Comprender y configurar EAP-TLS con Mobility Express e ISE

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Flujo EAP-TLS Pasos en el Flujo EAP-TLS Configurar **Cisco Mobility Express** ISE con Cisco Mobility Express Configuración EAP-TLS Configuración de Mobility Express en ISE Certificado de confianza en ISE **Cliente para EAP-TLS** Descargar certificado de usuario en 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 seguridad 802.1x en un controlador Mobility Express. Este documento también explica el uso específico del protocolo de autenticación extensible (EAP): seguridad de la capa de transporte (TLS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración inicial de Mobility Express
- 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 5508 versión 8.5
- Identity Services Engine (ISE) versión 2.1

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 en el Flujo EAP-TLS

- 1. El cliente inalámbrico se asocia con el punto de acceso (AP).
- 2. AP no permite que el cliente envíe ningún dato en este punto y envía una solicitud de autenticación.
- 3. A continuación, el suplicante responde con una identidad de respuesta EAP. A continuación, el WLC comunica la información de ID de usuario al servidor de autenticación.
- 4. El servidor RADIUS responde al cliente con un paquete de inicio EAP-TLS. La conversación EAP-TLS comienza en este punto.
- 5. El par envía un EAP-Response de vuelta al servidor de autenticación que contiene un mensaje de entrada en contacto "client_hello", un dígito que está configurado como NULL.

6. 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.

7. 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 ¬ Verifies the server is trusted

change_cipher_spec

TLS finished

- 8. Después de que el cliente se autentica correctamente, el servidor RADIUS responde con un desafío de acceso, que contiene el mensaje "change_cipher_spec" y entrada en contacto. Al recibir esto, el cliente verifica el hash para autenticar el servidor RADIUS. Una nueva clave de cifrado se deriva dinámicamente del secreto durante el intercambio de señales TLS.
- 9. En este momento, el cliente inalámbrico habilitado para EAP-TLS puede acceder a la red inalámbrica.

Configurar

Cisco Mobility Express

Paso 1. El primer paso es crear una WLAN en Mobility Express. Para crear una WLAN, navegue hasta WLAN > Add new WLAN como se muestra en la imagen.

-								
-	Monitoring	Cisco Aironet 1850 Series Mobili	ty Express	Q	▲ ④	= 2	\geq	٥
۵	Wireless Settings	WLAN CONFIGURATION						
Ļ	Access Points	Active WLANs 5						
ľ	😁 WLAN Users							
	📽 Guest WLANs							
	OHCP Server	Add new WLAN						
ġ.	Management	Active	Name	Security Policy	Radio Policy			
÷	Advanced	C × Enabled	PSK	WPA2Personal	ALL			
	Auvanceu	🛛 🗙 Enabled	Dotty	WPA2Enternrise	ALL			

Paso 2. Aparecerá una nueva ventana emergente cuando haga clic en **Agregar nueva WLAN**. Para crear un nombre de perfil, navegue hasta **Add new WLAN > General** como se muestra en la imagen.

B	Monitoring	8	ulu ci:	Cisco Airor					Q	A	٩	8	≓	M	٥
\$	Wireless Settings														
	🖬 Access Points	2		ve WLANs 5											
	📽 WLAN Users				Add new WLAN										
	📽 Guest WLANs				General WLAN Securit	neral WLAN Security VLAN & Firewall Traffic Shaping									
	DHCP Server		Add new	WLAN											
÷.	Management			Active	WLAN II	6	•	Policy		Rad	io Policy				
Ł	Advanced	C	×	Enabled	Profile Name	ME_EAP				ALL					
		8	×	Enabled	SSID	• ME_EAP		rsonal		5 GI					
		C	×	Enabled	Admin Stat	e Enabled	•	rsonal		5 GI	Hz only				
		C	×	Enabled	Radio Polic	y ALL	• 0	rsonal		2.4	GHz only				
		C	×	Enabled	Broadcast SSI					ALL					
					Local Profilin	0									
						Apply	Cancel								

Paso 3. Configure el tipo de autenticación como WPA Enterprise para 802.1x y configure el servidor RADIUS bajo **Agregar nueva WLAN > Seguridad WLAN** como se muestra en la imagen.

