# Certificado localmente significativo (LSC) com exemplo de configuração de WLC e Windows Server 2012

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Configuração do Microsoft Windows Server Configurar o WLC Verificar Troubleshoot

### Introduction

Este documento descreve como configurar o LSC (Locally Significant Certificate) com um WLC (Wireless LAN Controller) e um Microsoft Windows Server 2012 R2 instalado recentemente.

**Note**: As implantações reais podem ser diferentes em muitos pontos e você deve ter controle total e conhecimento das configurações no Microsoft Windows Server 2012. Este exemplo de configuração é fornecido apenas como um modelo de referência para que os clientes da Cisco implementem e adaptem sua configuração do Microsoft Windows Server para fazer o LSC funcionar.

### Prerequisites

#### Requirements

A Cisco recomenda que você compreenda todas as alterações feitas no Microsoft Windows Server e verifique a documentação relevante da Microsoft, se necessário.

**Note**: O LSC na WLC não é suportado com CA intermediário, pois a CA raiz será perdida da WLC, já que a controladora recebe apenas a CA intermediária.

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

• WLC versão 7.6

Microsoft Windows Server 2012 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Configurar

#### Configuração do Microsoft Windows Server

Esta configuração é mostrada como executada em um Microsoft Windows Server 2012 recéminstalado. Você deve adaptar as etapas ao seu domínio e à sua configuração.

**Etapa 1.**Instalar os Serviços de Domínio do Ative Diretory para o assistente de funções e recursos.

Before You Begin	Select one or more roles to install on the elected server.		
installation Type	Roles		Description
Server Selection	Active Directory Certificate Services		Active Directory Domain Services
Server Roles	Active Directory Domain Services		(AD DS) stores information about
Features	Active Directory Ederation Services		this information available to users
AD DS	Active Directory Lightweight Directory Services		and network administrators. AD D
Confirmation	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	-	

Etapa 2. Após a instalação, você deve promover o servidor para o controlador de domínio.

<b>a</b>	Add Roles and Features Wizard	
Installation progr	ess	DESTINATION SERVER WIN-ODEF7N1GRUB
Before You Begin	View installation progress	
Installation Type	Feature installation	
Server Selection		I IIII
Server Roles	Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.	
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 Role Administration Tools	=
	AD DS and AD LDS Tools	
	Active Directory module for Windows PowerShell	
	AD DS Tools	
	Active Directory Administrative Center	
	AD DS Shap-ins and Command-Line loois	~
	You can close this wizard without interrupting running tasks. View task pr page again by clicking Notifications in the command bar, and then Task E Export configuration settings	ogress or open this Jetails.
	< <u>P</u> revious <u>N</u> ext > Cl	ose Cancel

**Etapa 3.** Como esta é uma nova configuração, você configura uma nova floresta; mas normalmente em implantações existentes, basta configurar esses pontos em um controlador de domínio. Aqui, você escolhe o domínio **LSC2012.com**. Isso também ativa o recurso Servidor de Nomes de Domínio (DNS).

**Etapa 4.** Após uma reinicialização, instale o serviço Autoridade de Certificação (CA) e a inscrição na Web.

\_\_\_\_\_

- 0 X

DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com

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

Etapa 5.Configure-os.

Select role services

<b>a</b>	Add Roles and Features Wizard	X
Installation progre	SS DESTINATION SE WIN-ODEF7N1GRUB.LSC201	RVER 2.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)	
	Web Server (IIS)	•
	You can close this wizard without interrupting running tasks. View task progress or open the	nis
	<ul> <li>page again by closing Notifications in the command bar, and then rask Details.</li> </ul>	
	Export configuration settings	
	< Previous Next > Close Can	cel

Etapa 6. Escolha AC empresarial e deixe tudo como padrão.

<b>b</b>	AD CS Configuration	
Role Services		DESTINATION SERVER WIN-ODEF7N1GRUB.LSC2012.com
Credentials Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select Role Services to configure	
	More about AD CS Server Roles	> Configure Cancel

Passo 7. Clique no menu Iniciar do Microsoft Windows.

Etapa 8. Clique em Ferramentas administrativas.

Etapa 9. Clique em Usuários e Computadores do Ative Diretory.

