# Konfigurationsbeispiel für LSC (Locally Significant Certificates) mit WLC und Windows Server 2012

### Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Microsoft Windows Server-Konfiguration Konfigurieren des WLC Überprüfen Fehlerbehebung

## Einführung

In diesem Dokument wird beschrieben, wie Sie Locally Significant Certificates (LSC) mit einem Wireless LAN Controller (WLC) und einem neu installierten Microsoft Windows Server 2012 R2 konfigurieren.

**Hinweis**: Die tatsächlichen Bereitstellungen können sich in vielen Punkten unterscheiden, und Sie sollten über vollständige Kontrolle und Kenntnisse der Einstellungen in Microsoft Windows Server 2012 verfügen. Dieses Konfigurationsbeispiel wird nur als Referenzvorlage für Cisco Kunden bereitgestellt, um ihre Microsoft Windows Server-Konfiguration zu implementieren und anzupassen, damit LSC funktioniert.

### Voraussetzungen

#### Anforderungen

Cisco empfiehlt, dass Sie alle Änderungen in Microsoft Windows Server verstehen und ggf. die entsprechende Microsoft-Dokumentation überprüfen.

**Hinweis**: LSC auf dem WLC wird nicht von einer intermediären CA unterstützt, da die Root-CA vom WLC nicht unterstützt wird, da der Controller nur die mittlere CA empfängt.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- WLC-Version 7.6
- Microsoft Windows Server 2012 R2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Konfigurieren

#### **Microsoft Windows Server-Konfiguration**

Diese Konfiguration wird als mit einem neu installierten Microsoft Windows Server 2012 ausgeführt angezeigt. Sie müssen die Schritte an Ihre Domäne und Ihre Konfiguration anpassen.

Schritt 1: Active Directory-Domänendienste für den Assistenten für Rollen und Funktionen installieren.

efore You Begin	Select one or more roles to install on the elected server.		
nstallation Type	Roles		Description
erver Selection	Active Directory Certificate Services		Active Directory Domain Services
erver Roles	Active Directory Domain Services		(AD DS) stores information about
eatures	Active Directory Federation Services		this information available to users
D DS	Active Directory Lightweight Directory Services		and network administrators. AD D
onfirmation	Active Directory Rights Management Services		network users access to permitted
esults	Application Server	_	resources anywhere on the netwo
	DHCP Server	-	through a single logon process.
	DNS Server		
	Fax Server		
	File and Storage Services (1 of 12 installed)		
	Hyper-V		
	Network Policy and Access Services		
	Print and Document Services		
	Remote Access		
	Remote Desktop Services		

Schritt 2. Nach der Installation müssen Sie den Server für den Domänen-Controller bewerben.

<b>a</b>	Add Roles and Features Wizard	- 0 ×
Installation progr	ess	DESTINATION SERVER WIN-ODEF7N1GRUB
Before You Begin	View installation progress	
Installation Type	Feature installation	
Server Selection Server Roles	Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.	
Features	Active Directory Domain Services	^
Confirmation	Promote this server to a domain controller	
Results	Group Policy Management Remote Server Administration Tools	
	Role Administration Tools	=
	Active Directory module for Windows PowerShell	
	AD DS Tools Active Directory Administrative Center	
	AD DS Snap-Ins and Command-Line Tools	~
	You can close this wizard without interrupting running tasks. View task propage again by clicking Notifications in the command bar, and then Task D Export configuration settings	ogress or open this Details.
	< Previous Next > Cl	Cancel

**Schritt 3:** Da es sich um eine neue Konfiguration handelt, konfigurieren Sie einen neuen Wald. konfigurieren Sie diese Punkte jedoch in der Regel in vorhandenen Bereitstellungen einfach auf einem Domänencontroller. Wählen Sie hier die Domäne **LSC2012.com** aus. Dadurch wird auch die Funktion Domain Name Server (DNS) aktiviert.

Schritt 4: Installieren Sie nach einem Neustart den Service Certificate Authority (CA) sowie die Webregistrierung.



Schritt 5. Konfigurieren Sie sie.

