Understand and Configure EAP-TLS with a WLC and ISE

Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
Background Information
EAP-TLS Flow Steps in EAP-TLS Flow
<u>Configure</u>
Cisco Wireless LAN Controller
ISE with Cisco WLC EAP-TLS Settings
WLC Settings on ISE
Create New User on ISE
Trust Certificate on ISE
Client for EAP-TLS
Download User Certificate on Client Machine (Windows Desktop)
Wireless Profile for EAP-TLS
Verify
<u>Troubleshoot</u>

Introduction

This document describes how to set up a Wireless Local Area Network (WLAN) with 802.1X and Extensible Authentication Protocol EAP-TLS.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 802.1X authentication process
- Certificates

Components Used

The information in this document is based on these software and hardware versions:

- WLC 3504 version 8.10
- Identity Services Engine (ISE) version 2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

EAP-TLS Flow



Steps in EAP-TLS Flow

- 1. Wireless Client gets associated with the Access Point (AP). AP does not permit the client to send any data at this point and sends an authentication request. The supplicant then responds with an EAP-Response Identity. The WLC then communicates the user-id information to the Authentication Server. RADIUS server responds back to the client with an EAP-TLS Start Packet. The EAP-TLS conversation starts at this point.
- 2. The peer sends an EAP-Response back to the authentication server which contains a client_hello handshake message, a cipher that is set for NULL
- 3. The authentication server responds with an Access-challenge packet that contains:

TLS server_hello handshake message certificate server_key_exchange certificate request server_hello_done. 4. Client responds with a EAP-Response message that contains:

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

5. After the client authenticates successfully, the RADIUS server responds with an Access-challenge, which contains the change_cipher_spec and handshake finished message.

6. When it receives this, the client verifies the hash in order to authenticate the radius server.

7. A new encryption key is dynamically derived from the secret during the TLS handshake.

8/9. EAP-Success is finally sent from server to authenticator which then is paased to the supplicant.

At this point, the EAP-TLS enabled wireless client can access the wireless network.

Configure

Cisco Wireless LAN Controller

Step 1. The first step is to configure the RADIUS server on the Cisco WLC. In order to add a RADIUS server, navigate to **Security > RADIUS > Authentication**. Click **New** as shown in the image.

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP Security RADIUS Authentication Servers Auth Called Station ID Type AP Name:SSID V RADIUS Use AES Key Wrap Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Security RADIUS Authentication Servers AAA Auth Called Station ID Type General Auth Called Station ID Type * RADIUS Use AES Key Wrap Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant BADIUS server)
AAA Auth Called Station ID Type AP Name:SSID Authous Use AES Key Wrap Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Authentication (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Accounting
Auth Cached Users MAC Delimiter Colon v
Fallback Framed MTU 1300
UNS Develoaded AVP
TACACS+ Network Tunnel Server Liser Management Provi Index Server Address/Inv4/Inv6) Port IPSec Admin Status
DAP over reiningenetic from index outer notices (primary) for a size notic
MAC Filtering C 2 118270.83 1912 Disabled Disabled C
Visabled Clients Comparison
User Login Policies
Password Policies C S 4 J05/197-21 4012 Disabled Eashed
Local EAP
Advanced FAP
Pronty order
Certificate
Access Control Lists
Wireless Protection Policies
▶ Web Auth
TrustSec
Local Policies
Umbrella
Advanced
r Advanced

Step 2. Here, you need to enter the IP address and the shared secret <password> that is used in order to validate the WLC on the ISE. Click **Apply** in order to continue as shown in the image.

