Comprensión y configuración de EAP-TLS con un WLC e ISE

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Flujo EAP-TLS Pasos del flujo EAP-TLS Configurar Controlador de LAN inalámbrica de Cisco ISE con Cisco WLC Configuración de EAP-TLS Configuración de WLC en ISE Creación de un usuario nuevo en ISE Certificado de confianza en ISE **Cliente para EAP-TLS** Descargar certificado de usuario en el equipo cliente (escritorio de Windows) Perfil inalámbrico para EAP-TLS Verificación Troubleshoot

Introducción

Este documento describe cómo configurar una red de área local inalámbrica (WLAN) con 802.1X y protocolo de autenticación extensible EAP-TLS

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Proceso de autenticación 802.1X
- Certificados

Componentes Utilizados

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

hardware.

- WLC 3504 versión 8.10
- Identity Services Engine (ISE) versión 2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Flujo EAP-TLS



Pasos del flujo EAP-TLS

- El cliente inalámbrico se asocia al punto de acceso (AP). El AP no permite que el cliente envíe ningún dato en este punto y envía una solicitud de autenticación.El solicitante responde entonces con una identidad de respuesta EAP. El WLC luego comunica la información de la ID de usuario al servidor de autenticación. El servidor RADIUS responde al cliente con un paquete de inicio EAP-TLS. La conversación EAP-TLS comienza en este punto.
- 2. El par envía una respuesta EAP al servidor de autenticación que contiene un mensaje de intercambio de señales "client_hello", un cifrado que se establece en NULL
- 3. El servidor de autenticación responde con un paquete de desafío de acceso que contiene:

TLS server_hello handshake message certificate server_key_exchange
certificate request
server_hello_done.

4. El cliente responde con un mensaje EAP-Response que contiene:

Certificate \neg Server can validate to verify that it is trusted.

client_key_exchange

certificate_verify \neg Verifies the server is trusted

change_cipher_spec

TLS finished

5.Después de que el cliente se autentique con éxito, el servidor RADIUS responde con un desafío de acceso, que contiene el mensaje "change_cipher_spec" y entrada en contacto finalizado.

6. Cuando recibe esto, el cliente verifica el hash para autenticar el servidor RADIUS.

7.Una nueva clave de cifrado se deriva dinámicamente del secreto durante el intercambio de señales TLS

8/9.EAP-El éxito finalmente se envía del servidor al autenticador que luego se pasa al solicitante.

En este momento, el cliente inalámbrico con EAP-TLS activado puede acceder a la red inalámbrica.

Configurar

Controlador de LAN inalámbrica de Cisco

Paso 1. El primer paso es configurar el servidor RADIUS en el WLC de Cisco. Para agregar un servidor RADIUS, navegue hasta **Seguridad > RADIUS > Autenticación**. Haga clic en **Nuevo** como se muestra en la imagen.

	cisco	MONITOR	WLANS CO	ONTROL	LER V	VIREL	ESS SECURT	TY MANAGEMEN	NT COMMANDS	HELP				
3	ecurity	RADIUS	Authenticat	tion Se	rvers									
'	AAA General	Auth Ca	elled Station ID T	ype (AP Name	e:SSID	v)						
	Authentication	Use AES	5 Key Wrap		(Designe	ed for F	TPS customers a	and requires a key w	wrap compliant RAD	DIUS server)				
	Auth Cached Users Fallback	Framed	MTU	(1300		*							
	Downloaded AVP TACACS+	Network User	Management	Tunne Proxy	I Serve	er K	Server Addre	ss(Ipv4/Ipv6)		Port	IPS	ec	Admin Status	
	Local Net Users				1		138.77.0.84			1812	Disa	bled	Disabled	
	MAC Filtering				2		138.77.0.83			1812	Disa	abled	Disabled	
	User Login Policies				3		138.77.97.20			1812	Disa	abled	Disabled	
	AP Policies				4		138.77.97.21			1812	Disa	abled	Disabled	
1	Password Policies				5	•	172.27.1.71			1812	Disa	bled	Enabled	
•	Local EAP				6		10.100.120.41			1812	Disa	abled	Enabled	
	Advanced EAP													
,	Priority Order													
	Certificate													
•	Access Control Lists													
	Wireless Protection Policies													
1	Web Auth													
•	TrustSec													
	Local Policies													
	Umbrella													
ļ	Advanced													
ł														

Paso 2. Aquí, debe ingresar la dirección IP y el secreto compartido <contraseña> que se utiliza para validar el WLC en ISE. Haga clic en **Aplicar** para continuar como se muestra en la imagen.

