Configuración de asignación de VLAN dinámica con WLC basada en ISE para mapa de grupo de Active Directory

Contenido

 Introducción

 Prerequisites

 Requirements

 Componentes Utilizados

 Convenciones

 Asignación de VLAN dinámica con servidor RADIUS

 Diagrama de la red

 Configuraciones

 Integración de ISE a AD y configuración de políticas de autenticación y autorización para usuarios en ISE

 VErtFicación

 Vic Configuration to Supportdot1x Authentication and AAA Override for SSID 'office hg'

Introducción

Este documento describe el concepto de asignación de VLAN dinámica.

Prerequisites

El documento describe cómo configurar el controlador de LAN inalámbrica (WLC) y el servidor de Identity Services Engine (ISE) para asignar clientes de LAN inalámbrica (WLAN) a una VLAN específica de forma dinámica.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de controladores de LAN inalámbrica (WLC) y puntos de acceso ligeros (LAP)
- Conocimiento funcional de un servidor de autenticación, autorización y contabilidad (AAA) como ISE
- · Conocimiento completo de las redes inalámbricas y de los problemas de seguridad

inalámbrica

- Conocimiento funcional y configurable de la asignación de VLAN dinámica
- Conocimientos básicos de los servicios de Microsoft Windows AD, así como de los conceptos de controlador de dominio y DNS
- Conocimiento básico del protocolo de control y aprovisionamiento de puntos de acceso (CAPWAP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de Cisco serie 5520 que ejecuta la versión de firmware 8.8.111.0
- AP de Cisco serie 4800
- Suplicante nativo de Windows y NAM de Anyconnect
- Cisco Secure ISE versión 2.3.0.298
- Microsoft Windows 2016 Server configurado como controlador de dominio
- Switch Cisco serie 3560-CX que ejecuta la versión 15.2(4)E1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco para obtener más información sobre las</u> <u>convenciones del documento.</u>

Asignación de VLAN dinámica con servidor RADIUS

En la mayoría de los sistemas WLAN, cada WLAN tiene una política estática que se aplica a todos los clientes asociados a un identificador de conjunto de servicios (SSID) o WLAN en la terminología del controlador. Aunque es eficaz, este método tiene limitaciones porque requiere que los clientes se asocien con diferentes SSID para heredar diferentes QoS y directivas de seguridad.

La solución WLAN de Cisco aborda esta limitación gracias a la compatibilidad con las redes de identidad. Esto permite que la red anuncie un solo SSID, pero permite que usuarios específicos hereden diferentes QoS, atributos de VLAN y/o políticas de seguridad basadas en las credenciales del usuario.

La asignación de VLAN dinámica es una de estas funciones que colocan a un usuario inalámbrico en una VLAN específica en función de las credenciales suministradas por el usuario. Esta tarea de asignar usuarios a una VLAN específica es gestionada por un servidor de autenticación RADIUS, como Cisco ISE. Se puede utilizar, por ejemplo, para permitir que el host inalámbrico permanezca en la misma VLAN al desplazarlo dentro de una red del campus.

El servidor Cisco ISE autentica a los usuarios inalámbricos en una de las diversas bases de datos posibles, incluida su base de datos interna. Por ejemplo:

- BD interna
- Directorio activo
- · Protocolo ligero de acceso a directorios (LDAP) genérico
- Bases de datos relacionales compatibles con ODBC (Open Database Connectivity)
- Servidores de token de SecurID de Rivest, Shamir y Adelman (RSA)
- · Servidores de token compatibles con RADIUS

Los protocolos de autenticación de Cisco ISE y las fuentes de identidad externas admitidas enumeran los diversos protocolos de autenticación admitidos por las bases de datos internas y externas de ISE.

Este documento se centra en la autenticación de usuarios inalámbricos que utilizan la base de datos externa de Windows Active Directory.

Después de una autenticación correcta, ISE recupera la información de grupo de ese usuario de la base de datos de Windows y lo asocia al perfil de autorización correspondiente.

Cuando un cliente intenta asociarse con un LAP registrado con un controlador, el LAP pasa las credenciales del usuario al WLC con la ayuda del método EAP respectivo.

