Comprendre et configurer EAP-TLS avec un WLC et ISE

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales Flux EAP-TLS Étapes du flux EAP-TLS Configuration Contrôleur LAN sans fil Cisco ISE avec Cisco WLC Paramètres EAP-TLS Paramètres WLC sur ISE Créer un nouvel utilisateur sur ISE Certificat de confiance sur ISE **Client pour EAP-TLS** Télécharger le certificat utilisateur sur l'ordinateur client (Bureau Windows) Profil sans fil pour EAP-TLS Vérification Dépannage

Introduction

Ce document décrit comment configurer un réseau local sans fil (WLAN) avec 802.1X et le protocole d'authentification extensible EAP-TLS

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Processus d'authentification 802.1X
- Certificats

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- WLC 3504 version 8.10
- Identity Services Engine (ISE) version 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Flux EAP-TLS



Étapes du flux EAP-TLS

- Le client sans fil est associé au point d'accès. Le point d'accès ne permet pas au client d'envoyer des données à ce stade et envoie une demande d'authentification. Le demandeur répond alors avec une identité de réponse EAP. Le WLC communique ensuite les informations d'ID d'utilisateur au serveur d'authentification. Le serveur RADIUS répond au client avec un paquet de démarrage EAP-TLS. La conversation EAP-TLS commence à ce stade.
- 2. L'homologue renvoie une réponse EAP au serveur d'authentification qui contient un message d'échange « client_hello », un chiffre défini sur NULL
- 3. Le serveur d'authentification répond par un paquet de demande d'accès contenant :

TLS server_hello handshake message certificate server_key_exchange
certificate request
server_hello_done.

4. Le client répond par un message EAP-Response contenant :

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. Une fois que le client s'est authentifié avec succès, le serveur RADIUS répond par un Accesschallenge, qui contient le message « change_cipher_spec » et handshake finished.

6.Quand il reçoit ceci, le client vérifie le hachage afin d'authentifier le serveur radius.

7.Une nouvelle clé de chiffrement est dérivée dynamiquement du secret pendant la connexion TLS

8/9.EAP-Success est finalement envoyé du serveur à l'authentificateur qui est ensuite transmis au demandeur.

Àce stade, le client sans fil compatible EAP-TLS peut accéder au réseau sans fil.

Configuration

Contrôleur LAN sans fil Cisco

Étape 1. La première étape consiste à configurer le serveur RADIUS sur le WLC Cisco. Afin d'ajouter un serveur RADIUS, naviguez vers **Security > RADIUS > Authentication**. Cliquez sur **New** comme indiqué dans l'image.

	cisco	MONITOR	WLANS O	ONTROL	LER	WIREL	LESS SI	ECURITY	MANAGEMEN	NT C <u>O</u> MMA	NDS HELP			anaata
31	ecurity	RADIUS	Authenticat	tion Se	ervers									
	AAA General	Auth Ca	alled Station ID T	ype (AP Nam	e:SSII	D	¥						
	Authentication Use AES Key Wrap (Designed for Accounting MAC Delimiter Colon		FIPS custo	omers and	requires a key v	wrap complian	t RADIUS server))						
	Auth Cached Users Fallback	Framed	I MTU	(1300		•	5						
	Downloaded AVP TACACS+	Network User	Management	Tunne Proxy	Inde	er x	Server	Address(Ipv4/Ipv6)		Port	IPSec	Admin Status	
	Local Net Users				1		138.77.	0.84			1812	Disabled	Disabled	
	MAC Filtering				2		138.77.	0.83			1812	Disabled	Disabled	
	User Login Policies				3		138.77.	97.20			1812	Disabled	Disabled	
	AP Policies				4		138.77.	97.21			1812	Disabled	Disabled	
1	Password Policies				5	•	172.27.	1.71			1812	Disabled	Enabled	
ŀ	Local EAP				6	*	10.100.	120.41			1812	Disabled	Enabled	
	Advanced EAP													
Þ	Priority Order													
•	Certificate													
Þ	Access Control Lists													
•	Wireless Protection Policies													
Þ	Web Auth													
Þ	TrustSec													
	Local Policies													
Þ	Umbrella													
	Advanced													
H														

