使用無線LAN控制器和Cisco Secure ACS的每個 使用者ACL配置示例

目錄

簡介 必要條件 需求 採用元件 慣例 背景資訊 網路圖表 設定 設定無線LAN控制器 為無線使用者建立VLAN 配置WLC以使用Cisco Secure ACS進行身份驗證 為無線使用者建立新的WLAN 定義使用者的ACL 配置Cisco Secure ACS伺服器 <u>將無線區域網控制器配置為Cisco Secure ACS上的AAA客戶端</u> 在Cisco Secure ACS上配置使用者和使用者配置檔案 驗證 疑難排解 疑難排解提示 相關資訊

<u>簡介</u>

本檔案將通過範例說明如何在WLC上建立存取控制清單(ACL),並將其套用到依賴RADIUS授權的 使用者。

<u>必要條件</u>

<u>需求</u>

嘗試此組態之前,請確保符合以下要求:

- 有關如何配置Cisco Secure ACS伺服器以驗證無線客戶端的基本知識
- 瞭解Cisco Aironet輕量型存取點(LAP)和Cisco無線LAN控制器(WLC)的組態
- •思科統一無線安全解決方案知識

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- •執行5.0.148.0版的Cisco 4400系列無線LAN控制器
- 思科Aironet 1231系列輕量型接入點(LAP)
- 運行3.6版的Cisco Aironet 802.11 a/b/g Cisco無線LAN客戶端介面卡
- Cisco Aironet案頭實用程式版本3.6
- Cisco安全ACS伺服器版本4.1
- 執行IOS®版本12.4(11)T的Cisco 2800系列整合式服務路由器
- 執行12.0(5)WC3b版的Cisco Catalyst 2900XL系列交換器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>背景資訊</u>

每使用者訪問控制清單(ACL)是思科身份網路的一部分。Cisco無線LAN解決方案支援身份網路,雖 然它允許網路通告單個SSID,但也允許特定使用者根據其使用者配置檔案繼承不同的策略。

每使用者ACL功能提供將無線LAN控制器上配置的ACL基於RADIUS授權應用到使用者的功能。這 是使用Airespace-ACL-Name供應商特定屬性(VSA)完成的。

此屬性指明應用於客戶端的ACL名稱。當RADIUS存取接受中存在ACL屬性時,系統會在使用者站 進行驗證之後將ACL名稱套用到使用者站。這會覆蓋分配給介面的所有ACL。它會忽略分配的介面 ACL並應用新的介面ACL。

ACL-Name屬性格式的摘要如下所示。欄位從左向右傳輸

0 1 2 3 0 1 2 3 4 5 6 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 2 3 4 5 6 7 8 9 0 1 Type Length Vendor-Id Vendor type | Vendor length | Vendor-Id (cont.) ACL Name... • Type - 26 for Vendor-Specific • Length - >7• Vendor-Id - 14179 • Vendor type - 6 • Vendor length - >0 • Value - A string that includes the name of the ACL to use for the client. The string is case sensitive.

有關Cisco統一無線網路身份網路的詳細資訊,請參閱配置安全解決方案文檔的配置身份網路部分。

本檔案會使用以下網路設定:

在此設定中,無線LAN控制器WLC和LAP用於為部門A和部門B中的使用者提供無線服務。所有無線 使用者都使用通用的WLAN(SSID)Office來訪問網路,並且處於VLAN Office-VLAN中。



Cisco Secure ACS伺服器用於驗證無線使用者。EAP身份驗證用於驗證使用者。WLC、LAP和 Cisco Secure ACS伺服器連線到第2層交換機,如圖所示。

路由器R1通過第2層交換機連線有線端上的伺服器,如圖所示。路由器R1還充當DHCP伺服器,為 子網172.16.0.0/16中的無線客戶端提供IP地址。

您需要配置裝置以便發生以下情況:

部門A的User1隻能訪問伺服器172.16.1.100

部門B的使用者2僅訪問伺服器172.16.1.50

為此,您需要在WLC上建立2個ACL:一個用於User1,另一個用於User2。建立ACL後,您需要配置 Cisco Secure ACS伺服器,以便在無線使用者成功身份驗證時將ACL名稱屬性返回到WLC。接著 ,WLC會將ACL套用至使用者,因此網路會根據使用者設定檔而受限制。 **注意:**本文檔使用LEAP身份驗證對使用者進行身份驗證。Cisco LEAP易受字典攻擊。在即時網路 中,應使用更安全的身份驗證方法,如EAP FAST。由於本檔案的重點是解釋如何配置每使用者 ACL功能,因此使用LEAP是為了簡化。

下一節將提供為此設定配置裝置的逐步說明。

<u>設定</u>

設定每個使用者ACL功能之前,您必須設定WLC以達成基本操作,並向WLC註冊LAP。本檔案假設WLC已設定為基本操作,且LAP已註冊到WLC。如果您是嘗試設定WLC以使用LAP執行基本操作的新使用者,請參閱<u>向無線LAN控制器(WLC)註冊輕量AP(LAP)</u>。

註冊LAP後,請完成以下步驟,為此設定配置裝置:

- 1. <u>設定無線LAN控制器。</u>
- 2. <u>配置Cisco Secure ACS伺服器。</u>
- 3. <u>驗證設定.</u>

註:本文檔討論無線端所需的配置。本檔案假設有線組態已就緒。

設定無線LAN控制器

在無線LAN控制器上,您需要執行以下操作:

- •<u>為無線使用者建立VLAN。</u>
- 配置WLC以使用Cisco Secure ACS驗證無線使用者。
- <u>為無線使用者建立新的WLAN。</u>
- •<u>為無線使用者定義ACL。</u>

<u>為無線使用者建立VLAN</u>

要為無線使用者建立VLAN,請完成以下步驟。

- 1. 前往WLC GUI並選擇**Controller > Interfaces**。出現「Interfaces(介面)」視窗。此視窗列出 控制器上配置的介面。
- 2. 按一下「New」以建立一個新的動態介面。
- 在Interfaces > New視窗中,輸入介面名稱和VLAN ID。然後點選應用。在本示例中,動態介 面命名為Office-VLAN, VLAN ID分配為20。

G • O • 🖻 🖹 🐔 🔎	📌 😁 🌛	8 E							🥂 – 8 ×
ahaha							Saye C	onfiguration <u>Ping</u>	Logout Refresh
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECORITY	MONAGEMENT	COMMANDS	HELP	~
Controller	Interface	s > New						< Back	Apply
General	Interface	Name 0	ffice-VLAN						
Inventory	VI AN TO	2	0		-				
Interfaces	YLAN IU	I.	0						
Mobility Management									
Perts									
Master Controller Mode									
Network Time Protocol									
▶ QoS									
▶ CDP									

