Configurazione dell'assegnazione dinamica della VLAN con i WLC basati su ISE per la mappa del gruppo di Active Directory

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Assegnazione dinamica di VLAN con server RADIUS
Corfigurazione
Esempio di rete
Configurazione
Integrazione da ISE ad AD e configurazione dei criteri di autenticazione e autorizzazione per gli
utenti su ISE
Configurazione WLC per supporto autenticazione dot1x e override AAA per SSID 'office hq'
Verifica
Risoluzione dei problemi

Introduzione

Questo documento descrive il concetto di assegnazione dinamica delle VLAN.

Prerequisiti

Nel documento viene descritto come configurare il controller WLC (Wireless LAN Controller) e il server Identity Services Engine (ISE) in modo da assegnare dinamicamente i client WLAN (Wireless LAN) a una VLAN specifica.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Wireless LAN Controller (WLC) e Lightweight Access Point (LAP)
- Conoscenza funzionale di un server di autenticazione, autorizzazione e accounting (AAA), ad esempio ISE
- · Conoscenza approfondita delle reti wireless e dei problemi di sicurezza wireless
- Conoscenza funzionale e configurabile dell'assegnazione dinamica delle VLAN

- Conoscenza di base dei servizi Microsoft Windows AD, nonché di un controller di dominio e dei concetti relativi al DNS
- Conoscenze base di controllo e provisioning del protocollo CAPWAP (Access Point Protocol)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5520 WLC con firmware versione 8.8.11.0
- Cisco serie 4800 AP
- Supplicant Windows nativo e Anyconnect NAM
- Cisco Secure ISE versione 2.3.0.298
- · Microsoft Windows 2016 Server configurato come controller di dominio
- Cisco serie 3560-CX Switch con versione 15.2(4)E1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici.</u>

Assegnazione dinamica di VLAN con server RADIUS

Nella maggior parte dei sistemi WLAN, ogni WLAN dispone di un criterio statico che viene applicato a tutti i client associati a un SSID (Service Set Identifier) o a una WLAN nella terminologia del controller. Sebbene potente, questo metodo presenta delle limitazioni in quanto richiede ai client di associarsi a SSID diversi per ereditare criteri QoS e di sicurezza diversi.

La soluzione WLAN di Cisco risolve questo limite con il supporto delle reti di identità. In questo modo, la rete può annunciare un singolo SSID, ma determinati utenti possono ereditare diversi attributi QoS e VLAN e/o criteri di sicurezza in base alle credenziali dell'utente.

L'assegnazione dinamica della VLAN è una di queste funzionalità che permette a un utente wireless di accedere a una VLAN specifica in base alle credenziali fornite dall'utente. L'attività di assegnazione degli utenti a una VLAN specifica viene gestita da un server di autenticazione RADIUS, ad esempio Cisco ISE. Questa funzionalità può essere utilizzata, ad esempio, per fare in

modo che l'host wireless rimanga sulla stessa VLAN su cui si sposta all'interno della rete di un campus.

Il server Cisco ISE esegue l'autenticazione degli utenti wireless su uno dei diversi database possibili, incluso il database interno. Ad esempio:

- DB interno
- Active Directory
- Protocollo LDAP (Generic Lightweight Directory Access Protocol)
- Database relazionali compatibili con ODBC (Open Database Connectivity)
- Server token Rivest, Shamir e Adelman (RSA) SecurID
- Server token conformi a RADIUS

<u>I protocolli di autenticazione Cisco ISE e le origini di identità esterne supportate</u> elencano i vari protocolli di autenticazione supportati dai database interni ed esterni di ISE.

In questo documento viene illustrata l'autenticazione degli utenti wireless che utilizzano il database esterno di Windows Active Directory.

Una volta completata l'autenticazione, ISE recupera le informazioni sul gruppo dell'utente dal database di Windows e lo associa al rispettivo profilo di autorizzazione.

Quando un client tenta di associarsi a un LAP registrato con un controller, il LAP passa le credenziali dell'utente al WLC con l'aiuto del rispettivo metodo EAP.

WLC invia queste credenziali ad ISE con l'uso del protocollo RADIUS (incapsulamento dell'EAP) e ISE passa le credenziali degli utenti ad AD per la convalida con l'aiuto del protocollo KERBEROS.

AD convalida le credenziali dell'utente e, se l'autenticazione ha esito positivo, informa ISE.

Una volta completata l'autenticazione, il server ISE passa alcuni attributi IETF (Internet Engineering Task Force) al WLC. Questi attributi RADIUS determinano l'ID VLAN che deve essere assegnato al client wireless. L'SSID (WLAN, in termini di WLC) del client non conta perché l'utente è sempre assegnato a questo ID VLAN predeterminato.

