Configuración de 802.1X en AP para PEAP o EAP-TLS con LSC

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Diagrama de la red
Configurar
CA SCEP de Windows Server 2016
Configurar la plantilla de certificado y el Registro
Configuración de LSC en el 9800
Pasos de Configuración de GUI de AP LSC
Pasos de Configuración de LSC CLI de AP
Verificación de LSC de AP
Resolución de Problemas del Aprovisionamiento de LSC
Autenticación 802.1X por cable AP mediante LSC
Pasos de Configuración de Autenticación 802.1x por Cable AP
Configuración GUI de autenticación 802.1x con cable AP
Configuración CLI de autenticación 802.1x por cable de PA
Configuración del switch de autenticación 802.1x por cable AP
Instalación del certificado del servidor RADIUS
Verificación de autenticación 802.1x por cable del PA
Solucionar problemas de autenticación 802.1X
Información Relacionada

Introducción

Este documento describe cómo autenticar los puntos de acceso de Cisco en su puerto de switch mediante los métodos 802.1X PEAP o EAP-TLS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

Controlador inalámbrico

- Punto de Acceso
- Switch
- servidor ISE
- Autoridad de certificados.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador inalámbrico: C9800-40-K9 que ejecuta 17.09.02
- Punto de acceso: C9117AXI-D
- Switch: C9200L-24P-4G que ejecuta 17.06.04
- Servidor AAA: ISE-VM-K9 con 3.1.0.518
- Autoridad de certificación: Windows Server 2016

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Si desea que sus puntos de acceso (AP) se autentiquen con su puerto de switch usando 802.1X, de forma predeterminada utilizan el protocolo de autenticación EAP-FAST que no requiere certificados. Si desea que los AP utilicen el método PEAP-mschapv2 (que utiliza credenciales en el lado AP pero un certificado en el lado RADIUS) o el método EAP-TLS (que utiliza certificados en ambos lados), primero debe configurar LSC. Es la única manera de aprovisionar un certificado raíz/de confianza en un punto de acceso (y también un certificado de dispositivo en el caso de EAP-TLS). No es posible que el AP haga PEAP e ignore la validación del lado del servidor. En este documento se trata primero la configuración de LSC y, a continuación, el lado de la configuración de 802.1X.

Utilice un LSC si desea que su PKI proporcione una mayor seguridad, tenga el control de su autoridad de certificación (CA) y defina políticas, restricciones y usos en los certificados generados.

Con LSC, el controlador obtiene un certificado emitido por la CA. Un AP no se comunica directamente con el servidor CA pero el WLC solicita certificados en nombre de los AP que se unen. Los detalles del servidor de la CA deben configurarse en el controlador y deben ser accesibles.

El controlador utiliza el Protocolo simple de inscripción de certificados (SCEP) para reenviar las solicitudes de certificado generadas en los dispositivos a la CA y vuelve a utilizar SCEP para obtener los certificados firmados de la CA.

SCEP es un protocolo de administración de certificados que los clientes PKI y los servidores CA

utilizan para admitir la inscripción y revocación de certificados. Se utiliza ampliamente en Cisco y es compatible con muchos servidores de CA. En SCEP, HTTP se utiliza como protocolo de transporte para los mensajes PKI. El principal objetivo de SCEP es la emisión segura de certificados para los dispositivos de red.

Diagrama de la red



Configurar

Hay dos cosas que configurar principalmente: la CA SCEP y el WLC 9800.

CA SCEP de Windows Server 2016

Este documento cubre una instalación básica de una CA SCEP de Windows Server para fines de laboratorio. Una CA de Windows real de nivel de producción debe configurarse de forma segura y adecuada para las operaciones empresariales. Esta sección está pensada para ayudarle a probarlo en el laboratorio, así como inspirarse en los ajustes requeridos para hacer que esta configuración funcione. Éstos son los pasos:

Paso 1.Instalar una experiencia de escritorio de Windows Server 2016 nueva.

Paso 2. Asegúrese de que el servidor está configurado con una dirección IP estática.

Paso 3.Instale un nuevo rol y servicio, comience con los servicios de dominio de Active Directory y el servidor DNS.

👝 Se	ver Manager					-	- 6	×
	🚵 Add Roles and Features Wizard		-		age To	ools	View	Help
	Select server roles		DESTINAT WIN-3E	TION SERVER 202T1QD0U				
i	Before You Begin	Select one or more roles to install on the selected server.						
	Installation Type	Roles	Description					
Ϊŝ	Server Selection Server Roles Features DNS Server AD DS Confirmation Results	 Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Rights Management Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server File and Storage Services (1 of 12 installed) Host Guardian Service Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Web Server (IIS) Windows Deployment Services 	Active Directory Domain 5 (AD DS) stores informatio objects on the network ar this information available and network administrato uses domain controllers t network users access to p resources anywhere on th through a single logon pr	Services n about nd makes to users ors. AD DS o give ermitted en entwork rocess.			Hid	e
2		< Previous Next	> Install	Cancel				
		Events 1 Events Performance 5 Service BPA results Performance BPA results	es mance sults		1			
			10/19/2022 11/26 AM					

