Comprendre et configurer EAP-TLS avec Mobility Express et ISE

Contenu

Introduction Conditions préalables Conditions requises **Components Used** Informations générales Flux EAP-TLS Étapes du flux EAP-TLS Configuration **Cisco Mobility Express ISE avec Cisco Mobility Express** Paramètres EAP-TLS Paramètres Mobility Express 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 la sécurité 802.1x dans un contrôleur Mobility Express. Ce document explique également l'utilisation du protocole EAP (Extensible Authentication Protocol) - TLS (Transport Layer Security).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration initiale de Mobility Express
- 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 5508 version 8.5
- Identity Services Engine (ISE) version 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 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

- 1. Le client sans fil est associé au point d'accès (AP).
- 2. Le point d'accès n'autorise pas le client à envoyer des données à ce stade et envoie une demande d'authentification.
- 3. Le demandeur répond ensuite avec une identité de réponse EAP. Le WLC communique ensuite les informations d'ID utilisateur au serveur d'authentification.
- 4. Le serveur RADIUS répond au client avec un paquet de démarrage EAP-TLS. La conversation EAP-TLS commence à ce stade.
- 5. L'homologue renvoie une réponse EAP au serveur d'authentification qui contient un message de connexion « client_hello », un chiffre défini sur NULL.
- 6. Le serveur d'authentification répond par un paquet Access-Challenge qui contient :

TLS server_hello handshake message certificate server_key_exchange certificate request server_hello_done.

7. Le client répond avec un message de réponse EAP qui contient :

Certificate ¬ 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. Une fois le client authentifié, le serveur RADIUS répond avec un défi d'accès, qui contient le message « change_cipher_spec » et le message de fin de la connexion. À la réception de ce message, le client vérifie le hachage afin d'authentifier le serveur RADIUS. Une nouvelle clé de chiffrement est dérivée dynamiquement du secret pendant la connexion TLS.
- 9. Àce stade, le client sans fil compatible EAP-TLS peut accéder au réseau sans fil.

Configuration

Cisco Mobility Express

Étape 1. La première étape consiste à créer un WLAN sur Mobility Express. Afin de créer un WLAN, accédez à WLAN > Add new WLAN comme indiqué dans l'image.



Étape 2. Une nouvelle fenêtre contextuelle apparaît lorsque vous cliquez sur **Ajouter un nouveau WLAN**. Afin de créer un nom de profil, accédez à **Ajouter un nouveau WLAN > Général** comme indiqué dans l'image.

B	Monitoring	8	Cisco Aironet 1830 Series Mobility Express							A	٩	8	Ħ		٥
\$	Wireless Settings														
	🖬 Access Points	2		e WLANs 5											
	📽 WLAN Users				Add new WLAN										
	📽 Guest WLANs				General WLAN Security	VLAN & Firewall Traf	fic Shaping								
	DHCP Server		Add new WLAN												
÷.	Management			Active	WLAN ID	6	•	Policy	Radio Policy						
Ł	Advanced	C	×	Enabled	Profile Name *	ME_EAP				ALL					
		C C C	×	Enabled	SSID *	ME EAP	-	rsonal							
		8	×	Enabled	Admin State	Enabled		rsonal							
		ß	×	Enabled	Padio Paliou			rsonal		2.4	GHz only				
		C	×	Enabled	Broadcast SSID	ALL	••••			ALL					
					Local Profiling										
						@ Apply	Cancel								

Étape 3. Configurez le type d'authentification en tant que WPA Enterprise pour 802.1x et configurez RADIUS Server sous **Ajouter un nouveau WLAN > WLAN Security** comme indiqué dans l'image.

