Configurar uma WLC e um ACS para autenticar usuários de gerenciamento

Contents

Introdução

Este documento descreve como configurar uma WLC e um Cisco Secure ACS para que o servidor AAA possa autenticar usuários de gerenciamento no controlador.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar parâmetros básicos em WLCs
- Conhecimento de como configurar um servidor RADIUS como o Cisco Secure ACS

Componentes Utilizados

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

- Controlador de LAN sem fio Cisco 4400 que executa a versão 7.0.216.0
- Um Cisco Secure ACS que executa a versão 4.1 do software e é usado como um servidor RADIUS nesta configuração.

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Este documento explica como configurar um Controller de LAN Wireless (WLC) e um Access Control Server (Cisco Secure ACS) para que o servidor de Autenticação, Autorização e Contabilização (AAA) possa autenticar usuários de gerenciamento no controlador. O documento também explica como diferentes usuários de gerenciamento podem receber privilégios diferentes com Atributos específicos do Fornecedor (VSAs) retornados do servidor RADIUS Cisco Secure ACS.

Configurar

Nesta seção, você verá informações sobre como configurar a WLC e o ACS para a finalidade descrita neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

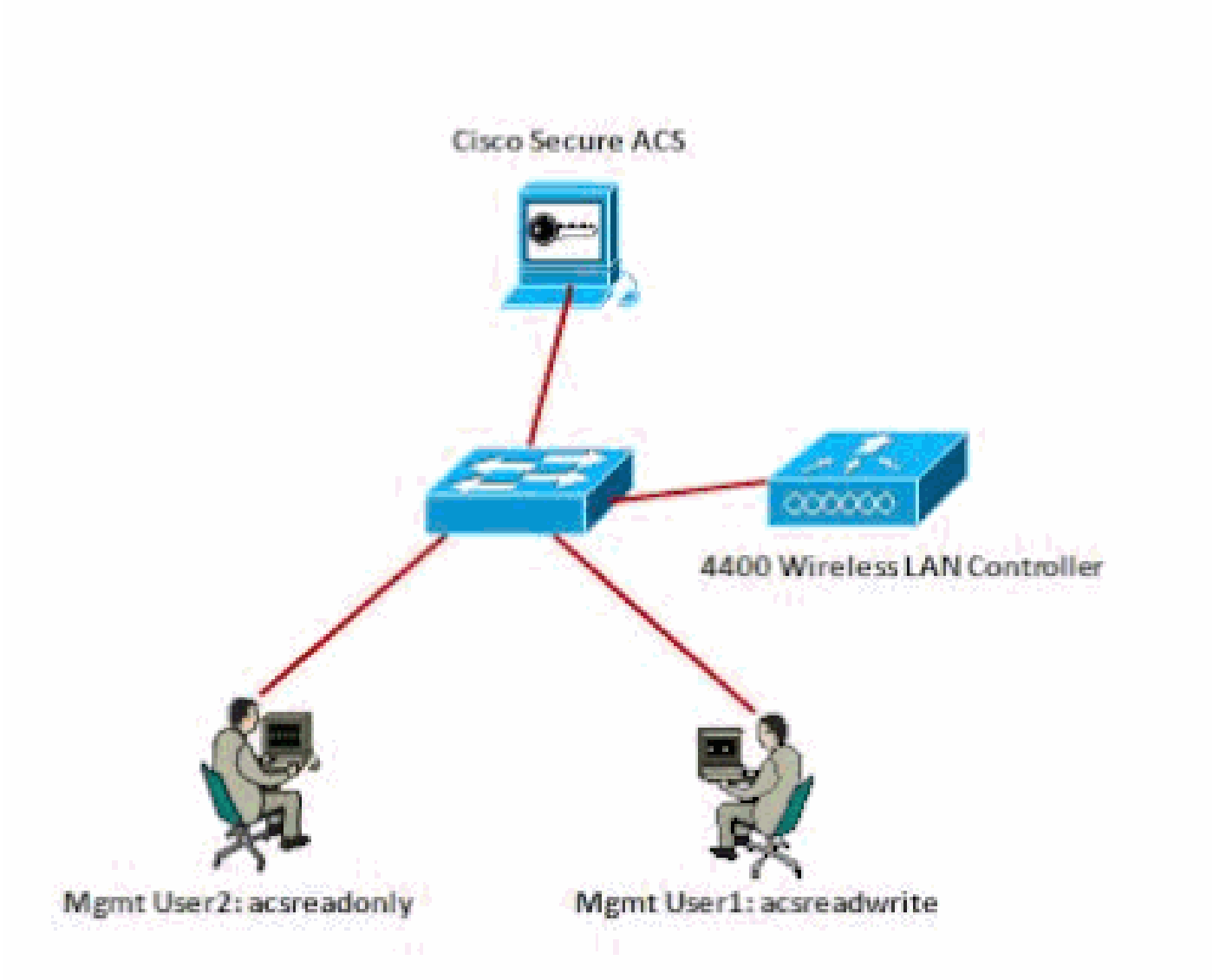


Diagrama de Rede

Este exemplo de configuração usa estes parâmetros:

- Endereço IP do Cisco Secure ACS —172.16.1.1/255.255.0.0
- Endereço IP da interface de gerenciamento do controlador—172.16.1.30/255.255.0.0
- Chave secreta compartilhada que é usada no ponto de acesso (AP) e no servidor RADIUS—asdf1234
- Estas são as credenciais dos dois usuários que este exemplo configura no ACS:
    - Nome de usuário - acsreadwrite

      Senha - acsreadwrite
    - Nome de usuário - acsreadonly

      Senha - acsreadonly

Você precisa configurar o WLC e o Cisco Secure Cisco Secure ACS para:

- Qualquer usuário que se conecta à WLC com o nome de usuário e a senha como acsreadwrite recebe acesso administrativo total à WLC.
- Qualquer usuário que se conecta à WLC com o nome de usuário e a senha como acsreadonly recebe acesso somente leitura à WLC.

Configurações

Este documento utiliza as seguintes configurações:

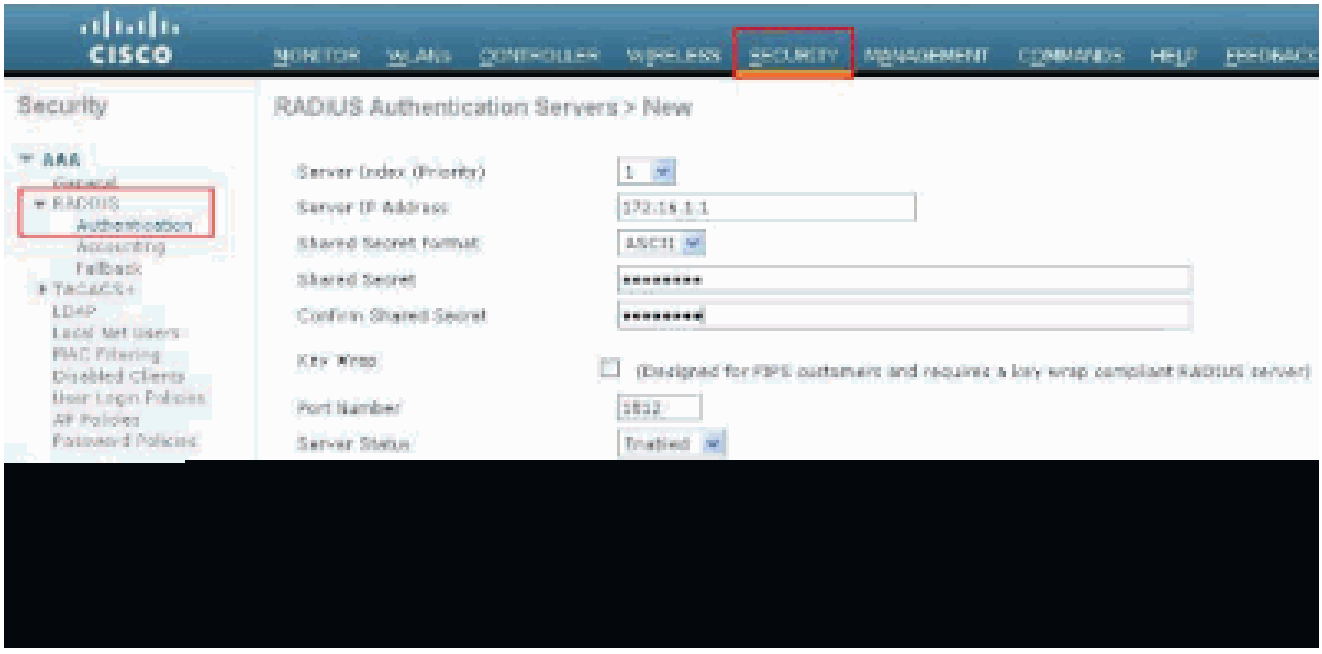
- Configuração de WLC
- Configuração do Cisco Secure ACS