Étape 2. Ici, vous devez entrer l'adresse IP et le secret partagé <password> qui est utilisé afin de valider le WLC sur l'ISE. Cliquez sur **Apply** afin de continuer comme indiqué dans l'image.

ahaha					-		 	Save Configu	ration Ping	Logout B	efresh
cisco	MONITOR WLANS CONTROLLER	R WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP			U	er:admin(Read)	Write) 🔒 I	Home
Security	RADIUS Authentication Serve	ers > Edit							< Back	Appl	ily
 AAA General RADIUS Authentication Accounting Authentication Accounting Authentication Accounting Databack DAP Downloaded AVP TACACSE DAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrelia Advanced 	Server Index Server Address(Ipv4/Ipv6) Shared Secret Format Confirm Shared Secret Confirm Shared Secret Apply Cisco ISE Default settings Apply Cisco ISE Default settings Port Number Server Status Support for CoA Server Timeout Network User Management Management Management Tunnel Proxy Realm List PAC Provisioning IPSec Cisco ACA	7 10.106.35.67 ASCII ~ (Designed for FIPS custor (Designed for FIPS custor 1812 Enabled ~ S seconds Enable S seconds Enable Enable Enable Enable Enable	ners and requires a l	key wrap complia	nt RADIUS server)						G
					_						

Étape 3 : création d'un WLAN pour l'authentification RADIUS

Vous pouvez maintenant créer un nouveau WLAN et le configurer pour qu'il utilise le mode WPA entreprise, afin qu'il puisse utiliser RADIUS pour l'authentification.

Étape 4. Sélectionnez **WLANs** dans le menu principal, choisissez **Create New** et cliquez sur **Go** comme indiqué dans l'image.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECU	RITY MANAGEMENT C	COMMANDS HELP	Saye Configuration Ping Logout Refresh User:admin(ReadWrite) 🔥 Home
WLANs	WLANs			Entries 1 - 15 of 15
WLANS WLANS	Current Filter: None [Change Filter] [Clear F	liter]	Create New Y	•
Advanced	WLAN ID Type Profile Name	WLAN SSID	Admin Status Security Policies	

Étape 5. Attribuez un nom au nouveau WLAN **EAP-TLS**. Cliquez sur **Apply** afin de continuer comme indiqué dans l'image.

սիսիս					Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS	HELP	User:admin(ReadWrite) 🔒 Home
WLANs	WLANs > New				< Back Apply
 WLANS WLANS Advanced 	Type Profile Name SSID ID	WLAN V EAP-TLS EAP-TLS 3 V			

Étape 6. Cliquez sur **General** et vérifiez que le statut est **Enabled**. Les stratégies de sécurité par défaut sont l'authentification 802.1X et WPA2, comme illustré dans l'image.

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

Étape 7. À présent, accédez à **Security > AAA Servers** tab, sélectionnez le serveur RADIUS que vous venez de configurer et comme indiqué dans l'image.

սիսիս						Save Co	nfiguration Ping Logout Refre	sh
cisco	MONITOR WL	ANS CONTROLLER WIRELE	SS SECURITY MANAGEMEN	t commands help			User:admin(ReadWrite) 🔒 Hon	ne
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 vied					
	Server 1	Authentication Servers Enabled IP-10.106.35.67. Port:1812	Accounting Servers	EAP Parameters Enable				
	Server 2	None	None v					
	Server 3	None v	None v					
	Server 4	None v	None v					
	Server 5	None v	None v					
	Server 6	None	None v					
		Authorization ACA Server	Enabled					
	Server	None v	None v					

Note: Il est conseillé de vérifier que vous pouvez atteindre le serveur RADIUS à partir du WLC avant de continuer. RADIUS utilise le port UDP 1812 (pour l'authentification). Vous devez donc vous assurer que ce trafic n'est bloqué nulle part sur le réseau.

