Configurar 802.1X em APs para PEAP ou EAP-TLS com LSC

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Diagrama de Rede
Configurar
CA SCEP do Windows Server 2016
Configurar o modelo de certificado e o registro
Configurar o LSC no 9800
Etapas de configuração da GUI do AP LSC
Etapas de configuração do AP LSC CLI
Verificação LSC do AP
Solucionar problemas de provisionamento de LSC
Autenticação 802.1X com fio AP usando LSC
Etapas de Configuração da Autenticação 802.1x com Fio AP
Configuração da GUI de autenticação do AP Wired 802.1x
Configuração CLI de autenticação 802.1x com fio do AP
Configuração do switch de autenticação 802.1x com fio AP
Instalação do Certificado de Servidor RADIUS
Verificação de autenticação AP Wired 802.1x
Solucionar problemas da autenticação 802.1X
Informações Relacionadas

Introdução

Este documento descreve como autenticar pontos de acesso Cisco em suas portas de switch usando métodos 802.1X PEAP ou EAP-TLS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

· Controlador sem fio

- Ponto de acesso
- Switch
- servidor ISE
- Autoridade de certificado.

Componentes Utilizados

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

- Controlador sem fio: C9800-40-K9 executando 17.09.02
- Ponto de acesso: C9117AXI-D
- Switch: C9200L-24P-4G executando 17.06.04
- Servidor AAA: ISE-VM-K9 executando 3.1.0.518
- Autoridade de Certificação: Windows Server 2016

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Se você quiser que seus pontos de acesso (APs) se autentiquem com suas portas de switch usando 802.1X, por padrão eles usam o protocolo de autenticação EAP-FAST, que não exige certificados. Se você quiser que os APs usem o método PEAP-mschapv2 (que usa credenciais no lado do AP, mas um certificado no lado do RADIUS) ou o método EAP-TLS (que usa certificados nos dois lados), é preciso configurar o LSC primeiro. É a única maneira de provisionar um certificado confiável/raiz em um ponto de acesso (e também um certificado de dispositivo no caso de EAP-TLS). Não é possível para o AP fazer PEAP e ignorar a validação do lado do servidor. Este documento aborda primeiro a configuração do LSC e, em seguida, o lado da configuração do 802.1X.

Use um LSC se desejar que sua PKI ofereça melhor segurança, tenha o controle de sua CA (Certificate Authority, autoridade de certificação) e defina políticas, restrições e usos nos certificados gerados.

Com o LSC, o controlador obtém um certificado emitido pela CA. Um AP não se comunica diretamente com o servidor de CA, mas a WLC solicita certificados em nome dos APs de junção. Os detalhes do servidor de autoridade de certificação devem ser configurados no controlador e devem estar acessíveis.

O controlador usa o protocolo SCEP para encaminhar certReqs gerados nos dispositivos para a CA e usa o SCEP novamente para obter os certificados assinados da CA.

O SCEP é um protocolo de gerenciamento de certificados que os clientes PKI e os servidores CA usam para oferecer suporte à inscrição e revogação de certificados. Ele é amplamente usado na Cisco e é suportado por muitos servidores CA. No SCEP, o HTTP é usado como o protocolo de

transporte para as mensagens PKI. O objetivo principal do SCEP é a emissão segura de certificados para dispositivos de rede.

Diagrama de Rede



Configurar

Há duas coisas para configurar principalmente: a CA SCEP e a WLC 9800.

CA SCEP do Windows Server 2016

Este documento aborda uma instalação básica de uma CA SCEP do Windows Server para fins de laboratório. Uma CA do Windows de nível de produção real deve ser configurada de forma segura e apropriada para operações corporativas. Esta seção tem o objetivo de ajudá-lo a testá-la no laboratório, bem como inspirar-se nas configurações necessárias para fazer essa configuração funcionar. Aqui estão as etapas:

Etapa 1.Instale uma nova experiência de desktop do Windows Server 2016.

Etapa 2. Verifique se o servidor está configurado com um endereço IP estático.

Etapa 3.Instale uma nova função e um novo serviço, inicie com os serviços de domínio do Ative Diretory e o servidor DNS.

