Entender e configurar EAP-TLS com Mobility Express e ISE

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Informações de Apoio Fluxo EAP-TLS Etapas do fluxo EAP-TLS Configurar **Cisco Mobility Express** ISE com Cisco Mobility Express Configurações EAP-TLS Configurações do Mobility Express no ISE Certificado de Confiança no ISE **Cliente para EAP-TLS** Fazer download do certificado do usuário na máquina cliente (Windows Desktop) Perfil sem fio para EAP-TLS Verificar Troubleshoot

Introduction

Este documento descreve como configurar uma rede local sem fio (WLAN) com segurança 802.1x em um controlador Mobility Express. Este documento também explica especificamente o uso do Extensible Authentication Protocol (EAP) - Transport Layer Security (TLS).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração inicial do Mobility Express
- processo de autenticação 802.1x
- Certificados

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC 5508 versão 8.5
- Identity Services Engine (ISE) versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Fluxo EAP-TLS



Etapas do fluxo EAP-TLS

- 1. O cliente sem fio é associado ao ponto de acesso (AP).
- 2. O AP não permite que o cliente envie dados neste momento e envia uma solicitação de autenticação.
- 3. Em seguida, o requerente responde com uma identidade EAP-Response. Em seguida, a WLC comunica as informações de ID de usuário ao Servidor de autenticação.
- 4. O servidor RADIUS responde de volta ao cliente com um pacote de início EAP-TLS. A conversação EAP-TLS começa neste ponto.
- 5. O peer envia uma Resposta EAP de volta ao servidor de autenticação que contém uma mensagem de handshake "client_hello", uma cifra definida para NULL.
- 6. O servidor de autenticação responde com um pacote de desafio de acesso que contém:

TLS server_hello handshake message certificate server_key_exchange certificate request server_hello_done.

7. O cliente responde com uma mensagem EAP-Response que contém:

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. Depois que o cliente se autentica com êxito, o servidor RADIUS responde com um desafio de acesso, que contém a mensagem "change_cipher_spec" e handshake concluído. Ao receber isso, o cliente verifica o hash para autenticar o servidor RADIUS. Uma nova chave de criptografia é derivada dinamicamente do segredo durante o handshake TLS.
- 9. Neste ponto, o cliente sem fio EAP-TLS ativado pode acessar a rede sem fio.

Configurar

Cisco Mobility Express

Etapa 1. A primeira etapa é criar uma WLAN no Mobility Express. Para criar uma WLAN, navegue até WLAN > Add new WLAN como mostrado na imagem.

æ	Monitoring	Cisco Aironet 1850 Series Mobi	ility Express	Q	A 🥹 🖺 💳	\geq	٥
*	Wireless Settings	WLAN CONFIGURATION					
	쓸 WLAN Users 矕 Guest WLANs	M Active WLANS					C
	DHCP Server	Add new WLAN					
ġ.	Management	Active	Name	Security Policy	Radio Policy		
. 土	Advanced	C X Enabled	PSK Dotte	WPA2Personal WPA2Enterorise	ALL		_

Etapa 2. Uma nova janela pop-up será exibida quando você clicar em Adicionar nova WLAN. Para criar um nome de perfil, navegue até Add new WLAN > General, como mostrado na imagem.

æ	Monitoring	•	cis	Cisco Airon					Q	A	۲	8	1	٥
\$	Wireless Settings													
	🖆 Access Points	2		e WLANs 5										
	📽 WLAN Users				Add new WLAN		×							
	📽 Guest WLANs				General WLAN Security	VLAN & Firewall Tra	affic Shaping							
	DHCP Server		Add new \	WLAN										
÷.	Management			Active	WLAN ID	6	•	Policy		Rad	io Policy			
*	Advanced	ß	×	Enabled	Profile Name *	ME_EAP				ALL				
	haranooa	ß	×	Enabled	SSID *	ME EAP	_	rsonal		5 GI				
		8	×	Enabled	Admin State	Easter		rsonal		5 GI				
		C C C C	×	Enabled	Administrate	Enabled	<u> </u>	rsonal		2.4				
		C	×	Enabled	Radio Policy	ALL	• 🔮			ALL				
					Broadcast SSID									
					Local Profiling									
						⊘ Apply	Cancel							

Etapa 3. Configure o tipo de autenticação como WPA Enterprise para 802.1x e configure o servidor RADIUS em Adicionar nova WLAN > Segurança WLAN, como mostrado na imagem.