æ	Monitoring	Cisco Alronet 1830 Series Mobility Express	Q	A	٩	8	#	٥
¢	Wireless Settings ⋒	WLAN CONFIGURATION						
	堂 Access Points 營 WLAN Users	Active WLANS 5 General WLAN Security VLAN & Firewall Traffic Shaping						
	Guest WLANs DHCP Server	Add new WLAN						
÷.	Management	Active MAC Filtering Security Type of Open is not allowed Policy when MAC Filtering is enabled.		Radio	Policy			
*	Advanced	Image: Ward with the security Type WPA2 Enterprise • Image: Ward with the security Type WPA2 Enterprise • Image: Ward with the security Type WPA2 Enterprise • Image: Ward with the security Type WPA2 Enterprise • Image: Ward with the security Type WPA2 Enterprise • Image: Ward with the security Type WPA2 Enterprise • Image: Ward with the security Type WPA2 Enterprise •		ALL 5 GHz only 5 GHz only				
		Image: Construction Server Image: Construction Server Image: Construction Server Image: Construction Server		5 GH: 2.4 G				
		X Enabled State Server IP Address Port		ALL				
		External Radius configuration applies to all O Apply O Cancel						

Paso 4. Haga clic en Add RADIUS Authentication Server y proporcione la dirección IP del servidor RADIUS y Shared Secret que debe coincidir exactamente con lo que se ha configurado en ISE y luego haga clic en Apply como se muestra en la imagen.

2	Monitoring	Cisco Aironet 1	330 Series Mobility Express	Q	A	٩	11	¢
\$	Wireless Settings ⋒ wLANs	WLAN CONFIGURATION	And any life All					
	堂 Access Points 答 WLAN Users	Active WLANS 5	Add Hew WEAN					
	營 Guest WLANs 參 DHCP Server	Add new WLAN	Server Index 1 •					
ġ.	Management	Active	Server IP Address The Address		Rad	io Policy		
*	Advanced	Image: Contract of the second seco	Shared Secret		ALL 5 GI	Hz only		
		C X Enabled	Show Password risonal risonal risonal risonal		5 G) 2.4	Hz only GHz only		
		C K Enabled	Server Timeout 5 Seconds		ALL			
			External Radius configuration applies to all WLANS © Apply © Cancel					

ISE con Cisco Mobility Express

Configuración EAP-TLS

Para generar la política, debe crear la lista de protocolos permitidos para utilizarla en la política. Dado que se escribe una política dot1x, especifique el tipo EAP permitido en función de cómo se configura la política.

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

Paso 1. Vaya a **Policy > Policy Elements > Results > Authentication > Allowed Protocols** y haga clic en **Add** como se muestra en la imagen.

dentity Services Engine	Home → Context Visibility → Operations → Policy → Administration → Work Centers
Authentication Authorization Profiling	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 L Duplicate X Delete
	Service Name Description
▶ Profiling	Default Network Access Default Allowed Protocol Service
▶ Posture	
Client Provisioning	

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

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Authentication Authorization Profi	Ing Posture Client Provisioning - Policy Elements
Dictionaries + Conditions - Resul	ts
0	Allowed Brotocolo Convisor List - New Allowed Brotocolo Conviso
 Authentication 	Allowed Protocols
Allowed Protocols	Name EAP-TLS
Authorization	Description
b Drafilia a	
▶ Proming	
Posture	
Client Provisioning	Authentication Bypass
	Process Host Lookup (i)
	Authentication Protocols
	Allow PAP/ASCII
	Allow CHAP
	Allow MS-CHAPv1
	Allow MS-CHAPv2
	Allow EAP-MD5
	✓ Allow EAP-TLS
	Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)
	Enable Stateless Session Resume
	Session ticket time to 2
	live
	Proactive session ticket update will occur after 10 % of Time To Live has expired
	Allow LEAP
	- Allow PEAP
	PEAP Inner Methods
	Allow EAP-MS-CHAPV2
	Allow Password Change Retries 1 (Valid Range 0 to 3)
	Allow EAP-GTC
	Allow Password Change Retries 1 (Valid Range 0 to 3)
	Allow EAP-TLS
	Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
	Require cryptobinding TLV (i)

