802.1X op AP's configureren voor PEAP of EAP-TLS met LSC

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Netwerkdiagram
Configureren
Windows Server 2016 SCEP CA
Het certificaatsjabloon en het register configureren
LSC op de 9800 configureren
Configuratiestappen AP LSC GUI
Configuratiestappen AP LSC CLI
AP LSC-verificatie
Probleemoplossing voor LSC-provisioning
AP-bekabelde 802.1X-verificatie met LSC
Configuratiestappen voor AP Wired 802.1x-verificatie
Configuratie van bekabelde AP-802.1x-verificatie en GUI
CLI-configuratie voor AP-bekabelde 802.1x-verificatie
Configuratie van bekabelde AP-Switch 802.1x-verificatie
Installatie van RADIUS-servercertificaat
Verificatie van bekabelde AP-802.1x-verificatie
Probleemoplossing 802.1X-verificatie
Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u Cisco-access points op hun switchpoort moet verifiëren met behulp van de 802.1X PEAP- of EAP-TLS-methoden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

Draadloze controller

- Access point
- Switch
- ISE-server
- Certificaatautoriteit.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Draadloze controller: C9800-40-K9 met 17.09.02
- Access point: C9117AXI-D
- Switch: C9200L-24P-4G met 17.06.04
- AAA-server: ISE-VM-K9 met 3.1.0.518
- Certificaatinstantie: Windows Server 2016

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Als u wilt dat uw access points (AP's) met hun switchport verifiëren met 802.1X, gebruiken zij standaard het EAP-FAST-verificatieprotocol waarvoor geen certificaten nodig zijn. Als u wilt dat de AP's de PEAP-mschappv2 methode (die referenties aan de AP-kant gebruikt maar een certificaat aan de RADIUS-kant) of de EAP-TLS methode (die certificaten aan beide kanten gebruikt) gebruiken, moet u LSC eerst configureren. Het is de enige manier om een vertrouwd/wortelcertificaat op een toegangspunt (en ook een apparaatcertificaat in het geval van EAP-TLS) te verstrekken. Het is niet mogelijk voor het toegangspunt om PEAP uit te voeren en de validatie aan serverzijde te negeren. Dit document behandelt eerst het configureren LSC en vervolgens de 802.1X-configuratiezijde.

Gebruik een LSC als u wilt dat uw PKI betere beveiliging biedt, controle heeft over uw certificaatautoriteit (CA) en beleid, beperkingen en gebruik definieert op de gegenereerde certificaten.

Met LSC krijgt de controller een certificaat van de CA. Een AP communiceert niet direct met de CA-server, maar de WLC vraagt certificaten aan namens de toetredende AP's. De CA-servergegevens moeten op de controller zijn geconfigureerd en toegankelijk zijn.

De controller maakt gebruik van het Simple Certificate Enrollment Protocol (SCEP) om bepaaldeReqs die op de apparaten zijn gegenereerd door te sturen naar de CA en maakt opnieuw gebruik van SCEP om de ondertekende certificaten van de CA te verkrijgen.

SCEP is een protocol voor certificaatbeheer dat de PKI-clients en CA-servers gebruiken om certificaatinschrijving en herroeping te ondersteunen. Het wordt veel gebruikt in Cisco en ondersteund door veel CA-servers. In SCEP wordt HTTP gebruikt als het transportprotocol voor

de PKI-berichten. Het primaire doel van SCEP is de veilige afgifte van certificaten aan netwerkapparaten.

Netwerkdiagram



Configureren

Er zijn twee dingen om voornamelijk te configureren: de SCEP CA en de 9800 WLC.

Windows Server 2016 SCEP CA

Dit document behandelt een fundamentele installatie van een Windows Server SCEP CA voor laboratoriumdoeleinden. Een echte productie-grade Windows CA moet veilig en geschikt worden geconfigureerd voor bedrijfsactiviteiten. Deze sectie is bedoeld om u te helpen het in het laboratorium testen en inspiratie te halen uit de vereiste instellingen om deze configuratie te laten werken. Dit zijn de stappen :

Stap 1.Installeer een nieuwe Windows Server 2016 Desktop Experience.

Stap 2.Controleer of de server is geconfigureerd met een statisch IP-adres.

Stap 3.Installeer een nieuwe rol en service, start met Active Directory Domain services en DNS server.

👝 Se	rver Manager								- 6	×
<	🚵 Add Roles and Features Wizard			-		×	age	Tools	View	Help
Ī	Select server roles			DEST	INATION SERV	/ER OU				
ī	Before You Begin	Select one or more roles to install on the selected s	server.							
	Installation Type	Roles		Description						
Ϊĝ	Server Selection Server Roles Features DNS Server AD DS Confirmation Results	 Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Device Health Attestation DHCP Server Fax Server DNS Server File and Storage Services (1 of 12 installed) Host Guardian Services Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Web Server (IIS) Windows Deployment Services 	nices ces	Active Directory Doma (AD DS) stores inform objects on the networ this information availa and network administ uses domain controlle network users access i resources anywhere o through a single logor	in Services ation about k and make ble to users rators. AD D rs to give to permittee n the netwo n process.	s ; IS H rk			Hid	e
es .		< Previous	Next >	Install	Cance	I				
		Events	1 Events							
		Performance	5 Services	s						
		BPA results	Perform	nance						
			BPA res	ults						
				10/10/2022 11/26 AI	4					

Active Directory-installatie

🚖 S	erver Manager								- 0	×
	🚡 Add Roles and Features Wizard			-		×	age	Tools	View	Help
111	Installation progre	ess		DESTINA WIN-3	ATION SER	VER DOU				^
	Installation progree Before You Begin Installation Type Server Selection Server Roles Features DNS Server AD DS Confirmation Results	View installation progress Feature installation Configuration required. Installation su 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 Role 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	cceeded on WIN-3E2O2T1QDOU. is machine a domain controller. ler r Windows PowerShell errupting running tasks. View task pro n the command bar, and then Task D	ogress or rietails.	open thi	s s s s s s s s s s s s s s s s s s s			Hid	e
		< Pr Events Services Performance BPA results	evious Next > Cla Events Services Performance BPA results	ose	Canc	el				

Einde AD-installatie

Stap 4.Als u klaar bent, klikt u op het dashboard op Promoot deze server naar een domeincontroller.