<b>a</b>	Add Roles and Features Wizard	- X
Installation progre	DESTINATION : SS WIN-ODEF7N1GRUB.LSC20	SERVER 12.com
Before You Begin	View installation progress	
Installation Type	Feature installation	
Server Selection		
Server Roles	Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.LSC2012.com.	
Features	Active Directory Certificate Services	^
AD CS	Additional steps are required to configure Active Directory Certificate Services on the	
Role Services	destination server	=
Web Server Role (IIS)	Certification Authority	
Role Services	Certification Authority Web Enrollment	
Confirmation	Remote Server Administration Tools	
Results	Role Administration Tools	
	Active Directory Certificate Services Tools	
	Web Server (IIS)	Y
	You can close this wizard without interrupting running tasks. View task progress or open page again by clicking Notifications in the command bar, and then Task Details.	this
	Export configuration settings	
	< Previous Next > Close Ca	ncel

Schritt 6: Wählen Sie Enterprise CA aus, und belassen Sie alle Standardeinstellungen.

<b>b</b>	AD CS Configuration	
Role Services		DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com
Image: Second	Select Role Services to configure  Certification Authority  Certification Authority Web Enrollment  Online Responder  Network Device Enrollment Service  Certificate Enrollment Web Service  Certificate Enrollment Policy Web Service	]
Results	More about AD CS Server Roles	> Configure Cancel

Schritt 7: Klicken Sie auf das Menü Microsoft Windows/Start.

Schritt 8: Klicken Sie auf Verwaltung.

Schritt 9: Klicken Sie auf Active Directory-Benutzer und -Computer.

Schritt 10: Erweitern Sie die Domäne, klicken Sie mit der rechten Maustaste auf den Ordner Benutzer, und wählen Sie Neues Objekt > Benutzer aus.

	New Object - User	_ <b>D</b> X
File Action View Help ← ➡ 2 1 4 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 ×	Create in: LSC2012.com/Users	
<ul> <li>▷ Saved Queries</li> <li>▲ ∰ LSC2012.com</li> <li>▷ 🛗 Builtin</li> <li>▷ 🔂 Computers</li> <li>▷ ☑ Domain Controllers</li> </ul>	Erst name: AP Intials:	
<ul> <li>ForeignSecurityPrincipa</li> <li>Managed Service Accou</li> <li>Users</li> </ul>	User logon name: APUSER @LSC2012.com ✓ User logon name (pre- <u>W</u> indows 2000): LSC2012\ APUSER	
	<u>Subset</u> User Built-in account for gue          Security Group       Members of this group	
< III >	KAS and IAS       Security Group       Servers in this group can         Read-only D       Security Group       Members of this group         Schema Ad       Security Group       Designated administrato         WinRMRem       Security Group       Members of this group	

Schritt 11: In diesem Beispiel wird es APUSER genannt. Nach der Erstellung müssen Sie den Benutzer bearbeiten und auf die Registerkarte MemberOf klicken, um ihn zur Gruppe IIS\_IUSRS zu machen.

Die erforderlichen Zuweisungen für Benutzerrechte sind:

- Lokale Anmeldung zulassen
- Melden Sie sich als Service an.

Schritt 12: Installieren Sie den Network Device Enrollment Service (NDES).

<b>b</b>	AD CS Configuration	_ <b>_</b> X
Role Services		DESTINATION SERVER WIN-ODEF7N1GRUB.wlaaan2012.com
Credentials Role Services Service Account for NDES RA Information Cryptography for NDES Confirmation Progress Results	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Policy Web Service Certificate Enrollment Policy Web Service	
	< <u>P</u> revious <u>N</u> e	xt > Configure Cancel

• Wählen Sie den Kontomember der Gruppe IIS\_USRS, **APUSER** in diesem Beispiel, als Dienstkonto für NDES aus.

Schritt 13: Navigieren Sie zu Verwaltung.

Schritt 14: Klicken Sie auf Internetinformationsdienste (IIS).

Schritt 15: Erweitern Sie Server > Sites > Default website > Cert Srv.

Schritt 16: Klicken Sie für mscep und mscep\_admin auf Authentifizierung. Stellen Sie sicher, dass die anonyme Authentifizierung aktiviert ist.

Schritt 17: Klicken Sie mit der rechten Maustaste auf Windows-Authentifizierung, und wählen Sie Provider (Anbieter) aus. Stellen Sie sicher, dass NT LAN Manager (NTLM) der erste in der Liste ist.

Andernfalls erwartet Simple Certificate Enrollment Protocol (SCEP) eine Kennwortauthentifizierung, die vom WLC nicht unterstützt wird.

Schritt 19: Öffnen Sie die Anwendung regedit.

Schritt 20: Besuchen Sie

HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

Schritt 21: Legen Sie EnforcePassword auf 0 fest.