ISE avec Cisco WLC

Paramètres EAP-TLS

Pour créer la stratégie, vous devez créer la liste de protocoles autorisés à utiliser dans notre stratégie. Comme une stratégie dot1x est écrite, spécifiez le type EAP autorisé en fonction de la configuration de la stratégie.

Si vous utilisez la valeur par défaut, vous autorisez la plupart des types EAP pour l'authentification qui ne sont pas préférés si vous devez verrouiller l'accès à un type EAP spécifique.

Étape 1. Accédez à Policy > Policy Elements > Results > Authentication > Allowed Protocols et cliquez sur Add comme indiqué dans l'image.

dentity Services Engine	ome	Policy Administration Work Centers						
Authentication Authorization Profiling	Posture Client Provisioning Policy E	Ilements						
Dictionaries								
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	X Delete						
	Service Name	scription						
Profiling	Default Network Access De	Default Allowed Protocol Service						
▶ Posture								
Client Provisioning								

Étape 2. Dans cette liste de protocoles autorisés, vous pouvez entrer le nom de la liste. Dans ce cas, la case **Allow EAP-TLS** est cochée et les autres cases sont décochées comme illustré dans l'image.

dentity Services Engine	Home → Co	ontext Visibility	Operations	Policy	Administration	Work Centers
Authentication Authorization Profi	ing Posture (Client Provisioning				
Dictionaries Conditions - Resul	s					
G	Allowed Protoc	ole Convisoe List > 1	New Allowed Proto	ole Comio		
- Authentication	Allowed Protoc	otocols	New Allowed Proto	JUS Service	5	
Allowed Protocols	Name	EAP-TLS				
Authorization	Description				1	
▶ Profiling					2	
► Posture	 Allowed Pr 	otocols				
Client Provisioning	Auth	nentication Bypass	6			
		Process Host Look	(i) au			
	Auth	nentication Protoc	ols			
		Allow PAP/ASCII				
		Allow CHAP				
		Allow MS-CHAPv1				
		Allow MS-CHAPv2				
		Allow EAP-MD5				
	▼ 🗹	Allow EAP-TLS				
		Allow Authe	ntication of expired	certificates	to allow certificate rer	newal in Authorization Policy (i)
		Enable Stat	eless Session Resu	me		
		Session tick	time to 2		Hours	
		live Broactive of	accion ticket undate	uill ecour o	flor 10 % of Tin	no To Live has evoired
	_	Floaduve se	ession licket update	will occur a	10 % 01 11	ne to Live has expired
		Allow LEAP				
	- □	Allow PEAP				
		PEAP Inner Meti	nods			
		Allow EAP-I	MS-CHAPv2			
		Allow I	Password Change	Retries 1	(Valid Range 0 to 3	3)
		Allow EAP-	GTC			
		Allow I	Password Change	Retries 1	(Valid Range 0 to 3	3)
		Allow EAP-	TLS			
		Allow	Authentication of exp	ired certific	ates to allow certification	te renewal in Authorization Policy
		Require cry	ptobinding TLV 👔			

Paramètres WLC sur ISE

Étape 1. Ouvrez la console ISE et accédez à **Administration > Network Resources > Network Devices > Add** comme indiqué dans l'image.

deale Identity Services Engine	Home + Control Visibility + Operations + Policy +Admit	Interfeor Work Centers		Lixense Warning 🔺 🔍 😐 🔿				
Oysten + Identity Management Network Devices Network Devices	Network Resources + Device Potal Management prOrid Services	Feed Service Threat Centric NAC		Click here to ds wireless setup and visibility setup Do not show this again				
THERE YES AND A REAL YES AND A								
Network devices	Network Devices							
Default Device				Seaced 0 Tabel 2 🔮 쯝 🖕				
Device Security Settings	Note: Note: <th< td=""><td>Stor Al 🔹 😼</td></th<>	Stor Al 🔹 😼						
	Name a IP/Hask Profile Name	Location Type	Desigtion					

