Esempio di certificati LSC (Locally Significant Certificates) con WLC e configurazione di Windows Server 2012

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Configurazione server di Microsoft Windows Configurare il WLC Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare i certificati LSC (Locally Significant Certificates) con un controller WLC (Wireless LAN Controller) e un nuovo Microsoft Windows Server 2012 R2 installato.

Nota: Le distribuzioni reali possono presentare differenze in molti punti e occorre avere il controllo completo e la conoscenza delle impostazioni in Microsoft Windows Server 2012. Questo esempio di configurazione viene fornito solo come modello di riferimento per i clienti Cisco per implementare e adattare la configurazione di Microsoft Windows Server in modo da consentire il funzionamento di LSC.

Prerequisiti

Requisiti

Cisco consiglia di comprendere tutte le modifiche apportate in Microsoft Windows Server e di consultare la documentazione Microsoft pertinente, se necessario.

Nota: LSC su WLC non è supportato con intermediate-CA, in quanto la CA radice non è presente nel WLC poiché il controller ottiene solo la CA intermedia.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- WLC versione 7.6
- Microsoft Windows Server 2012 R2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazione server di Microsoft Windows

Questa configurazione viene visualizzata come eseguita su un nuovo sistema operativo Microsoft Windows Server 2012. È necessario adattare i passaggi al dominio e alla configurazione.

Passaggio 1. Installare Servizi di dominio Active Directory per la procedura guidata relativa a ruoli e funzionalità.

Before You Begin	Select one or more roles to install on the elected server.		
nstallation Type	Roles		Description
Server Selection	Active Directory Cartificate Services		Active Directory Domain Services
Server Roles	Active Directory Certificate Services		(AD DS) stores information about
eatures	Active Directory Education Services		objects on the network and makes this information available to users
D DS	Active Directory Lightweight Directory Services		and network administrators. AD D
onfirmation	Active Directory Rights Management Services		uses domain controllers to give 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		

Passaggio 2. Dopo l'installazione, è necessario innalzare di livello il server a controller di dominio.

b	Add Roles and Features Wizard	X
Installation progr	ress	DESTINATION SERVER WIN-ODEF7N1GRUB
Before You Begin	View installation progress	
Installation Type	Feature installation	
Server Selection	Configuration provided between ended on Wilk ODER7N1C0110	
Server Roles	Configuration required. Installation succeeded on WIN-ODEF/NIGROB.	
Features	Active Directory Domain Services	^
AD DS	Additional steps are required to make this machine a domain controller.	
Confirmation	Promote this server to a domain controller	
Results	Group Policy Management	
	Remote Server Administration Tools	=
	AD DS and AD LDS 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 Netails.
	< <u>P</u> revious <u>N</u> ext > Cl	Cancel

Passaggio 3. Poiché si tratta di una nuova impostazione, è possibile configurare una nuova foresta. ma in genere, nelle implementazioni esistenti, è sufficiente configurare questi punti su un controller di dominio. In questa pagina è possibile scegliere il dominio LSC2012.com. In questo modo viene attivata anche la funzionalità DNS (Domain Name Server).

Passaggio 4. Dopo il riavvio, installare il servizio Autorità di certificazione (CA) e la registrazione Web.



- 1

х

DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com

Select the role services to install for Active Directory Certificate Services Before You Begin Installation Type Description Role services Server Selection Certification Authority Web Certification Authority Enrollment provides a simple Web Server Roles Certificate Enrollment Policy Web Service interface that allows users to Features Certificate Enrollment Web Service perform tasks such as request and renew certificates, retrieve certificate AD CS Certification Authority Web Enrollment revocation lists (CRLs), and enroll for Network Device Enrollment Service **Role Services** smart card certificates. Online Responder Web Server Role (IIS) Role Services Confirmation Results R < Previous Next > Install Cancel

Passaggio 5. Configurarle.

Select role services

à	Add Roles and Features Wizard	
Installation progre	SS DESTINATION WIN-ODEF7N1GRUB.LSC2	SERVER 012.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	Configure Active Directory Certificate Services on the destination server	=
Web Server Role (IIS)	Certification Authority	
Role Services	Certification Authority Web Enrollment	
Confirmation	Remote Server Administration Tools	
Results	Role Administration Tools	
	Certification Authority Management Tools	
	Web Server (IIS)	~
	You can close this wizard without interrupting running tasks. View task progress or oper page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings	this
	< Previous Next > Close C	ancel

Passaggio 6. Scegliere CA organizzazione (Enterprise) e lasciare tutto come valore predefinito.

b	AD CS Configuration	
Role Services		DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com
Image: Image	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	
	More about AD CS Server Roles	
	< Previous Next	> Configure Cancel

Passaggio 7. Fare clic sul menu Start di Microsoft Windows.

