# LSC를 사용하는 PEAP 또는 EAP-TLS에 대해 AP에 802.1X 구성

목차					
<u>소개</u>					
사전 요구 사항					
요구 사항					
사용되는 구성 요소					
<u>배경 정보</u>					
네트워크 다이어그램					
<u>구성</u>					
Windows Server 2016 SCEP CA					
<u>인증서 템플릿 및 레지스트리 구성</u>					
<u>9800에서 LSC 구성</u>					
AP LSC GUI 컨피그레이션 단계					
AP LSC CLI 컨피그레이션 단계					
<u>AP LSC 확인</u>					
LSC 프로비저닝 문제 해결					
<u>LSC를 사용하는 AP 유선 802.1X 인증</u>					
<u>AP 유선 802.1x 인증 컨피그레이션 단계</u>					
<u>AP 유선 802.1x 인증 GUI 컨피그레이션</u>					
<u>AP 유선 802.1x 인증 CLI 컨피그레이션</u>					
<u>AP 유선 802.1x 인증 스위치 컨피그레이션</u>					
RADIUS 서버 인증서 설치					
<u>AP 유선 802.1x 인증 확인</u>					
<u>802.1X 인증 문제 해결</u>					
<u>관련 정보</u>					

# 소개

이 문서에서는 802.1X PEAP 또는 EAP-TLS 방법을 사용하여 스위치 포트에서 Cisco 액세스 포인 트를 인증하는 방법에 대해 설명합니다.

# 사전 요구 사항

## 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

• 무선 컨트롤러

- 액세스 포인트
- 스위치
- ISE 서버
- 인증 기관.

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 무선 컨트롤러: 17.09.02를 실행하는 C9800-40-K9
- 액세스 포인트: C9117AXI-D
- 스위치: 17.06.04를 실행하는 C9200L-24P-4G
- AAA 서버: 3.1.0.518을 실행하는 ISE-VM-K9
- 인증 기관: Windows Server 2016

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

액세스 포인트(AP)가 802.1X를 사용하여 스위치 포트로 인증하도록 하려면 기본적으로 인증서가 필요하지 않은 EAP-FAST 인증 프로토콜을 사용합니다. AP가 PEAP-mschapv2 방법(AP 측에서는 자격 증명을 사용하지만 RADIUS 측에서는 인증서를 사용) 또는 EAP-TLS 방법(양측에서 인증서를 사용)을 사용하도록 하려면 먼저 LSC를 구성해야 합니다. 액세스 포인트에 신뢰할 수 있는/루트 인 증서를 프로비저닝하는 유일한 방법입니다(EAP-TLS의 경우 디바이스 인증서도 제공). AP가 PEAP를 수행하고 서버 측 검증을 무시하는 것은 불가능합니다. 이 문서에서는 먼저 LSC를 구성한 다음 802.1X 컨피그레이션 측면에 대해 다룹니다.

PKI가 더 나은 보안을 제공하고, CA(Certificate Authority)를 제어하고, 생성된 인증서에 대한 정책, 제한 및 사용을 정의하려면 LSC를 사용합니다.

LSC를 사용하면 컨트롤러는 CA에서 발급한 인증서를 받습니다. AP는 CA 서버와 직접 통신하지 않지만 WLC는 조인하는 AP를 대신하여 인증서를 요청합니다. CA 서버 세부사항은 컨트롤러에서 구성해야 하며 액세스할 수 있어야 합니다.

컨트롤러는 SCEP(Simple Certificate Enrollment Protocol)를 사용하여 디바이스에서 생성된 certReq를 CA로 전달하고 SCEP를 다시 사용하여 CA에서 서명된 인증서를 가져옵니다.

SCEP는 PKI 클라이언트 및 CA 서버가 인증서 등록 및 취소를 지원하는 데 사용하는 인증서 관리 프로토콜입니다. Cisco에서 널리 사용되며 많은 CA 서버에서 지원됩니다. SCEP에서는 HTTP가 PKI 메시지의 전송 프로토콜로 사용됩니다. SCEP의 기본 목표는 네트워크 디바이스에 인증서를 안전하게 발급하는 것입니다.

## 네트워크 다이어그램



# 구성

SCEP CA와 9800 WLC의 두 가지 주요 구성 사항이 있습니다.

Windows Server 2016 SCEP CA

이 문서에서는 실습을 위한 Windows Server SCEP CA의 기본 설치에 대해 설명합니다. 실제 프로 덕션 등급의 Windows CA는 기업 운영에 적합하도록 안전하고 적절하게 구성해야 합니다. 이 섹션 에서는 Lab에서 테스트하고 이 컨피그레이션이 작동하도록 하는 데 필요한 설정에서 영감을 얻을 수 있습니다. 단계는 다음과 같습니다.

1단계.새로운 Windows Server 2016 데스크톱 경험을 설치합니다.

2단계. 서버가 고정 IP 주소로 구성되어 있는지 확인합니다.

3단계.새 역할 및 서비스를 설치하고 Active Directory 도메인 서비스 및 DNS 서버부터 시작합니다.

