## ACL por usuário com controladores de LAN sem fio e exemplo de configuração do Cisco Secure ACS

## Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados Conventions** Informações de Apoio Diagrama de Rede Configurar Configurar o controlador de LAN sem fio Crie uma VLAN para os usuários sem fio Configurar a WLC para autenticação com o Cisco Secure ACS Crie uma nova WLAN para os usuários sem fio Definir as ACLs para os usuários Configurar o servidor Cisco Secure ACS Configure o controlador de LAN sem fio como um cliente AAA no Cisco Secure ACS Configurar usuários e perfil de usuário no Cisco Secure ACS Verificar Troubleshoot **Dicas para Troubleshooting** Informações Relacionadas

## **Introduction**

Este documento explica com um exemplo como criar listas de controle de acesso (ACL) nos WLC e aplicá-las aos usuários dependentes da autorização do RADIUS.

## **Prerequisites**

#### **Requirements**

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

 Conhecimento básico de como configurar um servidor Cisco Secure ACS para autenticar clientes sem fio

- Conhecimento da configuração dos Access Points (LAPs) Lightweight Cisco Aironet e Cisco Wireless LAN Controllers (WLCs)
- Conhecimento das soluções Cisco Unified Wireless Security

#### **Componentes Utilizados**

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

- Controlador de LAN sem fio Cisco 4400 Series que executa a versão 5.0.148.0
- Pontos de acesso Lightweight Cisco Aironet série 1231 (LAPs)
- Adaptador cliente Cisco Aironet 802.11 a/b/g Cisco Wireless LAN que executa a versão 3.6
- Cisco Aironet Desktop Utility versão 3.6
- Cisco Secure ACS Server versão 4.1
- Roteador de serviços integrados Cisco 2800 Series que executa a versão 12.4(11)T do  $\text{IOS}^{\texttt{R}}$   $\text{IOS}^{\texttt{R}}$
- Switch Cisco Catalyst 2900XL Series que executa a versão 12.0(5)WC3b

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 <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

## Informações de Apoio

A ACL (Access Control List, lista de controle de acesso) por usuário faz parte da rede Cisco Identity. A Cisco Wireless LAN Solution suporta redes de identidade, que, embora permita que a rede anuncie um único SSID, também permite que usuários específicos herdem diferentes políticas com base em seus perfis de usuário.

O recurso ACL por usuário fornece a capacidade de aplicar uma ACL configurada no Wireless LAN Controller a um usuário com base na autorização RADIUS. Isso é feito com o Airespace-ACL-Name Vendor Specific Attribute (VSA).

Este atributo indica o nome da ACL a ser aplicada ao cliente. Quando o atributo ACL está presente na Aceitação de Acesso RADIUS, o sistema aplica o ACL-Name à estação cliente depois de se autenticar. Isso substitui qualquer ACL atribuída à interface. Ignora a interface ACL atribuída e aplica a nova.

Um resumo do formato ACL-Name Attribute é mostrado abaixo. Os campos são transmitidos da esquerda para a direita

0										1										2										3	
0	1	2	3	4	5	б	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+	+ - +	+ - +	⊢−+	+	+ - +	+ - +	+ - +	+	+	+-+	+	+ - +	⊢−+	+ - +	+	+ - +	+ - +		+	+	+ - +	+		+	+ - +	+ - +	+ - +	⊢ – +	⊢−+	+	+-+
		1	ſyŗ	pe					Le	eng	gtŀ	ı										Ve	enc	loi	r-1	٤d					
+	+ - +	+ - +	+ - +	+	+ - +	+ - +	+ - +	+	+	+ - +	+	+ +	+ - +	+ - +	+ - +	+ - +	+ - +	+ - +	+	+	+ - +	+ - +	+ - +	+	+	+ - +	+ - +	+ - +	+ - +	+	+-+
		Ve	enc	loi	<u>-</u> ]	٤d	( (	cor	nt.	.)						7	/er	ndo	r	ty	γpe	9		1	Ver	ndo	or	le	eng	gtł	n

Para obter mais informações sobre o Cisco Unified Wireless Network Identity Networking, consulte a seção <u>Configuração de redes de identidade</u> do documento <u>Configuração de soluções</u> <u>de segurança</u>.

#### Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Nesta configuração, a WLC e o LAP da controladora de LAN sem fio são usados para fornecer serviços sem fio aos usuários do Departamento A e do Departamento B. Todos os usuários sem fio usam um escritório comum de WLAN (SSID) para acessar a rede e estão na VLAN Office-VLAN.



O servidor Cisco Secure ACS é usado para autenticar usuários sem fio. A autenticação EAP é usada para autenticar usuários. O servidor WLC, LAP e Cisco Secure ACS estão conectados a um Switch de Camada 2 como mostrado.

O roteador R1 conecta os servidores no lado com fio através do Switch de Camada 2, como mostrado. O roteador R1 também atua como um servidor DHCP, que fornece endereços IP para clientes sem fio da sub-rede 172.16.0.0/16.

Você precisa configurar os dispositivos para que isso ocorra:

O Usuário1 do Departamento A tem acesso somente ao servidor 172.16.1.100

O Usuário2 do Departamento B tem acesso somente ao servidor 172.16.1.50

Para fazer isso, você precisa criar 2 ACLs na WLC: um para User1 e outro para User2. Depois que as ACLs forem criadas, você precisará configurar o servidor Cisco Secure ACS para retornar o atributo de nome da ACL para a WLC após a autenticação bem-sucedida do usuário Wireless. Em seguida, a WLC aplica a ACL ao usuário e, portanto, à rede é restrita dependendo do perfil do usuário.

