Autenticação de servidor Radius de usuários do Gerenciamento no exemplo de configuração do controlador do Wireless LAN (WLC)

Índice

Introdução

Este documento explica como configurar um Controller de LAN Wireless (WLC) e um Access Control Server (Cisco Secure ACS) de modo que o servidor AAA possa autenticar usuários gerentes no controlador. O documento também explica como diferentes usuários gerentes podem receber diferentes privilégios usando os Atributos Específicos de Fornecedor (VSAs) retornados do servidor Cisco Secure ACS RADIUS.

Pré-requisitos

Requisitos

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

- Conhecimento de como configurar parâmetros básicos em WLC
- 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 do Wireless LAN de Cisco 4400 que executa a versão 7.0.216.0
- Um Cisco Secure ACS que executa a versão de software 4.1 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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

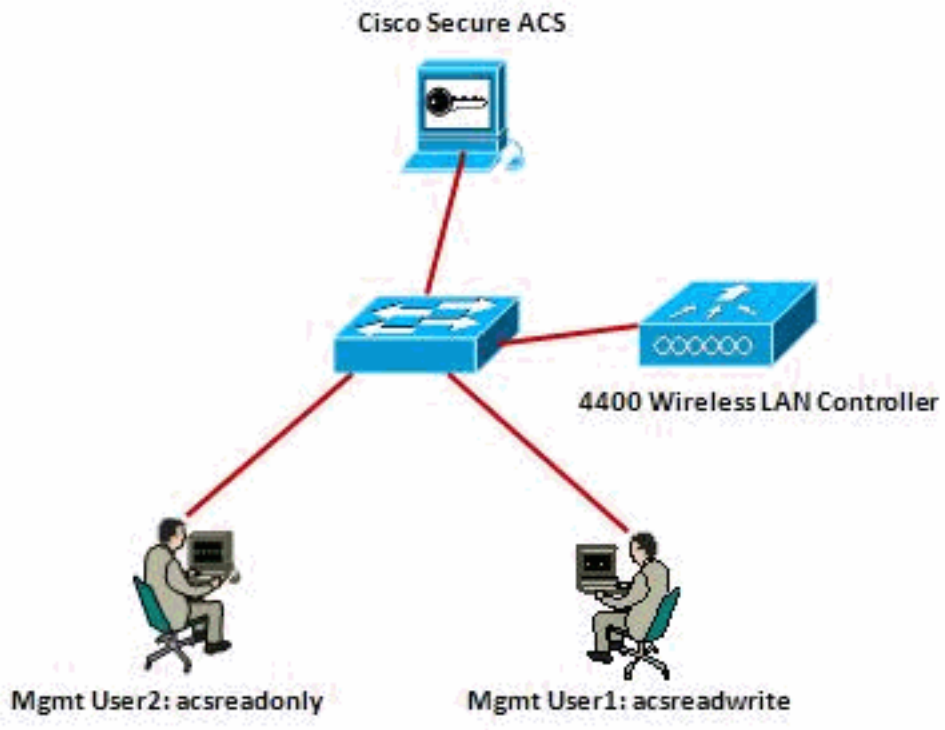
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você é presentado com a informação em como configurar o WLC e o ACS para a finalidade descrita neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este exemplo de configuração usa estes parâmetros:

- Endereço IP de Um ou Mais Servidores Cisco ICM NT do Cisco Secure ACS — 172.16.1.1/255.255.0.0

- Endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento do controlador — 172.16.1.30/255.255.0.0
- Chave secreta compartilhada que é usada no Access Point (AP) e no servidor Radius — asdf1234
- Estas são as credenciais dos dois usuários que este exemplo configura no ACS:Username - acsreadwriteSenha - acsreadwriteUsername - acsreadonlySenha - acsreadonly

Você precisa de configurar o WLC e o Cisco Secure ACS seguro de Cisco:

- Algum usuário que registrar no WLC com o nome de usuário e senha enquanto o **acsreadwrite** é dado o acesso administrativo completo ao WLC.
- Todo o usuário que registrar no WLC com o nome de usuário e senha como **acsreadonly** é dado o acesso somente leitura ao WLC.

Configurações

Este documento utiliza as seguintes configurações:

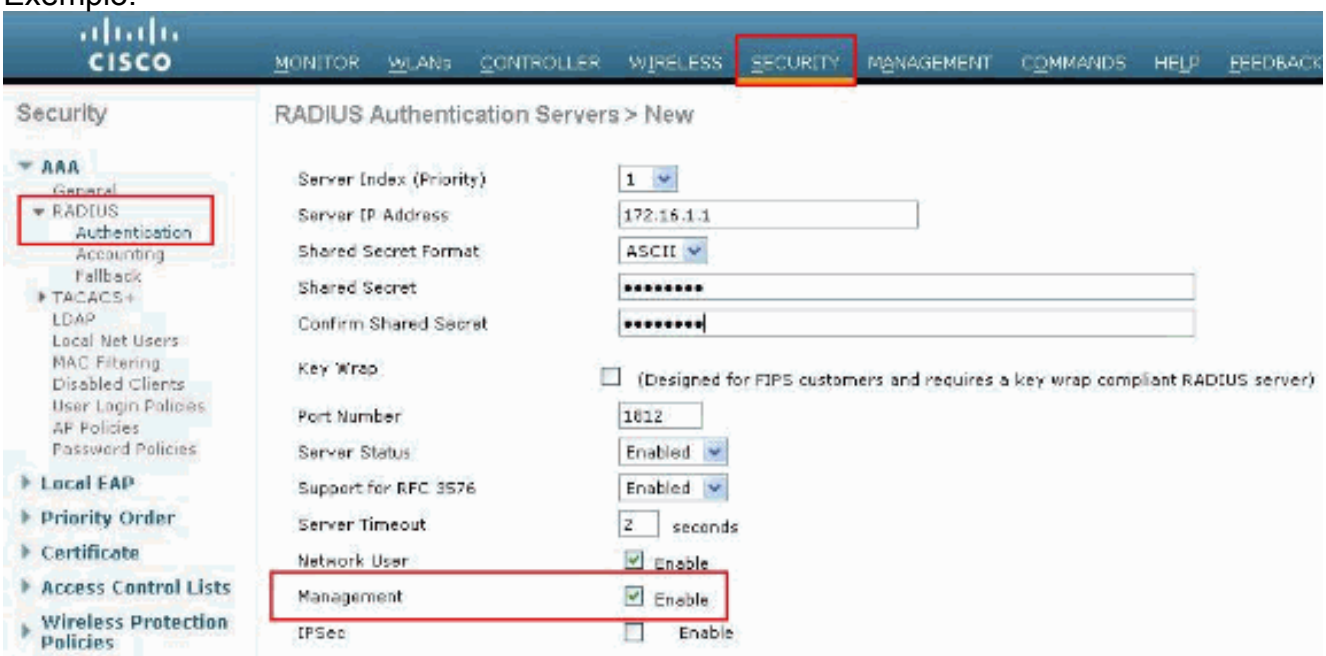
- Configuração de WLC
- Configuração do Cisco Secure ACS

