Verständnis und Konfiguration von EAP-TLS mit einem WLC und der ISE

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen **EAP-TLS-Fluss** Schritte im EAP-TLS-Fluss Konfigurieren Cisco Wireless LAN-Controller **ISE mit Cisco WLC EAP-TLS-Einstellungen** WLC-Einstellungen auf der ISE Neuen Benutzer auf ISE erstellen Zertifikat auf ISE vertrauen **Client für EAP-TLS** Benutzerzertifikat auf Client-Computer herunterladen (Windows-Desktop) Wireless-Profil für EAP-TLS Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument wird die Einrichtung eines Wireless Local Area Network (WLAN) mit 802.1X und Extensible Authentication Protocol EAP-TLS beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 802.1X-Authentifizierungsprozess
- Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

EAP-TLS-Fluss



Schritte im EAP-TLS-Fluss

- Der Wireless-Client wird mit dem Access Point (AP) verknüpft. AP erlaubt dem Client an dieser Stelle nicht, Daten zu senden und sendet eine Authentifizierungsanforderung.Der Supplicant antwortet dann mit einer EAP-Response-Identität. Der WLC übermittelt dann die Benutzer-ID-Informationen an den Authentifizierungsserver. Der RADIUS-Server antwortet mit einem EAP-TLS-Startpaket auf den Client. Die EAP-TLS-Konversation beginnt an diesem Punkt.
- 2. Der Peer sendet eine EAP-Antwort zurück an den Authentifizierungsserver, die eine "client_hello"-Handshake-Nachricht enthält, eine Chiffre, die auf NULL gesetzt ist
- 3. Der Authentifizierungsserver antwortet mit einem Access-Challenge-Paket, das Folgendes enthält:

TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.
4. Der Client antwortet mit einer EAP-Antwortnachricht, die Folgendes enthält:

Certificate ¬ 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.Nachdem der Client erfolgreich authentifiziert wurde, antwortet der RADIUS-Server mit einer Access-Challenge, die die Meldung "change_cipher_spec" und den Handshake-Abschluss enthält.

6. Wenn er dies erhält, überprüft der Client den Hash, um den Radius-Server zu authentifizieren.

7. Während des TLS-Handshakes wird dynamisch ein neuer Verschlüsselungsschlüssel aus dem geheimen Schlüssel abgeleitet.

8/9.EAP-Success wird schließlich vom Server an den Authentifikator gesendet, der dann an den Supplicant weitergeleitet wird.

An diesem Punkt kann der EAP-TLS-fähige Wireless-Client auf das Wireless-Netzwerk zugreifen.

Konfigurieren

Cisco Wireless LAN-Controller

Schritt 1: Im ersten Schritt wird der RADIUS-Server auf dem Cisco WLC konfiguriert. Um einen RADIUS-Server hinzuzufügen, navigieren Sie zu **Security > RADIUS > Authentication**. Klicken Sie wie im Bild dargestellt auf **Neu**.

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

Schritt 2: Geben Sie hier die IP-Adresse und den gemeinsamen geheimen Schlüssel <Kennwort> ein, der zur Validierung des WLC auf der ISE verwendet wird. Klicken Sie auf **Apply**, um fortzufahren, wie im Bild dargestellt.

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP	Save Configuration Ping Logout Refresh
Security	RADIUS Authentication Serve	ers > Edit	< Back Apply
AAA General RADIUS Authentication Accounting Auth Cached Users Paliback DNS Downloaded AVP Transfer	Server Index Server Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Key Wiso	7 10.106.35.67 ASCII v 	
IDAP LOAP LOAP LOAI Net Users MAC Filtering Disabled Clients User Login Policies Pessword Policies Local EAP Advanced EAP Priority Order	Apply Cisco ISE Default settings Apply Cisco ACA Default settings Port Number Server Status Support for CoA Server Timeout Network User	I (Desplied for First customers and requires a key wrap compliant outputs server) III2 III2 Enabled ~ S seconds I Enable IIII IIII IIII IIIIIIIIIIIIIIIIIIIII	,
Certificate Access Control Lists	Management Management Retransmit Timeout	C Enable S seconds	
Wireless Protection Policies	Tunnel Proxy Realm List PMC Providence		
Web Auth TrustSec Local Policies	IPSec Cisco ACA	Enable Enable	
Advanced			

Schritt 3: Erstellen eines WLAN für die RADIUS-Authentifizierung

Jetzt können Sie ein neues WLAN erstellen und es so konfigurieren, dass es den WPA-Enterprise-Modus verwendet, sodass es RADIUS für die Authentifizierung verwenden kann.