\$	Monitoring	8	Cisco Aironet 1830 Series Mobility Express							Q	A	٩	B	#		٥
\$	Wireless Settings				Add now W	LAN										
	🖆 Access Points			WLANS 5	Add new W	Add new WLAN										
	📽 WLAN Users				General WLAN Security VLAN & Firewall Traffic Shaping											
	📽 Guest WLANs															
	OHCP Server		Guest Network													
÷	Management			Active	Security Type of Open is not allowed Policy when MAC Filtering is enabled.				Policy	Radio Policy						
Ł	Advanced	ß	×	Enabled	Sec	curit	ty Type WPA2 Enterprise 🔻				ALL					
		C C C	×	Enabled	Authentication Server External Radius				5 GHz only 5 GHz only 5 GHz only 2.4 GHz only							
		ß	×	Enabled	rsonal											
		ß	×	Enabled	Add RADIUS Authentication Server											
		C	×	Enabled	Stat	te	Server IP Address	Port			ALL					
					External Radius co WLANs	onfigu	wration applies to all O Apply	Cancel								

Étape 4. Cliquez sur **Add RADIUS Authentication Server** et indiquez l'adresse IP du serveur RADIUS et du secret partagé qui doit correspondre exactement à ce qui a été configuré sur ISE, puis cliquez sur **Apply** comme indiqué dans l'image.

B	Monitoring	Cisco Aironet 1830 Series Mobility Express		Q	A	٩	Ħ	\$
\$	Wireless Settings	WLAN CONFIGURATION						
	헬 Access Points 答 WLAN Users	Add new WLAN	ation Server.					
	Guest WLANs	Server Index 1						
ġ.	Management	Add new WLAN State Enable Active Server IP Address	s •		Rad	io Policy		
*	Advanced	Image: Confirm Shared Secret Image: Confirm Shared Secret	rsonal		ALL 5 GI 5 GI	iz only		
		Image: Show Password Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password Image: Show Password	rsonal		5 GI	Hz only GHz only		
		Server Timeout 5	Seconds		ALL			
		External Redux configuration applies to WLANS	Cancel					

ISE avec Cisco Mobility Express

Paramètres EAP-TLS

Pour créer la stratégie, vous devez créer la liste de protocoles autorisée à utiliser dans votre stratégie. Étant donné qu'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, ce qui peut ne pas être préférable si vous devez verrouiller l'accès à un type EAP spécifique.

Étape 1. Accédez à Stratégie > Eléments de stratégie > Résultats > Authentification > Protocoles autorisés et cliquez sur Ajouter comme indiqué dans l'image.

Hule Identity Services Engine	ome Context Visibility Operations Policy Administration Work Centers
Authentication Authorization Profiling	Posture Client Provisioning Policy Elements
Dictionaries Conditions Results	
Ø	
✓ 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	

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

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 Convisos 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)

Paramètres Mobility Express sur ISE

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

-thulte Identity Services Engine	Home	rations + Policy + Administration	► Work Centers		License Warning 🔺 🧠 😐 🗴 🔿
System Hentity Management	Network Resources Device Portal Ma	anagement pxGrid Services + Feed	Service + PassiveID + Threat Centric NAC		
Network Devices Network Device 0	roups Network Device Profiles Externa	al RADIUS Servers RADIUS Server Se	quences NAC Managers External MDM + Lo	cation Services	
0					
Network devices	Network Devices				
Default Device					Selected 0 Total 1 😵 🏭 🖕
	/Edit 🕂 Add 🖓 Duplicate 🛞	Import 🚯 Export 🔹 🕲 Generate PAC	X Delete 👻		Show All 👻
	Name A IP/Mask	Profile Name I	ocation Type	Description	
	Name IP/Mask	Profile Name I	Location Type	Description	

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

<pre>istant backage is intoon Decorating is Date Tatat Management politik Barviss is Plasamb - That Latent Mudi intoon Devices Tatation Decorating is intoon Decorating is Dated Tatations is NGUS Server Sequences INGO Management Each MUGI + Location Services Termine Tatations Termine Termine Tatations Termine Termine Tatations Termine</pre>	dentity Services Engine	Home Context Visibility Operations Policy -Administration Work Centers	License Warning 🔺	۹, ۲	1 0
	System Identity Management	Network Resources + Device Portal Management pxGrld Services + Feed Service + PassiveID + Threat Centric NAC			
<pre>source comparison of the set of the set</pre>	Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services			
Nextor devices Defut Devices Image: Control of the co		2			
bried beree	Network devices	Network Devices Lin > New Network Devices			
RADIUS Authentication Settings Enable Authentication Settings Protocol RADIUS * Shared Secret * Shared Secret * Shared Secret * Shared Secret * Rey Input Format * ASCII Key Input Format * ASCII Key Input Format * ASCII Too Set To Default	Default Device	Network Device Type Al Device Types Set To Default. Location Set To Default.	⊚ •	I	
Enable Authentication Settings Protocol RADIUS Shared Secret Enable KeyWrap Key Encryption Key Show Key Encryption Key Show Key Input Format ASCII HEXADECIMAL CoA Pot T700 Set.To Default		RADIUS Authentication Settings			
		Enable Authentication Settings Protocol RADIUS Shared Secret Enable KeyWrap Rey Show Ney Enable KeyWrap Ney Enable Key Show Ney Input Format CoA Port T200 Set To Default:			

