Entender e configurar o EAP-TLS com uma WLC e um ISE

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Informações de Apoio Fluxo de EAP-TLS Etapas do fluxo EAP-TLS Configurar Controlador de LAN sem fio Cisco **ISE com Cisco WLC** Configurações de EAP-TLS Configurações de WLC no ISE Criar novo usuário no ISE Certificado de Confiança no ISE **Cliente para EAP-TLS** Baixar Certificado do Usuário na Máguina Cliente (Windows Desktop) Perfil sem fio para EAP-TLS Verificar Troubleshoot

Introduction

Este documento descreve como configurar uma rede local sem fio (WLAN) com 802.1X e protocolo de autenticação extensível EAP-TLS

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Processo de autenticação 802.1X
- Certificados

Componentes Utilizados

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

- WLC 3504 versão 8.10
- Identity Services Engine (ISE) versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Fluxo de EAP-TLS



Etapas do fluxo EAP-TLS

- 1. O cliente sem fio é associado ao ponto de acesso (PA). O AP não permite que o cliente envie nenhum dado neste ponto e envia uma solicitação de autenticação.O solicitante responde com uma Identidade de Resposta EAP. A WLC comunica as informações de id de usuário ao Servidor de autenticação. O servidor RADIUS responde de volta ao cliente com um pacote inicial EAP-TLS. A conversa EAP-TLS começa neste ponto.
- 2. O peer envia uma EAP-Response de volta ao servidor de autenticação que contém uma mensagem de handshake "client_hello", uma cifra definida como NULL
- 3. 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. 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. 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.

6. Quando recebe isso, o cliente verifica o hash para autenticar o servidor radius.

7. Uma nova chave de criptografia é derivada dinamicamente do segredo durante o handshake TLS

8/9.EAP-Success é finalmente enviado do servidor para o autenticador, que é então passado para o requerente.

Nesse ponto, o cliente sem fio habilitado para EAP-TLS pode acessar a rede sem fio.

Configurar

Controlador de LAN sem fio Cisco

Etapa 1. A primeira etapa é configurar o servidor RADIUS no Cisco WLC. Para adicionar um servidor RADIUS, navegue para **Segurança > RADIUS > Autenticação**. Clique em **New** conforme mostrado na imagem.

cisco	MONITOR	WLANS C	ONTROLI	ler Wir	ELESS SECURT	N MANAGEMENT	COMMANDS	HELP			User:admin(ReadWrite)
Security	RADIUS	Authenticat	tion Se	rvers							Apply
General	Auth Cal	led Station ID T	ype	AP Name:S	SID v)					
Authentication	Use AES	Key Wrap		(Designed f	or FIPS customers a	nd requires a key wr	ap compliant RAD	IUS server)			
Auth Cached Users Fallback	MAC Del	limiter MTU	6	Colon	*						
DNS Downloaded AVP	Natural		Turnel								
▶ TACACS+	User	Management	Proxy	Index	Server Addre	ss(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	
Disabled Clients User Looin Policies				3	138.77.97.20			1812	Disabled	Disabled	
AP Policies				4	138.77.97.21			1812	Disabled	Disabled	
Password Policies				5	• 172.27.1.71			1812	Disabled	Enabled	
Local EAP				6	* 10.100.120.41			1812	Disabled	Enabled	
Advanced EAP											
Priority Order											
Certificate											
Access Control Lists											
Wireless Protection Policies											
Web Auth											
TrustSec											
Local Policies											
Umbrella											
Advanced											

Etapa 2. Aqui, você precisa digitar o endereço IP e o segredo compartilhado <senha> que é usado para validar a WLC no ISE. Clique em **Apply** para continuar como mostrado na imagem.