Paso 3. Crear WLAN para la autenticación RADIUS.

Ahora puede crear una nueva WLAN y configurarla para utilizar el modo WPA-Enterprise, de modo que pueda utilizar RADIUS para la autenticación.

Paso 4. Seleccione **WLANs** en el menú principal, elija **Create New** y haga clic en **Go** como se muestra en la imagen.

uluulu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT CO	Saye Configuration Ping Logout: Refresh OMMANDS HELP User:admin(ReadWrite) A Home
WLANs	WLANs	Entries 1 - 15 of 15
WLANs WLANs	Current Filter: None [Change Filter] [Clear Filter]	Create New V Go
Advanced	WLAN ID Type Profile Name WLAN SSID	Admin Status Security Policies

Paso 5. Asigne el nombre **EAP-TLS** a la nueva WLAN. Haga clic en **Aplicar** para continuar como se muestra en la imagen.

սիսիս					Save Configuration Ping Logout Refresh
CISCO	MONITOR WLANS	CONTROLLER WIRELESS SEC	URITY MANAGEMENT COMMAND	S HELP	User:admin(ReadWrite) 🔒 Home
WLANs	WLANs > New				< Back Apply
 WLANS Mdvanced 	Type Profile Name SSID ID	WLAN v EAP-TLS EAP-TLS 3 v			

Paso 6. Haga clic en **General** y asegúrese de que el estado es **Activado**. Las políticas de seguridad predeterminadas son autenticación 802.1X y WPA2, como se muestra en la imagen.

11111			Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 🔒 Home
WLANs	WLANs > Edit 'EAP-	-TLS'	< Back Apply
WLANS	General Security	QoS Policy-Mapping Advanced	
Advanced	Profile Name	EAP-TLS	
	Туре	WLAN	
	SSID	EAP-TLS	
	Status	Z Enabled	
)	Security Policies Radio Policy	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) All	
	Interface/Interface Group(G)	management v	
	Multicast Vlan Feature	Enabled	
	Broadcast SSID	C Enabled	
	NAS-ID	none	
	11ax Status	C Enabled	
	Lobby Admin Access	0	

Paso 7. Ahora, navegue hasta **Seguridad > Servidores AAA**, seleccione el servidor RADIUS que acaba de configurar y como se muestra en la imagen.

ahaha					Save Configuration Ping Logout Refresh
cisco	MONITOR WL	ANS CONTROLLER WIRELE	SS SECURITY MANAGEMEN	T COMMANDS HELP	User:admin(ReadWrite) 🔒 Home
WLANs	WLANs > Edi	t 'EAP-TLS'			< Back Apply
WLANs WLANs	General	Security QoS Policy-	Mapping Advanced		
Advanced	Layer 2	Layer 3 AAA Servers			
1	Select AAA s RADIUS Sen RADIUS S Apply Cisc	ervers below to override use o vers erver Overwrite interface Enat o ISE Default Settings Enat	f default servers on this WLAN Ned		
	Server 1	Authentication Servers Enabled IP-10 106 35 67. Port:1812.	Accounting Servers C Enabled None V	EAP Parameters Enable	
	Server 2	None	None v		
	Server 3	None v	None v		
	Server 4	None ~	None v		
	Server 5	None	None v		
	Server 6	None	None v		
		Authorization ACA Server	Accounting ACA Server		
	Server	None v	None v		

Nota: Es una buena idea verificar que puede alcanzar el servidor RADIUS del WLC antes de continuar. RADIUS utiliza el puerto UDP 1812 (para la autenticación), por lo que debe asegurarse de que este tráfico no se bloquea en ninguna parte de la red.

ISE con Cisco WLC

Configuración de EAP-TLS

Para crear la política, debe crear la lista de protocolos permitidos para utilizar en nuestra política. Dado que se escribe una política dot1x, especifique el tipo de EAP permitido en función de la configuración de la política.

Si utiliza el valor predeterminado, permite la mayoría de los tipos de EAP para autenticación que no son preferibles si necesita bloquear el acceso a un tipo de EAP específico.