Schritt 4. Wählen Sie **WLANs** aus dem Hauptmenü, wählen Sie **Create New** und klicken Sie auf **Go** wie in der Abbildung dargestellt.

 cısco	MONITOR WLANS CONTROLLER WIRELESS SEC	URITY MANAGEMENT COMMANDS HE	Saye Con	iguration 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 Y Go	(
Advanced	WLAN ID Type Profile Name	WLAN SSID Admin S	tus Security Policies	

Schritt 5: Benennen Sie das neue WLAN **EAP-TLS**. Klicken Sie auf **Apply**, um fortzufahren, wie im Bild dargestellt.

սիսիս								Sage Configuration Ping Logout Refresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	User:admin(ReadWrite) 🔒 Home
WLANs	WLANs > New							< Back Apply
 WLANS WLANS Advanced 	Type Profile Name SSID ID	WLA EAP EAP	Ν v π.s τ.s v					

Schritt 6: Klicken Sie auf **Allgemein**, und stellen Sie sicher, dass der Status **aktiviert** ist. Die Standard-Sicherheitsrichtlinien sind 802.1X-Authentifizierung und WPA2, wie im Bild gezeigt.

11111			Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 🔒 <u>H</u> ome
WLANs	WLANs > Edit 'EAP-	TLS'	< Back Apply
WLANS	General Security	QoS Policy-Mapping Advanced	
> Advanced	Profile Name	EAP-TLS	
	Туре	WLAN	
	SSID	EAP-TLS	
	Status	Enabled	
1	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy	All	
	Interface/Interface Group(G)	management v	
	Multicast Vlan Feature	Enabled	
	Broadcast SSID	Enabled	
	NAS-ID	none	
	11ax Status	C Enabled	
	Lobby Admin Access		

Schritt 7: Navigieren Sie nun zur Registerkarte **Security** > **AAA Servers** (**Sicherheit** > **AAA-Server**), und wählen Sie den RADIUS-Server aus, den Sie gerade konfiguriert haben und wie im Bild dargestellt.

սիսիս							Save Co	nfiguration Ping Logout Refre	sh	
cisco	MONITOR WL	ANS CONTROLLER WIRELE	SS SECURITY MANAGEMEN	t commands help				User:admin(ReadWrite) 🔒 Hon	ne	
WLANs	WLANs > Edi	ILANS > Edit 'EAP-TLS'								
WLANs WLANs	General	Security QoS Policy-	Mapping Advanced							
Advanced	Layer 2	Layer 3 AAA Servers								
1	Select AAA s RADIUS Sen RADIUS S Apply Cisc	ervers below to override use o vers erver Overwrite interface Enat o ISE Default Settings Enat	f default servers on this WLAN vied							
	Server 1	Authentication Servers Enabled IP-10.106.35.67. Port:1812	Accounting Servers	EAP Parameters Enable						
	Server 2	None	None v							
	Server 3	None v	None v							
	Server 4	None v	None v							
	Server 5	None v	None v							
	Server 6	None	None v							
		Authorization ACA Server	Enabled							
	Server	None v	None v							

Anmerkung: Bevor Sie fortfahren, sollten Sie überprüfen, ob Sie vom WLC aus auf den RADIUS-Server zugreifen können. RADIUS verwendet den UDP-Port 1812 (für die Authentifizierung), sodass Sie sicherstellen müssen, dass dieser Datenverkehr nicht irgendwo im Netzwerk blockiert wird.

ISE mit Cisco WLC

EAP-TLS-Einstellungen

Um die Richtlinie zu erstellen, müssen Sie die Liste der zulässigen Protokolle erstellen, die in unserer Richtlinie verwendet werden dürfen. Da eine dot1x-Richtlinie geschrieben wurde, geben Sie den zulässigen EAP-Typ basierend auf der Konfiguration der Richtlinie an.

Wenn Sie die Standardeinstellung verwenden, lassen Sie die meisten EAP-Typen für die Authentifizierung zu, die nicht bevorzugt werden, wenn Sie den Zugriff auf einen bestimmten EAP-Typ sperren müssen.