**Observação:** este documento usa autenticação LEAP para autenticar usuários. O Cisco LEAP é vulnerável a ataques de dicionários. Em redes em tempo real, devem ser usados métodos de autenticação mais seguros, como EAP FAST. Como o foco do documento é explicar como configurar o recurso ACL por usuário, o LEAP é usado para simplificar.

A próxima seção fornece instruções passo a passo para configurar os dispositivos para essa configuração.

## <u>Configurar</u>

Antes de configurar o recurso ACL por usuário, você deve configurar a WLC para a operação básica e registrar os LAPs na WLC. Este documento pressupõe que o WLC foi configurado para operação básica e que os LAPs foram registrados no WLC. Se você for um novo usuário, que tenta configurar a WLC para a operação básica com LAPs, consulte <u>Registro de AP Lightweight</u> (LAP) em um Controlador de LAN Wireless (WLC).

Depois que os LAPs estiverem registrados, faça o seguinte para configurar os dispositivos para esta configuração:

- 1. Configure o controlador de LAN sem fio.
- 2. Configure o servidor Cisco Secure ACS.
- 3. Verificar a configuração.

**Observação:** este documento discute a configuração necessária no lado Wireless. O documento pressupõe que a configuração com fio está estabelecida.

## Configurar o controlador de LAN sem fio

Na controladora Wireless LAN, você precisa fazer o seguinte:

• Crie uma VLAN para os usuários sem fio.

- Configure a WLC para autenticar usuários sem fio com o Cisco Secure ACS.
- Crie uma nova WLAN para os usuários sem fio.
- Defina as ACLs para os usuários sem fio.

#### Crie uma VLAN para os usuários sem fio

Para criar uma VLAN para os usuários sem fio, faça o seguinte.

- 1. Vá para a GUI da WLC e escolha **Controller > Interfaces**. A janela Interfaces é exibida. Essa janela lista as interfaces configuradas no controlador.
- 2. Clique em New para criar uma nova interface dinâmica.
- Na janela Interfaces > New, insira o nome da interface e o ID da VLAN. Em seguida, clique em Aplicar. Neste exemplo, a interface dinâmica é denominada Office-VLAN, e a ID da VLAN é atribuída a 20

Q • ○ • ⊡ ⊇ ☆   ♪	📌 e 🔗	& E							R	- 8 ×
ululu cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	Saya C C <u>O</u> MMANDS	nfiguration HELP	Ping Logout	Refresh
Controller	Interface	s > New						< 8 a	ck App	ly
Controller General Inventory Interfaces Internal DHCP Server Mobility Management Ports Master Controller Mode Network Time Protocol QoS CDP	Interface Interface VLAN Id	s > New Name [2	O					< 8a	ck App	ay and a second s

4. Na janela Interfaces > Edit, insira o endereço IP, a máscara de sub-rede e o gateway padrão da interface dinâmica. Atribua a uma porta física na WLC e insira o endereço IP do servidor DHCP. Em seguida, clique em Aplicar.

cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	Saya C COMMANDS	anfiguration <u>P</u> ing Logout <u>R</u> ef HELP
CISCO Controller General Inventory Interfaces Internal DHCP Server Mobility Management Ports Master Controller Mode Network Time Protocol QaS CDP	MONITOR WLANS Interfaces > Edit General Informatio Interface Name MAC Address Interface Address Interface Address VLAN Identifier IP Address Netmask Gateway Physical Informatio Port Number Configuration	CONTROLLER 00 00:06:0 20 172 205 172 00 172	W[RELESS		MANAGEMENT	COMMANDS	KELP Kack Apply
	DHCP Information Primary DHCP Serve Secondary DHCP Ser Access Control List ACL Name Note: Changing the Inte	r 172 rver t rface parameters d thus may result	16.1.75 causes the Wi in loss of cont	] ] LANS to be ectivity for			

Para este exemplo, estes parâmetros são usados para a interface Office-VLAN: Office-VLAN

```
IP address: 172.16.1.25
Netmask: 255.255.0.0
Default gateway: 172.16.1.75 (sub-interface on Router R1)
Port on WLC: 1
DHCP server: 172.16.1.75
```

#### Configurar a WLC para autenticação com o Cisco Secure ACS

A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo (neste caso, o Cisco Secure ACS). O servidor RADIUS valida as credenciais do usuário e retorna o atributo de nome da ACL para a WLC após a autenticação bem-sucedida do usuário sem fio.

Conclua estes passos para configurar a WLC para o servidor RADIUS:

- Escolha Segurança e Autenticação RADIUS na GUI do controlador para exibir a página Servidores de Autenticação RADIUS. Em seguida, clique em New para definir um servidor RADIUS.
- Defina os parâmetros do servidor RADIUS na página Servidores de Autenticação RADIUS > Novo. Esses parâmetros incluem o endereço IP do servidor RADIUS, o segredo compartilhado, o número da porta e o status do servidor.

cisco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT	Save Co COMMANDS	HELP	Eing Logout Befre
Security	RADIUS Authenticati	on Servers > New				< Bac	k Apply
Security AAA General Control Control Contro	RADIUS Authenticati Server Index (Priority Server IPAddress Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Retransmit Timeout Network User Management IPSec	In Servers > New 1. Image: 10.77.244.196 ASCII Image: 10.77.244.196 ASCII Image: 10.77.244.196 ASCII Image: 10.77.244.196 Image: 10.77.244.196 Image	FIPS customer	s and requires a k	ey wrap complian	< Bac	k Apply

 As caixas de seleção Network User and Management determinam se a autenticação baseada em RADIUS se aplica a usuários de gerenciamento e rede. Este exemplo usa o Cisco Secure ACS como o servidor RADIUS com endereço IP 10.77.244.196. Clique em Apply.