Passaggio 8. Fare clic su Strumenti di amministrazione.

Passaggio 9. Fare clic su Utenti e computer di Active Directory.

Passaggio 10. Espandere il dominio, fare clic con il pulsante destro del mouse sulla **cartella Utenti**, quindi scegliere **Nuovo oggetto > Utente**.

	New Object - User	X
File Action View Help Image: Second S	Create in: LSC2012.com/Users	
 ▷ Saved Queries ▲ Builtin ▷ Computers ▷ Domain Controllers 	Erst name: AP Initials:	
 ForeignSecurityPrincipa Managed Service Accound Content Users 	User logon name: APUSER @LSC2012.com ✓ User logon name (pre- <u>W</u> indows 2000): LSC2012\ APUSER	
	< Back Next > Cancel Image: Security Group Built-in account for gue Members of this group Image: Security Group Members of this group Security Group Image: Security Group Security Group Security Group	
< III >	Image: Security Dimensional Content of the security Group Members of this group Image: Security Group Designated administrato Image: Security Group Members of this group Image: Security Group Members of this group	

Passaggio 11. In questo esempio, il nome è **APUSER**. Una volta creato, è necessario modificare l'utente, fare clic sulla **scheda MemberOf** e impostarlo come membro del gruppo IIS_IUSRS

Le assegnazioni dei diritti utente richieste sono:

- Consenti accesso locale
- Accedi come servizio

Passaggio 12. Installare il servizio Registrazione dispositivi di rete (NDES).

b	AD CS Configuration	_ _ 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 Conline Responder Certificate Enrollment Veb Service Certificate Enrollment Policy Web Service	
	< <u>P</u> revious <u>N</u> e	ext > Configure Cancel

 Scegliere il membro account del gruppo IIS_USRS, APUSER in questo esempio, come account del servizio per NDES.

Passaggio 13. Passare a Strumenti di amministrazione.

Passaggio 14. Fare clic su Internet Information Services (IIS).

Passaggio 15. Espandere Server > Siti > Sito Web predefinito > Srv certificato.

Passaggio 16. Per **mscep** e **mscep_admin**, fare clic su **autenticazione**. Verificare che l'autenticazione anonima sia abilitata.

Passaggio 17. Fare clic con il pulsante destro del mouse su **autenticazione di Windows** e scegliere **Provider**. Assicurarsi che NT LAN Manager (NTLM) sia il primo nell'elenco.

Passaggio 18. Disabilitare la richiesta di verifica dell'autenticazione nelle impostazioni del Registro di sistema. In caso contrario, SCEP (Simple Certificate Enrollment Protocol) prevede

l'autenticazione della richiesta di verifica della password, che non è supportata dal WLC.

Passaggio 19. Aprire l'applicazione regedit.

Passaggio 20. Andare su HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

Passaggio 21. Impostare EnforcePassword su 0.

đ			Re	gistry Editor		
File	Edit	View Favorites Help				
		👂 🌗 Advanced INF 🔺	Name	Туре	Data	
		Þ- 🁪 ALG	ab) (Default)	REG_SZ	(value not set)	
		🔒 AllUserinstallA	EnforcePassword	REG_DWORD	0x00000000 (0)	
		👂 🍌 Assistance 🦳				
		⊳- 🎍 AuthHost 🛛 😑				
		BestPractices				
		👂 퉬 BidInterface 🦳				
		þ- 🍌 Chkdsk				
		р - 🍌 СОМЗ				
		Command Prc		•		
		4 🎳 Cryptography		13		
		AutoEnroll				
		D - 🎽 Calais				
		CatalogDB				
		CatDBTem				
		Defaults				
		Catype				
		- Darrowo				
<	1					
Comp	outer\H	KEY_LOCAL_MACHINE\SOF	TWARE\Microsoft\Cryp	tography\MSCEP\	EnforcePassword	Activate Wind

Passaggio 2. Fare clic sul menu Start di Microsoft Windows.

Passaggio 23. Digitare MMC.

Passaggio 24. Scegliere Aggiungi/Rimuovi snap-in dal menu File. Scegliere Autorità di certificazione.

Passaggio 25. Fare clic con il pulsante destro del mouse sulla cartella dei modelli di certificato e scegliere Gestisci.