4. 在Interfaces > Edit視窗中,輸入動態介面的IP地址、子網掩碼和預設網關。將其分配給 WLC上的物理埠,並輸入DHCP伺服器的IP地址。然後按一下「Apply」。

cisco	MONITOR WLANS	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Saya C COMMANDS	HELP	Cogout Retrest
Controller General Inventory Interfaces Internal DHCP Server > Mobility Management Ports Master Controller Mode Network Time Protocol > QoS > CDP	Interfaces > Edit General Information Interface Name MAC Address Interface Address VLAN Identifier IP Address Netmask Gateway Physical Information Port Number Configuration Quarantine DHCP Information Primary DHCP Server Secondary DHCP Server Secondary DHCP Server Access Control List ACL Name Note: Changing the Interface temporarily disabled and is some clients.	Office-V 00:0b:0 20 172 255 172 255 172 172 172 172 172 172 172 172 172 172	LAN 5:33:84:a0 .16.1.25 .255.0.0 .16.1.75 .16.1.75]]] LARs to be ectivity for			< Back	Apply

在本例中,以下引數用於Office-VLAN介面:

```
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
```

配置WLC以使用Cisco Secure ACS進行身份驗證

需要設定WLC,才能將使用者憑證轉送到外部RADIUS伺服器(在本案例中為Cisco Secure ACS)。 接著,RADIUS伺服器會驗證使用者認證,並在無線使用者成功驗證後,將ACL name屬 性返回到WLC。

完成以下步驟,以便為RADIUS伺服器設定WLC:

- 1. 從控制器GUI中選擇Security和RADIUS Authentication,以顯示RADIUS Authentication Servers頁面。然後按一下New以定義RADIUS伺服器。
- 2. 在**RADIUS Authentication Servers > New**頁中定義RADIUS伺服器引數。這些引數包括 RADIUS伺服器IP地址、共用金鑰、埠號和伺服器狀態。

cisco		Save Configuration Bing Logout Bafrer
Security	RADIUS Authentication S	Cervers > New < Back Apply
 ★ AAA General ★ RADIUS 	Server Index (Priority)	1
Accounting TACACS+ LDAP	Shared Secret Format	ASCII \star
Local Net Users MAC Filtering	Shared Secret	
User Login Policies AP Policies	Confirm Shared Secret	••••
Local EAP Priority Order	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Access Control Lists	Port Number	1812
IPSec Certs Wireless Protection	Server Status	Enabled 💌
Policies Web Auth	Support for RFC 3576	Enabled 🗵
CIDS	Retransmit Timeout	30 seconds
	Network User	Enable
	Management	R Enable
	IPSec	Enable

3. Network User和Management覈取方塊確定基於RADIUS的身份驗證是否適用於管理和網路使用者。此示例使用Cisco Secure ACS作為IP地址為10.77.244.196的RADIUS伺服器。按一下Apply。

<u>為無線使用者建立新的WLAN</u>

接下來,您需要建立無線使用者可連線的WLAN。若要建立新的WLAN,請完成以下步驟:

- 1. 在無線LAN控制器GUI中,按一下「WLANs」。此頁面列出控制器上存在的WLAN。
- 2. 選擇New以建立一個新的WLAN。輸入WLAN的WLAN ID、Profile Name和WLAN SSID,然後 點選Apply。對於此設定,請建立WLAN Office。

9 • Q • 🗈 🖻 🛠 🕯	₽\$@ @• \$₽≣;				1919-1919-19			🔡 📲 – 8 ×
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	Sage Co COMMANDS	nfiguration Bing HELP	Lagout Befresh
WLANs	WLANs > New						< Back	Apply
WLANS	WLAN ID	1 1						
AP Groups VLAN	Profile Name	Office						
	WLAN SSID	Office						
							1	

3. 建立新的WLAN後,系統會顯示新WLAN的**WLAN > Edit**頁面。在此頁面中,您可以定義特定 於此WLAN的各種引數,其中包括常規策略、安全、QoS和高級引數。

cisco	Sage Configuration Bing Logout B 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: Enabled Security Policies [WPA2][Auth(802.1x)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface office-vlan BroadCast SSID Enabled
	Foot Notes I 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 excluded clients 5 Client MFP is not active unless WPA2 is configured

檢查General策略下的**WLAN Status**,以啟用WLAN。從下拉選單中選擇適當的介面。在本例 中,使用介面**Office-vlan**。本頁上的其他引數可以根據WLAN網路的要求進行修改。

4. 選擇**Security**頁籤。從Layer 2 security下拉選單中選擇**802.1x**(因為這是LEAP身份驗證)。 在802.1x引數下選擇適當的WEP金鑰大小。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
ANs	WLANs > Edit < Back	Apply
WLANS WLANS AP Groups VLAN	General Security QoS Advanced Layer 2 Layer 3 AAA Servers	
	Layer 2 Security 802.1X S MAC Filtering 802.1X Parameters	
	802.11 Data Encryption Type Key Size	
	I oki notes I ckiP is not supported by I0xx model APs A MARIA Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication A When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to rese S client MPP is not active unless WPA2 is configured	t excluded client

5. 在Security頁籤下,選擇AAA server子頁籤。選擇用於對無線客戶端進行身份驗證的AAA伺服 器。在本示例中,使用ACS伺服器10.77.244.196對無線客戶端進行身份驗證。

cisco	Sage Configuration Bing Logout Be MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
LANs	WLANs > Edit < Back Apply General Security OoS Advanced
WLANS WLANS AP Groups VLAN	Layer 2 Layer 3 AAA Servers
	Select AAA servers below to override use of default servers on this WLAN Radius Servers LDAP Servers
	Authentication Servers Accounting Servers Server 1 None
	Server 119:10.77.244.196, Port:1812 None Server 3 None S
	Server None None
	3 None None None S
	Local EAP Authentication 🗖 Enabled
	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 excluded clients) 5 Client MPR is not active unless WH22 is confoured
	s unext Him is not active unless in the is computed

6. 選擇Advanced 索引標籤。選中Allow AAA Override以配置通過無線LAN上的AAA的使用者策略覆蓋。

cisco	Sage Configuration Eing Logout MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
VLANS WLANS WLANS AP Groups VLAN	WLANs > Edit < Back
	Foot Notes I CKIP is not supported by I0xx 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 client 5 Client MPP is not active unless WPA2 is configured

如果啟用AAA覆蓋,且客戶端的AAA和Cisco無線LAN控制器無線LAN身份驗證引數發生衝突 ,則客戶端身份驗證由AAA伺服器執行。作為此驗證的一部分,作業系統會將客戶端從預設思 科無線LAN解決方案無線LAN VLAN移動到AAA伺服器返回並在Cisco無線LAN控制器介面配置 中預定義的VLAN中,這僅在針對MAC過濾、802.1X和/或WPA操作進行配置時發生。在所有 情況下,作業系統還使用AAA伺服器提供的QoS、DSCP、802.1p優先順序標籤值和ACL,只 要這些值是在Cisco無線LAN控制器介面配置中預定義的。

