SCEP configureren voor lokaal belangrijke provisioning op 9800 WLC

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram SCEP-services in Windows-server inschakelen Wachtwoord voor invoeren van SCEP uitschakelen Configuratie van de certificaatsjabloon en het register Het 9800 apparaatpunt configureren AP-inschrijvingsparameters definiëren en beheerstitel bijwerken Verifiëren Controleer de installatie van het controleleidingscertificaat Controleer de 9800 WLC LSC-configuratie Controleer de installatie van een access point Problemen oplossen Gemeenschappelijke kwesties Opdrachten voor debug en inloggen Voorbeeld van een succesvolle inschrijving

Inleiding

Dit document beschrijft hoe u de 9800 draadloze LAN-controller (WLC) kunt configureren voor een LSC-inschrijving (Local Significant certificaatinschrijving) voor een access point (AP), die zich bij doelstellingen aansluit via de Microsoft Network Apparaatinschrijving Service (NDES) en Simple certificaatinschrijving Protocol (SCEP) binnen Windows Server 2012 R2-standaard.

Voorwaarden

Om SCEP met de Windows Server succesvol te kunnen uitvoeren, moet de 9800 WLC aan deze vereisten voldoen:

- Er moet bereikbaarheid zijn tussen de controller en de server.
- De controller en de server zijn gesynchroniseerd op dezelfde NTP-server, of delen dezelfde datum en tijdzone (Als de tijd verschilt tussen de CA-server en de tijd vanaf de AP, geeft AP certificatie en installatie uit).

De Windows Server moet de Internet Information Services (IS) eerder ingeschakeld hebben.

Vereisten

Cisco raadt aan dat u kennis hebt van deze technologieën:

- 9800 draadloze LAN-controller versie 16.10.1 of hoger.
- Standaard Microsoft Windows Server 2012.
- Private Key Infrastructuur (PKI) en certificaten.

Gebruikte componenten

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

- 9800-L WLC software versie 17.2.1.
- Windows Server 2012 Standaard R2.
- 3802 access points.

Opmerking: De configuratie van de serverzijde in dit document is specifiek WLC SCEP. Raadpleeg Microsoft TechNet voor de configuratie van de server voor extra versterking, beveiliging en certificering.

Achtergrondinformatie

De nieuwe LSC-certificaten, zowel het certificaat van oorsprong als het certificaat van de certificeringsinstantie (CA), moeten op de controller worden geïnstalleerd om het uiteindelijk in de AP's te kunnen downloaden. Met SCEP worden de CA- en apparaatcertificaten ontvangen van de CA-server en later automatisch in de controller geïnstalleerd.

Dezelfde certificeringsprocedure vindt plaats wanneer de AP's voorzien zijn van LSC's; daartoe treedt de controller op als een CA-proxy en helpt hij bij het verkrijgen van het certificaatverzoek (zelf-gegenereerd) dat door de CA voor de AP is ondertekend.

Configureren

Netwerkdiagram



SCEP-services in Windows-server inschakelen

Stap 1. In de toepassing **Server Manager**, selecteer het menu **Manager** en selecteer vervolgens de optie **Rollen en functies toevoegen** om de rol Add Roles and Functies Configuration Wizard te openen. Selecteer vanuit dat punt de serverinstantie die wordt gebruikt voor SCEP serverinschrijving.

Stap 2 . Controleer dat de functies voor inschrijving van het netwerkapparaat en online responder zijn geselecteerd en selecteer vervolgens Volgende:

L	Add Roles and Features Wizard	_ 🗆 X
Before You Begin Installation Type Server Selection Server Roles Features	Add Roles and Features Wizard Select one or more roles to install on the selected server. Roles	DESTINATION SERVER Chuu-Win12.chuu-domain.local Description Windows Server Essentials Experience sets up the IT infrastructure and provides powerful functions such as PC backups that below servers that and Beneto Web
Confirmation Results	 Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder Active Directory Domain Services (Installed) Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server (Installed) Fax Server 	helps protect data, and Remote Web Access that helps access business information from virtually anywhere.
	< Previous	Next > Install Cancel

Stap 3 . Selecteer Volgende tweemaal en Voltooi de configuratie wizard. Wacht totdat de server het installatieproces van de optie heeft voltooid, en selecteer vervolgens Sluiten om de wizard te sluiten.

Stap 4. Zodra de installatie is voltooid, wordt een waarschuwingspictogram weergegeven in het pictogram Meldingen van Server Manager. Selecteer de optie en selecteer de optie **Active Directory Services instellen op de** optie **doelserver** om de wizard **AD CS Configuration** te starten.



Stap 5. Selecteer de Inschrijvingsservice voor het netwerkapparaat en de online RESPonderrolservices die in het menu moeten worden ingesteld, en selecteer Volgende.

Stap 6. Selecteer in de Service Account for NDES ofwel optie tussen de ingebouwde applicatie of de servicekening en selecteer vervolgens Volgende.

Opmerking: Controleer of de account deel uitmaakt van de groep IS_IUSRS.