Add Roles and Features Wizard - C X age Tools View He DESTINATION SERVER WIN-3E202T1QDOU Before You Begin Installation Type Server Selection Server Roles Features DNS Server AD DS Confirmation Results Before You Begin Installation Type Server Coles Features DNS Server AD DS Confirmation Results Confirmation Confirmation Results Confirmation Results Confirmation Confirmation Results Confirmation Results Confirmation Confirmation Confirmation Confirmation Confirmation Confirmation Results Confirmation Confir	$\times$		- 0									Manager	🚖 Serv
Select server roles       DESTINATION SERVER WIN-3E202T1QDOU         Before You Begin Installation Type Server Selection       Select one or more roles to install on the selected server.         Roles       Description         Active Directory Certificate Services Features DNS Server AD DS Confirmation Results       Active Directory Certificate Services Active Directory Releation Services Device Health Attestation DHCP Server DHCP Server DHC	P	Hel	View	Tools	age	×		-				Add Roles and Features Wizard	
Before You Begin       Select one or more roles to install on the selected server.         Installation Type       Roles         Server Selection       Active Directory Certificate Services         Server Roles       Active Directory Domain Services         Features       Active Directory Ightweight Directory Services         DNS Server       Active Directory Rights Management Services         Active Directory Rights Management Services       and network administrators. AD DS         Dos       DHCP Server         DNS Server       DHCP Server         Active Directory Rights Management Services       and network administrators. AD DS         Confirmation       DHCP Server         Pile and Storage Services (1 of 12 installed)       Host Guardian Service         Host Guardian Service       Host Guardian Service						VER DOU	ATION SERV E2O2T1QD	DESTIN/ WIN-3			;	Select server roles	
Installation Type       Roles       Description         Server Selection <ul> <li>Active Directory Certificate Services</li> <li>Active Directory Domain Services</li> <li>Active Directory Domain Services</li> <li>Active Directory Certificate Services</li> <li>Active Directory Domain Services</li> <li>Active Directory Certificate Services</li> <li>Active Directory Lightweight Directory Services</li> <li>Active Directory Rights Management Services</li> <li>Device Health Attestation</li> <li>DHCP Server</li> <li>DHCP Server</li> <li>DHCP Server</li> <li>Fax Server</li> <li>File and Storage Services (1 of 12 installed)</li> <li>Host Guardian Service</li> </ul> Active Directory Certificate Services (1 of 12 installed)										ed server.	Select one or more roles to install on the select	Before You Begin	i
Server Selection       Active Directory Certificate Services       Active Directory Domain Services         Server Roles       Active Directory Domain Services       (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS         DNS       Device Health Attestation       DHCP Server         AD DS       DHCP Server       DHCP Server         Confirmation       Phile and Storage Services (1 of 12 installed)       Host Guardian Service         Host Guardian Service       Host Guardian Service       Host Guardian Service									Description		Roles	Installation Type	
Hyper-V       Hide         MultiPoint Services       Hide         Print and Document Services       Remote Access         Remote Access       Volume Activation Services         Volume Activation Services       Web Server (IIS)         Windows Deployment Services       V		e	Hid			t 25 5 DS d ork	Services on about and make e to users cors. AD D to give permittee the netwo process.	r Domain informati network a availabl ministral ministral ministral ministral e logon p	Active Directory (AD DS) stores ir objects on the n this information and network addr uses domain cor network users ac resources anywh through a single	Services ervices led)	Active Directory Certificate Services     Active Directory Domain Services     Active Directory Federation Services     Active Directory Rights Management     Device Health Attestation     DHCP Server     Fax Server     File and Storage Services (1 of 12 inst     Host Guardian Service     Hyper-V     MultiPoint Services     Network Policy and Access Services     Print and Document Services     Network Policy Services     Volume Activation Services     Web Server (IIS)     Windows Deployment Services	Server Selection Server Roles Features DNS Server AD DS Confirmation Results	Ϊŝ
< Previous Next > Install Cancel						el	Cance	tall	Insta	ious Next	< Pre		er.
Events     I     Events										1 Events	Events		
Performance 5 Services									5	5 Servic	Performance		
BPA results Performance									nance	Perfor	BPA results		
BPA results									ults	BPA re			
10/19/2022 11/26 AM								1.26 AM	10/10/2022 11				

Active Directory 설치

🚖 Sen	ver Manager								- 0	$\times$
æ	📥 Add Roles and Features Wizard			-		×	208	Tools	View	Help
	Installation progre	ess		DESTINA WIN-3	ATION SER BE2O2T1Q	VER DOU				^ 
i.	Before You Begin Installation Type	<ol> <li>Feature installation</li> </ol>								
	Server Selection Server Roles	Configuration required. Installation su	cceeded on WIN-3E2O2T1QD0U.							
Ξ.	Features DNS Server AD DS Confirmation Results	Active Directory Domain Services         Additional steps are required to make the         Promote this server to a domain control         DNS Server         Group Policy Management         Remote Server Administration Tools         DNS Server Tools         AD DS and AD LDS Tools         Active Directory module for         AD DS Tools         You can close this wizard without inter         page again by clicking Notifications in         Export configuration settings	is machine a domain controller. ler r Windows PowerShell rrupting running tasks. View task pro n the command bar, and then Task Di	ogress or etails.	open thi	∧ ↓			Hid	e
		< Pr	evious Next > Clo	ose	Canc	el				
		Events Services Performance BPA results	Events Services Performance BPA results				_			

#### AD 설치 종료

## 4단계.작업이 완료되면 대시보드에서 Promote this server to a domain controller를 클릭합니다.

🚘 Server Manager				_	· 0	×
Server M	lanager • Dashboard	• 🕲   🍢	Manage	Tools	View	Help
📰 Dashboard	WELCOME TO SERVER MANAGE	Post-deployment Configuration     Configuration required for Active Directory Domain				
Local Server     All Servers     AD DS	<b>1</b> C	Services at WIN-3E2O2T1QD0U Promote this server to a domain controller				
AD DS DNS	QUICK START	Feature installation				
■File and Storage Services ▷	2	Configuration required. Installation succeeded on WIN-3E2O2T1QD0U.				
	WHAT'S NEW 4	Task Details				
	E	Connect this conver to cloud convices				

AD 서비스 구성

5단계.새 포리스트를 만들고 도메인 이름을 선택합니다.

	C		
<u></u>	Server	Manade	ľ
	001101	manage	

(	📥 Active Directory Domain Service	s Configuration Wizard					-		×
	Active Directory Domain Service Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select the deployment ope Add a domain controlle Add a new domain to a Add a new forest Specify the domain informa Root domain name:	eration er to an existir an existing for ation for this o	ng domair est operation mydoma	ain.local		TA WIN-3	RGET SEI	X RVER 2DOU
		More about deployment co	onfigurations						
		5	< Pre	evious	Next >	Insta		Cance	el
		EVANTS			EVENTC				

포리스트 이름 선택

## 6단계.서버에 인증서 서비스 역할을 추가합니다.

🚗 Server Manager						-	- Ć	) ×
Ser	ver Manager • Das	hboard •	, ( <b>3</b> )	🏲	Manage	Tools	View	Help
🔛 Dashboard	WELCOME TO SEE	EVER MANAGER						,
Local Server								
All Servers	🚡 Add Roles and Features Wizard				-		х	
AD DS								
B DNS	Select server role	s		WIN	DESTIN	ATION SERV	ER	
🖷 File and Storage Ser		-					-	
	Before You Begin	Select one or more roles to install on the selected server.						
	Installation Type	Roles		Descript	ion			
	Server Selection	Active Directory Certificate Services	^	Active Di	irectory Certific	ate Service	s	
	Server Roles	<ul> <li>Active Directory Domain Services (Installed)</li> </ul>		(AD CS)	s used to creat	e	.	
	Features	Active Directory Federation Services     Active Directory Lightweight Directory Services		role serv	ion authorities ices that allow	and relate you to issu	e	
	AD CS	Active Directory Eightweight Directory Services     Active Directory Rights Management Services		and man	age certificates	used in a	ic	de
	Role Services	Device Health Attestation     DHCP Septer		variety o	r applications.		-	
	Confirmation	DNS Server (Installed)						

인증서 서비스 추가

🚔 Server Manager				_	- 0	×
Ser Ser	ver Manager • Dasł	nboard •	闭   🏲 Manag	e Tools	View Help	2
<ul> <li>Dashboard</li> <li>Local Server</li> </ul>	WELCOME TO SER	VER MANAGER				
All Servers	📥 Add Roles and Features Wizard		-	- 0	×	
<ul> <li>AD DS</li> <li>DNS</li> <li>File and Storage Ser</li> </ul>	Select role service Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services	S Select the role services to install for Active Directory Certific Role services <u>Certification Authority</u> Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	DES WIN-3E2O2T1QD ate Services Description Certification Authori to issue and manage Multiple CAs can be public key infrastruc	STINATION SERVE OU.mydomain.loca ity (CA) is used a certificates. linked to form ture.	ia ide	
	Confirmation Results					

```
인증 기관만 추가
```

## 7단계.완료되면 인증 기관을 구성합니다.

🚖 Server	Manager			-	đΧ
$\mathbf{E}$	AD CS Configuration		×	age Tools V	/iew Help
III Das III Loc IIII AII III AD III AD III AD III File	Role Services Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select Role Services to configure  Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service	DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local	DESTINATION SERVER QD0U.mydomain.local main.local.	K
		< Previous	Next > Configure Cancel	ess or open this	

8단계.Enterprise CA를 선택합니다.