Configuração de WLC

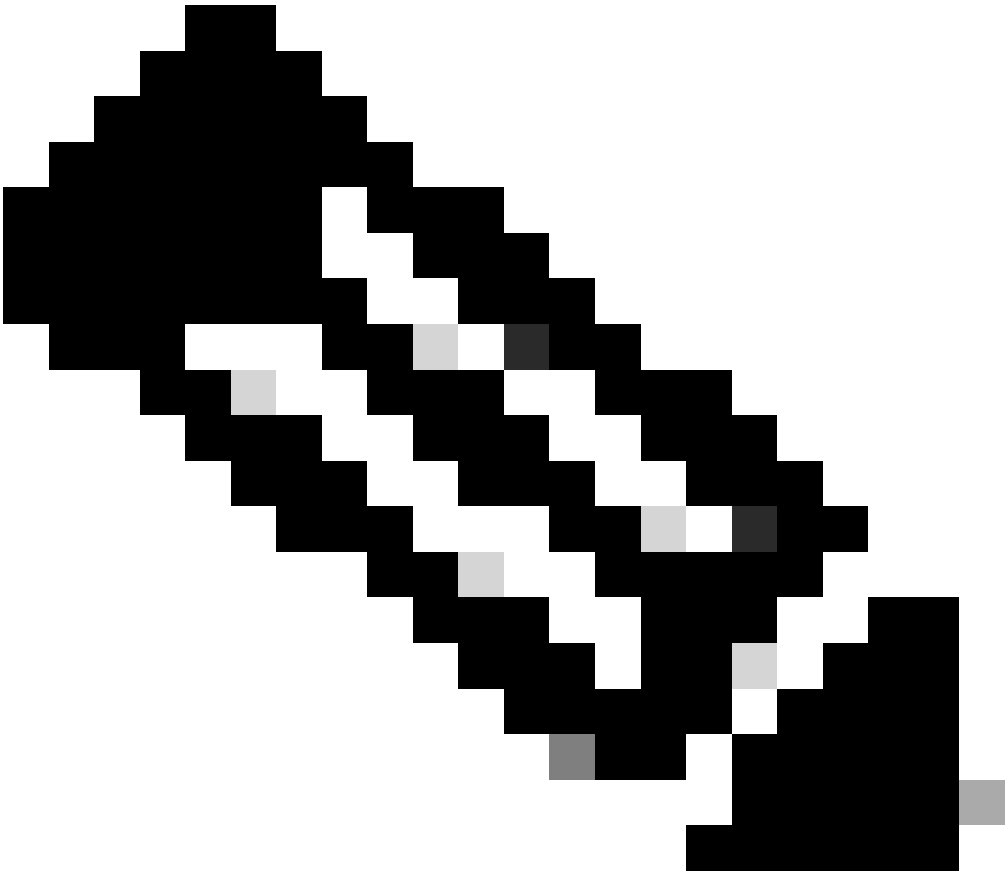
Configurar a WLC para aceitar o gerenciamento por meio do servidor Cisco Secure ACS

Conclua estes passos para configurar o WLC de modo que ele se comunique com o servidor RADIUS:

1. Na GUI da WLC, clique em Security. No menu à esquerda, clique em RADIUS > Authentication. A página RADIUS Authentication servers é exibida. Para adicionar um novo servidor RADIUS, clique em Novo. Na página Servidores de autenticação RADIUS > Novo, digite os parâmetros específicos do servidor RADIUS. Exemplo:

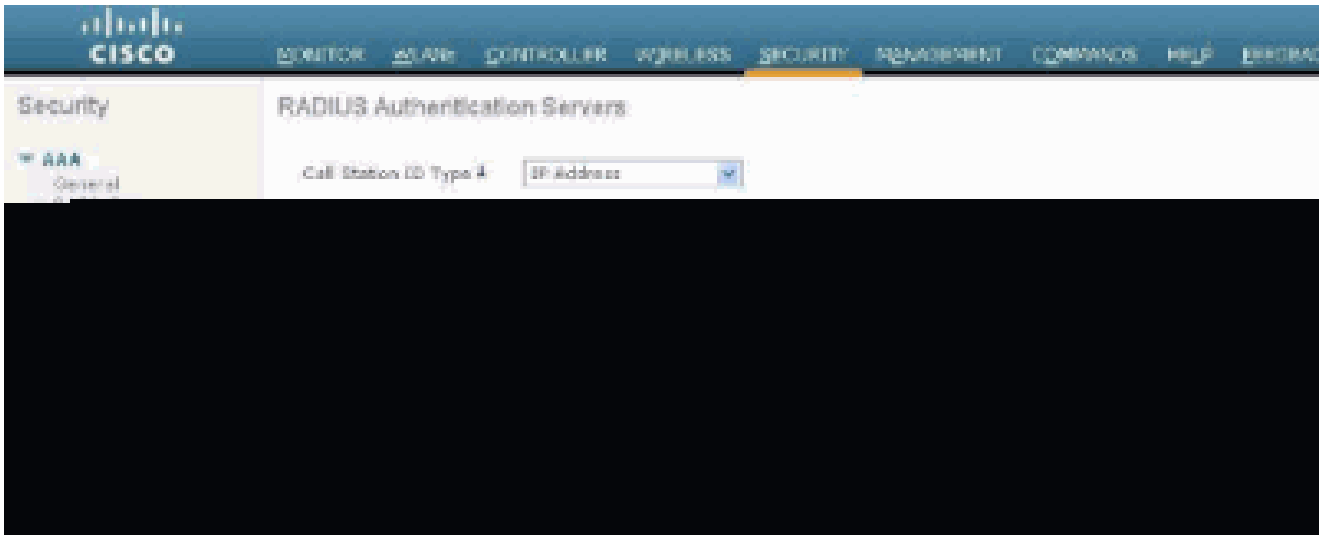


2. Marque o botão de opção Management para permitir que o servidor RADIUS autentique os usuários que fazem login na WLC.



Observação: certifique-se de que o segredo compartilhado configurado nesta página corresponda ao segredo compartilhado configurado no servidor RADIUS. Somente então a WLC poderá se comunicar com o servidor RADIUS.

3. Verifique se a WLC está configurada para ser gerenciada pelo Cisco Secure ACS. Para fazer isso, clique em Security na GUI da WLC. A janela resultante da GUI é semelhante a este exemplo.



Você pode ver que a caixa de seleção Gerenciamento está ativada para o servidor RADIUS 172.16.1.1. Isso ilustra que o ACS tem permissão para autenticar os usuários de gerenciamento na WLC.

Configuração do Cisco Secure ACS

Conclua as etapas nestas seções para configurar o ACS:

1. Adicione a WLC como um cliente AAA ao servidor RADIUS.
2. Configure os usuários e seus atributos RADIUS IETF apropriados.
3. Configure um usuário com acesso de leitura-gravação.
4. Configure um usuário com acesso somente leitura.

Adicione a WLC como um cliente AAA ao servidor RADIUS

Conclua estes passos para adicionar a WLC como um cliente AAA no Cisco Secure ACS:

1. Na interface gráfica do usuário do ACS, clique em Network Configuration.
2. Em AAA Clients, clique em Add Entry.
3. Na janela Add AAA Client, insira o nome de host da WLC, o endereço IP da WLC e uma chave secreta compartilhada.

   Neste exemplo, estas são as configurações:

   - O nome de host do cliente AAA é WLC-4400
   - 172.16.1.30/16 é o endereço IP do cliente AAA, que, neste caso, é o WLC.
   - A chave secreta compartilhada é "asdf1234".

Janela Adicionar Cliente AAA

Essa chave secreta compartilhada deve ser a mesma que você configura na WLC.

4. No menu suspenso Authenticate Using, selecione RADIUS (Cisco Airespace).
5. Clique em Submit + Restart para salvar a configuração.

Configurar usuários e seus atributos RADIUS IETF apropriados

Para autenticar um usuário por meio de um servidor RADIUS, para logon e gerenciamento do controlador, você deve adicionar o usuário ao banco de dados RADIUS com o atributoService-Typeset IETF RADIUS ao valor apropriado com base nos privilégios do usuário.

- Para definir privilégios de leitura-gravação para o usuário, defina Service-TypeAttribute como Administrative.
- Para definir privilégios somente leitura para o usuário, defina Service-TypeAttribute como NAS-Prompt.