👝 Se	rver Manager								- 6	×
<	🚵 Add Roles and Features Wizard			-		×	age	Tools	View	Help
Ī	Select server roles			DEST	NATION SERV	/ER OU				
ī	Before You Begin	Select one or more roles to install on the selected s	server.							
	Installation Type	Roles		Description						
Ϊĝ	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 Lightweight Directory Services Device Health Attestation DHCP Server Fax Server DNS Server File and Storage Services (1 of 12 installed) Host Guardian Services Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Web Server (IIS) Windows Deployment Services 	nices ces	Active Directory Doma (AD DS) stores inform objects on the networ this information availa and network administ uses domain controlle network users access i resources anywhere o through a single logor	in Services ation about k and make ble to users rators. AD D rs to give to permittee n the netwo n process.	s ; IS I rk			Hid	e
es .		< Previous	Next >	Install	Cance	I				
		Events	1 Events							
		Performance	5 Services	s						
		BPA results	Perform	nance						
			BPA res	ults						
				10/10/2022 11/26 AI	4					

Instalação do Ative Diretory

🝙 Se	erver Manager								- 0	×
(ᡖ Add Roles and Features Wizard	1		-		×	age	Tools	View	Help
	Installation progr	ress		DESTINA WIN-3	TION SER E2O2T1QI	VER DOU				^
ī	Before You Begin	View installation progress								
Ē	Installation Type	i Feature installation								
i ji i	Server Selection									
<u>e</u>	Server Roles	Configuration required. Installation su	cceeded on WIN-3E2O2T1QD0U.							
Ē	Features	Active Directory Domain Services				^				
	DNS Server	Additional steps are required to make th	is machine a domain controller.							
	AD DS	DNS Server								
	Confirmation	Group Policy Management								
	Results	Remote Server Administration Tools								
		Role Administration Tools								
		AD DS and AD LDS Tools							Hid	e
		Active Directory module for	r Windows PowerShell				-			
		AD DS Tools				~				
		You can close this wizard without inte	rrupting running tasks. View task pro	ogress or o letails.	open thi	s				
		Export configuration settings								
		export configuration settings								
		< Pr	evious Next > Cla	ose	Cance	el				
		Events	Events				-			
		Services	Services							
		Performance	Performance							
		BPA results	BPA results							
										~

Fim da instalação do AD

Etapa 4.Depois de concluir, clique em no painel em Promover este servidor a um controlador de domínio.

📥 Server Manager				-	o x
Server M	lanager • Dashboard	- © 🍢	Manage 1	Tools View	Help
Dashboard	WELCOME TO SERVER MANAG	Post-deployment Configuration Configuration Configuration required for Active Directory Domain			
All Servers	1 C	Services at WIN-3E2O2T1QD0U Promote this server to a domain controller			
B DNS	QUICK START	i Feature installation			
File and Storage Services	3	Configuration required. Installation succeeded on WIN-3E2O2T1QD0U. Add Roles and Features			
	WHAT'S NEW 4	Task Details			
	c .	Connect this conver to cloud convices			

Configurar os serviços do AD

Etapa 5.Crie uma nova floresta e escolha um nome de domínio.

👝 Sei	rver l	Ma	ana	aq	er

📥 Active Directory Domain Service	s Configuration Wizard				-		×
Active Directory Domain Service 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:	ation to an existing d existing forest tion for this oper my	omain ration rdomain.loca		TA WIN-3	RGET SEI	X RVER 2DOU
	More about deployment co	nfigurations < Previor	us Next >	Insta	11	Cance	el

Escolher um nome de floresta

Etapa 6. Adicione a função Serviços de certificado ao servidor:

📥 Server Manager							- 1) ×
Ser Ser	ver Manager • Das	hboard •	B	I 🗗	Manage	Tools	View	Help
Dashboard Local Server	WELCOME TO SE	RVER MANAGER						
All Servers	🔁 Add Roles and Features Wizard				-		×	
 AD DS DNS File and Storage Ser 	Select server role	S		WIN	DESTIN -3E2O2T1QD0U.i	IATION SER\ nydomain.lo	/ER ical	
	Before You Begin Installation Type Server Selection Server Roles	Select one or more roles to install on the selected server. Roles Image: Construction of the selected server. Roles Relevant of the selected server. Image: Construction of the selected server. Relevant of the selected server. Image: Construction of the selected server. Relevant of the selected server. Image: Construction of the selected server. Relevant of the selected server. Image: Construction of the server. Relevant of the selected server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server. Relevant of the server. Image: Construction of the server.	^	Description Active Dire (AD CS) is	on rectory Certific s used to creat	ate Servici	25	
	Features AD CS Role Services Confirmation	 Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server (Installed) 		certificati role servi and mana variety of	on authorities ces that allow age certificates applications.	and relate you to issu s used in a	d Je	de

Adicionar serviços de certificado



Adicionar apenas a autoridade de certificação

Etapa 7.Depois de concluir, configure sua autoridade de certificação.

Image: Configuration Image: Configuration Image: Config	age Tools View Help
Image: Dase in Loc DESTINATION SERVER Image: Loc Image: Loc Image: All credentials Select Role Services to configure Image: All credentials Setup Type Image: All credentials Certification Authority Image: All credentials Online Responder Image: File Private Key	- D X
Cryptography Certificate Enrollment Web Service Certificate Database Confirmation Progress Results More about AD CS Server Bales	DESTINATION SERVER QD0U.mydomain.local main.local. n the destination
< Previous Next > Configure Cancel	

Etapa 8. Escolha CA Corporativa.