Étape 2. Entrez les valeurs indiquées dans l'image.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
System Identity Manageme	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	Click be
▼Network Devices Network De	vice Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	Olive He
	•	
Network Devices	Natwork Davices List > New Network Device	
Default Device	t Name Revealed	
Device Security Settings		
	Cesarijum	
	IP Address + *IP: 10.106.35.67 / 32	
	* Device Profile deficience + (P)	
	Model Name T	
	Software Version	
	* Network Device Group	[
	Location All Locations Set To Default	
	IPSEC Is IPSEC Device O Set To Default	
	Device Type All Device Types 📀 Set To Default	
	RADIUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS	
	* Shared Secret Show	
	Use Second Shared Secret 🗌 @	
	Show	
	CoA Port Set To Default	
	RADIUS DTLS Settings @	

Créer un nouvel utilisateur sur ISE

Étape 1. Accédez à **Administration > Identity Management > Identities > Users > Add** comme indiqué dans l'image.

승규는 Identity Services Engine	Norme + Control Voldally + Connections + Falsy + Approximations + Wark Contents	License Warning 🛦 🔍 🔍 🔘										
+ System + Identity Management	Nithouth Resources Device Portal Management public Service + Feed Service + Thread Centric NAC	Click here to do wineless setup and visibility setup Do not show this equin. X										
Identifies Oroups External Ident	etities Groups Enternal identity Sources I electrica + Settings											
0	Reference Learners											
Users	INCLUSION OF A CONTRACT OF	Delener I Trar I 👙 🏭 🔒										
Latest Manual Network Scan Results	/ bit - spådd	thew Al * 75										
	Status Name Description Prist Name Enal Address User Identity Groups Admin											

Étape 2. Entrez les informations comme indiqué dans l'image.

dentity Services	s Engine	Home	d Visibility	Operations	Policy	▼ Admi	inistration	• Work Cen	ters
► System - Identity N	lanagement +	Network Resources	Device	Portal Management	pxGrid S	Services	Feed Ser	vice + Thre	at Centric NAC
◄ Identities Groups	External Identity	Sources Identity	Source Sequ	uences • Settings					
	G								
Users		Network Access L	sers List > N	lew Network Access	User				
Latest Manual Network Sca	an Results	▼ Network A	cess user						_
		* Name bha	ti						
		Status 🔽	Enabled 👻]					
		Email 🦳							
		▼ Password	s						
		Password Tv	e: Intern	al Users	Ŧ				
			Passw	rord		Re-Enter I	Password		
		* Login Pass	word						Generate Password
		Enable Pase	word			[-		Generate Password
		Endble Fass							Generate Password
		▼ User Info	mation						
		First Name	+I						
		Last Name	17 k = 4?						
		 Account C 	ptions						
			Descr	ription					
		Change pass	word on next	t login 🛛					
		▼ Account C	isable Poli	су					
		Disable	account if da	te exceeds 2018-0	2-17		(УУУ)	/-mm-dd)	
		▼ User Grou	ps						
		Select an ite	m	o - 4	F				
		Submit	ncel						
		Subjut	incer						

Certificat de confiance sur ISE

Étape 1. Accédez à Administration > System > Certificates > Certificate Management > Trusted certificates.

Cliquez sur **Import** afin d'importer un certificat vers ISE. Une fois que vous avez ajouté un WLC et créé un utilisateur sur ISE, vous devez faire la partie la plus importante de EAP-TLS qui est de faire confiance au certificat sur ISE. Pour cela, nous devons générer de la RSE.

Étape 2. Accédez à Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR) comme indiqué dans l'image.