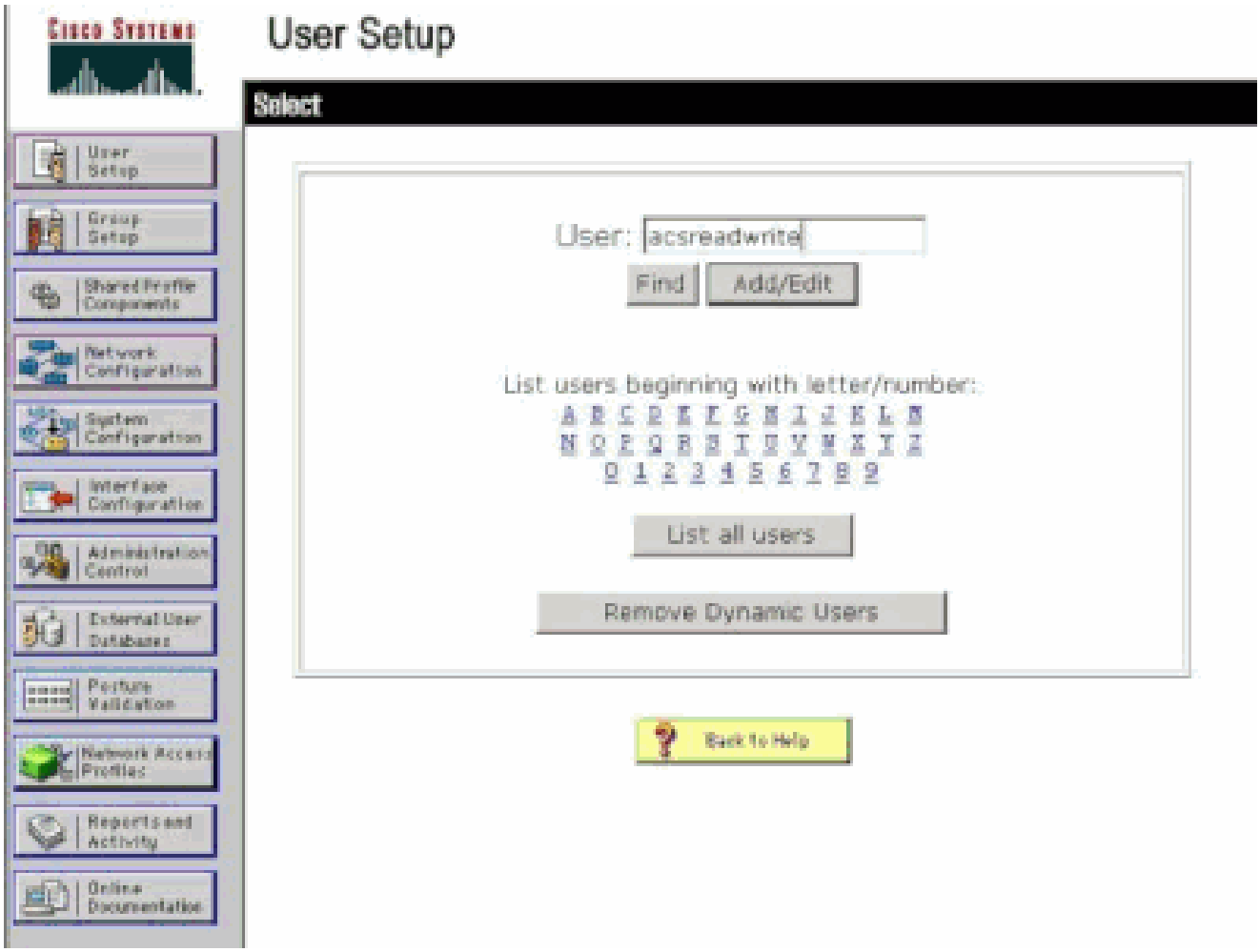
Configurar um usuário com acesso de leitura-gravação

O primeiro exemplo mostra a configuração de um usuário com acesso total à WLC. Quando este usuário tenta fazer login na controladora, o servidor RADIUS autentica e fornece a este usuário acesso administrativo completo.

Neste exemplo, o nome de usuário e a senha são acsreadwrite.

Conclua estas etapas no Cisco Secure ACS.

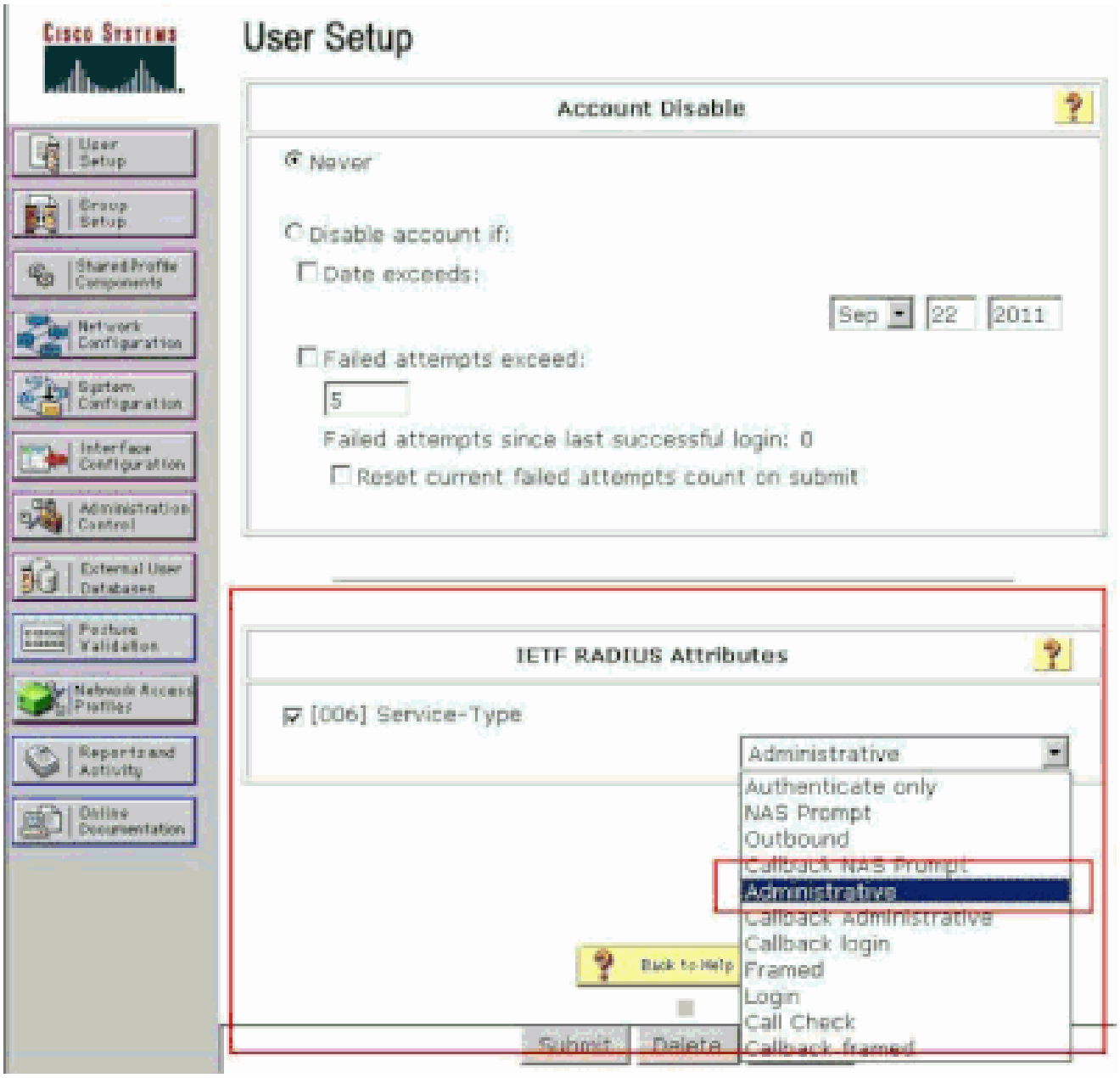
1. Na interface gráfica do usuário do ACS, clique em User Setup.
2. Digite o nome de usuário a ser adicionado ao ACS conforme mostrado nesta janela de exemplo.



Janela Configuração do usuário

3. Clique em Add/Edit para ir para a página User Edit.
4. Na página User Edit, forneça os detalhes de Nome real, Descrição e Senha desse usuário.
5. Role para baixo até a configuração IETF RADIUS Attributes e marque Service-Type Attribute.
6. Como, neste exemplo, o usuário acsreadwrite precisa ter acesso total, escolha Administrative no menu suspenso Service-Type e clique em Submit.

   Isso garante que esse usuário específico tenha acesso de leitura-gravação à WLC.