#### Crie uma nova WLAN para os usuários sem fio

Em seguida, é necessário criar uma WLAN à qual os usuários sem fio possam se conectar. Para criar uma nova WLAN, faça o seguinte:

- 1. Na GUI da controladora Wireless LAN, clique em **WLANs**. Esta página lista as WLANs que existem na controladora.
- Escolha New para criar uma nova WLAN. Insira o ID da WLAN, o Nome do perfil e o SSID da WLAN para a WLAN e clique em Aplicar. Para esta configuração, crie um WLAN Office.

🖸 • 😳 • 🖻 🖻 🐔 .	A 📌 🙆 🐼 🖗 🛛							🥂 – 5 ×
ululu cisco	MONITOR MLANS		WIRELESS	SECURITY	MANAGEMENT	Sage Co COMMANDS	nfiguration <u>B</u> in HELP	g Lagout <u>R</u> efresh
WLANs	WLANs > New						< Back	Apply
VLANS	WLAN ID	1 .						
AP Groups VLAN	Profile Name	Office						
	WLAN SSID	Office						
							1	

 Depois de criar uma nova WLAN, a página WLAN > Edit para a nova WLAN é exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN que incluem políticas gerais, segurança, QoS e parâmetros avançados.

cisco	Save Configuration Eing Logout Ba MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
LANs	WLANs > Edit Apply
WLANS WLANS AP Groups VLAN	General       Security       QoS       Advanced         Profile Name       Office         WLAN SSID       Office         WLAN Status       Image: Control of
	Foot Notes I CKIP is not supported by IOxx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MRP is not active unless WPA2 is configured

Verifique **WLAN Status** em General policies (Políticas gerais) para habilitar a WLAN. Escolha a interface apropriada no menu suspenso. Neste exemplo, use a interface **Office-vlan**. Os outros parâmetros desta página podem ser modificados com base no requisito da rede WLAN.

4. Escolha a **guia Segurança**. Escolha **802.1x** no menu suspenso de segurança da Camada 2 (já que essa é uma autenticação LEAP). Escolha o tamanho apropriado da chave WEP em parâmetros

802.1x.

ANs	WLANs > Edit < Back	Appl
<b>VLANS</b> WLANS AP Groups VLAN	General Security QoS Advanced Layer 2 Layer 3 AAA Servers	
	Layer 2 Security 802.1X Real Security 802.1X Real Security 802.1X Real Security 802.1X Parameters	
	802.11 Data Encryption Type Key Size	
	Foot Notes	
	1 CKIP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset exclu 5 Client MFP is not active unless WPA2 is configured	ded clieni

5. Na guia Segurança, escolha a subguia **servidor AAA**. Escolha o servidor AAA usado para autenticar clientes sem fio. Neste exemplo, use o servidor ACS 10.77.244.196 para autenticar clientes sem fio.

cisco	Sage Configuration Bing Logout B MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
LANS WLANS WLANS AP Groups VLAN	WLANs > Edit     < Back
	Foot Notes  I CKIP is not supported by IOxx model APs 3 M-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients; 5 Client MPP is not active unless WPA2 is configured

6. Escolha a guia **Avançado**. Marque **Permitir substituição de AAA** para configurar a substituição de política de usuário através da AAA em uma LAN sem fio.

cisco	Sage Configuration Eing Logout B MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
CISCO WLANS * WLANS MULANS AP Groups VLAN	MONITOR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HEIP         WLANS > Edit         Sack       Apply         General       Security       QoS       Advanced        Apply         General       Security       QoS       Advanced        DHCP         H-REAP Local Swhething *       Enabled       DHCP       Override       Override         Session Timeout (secs)       1800       DHCP Addr. Assignment       Required         Override       It nabled       DHCP Addr. Assignment       Required         Override       It nabled       DHCP P       Infrastructure MSP       (Global MFP Disabled)         Override       It nabled       Infrastructure MSP       (Global MFP Disabled)       MFP Client         Client Exclusion \$       If meaut Value (secs)       MFP Client       Optional       Image: Protection \$         Foot Notes       I       Image: CMP is not supported by 10xx model AP;       Statistical Protection \$       Optional       Image: Protection \$         I CKIP is not supported by 10xx model AP;       Statistical Protein Protection \$       Optional       Image: Protection \$       Image: Protection \$         I configure Protex subheting is not sup

Quando a substituição de AAA está habilitada e um cliente tem parâmetros conflitantes de autenticação de LAN sem fio de controlador AAA e Cisco Wireless LAN, a autenticação do cliente é executada pelo servidor AAA. Como parte dessa autenticação, o sistema operacional move os clientes da VLAN LAN sem fio da solução de LAN sem fio da Cisco para uma VLAN retornada pelo servidor AAA e predefinida na configuração da interface do controlador de LAN sem fio da Cisco, o que acontece somente quando configurada para filtragem de MAC, 802.1X e/ou operação WPA. Em todos os casos, o sistema operacional também usa QoS, DSCP, valores de marca de prioridade 802.1p e ACL fornecidos pelo servidor AAA, desde que sejam predefinidos na configuração da interface do controlador Cisco Wireless LAN.

7. Escolha os outros parâmetros com base nos requisitos da rede. Clique em Apply.

#### Definir as ACLs para os usuários

Você precisa criar duas ACLs para esta configuração:

- ACL1: Para fornecer acesso a User1 somente ao servidor 172.16.1.100
- ACL2: Para fornecer acesso ao Usuário2 ao servidor somente 172.16.1.50

Conclua estes passos para configurar as ACLs na WLC:

- Na GUI do WLC, escolha Security > Access Control Lists. A página Listas de controle de acesso é exibida. Esta página lista as ACLs configuradas na WLC. Também permite editar ou remover qualquer uma das ACLs. Para criar uma nova ACL, clique em Novo.
- 2. Esta página permite criar novas ACLs. Digite o nome da ACL e clique em **Apply** (**Aplicar**). Depois que a ACL for criada, clique em **Editar** para criar regras para a ACL.