엔터프라이즈 CA

9단계.루트 CA로 설정합니다. Cisco IOS XE 17.6부터 LSC에 대해 하위 CA가 지원됩니다.

🚖 Server I	Manager		_	đΧ
$\mathbf{E}$	AD CS Configuration		age Tools V	iew Help
Da:	CA Type	DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local	>	
AD AD AD AD AD AD AD AD AD AD AD AD AD A	Cleventais Role Services Setup Type CA Type Private Key	When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.	DESTINATION SERVER QD0U.mydomain.local	
	Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	<ul> <li>Root CA Root CAs are the first and may be the only CAs configured in a PKI hierarchy.</li> <li>Subordinate CA Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.</li> </ul>	main.local.	ide
		ess or open this tails.		

#### 루트 CA 선택

CA가 IIS\_IUSRS 그룹에 속하도록 하려면 해당 계정을 사용해야 합니다. 이 예에서는 관리자 계정 을 사용하고 Active Directory 사용자 및 컴퓨터 메뉴로 이동하여 IIS\_IUSRS 그룹에 관리자 사용자 를 추가합니다.

🚘 Server Manag	ger					– 0 ×
$\bigcirc$	Server Manag	ger • Dashboard			• 🕝   🚩 Manag	e Tools View Help
Dashbo     Local Se     Local Se     All Serv     AD CS     DNS     DNS     File and     IIS	Active Directory Users and File Action View Help Active Directory Users and C Saved Queries Saved Queries	Administrator Properties         Remote control       Remote         General       Address       Account         Member Of       Dial-in         Member of:       Name       Active Direct         Administrators       mydomain Jo         Domain Admins       mydomain Jo         Domain Users       mydomain Jo         Group Policy Cre       mydomain Jo         IIS_IUSRS       mydomain Jo         Schema Admins       mydomain Jo         Add       Remove         Primary group:       Domain Users         Set Primary Group       There is i you have applicated         OK       OK	Desktop Services Profile Profile Telephones Environment tory Domain Services Folder cal/Juers cancel Apply	? ×          COM+         Organization         Sessions    roup unless compliant    Help	Configure Cancel	Hide
		BPA results	BPA res	ults		
		of the outo	UTATES			
م 🖿	c) 🬔 📄 🖡	-			^ ¶	교 d <sub>≈</sub> ENG 10:47 PM BEFR 10/19/2023

IIS\_USER 그룹에 관리자 계정 추가

10단계.올바른 IIS 그룹에 사용자가 있으면 역할 및 서비스를 추가합니다. 그런 다음 인증 기관에 Online Responder 및 NDES 서비스를 추가합니다.

đ ×



NDES 및 Online responder 서비스 설치

11단계.완료되면 해당 서비스를 구성합니다.



온라인 응답기 및 NDES 서비스 설치

12단계.서비스 계정을 선택하라는 메시지가 표시됩니다. 이전에 IIS\_IUSRS 그룹에 추가한 계정입 니다.



IIS 그룹에 추가한 사용자 선택

13단계.이 작업은 SCEP 작업에 충분하지만 802.1X 인증을 달성하려면 RADIUS 서버에 인증서도 설치해야 합니다. 따라서 Windows Server에서 ISE 인증서 요청을 쉽게 복사하여 붙여넣을 수 있도 록 웹 등록 서비스를 쉽게 설치하고 구성합니다.



웹 등록 서비스 설치

AD CS Configuration			-		×
Role Services		WIN-	DESTINA 3E2O2T1QD0U.my	TION SER	VER ocal
Credentials Role Services Confirmation Progress Results	<ul> <li>Select Role Services to configure</li> <li>Certification Authority</li> <li>Certification Authority Web Enrollment</li> <li>Online Responder</li> <li>Network Device Enrollment Service</li> <li>Certificate Enrollment Web Service</li> <li>Certificate Enrollment Policy Web Service</li> </ul>				
-	< Previous	Next >	Configure	Cance	el 🛛

웹 등록 서비스 구성

14단계. http://<serverip>/certsrv/mscep/mscep.dll을 방문하여 SCEP 서비스가 제대로 <u>작동하고 있</u> <u>는지</u> 확인할 수<u>있습니다</u>.

S Network Device Enrollment Servic × +	_		X				
← → C ③ No seguro   172.16.80.8/certsrv/mscep/mscep.dll	☆	۲	:				
Network Device Enrollment Service							
Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).							
This URL is used by metwork devices to submit contificate remuchts							

This URL is used by network devices to submit certificate requests.

To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is <a href="http://chuu-Win12/CertSrv/mscep\_admin">http://chuu-Win12/CertSrv/mscep\_admin</a>

For more information see Using Network Device Enrollment Service .

SCEP 포털 확인

15단계.

기본적으로 Windows Server는 MSCEP(Microsoft SCEP) 내에서 등록하기 전에 클라이언트 및 엔 드포인트 요청을 인증하는 데 동적 챌린지 암호를 사용했습니다. 이렇게 하려면 관리자 계정이 웹 GUI로 이동하여 각 요청에 대해 온디맨드 비밀번호를 생성해야 합니다(비밀번호는 요청 내에 포함 되어야 함). 컨트롤러는 서버에 보내는 요청 내에 이 비밀번호를 포함할 수 없습니다. 이 기능을 제 거하려면 NDES 서버의 레지스트리 키를 수정해야 합니다.

레지스트리 편집기를 열고 시작 메뉴에서 Regedit를 검색합니다.

Computer(컴퓨터) > HKEY\_LOCAL\_MACHINE > SOFTWARE(소프트웨어) > Microsoft > Cryptography(암호화) > MSCEP > EnforcePassword(비밀번호 적용)로 이동합니다.

EnforcePassword 값을 0으로 변경합니다. 이미 0이면 그대로 두십시오.

۲		Registry Editor		_ <b>D</b> X
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
— 📜 САТуре		(Default)	REG SZ	(value not set)
		88 EnforcePassword	REG_DWORD	0x0000000 (0)
EnforcePassword		(		
PasswordVDir				
UseSinglePassword				
- OID	Ξ			
- Protect				
- Providers				
- Services				
Data Assass				
DataAccess				
Device Association Framework				
Device Association Flamework				R
DES				
DirectDraw				
DirectInput				
DirectPlay8				
DirectPlayNATHelp	$\overline{\mathbf{v}}$			
< III >		<	Ш	>
Computer\HKEY_LOCAL_MACHINE\	SOFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword

Enforcepassword 값 설정

## 인증서 템플릿 및 레지스트리 구성

인증서 및 연결된 키는 CA 서버 내의 애플리케이션 정책에 정의된 서로 다른 목적을 위해 여러 시나 리오에서 사용될 수 있습니다. 애플리케이션 정책은 인증서의 EKU(Extended Key Usage) 필드에 저장됩니다. 인증자가 이 필드를 구문 분석하여 클라이언트가 해당 용도로 사용하는지 확인합니다. 적절한 애플리케이션 정책이 WLC 및 AP 인증서에 통합되도록 하려면 적절한 인증서 템플릿을 생 성하고 이를 NDES 레지스트리에 매핑합니다.