Configuração de WLC

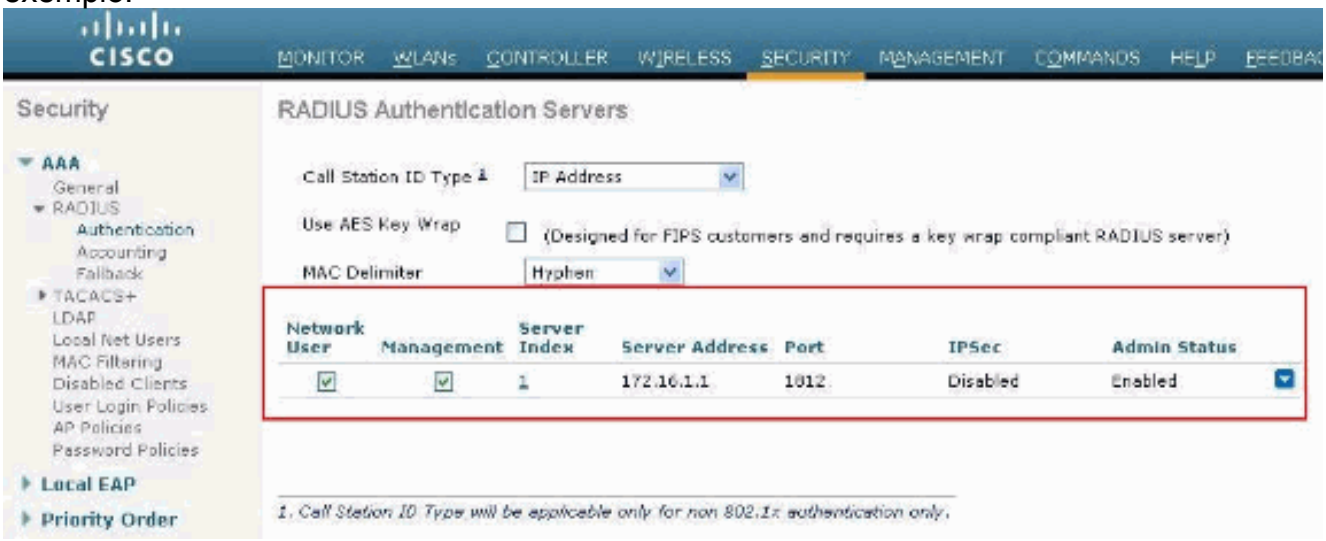
Configurar o WLC para aceitar o Gerenciamento através do server do Cisco Secure ACS

Termine estas etapas a fim configurar o WLC de modo que possa se comunicar com o servidor Radius.

1. Do WLC GUI, clique a **Segurança**. Do menu à esquerda, clique o **RAIO > a autenticação**. A página dos **servidores de autenticação RADIUS** publica-se. Para adicionar um servidor Radius novo, clique **novo**. **Nos servidores de autenticação RADIUS > a** página **nova**, incorpora os parâmetros específicos ao servidor Radius.
   Exemplo:



2. Verifique o botão de rádio do **Gerenciamento** a fim permitir que o servidor Radius autentique os usuários que entram o ao WLC.**Nota:** Assegure-se de que o segredo compartilhado configurado nesta página combine com o segredo compartilhado configurado no servidor Radius. Somente então o WLC pode comunicar-se com o servidor Radius.
3. Verifique se o WLC está configurado para ser controlado pelo Cisco Secure ACS. A fim fazer isto, clique a **Segurança do** WLC GUI. O indicador resultante GUI parece similar a este exemplo.



Você pode ver que a **caixa de verificação de gerenciamento** está permitida para o servidor Radius 172.16.1.1. Isto ilustra que o ACS está permitido autenticar os usuários do Gerenciamento no WLC.

Configuração do Cisco Secure ACS

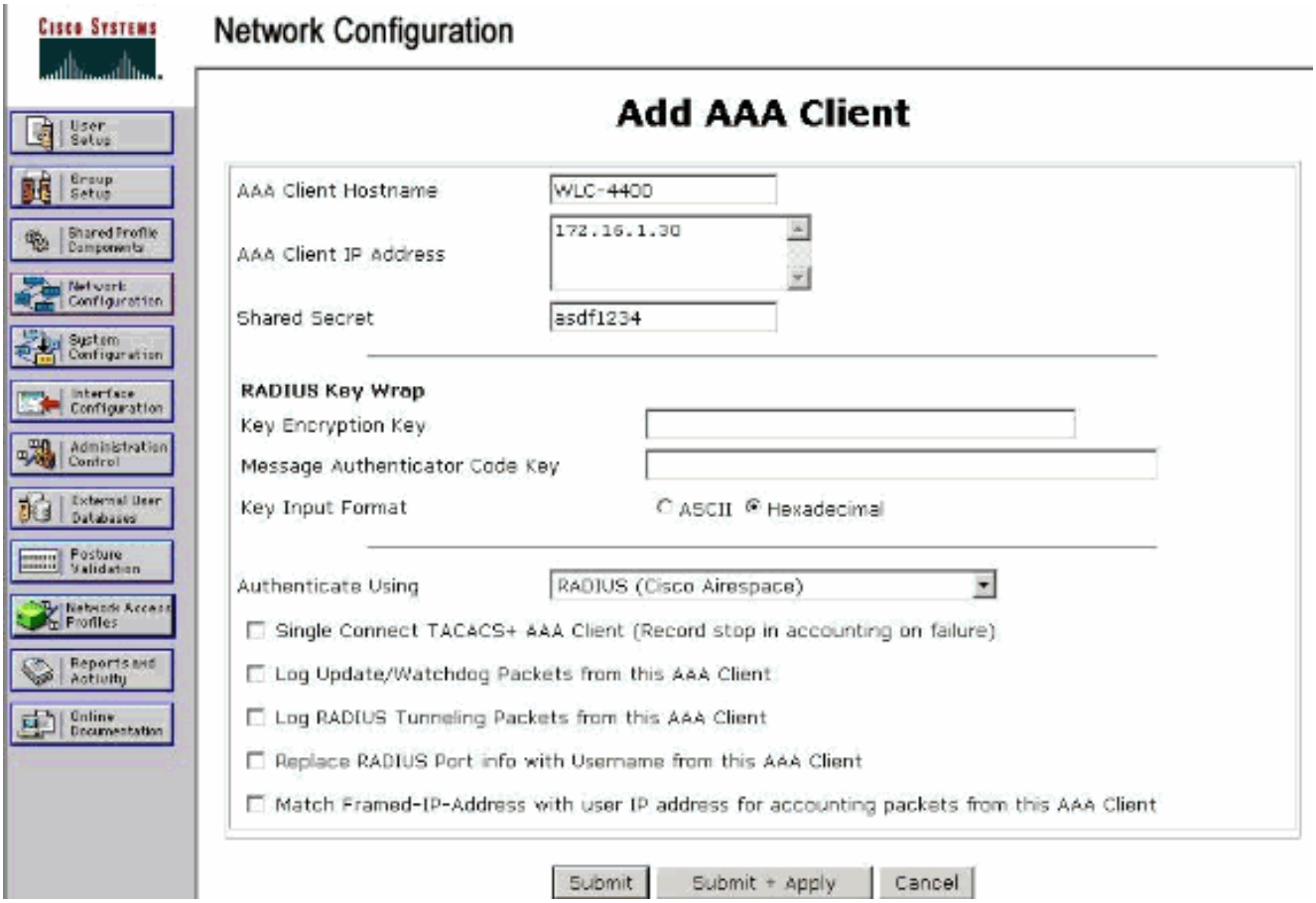
Termine as etapas nestas seções a fim configurar o ACS:

1. Adicionar o WLC como um cliente de AAA ao servidor Radius.
2. Configurar usuários e seus atributos apropriados do RAIO IETF.
3. Configurar um usuário com acesso de leitura/gravação.
4. Configurar um usuário com acesso somente leitura.