3. O usuário1 precisa ter acesso somente ao servidor 172.16.1.100 e deve ter acesso negado a todos os outros dispositivos. Para isso, você precisa definir essas regras.Consulte o <u>Exemplo de Configuração de ACLs em Wireless LAN Controller</u> para obter mais informações sobre como configurar ACLs em Wireless LAN

Controllers.

G • 🖯 • 🖻 🖻 🏠 🔎	\$ €	$\otimes 3$	• 🖾 🖓 🖓	(iss)	(Constant)		lin de	indexes of the	0000000000	Standnar	<u>energen</u>	🛛 🎊 – č
cisco	MONL	TOR W	LANS CONTR	OLLEP	WIRELESS	SE	CURITY I	MANAGEMENT	Saya C COMMANDS	onfiguration HELP	eing I	.ogout <u>R</u> efr
Security	Acce	ss Con	trol Lists > E	dit					< 1	lack	Add New	v Rule
▼ AAA General ▼ RADIUS	Gene	ral List Nam	ve User:	1								
Authentication Accounting + TACACS+	Seq	Action	Source IP/M	ask	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	
LDAP Local Net Users MAC Filtering	1	Permit	172.16.0.0 255.255.0.0	1	172.16.1.100 255.255.255.255	<i>'</i>	Any	Any	Any	Any	Inbound	
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.100 255.255.255.2	55	172.16.0.0 255.255.0.0	′	Any	Any	Any	Any	Outbound	۵
Local EAP	L											
Priority Order												
<ul> <li>Access Control Lists Access Control Lists CPU Access Control Lists         </li> </ul>												
> IPSec Certs												
Wireless Protection     Policies												
• Web Auth												
▶ CIDS												

4. Da mesma forma, você precisa criar uma ACL para User2, que permita que User2 acesse somente o servidor 172.16.1.50. Esta é a ACL necessária para o User2.

cisco	MONI	TOR M	(LANS CON	TROLLE	R WIRELESS	SE	CURITY M	NAGEMENT	Saye Ci COMMANDS	HELP	Eing	Logout <u>R</u> efre
ecurity	Acce	ss Con	ntrol Lists >	Edit					< 8	ack	Add Net	v Rule
General PAODUS	Gene	ral List Nam		er?								
Authentication Accounting + TACACS+	Seq	Action	Source IP	/Mask	Destination IP/Mask		Protocol	Source Port	Dest	DSCP	Direction	
LDAP Local Net Users MAC Filtering	1	Permit	172.16.0.0	1	172.16.1.50	, s	Any	Any	Αηγ	Any	Inbound	۰
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.50	5.255	172.16.0.0 255.255.0.0	1	Any	Any	Any	Any	Outbound	
Local EAP												
Priority Order	L											
Access Control Lists Access Control Lists CPU Access Control Lists												
IPSec Certs												
Wireless Protection Policies												
Web Auth												
CIDS												

Agora você configurou o Wireless LAN Controller para esta configuração. A próxima etapa é configurar o servidor Cisco Secure Access Control para autenticar os clientes sem fio e retornar o atributo Nome da ACL para a WLC após a autenticação bem-sucedida.

## Configurar o servidor Cisco Secure ACS

Para que o Cisco Secure ACS possa autenticar clientes sem fio, você precisa concluir estas etapas:

- Configure o Wireless LAN Controller como um cliente AAA no Cisco Secure ACS.
- Configure os perfis de usuário e usuários no Cisco Secure ACS.

# Configure o controlador de LAN sem fio como um cliente AAA no Cisco Secure ACS

Para configurar o Wireless LAN Controller como um cliente AAA no Cisco Secure ACS, faça o seguinte:

 Clique em Network Configuration > Add AAA client. A página Adicionar cliente AAA é exibida. Nesta página, defina o nome do sistema WLC, o endereço IP da Interface de Gerenciamento, o segredo compartilhado e autentique usando o Radius Airespace. Aqui está um exemplo:

Cisco Systems	Network Configuration	×
ad hoad ho	Edit	🖌 Help
User Setup Group Shared Profile Components Metwork Configuration System Configuration Interface Configuration	Add AAA Client AAA Client Hostname wlc AAA Client IP Address 10.77.244.210 Shared Secret cisco	AAA Client Hestmane     AAA Client Hestmane     AAA Client HP Address     Shared Secret     Network Device Group     BADIUS Key Yran     Authenticale Using     Authenticale Using     Single Connect TACACS - AAA Client     Log Update/Watchdeg Packets from this     AAA Client     Log AADIUS Towneling Packets from this     AAA Client     Reduce RADIUS Port info with Username     from this AAA Client     Mathentical Packets from this     AAAC Client     Mathentical Packets from this     AAAC Client     Mathentical Packets from this     AAA Client     Mathentical Packets from this     AAACCEnt
Control     Contro     Control     Control     Control     Control     Control     Co	Key Encryption Key Message Authenticator Code Key Key Input Format Authenticate Using RADIUS (Cisco Airespace)	AAA Client Hestname The AAA Client Hostnama is the name assigned to the AAA client. [Back to Tos]
Online Documentation	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	AAA Client IP Address The AAA Client IP Address is the IP address assigned to the AAA client.
	Replace RADIUS Port info with Usemame from this AAA Client     Match Framed-IP-Address with user IP address for accounting packets from     this AAA Client	If you want to designate more than one AAA client with a single AAA client entry in ACB, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.
	Back to Help	You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.160.13.1

**Observação:** o segredo compartilhado configurado no Cisco Secure ACS deve corresponder ao segredo compartilhado configurado na WLC em **RADIUS Authentication Servers > New**.