El WLC envía esas credenciales a ISE con el uso del protocolo RADIUS (encapsulando el EAP) e ISE pasa las credenciales de los usuarios a AD para su validación con la ayuda del protocolo KERBEROS.

AD valida las credenciales del usuario y, tras una autenticación correcta, informa al ISE.

Una vez que la autenticación es exitosa, el servidor ISE pasa ciertos atributos del Grupo de Trabajo de Ingeniería de Internet (IETF) al WLC. Estos atributos RADIUS deciden el ID de VLAN que se debe asignar al cliente inalámbrico. El SSID (WLAN, en términos de WLC) del cliente no importa porque el usuario siempre está asignado a este ID de VLAN predeterminado.

Los atributos del usuario de RADIUS que se utilizan para la asignación del ID de VLAN son:

- IETF 64 (tipo de túnel)—Establezca esto en VLAN
- IETF 65 (tipo de túnel medio)—Establezca esta opción en 802

• IETF 81 (ID de grupo privado de túnel)-Establezca esto en ID de VLAN

El ID de VLAN es de 12 bits y toma un valor entre 1 y 4094, ambos inclusive. Debido a que Tunnel-Private-Group-ID es de tipo cadena, como se define en RFC2868 para su uso con IEEE 802.1X, el valor entero de ID de VLAN se codifica como una cadena. Una vez que se envían estos atributos del túnel, es necesario rellenar el campo Tag (Etiqueta).

Como se indicó en <u>RFC 2868</u>, sección 3.1: el campo Tag tiene un octeto de longitud y está pensado para proporcionar un medio de agrupar atributos en el mismo paquete que hacen referencia al mismo túnel. Los valores válidos para este campo son de 0x01 a 0x1F, ambos incluidos. Si el campo Tag (Etiqueta) no se utiliza, debe tener el valor cero (0x00). Consulte <u>RFC 2868 para obtener más información sobre todos los atributos de RADIUS.</u>

Configurar

Esta sección proporciona la información necesaria para configurar las funciones descritas en el documento.

Diagrama de la red



Configuraciones

Estos son los detalles de configuración de los componentes utilizados en este diagrama:

- La dirección IP del servidor ISE (RADIUS) es 10.48.39.128.
- La dirección de la interfaz de administración y del administrador AP del WLC es 10.48.71.20.
- El servidor DHCP reside en la red LAN y está configurado para los grupos de clientes respectivos; no se muestra en el diagrama.
- VLAN1477 y VLAN1478 se utilizan en esta configuración. Los usuarios del departamento de Marketing se configuran para ser colocados en la VLAN1477 y los usuarios del departamento de HR se configuran para ser colocados en la VLAN1478 por el servidor RADIUS cuando ambos usuarios se conectan al mismo SSID: office_hq.

VLAN1477: 192.168.77.0/24. Gateway: 192.168.77.1 VLAN1478: 192.168.78.0/24. Gateway: 192.168.78.1

• Este documento utiliza 802.1x conPEAP-mschapv2como mecanismo de seguridad.



Nota: Cisco recomienda que utilice métodos de autenticación avanzados, como EAP-

FAST y EAP-TLS, para proteger la WLAN.

Estas suposiciones se realizan antes de realizar esta configuración:

- El LAP ya está registrado con el WLC
- · Al servidor DHCP se le asigna un ámbito DHCP
- · Existe conectividad de capa 3 entre todos los dispositivos de la red
- El documento describe la configuración requerida en el lado inalámbrico y asume que la red con cables está en su lugar
- · Los usuarios y grupos respectivos se configuran en AD

Para lograr la asignación de VLAN dinámica con WLC basados en la asignación de grupo de ISE a AD, se deben realizar estos pasos:

- 1. Integración de ISE a AD y configuración de políticas de autenticación y autorización para usuarios en ISE.
- 2. Configuración de WLC para soportar la autenticación dot1x y la invalidación AAA para el SSID 'office_hq'.
- 3. Configuración del solicitante del cliente final.