ее м	lonitoring	•	Cisco Airone	1830 Series M	lobility I	Express			Q	A	٩	₽	M	٥
🗱 Wi	ïreless Settings WLANs	WLAN		Add now				×						
연 / 성 ·	Access Points WLAN Users	۵۵ ال	tive WLANs 5	General	WLAN Se	ecurity VLAN & Firewall	Traffic Shaping							
알 종 [Guest WLANs DHCP Server	Add n	ew WLAN	G	iuest Ne	etwork								
й- Ма	anagement		Active		MAC Filt	Security Type of Oper when MAC Filtering is	is not allowed enabled.	Policy		Rad	io Policy			
📥 Ad	dvanced	8 x 8 x	Enabled Enabled Enabled Enabled	Authenti	Security	y Type WPA2 Enterprise Server External Radius	•	rsonal rsonal rsonal		ALL 5 GF 5 GF	Hz only Hz only Hz only			
		C ×	Enabled	Add RAD	NUS Authe State	Server IP Address	Port	rsonal		2.4 (GHz only			
				External Radii WLANs	us configur	ration applies to all	ply (8 Cancel							

Etapa 4. Clique em **Add RADIUS Authentication Server** e forneça o endereço IP do servidor RADIUS e do segredo compartilhado que devem corresponder exatamente ao que foi configurado no ISE e clique em **Apply** conforme mostrado na imagem.

2	Monitoring		Cisco Aironet 1	830 Series Mobility Expr	ess			Q	A	٩	Ħ	\$
\$	Wireless Settings	WLAN CO		Add new WI AN		×						
	별 Access Points 營 WLAN Users	Active	WLANS 5	Add/Edit RADIUS Au	thentication Ser	ver.						
	영 DHCP Server			Server Index	1	•						
ġ.	Management	Add new Wi	Active	State Server IP Address	Enabled	•	r Policy		Rad	io Policy		
*	Advanced	8 × 8 ×	Enabled Enabled	Shared Secret			rsonal		5 GF	iz only iz only		
		8 ×	Enabled Enabled	Show Password Port Number	1812		rsonal		5 Gł	iz only GHz only		
		© ×	Enabled	Server Timeout	5	Seconds	-		ALL			
						(a cancer						
				External Radius configuration a WLANs	pplies to all	pply Cancel						
					-							

ISE com Cisco Mobility Express

Configurações EAP-TLS

Para criar a política, você precisa criar a lista de protocolos permitidos para usar em sua política. Como uma política dot1x é gravada, especifique o tipo de EAP permitido com base em como a política é configurada.

Se você usar o padrão, você permitirá a maioria dos tipos de EAP para autenticação que talvez não seja preferível se precisar bloquear o acesso a um tipo específico de EAP.

Etapa 1. Navegue até **Política > Elementos de política > Resultados > Autenticação > Protocolos permitidos** e clique em **Adicionar** conforme mostrado na imagem.

Hole Identity Services Engine	orne 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	

Etapa 2. Nessa lista de Protocolos Permitidos, você pode digitar o nome da lista. Nesse caso, a caixa **Permitir EAP-TLS** está marcada e outras caixas estão desmarcadas, como mostrado na imagem.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
Authentication Authorization Profili	ng Posture Client Provisioning - Policy Elements	
Dictionaries Conditions - Results	3	
0	Allowed Protocole Sources List > New Allowed Protocole Comice	
 Authentication 	Allowed Protocols	
Allowed Protocols	Name EAP-TLS	
Authorization	Description	
Profiling		
► Posture	✓ Allowed Protocols	
 Otient Provisioning 	Authentication Bypass	
Client Provisioning	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 Hours	
	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 Police (i)	су
	Require cryptobinding TLV (j)	

Configurações do Mobility Express no ISE

Etapa 1. Abra o console do ISE e navegue até **Administration > Network Resources > Network Devices > Add**, como mostrado na imagem.