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						

Étape 3. Afin de générer CSR, naviguez vers **Usage** et à partir du **ou des certificats sont utilisés pour les** options déroulantes sélectionnez **EAP Authentication** comme indiqué dans l'image.

cisco Identity Services Engine	Home	tions + Policy + Administr	tion Work Centers		License Warning 🔺	्	9 0	- Ö
▼ System → Identity Management	Network Resources Device Portal Man	agement pxGrid Services + Fe	ed Service + Threat Centric NAC					
Deployment Licensing - Certificate	is → Logging → Maintenance Upgrade	+ Backup & Restore + Admir	Access + Settings					
0								
- Certificate Management	Certificate Signing Request							
System Certificates	Certificate types will require different e	extended key usages. The list below	outlines which extended key usages are requi	ed for each certificate type:				
To start Cartificates	ISE Identity Certificates:							
OCSD Client Broßie	 Multi-Use (Admin, EAP, Portal Admin - Server Authentication 	, pxGrid) - Client and Server Authent	cation					
Cartificate Signian Requeste	EAP Authentication - Server A	uthentication						
Certificate Deriver Chark Setti	 DTLS Authentication - Server . Portal - Server Authentication 	Authentication						
Contrate Period Coneta Sett	 pxGrid - Client and Server Aut 	hentication						
Certificate Authority	 SAML - SAML Signing Certific 	ate						
)	ISE Certificate Authority Certificate	s:						
	 ISE Root CA - This is not a signification of the second sec	ning request, but an ability to genera an Intermediate CA Sicning Request	te a brand new Root CA certificate for the ISE	CA functionality.				
	Renew ISE OCSP Responder	Certificates - This is not a signing re	quest, but an ability to renew the OCSP respo	der certificate that is signed by the				
	ISE Root CAUSE Intermediate	CA.						
	Usage		_					
	Certificate(s) will be used for EAP	Authentication						
	Allow Wildcard Certificates)						
	Node (=)							
	Generate CSR's for these Nodes:							
	Node	CSR Friendly	Name					
	✓ labise	labise#EAP A	uthentication					

Étape 4. Le CSR généré sur ISE peut être affiché. Cliquez sur View comme indiqué dans l'image.



Étape 5. Une fois la CSR générée, recherchez le serveur AC et cliquez sur **Request a certificate** (**Demander un certificat)** comme indiqué dans l'image :

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

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: Request a certificate

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

Étape 6. Une fois que vous avez demandé un certificat, vous obtenez les options **User Certificate** et **advanced certificate request**, cliquez sur **advanced certificate request** comme indiqué dans l'image.

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

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request

Étape 7. Collez le CSR généré dans la **demande de certificat codé en base 64**. À partir du **modèle de certificat :** , choisissez **Web Server** et cliquez sur **Submit**, comme illustré dans l'image.

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 >]

Étape 8. Une fois que vous cliquez sur **Submit**, vous obtenez l'option pour sélectionner le type de certificat, sélectionnez **Base-64 encoded** et cliquez sur **Download certificate chain** comme indiqué dans l'image.

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									

Étape 9. Le téléchargement du certificat est terminé pour le serveur ISE. Vous pouvez extraire le certificat, qui contient deux certificats, un certificat racine et un certificat intermédiaire. Le certificat racine peut être importé sous Administration > Certificates > Trusted certificates > Import comme indiqué dans les images.

dentity Services Engine	Home + Context Visibility + Operations + Policy	- Administrat	on Work Centers				Lic	cense Warning 🔺 🔍	0 0	•
System Identity Management	Network Resources	d Services + Fe	ed Service + Threat Centr	tic NAC		Cic	chere to do wireless setu	p and visibility setup Do n	ot show this again.	×
Deployment Licensing - Certificates	Logging → Maintenance Upgrade → Backup & F	testore + Admin	Access + Settings							
0										
Certificate Management	Trusted Certificates									_
System Certificates	/ Edit -Import Export X Delete View							Show All	* *	ő
Trusted Certificates	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date		

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	
Deployment Licensing - Certificat	as > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings	
Certificate Management	Import a new Certificate into the Certificate Store	
System Certificates		_
Trusted Certificates	Friendly Name EAP-TLS	(i)
OCSP Client Profile	Trusted For: (j)	
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	

Étape 10. Une fois que vous avez cliqué sur **Submit**, le certificat est ajouté à la liste des certificats de confiance. En outre, le certificat intermédiaire est nécessaire pour établir une liaison avec CSR, comme illustré dans l'image.

