WLC 및 ISE를 사용하여 EAP-TLS 이해 및 구성

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 EAP-TLS 흐름 EAP-TLS 흐름의 단계 구성 Cisco Wireless LAN Controller Cisco WLC를 사용하는 ISE EAP-TLS 설정 ISE의 WLC 설정 ISE에서 새 사용자 생성 ISE의 인증서 신뢰 EAP-TLS용 클라이언트 클라이언트 컴퓨터에 사용자 인증서 다운로드(Windows 데스크톱) EAP-TLS용 무선 프로파일 다음을 확인합니다. 문제 해결

소개

이 문서에서는 802.1X 및 EAP-TLS를 사용하여 WLAN(Wireless Local Area Network)을 설정하는 방법에 대해 설명합니다

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 802.1X 인증 프로세스
- 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• WLC 3504 버전 8.10

• ISE(Identity Services Engine) 버전 2.7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

EAP-TLS 흐름



EAP-TLS 흐름의 단계

- 1. 무선 클라이언트가 액세스 포인트(AP)에 연결됩니다. AP는 클라이언트가 이 시점에서 데이터 를 전송하도록 허용하지 않으며 인증 요청을 보냅니다. 그러면 신청자가 EAP-Response ID로 응답합니다. 그런 다음 WLC는 사용자 ID 정보를 인증 서버에 전달합니다. RADIUS 서버는 EAP-TLS 시작 패킷으로 클라이언트에 응답합니다. EAP-TLS 대화가 이 시점에서 시작됩니다
- 2. 피어는 NULL로 설정된 암호인 "client_hello" 핸드셰이크 메시지가 포함된 인증 서버로 EAP-Response를 다시 보냅니다
- 3. 인증 서버는 다음을 포함하는 Access-challenge 패킷으로 응답합니다.

TLS server_hello handshake message certificate server_key_exchange certificate request server_hello_done. 4. 클라이언트는 다음 항목을 포함하는 EAP 응답 메시지로 응답합니다. 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.클라이언트가 성공적으로 인증되면 RADIUS 서버는 "change_cipher_spec" 및 핸드셰이크 완료 메시지를 포함하는 Access-challenge로 응답합니다.

6.이를 수신하면 클라이언트는 radius 서버를 인증하기 위해 해시를 확인합니다.

7. 새 암호화 키는 TLS 핸드셰이크 중에 암호에서 동적으로 파생됩니다

8/9.EAP-Success가 서버에서 인증자로 최종 전송되면 신청자에게 전달됩니다.

이때 EAP-TLS가 활성화된 무선 클라이언트는 무선 네트워크에 액세스할 수 있습니다.

구성

Cisco Wireless LAN Controller

1단계. 첫 번째 단계는 Cisco WLC에서 RADIUS 서버를 구성하는 것입니다. RADIUS 서버를 추가 하려면 Security(보안) > RADIUS > Authentication(인증)으로 이동합니다. 이미지에 표시된 대로 New(새로 만들기)를 클릭합니다.

