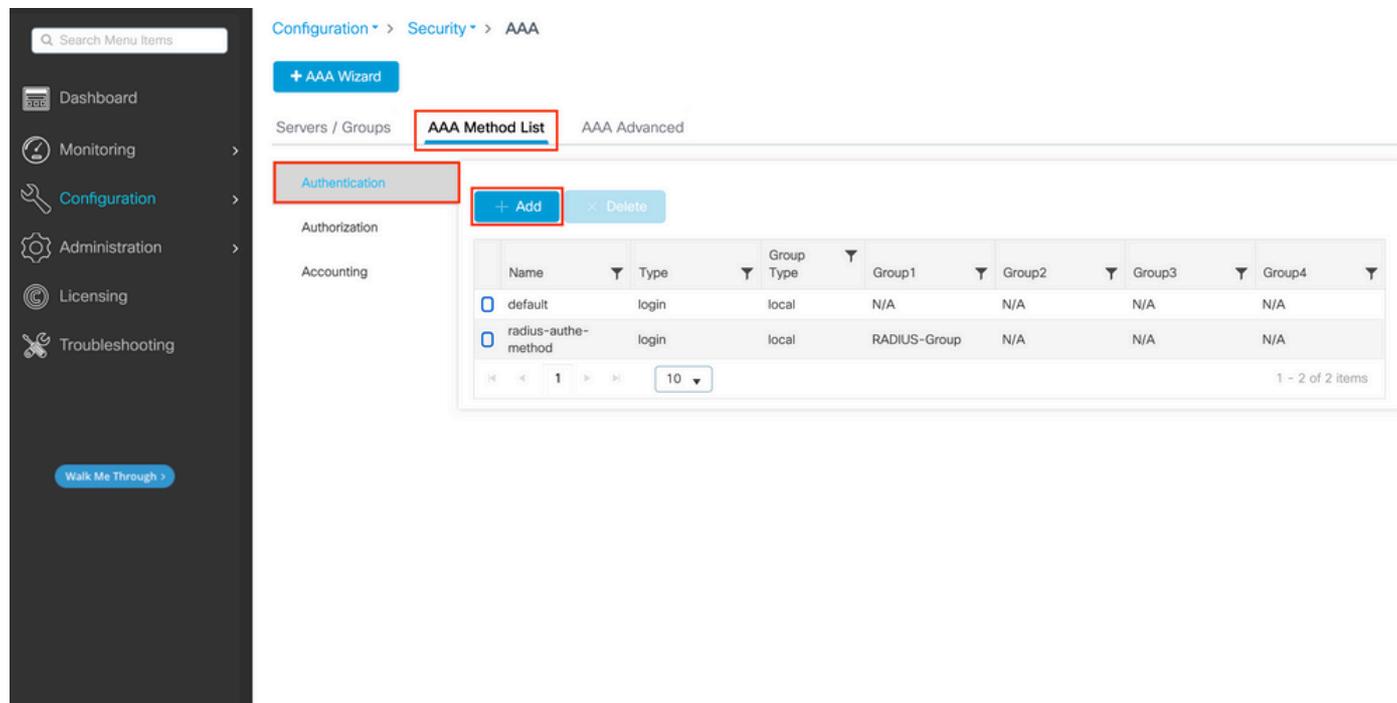
WLC-9800(config-sg-radius)# server name

ISE-lab

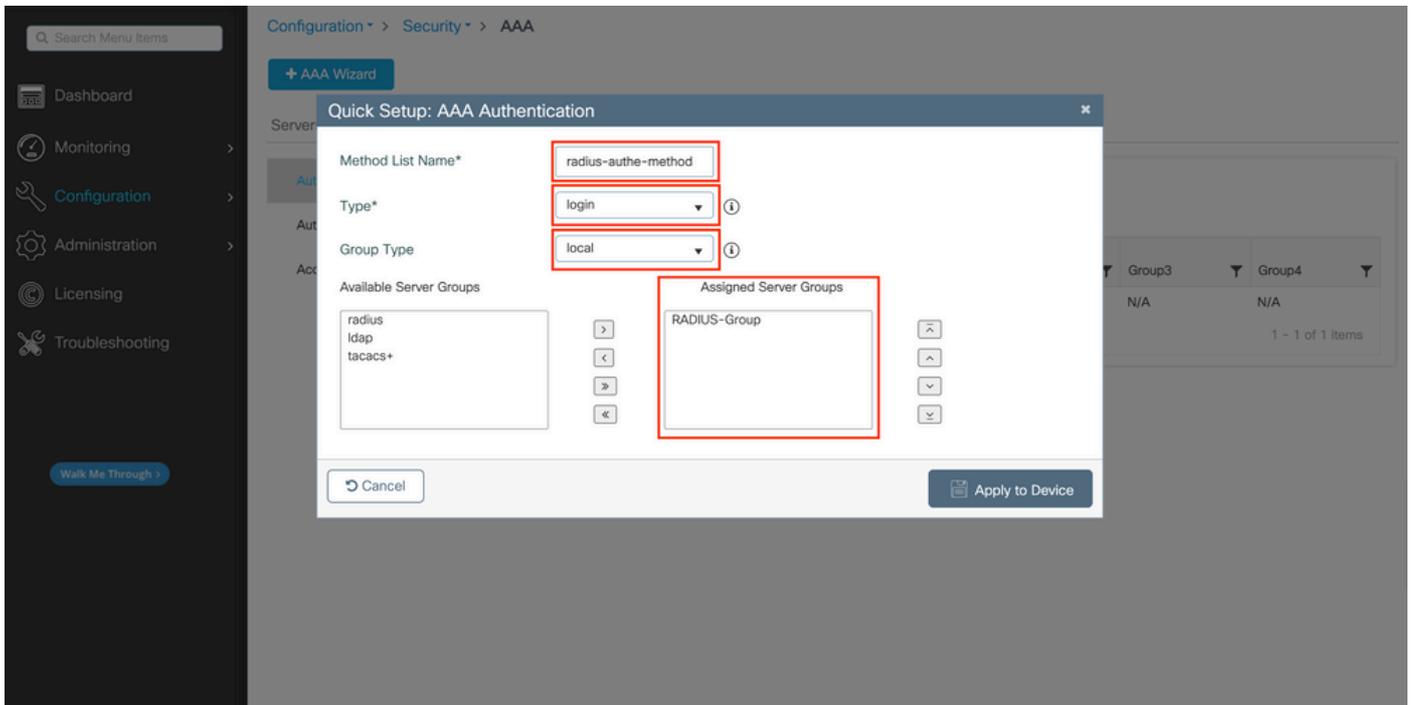
Etapa 3. Crie um método de logon de autenticação AAA que aponte para o grupo de servidores RADIUS.

Da GUI:

Ainda na página <https://<WLC-IP>/webui/#/aaa> GUI, navegue até a guia AAA Method List > Authentication e crie um método de autenticação como mostrado nesta imagem.



Como de costume, quando você usa o botão Adicionar para criar um método de autenticação, uma janela pop-up de configuração é exibida, semelhante àquela descrita nesta imagem.



Nessa janela pop-up, forneça um nome para o método. Escolha Type como login e adicione o servidor de grupo criado na etapa anterior à lista Assigned Server Groups. Com relação ao campo Tipo de grupo, várias configurações são possíveis.

- Se você escolher Tipo de grupo como local, a WLC primeiro verifica se as credenciais do usuário existem localmente e depois volta para o grupo de servidores.
- Se você escolher o Tipo de grupo como um grupo e não marcar a opção Fall back to local, a WLC simplesmente verificará as credenciais do usuário em relação ao grupo de servidores.
- Se você escolher o Tipo de grupo como um grupo e marcar a opção Fallback to local, o WLC verificará as credenciais do usuário em relação ao grupo de servidores e consultará o banco de dados local somente se o servidor não responder. Se o servidor enviar uma rejeição, o usuário será autenticado, mesmo que possa existir no banco de dados local.

Do CLI:

Se quiser que as credenciais do usuário sejam verificadas com um grupo de servidores somente se não forem localmente primeiro, use:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```

local group

RADIUS-Group

Se quiser que as credenciais do usuário sejam verificadas apenas com um grupo de servidores, use:

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

Se quiser que as credenciais do usuário sejam verificadas com um grupo de servidores e se este último não responder com uma entrada local, use:

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

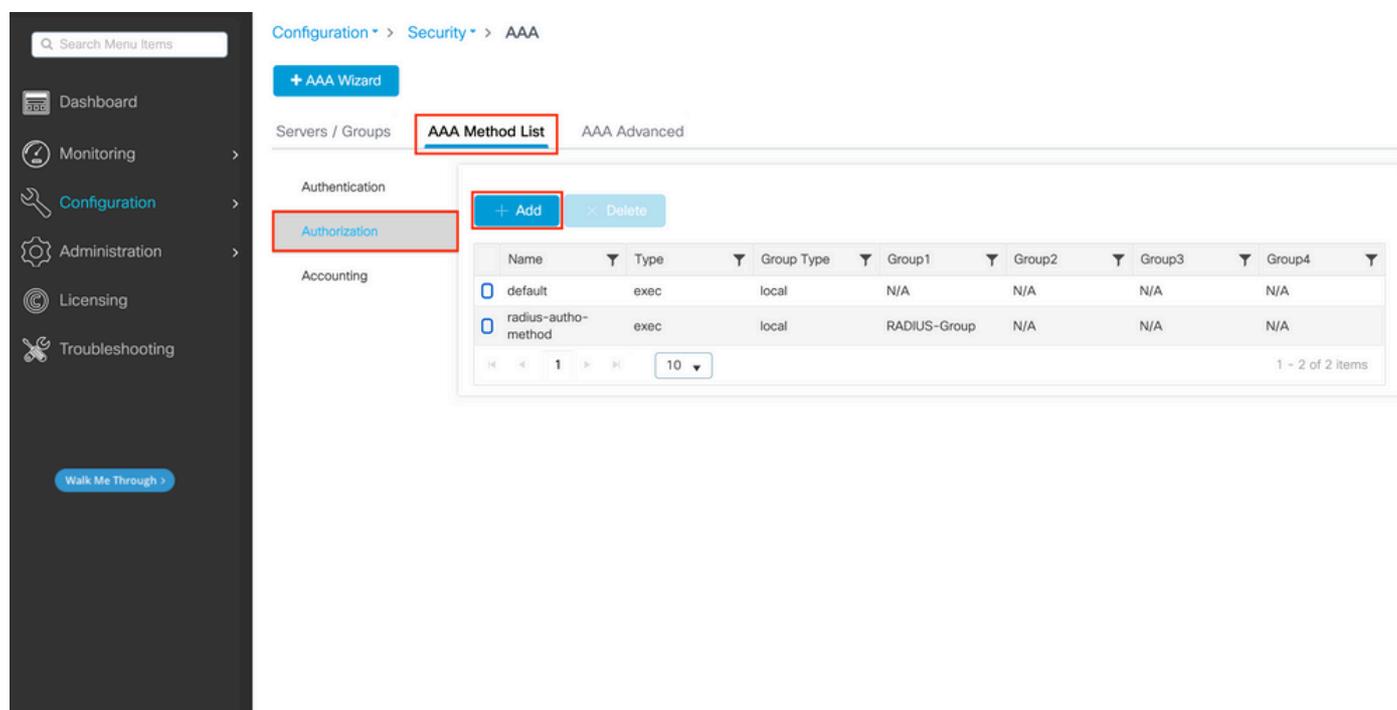
local

Neste exemplo de configuração, há alguns usuários que são criados apenas localmente, e alguns usuários somente no servidor ISE, portanto, faça uso da primeira opção.