7. 根據網路要求選擇其他引數。按一下「Apply」。

<u>定義使用者的ACL</u>

您需要為此設定建立兩個ACL:

- ACL1:為了僅提供對User1對伺服器172.16.1.100的訪問
- ACL2:為了僅提供對User2對伺服器172.16.1.50的訪問

完成以下步驟即可在WLC上設定ACL:

- 在WLC GUI中選擇Security > Access Control Lists。系統將顯示Access Control Lists頁面。此 頁列出在WLC上配置的ACL。此功能也允許您編輯或刪除任何ACL。若要建立新的ACL,請按 一下New。
- 2. 此頁允許您建立新的ACL。輸入ACL的名稱,然後按一下**Apply**。建立ACL後,按一下**Edit**為 ACL建立規則。
- 3. User1只需要能夠訪問伺服器172.16.1.100,並且必須拒絕訪問所有其他裝置。為此,您需要 定義這些規則。有關如何配置無線LAN控制器上ACL的詳細資訊,請參閱<u>無線LAN控制器上的</u> ACL配置示例。

cisco	MONL	ror <u>w</u>	LANS <u>C</u> ONTRO	DLLER	WIRELESS	SECI	URITY M	9NAGEMENT	Saya Co COMMANDS	nfiguration HELP	Eing	ogout Befn
Security	Acce	ss Con	trol Lists > Ec	lit					< 84	ick	Add Nev	Rule
▼ AAA General ▼ RADIUS	Gene	rəl										
	Access List Name User1											
Accounting + TACACS+	Seq	Action	Source IP/Ma	sk	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	
LDAP Local Net Users MAC Filtering	٤	Permit	172.16.0.0 255.255.0.0	1	172.16.1.100 255.255.255.255	1	Any	Any	Any	Any	Inbound	
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.100 255.255.255.25	5	172.16.0.0 255.255.0.0	<i>'</i>	Any	Any	Any	Any	Outbound	۵
Local EAP	L											
Priority Order												
 Access Control Lists Access Control Lists CPU Access Control Lists 												
IPSec Certs												
Wireless Protection Policies												
Web Auth												
CIDS												

4. 同樣,您需要為User2建立ACL,僅允許User2訪問伺服器172.16.1.50。這是User2所需的 ACL。

cisco	MONI	TOR M	(LANS <u>C</u> ONT	ROLLE	R WIRELESS	SE	CURITY M	ANAGEMENT		ifiguration HELP	Eing	Logout Befre		
Security	Acce	ss Con	ntrol Lists >	Edit					< 8 a	ck	Add Net	v Rule		
General	Gene	ral												
 RADIUS Authentication 	Access List Name User2													
Accounting + TACACS+	Seq	Action	Source IP/	Mask	Destination IP/Mask		Protocol	Source Port	Port	DSCP	Direction			
Local Net Users MAC Filtering	4	Permit	172.16.0.0 255.255.0.0	/	172.16.1.50 255.255.255.25	/ ۶	Any	Any	Any	Anγ	Inbound	0		
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.50 255.255.255	255	172.16.0.0 255.255.0.0	1	Any	Any	Απγ	Any	Outbound	۵		
Local EAP														
Priority Order	L													
 Access Control Lists Access Control Lists CPU Access Control Lists 														
IPSec Certs														
Wireless Protection Policies														
▶ Web Auth														
▶ CIDS														

現在您已為此設定配置無線LAN控制器。下一步是將Cisco安全存取控制伺服器設定為驗證無線使用者端,並在成功驗證後將ACL Name屬性傳回WLC。

配置Cisco Secure ACS伺服器

:

要使Cisco Secure ACS能夠對無線客戶端進行身份驗證,您需要完成以下步驟:

- 將無線區域網控制器配置為Cisco Secure ACS上的AAA客戶端。
- 在Cisco Secure ACS上配置使用者和使用者配置檔案。

將無線區域網控制器配置為Cisco Secure ACS上的AAA客戶端

若要將無線LAN控制器設定為Cisco Secure ACS上的AAA使用者端,請完成以下步驟:

 按一下Network Configuration > Add AAA client。系統將顯示Add AAA client頁面。在此頁面 中,定義WLC系統名稱、管理介面IP位址、共用金鑰和使用Radius Airespace進行驗證。以下 是範例

Cisco Systems	Network Configuration	×
adhaadha	Edit	Help
User Setup Setup Shared Profile Components Network Configuration Signation Configuration	Add AAA Client AAA Client Hostname wtc AAA Client IP Address 10.77.244.210 Shared Secret cisco	AAA Client Hestname AAA Client IP Address Shared Secret Sistered Secret Sistered Secret Authenticate Using Authenticate Using Single Secret TAEACS + AAA Client Log Sadate/Watchdeg Packets from this AAA Client Log RADIUS Tomeling Packets from this AAA Client Replace RADIUS Part info with Username from this AAA Client Machine TaP. Address with user IP
Administration Centrel Databases Postare Validation Validation Profiles	RADIUS Key Wrap Key Encryption Key Message Authenticator Code Key Key Input Format C ASCII @ Hexadecimal	AAA Client Hestname The AAA Client Hostname The AAA Client Hostname is the name assigned to the AAA client.
Activity	Authenticate Using RADIUS (Cisco Airespace)	Rack to Teal
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 Username 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.
	Submit Submit + Apply Cancel	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

注意:在Cisco Secure ACS上配置的共用金鑰必須與WLC上在**RADIUS Authentication** Servers > New下配置的共用金鑰匹配。

2. 按一下「Submit+Apply」。

在Cisco Secure ACS上配置使用者和使用者配置檔案

要在Cisco Secure ACS上配置使用者,請完成以下步驟:

1. 從ACS GUI中選擇**User Setup**,輸入使用者名稱,然後按一下**Add/Edit**。在本示例中,使用者 為**User1**。

Cisco Systems	User Setup	×
ad brad bra	Select	Help
User Setop Setop Setop Setop Setop Setop Setop Setop Configuration Confi	User: User1 Find Add/Edit List users beginning with letter/number: ABGBALGABALASE DESTINATION List all users Remove Dynamic Users	 9. See Selve and External Back Database 9. Printing a Search (Cuterrin the ACS Internal Database) 9. Adding a User a back ACS Internal Database 9. Initian All Usermannes in the ACS Internal Database 9. Adding a Usermannes in the ACS Internal Database 9. Database (Database Database) 9. Database (Database) 9. D

2. 顯示「**使用者設定**」頁時,定義特定於使用者的所有引數。在本示例中,由於僅需要這些引數 進行EAP身份驗證,因此配置了username、password、Supplementary User Information和 RADIUS屬性。

