# 使用 RADIUS 服务器进行的外部 Web 身份验证

## 目录

简介 先决条件 要求 使用的组件 网络图 规则 外部 Web 身份验证 配置 WLC 为 Cisco Secure ACS 配置 WLC 在 WLC 上配置用于 Web 身份验证的 WLAN 在 WLC 上配置 Web 服务器信息 配置 Cisco Secure ACS 在 Cisco Secure ACS 上配置用户信息 在 Cisco Secure ACS 上配置 WLC 信息 客户端身份验证过程 客户端配置 客户端登录过程 验证 验证 ACS 验证 WLC 故障排除 故障排除命令 相关信息

# <u>简介</u>

本文介绍如何使用外部 RADIUS 服务器执行外部 Web 身份验证。

## <u>先决条件</u>

#### <u>要求</u>

尝试进行此配置之前,请确保满足以下要求:

- •了解轻量接入点 (LAP) 和 Cisco WLC 配置的基础知识
- 有关如何设置和配置外部 Web 服务器的知识
- 有关如何配置 Cisco Secure ACS 的知识

### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行固件版本 5.0.148.0 的无线 LAN 控制器
- Cisco 1232 系列 LAP
- Cisco 802.11a/b/g 无线客户端适配器 3.6.0.61
- •托管 Web 身份验证登录页面的外部 Web 服务器
- •运行固件版本 4.1.1.24 的 Cisco Secure ACS 版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

### <u>网络图</u>

本文档使用以下网络设置:



- 《下定本文扫下使用的下 地址:
  - WLC 使用 IP 地址 10.77.244.206
  - LAP 已使用 IP 地址 10.77.244.199 注册到 WLC
  - •Web 服务器使用 IP 地址 10.77.244.210
  - Cisco ACS 服务器使用 IP 地址 10.77.244.196
  - 客户端收到来自管理接口的一个映射到 WLAN 的 IP 地址 10.77.244.208

#### <u>规则</u>

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

## <u>外部 Web 身份验证</u>

Web 身份验证是第 3 层身份验证机制,用于对来宾用户进行身份验证以进行 Internet 访问。使用此 过程进行验证的用户在其成功完成验证过程之前无法访问 Internet。有关外部 Web 身份验证过程的 完整信息,请阅读文档<u>使用无线 LAN 控制器进行外部 Web 身份验证配置的示例的外部 Web 身份</u> 验证过程</u>部分。

在本文中,我们来看看一个配置示例,该示例中使用外部 RADIUS 服务器执行外部 Web 身份验证 。

### <u>配置 WLC</u>

在本文中,我们假设 WLC 已配置且具有一个注册到 WLC 的 LAP。此外,本文档进一步假设已配置 WLC 进行基本操作,并且已在 WLC 中注册 LAP。如果您是尝试设置WLC以便使用LAP执行基本操作的新用户,请参阅<u>轻量AP(LAP)注册到无线LAN控制器(WLC)</u>。要查看注册到 WLC 的 LAP,请导航到 Wireless > All APs。

一旦配置 WLC 进行基本操作并在其中注册一个或多个 LAP,即可使用外部 Web 服务器为外部 Web 身份验证配置 WLC。在本示例中,我们使用 Cisco Secure ACS 4.1.1.24 版作为 RADIUS 服 务器。首先,我们将配置此 RADIUS 服务器的 WLC,然后我们将查看 Cisco Secure ACS 上关于 此设置所需的配置。

#### <u>为 Cisco Secure ACS 配置 WLC</u>

执行这些步骤以便在 WLC 上添加 RADIUS 服务器:

- 1. 从 WLC GUI 中,单击 Security 菜单。
- 2. 在 AAA 菜单下,导航到 Radius > Authentication 子菜单。
- 3. 单击 New, 并输入 RADIUS 服务器的 IP 地址。在本示例中,服务器的 IP 地址为 10.77.244.196。
- 4. 在 WLC 中输入共享密钥。共享密钥在 WLC 上的配置应相同。
- 5. 选择 ASCII 或 Hex 为共享密钥格式。在 WLC 上需要选择同一格式。
- 6. 1812 是用于 RADIUS 验证的端口号。
- 7. 确保 Server Status 选项设置为 Enabled。
- 8. 选中 Network User Enable 框以对网络用户进行身份验证。
- 9. 单击 Apply。