Paso 1. Navegue hasta Política > Elementos de Política > Resultados > Autenticación > Protocolos Permitidos y haga clic en Agregar como se muestra en la imagen.

Identity Services Engine	Home	Operations					
Authentication Authorization Profiling	g Posture Client Provisioning	▼ Policy Elements					
Dictionaries + Conditions - Results							
0							
- Authentication	Allowed Protocols Services For Policy Export go to Administration > System > Backup & Restore > Policy Export Page						
Allowed Protocols							
► Authorization	/ Edit 🕂 Add 🖓 Duplicate	X Delete					
	Service Name	Description					
▶ Profiling	Default Network Access	Default Allowed Protocol Service					
► Posture							
Client Provisioning							

Paso 2. En esta lista de protocolos permitidos, puede introducir el nombre de la lista. En este caso, la casilla **Allow EAP-TLS** está marcada y las demás casillas están desmarcadas como se muestra en la imagen.

dentity Services Engine	Home → Conte	ext Visibility	Operations	Policy	Administration	Work Centers
Authentication Authorization Prot	iling Posture Clie	nt Provisioning				
Dictionaries Conditions - Resu	Its					
(Allowed Protocols	Services List > N	Jour Allowed Drotes	als Comico		
✓ Authentication	Allowed Proto	cols	vew Allowed Protoc	UIS Service		
Allowed Protocols	Name	AP-TLS				
Authorization	Description]	
▶ Profiling				/	2	
▶ Posture	 Allowed Proto 	cols				
Client Provisioning	Authen	tication Bypass				
/ citerit / rovisioning	Pr	ocess Host Look	up (į́)			
	Authen	tication Protoco	ols			
		ow PAP/ASCII				
		ow CHAP				
		ow MS-CHAPv1				
		ow MS-CHAPv2				
		ow EAP-MD5				
	🖌 🗹 All	ow EAP-TLS				
	(Allow Auther	ntication of expired c	ertificates t	to allow certificate ren	ewal in Authorization Policy (j)
	(Enable State	eless Session Resun	ne		
		Session tick	et time to 2		Hours	
		Proactive se	ssion ticket update v	vill occur at	fter 10 % of Tim	e To Live has expired
		ow LEAP				
	🗸 🗆 AII	ow PEAP				
	1	PEAP Inner Meth	ods			
	6	Allow EAP-N	IS-CHAPv2			
		Allow P	assword Change F	etries 1	(Valid Range 0 to 3)
	(Allow EAP-0	этс			
		Allow P	assword Change F	etries 1	(Valid Range 0 to 3)
	6	Allow EAP-T	LS			
		Allow A	authentication of expl	red certific	ates to allow certificat	e renewal in Authorization Policy
	(Require cryp	otobinding TLV (j)			

Configuración de WLC en ISE

Paso 1. Abra la consola de ISE y navegue hasta **Administration > Network Resources > Network Devices > Add**, como se muestra en la imagen.

Hole Identity Services Engine	Home + Control Visibility + Operations + Policy = Administration + Work C	erlini		License Warning 🔺 🔍 🔍 🔘
Bysten + Identity Management Websch Devices Network Device G	Network Resources + Device Postal Management px/0xid Services + Feed Service + 1 rups Network Device Profiles External RADIUS Servers RADIUS Servers RADIUS Servers RADIUS Servers RADIUS Servers	nnait Cantric NAC C Managers External MDM + Location Services		Click here to do wreless setup and visibility setup Do not show this again
Network deutoes	Network Devices			
Default Device	/ ER +AM Contone Geinant Gelant - O Generate PAC Xonte -			Steric () Total 😨 🙀
Device security security	Name IP/Plask Profile Name Location	Type	Description	

Paso 2. Introduzca los valores como se muestra en la imagen.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	Click be
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	Glick He
G		
Network Devices	Notwork Devices List > New Network Device Notwork Devices	
Default Device		
Device Security Settings	Percenting Data-WLL	
	Description	
	IP Address * IP : 10.106.35.67 / 32	
	* Device Profile 🔐 Cisco 💌 💬	
	Model Name 🕎	
	Software Version	
	* Network Device Group	C
	Location All Locations 🚫 Set To Default	
	IPSEC Is IPSEC Device 🔿 Set To Default	
	Device Type All Device Types	
	RADIUS Authentication Settings	
	· · · · · · · · · · · · · · · · · · ·	
	RADIUS UDP Settings	
	Protocol RADIUS	
	* Shared Secret Show	
	Use Second Shared Secret 🔲 🕢	
	Show	
	CoA Port Set To Default	
	RADIUS DTLS Settings (i)	