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

Certificat de confiance sur ISE

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

Cliquez sur **Import** afin d'importer un certificat dans 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 d'approuver le certificat sur ISE. Pour cela, vous devez générer CSR.

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



Étape 3. Afin de générer CSR, accédez à **Utilisation** et à partir du **ou des certificats seront utilisés pour** les options de liste déroulante sélectionnez **Authentification EAP** comme indiqué dans

l'image.



Étape 4. La CSR générée sur ISE peut être affichée. Cliquez sur **Affichage** comme indiqué dans l'image.

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 PassiveID Threat Centric NAC	
Deployment Licensing - Certificate	es + Logging + Maintenance Upgrade Backup & Restore + Admin Access + Settings	
0		
- Certificate Management	Certificate Signing Requests	
Overview	Generate Certificate Signing Requests (CSR)	
System Certificates	A Certificate Signing Requests (CSRs) 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. Click "export" to download one or more CSRs so that they may be signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority.	ernal authority. After a request has been signed, click "bind" to bind the request to the
Endpoint Certificates	agried caranaale issued of stat addrardy. Once a color	
Trusted Certificates	View Debeort X Delete Bind Certificate CSR Details CSR Contents	Show All 💌 🔽
OCSP Client Profile	Elevidy Name Elevidy Name MICVCCAVCAD0xFDESMBAGAUEAvM3xXILmMv/29tMIBIANBokobi/09w0B	Host
Certificate Signing Requests	self EAP Authentication AQEFAAOCAQ8AMIIBCpXCAQEA0F7/HuooCAOS/Fkwct2NP2+komP9+jHX0IMgab WP8.454/82/0F/v1845FUXcminths.tmC2xmannofba328m/5x2xekp50/03	<u>86</u>
Certificate Periodic Check Setti	4v8HXglcvy+zgMXJUSKJWKZWIWTXMQbTat+S28H(Qtmm0Qv68qQuD4kp3 6v7202V21000000000000000000000000000000000	
Certificate Authority	a)/27mk2531mm80/z048pcze08ii.0728Bchv1/shj5578m/0799652kmBj2 9km250cg/02963ack1efc47bchv798c31bch2058kg1020A98cg102V478c21 hwtMQc0MY+V20A1BgN470EEBA4CBa4Hg70780208F0205455548cB1020438cg102V478bg CLV2x2km80A3LUBJQ2MA4CCCEAReby170520keEJL0288BcQ14262ac80B005YcjW LKV2E28bcg506cB102V25550cEJL02958F02149240205457c3548cB10297cjW155 4sQUTm8cm9/54A0cmae/g02cL+95gWmLa2X1H9/mc5002U54727U3U2CL4201 wPc2WB0++V96E29ke9c02BcH24QQ425EB28bs1572v47hrs57cas5mA3A6 1E6aj1179F8d94v1/EP16G2Ea3W}/sk0ze453725+817(K54cah6ach1C+87YU AV/97V102U1CL41+ku62BF8A9W18EJ4240297bgAs1A6LQ== END CERTIFICATE REQUEST	
	Core	

Étape 5. Une fois le CSR généré, recherchez le serveur AC et cliquez sur **Demander un certificat** comme indiqué dans l'image :



Étape 6. Une fois que vous avez demandé un certificat, vous obtenez des options pour **le certificat utilisateur** et la **demande de certificat avancée**, cliquez sur **demande de certificat avancée** 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 la CSR générée dans la **demande de certificat codée Base-64**. Dans l'option **Modèle de certificat :** déroulante, sélectionnez **Serveur Web** et cliquez sur **Envoyer** comme indiqué dans l'image.