AAP Promit Promit <	cisco	MONITOR	WLANS CO	NTROLLER	WIRELE	SS SECURITY	MANAGEMENT	T COMMANDS	HELP				User:admi
AA Benel A. Cardet Sker A. Cardet Sker A. Cardet Sker B. Cardet Sker	Security	RADIUS /	Authenticati	on Serve	ers								A
 With and the second of the second o	General	Auth Calle	ed Station ID Typ	AP N	Name:SSID	v							
Accounting Auth Codenduers Falback Dors Downloaded AVP P CACCS+ Dard Develoaded AVP P CACCS+ Load Net Werk MAC Delinities Auth Codenduers P Falorities P Falorities Auth Codenduers P Falorities P Falorities P Falorities Auth Codenduers P Falorities P Falorities </td <td>* RADIUS Authentication</td> <td>Use AES K</td> <td>Key Wrap</td> <td>(Der</td> <td>signed for FI</td> <td>PS customers an</td> <td>d requires a key wr</td> <td>rap compliant RAD</td> <td>IUS server)</td> <td></td> <td></td> <td></td> <td></td>	* RADIUS Authentication	Use AES K	Key Wrap	(Der	signed for FI	PS customers an	d requires a key wr	rap compliant RAD	IUS server)				
Pathack: Prend MU DNS Dominoladd AVP LADAP Immode MVP LADAP Immode MVP LADAP Immode MVP LADAP Immode MVP MAC Fliering Immode MVP Priority Order Immode MVP Policies Immode MVP Policies Immode MVP MAC Fliering Immode MVP MAC Fliering Immode MVP Priority Order Immode MVP Machance Immode MVP Machance Immode MVP Machance I	Accounting Auth Cached U	Jsers MAC Delin	niter	Colo	yn v	•							
Demioside AVP Network Tunnel Server Address [1pv4/1pv6) Pot 1984c Admin Satus Local Net Users 1 138.77.0.84 1812 Disabled Disabled 0 Bisable (Disabled) 0 2 138.77.0.83 1812 Disabled 0 Disable (Disabled) 0 3 138.77.97.20 1812 Disabled Disabled 0 AP Policies 0 4 138.77.97.21 1812 Disabled Disabled 0 Password Policies 0 5 172.27.171 1812 Disabled Enabled 0 Password Policies 0 6 10.100.120.41 1812 Disabled Enabled 0 Priority Order 5 172.27.171 1812 Disabled Enabled 0 Advanced EAP 0 6 10.100.120.41 1812 Disabled Enabled 0 Priority Order 5 10.100.120.41 1812 Disabled Enabled 0 Vitreless Protection Policies 0 6 10.100.120.41 1812 Disabled Enabled 0 Vitreless Protection Policies 0 6 10.100.120.41 1812 Disabled Enabled 0 Vitreless Protection Policies 0 0 0 0 0 0 0 Vitreless Protection Policies 0 0 0 0 0 0 Vitreless Protection Policies 0 0 0 0 0 0 Vit	Fallback DNS	Framed M	πυ	1300	0								
Local Net Users 1 138.77.97.20 1812 Disabled D	Downloaded AV TACACS+	VP Network User	Management	Tunnel Se Proxy In	erver	Server Address	s(Ipv4/Ipv6)		Port	IPSec	Admin Status		
McCelltering • Disabled • Disabled </td <td>Local Net Users</td> <td></td> <td></td> <td>1</td> <td></td> <td>138.77.0.84</td> <td></td> <td></td> <td>1812</td> <td>Disabled</td> <td>Disabled</td> <td></td> <td></td>	Local Net Users			1		138.77.0.84			1812	Disabled	Disabled		
User Login Policies Advanced Mirelas Mirela	MAC Filtering			2		138.77.0.83			1812	Disabled	Disabled		
AP Policies Password Policies Cal EAP 6 10.100.120.41 1812 Disabled Enabled Priority Order Certificate Access Control Lists Wireless Protection Policies Umbrelia Advanced	 Disabled Clients User Login Policies 			3		138.77.97.20			1812	Disabled	Disabled		
Password Policies Cecil EAP Advanced EAP Priority Order Certificate Access Control Lists Wieb Auth TrustSec Local Policies Umbrelia Advanced	AP Policies			4		138.77.97.21			1812	Disabled	Disabled		
Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrelia Advanced	Password Policies			D 5	•	172.27.1.71			1812	Disabled	Enabled		
Advanced EAP Priority Order Certificate Access Control Lists Wineless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced	Local EAP			6		10.100.120.41			1812	Disabled	Enabled		
 Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrelia Advanced 	Advanced EAP												
 Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced 	Priority Order												
 Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced 	Certificate												
Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced	Access Control L	Lists											
Web Auth TrustSec Local Policies Umbrella Advanced	Wireless Protect Policies	tion											
TrustSec Local Policies Umbrella Advanced	Web Auth												
Local Policies Umbrella Advanced	TrustSec												
Umbrella Advanced	Local Policies												
Advanced	Umbrella												
	Advanced												
									_				

2단계. 여기서 ISE의 WLC를 검증하기 위해 사용되는 IP 주소와 공유 암호 <password>를 입력해야 합니다. 이미지**에** 표시된 대로 계속하려면 Apply를 클릭합니다.