li.ili. cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication	Servers > New
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> <li>Accounting</li> </ul>	Server Index (Priority) Server IPAddress	2 • 10.77.244.196
Fallback FACACS+ LDAP	Shared Secret Format	ASCII 💌
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Shared Secret Confirm Shared Secret	••••••
▶ Local EAP	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
<ul> <li>Priority Order</li> <li>Access Control Lists</li> </ul>	Port Number	1812
Wireless Protection Policies	Server Status	Enabled 👻
Web Auth     Advanced	Support for RFC 3576	Enabled 💌
- Addition	Server Timeout	2 seconds
	Network User	Enable
	Management	Enable
	IPSec	Enable

#### 在 WLC 上配置用于 Web 身份验证的 WLAN

下一步是在 WLC 上为 Web 身份验证配置 WLAN。执行这些步骤以便在 WLC 上配置 WLAN:

- 1. 从控制器 GUI 中单击 WLAN 菜单,并选择 New。
- 2. 选择 WLAN 作为类型。
- 3. 输入配置文件名称和您所选的 WLAN SSID,并单击 Apply。注意:WLAN SSID区分大小写。

cisco			WIRELESS	SECURITY	MANAGEMENT
WLANs	WLANs > New				
WLANS WLANS	Туре	WLAN	~		
Advanced	Profile Name	WLAN1			
	WLAN SSID	WLAN1			

4. 在 General 选项卡下,确保为 Status 和 Broadcast SSID 选中了 Enabled 选项。WLAN 配置

/LANS	WLANs > E	dit	Sector and the					
WLANs WLANs	General	Security	Q05	Advanced				
Advanced	Profile Na	me	WLAN1					
	Туре		WLAN					
	SSID		WLAN1					
	Status		🗹 Ena	bled				
	Security (	Policies	[WPA2] (Modifica	[[Auth(882.1X tions done unde	)] r security tab	will appear after	applying the change	:5.)
	Radio Pol	icy	Al	*				
	Interface	Interface		ment 💌				
	Broadcas	t SSID	Enal	bled				

- 5. 为 WLAN 选择一个接口。通常,唯一 VLAN 中配置的接口将映射到 WLAN,以便客户端能接 收该 VLAN 中的一个 IP 地址。在本例中,我们使用*管理 接口。*
- 6. 选择 Security 选项卡。
- 7. 在 Layer 2 菜单下,为 Layer 2 Security 选择 None。
- 8. 在 Layer 3 菜单下,为 Layer 3 Security 选择 None。选中 Web Policy 复选框并选择 Authentication。

W/LANe	MI AND SEdit
WLANS	WLANS > Edit
* WLANS	General Security QoS Advanced
WLANs	Layer 2 Layer 3 AAA Servers
Advanced	
	Layer 3 Security None
	V Web Policy 2
	Authantication
	O Passthrough
	O Conditional Web Redirect
	Solach Bane Web Bedirect
	Over-ride Global Config 🔲 Enable
	Easthister
	1 CKIP is not supported by 10xx model APs
	2 Web Policy cannot be used in combination with IPsec
	4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded client)

9. 在 AAA servers 菜单下,对于身份验证服务器,请选择在此 WLC 上配置的 RADIUS 服务器。 其他菜单应保留默认值。

₩LANS WLANS # Advanced	General Security QoS Advanced Layer 2 Layer 3 AAA Servers							
	Radius Servers	LDAP Server	5					
	Authentication Servers Accounting Servers	Server 1 Server 2 Server 3	None None None					
	Foot Notes      Foot Notes      CKIP is not supported by 10xx model APs      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination      Web Roley cannot be used in combination with IPsec      Web Roley cannot be used in combination      Kenter State      Ken	istrative override to reset e	voluded clients)					

### 在 WLC 上配置 Web 服务器信息

托管 Web 验证页的 Web 服务器应在 WLC 上进行配置。执行这些步骤以配置 Web 服务器:

- 1. 单击"Security"选项卡。转到 Web Auth > Web Login Page。
- 2. 将 Web 身份验证类型设置为 External。
- 3. 在 Web Server IP Address 字段中,输入托管 Web 身份验证页的服务器的 IP 地址,并单击 Add Web Server。在本例中,IP 地址是 *10.77.244.196*,显示在外部 Web 服务器下。
- 4. 在 URL 字段中输入 Web 身份验证页的 URL (在本例中为 http://10.77.244.196/login.html)。

cisco		R <u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Security	Web Lo	ogin Page				
General	Web Au	thenticati	on Type	External (	Redirect to ex	ternal server) 🔽
Authentication	URL htt	p://10.77.24	4.196/login.html			
Fallback	Externa	al Web Serv	ers			
LDAP	10.77.244.196 <u>Remove</u>					
Local Net Users MAC Filtering Disabled Clients	Web Se	rver IP Ad	dress		]	
AP Policies				Add Web Ser	ver	
Local EAP						
Priority Order						
Access Control Lists						
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>						
<ul> <li>Web Auth</li> <li>Web Login Page</li> <li>Certificate</li> </ul>						
Advanced						

## 配置 Cisco Secure ACS

在本文中,我们假设 Cisco Secure ACS 服务器已安装并在计算机上运行。有关如何设置 Cisco Secure ACS 的详细信息,请参阅 <u>Cisco Secure ACS 4.2 配置指南</u>。

#### 在 Cisco Secure ACS 上配置用户信息

执行这些步骤以便在 Cisco Secure ACS 上配置用户:

1. 从 Cisco Secure ACS GUI 中选择 **User Setup,输入用户名,并单击 Add/Edit**。在本例中,用 户为 *user1*。

CISCO SYSTEMS	User Setup
	Select
User Setup	
Group Setup	User: user1
Shared Profile Components	Find Add/Edit
Network Configuration	List users beginning with letter/number:
System Configuration	<u>A B C D E F G H I J K L M</u> <u>N O P Q R S T U V U X Y Z</u>
Interface Configuration	0123456789
Administration Control	List all users
External User Databases	Remove Dynamic Users
Posture Validation	
Network Access Profiles	Back to Help
Reports and Activity	
Documentation	

2. 默认情况下,PAP 用于验证客户端。用户的密码在 User Setup > Password Authentication > Cisco Secure PAP 下输入。确保您选择 ACS Internal Database 进行密码验证。

STSTEMS	User Setup				
ier Hup	Edit	User: us	er1 (New L	ser)	
roup	-	00011 00		,	
ared Profile imponents		□ A	ccount Disabled		
work figuration		Suppleme	entary User Info		?
tem figuration	Real Name	User1			
erface figuration	Description				
ninistration trol					
ernal User abases		Us	er Setup		?
ture	Password Aut	hentication:			
ork Access			AC	S Internal Database	-
les	CiscoSec	ure PAP (Also used	for CHAP/MS-CH	HAP/ARAP, if the Separat field is not checked	.e
orts and vity	Pas	sword			Î
mentation	Confirm Pas	sword	•••••		
	🗆 Separate	(CHAP/MS-CHAP/A	RAP)		
	Pas	sword			]
	Confirm Pas	sword			
	When a token CHAP passwo especially use	r server is used for rd for a token card ful when token car	authentication, user allows CHA ching is enabled.	supplying a separate P authentication. This is	
		Group to whic	ch the user is as	signed:	
		Default Group		•	
				and a second	

- 3. 需要向用户分配用户所属的组。选择 Default Group。
- 4. 单击"Submit"。

### <u>在 Cisco Secure ACS 上配置 WLC 信息</u>

执行这些步骤以便在 Cisco Secure ACS 上配置 WLC 信息:

- 1. 在 ACS GUI 中,单击 Network Configuration 选项卡,并单击 Add Entry。
- 2. Add AAA client 屏幕将显示。
- 3. 输入客户端的名称。在本例中,我们使用 WLC。
- 4. 输入客户端的 IP 地址。WLC 的 IP 地址是 10.77.244.206。
- 5. 输入共享密钥和密钥格式。这应该与 WLC 的 Security 菜单中设置的条目相匹配。
- 6. 选择 ASCII 作为关键词输入格式,这在 WLC 上应该是相同的。
- 7. 选择 RADIUS (Cisco Airespace) 用于进行身份验证,以便设置 WLC 和 RADIUS 服务器之间 使用的协议。
- 8. 单击 Submit+Apply。