ġ	Re	egistry Editor		
File Edit View Favorites Help				
Advanced INF	A Name	Туре	Data	
👂 - 🚹 ALG	ab (Default)	REG_SZ	(value not set)	
🕌 AllUserInstallA	<b>職 EnforcePassword</b>	REG_DWORD	0x00000000 (0)	
👂 归 Assistance				
👂 - 퉲 AuthHost	=			
b - BestPractices				
👂 - 퉲 BidInterface				
þ- 뷆 Chkdsk				
þ-퉲 СОМЗ				
Command Pro		N		
⊿ U Cryptography		43		
Þ - 🏭 AutoEnroll				
Þ- 🏭 Calais				
CatalogDB				
Catyp				
	~			
<				
Computer\HKEY_LOCAL_MACHINE\S	OFTWARE\Microsoft\Cryp	tography\MSCEP\En	forcePassword	Activate Wind

Schritt 22: Klicken Sie auf das Menü Microsoft Windows/Start.

Schritt 23: Geben Sie MMC ein.

Schritt 24: Wählen Sie im Menü Datei die Option Snap-In hinzufügen/entfernen. Wählen Sie Zertifizierungsstelle aus.

Schritt 25: Klicken Sie mit der rechten Maustaste auf den Ordner Zertifikatvorlage und anschließend auf Verwalten.

Schritt 26: Klicken Sie mit der rechten Maustaste auf eine vorhandene Vorlage, z. B. Benutzer, und wählen Sie Vorlage duplizieren aus.

File Action View Help				
🔄 🛐 🔚 🗐 🕞				
Certificate Templates (WIN-ODE	Template Display Name	Schema Version	Versi	Intended Purp
	CA Exchange	2	106.0	Private Key Arc
	CEP Encryption	1	4.1	
	🗟 Code Signing	1	3.1	_
	Computer	1	5.1	
	Cross Certification Authority	2	105.0	
	Directory Email Replication	2	115.0	Directory Servi
	Domain Controller	1	4.1	
	Domain Controller Authentication	2	110.0	Client Authent
	EFS Recovery Agent	1	6.1	
	🗷 Enrollment Agent	1	4.1	
	Enrollment Agent (Computer)	1	5.1	
	Exchange Enrollment Agent (Offline requ	1	4.1	
	Exchange Signature Only	1	6.1	
	Exchange User	1	7.1	
	IPSec	1	8.1	
	IPSec (Offline request)	1	7.1	_
	Kerberos Authentication	2	110.0	Client Authent
	Key Recovery Agent	2	105.0	Key Recovery A
	OCSP Response Signing	3	101.0	OCSP Signing
	RAS and IAS Server	2	101.0	Client Authent
	Root Certification Authority	1	5.1	
	Router (Offline request)	1	4.1	
	Smartcard Logon	1	6.1	
	Smartcard User	1	11.1	
	Subordinate Certification Authority	1	5.1	
	Trust List Signing	1	3.1	
	🖳 User	1	3.1	
	🖳 User Signative Only	1	4.1	
	P Web Server	1	4.1	Activat
	Workstation Authentication	2	101.0	Client Authent

Schritt 27: Wählen Sie die CA als Microsoft Windows 2012 R2 aus.

**Schritt 28:** Fügen Sie auf der Registerkarte Allgemein einen Anzeigenamen wie WLC und eine Gültigkeitsdauer hinzu.

Schritt 29: Vergewissern Sie sich auf der Registerkarte Betreffname, dass die Option Angebot in der Anfrage ausgewählt ist.

Properties of New Template								
Superseded Templates Extensions Security								
Compatibility General	Request	Handling	Cryptograph	y Key Attesta	tion			
Subject Name	Sen	ver	Issuance	Requirements				
Supply in the request								
renewal requests	mation no ;	in existing	Certificates 10	autoenioiimen				
○ <u>B</u> uild from this Active	Directory	informatio	n					
Select this option to e	nforce co	nsistency	among subjec	t names and to				
simpliny certificate add	ninistration	1.						
Subject name format:								
None				×				
Include e-mail nan	ne in subje	ect name						
Include this informatio	n in alterr	nate subie	ct name:					
E-mail name		-						
DNS name								
User principal nam	ne (UPN)							
Service principal r	name (SPI	an a		Ν				
	10110	-/		6				
					- 1			
OK		ancel	Apply	Hele				
		Jancer		nep				