🚘 Server Manager					- 0	×
Server M	lanager • Dashboard	• @ 🎢	Manage	Tools	View	Help
📰 Dashboard	WELCOME TO SERVER MANAGE	Post-deployment Configuration				
Local Server	1	Configuration required for Active Directory Domain 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	Add Roles and Features Task Details				
	E.	Connect this converte cloud convisor	1			

De AD-services configureren

Stap 5.Maak een nieuw bos en kies een domeinnaam.

👝 Sei	rver l	Ma	ana	aq	er

(📥 Active Directory Domain Services	Configuration Wizard					-		×
	Active Directory Domain Services Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select the deployment oper Add a domain controlle Add a new domain to a Add a new forest Specify the domain informat Root domain name:	ration r to an existin n existing fore ation for this c	g domain est operation mydomai	n.local		TA WIN-3	RGET SEI	X RVER 2DOU
		More about deployment co	onfigurations	vious	Next >	Insta	11	Cance	el
1		Evente			Evente				

Kies een bosnaam

Stap 6.Voeg de rol Certificaatservices toe aan uw server:

📥 Server Manager							- () ×
Ser Ser	ver Manager • Das	hboard •	B	I 🗗	Manage	Tools	View	Help
Dashboard Local Server	WELCOME TO SE	RVER MANAGER						
All Servers	🔁 Add Roles and Features Wizard				-		×	
 AD DS DNS File and Storage Ser 	Select server role	S		WIN	DESTIN -3E2O2T1QD0U.i	IATION SER\ nydomain.lo	/ER ical	
	Before You Begin Installation Type Server Selection Server Roles	Select one or more roles to install on the selected server. Roles Image: Comparison of the selected server. Roles Image: Comparison of the selected server. Image: Comparison of the selected server. Image: Comparison of the selected server. Image: Comparison of the selected server. Image: Comparison of the selected server. Image: Comparison of the selected server. Image: Comparison of the selected server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: Comparison of the server. Image: C	^	Description Active Dire (AD CS) is	on rectory Certific s used to creat	ate Servici	25	
	Features AD CS Role Services Confirmation	 Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server (Installed) 		certificati role servi and mana variety of	on authorities ces that allow age certificates applications.	and relate you to issu s used in a	d Je	de

Certificaatservices toevoegen



Alleen de certificeringsinstantie toevoegen

Stap 7.Nadat u dit hebt gedaan, configureert u uw certificeringsinstantie.

🚖 Server	Manager			-	0 X
\mathbf{E}	AD CS Configuration		×	age Tools	View Help
	Role Services	Solact Polo Sorvisos to configuro	DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local	- 0	× 1
AD AD AD AD AD AD File	Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name	Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service		DESTINATION SERVER QDOU.mydomain.local	
	Validity Period Certificate Database Confirmation Progress Results			main.local.	ide
		More about AD CS Server Roles	Next > Configure Cancel	ess or open this	

Stap 8.Kies Enterprise CA.



CA voor ondernemingen

Stap 9.Maak er een root-CA van. Sinds Cisco IOS XE 17.6 worden ondergeschikte CA's ondersteund voor LSC.



Kies een root-CA

Het is belangrijk dat de account die u gebruikt voor uw CA deel uitmaakt van de groep IIS_IUSRS. In dit voorbeeld, gebruikt u de rekening van de Beheerder en gaat naar het Actieve menu van de Gebruikers en van Computers van de Folder om de gebruikers van de Beheerder aan de groep toe te voegen IIS_IUSRS.

🚔 Server Manager				– 0 ×
Server Manag	ger • Dashboard		🕄 🚩 Manage Too	ols View Help
Dashbo Local S All Server AD CS AD DS DNS File and IIS All Server AD DS DNS File and With anged Service Action Users Users	Administrator Properties Remote control Remote Desktop Services Profile General Address Account Profile Telepho Member Of Dial-in Environment Member of: Image: Services of the	? × ile COM+ nes Organization Sessions Folder Folder Folder Folder many group unless POSIX-compliant by Help	- Configure Cancel	Hide
	DPA results BPA	A results		
# > © 🤅 🗔			^ 覧 d <mark>×</mark> [ENG 10:47 PM BEFR 10/19/2023

Voeg je admin account toe aan de IIS_USER groep

Stap 10.Zodra u een gebruiker in de juiste IIS-groep hebt, voeg rollen en services toe. Voeg vervolgens de Online Responder- en NDES-services toe aan uw certificeringsinstantie.

٥ ×



Installeer de NDES- en Online Responder-services

Stap 11.Zodra u klaar bent, configureer deze services.



Installeer de Online responsder en de NDES-service.

Stap 12.U wordt gevraagd een serviceaccount te kiezen. Dit is de account die u eerder aan de groep IIS_IUSRS hebt toegevoegd.



Selecteer de gebruiker die u aan de IIS-groep hebt toegevoegd

Stap 13.Dit is genoeg voor SCEP-bewerkingen, maar om 802.1X-verificatie te kunnen realiseren, moet u ook een certificaat op de RADIUS-server installeren. Daarom, voor gemak, installeer en vorm de dienst van de Webinschrijving om het ISE- certificaatverzoek op onze Server van Windows gemakkelijk te kunnen kopiëren en kleven.