Etapa 4. Crie um método de execução de autorização AAA que aponte para o grupo de servidores RADIUS.

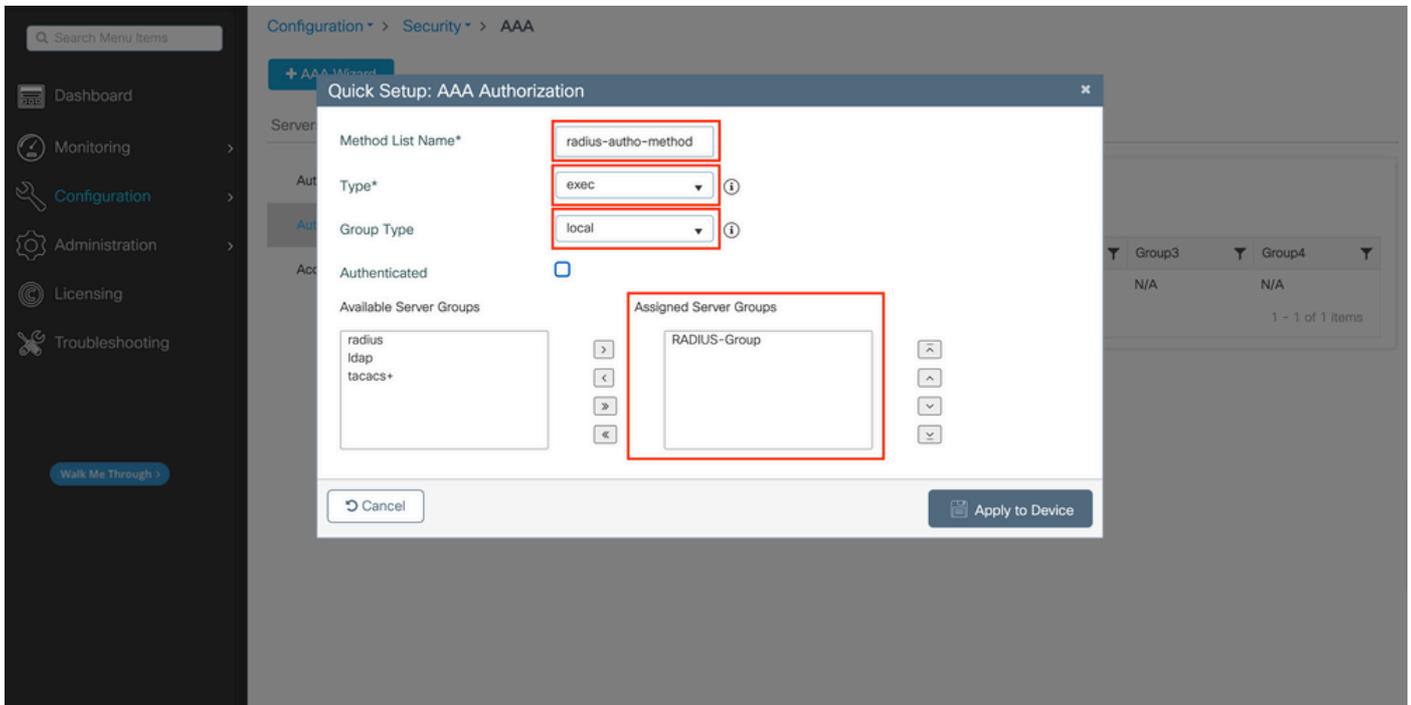
Da GUI:

O usuário também precisa ser autorizado para receber acesso. Ainda no GUI Page Configuration > Security > AAA, navegue até a guia AAA Method List > Authorization e crie um método de autorização como mostrado nesta imagem.



Criação de método de autorização

Um pop-up de configuração de método de autorização semelhante ao descrito é exibido quando você adiciona um novo com o botão Adicionar.



Nessa janela pop-up de configuração, forneça um nome para o método de autorização, escolha o Tipo como exec e use a mesma ordem do Tipo de grupo que a usada para o método de autenticação na Etapa 3.

Do CLI:

Quanto ao método de autenticação, a autorização é atribuída primeiro para verificar os usuários em relação às entradas locais e, em seguida, em relação às entradas em um grupo de servidores.

<#root>

WLC-9800(config)#aaa authorization exec

radius-autho-method

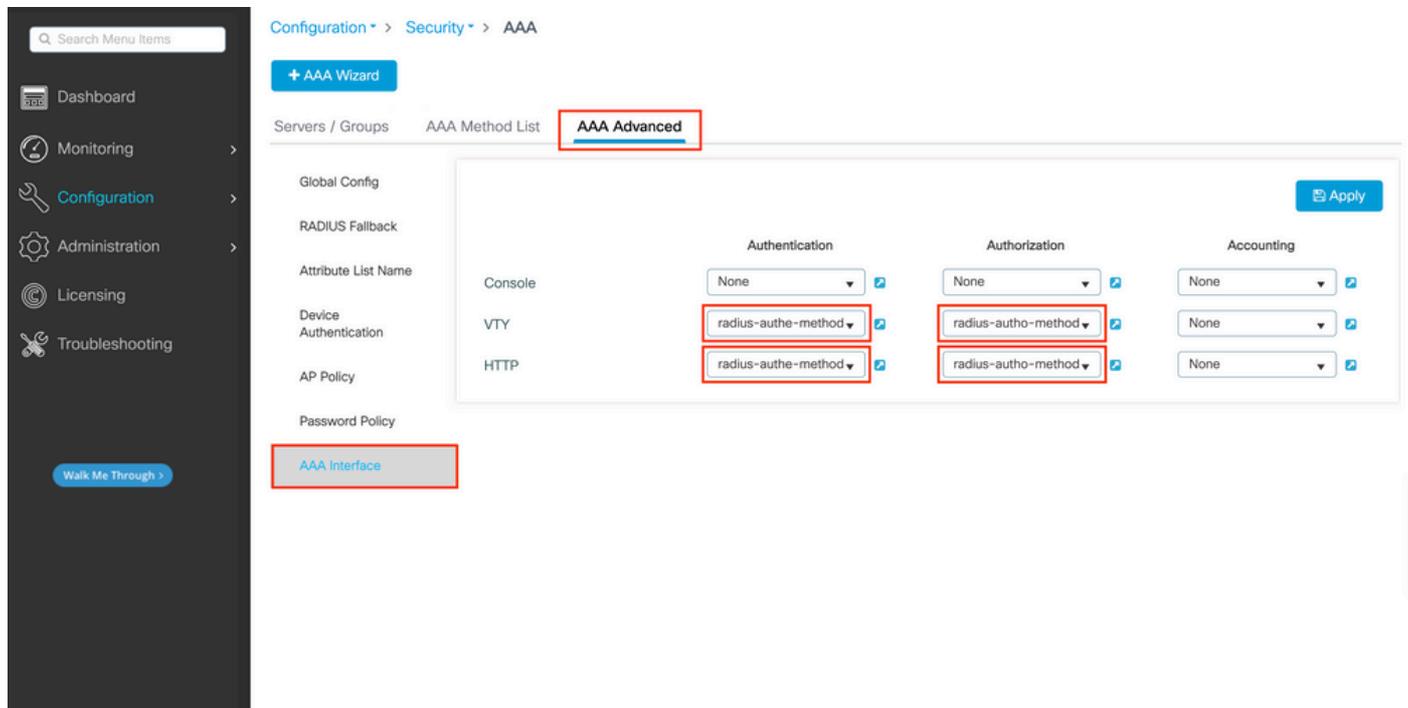
local group

RADIUS-Group

Etapa 5. Atribua os métodos às configurações HTTP e às linhas VTY usadas para Telnet/SSH.

Da GUI:

Os métodos de autenticação e autorização criados podem ser usados para conexão de usuário HTTP e/ou Telnet/SSH, que é configurável a partir da AAA Advanced > AAA Interface guia ainda da página da GUI WLC acessível em <https://<WLC-IP>/webui/#/aaa>, como mostrado nesta imagem:



CLI para autenticação de GUI:

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

radius-auth-method

WLC-9800(config)#ip http authentication aaa exec-authorization

radius-auth-method

CLI para autenticação Telnet/SSH:

```
<#root>
```

```
WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication
```

```
radius-auth-method
```

```
WLC-9800(config-line)#authorization exec
```

```
radius-auth-method
```

Observe que quando são feitas alterações nas configurações HTTP, é melhor reiniciar os serviços HTTP e HTTPS. Isso pode ser obtido com estes comandos:

```
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server
```

Configurar ISE para RADIUS

Etapa 1. Configure a WLC como um dispositivo de rede para o RADIUS.

Da GUI:

Para declarar a WLC usada na seção anterior como um dispositivo de rede para o RADIUS no ISE, navegue até Administration > Network Resources > Network Devices e abra a guia Network devices (Dispositivos de rede), conforme mostrado na imagem a seguir.

Network Devices

- Network Device Groups
- Network Device Profiles
- External RADIUS Servers
- RADIUS Server Sequences
- More

Network Devices

- Default Device
- Device Security Settings

Network Devices

Selected 0 Total 1

- Edit
- Add**
- Duplicate
- Import
- Export
- Generate PAC
- Delete

| <input type="checkbox"/> | Name | IP/Mask | Profile Name | Location | Type | Description |
|--------------------------|----------|-----------------|--------------|---------------|------------------|-------------|
| <input type="checkbox"/> | WLC-9800 | 10.48.39.133/32 | Cisco | All Locations | All Device Types | |

Para adicionar um dispositivo de rede, use o botão Add (Adicionar), que abre o formulário de configuração do novo dispositivo de rede.

Network Devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

Name Description IP Address Device Profile Model Name Software Version

Network Device Group

Location [Set To Default](#)IPSEC [Set To Default](#)Device Type [Set To Default](#) RADIUS Authentication Settings

RADIUS UDP Settings

Protocol Shared Secret [Show](#) Use Second Shared Secret [?](#)Second Shared Secret [Show](#)CoA Port [Set To Default](#)RADIUS DTLS Settings [?](#) DTLS Required [?](#)Shared Secret [?](#)

Na nova janela, forneça um nome para o dispositivo de rede e adicione seu endereço IP. Escolha as Configurações de Autenticação RADIUS e configure o mesmo Segredo Compartilhado RADIUS que o usado no WLC.

