在統一無線網路中配置接入點授權

目錄

簡介 必要條件 需求 採用元件 輕量AP授權 設定 使用WLC上的內部授權清單設定 驗證 針對AAA伺服器的AP授權 配置Cisco ISE以授權AP 配置MAB不需要NAS埠型別屬性的新裝置配置檔案 將WLC配置為Cisco ISE上的AAA客戶端 將AP MAC地址新增到思科ISE上的終端資料庫 將AP MAC地址新增到思科ISE上的使用者資料庫(可選) 定義策略集 驗證 疑難排解

簡介

本檔案將說明如何設定WLC,以根據AP的MAC位址授權存取點(AP)。

必要條件

需求

思科建議您瞭解以下主題:

- 有關如何配置思科身份服務引擎(ISE)的基本知識
- Cisco AP和Cisco WLC的配置知識
- •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AireOS 8.8.111.0軟體的WLCWave1 AP:1700/2700/3700和3500(1600/2600/3600仍受支援,但AireOS支援在8.5.x版結束)Wave2 AP:1800/2800/3800/4800、1540和1560 ISE版本 2.3.0.298

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

輕量AP授權

在AP註冊過程中,AP和WLC使用X.509證書相互進行身份驗證。Cisco在工廠將X.509證書燒錄到 AP和WLC上的受保護快閃記憶體中。

在AP上,出廠安裝的證書稱為製造安裝的證書(MIC)。 所有在2005年7月18日之後生產的思科AP都 具有MIC。

除了在註冊過程中發生的這種相互身份驗證外,WLC還可以根據AP的MAC地址限制向其註冊的 AP。

使用AP MAC位址時缺少強式密碼不會造成問題,因為控制器在透過RADIUS伺服器授權AP之前 ,會使用MIC來驗證AP。MIC的使用提供了強大的身份驗證。

AP授權可通過兩種方式執行:

- 使用WLC上的內部授權清單
- 在AAA伺服器上使用MAC地址資料庫

AP的行為因使用的證書而異:

- 具有SSC的AP WLC僅使用內部授權清單,不會將請求轉發到這些AP的RADIUS伺服器
- 使用MIC的AP WLC可以使用WLC上配置的內部授權清單,或使用RADIUS伺服器來授權AP

本文討論使用內部授權清單和AAA伺服器進行AP授權。

設定

使用WLC上的內部授權清單設定

在WLC上,使用AP授權清單根據其MAC地址限制AP。AP授權清單位於 Security > AP Policies 在WLC GUI中。

此示例說明如何新增具有MAC地址的AP 4c:77:6d:9e:61:62.

- 1. 在WLC控制器GUI上,按一下 Security > AP Policies 並顯示AP策略頁面。
- 2. 按一下 Add 螢幕右側的按鈕。

alialia								Save Configuration	Ping	Logout <u>R</u> efre	sh
cisco	MONITOR WLA	Ns <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		no <u>H</u> n	e
Security	AP Policies								Apply	Add	ה
▼ AAA General ▼ RADIUS	Policy Configura	ation						-			
Authentication Accounting Auth Cached Users	Accept Self Sign	ed Certificate (SSC)									
Fallback	Accept Manufact	ured Installed Certific	ate (MIC)								
DNS Downloaded AVP	Accept Local Sig	nificant Certificate (LS	SC)								
► TACACS+	Authorize MIC A	Ps against auth-list or	AAA								
Local Net Users MAC Filtering	Authorize LSC A	^p s against auth-list									
 Disabled Clients User Login Policies 	AP Authorizatio	n List			Ent	tries 1 - 5 of 5					
AP Policies Password Policies	Search by MAC		Searc	h							
Local EAP											
Advanced EAD	MAC address / S	erial Number	Certificate	Type S	HA1 Key Hash						

3. 在 Add AP to Authorization List,請輸入 AP MAC 地址(不是AP無線電mac地址)。 然後,選擇證 書型別,然後按一下 Add.在此範例中,新增了一個具有MIC憑證的AP。**附註**:對於具有 SSC的AP,請選擇 ssc 在Certificate Type下。