Installeer de webinschrijvingsservice

🚡 AD CS Configuration		×	(
Role Services		DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local	
Credentials Role Services	Select Role Services to configure		
Confirmation	Certification Authority		
Progress	 Online Responder 		
Results	Network Device Enrollment Service		
	Certificate Enrollment Web Service		
	Certificate Enrollment Policy Web Service		
	More about AD CS Server Roles		
-	< Previous	Next > Configure Cancel	

de webinschrijvingsservice configureren

Stap 14. U kunt controleren of de SCEP-service correct werkt door te gaan naar <u>http://<serverip>/certsrv/mscep/mscep.dll</u> :

S Network Device Enrollment Servic × +	[x
← → C ③ No seguro 172.16.80.8/certsrv/mscep/mscep.dll	\$	Ð	:
Network Device Enrollment Service			
Network Device Enrollment Service allows you to obtain certificates for routers or other network using the Simple Certificate Enrollment Protocol (SCEP).	ork de	vice	5
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 <u>http://Chuu-Win12/CertSrv/mscep_admin</u>	L is		
For more information see Using Network Device Enrollment Service.			

Verificatie van SCEP-portal

Stap 15.

Standaard gebruikt de Windows Server een dynamisch wachtwoord om client- en endpointverzoeken te verifiëren voordat u zich inschrijft bij Microsoft SCEP (MSCEP). Dit vereist een admin-account om naar de web GUI te bladeren om een on-demand wachtwoord voor elk verzoek te genereren (het wachtwoord moet in het verzoek worden opgenomen).De controller is niet in staat om dit wachtwoord op te nemen in de verzoeken die het naar de server stuurt. Om deze functie te verwijderen, moet de registersleutel op de NDES-server worden gewijzigd:

Open de Register-editor, zoek naar Regedit in het menu Start.

Ga naar Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptografie > MSCEP > EnforcePassword

Verander de EnforcePassword waarde in 0. Als het al 0 is, laat het dan zoals het is.

B		Registry Editor		_ D X
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
— 👢 САТуре		(Default)	REG SZ	(value not set)
		110 EnforcePassword	REG DWORD	0x00000000 (0)
			-	
UseSinglePassword				
- 📜 OID	≡			
- Notect				
- Providers				
- L Services				
🐌 UserInterface				
, CTF				
DataAccess				
, DevDiv				
Device Association Framework				<i>b</i> ₹
, Dfrg				.0
, DFS				
DHCPMibAgent				
, DirectDraw				
, DirectInput				
, DirectPlay8				
DirectPlayNATHelp	\sim			
< III >		<	III	>
Computer\HKEY_LOCAL_MACHINE\S	OFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword

De waarde van het handhavingswachtwoord instellen

Het certificaatsjabloon en het register configureren

Certificaten en bijbehorende sleutels kunnen worden gebruikt in meerdere scenario's voor verschillende doeleinden die worden gedefinieerd door het toepassingsbeleid binnen de CA-server. Het toepassingsbeleid wordt opgeslagen in het veld Uitgebreide sleutelgebruik (EKU) van het certificaat. Dit veld wordt door de verificator geparseerd om te controleren of de client het voor het beoogde doel gebruikt. Om ervoor te zorgen dat het juiste toepassingsbeleid wordt geïntegreerd in de WLC- en AP-certificaten, maakt u de juiste certificaatsjabloon en brengt u deze in het NDES-register in kaart:

Stap 1. Ga naar Start > Administratieve tools > Certificeringsinstantie.

Stap 2. Breid de mappenstructuur van CA Server uit, klik met de rechtermuisknop op de mappen Certificaatsjablonen en selecteer Beheren.

Stap 3. Klik met de rechtermuisknop op de certificaatsjabloon Gebruikers en selecteer Sjabloon dupliceren in het contextmenu.

Stap 4. Navigeer naar het tabblad Algemeen, verander de naam van de sjabloon en de geldigheidsperiode zoals gewenst, laat alle andere opties onaangevinkt.

A Waarschuwing: als de geldigheidsperiode wordt gewijzigd, zorg er dan voor dat deze niet langer is dan de basisgeldigheid van het certificaat van de certificeringsinstantie.

Properties of New Template

X

Subject Name	Sen	ver	Issuance Re	equirements
Superseded Templa	tes	Exte	nsions	Security
Compatibility General	Request	Handling	Cryptography	Key Attestation
Template display name: 9800-LSC				
Template name: 9800-LSC				
Validity period: 2 years v Publish certificate in Do not automatic Directory	Active Dir	Renewal 6	period: weeks v	xists in Active
OK		Cancel	Apply	Help

De certificaatsjabloon configureren

Stap 5. Navigeer naar het tabblad Onderwerpnaam en zorg ervoor dat Levering in het verzoek is geselecteerd. Een pop-up lijkt aan te geven dat gebruikers geen admin goedkeuring nodig hebben om hun certificaat ondertekend te krijgen, OK selecteren.



Levering in het verzoek

Stap 6. Navigeer naar het tabblad Uitbreidingen en selecteer vervolgens de optie Toepassingsbeleid en selecteer de knop Bewerken.... Zorg ervoor dat de Clientverificatie in het venster Toepassingsbeleid staat; anders selecteert u Toevoegen en voegt u deze toe.

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

Controleer de uitbreidingen

Stap 7. Navigeer naar het tabblad Security en zorg ervoor dat de serviceaccount die is gedefinieerd in Stap 6 van het tabblad Enable SCEP Services in de Windows Server beschikt over volledige controle-rechten van de sjabloon, en selecteer vervolgens Toepassen en OK.