Gli attributi utente RADIUS utilizzati per l'assegnazione dell'ID VLAN sono:

- IETF 64 (tipo tunnel)—Impostare su VLAN
- IETF 65 (tipo tunnel medio)—Impostare su 802
- IETF 81 (ID gruppo privato tunnel)—Impostare su ID VLAN

L'ID VLAN è 12 bit e assume un valore compreso tra 1 e 4094 inclusi. Poiché Tunnel-Private-Group-ID è di tipo stringa, come definito nella RFC2868 per l'utilizzo con IEEE 802.1X, il valore intero dell'ID VLAN viene codificato come stringa. Quando vengono inviati questi attributi del tunnel, è necessario compilare il campo Tag.

Come indicato nella <u>RFC 2868</u>, sezione 3.1: il campo Tag è lungo un ottetto e serve a raggruppare gli attributi nello stesso pacchetto e fa riferimento allo stesso tunnel. I valori validi per questo campo sono compresi tra 0x01 e 0x1F inclusi. Se il campo Tag non è utilizzato, deve essere zero (0x00). Per ulteriori informazioni su tutti gli attributi RADIUS, consultare la <u>RFC 2868</u>.

Configurazione

In questa sezione vengono fornite le informazioni necessarie per configurare le funzionalità descritte nel documento.

Esempio di rete



Configurazioni

Di seguito sono riportati i dettagli di configurazione dei componenti utilizzati nel diagramma:

- L'indirizzo IP del server ISE (RADIUS) è 10.48.39.128.
- L'indirizzo dell'interfaccia di gestione e AP-manager del WLC è 10.48.71.20.
- Il server DHCP risiede nella rete LAN ed è configurato per i rispettivi pool di client; non viene visualizzato nel diagramma.
- In questa configurazione vengono usate le VLAN1477 e VLAN1478. Gli utenti del reparto Marketing sono configurati in modo da essere inseriti nella VLAN1477 e gli utenti del reparto HR sono configurati in modo da essere inseriti nella VLAN1478 dal server RADIUS quando entrambi gli utenti si connettono allo stesso SSID — office_hq.

VLAN147: 192,168.77.0/24. Gateway: 192.168.77.1 VLAN1478: 192.168.78.0/24. Gateway: 192.168.78.1

• Per la sicurezza, questo documento usaPEAP-mschapv2802.1x con.



Nota: Cisco consiglia di utilizzare metodi di autenticazione avanzati, come l'autenticazione EAP-FAST e EAP-TLS, per proteggere la WLAN.

Prima di eseguire la configurazione, vengono fatti i seguenti presupposti:

- II LAP è già registrato nel WLC
- Al server DHCP è assegnato un ambito DHCP
- · Connettività di livello 3 esistente tra tutti i dispositivi della rete
- Nel documento viene descritta la configurazione richiesta sul lato wireless e si presume che la rete cablata sia installata
- I rispettivi utenti e gruppi sono configurati in Active Directory

Per eseguire l'assegnazione dinamica della VLAN con i WLC basati sulla mappatura ISE al gruppo AD, è necessario eseguire i seguenti passaggi:

- 1. Integrazione da ISE ad AD e configurazione dei criteri di autenticazione e autorizzazione per gli utenti su ISE.
- 2. Configurazione WLC per supportare l'autenticazione dot1x e l'override AAA per SSID 'office_hq'.
- 3. Fine configurazione del supplicant client.

Integrazione da ISE ad AD e configurazione dei criteri di autenticazione e autorizzazione per gli utenti su ISE

- 1. Accedere all'interfaccia utente Web ISE utilizzando un account admin.
- 2. Passare aAdministration > Identity management > External Identity Sources > Active directory.



3. Fare clic su Aggiungi e immettere il nome del dominio e il nome dell'archivio identità dalle impostazioni di Nome punto di accesso Active Directory. Nell'esempio, l'ISE è registrato sul dominiowlaaan.come il nome joinpoint èAD.wlaaan.com- localmente significativo per ISE.

xternal Identity Sources		Connection		
	<u>نې</u>	t Jain Deint Mana		
Certificate Authentication Profile		Join Point Name	AD.wiaaan.com	(1)
Contractive Directory		 Active Directory Domain 	wlaaan.com	()
EDAP			L	
ODBC				
RADIUS Token		Cubmit Cancel		
RSA SecurID		Submic Cancel		
SAML Id Providers				
Social Login				

4. Una finestra popup si apre dopo chesubmitè stato premuto il pulsante che chiede se si desidera partecipare immediatamente ad ISE to AD. Premereyese fornire le credenziali utente di Active Directory con diritti di amministratore per aggiungere un nuovo host al dominio.

Connection Whiteliste	ed Domains PassiveID G	roups Attributes Adv	vanced Settings	
* Join Point Name AD. * Active Directory Domain wla	wlaaan.com i aan.com	ı) D		
야클 Join 약클 Leave 🧕 Test User 🛉	Diagnostic Tool 🔗 Refresh Table			
ISE Node rmanchur-ise.wlaaan.com	ISE Node Role Status STANDALONE A Not Joined	Domain Controller	Site	
	Join Domain Please specify the credentials required to	Join ISE node(s) to the Active Directory Iministrator	r Domain.	