Passaggio 26. Fare clic con il pulsante destro del mouse su un modello esistente, ad esempio Utente, e scegliere **Duplica modello**.

Image: Certificate Templates (WIN-ODE Template Display Name Schema Version Versi International internatinternational international international international i	ded Purp
Image: Certificate Templates (WIN-ODE Template Display Name Schema Version Versi International Image: CA Exchange 2 106.0 Privation Image: CEP Encryption 1 4.1 4.1 Image: Code Signing 1 3.1 5.1 Image: Cross Certification Authority 2 105.0 105.0 Image: Cross Certification Authority 2 115.0 Directory Email Replication Image: Domain Controller 1 4.1 110.0 Client Image: EFS Recovery Agent 1 6.1 5.1 5.1	ded Purp
Image: CA Exchange2106.0PrivationImage: CEP Encryption14.11Image: Code Signing13.11Image: Computer15.11Image: Cross Certification Authority2105.0Image: Cross Certification Authority2105.0Image: Cross Certification Authority2115.0Image: Directory Email Replication2115.0Image: Directory Email Replication14.1Image: Domain Controller14.1Image: Domain Controller Authentication2110.0Image: CFS Recovery Agent16.1	
Image: CEP Encryption14.1Image: Code Signing13.1Image: Computer15.1Image: Cross Certification Authority2105.0Image: Cross Certification Authority2115.0Image: Directory Email Replication2115.0Image: Directory Email Replication14.1Image: Domain Controller14.1Image: Domain Controller Authentication2110.0Image: CFS Recovery Agent16.1	te Key Arc
Image: Code Signing13.1Image: Computer15.1Image: Cross Certification Authority2105.0Image: Directory Email Replication2115.0Image: Directory Email Replication2115.0Image: Directory Email Replication14.1Image: Domain Controller Authentication2110.0Image: Client Image: Client Image	
Image: Computer15.1Image: Cross Certification Authority2105.0Image: Cross Certification Authority2115.0Image: Directory Email Replication2115.0Image: Directory Email Replication14.1Image: Domain Controller Authentication2110.0Image: Clipped EFS Recovery Agent16.1	_
Image: Cross Certification Authority2105.0Image: Directory Email Replication2115.0DirectoryImage: Domain Controller14.1Image: Directory Email Controller Authentication2110.0ClientImage: Cross Certification2110.0ClientClientClientClientImage: Cross Certification216.1ClientClient	
Image: Control of the control of th	
Image: Domain Controller14.1Image: Domain Controller Authentication2110.0Image: CFS Recovery Agent16.1	tory Servi
Image: Controller Authentication 2 110.0 Client Image: Controller Authentication 2 110.0 Client Image: Controller Authentication 2 6.1 Client	
EFS Recovery Agent 1 6.1	t Authent
Enrollment Agent 1 4.1	
Enrollment Agent (Computer) 1 5.1	
Rechange Enrollment Agent (Offline requ 1 4.1	
Exchange Signature Only 1 6.1	
Exchange User 1 7.1	
IPSec 1 8.1	
PSec (Offline request) 1 7.1	-
Rerberos Authentication 2 110.0 Clien	t Authent
Recovery Agent 2 105.0 Key F	Recovery A
OCSP Response Signing 3 101.0 OCSP	Signing
RAS and IAS Server 2 101.0 Clien	t 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	
Real User Signat	
R Web Server 1 4.1	
Workstation Authentication 2 101.0 Clien	Activat

Passaggio 27. Scegliere la CA come Microsoft Windows 2012 R2.

Passaggio 28. Nella scheda Generale aggiungere un nome visualizzato, ad esempio WLC, e un periodo di validità.

Passaggio 29. Nella scheda Nome soggetto, confermare che Fornitura nella richiesta è selezionata.