Integración de ISE a AD y configuración de políticas de autenticación y autorización para usuarios en ISE

- 1. Inicie sesión en la interfaz de usuario web de ISE con una cuenta de administrador.
- $\label{eq:linear} 2. \ Desplacese \ hasta {\rm Administration} > {\rm Identity} \ {\rm management} > {\rm External} \ {\rm Identity} \ {\rm Sources} > {\rm Active} \ {\rm directory}.$

uluilie Identity Services Engine Home	Context Visibility Operations	Policy Administration Work Centers	
System Identity Management Network R	esources	pxGrid Services + Feed Service + Threat Centric NAC	
Identities Groups External Identity Sources	Identity Source Sequences		
External Identity Sources	Active Directory		
<□ ▼ 1 ▼ 88	/ Edit 😤 Add 💥 Delete 🔎 No	ode View 🚔 Advanced Tools 👻 Scope Mode	
Certificate Authentication Profile	Join Point Name	 Active Directory Domain 	
Active Directory			No data available
LDAP			
COBC ODBC			
RADIUS Token			
RSA SecurID			
SAML Id Providers			
Social Login			

3. Haga clic en Agregar e ingrese el nombre de dominio y el nombre de almacén de identidad de la configuración de Nombre de punto de unión de Active Directory. En el ejemplo, ISE se registra en el dominiowlaaan.comy se especifica joinpoint comoAD.wlaaan.com: nombre localmente

significativo para ISE.

External Identity Sources		Connection		
	₩ .	* Join Point Name	AD.wiaaan.com] ()
Active Directory		* Active Directory Domain	wlaaan.com	
CDBC		Submit Cancel		
RSA SecurID SAML Id Providers Social Login				

4. Se abre una ventana emergente después desubmitpulsar un botón que le pregunta si desea unirse a ISE para AD inmediatamente. PulseYesy proporcione credenciales de usuario de Active Directory con derechos de administrador para agregar un nuevo host al dominio.

Connection Whitelisted	Domains Passive	PID Groups	Attributes	Advanced Settings	
* Join Point Name AD.w * Active Directory Domain wlaa	laaan.com an.com		ı T		
야 Join 야 Leave 🧕 Test User 🔮	Diagnostic Tool 🛛 🛞 Refres	h Table			
ISE Node	▲ ISE Node Role	Status	Domain Controller	Site	
	Join Domain Please specify the creder • AD U:	tials required to Join ISE ser Name () Administrat * Password	node(s) to the Active Dire	ctory Domain.	

5. Después de este punto, debe haber registrado ISE correctamente en AD.

xternal Identity Sources	Connection White	listed Doma	ains Passiv	eID Groups	Attributes Advance	d Settings	
Certificate Authentication Profile Active Directory LDAP OBC	Join Point Name Active Directory Domain	AD.wlaaan. wlaaan.co	.com		Ū.		
RADIUS Token	9 Join 9 Leave 9 Test User	👕 Diagr	nostic Tool 🛛 🏀 Refre	sh Table	Demois Controller	Cite	
RSA SecuriD		-	ISE NODE ROLE	Status	Domain Controller	Site	

En caso de que tenga algún problema con el proceso de registro, puede utilizar_{Diagnostic} Tool para ejecutar las pruebas necesarias para la conectividad de AD.

6. Debe recuperar los grupos de los directorios activos que se utilizan para asignar los perfiles de autorización respectivos. Desplácese hastaAdministration > Identity management > External Identity Sources

> Active directory >

> Groups

, haga clic enAddy elijaSelect Groups from Active Directory.

► System	esources	
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	
Certricate Authentication Profile Active Directory	Nam Select Groups From Directory Add Group	
2 AD.wlaaan.com		No data available
EDAP LDAP		
COBC		
RADIUS Token		
RSA SecurID		
SAML Id Providers		
Social Login		

 Se abre una nueva ventana emergente donde puede especificar un filtro para recuperar grupos específicos o recuperar todos los grupos de AD.
 Elija las amunas recuperativas de la liste de amunas de AD.

Elija los grupos respectivos de la lista de grupos de AD y pulseok.