Schritt 1: Navigieren Sie **zuRichtlinie > Richtlinienelemente > Ergebnisse > Authentifizierung > Zugelassene** Protokolle, und **klicken Sie auf Hinzufügen**, wie im Bild dargestellt.

dentity Services Engine	Home	
Authentication Authorization Profiling	g Posture Client Provisioning - Policy Eler	nents
Dictionaries + Conditions - Results		
✓ Authentication	Allowed Protocols Services For Policy Export go to Administration > System >	Backup & Restore > Policy Export Page
Allowed Protocols		
Authorization	Edit HAdd Duplicate Delete	ption
Profiling	Default Network Access Defaul	t Allowed Protocol Service
Posture		
Client Provisioning		

Schritt 2: In dieser Liste der zulässigen Protokolle können Sie den Namen der Liste eingeben. In diesem Fall ist das Kontrollkästchen **EAP-TLS zulassen** aktiviert, und andere Kontrollkästchen sind deaktiviert, wie im Bild gezeigt.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Authentication Authorization Prof	iling Posture Client Provisioning Policy Elements
Dictionaries + Conditions - Resu	its
(Allowed Declarate Consistent Lints, New Allowed Declarate Consistent
▼ Authentication	Allowed Protocols
Allowed Protocols	Name EAP-TLS
Authorization	Description
▶ Profiling	
Posture	* Allowed Plotocols
Client Provisioning	Authentication Bypass
-	Process Host Lookup ()
	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
	live
	Proactive session ticket update will occur after 10 % of Time To Live has expired
	Allow LEAP
	- Allow PEAP
	PEAP Inner Methods
	Allow EAP-MS-CHAPV2
	Allow Password Change Retries 1 (Valid Range 0 to 3)
	Allow EAP-GTC
	Allow Password Change Retries 1 (Valid Range 0 to 3)
	Allow EAP-TLS
	Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)
	Require cryptobinding TLV (i)

WLC-Einstellungen auf der ISE

Schritt 1: Öffnen Sie die ISE-Konsole, und navigieren Sie zu Administration > Network Resources > Network Devices > Add wie im Bild dargestellt.

dealer Identity Services Engine	tome + Control Visibility + Operations + Policy #Admin	stration + Work Centers		Lixansa Warning 🔺 🔍 🔍 🔘
Bysten + Identity Management Network Device Network Device Gro	Network Resources	Feed Service Threat Centric NAC rver Sequences NAC Managers External MDM + Location	Services	Citick here to do wineless setup and vebibility setup Do not show this again
0	Network Devices			
Default Device				Sender 0 Text 2 👼 👰 🔒
Device Security Settings	None - 19/Hask Profile None	Location Type	Description	Stev 🔝 🔹 🔥

Schritt 2: Geben Sie die im Bild angezeigten Werte ein.

dentity Services Engine	Home ► Cor	text Visibility	 Operations 	Policy	 Administration 	 Work Centers 			
For a straight of the stra	* Network Resource	Device Point	ortal Management	t pxGrid Se	rvices + Feed Ser	vice	tric NAC		Click be
Network Devices Network Device (Groups Network D	evice Profiles	External RADIUS	Servers R/	ADIUS Server Seque	nces NAC Manag	ers External MDM	 Location Services 	
0	Natural David								
Network Devices	Network Devices	ices	vork Device						
Default Device		* N	ame Rharti-M//	r l					
Device Security Settings		Descrin	ition						
		boothp							
	IP Add	ress 👻 * IF	. 10.106.35.6	7		/ 32			
			-						
		* Device Pr	ofile 🎎 Cisco	• ⊕					
		Model Na	ame	Ŧ					
		Software Ven	sion	ť					
	* Network	Device Group							(
	Locatio	All Locations	S	et To Default]				
	IPSE	Is IPSEC Devi	ce 📀 S	et To Default)				
	Device Typ	e All Device Typ	es 🙄 S	et To Default)				
	🗹 👻 RADIU	IS Authentication	Settings						
	RADI	US UDP Settings	6						
				Prot	tocol RADIUS				
				* Shared Se	ecret	9	ihow		
			Use Sec	ond Shared Se	ecret 🗌 🕢				
						5	ihow		
				CoA	Port	5	iet To Default		
	RADI	US DTLS Setting	is 🕧						

Neuen Benutzer auf ISE erstellen

Schritt 1: Navigieren Sie zu Administration > Identity Management > Identities > Users > Add (Verwaltung > Identitätsverwaltung > Identitäten > Benutzer > Hinzufügen wie im Bild dargestellt.