սիսիս			Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 🔒 Home
Security	RADIUS Authentication Serve	rs > Edit	< Back Apply
AAA General KADIUS Authentication Accounting Authentication Accounting Authentication Accounting Authentication Authentication Authentication Authentication Authentication Authentication Painet DNS Downloaded AVP TACACS+ LOAP LOAR LOAR	Server Index Server Index Server Address([pv4/[pv6) Shared Secret Confirm 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	rs > Exit 7 10.106.35.67 ASCII •• •••	< Back Apply

3단계. RADIUS 인증을 위한 WLAN을 생성합니다.

이제 새 WLAN을 생성하고 WPA-엔터프라이즈 모드를 사용하도록 구성하여 인증에 RADIUS를 사용할 수 있습니다.

4단계. 주 메뉴에서 WLANs를 선택하고 Create New(새로 만들기)를 선택한 후 Go(이동)를 클릭합 니다.

uluulu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	Save 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 Y Go	
Advanced	WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies	

5단계. 새 WLAN EAP-TLS의 **이름을 지정합니다**. 이미지**에** 표시된 대로 계속하려면 Apply를 클릭 합니다.

uluulu cisco		TROLLER WIRELESS SE	CURITY MANAGEMENT	COMMANDS	HELP	Save Configuration Ping Logout Refresh User:admin(ReadWrite) n Home
WLANs	WLANs > New					< Back Apply
 WLANS WLANS Advanced 	Type Profile Name SSID ID	WLAN V EAP-TLS EAP-TLS 3 V				

6단계. **General(일반)**을 클릭하고 Status(상태)가 Enabled(활성화됨)**인지 확인합니다**. 기본 보안 정 책은 이미지에 표시된 802.1X 인증 및 WPA2입니다.

cisco	MONITOR WLANS CON	TROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	Save Configuration Ping User:admin(Read)	Logout <u>R</u> efresh Nrite) <mark>A H</mark> ome
WLANs	WLANs > Edit 'EAP-1	rLS'	< Back	Apply
WLANs WLANS	General Security	QoS Policy-Mapping Advanced		
Advanced	Profile Name	EAP-TLS		
	SSID	EAP-TLS		
1	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)		
	Radio Policy Interface/Interface Group(G)	All v management v		
	Multicast Vlan Feature	Enabled		
	Broadcast SSID NAS-ID	C Enabled none		
	11ax Status	Z Enabled		
,	Lobby Admin Access	0		

7단계. 이제 Security(보안) > AAA Servers(AAA 서버) 탭으로 이동하여 이미지에 표시된 대로 방금 구성한 RADIUS 서버를 선택합니다.

ahaha	, in the second s	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	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 Apply Cisco ISE Default Settings Enabled Authentication Servers Accounting Servers EAP Parameters EAP Parameters Enabled Enabled Enabled Enabled	
	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 v	

참고: 계속하기 전에 WLC에서 RADIUS 서버에 연결할 수 있는지 확인하는 것이 좋습니다. RADIUS는 (인증을 위해) UDP 포트 1812를 사용하므로 이 트래픽이 네트워크의 어느 곳에서 도 차단되지 않도록 해야 합니다.

Cisco WLC를 사용하는 ISE

EAP-TLS 설정

정책을 빌드하려면 정책에서 사용할 수 있는 프로토콜 목록을 만들어야 합니다. dot1x 정책이 작성 되었으므로 정책 구성 방법에 따라 허용되는 EAP 유형을 지정합니다.

기본값을 사용하는 경우, 특정 EAP 유형에 대한 액세스를 잠가야 하는 경우 선호되지 않는 인증에 대부분의 EAP 유형을 허용합니다.