**Etapa 10.** Expanda o domínio, clique com o botão direito do mouse na **pasta Usuários** e escolha **Novo objeto > Usuário**.

	New Object - User	X
File     Action     View     Help       Image: Second S	Create in: LSC2012.com/Users	
<ul> <li>▷ Saved Queries</li> <li>▲ Builtin</li> <li>▷ Computers</li> <li>▷ Domain Controllers</li> </ul>	Erst name: AP Initials:	
<ul> <li>ForeignSecurityPrincipa</li> <li>Managed Service Accound Content</li> <li>Users</li> </ul>	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         Image: Security Group       Members of this group	

**Etapa 11.** Neste exemplo, ele é chamado **APUSER**. Depois de criado, você deve editar o usuário e clicar na **guia MemberOf** e torná-lo um membro do grupo IIS\_IUSRS

As atribuições de direitos de usuário necessárias são:

- Permitir logon local
- Fazer logon como um serviço

Etapa 12. Instale o 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 Conline Responder Certificate Enrollment Veb Service Certificate Enrollment Policy Web Service	
	< <u>P</u> revious <u>N</u> e	xt > Configure Cancel

 Escolha o membro da conta do grupo IIS\_USRS, APUSER neste exemplo, como a conta de serviço para NDES.

Etapa 13. Navegue até Ferramentas administrativas.

Etapa 14. Clique em Internet Information Services (IIS).

Etapa 15. Expanda Server > Sites > Default web site > Cert Srv.

**Etapa 16.** Para **mscep** e **mscep\_admin**, clique em **authentication**. Verifique se a autenticação anônima está habilitada.

**Etapa 17.** Clique com o botão direito do mouse em **autenticação do Windows** e escolha **Provedores**. Certifique-se de que o NT LAN Manager (NTLM) esteja primeiro na lista.

**Etapa 18.** Desative o desafio de autenticação nas configurações do registro, caso contrário, o protocolo SCEP (Simple Certificate Enrollment Protocol) espera a autenticação de senha de

desafio, que não é suportada pelo WLC.

Etapa 19. Abra o aplicativo regedit.

Etapa 20. Vá para HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

Etapa 21. Defina EnforcePassword como 0.

đ			Re	gistry Editor		
File	Edit	View Favorites Help				
		🛛 🔐 Advanced INF 🔨	Name	Туре	Data	
		🔉 - 🍌 ALG	ab) (Default)	REG_SZ	(value not set)	
		🐌 AllUserInstallA	EnforcePassword	REG_DWORD	0x00000000 (0)	
		👂 🍌 Assistance 👘				
		⊳- 🎍 AuthHost 🛛 🚊				
		BestPractices				
		b BidInterface				
		⊳- 🍌 Chkdsk				
		р - 📕 СОМЗ				
		Command Prc		N		
		4 🎳 Cryptography		13		
		D- Calais				
		CatUBTem				
		Certsin				
		Enforce				
		Passwo				
		UseSinc				
<		III >				
Comp	outer\H	KEY_LOCAL_MACHINE\SOF	TWARE\Microsoft\Cryp	tography\MSCEP\Enf	orcePassword	ctivate Wind

Etapa 22. Clique no menu Iniciar do Microsoft Windows.

Etapa 23. Digite MMC.

Etapa 24. No menu Arquivo, escolha Adicionar/remover snap-in. Escolha Autoridade de Certificação.

Etapa 25. Clique com o botão direito do mouse na pasta Modelo de certificado e clique em Gerenciar.

**Etapa 26.** Clique com o botão direito do mouse em um modelo existente, como Usuário, e escolha **Modelo duplicado**.

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	
	R Exchange User	1	7.1	
	PSec 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	
	Reb Server	1	4.1	Activat
	Workstation Authentication	2	101.0	Client Authent

Etapa 27. Escolha a CA para o Microsoft Windows 2012 R2.

Etapa 28. Na guia Geral, adicione um nome de exibição, como WLC e um período de validade.

Etapa 29. Na guia Nome do assunto, confirme se Suprimento na solicitação está selecionado.