2. Clique em Enviar+Aplicar.

#### Configurar usuários e perfil de usuário no Cisco Secure ACS

Para configurar usuários no Cisco Secure ACS, faça o seguinte:

 Escolha User Setup na GUI do ACS, digite o nome de usuário e clique em Add/Edit. Neste exemplo, o usuário é User1.



 Quando a página User Setup for exibida, defina todos os parâmetros específicos do usuário. Neste exemplo, os atributos nome de usuário, senha, Informações de usuário suplementares e RADIUS estão configurados porque você só precisa desses parâmetros para autenticação EAP.

3·0·1	合 2 今日 ② 3 日	🕅 = 8 ×
Cisco Systems	User Setup	×
.dlbdlb	Edit	Help
User Setup	User: UserA (New User)	Account Disabled     Deleting a Unername     Supplementary User Info
Shared Profile Components	Supplementary liver lefa	Passweed Authentication     Group to which the user is assigned     Caliback     Client IP Address Assignment
Sector Configuration	Real Name User 1 Description	Advanced Settings     Network Access Restrictions     Han Sections     Hange Chartas     Access Disable     Bounsianable Acts
Administration Centrel Dutabases Pentere Validation Validation	User Setup ?	TACACS - Enable Password     TACACS - Enable Password     TACACS - Enable Password     TACACS - Dutheund Password     TACACS - Shell Command Authorization     Command Authorization for Network Device Hanagement Applications     TACACS - Unknown Services     IETT RADIUS Attributes     RADIUS Yeador Specific Attributes
Reports and Activity Otalise Documentation	CMAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP)	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account.
	Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is	[Back to Tap] Defeting a Username The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click DK.
	Group to which the user is assigned:	[back to Top] Supplementary User Info Type the applicable information in any supplemental user information bores that appear. To add or change fields, click Reterface

Role para baixo até ver os atributos do Cisco Airespace RADIUS específicos ao usuário. Verifique o **Aire-ACL-Name** para permitir que o ACS retorne o nome da ACL ao WLC juntamente com a resposta de autenticação bem-sucedida. Para User1, crie um ACL User1 na WLC. Insira o nome da ACL como User1.

😋 • 🗇 • 💽 🖻	🚳 🖍 🚖 🔗 🔕 🖬	🥂 – 8 ×
Cinco Systems	User Setup	×
اله	Date exceeds:	Help
User Setup Setup Setup Shared Profile Components Network Configuration Spitem Configuration	Sep 9 2007 Failed attempts exceed: 5 Failed attempts since last successful login: 0 Reset current failed attempts count on submit	Account Disabled     Beletine a Wermann     Suplementary User Info     Pansword Authentication     Group to which the user is assigned     Callback     Client IP Address Assignment     Advanced Settings     Natural Access Restrictions     Han Sessions     Wrape Quetas     Account Disable     Downloadable ACLs
Administration Centrel Databases Pestere Validation Profiles	Clisce Alirespace RADIUS Attributes	Advanced TACACS+ Settings     TACACS+ Enable Deserved     TACACS+ Enable Deserved     TACACS+ Conformed Authorization     Cammand Authorization     Cammand Authorization     TACACS+ Shell Command Authorization     TACACS+ Unknown Services     TACACS+ Unknown Services     TETT RADIUS Attributes     BADDUS Yeador-Specific Attributes
Reports and Activity Online Documentation	[141794004] Aire-802.1P-T ag [141794005] Aire-Interface-Name M [141794006] Aire-AcL-Name USer1 Back to Help	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [Rack to Teo] Deleting a Uvername The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the construct user account from the database, click Delete. When asked to confirm your action, click DK. [Rack to Teo] Supplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information boxes that appear. To add or chance fields, click <b>Interface</b>

3. Repita o mesmo procedimento para criar User2 como mostrado aqui.

Cisco Systems	User Setup					
-dlb-dlb-	Select	Help				
User         Stared Profile         Shared Profile </th <th>Select User: User2 Find Add/Edit List users beginning with letter/number: ABCPEFSSIIVYXXII QIIIISSIIVYXXII QIIIISS List all users Remove Dynamic Users 2 bek to Help</th> <th><ul> <li>Help</li> <li>Person and a factor of these Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rational Rationant Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rat</li></ul></th>	Select User: User2 Find Add/Edit List users beginning with letter/number: ABCPEFSSIIVYXXII QIIIISSIIVYXXII QIIIISS List all users Remove Dynamic Users 2 bek to Help	<ul> <li>Help</li> <li>Person and a factor of these Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rationant Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rational Rationant Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rational Rationants</li> <li>Person a factor of the ACS Internal Rat</li></ul>				
0 · O · E E ·	<ul> <li>A ≠ € ⊗ 5 B</li> </ul>	🕅 - 5 ×				
Cisco Systems	User Setup	X				
adbad ba	Edit	Help E				
User Setup Group Setup Setup Setup Setup Setup Setup Configuration Setup Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	User: UserA (New User)          Account Disabled         Supplementary User Info         Real Name       User2         Description         User Setup         Password Authentication:         ACS Internal Database         CiscoSecure PAP (Also used for CHAP/MS-	Account Disabled     Beletima a Distributed     Supplementary User Info     Supplementary User Info     Destroard Authentication     Comp to which the user is assigned     Calback     Client IP Address Assignment     Advanced Settings     Network Access Restrictions     Max Sessions     Unage Quetas     Network Access Restrictions     Max Sessions     Disable Aftact     Advanced TACACS - Settings     TACACS - Inable Password     TACACS - Inable Password     TACACS - Undersmod Password     TACACS - RADIUS Attributes				
Reports and Activity Documentation	Password Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: Submit Cancel	Account Disabled Status         Select the Account Disabled check box to disable this account; clear the check box to enable the account.         [hack to Teo]         Deleting a Username         The Delete buttos appears only when you are editing as existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When added to certify your action, click OK.         [hack to Teo]         Supplementary User Info         Type the applicable information in any supplemental user information				