Adicionar o WLC como um cliente de AAA ao servidor Radius

Termine estas etapas a fim adicionar o WLC como um cliente de 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. No indicador do **cliente de AAA adicionar**, incorpore o nome de host WLC, o endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC, e uma chave secreta compartilhada.Neste exemplo, estes são os ajustes:O nome de host do cliente AAA é WLC-4400172.16.1.30/16 são o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA, que, é neste caso o WLC.A chave secreta compartilhada é "asdf1234".



Esta chave secreta compartilhada deve ser a mesma que a chave secreta compartilhada que você configura no WLC.

4. Da autenticação usando o menu suspenso, escolha o **RAIO (Cisco Airespace)**.
5. Clique **Submit + Restart** a fim salvar a configuração.

Configurar usuários e seus atributos apropriados do RAIO IETF

A fim autenticar um usuário através de um servidor Radius, para o início de uma sessão do controlador e o Gerenciamento, você deve adicionar o usuário ao base de dados RADIUS com o grupo do *tipo de serviço do* atributo de raio de IETF ao valor apropriado de acordo com os privilégios do usuário.

- A fim ajustar privilégios de leitura/gravação para o usuário, ajuste o atributo de *tipo de serviço a* **administrativo**.
- A fim ajustar privilégios de leitura apenas para o usuário, ajuste a NAS-**alerta do** atributo de *tipo de serviço*.

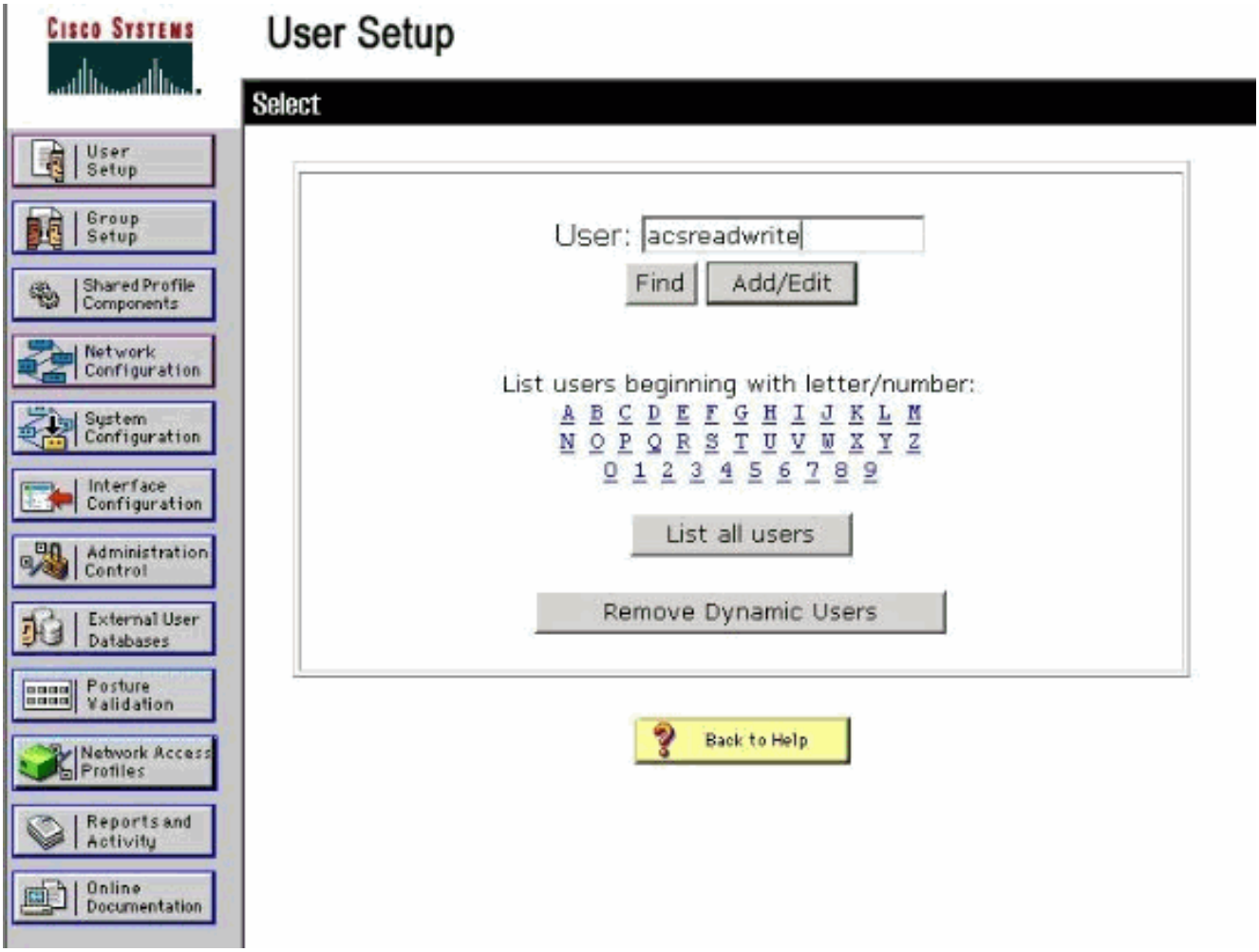
Configurar um usuário com acesso de leitura/gravação

O primeiro exemplo mostra a configuração de um usuário com acesso direto ao WLC. Quando este usuário tenta entrar ao controlador, o servidor Radius autentica e fornece este usuário o acesso administrativo completo.

