

# Configuração TACACS+ da Cisco Unified Wireless Network

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Implementação TACACS+ no controlador](#)

[Autenticação](#)

[Autorização](#)

[Relatório](#)

[Configuração TACACS+ na WLC](#)

[Adicionar um servidor de autenticação TACACS+](#)

[Adicionar um servidor de autorização TACACS+](#)

[Adicionar um servidor de contabilidade TACACS+](#)

[Configurar o pedido de autenticação](#)

[Verifique a configuração](#)

[Configurar o servidor Cisco Secure ACS](#)

[Configuração de rede](#)

[Configuração da interface](#)

[Configuração de usuário/grupo](#)

[Registros contábeis no Cisco Secure ACS](#)

[Configuração TACACS+ no WCS](#)

[WCS usando domínios virtuais](#)

[Configurar o Cisco Secure ACS para usar o WCS](#)

[Configuração de rede](#)

[Configuração da interface](#)

[Configuração de usuário/grupo](#)

[Debugs](#)

[Depurações do WLC para role1=ALL](#)

[Depurações de WLC para várias funções](#)

[Depurações de uma WLC para falha de autorização](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento fornece um exemplo de configuração do Terminal Access Controller Access Control System Plus (TACACS+) em um Controller de LAN Wireless (WLC) e de um Cisco

Wireless Control System (WLC) para uma Cisco Unified Wireless Network. Este documento também fornece dicas básicas de troubleshooting.

TACACS+ é um protocolo cliente/servidor que fornece segurança centralizada para usuários que tentam obter acesso de gerenciamento a um roteador ou servidor de acesso à rede. O TACACS+ fornece estes serviços AAA:

- Autenticação dos usuários que tentam fazer login no equipamento de rede
- Autorização para determinar que nível de acesso os usuários devem ter
- Contabilização para acompanhar todas as alterações feitas pelo usuário

Consulte [Configuração do TACACS+](#) para obter mais informações sobre os serviços AAA e a funcionalidade TACACS+.

Consulte [Comparação TACACS+ e RADIUS](#) para uma comparação de TACACS+ e RADIUS.

## [Prerequisites](#)

### [Requirements](#)

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como configurar WLCs e pontos de acesso lightweight (LAPs) para operação básica
- Conhecimento de Lightweight Access Point Protocol (LWAPP) e métodos de segurança sem fio
- Conhecimento básico RADIUS e TACACS+
- Conhecimento básico da configuração do Cisco ACS

### [Componentes Utilizados](#)

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

- Cisco Secure ACS para Windows versão 4.0
- Cisco Wireless LAN Controller que executa a versão 4.1.171.0. A funcionalidade TACACS+ em WLCs é suportada na versão de software 4.1.171.0 ou posterior.
- Cisco Wireless Control System que executa a versão 4.1.83.0. A funcionalidade TACACS+ no WCS é suportada na versão de software 4.1.83.0 ou posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### [Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

## [Implementação TACACS+ no controlador](#)

## Autenticação

A autenticação pode ser realizada usando um banco de dados local, RADIUS ou servidor TACACS+ que usa um nome de usuário e uma senha. A implementação não é totalmente modular. Os serviços de autenticação e autorização estão ligados entre si. Por exemplo, se a autenticação for executada usando o banco de dados RADIUS/local, a autorização não será executada com TACACS+. Ele usaria as permissões associadas para o usuário no banco de dados local ou RADIUS, como somente leitura ou leitura/gravação, enquanto quando a autenticação é executada com TACACS+, a autorização é vinculada ao TACACS+.

Nos casos em que vários bancos de dados são configurados, uma CLI é fornecida para indicar a sequência na qual o banco de dados de back-end deve ser chamado.

## Autorização

A autorização é baseada em tarefas em vez de uma autorização real baseada em comandos. As tarefas são mapeadas para várias guias que correspondem aos sete itens da barra de menus atualmente na GUI da Web. Estes são os itens da barra de menus:

- MONITOR
- WLANS
- CONTROLADOR
- Tecnologia Wireless
- SECURITY
- GERENCIAMENTO
- COMANDO

O motivo desse mapeamento é baseado no fato de que a maioria dos clientes usa a interface da Web para configurar o controlador em vez da CLI.

Uma função adicional para o LOBBY (lobby admin management, gerenciamento de admin de lobby) está disponível para usuários que precisam ter apenas privilégios de administrador de lobby.