instalación de Active Directory

🕋 Se	erver Manager								- 0	×
(📥 Add Roles and Features Wizard	d		-		×	age	Tools	View	Help
	Installation progr	ess		DESTINA WIN-3	ATION SER E2O2T1Q	VER DOU				^
Ĩ	Before You Begin	View installation progress								
Ī	Installation Type	i Feature installation								
i ji i	Server Selection									
<u>e</u>	Server Roles	Configuration required. Installation suc	ceeded on WIN-3E2O2T1QD0U.							
Ē	Features	Active Directory Domain Services				^				
	DNS Server	Additional steps are required to make this	s machine a domain controller.							
	AD DS	DNS Server	er							
	Confirmation	Group Policy Management								
	Results	Remote Server Administration Tools								
		Role Administration Tools								
		AD DS and AD LDS Tools							Hid	e
		Active Directory module for	Windows PowerShell				-			
		AD DS Tools				\sim				
		You can close this wizard without inter	rrupting running tasks. View task pro	ogress or o	open thi	s				
		Event configuration settings	the command bar, and their lask b	ctans.						
		export configuration settings								
		< Pre	vious Next > Cl	ose	Cano	el				
		Events	Events				_			
		Services	Services							
		Performance	Performance							
		BPA results	BPA results							
										~

Fin de la instalación de AD

Paso 4.Una vez hecho, haga clic en el panel de Promover este servidor a un controlador de dominio.



Configurar los servicios de AD

Paso 5.Cree un nuevo bosque y elija un nombre de dominio.

👝 Sei	rver l	Ma	ana	aq	er

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

Elija un nombre de bosque

Paso 6.Agregue el rol Servicios de Certificate Server:

🖴 Server Manager							— í) ×
Ser Ser	ver Manager • Das	hboard -	3	🏲	Manage	Tools	View	Help
Dashboard Local Server	WELCOME TO SEE	RVER MANAGER						Ĺ
All Servers	🔁 Add Roles and Features Wizard				-		х	
DNS	Select server role	S		WIN	DESTIN 3E2O2T1QD0U.	NATION SERV	/ER ical	
■ File and Storage Ser	Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Domain Services (Installed) Active Directory Federation Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server (Installed)	<	Description Active Dir (AD CS) is certification role service and manana variety of	ectory Certific used to creat on authorities tes that allow ge certificate applications.	tate Servic te and relate you to issi s used in a	es Id	de

Agregar servicios de certificados



Agregue sólo la entidad emisora de certificados

Paso 7.Una vez hecho esto, configure su entidad emisora de certificados.

AD CS Configuration AD CS Configuration AD CS Configuration AD C Credentials Credentials Credentials Select Role Services to configure AD Setup Type Certification Authority Certification Authority Certificate Enrollment Service Cryptography Certificate Enrollment Policy Web Service Validity Period Certificate Enrollment Policy Web Service Confirmation Powee Policy	🚔 Server	Manager			-	- ć	X
Destination SERVER Role Services Credentials Credentials Select Role Services to configure Role Services Setup Type CA Type Private Key Cryptography Catificate Database Confirmation Velociticate Database Confirmation	\mathbf{E}	AD CS Configuration			× age Tools	View	Help
Image: All credentials Select Role Services to configure - - × - - - × - - × - - × - - - × - - - × - - - - - - - - - - - -	iii Dat	Role Services		DESTINATION SERV WIN-3E2O2T1QD0U.mydomain.log	ER		
Image: AD Role Services Image: AD Setup Type Image: AD CA Type Image: CA Type Online Responder Image: Cryptography Certificate Enrollment Service Image: CA Name Certificate Enrollment Policy Web Service Validity Period Main.local. Image: Confirmation Image: Confirmation Image: Response Image: Response	All 🖬	Credentials	Select Role Services to configure			×	
Image: AD Setup Type Image: Certification Authority Destiniation Server of Certification Authority Image: DN CA Type Certification Authority Web Enrollment Online Responder Image: File Private Key Network Device Enrollment Service Cryptography Certificate Enrollment Web Service Main.local Validity Period Certificate Database Main.local Confirmation Image: Database Image: Database Confirmation Image: Database	🖳 AD	Role Services					
PN CA Type Online Responder Image: File Private Key Online Responder Cryptography Certificate Enrollment Web Service Cartificate Enrollment Web Service CA Name Certificate Enrollment Policy Web Service main.local. Validity Period Certificate Database ide Confirmation In the destination ide	i∎i AD	Setup Type	Certification Authority		DESTINATION SERV QD0U.mydomain.lo	/ER /cal	
File Private Key Network Device Enrollment Service Cryptography Certificate Enrollment Web Service CA Name Certificate Enrollment Policy Web Service Validity Period main.local. Certificate Database n the destination Reservers ide	🛱 DN	CA Type	Online Responder				
Cryptography Certificate Enrollment Web Service CA Name Certificate Enrollment Policy Web Service Validity Period main.local. Certificate Database confirmation Confirmation ide	File File	Private Key	Network Device Enrollment Service				
CA Name Certificate Enrollment Policy Web Service Validity Period main.local. Certificate Database main.local. Confirmation ide		Cryptography	Certificate Enrollment Web Service				
Validity Period main.local. Certificate Database Confirmation n the destination ide		CA Name	Certificate Enrollment Policy Web Service				
Certificate Database Confirmation n the destination ide		Validity Period			main.local.		
Confirmation n the destination ide		Certificate Database					
Program		Confirmation			n the destination	n ^{ir}	de
Progress		Progress				-	
Results		Results					
More about AD CS Server Roles			More about AD CS Server Roles				
< Previous Next > Configure Cancel ess or open this			< Previous	Next > Configure Cancel	ess or open this		

Paso 8. Seleccione Enterprise CA.



