LSCを使用したPEAPまたはEAP-TLS用のAPで の802.1Xの設定

<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>ネットワーク図</u>
<u>設定</u>
Windows Server 2016 SCEP CA
<u>証明書テンプレートとレジストリの設定</u>
<u>9800でのLSCの設定</u>
<u>AP LSC GUIの設定手順</u>
<u>AP LSC CLIの設定手順</u>
<u>AP LSCの検証</u>
<u>LSCプロビジョニングのトラブルシューティング</u>
<u>LSCを使用したAP有線802.1X認証</u>
<u>AP有線802.1x認証の設定手順</u>
<u>APの有線802.1x認証GUI設定</u>
<u>APの有線802.1x認証のCLI設定</u>
<u>AP有線802.1x認証スイッチの設定</u>
<u>RADIUSサーバ証明書のインストール</u>
<u>AP有線802.1x認証の検証</u>
<u>802.1X認証のトラブルシューティング</u>
<u>関連情報</u>

はじめに

このドキュメントでは、802.1X PEAPまたはEAP-TLS方式を使用して、スイッチポートでシスコのアクセスポイントを認証する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

・ ワイヤレス コントローラ

- ・ アクセス ポイント
- 最大 300 のアクセス ポイント グループ
- ・ ISEサーバ
- 認証局.

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ ワイヤレスコントローラ: 17.09.02を実行するC9800-40-K9
- アクセスポイント: C9117AXI-D
- スイッチ: 17.06.04が稼働するC9200L-24P-4G
- AAAサーバ: 3.1.0.518を実行するISE-VM-K9
- 認証局: Windows Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

アクセスポイント(AP)を802.1Xを使用してスイッチポートで認証する場合、デフォルトでは、証 明書を必要としないEAP-FAST認証プロトコルが使用されます。APでPEAP-mschapv2方式 (AP側ではクレデンシャルを使用するが、RADIUS側では証明書を使用)またはEAP-TLS方式 (両側で証明書を使用)を使用する場合、最初にLSCを設定する必要があります。これは、信頼 できる/ルート証明書をアクセスポイント(およびEAP-TLSの場合はデバイス証明書)にプロビジ ョニングする唯一の方法です。APがPEAPを実行して、サーバ側の検証を無視することはできま せん。このドキュメントでは、最初にLSCの設定について説明し、次に802.1Xの設定側について 説明します。

PKIでセキュリティを強化し、認証局(CA)を制御し、生成された証明書に対してポリシー、制限 、および使用法を定義する場合は、LSCを使用します。

LSCを使用すると、コントローラはCAによって発行された証明書を取得します。APはCAサーバ と直接通信しませんが、WLCは参加しているAPに代わって証明書を要求します。CAサーバの詳 細は、コントローラ上で設定し、アクセス可能である必要があります。

コントローラは、Simple Certificate Enrollment Protocol(SCEP)を使用して、デバイスで生成され たcertReqsをCAに転送し、再度SCEPを使用してCAから署名付き証明書を取得します。

SCEPは、PKIクライアントとCAサーバが証明書の登録と失効をサポートするために使用する証 明書管理プロトコルです。これはシスコで広く使用されており、多くのCAサーバでサポートされ ています。SCEPでは、PKIメッセージのトランスポートプロトコルとしてHTTPが使用されます 。SCEPの主な目標は、ネットワークデバイスへの証明書のセキュアな発行です。

ネットワーク図



設定

主に設定する項目は、SCEP CAと9800 WLCの2つです。

Windows Server 2016 SCEP CA

このドキュメントでは、ラボでのWindows Server SCEP CAの基本的なインストールについて説 明します。実際の実稼働グレードのWindows CAは、企業運用に合わせて安全かつ適切に設定す る必要があります。このセクションは、ラボでテストし、この設定を機能させるために必要な設 定から着想を得ることを目的としています。内容は次のとおりです。

ステップ1:新しいWindows Server 2016デスクトップエクスペリエンスをインストールします。

ステップ2:サーバにスタティックIPアドレスが設定されていることを確認します。

手順3:新しい役割とサービスをインストールし、Active DirectoryドメインサービスとDNSサーバから開始します。

Ē X



Active Directoryのインストール

🝙 Se	erver Manager								- 0	×
	🚘 Add Roles and Features Wizard	1		-		×	age	Tools	View	Help
122	Installation progr	ess		DESTINA WIN-3	TION SER	VER DOU				^
i	Before You Begin	View installation progress								
	Installation Type	 Feature installation 								
i i i	Server Selection									
Ē	Server Roles	Configuration required. Installation su	cceeded on WIN-3E2O2T1QD0U.							
Ēr	Features	Active Directory Domain Services				^				
	DNS Server	Additional steps are required to make the Promote this server to a domain control	is machine a domain controller. ller							
	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 fo	r Windows PowerShell							
		AD DS Tools				~				
		You can close this wizard without inte	errupting running tasks. View task pro	ogress or o	open this	s				
		page again by clicking Notifications	n the command bar, and then Task D	etalls.						
		Export configuration settings								
		< Pr	evious Next > Cl	ose	Cance	el				
		Events	Events							
		Services	Services							
		Performance	Performance							
		BPA results	BPA results							
			birit could							
										~

ADインストールの終了

ステップ4:完了したら、「Promote this server to a domain controller(このサーバをドメインコン トローラに昇格させる)」のダッシュボードをクリックします。

🚘 Server Manager			- D	×
Server M	lanager • Dashboard	- © 🍢	Manage Tools View Hel	p
🔛 Dashboard	WELCOME TO SERVER MANAGE	Post-deployment Configuration Configuration required for Active Directory Domain		
Local Server All Servers	1 0	Services at WIN-3E2O2T1QD0U Promote this server to a domain controller		
DNS	QUICK START	Feature installation		
■File and Storage Services ▷	3	Configuration required. Installation succeeded on WIN-3E2O2T1QD0U. Add Roles and Features		
	WHAT'S NEW 4	Task Details		
	E	Connect this converte cloud convices	-	