A tarefa que um usuário tem direito é configurada no servidor TACACS+ (ACS) usando os pares de valor de atributo (AV) personalizados. O usuário pode ser autorizado para uma ou várias tarefas. A autorização mínima é MONITOR apenas e o máximo é ALL (autorizado a executar todas as sete guias). Se um usuário não tiver direito a uma tarefa específica, ele ainda poderá acessar essa tarefa no modo somente leitura. Se a autenticação estiver habilitada e o servidor de autenticação se tornar inacessível ou incapaz de autorizar, o usuário não poderá fazer login no controlador.

**Observação:** para que a autenticação de gerenciamento básica via TACACS+ seja bem-sucedida, você deve configurar servidores de autenticação e autorização na WLC. A configuração de contabilização é opcional.

## Relatório

A contabilização ocorre sempre que uma determinada ação iniciada pelo usuário é executada com êxito. Os atributos alterados são registrados no servidor de contabilidade TACACS+ junto com estes:

- A ID de usuário do indivíduo que fez a alteração
- O host remoto de onde o usuário está conectado
- A data e a hora em que o comando foi executado
- Nível de autorização do usuário
- Uma string que fornece informações sobre qual ação foi executada e os valores fornecidos

Se o servidor de contabilidade ficar inacessível, o usuário ainda poderá continuar a sessão.

**Observação:** os registros contábeis não são gerados do WCS na versão de software 4.1 ou anterior.

## Configuração TACACS+ na WLC

O Software WLC versão 4.1.171.0 e posterior apresenta novas CLIs e alterações na GUI da Web para habilitar a funcionalidade TACACS+ na WLC. As CLIs introduzidas estão listadas nesta seção para referência. As alterações correspondentes da GUI da Web são adicionadas na guia Segurança.

Este documento pressupõe que a configuração básica da WLC já está concluída.

Para configurar o TACACS+ no controlador WLC, você precisa concluir estas etapas:

1. [Adicionar um servidor de autenticação TACACS+](#)
2. [Adicionar um servidor de autorização TACACS+](#)
3. [Adicionar um servidor de contabilidade TACACS+](#)
4. [Configurar o pedido de autenticação](#)

### Adicionar um servidor de autenticação TACACS+

Conclua estes passos para adicionar um TACACS+ Authentication Server:

1. Use a GUI e vá para **Security > TACACS+ > Authentication**.



2. Adicione o endereço IP do servidor TACACS+ e insira a chave secreta compartilhada. Se necessário, altere a porta padrão do TCP/49.

3. Clique em Apply. Você pode realizar isso na CLI usando o comando **config tacacs auth add <Server Index> <IP addr> <port> [ascii/hex] comando <secret>**:

(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123

## [Adicionar um servidor de autorização TACACS+](#)

Conclua estes passos para adicionar um TACACS+ Authorization Server:

1. Na GUI, vá para **Security > TACACS+ > Authorization (Segurança > TACACS+ > Autorização)**.
2. Adicione o endereço IP do servidor TACACS+ e insira a chave secreta compartilhada. Se necessário, altere a porta padrão do TCP/49.

3. Clique em Apply. Você pode realizar isso na CLI usando o comando **config tacacs athr add <Server Index> <IP addr> <port> [ascii/hex] comando <secret>**:

(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123

## [Adicionar um servidor de contabilidade TACACS+](#)

Conclua estes passos para adicionar um TACACS+ Accounting Server:

1. Use a GUI e vá para **Segurança > TACACS+ > Contabilidade**.
2. Adicione o endereço IP do servidor e digite a chave secreta compartilhada. Se necessário, altere a porta padrão do TCP/49.



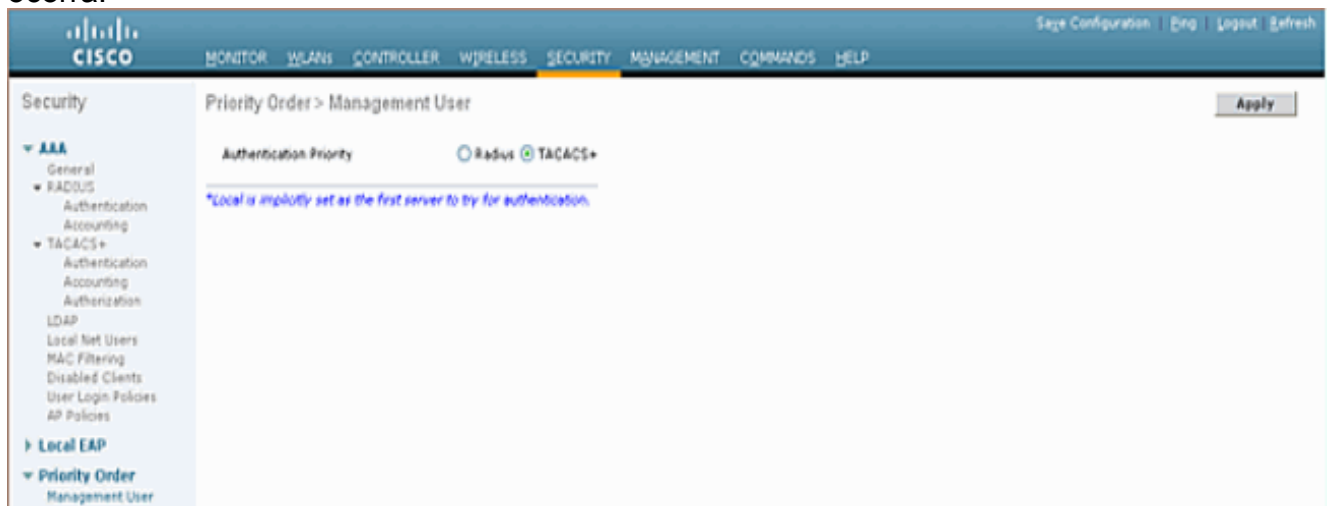
3. Clique em Apply. Você pode realizar isso na CLI usando o comando **config tacacs acct add <Server Index> <IP addr> <port> [ascii/hex] comando <secret>**:  
(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123