Etapa 2. Crie um resultado de autorização para retornar o privilégio.

Da GUI:

Para ter direitos de acesso de administrador, o adminuser precisa ter um nível de privilégio de 15, que permite acessar o shell de prompt exec. Por outro lado, o helpdeskuser não precisa de acesso ao shell de prompt de exec e, portanto, pode ser atribuído com um nível de privilégio inferior a 15. Para atribuir o nível de privilégio adequado aos usuários, os perfis de autorização podem ser usados. Eles podem ser configurados no ISE GUI Page Policy > Policy Elements > Results, na guia Authorization > Authorization Profiles mostrada na imagem a seguir.

- Authentication
- Authorization
- Authorization Profiles**
- Downloadable ACLs
- Profiling
- Posture
- Client Provisioning

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 Total 11

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

All

| <input type="checkbox"/> | Name | Profile | Description |
|--------------------------|------------------------|---------|---|
| <input type="checkbox"/> | 9800-admin-priv | Cisco | |
| <input type="checkbox"/> | 9800-helpdesk-priv | Cisco | |
| <input type="checkbox"/> | Block_Wireless_Access | Cisco | Default profile used to block wireless devices. Ensure ti |
| <input type="checkbox"/> | Cisco_IP_Phones | Cisco | Default profile used for Cisco Phones. |
| <input type="checkbox"/> | Cisco_Temporal_Onboard | Cisco | Onboard the device with Cisco temporal agent |
| <input type="checkbox"/> | Cisco_WebAuth | Cisco | Default Profile used to redirect users to the CWA portal |
| <input type="checkbox"/> | NSP_Onboard | Cisco | Onboard the device with Native Supplicant Provisioning |
| <input type="checkbox"/> | Non_Cisco_IP_Phones | Cisco | Default Profile used for Non Cisco Phones. |
| <input type="checkbox"/> | UDN | Cisco | Default profile used for UDN. |
| <input type="checkbox"/> | DenyAccess | Cisco | Default Profile with access type as Access-Reject |

Para configurar um novo perfil de autorização, use o botão Adicionar, que abre o formulário de configuração do novo perfil de autorização. Este formulário deve ser especialmente semelhante a este para configurar o perfil atribuído ao adminuser.

Dictionary Conditions Results

Authentication > Authorization Profiles > New Authorization Profile

Authorization Profile

* Name 9800-admin-priv

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

> Common Tasks

Advanced Attributes Settings

Cisco:cisco-av-pair = shell:priv-lvl=15

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:priv-lvl=15

Submit Cancel

A configuração mostrou que o concede o nível de privilégio 15 a qualquer usuário ao qual ele esteja associado. Como mencionado anteriormente, esse é o comportamento esperado para o adminuser que é criado durante a próxima etapa. No entanto, o helpdeskuser deve ter um nível de privilégio inferior e, portanto, um segundo elemento de política deve ser criado.

O elemento de política para o helpdeskuser é semelhante ao criado logo acima, exceto que a string shell:priv-lvl=15 deve ser alterada para shell:priv-lvl=X e substituir X pelo nível de privilégio desejado. Neste exemplo, 1 é usado.

Etapa 3. Crie grupos de usuários no ISE.

Na GUI:

Os grupos de usuários do ISE são criados na guia User Identity Groups do Administration > Identity Management > Groups GUI Page, que é mostrada na captura de tela.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is Administration > Identity Management. The left sidebar has 'Groups' selected. The main content area is titled 'User Identity Groups' and shows a table of existing groups. The '+ Add' button is highlighted with a red box.

| Name | Description |
|---------------------------------|---|
| helpdesk-group | This is the group containing all users with read-only privileges. |
| admin-group | This is the group containing all users with administrator privileges. |
| OWN_ACCOUNTS (default) | Default OWN_ACCOUNTS (default) User Group |
| GuestType_Weekly (default) | Identity group mirroring the guest type |
| GuestType_SocialLogin (default) | Identity group mirroring the guest type |
| GuestType_Daily (default) | Identity group mirroring the guest type |
| GuestType_Contractor (default) | Identity group mirroring the guest type |
| GROUP_ACCOUNTS (default) | Default GROUP_ACCOUNTS (default) User Group |
| Employee | Default Employee User Group |
| ALL_ACCOUNTS (default) | Default ALL_ACCOUNTS (default) User Group |

Para criar um novo usuário, use o botão Adicionar, que abre o formulário de configuração de grupo de identidade do novo usuário, conforme mostrado.

The screenshot shows the 'New User Identity Group' form in the Cisco ISE Administration interface. The breadcrumb trail is Administration > Identity Management > User Identity Groups > New User Identity Group. The form has a 'Name' field containing 'admin-group' and a 'Description' field containing 'This is the group containing all users with administrator privileges.' The 'Name' field is highlighted with a red box. There are 'Submit' and 'Cancel' buttons at the bottom.

Forneça o nome do grupo criado. Crie os dois grupos de usuários discutidos acima, ou seja, o admin-group e helpdesk-group.

Etapa 4. Crie usuários no ISE.

Na GUI:

Os usuários do ISE são criados na guia Usuários do Administration > Identity Management > Identities GUI Page, exibida na captura de tela.

Users

Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

Edit **+ Add** Change Status Import Export Delete Duplicate

All

| Status | Username | Description | First Name | Last Name | Email Address | User Identity Groups | Admin |
|--------------------------|----------|---------------|------------|-----------|---------------|----------------------|-------|
| <input type="checkbox"/> | Enabled | adminuser | | | | admin-group | |
| <input type="checkbox"/> | Enabled | helpdeskus... | | | | helpdesk-group | |

Para criar um novo usuário, use o botão Add (Adicionar) para abrir o formulário de configuração do novo usuário de acesso à rede, conforme mostrado.

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username **adminuser**

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration
Password will expire in 60 days

Never Expires

Password Re-Enter Password

* Login Password Generate Password

Enable Password Generate Password

> User Information

> Account Options

> Account Disable Policy

User Groups

admin-group

Forneça as credenciais aos usuários, ou seja, seu nome de usuário e senha, que são os usados para autenticação no WLC. Além disso, certifique-se de que o Status do usuário seja Enabled. Por fim, adicione o usuário ao seu grupo relacionado, que foi criado na Etapa 4., com o menu suspenso User Groups (Grupos de usuários) no final do formulário.

Crie os dois usuários discutidos acima, ou seja, o adminuser e helpdeskuser.

Etapa 5. Autentique os usuários.

Da GUI:

Neste cenário, a política de autenticação dos conjuntos de políticas padrão do ISE, que já está pré-configurada, permite o acesso padrão à rede. Esse conjunto de políticas pode ser visto na página Policy > Policy Sets da GUI do ISE, como mostrado nesta imagem. Por isso, não há necessidade de alterá-lo.

Policy Sets → Default

Reset

Reset Policyset Hitcounts

Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|--------|-----------------|--------------------|------------|-------------------------------------|------|
| ✓ | Default | Default policy set | | Default Network Access | 0 |

Authentication Policy (3)

| Status | Rule Name | Conditions | Use | Hits | Actions |
|--------|-----------|---------------------------------------|---------------------------------|------|---------|
| ✓ | MAB | OR Wired_MAB Wireless_MAB | Internal Endpoints > Options | 0 | ⚙️ |
| ✓ | Dot1X | OR Wired_802.1X Wireless_802.1X | All_User_ID_Stores > Options | 0 | ⚙️ |
| ✓ | Default | | All_User_ID_Stores > Options | 0 | ⚙️ |

Etapa 6. Autorize os usuários.

Da GUI:

Depois que o log in tenta passar pela política de autenticação, ele precisa ser autorizado e o ISE precisa retornar o perfil de autorização criado anteriormente (permitir aceitação, junto com o nível de privilégio).

Neste exemplo, as tentativas de login são filtradas com base no endereço IP do dispositivo (que é o endereço IP da WLC) e distinguem o nível de privilégio a ser concedido com base no grupo ao qual o usuário pertence. Outra abordagem válida é filtrar usuários com base em seus nomes de usuário, já que cada grupo contém apenas um único usuário neste exemplo.

Policy Sets → Default

Reset Reset Policyset Hitcounts Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|--------|-----------------|--------------------|------------|-------------------------------------|------|
| ✓ | Default | Default policy set | | Default Network Access | 152 |

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions (2)

| Status | Rule Name | Conditions | Results | | Hits | Actions |
|--------|---------------------|--|--------------------|------------------|------|---------|
| | | | Profiles | Security Groups | | |
| ✓ | 9800 Helpdesk Users | AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group | 9800-helpdesk-priv | Select from list | 1 | ⚙️ |
| ✓ | 9800 Admin Users | AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group | 9800-admin-priv | Select from list | 2 | ⚙️ |

> Authorization Policy (12)

Reset Save

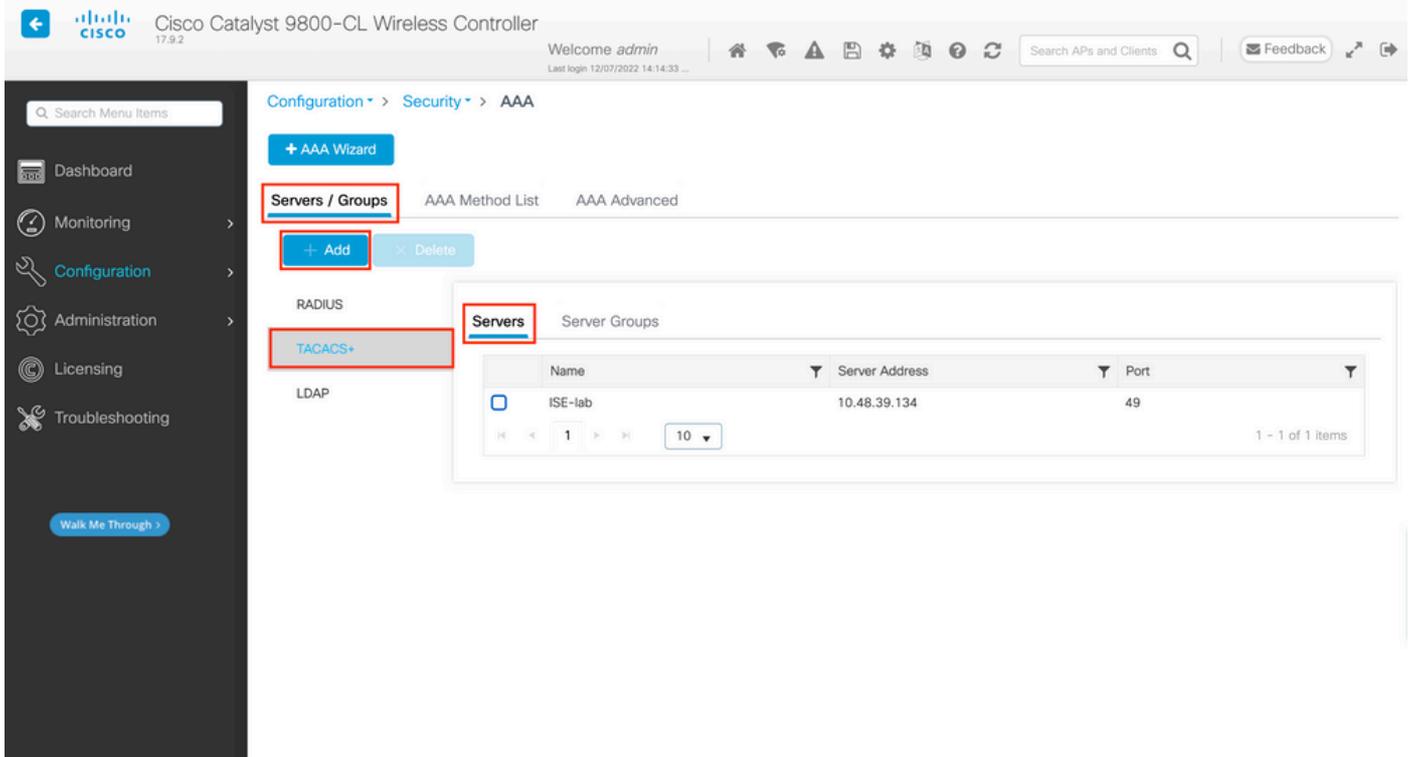
Depois que essa etapa for concluída, as credenciais configuradas para adminuser e helpdesk usuário podem ser usadas para autenticar na WLC através da GUI ou através de Telnet/SSH.