dentity Services Engine	Home Context Visibility Operations Poli	cy Administration + Work C	Centers		License Warning 🔺 🔍 😑 💿 🔿
System Identity Management	Network Resources Device Portal Management pxG	ind Services + Feed Service + T	hreat Centric NAC		Clink have to do wirelass sature and visibility sature Do not show this again
Deployment Licensing - Certificate	es + Logging + Maintenance Upgrade + Backup &	Restore + Admin Access + Sett	ings		
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	is so that they may be signed by an external	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 i	bound, it will be removed from this list.			
Certificate Signing Requests	PView Export X Delete Bind Certificate				Show All 🔻 😽
Certificate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group tag	Timestamp 🔺 Host	1
	ise#EAP Authentication	CNwise c.com	2048	Mon. 9 Jul 2018 ise	Created by Paint X

Étape 11. Une fois que vous avez cliqué sur **Lier le certificat**, il y a une option pour choisir le fichier de certificat enregistré sur votre bureau. Accédez au certificat intermédiaire et cliquez sur **Submit** comme indiqué dans l'image.

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 - Certificate	es Logging Maintenance Upgrade Backup & Restore Admin Access Settings
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

Étape 12. Pour afficher le certificat, accédez à **Administration > Certificates > System Certificates** comme indiqué dans l'image.

cisce Identity Services Engine	Home	Context Visibility Operation	s → Policy - Ad	ministration				License Warning 🔺	۹. 0	1 L
System Identity Management	Network	Resources	ement pxGrid Services	Feed Service PassiveID	Threat Centric NAC					
Deployment Licensing - Certificate	is → Log	gging + Maintenance Upgrade	Backup & Restore	Admin Access + Settings						
0		0.117								
 Certificate Management 	Syste	m Certificates 🛕 For disaster re-	covery it is recommended	to export certificate and private key p	airs of all system certificates.					
Overview	/ E	dit 🛛 🕂 Generate Self Signed Certific	ate 🕂 Import 🚱	Export X Delete View						
System Certificates		Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration	Date	
Endpoint Certificates	▼ ise									
Trusted Certificates	0	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	2
OCSP Client Profile		intermediate	EAP Authentication, Admin, Portal	Default Portal Certificate Group ①	ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Ju	2020	
Certificate Signing Requests										
Certificate Periodic Check Setti										
Certificate Authority										

Client pour EAP-TLS

Télécharger le certificat utilisateur sur l'ordinateur client (Bureau Windows)

Étape 1. Pour authentifier un utilisateur sans fil via EAP-TLS, vous devez générer un certificat client. Connectez votre ordinateur Windows au réseau afin de pouvoir accéder au serveur. Ouvrez un navigateur Web et entrez l'adresse suivante : <u>https://sever ip addr/certsrv :</u>

Étape 2. Notez que l'autorité de certification doit être identique à celle avec laquelle le certificat a été téléchargé pour ISE.

Pour cela, vous devez rechercher le même serveur AC que celui que vous avez utilisé pour télécharger le certificat pour le serveur. Sur la même autorité de certification, cliquez sur **Demander un certificat** comme précédemment fait, mais cette fois vous devez sélectionner **User** comme modèle de certificat comme indiqué dans l'image.

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 (CMC or	ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIsPJry aF412aLpmDFp1PfVZ3VaP6Oa/mej3IXh0RFxBUII weOhO6+V+eh71jeTgiwzEZGr/ceYJIakco5zLjgR
PKCS #10 or PKCS #7):	dD7LeujkxF1j3SwvLTKLDJq+00VtAhrx1p1PyDZ3 ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX END CERTIFICATE REQUEST

Certificate Template:

oertimente remp	uto.		_
	User	٥	
Additional Attrib	utes:		·
Attributes:		11.	
		Subm	it >

Étape 3. Cliquez ensuite sur **télécharger la chaîne de certificats** comme cela a été fait précédemment pour le serveur.