5. A questo punto, è necessario che ISE sia stata correttamente registrata in Active Directory.

ernal Identity Sources	Connection Whitelisted Dor	nains Passi	veID Groups	Attributes Advanced	Settings
End Y Certificate Authentication Profile Active Directory LDAP Onpec	Join Point Name AD.wlaaa Active Directory Domain wlaaan.d	n.com		0	
RADIUS Token	👷 Join 🛛 👷 Leave 👤 Test User 💼 Dia	gnostic Tool 🛛 🛞 Refr	esh Table		
RSA SecurID	ISE Node	ISE Node Role	Status	Domain Controller	Site
SAML Id Providers	rmanchur-ise.wlaaan.com	STANDALONE	Operational	WIN-CFA29CSRIL9.wlaaan.com	Default-First-Site-Name

In caso di problemi con il processo di registrazione, è possibile utilizzareDiagnostic Tool per

eseguire i test richiesti per la connettività AD.

6. È necessario recuperare i gruppi per le directory attive utilizzate per assegnare i rispettivi profili di autorizzazione. Passare aAdministration > Identity management > External Identity Sources > Active directory >

> Groups

, quindi fare clic suAdde scegliereSelect Groups from Active Directory.

	sources	
Identities Groups External Identity Sources	Identity Source Sequences	
External Identity Sources	Connection Whitelisted Domains PassiveID Groups Attributes	Advanced Settings
🗇 🕶 🖽 🕶 💮 🗸	/ Edit - Add - X Delete Group Update SID Values	
Certificate Authentication Profile	Nam Select Groups From Directory	
AD.wlaaan.com	Add Group	No data available
CDBC		
RADIUS Token		
RSA SecurID		
SAML Id Providers		
Social Login		

 Viene visualizzata una nuova finestra popup in cui è possibile specificare un filtro per recuperare gruppi specifici o recuperare tutti i gruppi da Active Directory. Scegliere i rispettivi gruppi dall'elenco dei gruppi AD e premereok.

Sele	ect Direct	ory Groups							×
This	dialog is u	sed to select groups from the Directo	ory.						
	Domair	wlaaan.com		*]				
1	Name Filter	*	SID Filter	*	Type Filter	GLOBAL		Ŧ	
		Retrieve Groups 13 Groups Retrie	eved.						
	Name		*	Group SID			Group Type		
	wlaaan.co	m/Users/Cloneable Domain Control	ers	S-1-5-21-2222429329-410808516	4-322034527	1-522	GLOBAL		
	wlaaan.co	om/Users/DnsUpdateProxy		S-1-5-21-2222429329-410808516	4-322034527	1-1102	GLOBAL		
	wlaaan.co	om/Users/Domain Admins		S-1-5-21-2222429329-410808516	4-322034527	1-512	GLOBAL		
	wlaaan.co	m/Users/Domain Computers		S-1-5-21-2222429329-410808516	4-322034527	1-515	GLOBAL		
	wlaaan.co	om/Users/Domain Controllers		S-1-5-21-2222429329-410808516	4-322034527	1-516	GLOBAL		
	wlaaan.co	om/Users/Domain Guests		S-1-5-21-2222429329-410808516	4-322034527	1-514	GLOBAL		
	wlaaan.co	om/Users/Domain Users		S-1-5-21-2222429329-410808516	4-322034527	1-513	GLOBAL		
	wlaaan.co	m/Users/Group Policy Creator Own	ers	S-1-5-21-2222429329-410808516	4-322034527	1-520	GLOBAL		
	wlaaan.co	om/Users/HR		S-1-5-21-2222429329-410808516	4-322034527	1-1105	GLOBAL		
	wlaaan.co	m/Users/Key Admins		S-1-5-21-2222429329-410808516	4-322034527	1-526	GLOBAL		
	wlaaan.co	m/Users/Marketing		S-1-5-21-2222429329-410808516	4-322034527	'1-1104	GLOBAL		
	wlaaan.co	om/Users/Protected Users		S-1-5-21-2222429329-410808516	4-322034527	1-525	GLOBAL		
	wlaaan.co	om/Users/Read-only Domain Control	lers	S-1-5-21-2222429329-410808516	4-322034527	1-521	GLOBAL		



8. I rispettivi gruppi vengono aggiunti ad ISE e possono essere salvati. Premeresave.

	Co	onnection		Wh	itelisted	Domains	PassiveID	Groups	;	Attributes	Advanced Settings	
0	Edit	_الـ م م م ا		Delete	Crown	Undate CID Values						
	Edit	TADO	_	∧ Delete	Group	opuate SID values		010				
	Nar	ne						SID				
	wla	aan.com/U	sers	s/HR				S-1-5-21-2	22242932	9-4108085164-32203	345271-1105	
	wla	aan.com/U	sers	s/Marketi	ng			S-1-5-21-2	22242932	9-4108085164-32203	345271-1104	
Sa	ve	Reset										