Sel This	ect Directory Groups s dialog is used to select groups from the Directo	ory.				×
	Domain wlaaan.com		*			
	Name Filter *	SID Filter	*	Type Filter GLOBAL	•	
	Retrieve Groups 13 Groups Retrie	eved.				
	Name	*	Group SID		Group Type	
	wlaaan.com/Users/Cloneable Domain Controll	ers	S-1-5-21-2222429329-410808516	4-3220345271-522	GLOBAL	
	wlaaan.com/Users/DnsUpdateProxy		S-1-5-21-2222429329-410808516	4-3220345271-1102	GLOBAL	
	wlaaan.com/Users/Domain Admins		S-1-5-21-2222429329-410808516	4-3220345271-512	GLOBAL	
	wlaaan.com/Users/Domain Computers		S-1-5-21-2222429329-410808516	4-3220345271-515	GLOBAL	
	wlaaan.com/Users/Domain Controllers		S-1-5-21-2222429329-410808516	4-3220345271-516	GLOBAL	
	wlaaan.com/Users/Domain Guests		S-1-5-21-2222429329-410808516	4-3220345271-514	GLOBAL	
	wlaaan.com/Users/Domain Users		S-1-5-21-2222429329-410808516	4-3220345271-513	GLOBAL	
	wlaaan.com/Users/Group Policy Creator Owned	ers	S-1-5-21-2222429329-410808516	4-3220345271-520	GLOBAL	
✓	wlaaan.com/Users/HR		S-1-5-21-2222429329-410808516	4-3220345271-1105	GLOBAL	
	wlaaan.com/Users/Key Admins		S-1-5-21-2222429329-410808516	4-3220345271-526	GLOBAL	
\checkmark	wlaaan.com/Users/Marketing		S-1-5-21-2222429329-410808516	4-3220345271-1104	GLOBAL	
	wlaaan.com/Users/Protected Users		S-1-5-21-2222429329-410808516	4-3220345271-525	GLOBAL	
	wlaaan.com/Users/Read-only Domain Control	lers	S-1-5-21-2222429329-410808516	4-3220345271-521	GLOBAL	



8. Los grupos respectivos se agregan a ISE y se pueden guardar. Pulsesave.

Connec	tion	Whit	elisted	Domains	PassiveID		Groups		Attributes	Advanced Settings	
/ Edit	Add 👻	X Delete G	Sroup	Update SID Values							
Name		A Delete e	noup	-,			SID				
wlaaan.c	om/Use	ers/HR				-	5-1-5-21-2222	42932	9-4108085164-32	20345271-1105	
wlaaan.c	om/Use	ers/Marketing	g			:	S-1-5-21-2222	42932	9-4108085164-32	20345271-1104	
Cours Day	-										
Save	et										

9. Agregue el WLC a la lista de dispositivos de red ISE: navegue hastaAdministration > Network Resources > Network Devicesy presioneAdd.

Configuración completa, proporcionando la dirección IP de la administración del WLC y el secreto compartido del RADIUS entre el WLC e ISE.

dentity Service	Engine Home Context Vability Operations Policy -Administration Work Centers
F System → Identity M	nagement Network Resources
▼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
Default Device	* Name 1987/5520
Device Security Settings	
	IP Address v *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 data Class 🖌 🕀
	Model Name 📃 👻
	Software Version
	- Network Davide Group
	Location LAB S Set To Default
	IPSEC Is IPSEC Device 📀 Set To Default.
	Device Type WLC-tab O Set To Default
	 RADIUS Authentication Settings
	RADIUS UDP Settings
	Protocol RADIUS
	* Shared Secret Show
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings (i)

- 10. Ahora, después de unirse a ISE en AD y agregar el WLC a la lista de dispositivos, puede iniciar la configuración de las políticas de autenticación y autorización para los usuarios.
 - Cree un perfil de autorización para asignar usuarios de Marketing a VLAN1477 y del grupo HR a VLAN1478.

