Autenticação do Administrador do Lobby de Controladoras Wireless LAN via servidor RADIUS

Índice

Introdução

Este documento explica as etapas de configuração envolvidas para autenticar um administrador da entrada do controlador do Wireless LAN (WLC) com um servidor 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, tal como o Cisco Secure ACS
- Conhecimento dos usuários convidado no WLC

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.

Informações de Apoio

Um administrador da entrada, igualmente conhecido como um embaixador da entrada de um WLC, pode criar e controlar contas de usuário convidado no controlador do Wireless LAN (WLC). O embaixador da entrada limitou privilégios da configuração e pode alcançar somente os página da web usados para controlar as contas do convidado. O embaixador da entrada pode especificar a quantidade de tempo que as contas de usuário convidado permanecem ativas. Após as passagens do tempo especificado, as contas de usuário convidado expiram automaticamente.

Refira o guia de distribuição: Acesso do convidado de Cisco usando o controlador de LAN do Cisco Wireless para obter mais informações sobre dos usuários convidado.

A fim criar uma conta de usuário convidado no WLC, você precisa de entrar ao controlador como um administrador da entrada. Este documento explica como um usuário é autenticado no WLC como um administrador da entrada baseado nos atributos retornou pelo servidor Radius.

Nota: A Autenticação do Administrador da entrada pode igualmente ser executada baseou na conta de administrador da entrada configurada localmente no WLC. Refira a criação de um embaixador da entrada esclarecem a informação de como criar localmente uma conta de administrador da entrada em um controlador.

Configurar

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

Configurações

Este documento utiliza as seguintes configurações:

- O endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento do WLC é 10.77.244.212/27.
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius é 10.77.244.197/27.
- A chave secreta compartilhada que é usada no Access Point (AP) e no servidor Radius é cisco123.
- O nome de usuário e senha do administrador da entrada configurado no servidor Radius é

ambo lobbyadmin.

No exemplo de configuração neste documento, todo o usuário que registra no controlador com nome de usuário e senha como o lobbyadmin é atribuído o papel de um administrador da entrada.

Configuração de WLC

Antes que você comece a configuração necessária WLC, assegure-se de que seu controlador execute a versão 4.0.206.0 ou mais tarde. Isto é devido à identificação de bug Cisco CSCsg89868 (clientes registrados somente) em que a interface da WEB do controlador indica página da web errados para o usuário de LobbyAdmin quando o username é armazenado em um base de dados RADIUS. O LobbyAdmin é presentado com a relação de leitura apenas em vez da relação de LobbyAdmin.

Este erro foi resolvido na versão 4.0.206.0 WLC. , Assegure-se de consequentemente que sua versão do controlador seja 4.0.206.0 ou mais tarde. Refira o upgrade de software do controlador do Wireless LAN (WLC) para instruções em como promover seu controlador à versão apropriada.

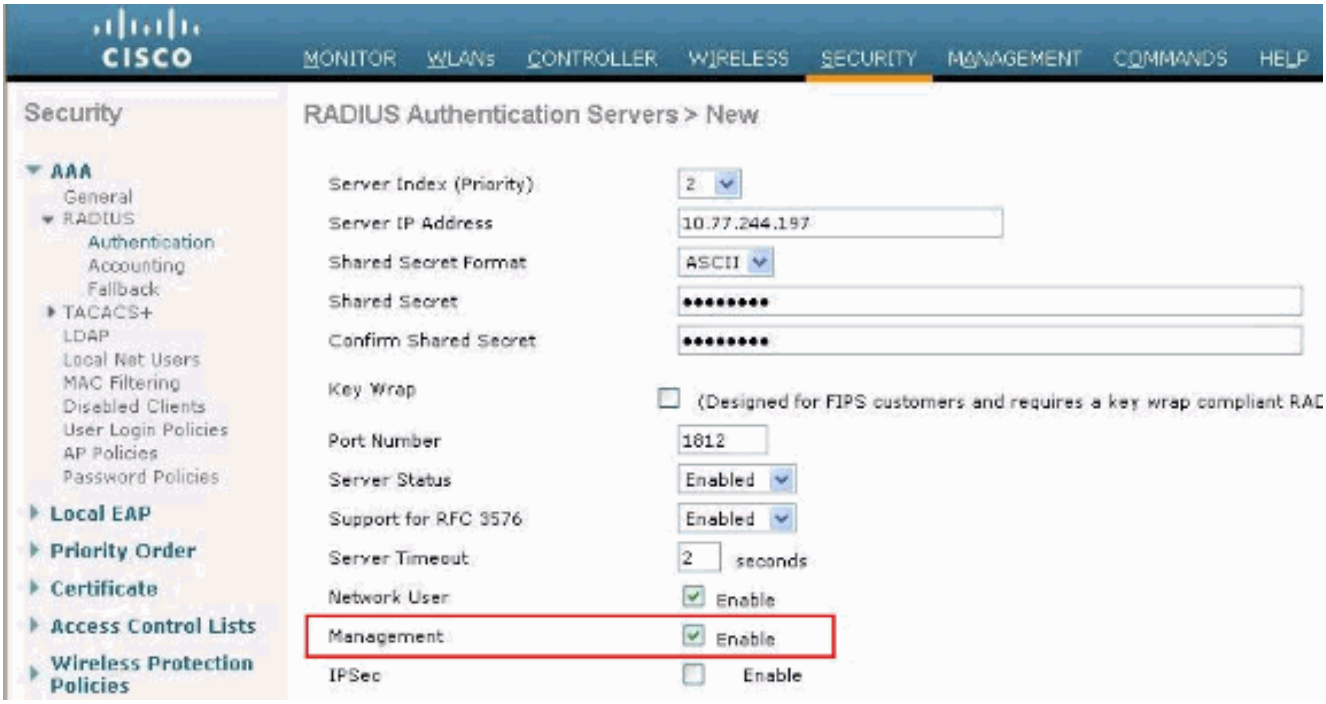
A fim executar a autenticação do Gerenciamento do controlador com o servidor Radius, assegure-se de que a bandeira do Admin-AUTH-através-**RAIO** esteja permitida no controlador. Isto pode ser verificado da saída do **comando summary do raio da mostra**.