Creación de un usuario nuevo en ISE

Paso 1. Navegue hasta Administration > Identity Management > Identities > Users > Add como se muestra en la imagen.

dentity Services Engine	Nome + Context Visibility + Operations + Policy	Administration Work Centers		Lixense Warning 🛦 🔍 🔍 🔘 🔘
+ Dystem + Identity Management	Network Resources -> Device Portal ManagementpuGrid Service	ices + Feed Service + Threat Centric NAC		Cick here to do wreates justice and visibility online Do not show the span. X
Identifies Oroups External Identi	y Sources identity Source Sequences + Settings			
0	Nationale Access Disease			
Users	NEW ALLESS USES			Suburi Suburi Sala
Latest Manual Network Scan Results	/ Dilt - Add BCharge Dates @ Prest @ Open	X Culata B Dupleate		they Al *) 13
	Status Name . Description	First Name Last Name Email Address	User Identity Groups Admin	

Paso 2. Ingrese la información como se muestra en la imagen.

cisco	Identi	ty Service	es Engine	Home	▸ Context	Visibility	 Operations 	Policy	▼ Adm	inistration	• Work Cer	nters
Sys	stem	- Identity	Management	Network	Resources	Device	e Portal Management	pxGrid S	Services	Feed Ser	rvice F Thr	eat Centric NAC
- Ider	ntities	Groups	External Ide	ntity Sources	Identity S	ource Seq	uences + Settings					
			(3	A	and list a						
Users					Access Us	ers List > N	lew Network Access	User				
Latest M	Manual	Network S	can Results	V NC		.635 0361						
				* Na	me bharti							
				Sta	tus 🔽 E	nabled 👻						
				En	nail 🦳							
				▼ P	asswords							
				Pa	ssword Type	: Intern	nal Users					
						Passy	vord		Re-Enter	Password		
				*14	ogin Passwo	ord •••••	••••			•		Generate Password
				En	able Passwi	ord						Generate Password
				21								
				▼ U	ser Inforn	nation						
				Firs	st Name 🔒							
				Las	st Name 📑	/L = L.:						
				-								
				▼ A	ccount Op	tions						
						Desc	ription					
				Ch	ange passw	ord on nex	t login 🛛					
					count Di	able Del	lau					
				▼ A	count Dr	sable Pol						
					Disable a	ccount if da	ate exceeds 2018-0	2-17		(УУУ)	y-mm-dd)	
				√ U	ser Group	s						
				Is	elect an iten	1	o = 4	4				
				Subr	nit Can	cel						

Certificado de confianza en ISE

Paso 1. Navegue hasta Administración > Sistema > Certificados > Administración de certificados > Certificados de confianza.

Haga clic en **Importar** para importar un certificado a ISE. Una vez que agrega un WLC y crea un usuario en ISE, necesita hacer la parte más importante de EAP-TLS que es confiar en el certificado en ISE. Para eso necesitamos generar RSE.

Paso 2. Vaya a Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR) como se muestra en la imagen.

diale i	dentity Services Engine	Home + Context Vi	Isibility + Operations + I	Policy + Administration + W	fork Centers					License Warning 🔺	् (0	٥
▼ Syster	 Identity Management 	Network Resources	Device Portal Management p	xGrid Services → Feed Service	Threat Centric NAC								
Deploym	ient Licensing - Certi	cates + Logging + Main	itenance Upgrade + Backup	& Restore + Admin Access + 2	Settings								
		0											
	ate Management	Certificate Signin	g Requests										
System	Certificates	Generate Certificate S	Signing Requests (CSR)										
Trustee	l Certificates	A Certificate Signing R	Requests (CSRs) must be sent to a	and signed by an external authority. O	Click "export" to downloa	ad one or more CSR	is so that they may	be signed by an ex	xtemal authority. After a rec	quest has been signed, click "bin	i" to bind the	e request t	lo the
OCSP	Client Profile	signed del tindate issue	ed by that autionity. Once a Gord	s bound, it will be removed indiri dits i	liet.								
Certific	ate Signing Requests	PView 🔂 Export	X Delete Bind Certificate							Show All		7	8
Certific	ate Periodic Check Setti	Friendly Name		Certificate Subject	Key Length	Portal group tag	Timestamp		Host				
+ Certific	ate Authority					No data avai	lable						