Properties of New Template

X

Subject Name Server Issuance requirements Superseded Templates Extensions Security Group or user names: Administrator Security Administrator Administrator Security Domain Admins (CHUU-DOMAIN\Domain Admins) Security Domain Users (CHUU-DOMAIN\Domain Users) Security Enterprise Admins (CHUU-DOMAIN\Enterprise Admins) Add Remove Add Remove Permissions for Administrator Allow Deny Full Control Image: Control Image: Control Image: Control Read Image: Control Image: Control Image: Control Autoenroll Image: Control Image: Control Image: Control For special permissions or advanced settings, click Advanced	Colorada B	lama.	Carrier	aing	Cryptograpny	Ney Attestation
Superseded Templates Extensions Security Group or user names: Administrator Administrator Domain Adminis (CHUU-DOMAIN\Domain Admins) Domain Users (CHUU-DOMAIN\Domain Users) Enterprise Admins (CHUU-DOMAIN\Enterprise Admins) Add Remove Add Remove Permissions for Administrator Add Remove Permissions for Administrator Add Remove Control Co	Subject I	vame	Server		Issuance H	Security
Group or user names: Authenticated Users Administrator Domain Admins (CHUU-DOMAIN\Domain Admins) Domain Users (CHUU-DOMAIN\Domain Users) Enterprise Admins (CHUU-DOMAIN\Enterprise Admins) Add Remove Add Remove Permissions for Administrator Allow Deny Full Control Read Write Enroll Autoenroll Cor special permissions or advanced settings, click Advanced	Superse	ded Templa	tes	Exte	nsions	Security
Administrator Domain Admins (CHUU-DOMAIN\Domain Admins) Domain Users (CHUU-DOMAIN\Domain Users) Enterprise Admins (CHUU-DOMAIN\Domain Users) Enterprise Admins (CHUU-DOMAIN\Enterprise Admins) Add Remove Permissions for Administrator Allow Deny Full Control Read Write Enroll Autoenroll For special permissions or advanced settings, click Advanced	Group or use	er names:				
Administrator CHUU-DOMAIN\Domain Admins) Domain Users (CHUU-DOMAIN\Domain Users) Enterprise Admins (CHUU-DOMAIN\Enterprise Admins) Add Remove Add Remove Add Remove Permissions for Administrator Allow Deny Full Control Read Write Enroll Autoenroll Of Coucle add add add add add add add add add ad	St. Authen	ticated Use	18			
Domain Admins (CHUU-DOMAIN\Domain Admins) Domain Users (CHUU-DOMAIN\Domain Users) Enterprise Admins (CHUU-DOMAIN\Enterprise Admins) Add Remove Add Remove Permissions for Administrator Allow Deny Full Control Read Write Enroll Autoenroll For special permissions or advanced settings, click Advanced.	Adminis	strator				
Cheve and the settings, click Cheve and the settings, click	Be Domain	Admins (C	HUU-DOMAIN	NDom:	ain Admins)	
Add Remove Add Remove Add Remove Permissions for Administrator Allow Deny Full Control Read Write Enroll Autoenroll For special permissions or advanced settings, click Advanced.	Se Domain	Users (CH	IUU-DOMAIN\	Domai	n Users)	
Add Remove Permissions for Administrator Allow Permissions for Administrator Allow Permissions for Administrator Image: Control image: C	and threepe		(CHOO-DOMA		corprise Automis)	
Add Remove Permissions for Administrator Allow Permissions for Administrator Allow Full Control Image: Control Read Image: Control Write Image: Control Enroll Image: Control Autoenroll Image: Control						
Add Remove Permissions for Administrator Allow Penny Full Control Read Write Enroll Autoenroll For special permissions or advanced settings, click Advanced						
Add Remove Permissions for Administrator Allow Permissions for Administrator Allow Full Control Image: Control in the second s						
Permissions for Administrator Allow Deny Full Control Image: Control Read Image: Control Write Image: Control Enroll Image: Control Autoenroll Image: Control For special permissions or advanced settings, click Advanced					Add	Remove
Permissions for Administrator Allow Deny Full Control Image: Control						
Full Control Read Write Enroll Autoenroll For special permissions or advanced settings, click Advanced.	Permissions	for Adminis	trator		Allow	Deny
Read Write Enroll Autoenroll	Full Contra	al				
Write Enroll Autoenroll For special permissions or advanced settings, click Advanced. Advanced	Full Control	UI II			Y	
Enroll Autoenroll	Read				 ✓ 	
Autoenroll For special permissions or advanced settings, click Advanced.	Read Write				 	
For special permissions or advanced settings, click Advanced	Read Write Enroll				> > >	
For special permissions or advanced settings, click Advanced	Read Write Enroll Autoenrol	I			> > > >	
For special permissions or advanced settings, click Advanced	Read Write Enroll Autoenrol	l			> > > >	
For special permissions or advanced settings, click Advanced	Read Write Enroll Autoenrol	l			> > > >	
	Read Write Enroll Autoenrol					
	For special p	l permissions	or advanced s	ettings	v V V V	Advanced
	For special p Advanced.	l	or advanced s	ettings	v V V V	Advanced
	For special p Advanced.	l	or advanced s	ettings	v V V V	Advanced
	For special p Advanced.	permissions	or advanced s	ettings	v V V V	Advanced

Stap 8. Ga terug naar het venster Certificatie-instantie, klik met de rechtermuisknop in de map Certificaatsjablonen en selecteer Nieuw > Certificaatsjabloon voor afgifte.

Stap 9. Selecteer de certificaatsjabloon die eerder is gemaakt. In dit voorbeeld is 9800-LSC en selecteer OK.

Opmerking: het kan langer duren voordat de nieuw gemaakte certificaatsjabloon in meerdere serverimplementaties wordt vermeld, aangezien deze op alle servers moet worden gerepliceerd.

ote: If a certificate template that	was recently created does not appear on this list, you may need to wait unt the prenicated to all domain controllers	il
of the certificate templates in the	e organization may not be available to your CA.	
Name	Intended Pumose	/
2 9800-LSC	Client Authentication, Secure Email, Encrypting File System	
CA Exchange	Private Key Archival	
Code Signing	Code Signing	=
Cross Certification Authority	<ai></ai>	
Enrollment Agent	Certificate Request Agent	
Enrollment Agent (Computer)	Certificate Request Agent	- 15
Exchange Signature Only	Secure Email	
Exchange User	Secure Email	
IPSec	IP security IKE intermediate	
Key Recovery Agent	Key Recovery Agent	
		N

De sjabloon kiezen

De nieuwe certificaatsjabloon is nu opgenomen in de inhoud van de map Certificaatsjablonen.