## Configurar o pedido de autenticação

Esta etapa explica como configurar a ordem de autenticação AAA quando há vários bancos de dados configurados. A ordem de autenticação pode ser **local e RADIUS**, ou **local e TACACS**. A configuração padrão do controlador para a ordem de autenticação é **local e RADIUS**.

Conclua estes passos para configurar a ordem da autenticação:

1. Na GUI, vá para **Security > Priority Order > Management User**.
2. Selecione a prioridade de autenticação. Neste exemplo, TACACS+ foi selecionado.
3. Clique em **Apply** para que a seleção ocorra.



Você pode realizar isso na CLI usando o comando **config aaa auth mgmt <server1> <server2>**:

```
(Cisco Controller) >config aaa auth mgmt tacacs local
```

## Verifique a configuração

Esta seção descreve os comandos usados para verificar a configuração TACACS+ na WLC. Estes são alguns comandos **show** úteis que ajudam a determinar se a configuração está correta:

- **show aaa auth** — Fornece informações sobre a ordem da autenticação.

```
(Cisco Controller) >show aaa auth
Management authentication server order:
 1..... local
 2..... Tacacs
```

- **show tacacs summary** — Exibe um resumo dos serviços e estatísticas TACACS+.

```
(Cisco Controller) >show tacacs summary
Authentication Servers

Idx  Server Address  Port  State  Tout
---  -
1    10.1.1.12      49   Enabled  2

Authorization Servers

Idx  Server Address  Port  State  Tout
---  -
1    10.1.1.12      49   Enabled  2

Accounting Servers

Idx  Server Address  Port  State  Tout
---  -
1    10.1.1.12      49   Enabled  2
```

- **show tacacs auth stats** — Exibe estatísticas do servidor de autenticação TACACS+.

```
(Cisco Controller) >show tacacs auth statistics
Authentication Servers:

Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 7
Retry Requests..... 3
Accept Responses..... 3
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 12
Unknowntype Msgs..... 0
Other Drops..... 0
```

- **show tacacs athr stats** — Exibe estatísticas do servidor de autorização TACACS+.

```
(Cisco Controller) >show tacacs athr statistics
Authorization Servers:

Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 3
```

```

Retry Requests..... 3
Received Responses..... 3
Authorization Success..... 3
Authorization Failure..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Athrenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0

```

- **show tacacs acct stats** —Exibe estatísticas do servidor de contabilidade TACACS+.

```

(Cisco Controller) >show tacacs acct statistics
Accounting Servers:

```

```

Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 133
Retry Requests..... 0
Accounting Response..... 0
Accounting Request Success..... 0
Accounting Request Failure..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 399
Unknowntype Msgs..... 0
Other Drops..... 0

```

## [Configurar o servidor Cisco Secure ACS](#)

Esta seção fornece as etapas envolvidas no Servidor TACACS+ ACS para criar serviços e atributos personalizados e atribuir as funções aos usuários ou grupos.

A criação de usuários e grupos não é explicada nesta seção. Supõe-se que os usuários e grupos sejam criados conforme necessário. Consulte o [Guia do usuário do Cisco Secure ACS for Windows Server 4.0](#) para obter informações sobre como criar usuários e grupos de usuários.

### [Configuração de rede](#)

Conclua esta etapa:

Adicione o endereço IP de gerenciamento do controlador como cliente AAA com mecanismo de autenticação como TACACS+ (Cisco IOS).