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP User:admin(ReadW Security RADIUS Authentication Server John 7 Server Sec	Save Computation Ping Logout Kernes		
Security RADIUS Authentication Server > Edit < Back	Y MANAGEMENT COMMANDS HELP User:admin(ReadWrite) A Hom	MONITOR WLANS CONTROLLER WIRELESS	CISCO
VAA Server Index 7 General Server Address([Ipv4/I]pv6) 10.106.35.67 Authenication Shared Secret Format ASCII v Accounting Ath Cached Users Shared Secret Format Authonication Shared Secret ••••• Fallback OhiS Shared Secret Divisionaded AVP •••• •••• ICDAI Net Users Apply Cisco ISE Default settings ••• ICDAI Net Users Apply Cisco ACA Default settings • VISIONAL Cinits Port Number 1812 VISIONAL Cinits Support for CoA Disabled v Password Pulicies Support for CoA Disabled v Server Timeout S seconds Advanced EAP Network User S isologi	< Back Apply	RADIUS Authentication Servers > Edit	Security
Protry Order Access Control Lists Access Control Lists Wireless Protection Policies Visters Protection Policies Protsioning Enable ISSec Local Policies Vurberlia Advanced	Image: Apply Image: And requires a key wrap compliant RADIUS server)	RADIUS Autmentication Servers > Eait Server Index 7 Server Address(Ipv4/Ipv6) 10.106.35.67 Shared Secret ••• Confirm Shared Secret ••• Key Wrap (Designed for Apply Cisco ISE Default settings Apply Cisco ISE Default settings • Port Number 1812 Server Timeout 5 Server Timeout 5 Network User © Enable Management © seconds Tunnel Proxy Enable Realm List PAC Provisioning IPSec Enable Cisco ACA Enable	 Carriel AAA General RADIUS Authentication Accounting Auth Cached Users Falback DNS Downloaded AVP TACACS+ LDAP LOACI Net Users MAC Filtering Disabled Clients User Login Policies Password Policies Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Web Policies Web Policies Webelia Advanced

Step 3. Create WLAN for RADIUS Authentication.

Now, you can create a new WLAN and configure it to use WPA-enterprise mode, so it can use RADIUS for authentication.

Step 4. Select WLANs from the main menu, choose Create New and click Go as shown in the image.

սիսիս			Sav	e Configuration Ping Logout Refresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECO	KITT MANAGEMENT COMMANDS HELP		User:admin(ReadWrite)
WLANs	WLANs			Entries 1 - 15 of 15
WLANS	Current Filter: None [Change Filter] [Clear.]	litter]	Create New V Go	
Advanced	UKLAN ID Type Profile Name	WLAN SSID Admin Status	iecurity Policies	

Step 5. Name the new WLAN EAP-TLS. Click Apply in order to continue as shown in the image.

սիսիս				Save Configuration Ping Logout Refresh
CISCO		ROLLER WIRELESS SECURITY M	ANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 4 Home
WLANs	WLANs > New			< Back Apply
 WLANS WLANS Advanced 	Type Profile Name SSID ID	WLAN v EAP-TLS EAP-TLS 3 v		·

Step 6. Click General and ensure that the Status is Enabled. The default Security Policies is 802.1X

authentication and WPA2 as shown in the image.

սիսիս			Save Configuration Ping Logout Refresh
CISCO	MONITOR WLANS CON	NTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 🔒 Home
WLANs	WLANs > Edit 'EAP-1	-TLS'	< Back Apply
WLANs WLANs	General Security	QoS Policy-Mapping Advanced	
Advanced	Profile Name	EAP-TLS	
	Туре	WLAN	
	SSID	EAP-TLS	
	Status	C Enabled	
1	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy	All v	
	Interface/Interface Group(G)	management v	
	Multicast Vlan Feature	Enabled	
	Broadcast SSID	Z Enabled	
	NAS-ID	none	
	11ax Status	C Enabled	
	Lobby Admin Access	0	

Step 7. Now, navigate to **Security> AAA Servers** tab, select the RADIUS server that you just configured as shown in the image.

սիսիս		Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 🔒 Home
WLANs	WLANs > Edit 'EAP-TLS'	< Back Apply
WLANs WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
,	Select AAA servers below to override use of default servers on this WLAN RADIUS Servers RADIUS Server Overwrite interface Enabled Apply Cisco ISE Default Settings Enabled Authentication Servers Accounting Servers Enabled Enabled Server 1 IB-10.106.35.67. Bert: 1812 Server 1 IB-10.106.35.67. Bert: 1812	
	Server 2 None v Server 3 None v Server 4 None v Server 5 None v Server 6 None v Authorization ACA Server Accounting ACA Server Enabled Enabled Server None	



Note: It is a good idea to verify that you can reach the RADIUS server from the WLC before you continue. RADIUS uses UDP port 1812 (for authentication), so you need to ensure that this traffic does not get blocked anywhere in the network.