CA Corporativa

Etapa 9.Torne-a uma CA raiz. Desde o Cisco IOS XE 17.6, CAs subordinadas são suportadas para LSC.



Escolher uma CA Raiz

É importante que a conta que você usa para sua autoridade de certificação faça parte do grupo IIS_IUSRS. Neste exemplo, você usa a conta Administrador e vai para o menu Usuários e Computadores do Ative Diretory para adicionar os usuários Administrador ao grupo IIS_IUSRS.

🚘 Server Manager			– 0 ×
Server Manager	er • Dashboard	- 🕄 📕 Manage	Tools View Help
 Active Directory Users and File Action View Help All Serv AD CS AD DS DNS File and Sile and IIS All Service Action Computers Computers Domain Controllers ForeignSecurityPrind Managed Service Action 	Administrator Properties Remote control Remote Desktop Services Profile General Address Account Profile Telephones Member Of Dial-in Environment Member of:	? X COM+ Organization Sessions Sessions roup unless compliant Help Next > Configure Cancel ults	Hide
🖬 🔎 🗆 😂 📑 🖶	2	~ 🖫	d _≥ ENG 10:47 PM BEER 10/19/2023

Adicione sua conta de administrador ao grupo IIS_USER

Etapa 10.Depois que você tiver um usuário no grupo do IIS correto, adicione funções e serviços. Em seguida, adicione o Respondente Online e os serviços NDES à sua Autoridade de Certificação.

Ø X



Instalar o NDES e os serviços de respondente online

Etapa 11.Depois de concluído, configure esses serviços.



Instalar o Respondente Online e o serviço NDES

Etapa 12.Você será solicitado a escolher uma conta de serviço. Esta é a conta que você adicionou anteriormente ao grupo IIS_IUSRS.



Selecione o usuário que você adicionou ao grupo IIS

Etapa 13.Isso é suficiente para operações SCEP, mas para obter a autenticação 802.1X, você também precisa instalar um certificado no servidor RADIUS. Portanto, para facilitar, instale e configure o serviço de inscrição na Web para poder copiar e colar facilmente a solicitação de certificado ISE em nosso Windows Server.



Instalar o serviço de registro na Web

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

configurar o serviço de registro na web

Etapa 14. Você pode verificar se o serviço SCEP está operando corretamente visitando <u>http://<serverip>/certsrv/mscep/mscep.dll</u>:

S Network Device Enrollment Servic × +
$\leftarrow \rightarrow C$ (1) No seguro 172.16.80.8/certsrv/mscep/mscep.dll \Rightarrow (1) :
Network Device Enrollment Service
Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).
This URL is used by network devices to submit certificate requests.
To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is http://chuu-Win12/CertSrv/mscep_admin
For more information see Using Network Device Enrollment Service.

Verificação do portal SCEP

Etapa 15.

Por padrão, o Windows Server usava uma senha de desafio dinâmico para autenticar solicitações de cliente e de endpoint antes da inscrição no Microsoft SCEP (MSCEP). Isso exige que uma conta de administrador navegue até a GUI da Web para gerar uma senha sob demanda para cada solicitação (a senha deve ser incluída na solicitação).O controlador não é capaz de incluir essa senha nas solicitações que ele envia ao servidor. Para remover este recurso, a chave do Registro no servidor NDES precisa ser modificada:

Abra o Editor do Registro, procure Regedit no menu Iniciar.

Navegue até Computador > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografia > MSCEP > Aplicar senha

Altere o valor de EnforcePassword para 0. Se já for 0, deixe-o como está.

B		Registry Editor		_ 🗆 X
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
— 📜 САТуре		(Default)	REG SZ	(value not set)
		100 EnforcePassword	REG_DWORD	0x0000000 (0)
		, - · · · · · · · · · · · · · · · · · ·		
UseSinglePassword				
- L OID	Ξ			
- Protect				
- Providers				
- Services				
- UserInterface				
CTF				
DataAccess				
DevDiv				
Device Association Framework				2
Dfrg				
DFS				
DHCPMibAgent				
DirectDraw				
DirectInput				
DirectPlay8				
DirectPlayNATHelp	\sim			
< 111 >		<	Ш	>
Computer\HKEY_LOCAL_MACHINE\	OFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword .

Defina o valor de Enforcepassword

Configurar o modelo de certificado e o registro

Os certificados e suas chaves associadas podem ser usados em vários cenários para diferentes finalidades definidas pelas políticas de aplicativo no servidor CA. A política de aplicativo é armazenada no campo Uso Estendido de Chave (EKU) do certificado. Esse campo é analisado pelo autenticador para verificar se é usado pelo cliente para a finalidade pretendida. Para certificar-se de que a política de aplicativo apropriada esteja integrada aos certificados WLC e AP, crie o modelo de certificado apropriado e mapeie-o para o registro NDES:

Etapa 1. Navegue até Start > Administrative Tools > Certification Authority.