CA empresarial

Paso 9.Conviértalo en una CA raíz. Desde Cisco IOS XE 17.6, las CA subordinadas son compatibles con LSC.



Elija una CA raíz

Es importante tener la cuenta que utiliza para que la CA forme parte del grupo IIS_IUSRS. En este ejemplo, se utiliza la cuenta Administrador y se va al menú Usuarios y equipos de Active Directory para agregar los usuarios Administrador al grupo IIS_IUSRS.

🚔 Server Manager				– 0 ×
Server Manag	ger • Dashboard		🕄 🚩 Manage Too	ols View Help
Computers Co	Administrator Properties Remote control Remote Desktop Services Profile General Address Account Profile Telepho Member Of Dial-in Environment Member of: Image: Services of the	? × ile COM+ nes Organization Sessions Folder Folder Folder Folder many group unless POSIX-compliant by Help A security for the security of	- Configure Cancel	Hide
	DPA results BPA	A results		
# > © 🤅 🗔			^ 팀 d <mark>×</mark> [ENG 10:47 PM BEFR 10/19/2023

Agregue su cuenta de administrador al grupo IIS_USER

Paso 10.Una vez que tenga un usuario en el grupo de IIS adecuado, agregue funciones y servicios. A continuación, agregue los servicios Respondedor en línea y NDES a la entidad emisora de certificados.

٥ ×



Instalar los servicios NDES y Respondedor en línea

Paso 11.Una vez hecho esto, configure esos servicios.



Instalar el Respondedor en línea y el servicio NDES

Paso 12.Se le solicita que elija una cuenta de servicio. Ésta es la cuenta que agregó previamente al grupo IIS_IUSRS.



Seleccione el usuario que agregó al grupo IIS

Paso 13. Esto es suficiente para las operaciones SCEP, pero para lograr la autenticación 802.1X, también necesita instalar un certificado en el servidor RADIUS. Por lo tanto, para mayor facilidad, instale y configure el servicio de inscripción web para poder copiar y pegar fácilmente la solicitud de certificado de ISE en nuestro servidor Windows.



Instalar el servicio de inscripción en la Web

AD CS Configuration		– 🗆 X
Role Services		DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local
Credentials Role Services	Select Role Services to configure	
Confirmation Progress Results	 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

configurar el servicio de inscripción web

Paso 14. Puede verificar que el servicio SCEP funciona correctamente visitando <u>http://<serverip>/certsrv/mscep/mscep.dll</u>:

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

Verificación del portal SCEP

Paso 15.

De forma predeterminada, Windows Server utilizó una contraseña de desafío dinámico para autenticar las solicitudes de cliente y de extremo antes de la inscripción en Microsoft SCEP (MSCEP). Esto requiere una cuenta de administrador para navegar a la GUI web y generar una contraseña a pedido para cada solicitud (la contraseña debe incluirse en la solicitud). El controlador no puede incluir esta contraseña en las solicitudes que envía al servidor. Para quitar esta característica, es necesario modificar la clave del Registro en el servidor NDES:

Abra el Editor del Registro y busque Regedit en el menú Inicio.

Vaya a Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword

Cambie el valor de EnforcePassword a 0. Si ya es 0, déjelo tal cual.

۵.		Registry Editor		_ 🗆 🗙
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
— 📜 САТуре		(Default)	REG SZ	(value not set)
CertsInMYStore		8 EnforcePassword	REG_DWORD	0x00000000 (0)
EnforcePassword		(- 4	_	
PasswordVDir				
- LOID	Ξ			
- Protect				
- Providers				
- Services				
Data Associa				
DataAccess				
Device Association Framework				
Device Association Framework				R
DES				
DHCPMibAgent				
DirectDraw				
DirectIonut				
DirectPlay8				
	$\overline{}$			
	-	<	111	>
Computer\HKEY_LOCAL_MACHINE\S	OFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword

Establecer el valor de EnforcePassword

Configurar la plantilla de certificado y el Registro

Los certificados y sus claves asociadas se pueden utilizar en varios escenarios para diferentes propósitos definidos por las directivas de la aplicación dentro del servidor de la CA. La directiva de aplicación se almacena en el campo Uso extendido de claves (EKU) del certificado. El autenticador analiza este campo para comprobar que el cliente lo utiliza para el fin previsto. Para asegurarse de que la política de aplicación adecuada esté integrada en los certificados WLC y AP, cree la plantilla de certificado adecuada y asígnela al registro NDES:

Paso 1. Vaya a Inicio > Herramientas administrativas > Entidad emisora de certificados.

Paso 2. Expanda el árbol de carpetas Servidor de la CA, haga clic con el botón derecho en las carpetas Plantillas de certificado y seleccione Administrar.

Paso 3. Haga clic con el botón derecho en la plantilla de certificado Users y, a continuación, seleccione Duplicate Template en el menú contextual.

Paso 4. Vaya a la pestaña General, cambie el nombre de la plantilla y el período de validez según

desee y deje todas las demás opciones sin marcar.