ahaha			Save Configuration Ping Logout Refresh
CISCO	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 🔒 Home
Security	RADIUS Authentication Serve	ors > Edit	< Back Apply
Security AAA General General Authentication Accounting Authonization Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP LOAP ITACACS+ LDAP LOAR Net Users MAC Filtering Disabled Clients User Login Policies Disabled Clients Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Wireless Protection Policies Wireless Protection Policies Wireles Protection Policies Wireles Protection Policies Wireles Protection Policies Wireles Policies Access Control Lists Wireles Policies Access Control Lists Wireles Policies Access Control Lists Access Access Control Lists Access Control Lists Access Control L	RADIUS Authentication Server Server Index Server Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Apply Cisco ISE Default settings Apply Cisco ISE Default settings Apply Cisco ACA Default settings Port Number Server Status Support for CoA Server Timeout Network User Management Retransmit Timeout Tunnel Proxy Realm List PAC Provisioning IPSec Cisco ACA	<pre>rs > Edit 7 10.106.35.67 ASCI ASCI *** *** *** *** *** *** *** *** *** *</pre>	< Back Apply

Etapa 3. Criar WLAN para Autenticação RADIUS.

Agora, você pode criar uma nova WLAN e configurá-la para usar o modo WPA-empresa, de modo que ela possa usar o RADIUS para autenticação.

Etapa 4. Selecione **WLANs** no menu principal, escolha **Create New** e clique em **Go** como mostrado na imagem.

ll cısco		JRITY MANAGEMENT COMMA	Saye	Configuration Ping Logout Refresh User:admin(ReadWrite) 🛉 Home
WLANs	WLANs			Entries 1 - 15 of 15
WLANs WLANs	Current Filter: None [Change Filter] [Clear	Filter]	Create New V Go	r
Advanced	WLAN ID Type Profile Name	WLAN SSID	Admin Status Security Policies	

Etapa 5. Nomeie a nova WLAN **EAP-TLS**. Clique em **Apply** para continuar como mostrado na imagem.

ı. cısco	MONITOR WLANS	CONTROLLER WIRELESS S	ECURITY MANAGEMENT	COMMANDS HELP		Save Configuration Ping Logout User:admin(ReadWrite)	Befresh
VLANS VLANS VLANS Advanced	WLANS > New Type Profile Name SSID ID	WLAN V EAP-TLS EAP-TLS 3 V		oommands heed		User:admin(ReadWrite)	Apply

Etapa 6. Clique em **Geral** e verifique se o Status está **Habilitado**. As Políticas de segurança padrão são a autenticação 802.1X e WPA2, como mostrado na imagem.

սիսիս		Saye Configurati	on Ping L	gout Refresh
CISCO	MONITOR WLANS CON	IIRULLER WIRELESS SECURIT MANAGEMENT COMMANDS HELP User:	admin(ReadWi	ite) 🖬 <u>H</u> ome
WLANs	WLANs > Edit 'EAP-T	TLS'	< Back	Apply
WLANS WLANS	General Security	QoS Policy-Mapping Advanced		
Advanced	Profile Name	EAP-TLS		
	Туре	WLAN		
	SSID	EAP-TLS		
	Status	Z Enabled		
1	Security Policies Radio Policy Interface/Interface	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)		
	Group(G)	management V		
	Multicast Vlan Feature	Enabled		
	Broadcast SSID	C Enabled		
	NAS-ID	none		
	11ax Status	C Enabled		
	Lobby Admin Access			

Etapa 7. Agora, navegue até a guia **Security > AAA Servers**, selecione o servidor RADIUS que você acabou de configurar e como mostrado na imagem.