Configurar TACACS+ WLC

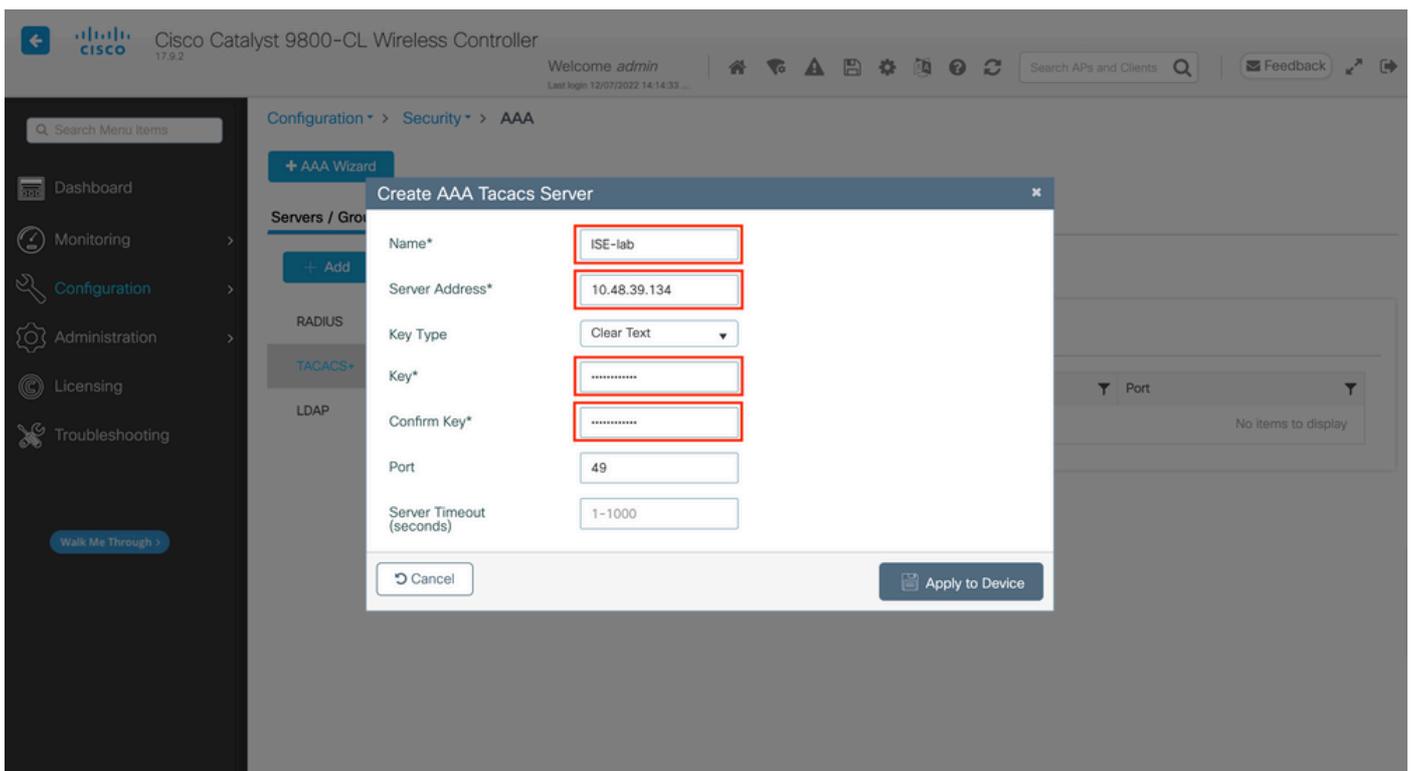
Etapa 1. Declare o servidor TACACS+.

Da GUI:

Primeiro de tudo, crie o servidor Tacacs+ ISE no WLC. Isso pode ser feito a partir da guia Servers/Groups > TACACS+ > Servers da página GUI WLC acessível no <https://<WLC-IP>/webui/#/aaa> ou se você navegar para [Configuration > Security > AAA](#), como mostrado nesta [imagem](#).



Para adicionar um servidor TACACS na WLC, clique no botão Add (Adicionar) emoldurado em vermelho na imagem acima. Isso abre a janela pop-up descrita.



Quando a janela pop-up abrir, forneça o nome do servidor (ele não precisa corresponder ao nome do sistema ISE), seu endereço IP, a chave compartilhada, a porta usada e o tempo limite.

Nessa janela pop-up, você deve fornecer:

- O nome do servidor (observe que ele não precisa corresponder ao nome do sistema ISE)

- O endereço IP do servidor
- O segredo compartilhado entre o WLC e o servidor TACACS+

Outros parâmetros podem ser configurados, como as portas usadas para autenticação e contabilização, mas eles não são obrigatórios e são deixados como padrão para esta documentação.

Do CLI:

```
<#root>
```

```
WLC-9800(config)#tacacs server
```

```
ISE-1ab
```

```
WLC-9800(config-server-tacacs)#address ipv4
```

```
10.48.39.134
```

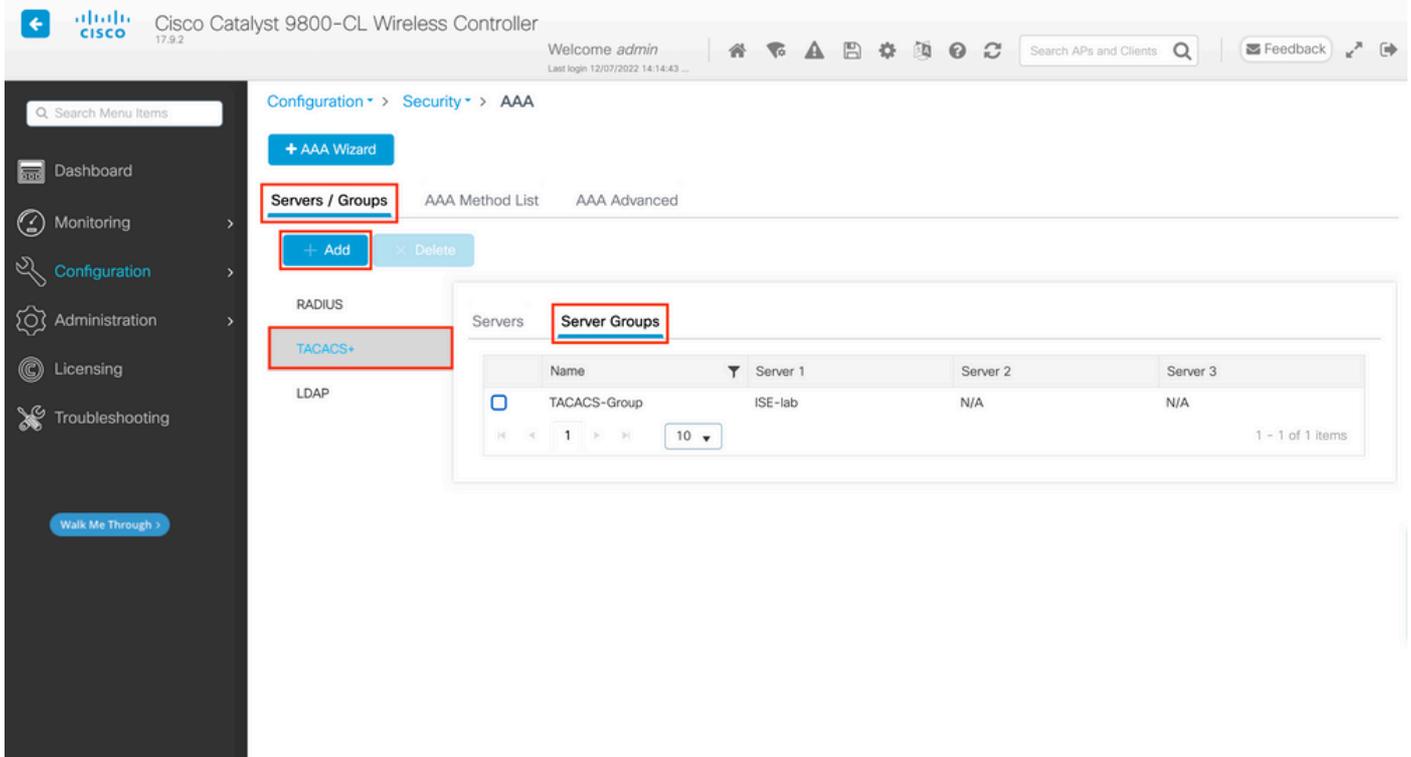
```
WLC-9800(config-server-tacacs)#key
```

```
Cisco123
```