**AAA Clients**

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">DOBSL12-2</a>	10.22.8.21	TACACS+ (Cisco IOS)

**AAA Servers**

AAA Server Name	AAA Server IP Address	AAA Server Type
<a href="#">wnbu-dt-srvr01</a>	11.11.13.2	CiscoSecure ACS

**Help**

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Editing a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [Searching for Network Devices](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)
- [Editing a Proxy Distribution Table Entry](#)
- [Deleting a Proxy Distribution Table Entry](#)

## Configuração da interface

Conclua estes passos:

1. No menu Interface Configuration, selecione o link TACACS+ (Cisco IOS).
2. Ative os **novos serviços**.
3. Marque as caixas de seleção **Usuário** e **Grupo**.
4. Digite **ciscowlc** for Service e **common** for Protocol.
5. Ative os **recursos avançados TACACS+**.

Address <http://127.0.0.1:1767/> Go Links

**CISCO SYSTEMS**

## Interface Configuration

**TACACS+ Services**

User	Group	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

---

**New Services**

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="ciscowlc"/>	<input type="text" value="common"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

---

**Advanced Configuration Options**

Advanced TACACS+ Features

Display a Time-of-Day access grid for every TACACS+ service where you can

Submit Cancel

6. Clique em **Enviar** para aplicar as alterações.

## Configuração de usuário/grupo

Conclua estes passos:

1. Selecione um Usuário/Grupo criado anteriormente.
2. Vá para **TACACS+ Settings**.
3. Marque a caixa de seleção que corresponde ao serviço *ciscowlc* criado na seção Interface Configuration.
4. Marque a caixa de seleção **Atributos personalizados**.



## Group Setup

Jump To Access Restrictions

### Shell Command Authorization Set

None

Assign a Shell Command Authorization Set for any network device

Per Group Command Authorization

Unmatched Cisco IOS commands

Permit

Deny

Command:

Arguments:

Unlisted arguments

Permit

Deny

**ciscowlc common**

Custom attributes

role1=ALL

**Wireless-WCS HTTP**

Custom attributes

### IETF RADIUS Attributes

[006] Service-Type

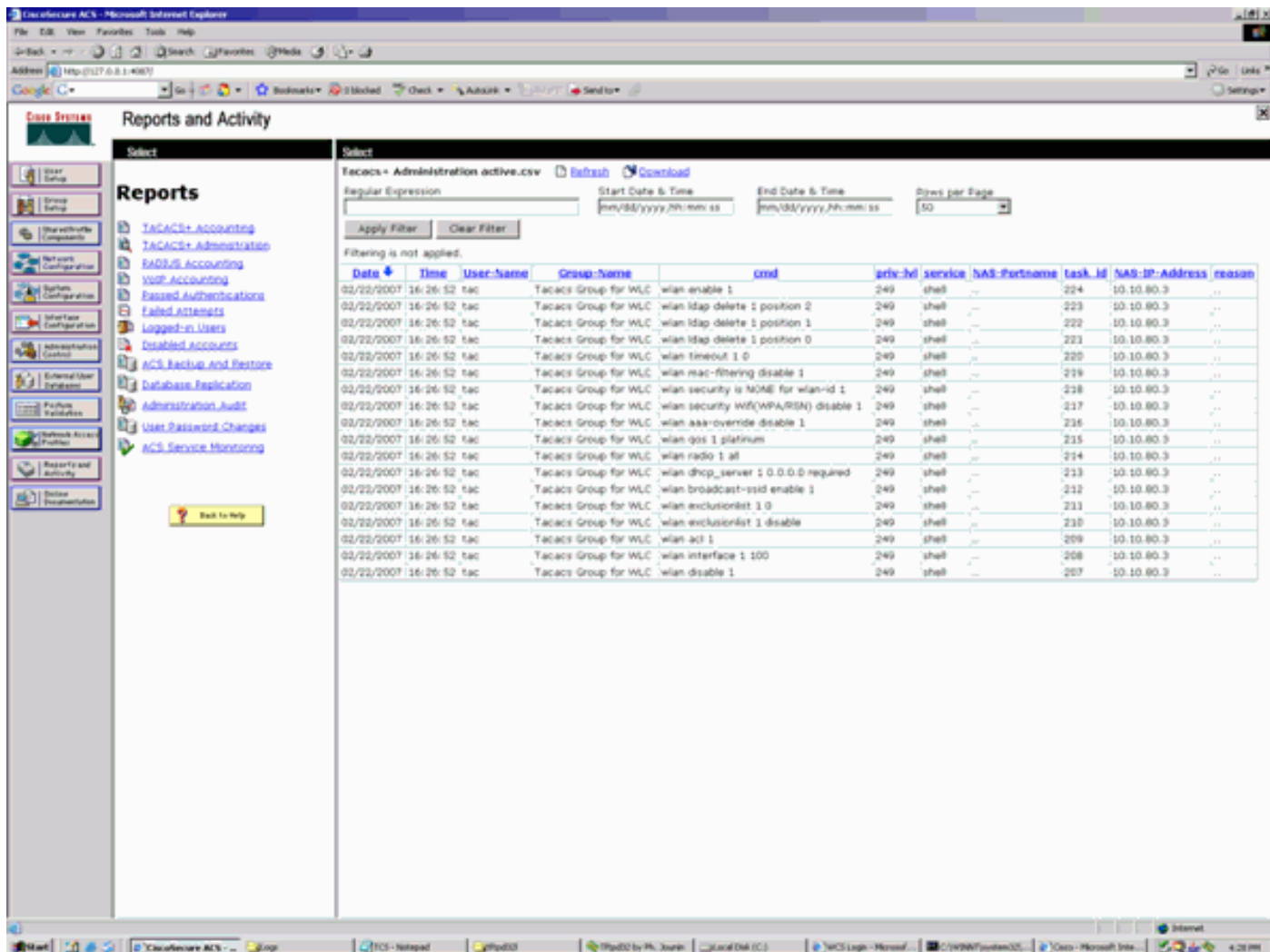
Callback: N/A, Prompt

Submit Submit + Restart Cancel

5. Na caixa de texto abaixo de Atributos personalizados, insira este texto se o usuário criado precisar de acesso somente à WLAN, SEGURANÇA e CONTROLADOR: **role1=WLAN role2=SECURITY role3=CONTROLLER**. Se o usuário precisar acessar apenas a guia SEGURANÇA, insira este texto: **role1=SEGURANÇA**. A função corresponde aos sete itens da barra de menus na GUI da Web do controlador. Os itens da barra de menus são MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT e COMMAND.
6. Digite a função que um usuário precisa para a função1, a função2 e assim por diante. Se um usuário precisa de todas as funções, então a palavra-chave **ALL** deve ser usada. Para a função de administrador do lobby, a palavra-chave **LOBBY** deve ser usada.

## Registros contábeis no Cisco Secure ACS

Os registros contábeis TACACS+ da WLC estão disponíveis no Cisco Secure ACS na Administração TACACS+ de relatórios e atividade:



The screenshot shows the Cisco Secure ACS web interface. The main content area is titled "Reports and Activity" and displays a table of TACACS+ logs. The table has columns for Date, Time, User-name, Group-name, cmd, priv-lev, service, NAS-Portname, task\_id, NAS-IP-Address, and reason. The logs show various commands being executed by users from the "Tacacs Group for WLC" group, such as "wlan enable 1", "wlan ldap delete 1 position 2", "wlan mac-filtering disable 1", and "wlan disable 1".

Date	Time	User-name	Group-name	cmd	priv-lev	service	NAS-Portname	task_id	NAS-IP-Address	reason
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan enable 1	249	shell	---	224	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan ldap delete 1 position 2	249	shell	---	223	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan ldap delete 1 position 1	249	shell	---	222	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan ldap delete 1 position 0	249	shell	---	221	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan timeout 1 0	249	shell	---	220	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan mac-filtering disable 1	249	shell	---	219	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan security is NONE for wlan-id 1	249	shell	---	218	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan security Wf(WPA/RSN) disable 1	249	shell	---	217	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan aaa-override disable 1	249	shell	---	216	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan qos 1 platinum	249	shell	---	215	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan radio 1 all	249	shell	---	214	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan dhcp_server 1 0.0.0.0 required	249	shell	---	213	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan broadcast-sid enable 1	249	shell	---	212	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan exclusionlist 1 0	249	shell	---	211	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan exclusionlist 1 disable	249	shell	---	210	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan acl 1	249	shell	---	209	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan interface 1 100	249	shell	---	208	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan disable 1	249	shell	---	207	10.10.80.3	...

## Configuração TACACS+ no WCS

Conclua estes passos:

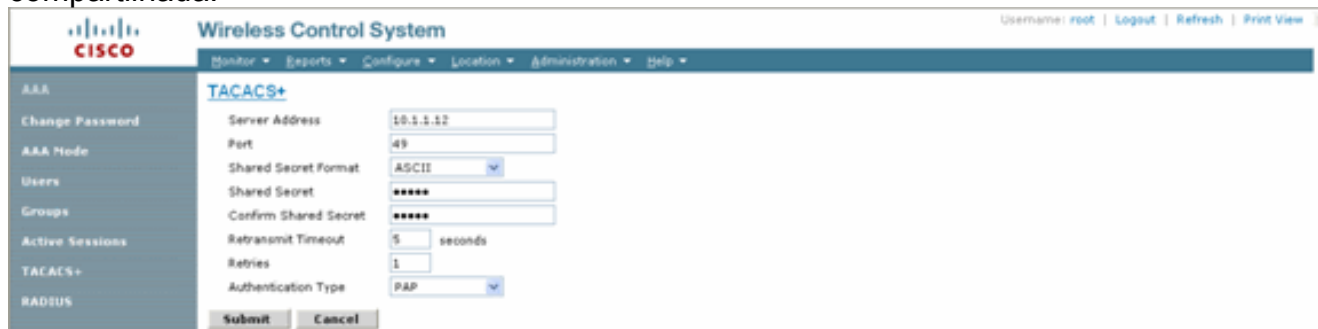
1. Na GUI, faça login no WCS com a conta raiz.
2. Adicione o servidor TACACS+. Vá para **Administration > AAA > TACACS+ > Add TACACS+ Server**.



The screenshot shows the Cisco Wireless Control System (WCS) web interface. The main content area is titled "TACACS+" and displays the message "No TACACS+ Servers found in the system". The left sidebar contains a navigation menu with options like AAA, Change Password, AAA Node, Users, Groups, Active Sessions, TACACS+, and RADIUS. The top navigation bar includes "Monitor", "Reports", "Configure", "Location", "Administration", and "Help".

3. Adicione os detalhes do servidor TACACS+, como endereço IP, número da porta (49 é padrão) e chave secreta

compartilhada.



4. Ative a autenticação TACACS+ para administração no WCS. Vá para **Administration > AAA > AAA Mode > Select TACACS+**.



## WCS usando domínios virtuais

O domínio virtual é um novo recurso introduzido com o WCS versão 5.1. Um domínio virtual WCS consiste em um conjunto de dispositivos e mapas e restringe a visualização de um usuário a informações relevantes para esses dispositivos e mapas. Por meio de um domínio virtual, um administrador pode garantir que os usuários possam visualizar apenas os dispositivos e mapas pelos quais são responsáveis. Além disso, devido aos filtros do domínio virtual, os usuários podem configurar, exibir alarmes e gerar relatórios somente para a parte atribuída à rede. O administrador especifica um conjunto de domínios virtuais permitidos para cada usuário. Somente um desses pode estar ativo para esse usuário no login. O usuário pode alterar o domínio virtual atual selecionando um domínio virtual permitido diferente no menu suspenso Domínio virtual na parte superior da tela. Todos os relatórios, alarmes e outras funcionalidades agora são filtrados por esse domínio virtual.

Se houver apenas um domínio virtual definido (raiz) no sistema e o usuário não tiver nenhum domínio virtual nos campos de atributos personalizados no servidor TACACS+/RADIUS, o usuário recebe o domínio virtual raiz por padrão.

Se houver mais de um domínio virtual e o usuário não tiver nenhum atributo especificado, o usuário será bloqueado para fazer login. Para permitir que o usuário faça login, os atributos personalizados do Domínio Virtual devem ser exportados para o servidor Radius/TACACS+.

A janela Virtual Domain Custom Attributes permite indicar os dados específicos de protocolo apropriados para cada domínio virtual. O botão Exportar na barra lateral Hierarquia de domínio virtual formata previamente os atributos RADIUS e TACACS+ do domínio virtual. Você pode copiar e colar esses atributos no servidor ACS. Isso permite copiar somente os domínios virtuais aplicáveis na tela do servidor ACS e garante que os usuários tenham acesso apenas a esses domínios virtuais.

Para aplicar os atributos RADIUS e TACACS+ pré-formatados ao servidor ACS, faça as etapas

explicadas na seção [Atributos RADIUS de Domínio Virtual e TACACS+](#).

## [Configurar o Cisco Secure ACS para usar o WCS](#)

A seção fornece as etapas envolvidas no Servidor TACACS+ ACS para criar serviços e atributos personalizados e atribuir as funções aos usuários ou grupos.

A criação de usuários e grupos não é explicada nesta seção. Supõe-se que os usuários e grupos sejam criados conforme necessário.

### [Configuração de rede](#)

Conclua esta etapa:

Adicione o endereço IP WCS como cliente AAA com mecanismo de autenticação como TACACS+ (Cisco IOS).

The screenshot displays the Cisco Secure ACS Network Configuration interface. The main title is "Network Configuration" with a sub-header "Edit". The page is titled "AAA Client Setup For WCS". The configuration fields are as follows:

- AAA Client IP Address: 192.168.60.5
- Key: cisco
- Authenticate Using: TACACS+ (Cisco IOS)

There are four checkboxes for additional configuration options:

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom, there are five buttons: "Submit", "Submit + Apply", "Delete", "Delete + Apply", and "Cancel". A "Back to Help" button is also present at the bottom center.