A Precaución: cuando se modifique el período de validez, asegúrese de que no sea mayor que la validez del certificado raíz de la entidad emisora de certificados.

Properties of New Template

X

Subject Name	Sen	ver	Issuance R	equirements			
Superseded Templa	tes	Exte	nsions	Security			
Compatibility General	Request	Handling	Cryptography	Key Attestation			
Template display name: 9800-LSC							
Template name: 9800-LSC							
Validity period:]	Renewa 6	veeks v				
Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory							
OK	(Cancel	Apply	Help			

Paso 5. Vaya a la pestaña Nombre del Asunto, asegúrese de que Aprovisionar en la solicitud está seleccionado. Aparecerá una ventana emergente para indicar que los usuarios no necesitan la aprobación del administrador para firmar su certificado. Seleccione Aceptar.



Aprovisionamiento en la solicitud

Paso 6. Vaya a la pestaña Extensions, seleccione la opción Application Policies y seleccione el botón Edit.... Asegúrese de que Client Authentication esté en la ventana Application Policies; de lo contrario, seleccione Add y agréguelo.

Properties of New Template						
Compatibility	General	Request	Handling	Cryptography	Key Attestation	
Subject N	lame	Ser	ver	Issuance	Requirements	
Supersec	ded Templa	tes	Exte	insions	Security	
To modify an extension, select it, and then click Edit.						
Extensions in Applicat	ion Policies	his templa	ite:			
Edit	Applicati	on Poli	cies Exte	nsion 💌		
An application policy defines how a certificate can be used.						
Application p Client Author Encrypting Secure Ema	oolicies: entication File System il				Edt	

Verificar extensiones

Paso 7. Vaya a la ficha Seguridad, asegúrese de que la cuenta de servicio definida en el paso 6 de Habilitar servicios SCEP en el servidor de Windows tiene los permisos de Control total de la plantilla y, a continuación, seleccione Aplicar y Aceptar.

Properties of New Template

X

A 1			in rolling	Cryptography	rvey Attestation
Subject I	Name	Server		Issuance R	equirements
Superse	ded Templa	stes	Exte	ensions	Security
Group or use	er names:				
& Authen	ticated Use	¥18			
Admini:	strator				
Be Domain	n Admins (C	HUU-DOMAI	N\Dom	ain Admins)	
Se Domair	n Users (CH	IUU-DOMAIN	NDomai	in Users)	
as Enterpr	ise Admins	(CHOO-DOM		terprise Admins)	
			Γ	Add	Pemaua
				Add	Hemove
Demissione					
	for Administ	Instan		Allow	Decu
remissions	for Adminis	trator		Allow	Deny
Full Contro	for Adminis ol	trator		Allow	Deny
Full Contr Read	for Adminis ol	trator		Allow ✓	Deny
Full Contro Read Write	for Adminis ol	trator		Allow ✓ ✓	Deny
Full Contro Read Write Enroll	for Adminis	trator		Allow ✓ ✓ ✓	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol	trator		Allow ✓ ✓ ✓ ✓	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol	trator		Allow ✓ ✓ ✓ ✓	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol	trator		Allow V V V V	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis	trator		Allow	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol	or advanced	setting:	Allow Allow S. click	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol I	or advanced	settings	Allow Allow S, click	Deny
Full Control Read Write Enroll Autoenrol	for Adminis ol I	or advanced	settings	Allow	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol	or advanced	settings	Allow	Advanced
Full Contro Read Write Enroll Autoenrol	for Adminis ol	or advanced	settings	Allow	Advanced

Paso 8. Vuelva a la ventana Entidad de certificación, haga clic con el botón derecho en la carpeta Plantillas de certificado y seleccione Nuevo > Plantilla de certificado para emitir.

Paso 9. Seleccione la plantilla de certificado creada anteriormente, en este ejemplo es 9800-LSC, y seleccione Aceptar.

Nota: la plantilla de certificado recién creada puede tardar más en aparecer en varias implementaciones de servidores, ya que debe replicarse en todos los servidores.

		Enable Certificate Templates	X
Sele Note Infor All o For	ect one Certificate Template to e: If a certificate template that mation about this template has f the certificate templates in th 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.	
Na	me	Intended Purpose	~
	9800-LSC	Client Authentication, Secure Email, Encrypting File System	
199	CA Exchange	Private Key Archival	
	Code Signing	Code Signing	=
	Cross Certification Authority	<al></al>	
	Enrollment Agent	Certificate Request Agent	
	Enrollment Agent (Computer)	Certificate Request Agent	_
	Exchange Signature Only	Secure Email	
	Exchange User	Secure Email	
	IPSec	IP security IKE intermediate	
	Key Recovery Agent	Key Recovery Agent	
	OCSP Resnanse Signing	OCSP Signing	~
		OK Cano	el

Elija la plantilla

La nueva plantilla de certificado aparece ahora en el contenido de la carpeta Plantillas de certificado.

違 certsrv - [Cer	tification Authority (Local)\CHUU-WIN	N12-CA\Certificate Templates]	x
File Action View Help			
🗢 🏟 🙎 🙆 🔒 📓			
Certification Authority (Local) CHUU-WIN12-CA Revoked Certificates Pending Requests Failed Requests Certificate Templates	Name Name Image: Second Seco	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 Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all></all>	

Seleccione el LSC

Paso 10. Vuelva a la ventana Registry Editor y navegue hasta Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.