9. Add WLC to the ISE Network device list: passare aAdministration > Network Resources > Network Devicese premereAdd.

Configurazione completa, fornendo l'indirizzo IP di gestione WLC e il segreto condiviso RADIUS tra WLC e ISE.

dentity Servic	Engine Home Context Vsibility Operations Policy -Administration Work Centers
System → Identity N	anagement Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
▼ Network Devices N	work Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM > Location Services
	0
Network Devices	Network Devices List > New Network Device Network Devices Network Devices Network Devices
Default Device	• Name W1/7520
Device Security Settings	
	IP Address + IP: 10.48.71.20 / 32
	O IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected
	* Device Profile dati Clisco 💌 🕀
	Model Name 📃 👻
	Software Version
	A Maharda Davides Carrier
	Notwork Device Scioup
	Lecation LAB S Set To Default.
	IPSEC Is IPSEC Device O Set To Default
	Device Type WLC-lab O Set To Default
	RADIUS Authentication Settings
	RADIUS UDP Settings
	Protocol RADIUS
	* Shared Secret Show
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings ()

- 10. Ora, dopo aver aggiunto ISE ad AD e il WLC all'elenco dei dispositivi, è possibile avviare la configurazione dei criteri di autenticazione e autorizzazione per gli utenti.
 - Creare un profilo di autorizzazione per assegnare gli utenti da Marketing a VLAN1477 e dal gruppo HR a VLAN1478.

Per creare un nuovo profilo, individuarePolicy > Policy Elements > Results > Authorization > Authorization profilese fare clic sulAddpulsante.

dentity Services Engine	Home → Context Visibility → Operati	ons Policy Administration Work Center	are
Policy Sets Profiling Posture Clin	ent Provisioning Policy Elements		
Dictionaries + Conditions - Results	5		
0			
Authentication	Standard Authorization Profiles	1	
- Authorization	For Policy Export go to Administration > S	System > Backup & Restore > Policy Export Page	
	/ Edit + Add Duplicate XD	Delete	
Authorization Profiles	Name	Profile	 Description
Downloadable ACLs	Blackhole Wireless Access	dit Cisco 🕀	Default profile used to blacklist wireless dev
Profiling	Cisco_IP_Phones	inter cisco 🕀	Default profile used for Cisco Phones.
Posture	Cisco_Temporal_Onboard	🚓 Cisco 🕀	Onboard the device with Cisco temporal ag
	Cisco_WebAuth	🔐 Cisco 🕀	Default Profile used to redirect users to the
Client Provisioning	NSP_Onboard	🚓 Cisco 🕀	Onboard the device with Native Supplicant
	Non_Cisco_IP_Phones	👬 Cisco 🕀	Default Profile used for Non Cisco Phones.
	DenyAccess		Default Profile with access type as Access-
	PermitAccess		Default Profile with access type as Access-

• Completare la configurazione del profilo di autorizzazione con le informazioni sulla VLAN per il gruppo corrispondente. Nell'esempio vengono mostrate le impostazioni di configurazione del_{Marketing}gruppo.

Dictionaries Conditions Results		
0		
► Authentication	Authorization Profiles > New Authorization Profile Authorization Profile	
	Authorization Promie	
✓ Authorization	* Name Marketing	
Authorization Profiles	Description Marketing	
Downloadable ACLs	* Access Type ACCESS ACCEPT *	
Profiling	Network Device Profile 🛛 🌐 🕀	
Posture	Service Template	
Client Provisioning	Track Movement 🔲 🛈	
	Passive Identity Tracking 📋 🛈	
	* Common Tacke	
	· common rasks	
	DACL Name	
	ACL (Filter-ID)	
	Constanting Constant	
	B accurry group	
	VI AN Teo ID 1 Edit Teo IDNome 1477	
	Advanced Attributes Settings	
	Select an item 💟 = 💟 — 🕂	
	14 and 12 and an an at	
	▼ Attributes Details	
	Access Type = ACCESS_ACCEPT Tunnel-Private-Group-ID = 1:1477	
	Tunnel-Type = 1:13 Tunnel-Medium-Type = 1:6	
	"	
	Submit Cancel	

Una configurazione simile deve essere eseguita per altri gruppi e devono essere configurati i rispettivi attributi del tag VLAN.

 Dopo aver configurato i profili di autorizzazione, è possibile definire i criteri di autenticazione per gli utenti wireless. A tale scopo, è possibile configurareCustomo modificare il set di criteriDefault. In questo esempio viene modificato il set di criteri Predefinito. Passare aPolicy > Policy Sets > Default. Per impostazione predefinita perdot1xil tipo di autenticazione, ISE verrà utilizzatoAll_User_ID_Stores, anche se funziona anche con le impostazioni predefinite correnti poiché AD fa parte dell'elenco delle origini di identità diAll_User_ID_Stores, in questo esempio viene utilizzata una regolawLC_labpiù specifica per il rispettivo controller LAB e AD viene utilizzata come unica origine per l'autenticazione.