승규는 Mentity Services Engine	Nore + Costed Vebally + Cuexator + Fairy +Advancestator + Walk Center	License Warning 🛦 🧠 😆 😋 🔿						
+ System + Identity Management	n viterith Bangment + Nation Resource + Device Public Bangment polisi Service + Tend Device + Tend D							
Identifies Oroups External Ident	Idential Oncine External Identity Excess Identity Identity Excess Identity Identity Excess Identity I							
0								
Lisers	network access users	Delever 1 Tracit 👙 🛱 🖕						
Lakut Manual Nation's Scan Rounds								
	Status Name Description Prist Name Last Name Enal Address User Identity Groups Admin							

Schritt 2: Geben Sie die im Bild angezeigten Informationen ein.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▶ System ▼ Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
	ty Sources Identity Source Sequences
0	
Users	Network Access Users List > New Network Access User
Latest Manual Network Scan Results	▼ Network Access User
	* Name bharti
	Status Canabled -
	Email
	▼ Passwords
	Password Type: Internal Users
	Password Re-Enter Password
	* Login Password Generate Password (
	Enable Password Generate Password ()
	▼ User Information
	First Name
	Last Name
	✓ Account Options
	Description
	Change password on next login
	✓ Account Disable Policy
	Disable account if date exceeds 2018-02-17 (yyyy-mm-dd)
	▼ User Groups
	Select an item 📀 — 📲
	Submit Cancel

Zertifikat auf ISE vertrauen

Schritt 1: Navigieren Sie zu Administration > System > Certificates > Certificate Management > Trusted Certificates.

Klicken Sie auf **Importieren**, um ein Zertifikat in die ISE zu importieren. Wenn Sie einen WLC hinzufügen und einen Benutzer auf der ISE erstellen, müssen Sie den wichtigsten Teil von EAP-TLS ausführen, d. h. dem Zertifikat auf der ISE vertrauen. Dafür müssen wir CSR erzeugen.

Schritt 2: Navigieren Sie zu Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR), wie im Bild dargestellt.

dentity Services Engine	Home	ticy Administration Work Centers		License Warning 🔺 🔍 😝 🔿					
▼ System → Identity Management	Network Resources Device Portal Management px	Rid Services → Feed Service → Threat Centric N	AC						
Deployment Licensing - Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings									
0	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 airread actificate issued by that a thathy Orac a CSR is	d signed by an external authority. Click "export" to do	wricad one or more CSRs so that they may be signed by an external au	uthority. After a request has been signed, click "bind" to bind the request th	io the				
OCSP Client Profile	signed certificate issued by that autronity. Once a Cork is	oound, it will de removed from dits list.							
Certificate Signing Requests	PView Caport XDelete Bind Certificate			Show All	8				
Certificate Periodic Check Setti	Friendly Name	Certificate Subject Key Length	Portal group tag Timestamp 🔺 Host						
Certificate Authority			No data available						

Schritt 3: Um die CSR-Anfrage zu erstellen, navigieren Sie zu **Usage (Verwendung)** und wählen Sie aus den **Zertifikaten, die für die** Dropdown-Optionen **verwendet werden, EAP Authentication (EAP-Authentifizierung)** aus, wie im Bild dargestellt.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍 🔞 🔿 🔅
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC	
Deployment Licensing - Certificate	is + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings	
0		
- Certificate Management	Certificate Signing Request	
System Certificates	Certificate types wil require different extended key usages. The list below outlines which extended key usages are required for each certificate type: ISE identity Certificates:	
Trusted Certificates	Multi-Use (Admin, EAP, Portal, pxGrkd) - Client and Server Authentication	
OCSP Client Profile	Admin - Server Authentication EAD Authentication - Server Authentication	
Certificate Signing Requests	OTLS Authentication - Server Authentication	
Certificate Periodic Check Setti	Portal - Server Authentication which (Chart and Server Authentication	
Certificate Authority	SAML - SPML Signing Certificate	
1	ISE Certificate Authority Certificates:	
	 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. Renew ISE 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 CA/ISE Intermediate CA. 	
	Usage Certificate(s) will be used for EAP Authentication	
	Allow Wildcard Certificates 🔹	
	Node(s)	
	Generate CSR's for these Nodes:	
	Node CSR Friendly Name	
	☑ labise Isbise#EAP Authentication	

Schritt 4: Die von der ISE generierte CSR-Anfrage kann angezeigt werden. Klicken Sie auf **Ansicht**, wie im Bild dargestellt.