	Add AAA Client
AAA Client Hostname	WLC
AAA Client IP Address	×
m Shared Secret	abc 123
RADIUS Key Wrap Key Encryption Key	
Message Authenticator Code Key Input Format	€ ASCII C Hexadecimal
Authenticate Using	RADIUS (Cisco Airespace)
Single Connect TACACS+ /     Digle Connect TACACS+ /     Digle Connect TACACS+ /	AAA Client (Record stop in accounting on failure) kets from this AAA Client
Log RADIUS Tunneling Pac	kets from this AAA Client
Replace RADIUS Port info v     Match Framed-IP-Address	with Username from this AAA Client with user IP address for accounting packets from this AAA Client
	Submit Submit + Apply Cancel

# <u>客户端身份验证过程</u>

### <u>客户端配置</u>

在本例中,我们使用 Cisco Aironet Desktop Utility 执行 Web 身份验证。执行这些步骤以便配置 Aironet Desktop Utility。

- 1. 从"开始"> Cisco Aironet > Aironet Desktop Utility 中打开 Aironet Desktop Utility。
- 2. 单击 Profile Management 选项卡。

Cisco Aironet Desktop Utility - Current Profile: Default ion <u>O</u> ptions <u>H</u> elp	?
urrent Status Profile Management Diagnostics	
Default	<u>N</u> ew
	Modify
	Remo <u>v</u> e
	Activate
r Details	_
Network Type:	Import
Security Mode:	
Network Name 1 (SSID1):	<u>Export</u>
Network Name 2 (SSID2):	Scan
Network Name 3 (SSID3):	- ogana
Auto Select Profiles	Order <u>P</u> rofiles

3. 选择 **Default profile,并单击 Modify**。点击**常规选项卡。**配置配置文件名称。本例中使用的是 *Default。*在 Network Names 下,配置 SSID。本例中使用的是 *WLAN1。* 

Profile Management		2 🛛
General Security Advance	ced	
Profile Settings		-
Profile Name:	Default	
Client Name:	Client1	
Network Names		
SSID1:	WLAN1	
SSID2:		
SSID3:		
L		
	OK	Cancel

**注意:**SSID区分大小写,并且应该与WLC上配置的WLAN匹配。单击"Security"选项卡。请选 择 **None 作为 Web 身份验证的安全性。** 

Profile Management	? 🔀
General Security Advanced	
Set Security Options	
O WPA/WPA2/CCKM WPA/WPA2/CCKM EAP Type: LEAP ✓	
○ WPA/WPA2 Passphrase	
O 802.1x 802.1x EAP Type: LEAP ✓	
O Pre-Shared Key (Static WEP)	
None	
Configure Allow Association to Mixed Cells Locked Profile	
Group Policy Delay: 0 😂 sec	
ок с	Cancel

单击 Advanced 选项卡。在 Wireless Mode 菜单下,选择无线客户端与 LAP 通信的频率。在 Transmit Power Level 下,选择 WLC 上配置的电源。保留节电模式的默认值。选择 Infrastructure 作为网络类型。将 802.11b 前导码设置为 Short & Long 以获得更好的兼容性。 Click

OK.

Transmit Power Level	Power Save Mode:	CAM (Constantly A	wake Mode) 🛛 💙						
802.11b/g: 100 mW 💉	Network Type:	Infrastructure							
802.11a: 40 mW 💌	802.11b Preamble:	Short & Long	O Long Only						
Wireless Mode	Wireless Mode When Starting	g Ad Hoc Network							
S GHz 54 Mbps									
2.4 GHz 54 Mbps	🔿 5 GHz 54 Mbps								
2.4 GHz 11 Mbps	O 2.4 GHz 11 Mbps								
	O 2.4 GHz 54 Mbps	Channe	l: Auto 👻						
	802.11 Authentication Mode								
	O Auto 0 0	pen (	) Shared						

4. 一旦在客户端软件上配置了配置文件,客户端将顺利地关联并将收到为管理接口配置的 VLAN 池中的一个 IP 地址。

#### <u>客户端登录过程</u>

此部分说明客户端登录如何发生。

- 打开浏览器窗口并输入所有 URL 或 IP 地址。这将从 Web 身份验证页转到客户端。如果控制器运行任何早于 3.0 的版本,则用户必须输入 https://1.1.1.1/login.html 才能显示 Web 身份验证页。此时将显示安全警报窗口。
- 2. 单击 Yes 以继续操作。
- 3. 当登录窗口出现时,请输入在 RADIUS 服务器上配置的用户名和密码。如果登录成功,您将 看到两个浏览器窗口。较大的窗口表示您已成功登录,您可以使用此窗口浏览 Internet。完成