				.,		Click here to do wireless setup and visibility setup Do not show thi	s again.
icy S	iets →	Default				Resot	Sav
1	Status	Policy Set Name	Descrip	tion	Conditions	Allowed Protocols / Server Sequence	e HR
arch							
	0	Default	Default p	olicy se		Default Network Access × * +	•
Authe	nticatio	on Policy (4)					
٠	Statu	s Rule Name	Condi	tions		Use Hits	Action
Search							
	0		07	Wired_MAB Wired_MAB	Internal Endpoints * *	~	
_		ww	UR		Wireless_MAB	> Options	•
					Wireless_802.1X	AD wlasan.com × *	
/	Ø	WLC_lab	AND	F	DEVICE Device Type EQUALS AE Device Types#WLC-lab	Options	۰
				F	DEVICE Location EQUALS AI Locations#LAB		
	0	Durity.	0.0		Wred_802.1X	Al_User_ID_Stores * *	•
		DOTA	UR		Wireless_802.1X	> Options	•
	~					All_User_ID_Stores × *	
	0	Denaut				> Options	v
Autho	rization	Policy - Local Exceptions					
Autho	rization	n Policy - Global Exception	5				
	rization	Policy (12)					

• È ora necessario creare criteri di autorizzazione per gli utenti che assegnano i rispettivi profili di autorizzazione in base all'appartenenza ai gruppi. Per soddisfare questo requisito, passareAuthorization policyalla sezione e creare i criteri.

Policy Sets	Profiling Posture Client Provision	Ci	Click here to do wireless setup and visibility setup Do not show this ap			
Policy Sets	→ Default				Resol	Save
Stat.	IS Policy Set Name	Description Conditions		Allowed Protocols / Server S	equence	Hits
Search	Default	Default policy set		Default Network Access	** +	0
> Authentica	ation Policy (4)					
> Authorizat	ion Policy - Local Exceptions					
> Authorizat	ion Policy - Global Exceptions					
✓ Authorizat	ion Policy (14)					
+ sta	tus Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
/ (Wroless_Marketing	AND L Winese, Access L Al wisaen com Electration ECUALS wisaen com Users/Marketing	(# Marketing)	Select from list *	0	۰
1/ 0	Wreiess_HR	AND L Winness, Access L AD visiant com Editionad FIGUALS visiant combines MR	HR	Select from list *	•	۰

Configurazione WLC per il supporto dell'autenticazione dot1x e sostituzione AAA per SSID 'office_hq'

1. Configurare ISE come server di autenticazione RADIUS su WLC. Andare allaSecurity > AAA > RADIUS > AuthenticationSezione nell'interfaccia utente Web e fornire l'indirizzo IP ISE e le informazioni segrete condivise.

cisco	MONITOR WLANS CONTROLLER	R WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Serve	vers > New
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced 	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 Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Timeout Tunnel Proxy PAC Provisioning IPSec Cisco ACA	2 ¢ 10.48.39.128 ASCII \$ ASCII \$ (Designed for FIPS customers and requires a key wrap compliant RADIUS server) 1812 Enabled \$ Enabled \$ S seconds C Enable S seconds Enable Enable Enable Enable Enable Enable Enable Enable

2. Configurare SSID_{office_hq}nella sezionewLANsdel WLC; nell'esempio seguente viene configurato SSID conwPA2/AES+dot1xe AAA override. L'interfacciaDummyviene scelta per la WLAN, in quanto la VLAN corretta viene assegnata comunque tramite RADIUS. Questa interfaccia fittizia deve essere creata sul WLC e deve essere specificato un indirizzo IP, ma l'indirizzo IP non deve essere valido e la VLAN in cui viene inserita non può essere creata nello switch uplink in modo che se non viene assegnata alcuna VLAN, il client non possa andare da nessuna parte.

cisco	MONITOR	<u>W</u> LANs <u>C</u> C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK				
WLANs	WLANs												
WLANs	Current Filte	Current Filter: None [Change Filter] [Clear F								Create	New 🗘	Go	
Advanced	U WLAN ID	WLAN WLAN	Profile Nam test AndroidAP	ne		WLAN SSID test AndroidAP			Admin Status Enabled Enabled	Security Policies [WPA2][Auth(802.1X)] [WPA2][Auth(PSK)]	0		
		11Dat	DIEK-DIMI	public		or win-public			LINDICO	(meethourse)			
	ITOR WLANS CONTROL	LLER WIRELESS	SECURITY MAN	AGEMENT COM	AANDS HELP	FEEDBACK					Saye Compo	anou Eud	Home
WLANs WLA	ANs > New											< Back	Apply
✓ WLANs Tyr WLANs Pro ► Advanced SS ID	pe file Name ID	WLAN 8 office_hq affice_ba 3 8											