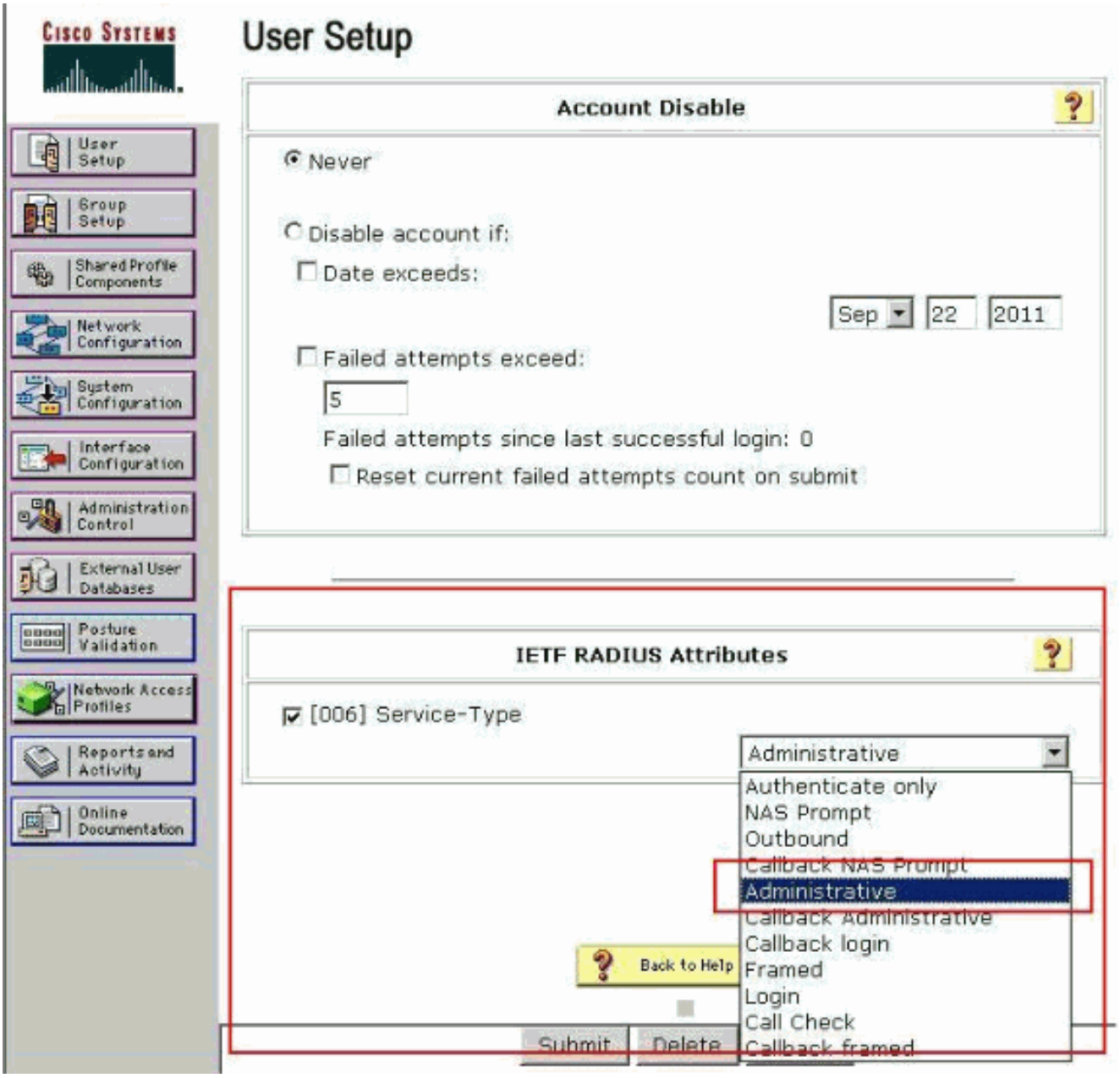
Neste exemplo, o nome de usuário e senha é **acsreadwrite**.

Termine estas etapas no Cisco Secure ACS.

1. Na interface gráfica do usuário do ACS, clique em **User Setup**.
2. Datilografe o username a ser adicionado ao ACS como este exemplo de janela mostra.

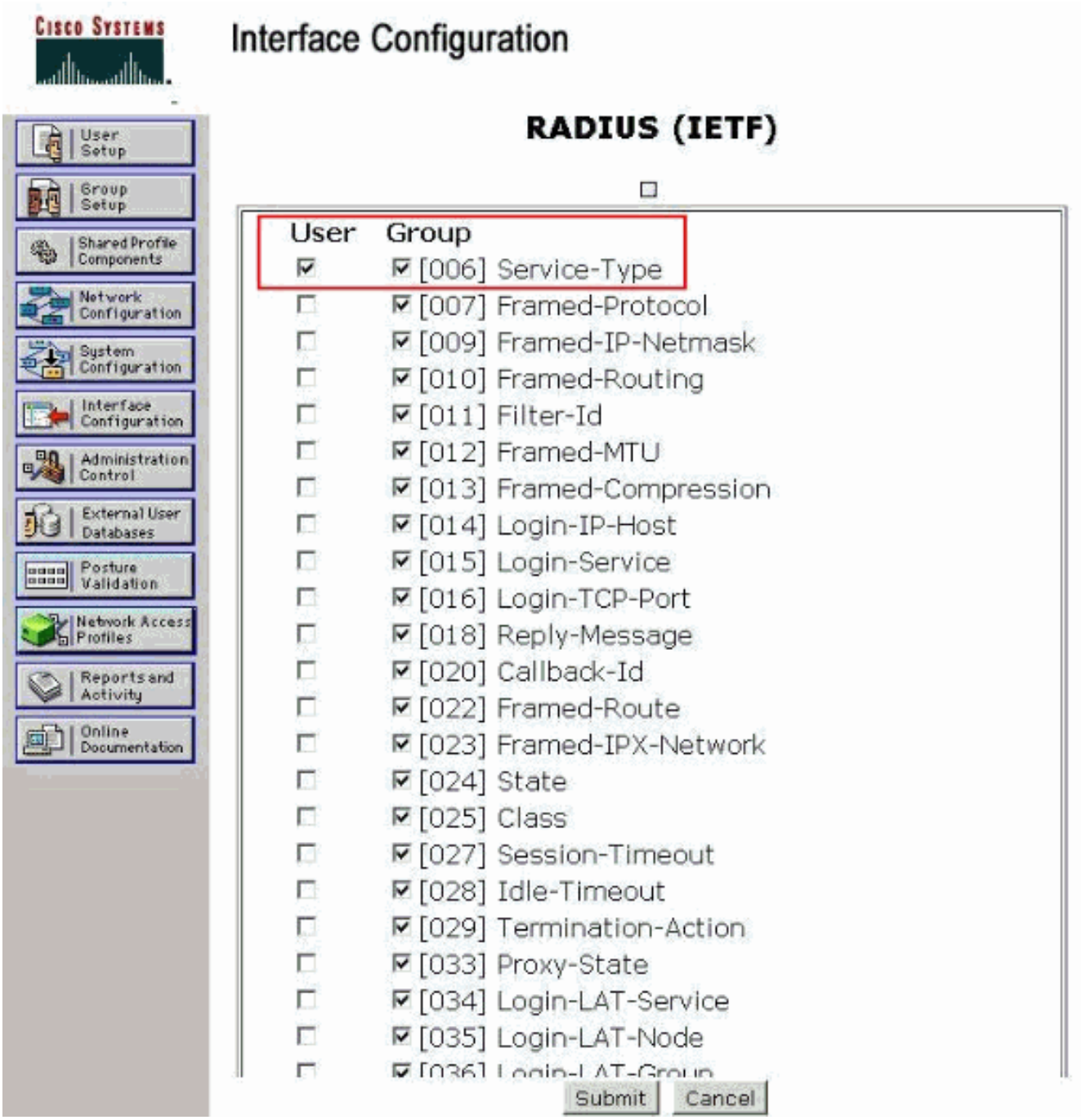


3. O clique **adiciona/edita** a fim ir ao usuário edita a página.
4. No usuário edite a página, forneça os detalhes do nome real, da descrição e da senha deste usuário.
5. Enrole para baixo os atributos de raio de IETF que ajustam-se e o **atributo de tipo de serviço da** verificação.
6. Desde que, neste exemplo, o acsreadwrite do usuário precisa de ser dado o acesso direto, escolha **administrativo** para o menu de destruição do tipo de serviço e o clique **submete-se**.Isto assegura-se de que este usuário particular tenha o acesso de leitura/gravação ao WLC.



Às vezes, este atributo de tipo de serviço não é visível sob as configurações de usuário. Nesses casos, termine estas etapas a fim fazê-lo visível.

1. Do ACS GUI, escolha a **configuração da interface > o RAIO (IETF)** a fim permitir atributos IETF no indicador da configuração do usuário.Isto toma-o à página dos ajustes do RAIO (IETF).
2. Dos ajustes página do RAIO (IETF), você pode permitir o atributo IETF que precisa de ser visível sob o usuário ou as configurações de grupo. Para esta configuração, verifique o **tipo de serviço** para ver se há a coluna do usuário e o clique **submete-se**. Este indicador mostra um
exemplo.