1단계. 이미지에 표시된 대로 Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authentication(인증) > Allowed Protocols(허용된 프로토콜)로 이동하고 Add(추가)를 클릭합니다.

dentity Services Engine	Home 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 X Delete
	Service Name Description
▶ Profiling	Default Network Access Default Allowed Protocol Service
► Posture	
Client Provisioning	

2단계. 이 Allowed Protocol(허용된 프로토콜) 목록에서 목록의 이름을 입력할 수 있습니다. 이 경우 이미지에 표시된 대로 **Allow EAP-**TLS(EAP-TLS 허용) 상자가 선택되고 다른 상자가 선택되지 않습 니다.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
Authentication Authorization Profili	ng Posture Client Provisioning - Policy Elements	
Dictionaries Conditions - Results	5	
0	Allowed Protocole Soprions List > New Allowed Protocole Somice	
✓ Authentication	Allowed Protocols	
Allowed Protocols	Name EAP-TLS	
Authorization	Description	
• Drofiling		
Proming	✓ Allowed Protocols	
 Posture 		
Client Provisioning	Authentication Bypass	
	Process Host Lookup ()	
	Authentication Protocols	
	Allow MS-CHAPV1	
	Allow MS-CHAPv2	
	Allow EAP-MD5	
	✓ Allow EAP-TLS	
	Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)	
	Enable Stateless Session Resume	
	Session ticket time to 2 Hours	
	Proactive session ticket update will occur after 10 % of Time To Live has expired	
	Allow LEAP	
	- Allow PEAP	
	PEAP Inner Methods	
	Allow EAP-MS-CHAPv2	
	Allow Password Change Retries 1 (Valid Range 0 to 3)	
	Allow EAP-GTC	
	Allow Password Change Retries 1 (Valid Range 0 to 3)	
	Allow FAP-TI S	
	Allow Authentication of avaired partificates to allow partificate renewal in Authorization Dallow	
	Require cryptobinding TLV (i)	_

ISE의 WLC 설정

1단계. ISE 콘솔을 열고 이미지에 표시된 대로 Administration > Network Resources > Network Devices > Add로 이동합니다.

Hole Identity Services Engine	ame + Control Visibility + Operations + Policy +Administration	en Vitark Centers		License Warning 🔺 🔍 🔍 🔘
+ System + Identity Management +	etwork Resources + Device Portal Management pr0rid Services + Fer	ed Service + Threat Centric NAC		Click here to do wireless setup and visibility setup Do not show this again
Network Devices Network Device Gro	ps Network Device Profiles External RADIUS Servers RADIUS Server	Sequences NAC Managers External MDM + Location Services		
•				
Network devices	Network Devices			
Default Device				Samand O Tasa 2 🥵 👺 🖕
Device Security Settings	/ Eft +44 Doulote @inant @inant . OGeneste Hit	C XOdete -		Stov Al 🔹 😵
	Name a 19/9task Profile Name	Location Type	Description	

2단계. 이미지에 표시된 대로 값을 입력합니다.

cisco Identity Services Engine	Home	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	Click b
Network Devices Network Device G	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	
Default Device		
Device Security Settings	Penetrika P	
	Lesuipun	
	IP Address v * IP : 10.106.35.67 / 32	
	Device Profile the Cisco + (f)	
	Model Name T	
	Software Version	
	Network Device Group	
	Location All Locations O 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 @	

ISE에서 새 사용자 생성

1단계. 이미지에 표시된 것과 같이 Administration(관리) > Identity Management(ID 관리) > ID > Users(사용자) > Add(추가)로 이동합니다.



2단계. 이미지에 표시된 정보를 입력합니다.

Identity Services Engin	e Home ► Context Visibility ► Operations ► Policy
► System - Identity Managem	ent Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
✓Identities Groups Externa	I Identity Sources Identity Source Sequences
	0
Users	Network Access Users List > New Network Access User
Latest Manual Network Scan Resu	ts
	* Name bharti
	Status Enabled -
	Email
	▼ Passwords
	Password Type: Internal Users 💌
	Password Re-Enter Password
	* Login Password Generate Password (i)
	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

ISE의 인증서 신뢰

1단계. Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인 증서 관리) > Trusted certificates(신뢰할 수 있는 인증서)로 이동합니다.