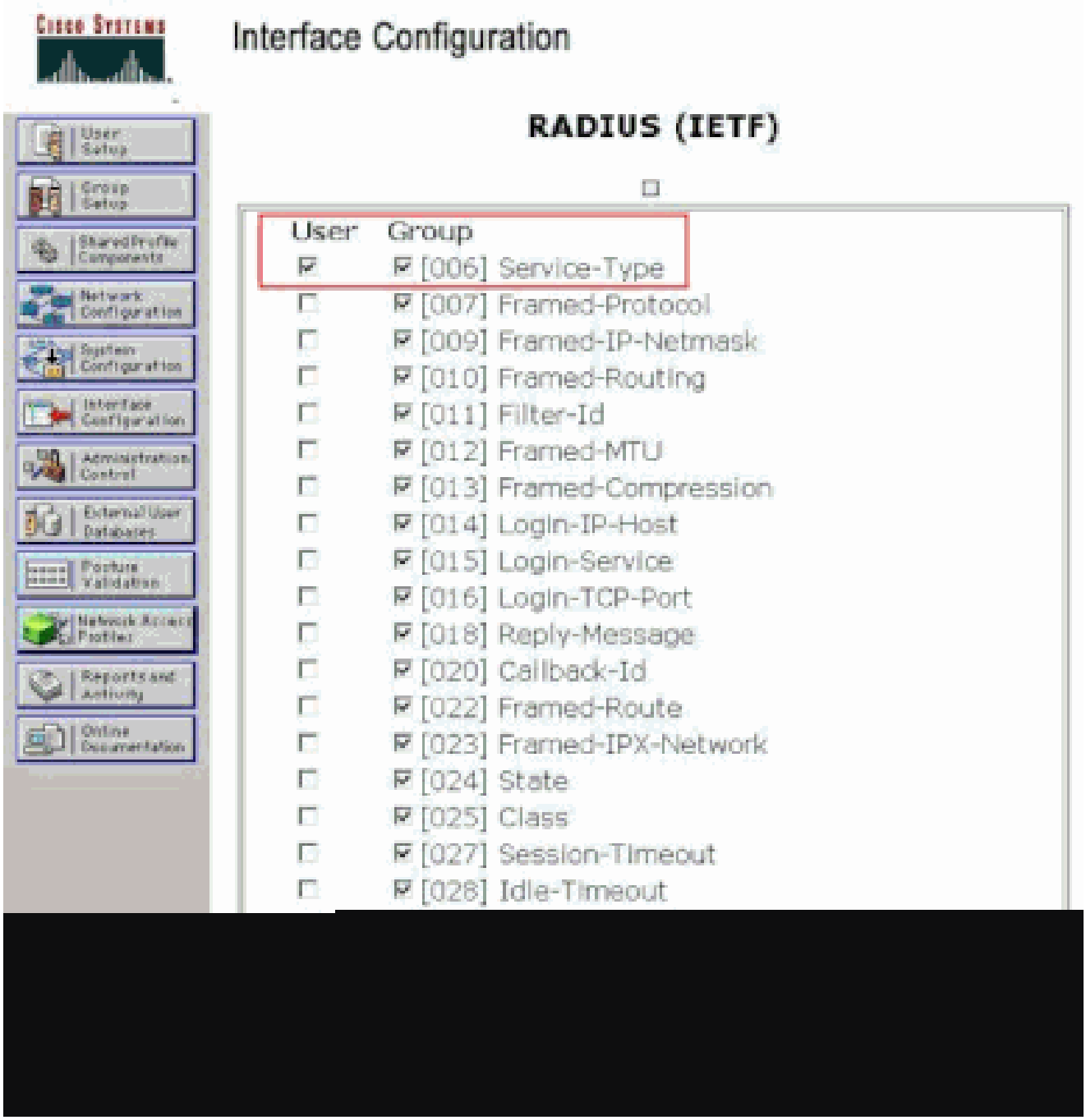
Configurações de Atributos RADIUS ETF

Às vezes, esse atributo Service-Type não fica visível nas configurações do usuário. Nesses casos, conclua estas etapas para torná-la visível.

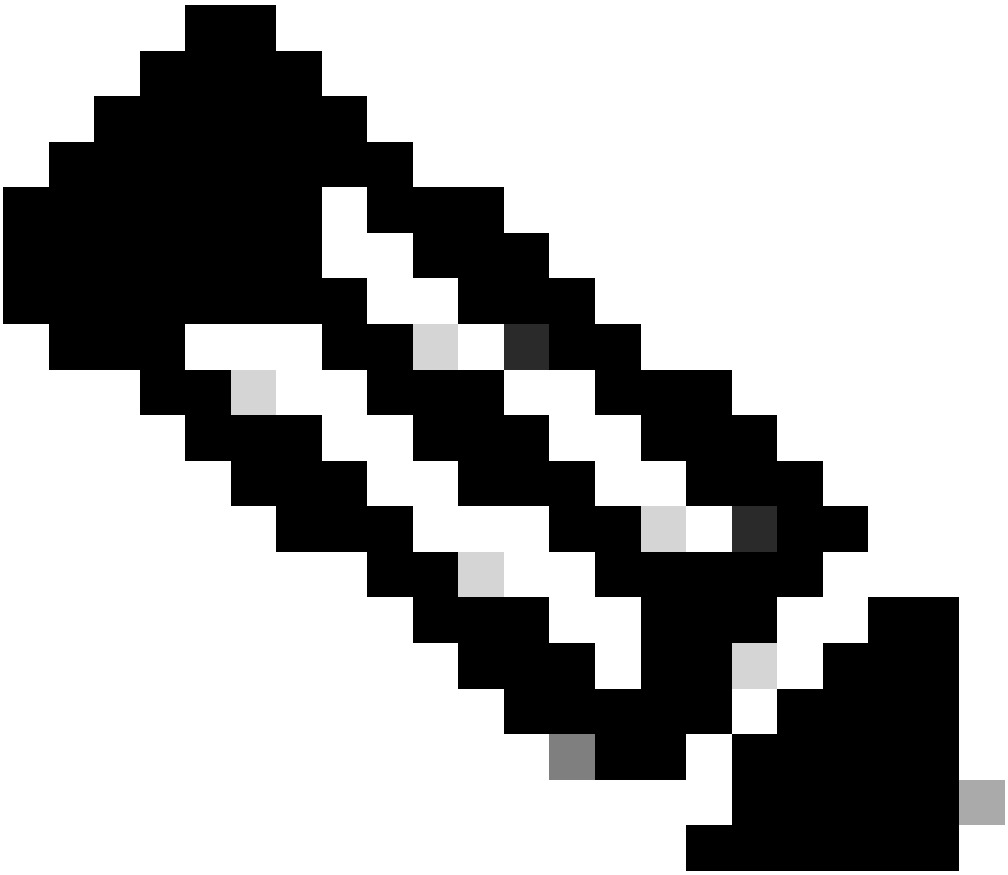
1. Na GUI do ACS, escolha Interface Configuration > RADIUS (IETF) para habilitar os atributos IETF na janela User Configuration.

   Isso o levará para a página de Configurações do RADIUS (IETF).

2. Na página Configurações do RADIUS (IETF), você pode ativar o atributo IETF que precisa estar visível nas configurações do usuário ou do grupo. Para essa configuração, marque Service-Type para a coluna User e clique em Submit. Essa janela mostra um exemplo.



Página de Configurações do RADIUS (IETF)



Observação: este exemplo especifica a autenticação por usuário. Você também pode executar a autenticação com base no grupo ao qual um usuário específico pertence. Nesses casos, ative a caixa de seleção Grupo para que esse atributo fique visível nas Configurações do grupo. Além disso, se a autenticação for em grupo, você precisará atribuir usuários a um grupo específico e definir a configuração de grupo dos atributos IETF para fornecer privilégios de acesso aos usuários desse grupo. Consulte Gerenciamento de grupos para obter informações detalhadas sobre como configurar e gerenciar grupos.