Stap 7. Selecteer **Volgende** voor de volgende schermen en laat het installatieproces voltooid zijn. Na de installatie is de SCEP url beschikbaar bij een webbrower. Navigeer naar de URL http://<server ip>/certsrv/mscep/mscep.dll om te controleren of de service beschikbaar is.

A Network Davice Enrollment Service X	_		X
← → C (① No seguro 172.16.80.8/certsrv/mscep/mscep.dll	\$	(P)	:
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 network devices to submit certificate requests.

To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is <u>http://Chuu-Win12/CertSrv/mscep_admin</u>

For more information see Using Network Device Enrollment Service.

Wachtwoord voor invoeren van SCEP uitschakelen

Standaard gebruikte de Windows Server een dynamisch uitdagingswachtwoord om client- en endpointverzoeken voor inschrijving binnen Microsoft SCEP (MSCEP) te authentiseren. Hiervoor is een beheeraccount nodig om naar de web GUI te bladeren om voor elk verzoek een wachtwoord op aanvraag te genereren (het wachtwoord moet in het verzoek worden opgenomen).De controller kan dit wachtwoord niet opnemen in de verzoeken die hij naar de server stuurt. Om deze optie te verwijderen, moet de registratiesleutel op de NDES-server worden aangepast:

Stap 1. Open het registratieformulier en zoek naar Regedit in het menu Start.

Stap 2 . Navigatie naar computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptografie > SCEP > Wachtwoord voor noodgevallen

Stap 3. Verander de waarde voor **EnforcePassword** naar 0. Als deze al 0 is, laat deze dan ongewijzigd.

۲		Registry Editor		_ 🗆 X
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
— 👢 САТуре		(Default)	REG SZ	(value not set)
CertsInMYStore		8 EnforcePassword	REG_DWORD	0x0000000 (0)
EnforcePassword				
PasswordVDir				
- L OID	≡			
- Protect	_			
- Providers				
DataAccess				
Device Association Framework				N
Dfra				4
DES				
DHCPMibAgent				
DirectDraw				
DirectInput				
DirectPlay8				
DirectPlayNATHelp	\sim			
< III >		<	III	>
Computer\HKEY_LOCAL_MACHINE\	OFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword

Configuratie van de certificaatsjabloon en het register

Certificaten en bijbehorende toetsen kunnen in meerdere scenario's worden gebruikt voor verschillende doeleinden die worden gedefinieerd door het toepassingsbeleid binnen de CA Server. Het toepassingsbeleid wordt opgeslagen in het veld Extended Key Use (EKU) van het certificaat. Dit veld wordt door de authenticator geparseerd om te controleren of het door de cliënt voor de doeleinden waarvoor het is ontworpen wordt gebruikt. Om ervoor te zorgen dat het juiste toepassingsbeleid in de WLC en AP certificaten wordt geïntegreerd, moet u het juiste certificaatsjabloon maken en naar het NDES-register toewijzen:

Stap 1 . Navigeer naar Start > Administratieve hulpmiddelen > certificeringsinstantie.

Stap 2. Vouw de map CA Server uit, klik met de rechtermuisknop op de mappen **certificaatsjablonen** en selecteer **Beheer**.

Stap 3. Klik met de rechtermuisknop op de-toepassingssjabloon en selecteer vervolgens **Dubbele sjabloon** in het contextmenu.

Stap 4 . Navigeer naar het tabblad **Algemeen**, verander de naam van de sjabloon en de geldigheidsperiode naar wens, laat alle andere opties ongecontroleerd.

Voorzichtig: Zorg er bij wijziging van de geldigheidsduur voor dat deze niet groter is dan de

geldigheid van het basiscertificaat van de certificeringsinstantie.

Properties of New Template					
Subject Name	Sen	ver	Issuance R	equirements	
Superseded Templa	tes	Exte	ensions	Security	
Compatibility General	Request	Handling	Cryptography	Key Attestation	
Template display name:					
9800-LSC					
Template name:					
9800-LSC					
Validity period:		Renewa	period:		
2 years	1	6	weeks v		
	1		HOOKS Y		
Publish certificate in	Active Di	rectory			
Do not automatic	ally reenro	oll if a dupli	cate certificate e	exists in Active	
Directory					
ОК	(Cancel	Apply	Help	

Stap 5. Navigeer naar het tabblad **Onderwerp**, zorg ervoor dat **Levering in het verzoek** is geselecteerd. Uit een pop-upvenster blijkt dat gebruikers geen admin-goedkeuring nodig hebben om hun certificaat te laten ondertekenen, maar selecteer **OK**.

Properties of New Template							
Compatibility General Request Handling Cryptography Key Attestation							
Supersec	ded Templa	ites	Exte	ensions	Security		
Subject N	lame	Sen	ver	Issuance R	equirements		
Supply in the request Use subject information from existing certificates for autoenrollment renewal requests (*)							
 Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. 							

Stap 6 . Navigeer naar het tabblad **Uitbreidingen**, selecteer vervolgens de optie **Toepassingsbeleid** en selecteer de knop **Bewerken...**. Zorg ervoor dat **clientverificatie** zich in het venster **Toepassingsbeleid** bevindt; anders selecteert u **Toevoegen** en voegt u dit toe.