Navegue hastaPolicy > Policy Elements > Results > Authorization > Authorization profilesy haga clic en elAddbotón para crear un nuevo perfil.

dentity Services Engine	Home		
Policy Sets Profiling Posture Clie	ent Provisioning Policy Elements		
Dictionaries + Conditions - Results			
Ø			
Authentication	Standard Authorization Profiles		
- Authorization	For Policy Export go to Administration > System	> Backup & Restore > Policy Export Page	
	/ Edit +Add Da Duplicate X Delete		
Authorization Profiles	□ Name	Profile	Description
Downloadable ACLs	Blackhole Wireless Access	dta Cisco ⊕	Default profile used to blacklist wireless dev
Profiling	Cisco_IP_Phones	sta Cisco 🕀	Default profile used for Cisco Phones.
Posture	Cisco_Temporal_Onboard	誌 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-

• Complete la configuración del perfil de autorización con información de VLAN para el grupo respectivo; el ejemplo muestra las Marketing configuraciones de grupo.

Dictionaries Conditions Results	
G	Authorization Profiles > New Authorization Profile
Authentication	Authorization Profile
- 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 Tasks
	DACL Name
	ACL (Filter-ID)
	Service Group
	Booleny Gloup
	✓ VLAN Tag ID 1 Edit. Tag ID/Name 1477
	✓ Advanced Attributes Settings
	Select an item 💟 =
	▼ Attributes Details
	Access Type = ACCESS_ACCEPT
	Tunnel-Millim Tune 1:6
	rama nasian the - re-
	Submit Cancel

Se debe realizar una configuración similar para otros grupos y se deben configurar los atributos de etiqueta de VLAN respectivos.

 Una vez configurados los perfiles de autorización, puede definir directivas de autenticación para los usuarios inalámbricos. Esto se puede hacer configurandoCustomo modificando el conjunto deDefaultdirectivas. En este ejemplo, se modifica el conjunto de directivas Predeterminado. Desplácese hastaPolicy > Policy Sets > Default. De forma predeterminada para eldot1xtipo de autenticación, ISE va a utilizarAll_User_ID_Stores, aunque funciona incluso con la configuración predeterminada actual, ya que AD forma parte de la lista de origen de identidad deAll_User_ID_Stores, este ejemplo utiliza una regla más específicawLC_labpara ese controlador de LAB respectivo y utiliza AD como único origen para la autenticación.

				.,		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		0.0		Wred_MA8	Internal Endpoints * *	~
_		ww	UR		Wireless_MAB	> Options	•
					Wireless_802.1X	AD wasan.com × *	
/	Ø	WLC_lab	AND	F	DEVICE Device Type EQUALS AE Device Types#WLC-lab	Options	۰
					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)					

• Ahora debe crear directivas de autorización para los usuarios que asignen los perfiles de autorización respectivos en función de la pertenencia a grupos. Navegue hastaAuthorization policyla sección y cree políticas para cumplir ese requisito.

Policy Sets	Prof	lling Posture Client Provisionin	g 🕨 Polk	cy Demo	nta			Click here to d	to wireless setup and visibility setup	Do not shr	ow this p	gain.
Policy Se	its →	Default								Res	at (Save
St	tatus	Policy Set Name	Descript	tion	Conditions				Allowed Protocols / Ser	ver Sequ	ence	Hits
Search												
	0	Default	Default pr	olicy set					Default Network Access	* *	+	0
> Authen	tication	n Policy (4)										
> Authori	zation	Policy - Local Exceptions										
> Authori	zation	Policy - Global Exceptions										
♥ Authori	zation	Policy (14)										
+							Results					
	Status	Rule Name	Condit	tions			Profiles	Sec	urity Groups	н	its /	Actions
Search												
	0	Walass Madation			Wireless_Access		u Marketine		iact from list •	a -		•
ĺ	Wreless_Marketing	AND	F	AD wlasan.com ExternalGroups EQUALS wlasan.com/Users/Marketing		(warkesing)				×	Ť	
	~			8	Wreless_Access	<i>e</i> :	[110]		instance between the			
	9	W/RIGSS_FIK	AND	Ł	AD waaan com External Groups EQUALS waaan com UsersHR	8	(THR)					~

Configuración WLC para soportar la autenticación dot1x y la invalidación AAA para el SSID 'office_hq'

1. Configure ISE como servidor de autenticación RADIUS en WLC. Vaya a lasecurity > AAA > RADIUS > AuthenticationSección de la interfaz de usuario web y proporcione la dirección IP de ISE y la información secreta compartida.