인증서를 ISE로 가져오려면 Import(가져오기)를 클릭합니다. ISE에서 WLC를 추가하고 사용자를 생성하면 EAP-TLS에서 가장 중요한 부분인 ISE의 인증서를 신뢰해야 합니다. 이를 위해 CSR을 생 성해야 합니다.

2단계. 이미지에 표시된 대로 Administration(관리) > Certificates(인증서) > Certificate Signing Requests(인증서 서명 요청) > Generate Certificate Signing Requests (CSR)(CSR(인증서 서명 요 청 생성)로 이동합니다.

dentity Services Engin	Home	License Warring 🔺 🔍 📵 🔿 🗘
▼ System → Identity Manageme	nt → Network Resources → Device Portal Management pxGrid Services → Feed Service → Threat Centric NAC	
Deployment Licensing - Cer	ficates + 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 "bind" to bind the request to the
OCSP Client Profile	signed definicate issues by that automity. Once a Concis bound, it will be removed from this list.	
Certificate Signing Requests	Diview Carbinate Bind Certificate	Show All V
Certificate Periodic Check Setti	Friendly Name Certificate Subject Key Length	Portal group tag Timestamp 🔺 Host
Certificate Authority		No data available

3단계. CSR을 생성하려면 Usage(**사용)**로 이동하고 **Certificate(s) is used for** drop(인증서**(s) is** used for 드롭다운 옵션에서 이미지에 표시된 대로 EAP Authentication(EAP **인증)을** 선택합니다.

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 will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:			
Tristeri Certificates	ISE Identity Certificates:			
OCSP Client Profile	Multi-Use (Admin, EAP, Pontal, pxGrid) - Client and Server Authentication Admin, Server & thentication			
Cartificate Signian Requests	EAP Authentication - Server Authentication			
Certificate Deriver Chark Setti	DTLS Authentication - Server Authentication Pontal - Server Authentication			
Contracto Parkard on Contractor	pxGrid - Client and Server Authentication			
Certificate Authority	SAML - SAML Signing Certificate			
)	ISE Certificate Authority Certificates:			
	 ISE Noti CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality. ISE Informediate CA - This is an Informediate 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 Double Address and the signing request, but an ability to renew the DCSP responder certificate that is signed by the 			
	ISE Root CANSE Intermediate CA			
	Usage			
	Certificate(s) will be used for EAP Authentication			
	Allow Wildcard Certificates 🛛 🛈			
	Nodels			
	Generate CSR's for these Nodes:			
	Nuclea OOD Eduards Name			
	Note Con Friendy name			
	☑ labisetEAP Authentication			

4단계. ISE에서 생성된 CSR을 볼 수 있습니다. 이미지에 표시된 대로 View(보기)를 클릭합니다.



5단계. CSR이 생성되면 이미지에 표시된 대로 CA 서버를 찾아 **Request a certificate(인증서 요청**)를 클릭합니다.

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

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

6단계. 인증서를 요청하면 이미지에 표시된 대로 **사용자 인증서** 및 **고급 인증서 요청**에 대한 옵션을 얻고 **고급 인증서 요청**을 클릭합니다.

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

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request

7단계. Base-64 인코딩 인증서 요청에서 생성된 CSR을 붙여넣습니다. 인증서 템플릿에서 드롭다 운 옵션에서 웹 서버를 선택하고 이미지에 표시된 대로 Submit(제출)을 클릭합니다.

Microsoft Active Director	y Certificate Services - 1	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	
Additional Attribu	utes:	
Attributes:	li l	
	Submit >	

8단계. Submit(제출)을 클릭하면 인증서 유형을 선택하고 Base-64 encoded(Base-64 인코딩)를 선 택한 다음 그림과 같이 Download certificate chain(인증서 체인 다운로드)을 클릭하는 옵션이 제공 됩니다.