Properties of New Template						
Compatibility	General	Request	Handling	Cryptography	Key Attestation	
Subject N	Name	Ser	ver	Issuance F	lequirements	
Superse	ded Templa	tes	Exte	insions	Security	
To modify an	n extension	, select it, his templa	and then c te:	lick Edit.		
Applicat	ion Policies			_		
Edit	Applicati	on Poli	cies Exte	nsion 💌		
An application policy defines how a certificate can be used.						
Application p Client Auth Encrypting Secure Ema	oolicies: entication File System ail				Edit	

Stap 7. Navigeer naar het tabblad **Security**, zorg ervoor dat de servicekaart die is gedefinieerd in Stap 6 van de **SCEP-services in de Windows** Server **alle**beheerrechtenvan de

	Properties	of New	Template			
Compatibility Gene	eral Request	Handling	Cryptography	Key Attestation		
Subject Name	Ser	ver	Issuance R	equirements		
Superseded Te	emplates	Exte	ensions	Security		
Group or user names:						
& Authenticated	Users					
Administrator						
Standard Domain Admin	ns (CHUU-DOI	MAIN\Dom	iain Admins)			
Section 2018	(CHUU-DOM	AIN\Doma	in Users)			
Senterprise Ad	mins (CHUU-D	OMAIN\Er	nterprise Admins)			
			Add	Remove		
		L	Add	Remove		
Permissions for Ad	ministrator		Add Allow	Remove Deny		
Permissions for Ad	ministrator		Add Allow	Deny		
Permissions for Adr Full Control Read	ministrator		Add Allow	Remove Deny		
Permissions for Adr Full Control Read Write	ministrator		Add Allow	Deny		
Permissions for Adr Full Control Read Write Enroll	ministrator		Add Allow	Remove Deny		
Permissions for Adr Full Control Read Write Enroll Autoenroll	ministrator		Add Allow	Remove Deny		
Permissions for Adr Full Control Read Write Enroll Autoenroll	ministrator		Add Allow	Remove Deny		
Permissions for Adr Full Control Read Write Enroll Autoenroll	ministrator		Add Allow	Remove Deny		
Permissions for Adr Full Control Read Write Enroll Autoenroll	ministrator		Add Allow	Remove Deny		
Permissions for Adr Full Control Read Write Enroll Autoenroll For special permiss Advanced.	ninistrator	ced setting	Add Allow V V s, click	Remove Deny		
Permissions for Adr Full Control Read Write Enroll Autoenroll For special permiss Advanced.	ions or advance	ced setting	Add Allow V V s, click	Remove Deny		
Permissions for Adr Full Control Read Write Enroll Autoenroll For special permiss Advanced.	ions or advance	ced setting	Add Allow I	Remove Deny		
Permissions for Adr Full Control Read Write Enroll Autoenroll For special permiss Advanced.	ninistrator	ced setting	Add Allow V V s, click	Remove Deny		

Stap 8. Ga terug naar het venster **van de certificeringsinstantie**, 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 nieuwe certificaatsjabloon in meerdere serverimplementaties wordt opgenomen, aangezien deze over alle servers moet worden gerepliceerd.

	Enable Certificate Templates	X
Select one Certificate Template to Note: If a certificate template that information about this template has All of the certificate templates in th For more information, see <u>Cert</u>	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. tificate Template Concepts.	
Name	Intended Purpose	~
9800-LSC CA Exchange Code Signing Cross Certification Authority Enrollment Agent Enrollment Agent (Computer) Exchange Signature Only Exchange User	Client Authentication, Secure Email, Encrypting File System Private Key Archival Code Signing <all> Certificate Request Agent Certificate Request Agent Secure Email Secure Email</all>	Ξ
IPSec Key Recovery Agent OCSP Resnanse Signing	IP security IKE intermediate Key Recovery Agent OCSP Signing OK Cano	.⊳

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

違 certsrv - [Cer	tification Authority (Local)\CHUU-WI	N12-CA\Certificate Templates]	- 🗆 🗙	
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 Kerberos 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>		
				_

Stap 10. Ga terug naar het venster Registereditor en navigeer naar Computer >

Stap 11. Bewerk de registers **EncryptionSjabloon**, **GeneralPurposeSjabloon** en **SignatureSjabloon** zodat deze op de nieuw gemaakte certificaatsjabloon wijzen.

٤.	Registry Editor		_ 🗆 X
File Edit View Favorites Help			
File Edit View Favorites Help Defaults Defaults MSCEP CAType CertsInMYStore EnforcePassword PasswordVDir Defaults Protect Providers Defaults Defaults EnforcePassword EnforcePassword PasswordVDir PasswordVDir Defaults Defaults EnforcePassword EnforcePassword PasswordVDir EnforcePassword Defaults Defaults EnforcePassword Enforces Enforces Enforces Enforces Enforces Enforces	Name (Default) (Defa	Type REG_SZ REG_SZ REG_SZ REG_SZ	Data (value not set) 9800-LSC 9800-LSC 9800-LSC
DFS DHCPMibAgent DirectDraw			
▷-↓ DirectInput ✓			
<	<	Ш	>
Computer\HKEY_LOCAL_MACHINE\SOFT	WARE\Microsoft\Crypto	ography\MSCEP	.:

Stap 12. Start de NDES-server opnieuw, ga dus terug naar het venster **Certified Authority**, selecteer de naam van de server en selecteer achtereenvolgens de knop **Stop** en **Play**.