Prop	perties	of New	Template		x
Superseded Templa	tes	Ext	ensions	Security	
Compatibility General	Request	Handling	Cryptograph	y Key Attestat	tion
Subject Name	Sen	ver	Issuance	Requirements	
Supply in the request	•				
Use subject infe			and the stars for		a
renewal request	s	m existing	centificates to	rautoenroliment	
O Build from this Active	e Directory	informatio	n		
Select this option to e	enforce co	nsistency	among subjec	t names and to	
simplify certificate add	ninistratior	1.			
Subject <u>name format</u>					
None				¥	
lnclude e-mail nar	ne in subje	ect name			
Include this information	on in alterr	nate subje	ct name:		
E-mail name					
DNS name					
User principal nar	ne (UPN)				
Service principal	name (SPI	N)		Ν	
				45	
					-
ОК	(	Cancel	Apply	Help	

**Etapa 30.** Clique na guia **Issuance Requirements (Requisitos de problema)**. A Cisco recomenda que você deixe as políticas de emissão em branco em um ambiente de CA hierárquico típico:

Supersec	ded Templa	tes	Exte	ensions	Security	
Compatibility	General	Request	Handling	Cryptography	/ Key Attestation	
Subject N	lame	Sen	ver	Issuance Requirements		
Require the f	following fo cate manag	r enrollmer ger approv	nt: val			
T <u>h</u> is num	ber of auth	orized sigr	natures:	0		
lf you re	quire more	than one :	signature, a	autoenrollment	is not allowed.	
Policy ty	pe required	in signatu	ire:			
					~	
Applicati	on policy:					
Issuance	e policies:				· ·	
	- ponereo.				A <u>d</u> d	
					Pamaua	
					<u>R</u> emove	
Require the f	followina fo	r reenrollm	ent:			
Same crit	eria as for (	enrollment				
○ Valid exis	ting certific	ate				
Allow	key based	renewal				
Requires request.	subject inf	omation t	o be provid	ded within the	certificate	
[	ОК	(	Cancel	<u>A</u> pply	Help	

**Etapa 31.** Clique na **guia Extensions**, **Application Policies** e depois **Edit**. Clique em **Adicionar** e certifique-se de que a Autenticação do Cliente seja adicionada como uma política de aplicação. Click **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

**Etapa 32.** Clique na **guia Segurança** e, em seguida, clique em **Adicionar...** Certifique-se de que a conta de serviço SCEP definida na instalação do serviço NDES tem o controlo total do modelo e clique em **OK**.

Subject Name		Server		Issuance	Requ	equirements	
Compatibility	General	Request Handling		Cryptograph	y Key Attestation		
Superseded Templates			Ext	ensions		Security	
Group or use	r names:						
& Authent	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 Use	rs)			
👫 Enterpri	ise Admins	(LSC2012	\Enterpris	e Admins)			
Add <u>R</u> emove							

Etapa 33. Retorne à interface GUI da autoridade de certificação. Clique com o botão direito do mouse no diretório Modelos de certificado. Navegue até New > Certificate Template to Issue (Novo > Modelo de certificado a ser emitido). Selecione o modelo de WLC configurado anteriormente e clique em OK.

	on new renonces minuo	n nap		
(= 🔿 🖄				
sole Root		Enable Certificate Templates	x	<u> </u>
Certification A diaaan201 Revoko lssued Pendir	Select one Certificate Template to Note: If a certificate template that information about this template ha All of the certificate templates in to For more information, see <u>Ce</u>	to enable on this Certification Authority. It was recently created does not appear on this list, you may ne as been replicated to all domain controllers. The organization may not be available to your CA. <u>ertificate Template Concepts.</u>	ed to wait until	Tem tions
🧾 Failed <u> </u> Certifi	Name Key Recovery Agent OCSP Response Signing RAS and IAS Server Router (Offline request) Smartcard Logon Smartcard User Trust List Signing User Signature Only WLC Workstation Authentication	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 Client Authentication Client Authentication		
		ОК	Cancel	
<		Ш	>	

**Etapa 34.** Altere o modelo SCEP padrão nas configurações do Registro em **Computador > HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Criptografia > MSCEP**. Altere as chaves EncryptionTemplate, GeneralPurposeTemplate e SignatureTemplate de IPsec (Solicitação Offline) para o modelo WLC criado anteriormente.