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

9단계. ISE 서버에 대한 인증서 다운로드가 완료되었습니다. 인증서를 추출할 수 있으며, 인증서에 는 두 개의 인증서, 하나의 루트 인증서 및 다른 중간 인증서가 포함됩니다. 이미지에 표시된 대로 Administration(관리) > Certificates(인증서) > **Trusted certificates(신뢰할 수 있는 인증서) >** Import(가져오기)에서 루트 인증서를 가져올 수 있습니다.

dentity Services Engine	Home + Context Visibility + Operations + Po	icy - Administrat	ion + Work Centers				Lic	cense Warning 🔺 🔍 🔍	0 0	•
System Identity Management	Network Resources	Grid Services + Fe	ed Service + Threat Cent	ric NAC		Cic	chere to do wireless setu	p and visibility setup Do n	tot show this again.	×
Deployment Licensing - Certificates	Logging Maintenance Upgrade Backup	& Restore + Admin	Access > Settings							
0										- 1
- Certificate Management	Trusted Certificates									_
System Certificates	/ Edit -Import Delete View							Show All	*	õ
Trusted Certificates	Friendly Name	 Status 	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date		

Hom

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	Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings	
0		
✓ 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>i</i>
OCSP Client Profile	Trusted For:	
Certificate Signing Requests	Truct for authentication within ICE	
Certificate Periodic Check Setti		
 Cortificate Authority 	Irust for client authentication and Syslog	
Certificate Authority	Trust for authentication of Cisco Services	
	Validate Certificate Extensions	
	Description	1
	Submit Cancel	-

10단계. Submit(제출)을 클릭하면 인증서가 신뢰할 수 있는 인증서 목록에 추가됩니다. 또한 중간 인증서가 필요한 이유는 그림과 같이 CSR과 바인딩하기 위해서입니다.



11단계. Bind certificate(**인증서 바인딩**)를 클릭하면 데스크톱에 저장된 인증서 파일을 선택할 수 있 습니다. 중간 인증서를 찾아 이미지에 표시된 대로 **Submit**(제출)을 클릭합니다.

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
0	
- Certificate Management	Bind CA Signed Certificate
System Certificates	* Certificate File Choose file No file chosen
Trusted Certificates	
OCSP Client Profile	Friendly Name (i)
Certificate Signing Requests	Validate Certificate Extensions
Certificate Periodic Check Setti	
Certificate Authority	Usage
	EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
	Submit Cancel

12단계. 인증서를 보려면 이미지에 표시된 대로 Administration > Certificates > System Certificates로 이동합니다.

dentity Services Engine	Home + Context Visibility + Operation	ons + Policy - Administration + Work Centers			License W	taming 🔺 🔍 🌖	• 1 •
System Identity Management	Network Resources	gement pxGrid Services + Feed Service + PassiveID	Threat Centric NAC				
Deployment Licensing - Certificates	+ Logging + Maintenance Upgrade	Backup & Restore + Admin Access + Settings					
0							
Certificate Management	System Certificates 🛕 For disaster	recovery it is recommended to export certificate and private key	pairs of all system certificates.				
Overview	📝 Edit 🛛 🕂 Generate Self Signed Certi	ficate 🕂 Import 😨 Export 🗶 Delete 🔎 View					
System Certificates	Friendly Name	Used By Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
Endpoint Certificates	▼ ise						
Trusted Certificates	 Default self-signed sami server ce ficate - CN=SAML_ise.c.com 	^{rti} SAML	SAML_ise.c.com	SAML_ise.c.com	Wed, 11 Jul 2018	Thu, 11 Jul 2019	2
OCSP Client Profile	 intermediate 	EAP Authentication, Admin, Portal Default Portal Certificate Group ()	ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 2020	
Certificate Signing Requests	L						
Certificate Periodic Check Setti							

Certificate Authority

EAP-TLS용 클라이언트

클라이언트 컴퓨터에 사용자 인증서 다운로드(Windows 데스크톱)

1단계. EAP-TLS를 통해 무선 사용자를 인증하려면 클라이언트 인증서를 생성해야 합니다. 서버에 액세스할 수 있도록 Windows 컴퓨터를 네트워크에 연결합니다. 웹 브라우저를 열고 다음 주소를 입력합니다. <u>https://sever ip addr/certsrv—</u>

2단계. CA는 ISE에 대해 인증서를 다운로드한 것과 동일해야 합니다.

