適用於每個WLAN的ACS 5.2和WLC驗證組態範 例

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>設定</u> <u>設定WLC</u> <u>配置Cisco Secure ACS</u> <u>驗證</u> 疑難排解

簡介

本文提供根據服務組識別碼(SSID)限制每個使用者存取無線LAN(WLAN)的組態範例。

必要條件

需求

思科建議您瞭解以下主題:

- •如何設定無線LAN控制器(WLC)和輕量型存取點(LAP)以達成基本操作
- 如何設定思科安全存取控制伺服器(ACS)
- •輕量型存取點通訊協定(LWAPP)和無線安全方法

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco 5500系列WLC(執行韌體版本7.4.110)
- 思科1142系列LAP
- Cisco安全ACS伺服器版本5.2.0.26.11

設定

要為此設定配置裝置,您需要:

- 1. 為兩個WLAN和RADIUS伺服器配置WLC。
- 2. 配置Cisco Secure ACS。
- 3. 配置無線客戶端並驗證配置。

設定WLC

完成以下步驟,以便為此設定設定WLC:

 設定WLC以將使用者認證轉送到外部RADIUS伺服器。外部RADIUS伺服器(此案例為思科安全ACS)然後驗證使用者認證並提供對無線使用者端的存取許可權。請完成以下步驟:從控制器GUI中選擇Security > RADIUS Authentication,以顯示「RADIUS Authentication Servers」頁面。

		Taxa Configuration 1 Time 1	annet Defrech
cisco	MONITOR WLANG CONTROLLER AGRELESS SECURITY NAVADEMENT CONTRANCS HELE ESERBACK		
Security	RADIUS Authentication Servers	Apply	New
AM General General General Gubentication Gounting nalbuck Tracforts Tracforts Invar Loosi Net Bours MCC Differing Disabled Climb Invertige Raineet AP roblets Berevoort Robuse	Cali Station 10 Type I II foldmas III Law Atts two What III (Congred for FIPS automore and requires a key area conclust RADILS server) Hit Delimiter III (Sphen III) Network User Planagement Server Index Server Address Port (Pher Admin Status A Cali Station 12 Type of the applicable care for one 2004 in summitted to page		
Encal ENP			
Priority Order			
Certificate			
Access Control Lists			
Wireless Protection Policies			
Web Auth			
TrestSec SXP			
Advanced			

按一下「New」以定義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。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10.104.208.56的 RADIUS伺服器。

11 111 11								
CISCO	MONITOR MUANE CONTRO	ULER AURELESS SECUR	TY MANAGEMENT	OOMMANDS	ΗEJE	ESEDBACK		
ecurity	RADIUS Authentication S	ervers > New						
888	Server Index (Priority)	1 .					1	
RADUS	Server 37 Address	10104.20555						
Authentication	Shared Secret Format	65C3 m						
Fallback	Shared Secret	*******						
LDIAP	Confirm Shared Secret	*******						
Local Net Barra MAC Differing Disabled Clients	Kuy Wrap	Catgree for FIR and		key arep count	A-PROD	ES (enver)		
liter Logo Rolisses	Pert Banker	1:12						
Parenant Policiae	Server Status	Tashiari 📼						
Local EAP	Support for INC 3576	backed as						
Priority Order	Server Timeo It	2 seconds						
Certificate	Notwork User	2 Chatle						
Access Control Lists	Vanagamart	🖾 6 nable						
Wireless Protection Policies	IPSec	📰 insbie						
Web Auth								
TrestSec SXP							-	
Advanced								

按一下「Apply」。

2. 完成這些步驟,為使用SSID Employee的員工配置一個WLAN,為使用SSID Contractor的承包 商配置另一個WLAN。在控制器GUI上按一下「WLANs」以建立WLAN。出現WLANs視窗。 此視窗列出控制器上設定的WLAN。按一下New以設定新的WLAN。此範例建立名為 Employee的WLAN,且WLAN ID為1。按一下Apply。

cisco	MONITOR MLANE	CONTROLLER WRELESS	SECURTY	NS/AGENE/T	CONVANCE	H€,β	EEEBACK	Sage Configuration ging	Leger	t Befrech
WLANs	WLANs > New							< Back		Apply
 WILANS WILDIS Advanced 	Type Profile Name SSID ID	et.AA								