Security RADIUS Author AAA Server Index (Pri General RADIUS Server IP Address Server IP Address	iority)	2 \$						
AAA Server Index (Pr General RADIUS Server IP Addres	iority) s(Ipv4/Ipv6)	2 🛊						
Accounting Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Disabled Clients User Login Policies Password Policies Certificate Advanced EAP Certificate Access Control Lists Wireless Protection Policies Pace Cisco ACA Confirm Shared S Confirm Shared S Confirm Shared S Apply Cisco ISE I Apply Cisco ACA Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Ret Tunnel Proxy PAC Provisioning Web Auth Cisco ACA Local Policies	rrmat Secret Default settings Default settings	10.48.39.128 ASCII \$ (Designed 1812 Enabled \$ 5 seconds Enable Enable Enable Enable Enable Enable Enable Enable	for FIPS custom	ers and requires a	key wrap comp	liant RADI	US server)	

2. Configure el SSID_{office_hq}bajo la secciónwLANsen el WLC; este ejemplo configura el SSID conwPA2/AES+dot1xy la invalidación AAA. Se elige la interfazDummypara la WLAN ya que la VLAN adecuada se asigna a través de RADIUS de todos modos. Esta interfaz ficticia se debe crear en el WLC y se le debe dar una dirección IP, pero la dirección IP no tiene que ser válida y la VLAN en la que se coloca no se puede crear en el switch de link ascendente de modo que si no se está asignando ninguna VLAN, el cliente no puede ir a ninguna parte.

CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK			
WLANs	WLANs											
▼ WLANs WLANs	Current Filte	r: Nor	ne	[Change Filte	r] [Clear Filter	1				Create	lew 🗘	Go
Advanced	U WLAN ID	Туре	Profile Na	me		WLAN SSID			Admin Status	Security Policies		
		WLAN	test			test		1	Enabled	[WPA2][Auth(802.1X)]	•	
	□ <u>2</u>	WLAN	AndroidAP			AndroidAP		1	Enabled	[WPA2][Auth(PSK)]		
	253	WLAN	BTER-BTwi	fi-public		BTwifi-public		1	Enabled	[WPA2][Auth(PSK)]	•	
սիսիս											Saye Configura	tion Eing Logout Befresi

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK			A Home
WLANs	WLANs > New								< Back	- 1	Apply
✓ WLANS WLANS > Advanced	Type Profile Name SSID ID	WLA office office 3	N 8 Lha Lha 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	2 ÷)				
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 ‡	

neral Security QoS Po	licy-Mapping Advanced	
Allow AAA Override	Z Enabled	DHCP
Coverage Hole Detection	Enabled	DHCP Server Override
Enable Session Timeout 2 1800 Session	Timeout (secs)	DHCP Addr. Assignment CRequired Management Frame Protection (MFP)
		MER Client Protection
aver2 Acl		DTIM Period (in beacon intervale)
RI ACI	None 1	
22P Blocking Action	Disabled +	802.11a/n (1 - 255) 1
Client Exclusion 2	CEnabled I80 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
Maximum Allowed Clients Per AP Radio	200	Client Band Select
Clear HotSpot Configuration	Enabled	Brooks Olient

3. También debe crear interfaces dinámicas en el WLC para las VLAN de usuario. Vaya al menú de laController > Interfaces interfaz de usuario. El WLC puede honrar solamente la asignación de VLAN recibida vía AAA si tiene una interfaz dinámica en esa VLAN.

iliilii cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u>	ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller								
General	General Information							
Icons	Interface Name	vlan147	77					
Inventory	MAC Address	00:a3:8	Be: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	L					
▶ NTP	Backup Port	()					
▶ CDP	Active Port		L					
▶ PMIPv6	Enable Dynamic AP Man	agement						
Tunneling	Tatorfaco Addroco							
▶ IPv6	Interface Address							
▶ mDNS	VLAN Identifier		1477					
Advanced	IP Address		192.168.77.5					
Lawful Interception	Netmask		255.255.255.0					
	Gateway							
	Profix Length		128					
	IPv6 Gateway	L:						
	Link Local IPv6 Address	f	e80::2a3:8eff:f	ee3:5a1a/64				
	DHCP Information			,_				
	Primary DHCP Server		192 168 77 1					
	Secondary DHCP Server							
	DHCP Proxy Mode		Global 🛔					

Verificación

Utilice el suplicante nativo de Windows 10 y el NAM de Anyconnect para probar las conexiones.