😋 • 🕗 • 🖻 🖻	🏠 🔎 🗢 🖾 · 🎍 🗖	🥂 - θ ×
Cisco Systems	User Setup	X
dbdb	Date exceeds:	Help
User Setup Greup Setup Components Configuration Configuration Configuration	Sep 9 2007 Failed attempts exceed: S Failed attempts since last successful login: 0 Reset current failed attempts count on submit	Account Disabled     Definition a Unername     Supplementary User Info     Password Authentication     Group to which the user is assigned     Caliback     Clent IP Advanced Autionment     Advanced Settings     Natural Access Restrictions     Has Sensions     Usage Operas     Busage Operas     Access Restrictions     Has Sensions     Disage Operas     Access Restrictions     Access Restrictions     Busage Operas     Access Restrictions     Busage Operas     Access Restrictions
Administration Confrol	Cloce Airespace RADIUS Attributes	Advanced TACACS+ Settings     TACACS+ Enable Control     TACACS+ Enable Control
Porternal User Databases Validation Validation	[14179402] Aize-QoS-Level     Bronze     [14179403] Aize-DSCP     [	TACACS - Online Parameter     TACACS - Scheman Parameter     TACACS - Schema Parameter     TACACS - Schema Parameter     TACACS - Schema Parameter     TACACS - Unknown Services     TACACS - Unknown Services     IETE PADIUS Attributes     RADUS Vender-Specific Attributes
Reports and Activity	[14179404] Aire-802.1P-T ag	Account Disabled Status
Documentation	[14179005] Aire-Interface-Name	Select the Account Disabled check box to disable this account; clear the check box to enable the account.
(	F [14179006] Adv-Acl-Name	(Bask m Tan)
	User2	Deleting a Username
		The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click <b>Delete</b> . When asked to confirm your action, click <b>DK</b> .
	P Back to Melp	[Back to Tep]
		Sapplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information

4. Clique em Configuração do sistema e Configuração de autenticação global para garantir que o servidor de autenticação esteja configurado para executar o método de autenticação EAP desejado. Nas definições de configuração do EAP, escolha o método EAP apropriado. Este exemplo usa autenticação LEAP. Clique em Enviar quando terminar.

Cisco Systems	System Configuration	×.
all seal in a	PEAP	Help
TA LUser	Allow EAP-MSCHAPv2	
Le Setup	Allow EAP-GTC	Use this page to specify settings for various authentication protocols.
Graup Setup	C Allow Posture Validation	EAP Configuration
Shared Profile		EAP-FAST
- I Components	Calent one or more of the following antians:	• EAP-TLS
Configuration	E Castillasta SAN comparison	• LEAP • EAP-HOS
What Sustem	in Certificate SAN companison	AP_EAP_Request Timeout
Configuration	M Certificate CN companison	MS-CHAP.Configuration
Interface	M Certificate Binary comparison	
- Consideration	EAP-TLS session timeout (minutes): 120	
Administration Centrel		EAP Configuration
ale. I Feternal liter	Cisco client initial message:	EAD is a flexible request-response pratocol for arbitrary
Stal Databases	PEAP session timeout (minutes): 120	authentication information (RFC 2204). EAP is tagered on tap of another protocol such as UDP, 802.1x or RADIUS and supports
manal Pestere	Enable East Reconnect:	multiple "authentication" types.
		[Back to Tep]
Profilez	EAP-FAST	PEAD
Ch   Reports and	EAP-FAST Configuration	
Activity		PEAP is the outer layer protocol for the secure tunnel.
Deline	EAP-TLS	
Contra L poccasion and a	Allow EAP-TLS	Notes IEAP is a certificate-based authentication protect. IEAP authentication can occur only after you have completed the required steps
	Select one or more of the following options:	to the ACS Centificate Setup page.
	File Certificate SAN comparison	Allow EAP-MSCHAPv2 - Use to anable EAP-MSCHAPv2 within MS PEAP
	Certificate CN comparison	authentication. Enable this protocol for any repository that supports MS- CHAPV2, such as Microsoft AD, and the ACS Internal Durahase.
	F Certificate Binary comparison	
	EAP-TLS session timeout (minutes): 120	<ul> <li>Allow EAP-GTC — Use to enable EAP-GTC within Ciscs PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.</li> </ul>
1	LEAP	Allow Parture Validation when to enable the DEAD (EAD-T) VI surrough for
C	Allow LEAP (For Aironet only)	posture validation of Network Admission Control (NAC) clients.
	Submit Submit + Restart Cancel	<ul> <li>Allow EAP-TLS - Use to enable the EAP-TLS protocol as an additional inner method for PEAP. The PEAP/EAP-TLS Secture attends lowercose the existing "</li> </ul>

## **Verificar**

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

Tente associar um cliente sem fio ao AP Lightweight com autenticação LEAP para verificar se a configuração funciona como esperado.

**Observação:** este documento pressupõe que o perfil do cliente está configurado para autenticação LEAP. Consulte <u>Usando a Autenticação EAP</u> para obter mais informações sobre como configurar o Adaptador de Cliente Wireless 802.11 a/b/g para autenticação LEAP.

Quando o perfil do cliente sem fio for ativado, o usuário será solicitado a fornecer o nome de usuário/senha para a autenticação LEAP. Isso é o que acontece quando o Usuário1 tenta autenticar no LAP.