Paso 3. Para generar CSR, navegue hasta **Uso** y desde **Se utilizan los certificados para las** opciones desplegables seleccione **Autenticación EAP** como se muestra en la imagen.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍 🔘 🔿	¢.				
▼System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC						
Deployment Licensing - Certificate	is → Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings						
0							
- Certificate Management	Certificate Signing Request						
System Certificates	Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:						
Trusted Certificates	iac identity vertiticates.						
OCSP Client Profile	Admin - Server Authentication						
Certificate Signing Requests	EAP Authentication - Server Authentication DTLS Authentication - Server Authentication						
Certificate Periodic Check Setti	Portal - Server Authentication						
Certificate Authority	pxGrd - Client and Server Authentication SAML - SAML Signing Certificate						
1	ISE Certificate Authority Certificates:						
	 ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality. ISE Intermediate CA - This is an Intermediate CA Signing Request. Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA. 						
	Usage Certificate(s) will be used for EAP Authentication T Allow Wildcard Certificates						
	Nodelci						
	Generate CSR's for these Nodes:						
	Node CSR Friendly Name						
	☑ labisetEAP Authentication						

Paso 4. Se puede ver la CSR generada en ISE. Haga clic en View como se muestra en la imagen.



Paso 5. Una vez generado CSR, busque el servidor de la CA y haga clic en **Solicitar un** certificado, como se muestra en la imagen:

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task: Request a certificate

View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Paso 6. Una vez que solicite un certificado, obtendrá las opciones **Certificado de usuario** y **solicitud de certificado avanzado**, haga clic en **Solicitud de certificado avanzado** como se muestra en la imagen.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request

Paso 7. Pegue el CSR generado en la **solicitud de certificado codificado en Base-64**. En la **plantilla de certificado:** seleccione **Web Server** y haga clic en **Submit** como se muestra en la imagen.

Microsoft Active Director	y Certificate Services f	fixer-WIN-97Q5HOKP9IG-C/
---------------------------	--------------------------	--------------------------

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

	Saved Request:		
)	Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):		11.
	Certificate Templa	ate:	
	[Web Server	
	Additional Attribu	ites:	_
	Attributes:	li.	
		Submit >]

Paso 8. Una vez que haga clic en **Submit**, tendrá la opción de seleccionar el tipo de certificado, seleccione **Base-64 codificado** y haga clic en **Download certificate chain** como se muestra en la imagen.

Microsoft Active Directory Certificate Services fixer-WIN-97Q5HOKP9IG-CA
Certificate Issued
The certificate you requested was issued to you.
DER encoded or Base 64 encoded
Download certificate
Download certificate chain

Paso 9. La descarga del certificado se completa para el servidor ISE. Puede extraer el certificado, el certificado contiene dos certificados, un certificado raíz y otro intermedio. El certificado raíz se puede importar en Administration > Certificates > Trusted certificates > Import como se muestra en las imágenes.

dentity Services Engine	Home	• Administra	tion + Work Centers				u	cense Warning 🔺 🔍 😐	• •
System Identity Management	Network Resources	rid Services + Fe	ed Service + Threat Cent	ric NAC		Cic	here to do wireless set	up and visibility setup Do not show t	his again. ×
Deployment Licensing - Certificates	s + Logging + Maintenance Upgrade + Backup &	Restore + Admir	Access > Settings						_
0									
Certificate Management	Trusted Certificates								
System Certificates	/ Edit Import Export X Delete Divew							Show All	- 8
Trusted Certificates	Friendly Name	 Status 	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	

·Indentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Deployment Licensing - Certificat	→ Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings	
Certificate Management	Import a new Certificate into the Certificate Store	
System Certificates	Certificate File Choose file Choose file Choose file	
Trusted Certificates	Friendly Name EAP-TLS	i
OCSP Client Profile	Trusted For: 👔	
Certificate Signing Requests	✓ Trust for authentication within ISE	
Certificate Periodic Check Setti	Trust for client authentication and Syslog	
Certificate Authority	Trust for authentication of Cisco Services	
	Validate Certificate Extensions	
	Description	
	Submit Cancel	