1단계. Start(시작) > Administrative Tools(관리 툴) > Certification Authority(인증 기관)로 이동합니 다.

2단계. CA Server(CA 서버) 폴더 트리를 확장하고 Certificate Templates(인증서 템플릿) 폴더를 마 우스 오른쪽 버튼으로 클릭한 후 Manage(관리)를 선택합니다.

3단계. 사용자 인증서 템플릿을 마우스 오른쪽 단추로 클릭한 다음 컨텍스트 메뉴에서 Duplicate Template을 선택합니다.

4단계. General(일반) 탭으로 이동하여 템플릿 이름 및 유효 기간을 원하는 대로 변경하고 다른 모

⚠️ 주의: 유효 기간을 수정할 경우 인증 기관 루트 인증서 유효보다 크지 않은지 확인합니다.

# Properties of New Template

X

Subject Name	Sen	ver	Issuance R	equirements
Superseded Templa	ites	Exte	nsions	Security
Compatibility General	Request	Handling	Cryptography	Key Attestation
Template display name:				
9800-LSC				
Template name:				
9800-LSC				
<u></u>				
Validity period:	-	Renewa	l period:	
2 years V		6	weeks 🗸	
	-			
Publish certificate in	Active Dir	rectory		
Do not automatic	cally reenro	oll if a dupli	cate certificate e	xists in Active
Directory				
ОК		Cancel	Apply	Help

5단계. Subject Name(주체 이름) 탭으로 이동하여 요청의 Supply(공급)가 선택되었는지 확인합니 다. 사용자가 인증서를 서명하기 위해 관리자 승인이 필요하지 않음을 나타내는 팝업이 나타나면 OK(확인)를 선택합니다.

Properties of New Template					
Compatibility General	Request	Handling	Cryptography	Key Attestation	
Superseded Templa	tes	Exte	nsions	Security	
Subject Name	Sen	ver	Issuance F	Requirements	
Use subject information from existing certificates for autoenrollment renewal requests (*)					
O Build from this Active Directory information					
Select this option to enforce consistency among subject names and to simplify certificate administration.					
이 공급					

6단계. Extensions(확장) 탭으로 이동한 다음 Application Policies(애플리케이션 정책) 옵션을 선택 하고 Edit...(편집..) 버튼을 선택합니다. 클라이언트 인증이 Application Policies(애플리케이션 정책) 창에 있는지 확인합니다. 그렇지 않으면 Add(추가)를 선택하여 추가합니다.

Properties of New Template						
Compatibility	General	Request	Handling	Cryptography	Key Attestation	
Subject N	lame	Ser	ver	Issuance	Requirements	
Supersec	ded Templa	tes	Exte	ensions	Security	
To modify an	n extension,	select it,	and then c	lick Edit.		
Extensions in Applicat	ion Policies	bis templa	te:			
Edit /	Applicati	on Poli	cies Exte	nsion X		
An application policy defines how a certificate can be used.						
Application p Client Author Encrypting Secure Ema	olicies: entication File System il				Edit	

내선 번호 확인

7단계. Security(보안) 탭으로 이동하여 Windows Server에서 SCEP 서비스 활성화의 6단계에 정의 된 서비스 계정에 템플릿의 전체 제어 권한이 있는지 확인한 다음 Apply(적용) 및 OK(확인)를 선택 합니다.

# Properties of New Template

X

Subject	Name	Serve	se l	Issuance R	equirements
Superceded Template		tes	Exte	issuance in	Security
Group or us	ernames:				
Re Auther	ticated Use	ers			
St Domain	strator a Admine (C	HILLDOM		ain Admine)	
St. Domain	n Users (CH	UU-DOMAI	N\Domai	in Users)	
St Enterp	rise Admins	(CHUU-DO	MAIN\En	terprise Admins)	0
				Add	Remove
Permissions	And Addressed				
	for Administ	trator		Allow	Deny
Full Contr	tor Administ ol	trator		Allow	Deny
Full Contr Read	tor Administro	trator		Allow	Deny
Full Contr Read Write	ol	trator		Allow ✓ ✓	Deny
Full Contr Read Write Enroll	ol	trator		Allow ✓ ✓ ✓	
Full Contr Read Write Enroll Autoenrol	ol	trator		Allow	Deny
Full Contr Read Write Enroll Autoenrol	ol	trator		Allow V V V V	Deny
Full Contr Read Write Enroll Autoenrol	ol	trator		Allow	Deny
Full Contr Read Write Enroll Autoenrol	ol permissions	or advance	d settings	Allow	Deny
Full Contr Read Write Enroll Autoenrol	ol permissions	or advance	d settings	Allow	Advanced
Full Contr Read Write Enroll Autoenrol	ol permissions	or advance	d settings	Allow	Advanced
Full Contr Read Write Enroll Autoenrol	ol permissions	or advance	d settings	Allow	Advanced

8단계. Certification Authority 창으로 돌아가 Certificate Templates(인증서 템플릿) 폴더를 마우스 오른쪽 버튼으로 클릭하고 New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿) )를 선택합니다.

9단계. 이전에 생성한 인증서 템플릿을 선택합니다. 이 예에서는 9800-LSC이고 OK를 선택합니다.

참고: 새로 생성된 인증서 템플릿은 모든 서버에 걸쳐 복제해야 하므로 여러 서버 구축에 나열 되는 데 시간이 더 걸릴 수 있습니다.

Select one Certificate Template to Note: If a certificate template that Information about this template has No of the certificate templates in the	Enable Certificate Templates enable on this Certification Authority. was recently created does not appear on this list, you may need to wait until been replicated to all domain controllers. e organization may not be available to your CA.	
or more information, see <u>Cert</u>	ificate Template Concepts.	
9800-LSC	Client Authentication, Secure Email, Encrypting File System	
R Exchange	Private Key Archival	
Code Signing	Code Signing	=
Cross Certification Authority	<al></al>	
Enrolment Agent	Certificate Request Agent	
Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Signature Only	Secure Email	
Exchange User	Secure Email	
IPSec	IP security IKE intermediate	
Key Recovery Agent	Key Recovery Agent	
OCSP Response Signing	OCSP Signing	~
	OK Cano	el

템플릿 선택

이제 새 인증서 템플릿이 Certificate Templates(인증서 템플릿) 폴더 내용에 나열됩니다.