**Schritt 30:** Klicken Sie auf die Registerkarte **Issuance Requirements**. Cisco empfiehlt, Ausgaberichtlinien in einer typischen hierarchischen CA-Umgebung leer zu lassen:

Supersec	ded Templa	ites	Exte	ensions	Security					
Compatibility	General	Request	Handling	Cryptography Key Attesta						
Subject Name Server Issuance Requireme										
Require the following for enrollment:										
I <u>n</u> is num	ber of auth	onzed sigr	natures:	0						
lf you re	quire more	than one :	signature, a	autoenrollment	is not allowed.					
Policy ty	pe required	l in signatu	ire:							
					~					
Applicati	on policy:									
					~					
l <u>s</u> suance	e policies:									
					A <u>d</u> d					
					<u>R</u> emove					
Require the f	following fo	r reenrollm	ient:							
Same crit	eria as for (	enrollment								
⊖ Valid <u>e</u> xis	ting certific	ate								
Allow	key based	renewal								
Requires subject information to be provided within the certificate request.										
Г	014		<b>C</b> 1							
	OK	(	Jancel	Арріу	нер					

Schritt 31: Klicken Sie auf die Registerkarte Erweiterungen, Anwendungsrichtlinien und dann auf Bearbeiten. Klicken Sie auf Hinzufügen, und stellen Sie sicher, dass die Client-Authentifizierung als Anwendungsrichtlinie hinzugefügt wird. Klicken Sie auf OK.

An application policy defines how a certificate can be used.
Application policies: Client Authentication Encrypting File System Secure Email
Add       Edit       Remove         Make this extension critical
OK Cancel

Schritt 32: Klicken Sie auf die Registerkarte Sicherheit und dann auf Hinzufügen..... Stellen Sie sicher, dass das in der NDES-Dienstinstallation definierte SCEP-Dienstkonto über die vollständige Kontrolle über die Vorlage verfügt, und klicken Sie auf OK.

Subject N	lame	Sen	Server Issuance Requiremen		Issuance Requirements	
Compatibility	General	Request	Handling	Cryptography Key Attesta		y Attestation
Supersec	led Templa	tes	Ext	ensions	Security	
<u>G</u> roup or use	rnames:					
& Autheni	ticated Use	rs				
🔏 Adminis	trator					
👗 AP USI	ER (APUSE	R@LSC2	012.com)			
👫 Domain	Admins (L	SC2012\D	)omain Ad	mins)		
👫 Domain	Users (LS	C2012\Do	main User	rs)		
👫 Enterpri	se Admins	(LSC2012	\Enterpris	e Admins)		
				l	à	
			1	A <u>d</u> d	B	emove

Schritt 33: Kehren Sie zur GUI-Schnittstelle der Zertifizierungsstelle zurück. Klicken Sie mit der rechten Maustaste auf das Verzeichnis Zertifikatvorlagen. Navigieren Sie zu Neu > Zu erteilende Zertifikatsvorlage. Wählen Sie die zuvor konfigurierte WLC-Vorlage aus, und klicken Sie auf OK.

		risk.		-1-
Þ 🔿 🖄				
sole Root		Enable Certificate Templates	×	
Certification A Waaan201 Revoke Issued Pendir	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>Cer</u>	enable on this Certification Authority. was recently created does not appear on this list, you may new s been replicated to all domain controllers. ne organization may not be available to your CA. tificate Template Concepts.	ed to wait until	Tem tions
Eailed	Name Rey Recovery Agent OCSP Response Signing RAS and IAS Server Router (Offline request) Smartcard Logon Smartcard User Trust List Signing User Signature Only WIC	Intended Purpose Key Recovery Agent OCSP Signing Client Authentication, Server Authentication Client Authentication, Server Authentication Client Authentication, Smart Card Logon Secure Email, Client Authentication, Smart Card Logon Microsoft Trust List Signing Secure Email, Client Authentication		
	Workstation Authentication	Client Authentication	✓ Cancel	
<			>	

Schritt 34: Ändern Sie die Standard-SCEP-Vorlage in den Registrierungseinstellungen unter Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP. Ändern Sie die Schlüssel für EncryptionTemplate, GeneralPurposeTemplate und SignatureTemplate von IPsec (Offline Request) in die zuvor erstellte WLC-Vorlage.