Nota: Este exemplo especifica a autenticação em uma base do usuário per. Você pode igualmente executar a autenticação baseada no grupo a que um usuário particular pertence. Nesses casos, permita a caixa de **verificação de atributo** de modo que este atributo seja visível sob configurações de grupo.**Nota:** Também, se a autenticação está em uma base do grupo, você precisa de atribuir usuários a um grupo particular e de configurar os atributos da configuração de grupo IETF para fornecer privilégios de acesso aos usuários desse grupo. Refira o Gerenciamento do grupo para informações detalhadas sobre de como configurar e controlar grupos.

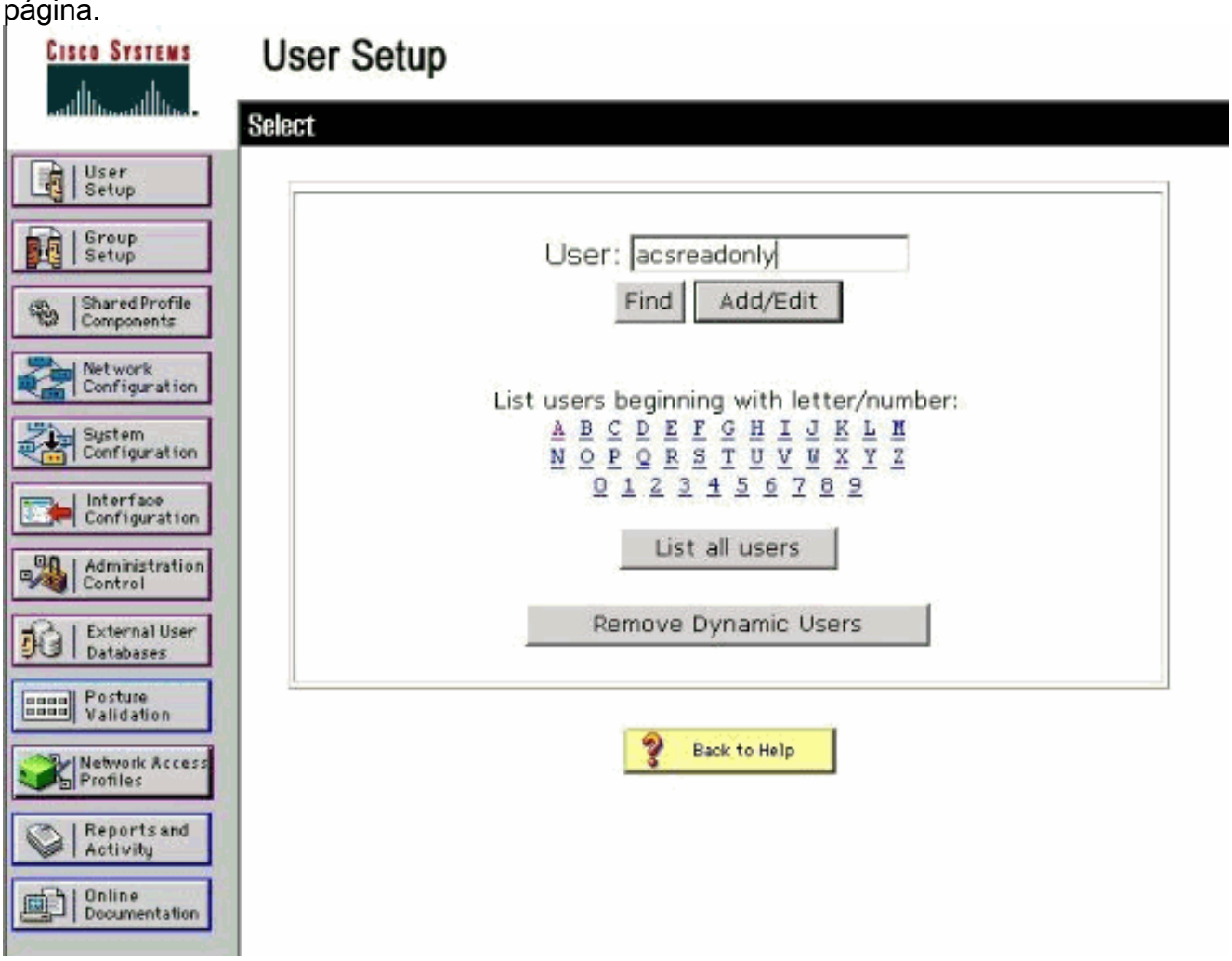
Configurar um usuário com acesso somente leitura

Este exemplo mostra a configuração de um usuário com acesso somente leitura ao WLC. Quando este usuário tenta entrar ao controlador, o servidor Radius autentica e fornece este usuário o acesso somente leitura.

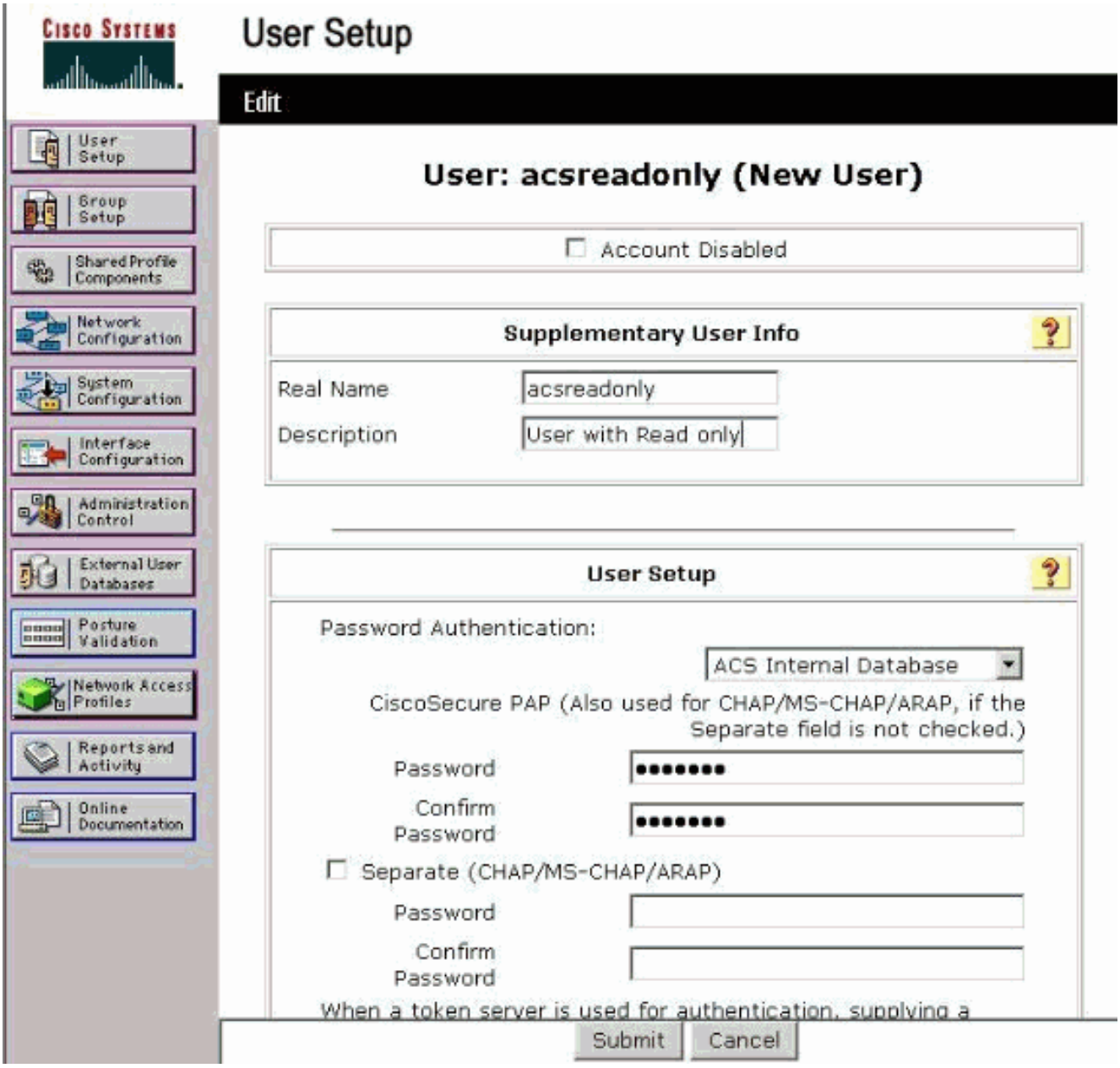
Neste exemplo, o nome de usuário e senha é **acsreadonly**.