이 경우 서버용 인증서를 다운로드하는 데 사용한 것과 동일한 CA 서버를 찾아야 합니다. 동일한 CA에서 이전에 수행한 것처럼 **Request a certificate(인증서 요청)**를 클릭합니다. 그러나 이번에는 이미지에 표시된 것처럼 Certificate Template(인증서 템플릿)으로 **User(사용자)**를 선택해야 합니다 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	weOhO6+V+eh71jeTgiwzEZGr/ceYJIakco5zLjgR dD7LeujkxF1j3SwvLTKLDJq+00VtAhrx1p1PyDZ3
PKCS #10 or PKCS #7):	ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX END CERTIFICATE REQUEST

Certificate Template:

	User	۵	
L Additional Attribu	utes:		
Attributes:		//.	
		Subr	nit >

3단계. 그런 다음 서버에 대해 이전에 수행한 **인증서 체인** 다운로드를 클릭합니다.

인증서를 가져오면 다음 단계에 따라 Windows 노트북 컴퓨터에서 인증서를 가져옵니다.

4단계. 인증서를 가져오려면 MMC(Microsoft Management Console)에서 액세스해야 합니다.

- 1. MMC를 열려면 시작 > 실행 > MMC로 이동합니다.
- 2. File(파일) > Add/Remove Snap In(스냅인 추가/제거)으로 이동합니다.
- 3. Certificates(**인증서**)를 두 **번 클릭합니다**.
- 4. 컴퓨터 계정을 선택합니다.
- 5. 로컬 **컴퓨터 > 마침** 선택
- 6. 스냅인 **창**을 종료하려면 확인을 클릭합니다.
- 7. Certificates(인증서) > Personal(개인) > Certificates(인증서) 옆에 있는 [+]를 클릭합니다.
- 8. Certificates(**인증서**)를 마우스 오른쪽 버튼으로 클릭하고 **All Tasks(모든 작업)** > Import(가져 오기**)를** 선택합니다.
- 9. Next(다음)를 클릭합니다.
- 10. Browse(찾아보기)**를 클릭합니다**.
- 11. 가져올 .cer, .crt 또는 .pfx를 선택합니다.
- 12. 열기를 **클릭합니다**.

13. Next(다음)를 클릭합니다.

14. 인증서**의 유형에 따라 자동으로 인증서 저장소를 선택합니다**.

15. Finish(마침) 및 OK(확인)를 클릭합니다.

인증서 가져오기가 완료되면 EAP-TLS에 대한 무선 클라이언트(이 예에서는 windows 데스크톱)를 구성해야 합니다.

EAP-TLS용 무선 프로파일

1단계. 이전에 PEAP(Protected Extensible Authentication Protocol)에 대해 생성한 무선 프로파일을 변경하여 EAP-TLS를 대신 사용합니다. EAP **무선 프로파일을 클릭합니다**.

2단계. Microsoft **선택: 스마트 카드 또는 기타 인증서**를 선택하고 이미지에 표시된 OK(확인)를 클 릭합니다.

EAP Wireless Network	Properties		×
Connection Security			
Security type:	WPA2-Enterprise	~	
Encryption type:	AES	~	
Choose a network auth Microsoft: Smart Card	or other certificate	Sattings	
		Settings	
Remember my cre	dentials for this connecti	on each	c c
time I'm logged on	1		
Advanced settings			
		ОК	Cancel
L			

3단계. 설정을 클릭하고 이미지에 표시된 대로 CA 서버에서 발급된 루트 인증서를 선택합니다.