osoft 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.										
d Request:										
84-encoded cate request or \$#10 or \$#7):										
ficate Template:										
Web Server 0										
ilonal Attributes:										
Attributes:										
Submit >										

Étape 8. Une fois que vous avez cliqué sur **Soumettre**, vous avez la possibilité de sélectionner le type de certificat, sélectionnez **Codé Base-64** et cliquez sur **Télécharger la chaîne de certificats** 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, le certificat contient deux certificats, un certificat racine et un autre certificat intermédiaire. Le certificat racine peut être importé sous Administration > Certificats > Certificats approuvés > Importer comme indiqué dans les images.

dentity Services Engine	Home	ibility + Operations	Policy Administr	ation + Work Centers					License Warning 🔺	9 0 0 0
System Identity Management	Network Resources	Device Portal Managemen	nt pxGrid Services + F	eed Service + Threat	Centric NAC			Click here to do wireles	is setup and visibility setup	Do not show this again. ×
Deployment Licensing - Certificates	Logging Maint	tenance Upgrade + B	Backup & Restore + Adm	in Access						
0										
 Certificate Management 	Trusted Certificat	es								
System Certificates	/ Edit -Import	Export XDelete	₽View						Show All	- 8
Trusted Certificates	Friendly Name		 Status 	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	
dentity Service	s Engine	Home ► C	Context Visibility	 Operations 	s Folicy	- Adminis	tration • Work	Centers		
- System → Identity N	Management	Network Reso	urces + Device	e Portal Manage	ment pxGrid	Services +	Feed Service +	Threat Centric	NAC	
Deployment Licensin	g - Certificat	es + Logging	 Maintenance 	e Upgrade	Backup & Re	estore + Adr	min Access	ettings		
	G									
- Certificate Managemer	at	Import a r	new Certificat	te into the C	ertificate St	ore				
· Certificate Managemen			Γ.							
System Certificates			Ľ	Certificate File	Choose file	No file chosen				
Tourist Conditionation			Г	Friendly Name	EAP-TLS					<i>i</i>)
Trusted Certificates			L							
OCSP Client Profile					Trusted For:	D				
Certificate Signing Req	uests				✓ Trust for au	thentication w	ithin ISE			
Certificate Periodic Che	eck Setti				Trust	for client author	entication and Syslo	0		
Certificate Authority								9		
· Certinoate Authonity					Trust for au	uthentication of	Cisco Services			
					Validate Ce	rtificate Extens	ions			
				Description						
					Submit	ncel				

Étape 10. Lorsque vous cliquez sur **Soumettre**, le certificat est ajouté à la liste des certificats approuvés. En outre, le certificat intermédiaire est nécessaire pour se lier à CSR comme indiqué dans l'image.

altable Identity Services Engine	Home Context Visibility Operations Polic	y Administration Work C	enters		License Warning 🔺 🔍 💿 🗢		
System → Identity Management	Network Resources	rid Services + Feed Service + Th	hreat Centric NAC		Click here to do wireless setup and visibility setup Do not show this again.		
Deployment Licensing - Certificate	Logging Maintenance Upgrade Backup &	Restore + Admin Access + Setti	ngs		crick hard to do write as a study and making accepted in the agent.		
0							
- Certificate Management	Certificate Signing Requests						
System Certificates	Generate Certificate Signing Requests (CSR)						
Trusted Certificates	A Certificate Signing Requests (CSRs) must be sent to and	signed by an external authority. Click	"export" to download one or more C	SRs so that they may be signed by an exte	mal authority. After a request has been signed, click "bind" to bind the request to the		
OCSP Client Profile	signed deruncate issued by that adminity. Once a Cork is b	ound, it will be removed from bits list.					
Certificate Signing Requests	View Export X Delete Bind Certificate				Show All 🔹 😼		
Certificate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group ta	g Timestamp 🔺	Host		
Certificate Authority	✓ ise#EAP Authentication	CN=ise.c.com	2048	Mon, 9 Jul 2018	se Created by Paint X		