A primeira etapa é configurar a informação do servidor Radius no controlador e estabelecer a alcançabilidade da camada 3 entre o controlador e o servidor Radius.

Configurar a informação do servidor Radius no controlador

Termine estas etapas a fim configurar o WLC com detalhes sobre o ACS:

1. Do WLC GUI, escolha a **ABA de segurança** e configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT e o segredo compartilhado do servidor ACS.Este segredo compartilhado precisa de ser o mesmo no ACS para que o WLC comunique-se com o ACS.**Nota:** O segredo compartilhado ACS é diferenciando maiúsculas e minúsculas. , Certifique-se consequentemente incorporar corretamente a informação secreta compartilhada.Esta figura mostra um exemplo:



2. Verifique a **caixa de verificação de gerenciamento** a fim permitir que o ACS controle os usuários WLC segundo as indicações da figura em etapa 1. Então, o clique **aplica-se**.
3. Verifique a alcançabilidade da camada 3 entre o controlador e o servidor radius configurado com a ajuda do **comando ping**. Esta opção do sibilo está igualmente disponível na página do servidor radius configurado no WLC GUI na aba da **autenticação de Security>RADIUS**.Este diagrama mostra uma resposta do ping bem-sucedido do servidor Radius. Consequentemente, a alcançabilidade da camada 3 está disponível entre o controlador e o servidor
Radius.

Configuração de servidor RADIUS

Termine as etapas nestas seções a fim configurar o servidor Radius:

1. Adicionar o WLC como um cliente de AAA ao servidor Radius
2. Configurar o atributo de tipo de serviço apropriado do RAIO IETF para um administrador da entrada