սիսիս			Saye Configuration Ping Logout Refresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 📫 Home
WLANs	WLANs > Edit 'EAP-TLS'		< Back Apply
VLANs WLANs	General Security QoS Policy-Mapp	ping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers		
1	Select AAA servers below to override use of defa RADIUS Servers RADIUS Server Overwrite interface Enabled Apply Cisco ISE Default Settings Enabled Authentication Servers Accor Enabled	ounting Servers EAP Parameters Enable Enable	
	Server 1 IP-10:106:35.67.000011812 v Non Server 2 None v Non Server 3 None v Non Server 4 None v Non Server 5 None v Non Server 6 None v Non Authorization ACA Server Accc Enabled Enabled	ne v ne v ne v ne v ne v ne v sunting ACA Server Enabled	

Note: É uma boa ideia verificar se você pode acessar o servidor RADIUS a partir da WLC antes de continuar. O RADIUS usa a porta UDP 1812 (para autenticação), portanto, você precisa garantir que esse tráfego não seja bloqueado em nenhum lugar da rede.

ISE com Cisco WLC

Configurações de EAP-TLS

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

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

Etapa 1. Navegue **atéPolicy > Policy Elements > Results > Authentication > Allowed** Protocolse **clique em Add** conforme mostrado na imagem.

dentity Services Engine	Iome → Context Visibility → Operations → Policy → Administration → Work Centers
Authentication Authorization Profiling	Posture Client Provisioning Policy Elements
Dictionaries Conditions - Results	
0	
- Authentication	Allowed Protocols Services For Policy Export go to Administration > System > Backup & Restore > Policy Export Page
Allowed Protocols	
Authorization	/ Edit - Add Duplicate Delete
	Service Name
 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 **Allow EAP-TLS** (Permitir EAP-TLS) é marcada e outras caixas são desmarcadas, como mostrado na imagem.

cisco Identity Services Engine	Home								
Authentication Authorization Profili	ng Posture Client Provisioning Policy Elements								
Dictionaries + Conditions - Result	s								
G	Allowed Brotopolo Convised List & New Allowed Bastanda Convise								
 Authentication 	Allowed Protocols								
Allowed Protocols	Name EAP-TLS								
Authorization	Description								
Profiling									
Froming	▼ Allowed Protocols								
 Posture 									
Client Provisioning	Authentication Bypass								
	Process Host Lookup ()								
	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								
	IVe								
	Allow LEAP								
	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 ()								

Configurações de WLC no ISE

Etapa 1. Abra o console do ISE e navegue até Administração > Recursos de rede > Dispositivos de rede > Adicionar conforme mostrado na imagem.

dede Identity Services Engine	tome + Control Visibility + Operations + Policy +Administration + Work Com	m		License Warning 🔺 🔍 🔍 🔘
Stythen + Identity Management Network Devices Network Device Gro	Network Resources	# Centric NAC Fanagers External WDM + Location Services	r	Click here to do wireless setup and visibility setup Co not show this again
O Notice in American	Network Devices			
Default Device	The Life Debuilds Debuild Debuild Debuild Middle -			Service () Tarra 😨 👰 🔒
Device Security Settings	Name - 19/Hask Profile Name Location	Type	Description	anna [m]

Etapa 2. Digite os valores 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	Glick he
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 List > New Network Device Network Devices	
Default Device	* Name Bhuti-Mil C	
Device Security Settings		
	IP Address v *IP: 10.106.35.67 / 32	
	* Device Profile and Ciaco V	
	Model Name 📃 🛬	
	Software Version	
	* Network Device Group	(
	Location All Locations 📀 Set To Default	
	IPSEC Is IPSEC Device 🛇 Set To Default	
	Device Type All Device Types 📀 Set To Default	
	rRADIUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS	
	* Shared Secret Show	
	Use Second Shared Secret 🔲 🕢	
	Show	
	CoA Port Set To Default	
	RADIUS DTLS Settings ()	

Criar novo usuário no ISE

Etapa 1. Navegue até Administração > Gerenciamento de identidades > Identidades > Usuários > Adicionar conforme mostrado na imagem.