Web Authentication
Login Successful I
You can now use all regular network services over the wireless network.
Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page: https://linka.com/html Logout

对访客网络的使用时,可使用较小的窗口注销。

## <u>验证</u>

为使 Web 验证成功,您需要检查设备是否以适当的方式进行了配置。此部分说明如何验证过程中 使用的设备。

### <u>验证 ACS</u>

1. 单击 User Setup,然后在 ACS GUI 上单击 List All Users。

CISCO SYSTEMS	User Setup
antilliterantillitera-	Select
User Setup	
Setup	User:
Shared Profile Components	Find Add/Edit
Network Configuration	List users beginning with letter/number:
System Configuration	<u>A B C D E F G H I J K L M</u> <u>N O P Q R S T U V W X Y Z</u> O 1 2 3 4 5 6 7 8 9
Configuration	List all users
Administration Control	
Databases	Remove Dynamic Users
nono Posture Validation	
Network Access Profiles	Back to Help
Reports and Activity	
Documentation	

确保用户的状态为 Enabled,并且默认组已映射到用户。

er List			
User	Status	Group	Network Access Profile
	Enabled	Default Croup (2 users)	(Dofpult)

2. 单击 Network Configuration 选项卡,并在 AAA Clients 表中进行查找,以便验证 WLC 是否配置为 AAA 客户端。

Setup									
Setup	<b>\$</b>	AAA Clients							
tared Profile onponents	AAA Client Hostname	AAA Client IP Address	Authent	ticate Using					
at work onfiguration	wici	10.77.244.206	RADIUS (C	isco Airespace)					
usten onfiguration		Add Entry Search							
configuration dministration ontrol	<b>%</b> Q	AAA Servers	AAA Servers						
Octernal Uper	AAA Server Name	AAA Server IP Address	AAA Server IP Address AAA Server						
Autobases	TS-Web	10.77.244.196	.77.244.196 CiscoSecure ACS						
etwork Access tatle: Reports and Ketivity Daline		Add Entry Search Proxy Distribution Table	( att						
A CONTRACTOR OF	Character String	AAA Servers	Strip	Account					
	(Default)	TS-Web	NO	Local					
		Add Entry Sort Entries							

#### <u>验证 WLC</u>

1. 单击 WLC GUI 中的 **WLAN 菜单。**确保用于 Web 身份验证的 WLAN 在页面上列出。确保 WLAN 的 Admin Status 为 *Enabled*。确保 WLAN 的安全策略显示 *Web-Auth*。

cisco	MONITOR WLANS	CONTROLLER WIRELES	S SECURITY MONAGEMEN	t commands	неца	
WLANS	WLANs Profile Name	Туре W	LAN 551D	Admin Status	Security Policies	
Advanced	WLAN1	WLAN W	LAN1	Enabled	Web-Auth	

2. 单击 WLC GUI 中的 **Security 菜单。**确保 Cisco Secure ACS (10.77.244.196) 在页面上列出。 确保已选中 Network User 框。确保端口是 *1812,并且 Admin Status 为 Enabled*。

uluilu cisco	MONITOR	<u>W</u> LANS <u>C</u> O	ONTROLLER	WIRELESS S	ECURITY	MANAGEMENT C	OMMANDS HELP	
Security	RADIUS	Authenticati	ion Serve	rs				
▼ AAA General ▼ RADIUS Authentication Accounting	Call Stati Use AES	ion ID Type [ Key Wrap	IP Address	ed for FIPS custome	ers and requi	res a key wrap com	pliant RADIUS server)	
Fallback TACACS+	Network	Management	Server Index	Server Address	Port	IPSec	Admin Status	
LDAP Local Net Users			1	10.77.244.196	1812	Disabled	Enabled	
Disabled Clients User Login Policies AP Policies Local EAP								
Priority Order								
Access Control Lists								
Wireless Protection Policies								
▶ Web Auth								
Advanced								

Web 身份验证不成功有许多原因。文档<u>对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排</u> 除将清楚地说明详细原因。

故障排除命令

故障排除

**注意:使**用这些<u>debug命令之前,请参</u>阅有关Debug命令的**重要**信息。

通过 Telnet 连接到 WLC 并发出这些命令以对身份验证进行故障排除:

#### · debug aaa all enable

Fri	Sep	24	13:59:52	2010:	00:40	):96:	ac:	dd:(	)5 \$	Succ	cess	sful	l tı	ansi	miss	sior	ı of	ΞAι	ithe	enti	ĹС
atio	n Pa	acke	et (id 1)	to 10	.77.24	14.19	6:18	812,	p	roxy	r st	tate	e 00	):40	:96:	ac	dd	:05-	-00:	01	
Fri	Sep	24	13:59:52	2010:	00000	0000:	01	01	00	73	00	00	00	00	00	00	00	00	00	00	0
0 00		.s																			
Fri	Sep	24	13:59:52	2010:	00000	0010:	00	00	00	00	01	07	75	73	65	72	31	02	12	93	С
3 66			user1	f																	
Fri	Sep	24	13:59:52	2010:	00000	030:	75	73	65	72	31										
	us	seri	1																		
Fri	Sep	24	13:59:52	2010:	****B	Inter	pro	oces	ssIn	lcon	ning	gMes	ssag	ges:	res	spor	ıse	cod	le=2	2	
Fri	Sep	24	13:59:52	2010:	****B	Inter	pro	oces	ssRa	adiu	ısRe	espo	onse	e: r	espo	onse	e co	ode=	=2		
Fri	Sep	24	13:59:52	2010:	00:40	):96:	ac:	dd:(	)5 2	Acce	ess	-Acc	cept	re	ceiv	<i>r</i> ed	fro	om F	RADI	US	S
erve	r 10	).77	7.244.196	for mo	obile	00:4	0:9	6:a0	:do	<b>1:</b> 05	5 re	ecei	lvel	Id =	0						
Fri	Sep	24	13:59:52	2010:	Autho	oriza	tio	nRes	spor	ise:	02	x122	2386	lb0							
Fri	Sep	24	13:59:52	2010:		str	ucti	ures	Size	∍	•••									.89	)
Fri	Sep	24	13:59:52	2010:		res	ult	Code	≥		•••									.0	
Fri	Sep	24	13:59:52	2010:		pro	toc	olUs	sed		•••									. 03	к0
0000	001																				
Fri	Sep	24	13:59:52	2010:		pro	xyS	tate	≥		•••									.00	):
40:9	6:AC	C:DI	0:05-00:00	C																	
Fri	Sep	24	13:59:52	2010:		Pac	ket	cor	nta	lns	27	AVPs	5:								
Fri	Sep	24	13:59:52	2010:			AV	P[01	L] I	Fran	ned-	-IP-	-Add	lres	s						•••
	.0xf	Eff	Effff (-1)	) (4 by	/tes)																
Fri	Sep	24	13:59:52	2010:			AV	P[02	2] (	Clas	ss.										
	.CAC	CS:(	)/5183/a40	df4ce/u	lser1	(25	byt	es)													
Fri	Sep	24	13:59:52	2010:	Authe	entic	ati	on f	ai	Led	foi	r us	ser1	, s	ervi	Lce	Tyr	be:	0		

Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio n 00:40:96:ac:dd:05 Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96 :ac:dd:05 source: 48, valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s tation 00:40:96:ac:dd:05 Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c Fri Sep 24 13:59:52 2010: Packet contains 12 AVPs: AVP[01] User-Name..... Fri Sep 24 13:59:52 2010: .....user1 (5 bytes) Fri Sep 24 13:59:52 2010: AVP[02] Nas-Port..... .....0x00000002 (2) (4 bytes) Fri Sep 24 13:59:52 2010: AVP[03] Nas-Ip-Address..... .....0x0a4df4ce (172881102) (4 bytes) AVP[04] Framed-IP-Address..... Fri Sep 24 13:59:52 2010: ....0x0a4df4c7 (172881095) (4 bytes)

debug aaa detail enable

失败的身份验证尝试在位于 Reports and Activity > Failed Attempts 处的菜单中列出。

# 相关信息

- 无线局域网控制器 Web 身份验证配置示例
- 对无线 LAN 控制器 (WLC) 上的 Web 身份验证进行故障排除
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 在无线局域网控制器(WLCs)上使用LDAP的Web认证配置示例
- <u>技术支持和文档 Cisco Systems</u>

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。