Etapa 2. Expanda a árvore de pastas do servidor CA, clique com o botão direito do mouse nas pastas Modelos de certificado e selecione Gerenciar.

Etapa 3. Clique com o botão direito do mouse no modelo de certificado Users e selecione Duplicate Template no menu de contexto.

Etapa 4. Navegue até a guia Geral, altere o nome do modelo e o período de validade conforme

desejado e deixe todas as outras opções desmarcadas.

A Cuidado: quando o período de Validade for modificado, verifique se ele não é maior que a validade do certificado raiz da Autoridade de Certificação.

Properties of New Template

X

Subject Name	Sen	ver	Issuance Re	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:	Active Dir ally reenro	Renewa 6	l period: weeks ✓	xists in Active
OK		Cancel	Apply	Help

Etapa 5. Navegue até a guia Nome do assunto, certifique-se de que Suprimento na solicitação esteja selecionado. Um pop-up aparece para indicar que os usuários não precisam de aprovação do administrador para obter seu certificado assinado. Selecione OK.



Fornecimento na Solicitação

Etapa 6. Navegue até a guia Extensions, selecione a opção Application Policies e selecione o botão Edit.... Certifique-se de que Client Authentication esteja na janela Application Policies; caso contrário, selecione Add e adicione-a.

Properties of New Template						x	
		-			_		
Compatibility	General	Request	Handling	Cryptograph	y	Key Attestation	
Subject N	lame	Ser	ver	Issuance Requirements			
Supersec	ded Templa	tes	Exte	ensions		Security	
To modify an	n extension,	select it,	and then c	lick Edit.			
Extensions in Applicat	ion Policies	bis templa	te:				
Edit Application Policies Extension							
An application policy defines how a certificate can be used.							
Application p Client Author Encrypting Secure Ema	oolicies: entication File System iil				[Edit	

Verificar extensões

Passo 7. Navegue até a guia Segurança, certifique-se de que a conta de serviço definida na Etapa 6 de Ativar serviços SCEP no Windows Server tenha permissões de Controle Total do modelo e selecione Aplicar e OK.

Properties of New Template

X

Subject N	Vame	Server	ver lesuance		equirements
Superse	ded Templa	tes	Extensions Security		Security
Group or un					
da Author	er names.				
R Adminis	trator	ins.			
S. Domain	n Admins (C	HUU-DOMAIN	N\Dom	ain Admins)	
Se Domain	Users (CH	UU-DOMAIN	Domai	n Users)	
Senterpr	ise Admins	(CHUU-DOMA	AIN\En	terprise Admins)	
				Add	Remove
					B
ennissions	for Adminis	trator		Allow	Deny
Full Contro	for Adminis ol	trator		Allow	Deny
Full Contro Read	for Adminis ol	trator		Allow	Deny
Full Contro Read Write	for Adminis	trator		Allow	Deny
Full Contro Read Write Enroll	for Adminis	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 V V V V	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis	trator		Allow V V V V	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol l	or advanced s	settings	Allow	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol	or advanced s	settings	Allow	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol	or advanced s	settings	Allow	Deny
Full Contro Read Write Enroll Autoenrol	for Adminis ol	or advanced s	settings	Allow	Deny

Etapa 8. Retorne à janela Autoridade de certificação, clique com o botão direito do mouse na pasta Modelos de certificado e selecione Novo > Modelo de certificado a ser emitido.

Etapa 9. Selecione o modelo de certificado criado anteriormente, neste exemplo é 9800-LSC, e selecione OK.

Observação: o modelo de certificado recém-criado pode demorar mais para ser listado em várias implantações de servidor, pois precisa ser replicado em todos os servidores.

E	Enable Certificate Templates	X
Select one Certificate Template to Note: If a certificate template that information about this template has All of the certificate templates in th For more information, see Cert	enable on this Certification Authority. was recently created does not appear on this list, you may need to wait us been replicated to all domain controllers. e organization may not be available to your CA. <u>tificate Template Concepts.</u>	ntil
Name	Intended Purpose	~
@ 9800-LSC	Client Authentication, Secure Email, Encrypting File System	
CA Exchange	Private Key Archival	
Code Signing	Code Signing	=
Cross Certification Authority	<al></al>	
Renrolment Agent	Certificate Request Agent	
Renrolment Agent (Computer)	Certificate Request Agent	
Rechange Signature Only	Secure Email	
Exchange User	Secure Email	
@ IPSec	IP security IKE intermediate	
Key Recovery Agent	Key Recovery Agent	
OCSP Response Signing	OCSP Signing	~
	ОК	Cancel

Escolha o modelo

O novo modelo de certificado está listado agora no conteúdo da pasta Modelos 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 9800-LSC Authenticated Session Exchange Enrollment Agent (Offline r IPSec (Offline request) CEP Encryption Directory Email Replication Domain Controller Authentication Kerberos Authentication EFS Recovery Agent Basic EFS Domain Controller Web Server Computer User Subordinate Certification Authority Administrator	Intended Purpose Client Authentication, Secure Email, En Client Authentication Certificate Request Agent IP security IKE intermediate Certificate Request Agent Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication Client Authentication Client Authentication Client Authentication Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all></all>	

Selecione o LSC

Etapa 10. Retorne à janela Editor do Registro e navegue para Computador > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografia > MSCEP.