違 certsrv - [Cer	tification Authority (Local)\CHUU-WIN	N12-CA\Certificate Templates]	
File Action View Help			
🗢 🔿 🙎 🙆 📓			
Certification Authority (Local) CHUU-WIN12-CA Revoked Certificates Pending Requests Failed Requests Certificate Templates	Name Image: Second S	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 Client Authentication Client Authentication Client Authentication Server Server Authentic	

Selecteer de LSC

Stap 10. Ga terug naar het venster Registry Editor en navigeer naar Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.

Stap 11. Bewerk de registraties EncryptionTemplate, GeneralPurposeTemplate, en SignatureTemplate zodat ze naar het nieuw gemaakte certificaatsjabloon verwijzen.



De sjabloon in het register wijzigen

Stap 12. Start de NDES-server opnieuw op, ga dus terug naar het venster Certificatie-instantie, selecteer de servernaam en selecteer achtereenvolgens de knop Stop en Play.

b	certsrv - [Certification Authority (Local)\CHUU-WIN12-CA]
File Action View Help	▶ ■
Certification Authority (Local)	Name Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates

LSC op de 9800 configureren

Hier volgen de stappen voor het configureren van LSC voor AP in WLC.

- 1. Maak een RSA-sleutel. Deze sleutel wordt later gebruikt voor PKI trustpoint.
- 2. Maak een trustpoint en breng de gemaakte RSA-sleutel in kaart.
- 3. Laat LSC levering voor APs toe en breng trustpoint in kaart.
 - 1. LSC inschakelen voor alle aangesloten AP's.
 - 2. LSC voor geselecteerde AP's inschakelen via voorzieningslijst.
- 4. Verander het Draadloze beheer trustpoint en punt aan LSC trustpoint.

Configuratiestappen AP LSC GUI

Stap 1.Navigeer naar configuratie > Beveiliging > PKI-beheer > genereren van sleutelparen.

- 1. Klik op Add en geef het een relevante naam.
- 2. Voeg de RSA-sleutelgrootte toe.
- 3. De belangrijkste exporteerbare optie is optioneel. Dit is alleen nodig als u de sleutel uit het vak wilt exporteren.
- 4. Selecteer Generate

 Configuration Administration Licensing Troubleshooting Troubleshooting Cost of 5 terms 	Configuration Key Name Type Exportable Zeroize Key Name RSA No Zeroize Key Type* RSA No Zeroize Key Type* RSA No Zeroize Key Type* RSA Key (The second second	
Administration TP-self-signed-2147029136 RSA No Image: Constraint of the second	Administration Pself-signed-2147029136 RSA No Image: Constraint of the second s	
Administration 9800-40.cisco.com RSA No Image: Comparison of the server of the se	OS Administration 9800-40.cisco.com RSA No Image: Comparison of the second seco	
Cisco_idevid_server RSA No Image: Cisco_idevid_server Z048 Cisco_idevid_server RSA No Image: Cisco_idevid_server Z048 Cisco_idevid_server RSA No Image: Cisco_idevid_server Z048 Cisco_idevid_server RSA No Image: Cisco_idevid_server Image: Cisco_i	C Licensing TP-self-signed- 2147029136.server RSA No 22rd Modulus Size* 2048	EC Key
CISCO_IDEVID_SUDI RSA No Image: contrast of the second sec		
CISCO_IDEVID_SUDI_LEGACY RSA No Image: Cisco_IDEVID_SUDI_LEGACY RSA Image: Cisco_IDEVID_SUDI_LEGACY RSA No Image: Cisco_IDEVID_SUDI_LEGACY RSA Image: Cisco_IDEVID_SUDI_LEGACY RSA<	CISCO_IDEVID_SUDI RSA No 2010	
H I </td <td>CISCO_IDEVID_SUDI_LEGACY RSA No 🔒 Zero Key Exportable*</td> <td></td>	CISCO_IDEVID_SUDI_LEGACY RSA No 🔒 Zero Key Exportable*	
	H 4 1 ⊨ H 10 - 1 - 5 of 5 items Cancel	✓ Generate

Stap 2. Navigeren naar configuratie > Beveiliging > PKI-beheer > Trustpoints

- 1. Klik op Add en geef het een relevante naam.
- 2. Voer de URL van de inschrijving in (hier is de URL <u>http://10.106.35.61:80/certsrv/mscep/mscep.dll</u>) en de rest van de gegevens.
- 3. Selecteer RSA-sleutelparen die in stap 1 zijn gemaakt.
- 4. Klik op Verifiëren.
- 5. Klik op Inschrijven op trustpoint en voer een wachtwoord in.
- 6. Klik op Toepassen op apparaat.

Q Search Menu Items	Configuration • > Set	curity * > PKI Management		
🚍 Dashboard	Add Trustpoint			×
	Label*	Access_Point-MS-CA	Enrollment Type	SCEP O Terminal
(Monitoring >	Subject Name			
Configuration >	Country Code	IN	State	КА
Administration	Location	Bengaluru	Domain Name	TAC-LAB.cisco.local
C Licensing	Organization	TAC	Email Address	mail@tac-lab.local
K 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

Stap 3.Navigeer naar Configuration > Wireless > Access points. Scroll naar beneden en selecteer LSC Provision.

- 1. Selecteer de status zoals deze is ingeschakeld. Dit laat LSC voor alle APs toe die aan deze WLC worden aangesloten.
- 2. Selecteer de trustpoint naam die we in Stap 2 gecreëerd hebben.