Paso 10. Una vez que haga clic en **Enviar**, el certificado se agrega a la lista de certificados de confianza. Además, el certificado intermedio es necesario para enlazar con CSR como se muestra en la imagen.

eltado Id	entity Services Engine	Home + Context Visibility + Operations + Police	y ▼Administration → Work C	Centers		License Warning 📥 🔍 💿 🔿
- System	 Identity Management 	Network Resources	rid Services + Feed Service + T	hreat Centric NAC		Click here to do wireless setup and visibility setup Do not show this again
Deploym	ent Licensing - Certificate	s + Logging + Maintenance Upgrade + Backup &	Restore + Admin Access + Sett	ings		
	0					
- Certifica	ite Management	Certificate Signing Requests				
System	Certificates	Generate Certificate Signing Requests (CSR)				
Trusted	Certificates	A Certificate Signing Requests (CSRs) must be sent to an	d signed by an external authority. Click	"export" to download one or more CSR	Rs so that they may be signed by an extern	al authority. After a request has been signed, click "bind" to bind the request to the
OCSP	Client Profile	signed certricate issued by that authority. Once a CSR is to	ound, it will be removed from this list.			
Certifica	ate Signing Requests	New Deport X Delete Bind Certificate				Show All *
Certifica	ate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group tag	Timestamp 🔺 Ho	st
		✓ ise#FAP Authentication	CNwise c.com	2048	Mon. 9 Jul 2018 ise	Created by Paint Y

Paso 11. Una vez que haga clic en **Bind certificate**, hay una opción para elegir el archivo de certificado guardado en su escritorio. Busque el certificado intermedio y haga clic en **Submit** como se muestra en la imagen.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing - Certificat	es
0	
- Certificate Management	Bind CA Signed Certificate
System Certificates	* Certificate File Choose file No file chosen
Trusted Certificates	
OCSP Client Profile	Friendly Name (i)
Certificate Signing Requests	Validate Certificate Extensions
Certificate Periodic Check Setti	
Certificate Authority	Usage
	EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
	Submit Cancel

Paso 12. Para ver el certificado, navegue hasta **Administration > Certificates > System Certificates** como se muestra en la imagen.

dentity Services Engine	Home	Context Visibility Operations	s → Policy →Ad	ministration + Work Centers				License Warning 🔺 🔍	0 <u>1</u> 0
System Identity Management	Network I	Resources	ment pxGrid Services	Feed Service PassiveID	Threat Centric NAC				
Deployment Licensing - Certificated	s → Log	ging + Maintenance Upgrade	Backup & Restore	Admin Access + Settings					
0									
 Certificate Management 	System	m Certificates 🛕 For disaster rec	covery it is recommended	to export certificate and private key p	airs of all system certificates.				
Overview	/ Ec	lit 🔶 Generate Self Signed Certific	ate 🔶 Import 🚱	Export 🗙 Delete 🔎 View					
System Certificates		Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
Endpoint Certificates	▼ ise								
Trusted Certificates		Default self-signed sami server certi ficate - CN=SAML_ise.c.com	SAML		SAML_ise.c.com	SAML_ise.c.com	Wed, 11 Jul 2018	Thu, 11 Jul 2019	
OCSP Client Profile	0	Intermediate	EAP Authentication, Admin, Portal	Default Portal Certificate Group ①	ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 2020	
Certificate Signing Requests									
Certificate Periodic Check Setti									
Certificate Authority									

Cliente para EAP-TLS

Descargar certificado de usuario en el equipo cliente (escritorio de Windows)

Paso 1. Para autenticar un usuario inalámbrico a través de EAP-TLS, debe generar un certificado de cliente. Conecte el ordenador Windows a la red para poder acceder al servidor. Abra un navegador web e introduzca esta dirección: <u>https://sever ip addr/certsrv—</u>

Paso 2. Tenga en cuenta que la CA debe ser la misma con la que se descargó el certificado para ISE.

Para ello, debe buscar el mismo servidor de CA que utilizó para descargar el certificado para el servidor. En la misma CA, haga clic en **Solicitar un certificado** como se hizo anteriormente; sin embargo, esta vez debe seleccionar **Usuario** como Plantilla de certificado, como se muestra en la imagen.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request	ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIsPJry aF412aLpmDFp1PfVZ3VaP60a/mej3IXh0RFxBUII weOh06+V+eh71jeTgiwzEZGr/ceYJIakco5zLjgR
CIVIC OF	dD7LeujkxFlj3SwvLTKLDJg+00VtAhrxlp1PyDZ3
PKCS #10 or	ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX
PKCS #7):	END CERTIFICATE REQUEST

Certificate Template:

	User	O	
dditional Attribu	utes:		
Attributes:		11.	
		Submit >	

Paso 3. Luego, haga clic en **descargar cadena de certificados** como se hizo anteriormente para el servidor.