Schritt 5: Sobald der CSR generiert wurde, suchen Sie nach dem CA-Server und klicken Sie auf **Request a certificate** wie in der Abbildung dargestellt:

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

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

Schritt 6. Nachdem Sie ein Zertifikat angefordert haben, erhalten Sie Optionen für **Benutzerzertifikat** und **erweiterte Zertifikatanforderung.** Klicken Sie auf **Erweiterte Zertifikatanforderung**, wie im Bild dargestellt.

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

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request

Schritt 7: Fügen Sie die in der **Base-64-kodierten Zertifikatsanforderung** erzeugte CSR ein. Aus der **Zertifikatvorlage:** Wählen Sie **Web Server** aus, und klicken Sie auf **Submit (Senden**), wie im Bild dargestellt.

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 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	
Additional Attribu	ites:	
Attributes:	10	
	Submit >]

Schritt 8. Sobald Sie auf **Senden** klicken, erhalten Sie die Option, den Typ des Zertifikats auszuwählen, **Base-64 verschlüsselt** auszuwählen und auf **Download certificate chain** klicken, wie im Bild gezeigt.

Microsoft Active Directory Certificate Services fixer-WIN-97Q5HOKP9IG-CA
Certificate Issued
The certificate you requested was issued to you.
ODER encoded or OBase 64 encoded
Download certificate
Download certificate chain

Schritt 9: Der Zertifikatsdownload für den ISE-Server ist abgeschlossen. Sie können das Zertifikat extrahieren, das Zertifikat enthält zwei Zertifikate, ein Stammzertifikat und ein anderes Zwischenprodukt. Das Stammzertifikat kann importiert werden unter **Administration > Certificates > Trusted Certificates > Import** wie in den Bildern dargestellt.

dentity Services Engine	Home + Context Visibility + Operations + Polic	y -Administrat	ion + Work Centers				U	cense Warning 🔺 🔍	0 0	•
System → Identity Management →	Network Resources	id Services + Fe	ed Service + Threat Cent	ric NAC		Cic	here to do wireless set.	p and visibility setup Do r	tot show this again	. ×
Deployment Licensing Certificates	Logging + Maintenance Upgrade + Backup &	Restore + Admin	Access + Settings							
0										
Certificate Management	Trusted Certificates									_
System Certificates	/ Edit - Import Export Celete View							Show All	٣	8
Trusted Certificates	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date		

Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Deployment Licensing - Certificat	as ►Logging ► Maintenance Upgrade ► Backup & Restore ► Admin Access ► Settings	
Certificate Management	Import a new Certificate into the Certificate Store	
System Certificates	Certificate File Choose file No file chosen	
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	

Schritt 10: Wenn Sie auf **Senden** klicken, wird das Zertifikat der Liste der vertrauenswürdigen Zertifikate hinzugefügt. Außerdem wird das Zwischenzertifikat benötigt, um eine Bindung mit CSR herzustellen, wie im Bild dargestellt.

dentity Services Engine	Home Context Visibility Operations P	olicy Administration Work	Centers		License Warning 🔺 🧠 💿 🔿
System Identity Management	Network Resources Device Portal Management p	xGrid Services + Feed Service +	Threat Centric NAC		Click here to do wireless setup and visibility setup Do not show this again.
Deployment Licensing - Certif	cates + Logging + Maintenance Upgrade + Backup	& Restore + Admin Access + Se	ettings		
	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. Cli	ck "export" to download one or more CS	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	s bound, it will be removed from this its	L		
Certificate Signing Requests	PView ⊕Export ¥Delete Bind Certificate				Show All * 6
Certificate Periodic Check Setti	Friendly Name	Certificate Subject	Key Length Portal group tag	Timestamp 🔺 Host	t
	✓ ise#EAP Authentication	CN=ise.c.com	2048	Mon. 9 Jul 2018 ise	Created by Paint X

Schritt 11. Sobald Sie auf **Zertifikat binden** klicken, gibt es eine Option, um die Zertifikatsdatei auf Ihrem Desktop gespeichert wählen. Navigieren Sie zum Zwischenzertifikat, und klicken Sie wie im Bild dargestellt auf **Senden**.