Paso 11. Edite los registros EncryptionTemplate, GeneralPurposeTemplate y SignatureTemplate para que señalen a la plantilla de certificado recién creada.



Cambiar la plantilla en el Registro

Paso 12. Reinicie el servidor NDES, de modo que vuelva a la ventana Certification Authority, seleccione el nombre del servidor y seleccione el botón Stop y Play sucesivamente.

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

Configuración de LSC en el 9800

Estos son los pasos en secuencia para configurar LSC para AP en WLC.

- 1. Crear clave RSA. Esta clave se utiliza más adelante para el punto de confianza PKI.
- 2. Cree un punto de confianza y asigne la clave RSA creada.
- 3. Habilite el aprovisionamiento de LSC para los AP y asigne el punto de confianza.
 - 1. Habilite LSC para todos los AP unidos.
 - 2. Habilite el LSC para los AP seleccionados a través de la lista de aprovisionamiento.
- 4. Cambie el punto de confianza de administración inalámbrica y señale al punto de confianza LSC.

Pasos de Configuración de GUI de AP LSC

Paso 1.Vaya a Configuration > Security > PKI Management > Key Pair Generation .

- 1. Haga clic en Agregar y asígnele un nombre relevante.
- 2. Agregue el tamaño de la clave RSA.
- 3. La opción de clave exportable es opcional. Esto sólo es necesario si desea exportar la clave fuera de la caja.
- 4. Seleccione Generar

Dashboard		Trustpoints CA Serv	er	Key Pai	r Generation	Add Ce	ertificate Trustp	ool
) Monitoring	>	+ Add						
Configuration	>	Key Name	Ŧ	Key Type	Key Exportable	Zeroize	Key Name*	AP-SCEP
<u> </u>		TP-self-signed-2147029	136	RSA	No	🖹 Zer		
Administration	>	9800-40.cisco.com		RSA	No	🗟 Zer	Key Type*	RSA Key O EC Key
Licensing		TP-self-signed- 2147029136.server		RSA	No	🗎 Zer	Modulus Size*	2048
		CISCO_IDEVID_SUDI		RSA	No	🖹 Zer		
Troubleshooting		CISCO_IDEVID_SUDI_LE	GACY	RSA	No	🖹 Zer	Key Exportable*	
		H H		10 🗸	1 - 5 0	f 5 items	Cancel	✓ Generate

Paso 2. Vaya a Configuration > Security > PKI Management > Trustpoints

- 1. Haga clic en Agregar y asígnele un nombre relevante.
- Introduzca la URL de inscripción (donde la URL es <u>http://10.106.35.61:80/certsrv/mscep/mscep.dll</u>) y el resto de los detalles.
- 3. Seleccione los pares de claves RSA creados en el paso 1.
- 4. Haga clic en Authenticate.
- 5. Haga clic en Inscribir punto de confianza e introduzca una contraseña.
- 6. Haga clic en Aplicar al dispositivo.

Q Search Menu Items	Configuration • > Security • > PKI Management							
Dashboard	Add Trustpoint			×				
	Label*	Access_Point-MS-CA	Enrollment Type	SCEP O Terminal				
(Monitoring >	Subject Name							
Configuration	Country Code	IN	State	КА				
Administration	Location	Bengaluru	Domain Name	TAC-LAB.cisco.local				
C Licensing	Organization	TAC	Email Address	mail@tac-lab.local				
X Troubleshooting	Enrollment URL	/certsrv/mscep/mscep.dll	Authenticate					
	Key Generated		Available RSA Keypairs	AP-SCEP 👻				
	Enroll Trustpoint							
	Password*							
	Re-Enter Password*							
	Cancel			Apply to Device				

Paso 3.Vaya a Configuración > Inalámbrico > Puntos de acceso. Desplácese hacia abajo y seleccione LSC Provisioning.

- 1. Seleccione el estado como activado. Esto habilita el LSC para todos los AP que están conectados a este WLC.
- 2. Seleccione el nombre de punto de confianza que creamos en el paso 2.

Rellene el resto de los datos según sus necesidades.

Q, Search Menu Items	Configuration * > Wireless * > Access Points				
🚃 Dashboard	 All Access Points 				
Monitoring	Total APs : 1		Misconfigure Tag : 0	Country Code : 0 LSC Failback : 0	Select an Action 🔹
Configuration >	AP Name : AP Model :	Admin : Slots : Status Up Time : IP Address	Ethernet	AP : Power Derate MAC : Mode Capable	i Operation i Config Status Status
(Õ) Administration →	AP0CD0-F89A-46E0 4 M C9117AXI-D	2 O days 0 hrs 26 10.105.101.1	68 d0ec.3579.0300 0cd0.189e	L45e0 Local Yes	Registered Healths
C Licensing	H 4 1 H 10 V				1 - 1 of 1 access points
X Troubleshooting	> 6 GHz Radios				
	> 5 GHz Radios				
	> 2.4 GHz Radios				
	> Dual-Band Radios				
	> Country				
	 LSC Provision 				
	Status	Enabled •	Subject Name Parameters		B Apply
	Trustpoint Name	Access_Point-MS.# +	Country	IN	
	Number of Join Attempts	3	State	КА	
	Key Size	2048 💌	City	Bengaluru	
	Certificate chain status	Not Available	Organization	TAC:	

Una vez que habilita el LSC, los AP descargan el certificado vía el WLC y reinician. En la sesión de la consola AP, verá algo como este fragmento de código.