Superseded Templates Extensions Security Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements	Prop	perties	of New	Template		x		
Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements 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. Subject name format: ✓ Include e-mail name in subject name ✓ Include this information in alternate subject name: ✓ DNS name User principal name (UPN) Service principal name (SPN) ✓	Superseded Templa	tes	Exte	ensions	Security			
Subject Name Server Issuance Requirements Supply in the request Use subject information from existing certificates for autoenrollment renewal requests Build from this Active Directory information Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None Include e mail name in subject name Include this information in alternate subject name: Brmail name DNS name User principal name (UPN) Service principal name (SPN)	Compatibility General Request Handling Cryptography Key Attestation							
 Supply in the request ✓ Use subject information from existing certificates for autoenrollment renewal requests Outer the subject information is active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None Include e-mail name in subject name Include this information in alternate subject name: Germail name User principal name (UPN) Service principal name (SPN) 	Subject Name Server Issuance Requirements							
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. Subject name format: None Include e-mail name in subject name Include this information in alternate subject name: Email name DNS name User principal name (UPN) Service principal name (SPN)								
We subject information from existing certificates for autoenroliment Puild from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)	Supply in the reques	L						
Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None ✓ Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)	renewal requests	mation fro s	m existing	certificates to	r autoenroliment			
○ Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None ✓ Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)								
Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None ✓ Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)	O Build from this Active	Directory	informatio	n				
simplify certificate administration. Subject <u>name format: None Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)</u>	Select this option to e	enforce co	nsistency	among subjec	t names and to			
Subject name format: None Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)	simplify certificate adr	ninistratior	1.					
None Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN) OK Cancel Apply	Subject <u>name</u> format							
□ Include e-mail name in subject name Include this information in alternate subject name: □ E-mail name □ DNS name □ User principal name (UPN) □ Service principal name (SPN)	None				¥			
Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN) ØK Cancel Apply Help	Include e-mail nar	ne in subje	ect name					
E-mail name DNS name User principal name (UPN) Service principal name (SPN)	loolude this informatic	on in alterr	osto subio	ot name:				
OK Cancel Apply Help	E-mail name	ATTIT diten	late subje	ci name.				
OK Cancel Apply Help								
OK Cancel Apply Help								
OK Cancel Apply Help								
OK Cancel Apply Help	Service principal i	name (SPI	N)		2			
OK Cancel Apply Help								
OK Cancel Apply Help								
OK Cancel <u>Apply</u> Help								
OK Cancel <u>Apply</u> Help								
OK Cancel <u>Apply</u> Help								
OK Cancel Apply Help								
OK Cancel Apply Help	014							
	OK	(Jancel	Apply	Help			

Passaggio 30. Fare clic sulla scheda **Requisiti di rilascio**. Cisco consiglia di lasciare vuoti i criteri di rilascio in un ambiente CA gerarchico tipico:

Supersec	Superseded Templates Extensions Security							
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation			
Subject N	Subject Name Server Issuance Requirements							
Require the following for enrollment:								
This number of authorized signatures:								
If you require more than one signature, autoenrollment is not allowed.								
Policy ty	pe required	in signatu	ire:					
					~			
Applicati	<u>on policy:</u>							
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	<u>k</u> ey based	renewal						
Requires subject information to be provided within the certificate request.								
	ОК	(Cancel	Apply	Help			

Passaggio 31. Fare clic sulla **scheda Estensioni**, **Criteri di applicazione**, quindi su **Modifica**. Fare clic su **Aggiungi** e verificare che l'autenticazione client sia stata aggiunta come criterio di applicazione. Fare clic su **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

Passaggio 32. Fare clic sulla **scheda Protezione**, quindi su **Aggiungi...** Verificare che l'account del servizio SCEP definito nell'installazione del servizio NDES disponga del controllo completo del modello e fare clic su **OK**.

Subject N	lame	Sen	ver	Issuance Requirements			
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation		
Superseded Templates Extensions Security					Security		
<u>G</u> roup or use	rnames:						
& Authen	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	ise Admins	(LSC2012	\Enterpris	e Admins)			
\mathbf{k}							
A <u>d</u> d <u>R</u> emove							

Passaggio 3. Tornare all'interfaccia GUI dell'Autorità di certificazione. Fare clic con il pulsante destro del mouse sulla **directory dei modelli di certificato**. Passare a **Nuovo > Modello di certificato da emettere**. Selezionare il modello WLC configurato in precedenza e fare clic su **OK**.

	in the stores that	. icik		-1-
(= 🔿 🖄	📅 🖪 📑 🚺 🖬			_
sole Root		Enable Certificate Templates	x	
Certification A Welaaan201 Certification A Certification A Certificati	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 ne s been replicated to all domain controllers. le organization may not be available to your CA. tificate Template Concepts.	ed to wait until	Tem tions
📔 Failed	Name	Intended Purpose	<u>^</u>	
Certifi	Image: Construction of the system of the	Key Recovery Agent OCSP Signing Client Authentication, Server Authentication Client Authentication Client Authentication, Smart Card Logon Secure Email, Client Authentication, Smart Card Logon Microsoft Trust List Signing Secure Email, Client Authentication Client Authentication Client Authentication		
		ОК	Cancel	
<	III > <	III	>	-

Passaggio 34. Modificare il modello SCEP predefinito nelle impostazioni del Registro di sistema in **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Crittografia > MSCEP**. Modificare le chiavi EncryptionTemplate, GeneralPurposeTemplate e SignatureTemplate da IPsec (richiesta offline) al modello WLC creato in precedenza.