ISE with Cisco WLC

EAP-TLS Settings

In order to build the policy, you need to create the allowed protocol list to use in our policy. Since a dot1x policy is written, specify the allowed EAP type based on how the policy is configured.

If you use the default, you allow most EAP types for authentication which are not preferred if you need to lock down access to a specific EAP type.

Step 1. Navigate to**Policy > Policy Elements > Results > Authentication > Allowed Protocols**and click**Add** as shown in the image.

dentity Services Engine	forme → Context Visibility → Operations → Policy → Administration → Work Centers
Authentication Authorization Profiling	Posture Client Provisioning Policy Elements
Dictionaries + Conditions - Results	
♥ Authentication	Allowed Protocols Services For Policy Export go to Administration > System > Backup & Restore > Policy Export Page
Allowed Protocols	A Edit - L Add De Duplicata - M Dalata
Authorization	Service Name Description
▶ Profiling	Default Network Access Default Allowed Protocol Service
▶ Posture	
Client Provisioning	

Step 2. On this Allowed Protocol list, you can enter the name for the list. In this case, **Allow EAP-TLS** box is checked and other boxes are unchecked as shown in the image.

Authentication Authorization Profiling Posture Client Provisioning Policy Elements Dictionaries Conditions Results Conditions Conditions<th></th>	
Dictionaries Conditions Results	
0	
Allowed Drotocolo Convised List's New Allowed Declarate Convise	
Authentication Allowed Protocols Services List > New Allowed Protocols Services	
Allowed Protocols Name EAP-TLS	
Authorization Description	
- Drofiling	
► Posture	
Client Provisioning	
Process Host Lookup (i)	
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 (
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 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 Pol	су
Require cryptobinding TLV (i)	

WLC Settings on ISE

Step 1. Open ISE console and navigate to Administration > Network Resources > Network Devices > Add as shown in the image.

deater Identity Services Engine	Home + Context Visibility + Operations + Policy +Administration	on Vark Centers		License Warning 🔺 🧠 😐 O
+ System -+ identity Management -+	Network Resources	ed Service + Threat Centric NAC		Click here to do wireless setup and visibility setup Do not show this again
Network Devices Network Device On	tups Network Device Profiles External RADIUS Servers RADIUS Server	Sequences NAC Managers External MDM + Location Services		
0				
Network devices	Network Devices			
Default Device				Selected 2 Total 2 🧐 🏭 🖬
Device Security Settings	/ Edit +Add Palluplicate @ Import @ Export • O Generate 74	Colete -		Show All 🔹 🖌
	Name IP/Mask Profile Name	Location Type	Description	

Step 2. Enter the values as shown in the image.

cisco Identity Services Engine	Home	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	Click be
Network Devices Network Device 0	Troups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	Older He
0		
Network Devices	Network Devices	
Default Device	* Name Rharti-WLC	
Device Security Settings	Description	
	IP Address v *IP: 10.106.35.67 / 32	
	* Device Profile 🔯 Cisco 🔻 🕀	
	Model Name v	
	Software Version	
	* Network Device Group	
	Location All Locations 📀 Set To Default	
	IPSEC Is IPSEC Device O Set To Default	
	Device Type All Device Types 🔿 Set To Default	
	RADIUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS	
	* Shared Secret Show	
	Use Second Shared Secret 🔲 🕢	
	Show	
	CoA Port Set To Default	
	RADIUS DTLS Settings ()	

Create New User on ISE

Step 1. Navigate to **Administration > Identity Management > Identities > Users > Add** as shown in the image.

dentity Services Engine	Nome + Control VoldMY + Copendance + Fairy - Knyster Sec. + Vold Content	License Warning 🔺 🧠 🔍 O 🔍
+ System + Identity Management	Nietourk Resources Device Partal Management profest Services Freed Service Thread Centric NAC	Click here to do winders setue and visibility setue Do red show the asian
Identifies Oroups External Ident	ly Sources i identity Source Sequences + Settings	
0		
Users	Network Access Users	Sevena () franci 🔞 🍪 🖕
Latest Manual Network Scan Results	/fit +44 Bougstans @depet @court Xcene @dourt	Show AL
	Order None Parrieton Eart Name Lut Name Engl Address User Marie Admin	

Step 2. Enter the information as shown in the image.