Una vez que obtenga los certificados, siga estos pasos para importar el certificado en el equipo portátil con Windows:

Paso 4. Para importar el certificado, debe tener acceso a él desde Microsoft Management Console (MMC).

- 1. Para abrir MMC navegue hasta **Inicio > Ejecutar > MMC**.
- 2. Vaya a Archivo > Agregar o quitar complemento
- 3. Haga doble clic en Certificates.
- 4. Seleccione Cuenta de equipo.
- 5. Seleccione Equipo local > Finalizar
- 6. Haga clic en Aceptar para salir de la ventana Snap-In.
- 7. Haga clic en [+] junto a Certificados > Personal > Certificados.
- 8. Haga clic con el botón derecho en Certificados y seleccione Todas las tareas > Importar.
- 9. Haga clic en Next (Siguiente).
- 10. Haga clic en Browse.

- 11. Seleccione el archivo .cer, .crt o .pfx que desee importar.
- 12. Haga clic en Abrir.
- 13. Haga clic en Next (Siguiente).
- 14. Seleccione Seleccionar automáticamente el almacén de certificados según el tipo de certificado.
- 15. Haga clic en Finalizar y aceptar

Una vez que haya terminado la importación del certificado, debe configurar el cliente inalámbrico (escritorio de Windows en este ejemplo) para EAP-TLS.

Perfil inalámbrico para EAP-TLS

Paso 1. Cambie el perfil inalámbrico que se creó anteriormente para el protocolo de autenticación extensible protegido (PEAP) para utilizar el EAP-TLS en su lugar. Haga clic en **Perfil inalámbrico EAP**.

Paso 2. Seleccione **Microsoft: Tarjeta inteligente u otro certificado** y haga clic en **OK** que se muestra en la imagen.

EAP Wireless Network	Properties		×
Connection Security			
Security type:	WPA2-Enterprise	~	
Encryption type:	AES	~	
Choose a network aut	nentication method:		
Microsoft: Smart Card	Microsoft: Smart Card or other certificate \checkmark Settings		
☐ Remember my credentials for this connection each time I'm logged on			
Advanced settings			
		OK	Cancel

Paso 3. Haga clic en **configuración** y seleccione el certificado raíz emitido desde el servidor de la CA como se muestra en la imagen.

Smart Card or other Certificate Properties		
Sinari cara or other certificate Properties		
When connecting:		
O Use my smart card	Advanced	
Use a certificate on this computer		
Use simple certificate selection (Recommended)		
Verify the server's identity by validating the certif	icate	-
Connect to these convers (eventions) is a first of the	them (2) eem);	
Connect to these servers (examples:srv1;srv2;."	\.srv3\.com):	
Trusted Root Certification Authorities:		4
Entrust.net Certification Authority (2048)		^
Equifax Secure Certificate Authority		
GeoTrust Global CA		
GeoTrust Primary Certification Authority		
GeoTrust Primary Certification Authority - G3		
GlobalSign		
GlobalSign		
		~
	>	
Vi	ew Certificate	

Paso 4. Haga clic en **Advanced Settings** y seleccione **User or computer authentication** en la pestaña 802.1x settings (Configuración 802.1x), como se muestra en la imagen.

02.1X settings	802.11 settings		
Specify a	uthentication mode:		
User or	computer authentication	✓ Save cr	edentials
Delet	e credentials for all users		
Enable si	ngle sign on for this netwo	ork	
Perfo	orm immediately before use	er logon	
O Perform immediately after user logon			
Maximur	n delay (seconds):	10	•
	additional dialogs to be di	isplayed during s	single
Sight			

Paso 5. Ahora, intente conectarse de nuevo a la red inalámbrica, seleccione el perfil correcto (EAP en este ejemplo) y **Connect**. Está conectado a la red inalámbrica como se muestra en la imagen.