	(a) ≠ ≈ € ⊘• ↓ ⊡	📲 = 8 ×
Cisco Systems	User Setup	×
adhaadhaa	Edit	🚔 Help
User Setup	User: UserA (New User)	Account Disabled Balatra a Stername Sundamentary lines late
Shared Profile Components	Account Disabled	Descrived Authentication Group to which the user is assigned Cillarde
Network Configuration	Supplementary User Info	Cleant IP Advass Assignment Advasced Settings
System Configuration	Real Name User 1 Description	histowerk Access Restrictions than Sessions Wrage Questas Accessent Disable Downleadable ACLs Advanced TACACS - Settings Topologie Actions
Control Control Cutornal User Databases Pestere Validation Network Access Prefiles	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not Checked.)	IACACS - Instee Castor TACACS - Duble Dassreed TACACS - Duble and Passreed TACACS - Duble and Passreed TACACS - Shell Command Authorization Command Authorization for Network Device Management Applications TACACS - Unknown Services IETT RADIUS Attributes BADDUS Yeador-Specific Attributes
Reports and Activity Documentation	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP pauthentication. This is especially useful when token caching is enabled.	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [Rack to Tap] 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 asked to confirm your action, click DK.
	Group to which the user is assigned: Submit Cancel	[Back to Top] • Supplementary User Info Type the applicable information in any supplemental user information between that appear. To add or chance fields, click Interface

向下滾動,直到看到特定於使用者的Cisco Airespace RADIUS屬性。檢查**Aire-ACL-Name**,以使ACS能夠將ACL名稱與成功的身份驗證響應一起返回到WLC。對於User1,在 WLC上建立ACL User1。輸入ACL名稱作為User1。