Identity Services Engine	Home	▶ Operations	Policy -A	Administration	Work Centers
► System - Identity Management	Network Resources Devic	e Portal Management	pxGrid Service	es Feed Servic	e
✓Identities Groups External Ident	ity Sources Identity Source Sec	quences + Settings			
G	Network Assess House Lists				
Users	Network Access Users List >	New Network Access U	Jser		
Latest Manual Network Scan Results	t Name Ltart				
	name bharti	7			
	Status 🗹 Enabled 👻				
	Email				
	▼ Passwords				
	Password Type: Inter	nal Users	*		
	Pass	word	Re-En	nter Password	
	* Login Password				Generate Password
	Enable Password				Generate Password
	 User Information 				
	First Name				
	Last Name				
	 Account Options 				
	Desc	cription			
	Change password on nex	kt login 🛛			
	- Account Displa Da	liau			
	Disable account if d	ate exceeds 2018-02	2-17	(уууу-т	im-dd)
	▼ User Groups				
	Select an item	<u> </u>			
	Submit Cancel				

Trust Certificate on ISE

Step 1. Navigate to Administration > System > Certificates > Certificate Management > Trusted certificates.

Click **Import** in order to import a certificate to ISE. Once you add a WLC and create a user on ISE, you need to do the most important part of EAP-TLS that is to trust the certificate on ISE. For that we need to generate CSR.

Step 2. Navigate to Administrauon > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR) as shown in the image.

dentity Services Engine	Home	icy - Administration - Work	Centers		License Warning 🔺	<u>् ७ ० ०</u>			
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC									
Deployment Licensing -Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings									
0									
	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 CSRs so that they may be signed by an external authority. After a request has been signed, click "oind" to bind the request to the								
OCSP Client Profile	signed certificate issued by that authority. Once a Cork is	sound, il will be removed from this list.							
Certificate Signing Requests	PView 🏶 Export 🗙 Delete 🛛 Bind Certificate				Show All	7 0			
Certificate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group tag	Timestamp 🔺 Host	:				
Certificate Authority			No data ava	lable					

Step 3. In order to generate CSR, navigate to **Usage** and from the **Certificate(s)** are used for drop down options select **EAP Authentication** as shown in the image.

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License Warning 🔺	୍ ୧	0	\$
▼System → Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC				
Deployment Licensing - Certificate	s > Logging > Maintenance Upgrade > Backup & Restore > Admin Access > Settings				
0					
	Certificate Signing Request				
System Certificates	Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:				
Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Setti • Certificate Authority	Multi-Use (Administration Multi-Use (Administration Administration Administration EAP Authentication EAP Authentication DTLS Authentication - Server Authentication Portal - Server Authentication Portal - Server Authentication pxGrid - Client and Server Authentication sAKL Synthesition Coefficient				
	ISE Cartificate authority Cartificates				
1	 ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality. ISE Intermediate CA - This is an Intermediate CA Signing Request. Rerew VSE DCSP Responder Certificates - This is not a signing request, but an ability to renew the DCSP responder certificate that is signed by the ISE Root CAISE Intermediate CA. 				
	Usage Certificate(s) will be used for EAP Authentication				
	Node(s)				
	Generate CSR's for these Nodes:				
	Node CSR Friendly Name				
	☑ labise#EAP Authentication				

Step 4. The CSR generated on ISE can be viewed. Click View as shown in the image.



Step 5. Once CSR is generated, browse for CA server and click **Request a certificate** as shown in the image:

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

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

Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Step 6. Once you request a certificate, you get options for **User Certificate** and **advanced certificate request**, click **advanced certificate request** as shown in the 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

Step 7. Paste the CSR generated in **Base-64 encoded certificate request**. From the **Certificate Template:** drop down option, choose **Web Server** and click **Submit** as shown in the image.