選擇WLAN > Edit視窗並定義特定於WLAN的引數: 在Layer 2 Security頁籤中選擇802.1x。預 設情況下,第2層安全選項為802.1x。這將為WLAN啟用802.1 x/可擴展身份驗證協定(EAP)身 份驗證。

cisco	Novitor Minane Controlter Miseless Secteal Management offenance here seedence	Sage Configuration Eng. Lagood Befreek
WLANs	WLANs > Edit 'Employee'	< Back Apply
* WLANS	General Security QoS Advanced	
> Advanced	Lever 2 Loper 3 AAA Servers	
	Leger 2 Security & With the Ag	Î
	Paul Transition Paul Transition Post Transition Protoc.ted Humagement Prance	
	IPP Usedud +	z
	WPA holicy	
	WHAT Energyton Milets Entropy Anthentication Key Nanagement	
	BO2 1.H M Teacher CCKM Escobe	
	TON LETERADO	
	Food Notes 2 Web Julies council to specify develop with Proce	

在AAA servers頁籤中,從RADIUS Servers下的下拉選單中選擇適當的RADIUS伺服器。其它 引數可以根據WLAN網路的要求進行修改。按一下「**Apply**」。

	WEARS > East Employee		< Deck Apply
LANs LANs	General Security QaS	#dvanced	
vanced	Layer 2 Layer 3 AAA S	ITER T	
	Select ALL carpars being to our	mide use at default services on this RUAS	ŕ.
	Redex Research		
	Names Strvers	Sauth here	ī l
		Authentication Survers Accounting Survers Sarver 2 tors	-
		Mitselan Victoria Survey aver	
	Over 1	12 10.04210.16.16 8 2 m 316 m	
	Server 2	tore a R.n. a	
	Second 2	tors z z z	
	Samar 5	tota	
	Server 6	tore a Tet a	
	Radius Server Accounting	(11.5) III (111.2)	
	Interim Update		
	Local EAP Authentication		
	*1	1	

同樣地,若要為承建商建立WLAN,請重複步驟b至d。

配置Cisco Secure ACS

在Cisco Secure ACS伺服器上,您需要:

- 1. 將WLC配置為AAA客戶端。
- 2. 為基於SSID的身份驗證建立使用者資料庫(憑據)。
- 3. 啟用EAP身份驗證。

在Cisco Secure ACS上完成以下步驟:

- 1. 若要將控制器定義為ACS伺服器上的AAA使用者端,請從ACS GUI中選擇**Network Resources** > **Network Devices and AAA Clients**。在Network Devices and AAA Clients下,**單**擊**Create。**
- 2. 顯示「網路組態」頁面時,定義WLC的名稱、IP位址和共用金鑰和驗證方法(RADIUS)。

O O Interfact 2013 42005 5 Securition O O Control 2 G X Class Secure ACS X O Share Browner Webbs •							
cisco Eval(Dags left: 5)	CS				scautnin	acalismplais (Primary)	Log Chil About Help
» ∰ MyWorkspace	Network Resources > Netw	rk Devices and AAA Clients > Create					
Auford Research Automatic Research Automatic Research Automatic Device Groups Location Device Type Source Research Autorises Device Device and Autorises Device Research Research Device Research Research Device Research Research Device Research Research Device Research	Name: DOTA Description: Network Device Geo Location Device Type IP Address Single IP Addr IP: 10.105.98.4	95 41 Locatore 41 Device Types ess	Serect.	Authentikation Options	e Connect Suppor	t Hänget	
	Submit Cancel						

 從ACS GUI中選擇Users and Identity Stores > Identity Groups。為員工和承包商建立相應的 組,然後按一下建立。在此示例中,建立的組名為Employees。