đ					Re	gistry Edi	tor	_ <b>_</b> ×
<u>F</u> ile	<u>E</u> dit	View	Favorites	lelp				
		Þ- (	🔓 Advanced	INF 🔨	Name	Туре	Data	
		Þ - [	ALG		赵 (Default)	REG_SZ	(value not set)	
			AllUserInst	allA	EncryptionTem	REG_SZ	WLC	
		Þ-	Assistance		💩 GeneralPurpose	REG_SZ	WLC	
		Þ-	AuthHost	≡	a Signature Template	REG_SZ	WLC	
		Þ-	BestPractio	es	1			
		Þ-	BidInterfac	e				
		Þ-	Chkdsk					
		▶ -	COM3					
			Command	Pro				
		4-	Cryptogra	ony				
			Calair	roll				
			Catalo	DB				
			CatDR	em				
			Certific	atel				
			b -	s				
			CA	Гурс				
			🚺 Cer	tsin				
			🚺 Enf	orce				
			🚺 Pas	swo				
			🚺 Use	Sing				
<				>				
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP								Activate Wind

Schritt 35: Starten Sie das System neu.

#### Konfigurieren des WLC

Schritt 1: Navigieren Sie im WLC zum Menü Security (Sicherheit). Klicken Sie auf Certificates > LSC.

Schritt 2: Aktivieren Sie das Kontrollkästchen LSC auf Controller aktivieren.

Schritt 3: Geben Sie Ihre Microsoft Windows Server 2012-URL ein. Standardmäßig wird sie an /certsrv/mscep/mscep.dll angehängt.

Schritt 4: Geben Sie Ihre Daten im Bereich Params ein.

Schritt 5: Wenden Sie die Änderung an.

Local Significant Certificates (LSC)

General AP Provisioning					
Certificate Type	Status	^			
CA	Present 🔽				
General					
Enable LSC on Controller					
CA Server					
CA server URL	http://10.48.39.197/certsrv/mscep/mscep.dll (Ex: http://10.0.0.1:8080/caserver)				
Params					
Country Code	BE				
State	Belgium				
City	Brussel				
Organization	Cisco				
Department	R&D				
E-mail	rmanchur@wlaaan.com				
Key Size	2048				

Apply

Schritt 6. Klicken Sie auf den blauen Pfeil in der oberen CA-Zeile, und wählen Sie Hinzufügen aus. Sie sollte den Status von Nicht vorhanden in Gegenwart ändern.

Schritt 7: Klicken Sie auf die Registerkarte AP-Bereitstellung.

Schritt 8. Aktivieren Sie das Kontrollkästchen Aktivieren unter AP-Bereitstellung, und klicken Sie auf Aktualisieren.

Schritt 9. Starten Sie die Access Points neu, wenn sie nicht selbst neu gestartet wurden.

# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Der Access Point schließt sich nach dem Neustart wieder an und wird im Menü Wireless mit LSC als Zertifikatstyp angezeigt.

CISCO	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нер	EEEDBACK						
Wireless	All APs										Entries 3	- 2 of 2	~
Access Points     Al: APs     Red cs     S02.11a/n     S02.11b/g/n     Dual-Band Radios	Current Filter Number of APs	None 2		Change Filt	er) (Clear Filter)								
Global Configuration	AP Name	AP Nodel		AP NAC	AP Up Tir	ne	Admin Status	Operational Status	Port	AP Node		Certificate	1
Hesh RF Profiles	CAP15011-1 LAP1142-1	AIR-CAP15011-0-4 AIR-LAP1142N-1-4	(9 (9	c0:9c:1d:6e:a3:cd ac:12:c5:73:33:ce	0 d, 00 h i 0 d, 00 h i	35 m 21 s 02 m 35 s	Disabled Enabled	ROG ROG	1	Local Local		LSC LSC	
FlexConnect Groups FlexConnect ACLs 502.11a/n													
▶ 802.11b/g/n													
<ul> <li>Media Stream</li> <li>Application Visibility</li> </ul>													
And Control													Ш
Country													Ш
Timers • Netflow													Ш
▶ Qo5													Ш
	< .											>	
	2 📋	× 📖 🚺	2	📮 💰	3				Re 1	a (6	ENG UK 1	6:41 PM	

**Hinweis**: Nach 8.3.112 können MIC-APs nicht mehr beitreten, wenn LSC aktiviert ist. Daher wird die Funktion "versucht, LSC-Zähler zu erfassen" nur in begrenztem Umfang genutzt.

### Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.