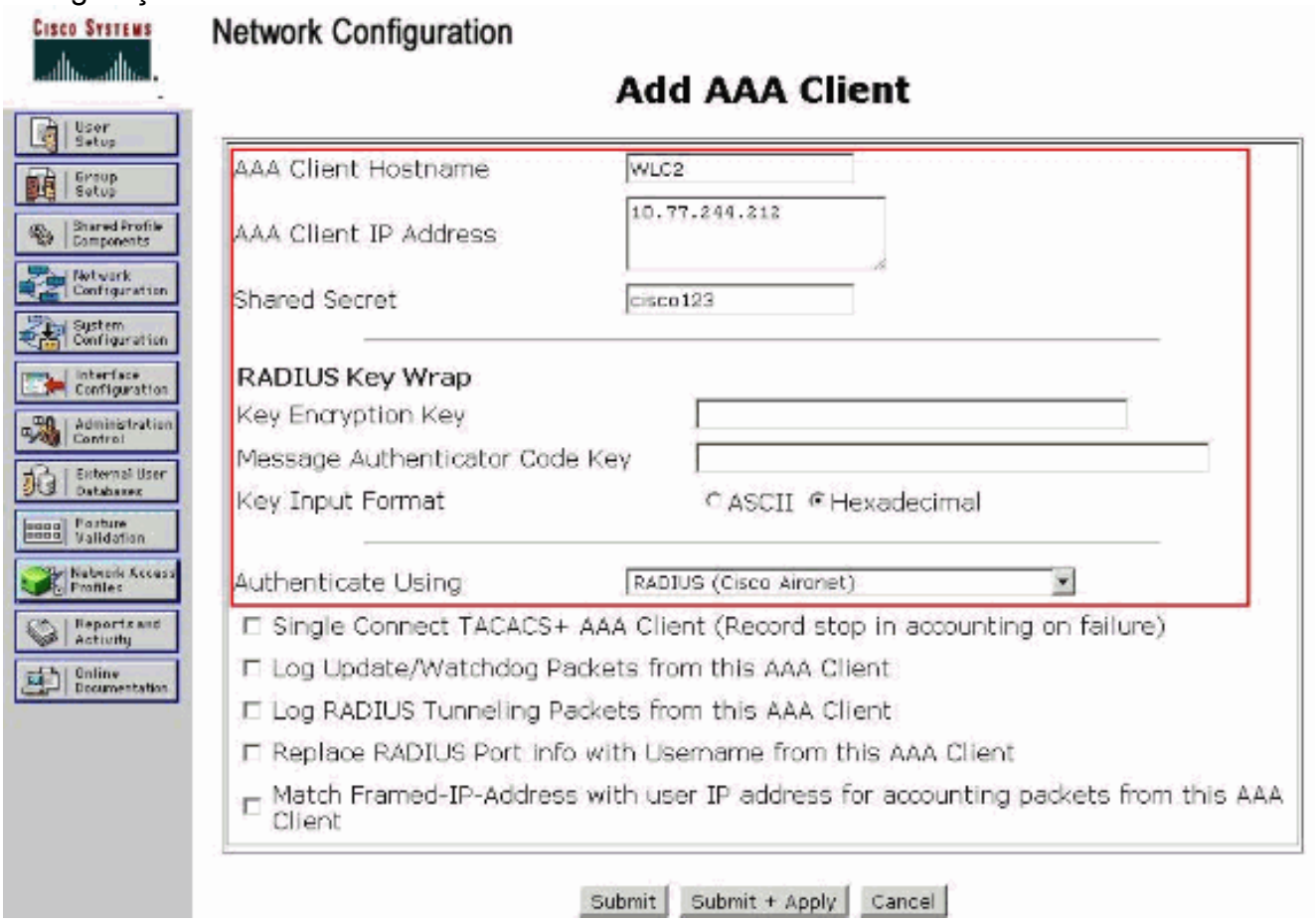
Adicionar o WLC como um cliente de AAA ao servidor Radius

Termine estas etapas a fim adicionar o WLC como um cliente de AAA no servidor Radius. Como

mencionado mais cedo, este documento usa o ACS como o servidor Radius. Você pode usar todo o servidor Radius para esta configuração.

Termine estas etapas a fim adicionar o WLC como um cliente de AAA no ACS:

1. Do ACS GUI, escolha a aba da **configuração de rede**.
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. Veja o diagrama do exemplo sob a etapa 5.
4. Da autenticação usando o menu suspenso, escolha o **RAIO (Cisco Aironet)**.
5. Clique **Submit + Restart** a fim salvar a configuração.