	0·0·2	4) A 🗄 🔗 (S+ % 🖪	🧗 - 8 ×
	Cinco Systems	User Setup	×
	dbdb	Date exceeds:	Heln
	User	Sep 9 2007	
	Eng secup	Failed attempts exceed:	Account Disabled Deleting a Bername
	Setup	5	Supplementary User Info Password Authentication
	Shared Profile Components	Failed attempts since last successful login: 0	Group to which the user is assigned Callback
	Network Configuration	Reset current failed attempts count consultant	Client IP Address Assignment Advanced Settings
	2 Sustem	on submit	Notwark Access Restrictions Han Sessions
	Linterface		Usage Quotas Account Disable
	Configuration		Downlaadable ACLs Advanced TACACS - Settings
	Administration Centrol	Cisco Airespace RADIUS Attributes	TACACS + Enable Control TACACS + Enable Parsword
	Deternal User	[14179:002] Aize-QcS-Level	TACACS + Outbound Passwood TACACS + Shell Command Authorization
	Pestare	Bronze	Command Authorization for Network Device Management Applications TACALS + Unknown Services
	BeiNebrock Screece	[14179:003] Aire-DSCP	IETE RADIUS Attributes RADIUS Yendar: Specific Attributes
	Ca Profilez		
	Reports and Activity	L [] [] 4179/004] Aire-802.1P-Tag	
	Documentation	0 [14179005] Aire-Interface-Name	Account Disabled Status Select the Account Disabled chark has to disable this account clear
			the check box to enable the account.
		M [14179006] Aze-Acl-Nane	[Back to Tan]
		User1	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 Delete. When asked to confirm your action, click OK.
		😨 Back to Melp	[Back to Tap]
			Supplementary User Info
		Submit Cancel	Type the applicable information in any supplemental user information houses that appear. To add or change fields, click Interface
		-	
3.	重複相同步	- 驟以建立User2,如下所示。	
3.	重複相同步 ♀・○ ・● ■	驟以建立User2,如下所示。	🦉 - 8 ×
3.	重複相同步 G····································	驟以建立User2,如下所示。 [◆] ● 	<i>∎</i> - 3 ×
3.	重複相同步 〇・〇・〇 3 Ciste Status	- 驟以建立User2,如下所示。 [◆]	Help
3.	重複相同步 G····································	驟以建立User2,如下所示。 ● ● ● ● ● ● ● ● User Setup	Help
3.	重複相同步 G····································	驟以建立User2,如下所示。 User Setup	Help
3.	重複相同步 G····································	驟以建立User2,如下所示。 User Setup User: User: Find Add/Edit	Help
3.	重複相同步 Cisco Systems Cisco Systems	驟以建立User2,如下所示。 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	HEIP
3.	重複相同步 ③····································	驟以建立User2,如下所示。 User Setup Select User: User: User: Find Add/Edit List users beginning with letter/number:	HEP • User Setup and External User Databases • Endine a Specific User in the ACS Internal Database • Adding a User to the ACS Internal Database • Litting Usernames that Degin with a Particular Character • Litting Usernames in the ACS Internal Database • Changing a Username in the ACS Internal Database • Changing a Username in the ACS Internal Database • Changing a Username in the ACS Internal User Database
3.	重複相同步 Cisco Systems Cisco Systems Setup Setup Setup Setup Setup Setup Setup Setup Setup Setup Setup Setup Setup Setup Setup Setup	驟以建立User2,如下所示。 User Setup User: User: Use	Help
3.	重複相同步 Cisce States Cisce States Cisce States Cisce States Sature Composed Comp	驟以建立User2,如下所示。 User Setup Select User: User: User2 Find Add/Edit List users beginning with letter/number: ▲BGPBEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE	HEP • User Setup and External User Datakases • Ending a Specific User in the ACS Internal Catabase • Adding a User to the ACS Internal Database • Adding a User to the ACS Internal Database • Ending of User and in the ACS Internal Database • Listing User anows that Beering With a Database • Listing All Beenames in the ACS Internal Database • Ensure Evenance Users • Ensure Evenance Users • User Setup anables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases • Before ACS can aethenticate users with an external user database • You must have the database up and running on the enternal server. For
3.	重複相同步 Cisco Systems Cisco Systems Cisco Systems Composed Profile Composed Profile Composed State Composed State Comp	驟以建立User2,如下所示。 User Setup User: User: User2 Find Add/Edit List users beginning with letter/number: ▲ ■ C ■ L Z = L Z =	Help Visce Schup and External User Databases Help Visce Schup and External User Databases Hoding a Specific User in the ACS Internal Database Adding a User to the ACS Internal Database Listing All Remainers that Brein with a Particular Character Listing All Remainers in the ACS Internal Database Leanging a Username in the ACS Internal Database Remainer Database User Schup and External User Databases Refere ACS Can authenticate users with an external User Databases Refere ACS Can authenticate users with an external User Databases Refere ACS Can authenticate users with an external user databases Nou must have the database up and running an the external server. For example, if you are using texing and quedentication, your token server must be running and properly configured.
3.	重複相同步 Cisco States Cisco States Cisco States Cisco States Cisco States Cisco States Cisco States Components Components Components Components Components Components Components Components Components Components Components Components Components Components Components Components	驟以建立User2,如下所示。 User Setup User Setup User: User:	 Hep Vier Schop and External User Databases Ending a Specific User in the ACS Internal Catabase Adding a User to the ACS Internal Database Adding a User to the ACS Internal Database Enting Usernances that Decin with a Particular Character Enting All Beenases in the ACS Internal Database Changing a Usernance in the ACS Internal Database Changing a Usernance in the ACS Internal User Database Between Dynamic Users Der Serug enables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases Before ACS can activaticate users with an external user database Stormust have the database up and running an the external User For usering and properly configured. You must have configured the applicable parameters in the External User Databases section.
3.	重複相同步 Cisce States Cisce States Cisce States Cisce States Cisce States Cisce States Composed Com	驟以建立User2,如下所示。 User Setup Select 「User: User: User2 Find Add/Edit List users beginning with letter/number: ▲BSP # # S # # # # # # # # # # # # # # # #	 Hep Her Setup and External User Databases Endited a Specific User in the ACS Internal Database Adding a User to the ACS Internal Database Entited Usernames that Begin with a Partwoke Cheracter Exting Usernames in the ACS Internal Database Exting Usernames in the ACS Internal User Database Barson Dramic Ibers Barson Dramic Ibers Barson ACS can artheoticate users with an external user database You must have the database up and running on the external Server. For asangle, if you are using token card authentication, your taken server must be preving token card authentication, your taken server must be preving token card authentication, your taken server must be bases section. Note: User Setup configuration overrides Group Setup configuration.
3.	重複相同步 ②・○・○・○ Cisce Systems Cisce Systems ③ User User Setup ③ Stared Profile ③ Shared Profile ④ Shared Profile ⑤ Shared Profile ⑤ Shared Profile ⑤ Shared Profile ⑤ Shared Profile Ø Shared Profi	驟以建立User2,如下所示。 User Setup Select 「User: User: User: 「Find Add/Edit List users beginning with letter/number: ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Even set of the s