Configurar um usuário com acesso somente leitura

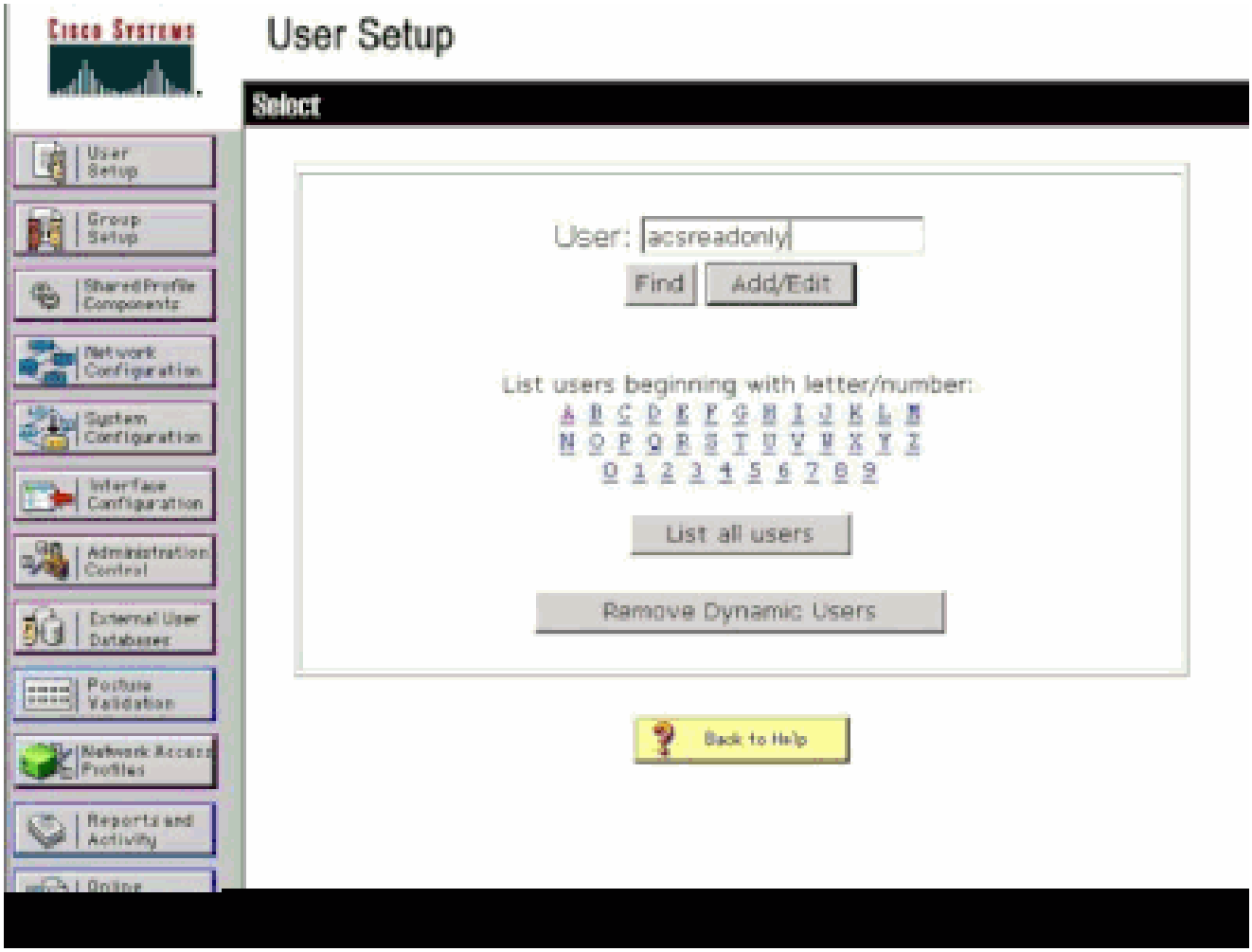
Este exemplo mostra a configuração de um usuário com acesso somente leitura à WLC. Quando este usuário tenta fazer login na controladora, o servidor RADIUS autentica e fornece a este usuário acesso somente leitura.

Neste exemplo, o nome de usuário e a senha são acsreadonly.

Conclua estas etapas no Cisco Secure ACS:

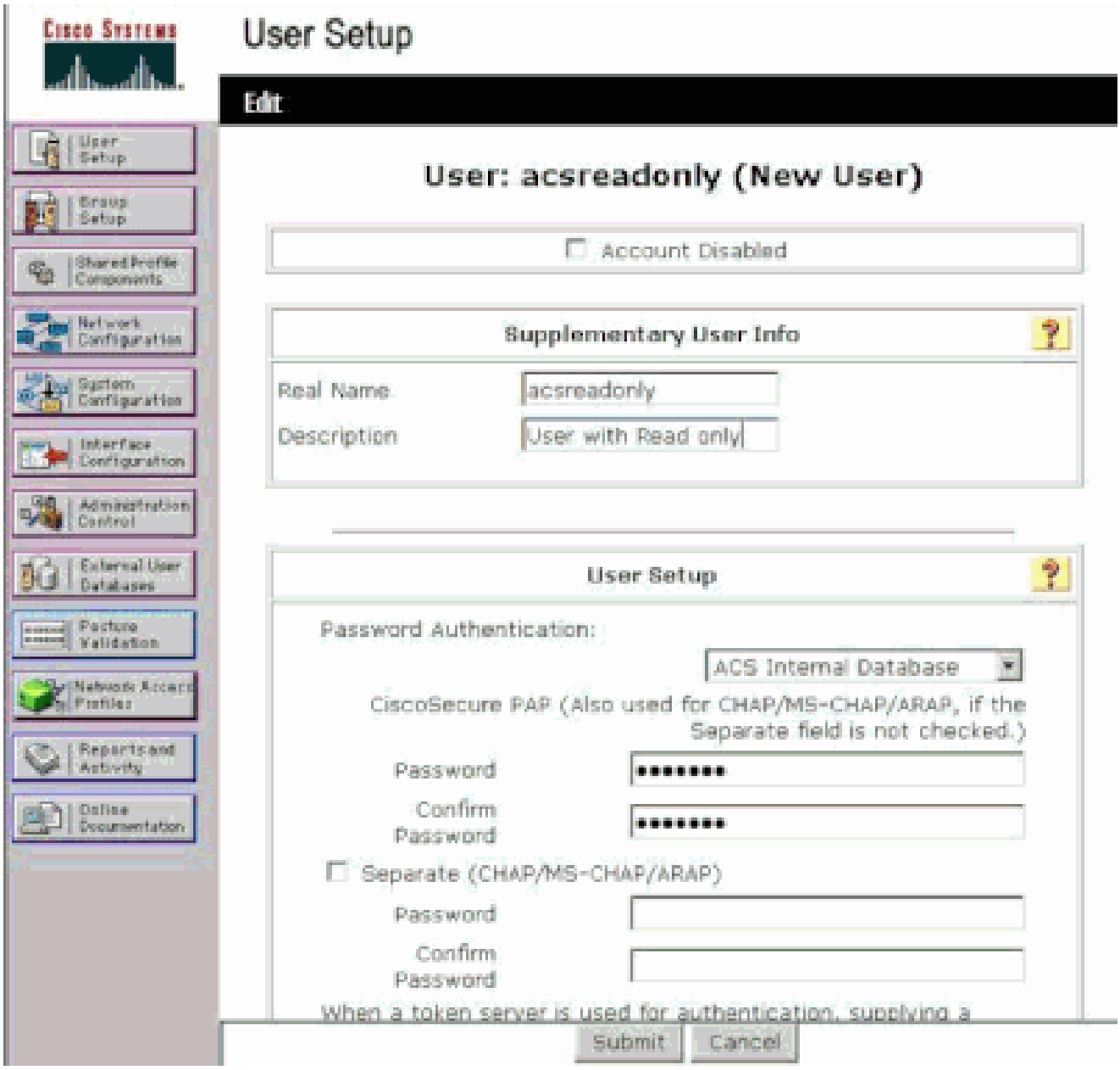
1. Na interface gráfica do usuário do ACS, clique em User Setup.