		Berlings Washing - March Barl		include a
(- 10) (- https://20.284.208.58/scratte	nn/ D + O Centife E C X 6 Cisco Secure A	kcs ×		A 🛨 🗆
V Dana Breaner Wahler +				
X Superioral August				
Juliulu, Cisco Secure Ar			aca admin	scalemplate (Primary) Log Out About Help
CISCO EVALIDADA RET ST				
* 😚 MyWorkspace	Users and Identity Stones > Manify Groups > Grade			
+ (5) Network Resources	Convert			
- 📸 Users and Identity Stores	Name: Employees			
Herity Croups	Description			
 Internal Identity Stores 	Burnet .			
Users	 Parent All Groups 	Serect.		
* External Identity Stores	0 = Required fields			
LDAP				
Active Directory				
RADIUS Identity Servers				
Certificate Authorities				
Certificate Authentication Profile				
Kently obre Sequences				
* W Polcyclamans				
* Access Policies				
 [1] Monitoring and Reports 				
System Administration				
	Submit Carcel			

 選擇Users and Identity Stores > Internal Identity Stores。按一下「Create」,然後輸入使用 者名稱。將它們放在正確的組中,定義其密碼,然後按一下提交。在此示例中,建立了 Employee組中名為employee1的使用者。同樣,在組contractors下建立一個名為 contractor1的使用者。



5. 選擇Policy Elements > Network Conditions > End Station Filters。按一下「Create」。



輸入一個有意義的名稱,然後在**IP address**頁籤下輸入WLC的IP地址。在本示例中,名稱是 Employee和Contractor。

X 🚱 Shere Browner WebEs •	···· D + Q Cettle E d X Ø Cisco Securi ACS ×		i i i i i i i i i i i i i i i i i i i
cisco Secure Al cisco EVAL(Days left: 5)	CS	acaadmin acalomplatu (Primary) Lo	DM About Help
» ∯ MyWariapace	Policy Bernetis > Sension Conditions > Network Conditions > End Station Plans > Create		
So Network Resources So Network Resources So Versey Extension Session Conditions Date and Time	General Name: Employee Description: Address IAPC Address CLIONIS		
Custom * Nation: Conditions Conditions Device Port/Filters Partice Port/Filters * Automation and Permissions	Network Devices Filter: End Station P • Match & Contains • Chear Filter: Do * End Station P 10.105.98.4	Showing t-1 of t 30 * per page	00
Autorization Profiles • Device Administration • Named Permission Objects	Create Duplicate Est Delete Exports File Replace from File	Page 1 of 1 H 4 >	H
System Administration			
	Submit Carce		

在CLI/DNIS頁籤下,將CLI保留為 — ANY-,並將DNIS輸入為*<SSID>。在此示例中 ,DNIS欄位輸入為*Employee,因為此終端站過濾器用於限制僅對員工WLAN的訪問。 DNIS屬性定義允許使用者訪問的SSID。WLC將DNIS屬性中的SSID傳送到RADIUS伺服器。 對承包商終端站過濾器重複相同步驟。

A ST P & South Party	the second se	
Caller Stringer/ (20, 28 4.200, 56 / scrael	innin/ D + O Centric E C X Cricco Secure ACS ×	බ ද 6
🗙 🤪 Shara Browser WebEc 💌		
clisco Secure A cisco Eval(Dags wit 5)	ACS	acaadmin acabemphile (Primary) Log Out About Help
 S MyWorkspace 	Policy Benerits > Session Conditions > Network Conditions > End Station Place > Edit "Emp	stryee End Sin Piller"
> (5) Nelwork Resources	General	
Users and identity Stores	Name: Employee End Str. Filter	
 Qu Policy Elements 	Description:	
 Session Conditions Date and Time 	P Address NAC Address CLIDNIS	Costo Secure ACS Webpage Dialog
Custom	Network Devices	🌀 https://20.204.200.56/scienterin/project/terrorenth/ortpjpp. 🔘 Cartificate error
End Station Filters	Filter: CLI + Natch 7: Contains +	Clear Filter (Do.
Device Filters Device Part Filters	PI CLI DNID	
* Autorization and Permissions	JANY- "Employee	ONS: V Employee
 Network Access a thorization Profiles 	Create Duckate Bit Delete Exectin File	Replace from File
 Device Administration 		
 Named Permission Objects 		
* Access Policies		OK Close Hep
 g) Monitoring and Happins a) Reports 		
* 🐟 ayalem Administration		
	Sumit Carrel	
	And	