thereity Services Engine	Home + Content Visibility + Operations + P	teley Administration + Work Center	1			License Warning 🔺 🧠 😝 😋 🔍
+ System + Identity Management	Network Resources Povice Portal Management p	wGrid Services + Feed Service + Threat	Centric NAC			Click here to do wineless setup and visibility setup Do not show this equin. X
Identifies Oroups External Identif	ty Sources identity Source Sequences + Settings					
0	National Assess Dama					
Users	Network Access Users					Telefel I Telef T 🤹 🍪 🖕
Latest Manual Network Scan Results	/ Dit Add	Detaport X Delate Ry Depicate				Show M * 10
	Status Name . Dr	ecription First Name La	ast Name Email Address	User Identity Groups	Admin	

Etapa 2. Insira as informações conforme mostrado na imagem.

dentity Serv	ices Engine	Home	Context V	<i>'isibility</i>	Operations	▶ Policy	→ Adm	inistration	Work Cen	iters	
► System - Identi	ty Management	Network R	esources	Device F	ortal Management	pxGrid §	Services	Feed Ser	vice • Thre	eat Centric NAC	
-Identities Group	s External Iden	tity Sources	Identity So	urce Seque	nces • Settings						
	G	•									
Users		Network	Access User	s List > Nev	w Network Access	User					
Latest Manual Network	Scan Results	▼ Net	work Acce	ss user							
		* Nan	ne bharti								
		State	us 🗹 En	abled 👻							
		Em	ail	_							
		▼ Pa	sswords								
		Pas	sword Type:	Internal	Users	Ŧ					
				Passwor	d		Re-Enter	Password			
		* Lo	gin Passwor	d ••••••	••		•••••	•		Generate Password	<i>i</i>)
		Ena	ble Passwor	d						Generate Password	
		▼ Us	er Informa	ation							
		First	t Name 📃	-+1							
		Last	t Name	- 41							
		▼ Ac	count Opt	ions							
				Descrip	tion						
		Cha	nge passwo	rd on next lo	ogin 🗆						
		▼ Ac	count Disa	able Policy	/						
			Disable acc	ount if date:	exceeds 2018-0)2-17		(ууу)	/-mm-dd)		
		▼ Us	er Groups								
		Sel	ect an item		0	F					
		Subm	it Cance	ł							

Certificado de Confiança no ISE

Etapa 1. Navegue até Administration > System > Certificates > Certificate Management > Trusted certificates.

Clique em **Import** 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, precisamos gerar CSR.

Etapa 2. Navegue até Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR) conforme mostrado na imagem.

dentity Services Engine	Home + Context Visibility + Operations + Po	licy - Administration - Work C	Centers	U	cense Warning 🔺	ৎ 🛛	0 0	
▼ System → Identity Management	Network Resources Device Portal Management px	ind Services + Feed Service + Th	nreat Centric NAC					
Deployment Licensing Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings								
0								
▼ Certificate Management	Certificate Signing Requests							
System Certificates	Generate Certificate Signing Requests (CSR)							
Trusted Certificates	A Certificate Signing Requests (CSRs) must be sent to a almost contificate leaved by that a that by One on CSR is	d signed by an external authority. Click "	"export" to download one or more CSRs so that they may	r be signed by an external authority. After a request has br	een signed, click "bind	d" to bind the re	equest to the	
OCSP Client Profile	signed certificate issued by that authority. Once a USR is	oounia, it will be removed from this list.						
Certificate Signing Requests	µView ♀Export XDelete Bind Certificate				Show All		- 7	
Certificate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group tag Timestamp	▲ Host				
Certificate Authority			No data available					

Etapa 3. Para gerar o CSR, navegue até **Usage** e, nas opções suspensas **Certificate(s) are used for**, selecione **EAP Authentication** conforme mostrado na imagem.