-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

Etapa 2. Insira as informações conforme mostrado na imagem.

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	
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services	
0		
Network devices	Network Devices Las > New Network Device	
Default Device	* Name Vyrame Description	
	* IP Address: University / 32	@ -
	Device Profile and Olsco	
	Model Name Software Version	
	* Network Device Group	
	Device Type All Device Types O Set. To Default.	
	RADIUS Authentication Settings	
	Enable Authentication Settings	
	Protocol RADIUS Shared Secret Show	
	Enable KeyWrap	
	* Key Encryption Key Show	
	* Message Authenticator Code Key Show	
	Key Input Format ASCII HEXADECIMAL CoA Port T00 Set To Default.	

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

Certificado de Confiança no ISE

Etapa 1. Navegue até Administração > Sistema > Certificados > Gerenciamento de Certificados > Certificados Confiáveis.

Clique em **Importar** para importar um certificado para o ISE. Depois de adicionar uma WLC e criar um usuário no ISE, você precisa fazer a parte mais importante do EAP-TLS que é confiar no certificado no ISE. Para isso, você precisa gerar CSR.

Etapa 2. Navegue até Administrador > Certificados > Solicitações de Assinatura de Certificado > Gerar Solicitações de Assinatura de Certificado (CSR) conforme mostrado na imagem.

sco Identity Services Engine	Home Context Visibility Operations Poli	y Administration Work C	ienters		License Warni	ng 📥 🔍 🕘 🔳 🌣
System Identity Management	Network Resources	d Services + Feed Service + Pa	ssiveID + Threat Centric NAC			
Deployment Licensing - Certificates	Logging Maintenance Upgrade Backup & Re	store + Admin Access + Setting	\$			
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 CSR	ts so that they may be signed by an ex	ternal authority. After a request has been signed	, click "bind" to bind the request to the
Endpoint Certificates	signed certificate issued by that authority. Once a CSR is b	und, it will be removed from this list.				
Trusted Certificates	View Deport X Delete Bind Certificate				Show	All 🔹 😼
OCSP Client Profile	Friendly Name	Certificate Subject	Key Length Portal group tag	Timestamp .	Host	
Certificate Signing Requests	ise#EAP Authentication	CN=ise.c.com	2048	Wed, 11 Jul 2018	ise	
Certificate Periodic Check Setti						
Certificate Authority						

Etapa 3. Para gerar CSR, navegue até **Usage** e, a partir dos **certificados, os certificados serão usados para** as opções suspensas, selecione **EAP Authentication** como mostrado na imagem.

cisco	Identity	y Services	Engine	Home	Context	Visibility	 Operations 	Policy	- Adm	inistration	Work Centers
▼ Sys	tem	Identity Ma	anagement	Network I	Resources	Device	Portal Manager	nent pxGrid	Services	Feed Ser	vice Threat Centric NAC
Deplo	yment	Licensing	- Certificat	es 🔸 Log	ging 🕨 M	laintenance	Upgrade	Backup & Res	store +	Admin Acces	ss > Settings
Certif Syst Trus OCS Certif Certif	ficate M em Cert ted Cert ificate Si ficate Pi ficate A	anagement ificates ificates : Profile eriodic Chec uthority	ests k Setti	Certific Ce ISI US US A No	cate Sign rtificate type E Identity C • Multi-U • Admin • EAP A • DTLS / • Portal - • pxGrid • SAML E Certificate • ISE Ro • ISE Int • Renew ISE Ro • ISE RO	ing Reque es will requir certificates: Jse (Admin, - Server Aut uthenticatior Authenticatior Authentication - Server Aut - Client and - SAML Sigr e Authority bot CA - This termediate C JSE OCSP bot CA/ISE In) will be use rd Certificate	est EAP, Portal, pxC thentication n - Server Authen on - Server Authen on - Server Authenting Certificates: s is not a signing CA - This is an In Responder Cert ntermediate CA. d for EAP Auth es (i) e Nodes:	aded key usages and a key usages and a client and ntication entication ication request, but ar termediate CA ificates - This is entication	a bility to Signing Ri not a sign	generate a bra equest. ning request, t	s which extended key usages are required for each certificate type: rand new Root CA certificate for the ISE CA functionality. but an ability to renew the OCSP responder certificate that is signed by the
									COK FI	Authoritication	
					ISE				ISE#EAP	Authenticatio	AL T