Étape 11. Lorsque vous cliquez sur **Lier le certificat**, vous pouvez choisir le fichier de certificat enregistré sur votre bureau. Accédez au certificat intermédiaire et cliquez sur **Soumettre** 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	Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings
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

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

dualse Identity Services Engine	Home +	Context Visibility	Policy Ad	ministration			License V	Varning 🔺 🔍 🔍	1	
System + Identity Management + Network Resources + Device Pontal Management pxGirld Services + Feed Service + PassiveID + Threat Centric NAC										
Deployment Licensing Cartificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings										
0										
- Certificate Management System Certificates 🛕 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.										
Overview	/ Edit	🕂 Generate Self Signed Certifica	te 🕂 Import 🚱	Export 🗙 Delete 🔎 View						
System Certificates	Fr	riendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date		
Endpoint Certificates	▼ ise									
Trusted Certificates		efault self-signed sami server certi ate - 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	_ int	termediate	EAP Authentication, Admin, Portal	Default Portal Certificate Group ()	ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 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 pour accéder au serveur. Ouvrez un navigateur Web et entrez cette adresse : <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 **Utilisateur** 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	ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIsPJry
certificate request	aF412aLpmDFp1PfVZ3VaP60a/mej3IXh0RFxBUII
(CMC or	weOhO6+V+eh71jeTgiwzEZGr/ceYJIakco5zLjgR
PKCS #10 or	dD7LeujkxF1j3SwvLTKLDJq+00VtAhrx1p1PyDZ3
PKCS #7):	ieC/XQshm/OryD1XuMF4xhq5ZWo1oDOJHG1g+dKX
PKCS #7):	END CERTIFICATE REQUEST

Certificate Template:

	User	
Additional Attrib	utes:	
Attributes:		11.
		Submit >

Étape 3. Ensuite, cliquez sur **télécharger la chaîne de certificats** comme précédemment pour le serveur.

Une fois les certificats obtenus, 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 Microsoft Management Console (MMC).

- 1. Pour ouvrir MMC, accédez 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 Certificats et sélectionnez Toutes les tâches > Importer.
- 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 OK**

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

Profil sans fil pour EAP-TLS

Étape 1. Modifiez le profil sans fil créé précédemment pour le protocole PEAP (Protected Extensible Authentication Protocol) afin d'utiliser 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** comme indiqué dans l'image.

1
ς

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

When connecting:		
O Use my smart card		
Use a certificate on this computer	Advanced	
Use simple certificate selection (Recommended	i)	
Verify the server's identity by validating the cert	ificate	
Connect to these servers (examples:srv1;srv2;	.*\.srv3\.com):	
Trusted Root Certification Authorities:		[
Trusted Root Certification Authorities:		(^
Trusted Root Certification Authorities: Entrust.net Certification Authority (2048) Equifax Secure Certificate Authority		^
Trusted Root Certification Authorities: Entrust.net Certification Authority (2048) Equifax Secure Certificate Authority fixer-WIN-97Q5HOKP9IG-CA		^
Trusted Root Certification Authorities: Entrust.net Certification Authority (2048) Equifax Secure Certificate Authority fixer-WIN-97Q5HOKP9IG-CA GeoTrust Global CA GeoTrust Primary Certification Authority		^
Trusted Root Certification Authorities: Entrust.net Certification Authority (2048) Equifax Secure Certificate Authority fixer-WIN-97Q5HOKP9IG-CA GeoTrust Global CA GeoTrust Primary Certification Authority GeoTrust Primary Certification Authority - G3		^
Trusted Root Certification Authorities:		^
Trusted Root Certification Authorities: Entrust.net Certification Authority (2048) Equifax Secure Certificate Authority fixer-WIN-97Q5HOKP9IG-CA GeoTrust Global CA GeoTrust Primary Certification Authority GeoTrust Primary Certification Authority - G3 GlobalSign GlobalSign		^
Trusted Root Certification Authorities: Entrust.net Certification Authority (2048) Equifax Secure Certificate Authority fixer-WIN-97Q5HOKP9IG-CA GeoTrust Global CA GeoTrust Primary Certification Authority GeoTrust Primary Certification Authority - G3 GlobalSign GlobalSign GlobalSign Root CA		~
Trusted Root Certification Authorities: Entrust.net Certification Authority (2048) Equifax Secure Certificate Authority fixer-WIN-97Q5HOKP9IG-CA GeoTrust Global CA GeoTrust Primary Certification Authority GeoTrust Primary Certification Authority - G3 GlobalSign GlobalSign GlobalSign Root CA 		^ ~