Termine estas etapas no Cisco Secure ACS:

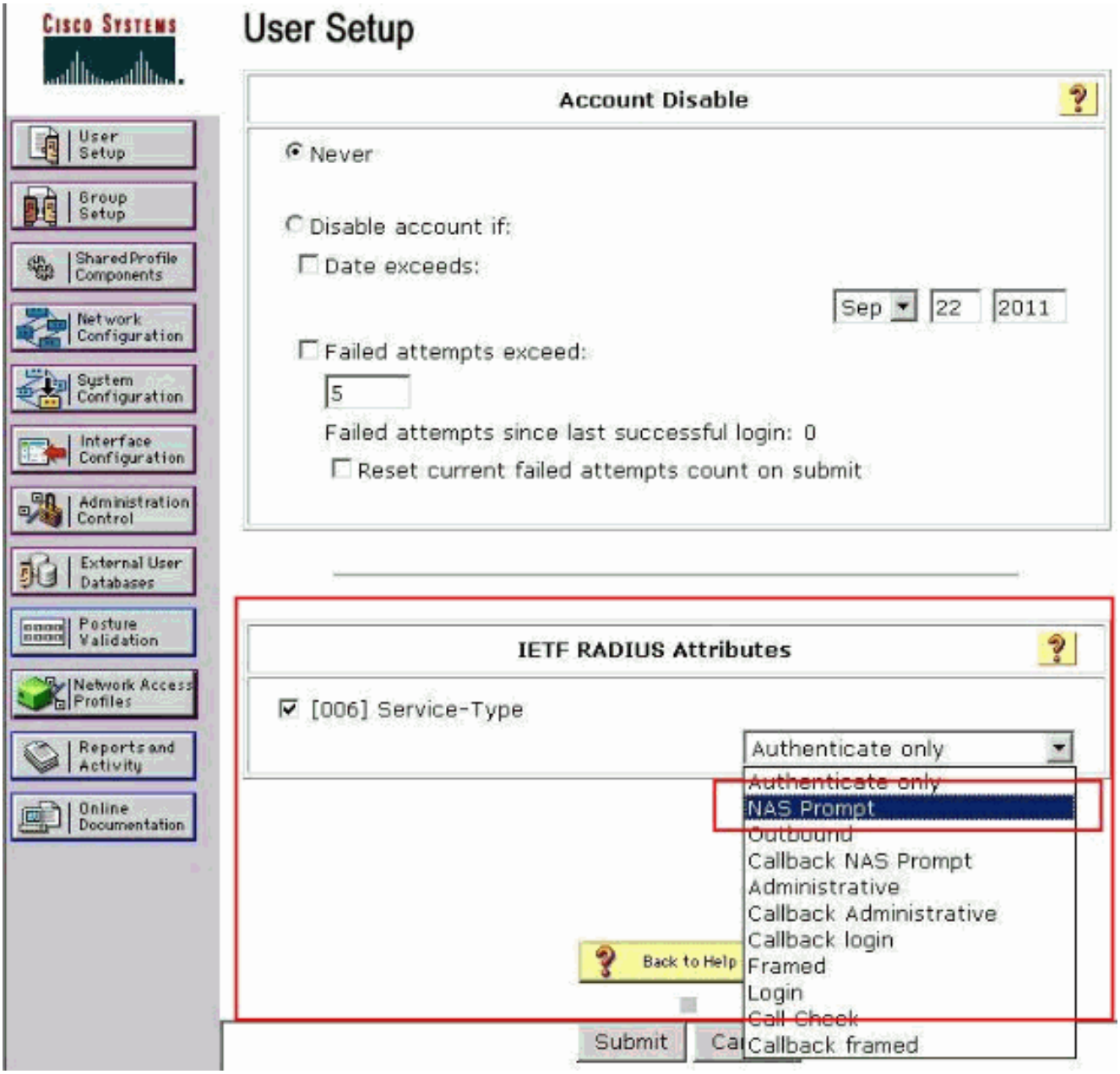
1. Na interface gráfica do usuário do ACS, clique em **User Setup**.
2. Datilografe o username que você quer adicionar ao ACS e ao clique **adiciona/edita** a fim ir ao usuário edita a
   página.



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

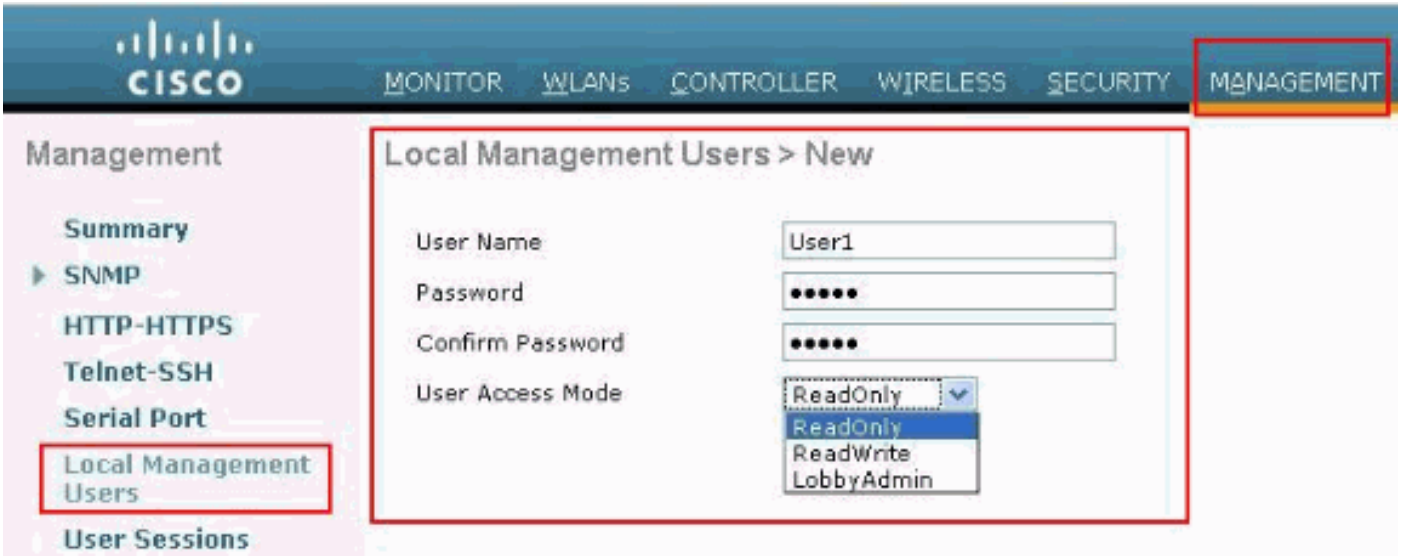


4. Enrole para baixo os atributos de raio de IETF que ajustam-se e o **atributo de tipo de serviço da** verificação.
5. Desde que, neste exemplo, o usuário precisa acsreadonly de ter o acesso somente leitura, para escolher a **alerta NAS do** menu de destruição e do clique do tipo de serviço **submeta**.Isto assegura-se de que este usuário particular tenha o acesso somente leitura ao WLC.