2. Digite o nome de usuário que deseja adicionar ao ACS e clique em Add/Edit para ir para a página User Edit.



Adicionar um nome de usuário

3. Forneça o nome real, a descrição e a senha deste usuário. Essa janela mostra um exemplo.

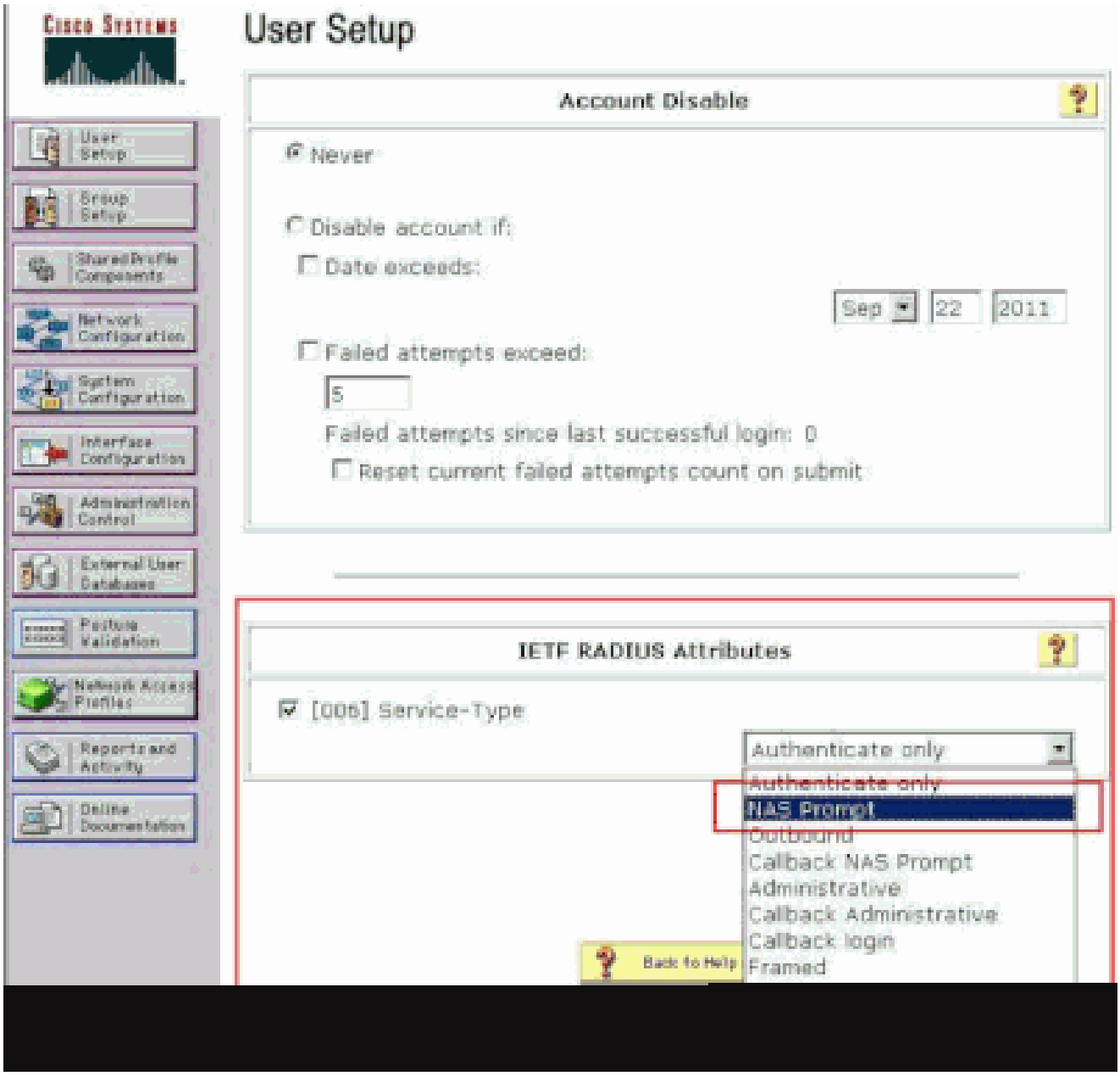


Forneça o nome real, a descrição e a senha do usuário adicionado

4. Role para baixo até a configuração IETF RADIUS Attributes e marque Service-Type Attribute.

5. Como, neste exemplo, o usuário acsreadonly precisa ter acesso somente leitura, escolha Prompt NAS no menu suspenso Tipo de serviço e clique em Enviar.

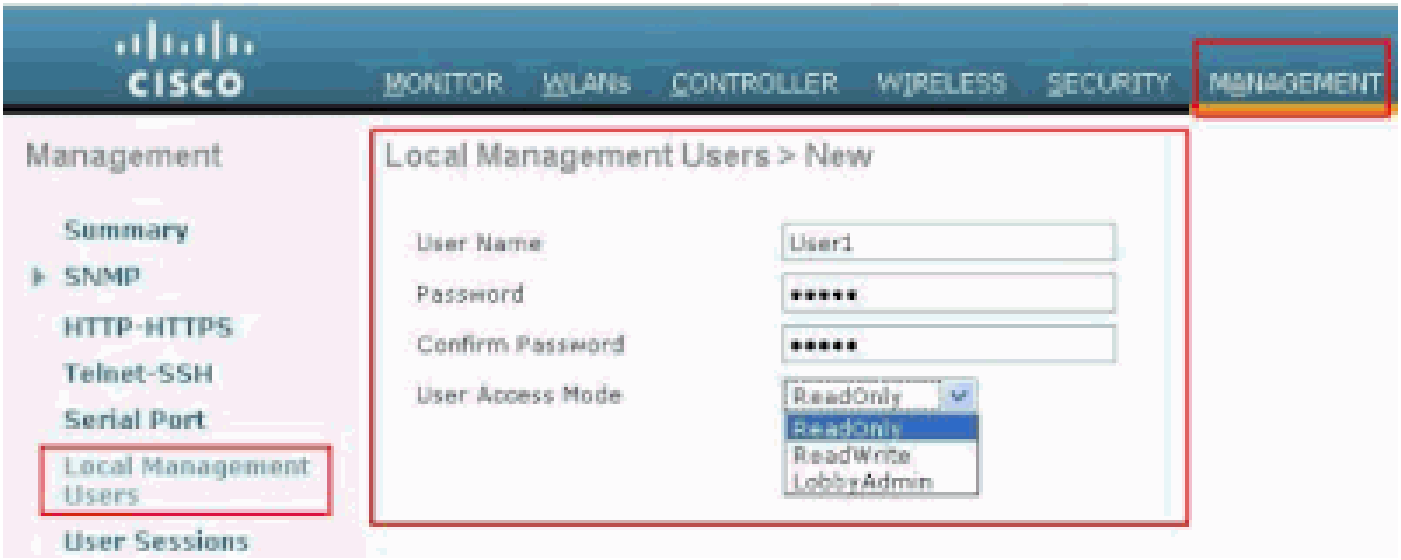
   Isso garante que esse usuário específico tenha acesso somente leitura à WLC.



Verificar Atributo de Tipo de Serviço

Gerenciar a WLC localmente e através do servidor RADIUS

Você também pode configurar os usuários de gerenciamento localmente no WLC. Isso pode ser feito na GUI do controlador, em Gerenciamento > Usuários de gerenciamento local.



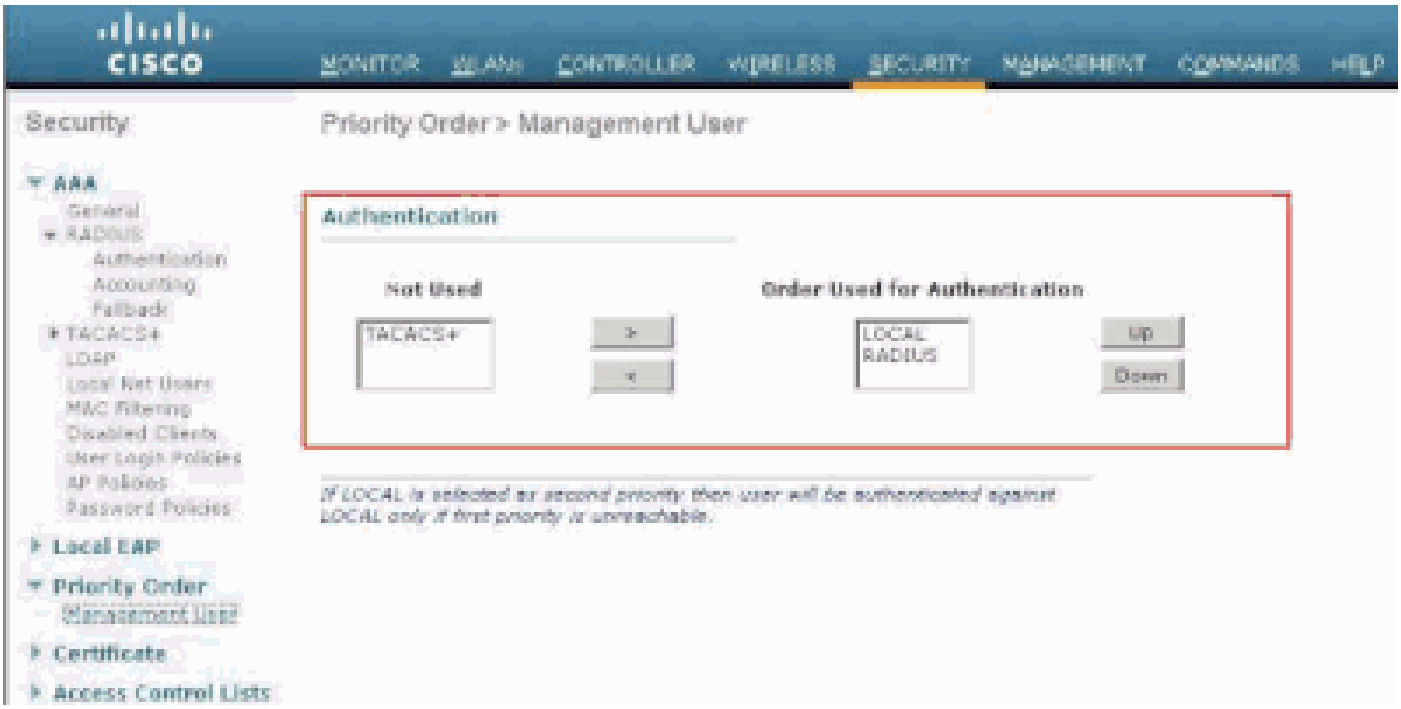
Configurar os usuários de gerenciamento localmente no WLC

Suponha que a WLC esteja configurada com usuários de gerenciamento tanto localmente quanto no servidor RADIUS com a caixa de seleção Gerenciamento ativada. Nesse cenário, por padrão, quando um usuário tenta fazer login na WLC, a WLC se comporta desta maneira:

1. Primeiro, a WLC examina os usuários de gerenciamento local definidos para validar o usuário. Se o usuário existir em sua lista local, ele permitirá a autenticação para esse usuário. Se esse usuário não aparecer localmente, ele procurará o servidor RADIUS.