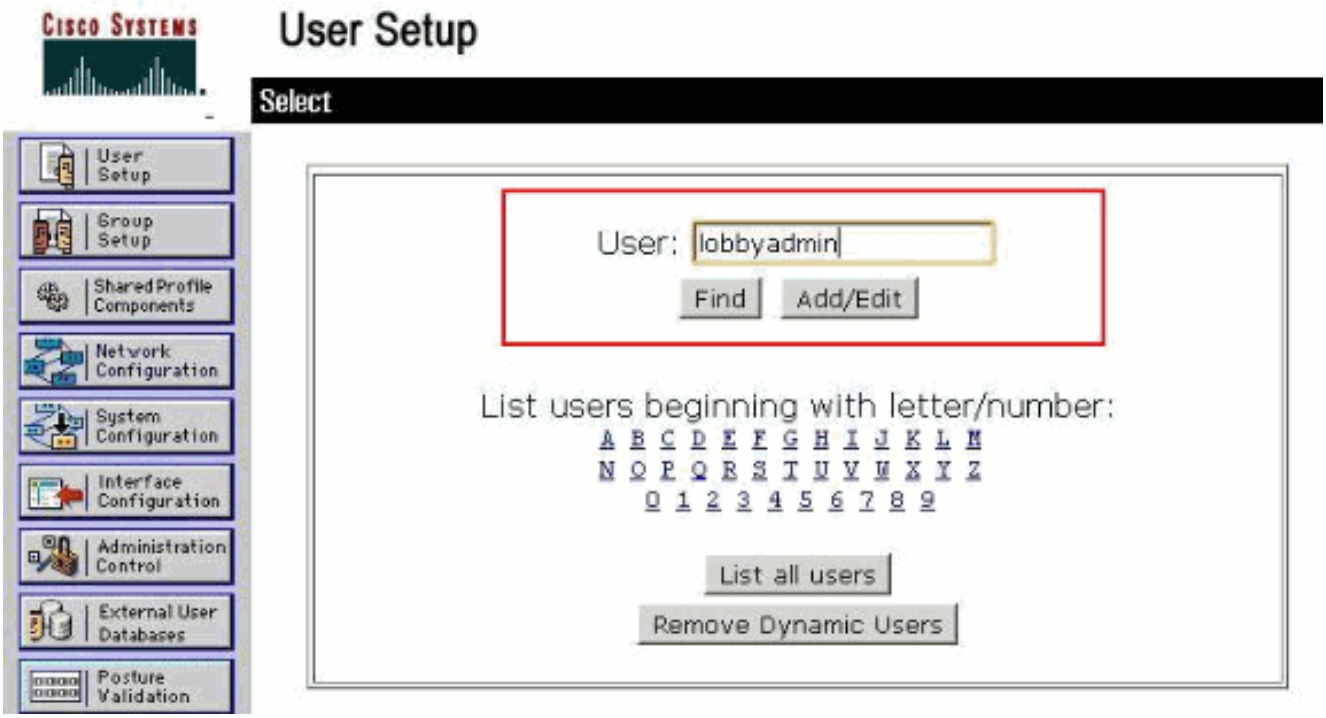
Configurar o atributo de tipo de serviço apropriado do RAIO IETF para um administrador da entrada

A fim autenticar um usuário do Gerenciamento de um controlador como um administrador da entrada através do servidor Radius, você deve adicionar o usuário ao base de dados RADIUS com o atributo de tipo de serviço do RADIUS IETF ajustado à **rechamada administrativo**. Este atributo atribui ao usuário específico o papel de um administrador da entrada em um controlador.

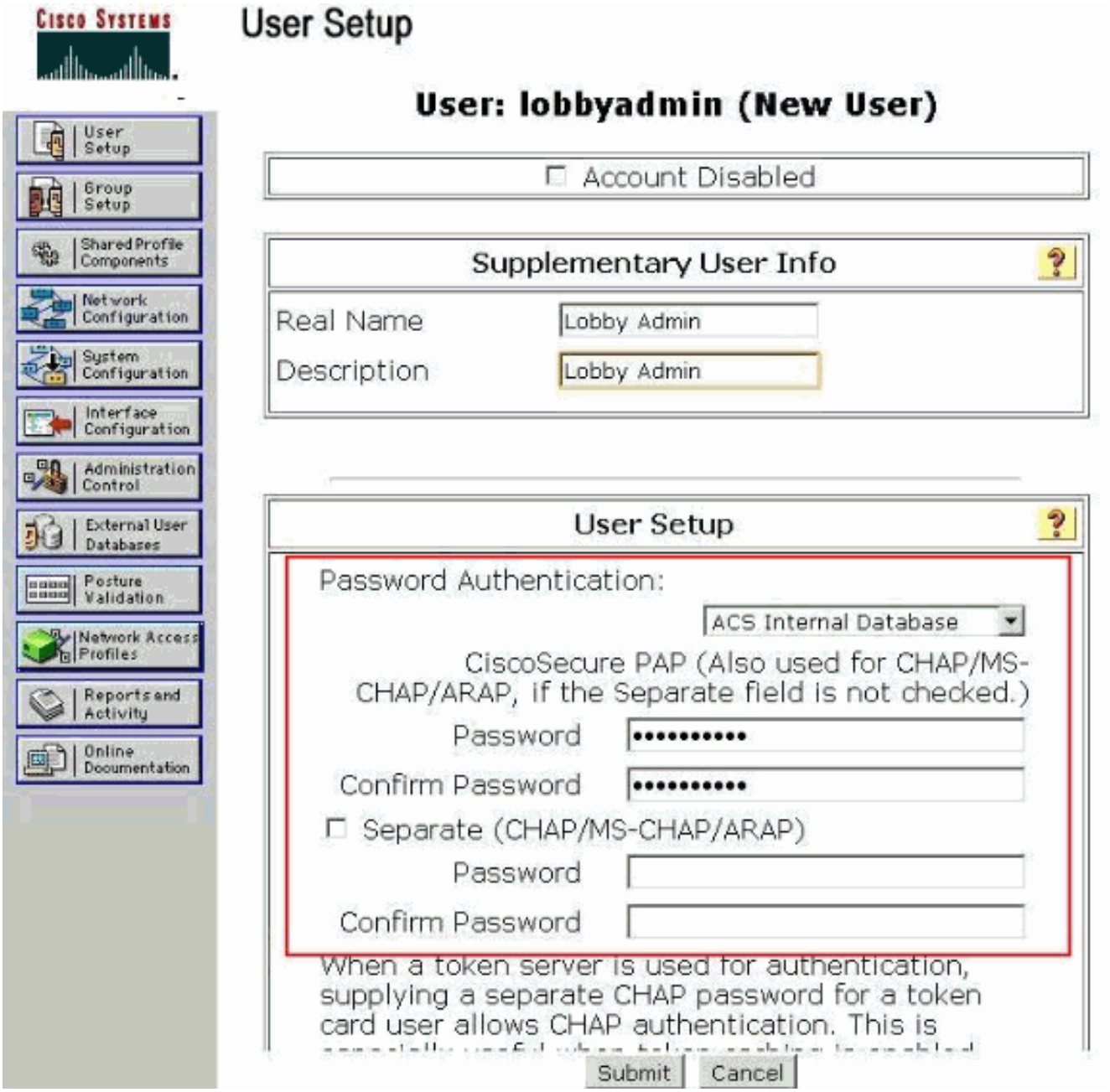
Este documento mostra o lobbyadmin do usuário do exemplo como um administrador da entrada. A fim configurar este usuário, termine estas etapas no ACS:

1. Do ACS GUI, escolha a aba da **instalação de usuário**.
2. Incorpore o username a ser adicionado ao ACS como este exemplo de janela

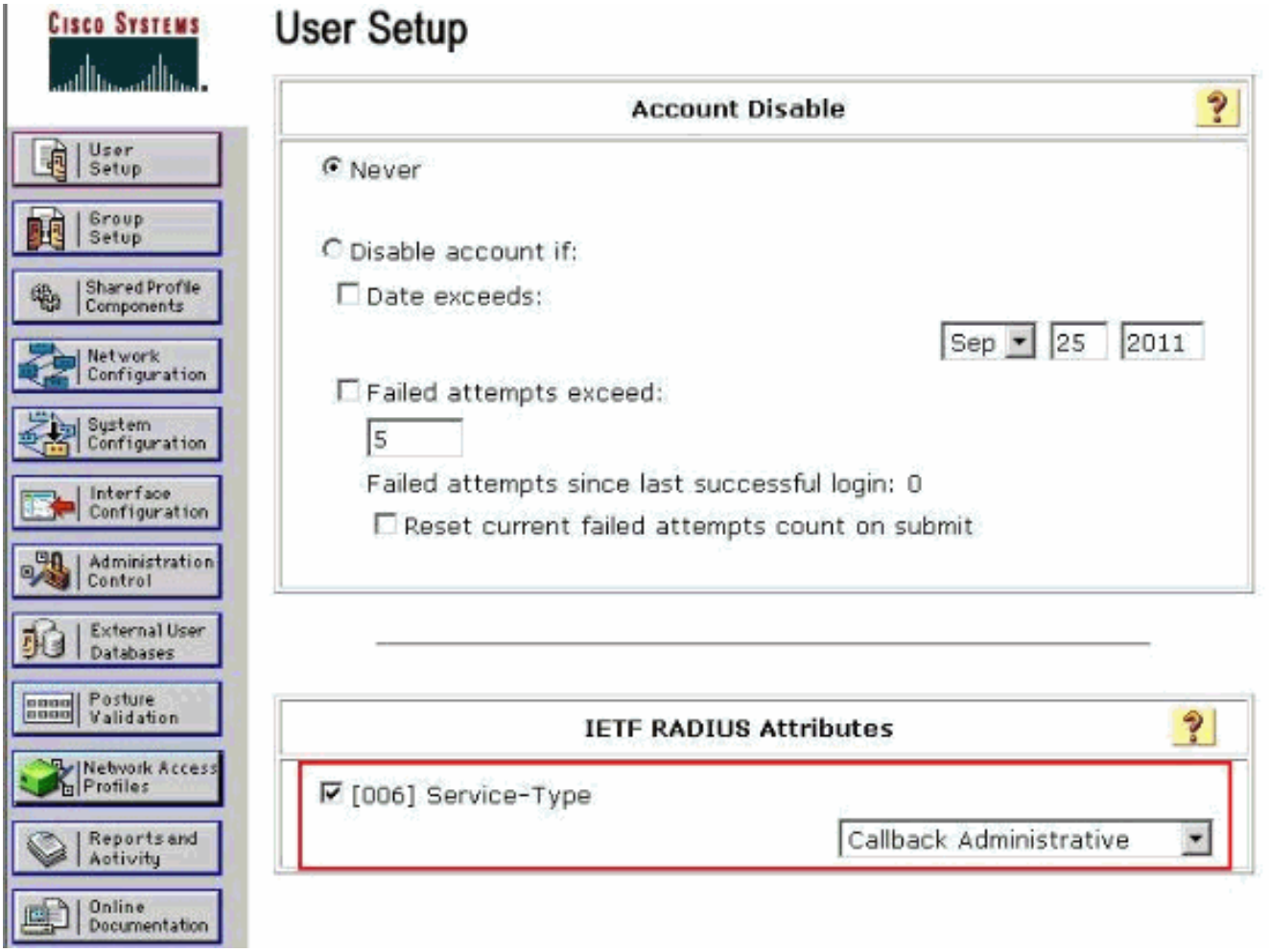
mostra:



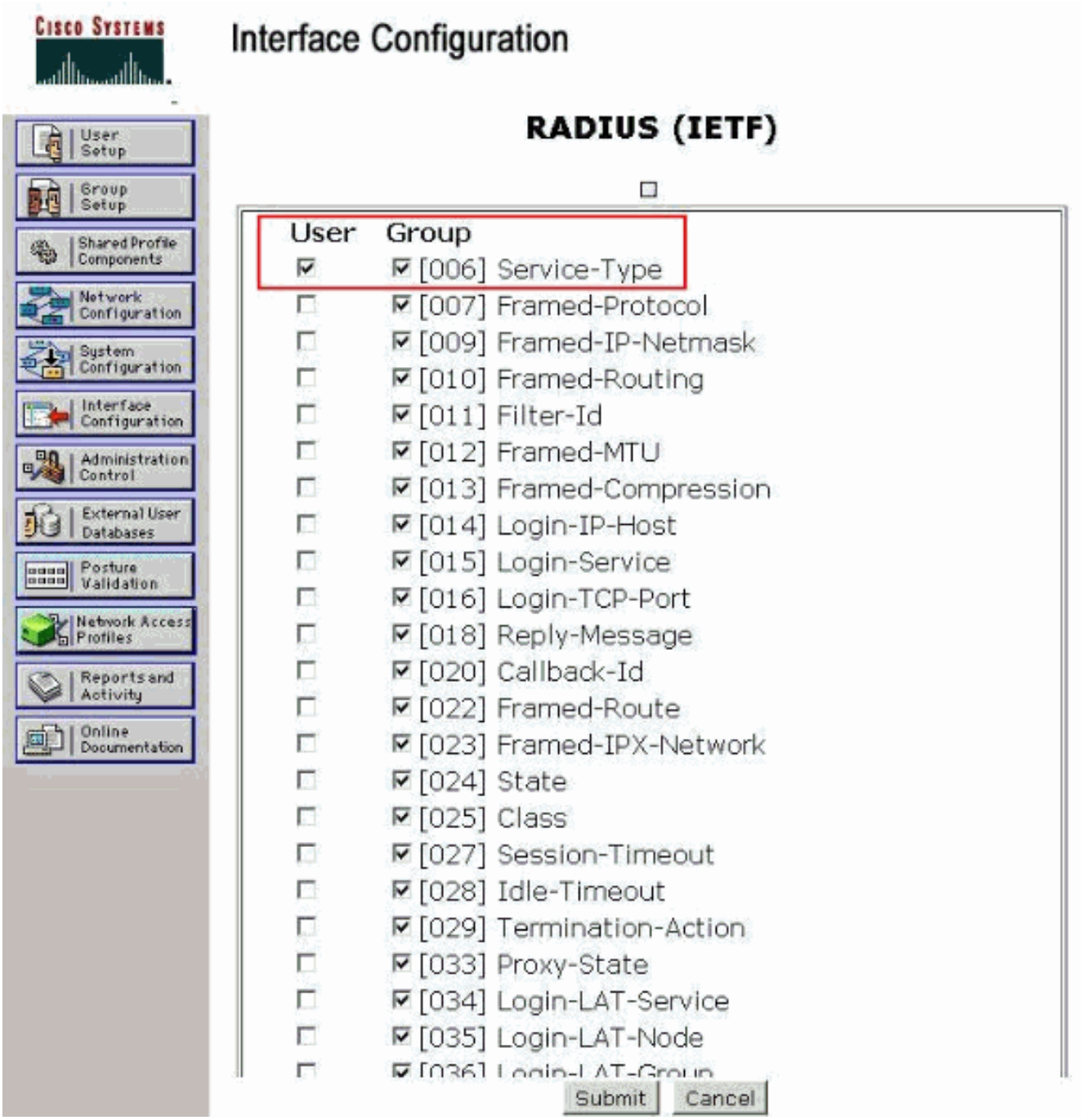
3. O clique **adiciona/edita** a fim ir ao usuário edita a página.
4. No usuário edite a página, forneça os detalhes do nome real, da descrição e da senha deste usuário.Neste exemplo, o nome de usuário e senha usado é ambo lobbyadmin.