1111111									Save	Configuration	Eing	Logout Refresh
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK			🔒 <u>H</u> ome
Security	AP Polici	es										Apply
▼ AAA General ▼ RADIUS	Policy Con	figuratio	1									
Accounting	Accept Se	lf Signed C	ertificate (SSC)									
Fallback	Accept Ma	nufactured	Installed Certific	ate (MIC)								
Downloaded AVP	Accept Lo	cal Significa	nt Certificate (LS	SC)								
TACACS+	Authorize	MIC APs ag	ainst auth-list or	AAA								
Local Net Users MAC Filtering	Authorize	LSC APs ag	ainst auth-list				_					
User Login Policies	Add AP to	Authoriza	tion List									
AP Policies Password Policies	MAC Addr	ess	1	4c:77:6d:9e:61	:62							
Local EAP	Certificate	Туре	(MIC	•							
Advanced EAP				Add								
Priority Order												
Certificate	AP Author	ization Li	st			En	tries 0 - 0 of 0					
Access Control Lists				Coord	b 1			-				
Wireless Protection Policies	MAC addre		ificate									
Web Auth	Serial Num	ber Typ	e SHA1 H	(ey Hash								
TrustSec												
Local Policies												
▶ Umbrella												
Advanced												

該AP將新增到AP授權清單中,並列在 AP Authorization List.

4. 在Policy Configuration(策略配置)下,選中 Authorize MIC APs against auth-list or AAA.選擇此引數時,WLC會先檢查本機授權清單。如果AP MAC不存在,它會檢查RADIUS伺服器。

alada						Sa <u>v</u> e Conf	figuration <u>P</u> ing Logout <u>R</u> efres
cisco	MONITOR WLANS CONTROLLER	R WIRELESS SECUR	ITY MANAGEMENT	COMMANDS	HELP	FEEDBACK	A Hom
Security	AP Policies						Apply Add
General RADIUS	Policy Configuration				-		
Authentication Accounting Auth Cached Users	Accept Self Signed Certificate (SSC)						
Fallback DNS Downloaded AVP	Accept Manufactured Installed Certif Accept Local Significant Certificate (I	icate (MIC) LSC)					
TACACS+ LDAP Loss	Authorize MIC APs against auth-list o	or AAA					
MAC Filtering • Disabled Clients	AP Authorization List		En	tries 1 - 5 of 5			
AP Policies Password Policies	Search by MAC	Search					
Advanced FAP	MAC address / Serial Number	Certificate Type	SHA1 Key Hash				
Driority Order	4c:77:6d:9e:61:62	MIC					
r Phoney order	70:d3:79:26:39:68	MIC					
Certificate	88:f0:31:7e:e0:38	MIC					
Access Control Lists	f4:db:e6:43:c4:b2	MIC					
Wireless Protection Policies	fc:5b:39:e7:2b:30	MIC					
Web Auth							

TrustSec

驗證

為了驗證此配置,您需要使用MAC地址連線AP 4c:77:6d:9e:61:62 到網路和顯示器。使用 debug capwap events/errors enable 和 debug aaa all enable 命令。

此輸出顯示了當AP MAC地址不在AP授權清單中時的調試:

附註:由於空間限制,輸出中的某些行已移動到第二行。

(Cisco Controller) >debug capwap events enable (Cisco Controller) >debug capwap errors enable (Cisco Controller) >debug aaa all enable

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5256, already allocated index 277

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 AP Allocate request at index 277 (reserved)
*spamApTask4: Feb 27 10:15:25.593: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response, state Capwap_no_state

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0 *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Request failed!

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5256 *aaaQueueReader: Feb 27 10:15:25.593: Unable to find requested user entry for 4c776d9e6162 *aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9 *aaaQueueReader: Feb 27 10:15:25.593: ReProcessAuthentication previous proto 8, next proto 4000001 *aaaQueueReader: Feb 27 10:15:25.593: AuthenticationRequest: 0x7f01b4083638 *aaaQueueReader: Feb 27 10:15:25.593: Callback..... *aaaQueueReader: Feb 27 10:15:25.593: proxyState......70:69:5A:51:4E:C0-00:00 *aaaQueueReader: Feb 27 10:15:25.593: Packet contains 9 AVPs: *aaaQueueReader: Feb 27 10:15:25.593: AVP[01] User-Name.....4c776d9e6162 (12 bytes) 51-4e-c0 (17 bytes) 9e-61-62 (17 bytes) *aaaQueueReader: Feb 27 10:15:25.593: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes) *aaaQueueReader: Feb 27 10:15:25.593: AVP[05] Nas-Ip-*aaaQueueReader: Feb 27 10:15:25.593: AVP[06] NAS-Identifier......0x6e6f (28271) (2 bytes) *aaaQueueReader: Feb 27 10:15:25.593: AVP[08] Service-Type.....0x0000000a (10) (4 bytes) *aaaQueueReader: Feb 27 10:15:25.593: AVP[09] Message-Authenticator................DATA (16 bytes) *aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Error Response code for AAA Authentication : -7*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Returning AAA Error 'No Server' (-7) for mobile 70:69:5a:51:4e:c0 serverIdx 0 *aaaQueueReader: Feb 27 10:15:25.593: AuthorizationResponse: 0x7f017adf5770 *aaaQueueReader: Feb 27 10:15:25.593: RadiusIndexSet(0), Index(0) *aaaQueueReader: Feb 27 10:15:25.593: protocolUsed..... *aaaQueueReader: Feb 27 10:15:25.593: proxyState.....70:69:5A:51:4E:C0-00:00 *aaaQueueReader: Feb 27 10:15:25.593: Packet contains 0 AVPs: *aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB

for the client.

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Failure Response sent to 0.0.0.0:5256

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Radius Authentication failed. Closing dtls Connection. *spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Disconnecting DTLS Capwap-Ctrl session 0xd6f0724fd8 for AP (192:168:79:151/5256). Notify(true) *spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 CAPWAP State: Dtls tear down

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 acDtlsPlumbControlPlaneKeys: lrad:192.168.79.151(5256) mwar:10.48.71.20(5246)

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS keys for Control Plane deleted successfully for AP 192.168.79.151

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS connection closed event receivedserver (10.48.71.20/5246) client (192.168.79.151/5256) *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Entry exists for AP (192.168.79.151/5256) *spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Unable to find AP 70:69:5a:51:4e:c0 *spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 No AP entry exist in temporary database for 192.168.79.151:5256

此輸出顯示了將LAP MAC地址新增到AP授權清單時的調試:

附註:由於空間限制,輸出中的某些行已移動到第二行。

(Cisco Controller) >debug capwap events enable (Cisco Controller) >debug capwap errors enable (Cisco Controller) >debug aaa all enable

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 using already alloced index 274
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5256, already allocated index 274

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP Allocate request at index 274 (reserved)
*spamApTask4: Feb 27 09:50:25.393: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response, state Capwap_no_state

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is not allowed to send in state Capwap_no_state for AP 192.168.79.151

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0 *spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Request failed! *aaaQueueReader: Feb 27 09:50:25.394: User 4c776d9e6162 authenticated *aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : 0*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Returning AAA Success for mobile 70:69:5a:51:4e:c0 *aaaQueueReader: Feb 27 09:50:25.394: AuthorizationResponse: 0x7f0288a66408 *aaaQueueReader: Feb 27 09:50:25.394: resultCode.....0 *aaaQueueReader: Feb 27 09:50:25.394: proxyState.....70:69:5A:51:4E:C0-00:00 *aaaQueueReader: Feb 27 09:50:25.394: Packet contains 2 AVPs: *aaaQueueReader: Feb 27 09:50:25.394: AVP[01] Service-Type.....0x00000065 (101) (4 bytes) *aaaQueueReader: Feb 27 09:50:25.394: AVP[02] Airespace / WLAN-Identifier.....0x00000000 (0) (4 bytes) *aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 User authentication Success with File DB on WLAN ID :0 *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Version: = 134770432 *spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K *spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType: 0x36 bundleApImageVer: 8.8.111.0 *spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0 *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len = 79 *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5256 *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 CAPWAP State: Join *spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 capwap_ac_platform.c:2095 - Operation State 0 ===> 4*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Capwap State Change Event (Reg) from capwap_ac_platform.c 2136

*apfReceiveTask: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Register LWAPP event for AP 70:69:5a:51:4e:c0 slot 0

針對AAA伺服器的AP授權

您還可以將WLC配置為使用RADIUS伺服器授權使用MIC的AP。將資訊傳送到RADIUS伺服器時 ,WLC會使用AP MAC位址作為使用者名稱和密碼。例如,如果AP的MAC地址是 4c:77:6d:9e:61:62中 ,控制器用於授權AP的使用者名稱和密碼都是使用定義的傳遞器的mac地址。