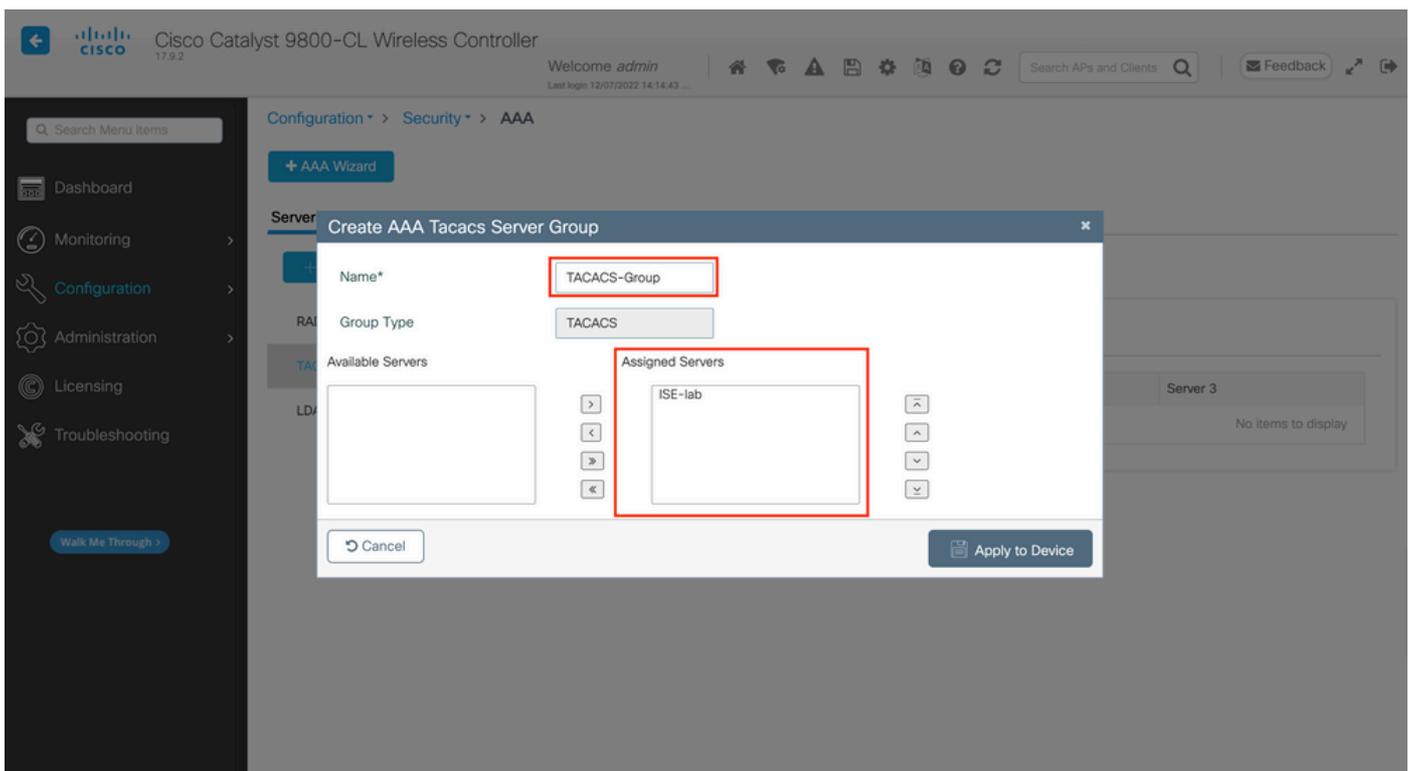
Etapa 2. Mapeie o servidor TACACS+ para um grupo de servidores.

Da GUI:

Caso você tenha vários servidores TACACS+ que possam ser usados para autenticação, é recomendável mapear todos esses servidores para o mesmo grupo de servidores. A WLC então cuida do balanceamento de carga de diferentes autenticações entre os servidores no grupo de servidores. Os grupos de servidores TACACS+ são configurados na guia Servers/Groups > TACACS > Server Groups da mesma página da GUI que a mencionada na Etapa 1., que é mostrada na imagem.



Quanto à criação do servidor, uma janela pop-up aparece quando você clica no botão Adicionar enquadrado na imagem anterior, que é representada na imagem.



Na janela pop-up, dê um nome ao grupo e mova os servidores desejados para a lista Servidores atribuídos.

Do CLI:

<#root>

WLC-9800(config)#aaa group server tacacs+

TACACS-Group

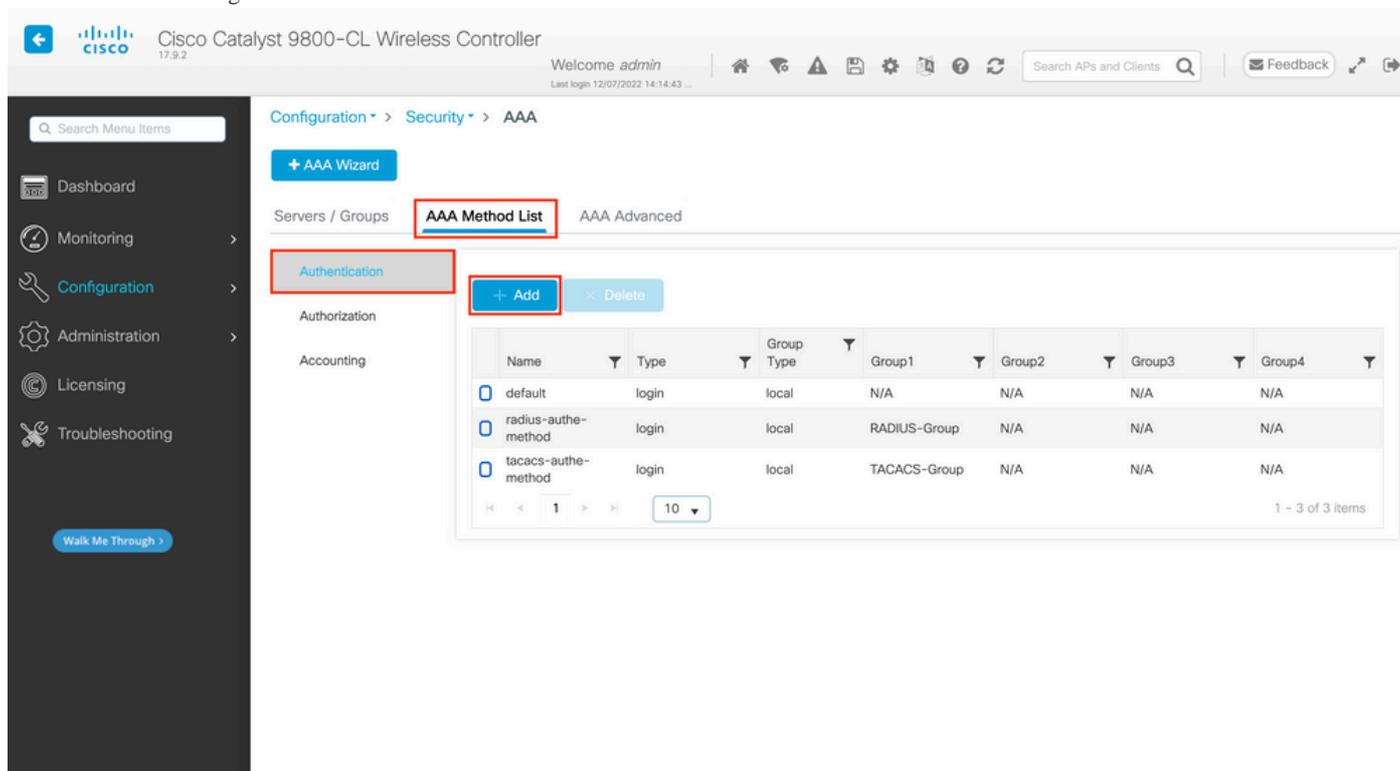
WLC-9800(config-sg-tacacs+)#server name

ISE-lab

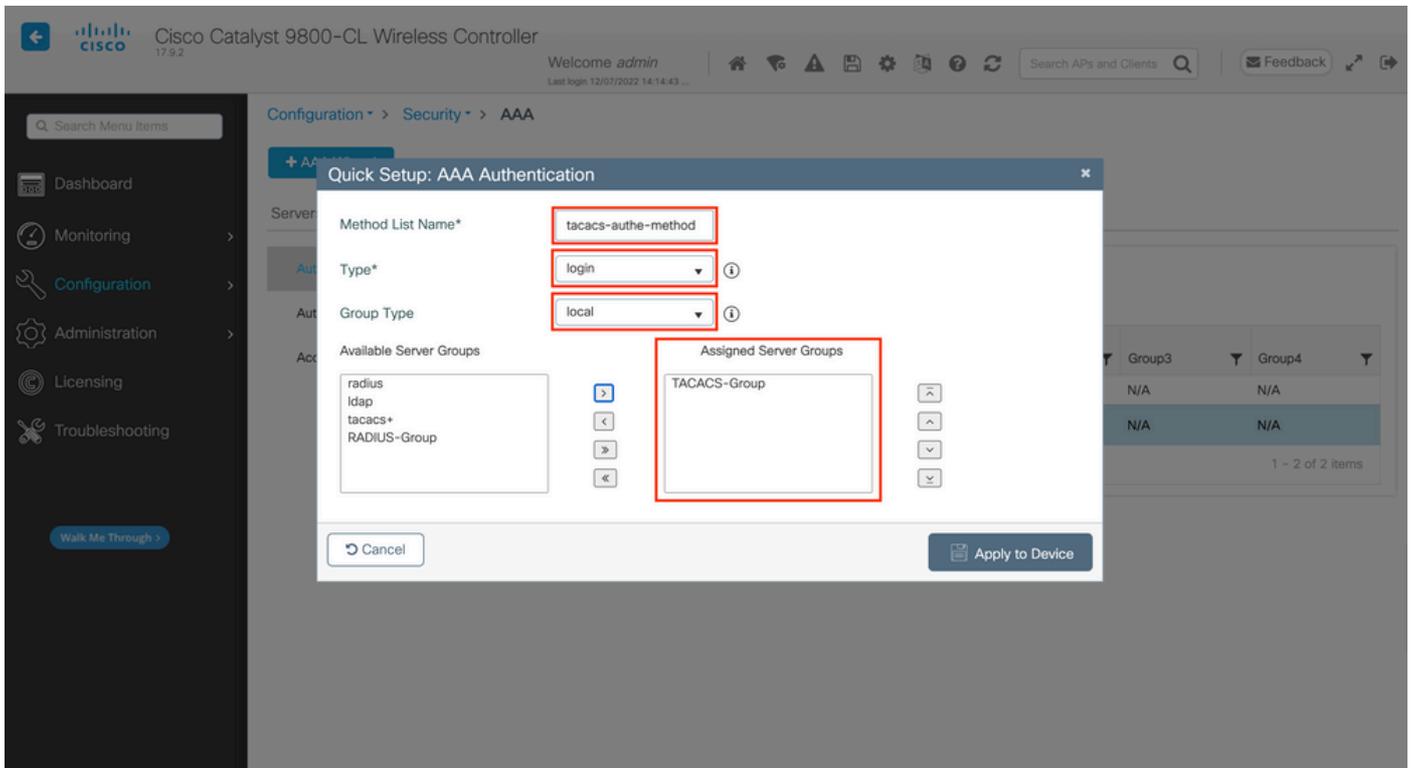
Etapa 3. Crie um método de login de autenticação AAA que aponte para o grupo de servidores TACACS+.

Da GUI:

Ainda na página <https://<WLC-IP>/webui/#/aaa> GUI, navegue até a guia AAA Method List > Authentication e crie um método de autenticação como mostrado na imagem.