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

o Li Li Coo Con Igo	802.11 settings		
Specify a	authentication mode:		
User or	computer authentication	n ~ Save c	redentials
Dele	te credentials for all use	rs	
Enable s	ingle sign on for this ne	twork	
Perfo	orm immediately before	user logon	
		ser logon	
OPerfo	orm immediately after us	ser legen	
O Perfo Maximu	orm immediately after us m delay (seconds):	10	•
 Perfo Maximu Maximu Allov sign 	orm immediately after us m delay (seconds): v additional dialogs to be on	10 e displayed during	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 l'illustre l'image.



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Le type EAP du client doit être EAP-TLS. Cela signifie que le client a terminé l'authentification, avec l'utilisation d'EAP-TLS, obtenu l'adresse IP et est prêt à transmettre le trafic comme indiqué dans les images.

				<u></u>			
		CLIENT VIEW		0			
æ	Monitoring Network Summary Access Points Clients Applications Creass Points	GENERAL	User Name Administrator Host Name Unknown 34:02:86:96:2f:57 Associated since 37 Seconds		CONNECTIVITY Start Association TOP APPLICATIONS	Onine	
	Access Points	ssin	ME FAP		Name	Us Oats trailable!	n Usage
	Clients	AP Name	Munuton and Transon ser			No Data Available!	
	I Interferers	Nearest APs	AP4420.0339.772 (Cn 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	Connection Score					
ġ.	Management						
*	Advanced	MOBILITY STATE	(EXPWAP)	AP (FlexConnect)	Wireless (802.11n (5GHz))	Client (VLAN1)	

æ	Monitoring Network Summary Access Points Clients O Applications	MOBILITY STATE (LOCAL) Nº_30 Nº_30 AIR-AP1832H-D-K9		AP (FlexConnect) (010) AP442b 03a9.7f72 10 127 209.54 AIR-CAP3602I-A-K9	(802.11n (5GHz)) 	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)	
2	🔁 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	
•	Wireless Settings	U-APSD	Disabled				
*	Management	QoS Level	Silver				
*	Advanced						
		CLIENT TEST PING TEST	CONNECTION	EVENT LOG PAC	CKET CAPTURE		

Étape 2. Voici les détails client de l'interface de ligne de commande du contrôleur (sortie clipsée) :

(Cisco Controller) > show client detail 34:02:86:96	5:2f: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	6
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

Étape 3. Sur ISE, naviguez jusqu'à **Visibilité contextuelle > Terminaux > Attributs** comme indiqué dans les images.

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	8 🛛						
	Ę	MAC Address Username: Ad Endpoint Prof Current IP Ad Location:	: 34:02:86:9 dministrato ile: Intel-Der dress:	6:2F:B7 @fixer.c rice	om					
		Attributes Authen	tication	Threats	s Vulnerabilitie	15				
	General	Attributes								
	Descript	ion								
	Static As	ssignment f	alse							
	Endpoin	t Policy I	ntel-Device							
	Static G	roup Assignment f	alse							
	Identity Group Assignment Profiled									
1	Custom	Custom Attributes								
									▼ Filter •	• •
		Attribute Name			Attribute Val	ue				
	×	Attribute Name			Attribute Valu	0				
	No d	lata found. Add custom	attributes h	ere.						
	Other A	ttributes								
	AAA-Se	rver		ise						
	AKI			88:20:a7	:c9:96:03:5a:26:58:1	d:67:58:83:71:e8:b	::c6:6d:97:bd			
_	Airespac	ce-Wian-Id		6	_					
	Allowed	ProtocolMatchedRule		Dot1X						
	Authenti	cationIdentityStore		Internal L	Jsers					
	Authenti	cationMethod		x509_PK	3					
	Authoriz	ationPolicyMatchedRu	lie	Basic_Au	thenticated_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

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.