Dado que utiliza autenticación EAP-PEAP e ISE utiliza un certificado de firma automática (SSC), debe aceptar una advertencia de certificado o deshabilitar la validación de certificados. En un entorno corporativo, debe utilizar un certificado firmado y de confianza en ISE y asegurarse de que los dispositivos del usuario final tienen el certificado raíz adecuado instalado en la lista de CA de confianza.

Probar conexión con Windows 10 y suplicante nativo:

1. AbraNetwork & Internet settings > Wi-Fi > Manage known networksy cree un nuevo perfil de red pulsando elAdd new networkbotón; rellene la información necesaria.

← Settings	
命 Wi-Fi	
Manage known networks	
Add a new network	Add a new network
+	Network name
Search this list $ \wp $	office_hq
Sort by: Preference $ \smallsetminus $ Filter by: All $ \smallsetminus $	Security type
	WPA2-Enterprise AES \checkmark
(in the second s	EAP method
The second second	Authentication method
177	Secured password (EAP-MSCHAP v2)
	Connect automatically
The second second	Connect even if this network is not broadcasting
	Save Cancel

2. Compruebe el registro de autenticación en ISE y asegúrese de que se ha seleccionado el perfil adecuado para el usuario.

c	Refresh Reset Repeat Counts	Export To *														,	Filter	۰.
	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 Status	Server	
	Feb 15, 2019 02:16:43:300 PM	•	a	3	Bob		F4.8C.50.62.14.68	Unknown	Default >> W	Default >> Wireless_HR	HR						manchur-	ise
	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-	ise

3. Verifique la entrada del cliente en el WLC y asegúrese de que esté asignado a la VLAN correcta y que esté en el estado RUN.

.ı ı.ı ı. cısco	MONITOR WIANS CONTROLLER WIRELESS SEC	urity management commands help fe	EEDBACK				Saya Configuri	ation <u>P</u> ing	Logout	Befresh
Monitor	Clients								Entries 1	1 of 1
Summary Access Points Cisco CleanAir	Current Filter None [Chaos	e.Filter] (Clear Filter)								
Statistics CDP	Client MAC Addr IP.Address/Jov6/Jov6) (d:8x:50:50:14:50 192.168.78.36	AP Name AP4C77.6D9E.6162	WLAN Profile office_hq	WLAN SSID Use office_hq Bob	Protocol 802.11ac(5 GHz)	Status Associated	Auth Port Yes 1	Slot Id 1	Tunnel No	Pastlane No
Rogues Clients										
Sleeping Clients Multicast Applications										

4. Desde la WLC CLI, el estado del cliente se puede verificar con elshow 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

Pruebe la conexión con Windows 10 y Anyconnect NAM:

1. Elija el SSID de la lista de SSID disponibles y el tipo de autenticación EAP respectivo (en este ejemplo PEAP) y el formulario de autenticación interno.

	🕥 Cisco AnyC	yConnect Secure Mobility Client — 🗆 🗙	
	Web Authent	VPN: Use a browser to gain access. Connect	
	Ľ	Network: Connected (10.103.150.57) internet	
Cisco AnyConnect		× curity:	
Enter information	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 ~	PEAP ~	g Security:	
	OK Can	Cancel	
A STANDARD			

2. Proporcione el nombre de usuario y la contraseña para la autenticación de usuarios.

Sisco AnyConnect Secure Mobility Client − □ ×	
VPN: Verify your network connection.	
No Network Connectivity	
Network: Authenticating	
office_hq 🗎 🖓 🔚	
Web Security: No License Key.	
System Scan: Limited or no connectivity.	
	 Cisco AnyConnect Secure Mobility Client – × VPN: Verify your network connection. Connect No Network Connectivity Network: Authenticating office_hq Ifle Ifle

3. Dado que ISE envía un SSC al cliente, debe elegir manualmente confiar en el certificado (en el entorno de producción se recomienda instalar el certificado de confianza en 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 Trust Do Not Trust	VPN: Verify your network connection. Connect No Network Connectivity Network: Authenticating office_hq	
	Web Security: No License Key.	