Paso 4.Una vez habilitado LSC, puede cambiar el certificado de administración inalámbrica para que coincida con el punto de confianza de LSC. Esto hace que los AP se unan con sus certificados LSC y que el WLC utilice su certificado LSC para la unión AP. Este es un paso opcional si su único interesado es hacer la autenticación 802.1X de sus AP.

- 1. Vaya a Configuration > Interface > Wireless y haga clic en Management Interface.
- 2. Cambie el Trustpoint para que coincida con el trustpoint que creamos en el paso 2.

Esto concluye la parte de configuración de la GUI de LSC. Los AP deben poder unirse al WLC usando el certificado LSC ahora.



Pasos de Configuración de LSC CLI de AP

1. Cree una clave RSA con este comando.

9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP

% You already have RSA keys defined named AP-SCEP. % They will be replaced % The key modulus size is 2048 bits % Generating 2048 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 0 seconds) Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storage Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported

2. Cree el punto de confianza PKI y asigne el par de claves RSA. Introduzca la URL de inscripción y el resto de los detalles.

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,0=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. Autentique e inscriba el punto de confianza PKI con el servidor CA mediante el comando crypto pki authenticate <trustpoint>. Introduzca una contraseña en la solicitud de contraseña.

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
Certificate has the following attributes:
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-40(config)#crypto pki enroll Access_Point-MS-CA
%
% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
Re-enter password:
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
% The subject name in the certificate will include: 9800-40.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: TTM244909MX
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Access_Point-MS-CA' commandwill show the fingerprint.
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
```

```
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-44
Serial-number: 5C000001400DD405D77E6FE7F00000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

4. Configure la unión de AP con el certificado LSC.

9800-40(config)#ap lsc-provision join-attempt 10 9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L 9800-40(config)#ap lsc-provision key-size 2048 9800-40(config)#ap lsc-provision trustpoint Access_Point-MS-CA 9800-40(config)#ap lsc-provision In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration Are you sure you want to continue? (y/n): y

5. Cambie el punto de confianza de gestión inalámbrica para que coincida con el punto de confianza creado anteriormente.

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

Verificación de LSC de AP

Ejecute estos comandos en el WLC para verificar el LSC.

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

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



Una vez que se recargan los AP, inicie sesión en la CLI del AP y ejecute estos comandos para verificar la configuración de LSC.

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

```
AP0CD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
                           --- Device Certificate -
Certificate:
   Data:
       Version: 3 (0x2)
      Serial Number:
           5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
       Signature Algorithm: sha256WithRSAEncryption
       Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
       Validity
           Not Before: Sep 28 04:15:28 2023 GMT
           Not After : Sep 27 04:15:28 2024 GMT
       Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0, emailAddress = mail@tac-lab.local
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
               RSA Public-Key: (2048 bit)
               Modulus:
```

APBCD0.F89A.46E0#sho crypto in LSC LSC: Enabled APBCD0.F89A.46E0#sho canwap cli config in lsc APP lsc enable : 1 AP lsc reboot cnt : 0 AP lsc reboot cnt : 0 AP lsc mode : 0x1 AP lsc dtls fallback state : 0 AP0CD0.F89A.46E0# Read timed out
AP0CD0.F89A.46E0#sho dtls connections
Number of DTLS connection = 1
<pre>[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version</pre>
[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2
Current connection certificate issuer name: sumans-lab-ca

Resolución de Problemas del Aprovisionamiento de LSC

Puede tomar una captura EPC del puerto del switch de link ascendente WLC o AP para verificar el certificado que AP está utilizando para formar el túnel CAPWAP. Verifique desde el PCAP si el túnel DTLS se ha construido correctamente.



Los debugs DTLS se pueden ejecutar en AP y WLC para comprender el problema del certificado.

Autenticación 802.1X por cable AP mediante LSC

El AP está configurado para utilizar el mismo certificado LSC para autenticarse. El AP actúa como suplicante de 802.1X y es autenticado por el switch contra el servidor ISE. El servidor ISE se dirige al AD en el back-end.



Nota: Una vez que se habilita la autenticación dot1x en el puerto del switch de link ascendente AP, los AP no pueden reenviar ni recibir tráfico hasta que se pasa la autenticación. Para recuperar los AP con autenticación fallida y obtener acceso al AP, inhabilite la autenticación dot1x en el puerto del switch cableado AP.

Flujo de trabajo de autenticación EAP-TLS e intercambio de mensajes



Pasos de Configuración de Autenticación 802.1x por Cable AP

- 1. Active la autenticación de puerto dot1x junto con CAPWAP DTLS y seleccione el tipo de EAP.
- 2. Cree credenciales dot1x para AP.
- 3. Habilite dot1x en el puerto del switch.
- 4. Instale un certificado de confianza en el servidor RADIUS.

Configuración GUI de autenticación 802.1x con cable AP

- 1. Navegue hasta el perfil de unión a AP y haga clic en el perfil.
 - 1. Haga clic en AP > General. Seleccione el tipo de EAP y el tipo de autorización de AP como "CAPWAP DTLS + autenticación de puerto dot1x".
 - 2. Navegue hasta Administración > Credenciales y cree un nombre de usuario y una contraseña para AP dot1x auth.