Como de costume, quando você usa o botão Adicionar para criar um método de autenticação, uma janela pop-up de configuração é exibida, semelhante àquela descrita nesta imagem.



Nessa janela pop-up, forneça um nome para o método, escolha Digitar como login e adicione o servidor de grupo criado na etapa anterior à lista Grupos de servidores atribuídos. Com relação ao campo Tipo de grupo, várias configurações são possíveis.

- Se você escolher Tipo de grupo como local, a WLC primeiro verifica se as credenciais do usuário existem localmente e depois volta para o grupo de servidores.
- Se você escolher o Tipo de grupo como um grupo e não marcar a opção Fall back to local, a WLC simplesmente verificará as credenciais do usuário em relação ao grupo de servidores.
- Se você escolher o Tipo de grupo como um grupo e marcar a opção Fallback to local, o WLC verificará as credenciais do usuário em relação ao grupo de servidores e consultará o banco de dados local somente se o servidor não responder. Se o servidor enviar uma rejeição, o usuário será autenticado, mesmo que possa existir no banco de dados local.

Do CLI:

Se quiser que as credenciais do usuário sejam verificadas com um grupo de servidores somente se não forem localmente primeiro, use:

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
tacacs-auth-method
```

local group

TACACS-Group

Se quiser que as credenciais do usuário sejam verificadas apenas com um grupo de servidores, use:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

Se quiser que as credenciais do usuário sejam verificadas com um grupo de servidores e se este último não responder com uma entrada local, use:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

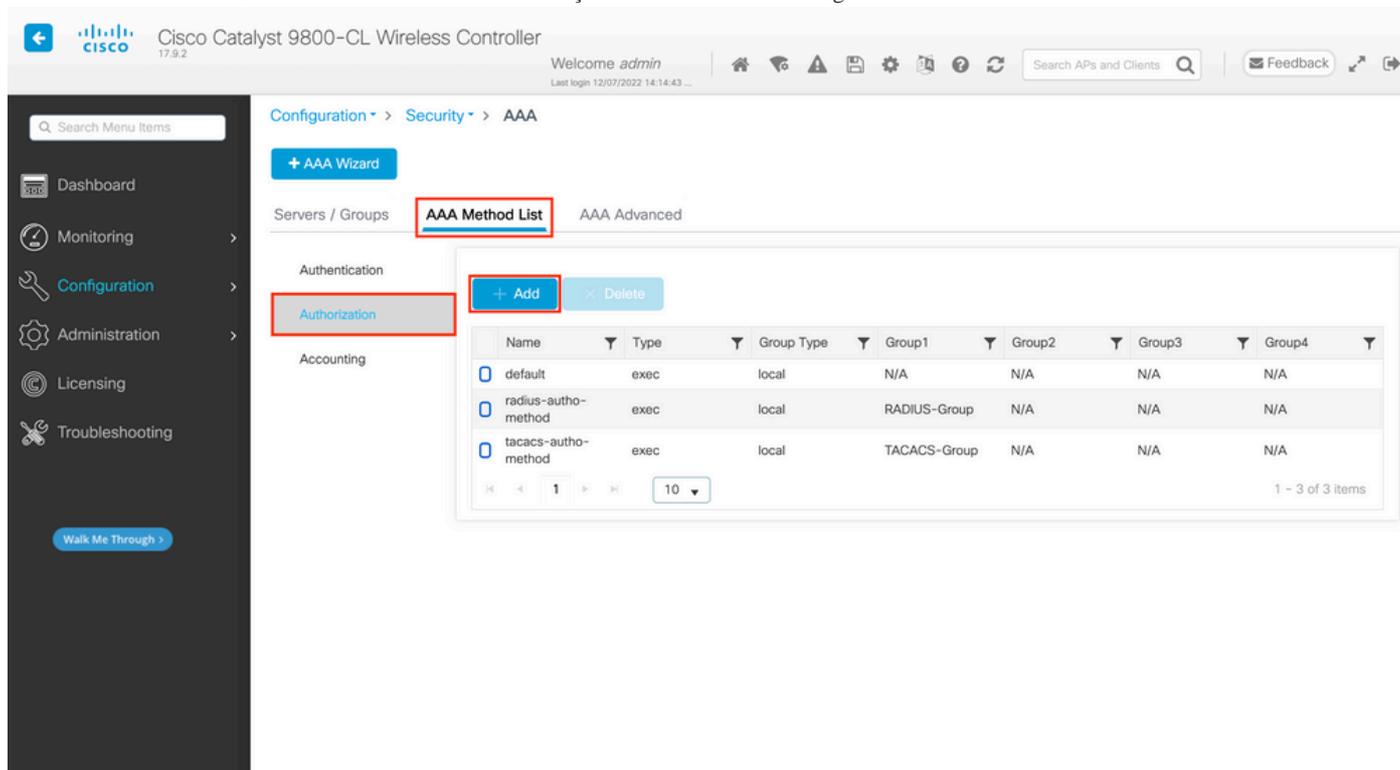
local

Neste exemplo de configuração, há alguns usuários que são criados apenas localmente, e alguns usuários apenas no servidor ISE, portanto, faça uso da primeira opção.

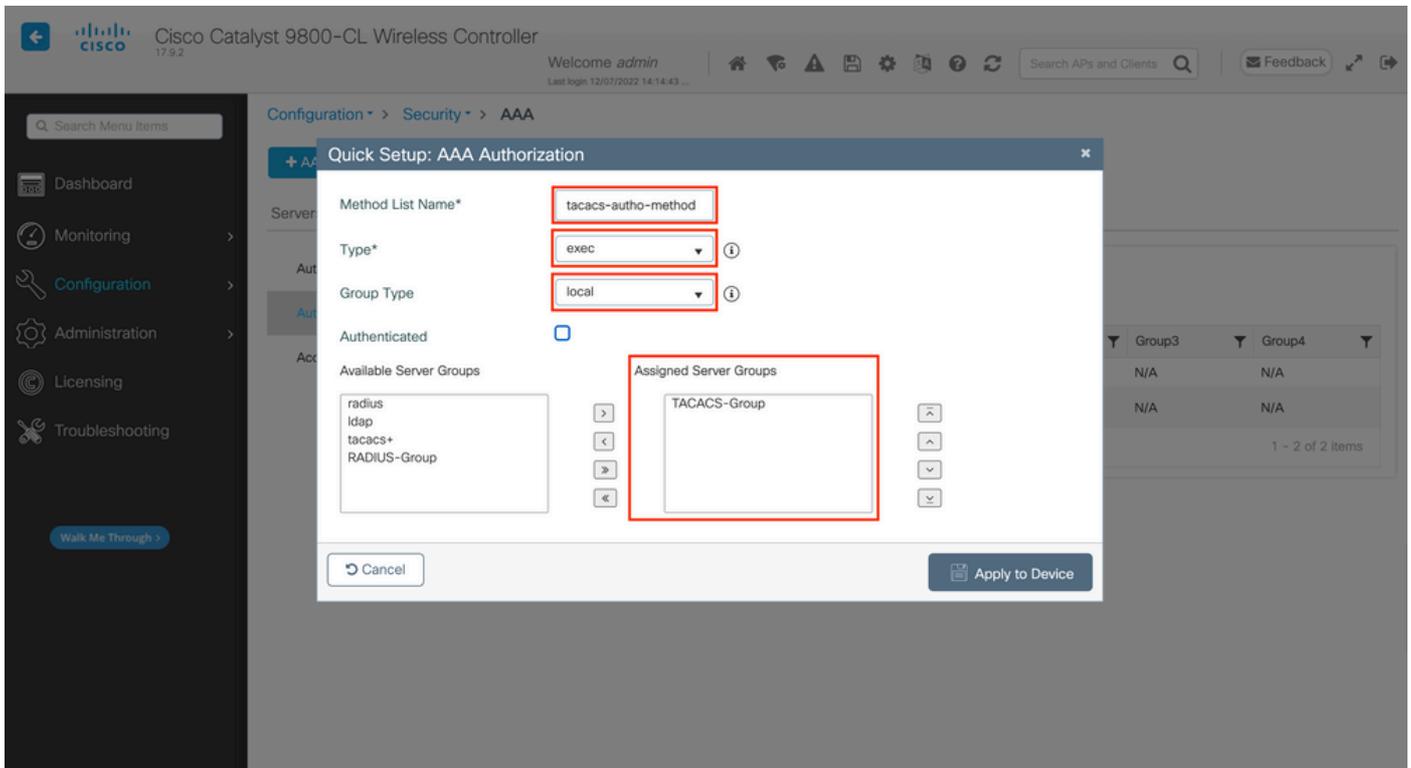
Etapa 4. Crie um método de execução de autorização AAA que aponte para o grupo de servidores TACACS+.

Da GUI:

O usuário também precisa ser autorizado para receber acesso. Ainda na página GUI, Configuration > Security > AAA navegue até a guia AAA Method List > Authorization e crie um método de autorização como mostrado na imagem.



Um pop-up de configuração de método de autorização semelhante ao descrito é exibido quando você adiciona um novo com o botão Adicionar.



Nessa janela pop-up de configuração, forneça um nome para o método de autorização, escolha Tipo como exec e use a mesma ordem de Tipo de grupo que a usada para o método de autenticação na etapa anterior.

Do CLI:

```
<#root>
```

```
WLC-9800(config)#aaa authorization exec
```

```
tacacs-autho-method
```

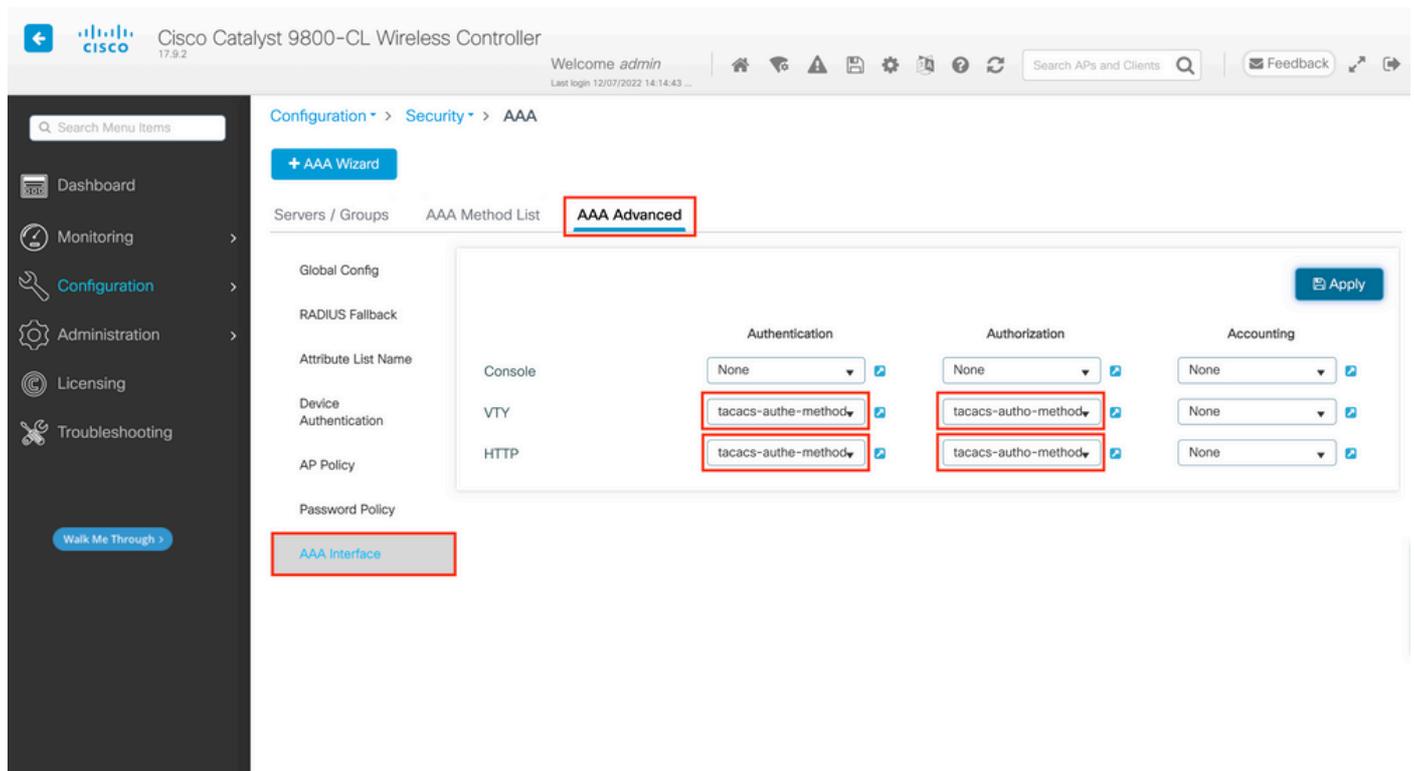
```
local group
```

```
TACACS-Group
```

Etapa 5. Atribua os métodos às configurações HTTP e às linhas VTY usadas para Telnet/SSH.

Da GUI:

Os métodos de autenticação e autorização criados podem ser usados para conexão de usuário HTTP e/ou Telnet/SSH, que é configurável a partir da AAA Advanced > AAA Interface guia ainda da página WLC da GUI acessível no <https://<WLC-IP>/webui/#/aaa>, como mostrado na imagem.



Do CLI:

Para a autenticação da GUI:

```
<#root>
```

```
WLC-9800(config)#ip http authentication aaa login-authentication
```

```
tacacs-auth-method
```

```
WLC-9800(config)#ip http authentication aaa exec-authorization
```

```
tacacs-auth-method
```

Para autenticação Telnet/SSH:

```
<#root>
```

```
WLC-9800(config)#line vty 0 15  
WLC-9800(config-line)#login authentication
```

```
tacacs-auth-method
```

```
WLC-9800(config-line)#authorization exec
```

```
tacacs-auth-method
```

Observe que quando são feitas alterações nas configurações HTTP, é melhor reiniciar os serviços HTTP e HTTPS. Isso pode ser obtido com esses comandos.

```
WLC-9800(config)#no ip http server  
WLC-9800(config)#no ip http secure-server  
WLC-9800(config)#ip http server  
WLC-9800(config)#ip http secure-server
```

Configuração do TACACS+ ISE

Etapa 1. Configure a WLC como um dispositivo de rede para TACACS+.

Da GUI:

Para declarar a WLC usada na seção anterior como um dispositivo de rede para o RADIUS no ISE, navegue até Administration > Network Resources > Network Devices e abra a guia Network devices (Dispositivos de rede), conforme mostrado nesta imagem.

The screenshot shows the Cisco ISE Administration interface. At the top, the breadcrumb is "Administration · Network Resources". The main navigation bar includes "Network Devices", "Network Device Groups", "Network Device Profiles", "External RADIUS Servers", "RADIUS Server Sequences", and "More". The left sidebar has "Network Devices", "Default Device", and "Device Security Settings". The main content area is titled "Network Devices" and shows a table with one device selected:

| <input type="checkbox"/> | Name | IP/Mask | Profile Name | Location | Type | Description |
|-------------------------------------|----------|--------------|--------------|---------------|------------------|-------------|
| <input checked="" type="checkbox"/> | WLC-9800 | 10.48.39.... | Cisco | All Locations | All Device Types | |

Buttons for "Edit", "Add", "Duplicate", "Import", "Export", "Generate PAC", and "Delete" are visible above the table. The "Edit" button and the checkbox for the selected device are highlighted with red boxes.

Neste exemplo, a WLC já foi adicionada para a autenticação RADIUS (consulte a Etapa 1 da seção [Configurar RADIUS ISE](#)). Portanto, sua configuração simplesmente precisa ser modificada para configurar a autenticação TACACS, que pode ser feita quando você escolhe a WLC na lista de dispositivos de rede e clica no botão Editar. Isso abre o formulário de configuração do dispositivo de rede como mostrado nesta imagem.

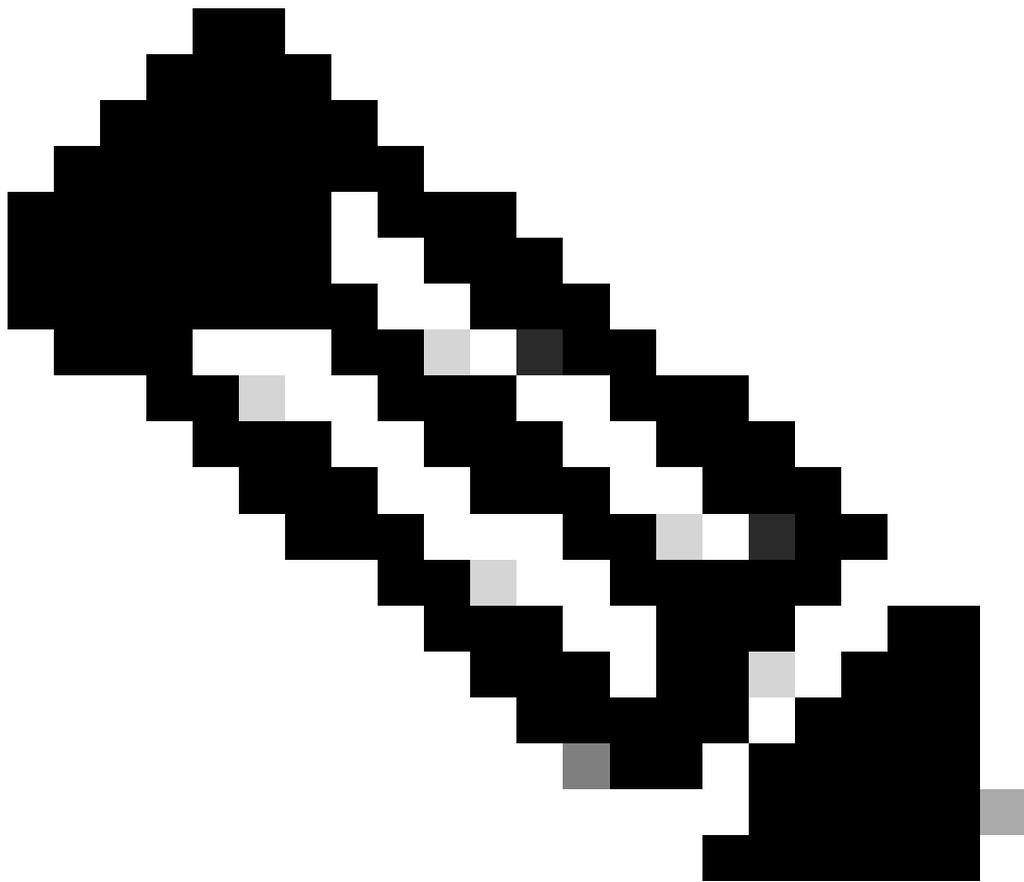
The screenshot shows the configuration page for the selected device. The breadcrumb is "Administration · Network Resources". The main navigation bar is the same as in the previous image. The left sidebar is the same. The main content area is titled "General Settings" and includes the following sections:

- Enable KeyWrap
- Key Encryption Key Show
- Message Authenticator Code Key Show
- Key Input Format: ASCII HEXADECIMAL
- TACACS Authentication Settings
 - Shared Secret Show
- Enable Single Connect Mode
 - Legacy Cisco Device
 - TACACS Draft Compliance Single Connect Support
- SNMP Settings
- Advanced TrustSec Settings

The "TACACS Authentication Settings" section is expanded, and the "Shared Secret" field is highlighted with a red box.

Depois que a nova janela for aberta, role para baixo até a seção Configurações de autenticação TACACS, habilite essas configurações e adicione o segredo compartilhado inserido durante a Etapa 1 da seção [Configurar TACACS+ WLC](#).

Etapa 2. Ative o recurso Device Admin para o nó.



Observação: para usar o ISE como o servidor TACACS+, você deve ter um pacote de licença de Administração de dispositivo e uma licença Base ou Mobility.

Da GUI:

Depois que as licenças de Administração do dispositivo estiverem instaladas, você deve habilitar o recurso Administrador do dispositivo para o nó para poder usar o ISE como o servidor TACACS+. Para fazer isso, edite a configuração do nó de implantação do ISE usado, que pode ser encontrado em Administrator > Deployment, e clique em seu nome ou faça isso com a ajuda do Edit botão.

Deployment

- Deployment
- PAN Failover

Deployment Nodes

Selected 0 Total 1

Edit Register Syncup Deregister

| <input type="checkbox"/> | Hostname | Personas | Role(s) | Services | Node Status |
|--------------------------|----------|--|-------------|------------------|-------------------------------------|
| <input type="checkbox"/> | ise | Administration, Monitoring, Policy Service | STANDALO... | SESSION,PROFILER | <input checked="" type="checkbox"/> |

Quando a janela de configuração do nó for aberta, marque a opção Enable Device Admin Service na seção Policy Service, como mostrado nesta imagem.

Deployment

Deployment Nodes List > ise

Edit Node

General Settings Profiling Configuration

Hostname **ise**

FQDN **ise.cisco.com**

IP Address **10.48.39.134**

Node Type **Identity Services Engine (ISE)**

Role **STANDALONE** [Make Primary](#)

Administration

Monitoring

Role **PRIMARY**

Other Monitoring Node _____

Dedicated MnT ⓘ

Policy Service

Enable Session Services ⓘ

Include Node in Node Group **None**

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

pxGrid ⓘ

[Reset](#) [Save](#)

Etapa 3. Crie perfis TACACS para retornar o privilégio.

Da GUI:

Para ter direitos de acesso de administrador, o adminuser precisa ter um nível de privilégio de 15, que permite acessar o shell de prompt exec. Por outro lado, o helpdeskuser não precisa de acesso ao shell de prompt de exec e, portanto, pode ser atribuído com um nível de privilégio inferior a 15. Para atribuir o nível de privilégio adequado aos usuários, os perfis de autorização podem ser usados. Eles podem ser configurados na página Work Centers > Device Administration > Policy Elements da GUI do ISE, na guia Results > TACACS Profiles, como mostrado na imagem a seguir.

- Conditions
 - Library Conditions
 - Smart Conditions
- Network Conditions
- Results
 - Allowed Protocols
 - TACACS Command Sets
 - TACACS Profiles**

TACACS Profiles

Rows/Page 6 << 1 >> Go 6 Total Rows

Add Duplicate Trash Edit

| <input type="checkbox"/> | Name | Type | Description |
|--------------------------|------------------------|-------|---|
| <input type="checkbox"/> | Default Shell Profile | Shell | Default Shell Profile |
| <input type="checkbox"/> | Deny All Shell Profile | Shell | Deny All Shell Profile |
| <input type="checkbox"/> | IOS Admin | Shell | Assigned to each user in the group admin-group |
| <input type="checkbox"/> | IOS Helpdesk | Shell | Assigned to each user in the group helpdesk-group |
| <input type="checkbox"/> | WLC ALL | WLC | WLC ALL |
| <input type="checkbox"/> | WLC MONITOR | WLC | WLC MONITOR |

Para configurar um novo perfil TACACS, use o botão Add (Adicionar), que abre o formulário de configuração do novo perfil semelhante ao mostrado na imagem. Este formulário deve ser especialmente semelhante a este para configurar o perfil atribuído ao adminuser (ou seja, com privilégios de shell de nível 15).

Cisco ISE Work Centers - Device Administration Evaluation Mode 82 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets More

TACACS Profiles > IOS Admin
TACACS Profile

Name: **IOS Admin**

Description: Assigned to each user in the group admin-group

Task Attribute View Raw View

Common Tasks

Common Task Type: **Shell**

Default Privilege 15 (Select 0 to 15)

Maximum Privilege 15 (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

Custom Attributes

Add Trash Edit

| Type | Name | Value |
|----------------|------|-------|
| No data found. | | |

Cancel Save

Repita a operação para o perfilhelpdesk. Para este último, o Privilégio Padrão, assim como o Privilégio Máximo, são definidos como 1.

Etapa 4. Crie grupos de usuários no ISE.

Isso é o mesmo apresentado na Etapa 3 da seção [Configure RADIUS ISE](#) deste documento.

Etapa 5. Crie os usuários no ISE.

Isso é o mesmo apresentado na Etapa 4 da seção [Configurar ISE RADIUS](#) deste documento.

Etapa 6. Crie um Conjunto de Políticas Administrativas do Dispositivo.

Da GUI:

Quanto ao acesso RADIUS, uma vez que os usuários são criados, suas políticas de autenticação e autorização ainda precisam ser definidas no ISE para conceder a eles os direitos de acesso apropriados. A autenticação TACACS usa os Device Admin Policy Sets para esse fim, que podem ser configurados a partir do Work Centers > Device Administration > Device Admin Policy Sets GUI Page como mostrado.

Policy Sets

Reset [Reset Policyset Hitcounts](#) [Save](#)

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|---|---------------------------|---------------------------|--|--|------|---|---|
|  | | | | | | | |
|  | Search | | | | | | |
|  | WLC TACACS Authentication | |  Network Access-Device IP Address EQUALS 10.48.39.133 | Default Device Admin    | 0 |  |  |
|  | Default | Tacacs Default policy set | | Default Device Admin    | 0 |  |  |

[Reset](#) [Save](#)

Para criar um conjunto de políticas de administração de dispositivos, use o botão adicionar com quadros em vermelho na imagem anterior. Isso adiciona um item à lista de conjuntos de políticas. Forneça um nome para o conjunto recém-criado, uma condição sob a qual ele deve ser aplicado e a Sequência de Protocolos/Servidor Permitidos (aqui, o Default Device Admin é suficiente). Use o botão Save para finalizar a adição do conjunto de políticas e use a ponta de seta à sua direita para acessar sua página de configuração, como ela se parece na ilustrada.

Policy Sets → **WLC TACACS Authentication**

Reset

Reset Policyset Hitcounts

Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|--------|---------------------------|-------------|--|-------------------------------------|------|
| ✓ | WLC TACACS Authentication | | Network Access-Device IP Address EQUALS 10.48.39.133 | Default Device Admin | 0 |

Authentication Policy (1)

| Status | Rule Name | Conditions | Use | Hits | Actions |
|--------|-----------|------------|---------------------------------|------|---------|
| ✓ | Default | | All_User_ID_Stores > Options | 0 | |

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

| Status | Rule Name | Conditions | Results | | | Hits | Actions |
|--------|------------------------------|---|------------------|------------------------|---|------|---------|
| | | | Command Sets | Shell Profiles | | | |
| ✓ | Helpdesk users authorization | InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group | AllowAllCommands | IOS Helpdesk | 0 | | |
| ✓ | Admin users authorization | InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group | AllowAllCommands | IOS Admin | 0 | | |
| ✓ | Default | | DenyAllCommands | Deny All Shell Profile | 0 | | |

Reset

Save

O conjunto de políticas específico 'WLC TACACS Authentication' neste exemplo filtra solicitações com o endereço IP igual ao endereço IP da WLC C9800 do exemplo.

Como uma política de autenticação, a regra padrão foi deixada, pois atende às necessidades do caso de uso. Foram criadas duas regras de autorização:

- O primeiro é acionado quando o usuário pertence ao grupo definido admin-group. Ele permite todos os comandos (por meio da regra padrão Permit_all) e atribui o privilégio 15 (por meio do perfil TACACS definido IOS_Admin).
- O segundo é acionado quando o usuário pertence ao grupo definido helpdesk-group. Permite todos os comandos (através da Permit_all regra padrão) e atribui o privilégio 1 (através do perfil TACACS definido IOS_Helpdesk).

Após esta etapa ser concluída, as credenciais configuradas para adminuser e helpdesk usuários podem ser usadas para autenticar na WLC através

da GUI ou com Telnet/SSH.

Troubleshooting

Se o servidor RADIUS espera que o atributo service-type RADIUS seja enviado, você pode adicionar na WLC :