Controle o WLC localmente assim como através do servidor Radius

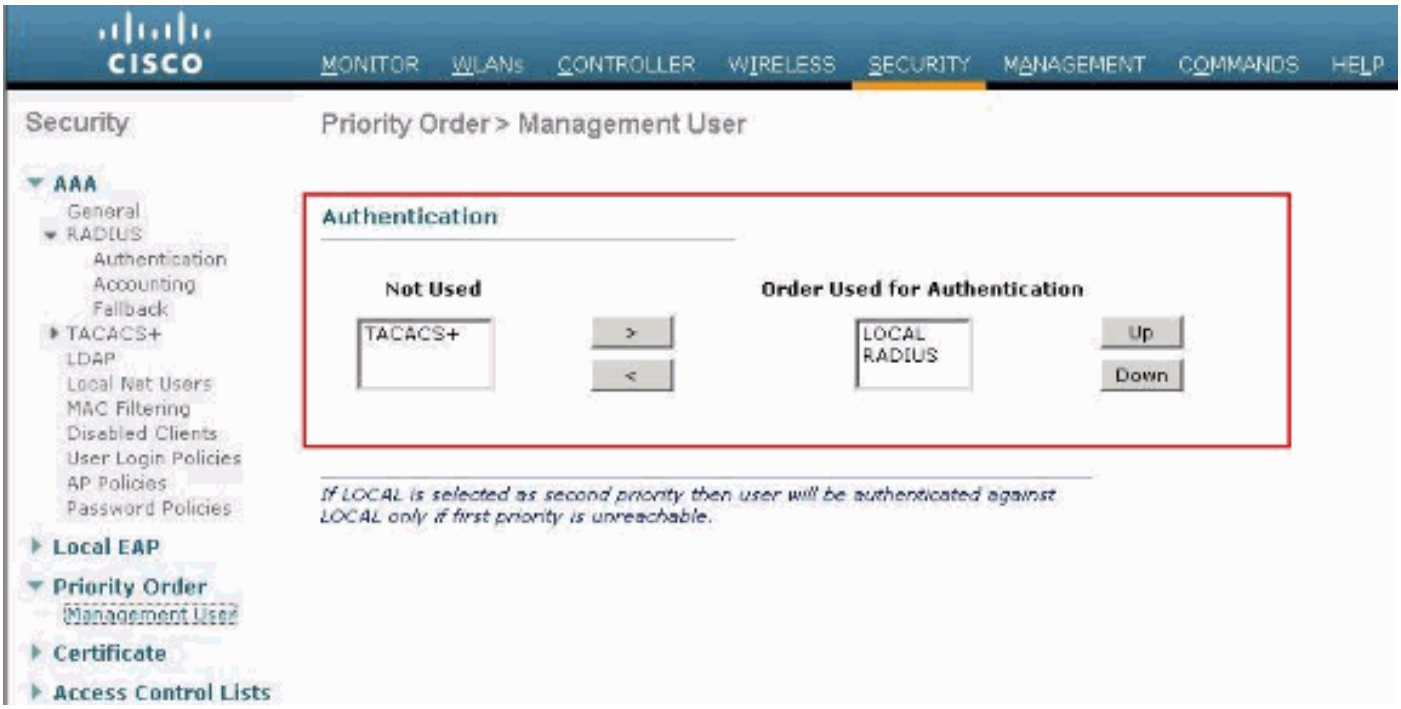
Você pode igualmente configurar os usuários do Gerenciamento localmente no WLC. Isto pode ser feito do controlador GUI, sob **usuários do Gerenciamento > do gerenciamento local**.



Supõe que o WLC está configurado com usuários do Gerenciamento localmente assim como no servidor Radius com a **caixa de verificação de gerenciamento** permitida. Em tal encenação, à revelia, quando um usuário tenta entrar ao WLC, o WLC comporta-se desse modo:

1. O WLC olha primeiramente os usuários do gerenciamento local definidos para validar o usuário. Se o usuário existe em sua lista local, a seguir permite a autenticação para este usuário. Se este usuário não aparece localmente, a seguir olha ao servidor Radius.
2. Se o mesmo usuário existe localmente assim como no servidor Radius mas com privilégios de acesso diferentes, a seguir o WLC autentica o usuário com os privilégios especificados localmente. Ou seja a configuração local no WLC toma sempre a precedência quando comparada ao servidor Radius.

A ordem de autenticação para usuários do Gerenciamento pode ser mudada no WLC. A fim fazer isto, da página da **Segurança no** WLC, **ordem da prioridade do** clique **> usuário do Gerenciamento**. Desta página você pode especificar a ordem de autenticação. Exemplo:



Nota: Se o LOCAL é selecionado como a segunda prioridade, a seguir o usuário estará autenticado usando este método somente se o método definido como a prioridade principal (RADIUS/TACACS) é inacessível.

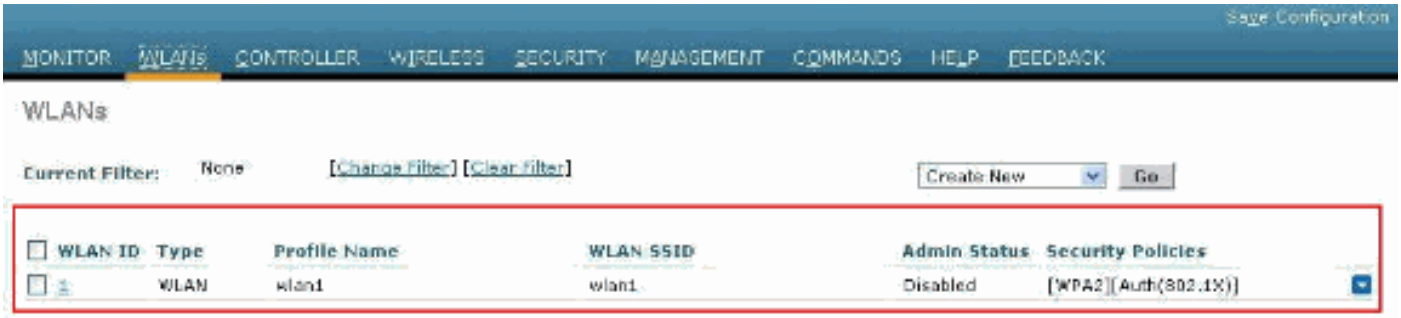
Verificar

A fim verificar se sua configuração trabalha corretamente, alcance o WLC com o modo CLI ou GUI (HTTP/HTTPS). Quando a alerta de login aparece, datilografe o nome de usuário e senha como configurado no Cisco Secure ACS.