此示例說明如何配置WLC以使用Cisco ISE授權AP。

- 1. 在WLC控制器GUI上,按一下 Security > AP Policies.系統將顯示AP Policies頁面。
- 2. 在Policy Configuration(策略配置)下,選中 Authorize MIC APs against auth-list or AAA.選擇此引數時,WLC會先檢查本機授權清單。如果AP MAC不存在,它會檢查RADIUS伺服器。

ياليتان.								Sa <u>v</u> e Cor	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		n <u>H</u> ome
Security	AP Policies								Appl	y Add
 ▼ AAA General ▼ RADIUS 	Policy Configuration									
Authentication Accounting Auth Cached Users Fallback	Accept Self Signed Ce Accept Manufactured I	rtificate (SSC) Installed Certifica	te (MIC)							
DNS Downloaded AVP	Accept Local Significar	nt Certificate (LSC	:)							
 TACACS+ LDAP Local Net Users MAC Filtering 	Authorize MIC APs aga Authorize LSC APs aga	iinst auth-list or / iinst auth-list	AAA	_						
Disabled Clients Discrete Policies AP Policies	AP Authorization Lis	t			Ent	tries 1 - 5 of 5	÷			
Password Policies	Search by MAC		Searc	h						
Local EAP	MAC address / Serial	Number	Certificate	Type 6	HA1 Key Hash					
Advanced EAP	4c:77:6d:9e:61:62	inditioer	MIC	iffe 5	they mush					
Priority Order	70:d3:79:26:39:68		MIC							
Certificate	88:f0:31:7e:e0:38		MIC							
Access Control Lists	f4:db:e6:43:c4:b2		MIC							
Wireless Protection Policies	fc:5b:39:e7:2b:30		MIC							
▶ Web Auth										
TrustSec										

3. 導航至 Security > RADIUS Authentication 從控制器GUI顯示 RADIUS Authentication Servers 頁面。在此 頁面中,您可以定義MAC分隔符。WLC會取得AP Mac位址,並使用此處定義的分隔符將其傳 送到Radius伺服器。這很重要,因為使用者名稱會與Radius伺服器中設定的相符。在本示例 中, No Delimiter 用於使使用者名稱 4c776d9e6162.

cisco	MONITOR	<u>W</u> LANs <u>C</u> (ONTRO	ller w <u>i</u> rele		HELP FEEDBACK	Sa <u>v</u> e Configu	ration Ping Logout	<u>R</u> efresh Horne
Security	RADIUS	Authenticat	ion S	ervers				Apply Nev	v
▼ AAA General ▼ RADIUS Authentication	Auth Ca Use AES	illed Station ID T S Key Wrap	vpe	AP MAC Address (Designed for FI	SSID ••	IUS server)			
Accounting Auth Cached Users Fallback DNS Downloaded AVP	MAC De Frameo	limiter MTO	_	No Delimiter	P				
TACACS+ LDAP	Network User	Management	Tunn	Hyphen	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status	
Local Net Users				Single Hyphen	10.48.39.100	1812	Disabled	Enabled	
 Disabled Clients User Login Policies AP Policies Password Policies 		2		No Delimiter	10.48.39.128	1812	Disabled	Enabled	
Local EAP									
Advanced EAP									
Priority Order									
Certificate									
Access Control Lists									
Wireless Protection Policies									
Web Auth									
TrustSec									
Local Policies									

4. 然後,按一下 New 以便定義RADIUS伺服器。

ահահո			Sage Configuration Ping Logout Refresh
cisco	MONITOR WLANS CONTROLLER	N WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	🔒 <u>H</u> ome
Security	RADIUS Authentication Serve	ers > New	< Back Apply
AAA General Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users	Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisco ISE Default settings Apply Cisco ACA Default settings	3 10.48.39.128 ASCII	
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Key Wrap Port Number Server Status	 Designed for FIPS customers and requires a key wrap compliant RADIUS server) 1812 Enabled 	
Local EAP	Support for CoA	Enabled T	
Advanced EAP	Server Timeout	5 seconds	
Priority Order	Network User	C Enable	
Certificate	Management	C Enable	
► Access Control Lists	Management Retransmit Timeout	5 seconds	
Wireless Protection	Tunnel Proxy	Enable	
' Policies	PAC Provisioning	Enable	
Web Auth	IPSec	Enable Enable	
TrustSec	Cisco ACA	Enable	
Local Policies			