WL	ANs > Edit 'office_hq	
G	eneral Security Q	oS Policy-Mapping Advanced
	Profile Name Type SSID Status	office_hq WLAN office_hq Imabled
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy Interface/Interface Group(G Multicast Vlan Feature	All dummy Enabled
	Broadcast SSID NAS-ID	Enabled none

WLANs > Edit 'office_hq'

General See	curity QoS	Policy-Map	ping Adva	nced			
Layer 2	ayer 3 AAA Se	ervers					
Layer 2 Secur	rity ⁶ WPA+WPA2 MAC Filtering	÷ +)				
Fast Transition							
Fast Transition Over the DS Reassociation Tin	Ada aneout 20 Seconds	ptive 🕈					
Protected Mana	gement Frame						
PMF	Disa	abled \$					
WPA+WPA2 Pa	rameters						
WPA Policy							
WPA2 Policy	V						
WPA2 Encrypt	tion 🗸 🗹 AES	5 TKIP	CCMP256	GCMP128	GCMP256		
OSEN Policy							
Authentication	Key Management	<u>19</u>					
802.1X	🕑 Enable						

WLANs	VLANs > Edit 'office_hq'	
WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN RADIUS Servers RADIUS Server Overwrite interface Enabled Apply Cisco ISE Default Settings Enabled Authentication Servers EAP Parameters Enabled 2 Enabled Server 1 IP:10.48.39.128, Port:1812 ‡ Server 2 None Server 3 None Server 4 None Server 5 None Server 6 None Authorization ACA Server Enabled Server None ‡ None ‡ Enabled ‡	

Allow AAA Override	🔽 Enabled		DHCP		
Coverage Hole Detection	Enabled		DHCP Server	Override	
Enable Session Timeout 21800 Session	Timeout (secs)		DHCP Addr. Assignment Management Frame Prot	ection (MFP)	
Diagnostic Channel	Enabled				
Override Interface ACL	IPv4 None CIPv6	None 🗘	MFP Client Protection 2	Optional 🗧	
Layer2 Acl	None \$		DTIM Period (in beacon i	ntervals)	
RL ACL	None \$				
P2P Blocking Action	Disabled \$		802.11a/n (1 - 255)	1	
Client Exclusion ²	CEnabled 180 Timeout Value (secs)		802.11b/g/n (1 - 255)	1	
Maximum Allowed Clients ⁸	0		NAC State None	•	
Static IP Tunneling 11	Enabled		Load Balancing and Band	Select	
Wi-Fi Direct Clients Policy	Disabled \$		Client Load Balancing		0
			-		

3. Inoltre, è necessario creare interfacce dinamiche sul WLC per le VLAN utente. Passare al menu dell_{Controller > Interfaces}'interfaccia utente. Il WLC può onorare l'assegnazione VLAN ricevuta tramite AAA solo se ha un'interfaccia dinamica in quella VLAN.

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u>	ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller								
General	General Information							
Icons	Interface Name	vlan147	7					
Inventory	MAC Address	00:a3:8	e:e3:5a:1a					
Interfaces Interface Groups	Configuration				_			
Multicast	Guest Lan							
Network Routes	Quarantine							
Fabric Configuration	Quarantine Vlan Id	0						
Redundancy	NAS-ID	none						
Mobility Management	Physical Information	1						
Ports	Port Number	1						
▶ NTP	Backup Port	C)					
> CDP	Active Port	1						
PMIPv6	Enable Dynamic AP Man	agement)					
Tunneling	Interface Address							
▶ IPv6	Interface Address							
▶ mDNS	VLAN Identifier	1	.477					
Advanced	IP Address	1	92.168.77.5					
Lawful Interception	Netmask	2	02 160 77 1					
	IPv6 Address							
	Prefix Length	•	28					
	IPv6 Gateway	:	:					
	Link Local IPv6 Address	f	e80::2a3:8eff:f	ee3:5a1a/64				
	DHCP Information							
	Primary DHCP Server	1	92.168.77.1					
	Secondary DHCP Server							
	DHCP Proxy Mode		Global 🛟					
		-	n					

Verifica

Per verificare le connessioni, usare il supplicant nativo Windows 10 e Anyconnect NAM.

Poiché si utilizza l'autenticazione EAP-PEAP e ISE utilizza un certificato autofirmato (SSC), è necessario accettare un avviso di certificato o disabilitare la convalida del certificato. In un ambiente aziendale, è necessario utilizzare un certificato firmato e attendibile su ISE e verificare che i dispositivi dell'utente finale dispongano del certificato radice appropriato installato nell'elenco delle CA attendibili.

Test connessione con Windows 10 e supplicant nativo:

1. AprireNetwork & Internet settings > Wi-Fi > Manage known networkse creare un nuovo profilo di rete premendo ilAdd new networkpulsante; immettere le informazioni richieste.