3.	重複相同步 ③・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	驟以建立User2,如下所示。 User Setup Select 「User: User: User2 「Find Add/Edit List users beginning with letter/number: ▲BGP&EGP&EGP&EGP Users List all users Remove Dynamic Users	Ever Setup and External User Databases Ever Setup and External Database Ever Setup analysis of the ACS Internal Databases Ever Setup analysis of the analysis of the Ever ACS Databases Ever Setup analysis of the analysis of the Setup and Ever Databases Ever Setup analysis of the applicable parameters in the External User Databases section. Note: User Setup configuration overnides Group Setup configuration Ever Setup of the Unknown User Policy in the Ever anal User Databases section to create antice in the ACS internal database for users defined in an asternal user database, usersamas cannot he located ar listed here until the asternal user Setup in the ACS internal database for users defined in an asternal user database, usersamas cannot he located ar listed here until the
3.	重複相同步 ②・・・・・ Cisce System Cisce System Setup ③ StaredProfile ③ SharedProfile ③ Sh	驟以建立User2,如下所示。 We of Setup Select 「User: User: User: Find Add/Edit User: User: Find Add/Edit User: User: User: Find Add/Edit Not Dynamic User: Find User: Find User: User: Find Add/Edit Not Dynamic User: Find User: Find User: Find Add/Edit Not Dynamic User: Find User: Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Statistics Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Add/Edit Find Statistics Find Find Find Find Find Find Find Find Find Find Find Fi	Every Setup and External User Databases Every Setup and External Database Every Setup and Externation of the ACS Internal Database Every Setup and Externation of the ACS Internal Database Every Setup and Externation of the ACS Internal Database Every Setup and Externation of the ACS Internal Database Every Setup and Externation of the ACS Internal Database Every Setup and Externation of the ACS Internal Database Every Every Setup and Externation of the ACS Internal Database Every Every Setup and Externations Every Every Setup and Externations, add users, and delete users in the ACS Internal Database Every Every Every Setup and External User Databases Every Every every the adatabase, User Setup and External User Databases Every Every every the database up and running an the external User Databases You must have the database up and running an the external User Databases You must have the database up and running an the external User Databases You must have the database up and running an the external User Databases You must have the database up and running an the external User Databases You must have configured the applicable parameters in the External User Databases section. Note: User Setup configuration overrides Group Setup configuration. Hypu rely on the Unknown User Policy in the External User Databases section atabase, User Policy in the External User Databases section atabase, users have the database of a later database until the user has successfully arthenticated once. External user database are obtained on the external User
3.	重複相同步 Cisce Status Cisce Status Cisce Status Cisce Status Cisce Status Cisce Status Cisce Status Cisce Status Composed Compo	驟以建立User2,如下所示。 Wer Setup SECT User Setup User: User: User: Find Add/Edit List users beginning with letter/number: NOPOBSIIVYXXII QIIIISS SIZER List all users Remove Dynamic Users	Ever Settys and External User Databases Ending a Specific User in the ACS Internal Catabase Ending a User Factor and the ACS Internal Catabase Adding a User To the ACS Internal Database Exting User memory that Receive Internal User Database Exting User Setup anables up and running and the enternal User Readown Sou must have the database up and running and the enternal Server. For example, if you are using token and authentication, your token server must be develowed up and properly configured. You must have the database up and running and the enternal User Databases External user deatbases, user and subtentication, your token server must be deatbases up and running and properly configured. You must have the databases up and running and the enternal User Databases External user deatbases, user and subtentication, your token server must be deatbases section. Note: User Setup configuration overrides Group Setup configuration over databases in the ACS Internal distabase for user defined in an external user databases, usernames cannot be located ar listed here until due user has successfully authenticated once. Databases sections fuely anthenticated once. Databases itself. For added security, subtorization, and accounting proposely configured once. Databases itself. For added security, subtorization, and accounting proposely user field as security, subtorization, and accounting proposely user field as security, subtorization, and accounting proposely. User Setup is there weet added security, subtorization and is the external due dat
3.	重複相同步 Cisce System Cisce System Cisce System Cisce System Composed	驟以建立User2,如下所示。 User Setup Setert 「User: User: User2 Find Add/Edit List users beginning with letter/number: ABSE # # 9 # # 3 # 4 # # NOFOR # T # V # X #	Image:
3.	重複相同步 Cisco Status Cisco	驟以建立User2,如下所示。 User Setup Stert 「Ind Add/Edit List users beginning with letter/number: NOPORSTITUTITI OIIII SETITUTITI OIIII SETITUTITI OIIII SETITUTITI OIIII SETITUTITI OIIII SETITUTITI OIIII SETITUTITI OIIII SETITUTITI	
3.	重複相同步 Cisce States Cisce States Cisce States Cisce States Composition Compo	驟以建立User2,如下所示。 User Setup Setert 「User: User: User: Find Add/Edit List users beginning with letter/number: ABCERTING Add/Edit User Set I S A I J X L N NO POR ITIVY X Y I SIZI I S C Z S C C C S C C C S C C S C C S C C C S C C C	
3.	重複相同步 ③ · · · · · · · · · · · · · · · · · · ·	驟以建立User2,如下所示。 User Setup Steet 「User: User: User2 Find Add/Edit User users beginning with letter/number: ABSE AISSI Add/Edit Ust users beginning with letter/number: ABSE AISSI Add/Edit User Set ISSI Add/Edit NOFOR SITUATION OII21155728 List all users Remove Dynamic Users	
3.	重複相同步 ③ ● ■ ■ ■ Cisce Status Cisce Status ● Setup ● Setup ● Setup ● Composed Composed ● Composed ● Co	驟以建立User2,如下所示。 User Setup Stert 「User: User: User? 「Find Add/Edit Uset users beginning with letter/number: ABGE & F & M & Z & K & M N & P & D & B & T & V & X & Y & J Uset all users Remove Dynamic Users	 Person and External Decription in the ACS Internal Database. Person and External Decription in the ACS Internal Database. Person Decription Decription Decription in the Internal Database. Person Decription Decription Decription Decription Decription Database. Person Decription Decriptio
3.	重複相同步 Cisce System Cisce System Cisce System Setup Composed Compose	驟以建立User2,如下所示。 User Setup Seter 「「User: User: User2 「Find Add/Edit 」 List users beginning with letter/number: ABSE IIS SIIS SIIS SIIS DIZIIS SIIS DIZIIS SIIS List all users Remove Dynamic Users	<text><image/><section-header></section-header></text>
3.	重複相同步 Cisce Status Cisce	驟以建立User2,如下所示。 User Setup Stect User: User: Find Add/Edit Ust users beginning with letter/number: M 2 2 0 M 2 1 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1	<image/> <image/> <image/> <image/> <section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header>
3.	重複相同步 Cisce States Cisce States Cisce States Cisce States Composed C	驟以建立User2,如下所示。 User Setup Stect User users beginning with letter/number: M 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Alignment of the Addition o