Etapa 11. Edite os registros EncryptionTemplate, GeneralPurposeTemplate e SignatureTemplate para que eles apontem para o modelo de certificado recém-criado.

<i>š</i>	Registry Editor		_ 🗆 🗙
File Edit View Favorites Help			
File Edit View Favorites Help Defaults Defaults Defaults MSCEP CAType CertsInMYStore Defaults CertsInMYStore EnforcePassword Defaults View Favorites EnforcePassword Defaults View Favorites EnforcePassword Defaults View Favorites EnforcePassword Defaults View Favorites EnforcePassword Devolut Devolutes View Favorites Devolutes View Favorites View Favorites Devolutes View Favorites View Favorites Devolutes View Favorites View Favorites Devolute Devolute Devolute Devolute Devolute View Favorites Devolute Devolute Devolute Devolute Devolute Devolute	Name (Default) (Defa	Type REG_SZ REG_SZ REG_SZ REG_SZ	Data (value not set) 9800-LSC 9800-LSC 9800-LSC
 ▷ - ↓ DFS ▷ - ↓ DHCPMibAgent ▷ - ↓ DirectDraw ▷ - ↓ DirectInput 	<	111	>
Computer\HKEY_LOCAL_MACHINE\SOFT	WARE\Microsoft\Crypto	ography\MSCEP	

Alterar o Modelo no Registro

Etapa 12. Reinicialize o servidor NDES, então retorne à janela Certification Authority, selecione o nome do servidor e selecione o botão Stop e Play sucessivamente.

b	certsrv - [Certification Authority (Local)\CHU	U-WIN12-CA]	x
File Action View Help <hr/>	▶ ■		
Certification Authority (Local)	Name Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates		

Configurar o LSC no 9800

Aqui estão as etapas na sequência para configurar o LSC para AP no WLC.

- 1. Criar chave RSA. Essa chave é usada posteriormente para o ponto de confiança PKI.
- 2. Crie um ponto confiável e mapeie a chave RSA criada.
- 3. Habilite o provisionamento LSC para APs e mapeie o ponto de confiança.
 - 1. Habilite o LSC para todos os APs associados.
 - 2. Habilitar LSC para APs selecionados através da lista de provisionamento.
- 4. Altere o ponto confiável de gerenciamento sem fio e aponte para o ponto confiável LSC.

Etapas de configuração da GUI do AP LSC

Etapa 1.Navegue até Configuration > Security > PKI Management > Key Pair Generation.

- 1. Clique em adicionar e atribua a ele um nome relevante.
- 2. Adicione o tamanho da chave RSA.
- 3. A opção de chave exportável é opcional. Isso só é necessário se você quiser exportar a chave fora da caixa.
- 4. Selecione Gerar

Q Search Menu Items	Configuration • > Security •	> PKI Ma	nagement		
Dashboard	Trustpoints CA Server	Key Pair G	Add Ce	ertificate Trustp	lool
Monitoring	+ Add				
Configuration	> Key Name T	Key Y Type	Key Y Exportable Zeroize	Key Name*	AP-SCEP
~	TP-self-signed-2147029136	RSA	No 🗎 Zero		
O Administration	> 9800-40.cisco.com	RSA	No 🗎 Zero	Key Type*	● RSA Key ○ EC Key
C Licensing	TP-self-signed- 2147029136.server	RSA	No 🔒 Zero	Modulus Size*	2048
	CISCO_IDEVID_SUDI	RSA	No 🗎 Zero		
X Troubleshooting	CISCO_IDEVID_SUDI_LEGACY	RSA	No 🗟 Zero	Key Exportable*	
	H 1 ⊨ H [10 🔻	1 - 5 of 5 items	Cancel	✓ Generate
Walk Me Through >					

Etapa 2. Navegue até Configuration > Security > PKI Management > Trustpoints

- 1. Clique em adicionar e atribua a ele um nome relevante.
- 2. Insira o URL de inscrição (aqui o URL é <u>http://10.106.35.61:80/certsrv/mscep/mscep.dll</u>) e o restante dos detalhes.
- 3. Selecione os pares de chaves RSA criados na etapa 1.
- 4. Clique em Authenticate.
- 5. Clique em registrar ponto confiável e insira uma senha.
- 6. Clique em Aplicar ao dispositivo.