Cisco Cat	talyst 9800-40 Wireless Controller		Welcome admin 🐐 🌾 🛕 🖺 🔅 🔞 📿 🕻	Search APs and Clients Q
Q. Search Manu Items	Configuration * > Tags & Profiles * > AP Join		Edit AP Join Profile General Client CAPWAP AP Management Secur	ity ICap QoS
Dashboard	AP Join Profile Name	T Des	General Power Management Hyperiocation AP Statistics Power Over Ethernet	Client Statistics Reporting Interval
Configuration	APG_test totSto APG_stotFin-APs		Switch Flag Power Injector State	5 GHz (sec) 90 2.4 GHz (sec) 90
Clicensing Troubleshooting	APG_4th-FF-APs APG_6th-FF-APs APG_7th-FF-APs		Power Injector Type Unknown Injector Switch MAC 0000.0000	Extended Module
	APG_80+Fi+APs APG_110+Fi+APs		AP EAP Auth Configuration EAP Type EAP-TLS AP Authorization Type CAPNAP DTLS + DDT=	Mesh Profile Name default-mesh-pro Clear
Work Me Through 1	APG_12m-Pir-APs H ← 1 2 3 → ₩ 10 Ψ		CAPWAP DTLS + DOTTx port auth CAPWAP DTLS Dottx port auth	
			D Cancel	👸 Update & Apply to Device

Cisco Cisco Ca	atalyst 9800-40 Wireless Controller	Welcome admin 🛛 🕷 🥵 🛕	
Q. Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile	×
Dashboard	+ Add X Delete	General Client CAPWAP AP	Management Security ICap QoS
	AP Join Profile Name	T Des	
(Monitoring)	ap-auth	Dot1x Credentials	
Configuration	APG_test	Dot1x Username ap-win	ad-user
ි Administration	testSite	Dot1x Password	
ç,	APG_3rd-Fir-APs	Postly Dessured Turns	
C Licensing	APG_4th-Fir-APs	Contra Passanora Type	•
W Troubleshooting	APG_6th-Fir-APs		
	APG_7th-Fk-APs		
	APG_8th-Fir-APs		
	APG_11th-Fir-APs		
Walk Me Through 3	APG_1201-HI-APS		
	H < 1 2 3 + H 10 +		
		D Cancel	🔀 Update & Apply to Device

Configuración CLI de autenticación 802.1x por cable de PA

Utilice estos comandos para habilitar dot1x para AP desde la CLI. Esto solo habilita la autenticación por cable para los AP que están usando el perfil de unión específico.

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

Configuración del switch de autenticación 802.1x por cable AP

Esta configuración del switch se utiliza en LAB para habilitar la autenticación por cable AP. Puede tener diferentes configuraciones basadas en el diseño.

```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
1
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
switchport access vlan 101
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication priority dot1x
authentication port-control auto
dot1x pae authenticator
end
```

Instalación del certificado del servidor RADIUS

La autenticación se produce entre el AP (que actúa como el solicitante) y el servidor RADIUS. Ambos deben confiar en el otro certificado. La única manera de que el AP confíe en el certificado del servidor RADIUS es hacer que el servidor RADIUS utilice una velocidad certici emitida por la CA SCEP que también emitió el certificado AP.

En ISE, vaya a Administration > Certificates > Generate Certificate Signing Requests.

Genere una CSR y rellene los campos con la información de su nodo de ISE.

Cisco ISE

Administration · System

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings			
		0										
Certificate Managem	nent 🗸	Certifica	Certificate Signing Request									
System Certificate	15	Certificate t	types will require a	different extended key	usages. The list t	below outlines which exter	ided key usages are required	for each certificate type:				
Trusted Certificate	55	ISE Ident	ISE Identity Certificates:									
OCSP Client Profil	le	- Multi	Mutti-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication									
Certificate Signing	Requests	Admi	in - Server Authen	tication								
Certificate Periodi	c Check Se	• EAP /	Authentication - S	erver Authentication								
		 DTLS 	Authentication - 1	Server Authentication								
		 Porta 	I - Server Authent	tication								
Certificate Authority	· >	 pxGri 	id - Client and Ser	rver Authentication								
		 SAMI 	L - SAML Signing	Certificate								
		 ISE N 	Jessaging Service	- Generate a Signing	Certificate or gen	erate a brand new Messa	ging Certificate.					
		ISE Cost	Gonnect Ceronical	te - Connect to Oracle	Database							
		ISE Gera	incate Aution	ity certificates.								
		• ISE R	.oot GA - This is n	iot a signing request, c	CA Signing Regu	merate a brand new Koot	GA certificate for the ISE GA I	functionality.				
		- Repe	w ISE OCSP Resp	onder Certificates - Th	is is not a signing	a request, but an ability to	renew the OCSP responder c	ertificate that is signed by	the ISE Root CA/ISE Intermediate CA			
		llesses				request, out an admity to		and a start of angles of				
		Usage										
		Certific	cate(s) will be us	sed for EAP Aut	hentication	~						
		Allow W	vildcard Certificate	s 🗌 🕡								
		Node(s)										
		Generat	te CSR's for these	Nodes:								
		Node		CSR	Friendly Name							
		🖂 isi	E99	ISES	9#EAP Authen	tication						
		Subject										
		Comm	on Name (CN)									
		\$FQD	INS			0						
		Organi	izational Unit (O	U)								
						0						
		Organi	zation (O)									
						0						
		City (L)									
		State ((ST)									

Una vez generado, puede exportarlo y copiarlo y pegarlo como texto también.