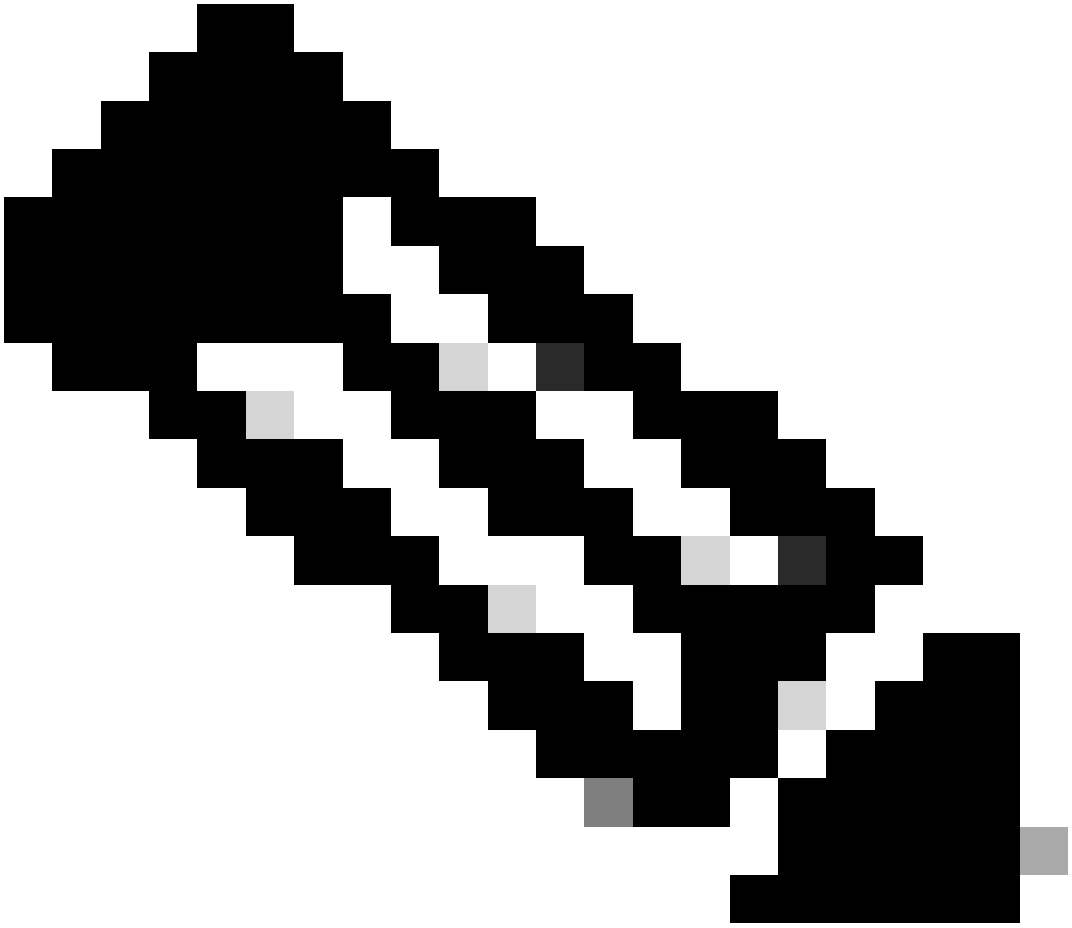
2. Se o mesmo usuário existir tanto localmente como no servidor RADIUS, mas com privilégios de acesso diferentes, a WLC autenticará o usuário com os privilégios especificados localmente. Em outras palavras, a configuração local na WLC sempre tem precedência quando comparada ao servidor RADIUS.

A ordem de autenticação para usuários de gerenciamento pode ser alterada na WLC. Para fazer isso, na página Security na WLC, clique em Priority Order > Management User. Nessa página, você pode especificar a ordem da autenticação. Exemplo:



Seleção de Usuário de Gerenciamento" />

Ordem de Prioridade > Seleção de Usuário de Gerenciamento



Nota: se LOCAL for selecionado como segunda prioridade, então o usuário será autenticado com este método somente se o método definido como primeira prioridade (RADIUS/ TACACS) estiver inacessível.

Verificar

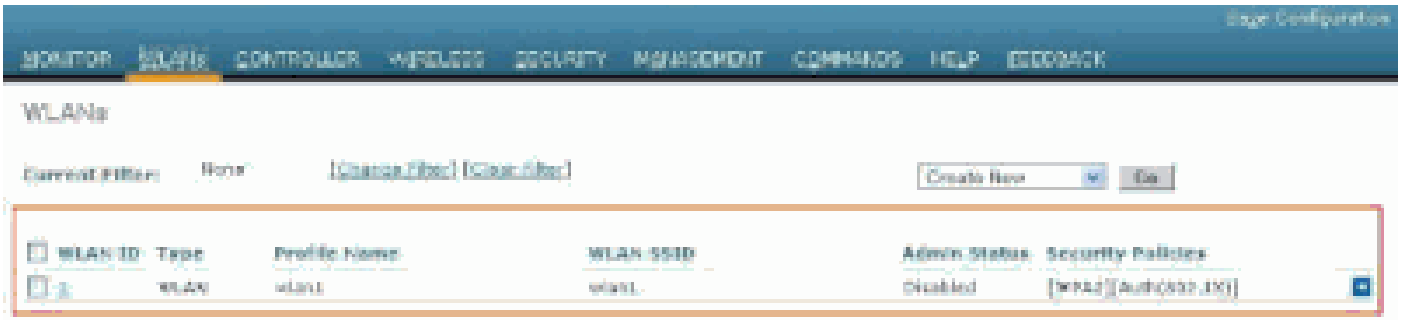
Para verificar se sua configuração funciona corretamente, acesse a WLC através do modo CLI ou GUI (HTTP/HTTPS). Quando o prompt de login for exibido, digite o nome de usuário e a senha configurados no Cisco Secure ACS.

Se as configurações estiverem corretas, você será autenticado com êxito na WLC.

Você também pode garantir que o usuário autenticado receba restrições de acesso conforme especificado pelo ACS. Para fazer isso, acesse a GUI da WLC por meio de HTTP/HTTPS (certifique-se de que a WLC esteja configurada para permitir HTTP/HTTPS).

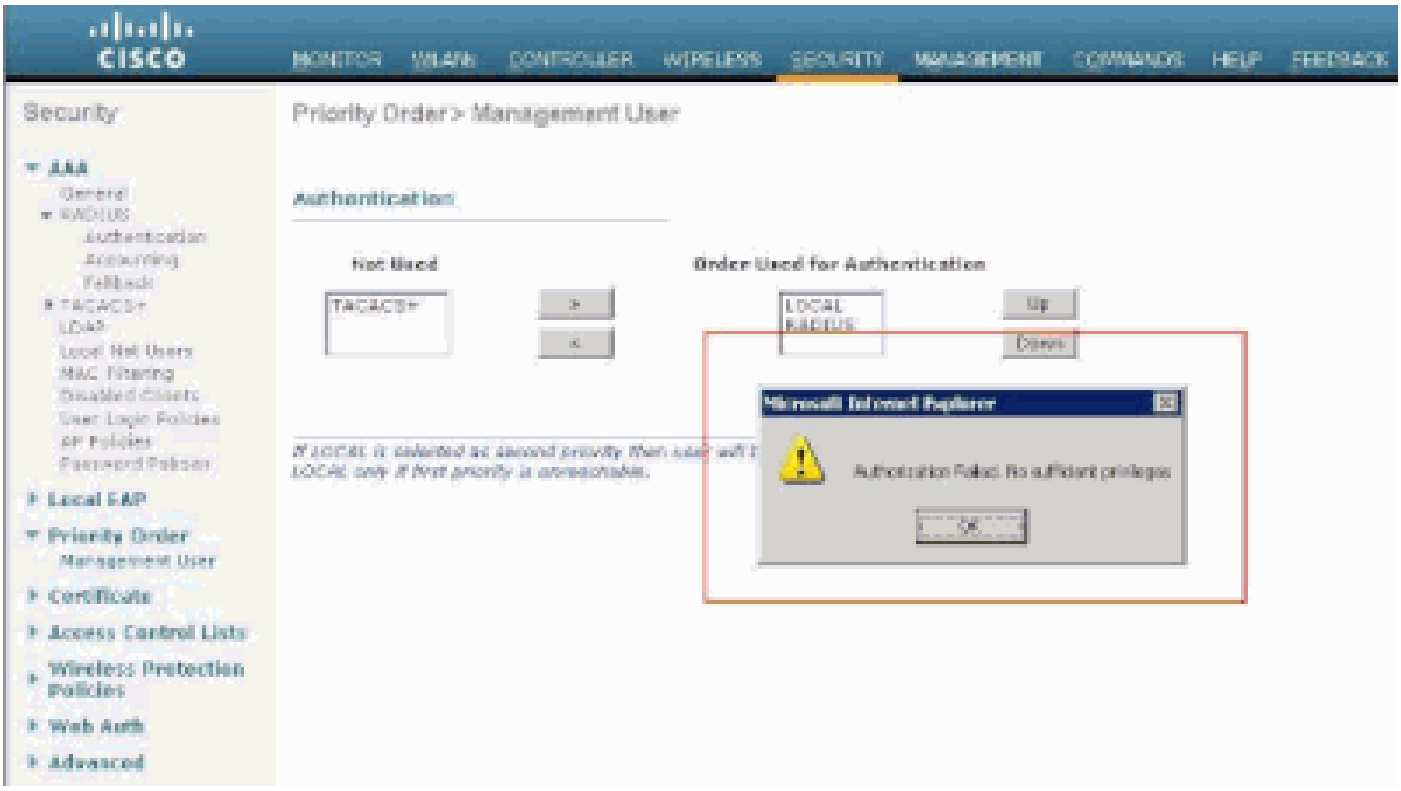
Um usuário com acesso de leitura-gravação definido no ACS tem vários privilégios configuráveis

no WLC. Por exemplo, um usuário de leitura-gravação tem o privilégio de criar uma nova WLAN na página WLANs da WLC. Essa janela mostra um exemplo.