Etapa 4. O CSR gerado no ISE pode ser visualizado. Clique em **Exibir** conforme mostrado na imagem.



Etapa 5. Depois que o CSR for gerado, procure o servidor CA e clique em **Solicitar um certificado** conforme mostrado na imagem:



Etapa 6. Depois de solicitar um certificado, você obtém opções para **Certificado do usuário** e **solicitação de certificado avançado**, clique em **solicitação de certificado avançado** como mostrado na imagem.

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

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request

Passo 7. Cole o CSR gerado na **solicitação de certificado codificada em Base 64**. Na opção suspensa **Modelo de certificado:**, escolha **Servidor Web** e clique em **Enviar** conforme mostrado na imagem.

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):
Certificate Template:
Web Server C
Additional Attributes:
Attributes:
Submit >

Etapa 8. Depois de clicar em **Enviar**, você terá a opção de selecionar o tipo de certificado, selecionar **Base 64 codificado** e clicar em **Baixar cadeia de certificados** como mostrado na imagem.

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						

Etapa 9. O download do certificado foi concluído para o servidor ISE. Você pode extrair o certificado, o certificado conterá dois certificados, um certificado raiz e outro intermediário. O certificado raiz pode ser importado em Administração > Certificados > Certificados Confiáveis > Importar como mostrado nas imagens.

dentity Services Engine	Home + Context Vis	ibility Operations	Policy Administr	ation + Work Centers					License Warning 🔺	9. 0 0 0
System Identity Management	Network Resources	Device Portal Manageme	ent pxGrid Services + I	Feed Service + Threat	Centric NAC			Click here to do wireles	is setup and visibility setup	Do not show this again. ×
Deployment Licensing - Certificate	s + Logging + Maint	tenance Upgrade +	Backup & Restore + Adm	in Access + Settings						
0										
Certificate Management	Trusted Certificat	es								
System Certificates	/ Edit Import	Export X Delete	€ View						Show All	- 8
Trusted Certificates	Friendly Name		▲ Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	
ululu Identity Service	s Engine	Home 🕨	Context Visibility	Operations	s Policy	- Adminis	tration • Wor	k Centers		
▼ System ► Identity	Management	Network Reso	ources	e Portal Manage	ment pxGrid	Services +	Feed Service	Threat Centric	NAC	
Deployment Licensin	g - Certificat	es 🕨 Logging	Maintenance	e Upgrade	Backup & Re	estore + Ad	min Access + S	ettings		
	G									
- Cortificato Managama	at	Import a	new Certificat	te into the C	ertificate St	ore				
• Certificate management	in		Γ							
System Certificates				Certificate File	Choose file	No file chosen				
eyetenn een moutee			Г	Friendly Name	EAP-TLS					(i)
Trusted Certificates			L							
OCSP Client Profile					Trusted For:	D				
Certificate Signing Rec	uests				Trust for au	uthentication w	ithin ISE			
Certificate Periodic Ch	eck Setti				Trust	for client auth	entication and Sysl	og		
Certificate Authority					Trust for au	uthentication of	f Cisco Services			
					Validate Ce	rtificate Extens	sions			
				Description						
					Submit	ncel				

Etapa 10. Depois de clicar em **Enviar**, o certificado é adicionado à lista de certificados fidedignos. Além disso, o certificado intermediário é necessário para se vincular ao CSR, como mostrado na imagem.