and the other states where			
🗲 🛞 🥝 https://20.284.208.56/scrade	ni/ "D + O Centric E d X 6 Cisco Securi ACS ×		6 🕁 🗄
🗙 🎱 Shara Browser WebEc 🔹			
CISCO CISCO Secure A	CS	acadmin acabonybila (Prin ary)	Log Out About 148
 MyWorkspace 	Policy Bernetia > Session Conditions > Network Conditions > End Station Plans > Edit "Con	ninacion Brut Sie Miler"	
Soft Network Resources Soft Venns and Identity Stores QuiPologi Elements Session Conditions Data and Trins	General Rame. Contractor End Ste Filter Description: P Address TARC Address CLUDNIS		
Custom Custom * Nativos: Canditiane Gestare Titors Device Potitians Partice Potitians * Autorotazion Profiles Autorotazion Profiles * Device Administration * Named Permission Objects * Named Permission Objects	Network Devices Filter: CLI Match & Contains CLI Dvdb JANA "Contractor Greate Duplicate Edit Delete ExportIoPie	Clean Filter 0 Replace from File	Certificate error
 Monitoring and Reports Bjøten Administration 	Submit Carce	CK Close	

6. 選擇Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles。Permit Access應該有一個預設配置檔案。



7. 選擇Access Policies > Access Services > Service Selection Rules。按一下「Customize」。 新增任何適當的條件。此範例使用Protocol as Radius作為匹配條件。按一下「Create」。命 名規則。選擇Protocol,然後選擇Radius。在Results下,選擇適當的訪問服務。在本例中,保 留為Default Network Access。

		×
遵 https://10.104.208.56/acsadm	in/PolicyInputAction.do	😵 Certificate error
Customize Conditions Available: ACS Host Name Compound Condition Device Filter Device IP Address Device Port Filter End Station Filter NDG:Device Type NDG:Location Time And Date UseCase	Selected: Protocol	
OK Cancel		

Cisco Secure ACS Webpage Dia	alog	
@ https://10.104.208.56/acsadmin/4	PolicyInputAction.do	💈 Certificate error
General		
Name: Rule-4	Status: Enabled 🝷 \Theta	
The Customize butt conditions and resu	on in the lower right area of the polic Its are available here for use in polic	cy rules screen controls which policy cy rules.
Conditions		
Protocol: match	 Radius 	Select
Results		
Service: Default Network Acces	is ▼	
OK Cancel		Help

8. 選擇Access Policies > Access Services > Default Network Access > Identity。選擇單個結果 選擇和**身份源**作為內部使用者。

Concernance Concernan			and the second second second			
X ² Hey Howner White • 11.11. Cisco Secure ACS Cisco Evaluations ² Hey Montragete - Q Havanin Resources ² Single result selection - Q Havanin Resources ² Advanced Optore - Multicing and Repote ² Advanced Optore - Q Havanin Resources ² Bound Repote - Q Havanin Resources ² Bound Repote - Q Havanin Resources ² Advanced Optore - Q Havanin Resources ² Bounin Resources	🗲 🛞 🍊 https://10.184.208.56/scrade	nin/ D + O Cattle., E d X 6 Cisco Secure Ad	cs ×			6 🔶 🖯
Intellit: Clsco Secure ACS Reader Water Reader Read	🗶 🍘 Shara Browner WebEc 🔹					
Image: Strate	cisco Secure Al	CS		acasteria	acatemplate (Primary)	Log Out About Help
	CISCO EVAL(Daps with 5) Solution Solution	Access Robers - Access Service - Default live of Acce Single result selection Rule based result se Identity Boune Internal Users Advanced Options Seve Changes Depart Changes	etection Servet.			