cisco Identity Services Engine	Home	istration Work Centers		License Warning 🔺	୍ 0	0 ¢
▼System → Identity Management	Network Resources	Feed Service + Threat Centric NAC				
Deployment Licensing - Certificate		tmin Access + Settings				
0						
- Certificate Management	Certificate Signing Request					
System Certificates	Certificate types will require different extended key usages. The list be ISE Identity Certificates:	low outlines which extended key usages are require	d for each certificate type:			
Trusted Certificates	Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Au	hentication				
OCSP Client Profile	Admin - Server Authentication					
Certificate Signing Requests	 EAP Authentication - Server Authentication DTLS Authentication - Server Authentication 					
Certificate Periodic Check Setti	Portal - Server Authentication					
Certificate Authority	 pxGrid - Client and Server Authentication SAML - SAML Signing Certificate 					
)	ISE Certificate Authority Certificates:					
	 ISE Root CA - This is not a signing request, but an ability to ge ISE Intermediate CA - This is an Intermediate CA Signing Req Renew ISE OCSP Responder Certificates - This is not a signi ISE Root CA/ISE Intermediate CA. 	nerate a brand new Root CA certificate for the ISE uest. g request, but an ability to renew the OCSP respon	CA functionality. der certificate that is signed by the			
	_Usage					
	Certificate(s) will be used for EAP Authentication					
	Allow Wildcard Certificates					
	Node(s)					
	Generate CSR's for these Nodes:					
	Node CSR Frie	ndly Name				
	🗹 iabise	AP Authentication				

Etapa 4. O CSR gerado no ISE pode ser visualizado. Clique em **View** 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:

Milcrosoft Active Directory Certificate Services - fixer-WIN-97Q5HOKP9IG-CA Home Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task: <u>Request a certificate</u> View the status of a pending certificate reques

Download a CA certificate, certificate chain, or CRL

Etapa 6. Depois de solicitar um certificado, você obterá opções para **Certificado do usuário** e **solicitação de certificado avançada**, clique em **solicitação de certificado avançada**, conforme 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

Etapa 7. Cole o CSR gerado na **solicitação de certificado codificada na Base 64**. No campo **Modelo de certificado:** selecione **Web Server** e clique em **Submit** conforme mostrado na imagem.

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):		14.
Certificate Templ	ate:	
	Web Server C	
Additional Attribu	ites:	_
Attributes:	lie	
	Submit >	

Etapa 8. Depois de clicar em **Submit**, você terá a opção de selecionar o tipo de certificado, selecionar a **codificação Base-64** e clicar em **Fazer download da 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 está concluído para o servidor ISE. Você pode extrair o certificado, o certificado contém dois certificados, um certificado raiz e outro intermediário. O certificado raiz pode ser importado em Administration > Certificates > Trusted certificates > Import, conforme mostrado nas imagens.

dentity Services Engine	Home	• Administra	tion				U	cense Warning 🔺 🔍		•
System Identity Management	Network Resources	rid Services + Fe	eed Service + Threat Cent	ric NAC		Clic	chere to do wireless set.	p and visibility setup Do no	t show this again.	×
Deployment Licensing - Certificated	sployment Licensing						3			
0	0									
Certificate Management	Trusted Certificates									
System Certificates	/ Edit Import Export XDelete DView							Show All	- 8	5
Trusted Certificates	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date		

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

Etapa 10. Quando você clicar em **Submeter**, o certificado será adicionado à lista de certificados confiáveis. Além disso, o certificado intermediário é necessário para vincular com o CSR, como mostrado na imagem.

dentity Services Engine	Home	icy Administration > Work C	Centers		License Warning 🔺 🧠 💿 🔿	
System Identity Management	Network Resources Povice Portal Management px	Grid Services + Feed Service + T	hreat Centric NAC		Click here to do wireless setup and visibility setup Do not show this again.	
Deployment Licensing - Certificat	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 a	nd signed by an external authority. Click	"export" to download one or more CSF	Rs so that they may be signed by an externa	al authority. After a request has been signed, click "bind" to bind the request to the	
OCSP Client Profile	signed certricate issued by that authority. Once a CSR is	bound, it will be removed from this list.				
Certificate Signing Requests	PView Deport X Delete Bind Certificate				Show All *	
Certificate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group tag	Timestamp A Hos	t	
	ise#FAP Authentication	CNwise c.com	2048	Mon. 9 3ul 2018 ise	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 **Submit** 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
Cartificate Management	Bind CA Signed Certificate
System Certificates	Certificate File Choose file No file chosen
OCSP Client Profile	Friendly Name (1)
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