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 Deport 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

Etapa 11. Depois de clicar em **Vincular certificado**, há uma opção para escolher o arquivo de certificado salvo em sua área de trabalho. Navegue até o certificado intermediário e clique em **Enviar** conforme mostrado na imagem.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing - Certificat	es + 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 (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

Etapa 12. Para visualizar o certificado, navegue para **Administração > Certificados > Certificados do Sistema**, conforme mostrado na imagem.

Identity Services Engine	Home + Context Visibility	Operations Policy //	Idministration Vork Centers				License Warning 🔺 🔍 🥥	1		
System Identity Management	Network Resources Device P	ortal Management pxGrid Service	es + Feed Service + PassiveID	Threat Centric NAC						
Deployment Licensing -Certificates Logging + Maintenance Upgrade Backup & Restore + Admin Access + Settings										
0	0									
Certificate Management	System Certificates 🛕 Fo	or disaster recovery it is recommende	ed to export certificate and private key p	airs of all system certificates.						
Overview	🕖 Edit 🕂 Generate Self S	igned 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 sam ficate - CN+SAML_ise.org/li> 	I server certi s.com		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 ()	ise.c.com	fixer-WIN-97Q5H0KP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 2020	2		
Certificate Signing Requests										
Certificate Periodic Check Setti										
Cartificate Authority										

Cliente para EAP-TLS

Fazer download do certificado do usuário na máquina cliente (Windows Desktop)

Etapa 1. Para autenticar um usuário sem fio por meio do EAP-TLS, você precisa gerar um certificado de cliente. Conecte seu computador Windows à rede para que você possa acessar o servidor. Abra um navegador da Web e digite este endereço: <u>https://sever ip addr/certsrv—</u>

Etapa 2. Observe que a CA deve ser a mesma com a qual o certificado foi baixado para o ISE.

Para isso, você precisa procurar o mesmo servidor CA que você usou para baixar o certificado para o servidor. Na mesma CA, clique em **Solicitar um certificado** como feito anteriormente, mas desta vez você precisa selecionar **Usuário** como o Modelo de certificado como mostrado na imagem.

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:

Certificate Template:

	User	0	
Additional Attrib	utes:		
Attributes:		11.	
		Submit >	

Etapa 3. Em seguida, clique em **baixar a cadeia de certificados** como foi feito anteriormente para o servidor.

Depois de obter os certificados, siga estas etapas para importar o certificado no windows laptop.

Etapa 4. Para importar o certificado, você precisa acessá-lo do Console de Gerenciamento da Microsoft (MMC).

- 1. Para abrir o MMC, navegue até Start > Run > MMC.
- 2. Navegue até Arquivo > Adicionar/remover snap-in
- 3. Clique Duas Vezes Em Certificados.
- 4. Selecione Conta do computador.
- 5. Selecione Computador local > Concluir
- 6. Clique em **OK** para sair da janela Snap-In.
- 7. Clique em [+] ao lado de Certificados > Pessoal > Certificados.

- 8. Clique com o botão direito em Certificados e selecione Todas as Tarefas > Importar.
- 9. Clique em Next.
- 10. Clique em **Procurar**.
- 11. Selecione o .cer, .crt ou .pfx que deseja importar.
- 12. Clique em Abrir.
- 13. Clique em Next.
- 14. Selecione Selecionar automaticamente o arquivo de certificados com base no tipo de certificado.
- 15. Clique em Concluir e OK

Quando a importação do certificado estiver concluída, você precisará configurar seu cliente sem fio (desktop do windows neste exemplo) para EAP-TLS.

Perfil sem fio para EAP-TLS

Etapa 1. Altere o perfil sem fio criado anteriormente para o PEAP (Protected Extensible Authentication Protocol) para usar EAP-TLS. Clique em **EAP Wireless Profile**.

Etapa 2. Selecione **Microsoft: Smart Card ou outro certificado** e clique em **OK** conforme mostrado na imagem.