5. 在上定義RADIUS伺服器引數 RADIUS Authentication Servers > New 頁面。這些引數包括 RADIUS Server IP Address中, Shared Secret中, Port Number,和 Server Status.完成後,按一下 Apply.此示例使用Cisco ISE作為IP地址為10.48.39.128的RADIUS伺服器。

配置Cisco ISE以授權AP

要啟用思科ISE授權AP,您需要完成以下步驟:

- 1. 將WLC配置為Cisco ISE上的AAA客戶端。
- 2. 將AP MAC地址新增到思科ISE上的資料庫。

但是,您可以將AP MAC地址新增為終端(最佳方法)或使用者(其密碼也是MAC地址),但這要 求您降低密碼安全策略要求。

由於WLC不傳送NAS-Port-Type屬性(該屬性是ISE匹配Mac地址身份驗證(MAB)工作流程的要求),因此需要對其進行調整。

配置MAB不需要NAS埠型別屬性的新裝置配置檔案

導航至 Administration > Network device profile 並建立新的裝置配置檔案。啟用RADIUS並將有線MAB流 設定為需要service-type=Call-check,如圖所示。您可以從傳統思科配置檔案複製其他設定,但我 們的想法是不需要「Nas-port-type」屬性來實現有線MAB工作流程。



Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers
* Name	Ciscotemp		
Description			
lcon	change icon	Default (i)	
Vendor	Cisco		
Supported Protoc	cols		
RADIUS			
TACACS+			
TrustSec			
RADIUS Dictionaries			
Templates			
Expand All / Collapse All			
\vee Authentication	/Authorization		
✓ Flow Type Co	onditions		
Vired MAB deter	cted if the following condition(s) are m	net :	
Radius:Se	ervice-Type 🗸	Call Check V	

將WLC配置為Cisco ISE上的AAA客戶端

- 1. 轉到 Administration > Network Resources > Network Devices > Add.系統將顯示New Network Device頁面。
- 2. 在此頁面上,定義WLC Name,管理介面 IP Address 和 Radius Authentications Settings 喜歡 Shared Secret.如果您計畫輸入AP MAC地址作為終端,請確保使用之前配置的自定義裝置配置檔案,而不是預設的Cisco配置檔案!

cisco	Identity Sen	vices Engine	Home	► Context Vi	isibility	 Operations 	▶ Policy	✓ Administration	in ⊧W	ork Centers		License Warning 🔺		
Sy:	stem 🕨 Iden	tity Management	✓ Networ	k Resources	Device F	ortal Manageme	ent pxGrid	Services + Fee	d Service	Threat Centric	NAC			
Net	work Devices	Network Device G	Broups	Network Device	Profiles	External RADIU	JS Servers	RADIUS Server S	equences	NAC Managers	External MDM	Location Services		
		0	Netv	work Devices	;									
etwor	k Devices			- 1	Name WI	LC5520								
efault	Device			Descr	iption									
avice	Security Settin	igs			12	-								
				IP Address	· ·	P: 10.48.71.	20			32			@ .	
				* Device F Model N Software Ve ' Network Devic Location L IPSEC M Device Type M	Profile ANAME CONTRACTOR CONTRACT	Cisco • ⊕ • •	Set To Def. Set To Def. Set To Def.	ault						
			V		thentication	n Settings								
				RADIUS	DP Setting	S								
				RADIUS U	DP Setting	5	F	rotocol RADIU	6		_			
				RADIUS U	DP Setting	5	F * Shared	Protocol RADIU	s	Shov				
				RADIUS U	DP Setting	5	F * Shared C	Secret APOIL	s 	Shov	o Default			
				RADIUS U RADIUS D	DP Setting TLS Settin	s gs (j)	F * Shared C	Secret A Port 1700		Shov	o Default			
				RADIUS U RADIUS D	DP Setting TLS Settin	s gs (į)	F * Shared C DTLS R	Protocol RADIU: Secret DA Port 1700 equired ()	\$	Shov	o Default			

3. 按一下 Submit.