Het 9800 apparaatpunt configureren

De controller moet beschikken over een betrouwbaar punt om AP's te authentificeren zodra er

voorzieningen zijn getroffen. Het vertrouwde punt omvat het 9800 device certificaat, samen met het CA root certificaat dat beide van dezelfde CA server (Microsoft CA in dit voorbeeld) wordt verkregen. Om een certificaat in het trustpoint te kunnen installeren, moet het de onderwerpreigenschappen bevatten samen met een paar RSA toetsen verbonden aan het. De configuratie wordt uitgevoerd via de webinterface of de opdrachtregel.

Stap 1. Navigeer naar Configuration > Security > PKI Management en selecteer het tabblad RSAsleutelpaar. Selecteer de knop + Add.

Stap 2. Defineer een etiket dat aan het toetsenbord is gekoppeld en zorg ervoor dat het vakje **Exporteerbaar** is geselecteerd.

Server RSA Keypair Gener	Trustpoint			
+ Add				
(ey Label ~	Key Exportable 🗸	Zeroise RSA Key	(
P-self-signed-1997188793	No	E Zeroise	Key Label*	AP-LSC
AP-KEY	Yes		Madulua Cine#	2048
chaincert.pfx	No	🖹 Zeroise	Modulus Size-	2040
P-self-signed-1997188793.server	No	2 Zeroise	Key Exportable*	
SISCO_IDEVID_SUDI_LEGACY	No	2 Zeroise	Cancel	Generate
CISCO_IDEVID_SUDI	No	🖹 Zeroise	Cancer	Concrate
SLA-KeyPair	Yes	🖹 Zeroise		
	Vec	2 Zarojsa		

CLI-configuratie voor stap één en twee, in dit configuratievoorbeeld, wordt het sleutelpaar gegenereerd met een label AP-LSC en een modulusgrootte van 2048 bits:

9800-L(config)#crypto key generate rsa exportable general-keys modulus

The name for the keys will be: AP-LSC % The key modulus size is 2048 bits % Generating 2048 bit RSA keys, keys will be exportable... [OK] (elapsed time was 1 seconds)

Stap 3. Selecteer in dezelfde sectie het tabblad Trustpunt en selecteer de knop + Add.

Stap 4 . Vul de trustpuntgegevens met de apparaatinformatie in en selecteer vervolgens Toepassen op apparaat:

- Het veld Label is de naam die aan het trustpunt is gekoppeld
- Voor URL-inschrijving gebruikt u de URL die is gedefinieerd in stap 7 van het gedeelte SCEPservices inschakelen in het gedeelte Windows Server
- Controleer of het selectieteken voor authenticatie is geselecteerd zodat het CA-certificaat wordt gedownload

- Het veld **Domain Name** wordt geplaatst als de eigenschap common name van het certificaatverzoek
- Controleer het selectieteken **Key Generated**, een uitrolmenu verschijnt en selecteer het sleutelpaar dat in Stap 2 gegenereerd is
- Controleer het selectieteken invoeren, twee wachtwoorden instellen. Typ een wachtwoord. Dit wordt gebruikt om de certificaatsleutels te binden met het certificaat van het apparaat en het CA-certificaat

Waarschuwing: De 9800-controller ondersteunt serverketens met meerdere lagen niet voor een LSC-installatie. Daarom moet de kern-CA de code zijn die de certificaatverzoeken van de controller en de AP's tekent.

Add Trustpoint				×
Label*	9800-LSC		Enrollment URL	certsrv/mscep/mscep.dll
Authenticate				
Subject Name				
Country Code	MX		State	CDMX
Location	Juarez		Organisation	Wireless TAC
Domain Name	chuu-domain.local		Email Address	jesuherr@cisco.com
Key Generated	 Image: A start of the start of	1		
Available RSA Keypairs	AP-LSC T)		
Enroll Trustpoint	 Image: A start of the start of			
Password	•••••]		
Re-Enter Password	•••••			
Cancel				Apply to Device

CLI-configuratie voor stap drie en vier:

Voorzichtig: De onderwerpregel moet worden geformatteerd in de LDAP-syntaxis, anders wordt hij niet door de controller geaccepteerd.