EAP Wireless Network	Properties		×
Connection Security			
Security type:	WPA2-Enterprise	~	
Encryption type:	AES	\sim	
Choose a network auth Microsoft: Smart Card	nentication method: or other certificate \sim	Settings	
Remember my cree	dentials for this connect	ion each	
time I'm logged on	l		
Advanced settings			
		ОК	Cancel

Etapa 3. Clique em **Configurações** e selecione o certificado raiz emitido do servidor CA como mostrado na imagem.

Sm	art Card or other Certificate Properties		
N	/hen connecting:		
	O Use my smart card	Advanced	
L	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):	
1			
	Trusted Root Certification Authorities:		
	Entrust.net Certification Authority (2048)		^
F	Equifax Secure Certificate Authority		
	GeoTrust Global CA		_
	GeoTrust Primary Certification Authority		
	GeoTrust Primary Certification Authority - G3		
	GlobalSign Root CA		~
	<	>	
	View	v Certificate	

Etapa 4. Clique em **Configurações avançadas** e selecione **Autenticação de usuário ou computador** na guia Configurações 802.1x, conforme mostrado na imagem.

802.1X settings Specify authentication mode: User or computer authentication ∨							
Specify authentication mode: User or computer authentication v							
User or computer authentication \vee							
	Save creden	tials					
Delete credentials for all users							
Enable single sign on for this network							
Perform immediately before user logor	1						
Maximum delay (seconds):	10	•					
Allow additional dialogs to be displayed sign on	d during single	e					
This network uses separate virtual LAN and user authentication	s for machine	l					

Etapa 5. Agora, tente se conectar novamente à rede sem fio, selecione o perfil correto (EAP neste exemplo) e **Conecte**. Você está conectado à rede sem fio conforme mostrado na imagem.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. O cliente EAP-Type deve ser EAP-TLS. Isso significa que o cliente concluiu a autenticação, com o uso de EAP-TLS, obteve o endereço IP e está pronto para passar o tráfego, como mostrado nas imagens.

		CLIENT VIEW		0			
æ	Monitoring Network Summary Access Points Clients	GENERAL	User Name Administrator Host Name		CONNECTIVITY	hentication DHCP Online	
	Applications		Unknown				
	r∜ Rogues	MAC Address	34:02:86:96:2f:b7		TOP APPLICATIONS		
	Access Points	Uptime	Associated since 37 Seconds		Name	Usage	% Usage
	Clients	SSID AR Name	ME_EAP			No Data Available!	
	D Interferers	Ar Name	TAP442b.03a9.7172 (Ch 56)				
	🕏 Wireless Dashboard	Device Type					
	AP Performance	Performance	Signal Strength: 0 dBm Signal Qu	uality: 0 dB Connection			
	Client Performance	Capabilities	802.11n (5GHz) Spatial Stream: 0)			
	T Best Practices	Cisco Compatible	Supported (CCX v 4)				
٥	Wireless Settings	Connection Score	0%				
ġ.	Management						
¥	Advanced	MOBILITY STATE	Wired (CAPWAP)	AP (FlexConnect)	Wireless (802.11n (5GHz))	Client (VLAN1)	
				010	®1@	-20	

æ	Monitoring Network Summary Access Points Clients O Applications	MOBILITY STATE WLC (LOCAL) 00_8P 1027209.56 AIR-AP1832I-D-K9	(CSPWAP)	AP (FleeConnect)	(882,918, (5GHz)) @¶®	Cilent (VLAN1) 20 Unknown 10.127.209.55
	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
		Fastlane Client	No		ACL (IP/IPv6)	None/None
	Client Performance	Mobility Role	Local		mDNS Profile	None
	P Best Practices	WMM	Supported		AAA Role	None
ø	Wireless Settings	U-APSD	Disabled			
÷.	Management	QoS Level	Silver			
*	Advanced					
		CLIENT TEST	CONNECTION	EVENT LOG PAC	CKET CAPTURE	

Etapa 2. Aqui estão os detalhes do cliente da CLI da controladora (saída 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	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
EAP Type	EAP-TLS

Etapa 3. No ISE, navegue até **Context Visbility > End Points > Attributes**, como mostrado nas imagens.

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:c9:5		: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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.