將AP MAC地址新增到思科ISE上的終端資料庫

導航至 Administration > Identity Management > Identities 並將MAC地址新增到終端資料庫。

將AP MAC地址新增到思科ISE上的使用者資料庫(可選)

如果您不想修改有線MAB配置檔案並選擇將AP MAC地址作為使用者放置,則必須降低密碼策略要求。

 導航至 Administration > Identity Management.在這裡,我們需要確保密碼策略允許將使用者名稱用作 密碼,並且策略還必須允許使用mac地址字元,而不再需要不同型別的字元。導航至 Settings > User Authentication Settings > Password Policy:

cisco Identity Services Engine	Home 🔸 Context Visibility 🔸 Operations 🔸 Policy 🔫 Administration 🔸 Work Centers License Warning 🛕 🔍 💿 💈
System Identity Management	t Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
Identities Groups External Ide	dentity Sources Identity Source Sequences - Settings
	°
User Custom Attributes	Password Policy Account Disable Policy
User Authentication Settings	Password Policy
Endpoint Purge	* Minimum Length: 4 characters (Valid Range 4 to 127)
Endpoint Custom Attributes	Password must not contain:
	User name or its characters in reverse order
	Cisco" or its characters in reverse order
	This word or its characters in reverse order:
	Repeated characters four or more times consecutively
	Dictionary words, their characters in reverse order or their letters replaced with other characters ()
	Default Dirlinger: ()
	S Delater Dictional ()
	Custom Dictionary () Choose File. No file chosen
	The newly added custom dictionary file will replace the existing custom dictionary file.
	Password must contain at least one character of each of the selected types:
	Lowercase alphabetic characters
	Uppercase alphabetic characters
	V Numeric characters
	Non-alphanumeric characters
	Password History

2. 然後導航至 Identities > Users 然後按一下 Add.顯示「使用者設定」頁面時,定義此AP的使用者名 稱和密碼,如下所示。

提示:使用 Description 用於輸入密碼的欄位,以便以後輕鬆了解密碼的定義是什麼。 密碼也必須是AP MAC地址。在本例中, 4c776d9e6162.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers License Warning	g 🔺 🔍 💿 😋								
System - Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC									
dentities Groups External Identity	y Sources Identity Source Sequences									
	Network Access Users List > New Network Access User									
st Manual Network Scan Results	▼ Network Access User									
	* Name 4c776d9e6162									
	Status Zabled -									
	Email									
	▼ Passwords									
	Password Type: Internal Users 💌									
	Password Re-Enter Password									
	* Login Password Generate Password (
	Enable Password Generate Password									
	User Information									
	First Name									
	Last Name									
	▼ Account Options									
	Description pass=4c776d9e6162									
	Change password on next login									
	▼ Account Disable Policy									
	Disable account if date exceeds 2019-04-28 (yyyy-mm-dd)									
	▼ User Groups									

3. 按一下 Submit.

定義策略集

1. 您需要定義 Policy Set 以匹配來自WLC的驗證請求。首先,通過導航到 Policy > Policy Elements > Conditions,並建立新的條件以匹配WLC位置,在本例中為「 LAB_WLC」和 Radius:Service-Type Equals Call Check 用於Mac身份驗證。此處的條件名為「 AP_Auth」。

cisco Identity Services Engine	Home	Context Visibility	Operations		Administration	Work Centers	al	License Warning 🔺	Q		0	ø
Policy Sets Profiling Posture C	lient Provis	sioning - Policy Element	nts									
Dictionaries Conditions + Resu	Its		1000									
Library Conditions	Librar	у			Editor							
Smart Conditions	Sea	rch by Name										°° ^
Time and Date						Radius Service	е-Туре					
Profiling	Q 🛱		5 I 🗄 🖱 📕	S 5 🕹		Fouals .	Call Check			-		
▹ Posture	1	AP Auth				Equals					-	
✓ Network Conditions		Condition for authe/auth	z of APs.	0	AND •	LAB_WLC						0
Endstation Network Conditions Device Network Conditions Device Port Network Conditions		BYOD_is_Registered Default condition for BY device that has passed to process	OD flow for any (D		l	F New AN	ID OR				
		Catalyst_Switch_Loca ntication	I_Web_Authe		Set	to 'Is not'			Dupli	cate	Sav	
		Default condition used to authentication requests Authentication from Cisc Switches	o match for Local Web co Catalyst	D								