(iii	EAP Connected, secured
a	blizzard-legacy Secured
a	blizzard Secured
96	internet Open
la	dot1x_test Secured
(JioPrivateNet Secured, Hotspot 2.0
1	mac_filter Secured
N Cł	etwork & Internet settings ange settings, such as making a connection metere
<i>iii</i> . Wi	Fi Airplane mode hotspot

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. El estado del administrador de políticas de cliente debe mostrarse como **RUN**. Esto significa que el cliente ha completado la autenticación, obtenido la dirección IP y está listo para pasar el tráfico que se muestra en la imagen.

Summary Access Points Cisco CleanAir	Max Number of Records General AVC Sta	Clear AVC Stats		
Statistics	Client Properties		AP Properties	
Boques	MAC Address	34:02:86:96:2f:b7	AP Address	00:d7:8f:52:db:a0
Rogues	IPv4 Address	10.106.32.239	AP Name	Alpha2802_3rdfloor
Clients	IPv6 Address	fe80::2818:15a4:65f9:842,	AP Type	802.11bn
Sleeping Clients			AP radio slot Id	0
Multicast			WLAN Profile	EAP
Applications			WLAN SSID	EAP
vnc			Data Switching Central	
ocal Profiling			Authentication Central	
ocur Proning			Status	Associated
			Association ID	1
			// 802.11 Authentication	Open System
	Client Type	Simple IP	Reason Code	1
	User Name	Administrator	Status Code	0
	Port Number	1	CF Pollable	Not Implemented
	Interface	management	CF Poll Request	Not Implemented
	VLAN ID	32	Short Preamble	Not Implemented
	Quarantine VLAN ID	0	PBCC	Not Implemented
	CCX Version	CCXv1	Channel Agility	Not Implemented
	E2E Version	Not Supported	Re-authentication timeout	1682
	Mobility Role	Local	Remaining Re-authentication timeou	it 0
	Address	N/A	WEP State	WEP Enable
	Mobility Move Count Policy Manager State	0 BUN	Lync Properties	
	Management Frame	No	Lync State	Disabled
	UnTime (Sec)	145	Audio Cos Policy	Cilver

Paso 2. Verifique también el método EAP correcto en el WLC en la página de detalles del cliente como se muestra en la imagen.

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Auth Key Mgmt	802.1x
Encryption Cipher	CCMP (AES)
EAP Type	EAP-TLS
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied	Unavailable

Paso 3. Aquí están los detalles del cliente de CLI del controlador (salida recortada):

(Cisco Controller-Standby) > show client detail 34:	02:86:96:2f:b7
Client MAC Address	34:02:86:96:2f:b7
Client Username	Administrator
AP MAC Address	00:d7:8f:52:db:a0
AP Name	Alpha2802_3rdfloor
AP radio slot Id	0
Client State	Associated
Wireless LAN Id	5
Wireless LAN Network Name (SSID)	EAP
Wireless LAN Profile Name	EAP
Hotspot (802.11u)	Not Supported
BSSID	00:d7:8f:52:db:a4
Connected For	48 secs
Channel	1
IP Address	10.106.32.239
Gateway Address	10.106.32.1
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..... EAP-TLS

Paso 4. En ISE, navegue hasta Visibilidad del contexto > Terminales > Atributos como se muestra en las imágenes.



BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CADC=fixerDC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

1.00		
	Location	Location#All Locations
	MACAddress	34:02:86:96:2F:B7
	MatchedPolicy	Intel-Device
	MessageCode	5200
	NAS-IP-Address	10.106.32.223
	NAS-Identifier	HA_Pri
	NAS-Port	1
	NAS-Port-Type	Wireless - IEEE 802.11
	Network Device Profile	Cisco
	NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
	NetworkDeviceName	HA_Pri
	NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
	NetworkDeviceProfileName	Cisco
]	OUI	Intel Corporate
	OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
	OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
	PolicyVersion	0
	PostureApplicable	Yes
	PostureAssessmentStatus	NotApplicable
	RadiusFlowType	Wireless802_1x
	RadiusPacketType	AccessRequest
	SSID	00-d7-8f-52-db-a0:EAP
	SelectedAccessService	Default Network Access
	SelectedAuthenticationIdentityStores	EAPTLS
	SelectedAuthorizationProfiles	PermitAccess
	Serial Number	10 29 41 78 00 00 00 00 11

Troubleshoot

Actualmente no hay información específica disponible para resolver problemas de esta configuración.

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).