🧔 certsrv - [Cer	tification Authority (Local)\CHUU-WIN	N12-CA\Certificate Templates]	x
File Action View Help			
🗢 🏟 🙎 🙆 🔒 📓			
Certification Authority (Local) CHUU-WIN12-CA Revoked Certificates Pending Requests Failed Requests Certificate Templates	Name 9800-LSC Authenticated Session Exchange Enrollment Agent (Offline r IPSec (Offline request) CEP Encryption Directory Email Replication Domain Controller Authentication EFS Recovery Agent Basic EFS Domain Controller Web Server Computer User Subordinate Certification Authority Administrator	Intended Purpose Client Authentication, Secure Email, En Client Authentication Certificate Request Agent IP security IKE intermediate Certificate Request Agent Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all> Microsoft Trust List Signing, Encrypting</all>	

LSC 선택

10단계. 레지스트리 편집기 창으로 돌아가 Computer(컴퓨터) > HKEY\_LOCAL\_MACHINE > SOFTWARE(소프트웨어) > Microsoft > Cryptography(암호화) > MSCEP로 이동합니다.

11단계. EncryptionTemplate, GeneralPurposeTemplate 및 SignatureTemplate 레지스트리가 새로 생성된 인증서 템플릿을 가리키도록 편집합니다.

File       Edit       View       Favorites       Help         Image: Defaults       Image: Defaults	۵.	Registry Editor		_ 🗆 🗙
D-       CertificateTemplateCa         D-       Defaults         D-       Defaults         MSCEP       CAType         CatsinMYStore       EnforcePassword         P-       CatsinMYStore         PasswordVDir       EnforcePassword         P-       OID         P-       OID         P-       Protect         P-       Protect         P-       DevDiv         P-       Drg         P-       DrectDraw         P-       DirectInput         P-       DirectInput         P-       DirectInput         P-       DrectInput	File Edit View Favorites Help			
	File       Edit       View       Favorites       Help <ul> <li>Defaults</li> <li>MSCEP</li> <li>CartsInMYStore</li> <li>EnforcePassword</li> <li>PasswordVDir</li> <li>UseSinglePassword</li> <li>Providers</li> <li>Services</li> <li>UserInterface</li> <li>CTF</li> <li>DetauAccess</li> <li>DevDiv</li> <li>Device Association Frame</li> <li>Dfrg</li> <li>DHCPMibAgent</li> <li>DirectDraw</li> <li>DirectDraw</li> <li>DirectInput</li> </ul>	Name (Default) (Defa	Type REG_SZ REG_SZ REG_SZ REG_SZ	Data (value not set) 9800-LSC 9800-LSC 9800-LSC
CONTRACTOR EX (1.8. CL BACK BURNELS) DELIVICED BURNELS (CONTRACTOR OTHER DURING AND EV		<	III	>

레지스트리에서 템플릿 변경

12단계. NDES 서버를 재부팅하여 Certification Authority 창으로 돌아가서 서버 이름을 선택하고 Stop and Play 버튼을 차례로 선택합니다.

<b>b</b>	certsrv - [Certification Authority (Local)\CHUU-WI	N12-CA] 📃 🗖 🗙
File Action View Help	▶ ■	
Certification Authority (Local)	Name Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates	

# 9800에서 LSC 구성

다음은 WLC에서 AP에 대해 LSC를 구성하는 단계입니다.

- 1. RSA 키를 생성합니다. 이 키는 나중에 PKI 신뢰 지점에 사용됩니다.
- 2. 신뢰 지점을 생성하고 생성된 RSA 키를 매핑합니다.
- 3. AP에 대한 LSC 프로비저닝을 활성화하고 신뢰 지점을 매핑합니다.
  - 1. 조인된 모든 AP에 대해 LSC를 활성화합니다.
  - 2. 프로비전 목록을 통해 선택한 AP에 대해 LSC를 활성화합니다.
- 4. 무선 관리 신뢰 지점을 변경하고 LSC 신뢰 지점을 가리킵니다.

#### AP LSC GUI 컨피그레이션 단계

1단계.Configuration(컨피그레이션) > Security(보안) > PKI Management(PKI 관리) > Key Pair Generation(키 쌍 생성)으로 이동합니다.

- 1. Add(추가)를 클릭하고 관련 이름을 지정합니다.
- 2. RSA 키 크기를 추가합니다.
- 내보낼 수 있는 키 옵션은 선택 사항입니다. 이 명령은 키를 상자에서 내보내려는 경우에만 필 요합니다.
- 4. Generate(생성)를 선택합니다

Q Search Menu Items		Configuration	> PKI M	anagement		
n Dashboard		Trustpoints CA Server	Key Pair	Generation Add C	ertificate Trustp	bool
	>	+ Add				
Configuration	>	Key Name	Key Type	Key T Exportable Zeroize	e Key Name*	AP-SCEP
3		TP-self-signed-2147029136	RSA	No 🗎 Zer	"	
Administration	>	9800-40.cisco.com	RSA	No 🔒 Zer	Key Type*	RSA Key O EC Key
Licensing		TP-self-signed- 2147029136.server	RSA	No 🗎 Zer	Modulus Size*	2048
		CISCO_IDEVID_SUDI	RSA	No 🗎 Zer	re	
Troubleshooting		CISCO_IDEVID_SUDI_LEGACY	RSA	No 🗎 Zer	Key Exportable*	
		H 4 1 F H	10 🗸	1 - 5 of 5 items	Cancel	✓ Generate
Walk Me Through >						

2단계. Configuration(컨피그레이션) > Security(보안) > PKI Management(PKI 관리) > Trustpoints(신뢰 지점)로 이동합니다

- 1. Add(추가)를 클릭하고 관련 이름을 지정합니다.
- 2. 등록 URL(URL은 http://10.106.35.61:80/certsrv/mscep/mscep.dll)과 나머지 세부사항을 입력 합니다.
- 3. 1단계에서 생성한 RSA 키 쌍을 선택합니다.
- 4. Authenticate를 클릭합니다.
- 5. Enroll trustpoint(신뢰 지점 등록)를 클릭하고 비밀번호를 입력합니다.
- 6. Apply to Device(디바이스에 적용)를 클릭합니다.

Q Search Menu Items	Configuration • > Se	curity * > PKI Management		
🔜 Dashboard	Add Trustpoint			×
	Label*	Access_Point-MS-CA	Enrollment Type	SCEP () Terminal
( Monitoring >	Subject Name			
Configuration >	Country Code	IN	State	КА
O Administration	Location	Bengaluru	Domain Name	TAC-LAB.cisco.local
C Licensing	Organization	TAC	Email Address	mail@tac-lab.local
X Troubleshooting	Enrollment URL	/certsrv/mscep/mscep.dll	Authenticate	
	Key Generated		Available RSA Keypairs	AP-SCEP 🔻
	Enroll Trustpoint			
	Password*			
	Re-Enter Password*			
	Cancel			Apply to Device

3단계.Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동합니 다. 아래로 스크롤하여 LSC Provision(LSC 프로비저닝)을 선택합니다.

- 1. 상태를 enabled(활성화됨)로 선택합니다. 이렇게 하면 이 WLC에 연결된 모든 AP에 대해 LSC가 활성화됩니다.
- 2. 2단계에서 생성한 신뢰 지점 이름을 선택합니다.

당신의 필요에 따라 나머지 세부사항을 작성하세요.