- 2. 按一下 Save.
- 3. <u>然後新建 Allowed Protocols Service</u> 用於AP身份驗證。請確保您僅選擇 Allow PAP/ASCII:

cisco Identity Services Engine	Home + Co	ontext Visibility	Operations		Administration	Work Centers	License Warning 🔺	Q,	0	•	•
Policy Sets Profiling Posture C	ient Provisioning	· Policy Elements									
Dictionaries Conditions Result	s										
Authentication	Allowed Protoco Allowed Protoco	ols Services List > /	AP_authenticati	on							
Allowed Protocols	Name	AP_authentication	1								
Authorization	Description	-		96	7						
► Profiling					//						
Posture		otocols									
Client Provisioning	Auth	entication Bypass Process Host Looku	ID (j)								
	Auth	entication Protoco Allow PAP/ASCII	Is								
		Allow CHAP									
		Allow MS-CHAPv1									
	□,	Allow MS-CHAPv2									
	□,	Allow EAP-MD5									
	, 🗆 ,	Allow EAP-TLS									
	□,	Allow LEAP									
	, 🗆 ,	Allow PEAP									

4. 在 Allowed Protocols/Server Sequence.展開 View 和 Authentication Policy > Use > Internal Users 以便ISE在 內部資料庫中搜尋AP的使用者名稱/密碼。

cisco	Identity S	ervices Engine	Home	Context Visibility	 Operations 		Administration	Work Centers	Lice	nse Warning 🔺			
Policy :	Sets Pro	ofiling Posture Clier	nt Provisioni	ing Policy Element	nts								
Policy	Sets											Reset	Save
+	Status	Policy Set Name		Description		Condition	IS		Allowed Protocols / Serve	er Sequence	Hits	Actions	View
Search						_	_						
	0	Policy4APsAuth				AF	P_Auth		AP_authentication	× • +	19	٥	\triangleright
/	ø	Default		Default policy set					Default Network Access	× + +	591	٥	>

Policy Sets Profiling Policy Elements Policy Sets Policy4APsAuth Allower Status Policy Set Name Description Conditions Allower Search Image: AP_Auth Image: AP_Auth	Reset Save d Protocols / Server Sequence Hits uthentication * * + 19
Policy Sets → Policy4APsAuth Status Policy Set Name Description Conditions Allowe Search Image: Search Image: Search Image: Search	Reset Save
Status Policy Set Name Description Conditions Allower Search Image: AP_Auth Image: AP_Auth Image: AP_Auth Image: AP_Auth	d Protocols / Server Sequence Hits uthentication * • + 19
Search Policy4APsAuth AP_auth AP_auth	uthentication * * + 19
Policy4APSAuth	uthentication × • + 19
Authentication Policy (1)	
+ Status Rule Name Conditions Use	Hits Actions
Search	
+	
Options	X V 19 🗘
Authorization Policy - Local Exceptions	
Authorization Policy - Global Exceptions	
Authorization Policy (1)	
	_

5. 按一下 Save.

驗證

為了驗證此配置,您需要將MAC地址為4c:77:6d:9e:61:62的AP連線到網路和監視器。使用 debug capwap events/errors enable 和 debug aaa all enable 命令。

從調試中可看出,WLC將AP MAC地址傳遞到RADIUS伺服器10.48.39.128,並且伺服器已成功驗 證AP。然後AP向控制器註冊。

附註:由於空間限制,輸出中的某些行已移動到第二行。

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5248

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 using already alloced index 437 *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Allocate database entry for AP 192.168.79.151:5248, already allocated index 437

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP Allocate request at index 437 (reserved)
*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5248 from
temporary database.
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5248) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response, state Capwap_no_state

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is not allowed to send in state Capwap_no_state for AP 192.168.79.151