Configuración de Mobility Express en ISE

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

-Indentity Services Engine	Home + Context Visibility + Open	ations + Policy -Administration + Work Centers		License Warning 🔺 🔍 🔍 🌲 🔿
System Identity Management	Network Resources Device Portal Ma	nagement pxGrid Services + Feed Service + Passivell	> Threat Centric NAC	
Network Devices Network Device 0	roups Network Device Profiles Externa	RADIUS Servers RADIUS Server Sequences NAC Man	gers External MDM + Location Services	
0				
Network devices	Network Devices			
Default Device				Selected 0 Total 1 😍 🎡 🚽
	/Edit 📫 Add 🖓 Duplicate 🚯 🕼	mport 🔂 Export + 🕲 Generate PAC 🗙 Delete +		Show All 💌 😽
	Name IP/Mask	Profile Name Location	Type Description	
	/ Edit Add C Duplicate Duplicate	nport Deport • Generate PAC Celete • Profile Name Location	Type Description	Show All

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

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍	0 1 0
System Identity Management	Network Resources + Device Portal Management pxGrid Services + Feed Service + PassiveID + Threat Centric NAC		
- Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services		
(
Network devices	Network Devices Lin > New Network Device Network Devices		
Default Device	Name • Name Description • 1P Address: • Device Profile Cisco • 0 Model Name • Device Profile Software Version • Network Device Group Device Type Device Type	ŵ∙	
	C - RADIUS Authentication Settings		
	Enable Authentication Settings Protocol RADIUS • Shared Secret Enable KeyWing : • Key Encryption Key • Message Authenticator Code Key Key Input Format • ASCII • HEXADECIMAL CoA Port 1700 Set. To Default.		

	TACACS Authentication Settings
	► SNMP Settings
	Advanced TrustSec Settings
Subr	nit Cancel

Certificado de confianza en ISE

Paso 1. Vaya a Administration > System > Certificates > Certificate Management > Trusted certificates.

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

Paso 2. Vaya a Administración > Certificados > Solicitudes de firma de certificados > Generar solicitudes de firma de certificados (CSR) como se muestra en la imagen.



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

cisco	Identit	y Services	Engine	Home	 Contex 	t Visibility	 Operations 	Policy	- → Adm	inistration	Work Centers
- Sys	stem	Identity M	anagement	Network	Resources	Device	Portal Manager	nent pxGrid S	Services	Feed Serv	vice Threat Centric NAC
Deple	oyment	Licensing	✓ Certificat	es 🕨 Log	ging 🕨 N	aintenance	Upgrade	Backup & Res	tore +	Admin Access	s > Settings
 Certi Sys Trus OC: Certi Certi 	ficate M tem Cert sted Cert SP Clien SP Clien tiffcate S ficate A	anagement ificates ificates t Profile ligning Requ eriodic Chec uthority	ests .k Setti	Certifi Cr IS IS	cate Sigr ertificate typ E Identity (Multi-1 Admin E AP / DTLS Portal pxGric SAML E Certifica ISE R ISE In Renew ISE R Sage Certificate(: Allow Wildca Me(s) Generate C	hing Requi- es will requir Certificates: Use (Admin,) - Server Au- Authentication - Server Au- d - Client and - SAML Sign te Authority oot CA - This termediate C w ISE OCSP oot CA/ISE In s) will be use and Certificate SR's for thes	est te different exten EAP, Portal, pxC thentication n - Server Authention on - Server Authention ing Certificates: is is not a signing A - This is an In Responder Cert ntermediate CA. d for EAP Auth es (i) e Nodes:	ided key usages Srid) - Client and Intication entication ication request, but an termediate CA s ifficates - This is entication	ability to Signing R not a sign	below outlines uthentication generate a bra aquest. hing request, t	s which extended key usages are required for each certificate type: and new Root CA certificate for the ISE CA functionality. but an ability to renew the OCSP responder certificate that is signed by the
					Node				CSR F	iendly Name	
					✓ ise				ise#EAP	Authentication	'n