đ			Re	gistry Editor		_ <b>D</b> X
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew F <u>a</u> vorites <u>H</u> elp				
		👂 - 퉲 Advanced INF 🔿	Name	Туре	Data	
		þ - 🕌 ALG	ab (Default)	REG_SZ	(value not set)	
		AllUserInstallA	EncryptionTem	REG_SZ	WLC	
		Assistance	赴 GeneralPurpose	REG_SZ	WLC	
		Þ- 🕌 AuthHost 📃	July Signature Template	EG_SZ	WLC	
		BestPractices				
		b - BidInterface				
		b - M Chkdsk				
		D- COM3				
		Command Pro				
		CatalooDB				
		CatDRTem				
		Defaults				
		MSCEP				
		- CAType				
		Certsin				
		Passwo				
		UseSing				
<						
<u> </u>				to one build MCCED		
Com	puter\F	IKEY_LOCAL_MACHINE\SOF	TWARE (MICrosoft (Cryp	tography(IVISCEP	Δ	ctivate Wind

Etapa 35. Reinicialize o sistema.

#### Configurar o WLC

Etapa 1. Na WLC, navegue até o menu Security. Clique em Certificados > LSC.

Etapa 2. Marque a caixa de seleção Enable LSC on Controller (Ativar LSC no controlador).

**Etapa 3.** Digite a URL do Microsoft Windows Server 2012. Por padrão, ele é anexado a /certsrv/mscep/mscep.dll.

Etapa 4. Digite seus detalhes na seção Params.

Etapa 5. Aplique a alteração.

Local Significant Certificates (LSC)

General AP Provisioning		
Certificate Type	Status	^
	Present	
CA		
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	

Apply

**Etapa 6.**Clique na seta azul na linha CA superior e escolha **Adicionar**. Ele deve alterar o status de **Não presente** para **presente**.

Passo 7. Clique na guia Provisionamento de AP.

cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Security	Local Sig	nificant	Certificates (	LSC)					
<ul> <li>AAA         General         RADIUS         Authentication         Accounting         Fallback         TACACS+         LDAP         Local Net Users         MAC Filtering         Disabled Clients         User Login Policies         Policies         Password Policies         Local EAP         Priority Order         Certificate         LSC         SSC         Access Control Lists         Wireless Protection         Policies         Wireless Control Lists         Web Auth         TrustSec SXP         Advanced         Asset Control Lists         Advanced         Advanced</li></ul>	General AP Provi Enable Update Numbe AP Etherr	AP P sioning	ts to LSC (0 to 25	5) 3					

Etapa 8. Marque a caixa de seleção Habilitar em Provisionamento de AP e clique em Atualizar.

Etapa 9. Reinicialize seus pontos de acesso se eles não tiverem sido reinicializados.

### Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O ponto de acesso, após a reinicialização, se junta novamente e é exibido com o LSC como o tipo de certificado no menu Sem fio.

CISCO	MONETOR WLANS	CONTROLLER WIRELESS SECURI	ПУ МАЛАЗЕНЕНТ СОММАЛО	EEEDBACK			
Wireless	All APs					Entrie	1.2 of 2
Access Points     All APs     Redics     R02.11n/n     R02.11h/pin     Dual-Band Racles	Current Filter Number of APs	/kon# 2	(Change Filter) (Clear Filt	el.			
Global Configuration	AP Name	AP Nodel	AP NAC AP Up	Time Admin Stat	Operational tus Status Pr	ort AP Node	Certificate Type
Hesh RF Profiles	C6P15011-1 LAP1142-1	AIR-CAP3S011-8-KP AIR-LAP1142N-1-KP	c0:9c:id:6e:a3:cd 0.4,00 ac:f2:c5:73:33:ce 0.4,00	h 35 m 21 s Disabled h 02 m 35 s Enabled	ROG 1 ROG 1	Local	LSC LSC
FlexConnect Groups FlexConnect ACLs B02.11a/n							
▶ 802.11b/g/n							
Media Stream							
And Control							
Country							
Timers							
Nettiow							
P Q05							~
							_

**Note**: Depois do 8.3.112, os APs MIC não podem se unir quando o LSC estiver ativado. Portanto, o recurso de contagem de "tentativas de LSC" torna-se de uso limitado.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.