Q Search Menu Items	Configuration * > Se	curity * > PKI Management		
Dashboard	Add Trustpoint			×
	Label*	Access_Point-MS-CA	Enrollment Type	SCEP () 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*			
	່ ບ Cancel			Apply to Device

Etapa 3.Navegue até Configuration > Wireless > Access Points. Role para baixo e selecione Provisionamento LSC.

- 1. Selecione o status como habilitado. Isso ativa o LSC para todos os APs que estão conectados a esta WLC.
- 2. Selecione o nome do ponto confiável que criamos na Etapa 2.

Preencha o restante dos detalhes de acordo com suas necessidades.

Q. Search Menu Items	Configuration * > Wireless * > Access Points				
🚃 Dashboard	 All Access Points 				
	Total APs : 1		Miscore Tag : (Ingured APs 0 Country Dode : 0 LSC Failback : 0	Select an Action 👻
	AP Name E AP Model	Admin : Slots : Status Up Time : IP Ad	dress : Base Radio MAC : Ethen	AP : Power Derate net MAC : Mode Capable	i Operation i Config Status Status
{Ô} Administration →	AP0CD0-F89A-46E0 4 M C9117AXI-D	2 O days 0 hrs 26 10.10 mins 42 secs	5.101.158 d0ec.3579.0300 0cd0.	189a.46e0 Local Yes	Registered Healths
(2) Licensing	H 4 1 F H 10 V				1 - 1 of 1 access points
X Traubleshooting	> 6 GHz Radios				
	> 5 GHz Radios				
	> 2.4 GHz Radios				
	> Dual-Band Radios				
	> Country				
	V LSC Provision				
	Status	Enabled •	Subject Name Parameters		E Apply
	Trustpoint Name	Access_Point-MS # +	Country	IN	
	Number of Join Attempts	3	State	КА	
	Key Size	2048 👻	City	Bengaluru	
	Certificate chein status	Not Aveilable	Organization	TAC	

Depois de habilitar o LSC, os APs baixam o certificado via WLC e reinicializam. Na sessão de console do AP, você verá algo como esse snippet.

[*09/25/2023 10:03:2	8.8993]
[+09/25/2023 10:03:2	8.7016]
[+09/25/2023 10:03:2	(8.7663) writing new private key to '/tmp/lsc/priv_key'
[+09/25/2023 10:03:2	8.7666]
[+09/25/2023 10:03:2	8.9212] LSC_ENABLE: saving ROOT_CERT
[+09/25/2023 10:03:2	8-9212]
[+09/25/2023 10:03:2	8.9293] LSC_ENABLE: saving DEVICE_CERT
[+09/25/2023 10:03:2	8,9293]
[+09/25/2023 10:03:2	8.9635] LSC certs and private key verified
[+09/25/2023 10:03:2	8,9635]
[+09/25/2023 10:03:2	9.4997] LSC private key written to hardware TAM
[+09/25/2023 10:03:2	9.4997]
[*09/25/2023 10:03:2	9.5526] A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed

Etapa 4.Quando o LSC estiver habilitado, você poderá alterar o certificado de Gerenciamento sem fio para corresponder ao ponto confiável do LSC. Isso faz com que os APs se unam com seus certificados LSC e a WLC use seu certificado LSC para junção de AP. Esta é uma etapa opcional se seu único interessado for fazer a autenticação 802.1X de seus APs.

- 1. Vá para Configuration > Interface > Wireless e clique em Management Interface.
- 2. Altere o ponto confiável para corresponder ao ponto confiável criado na etapa 2.

Isso conclui a parte de configuração da GUI do LSC. Os APs devem poder se unir à WLC usando o certificado LSC agora.



Etapas de configuração do AP LSC CLI

1. Crie uma chave RSA usando 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 storag Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported

2. Crie um ponto de confiança PKI e mapeie o par de chaves RSA. Insira o URL de inscrição e o restante dos detalhes.

```
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 registre o ponto de confiança PKI com o servidor de CA usando o comando crypto pki authenticate <trustpoint>. Digite uma senha no prompt de senha.

```
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 a junção de AP com o 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. Altere Wireless Management Trustpoint (Ponto confiável de gerenciamento sem fio) para corresponder ao ponto confiável criado acima.