Microsoft Active Directory Certificate Services – fixer-WIN-97Q5HOKP9IG-CA	me							
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								
Additional Attributes:								
Attributes:								
Submit >								

Step 8. Once you click **Submit**, you get the option to select the type of certificate, select **Base-64 encoded** and click **Download certificate chain** as shown in the 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						

Step 9. The certificate download is completed for the ISE server. You can extract the certificate, the certificate contains two certificates, one root certificate and other intermediate. The root certificate can be imported under **Administration > Certifictes > Trusted certificates > Import** as shown in the images.

dentity Services Engine	Home	Policy Administra	tion				U	icense Warning 🔺 🔍	0 0	•
System Hdentity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC Click here to do wreless setup and visibility setup Do not show this again.						in. ×				
Deployment Licensing - Certificate	Deployment Licensing Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings									
0										
Certificate Management	Trusted Certificates									_
System Certificates	/ Edit Import Export X Delete	PView						Show All	٣	8
Trusted Certificates	Friendly Name	 Status 	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date		



Step 10. Once you click **Submit**, the certificate is added to the trusted certificate list. Also, the intermediate certificate is needed in order to bind with CSR as shown in the image.

dentity Services Engine	Home Context Visibility Operations Poli	oy Administration Work	Centers		License Warning 🔺 🔍 🐵 💿 🌣		
System Hentity Management	Network Resources Device Portal Management px	Brid Services + Feed Service + T	hreat Centric NAC		Click here to do wireless setup and visibility setup Do not show this again		
Deployment Licensing - Certificate	es + Logging + Maintenance Upgrade + Backup &	Restore + Admin Access + Sett	ings				
0							
✓ Certificate Management	Certificate Signing Requests						
System Certificates	Generate Certificate Signing Requests (CSR)						
Trusted Certificates	A Certificate Signing Requests (CSRs) must be sent to an	d signed by an external authority. Click	"export" to download one or more CSI	Rs so that they may be signed by an external	authority. After a request has been signed, click "bind" to bind the request to the		
OCSP Client Profile	signed certificate issued by that authority. Once a CSR is	bound, it will be removed from this list.					
Certificate Signing Requests	√View				Show All 💌 😽		
Certificate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group tag	Timestamp 🔺 Host			
	✓ ise#EAP Authentication	CN=ise.c.com	2048	Mon. 9 Jul 2018 ise	Created by Paint X		

Step 11. Once you click **Bind certificate**, there is an option to choose the certificate file saved in your desktop. Browse to the intermediate certificate and click **Submit** as shown in the image.

dentity Services Engine	Home
	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing - Certificate	es
Certificate Management	Bind CA Signed Certificate
System 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: Jse certificate for EAP protocols that use SSL/TLS tunneling
	Submit Cancel

Step 12. In order to view the certificate, navigate to Administration > Certificates > System Certificates

as shown in the image.

Identity Services Engine	Home + C	Context Visibility	i → Policy ···Ac	Iministration + Work Centers			Licen	ise Warning 🔺 🔍 🌔	9 L
System Identity Management	Network Reso	urces	ment pxGrid Services	s + Feed Service + PassiveID	Threat Centric NAC				
Apployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings									
0									
Certificate Management	System Co	ertificates 🛕 For disaster rec	overy it is recommended	d to export certificate and private key p	airs of all system certificates.				
Overview	/ Edit	Generate Self Signed Certification	ite 🕂 Import 🕃	Export X Delete P View					
System Certificates	Frie	endly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
Endpoint Certificates	▼ ise								
Trusted Certificates	 Def fica 	ault self-signed saml server certi te - CN=SAML_ise.c.com	SAML		SAML_ise.c.com	SAML_ise.c.com	Wed, 11 Jul 2018	Thu, 11 Jul 2019	2
OCSP Client Profile	inte	rmediate	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									
Contificante Australia									

Client for EAP-TLS

Download User Certificate on Client Machine (Windows Desktop)

Step 1. In order to authenticate a wireless user through EAP-TLS, you have to generate a client certificate. Connect your Windows computer to the network so that you can access the server. Open a web browser and enter this address: <u>https://sever ip addr/certsrv---</u>

Step 2. Note that the CA must be the same with which the certificate was downloaded for ISE.