Enter Wireless Network Password				
Please enter your LE network	AP username and password to log on to the wireless			
User Name :	User1			
Password :	•••••			
Log on to :				
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter			
Profile Name :	Office			
	OK Cancel			

O AP leve e, em seguida, a WLC transmitem as credenciais do usuário ao servidor RADIUS externo (Cisco Secure ACS) para validar as credenciais. O servidor RADIUS compara os dados com o banco de dados do usuário e, após a autenticação bem-sucedida, retorna o nome da ACL configurado para o usuário para a WLC. Nesse caso, a ACL User1 é retornada à WLC.

😨 Cisco Aironet Desktop Utilit	y - Current Profil	e: Office-TSWEB	? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
utlluuutlluu Profile Name:	Office-TSWEB		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channet: 64	
Server Based Authentication:	LEAP	Data Encryption: WEP	
IP Address.	172.16.0.14		
Signal Strength:		Excellent	
		Advanced	

A controladora Wireless LAN aplica essa ACL ao User1. Esta saída de ping mostra que User1 pode acessar somente o servidor 172.16.1.100, mas não qualquer outro dispositivo.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 3ms, Average = 1ms
D:\Documents and Settings\Administrator>ping 172.16.1.50
Pinging 172.16.1.50 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Da mesma forma, quando o User2 tenta acessar a WLAN, o servidor RADIUS, após a autenticação bem-sucedida, retorna a ACL User2 para a WLC.

Enter Wireless Network Password		
Please enter your LE network	AP username and password to log on to the wireless	
User Name :	User2	
Password :	•••••	
Log on to :		
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter	
Profile Name :	Office	
	OK Cancel	

P Authentication Status	? :
Card Name: Cisco Aironet 802.11	1a/b/g Wireless Adapter
Profile Name: Office-TSWEB	
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Skipped because the domain name was not configured