Une fois que vous obtenez les certificats, suivez ces étapes afin d'importer le certificat sur l'ordinateur portable Windows :

Étape 4. Pour importer le certificat, vous devez y accéder à partir de la console MMC (Microsoft Management Console).

- 1. Afin d'ouvrir la MMC naviguez à Démarrer > Exécuter > MMC.
- 2. Accédez à Fichier > Ajouter/Supprimer un composant logiciel enfichable
- 3. Double-cliquez sur Certificats.
- 4. Sélectionnez Compte d'ordinateur.
- 5. Sélectionnez Ordinateur local > Terminer
- 6. Cliquez sur **OK** afin de quitter la fenêtre du composant logiciel enfichable.
- 7. Cliquez sur [+] en regard de Certificats > Personnel > Certificats.
- 8. Cliquez avec le bouton droit sur Certificates et sélectionnez All Tasks > Import.
- 9. Cliquez sur Next (Suivant).
- 10. Cliquez sur Browse.

- 11. Sélectionnez le fichier .cer, .crt ou .pfx que vous souhaitez importer.
- 12. Cliquez sur Open.
- 13. Cliquez sur **Next** (Suivant).
- 14. Sélectionnez Sélectionner automatiquement le magasin de certificats en fonction du type de certificat.
- 15. Cliquez sur **Terminer et sur OK**

Une fois l'importation du certificat terminée, vous devez configurer votre client sans fil (bureau Windows dans cet exemple) pour EAP-TLS.

Profil sans fil pour EAP-TLS

Étape 1 : modification du profil sans fil créé précédemment pour le protocole PEAP (Protected Extensible Authentication Protocol) afin d'utiliser le protocole EAP-TLS à la place Cliquez sur **Profil sans fil EAP**.

Étape 2. Sélectionnez **Microsoft : Carte à puce ou autre certificat** et cliquez sur **OK** affiché dans l'image.

1
`

Étape 3. Cliquez sur **settings** et sélectionnez le certificat racine émis à partir du serveur AC, comme indiqué dans l'image.

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	

Étape 4. Cliquez sur **Advanced Settings** et sélectionnez **User or computer authentication** dans l'onglet 802.1x settings comme indiqué dans l'image.

o Li Li Coo Con 195	802.11 settings		
Specify a	authentication mode:		
User or	computer authentication	n ~ Save	credentials
Dele	te credentials for all use	rs	
Enable s	ingle sign on for this ne	twork	
Perfo	orm immediately before	user logon	
	orm immediately after us	ser logon	
O Perfo Maximu	o <mark>rm immediately after us</mark> m delay (seconds):	ser logon	•
O Perfo Maximu Allov sign	orm immediately after us m delay (seconds): v additional dialogs to be on	10 10 e displayed durin	g single

Étape 5. Maintenant, essayez de vous reconnecter au réseau sans fil, sélectionnez le profil correct (EAP dans cet exemple) et **Connect**. Vous êtes connecté au réseau sans fil comme illustré dans l'image.

	(î.	EAP Connec	ted, secu	red		
	(i,	blizzaro Secureo	l-legacy d			
	(k)	blizzaro Secure	d d			
	°C.	interne Open				
	((,	dot1x_ Secure	test d			
	((,	JioPriv Secure	ateNet d, Hotspo	ot 2.0		
	(1.	mac_fi Secure	lter d			
	Net Cha	twork & nge setting	Internet si ps, such as m	ettings aking a conr	ection m	eterec
	ſā.		أ	¢j) Mobile		
1	Wi-F	1	Airplane m	ode hotspo	,t	

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. L'état du gestionnaire de stratégies client doit être **RUN**. Cela signifie que le client a terminé l'authentification, obtenu l'adresse IP et est prêt à transmettre le trafic affiché dans l'image.