5. Enrole para baixo os atributos de raio de IETF que ajustam-se e verifique a caixa de verificação do **atributo de tipo de serviço**.
6. Escolha a **rechamada administrativa do** menu de destruição do tipo de serviço e o clique **submete-se**.Este é o atributo que atribui a este usuário o papel de um administrador da entrada.



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:Do ACS GUI, escolha a **configuração da interface > o RAIO (IETF)** a fim permitir atributos IETF no indicador da configuração do usuário.Isto trá-lo à página dos ajustes do RAIO (IETF).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, verifique 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 de usuário para informações detalhadas sobre de como configurar e controlar grupos.

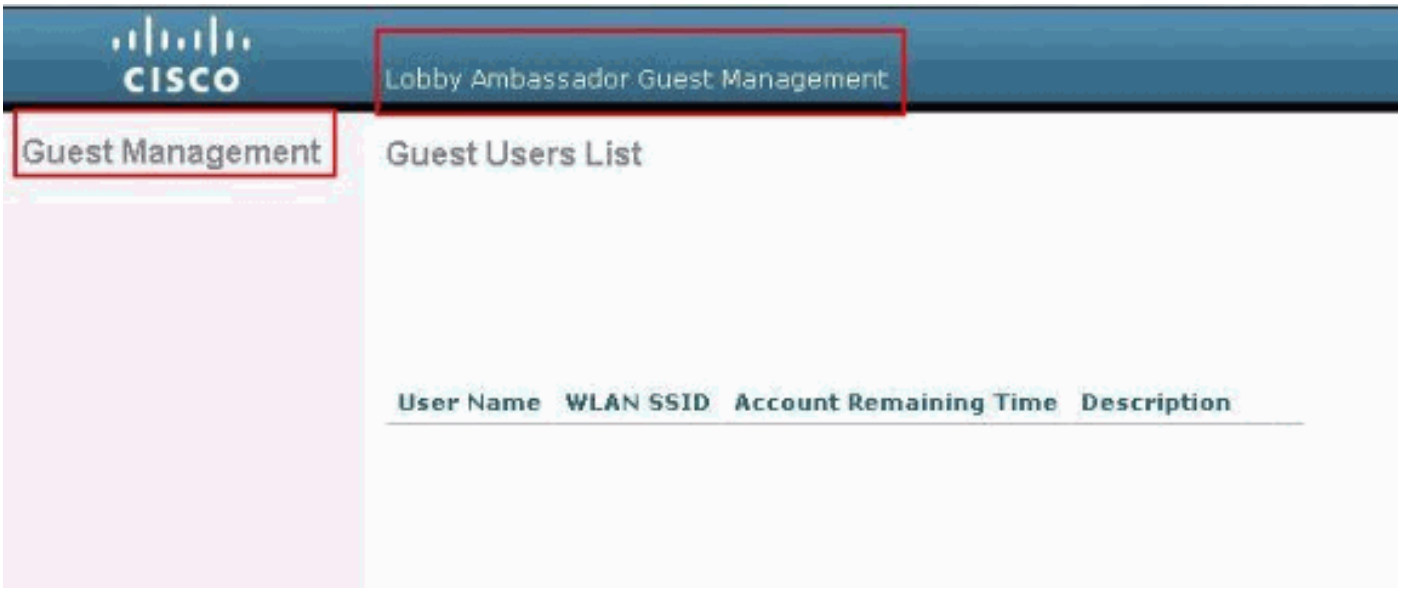
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A fim verificar que sua configuração trabalha corretamente, alcance o WLC com o modo GUI (HTTP/HTTPS).

Nota: Um embaixador da entrada não pode alcançar a interface CLI do controlador e pode consequentemente criar contas de usuário convidado somente do controlador GUI.

Quando a alerta de login aparece, incorpore o nome de usuário e senha como configurado no ACS. Se você tem as configurações corretas, você está autenticado com sucesso no WLC como o **administrador da entrada**. Este exemplo mostra como o GUI de um administrador da entrada ocupa da autenticação bem sucedida:



Nota: Você pode ver que um administrador da entrada não tem nenhuma outra opção independentemente do Gerenciamento do usuário convidado.