Navegue hasta la dirección IP de la CA de Windows y agregue /certsrv/ a la URL

Haga clic en Solicitar un certificado





Haga clic en Enviar una solicitud de certificado con un certificado base-64

Microsoft Active Directory Certificate Services - mydomain-WIN-3E2O2T1QD0U-CA

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to: <u>Create and submit a request to this CA</u>. Submit a cartificate request by using a base 64 exceeded CMC or DKCS #10 file, or submit a request by

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Pegue el texto CSR en el cuadro de texto. Elija la plantilla de certificado del servidor Web.

Microsoft Active Directory Certificate Services - mydomain-WIN-3E202T1QD0U-CA								
Submit a Certificate Request or Renewal Request								
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.								
Saved Request: Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):								
Certificate Template: (No templates found!) >								
Additional Attributes: Attributes:								

A continuación, puede instalar este certificado en ISE volviendo al menú Solicitud de firma de certificado y haciendo clic en Enlazar certificado. A continuación, puede cargar el certificado obtenido desde Windows C.

≡ Cisco ISE	Administration · System							
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings							
Certificate Management System Certificates Signing Requests								
Trusted Certificates OCSP Client Profile	Generate Certificate Signing Requests (CSR) A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click *export* to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click this list.							
Certificate Signing Requests								
Certificate Periodic Check Se	Q View 🖞 Export 📋 Delete Bind Certificate							
Certificate Authority >	Eriendly Name Certificate Subject Key Length Portal gro Timestamp A Host							
	ISE99#EAP Authentication CN=ISE99.mydomain.local 4096 Mon, 30 Oct 2023 ISE99							

Verificación de autenticación 802.1x por cable del PA

Tome el acceso de la consola al AP y ejecute el comando:

#show ap authentication status

La autenticación de AP no está habilitada:

Registros de la consola desde el AP después de habilitar la autenticación de AP:

```
AP0CD0.F89A.46E0#[*09/26/2023 08:57:40.9154]
[*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode
[*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL
```

AP autenticado correctamente:

NP0CD0,F89A.46E8#sho ap authentication status
kay_agat=TEFE_892_3X_(ap_MPA)
apa_state=(OMPLETED
Supplicat PAL state=AUTHENTICATES
supportStatus=Authorized
OVESTICETONICESS relectedHindmall (EAP-TLS
sap_tis_version=TLSv1.2
EAP TLS_CIPIE=RSA-AE5256-GOM-SHA384
200_session_id=007091a744885a668e460d49fee7d2d56684ea2bdd11f40494a4325dc98d1919af48b9fb33ee526f18eda11effcb2ea0238cf95244aafb5f17decf336ad11e88121
NP0CD0. F89A. 46E8#

Verificación del WLC:

9800-40#sho ap name AP0CD0.F89A.46E0 config general begin Certificate						
AP Certificate type : Locally Significant Certificate						
AP Certificate Expiry-time : 09/25/2024 06:48:23						
AP Certificate issuer common-name : sumans-lab-ca						
AP Certificate Policy : Default						
AP CAPWAP-DTLS LSC Status	CAPWAP-DTLS LSC Status					
Certificate status : A	tus : Available					
LSC fallback status : M	C fallback status : No					
Issuer certificate hash : 6	ash : 611255bc69f565af537bc59297f453593e432e1b					
Certificate expiry time : @	: 09/25/2024 06:48:23					
AP 802.1x LSC Status						
Certificate status : A	: Available					
Issuer certificate hash : 6	e hash : 611255bc69f565af537be59297f453593e432e1b					
Certificate expiry time : 8	Certificate expiry time : 89/25/2024 06:48:23					
AP LSC authentication state	: CAPWAP-DTLS and 802.1x authentication					

Estado de la interfaz de puerto de switch tras autenticación satisfactoria:

Switch#sho authenticatio Interface	n sessions inte MAC Address	rface gi Method	gabitEth Domain	ernet 1/0/2 Status Fg	Session ID
Gi1/0/2	0cd0.f89a.46e0	dot1x	DATA	Auth	9765690A0000005CCEED0FBF

Este es un ejemplo de los registros de la consola AP que indican una autenticación exitosa:

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 comp]
```

Solucionar problemas de autenticación 802.1X

Tome PCAP en el link ascendente del AP y verifique la autenticación del radio. Este es un fragmento de la autenticación exitosa.



TCPdump collect de ISE que captura la autenticación.



Si se observa un problema durante la autenticación, se necesitaría la captura simultánea de paquetes desde el enlace ascendente por cable AP y el lado ISE.

Comando de depuración para AP:

#debug ap authentication packet

Información Relacionada

- Soporte técnico y descargas de Cisco
- Configuración de 802.1X en AP con AireOS
- Guía de configuración de 9800 para LSC
- Ejemplo de configuración de LSC para 9800
- Configuración de 802.1X para AP en 9800

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).