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

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍 🔍 🕹 🖒
System Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Resources Threat Centric NAC	
Deployment Licensing - Certificat	s + Logging + Maintenance Upgrade Backup & Restore + Admin Access + Settings	
0		
- Certificate Management	Certificate Signing Requests	
Overview	Generate Certificate Signing Requests (CSR)	
System Certificates	A Conflictute Signing Requests (CSR) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request expending the right by the submit of the conflictute of the click of the cl	t has been signed, click "bind" to bind the request to the
Endpoint Certificates	agrec de tricale issued up their submitting. Unite a con-	
Trusted Certificates	View 2 Deport X Delete Bind Certificate CSR Details CSR Contants	Show All
OCSP Client Profile	Report Name The Context Part of Case	
Certificate Signing Requests	Ise #EAP Authentication AperAndActionation Commission Commission Commission Commission Commission AperAndAction Commission Commission Commission Commission AperAndAction A	
Certificate Periodic Check Setti	Werkdajar/cutryoutger/Vit/Ministysum_(2kthappineasulainkspc/keepsin1/3 44eBr0g/serkajar/2ktjar/Bahav/Pitzschur/TXHQD164+534+fQHMRhCUxdBgUD4Hp3	
Certificate Authority	6)/T708XcC/www8/UrApd84rdg98rm/998rm/00fer/094c7/MotogY2U/039A/034-0my a)/278m252/ms42/zdg0cc6505/028503/d436/s455788m/07890g228mg2 9er/12aQuG0yygC3apLE4rc11a4e/07799/2012A04Qp38rg(20AAGC04+10AQC20A) Drv404Qc0Mrv40ALg3WrV40Alg2WrV40C5C4G/Q2U/Ban4MBBCCVCC6G4C+10AQC26A) Bg4zh3C4WeAQFAACACAG24 (2012)/Ban4MBBCCVCC6G4C+10AQC26A) Bg4zh3C4WeAQFAACACAG24 (2012)/Ban4MBBCCVCCCCCCCCCCACA UA27C28acQf32ACC010A/2224Th11T11NW/076cQ1a+1A1A004,m174/15 4cQ2/m8c4m2A4Cman24Q24 (2012)/Ban4MBBCCVCCCCCCCCCACA *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBBCCVCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBBCCVCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBBCCVCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBBCCVCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBBCCVCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBBCCVCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBCCCCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBCCCCCCCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBCCCCCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBCCCCCCCCCCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBCCCCCCCCCCCCCCCCCCACAN *156aq(1795Ferder)/FINF0C24 (2012)/Ban4MBCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC	

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

Microsoft Active Directory Certificate Services – fixer-WIN-97Q5HOKP9IG-CA Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over

the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

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

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u> Paso 6. Una vez que solicita un certificado, obtiene opciones para **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 la CSR generada en la **solicitud de certificado codificado Base-64**. En la opción **Certificate Template:** desplegable, elija **Web Server** y haga clic en **Submit** como se muestra en la imagen.

crosoft Active Directory Certificate Services fixer-WIN-97Q5HOKP9IG-CA	Home							
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.								
ved Request:								
ie-64-encoded iffcate request IC or CS #10 or CS #7):								
tificate Template:								
Web Server								
ditional Attributes:								
Attributes:								
Submit >								

Paso 8. Una vez que haga clic en **Enviar**, tendrá la opción de seleccionar el tipo de certificado, seleccione **Base-64 codificado** y haga clic en **Descargar cadena de certificado** 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.							
ODER encoded or <a>Base 64 encoded							
Download certificate chain							

Paso 9. La descarga del certificado se ha completado para el servidor ISE. Puede extraer el

certificado, el certificado contendrá dos certificados, un certificado raíz y otro intermedio. El certificado raíz se puede importar bajo Administración > Certificados > Certificados de confianza > Importar como se muestra en las imágenes.

dentity 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	Click here to do wireless setup and visibility setup Do not show this again.
Deployment Licensing	gging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings	
0		
Certificate Management Trust	ted Certificates	
System Certificates 🥖 Ed	it 🕂 Import 🚱 Export 🗙 Delete 🔎 View	Show Al 🗾 🖌
Trusted Certificates	riendly Name	Valid From Expiration Date
ultulu Identity Services En		
cisco Identity Gervices En	Gine Home ► Context Visibility ► Operations ► Policy ► Administration ► Work C	Centers
System Identity Management	gement	Threat Centric NAC
Deployment Licensing		tings
	0	
- Certificate Management	Import a new Certificate into the Certificate Store	
	* Certificate File Choose file No file chosen	
System Certificates		
Trusted Certificates	Friendly Name EAP-TLS	<i>i</i>
OCCE Olivest Profile		
OCSP Client Profile	Trusted For: (j)	
Certificate Signing Requests	Trust for authentication within ISE	
Certificate Periodic Check Se	etti	
	Trust for client authentication and Syslog	1
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.