Vul de rest van de gegevens in volgens uw behoeften.

Q. Search Menu Items	Configuration * > Wireless * > Access Points				
🚃 Dashboard	 All Access Points 				
Monitoring	Total APs : 1		T	International APs Seg : 0 Country Code : 0 LSC	Fallback : 0 Select an Action 🔹
Configuration >	AP Name : AP Model :	Slots i Status Up Time i IP Address	Base Radio MAC E	AP i Po themet MAC i Mode Ca	wer Derate i Operation i Config spable Status Status
(Õ) Administration →	AP0CD0-F89A-46E0 🙏 🧮 C9117AXI-D	2 O days 0 hrs 26 10.105.101 mins 42 secs	.158 d0ec.3579.0300 0	cd0.189a.46e0 Local Ye	s Registered Health,
C Licensing	R K 1 P R 10 V				1 - 1 of 1 access points
X Troubleshooting	> 6 GHz Radios				
	> 5 GHz Radios				
	> 2.4 GHz Radios				
	> Dual-Band Radios				
	> Country				
	 LSC Provision 				
	Status	Enabled •	Subject Name Paramete	ers	E Apply
	Trustpoint Name	Access_Point-MS .# +	Country	IN	
	Number of Join Attempts	3	State	КА	
	Key Size	2048 v	City	Bengaluru	
	Seroncate crain status		Organization	TAC	

Zodra u LSC inschakelt, downloaden AP's het certificaat via WLC en rebooten. In de AP console sessie, zie je dan iets als dit fragment.

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

Stap 4.Zodra LSC is ingeschakeld, kunt u het certificaat voor draadloos beheer wijzigen in overeenstemming met het LSC-betrouwbaarheidspunt. Dit maakt AP's samenvoegen met hun LSC-certificaten en de WLC gebruikt zijn LSC-certificaat voor AP-samenvoegen. Dit is een optionele stap als uw enige interesse is om 802.1X-verificatie van uw AP's te doen.

- 1. Ga naar Configuration > Interface > Wireless en klik op Management Interface.
- 2. Verander het Trustpoint om het trustpoint aan te passen dat we in stap 2 hebben gemaakt.

Hiermee is het configuratieonderdeel van de LSC GUI voltooid. APs moet zich bij WLC kunnen nu aansluiten met behulp van de LSC cert.

Q. Search Menu Items	Configuration * > Interface * > Wireless Edit Management Interface *
Dashboard	Add Changing the interface or trustpoint will cause APs to disconnect and disrupt clients.
0	Interface Name Y Interface Type Y VLAN ID Y IP Address Y IP Netmask
Monitoring →	Van101 Management 101 10.105.101.160 255.255.25
Configuration	H < 1 > H 10 v There is no trustpoint configured on the controller. CISCO_DEVID_SUDI is used as the default trustpoint.
() Administration	NAT IDu/IDu/ Server Advisor 0.0.0.0
C Licensing	
Y Troubleshooting	
6.40	
	Cancel

Configuratiestappen AP LSC CLI

1. Maak een RSA-toets met deze opdracht.

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 storage Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported

 Maak PKI-trustpoint en breng het RSA-sleutelpaar in kaart. Voer de URL van de inschrijving en de rest van de gegevens in.

```
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. Verifieer en registreer het PKI-vertrouwenspunt met de CA-server met behulp van de opdracht crypto pki authenticate <trustpoint>. Voer een wachtwoord in als om het wachtwoord wordt gevraagd.

```
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. AP-verbinding configureren met LSC-certificaat.

```
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. Verander het Draadloze Management Trustpoint om het trustpoint aan te passen dat hierboven is gemaakt.

9800-40(config)#wireless management trustpoint Access_Point-MS-CA

AP LSC-verificatie

Voer deze opdrachten op WLC uit om de LSC te verifiëren.

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

```
9800-40#sho ap lsc-provision summ
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : Access_Point-MS-CA
    Certificate chain status : Available
   Number of certs on chain : 2
    Certificate hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
LSC Revert Count in AP reboots : 10
AP LSC Parameters :
Country : IN
State : KA
City : Bengaluru
Orgn : TAC
Dept : TAC-LAB.cisco.local
Email : mail@tac-lab.local
Key Size : 2048
EC Key Size : 384 bit
AP LSC-provision List :
Total number of APs in provision list: 0
Mac Addresses :
9800-40#sho wire
9800-40#sho wireless man
9800-40#sho wireless management tru
9800-40#sho wireless management trustpoint
Trustpoint Name : Access_Point-MS-CA
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
Private key Info : Available
FIPS suitability : Not Applicable
9800-40#
```



Zodra APs worden herladen, meld u aan bij AP CLI en voer deze opdrachten uit om LSCconfiguratie te verifiëren.

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