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

Verificação LSC do AP

Execute esses comandos no WLC para verificar o 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#
```



Depois que os APs forem recarregados, faça login na CLI do AP e execute esses comandos para verificar a configuração do 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:
```

APBCDB:RB9A.46E0#sho crypto in LSC LSC: Enabled APBCDB:RB9A.46E0#sho canwan cli config in lsc APB Lsc enable : 1 AP lsc reboot cnt : 0 AP lsc max num of retry : 10 AP lsc mode : 0x1 AP lsc dtls fallback state : 0 APBCDB:RB9A.46E0# Read timed out
AP0CD0.F89A.46E0#sho dtls connections
Number of DTLS connection = 1 [ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version
[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2
Current connection certificate issuer name: sumans-lab-ca

Solucionar problemas de provisionamento de LSC

Você pode fazer uma captura EPC da porta do switch de uplink da WLC ou do AP para verificar o certificado que o AP está usando para formar o túnel CAPWAP. Verifique a partir do PCAP se o túnel DTLS foi criado com êxito.



As depurações de DTLS podem ser executadas no AP e no WLC para entender o problema do certificado.

Autenticação 802.1X com fio AP usando LSC

O AP é configurado para usar o mesmo certificado LSC para se autenticar. O AP atua como solicitante 802.1X e é autenticado pelo switch no servidor ISE. O servidor ISE conversa com o AD no back-end.



Observação: depois que a autenticação dot1x é habilitada na porta do switch de uplink do AP, os APs não podem encaminhar ou receber nenhum tráfego até que a autenticação seja passada. Para recuperar APs com autenticação malsucedida e obter acesso ao AP, desabilite a autenticação dot1x na porta do switch com fio do AP.

Fluxo de trabalho de autenticação e troca de mensagens EAP-TLS



Etapas de Configuração da Autenticação 802.1x com Fio AP

- 1. Ative a autenticação de porta dot1x junto com CAPWAP DTLS e selecione o tipo de EAP.
- 2. Crie credenciais dot1x para APs.
- 3. Ative dot1x na porta do switch.
- 4. Instale um certificado confiável no servidor RADIUS.

Configuração da GUI de autenticação do AP Wired 802.1x

- 1. Navegue até o perfil de junção AP e clique no perfil.
 - 1. Clique em AP > Geral. Selecione o tipo de EAP e o tipo de autorização de AP como "CAPWAP DTLS + dot1x port auth".
 - 2. Navegue para Gerenciamento > Credenciais e crie um nome de usuário e uma senha para a autenticação dot1x do AP.

Cisco Cat	talyst 9800-40 Wireless Controller		Welcome admin 🛛 🐐 🌾 🛕 🖺 🏟 🕅 🕢 📿	Search APs and Clients (Q) EFeedback 2 (P)
Q. Search Manu Items	Configuration * > Tags & Profiles * > AP Join		Edit AP Join Profile General Client CAPWAP AP Management Se	x ecurity ICap QoS
Dashboard Monitoring	AP Join Profile Name	▼ Des	General Power Management Hyperlocation AP Statis	Client Statistics Reporting Internal
	APG_test tostSito		Switch Flag	5 GHz (soc) 90
(⊙) Administration → (©) Licensing	APQ_3rd-Fir-APs APQ_4th-Fir-APs		Power Injector State Power Injector Type Unknown	2.4 GHz (sec) 90 Extended Module
💥 Troubleshooting	APG_6hr-Fk-APs APG_7hr-Fk-APs APG_7hr-Fk-APs APG_8hr-Fk-APs		AP EAP Auth Configuration	Enable Mesh
Walk Me Through 2	APG_11th-Fir-APs APG_12th-Fir-APs		EAP Type EAP-TLS AP Authorization Type CAPVAP DTLS + DDT+ CAPVAP DTLS + DDT+ CAPVAP DTLS +	Profile Name default-mesh-pro • Clear
	H 4 1 2 3 * H 10 *		COTTX port auth CAPWAP DTLS Dottx port auth	
			"D Cancel	C Update & Apply to Device

Cisco Ca	talyst 9800-40 Wireless Controller	Welcome admin		Scenth Arts and Clents Q Second and Readback & Second
Q. Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile		×
Dashboard	🔆 + Add 🛛 × Delete 🔞 Done	General Client CAP	WAP AP Management S	iecurity ICap QoS
	AP Join Profile Name	Des		
Monitoring >	ap-auth	Dot1x Credentials		
🗞 Configuration 🔷 🔸	APG_test	Dot1x Username	ap-wired-user	
중 Administration >	testSite	Dot1x Password		
\$ •	APG_3rd-Fir-APs	Dot1x Password Type	clear •	
(c) Licensing	APG_4th-Fr-APs			
💥 Troubleshooting	APG_6th-FF-APs			
	APO_705-FP-APs			
	APG_UIN-P-949			
	APG_10trives			
Walk Me Through >				
				1
				1
		Cancel		Update & Apply to Device

Configuração CLI de autenticação 802.1x com fio do AP

Use estes comandos para ativar o dot1x para APs a partir da CLI. Isso só permite a autenticação com fio para APs que estão usando o perfil de junção 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
```

Configuração do switch de autenticação 802.1x com fio AP

Essas configurações de switch são usadas no LAB para ativar a autenticação com fio do AP. Você pode ter configurações diferentes com base no design.