dentity Services Engine	Home	cy Administration Work C	Centers		License Warning 🔺 🧠 💿 🔿			
▼ System → Identity Management	Network Resources Device Portal Management px	ind Services + Feed Service + T	hreat Centric NAC		Click here to do wireless setup and visibility setup Do not show this again.			
Deployment Licensing - Certificate								
0	0							
- Certificate 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 CSF	Rs so that they may be signed by an externa	al authority. After a request has been signed, click "bind" to bind the request to the			
OCSP Client Profile	signed certificate issued by that authority. Once a CSR is	bound, it will be removed from this list.						
Certificate Signing Requests	PView Deport X Delete Bind Certificate				Show All *			
Certificate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group tag	Timestamp A Hos	ź.			
	ise#FAP Authentication	CN=ise c.com	2048	Mon. 9 3ul 2018 ise	Created by Paint X			

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 **Enviar** 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 Service Feed Service Threat Centric NAC	
Deployment Licensing - Certificate	s + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings	
Certificate Management	Bind CA Signed Certificate	
System Certificates Trusted Certificates	Certificate File Choose file No file chosen	
OCSP Client Profile	Friendly Name 3	
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	9
	Submit Cancel	

Paso 12. Para ver el certificado, navegue hasta **Administración > Certificados > Certificados del sistema** como se muestra en la imagen.

dentity Services Engine	Home + Context Visibility + C	perations + Policy •A	dministration > Work Centers			L	cense Warning 🔺 🔍 💿	4
System Identity Management	Network Resources Device Portal	Management pxGrid Service	s + Feed Service + PassiveID	Threat Centric NAC				
Deployment Licensing Certificates + Logging + Maintenance Upgrade Backup & Restore + Admin Access + Settings								
0								
Certificate Management	System Certificates 🛕 For dis	saster recovery it is recommende	d to export certificate and private key p	airs of all system certificates.				
Overview	🖊 Edit 🛛 🕂 Generate Self Signe	d Certificate 🛛 🕂 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 ser ficate - CN+SAML_ise.c.com 	m SAML		SAML_ise.c.com	SAML_ise.c.com	Wed, 11 Jul 2018	Thu, 11 Jul 2019 🧧	1
OCSP Client Profile	Intermediate	EAP Authentication, Admin, Portal	Default Portal Certificate Group (2)	ise.c.com	fixer-WIN-97Q5H0KP9IG-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 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 con 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 la 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	ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIsPJry
partificato request	aF412aLpmDFp1PfVZ3VaP60a/mej3IXh0RFxBUII
certificate request	weOhO6+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR
CMC or	dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyDZ3
PKCS #10 or	ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX
PKCS #7):	END CERTIFICATE REQUEST

Certificate Template:

	User	\$	
dditional Attribu	tes:		
Attributes:		11.	
		Submi	t >

Paso 3. A continuación, 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 portátil de windows.

Paso 4. Para importar el certificado, debe tener acceso 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 **Certificados**.
- 4. Seleccione Cuenta de computadora.
- 5. Seleccione Equipo local > Finalizar
- 6. Haga clic en Aceptar para salir de la ventana Complemento.
- 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 **Examinar**.

- 11. Seleccione .cer, .crt o .pfx que desea importar.
- 12. Haga clic en Abrir.
- 13. Haga clic en Next (Siguiente).
- 14. Seleccione Automatically select the certificate store basado en el tipo de certificado.
- 15. Haga clic en Finalizar y Aceptar

Una vez realizada la importación del certificado, debe configurar su cliente inalámbrico (windows desktop 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 en su lugar EAP-TLS. Haga clic en **EAP Wireless Profile**.