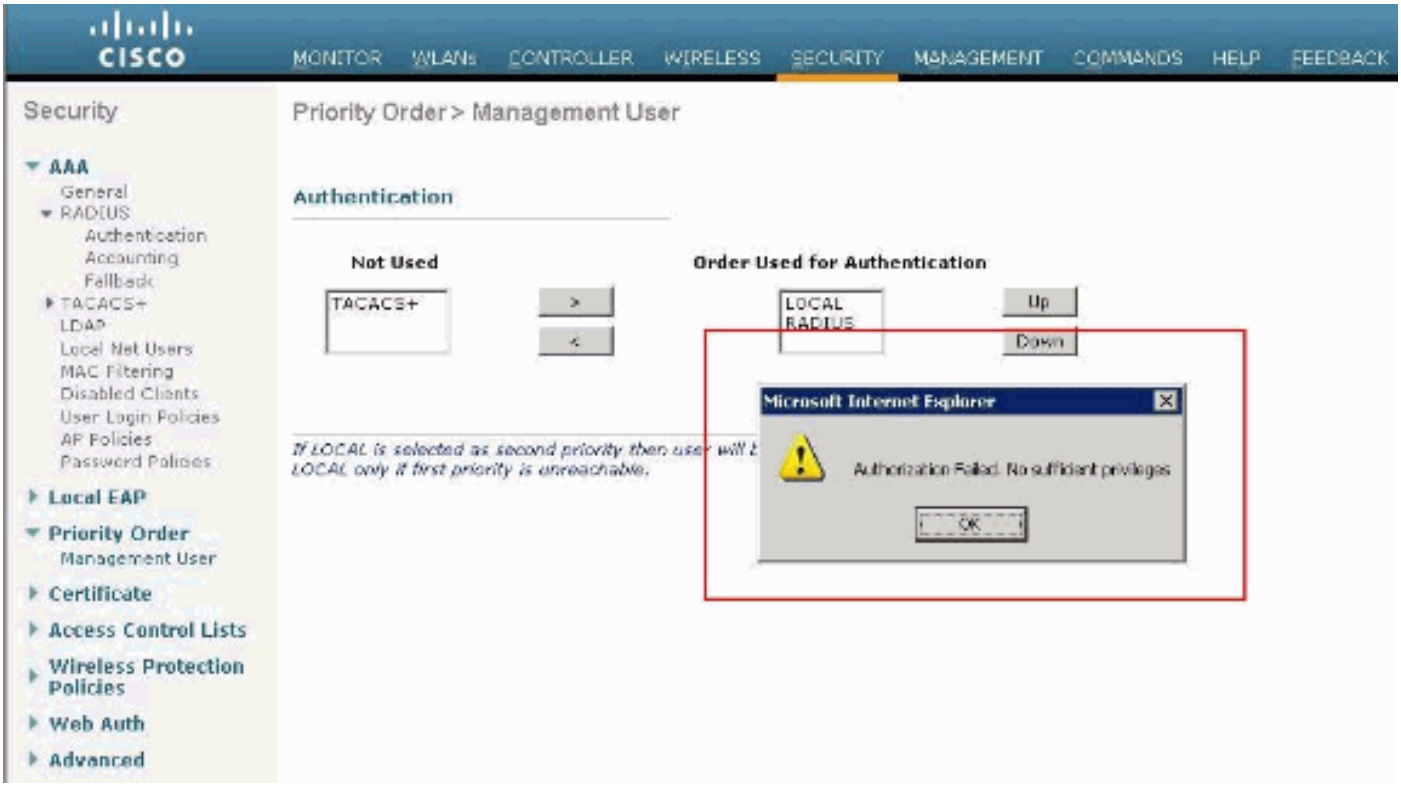
Se você tem as configurações corretas, você está autenticado com sucesso no WLC.

Você pode igualmente assegurar-se de se o usuário autenticado esteja fornecido com as restrições de acesso como especificado pelo ACS. A fim fazer assim, alcance o WLC GUI com o HTTP/HTTPS (se assegure de que o WLC esteja configurado para permitir o HTTP/HTTPS).

Um usuário com grupo de acesso de leitura/gravação no ACS tem diversos privilégios configuráveis no WLC. Por exemplo, um usuário de leitura/gravação tem o privilégio criar um WLAN novo sob a página WLAN do WLC. Este indicador mostra um exemplo.



Quando um usuário com provileges do read only tenta alterar a configuração no controlador, o usuário vê esta mensagem.



Estas restrições de acesso podem igualmente ser verificadas com o CLI do WLC. Esta saída mostra um exemplo.

```
(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 estas saídas de exemplo mostram, a**?** no controlador o CLI indica uma lista de comandos disponíveis para o usuário atual. Igualmente observe que o **comando config** não está disponível nestas saídas de exemplo. Isto ilustra que um usuário de leitura apenas não tem o privilégio fazer nenhuma configurações no WLC. Considerando que, um usuário de leitura/gravação tem os privilégios fazer configurações no controlador (GUI e modo de CLI).

Nota: Mesmo depois que você autentica um usuário WLC através do servidor Radius, porque você consulta da página para paginar, o server do [S] HTTP ainda autentica inteiramente o cliente cada vez. A única razão que você não é alertado para a autenticação em cada página é que seus caches de navegador e repetições suas credenciais.

Troubleshooting

Há determinadas circunstâncias quando um controlador autentica usuários do Gerenciamento através do ACS, os revestimentos da autenticação com sucesso (aceitação de acesso), e você não vê nenhum erro da autorização no controlador. *Mas, o usuário é alertado outra vez para a autenticação.*

Nesses casos, você não pode interpretar o que são errado e porque o usuário não pode registrar no WLC apenas usando o **comando enable dos eventos aaa debugar**. Em lugar de, o controlador indica uma outra alerta para a autenticação.

Uma razão possível para esta é que o ACS não está configurado para transmitir o atributo de tipo de serviço para esse usuário particular ou para o agrupar mesmo que o nome de usuário e senha seja configurado corretamente no ACS.

A saída do **comando enable dos eventos aaa debugar** não indica que um usuário não tem os atributos requerido (para este exemplo, o atributo de tipo de serviço) mesmo que uma **aceitação de acesso** seja enviada para trás do servidor AAA. Este exemplo **debuga o comando enable que dos eventos aaa a** saída mostra um exemplo.

```
 (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 **debugar a** saída do **comando enable dos eventos aaa**, você veem que a aceitação de acesso está recebida com sucesso do servidor Radius mas o atributo de tipo de serviço não está passado no WLC. Isto é porque o usuário particular não é configurado com este atributo no ACS.

O Cisco Secure ACS precisa de ser configurado para retornar o atributo de tipo de serviço após a autenticação de usuário. O valor de atributo do tipo de serviço deve ser ajustado a **administrativo** ou à NAS-**alerta** de acordo com os privilégios do usuário.

Este segundo exemplo mostra o **comando enable dos eventos aaa debugar** output outra vez. Contudo, esta vez o atributo de tipo de serviço é ajustado a **administrativo no** ACS.

```
(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 nestas saídas de exemplo que o atributo de tipo de serviço está passado no WLC.

Informações Relacionadas

- Configurando o guia de configuração de controle do Wireless LAN
- VLAN no exemplo de configuração dos controladores do Wireless LAN
- Exemplo de configuração de atribuição da VLAN dinâmica com servidor RADIUS e Wireless LAN Controller
- Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight
- Grupo VLAN AP com exemplo de configuração dos controladores do Wireless LAN
- Suporte Técnico e Documentação - Cisco Systems