Statistics CDP	Client Properties			
			AP Properties	
Roques	MAC Address	34:02:86:96:2f:b7	AP Address	00:d7:8f:52:db:a0
Redundancy	IPv4 Address	10.106.32.239	AP Name	Alpha2802_3rdfloor
Clients	IPv6 Address	fe80::2818:15a4:65f9:842,	АР Туре	802.11bn
Sleeping Clients			AP radio slot Id	0
Multicast			WLAN Profile	EAP
Applications			WLAN SSID	EAP
Lync			Data Switching Central	
ocal Profiling			Authentication Central	
local Profiling			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	. 0
	Address	N/A	WEP State	WEP Enable
	Mobility Move Count	0		
	Policy Manager State	RUN	Lync Properties	
	Management Frame Protection	No	Lync State	Disabled

Étape 2. Vérifiez également la méthode EAP correcte sur le WLC dans la page de détails du client, comme illustré dans l'image.

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	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	

Étape 3. Voici les détails du client de l'interface de ligne de commande du contrôleur (résultats écrêtés) :

(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

WPA2	
802.1x	
CCMP-128	(AES)
No	
No	
EAP-TLS	
	WPA2 802.1x CCMP-128 No NO EAP-TLS

Étape 4. Sur ISE, accédez à **Context Visbility > End Points > Attributes** comme indiqué dans les images.

	Home Context Visibil	ty Operations	Policy Admi	inistration	Work Centers	
Endpoints Network Devices						
Endpoints > 34:02:86:96:2F:B7						
34:02:86:96:2F:B7	168					
MAC Address: 34:02 Username: Administ	::86:96:2F:B7 trator@fixer.com					
Endpoint Profile: Inte Current IP Address:	I-Device					
Location:	_					
Attributes Authentication	Threats Vulnerat	lites				
General Attributes						
Description						
Static Assignment false						
Endpoint Policy Intel-De	vice					
Static Group Assignment false						
Identity Group Assignment Profiled						
6						
Custom Attributes						
					🝸 Filter 👻 📢	۶-
Attribute Name	Attribute	Value			▼ Filter - K)
Attribute Name × Attribute Name	Attribute	Value			¥ Filter - K	}-
Attribute Name Attribute Name No data found. Add custom attribute	Attribute Attribute	Value			¥ Filter - K) -
Attribute Name Attribute Name No data found. Add custom attribute	Attribute Attribute tes here.	Value			¥ Filter - K	}-
Attribute Name Attribute Name No data found. Add custom attribute Other Attributes	Attribute Attribute	Value			¥ Filter - K	}-
Attribute Name Attribute Name No data found. Add custom attribute Other Attributes AAA-Server	Attribute Attribute tes here.	Value			Ţ Filter ◄ K	}-
Attribute Name Attribute Name No data found. Add custom attribute Other Attributes AAA-Server AKI	Attribute Attribute tes here. Ise 88:20:a7:c9:96:03:5a:26:58	Value laiue fd:67:58:83:71:e8:bc:c6:6	d:97:bd		¥ Filter - K	}-
Attribute Name × Attribute Name No data found. Add custom attributes Other Attributes AAA-Server AKI Airespace-Wlan-Id	Attribute Attribute tes here.	Value Ialue 1d:67:58:83:71:e8:bc:c6:6	d:97:bd		¥ Filter - K	}-
Attribute Name × Attribute Name No data found. Add custom attributes Other Attributes AAA-Server AKI Airespace-Wlan-Id AllowedProtocolMatchedRule	Attribute Attribute Attribute tes here.	Value talue fd:67:58:83:71:e8:bc:c6:6	d:97:bd		Ţ Filter → K	}-
Attribute Name × Attribute Name No data found. Add custom attributes Other Attributes AAA-Server AKI Airespace-Wlan-Id AllowedProtocolMatchedRule AuthenticationIdentityStore	Attribute Attribute Attribute Attribute Attribute See 88:20:a7:c9:96:03:5a:26:58 5 Dot1X Internal Users	Value falue fd:67:58:83:71:e8:bc:c6:6	d:97:bd		Ţ Filter → K	}-

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

	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

Dépannage

Aucune information spécifique n'est actuellement disponible pour le dépannage de cette configuration.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.