Q, Search Menu Items	Configuration * > Wireless * > Access Points				
🚃 Dashboard	<ul> <li>All Access Points</li> </ul>				
Monitoring →	Total APs : 1		Miscon Tag :	egured APs 0 Country Code : 0 LSC Failback	Select an Action
Configuration	AP Name E AP Model E	Admin : Slots : Status Up Time : IP Address	EBase Radio MAC Ether	AP i Power De met MAC i Mode Capable	ate : Operation : Config Status Status
∑ Administration → 10 Licensing	APOCDO-F89A-46E0 A M C9117AXI-D	2 O days 0 hrs 26 10.105.101 mins 42 secs	.158 d0ec.3579.0300 0cd0	.199a.46e0 Local Yes	Registered Health,
* Troubleshooting					
	> 6 GHz Radios				
	> 5 GHz Radios				
	> 2.4 GHz Radios				
	Dual-Band Radios				
	Country				
	LSC Provision				
	Status Trustpoint Name	Access_Point-MS # +	Subject Name Parameters	N	E Apply
	Number of Join Attempts	3	State	KA	
	Key Size Certificate chain status	2048 • Not Available	City	Bengaluru	
	Number of certificates on chein	0	Organization	TAC	

LSC를 활성화하면 AP가 WLC를 통해 인증서를 다운로드하고 재부팅합니다. AP 콘솔 세션에서 이 코드 조각과 같은 내용이 표시됩니다.

[+09/25/2023 10:0	03:28.0993]	
[*09/25/2023 10:0	03:28.7016]	
[+09/25/2023 10:0	03:28.7663]	writing new private key to '/tmp/lsc/priv_key'
[*09/25/2023 10:0	03:28.7666]	
[*09/25/2023 10:0	3:28.9212]	LSC_ENABLE: saving ROOT_CERT
[*09/25/2023 10:0	03:28.9212]	
[+09/25/2023 10:0	03:28.9293]	LSC_ENABLE: saving DEVICE_CERT
[*09/25/2023 10:0	03:28.9293]	
[*09/25/2023 10:0	03:28.9635]	LSC certs and private key verified
[*09/25/2023 10:0	03:28.9635]	
[+09/25/2023 10:0	03:29.4997]	LSC private key written to hardware TAM
[*09/25/2023 10:0	3:29.4997]	
[*09/25/2023 10:0	03:29.5526]	A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed

4단계.LSC가 활성화되면 LSC 신뢰 지점과 일치하도록 무선 관리 인증서를 변경할 수 있습니다. 이 렇게 하면 AP가 LSC 인증서로 조인하고 WLC는 AP 조인에 해당 LSC 인증서를 사용합니다. AP의 802.1X 인증만 수행하려는 경우 이 단계는 선택 사항입니다.

- 1. Configuration(컨피그레이션) > Interface(인터페이스) > Wireless(무선)로 이동하고 Management Interface(관리 인터페이스)를 클릭합니다.
- 2. 2단계에서 생성한 신뢰 지점과 일치하도록 신뢰 지점을 변경합니다.

이것으로 LSC GUI 컨피그레이션 부분을 마치겠습니다. AP가 LSC 인증서를 사용하여 WLC에 조인 할 수 있어야 합니다.

Q. Search Menu Items	Configuration * > Interface * > Wireless Edit Management Interface *
Dashhoard	+ Add X Deleta
	Interface Name Y Interface Type Y VLAN ID Y IP Address Y IP Netmask Interface Viten101 + (1)
	Vian101         Management         101         10.105.101.160         255.255.255.           H          1         >         H         Tuatpoint         Access_Point-MS.x •         2
	There is no instpoint configured on the controller. CISCO_DEVID_SUDI is used as the default trustpoint.
	NAT IPv4/IPv6 Server Address 0.0.0.0
P Troublashooting	
a ricubieshooting	
	Cancel

## AP LSC CLI 컨피그레이션 단계

### 1. 이 명령을 사용하여 RSA 키를 만듭니다.

9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP

% You already have RSA keys defined named AP-SCEP. % They will be replaced % The key modulus size is 2048 bits % Generating 2048 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 0 seconds) Sep 27 05:08:13.144: %CRYPTO\_ENGINE-5-KEY\_DELETED: A key named AP-SCEP has been removed from key storag Sep 27 05:08:13.753: %CRYPTO\_ENGINE-5-KEY\_ADDITION: A key named AP-SCEP has been generated or imported

#### 2. PKI 신뢰 지점을 생성하고 RSA 키 쌍을 매핑합니다. 등록 URL과 나머지 세부사항을 입력합니다

9800-40(config)#crypto pki trustpoint Access\_Point-MS-CA 9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll 9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,0=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab. 9800-40(ca-trustpoint)#rsakeypair AP-SCEP 9800-40(ca-trustpoint)#revocation none 9800-40(ca-trustpoint)#exit

#### 3. crypto pki authenticate <trustpoint> 명령을 사용하여 CA 서버에 PKI 신뢰 지점을 인증하고 등록 합니다. 비밀번호 프롬프트에 비밀번호를 입력합니다.

9800-40(config)#crypto pki authenticate Access\_Point-MS-CA Certificate has the following attributes: Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2 % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted. 9800-40(config)#crypto pki enroll Access\_Point-MS-CA % % Start certificate enrollment ... % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: Sep 26 01:25:00.880: %PKI-6-CERT\_ENROLL\_MANUAL: Manual enrollment for trustpoint Access\_Point-MS-CA Re-enter password: % The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local % The subject name in the certificate will include: 9800-40.cisco.com % Include the router serial number in the subject name? [yes/no]: yes % The serial number in the certificate will be: TTM244909MX % Include an IP address in the subject name? [no]: no Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose Access\_Point-MS-CA' commandwill show the fingerprint. Sep 26 01:25:15.062: %PKI-6-CSR\_FINGERPRINT: CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667 CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005 CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525 Sep 26 01:25:15.062: CRYPTO\_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806 Sep 26 01:25:15.062: CRYPTO\_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9 Sep 26 01:25:15.063: CRYPTO\_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27 Sep 26 01:25:30.239: %PKI-6-CERT\_INSTALL: An ID certificate has been installed under Trustpoint : Access\_Point-MS-CA

Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C0000001400DD405D77E6FE7F00000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#

#### 4. LSC 인증서로 AP 조인을 구성합니다.

9800-40(config)#ap lsc-provision join-attempt 10 9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L 9800-40(config)#ap lsc-provision key-size 2048 9800-40(config)#ap lsc-provision trustpoint Access\_Point-MS-CA 9800-40(config)#ap lsc-provision In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration Are you sure you want to continue? (y/n): y

5. 위에서 생성한 신뢰 지점과 일치하도록 무선 관리 신뢰 지점을 변경합니다.