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

1
ς

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

Smart Card or other Certificate Properties		1
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 certific	ate	_
Connect to these servers (examples:srv1;srv2;.*\	.srv3\.com):	
Trusted Root Certification Authorities:		
Entrust.net Certification Authority (2048)		^
Equifax Secure Certificate Authority		
fixer-WIN-97Q5HOKP9IG-CA		
GeoTrust Global CA		
GeoTrust Primary Certification Authority		
GlobalSign		
GlobalSign		
GlobalSign Root CA		$\mathbf{\mathbf{v}}$
GlobalSign Root CA	>	~

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

2.1A settings	802.11 settings			
Specify a	authentication mode:			
User or	computer authentication	\sim	Save cr	edentials
Dele	te credentials for all user	S		
Enable s	ingle sign on for this net	work		
Perfo	orm immediately before u	iser logor	1	
O Perfo	orm immediately after us	er logon		
O Perfo Maximu	orm immediately after use m delay (seconds):	er logon	10	•
O Perfo Maximu Allov sign	orm immediately after use m delay (seconds): v additional dialogs to be on	displayed	10 during	single

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



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. El tipo EAP del cliente debe ser EAP-TLS. Esto significa que el cliente ha completado la autenticación, con el uso de EAP-TLS, ha obtenido la dirección IP y está listo para pasar el tráfico como se muestra en las imágenes.

_							
		CLIENT VIEW		0			
æ	Monitoring Network Summary Access Points Clients	GENERAL	User Name Administrator Host Name		CONNECTIVITY Start Association	Authentication DHCP Online	
	 Applications Rogues Access Points 	MAC Address Uptime	Unknown 34:02:86:96:2f:b7 Associated since 37 Seconds		TOP APPLICATIONS	Usage	se % Usage
	Clients	SSID	ME_EAP			No Data Available!	
	P Interferers	AP Name Nearest APs	₩AP442b.03a9.7f72 (Ch 56)				
	🔁 Wireless Dashboard	Device Type					
	AP Performance	Performance	Signal Strength: 0 dBm Signal Qua Speed: 0 Channel Width: 40 MHz	ality: 0 dB Connection			
	Client Performance	Capabilities	802.11n (5GHz) Spatial Stream: 0				
	P Best Practices	Cisco Compatible	Supported (CCX v 4)				
٥	Wireless Settings						
÷.	Management						
*	Advanced	MOBILITY STATE	(CAPWAP)	AP (FlexConnect)	Windless (802 11n (5GHz))	Client (VLAN1)	

æ	Monitoring Network Summary Access Points Clients O Applications	MOBILITY STATE W.C (LOCAL) 09_8P 107_2709.56 AIR-AP1832I-D-K9		AP (FlexConnect)	₩itgliges (852-19A (SGHz)) 	Client (VLAN1) 	
	r≮ Rogues	NETWORK & QOS			SECURITY & POLICY		
	Access Points	Description	Status		Description	Status	
	Clients	IP Address	10.127.209.55		Policy	RSN (WPA2)	
	D Interferers	IPv6 Address	fe80::2818:15a4:65f9:842		Cipher	CCMP (AES)	
	🔊 Wireless Dashboard	VLAN	1		Key Management	802.1x	
	AP Performance	Source Group Tag	N/A		EAP Type	EAP-TLS	
	Client Performance	Fastlane Client	No		ACL (IP/IPv6)	None/None	
	-	Mobility Role	Local		mDNS Profile	None	
	Y Best Practices	WMM	Supported		AAA Role	None	
۵	Wireless Settings	U-APSD	Disabled				
÷.	Management	QoS Level	Silver				
Ł	Advanced						
		CLIENT TEST					
		PING TEST	CONNECTION	EVENT LOG PAC	CKET CAPTURE		

Paso 2. A continuación se muestra el detalle del cliente de la CLI del controlador (salida recortada):

(Cisco Controller) > show client detail 34:02:86:9	96:2f:b7
Client MAC Address	34:02:86:96:2f:b7
Client Username	Administrator
AP MAC Address	c8:f9:f9:83:47:b0
AP Name	AP442b.03a9.7f72
AP radio slot Id	1
Client State	Associated
Client User Group	Administrator
Client NAC OOB State	Access
Wireless LAN Id	б
Wireless LAN Network Name (SSID)	ME_EAP
Wireless LAN Profile Name	ME_EAP
Hotspot (802.11u)	Not Supported
BSSID	c8:f9:f9:83:47:ba
Connected For	18 secs
Channel	56
IP Address	10.127.209.55
Gateway Address	10.127.209.49
Netmask	255.255.255.240
IPv6 Address	fe80::2818:15a4:65f9:842
More or (q)uit	
Security Policy Completed	Yes
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
ЕАР Туре	EAP-TLS