4. Compruebe los registros de autenticación en ISE y asegúrese de que se ha seleccionado el perfil de autorización correcto para el usuario.

C Refresh O Reset Repeat Count	Export To •																		T Filter -	۰۰
Time	Status	Details	Repeat	Identity		Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authoriz	ati I	P Address		Network Device	Device Port	Identity Group	Posture St	Server	Mdm
×				Alice	×	60	×	Endpoint Prof	Authentication	Authorization Policy	Authoriza	ation	IP Address		Network Device	Device Port	Identity Group	Posture Statu	Server	Mdm
Feb 15, 2019 02:51:27.163 PM	•	0	0	Alce		F4:80:50:62:14:68		Microsoft-W	Default >>	Default >> Wireless_Marketing	Marketing	1	192.168.77.32						manchur-ise	
Feb 15, 2019 02:51:24.837 PM	8	à +		Alce	٠	F4:8C:50:62:14:68	*	Morosoft-W	Default >>	Default >> Wireless_Marketing	Marketing)		*	WLC5520		Workstation �		manchur-ise 4	•

5. Verifique la entrada del cliente en el WLC y asegúrese de que esté asignado a la VLAN correcta y que esté en el estado RUN.

Clients												Entries 1 - :
Current Filter No	ne	[Change Filter] [Clear Filter]	1									
Client MAC Addr	IP Address(Ipv4/Ipv6)		AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port 5	Slot Id	Tunnel
141011001001144100	194.100.77.34		104077.0091.0102	unice_ing	unice_nq	Printe	002-110(() Only)	Associated	165		•	110

6. Desde la WLC CLI, el estado del cliente se puede verificar con elshow 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

:

User Authenticated by RADIUS Server Client User Group Alice Client NAC OOB State Access Wireless LAN Id	
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_hg	
Client NAC OOB State Access Wireless LAN Id 3 Wireless LAN Network Name (SSID) office_hq Wireless LAN Profile Name office_hg	
Wireless LAN Id 3 Wireless LAN Network Name (SSID) office_hq Wireless LAN Profile Name office_hg	
Wireless LAN Network Name (SSID) office_hq Wireless LAN Profile Name	
Wireless LAN Profile Name	
Hotspot (802.11u) Not Supported	
Connected For	
BSSID	: cd
Channel	
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	
Encryption Cipher CCMP-128 (AES)	
Protected Management Frame No	
Management Frame Protection No	
EAP Type PEAP	
Interface vlan1477	
VLAN 1477	

Troubleshoot

1. Utilicetest aaa radius username

password

wlan-id

para probar la conexión RADIUS entre WLC e ISE y eltest aaa show radiuspara mostrar los resultados.

test aaa radius username Alice password <removed> wlan-id 2 $\ensuremath{\mathsf{2}}$

Radius Test Request Wlan-id ApGroup Name	2 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 Class CACS:1447300a000003041d5665c:rmanchur-ise/339603379/59 Tunnel-Type 0x000000d (13) 0x0000006 (6) Tunnel-Medium-Type Tunnel-Group-Id 0x000005c5 (1477)

(Cisco Controller) >

2. Utilice el debug client

para resolver problemas de conectividad del cliente inalámbrico.

3. Utilicedebug aaa all enablepara resolver problemas de autenticación y autorización en el WLC.



Nota: Utilice este comando solamente con eldebug mac addrpara limitar la salida basada en la dirección MAC para la cual se realiza la depuración.

4. Consulte los registros en vivo y los registros de sesión de ISE para identificar problemas, fallas de autenticación y problemas de comunicación AD.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).