### [Configuração da interface](#)

Conclua estes passos:



1. No menu Interface Configuration, selecione o link **TACACS+** (Cisco IOS).
2. Ative os **novos serviços**.
3. Marque as caixas de seleção **Usuário e Grupo**.
4. Digite **Wireless-WCS** para Serviço e **HTTP** para Protocolo. **Observação:** o HTTP deve estar em CAPS.
5. Ative os recursos avançados **TACACS+**.

**CISCO SYSTEMS**

## Interface Configuration

<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

New Services		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Wireless-WCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		

**Advanced Configuration Options**

Advanced TACACS+ Features

6. Clique em **Enviar** para aplicar as alterações.

## Configuração de usuário/grupo

Conclua estes passos:

1. Na GUI do WCS, navegue até **Administration > AAA > Groups** para selecionar qualquer um dos grupos de usuários pré-configurados, como SuperUsers no WCS.

Group Name	Members	Audit Trail	Export
Admin	---		<a href="#">Task List</a>
ConfigManagers	---		<a href="#">Task List</a>
System Monitors	---		<a href="#">Task List</a>
Users Assistant	---		<a href="#">Task List</a>
LibbyAmbassador	libby ---		<a href="#">Task List</a>
Monitor Libs	---		<a href="#">Task List</a>
North Bound API	---		<a href="#">Task List</a>
Subscribers	---		<a href="#">Task List</a>
Root	root ---		<a href="#">Task List</a>
User Defined 1	---		<a href="#">Task List</a>
User Defined 2	---		<a href="#">Task List</a>
User Defined 3	---		<a href="#">Task List</a>
User Defined 4	---		<a href="#">Task List</a>

2. Selecione a Lista de tarefas para os grupos de usuários pré-configurados e copie e cole para o ACS.

Please cut and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

**TACACS+ Custom Attributes**

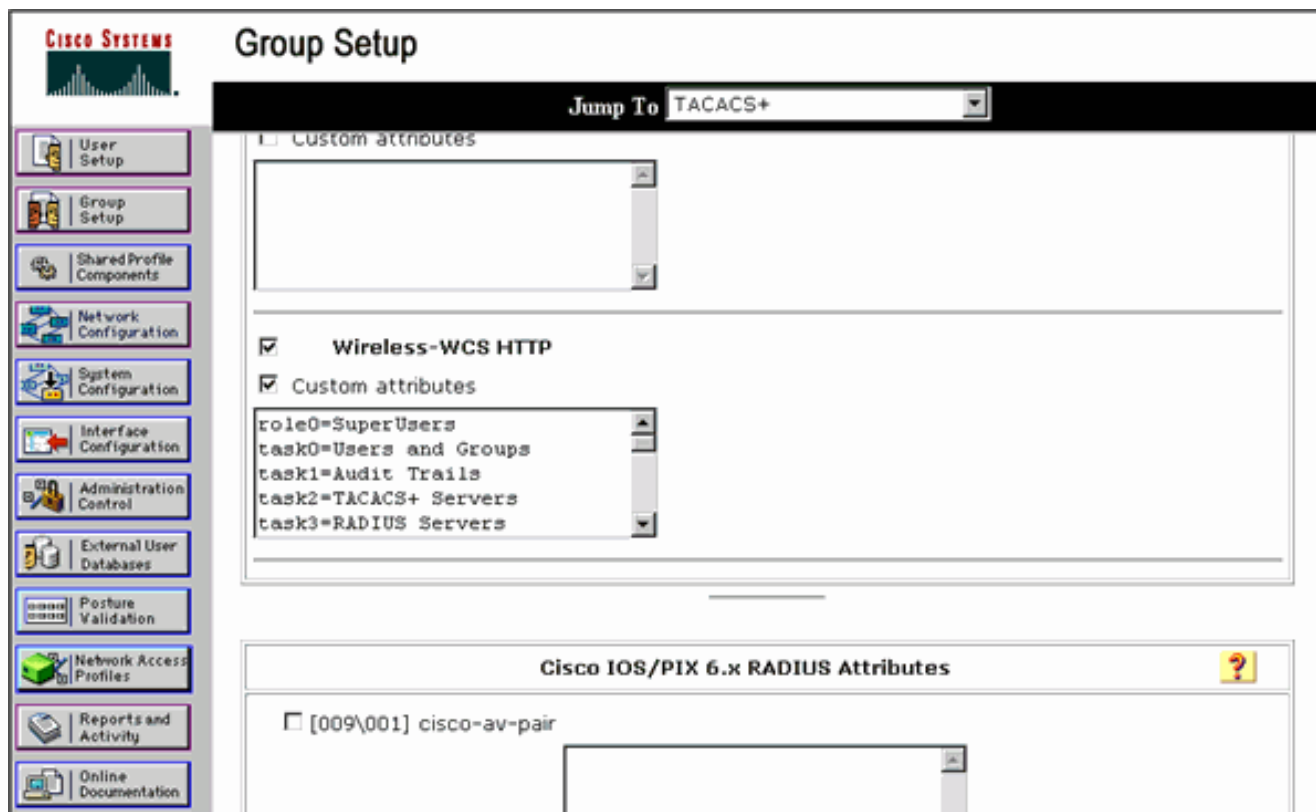
```
role=root
task0=Users and Groups
task1=Audit Trails
task2=TACACS+ Servers
task3=RADIUS Servers
task4=Logging
task5=Logging
task6=Schedule Tasks and Data Collection
task7=User Preferences
task8=System Settings
task9=Diagnostic Information
task10=View Alerts and Events
task11=View Alerts and Events
task12=Email Notification
task13>Delete and Clear Alerts
task14=Push and Unpush Alerts
task15=Severity Configuration
task16=Configure Controllers
task17=Configure Templates
task18=Configure Config Groups
task19=Configure Access Points
task20=Configure Access Point Templates
task21=Configure Choke Points
task22=Monitor Controllers
task23=Monitor Controllers
task24=Monitor Access Points
task25=Monitor Access Points
task26=Monitor Clients
task27=Monitor Clients
task28=Monitor Tags
```