選擇Access Policies > Access Services > Default Network Access > Authorization。單擊 Customize並新增自定義條件。此示例按順序使用身份組、NDG、裝置型別和終端站過濾器。

 Webpage Dialog 		
🙆 https://10.104.208.56/acsadmin	n/PolicyInputAction.do	😵 Certificate error
Customize Conditions Available: ACS Host Name Authentication Method Authentication Status Compound Condition Device Filter Device IP Address Device Port Filter Eap Authentication Method Eap Tunnel Building Method NDG:Location	Selector. Identity Group NDG:Device Type End Station Filter	
OK Cancel		٥

按一下「**Create**」。命名規則並在「所有組」下選擇適當的身份組。在本示例中,它是 Employee。

Closo Secure ACS Webpage Dialog	Cisco Secure ACS Webpage Dialog
🍘 https://10.114/200.14/accuderin:Policylepathetian.do 📀 Carificato area	🍘 https://10.114.200. 🖬 has a drein Network Device Grouph Kryst Action de Prontest Data, a torra Filter Scherity Group – Standbyller 🔮 0
General Name: Rule-2 Datus: Enabled + •	Falar: • Match II • 💿 🐨
The Custerrise butten in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	Name Description
Conditions	Instance
E Identity Droup: In • Belast	NLC NLC
IZ ND0.Devce Type: In	
2 End Blaton Filter: math *	(c) One Server 405 Weitspape Debug
Results	Newson David Groups
You may select multiple substantion profiles. Attibutes defined in multiple profiles will use the value from the first profile defined.	Prov. • Lador d' • Loop of theme • Transition • A Deck Toes • Loop of allow
	CK Center (Linear (Linear () Linear () Linear (Linear ()

按一下「**Employee End Stn Filter**」單選按鈕,或輸入在「Configure the WLC」一節的步驟 1b中輸入的名稱。

8	Cisco	Secure ACS Webpage	Dialog				X
6	https	://10.104.208.56/acsadm	n/NARsLPInput	Action.do?listTy	pe=EndStation		😒 Certificate error
	End Station Filters				Showing 1-2 of 2 50	🝷 per page 🙆	
	Filter:	 Match 	if.	- Go	~		
		Name	Description	1			
	0	Contractor End Stn Filte	r				
	۲	Employee End Stn Filte	r				
	Crea	te Duplicate Ed	Delete			 📧 🖣 Page	1 of 1 🕨 🕅
	ок] с	Cancel					Help

勾選「Permit Access」覈取方塊。

Cisco Secure ACS Webpage Dialog	×
https://10.104.208.56/acsadmin/NetworkAccessLPInputAction.do	Certificate error
Authorization Profiles	Showing 1-2 of 2 50 🔻 per page 🚱
Filter: Match if: Go	
Name Description	
DehyAccess	
Permit Access	
Create Duplicate Edit Delete	Page 1 of 1 🕨 📔
OK Cancel	Help

對「承包商規則」也重複上述相同步驟。確保預設操作為**Deny Access**。 完成步驟e後,規則

應如下所示

In In Cisco Secure ISCO EVAL(Days left 5)	ACS							scadore	aca template	(Prim scy)		*****
G MyWorkspace	Acce	en Policia	a > Acces	n Servitan P C	ielauð Nelwerk Access > Auð	torizalion						
Network Resources	- Sa	dard Po	olicy Enc	eption Policy								
Users and identity attres	- 14	Swork A	Access Ar	uthorization P	olicy							
Busers and identity Stores Policy Elements Access Policie Service Service Dennice Second Rules Obstut Device Amon Kently Autorization Obstut Network Access Kently		Fiter: Status			Match if Equals +	Glear R	ter Ge 🔻					
Access Services 1) Service Selecton Rules	1		Status	Name	identity Group	Conditions NDG/Device Type	End Station Filter	Results Authorization Profiles	HEGOLE			
O Default/Device Admin		•		Contractor	in All Groups:Contractor	in All Device Types:WLC	match Contractor End Stn Filter	Permit Access	7			
idently a desiration	2	8	•	Employee	in All Groups Employee	in All Device Types :WLC	match Employee End Stn Filter	Pernit Access	5			
O Debuit Network Access Identity Unincreated Maintenance Research	ľ								_			
Monitoring and Reports												
aysen Auniniscation	н.											
	н.,											
	ШÆ											
			Defailt		If no rules defined at no e	erabled rule matches.		DenyAccess	9			
		ireate	1. D	uplicate [💌	Edit Delete A N	love to 🗵				Custor	ize Hr	Cou

配置到此結束。在本節之後,需要使用SSID和安全引數相應地配置客戶端以進行連線。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。