A controladora Wireless LAN aplica essa ACL ao User2. Esta saída de ping mostra que User2 é capaz de acessar somente o servidor 172.16.1.50, mas não qualquer outro dispositivo.

```
D:\Documents and Settings\Administrator>ping 172.16.1.50
Pinging 172.16.1.50 with 32 bytes of data:
Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Ping statistics for 172.16.1.50:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 18ms, Average = 5ms
D:\Documents and Settings\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.1.100:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

## **Troubleshoot**

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

No Wireless LAN Controller, você também pode usar esses comandos debug para solucionar problemas de autenticação AAA

- debug aaa all enable Configura a depuração de todas as mensagens AAA
- debug dot1x packet enable Habilita a depuração de todos os pacotes dot1x
- debug client <MAC Address> Habilita a depuração do cliente sem fio

Aqui está um exemplo do comando debug aaa all enable

**Observação:** algumas das linhas na saída foram movidas para a segunda linha devido a restrições de espaço.

Thu Aug 16 14:42:54 2007: AuthenticationReguest: 0xblab104 

 Thu Aug 16 14:42:54 2007:
 Callback.....0x85ed228

 Thu Aug 16 14:42:54 2007:
 protocolType.....0x00140001

 Thu Aug 16 14:42:54 2007: 

 Thu Aug 16 14:42:54 2007:
 proxyState.....00:40:96:AF:3E:93-03:01

 Thu Aug 16 14:42:54 2007:
 Packet contains 16 AVPs (not shown)

 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00 Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99 b4 19 27 28 eb 5f 35 9c ....-4.....'(.\_5. Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73 65 72 31 1f 13 30 30 2d .....user1..00-Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 40-96-AF-3E-93.. Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06 0:Office-TSWEB.. Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a .....M....wlc. Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 01 06 06 00 00 00 ...7c..... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 13 40 06 00 . . . . . . . = . . . . . @ . . Thu Aug 16 14:42:54 2007: 0000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 27 02 ....Q.200'. Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d 87 9d 0b f9 dd e5 39 0d Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96 dc c3 55 ff 7c 51 4e 75 .....#....U.|QNu Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 ser1..SVC=0.1;P. Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0 c6 2f 5e f5 65 e9 3e 2d ..;5<sup>^</sup>..../<sup>^</sup>.e.>-Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4 27 e6 d4 0e 1b 8e 5d 19 ...6.1j.'....]. Thu Aug 16 14:42:54 2007: 00000010: 60 lc c2 16 4f 06 03 01 00 04 18 0a 53 56 43 3d Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb 90 ec 48 9b fb d7 ce ca 0.1;P.1...H.... Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09 ;d... Thu Aug 16 14:42:54 2007: \*\*\*\*Enter processIncomingMessages: response code=11 Thu Aug 16 14:42:54 2007: \*\*\*\*Enter processRadiusResponse: response code=11 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3 Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize.....104 resultCode.....255 Thu Aug 16 14:42:54 2007: Thu Aug 16 14:42:54 2007: protocolUsed.....0x0000001 Thu Aug 16 14:42:54 2007: proxyState.... 00:40:96:AF:3E:93-03:01

Thu Aug 16 14:42:54 2007: Packet contains 3 AVPs (not shown) Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xblab104 Thu Aug 16 14:42:54 2007: Callback.....0x85ed228 Thu Aug 16 14:42:54 2007: protocolType.....0x00140001 Thu Aug 16 14:42:54 2007: proxyState..... 00:40:96:AF:3E:93-03:02 Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00 Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20 ff 5b f2 16 64 df 02 61 ....8....[..d..a Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73 65 72 31 1f 13 30 30 2d ...K..User1..00-Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 40-96-AF-3E-93.. Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06 0:Office.. Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a .....M....wlc. Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 01 06 06 00 00 00 ...7c.... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 01 13 40 06 00 . . . . . . . . = . . . . . @ . . Thu Aug 16 14:42:54 2007: 0000080: 00 00 0d 41 06 00 00 06 51 04 32 30 4f 17 01 ...A....Q.200.. Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f 14 05 65 1b 28 61 c9 75 ....e.(a.u Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 ser1..SVC=0.1;P. Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1 a2 94 f8 39 80 ca 3c 96 Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8 6c 07 8e fb 58 84 8d f6 ....=].1...X... Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff ff ff 4f 27 02 01 00 25 3m.!...8 Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e 33 b5 4e 69 90 e7 84 25 ....% Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87 ca dc c9 b3 75 73 65 72 B....3....user Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01 35 6c 65 61 70 3a 73 65 1.;....5leap:se Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65 79 3d 29 80 1d 2c 1c 85 ssion-key=).... Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93 69 2a 55 d2 e5 46 89 8b ...)~@...i\*U..F.. Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e 95 29 47 54 1a 1f 00 00 ,;eI>D.~.)GT.... Thu Aug 16 14:42:54 2007: 0000080: 00 09 01 19 61 75 74 68 2d 61 6c 67 6f 2d 74 79 ....auth-algo-ty Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c 65 61 70 1a 0d 00 00 37 pe=eap-leap....7 Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31 19 14 43 41 43 53 3a 30 c..User1..CACS:0 Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34 64 32 2f 31 50 12 9a 71 /9/a4df4d2/1P..q Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5 c8 b1 71 94 97 d1 ..}t....q... Thu Aug 16 14:42:54 2007: \*\*\*\*Enter processIncomingMessages: response code=2 Thu Aug 16 14:42:54 2007: \*\*\*\*Enter processRadiusResponse: response code=2 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93

Access-Accept received from RADIUS server

10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3 Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize.....236 Thu Aug 16 14:42:54 2007: resultCode.....0 Thu Aug 16 14:42:54 2007: protocolUsed.....0x0 0000001 Thu Aug 16 14:42:54 2007: proxyState.....00: 40:96:AF:3E:93-03:02 Thu Aug 16 14:42:54 2007: Packet contains 6 AVPs: Thu Aug 16 14:42:54 2007: AVP[01] Framed-IP-Address.....0xffffffff (-1) (4 bytes) Thu Aug 16 14:42:54 2007: AVP[02] EAP-Message.....DATA (37 bytes) Thu Aug 16 14:42:54 2007: AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes) Thu Aug 16 14:42:54 2007: AVP[04] Airespace / ACL-Name.....User1 (5 bytes) Thu Aug 16 14:42:54 2007: AVP[05] Class.....CACS:0/9/a4df4d2/1 (18 bytes) Thu Aug 16 14:42:54 2007: AVP[06] Message-Authenticator.....DATA (16 bytes) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override for station 00:40:96:af:3e:93 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values for station 00:40:96:af:3e:93 source: 4, valid bits: 0x400 gosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName:User1 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into chain for station 00:40:96:af:3e:93

Você pode usar uma combinação do comando **show wlan summary** para reconhecer qual das suas WLANs emprega a autenticação de servidor RADIUS. Em seguida, você pode exibir o comando **show client summary** para ver quais endereços MAC (clientes) foram autenticados com êxito nas WLANs RADIUS. Você também pode correlacionar isso com as tentativas aprovadas ou os registros de tentativas com falha do Cisco Secure ACS.

A Cisco recomenda que você teste suas configurações de ACL com um cliente sem fio para garantir que você as tenha configurado corretamente. Se eles não funcionarem corretamente, verifique as ACLs na página da Web da ACL e se as alterações da ACL foram aplicadas à interface do controlador.

Você também pode usar estes comandos show para verificar sua configuração:

 show acl summary — Para exibir as ACLs configuradas no controlador, use o comando show acl summary.

Aqui está um exemplo:

(Cisco Controller)	>show acl	summary
ACL Name		Applied
Userl		Yes
User2		Yes

• show acl detailed <ACL\_Name> — Exibe informações detalhadas sobre as ACLs

configuradas.Aqui está um exemplo:**Observação:** algumas das linhas na saída foram movidas para a segunda linha devido a restrições de espaço.

Cisco Controller) >show acl detailed User1

Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action \_\_ \_\_\_ \_\_\_\_ \_\_\_\_\_ \_\_\_\_ 1 In 172.16.0.0/255.255.0.0 172.16.1.100/255.255.255.255 Any 0-65535 0-65535 Any Permit 2 Out 172.16.1.100/255.255.255 172.16.0.0/255.255.0.0 Any 0-65535 0-65535 Any Permit (Cisco Controller) >show acl detailed User2 Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action \_ \_\_\_ \_\_\_\_\_ ---- ----- ----- -----172.16.0.0/255.255.0.0 172.16.1.50/255.255.255.255 1 In 0-65535 0-65535 Any Permit Anv 2 Out 172.16.1.50/255.255.255.255 172.16.0.0/255.255.0.0 Any 0-65535 0-65535 Any Permit

 show client detail <MAC Address of the client> - Exibe informações detalhadas sobre o cliente Wireless.

#### **Dicas para Troubleshooting**

Use estas dicas para solucionar problemas:

- Verifique no controlador se o servidor RADIUS está no estado ativo e não no modo de espera ou desativado.
- No controlador, verifique se o servidor RADIUS está selecionado no menu suspenso da WLAN (SSID).
- Verifique se o servidor RADIUS recebe e valida a solicitação de autenticação do cliente sem fio.
- Verifique os relatórios Autenticações aprovadas e Tentativas com falha no servidor ACS para fazer isso. Esses relatórios estão disponíveis em Relatórios e atividades no servidor ACS.

## Informações Relacionadas

- <u>ACLs em Wireless LAN Controllers: Regras, limitações e exemplos</u>
- Exemplo de configuração de ACLs em Wireless LAN Controller
- Exemplo de Configuração de Filtros MAC com Controladores Wireless LAN (WLCs)
- Guia de configuração do Controlador de LAN sem fio da Cisco, versão 5.2
- Suporte Técnico e Documentação Cisco Systems