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

dentity Services Engine	Home	Context Visibility Operation	s → Policy × Ad	ministration				License Warning	۹.	۲	1 O
System Identity Management	Network I	Resources	ment pxGrid Services	Feed Service PassiveID	Threat Centric NAC						
Deployment Licensing - Certificater	s → Log	ging + Maintenance Upgrade	Backup & Restore	Admin Access + Settings							
0											
Certificate Management	Tertificate Management System Certificates 🛕 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.										
Overview	Overview 🥖 Edit 👍 Generate Self Signed Certificate 👍 Import 🕼 Export 🗶 Delete 🔎 View										
System Certificates		Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Exp	iration 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		
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 Jul 2020		
Certificate Signing Requests											_
Certificate Periodic Check Setti											
Certificate Authority											

Cliente para EAP-TLS

Baixar Certificado do Usuário na Máquina Cliente (Windows Desktop)

Etapa 1. Para autenticar um usuário sem fio por meio de EAP-TLS, é necessário gerar um certificado de cliente. Conecte o computador Windows à rede para poder acessar o servidor. Abra um navegador da Web e insira 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 de CA que usou para baixar o certificado do servidor. Na mesma CA, clique em **Solicitar um certificado** como feito anteriormente; no entanto, desta vez você precisará selecionar **Usuário** como o Modelo de certificado 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:

Base-64-encoded certificate request	ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIsPJry aF412aLpmDFp1PfVZ3VaP60a/mej3IXh0RFxBUII we0h06+V+eh7ljeTqjwzEZGr/ceVJJakco5zLjqR
(CMC or PKCS #10 or	dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyDZ3 ieC/XOshm/OryD1XuME4xhq5ZWoloDOJHG1q+dKX
PKCS #7):	END CERTIFICATE REQUEST

Certificate Template:

ocraneate remp	uto.		
	User	0	
Additional Attrib	utes:		
Attributes:		11.	
		Submi	t >

Etapa 3. Em seguida, clique em **baixar 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 Microsoft (MMC).

- 1. Para abrir o MMC, navegue para 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 do mouse 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 armazenamento de certificados com base no tipo de certificado.
- 15. Clique em Concluir e OK

Após a importação do certificado, você precisa configurar seu cliente sem fio (área de trabalho do Windows, neste exemplo) para EAP-TLS.

Perfil sem fio para EAP-TLS

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

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

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

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

Smart Card or other Certificate Properties	
When connecting:	
O Use my smart card Advance	ed
Use a certificate on this computer	
Use simple certificate selection (Recommended)	
Verify the server's identity by validating the certificate	_
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com	ı):
Trusted Root Certification Authorities:	
Entrust.net Certification Authority (2048)	^
fixer-WIN-97Q5HOKP9IG-CA	
GeoTrust Global CA	
GeoTrust Primary Certification Authority	
GeoTrust Primary Certification Authority - G3	
GlobalSign	
GlobalSign Root CA	~
<	>
View Certifica	ate

Etapa 4. Clique em **Advanced Settings** e selecione **User or computer authentication** na guia 802.1x settings, como mostrado na imagem.