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 (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

Schritt 12: Um das Zertifikat anzuzeigen, navigieren Sie zu **Administration > Certificates > System Certificates** wie im Bild dargestellt.

dentity Services Engine	Home + Context Visibility + Operation	ns + Policy - Administration + Work Center	rs -			License Warning 🔺 🔍 😐 🏦 🔿
System Identity Management	Network Resources + Device Portal Mana	ement pxGrid Services + Feed Service + Passi	veID + Threat Centric NAC			
Deployment Licensing Certificates + Logging + Maintenance Upgrade Backup & Restore + Admin Access + Settings						
0						
Certificate Management	System Certificates 🛕 For disaster r	ecovery it is recommended to export certificate and privat	e key pairs of all system certificates.			
Overview	/ Edit - Generate Self Signed Certi	icate 🕂 Import 🕃 Export 🗙 Delete 🔎 Vi	ew			
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 sami server cer ficate - CN=SAML_ise.c.com 	³ 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 Gro	up 🕧 ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 2020 🛛
Certificate Signing Requests						
Certificate Periodic Check Setti						
Certificate Authority						

Client für EAP-TLS

Benutzerzertifikat auf Client-Computer herunterladen (Windows-Desktop)

Schritt 1: Um einen Wireless-Benutzer über EAP-TLS zu authentifizieren, müssen Sie ein Client-Zertifikat generieren. Verbinden Sie den Windows-Computer mit dem Netzwerk, sodass Sie auf den Server zugreifen können. Öffnen Sie einen Webbrowser, und geben Sie die folgende Adresse ein: <u>https://sever ip addr/certsrv</u>

Schritt 2: Beachten Sie, dass die Zertifizierungsstelle mit der identisch sein muss, mit der das Zertifikat für die ISE heruntergeladen wurde.

Dazu müssen Sie nach dem gleichen CA-Server suchen, den Sie zum Herunterladen des Zertifikats für den Server verwendet haben. Klicken Sie auf derselben CA auf **Zertifikat anfordern** wie zuvor, diesmal müssen Sie jedoch **Benutzer** als Zertifikatvorlage auswählen, wie im Bild gezeigt.

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

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

Saved Request:

Base-64-encoded	ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIsPJry aF412aLpmDFp1PfVZ3VaP60a/mej3IXh0RFxBUII
(CMC or PKCS #10 or	weOhO6+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyDZ3
PKCS #70 01 PKCS #7):	ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX END CERTIFICATE REQUEST

Certificate Template:

ocranicate remp	u.o.		
	User	0	
Additional Attrib	utes:		
Attributes:		11.	
		Submit	t >

Schritt 3. Klicken Sie dann auf Download Zertifikatskette, wie zuvor für Server getan.

Wenn Sie die Zertifikate erhalten haben, gehen Sie wie folgt vor, um das Zertifikat auf Windows Laptop zu importieren:

Schritt 4: Um das Zertifikat zu importieren, müssen Sie von der Microsoft Management Console (MMC) darauf zugreifen.

- 1. Um die MMC zu öffnen, navigieren Sie zu Start > Ausführen > MMC.
- 2. Navigieren Sie zu Datei > Snap-In hinzufügen/entfernen
- 3. Doppelklicken Sie auf **Zertifikate**.
- 4. Wählen Sie Computerkonto aus.
- 5. Lokalen Computer auswählen > Fertig stellen
- 6. Klicken Sie auf **OK**, um das Snap-In-Fenster zu verlassen.
- 7. Klicken Sie auf [+] neben Zertifikate > Persönlich > Zertifikate.
- 8. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, und wählen Sie **Alle Aufgaben > Importieren aus**.
- 9. Klicken Sie auf Next (Weiter).
- 10. Klicken Sie auf Durchsuchen.

- 11. Wählen Sie die .cer, .crt oder .pfx aus, die Sie importieren möchten.
- 12. Klicken Sie auf Öffnen.
- 13. Klicken Sie auf Next (Weiter).
- 14. Wählen Sie den Zertifikatspeicher basierend auf dem Zertifikatstyp automatisch aus.
- 15. Klicken Sie auf Fertig stellen und OK.