9800-40(config)#wireless management trustpoint Access\_Point-MS-CA

### AP LSC 확인

#### LSC를 확인하려면 WLC에서 이 명령을 실행합니다.

#show wireless management trustpoint
#show ap lsc-provision summary
#show ap name < AP NAME > config general | be Certificate



9800-40#sho ap	name AP@CD@.F89A	.46E0 config g	ene	eral   begin Certificate
AP Certificate	type		1	Locally Significant Certificate
AP Certificate	Expiry-time		1	09/25/2024 06:48:23
AP Certificate	issuer common-na	me	:	sumans-lab-ca
AP Certificate	Policy		:	Default
AP CAPWAP-DTLS	LSC Status			
Certificate	status :	Available		
LSC fallbac	k status :	No		
Issuer cert	ificate hash :	611255bc69f565at	f53	37be59297f453593e432e1b
Certificate	expiry time :	09/25/2024 06:44	8:2	3
AP 802.1x LSC S	tatus			
Certificate	status :	Not Available		
AD LCC	and an adapted			CARLIND DTLC

#### AP가 다시 로드되면 AP CLI에 로그인하고 다음 명령을 실행하여 LSC 컨피그레이션을 확인합니다.

#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection

```
APOCD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
                           --- Device Certificate ---
Certificate:
   Data:
       Version: 3 (0x2)
      Serial Number:
           5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
       Signature Algorithm: sha256WithRSAEncryption
       Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
       Validity
           Not Before: Sep 28 04:15:28 2023 GMT
           Not After : Sep 27 04:15:28 2024 GMT
       Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0, emailAddress = mail@tac-lab.local
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
               RSA Public-Key: (2048 bit)
               Modulus:
```

	AP0CD0.F89A.46E0#sho crypto	in LSC	
	LSC: Enabled		
	AP@CD@,F89A,46E@#sho capwap	cli config   in	lsc
	AP lsc enable	: 1	
	AP lsc reboot cnt	: 0	
	AP lsc max num of retry	: 10	
	AP lsc mode	: 0×1	
	AP lsc dtls fallback state	: 0	
	AP0CD0.F89A.46E0#		
	Read timed out		
1			

AP0CD0.F89A.46E0#sho dtls connections

Number of DTLS connection = 1

[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version

[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

Current connection certificate issuer name: sumans-lab-ca

# LSC 프로비저닝 문제 해결

WLC 또는 AP 업링크 스위치 포트에서 EPC 캡처를 가져와 AP가 CAPWAP 터널을 형성하는 데 사 용하는 인증서를 확인할 수 있습니다. PCAP에서 DTLS 터널이 성공적으로 구축되었는지 확인합니 다.



DTLS 디버그는 인증서 문제를 파악하기 위해 AP 및 WLC에서 실행할 수 있습니다.

## LSC를 사용하는 AP 유선 802.1X 인증

AP는 자신을 인증하는 데 동일한 LSC 인증서를 사용하도록 구성됩니다. AP는 802.1X 신청자 역할 을 하며 ISE 서버에 대해 스위치에서 인증됩니다. ISE 서버가 백엔드에서 AD와 통신합니다.



참고: AP 업링크 스위치 포트에서 dot1x 인증이 활성화되면 AP는 인증이 통과될 때까지 트 래픽을 전달하거나 수신할 수 없습니다. 인증에 실패한 AP를 복구하고 AP에 액세스하려면 AP 유선 스위치 포트에서 dot1x 인증을 비활성화합니다.

EAP-TLS 인증 워크플로 및 메시지 교환



AP 유선 802.1x 인증 컨피그레이션 단계

- 1. CAPWAP DTLS와 함께 dot1x 포트 인증을 활성화하고 EAP 유형을 선택합니다.
- 2. AP에 대한 dot1x 자격 증명을 생성합니다.
- 3. 스위치 포트에서 dot1x를 활성화합니다.
- 4. RADIUS 서버에 신뢰할 수 있는 인증서를 설치합니다.

AP 유선 802.1x 인증 GUI 컨피그레이션

- 1. AP 가입 프로필로 이동하고 프로필을 클릭합니다.
  - 1. AP > General을 클릭합니다. EAP 유형 및 AP 권한 부여 유형을 "CAPWAP DTLS + dot1x port auth"로 선택합니다.
  - 2. Management(관리) > Credentials(자격 증명)로 이동하고 AP dot1x 인증을 위한 사용자 이름 및 비밀번호를 생성합니다.

Cisco Cat	alyst 9800-40 Wireless Controller		Welcome admin 🛛 🖨 🤻 🤷 🚳 🛛	C Search APs and Clients Q Eeedback . (*
Q. Search Manu Items	Configuration * > Tags & Profiles * > AP Join		Edit AP Join Profile General Client CAPWAP AP Management	x Security ICap QoS
Dashboard	Add × Devene Clone	T Des	General Power Management Hyperlocation AP St	tatistics
Monitoring >	ap-auth	<	Power Over Ethernet	Client Statistics Reporting Interval
	APG_test		Switch Flag	5 GHz (sec) 90
() Administration >	APC 3rd-Fir-APs		Power Injector State	2.4 GHz (sec) 90
C Licensing	APG_4th-FF-APs		Power Injector Type	Extended Module
💥 Troubleshooting	APG_6th-Fr-APs		Injector Switch MAC 0000.0000	Enable
	APG_2/th~Fir~APs APG_8th~Fir~APs		AP EAP Auth Configuration	Mesh
	APG_11th-Fir-APs		EAP Type	Profile Name default-mesh-pro v 2
Walk Me Through 3	APG_12th-Fir-APs		AP Authorization Type CAPWAP DTLS + DOTe.	
			DOT1x port auth CAPWAP DTLS	
			Dot1x port auth	
			D Cancel	Update & Apply to Device

Cisco Cat	alyst 9800-40 Wireless Controller	Welcome admin 🖷 🌾 🛕 🖺 🌣 🔞 🕢 🎜 Scent Afs and Clercs Q
Q. Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile ×
Dashboard	+ Add X Delete	General Client CAPWAP AP Management Security ICap QoS Device User Credentials CDP Interface
	AP Join Profile Name	T Des
( Monitoring >	ap-auth	Dot1x Credentials
🗞 Configuration 💦 🔸	APG_test	Dottx Username ap-wired-user
() Administration >	testSte     ADC. 3rd-Er-ADe	Dot1x Password
C Licensing	APQ_4th-Fk-APs	Dot1x Password Type elear
	APG_6th-Fr-APs	
Con the second s	APG_7th-Fir-APs	
	APG_8th-Fir-APs	
	APG_11th-Fir-APs	
Walk Me Through 2	APG_12th-Fir-APs	
	H K 1 2 3 M 10 W	
		Cancel

## AP 유선 802.1x 인증 CLI 컨피그레이션

CLI에서 AP에 대해 dot1x를 활성화하려면 다음 명령을 사용합니다. 이는 특정 가입 프로필을 사용 하는 AP에 대해서만 유선 인증을 활성화합니다.