← Settings	
ŵ Wi-Fi	
Manage known networks	
, Add a new network	Add a new network
+	Network name
Search this list	office_hq
Sort by: Preference $$ Filter by: All $$	Security type
	WPA2-Enterprise AES V
	EAP method Protected EAP (PEAP)
	Authentication method
112	Secured password (EAP-MSCHAP v2) \sim
	Connect automatically
- The second second	Connect even if this network is not broadcasting
	Save Cancel

2. Verificare che l'utente abbia selezionato il profilo corretto per l'accesso con autenticazione ISE.

01	Refresh O Reset Repeat Counts	Export To .															Filter • 0	»-
	Time	Status	Details	Repeat	Identity		Endpoint ID	Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address	Network Device	Device Port	Identity Group	Posture St	Server	
×					Bob	×	Endpoint ID	Endpoint Profil	Authentication	Authorization Policy	Authorization I	IP Address \$	Network Device	Device Port	Identity Group	Posture Statue	Server	
	Feb 15, 2019 02:16:43:300 PM	•	à	3	Bob		F4.8C.50.62.14.68	Unknown	Default >> W	Default >> Wireless_HR	HR						manchur-is	e
	Feb 15, 2019 02:09:56:389 PM		0		Bob		F4.8C.50.62.14.68	Unknown	Default >> W	Default >> Wireless_HR	HR		WLC5520		Unknown		manchur-is	e

3. Verificare che la voce del client sul WLC sia stata assegnata alla VLAN corretta e che si trovi nello stato RUN.

،، ،،، ،، cısco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS HELP FR	FEEDBACK		Saye Configuration Ping Logout Befresh n Home
Monitor	Clients				Entries 1 - 1 of 1
Summary Access Points Cisco CleanAir	Current Filter None (S	hanne Filter) (Clear Filter)	WIAN BFile WIAN CETD	liter Name Protocol	Status Anda Red Stat Id Turned Fasting
Statistics CDP	192.168.78.36	AP4C77.6D9E.6162	office_hq office_hq	Bob 802.11ac(5 GHz	2) Associated Yes 1 1 No No
Rogues Clients					
Sleeping Clients Multicast					

4. Dalla CLI del WLC, lo stato del client può essere verificato conshow client dertails

show client detail f4:8c:50:62:14:6b
Client MAC Address..... f4:8c:50:62:14:6b
Client Username Bob

:

Client Webauth Username N/A Hostname: Device Type: Intel-Device AP Name..... AP4C77.6D9E.6162 AP radio slot Id..... 1 Client State..... Associated User Authenticated by RADIUS Server Client User Group..... Bob Client NAC OOB State..... Access Wireless LAN Id..... 3 Wireless LAN Network Name (SSID)..... office_hq Wireless LAN Profile Name..... office_hq Hotspot (802.11u)..... Not Supported Connected For 242 secs IP Address..... 192.168.78.36 Gateway Address..... 192.168.78.1 Policy Manager State..... RUN EAP Type..... PEAP Interface.....vlan1478 Quarantine VLAN......0 Access VLAN..... 1478

Test della connessione a Windows 10 e Anyconnect NAM:

1. Scegliere il SSID dall'elenco SSID disponibili e il rispettivo tipo di autenticazione EAP (in questo esempio PEAP) e il modulo di autenticazione interna.

	🕥 Cisco AnyCo	nnect Secure Mobility Client — 🗆 🗙
	Web Authentic	VPN: Use a browser to gain access.
	<u> </u>	Network: Connected (10.103.150.57) internet
Cisco AnyConnect		× curity:
Enter information f	for the connection.	e Key.
Media:	Wi-Fi Hidden Network	
Descriptive Name:	office_hq	Scan:
SSID:	office_hq	can not required on current Wi-Fi.
Security:	WPA2 Enterprise AES	
802. 1X Configuration		
password V	PEAP ~	a Security:
		not currently protected by Umbrella.
	OK Cano	el missing.

2. Specificare nome utente e password per l'autenticazione utente.

	S Cisco AnyConnect Secure Mobility Client − □ ×	
Cisco AnyConnect office_hq X	VPN:	
Please enter your username and password for the network: office_hq	Connect	
Username: Alice	No Network Connectivity	
Password: ********	Network: Authenticating	
OK Cancel	office_hq 🔒 📶 🗸 🔚	
	Web Security: No License Key.	
	System Scan: Limited or no connectivity.	

3. Poiché ISE sta inviando un certificato SSC al client, è necessario scegliere manualmente di considerare attendibile il certificato (nell'ambiente di produzione si consiglia di installare il certificato attendibile su ISE).

Cisco AnyConnect X		
The server certificate for the network 'office_hq' has failed validation. Do you want to trust it? Certificate Name: rmanchur-ise.wlaaan.com@ Issued To: rmanchur-ise.wlaaan.com Issued By: rmanchur-ise.wlaaan.com Expiration Date: 2020-02-13 15:03:40 UTC	VPN: Verify your network connection. Connect No Network Connectivity Network: Authenticating office_hq Image: I	
	Web Security: No License Key.	