9800-L(config)#crypto pki trustpoint

```
9800-L(ca-trustpoint)#enrollment url http://
```

```
9800-L(ca-trustpoint)#subject-name C=
```

```
9800-L(ca-trustpoint)#rsakeypair
```

```
9800-L(ca-trustpoint)#revocation-check none
9800-L(ca-trustpoint)#exit
9800-L(config)#crypto pki authenticate
```

```
Certificate has the following attributes:
      Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
      Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-L(config)#crypto pki enroll <trustpoint name>
% 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:
Re-enter password:
% The subject name in the certificate will include: C=MX, ST=CDMX, L=Juarez, O=Wireless TAC,
CN=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
% The subject name in the certificate will include: 9800-L.alzavala.local
% Include the router serial number in the subject name? [yes/no]: no
% 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 AP-LSC' commandwill show the fingerprint.
```

AP-inschrijvingsparameters definiëren en beheerstitel bijwerken

AP-inschrijving gebruikt de eerder gedefinieerde trustpuntdetails om de serverdetails te bepalen waaraan de controller het certificaatverzoek doorstuurt. Aangezien de controller wordt gebruikt als een gevolmachtigde voor de inschrijving van certificaten, moet hij op de hoogte zijn van de parameters die in het certificaatverzoek zijn opgenomen. De configuratie wordt uitgevoerd via de webinterface of de opdrachtregel.

Stap 1. Navigeer naar Configuration > Wireless > Access Point en vergroot het LSC-menu.

Stap 2. Vul de **parameters** voor **de** onderwerpregel **op** met de eigenschappen die in de APcertificaatverzoeken zijn ingevuld, en selecteer vervolgens **Toepassen**.

Subject Name Parameters

MX
CDMX
Juarez
Cisco TAC
Wireless TAC
jesuherr@cisco.com

CLI-configuratie voor stap 1 en 2:

9800-L(config)#ap lsc-provision subject-name-parameter country

Opmerking: Onderwerp-naam-parameters beperkt tot 2 tekens zoals landencode moeten strikt in acht worden genomen, aangezien de WLC van 9800 deze eigenschappen niet valideert.

Zie voor meer informatie het defect <u>CSCvo72999</u> als referentie.

Stap 3. Selecteer in hetzelfde menu het eerder gedefinieerde trustpunt uit de vervolgkeuzelijst. Specificeer een aantal toetredingspogingen (dit definieert het aantal toetredingspogingen voordat de MIC opnieuw wordt gebruikt) en stel de grootte van de certificaattoets in. Klik vervolgens op **Toepassen**.

Status	Disabled •	Su	ubject Name		🖺 Apply
Trustpoint Name	AP-LSC x v		and motor o		
		Co	puntry	MX	
Number of Join Attempts	10	Cho.	ata (CDAIN	
Key Size	2048 •	50	316	CDMA	
		City	ly .	Juarez	
Add APs to LSC Provision List		Org	ganisation	Cisco TAC	

CLI-configuratie voor stap drie:

9800-L(config)#ap lsc-provision join-attempt

9800-L(config)#ap lsc-provision trustpoint

9800-L(config)#ap lsc-provision key-size

Stap 4. (Optioneel) AP LSC-voorziening kan worden geactiveerd voor alle AP's die zijn aangesloten op de controller of op specifieke AP's die zijn gedefinieerd in een mac-adreslijst. Voer in hetzelfde menu het AP Ethernet hoofdadres in formaat xxxx.xxxx in het tekstveld en klik op het + teken. U kunt ook een CSV-bestand uploaden dat de AP-hoofdadressen bevat, het bestand selecteren en vervolgens **Upload File** selecteren.

Opmerking: De controller slaat een hoofdadres in het CSV-bestand over dat het niet herkent uit de aangesloten AP-lijst.

Add APs to LSC Provision List

	Select File Select CSV File Cupload File	
AP MAC Address	Q Enter MAC/Sear	+
ADe in Drevision List :	1	
APS IN Provision List :	1	
APS IN Provision List :	286f.7fcf.53ac	Û
APS IN Provision List :	286f.7fcf.53ac	Û

CLI-configuratie voor stap vier:

Stap 5. Selecteer Ingeschakeld of Voorziening Lijst in het uitrolmenu naast het Status-label en klik vervolgens op Toepassen op Bijvoegen AP LSC invoeren.

Opmerking: APs beginnen certificaataanvraag, download, en installatie. Nadat het certificaat volledig is geïnstalleerd, start AP opnieuw en start het proces met het nieuwe certificaat.

Tip: Indien AP LSC-voorzieningen worden getroffen via een preproductiecontroller en de provisioninglijst wordt gebruikt, verwijdert u de AP-vermeldingen niet zodra het certificaat is voorzien. Als dit gebeurt en de AP's terugvallen op MIC en zich aansluiten bij dezelfde preproductie controller, worden hun LSC-certificaten gewist.

~	LSC Provision			
s	Status	Enabled	•	Subject Name
_		-		Parameters

CLI-configuratie voor stap vijf:

9800-L(config)#ap lsc-provision

In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration. In WLANCC mode APs will be provisioning with EC certificates with a 384 bit key by-default or 256 bit key if configured.

Are you sure you want to continue? (y/n): y If specific AP list provisioning is preferred then use: 9800-L(config)#ap lsc-provision provision-list

Stap 6 . Navigeer naar Configuration > Interface > Wireless en selecteer de beheerinterface.
Selecteer in het veld Trustpoint het nieuwe trustpunt in het vervolgkeuzemenu en klik op Uploaden & toepassen op apparaat.