```
AP0CD0.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:
```

APBCODe.F89A.46E0#sho crypto in LSC LSC: Enabled APBCODe.F89A.46F60#sho capwap cli config in lsc APB lsc mable : 1 AP lsc reboot cnt : 0 AP lsc reboot cnt : 0 AP lsc mode : 10t AP lsc dtls fallback state : 0 APBCODe.F89A.46E0# Read timed out
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

Probleemoplossing voor LSC-provisioning

U kunt een EPC-opname maken van de WLC of AP uplink switch poort om te controleren of het certificaat dat AP gebruikt om de CAPWAP- te vormen. Controleer vanuit de PCAP of de DTLStunnel met succes is gebouwd.



DTLS-debugs kunnen worden uitgevoerd op AP en WLC om het certificaatprobleem te begrijpen.

AP-bekabelde 802.1X-verificatie met LSC

AP is ingesteld om hetzelfde LSC-certificaat te gebruiken voor verificatie. AP fungeert als 802.1X aanvrager en wordt door de switch geverifieerd op basis van de ISE-server. ISE-server praat met de AD in het backend.



Opmerking: als dot1x-verificatie is ingeschakeld op de poort van de AP uplink-switch, kunnen AP's geen verkeer doorsturen of ontvangen totdat de verificatie is doorgegeven. Als u AP's met onsuccesvolle verificatie wilt herstellen en toegang tot AP wilt krijgen, schakelt u dot1x auth uit op de bekabelde AP-switch poort.

EAP-TLS-verificatie, werkstroom en berichtenuitwisseling



Configuratiestappen voor AP Wired 802.1x-verificatie

- 1. Schakel dot1x-poortadapter in samen met CAPWAP DTLS en selecteer het EAP-type.
- 2. Creeer dot1x geloofsbrieven voor APs.
- 3. Schakel dot1x in op de switch.
- 4. Installeer een vertrouwd certificaat op de RADIUS-server.

Configuratie van bekabelde AP-802.1x-verificatie en GUI

- 1. Navigeer naar het toetredingspartnersprofiel van het toegangspunt en klik op het profiel.
 - 1. Klik op AP > Algemeen. Selecteer het EAP-type en het AP-autorisatietype als "CAPWAP DTLS + dot1x port auth".
 - 2. Navigeer naar Beheer > Credentials en voer een gebruikersnaam en wachtwoord in voor AP dot1x-verificatie.

Cisco Ca	talyst 9800-40 Wireless Controller		Welcome admin 🛛 🛠 🌾 🛕 🖺 🏟 🗐 📿	Search APs and Clents Q
Q. Search Manu Items	Configuration * > Tags & Profiles * > AP Join		Edit AP Join Profile General Client CAPWAP AP Management Si	x iecurity ICap QoS
Dashboard Monitoring	AP Join Profile Name	▼ Des	General Power Management Hyperlocation AP Statis	Client Statistics Reporting Internal
	APG_test tootSte		Switch Flag	5 GHz (soc) 90
{⊙} Administration → (©) Licensing	APG_3rd-Fir-APs APG_4th-Fir-APs		Power Injector State Power Injector Type Unknown	2.4 GHz (sec) 90 Extended Module
💥 Troubleshooting	APG_00+Fr-APs APG_70+Fr-APs APG_80+Fr-APs		AP EAP Auth Configuration	Enable Mesh
Walk Me Through 2	APG_11th-Fir-APs APG_12th-Fir-APs APG_12th-Fir-APs		EAP Type EAP-TLS v AP Authorization Type CAPVAP DTLS + DDTs. CAPVAP DTLS +	Profile Name default-mesh-pro • Clear
	H < 1 2 3 → H 10 v		DOTTx port auth CAPWAP DTLS Dottx port auth	
			"D Cancel	🗄 Update & Apply to Device

Cisco Cisco C	Catalyst 9800-40 Wireless Controller	Welcome admin 🛛 🗰 🦚 🤷 🖄 🖗 🔅 🖗 🕫 Scenet APs and Choice Q
Q Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile ×
Dashboard	+ Add >> 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	Dot1x Username ap-wired-user
C Administration	testSite	Dottx Password
~	APG_3rd-Fir-APs	Dot tx Password Type
C Licensing	APG_4th-Fir-APs	
💥 Troubleshooting	APG_6th-Fir-APs	
	APG_7th-FP-APs	
	APG_80FFFFAPs	
	APG_100-FR-APs	
Walk Me Through >		
		Cancel

CLI-configuratie voor AP-bekabelde 802.1x-verificatie

Gebruik deze opdrachten om dot1x voor AP's vanuit de CLI in te schakelen. Dit maakt alleen bekabelde verificatie mogelijk voor AP's die gebruik maken van het specifieke Joed-profiel.

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

Configuratie van bekabelde AP-Switch 802.1x-verificatie

Deze switch configuraties worden gebruikt in LAB om bekabelde AP-verificatie in te schakelen. U kunt verschillende configuratie hebben op basis van ontwerp.

```
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
```

Installatie van RADIUS-servercertificaat

De verificatie vindt plaats tussen het toegangspunt (dat fungeert als de aanvrager) en de RADIUSserver. Beiden moeten elkaar vertrouwen. De enige manier om het AP-vertrouwen in het RADIUSservercertificaat te hebben, is om de RADIUS-server een certici-certificaat te laten gebruiken dat is afgegeven door de SCEP CA die ook het AP-certificaat heeft afgegeven.

In ISE, ga naar Administratie > Certificaten > Generate Certificaat Ondertekeningsaanvragen

Genereer een CSR en vul de velden met de informatie van uw ISE-knooppunt.

Administration - System

Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings							
Deployment Licensing Certificate Management ~ System Certificates ~ OCSP Client Profile ~ Certificate Signing Requests ~ Certificate Authority >	contribution logging Maintenance Upgrade Health Decks Backup & Restore Admin Access Settings							
	Certificate(s) will be used for EAP Authentication Allow Wildcard Certificates							
	Node(s) Generate CSR's for these Nodes:							
	Node CSR Friendly Name							
	ISE99 ISE99#EAP Authentication							
	Subject Common Name (CN)							
	SFQDN\$ O							
	Organizational Unit (OU)							
	Organization (O)							
	City (L)							
	State (ST)							

Nadat u deze hebt gegenereerd, kunt u deze exporteren en ook kopiëren en plakken als tekst.

Navigeer naar uw Windows CA IP-adres en voeg /certsrv/ toe aan de URL

Klik op Certificaat aanvragen

← → C ▲ Non sécurisé 192.168.1.98/certsrv/
Microsoft Active Directory Certificate Services mydomain-WIN-3E202T1QD0U-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
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

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

Klik op Een certificaataanvraag indienen met een base-64



Microsoft Active Directory Certificate Services -- mydomain-WIN-3E202T1QD0U-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 second CMC as DICCS (10.5)

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.

Plakt de MVO-tekst in het tekstvak. Kies de sjabloon voor het webservercertificaat.

← 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 (CMC or PKCS #10 or PKCS #7):
Certificate Template: (No templates found!) >
Additional Attributes:

U kunt dit certificaat vervolgens op ISE installeren door terug te gaan naar het menu Certificaatondertekeningsaanvraag en klik op Bindcertificaat. U kunt vervolgens het certificaat uploaden dat u bij uw Windows C hebt verkregen.

≡ Cisco ISI	E	Administration - System									
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Check	s Backu	p & Restore	Admin Access	Se	ettings
Certificate Managemen System Certificates	ıt ~	Certif	icate Si	gning Rec	luests						
Trusted Certificates OCSP Client Profile		Generate	Certificate Signi	ing Requests (CSR)							
Certificate Signing R	equests	A Certificate this list.	Signing Requests	(CSRs) must be sent to	o and signed by an	external authority. C	lick "export" to	download one or	more CSRs so that they	may be	signed by an external authority. After a request has been signed, click
	intern open.	Q View	🖞 Export 🏾 🗍	Delete Bind Ce	ertificate						
Certificate Authority	>	D F	riendly Name		Certificat	e Subject	Key Length	Portal gro	Timestamp	^	Host
			SE99#EAP Auth	entication	CN=ISE99	9.mydomain.local	4096		Mon, 30 Oct 2023		ISE99

Verificatie van bekabelde AP-802.1x-verificatie

Neem consoletoegang tot AP en voer de opdracht uit:

#show ap authentication status

Ap-verificatie is niet ingeschakeld:

Console logt vanaf AP na het inschakelen van ap auth:

```
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 is geverifieerd:



WLC-verificatie:

9800-40#sho ap name AP0CD0.F89)A.46E0 config general begin Certificate							
P Certificate type : Locally Significant Certificate								
P Certificate Expiry-time : 09/25/2024 06:48:23								
AP Certificate issuer common-n	AP Certificate issuer common-name : sumans-lab-ca							
AP Certificate Policy	: Default							
AP CAPWAP-DTLS LSC Status								
Certificate status	: Available							
LSC fallback status	: No							
Issuer certificate hash	hash : 611255bc69f565af537be59297f453593e432e1b							
Certificate expiry time	09/25/2024 06:48:23							
AP 802.1x LSC Status								
Certificate status	: Available							
Issuer certificate hash	ertificate hash : 611255bc69f565af537bc59297f453593e432e1b							
Certificate expiry time	1 09/25/2024 06:48:23							
AP LSC authentication state	: CAPWAP-DTLS and 882.1x authentication							

SwitchPort-interfacestatus na succesvolle verificatie:

Switch#sho authenticatio Interface	n sessions inte MAC Address	rface gi Method	gabitEth Domain	Status Fg	Session ID
Gi1/0/2	0cd0.f89a.46e0	dot1x	DATA	Auth	9765698A000005CCEED0FBF

Dit is een voorbeeld van logbestanden van de AP-console die wijzen op een succesvolle verificatie:

```
[*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
```

Probleemoplossing 802.1X-verificatie

Neem PCAP op de AP uplink en controleer de radius authenticatie. Hier is een fragment van succesvolle verificatie.

4	79	07:47:17.192983	Cisco_9a:46:e0	Nearest-non-TP_	EAP		Response, Identity(Packet size limited during capture)	
4	79	07:47:17.205983	Cisco_9a:46:e8	Nearest-non-TP_	TLSv1.2	514 55431	Encrypted Handshake Kessage	
4	79	07:47:17.256975	Cisco_9a:46:e0	Nearest-non-TP_	EAP	812 55431	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
4	79	07:47:17.267976	Cisco_9a:46:e8	10.105.101.151 Nearest-non-TP	EAP 1	812 55431	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
4	79	07:47:17.270982 07:47:17.274979	Cisco_9a:46:e8	10.105.101.151 Nearest-non-TP	EAP	812 55431	Access-Ctallange 20/249 Response, TLS EAP (EAP-TLS)[Packet size limited during capture]	
• 4	79 79 . .	07:47:17.277985 07:47:17.311980	10.186.34.170 Cisco_9a:46:e0	18.105.101.151 Nearest-non-TP.	EAP 1	812 55431	Access-Challenge 100247 Response, TLS EAP (EAP-TLS)	
• 4	79	07:47:17.318968	Cisco_9a:46:e8	10.105.101.151 Nearest-non-TP.	RADIUS 11 EAP	812 55431	Response, TLS EAP (EAP-TLS)	
	79	07:47:17.324988	10.126.34.170 Cisco 9a:46:e0	10.105.101.151 Nearest-non-TP_	RADIUS 11 TLSv1.2	512 55431	Screen Colleman 20040 Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake M	
4	79	07:47:17.339978 07:47:17.342959	10.185.34.170 Cisco 9a:46:e8	10.105.101.151	RADIUS 1	912 55431	Accest-Challenge 10:228 Researce. TIS FAP (FAP-TIS)[Parket size limited during canture]	
4	79	07:47:17.376979	10.106.34.170	18.105.101.151	RADIUS 1	812 55431	Access-Accest 16231	

TCPdump verzamelt van ISE-opnamen van de verificatie.



Als er een probleem wordt geobserveerd tijdens de verificatie, is er een gelijktijdige pakketopname van de bekabelde AP-uplink en de ISE-zijde nodig.

Debug opdracht voor AP:

#debug ap authentication packet

Gerelateerde informatie

- <u>Cisco Technical Support en downloads</u>
- <u>802.1X configureren op AP met AireOS</u>
- 9800 configuratiehandleiding voor LSC
- LSC-configuratievoorbeeld voor 9800
- 802.1X configureren voor AP's op 9800

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.