**RADIUS Custom Attributes**

```
Wireless-WCS-task0=Users and Groups
Wireless-WCS-task1=Audit Trails
Wireless-WCS-task2=TACACS+ Servers
Wireless-WCS-task3=RADIUS Servers
Wireless-WCS-task4=Logging
Wireless-WCS-task5=Logging
Wireless-WCS-task6=Schedule Tasks and Data Collection
Wireless-WCS-task7=User Preferences
Wireless-WCS-task8=System Settings
Wireless-WCS-task9=Diagnostic Information
Wireless-WCS-task10=View Alerts and Events
Wireless-WCS-task11=View Alerts and Events
Wireless-WCS-task12=Email Notification
Wireless-WCS-task13>Delete and Clear Alerts
Wireless-WCS-task14=Push and Unpush Alerts
Wireless-WCS-task15=Severity Configuration
Wireless-WCS-task16=Configure Controllers
Wireless-WCS-task17=Configure Templates
Wireless-WCS-task18=Configure Config Groups
Wireless-WCS-task19=Configure Access Points
Wireless-WCS-task20=Configure Access Point Templates
Wireless-WCS-task21=Configure Choke Points
Wireless-WCS-task22=Monitor Controllers
Wireless-WCS-task23=Monitor Controllers
Wireless-WCS-task24=Monitor Access Points
Wireless-WCS-task25=Monitor Access Points
Wireless-WCS-task26=Monitor Clients
Wireless-WCS-task27=Monitor Clients
Wireless-WCS-task28=Monitor Tags
```

3. Selecione um Usuário/Grupo criado anteriormente e vá para **TACACS+ Settings**.
4. Na GUI do ACS, marque a caixa de seleção que corresponde ao serviço Wireless-WCS criado anteriormente.
5. Na GUI do ACS, marque a caixa de **atributos personalizados**.
6. Na caixa de texto abaixo de Atributos personalizados, insira essas informações de função e tarefa copiadas do WCS. Por exemplo, insira a lista de tarefas permitidas pelos Superusuários.





7. Em seguida, faça login no WCS com o nome de usuário/senha recém-criado no ACS.

## Debugs

### Depurações do WLC para role1=ALL

```
(Cisco Controller) >debug aaa tacacs enable
```

```
(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole ffffffff8
```

### Depurações de WLC para várias funções

```
(Cisco Controller) >debug aaa tacacs enable
```

```
Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
session_id=b561ad88 length=16 encrypted=0
Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
```

```
length=6 encrypted=0
Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN]
Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER]
Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY]
Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS]
Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

## [Depurações de uma WLC para falha de autorização](#)

```
(Cisco Controller) >debug aaa tacacs enable
```

```
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007: User has the following mgmtRole 0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

## [Informações Relacionadas](#)

- [Exemplo de configuração do Cisco Wireless LAN Controller \(WLC\) e do Cisco ACS 5.x \(TACACS+\) para autenticação da Web](#)
- [Configurando TACACS+](#)
- [Como configurar a autenticação e a autorização TACACS para usuários Admin e não Admin no ACS 5.1](#)
- [Comparação TACACS+ e RADIUS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)