```
radius-server attribute 6 on-for-login-auth
```

Solucionar problemas de acesso RADIUS/TACACS+ de GUI ou CLI de WLC via CLI de WLC

Para solucionar problemas de acesso TACACS+ à GUI ou CLI da WLC, emita o debug tacacs comando, juntamente com terminal monitor um e veja a saída ao vivo quando uma tentativa de login é feita.

Por exemplo, um login bem-sucedido seguido por um logout do adminuser usuário gera essa saída.

```
<#root>
```

```
WLC-9800#
```

```
terminal monitor
```

```
WLC-9800#
```

```
debug tacacs
```

```
TACACS access control debugging is on
```

```
WLC-9800#
```

```
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
```

```
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

Pode ser visto nesses logs que o servidor TACACS+ retorna o privilégio correto (que é AV priv-lvl=15).

Quando você faz a autenticação RADIUS, uma saída de depuração semelhante é mostrada, que diz respeito ao tráfego RADIUS.

Os comandos debug aaa authentication e debug aaa authorization, em vez disso, mostram qual lista de métodos é escolhida pela WLC quando o

usuário tenta fazer login.

Solucionar problemas de acesso TACACS+ de GUI ou CLI de WLC através da GUI do ISE

Na página Operations > TACACS > Live Logs, cada autenticação de usuário feita com o TACACS+ até as últimas 24 horas pode ser visualizada. Para expandir os detalhes de uma autorização ou autenticação TACACS+, use o botão Detalhes relacionado a este evento.

The screenshot shows the Cisco ISE interface for Live Logs. The page title is "Operations · TACACS". The "Live Logs" tab is selected. The interface includes a "Refresh" dropdown set to "Never", a "Show" dropdown set to "Latest 20 records", and a "Within" dropdown set to "Last 3 hours". There is an "Export To" button and a "Filter" button. The main table has the following columns: Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, and N. The first row is expanded, showing details for a "helpdeskuser" with a status of "Success" and a type of "Authorization". The "Type" cell in this row is highlighted with a red box. The table footer indicates "Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time)" and "Records Shown: 6".

| Logged Time | Status | Details | Identity | Type | Authentication Policy | Authorization Policy | Ise Node | N |
|----------------------------|--------|---------|--------------|----------------|--------------------------------|--------------------------------|----------|---|
| Dec 08, 2022 06:51:46.1... | ✓ | | helpdeskuser | Authorization | | WLC TACACS Authentication >... | ise | W |
| Dec 08, 2022 06:51:46.0... | ✓ | | helpdeskuser | Authentication | WLC TACACS Authentication >... | | ise | W |
| Dec 08, 2022 06:38:38.2... | ✓ | | adminuser | Authorization | | WLC TACACS Authentication >... | ise | W |
| Dec 08, 2022 06:38:38.1... | ✓ | | adminuser | Authentication | WLC TACACS Authentication >... | | ise | W |
| Dec 08, 2022 06:34:54.0... | ✓ | | adminuser | Authorization | | WLC TACACS Authentication >... | ise | W |
| Dec 08, 2022 06:34:53.9... | ✓ | | adminuser | Authentication | WLC TACACS Authentication >... | | ise | W |

Quando expandida, uma tentativa de autenticação bem-sucedida para o helpdeskuser tem a seguinte aparência:

Overview

| | |
|--------------------------------|---|
| Request Type | Authentication |
| Status | Pass |
| Session Key | ise/459637517/243 |
| Message Text | Passed-Authentication: Authentication succeeded |
| Username | helpdeskuser |
| Authentication Policy | WLC TACACS Authentication >> Default |
| Selected Authorization Profile | IOS Helpdesk |

Authentication Details

| | |
|-----------------------|--|
| Generated Time | 2022-12-08 06:51:46.077000 -05:00 |
| Logged Time | 2022-12-08 06:51:46.077 |
| Epoch Time (sec) | 1670500306 |
| ISE Node | ise |
| Message Text | Passed-Authentication: Authentication succeeded |
| Failure Reason | |
| Resolution | |
| Root Cause | |
| Username | helpdeskuser |
| Network Device Name | WLC-9800 |
| Network Device IP | 10.48.39.133 |
| Network Device Groups | IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types |
| Device Type | Device Type#All Device Types |
| Location | Location#All Locations |
| Device Port | tty5 |
| Remote Address | 10.61.80.151 |

Steps

```

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Network Access.Device IP Address
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
13045 TACACS+ will use the password prompt from global
TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (
Step latency=3149ms)
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - InternalUser.IdentityGroup
13015 Returned TACACS+ Authentication Reply

```

A partir disso, você pode ver que o usuário helpdeskuser foi autenticado com êxito no dispositivo de rede WLC-9800 com a ajuda da política de autenticação WLC TACACS Authentication > Default. Além disso, o perfil IOS Helpdesk de autorização foi atribuído a esse usuário e recebeu o privilégio de nível 1.

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.