Privilégios configuráveis no WLC

Quando um usuário com privilégios somente leitura tenta alterar a configuração no controlador, o usuário vê esta mensagem.



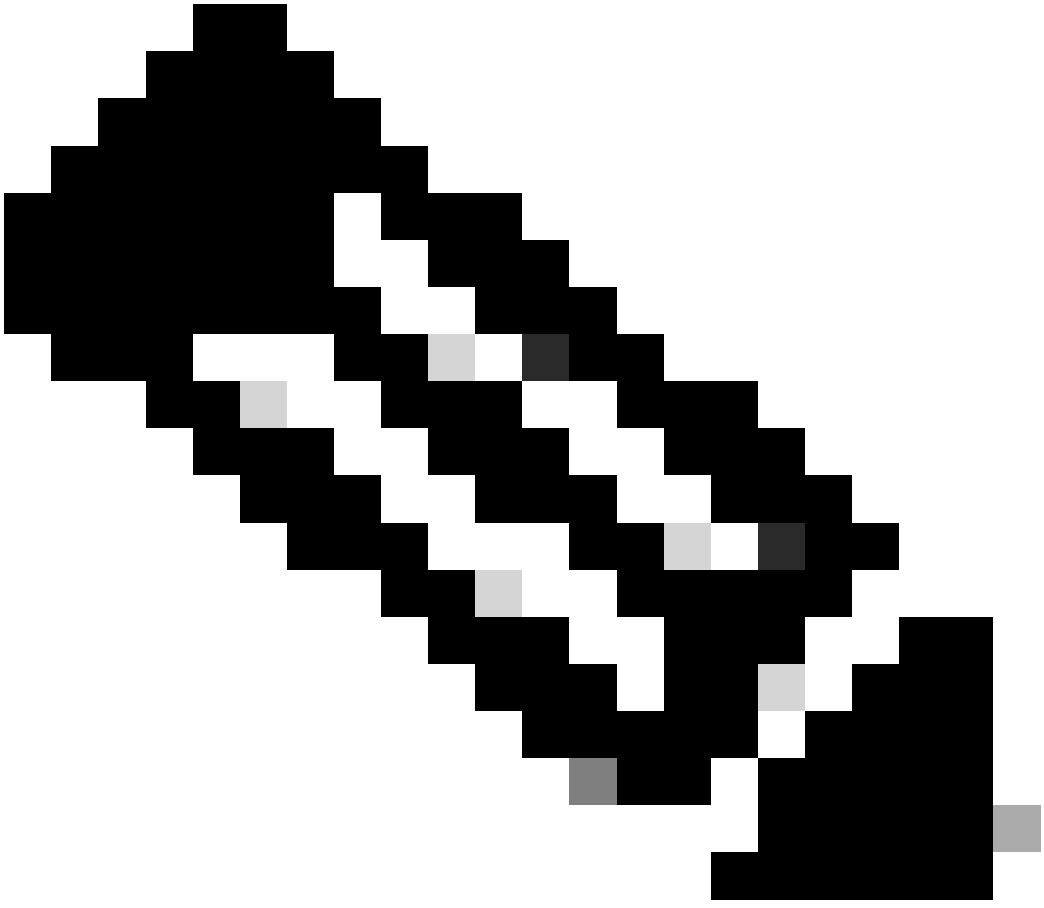
Não é possível alterar o controlador com acesso somente leitura

Essas restrições de acesso também podem ser verificadas através da CLI da WLC. Esta saída mostra um exemplo.

```
<#root>

(Cisco Controller) >

?

debug           Manages system debug options.
help            Help
linktest        Perform a link test to a specified MAC address.
logout          Exit this session. Any unsaved changes are lost.
```

```
show            Display switch options and settings.

(Cisco Controller) >config

Incorrect usage.  Use the '?' or <TAB> key to list commands.
```

Como mostra este exemplo, um?na CLI do controlador exibe uma lista de comandos disponíveis para o usuário atual. Observe também que o **config** comando não está disponível neste exemplo de saída. Isso ilustra que um usuário somente leitura não tem o privilégio de fazer configurações na WLC. Por outro lado, um usuário de leitura-gravação tem os privilégios para fazer configurações no controlador (modo GUI e CLI).



Observação: mesmo depois de autenticar um usuário WLC através do servidor RADIUS, à medida que você navega de página em página, o servidor HTTP[S] ainda autentica totalmente o cliente toda vez. A única razão pela qual você não é solicitado a fazer a

---

autenticação em cada página é que seu navegador armazena em cache e reproduz suas credenciais.

Troubleshooting

Há certas circunstâncias em que uma controladora autentica usuários de gerenciamento através do ACS, a autenticação termina com êxito (access-accept) e você não vê nenhum erro de autorização na controladora.*Mas, o usuário é solicitado novamente para a autenticação.*

Nesses casos, você não pode interpretar o que está errado e por que o usuário não pode fazer login na WLC apenas com o **debug aaa events enable** comando. Em vez disso, o controlador exibe outro prompt para autenticação.

Uma possível razão para isso é que o ACS não está configurado para transmitir o atributo Service-Type para esse usuário ou grupo específico, mesmo que o nome de usuário e a senha estejam configurados corretamente no ACS.

A saída do **debug aaa events enable** comando não indica que um usuário não tem os atributos necessários (para este exemplo, o atributo Service-Type) mesmo que um **access-accept** seja enviado de volta do servidor AAA. Este exemplo de saída de **debug aaa events enable** comando mostra um exemplo.

```
<#root>

(Cisco Controller) >

debug aaa events enable

Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c
Mon Aug 13 20:14:33 2011: Callback.....................................0x8250c40
Mon Aug 13 20:14:33 2011: protocolType.................................0x00020001
Mon Aug 13 20:14:33 2011: proxyState....................1A:00:00:00:00:00-00:00
Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)
Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of
```

```
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state
1a:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2
```

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0

```
Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:14:33 2011: structureSize.............................28

Mon Aug 13 20:14:33 2011: resultCode.................................0

Mon Aug 13 20:14:33 2011: protocolUsed.............................0x00000001

Mon Aug 13 20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

Neste primeiro exemplo de saída de **debug aaa events enable** comando, você vê que Access-Accept é recebido com êxito do servidor RADIUS, mas o atributo Service-Type não é passado para o WLC. Isso ocorre porque o usuário específico não está configurado com esse atributo no ACS.

O Cisco Secure ACS precisa ser configurado para retornar o atributo Service-Type após a autenticação do usuário. O valor do atributo Service-Type deve ser definido como **Administrative** ou **NAS-Prompt** com base nos privilégios **do usuário.**

Este segundo exemplo mostra a saída do **debug aaa events enable**comando novamente. No entanto, desta vez o atributo Service-Type é definido como **Administrative** no ACS.

<#root>

(Cisco Controller)>

debug aaa events enable

Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c

Mon Aug 13 20:17:02 2011: Callback.....................................0x8250c40

Mon Aug 13 20:17:02 2011: protocolType.................................0x00020001

Mon Aug 13 20:17:02 2011: proxyState.....................1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2

**Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0**

Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:17:02 2011: structureSize................................100

Mon Aug 13 20:17:02 2011: resultCode...................................0

Mon Aug 13 20:17:02 2011: protocolUsed.................................0x00000001

Mon Aug 13 20:17:02 2011: proxyState.....................1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:

Mon Aug 13 20:17:02 2011: AVP[01] Service-Type..........0x00000006 (6) (4 bytes)

Mon Aug 13 20:17:02 2011: AVP[02] Class.........
CISCOACS:000d1b9f/ac100128/acsserver (36 bytes)

Você pode ver nesta saída de exemplo anterior que o atributo Service-Type é passado para a WLC.

Informações Relacionadas

- **Configurar controladora de LAN sem fio - Guia de configuração**
- **Configurar VLANs em controladores de LAN sem fio**
- **Configurar um servidor RADIUS e uma WLC para atribuição de VLAN dinâmica**
- **Configurar o Wireless LAN Controller e o Lightweight Access Point Basic**
- **Configurar as VLANs do grupo AP com controladores de LAN sem fio**
- **Suporte técnico e downloads da Cisco**

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.