802.1X settings 802.11 settings Specify authentication mode: User or computer authentication Delete credentials for all users Enable single sign on for this network	Save credent	tials
Specify authentication mode: User or computer authentication V Delete credentials for all users Enable single sign on for this network	Save credent	tials
User or computer authentication User or computer authentication Delete credentials for all users Enable single sign on for this network	Save credent	tials
 Delete credentials for all users Enable single sign on for this network 		
Enable single sign on for this network		
Perform immediately before user logon		
Maximum delay (seconds):	10	*
Allow additional dialogs to be displayed a sign on	during single	<u>}</u>
This network uses separate virtual LANs and user authentication	for machine	

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

	(î.	EAP Connec	ted, secured		
	(k)	blizzard Secured	l-legacy		
	(h)	blizzaro Secureo	1		
	%	interne Open			
	(%,	dot1x_ Secure	test d		
	((;	JioPriv Secure	ateNet d, Hotspot 2.	0	
	((;	mac_fil Secure	lter d		
	Net Cha	twork & I nge setting	Internet settir s, such as makin	n <u>gs</u> g a connection m	netered
	G.		\$	(kji) Mobile	
1	Wi-F	1	Airplane mode	notspor	

Verificar

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

Etapa 1. O estado do gerenciador de políticas do cliente deve ser exibido como **RUN**. Isso significa que o cliente concluiu a autenticação, obteve o endereço IP e está pronto para passar o tráfego mostrado na imagem.

Summary Access Points Cisco CleanAir	Max Number of Records	Clear AVC Stats		
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,	AP Type	802.11bn
Sleening Clients			AP radio slot Id	0
Multicast			WLAN Profile	EAP
Applications			WLAN SSID	EAP
Lync			Data Switching Central	
Local Profiling			Authentication Central	
Locar Proning			Status	Associated
			Association ID	1
			// 802.11 Authentication	Open System
	Client Type	Simple IP	Reason Code	1
	User Name	Administrator	Status Code	0
	Port Number	1	CF Pollable	Not Implemented
	Interface	management	CF Poll Request	Not Implemented
	VLAN ID	32	Short Preamble	Not Implemented
	Quarantine VLAN ID	0	PBCC	Not Implemented
	CCX Version	CCXv1	Channel Agility	Not Implemented
	E2E Version	Not Supported	Re-authentication timeout	1682
	Mobility Role	Local	Remaining Re-authentication timeou	t 0
	Address	N/A	WEP State	WEP Enable
	Mobility Move Count Policy Manager State	0 RUN	Lync Properties	
	Management Frame	No	Lunc State	Disabled
	Protection	145	Audio Con Deller	Cilver

Etapa 2. Verifique também o método EAP correto no WLC na página de detalhes do cliente, conforme mostrado na imagem.

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

Etapa 3. Aqui estão os detalhes do cliente do CLI da controladora (saída cortada):

(Cisco Controller-Standby) > show client detail 34:	:02:86:96:2f:b7
Client MAC Address	34:02:86:96:2f:b7
Client Username	Administrator
AP MAC Address	00:d7:8f:52:db:a0
AP Name	Alpha2802_3rdfloor
AP radio slot Id	0
Client State	Associated
Wireless LAN Id	5
Wireless LAN Network Name (SSID)	EAP
Wireless LAN Profile Name	EAP
Hotspot (802.11u)	Not Supported
BSSID	00:d7:8f:52:db:a4
Connected For	48 secs
Channel	1
IP Address	10.106.32.239
Gateway Address	10.106.32.1
Netmask	255.255.255.0
Policy Manager State	RUN
Policy Type	WPA2
Authentication Key Management	802.1x

Encryption Cipher..... CCMP-128 (AES) Protected Management Frame No Management Frame Protection..... No EAP Type..... EAP-TLS

Etapa 4. No ISE, navegue até **Visualização de contexto > Pontos finais > Atributos** conforme mostrado nas imagens.



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
C	SelectedAuthenticationIdentityStores	EAPTLS
	SelectedAuthorizationProfiles	PermitAccess
	Serial Number	10 29 41 78 00 00 00 00 01 11

Troubleshoot

No momento, não há informações específicas disponíveis para solucionar problemas dessa configuração.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.