For this, you need to browse for the same CA server that you used to download the certificate for server. On the same CA, click **Request a certificate** as previously done, however, this time you need to select **User** as the Certificate Template as shown in the image.

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/3qJJeeM1ZqxnL7BVIsPJ	ry
cortificato request	aF412aLpmDFp1PfVZ3VaP60a/mej3IXh0RFxBU	II
	weOhO6+V+eh7ljeTgiwzEZGr/ceYJIakco5zLj	gR
	dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyD	23
PKCS #10 or	ieC/XQshm/OryD1XuMF4xhq5ZWo1oDOJHG1g+d	KΧ
PKCS #7):	END CERTIFICATE REQUEST	
		_

Certificate Template:

ocranoute remp	ato.				
	User	(
Additional Attrib	utes:				
Attributes:			11.		
			Submi	t >	

Step 3. Then, click **download certificate chain** as was done previously for server.

Once you get the certificates, use these steps in order to import the certificate on windows laptop:

Step 4. In order to import the certificate, you need to access it from the Microsoft Management Console (MMC).

- 1. In order to open the MMC navigate to **Start > Run > MMC**.
- 2. Navigate to File > Add / Remove Snap In
- 3. Double Click **Certificates**.
- 4. SelectComputer Account.
- 5. Select Local Computer > Finish
- 6. Click **OK** in order to exit the Snap-In window.
- 7. Click [+] next to **Certificates > Personal > Certificates**.
- 8. Right click on **Certificates** and select **All Tasks> Import**.
- 9. Click Next.
- 10. Click Browse.
- 11. Select the .cer, .crt, or .pfx you would like to import.
- 12. Click Open.
- 13. Click Next.

14. Select Automatically select the certificate store based on the type of certificate.15. Click Finish & OK

Once import of certificate is done, you need to configure your wireless client (windows desktop, in this example) for EAP-TLS.

Wireless Profile for EAP-TLS

Step 1. Change the wireless profile that was created earlier for Protected Extensible Authentication Protocol (PEAP) in order to use the EAP-TLS instead. Click **EAP wireless profile**.

Step 2. Select Microsoft: Smart Card or other certificate and click OK shown in the image.

EAP Wireless Network	Properties		×			
Connection Security						
Security type:	WPA2-Enterprise	~				
Encryption type:	AES	~				
Choose a network auth Microsoft: Smart Card	nentication method:	Calliana				
		Settings				
Remember my credentials for this connection each time I'm logged on						
Advanced settings						
		OK	Canaal			
L		UK	Cancel			

Step 3. Click settings and select the root certificate issued from CA server as shown in the image.

		-6
Smart Card or other Certificate Properties		
When connecting:		
O Use my smart card	Advanced	
Use a certificate on this computer		
Use simple certificate selection (Recommend	ed)	
Verify the server's identity by validating the ce	ertificate	_
Connect to these servers (examples:srv1;srv	2;.*\.srv3\.com):	
		5
Trusted Root Certification Authorities:		
Entrust.net Certification Authority (2048)	,	^
Equifax Secure Certificate Authority		
IVI fixer-WIN-97Q5HOKP9IG-CA		
GeoTrust Primary Certification Authority		
Geo Frust Primary Certification Authority - G3		
		×
<	>	
	View Certificate	
		-

Step 4. Click **Advanced Settings** and select **User** or **computer authentication** from the 802.1x settings tab as shown in the image.

Advanced settings

802.1X settings 802.11 settings					
Specify authentication mode:					
User or computer authentication \sim	Save credentials				
Delete credentials for all users					
Enable single sign on for this network					
Perform immediately before user logon					
O Perform immediately after user logon					
Maximum delay (seconds):	10				
Allow additional dialogs to be displaye sign on	d during single				
This network uses separate virtual LAN and user authentication	ls for machine				

Step 5. Now, try to connect again to the wireless network, select the correct profile (EAP, in this example) and **Connect**. You are connected to the wireless network as shown in the image.