```
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
```

Instalação do Certificado de Servidor RADIUS

A autenticação ocorre entre o AP (que está atuando como o solicitante) e o servidor RADIUS. Ambos devem confiar um no outro certificado. A única maneira de fazer com que o AP confie no certificado do servidor RADIUS é fazer com que o servidor RADIUS use uma taxa de certificação emitida pela CA SCEP que também emitiu o certificado do AP.

No ISE, vá para Administração > Certificados > Gerar solicitações de assinatura de certificado

Gere um CSR e preencha os campos com as informações do nó do ISE.

Cisco ISE

Administration · System

Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings				
0	Cartificate Signing Request				
Certificate Management V	Certificate Signing Request				
System Certificates	Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:				
Trusted Certificates	ISE Identity Certificates:				
OCSP Client Profile	Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication				
Certificate Signing Requests	Admin - Server Authentication				
Certificate Periodic Check Se	EAP automication - Server Automication				
	UL3 Automnication - server Automnication Portal - Searce Automnication				
Certificate Authority	solution of the substantial device and the second device of the second device of the second device and the second device of the se				
Genuncate Automy /	SAML - SAML Signing Certificate				
	ISE Messaging Service - Generate a Signing Certificate or generate a brand new Messaging Certificate.				
	Data Connect Certificate - Connect to Oracle Database				
	ISE Certificate Authority Certificates:				
	ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.				
	ISE Intermediate CA - This is an Intermediate CA Signing Request.				
	Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.				
	Usage				
	Certificate(s) will be used for EAP Authentication				
	Allow Wildcard Certificates				
	Node(s)				
	Generate CSR's for these Nodes:				
	Node CSR Friendly Name				
	SE99 ISE99 ISE99IIEAP Authentication				
	Subject				
	Common Name (CN) \$FQDN\$				
	Organizational Unit (OLD				
	e-Buildingenoung eine ferol.				
	Organization (O)				
	O.				
	City (L)				
	State (ST)				

Depois de gerada, você também pode exportá-la e copiá-la e colá-la como texto.

Navegue até o endereço IP da CA do Windows e adicione /certsrv/ à URL

Clique em Solicitar um certificado



For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

Clique em Submit a certificate request by using a base-64



Cole o texto CSR na caixa de texto. Escolha o modelo de certificado do servidor Web.

← C ▲ Non sécurisé 192.168.1.98/certsrv/certrgxt.asp
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 centificate request (CMC or PKCS #10 or PKCS #7):
Certificate Template: [No templates found]) >
Additional Attributes:

Você pode instalar este certificado no ISE voltando ao menu Certificate Signing Request e clicando em Bind certificate. Em seguida, você pode carregar o certificado obtido do Windows C.

≡ Cisco ISE	Administration · System			
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings			
Certificate Management ~ System Certificates	Certificate Signing Requests			
Trusted Certificates OCSP Client Profile	Generate Certificate Signing Requests (CSR)			
Certificate Signing Requests	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 Periodic Check Se	Q View 🗈 Export 🚦 Delete Bind Certificate			
Certificate Authority >	Erriendly Name Certificate Subject Key Length Portal gro Timestamp \wedge Host			
	ISE99#EAP Authentication CN=ISE99.mydomain.local 4096 Mon, 30 Oct 2023 ISE99			

Verificação de autenticação AP Wired 802.1x

Aceite o acesso do console ao AP e execute o comando:

#show ap authentication status

A autenticação do aplicativo não está habilitada:

APOCD0.F89A.46E0#sho ap authentication statu: AP dotlx feature is disabled. Registros de console do AP após ativar a autenticação do 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 com êxito:



Verificação de WLC:



Pós-autenticação bem-sucedida do status da interface da porta do switch:

ch#sho authenticatio	n sessions inte	rface gi Method	gabitEth Domain	ernet 1/0/2 Status Fo	Session TD
19/2	8cd9, f89a, 45e9	dot1x	DATA	Auth	976569848888885CCEED8ERE

Este é um exemplo de registros de console de AP indicando uma autenticação bem-sucedida:

```
[*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 da autenticação 802.1X

Pegue o PCAP no uplink do AP e verifique a autenticação radius. Aqui está um trecho da autenticação bem-sucedida.



Coleta de despejo TCP do ISE capturando a autenticação.



Se houver um problema observado durante a autenticação, será necessária a captura simultânea de pacotes do uplink com fio do AP e do lado do ISE.

Comando de depuração para AP:

#debug ap authentication packet

Informações Relacionadas

- Suporte técnico e downloads da Cisco
- <u>Configurando 802.1X em AP com AireOS</u>
- Guia de configuração do 9800 para LSC
- <u>Exemplo de configuração de LSC para 9800</u>
- <u>Configure 802.1X para APs no 9800</u>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.