Smart Card or other Certificate Properties		
When connecting:		
O Use my smart card	Advanced	
Use a certificate on this computer		
Use simple certificate selection (Recommende	d)	
Verify the server's identity by validating the cer	tificate	_
Connect to these servers (examples:srv1;srv2	;.*\.srv3\.com):	
Trusted Poot Cartification Authorities:		9
Entrust net Certification Authority (2048)		•
Equifax Secure Certificate Authority	,	
fixer-WIN-97Q5HOKP9IG-CA		
GeoTrust Global CA		
GeoTrust Primary Certification Authority		
GeoTrust Primary Certification Authority - G3		
GlobalSign Root CA		~
<	>	
	View Certificate	

4단계. Advanced Settings(고급 설정)를 클릭하고 이미지에 표시된 802.1x 설정 탭에서 User or computer authentication(사용자 또는 컴퓨터 인증)을 선택합니다.

gu	802.11 settings		
Specify a	authentication mode:		
User or	computer authentication	n \vee Save cr	edentials
Dele	te credentials for all use	rs	
Enable s	ingle sign on for this net	twork	
Perfo	orm immediately before	user logon	
O Perfo	orm immediately after us	ser logon	
h.d	m delay (seconds):	10	•
Maximu			
Maximu Allov sign	v additional dialogs to be on	e displayed during s	single

5단계. 이제 무선 네트워크에 다시 연결해 보십시오. 올바른 프로파일(이 예에서는 EAP)을 선택하 고 **연결합니다**. 이미지에 표시된 대로 무선 네트워크에 연결됩니다.

(i.	EAP Connected, secured
(k)	blizzard-legacy Secured
(h)	blizzard Secured
%	internet Open
(î.	dot1x_test Secured
(i.	JioPrivateNet Secured, Hotspot 2.0
6	mac_filter Secured
Net Cha	twork & Internet settings nge settings, such as making a connection metere
ر Wi-F	تي هري المحمد المحمد المحمد المحمد

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계. 클라이언트 정책 관리자 상태는 RUN으로 **표시되어야 합니다**. 이는 클라이언트가 인증을 완 료하고 IP 주소를 얻었으며 이미지에 표시된 트래픽을 전달할 준비가 되었음을 의미합니다.

Summary Access Points Cisco CleanAir	Max Number of Records General AVC Sta	10 ¢ 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_3rdfloo
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	
			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 timeor	ut 0
	Address	N/A	WEP State	WEP Enable
	Mobility Move Count	0 DUN	Lync Properties	
	Management Frame	No	Lync State	Disabled
	Protection	146	Audio Con Deliny	Cilver

2단계. 또한 이미지에 표시된 대로 클라이언트 세부사항 페이지에서 WLC의 올바른 EAP 방법을 확 인합니다.

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

3단계. 다음은 컨트롤러의 CLI에서 클라이언트 세부사항입니다(출력 잘림).

(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 4단계. ISE에서 이미지에 표시된 대로 Context Visibility(컨텍스트 가시성) > End Points(엔드포인트) > Attributes(특성)로 이동합니다.

dentity Services Engine	Home -Co	ntext Visibility	Operations	+ Policy	Administration	Work Centers	
Endpoints Network Devices							
Endpoints > 34:02:86:96:2F:B7							
34:02:86:96:2F:B7							
Username: Administ	trator@fixer.com						
Current IP Address:	N-Device						
Allebudes Authoritection	Threate	Misseshilling					
Aunenscason	Threats	vuinerabilities					
General Attributes							
Description							
Static Assignment false							
Endpoint Policy Intel-De	vice						
Static Group Assignment false							
Identity Group Assignment Profiled							
Custom Attributes							
						▼ Filter -	¢-
Attribute Name		Attribute Value	9				
× Attribute Name		Attribute Value					
No data found. Add custom attribu	utes here.						
Other Attributes							
AAA-Server	ise						
AKI	88:20:a7:c9:96:0	03:5a:26:58:fd:67	:58:83:71:e8:bc:c6:	6d:97:bd			
Airespace-Wlan-Id	5						
AllowedProtocolMatchedRule	Dot1X						
AuthenticationIdentityStore	Internal Users						
AuthenticationMethod	x509_PKI						

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

1.00		
	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
	Serial Number	10 29 41 78 00 00 00 00 11

문제 해결

현재 이 구성에 대한 문제 해결에 사용할 수 있는 특정 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.