đ						Re	gistry Edi	tor		_ _ X
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	F <u>a</u> vorit	tes <u>H</u> elp	,					
		Þ-	📙 Adva	inced INF	^	Name	Туре	D	ata	
		Þ-	📕 ALG			ab (Default)	REG_SZ	(v	value not set)	
		-	📙 AllUs	erInstallA		EncryptionTem	REG_SZ	W	VLC	
		Þ-	Assis	tance		💩 GeneralPurpose	REG_SZ	W	VLC	
		Þ-	📙 Auth	Host	≡	Signature Template	REG_SZ	W	VLC	
		Þ-	BestP	ractices						
		Þ-	BidIn	terface						
		Þ-	Chkd	lsk						
		₽-	COM	13						
		-	Com	mand Pro						
		4-	Crypt	tography						
				alaic						
				aiais atalogDB						
				atORTem						
				ertificate						
			6 - 🌆 D	efaults						
			4 🛄 N	ISCEP						
			T]	CATyp						
				CertsIn						
			i	Enforce						
				Passwo						
			L]	UseSin						
<		: i		>	Ľ,					
Comp	outer\H	KEY_L	DCAL_M		SOF	TWARE\Microsoft\Cryp	tography\M	ISCEP		Activate Wind

Passaggio 35. Riavviare il sistema.

Configurare il WLC

Passaggio 1. Sul WLC, passare al menu Security (Sicurezza). Fare clic su Certificati > LSC.

Passaggio 2. Selezionare la casella di controllo Abilita LSC sul controller.

Passaggio 3. Immettere l'URL di Microsoft Windows Server 2012. Per impostazione predefinita, viene aggiunto /certsrv/mscep/mscep.dll.

Passaggio 4. Inserire i dettagli nella sezione Parametri.

Passaggio 5. Applicare la modifica.

Local Significant Certificates (LSC)

General AP Provisioning							
Contificato Turo	Shahur						
Certificate Type	Status						
CA	Present 🔽						
General							
Enable LSC on Controller	\checkmark						
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						

Passaggio 6. Fare clic sulla freccia blu sulla linea CA superiore e scegliere **Aggiungi**. Lo stato dovrebbe essere modificato da **Non presente** a **Presente**.

Passaggio 7. Fare clic sulla scheda Provisioning AP.

cisco	MONITOR	<u>w</u> lans	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Security	Local Sig	nificant	Certificates (LSC)					
 AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Priority Order Certificate LSC SSC Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	General AP Provis Enable Update Numbe AP Ethern	AP Presioning	rovision	5) 3					

Passaggio 8. Selezionare la casella di controllo Abilita in AP Provisioning e fare clic su Aggiorna.

Passaggio 9. Riavviare i punti di accesso se non sono stati riavviati.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Il punto di accesso, dopo il riavvio, si unisce e visualizza LSC come tipo di certificato nel menu Wireless.

CISC	0	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK						
Wireless		All APs												Entries	1 - 2 of 2	^
 Access Po All APs Radics 802.112 802.111 Duel-Base 	n/n h/g/n and Radios	Current Filt	ar I APa		/kone 2		(Change Fil	inc) (Clear Filter	1							
Global Cerr	nguration	AP Name		A.P	Nodel		AP HAC	AP Up T	ime	Admin Status	Operational Status	Port	AP Node		Certificati Type	•
Hesh RF Profile	5	CAP15011-3 LAP1142-1		AIR	CAP35011-8-K LAP1142N-3-K	9 9	c8:9c:1d:6e:a3:cs ac:12:c5:73:33:ce	0 4, 00 1	35 m 21 02 m 35 :	s Disabled	REG REG	1	Local Local		LSC LSC	
FlexConned	ect Groups ± ACLs															
> 802.118/0 > 802.11b/0	n a/n															
Media Street	nam.															
Applicatio	en Visibility rol															
Country																
Timers																
Netflow																
▶ Qo5																<
				8			P	2				D	89.4	ENG	6:41 PM	
6		2			0		1	r				- I O	M8 10	ЦК	12/16/2014	4

Nota: Dopo la versione 8.3.112, i punti di accesso MIC non possono più unirsi se il protocollo LSC è abilitato. La funzione di conteggio "tentativi di LSC" ha pertanto un utilizzo limitato.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.