EAP Connected, secured



(îr,

blizzard-legacy G Secured



blizzard Secured



Open



Gecured



In JioPrivateNet Secured, Hotspot 2.0



mac_filter Secured

. This means that the client has completed authentication, obtained IP address and is ready to pass the traffic shown in the image.

lonitor	Clients > Detail			
Summary	Max Number of Records	s 10 \$ Clear AVC Stats		
Access Points	General AVC Sta	atistics		
Cisco CleanAir				
Statistics	Client Properties		AP Properties	
CDP	chent Properties	1	AFFIOPEITIES	
Rogues	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
Sleeping Clients			AP radio slot Id	0
Multicast			WLAN Profile	EAP
Applications			WLAN SSID	EAP
Lync			Data Switching Central	
Local Profiling			Authentication Central	
Local Froming			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	CE Dellable	Not Implemented
	Interface	management	CF Pollable	Not Implemented
	VLAN ID	32	CF Poll Request	Not Implemented
	Quarantine VLAN ID	0	Short Preamble	Not Implemented
	CCX Version	CCXv1	PBCC	Not Implemented
	E2E Version	Not Supported	Channel Agility	Not Implemented
	Mobility Role	Local	Re-authentication timeout	1682
	Mobility Peer IP	N/A	Remaining Re-authentication timeout	0
	Address	0	WEP State	WEP Enable
	Policy Manager State	RUN	Lync Properties	
	Management Frame	No	Lync State	Disabled
	UnTime (Sec)	146	Audio Oos Policy	Cilver

Step 2. Also verify the correct EAP method on WLC in the client details page as shown in the image.

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

Step 3. Here are the client details from CLI of the controller (output clipped):

(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
Channe1	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	

Step 4. On ISE, navigate to **Context Visbility > End Points > Attributes** as shown in the images.

dentity S	ervices Engine	Home -C	Context Visibility	Operations	+ Policy	Administration	Work Centers	
Endpoints Net	work Devices							
Endpoints > 34:02:86:96:2F:87								
24.02.06.0								
34:02:00:3	MAC Address: 34-02	-86-96-2E-B7						
	Username: Administ Endpoint Profile: Inte	rator@fixer.com	n					
<u>-</u> 2	Current IP Address: Location:							
Attribut	as Authentication	Threats	Vulnerabilities					
	_							
General Attrib	utes							
Description								
Static Assignm	ent false							
Endpoint Policy	/ Intel-De	vice						
Static Group A	ssignment false							
Identity Group	Assignment Profiled							
Custom Attrib	utes							
							V Either v	0 -
A11-0	hute blame		Attribute Melo				1 mar	
Aut	oue Name		Attribute value	8				
^ _Attri	bute Name		Attribute Value					
No data fou	nd. Add custom attribu	tes here.						
Other Attribut	M5							
AAA-Server		ise						
AKI		88:20:a7:c9:96	:03:5a:26:58:fd:67	:58:83:71:e8:bc:c6:	6d:97:bd			
Airespace-Wla	n-Id	5						
AllowedProtoco	oMatchedRule	Dot1X						
Authentication	dentityStore	Internal Users						
Authentication	Method	x509 PKI						

	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
1	OUI	Intel Corporate
	OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message=*Unknown CA - error unable to get issuer certificate locally*
	OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
	PolicyVersion	0
	PostureApplicable	Yes
	PostureAssessmentStatus	NotApplicable
	RadiusFlowType	Wireless802_1x
	RadiusPacketType	AccessRequest
	SSID	00-d7-8f-52-db-a0:EAP
_	SelectedAccessService	Default Network Access
	SelectedAuthenticationIdentityStores	EAPTLS
	SelectedAuthorizationProfiles	PermitAccess
	Serial Number	10 29 41 78 00 00 00 00 11

Troubleshoot

There is currently no specific information available to troubleshoot for this configuration.