4. Verificare i log di autenticazione su ISE e accertarsi che sia selezionato il profilo di autorizzazione corretto per l'utente.

CI	Reset Repeat Counts	Z Export To*																	¥ Filter •	۰-
	Time	Status	Details	Repeat	Identity		Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authorizat	IP Addr	1955	Network Device	Device Port	Identity Group	Posture St	Server	Mdm
×					Alice	×	60	×	Endpoint Prof	Authentication	Authorization Policy	Authorizatio	n IP Addr	100	Network Device	Device Port	Identity Group	Posture Statu	Server	Mdm
	Feb 15, 2019 02:51:27.163 PM	•	ò	0	Alce		F4:80:50:62:14:68		Microsoft-W	Default >>	Default >> Wireless_Marketing	Marketing	192.168	77.32					manchur-ise	
	Feb 15, 2019 02:51:24.807 PM	۵	à +		Alce	*	F4:8C:50:62:14:68	*	Mcrosoft-W	Default >>	Default >> Wireless_Marketing	Marketing		*	WLC5520		Workstation 💠		manchur-ise 💠	·

5. Verificare che la voce del client sul WLC sia stata assegnata alla VLAN corretta e che si trovi nello stato RUN.

Clients		Entries 1 - :
Current Filter None (Chaope.Filter) (Clear.Filter)		
Client MAC Addr TD Address(Truck/Truck) AD Name WIAN Drofile WIAN SSTD ser Name Drotorol Status 2007	Port Slot Id	Tunnel
Clinic Nucle Nucle Predmini Predmini <td>1 1</td> <td>No</td>	1 1	No

6. Dalla CLI del WLC, lo stato del client può essere verificato conshow client dertails

:

Client MAC Address	f4:8c:50:62:14:6b
Client Username	Alice
Client Webauth Username	N/A
Hostname:	
Device Type:	Intel-Device
AP MAC Address	70:69:5a:51:4e:c0
AP Name	AP4C77.6D9E.6162
AP radio slot Id	1

Client State	Associated
User Authenticated by	RADIUS Server
Client User Group	Alice
Client NAC OOB State	Access
Wireless LAN Id	3
Wireless LAN Network Name (SSID)	office_hq
Wireless LAN Profile Name	office_hq
Hotspot (802.11u)	Not Supported
Connected For	765 secs
BSSID	70:69:5a:51:4e:cd
Channe1	36
IP Address	192.168.77.32
Gateway Address	192.168.77.1
Netmask	255.255.255.0
Policy Manager State	RUN
Policy Type	WPA2
Authentication Key Management	802.1x
Encryption Cipher	CCMP-128 (AES)
Protected Management Frame	No
Management Frame Protection	No
EAP Type	PEAP
Interface	vlan1477
VLAN	1477

Risoluzione dei problemi

1. Per visualizzare i risultati, usare il comandotest aaa radius username

password

wlan-id

in modo da verificare la connessione RADIUS tra WLC, test aaa show radius ISE e.

test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request	
Wlan-id	2
ApGroup Name	none

Attributes	Values
User-Name	Alice
Called-Station-Id	00-00-00-00-00-00:AndroidAP
Calling-Station-Id	00-11-22-33-44-55
Nas-Port	0x0000001 (1)
Nas-Ip-Address	10.48.71.20

NAS-Identifier	0x6e6f (28271)
Airespace / WLAN-Identifier	0x0000002 (2)
User-Password	cisco!123
Service-Type	0x0000008 (8)
Framed-MTU	0x00000514 (1300)
Nas-Port-Type	0x00000013 (19)
Cisco / Audit-Session-Id	1447300a000003041d5665c
Acct-Session-Id	5c66d541/00:11:22:33:44:55/743

test radius auth request successfully sent. Execute 'test aaa show radius' for response (Cisco Controller) >test aaa show radius Radius Test Request Wlan-id..... 2 ApGroup Name..... none Radius Test Response Radius Server Retry Status -----1 Success 10.48.39.128 Authentication Response: Result Code: Success Attributes Values -----_____ User-Name Alice ReauthSession:1447300a000003041d5665c State CACS:1447300a000003041d5665c:rmanchur-ise/339603379/59 Class Tunnel-Type 0x000000d (13) Tunnel-Medium-Type 0x0000006 (6)

(Cisco Controller) >

Tunnel-Group-Id

- 2. Per risolvere i problemi di connettività dei client wireless, debug client utilizzare.
- 3. Usare il comando_{debug aaa all enable}per risolvere i problemi di autenticazione e autorizzazione sul WLC.

0x000005c5 (1477)



Nota: utilizzare questo comando solo condebug mac addrper limitare l'output in base all'indirizzo MAC per il quale viene eseguito il debug.

4. Per identificare i problemi relativi agli errori di autenticazione e ai problemi di comunicazione di Active Directory, consultare i log di ISE in tempo reale e i log delle sessioni.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).