V V U U	COLOR OF COLOR OF COLOR			_
Cisco Systems	User Setup			×
adhaadha	Edit	-	Help	•
User Setup	Licon Licont (New Licon)		Arrout Disabled	
Graup Satur	User: UserA (New User)		Delating a Biername Succession Bier Info	
(R) Shared Profile	Account Disabled		Password Authentication Group to which the user is assigned	
12 Components	Sumlamentary User Info		Calback Circot IP Address Assignment	
Configuration	aupplementary oser mito	1218	Advanced Settings Network Access Restrictions	
Configuration	Real Name User2		Hax Sessions Usage Quatas	
Configuration	Description		Account Disable Downleadable ACLs	
Administration			Advanced TACACS - Settings TACACS - Enable Control	
10 External User	User Setup		TACACS + Enable Password TACACS + Outbound Password	
(PLI Databases	Password Authentication:		 TACACS + Shell Command Authorization Command Authorization for Network Device Management Applications 	
Validation	ACS Internal Database		TACACS + Unknown Services IETF RADIUS Attributes	
Profilez	CiscoSecure PAP (Also used for CHAP/MS- CHAP/MDAP of the Separate field is not (herhed.)		 RADIUS Yesdor-Specific Attributes 	
Reports and Activity	Password •••••			-
and 1 Ordine	Confirm		Account Disabled Status	
Documentation	Separate (CHAP/MS-CHAP/ARAP)		Select the Account Disabled check box to disable this account) clear the check box to enable the account.	
	Password		[Back to Tap]	
	Confirm		Deleting a Username	
	When a token server is used for authentication,		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	
	card user allows CHAP authentication. This is		current user account from the database, click Delete . When asked to confirm your action, click GK .	
	especially useful when taken caching is enabled.		Back to Top	
	Group to which the user is assigned:	-	Supplementary User Info	
	Submit Cancel		Type the applicable information in any supplemental user information being that appear. To add or change fields, click later face	-
			stores that appear, to and or the store introst, thit is service.	0.00
Q • Q • 🖻 🖻	312 9 0 0· 5 B		17 -	8 ×
Cisco Status	or participe and the second s		1000 -	ð ×
Cisco Sisteras	Ole exceeds:	•	Martin -	e ×
Cisco Systems	User Setup	•	Halp	8×
Cisco Status Cisco Status Cisco Status Cisco Status Cisco Status	User Setup Date exceeds: Failed attempts exceed:	•	Holp AccountDisabled Defeting a Nermanet Sequement Nermanet	8 ×
Cisco Systems Cisco Systems Setup Setup Setup	Control Contro Control Control Control Control Control Control Control Control Co		Holp Account.Disabled Defining a Useranic Suplementary.User.Info Password Authentication Group to which the user is assigned	θ× X
Cisco States Cisco States Setup Setup Setup Setup Setup Setup	User Setup Date exceeds: Failed attempts exceed: Failed attempts since last successful login: 0 Pasted successful		Holp Account Disabled Defeting a Nerrane Support Authoritication Gauss to which the user is assigned Callback Clean UP Address Assignment	e ×
Cisco Sysrems Cisco Sysrems User User Setup Composed Comp	Constrained attempts count on submit		Holp Account Disabled Belating a Bremana Supplementary User Info Password Authentication Gallback Callback Client IP Address Assignment Advanced Settings Netword Access Restrictions	e ×
Cisco Stateus Cisco Stateus Setup Components Components Components Components	Constrained attempts count on submit		Holp Account Disabled Defining a User and Supplementary User Info Description of Automatication Gassared Automatication Gassared Settings Chent IP Address Assignment Advanced Settings Natural Access Restrictions Han Sessions User Questas	ø×
Cisco Srstrus Cisco Srstrus Setup Cisco Srstrus Setup Cisco Srstrus Setup Convertion Configuration Configuration	Constant on submit		Account Disabled Deleting a Username Supplementary User Info Password Authentication Group to which the user is assigned Callent IP Address Assignment Advanced Sections Naturate Access Restrictions Histor Costs Disable Account Disable Account Disable Downloadable ACLs	×××
Configuration	Clice Alermore RADIIIS Amphases		Holp Account Disabled Beleting a Useranie Supplementary User Info Bassword Authentication Gase to which the user is assigned Caliback Clent IP Address Assignment Advanced Settings Distrogent Access Restrictions Hain Sessions Disage Operate Access Restrictions Hain Sessions Disage Operate Access Restrictions Hain Sessions Disage Operate Access Restrictions Access R	s ×
Cisco Statuta Cisco Statuta Cisco Statuta Cisco Statuta Cisco Statuta Cisco Statuta Composents Composents Configuration Configuration Configuration Configuration Configuration Configuration			Account Disabled Deleting a Wormanne Supplementary Wer Lofe Password Authentication Gross to which the user is assigned Clent IP Address Assignment Advanced furthers Pastword Authentication Advanced furthers Pastword Authentication Has Sessions Wright Contact Advanced Sections Pastword Access Electrictions Main Sessions Disable Bowlinable Bowlinable Account Disable TotAccess Factored TACAces - Outhersed	s ×
Configuration Co			Account Disabled Belating a Username Supplementary User Info Belating a Username Supplementary User Info Bessword Authentication Galback Callback Call	e ×
Cisco Stattens Cisco Stattens Setup Composed Composed Composed Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	Clisce Alirespace RADIUS Attributes I [14179003] Aire-DSCP		Account Disabled Account Disabled Deleting a Wermanne Supplementary User Info Password Authentication Gross to which the user is assigned Eathack Chent IP Address Assignment Advanced factors Password Authentication Max Sessions Pringe Destas Pringe Destas Pringe Destas Pringe Destas Pringe Destas Pringe Destas TACACS - Enable Dessued TACACS - Settings	s ×
Cisco Stattana Cisco Stattana Setup User Setup Components Componen	Cisce Airespace RADIUS Antributes [14179/003] Aire-DSCP [14179/003] Aire-DSCP [14179/003] Aire-DSCP		Account Disabled Belating a Usermann Supplementary User Info Belating a Usermann Supplementary User Info Belating a Usermann Supplementary User Info Belating Supplementary User Info Callback Callback Clent IP Address Assignment Advanced Settings Patroack Access Patrictions Har Sessions Using Operate Account Disable Downloadable Atts Advanced Interfections TacActs - Enable Control TacActs - Couble Deserved TacActs - Usebace Deserved TacActs - Usebace Deserved TacActs - Usebace Services TacActs - Stackace Services	s ×
Cisco Statz Ha Cisco Statz Ha Setup Composed S Composed S Configuration	Clisce Alirespace RADIUS Antributes I [14179003] Alire-DSCP [14179004] Alire-802 JP-Tag		 Account Disabled Belefing a Usernane Supplementary User Info Bassword Authoritication Grap to which the user is assigned Callback Chent IP Address Assignment Callback Chent IP Address Assignment Account Disable Chent IP Address Assignment Account Disable Chent IP Address Assignment Account Disable Password Access Restrictions Han Sessions Bringe Qualas Account Disable Recont Disable TacActs - Enable Control TatActs - Enable Control TatActs - Unable Control TatActs - Conbas of Password TatActs - Unable Control TatActs - Unable Activation RADIUS Yendor Specific Attributes 	e ×
Cisco Srstrus Cisco			 Account Disabled Belating a Username Supplementary User Info Bessernary User Info Bessernary User Info Bessernary User Info Callback Cleant IP Address Assignment Advanced Settings Extended Access Flagstrictions Han Sessions Using Questas Account Disable Boundarable Actics Advanced Factors Flagstrictions TACACS - Enable Control TACACS - Underson Anthonication Command Authonication For Network Device Management Applications TACACS - Usebacom Services HTE RADIUS Attributes RADIUS Vendor Specific Attributes 	s ×
Cisco Systems Cisco Systems Setup Cisco Systems Cisco Systems Cisco System Components Configuration Con	Clisce Alirespace RADIUS Antributes (14179003) Alire-DSCP (14179004) Alire-S021P-Tag (14179005) Alire-Listerface-Name		Account Disabled Account Disabled Beleting a Unerrante Supplementary User Info Bassword Authoritation Sono to which the user is assigned Callback Clent IP Address Assignment Account Disabled Const IP Address Assignment Account Disable Private Outlant Private Outlant Private Outlant Account Disable TatActs - Couble Cantod TatActs - Couble Cantacts TatActs - Couble Cantod TatActs - Couble Cantod	e ×
Cisco Srstrus Cisco	Clicce Alrespace RADIUS Antributes		Account Disabled Account Disabled Account Disabled Belating a Bername Supplementary User Info Supplementary User Info Supplementary User Info Supplementary User Info Callback Callback Callback Clent IP Address Assignment Advanced Settings Proved Access Restrictions Har Sessions Using Ountar Advanced Settings Moved adable Attic Advanced IACACS - Settings TACACS - Inable Deasweed TACACS - Underson Authorization TACACS - Underson Authorization TACACS - Underson Authorization TACACS - Usebacem Services ItTT RADBUS Attributes RedBUGS Attributes RedBUGS Attributes RedBUGS Attributes RedBUGS Present Disabled check how to disable this accounty clear the check box to enable the account. Iback to TacA	
Cisco Stratt us Cisco Stratt us Cisco Stratt us Cisco Stratt us Cisco Stratt us Cisco Stratt us Components Components Comfiguration Configuration	Clice Airespace RADIUS Artributes		Account Disabled Account Disabled Belating a Username Supplementary User Info Callback	
Configuration Config	User Setup User Setup Date exceeds: Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit Clicce Alrespace RADIUS Antributes (14179002) Aire-DSCP [14179003] Aire-DSCP [0] [14179004] Aire-S021P-Tag [0] [14179005] Aire-Interface-Name [14179006] Aire-Act.Name [1417006] Aire-Act.Name [1417006] Aire-Act.N		Account Disabled Account Disabled Account Disabled Belating a Bermann Supplementary User Info Password Authentication Callback Clent IP Address Assignment Advanced Settings Provelacidable Attic Advanced Setting Bising Questa Account Disable Account Disable Account Disable TACACS - Enable Control TACACS - Enable Password TACACS - Enable Password TACACS - Underson Authorization Cannesd Authentiation Reserved TACACS - Underson Authorization TACACS - Underson Authorization TACACS - Underson Authorization TACACS - Underson Authorization TACACS - Underson Services TIT RADIUS Attributes Reserved States Select the Account Disabled check hos to disable this account; clear the check hos to enable the account. Incat TacACS	
Configuration Config	User Setup User Setup Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit Cloce Alrespace RADIUS Attributes (141794002) Aire-QoS-Level Bronze (141794003) Aire-DSCP (141794004) Aire-S021P-Tag (14179404) Aire-S04 (14179404) Air		 Account Disabled Belating a Username Supplementary User Info Supplementary User Info Supplementary User Info Supplementary User Info Caliback Cleant IP Address Assignment Advanced Sections Editored Access Enstrictions Advanced Sections Private Optimization Account Disabled Access Enstrictions Advanced Sections Advanced Information Account Disable Access Fractions Advanced Fractions Pressured TACACS - Enable Decompand Advanced Sections Advanced Sections Advanced Access Fractions Advanced Fractions Pressured TACACS - Enable Decompand Authorization Semmand Authorization for Natwork Device Management Applications TACACS - Unbiased Status BADUUS Attributes BADUUS Attributes Bading Section Disabled check bos to disable this account clear to check bos to analysis of the check bos to analysis	
Configuration Config	User Setup Date exceeds: Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit Clice Alrespace RADIUS Attributes (14179003) Aire-DSCP (14179003) Aire-Act-Name (14179003) Aire-Act-Name (14179003) Aire-Act-Name (14179003) Aire-Act-Name (14179003) Aire-Act-Name (14179003) Aire-Act-Name (14179004) Aire-Act-Name (14179005) Aire-Act-Name (14179005) Aire-Act-Name (14179005) Aire-Act-Name (14179005) Aire-Act-Name (14179005) Aire-Act-Name (14179005) Aire-Act-Name (1417905) Aire-Act-Name (1417905) Aire-Act-Name (1417905) Aire-Act-Name (1417905) Aire-Act-Name (1417905) Aire-Act-Name (1417905) Aire-Act-Name (141		Fields Account Disabled Basheed Automatical Section Supplementary Herr Info Herr Info Supplementary Herr Info Supplementary Herr Info Herr Info Supplementary Herr Info Herr Inf	
Cisco Srstrus Cisco	User Setup User Setup Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit Clicce Airespace RADIUS Antributes (141794002) Aire-QoS-Level Bronze (141794002) Aire-DSCP 0 (141794002) Aire-S0221P-Tag 0 (141794002) Aire-S0221P-Tag 0 (141794002) Aire-Act.Name User2		Fight and the state of the s	