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP

70:69:5a:51:4e:c0 *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request failed! *spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5248 *spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Failed to parse CAPWAP packet from 192.168.79.151:5248 *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9 *aaaQueueReader: Feb 27 14:58:07.566: ReProcessAuthentication previous proto 8, next proto 40000001 *aaaQueueReader: Feb 27 14:58:07.566: AuthenticationRequest: 0x7f01b404f0f8 *aaaQueueReader: Feb 27 14:58:07.566: Callback......0xd6cef02166 *aaaQueueReader: Feb 27 14:58:07.566: proxyState.....70:69:5A:51:4E:CO-00:00 *aaaQueueReader: Feb 27 14:58:07.566: Packet contains 9 AVPs: *aaaQueueReader: Feb 27 14:58:07.566: AVP[02] Called-Station-Id.....70:69:5a:51:4e:c0 (17 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[03] Calling-Station-Id.....4c:77:6d:9e:61:62 (17 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[06] NAS-Identifier......0x6e6f (28271) (2 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[08] Service-Type.....0x0000000a (10) (4 bytes) *aaaQueueReader: Feb 27 14:58:07.566: AVP[09] Message-Authenticator................DATA (16 bvtes) *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 radiusServerFallbackPassiveStateUpdate: RADIUS server is ready 10.48.39.128 port 1812 index 1 active 1 *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 NAI-Realm not enabled on Wlan, radius servers will be selected as usual *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Found the radius server : 10.48.39.128 from the global server list *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Send Radius Auth Request with pktId:185 into qid:0 of server at index:1 *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Sending the packet to v4 host 10.48.39.128:1812 of length 130 *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Successful transmission of Authentication Packet (pktId 185) to 10.48.39.128:1812 from server queue 0, proxy state 70:69:5a:51:4e:c0-00:00 *aaaQueueReader: Feb 27 14:58:07.566: 00000000: 01 b9 00 82 d9 c2 ef 27 f1 bb e4 9f a8 88 5a 6dZm *aaaQueueReader: Feb 27 14:58:07.566: 00000010: 4b 38 1a a6 01 0e 34 63 37 37 36 64 39 65 36 31 K8....4c776d9e61 *aaaQueueReader: Feb 27 14:58:07.566: 00000020: 36 32 1e 13 37 30 3a 36 39 3a 35 61 3a 35 31 3a

62..70:69:5a:51: *aaaQueueReader: Feb 27 14:58:07.566: 00000030: 34 65 3a 63 30 1f 13 34 63 3a 37 37 3a 36 64 3a 4e:c0..4c:77:6d: *aaaQueueReader: Feb 27 14:58:07.566: 00000040: 39 65 3a 36 31 3a 36 32 05 06 00 00 01 04 06 9e:61:62.... *aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38 .0G...no..TF.a*8 *aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 0a ZW"[A..a.l.... *aaaQueueReader: Feb 27 14:58:07.566: 00000080: 15 f9 .. *aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client. *radiusTransportThread: Feb 27 14:58:07.587: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9) *radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 *** Counted VSA 150994944 AVP of length 28, code 1 atrlen 22) *radiusTransportThread: Feb 27 14:58:07.588: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9) *radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 AVP: VendorId: 9, vendorType: 1, vendorLen: 22 *radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b profile-name=Unk *radiusTransportThread: Feb 27 14:58:07.588: 00000010: 6e 6f 77 6e nown *radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Processed VSA 9, type 1, raw bytes 22, copied 0 bytes *radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Access-Accept received from RADIUS server 10.48.39.128 (qid:0) with port:1812, pktId:185 *radiusTransportThread: Feb 27 14:58:07.588: RadiusIndexSet(1), Index(1) *radiusTransportThread: Feb 27 14:58:07.588: protocolUsed.....0x0000001 *radiusTransportThread: Feb 27 14:58:07.588: proxyState.....70:69:5A:51:4E:C0-00:00 *radiusTransportThread: Feb 27 14:58:07.588: Packet contains 4 AVPs: *radiusTransportThread: Feb 27 14:58:07.588: AVP[01] User-Name.....4c776d9e6162 (12 bytes) *radiusTransportThread: Feb 27 14:58:07.588: AVP[02] State.....ReauthSession:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3dr cFsHuYpChs (65 bytes) *radiusTransportThread: Feb 27 14:58:07.588: AVP[03] Class.....DATA (83 bytes) *radiusTransportThread: Feb 27 14:58:07.588: AVP[04] Message-Authenticator.....DATA (16 bytes) *spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Version: = 134770432 *spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K *spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType: 0x36 bundleApImageVer: 8.8.111.0 *spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0 *spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len = 79 *spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5248

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 CAPWAP State: Join

疑難排解

使用以下命令對組態進行疑難排解:

- debug capwap events enable 配置LWAPP事件的調試
- debug capwap packet enable 配置LWAPP資料包跟蹤的調試
- debug capwap errors enable 配置LWAPP資料包錯誤的調試
- debug aaa all enable 配置所有AAA消息的調試

如果RADIUS即時中的ISE報告在您對ISE授權AP時記錄使用者名稱「INVALID」,這意味著身份驗 證正在針對終端資料庫進行驗證,並且您未按照本文檔中的說明修改有線MAB配置檔案。如果 MAC地址身份驗證與有線/無線MAB配置檔案不匹配,則ISE認為MAC地址身份驗證無效,該配置檔 案預設需要WLC未傳送的NAS埠型別屬性。

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)。