#ap profile ap-auth
#dot1x eap-type eap-tls
#dot1x lsc-ap-auth-state both
#dot1x username ap-wired-user password 0 cisco!123

## AP 유선 802.1x 인증 스위치 컨피그레이션

이 스위치 컨피그레이션은 LAB에서 AP 유선 인증을 활성화하는 데 사용됩니다. 설계에 따라 다른 컨피그레이션을 가질 수 있습니다.

aaa new-model dot1x system-auth-control aaa authentication dot1x default group radius aaa authorization network default group radius radius server ISE address ipv4 10.106.34.170 auth-port 1812 acct-port 1813 key cisco!123 1 interface GigabitEthernet1/0/2 description "AP-UPLINK-PORT-AUTH-ENABLED" switchport access vlan 101 switchport mode access authentication host-mode multi-host authentication order dot1x authentication priority dot1x authentication port-control auto dot1x pae authenticator end

RADIUS 서버 인증서 설치

인증은 신청자 역할을 하는 AP와 RADIUS 서버 간에 발생합니다. 둘 다 서로 인증서를 신뢰해야 합 니다. AP가 RADIUS 서버 인증서를 신뢰하도록 하는 유일한 방법은 RADIUS 서버가 AP 인증서도 발급한 SCEP CA에서 발급한 인증서를 사용하도록 하는 것입니다.

ISE에서 Administration(관리) > Certificates(인증서) > Generate Certificate Signing Requests(인증 서 서명 요청 생성)로 이동합니다

CSR을 생성하고 필드를 ISE 노드의 정보로 채웁니다.

Cisco ISE

Administration · System

Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings	
Deployment       Licensing       Certificates       Logging       Maintenance       Upgrade       Health Checks       Backup & Restore       Admin Access       Settings         Certificates       System Certificates       System Certificates       Certificates       Signing Requests       Certificate Signing Requests       Certificate Signing Requests       Certificate Signing Requests       Certificate Signing Certificate       Main: User (Amin, EAP Pertal, packing) - Client and Server Authentication         Certificate Authority       State (Authority Certificates)       Main: Server Authentication       Server Authentication         Occertificate Authority       State Contributes       Signing Certificate       Signing Certificates         Output       State Contributes Authority       State Contributes       Server Authentication         Disc Control Certificate Authority       State Contributes       Signing Certificate         State Control Certificate - Control Certificates       Signing Certificate       Signing Certificate         State Control Certificate - Control Certificates       Signing Requests       State Control Certificates         Output       State Control Certificates       Signing Certificate       Signing Certificate         State Control Certificate Signing Certificates       Signing Certificate       Signing Certificate         State Control Certificates Control Ce		
	Contificate(s) will be used for EAP Authentication  Altow Wildcard Centificates       Altow Wildcard Centificates       O	
	Generate CSR's for these Nodes:	
	Node CSR Friendly Name	
	Subject	
	Subject         Common Name (CN)         SFQDN\$         Organizational Unit (OU)         Organization (O)	
	City (L) State (ST)	

#### 생성된 후에는 내보내고 텍스트로 복사하여 붙여넣을 수도 있습니다.

Windows CA IP 주소로 이동하여 URL에 /certsrv/를 추가합니다

Request a certificate(인증서 요청)를 클릭합니다



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

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

Submit a certificate request by using a base-64 ....(base-64를 사용하여 인증서 요청 제출)를 클릭 합니다. Microsoft Active Directory Certificate Services - mydomain-WIN-3E2O2T1QD0U-CA

#### Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to: <u>Create and submit a request to this CA.</u>

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file,

#### 텍스트 상자에 CSR 텍스트를 붙여넣습니다. 웹 서버 인증서 템플릿을 선택합니다.

← C ▲ Non sécurisé   192.168.1.98/certsrv/certrqxt.asp			
Microsoft Active Directory Certificate Services - mydomain-WIN-3E202T1QD0U-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 C/MC or PKCS #10 or PKCS #7):			
Certificate Templates: (No templates found!)			
Additional Attributes:			

그런 다음 Certificate Signing Request(인증서 서명 요청) 메뉴로 돌아가 Bind certificate(인증서 바 인딩)를 클릭하여 ISE에 이 인증서를 설치할 수 있습니다. 그런 다음 Windows C에서 가져온 인증 서를 업로드할 수 있습니다.

≡ Cisco ISE	Administration · System		
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings		
Certificate Management System Certificates	Certificate Signing Requests		
Trusted Certificates OCSP Client Profile	Generate Certificate Signing Requests (CSR)		
Certificate Signing Requests Certificate Periodic Check Se	A betimes arguing requests (cons) measure entries and agrice by an external externa External external		
	Q View 🖞 Export 🌐 Delete Bind Certificate		
Certificate Authority >	Erriendly Name Certificate Subject Key Length Portal gro Timestamp $\wedge$ Host		
	ISE99#EAP Authentication         CN=ISE99.mydomain.local         4096         Mon, 30 Oct 2023         ISE99		

## AP 유선 802.1x 인증 확인

AP에 대한 콘솔 액세스 권한을 가지고 다음 명령을 실행합니다.

#show ap authentication status

Ap 인증이 활성화되지 않았습니다.

#### AP 인증을 활성화한 후 AP에서 콘솔 로그:

AP0CD0.F89A.46E0#[\*09/26/2023 08:57:40.9154] [\*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode [\*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL

#### AP 인증 성공:



#### WLC 확인:

9800-40#sho ap name AP0CD0.F89A.4	46E0 config general   begin Certificate		
AP Certificate Expiry-time	: 00/01/07 2027/0204 05:48:23		
AP Certificate issuer common-name AP Certificate Policy	AP Certificate issuer common-name : sumans-lab-ca		
AP CAPWAP-DTLS LSC Status			
Certificate status : A	Available		
Issuer certificate hash : 6	LS. TOLLOBER STATUS : NO Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b		
Certificate expiry time : 0	Certificate expiry time : 09/25/2024 06:48:23		
AP 802.1x LSC Status Certificate status : A	Aveilable		
Issuer certificate hash : 6	611255bc69f565af537be59297f453593e432e1b		
AP ISC authentication state	09/75/2024_06f48f27		
A PAC ARTICULTOCITOR STOLE I CALMALANTA BIN ARTICULTOCITOR			

#### Switchport 인터페이스 상태가 인증 성공 후:

Switch#sho authenticatio Interface	n sessions inte MAC Address	rface gi Method	gabitEthe Domain	Status Fg	Session ID
Gi1/0/2	0cd0.f89a.46e0	dot1x	DATA	Auth	9765690A0000005CCEED0FBF

### 다음은 성공적인 인증을 나타내는 AP 콘솔 로그 샘플입니다.

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 comp]
```

# 802.1X 인증 문제 해결

AP 업링크에 PCAP를 적용하고 RADIUS 인증을 확인합니다. 다음은 성공적인 인증의 단편입니다.



## TCPdump는 인증을 캡처하는 ISE에서 수집합니다.



인증 중에 문제가 발견되면 AP 유선 업링크 및 ISE 측에서 동시 패킷 캡처가 필요합니다.

AP에 대한 디버그 명령:

#debug ap authentication packet

# 관련 정보

- Cisco 기술 지원 및 다운로드
- <u>AireOS를 사용하여 AP에 802.1X 구성</u>
- LSC용 9800 컨피그레이션 가이드
- <u>9800의 LSC 컨피그레이션 예</u>
- <u>9800의 AP에 대해 802.1X 구성</u>

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.