Voorzichtig: Als LSC is ingeschakeld maar het vertrouwde punt van 9800 WLC verwijst naar het MIC of een SSC, dan proberen de AP's zich bij de LSC aan te sluiten voor het geconfigureerde aantal samengevoegde pogingen. Zodra de maximale pooglimiet is bereikt, vallen de AP's terug naar MIC en sluiten zich opnieuw aan, maar aangezien de LSC voorziening in staat is, vragen de AP's om een nieuwe LSC. Dit leidt tot een lus waar de CA server certificaten constant voor de zelfde APs en APs vast in een aansluit-verzoek-herstart lijn tekent.

Opmerking: Zodra het beheertrustpoint is bijgewerkt om het LSC-certificaat te gebruiken, kunnen nieuwe AP's niet met de MIC worden aangesloten bij de controller. Op dit moment is er geen steun voor het openen van een provisioningvenster. Als u nieuwe APs moet installeren, moeten zij eerder van een LSC voorzien zijn door de zelfde CA ondertekend die in het beheer trustpoint.

Edit Management Interface		×
Interface	Vlan2622 🔻	
Trustpoint	AP-LSC X V	
NAT Status	DISABLED	
Cancel		Update & Apply to Device

CLI-configuratie voor stap zes:

9800-L(config)#wireless management trustpoint

Verifiëren

Controleer de installatie van het controleleidingscertificaat

Om te verifiëren dat de LSC-informatie aanwezig is in het 9800 WLC-trustpoint, wordt de opdracht **show crypto pki-certificaten met de naam <trustpoint>**gekoppeld aan twee certificaten die voor LSC-provisioning en -inschrijving zijn gemaakt. In dit voorbeeld is de naam van het trustpunt

"microsoft-ca" (er wordt alleen relevante uitvoer weergegeven):

```
9800-L#show crypto pki certificates verbose microsoft-ca
Certificate
 Status: Available
 Version: 3
 Certificate Usage: General Purpose
 Issuer:
   cn=CHUU-WIN12-CA
   dc=chuu-domain
   dc=local
 Subject:
   Name: 9800-L.alzavala.local
   cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
   o=Wireless TAC
   l=Juarez
   st=CDMX
    c=MX
   hostname=9800-L.alzavala.local
 CRL Distribution Points:
   ldap:///CN=CHUU-WIN12-CA,CN=Chuu-
Win12, CN=CDP, CN=Public%20Key%20Services, CN=Services, CN=Coint
Validity Date:
start date: 04:25:59 Central May 11 2020
end date: 04:25:59 Central May 11 2022 Subject Key Info: Public Key Algorithm: rsaEncryption RSA
Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption [...] Authority Info
Access: CA ISSUERS: ldap:///CN=CHUU-WIN12-
CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=chuu-
domain, DC=local?cACertificate?base?objectClass=certificationAuthority [...] CA Certificate
 Status: Available
 Version: 3
 Certificate Serial Number (hex): 37268ED56080CB974EF3806CCACC77EC
 Certificate Usage: Signature
 Issuer:
   cn=CHUU-WIN12-CA
   dc=chuu-domain
   dc=local
 Subject:
   cn=CHUU-WIN12-CA
   dc=chuu-domain
   dc=local
Validity Date:
start date: 05:58:01 Central May 10 2019
end date: 06:08:01 Central May 10 2024 Subject Key Info: Public Key Algorithm: rsaEncryption RSA
Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption
```

Controleer de 9800 WLC LSC-configuratie

Om de gegevens over het draadloze beheertrustpoint te verifiëren, voer de opdracht **Show Wireless Management trustpoint uit**, en zorg ervoor dat het juiste. (de opdracht die de LSC details bevat, AP-LSC in dit voorbeeld) in gebruik is en als Beschikbaar is gemarkeerd:

```
9800-L#show wireless management trustpoint
```

```
TrustpointName : AP-LSCCertificateInfo : AvailableCertificateType : LSCCertificateHash : 9e5623adba5307facf778e6ea2f5082877ea4bebPrivate keyInfo : Available
```

Om de details over de AP LSC leveringsconfiguratie te verifiëren, samen met de lijst van APs die

aan de leveringslijst worden toegevoegd, voer de **samenvatting van de show ap LSC** opdracht uit. Zorg ervoor dat de juiste voedingstoestand is aangegeven:

```
9800-L#show ap lsc-provision summary
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : AP-LSC
LSC Revert Count in AP reboots : 10
AP LSC Parameters :
Country : MX
State : CDMX
City : Juarez
Orgn : Cisco TAC
Dept : Wireless TAC
Email : josuvill@cisco.com
Key Size : 2048
EC Key Size : 384 bit
AP LSC-provision List :
Total number of APs in provision list: 2
Mac Addresses :
 _____
XXXX.XXXX.XXXX
xxxx.xxxx.xxxx
```