Paso 3. En ISE, navegue hasta Visibilidad de contexto > Terminales > Atributos como se muestra en las imágenes.

cise	la Ider	ntity Services Engin	е но	mo	- Context Visibility	 Operations 	Policy	+ Administration	Work Centers	
E	ndpoints	Network Devices								
E	Endpoints	> 34:02:86:96:2F:B	7							
	34:02	:86:96:2F:B7	Ø	3 🕅						
	Ę	MAC Address Username: Ad Endpoint Prof Current IP Ad Location:	: 34:02:86:9 dministrato ile: Intel-Der dress:	6:2F:B7 r@fixer.c vice	com					
		Attributes Authen	tication	Threat	s Vulnerabilitie	35				
	General	Attributes								
	Descript	ion								
	Static As	ssignment f	alse							
	Endpoin	t Policy I	ntel-Device							
	Static G	roup Assignment f	alse							
	Identity	Group Assignment F	Profiled							
1	Custom Attributes									
									¥ Filter	• • •
		Attribute Name			Attribute Val	ue				
	×	Attribute Name			Attribute Valu	0				
	No data found. Add custom attributes here.									
	Other A	ttributes								
	AAA-Se	rver		ise						
	AKI 88:20:a7:c9:		:c9:96:03:5a:26:58:1	d:67:58:83:71:e8:b	c:c6:6d:97:bd					
_	Airespace-Wian-Id 6									
	AllowedProtocolMatchedRule Dot1X									
	AuthenticationIdentityStore Internal User		Users							
	AuthenticationMethod x509_PKI		a							
	Authoriz	ationPolicyMatchedRu	lie	Basic_A	uthenticated_Access	1				

BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-21-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
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	12935 Supplicant stopped responding to ISE during
FailureReason	12935 Supplicant stopped responding to ISE during Profiled
FailureReason IdentityGroup InactiveDays	12935 Supplicant stopped responding to ISE during Profiled 0
FailureReason IdentityGroup InactiveDays IsThirdPartyDeviceFlow	12935 Supplicant stopped responding to ISE during Profiled 0 false
FailureReason IdentityGroup InactiveDays IsThirdPartyDeviceFlow Issuer	12935 Supplicant stopped responding to ISE during Profiled 0 false CN=fixer-WIN-97Q5HOKP9IG-CA\DC=fixerDC=co
FailureReason IdentityGroup InactiveDays IsThirdPartyDeviceFlow Issuer Issuer - Common Name	12935 Supplicant stopped responding to ISE during Profiled 0 false CN=fixer-WIN-97Q5HOKP9IG-CADC=fixerDC=cc fixer-WIN-97Q5HOKP9IG-CA
FailureReason IdentityGroup InactiveDays IsThirdPartyDeviceFlow Issuer Issuer - Common Name Issuer - Domain Component	12935 Supplicant stopped responding to ISE during Profiled 0 false CN=fixer-WIN-97Q5HOKP9IG-CA\DC=fixerDC=co fixer-WIN-97Q5HOKP9IG-CA
FailureReason IdentityGroup InactiveDays IsThirdPartyDeviceFlow Issuer Issuer - Common Name Issuer - Domain Component Key Usage	12935 Supplicant stopped responding to ISE during Profiled 0 false CN=fixer-WIN-97Q5HOKP9IG-CA\DC=fixerDC=co fixer-WIN-97Q5HOKP9IG-CA fixer, com
FailureReason IdentityGroup InactiveDays IsThirdPartyDeviceFlow Issuer Issuer - Common Name Issuer - Domain Component Key Usage Location	12935 Supplicant stopped responding to ISE during Profiled 0 false CN=fixer-WIN-97Q5HOKP9IG-CA\DC=fixerDC=co fixer-WIN-97Q5HOKP9IG-CA fixer, com 0, 2 Location#All Locations
FailureReason IdentityGroup InactiveDays IsThirdPartyDeviceFlow Issuer Issuer - Common Name Issuer - Domain Component Key Usage Location MACAddress	12935 Supplicant stopped responding to ISE during Profiled 0 false CN=fixer-WIN-97Q5HOKP9IG-CA_DC=fixer_DC=cc fixer-WIN-97Q5HOKP9IG-CA fixer, com 0, 2 Location#All Locations 34:02:86:96:2F:B7

MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
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	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.