4. 按一下System Configuration和Global Authentication Setup以確保身份驗證伺服器配置為執行

所需的EAP身份驗證方法。在EAP配置設定下,選擇適當的EAP方法。此示例使用LEAP身份 驗證。完成後按一下Submit。

😋 • 🗇 • 🖻 🖻 🚳 🗇 A 9 5



驗證

使用本節內容,確認您的組態是否正常運作。

嘗試將無線客戶端與採用LEAP身份驗證的輕量AP相關聯,以驗證配置是否按預期工作。

注意:本文檔假定客戶端配置檔案已配置為LEAP身份驗證。有關如何為LEAP身份驗證配置802.11 a/b/g無線客戶端介面卡的詳細資訊,請參閱使用EAP身份驗證。

啟用無線客戶端的配置檔案後,將要求使用者提供用於LEAP身份驗證的使用者名稱/密碼。這是使 用者1嘗試向LAP進行身份驗證時會發生的情況。

Enter Wireless No	etwork 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

輕量AP和WLC將使用者認證傳遞到外部RADIUS伺服器(Cisco Secure ACS)以驗證認證。 RADIUS伺服器會將資料與使用者資料庫進行比較,並在成功驗證後,將針對使用者設定的ACL名 稱傳回WLC。在這種情況下,ACL User1會傳回WLC。

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

無線LAN控制器將此ACL套用到User1。此ping輸出顯示User1隻能存取伺服器172.16.1.100,不能存取任何其他裝置。

```
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),
```

同樣地,當User2嘗試存取WLAN時,RADIUS伺服器會在成功驗證後將ACL User2傳回WLC。

Enter Wireless No	etwork 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

Authentication Status	? _ =
Card Name: Cisco Aironet 802.1	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

無線LAN控制器將此ACL套用到User2。此ping輸出顯示User2僅能存取伺服器172.16.1.50,不能存 取任何其他裝置。

```
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),
```

<u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

在無線LAN控制器上,您還可以使用這些debug命令來排除AAA身份驗證的故障

debug aaa all enable — 配置所有AAA消息的調試

debug dot1x packet enable — 啟用所有dot1x資料包的調試

• debug client <MAC Address> — 啟用無線客戶端調試

以下是debug aaa all enable指令的範例

註:由於空間限制,輸出中的某些行已移至第二行。

Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
 Thu Aug 16 14:42:54 2007:
 Callback.....0x85ed228
 Thu Aug 16 14:42:54 2007: protocolType.....0x00140001 proxyState.....00:40:96:AF:3E:93-03:01 Thu Aug 16 14:42:54 2007: 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 2duser1..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 1awlc. Thu Aug 16 14:42:54 2007: 0000060: 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: 00000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 27 02 ...A....0.200'. 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 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[^]..../[^].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 3dSVC= 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 Thu Aug 16 14:42:54 2007: resultCode.....255 protocolUsed.....0x0000001 Thu Aug 16 14:42:54 2007: proxyState.... Thu Aug 16 14:42:54 2007: 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

protocolType.....0x00140001 Thu Aug 16 14:42:54 2007: 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 02 618....[..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 1awlc. 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 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 75e.(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 ..k.....9...< 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 79auth-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

structureSize.....236

Thu Aug 16 14:42:54 2007:

resultCode.....0 Thu Aug 16 14:42:54 2007: 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 qosLevel: -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

您可以使用**show wlan summary**指令的組合來識別哪個WLAN使用RADIUS伺服器驗證。然後您可 以檢視**show client summary**命令,以瞭解哪些MAC位址(使用者端)在RADIUS WLAN上成功通過 驗證。您還可以將此項與Cisco Secure ACS已通過的嘗試或失敗的嘗試日誌關聯。

思科建議您使用無線客戶端測試ACL配置,以確保已正確配置ACL。如果無法正常工作,請驗證 ACL網頁上的ACL,並驗證您的ACL更改是否已應用到控制器的介面。

您還可以使用以下show命令來驗證您的設定:

• show acl summary — 若要顯示控制器上配置的ACL,請使用show acl summary命令。 以下是範例:

(Cisco Controller) >show acl summary

• show acl detailed <ACL_Name> — 顯示有關已配置ACL的詳細資訊。以下是範例:註:由於 空間限制,輸出中的某些行已移至第二行。

Cisco Controller) >show acl detailed User1

	Prot	Range	Range	DSCP	Action	
I	Dir	IP Add	ress/Netmas	c	IP	Address/Netmask
	Source	Port De	st Port			
	Source			Destination		

1 In 172.16.0.0/255.255.0.0 172.16.1.100/255.255.255.255 In 172.16.0.0/255.255.0.0 172. 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 Destination Source Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action __ ___ ____ ____ ____ 1 In 172.16.0.0/255.255.0.0 172.16.1.50/255.255.255.255 Any 0-65535 0-65535 Any Permit 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> — 顯示有關無線客戶端的詳細資訊。

疑難排解提示

使用以下提示進行疑難排解:

- 在控制器上驗證RADIUS伺服器是否處於活動狀態,而不是待機或禁用。
- 在控制器上,檢查是否從WLAN(SSID)下拉選單選擇RADIUS伺服器。
- 檢查RADIUS伺服器是否收到並驗證來自無線使用者端的驗證要求。
- · 檢查ACS伺服器上的Passed Authentications and Failed Attempts報告以完成此操作。這些報告 可在ACS伺服器的「報告和活動」下找到。

相關資訊

- <u>無線LAN控制器上的ACL:規則、限制和示例</u>
- <u>無線LAN控制器上的ACL組態範例</u>
- 使用無線LAN控制器(WLC)的MAC過濾器組態範例
- 思科無線LAN控制器組態設定指南5.2版
- 技術支援與文件 Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。