Nach dem Import des Zertifikats müssen Sie Ihren Wireless-Client (in diesem Beispiel Windows Desktop) für EAP-TLS konfigurieren.

Wireless-Profil für EAP-TLS

Schritt 1: Ändern Sie das Wireless-Profil, das zuvor für Protected Extensible Authentication Protocol (PEAP) erstellt wurde, um stattdessen EAP-TLS zu verwenden. Klicken Sie auf **EAP** Wireless Profile.

Schritt 2. Wählen Sie **Microsoft: Smartcard oder anderes Zertifikat** und klicken Sie auf **OK** im Bild angezeigt.

EAP Wireless Network	Properties		×
Connection Security			
Security type:	WPA2-Enterprise	~	
Encryption type:	AES	~	
Choose a network auth Microsoft: Smart Card	or other certificate $$	Settings	
Remember my credentials for this connection each			
time I'm logged on			
Advanced cettings			
Advanced settings			
		OK (Cancel

Schritt 3: Klicken Sie auf **Einstellungen** und wählen Sie das vom CA-Server ausgestellte Stammzertifikat aus, wie im Bild dargestellt.

Smart Card or other Certificate Properties		
When connecting:		
O Use my smart card	Advanced	
Use a certificate on this computer		
Use simple certificate selection (Recommended)		
Verify the server's identity by validating the certific	cate	_
Connect to these servers (examples:srv1;srv2;.*)	srv3\.com):	
		0
Trusted Root Certification Authorities:		
Entrust.net Certification Authority (2048)		^
Equifax Secure Certificate Authority		
IVI fixer-WIN-97Q5HOKP9IG-CA		
GeoTrust Global CA		
GeoTrust Primary Certification Authority - G3		
GlobalSign Root CA		~
<	>	
Vie	w Certificate	
		- m

Schritt 4: Klicken Sie auf **Erweiterte Einstellungen**, und wählen Sie **Benutzer- oder Computerauthentifizierung** aus der Registerkarte mit den 802.1x-Einstellungen aus, wie im Bild dargestellt.

avanced settings		
802.1X settings 802.11 settings		
Specify authentication mode:		
User or computer authentication $~~$	Save cr	edentials
Delete credentials for all users		
Enable single sign on for this network		
Perform immediately before user logo	on	
Maximum delay (seconds):	10	* *
Allow additional dialogs to be display sign on	ed during s	ingle
This network uses separate virtual LA	Ns for mac	hine
and user authentication		

Schritt 5. Versuchen Sie nun, erneut eine Verbindung zum Wireless-Netzwerk herzustellen, wählen Sie das richtige Profil (in diesem Beispiel EAP) aus, und **verbinden Sie**. Sie sind wie im Bild dargestellt mit dem Wireless-Netzwerk verbunden.



Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Der Status des Client-Richtlinienmanagers muss als **RUN** angezeigt werden. Das bedeutet, dass der Client die Authentifizierung abgeschlossen und die IP-Adresse abgerufen hat und bereit ist, den im Bild angezeigten Datenverkehr weiterzuleiten.

Summary Access Points Cisco CleanAir	Max Number of Records General AVC Sta	Clear AVC Stats		
Statistics	Client Properties		AP Properties	
Boques	MAC Address	34:02:86:96:2f:b7	AP Address	00:d7:8f:52:db:a0
Rogues	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
vnc			Data Switching Central	
ocal Profiling			Authentication Central	
tocal 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	ut 0
	Address	N/A	WEP State	WEP Enable
	Mobility Move Count Policy Manager State	0 RUN	Lync Properties	
	Management Frame	No	Lync State	Disabled
	UnTime (Sec)	145	Audio Cos Policy	Ciluor

Schritt 2: Überprüfen Sie auch die richtige EAP-Methode auf dem WLC auf der Client-Detailseite, wie im Bild gezeigt.

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 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

Schritt 3. Hier sind die Client-Details aus der CLI des Controllers (Ausgabe abgeschnitten):

(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

Schritt 4: Navigieren Sie auf der ISE zu **Kontexttransparenz > Endpunkte > Attribute,** wie in den Bildern gezeigt.



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
Ľ	SelectedAuthenticationIdentityStores	EAPTLS
	SelectedAuthorizationProfiles	PermitAccess
ų.	Serial Number	10 29 41 78 00 00 00 00 01 11

Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Problembehebung für diese Konfiguration verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.