Controleer de installatie van een access point

Om de certificaten te verifiëren die in AP geïnstalleerd zijn de **show crypto** opdracht van de AP CLI uitvoeren, zorg ervoor dat zowel het CA Root certificaat als het Apparaatcertificaat aanwezig zijn (de output toont slechts relevante gegevens):

```
AP3802#show crypto
[...]
----- LSC: Enabled
----- Device Certificate -----
Certificate:
  Data:
      Version: 3 (0x2)
      Serial Number:
         73:00:00:00:0b:9e:c4:2e:6c:e1:54:84:96:00:00:00:00:00:0b
   Signature Algorithm: sha256WithRSAEncryption
      Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
      Validity
         Not Before: May 13 01:22:13 2020 GMT
         Not After : May 13 01:22:13 2022 GMT
      Subject: C=MX, ST=CDMX, L=Juarez, O=Cisco TAC, CN=ap3g3-
286F7FCF53AC/emailAddress=josuvill@cisco.com
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
----- Root Certificate -----
Certificate:
  Data:
      Version: 3 (0x2)
      Serial Number:
         32:61:fb:93:a8:0a:4a:97:42:5b:5e:32:28:29:0d:32
```

```
Signature Algorithm: sha256WithRSAEncryption
Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
Validity
Not Before: May 10 05:58:01 2019 GMT
Not After : May 10 05:58:01 2024 GMT
Subject: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
```

Als LSC voor de configuratie van de switchpoort dot1x-verificatie wordt gebruikt, kunt u vanuit AP controleren of de poortverificatie is ingeschakeld.

```
AP3802#show ap authentication status
AP dot1x feature is disabled.
```

Opmerking: Om port dot1x voor APs toe te laten, is het nodig om de punt1x geloofsbrieven voor APs in of het AP profiel of de AP configuratie zelf met dummy waarden te definiëren.

Problemen oplossen

Gemeenschappelijke kwesties

- Als de sjablonen niet correct in kaart zijn gebracht in het serverregister of als de server een wachtwoorduitdaging nodig heeft, wordt de certificaataanvraag voor de 9800 WLC of de AP's afgewezen.
- Als de standaardinstellingen van IS worden uitgeschakeld, wordt de SCEP-service ook uitgeschakeld. Daarom is de URL die in het betrouwbaar punt is gedefinieerd niet bereikbaar en stuurt de 9800 WLC geen certificaataanvraag.
- 3. Als de tijd niet gesynchroniseerd is tussen de server en de 9800 WLC, zijn er geen certificaten geïnstalleerd sinds de controle van de geldigheid faalt.

Opdrachten voor debug en inloggen

Gebruik deze opdrachten om de 9800-controller-inschrijving in te voeren:

```
9800-L#debug crypto pki transactions
9800-L#debug crypto pki validation
9800-L#debug crypto pki scep
Om een oplossing te vinden en AP inschrijving te controleren gebruikt deze opdrachten:
```

AP3802#debug capwap client payload AP3802#debug capwap client events Vanuit de AP-opdrachtregel **toont** de **vastlegging** aan of het AP problemen had met de installatie van het certificaat en geeft het details over de reden waarom het certificaat niet is geïnstalleerd: Generating a RSA private key Mar 19 19:39:14 kernel: *03/19/2020 19:39:13.5989] Mar 19 19:39:15 kernel: *03/19/2020 19:39:14.4179] .. Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.2952] writing new private key to '/tmp/lsc/priv_key' Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.2955] ----- Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] cen_validate_lsc: Verification failed for certificate: Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] countryName = MX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] stateOrProvinceName = CDMX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] localityName = Juarez Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] organizationName = cisco-tac Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] commonName = ap3g3- Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] emailAddress = jesuherr@cisco.com Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5427] LSC certificates/key failed validation! Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5427]

Voorbeeld van een succesvolle inschrijving

Dit is de output van de debugs die eerder is vermeld voor een succesvolle inschrijving voor zowel de controller als de bijbehorende AP's.

CA-basiscertificaat invoer naar 9800 WLC:

[...]

Certificate has the following attributes: Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224 Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B % Do you accept this certificate? [yes/no]: yes CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:47:34 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and RA certificate CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_extract_ca_cert found cert CRYPTO_PKI: Bypassing SCEP capabilities request 0 CRYPTO_PKI: transaction CRYPTO_REQ_CA_CERT completed CRYPTO_PKI: CA certificate received. CRYPTO_PKI: CA certificate received. CRYPTO_PKI:

crypto_pki_get_cert_record_by_cert() CRYPTO_PKI: crypto_pki_authenticate_tp_cert() CRYPTO_PKI: trustpoint AP-LSC authentication status = 0 Trustpoint CA certificate accepted.

9800 WLC-apparaatinschrijving:

[...]

CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA Certificate Request: GET

/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and RA certificate CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs

CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI_SCEP: Client Sending GetCACaps request with msg = GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACaps&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 171 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (34) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: text/plain Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 34 CRYPTO_PKI: HTTP header content length is 34 bytes CRYPTO_PKI_SCEP: Server returned capabilities: 92 CA_CAP_RENEWAL CA_CAP_S alz_9800(config)#HA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: %PKI-6-CSR_FINGERPRINT: CSR Fingerprint MD5 : 9BFBA438303487562E888087168F05D4 CSR Fingerprint SHA1: 58DC7DB84C632A7307631A97A6ABCF65A3DEFEEF CRYPTO_PKI: Certificate Request Fingerprint MD5: 9BFBA438 30348756 2E888087 168F05D4 CRYPTO_PKI: Certificate Request Fingerprint SHA1: 58DC7DB8 4C632A73 07631A97 A6ABCF65 A3DEFEEF PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 CO 52 CO 0F 0E 00 00 00 00 38 CRYPTO PKI: Deleting cached key having key id 65 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI: Peer's public inserted successfully with key id 66 CRYPTO_PKI: Expiring peer's cached key with key id 66 PKI: Trustpoint AP-LSC has no router cert PKI: Signing pkcs7 with AP-LSC trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2807) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: received msg of 2995 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pkimessage Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 2807 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 66 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 67 CRYPTO_PKI: Expiring peer's cached key with key id 67 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuudomain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO PKI SCEP: Client received CertRep - GRANTED (AF58BA9313638026C5DC151AF474723F) CRYPTO PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Newly-issued Router Cert: issuer=cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial=1800043245DC93E1D943CA70000043 start date: 21:38:34 Central May 19 2020 end date: 21:38:34 Central May 19 2022 Router date: 21:48:35 Central May 19 2020 %PKI-6-CERT_INSTALL: An ID certificate has been installed under Trustpoint : AP-LSC Issuer-name : cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local Subject-name : cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com,o=Wireless TAC,l=Juarez,st=CDMX,c=MX,hostname=alz_9800.alzavala.local Serial-number:

1800000043245DC93E1D943CA700000000043 End-date : 2022-05-19T21:38:34Z Received router cert from CA CRYPTO_PKI: Not adding alz_9800.alzavala.local to subject-alt-name field because : Character allowed in the domain name. Calling pkiSendCertInstallTrap to send alert CRYPTO_PKI: All enrollment requests completed for trustpoint AP-LSC

AP-inschrijving debug uitvoer van controller kant, deze uitvoer wordt meerdere keren herhaald voor elke AP die wordt aangesloten bij de 9800 WLC:

[...]

CRYPTO_PKI: (A6964) Session started - identity selected (AP-LSC) CRYPTO_PKI: Doing re-auth to fetch RA certificate. CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and RA certificate

CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs

CRYPTO PKI:crypto_pkcs7_insert_ra_certs found RA_certs CRYPTO_PKI: Capabilites already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 PKCS10 request is compulsory CRYPTO_PKI: byte 2 in key usage in PKCS#10 is 0x5 May 19 21: alz_9800(config)#51:04.985: CRYPTO_PKI: all usage CRYPTO_PKI: key_usage is 4 CRYPTO_PKI: creating trustpoint clone Proxy-AP-LSC8 CRYPTO_PKI: Creating proxy trustpoint Proxy-AP-LSC8 CRYPTO_PKI: Proxy enrollment request trans id = 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: Proxy forwading an enrollment request CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI: Proxy send CA enrollment request with trans id: 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: No need to re-auth as we have RA in place CRYPTO_PKI: Capabilites already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 OF 0E 00 00 00 00 00 38 CRYPTO PKI: Deleting cached key having key id 67 CRYPTO PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 68 CRYPTO_PKI: Expiring peer's cached key with key id 68 PKI: Trustpoint Proxy-AP-LSC8 has no router cert and loaded PKI: Signing pkcs7 with Proxy-AP-LSC8 trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 3 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2727) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: received msg of 2915 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 2727 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 68 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 69 CRYPTO_PKI: Expiring peer's cached key with key id 69 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 alz_9800(config)# verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuudomain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO PKI SCEP: Client received CertRep - GRANTED (7CBB299A2D9BC77DBB1A8716E6474C0C) CRYPTO_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Received router cert from CA CRYPTO_PKI: Enrollment poroxy callback status: CERT_REQ_GRANTED CRYPTO_PKI: Proxy received router cert from CA CRYPTO_PKI: Rcvd request to end PKI session A6964. CRYPTO_PKI: PKI session A6964 has ended. Freeing all resources. CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Cleaning RA certificate for TP : AP-LSC CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_CS: removing trustpoint clone Proxy-AP-LSC8

AP inschrijving debug uitvoer van AP kant:

[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 40 len 407 ..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600 ...Vendor SubType: CERTIFICATE_PARAMETER_PAYLOAD(63) vendId 409600 LSC set retry number from WLC: 1

Generating a RSA private key
...
writing new private key to '/tmp/lsc/priv_key'
----[ENC] CAPWAP_WTP_EVENT_REQUEST(9)
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) Len 1135 Total 1135
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)

.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8 [DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 41 len 20 ..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600 ...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600 LSC_CERT_ENROLL_PENDING from WLC

[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
Received Capwap watchdog update msg.
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 42 len 1277
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving ROOT_CERT

[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8) .Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8 [DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 43 len 2233 ..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600 ...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600 LSC_ENABLE: saving DEVICE_CERT

SC private key written to hardware TAM

root: 2: LSC enabled AP Rebooting: Reset Reason - LSC enabled Dit sluit het configuratievoorbeeld voor LSC inschrijving door SCEP af.