A fim verificá-la do modo de CLI, telnet no controlador como um administrador de leitura/gravação. Emita o **comando debug aaa all enable no** controlador CLI.

```
(Cisco Controller) >debug aaa all enable (Cisco Controller) > *aaaQueueReader: Aug 26
18:07:35.072: ReProcessAuthentication previous proto 28, next proto 20001 *aaaQueueReader: Aug
26 18:07:35.072: AuthenticationRequest: 0x3081f7dc *aaaQueueReader: Aug 26 18:07:35.072:
Callback.....0x10756dd0 *aaaQueueReader: Aug 26 18:07:35.072:
protocolType.....0x00020001 *aaaQueueReader: Aug 26 18:07:35.072:
proxyState.....00:00:00:40: 00:00-00:00 *aaaQueueReader: Aug 26
18:07:35.072: Packet contains 5 AVPs (not shown) *aaaQueueReader: Aug 26 18:07:35.072:
apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr: 0x0, gw:0x0, mask:0x0, vlan:0,
dpPort:0, srcPort:0 *aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful
transmission of Authentication Packet (id 39) to 10.77.244.212:1812, proxy state
00:00:00:40:00:00-00:01 *aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00
00 00 00 00 00 00 00 00 .'.G..... *aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00
00 00 01 0c 6c 6f 62 62 79 61 64 6d 69 6e ......lobbyadmin *aaaQueueReader: Aug 26 18:07:35.073:
00000020: 02 12 5f 5b 5c 12 c5 c8 52 d3 3f 4f 4f 8e 9d 38 .._[\...R.?OO..8 *aaaQueueReader: Aug
26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07 04 06 0a 4e b1 1a 20 09 B.....N....
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1 f8 .'.@~.mS=.y..... *radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06
ff ffff ff 06 06 00 00 00 0b .Z.O..... *radiusTransportThread: Aug 26 18:07:35.080:
00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f 61 34 ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69 6e eb11a/lobbyadmin *radiusTransportThread: Aug 26 18:07:35.080: ****Enter
processIncomingMessages: response code=2 *radiusTransportThread: Aug 26 18:07:35.080: ****Enter
processRadiusResponse: response code=2 *radiusTransportThread: Aug 26 18:07:35.080:
00:00:00:40:00:00 Access-Accept received from RADIUS server 10.77.244.212 for mobile
00:00:00:40:00:00 receiveId = 0 *radiusTransportThread: Aug 26 18:07:35.080:
AuthorizationResponse: 0x13c73d50 *radiusTransportThread: Aug 26 18:07:35.080:
structureSize.....118 *radiusTransportThread: Aug 26 18:07:35.080:
```

```
resultCode.....................0 *radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.....................0x00000001 *radiusTransportThread: Aug 26
18:07:35.080: proxyState.....00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080: Packet contains 3 AVPs: *radiusTransportThread: Aug
26 18:07:35.080: AVP[01] Framed-IP-Address.....0xffffffff (-1) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080: AVP[02] Service-
Type.....0x0000000b (11) (4 bytes) *radiusTransportThread: Aug 26
18:07:35.080: AVP[03] Class..... CACS:0/ae26/a4eb11a/lobbyadmin
(30 bytes) *emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin
```

Na informação destacada nesta saída, você pode ver que o atributo de tipo de serviço 11 (rechamada administrativa) está passado no controlador do servidor ACS e do usuário está entrado como um administrador da entrada.

Estes comandos puderam ser da ajuda adicional:

- **debugar detalhes aaa permitem**
- **debugar eventos aaa permitem**
- **debug aaa packets enable**

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Troubleshooting

Quando você entra a um controlador com privilégios do embaixador da entrada, você não pode criar uma conta de usuário convidado com de “um valor do tempo da vida **0"**, que seja uma conta que nunca expire. Nestas situações, você recebe o `valor da vida não pode ser 0` Mensagens de Erro.

Isto é devido à identificação de bug Cisco CSCsf32392 (clientes registrados somente), que é encontrada principalmente com versão 4.0 WLC. Este erro foi resolvido na versão 4.1 WLC.

Informações Relacionadas

- Autenticação de servidor Radius de usuários do Gerenciamento no exemplo da configuração de controle
- Configuração da rede de Cisco Unified Wireless TACACS+
- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 4.0 - Controlando contas de usuário
- ACL no exemplo da configuração de controle do Wireless LAN
- Controlador do Wireless LAN (WLC) FAQ
- ACL em controladores do Wireless LAN: Regras, limitações, e exemplos
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Exemplo de configuração da autenticação da Web do controlador do Wireless LAN
- Convidado WLAN e WLAN interno usando o exemplo de configuração WLC
- Suporte Técnico e Documentação - Cisco Systems