ADサービスの設定

ステップ5:新しいフォレストを作成し、ドメイン名を選択します。

	-					
re-	Se	rve	r M	an	ag	er

(4	📥 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	s Configuration Wizard iguration Select the deployment operation Add a domain controller to an exis Add a new domain to an existing Add a new forest Specify the domain information for the Root domain name:	sting domain forest is operation mydomain.loca	V	TAR VIN-3E	GET SEF 202TIQ	X
		More about deployment configuratio	Previous Next >	Install		Cance	1
		Events	Events				

フォレスト名を選択してください

ステップ6:証明書サービスの役割をサーバに追加します。

	ê	Server	Manager	
--	---	--------	---------	--



0 X

証明書サービスの追加

🚔 Server Manager					-	- ć	
Ser Ser	ver Manager • Dasł	board •	۲ ا چ	Manage	Tools	View	Help
DashboardLocal Server	WELCOME TO SER	/ER MANAGER					_
All Servers	📥 Add Roles and Features Wizard			-		×	
 AD DS DNS File and Storage Ser 	Select role service	S Select the role services to install for Active Directory Certifica	WIN-3E2 ate Services	DESTINA 202T1QD0U.m	ATION SERV lydomain.lo	ER cal	
	Installation Type	Role services	Description				
	Server Selection Server Roles Features AD CS Role Services Confirmation Results	Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	Certification to issue and Multiple CAs public key in	Authority (C manage cer s can be link frastructure	CA) is used tificates. ed to form	i na	de

```
証明機関だけを追加する
```

ステップ7:設定が完了したら、認証局を設定します。

🚔 Server	Manager			– 0 ×
\mathbf{E}	AD CS Configuration			age Tools View Help
Da:	Role Services		DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local	
All AD	Credentials Role Services Setup Type	Select Role Services to configure Certification Authority Certification Authority Web Enrollment		DESTINATION SERVER QD0U.mydomain.local
📷 DN	Private Key Cryptography CA Name Validity Period	Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service		
	Certificate Database Confirmation Progress Recute			n the destination
	(haddia			
		More about AD CS Server Roles	ext > Configure Cancel	ess or open this

ステップ8:エンタープライズCAを選択します。



エンタープライズ CA

ステップ9:ルートCAにする。Cisco IOS XE 17.6以降、下位CAはLSCでサポートされています。

🚖 Server I	Manager		_	o ×
\mathbf{E}	AD CS Configuration		age Tools Vi	iew Help
	СА Туре	DESTINATION SERVER WIN-3E2O2TIQD0U.mydomain.local		
AD AD AD AD AD AD AD AD AD AD AD AD AD A	Credentials Role Services Setup Type CA Type Private Key Cryptography	When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy. Root CA 	DESTINATION SERVER QD0U.mydomain.local	·
	CA Name Validity Period Certificate Database Confirmation Progress Results	Root CAs are the first and may be the only CAs configured in a PKI hierarchy. Subordinate CA Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.	main.local.	ide
		More about CA Type < Previous Next > Configure Cancel Image again by clicking Notifications in the command bar, and then Task De Export configuration settings < Previous Next > Close	ess or open this tails. se Cancel	1
				~

ルートCAの選択

IIS_IUSRSグループに属するCAに使用するアカウントを持つことが重要です。この例では、 Administratorアカウントを使用してActive Directory Users and Computersメニューに移動し、 AdministratorユーザをIIS_IUSRSグループに追加します。

📤 Server Manag	ger						- 0	\times
\odot	Server Manag	ger 🕨 Dashboa	ard		• @ / 3	Manage Tools	View He	elp
 Dashbo Local Se All Serve AD CS AD DS DNS File and IIS 	Active Directory Users and File Action View Help Active Directory Users and (Saved Queries Managed Service Action Managed Service Action Users	Administrator Propertie Remote control General Address Member Of Name A Administrators m Domain Admins m Domain Users m Enterprise Admins m Group Policy Cre m IIS_IUSRS m Schema Admins m Concerning and the second secon	s Remote Desktop Servici Account Profile Tr Dial-in Environr Active Directory Domain Ser mydomain Jocal/Users move main Users There is no need to char you have Macintosh clier applications.	? × es Profile COM+ elephones Organization nent Sessions vices Folder vices Folder nge Primary group unless nts or POSIX-compliant Apply Help Previous Next > BPA results	Configure	Cancel	Hide	
م	□ 🤅 📜	-				へ 記 🔩 EN BEI	G 10:47 PM FR 10/19/2023	2

管理者アカウントをIIS_USERグループに追加します

ステップ10:適切なIISグループにユーザを追加したら、ロールとサービスを追加します。次に、 オンラインレスポンダとNDESサービスを認証局に追加します。

o ×



NDESおよびオンラインレスポンダーサービスのインストール

📥 Server Manager

ステップ11:完了したら、それらのサービスを設定します。



オンラインレスポンダとNDESサービスのインストール

ステップ12:サービスアカウントを選択するように求められます。これは、以前にIIS_IUSRSグル ープに追加したアカウントです。



IISグループに追加したユーザを選択します

ステップ13:これはSCEP操作には十分ですが、802.1X認証を実現するには、RADIUSサーバに 証明書をインストールする必要もあります。したがって、簡単にWeb登録サービスをインストー ルして設定し、ISE証明書要求をWindows Serverに簡単にコピーして貼り付けられるようにしま す。



Web登録サービスのインストール

🔁 AD CS Configuration			-		×
Role Services		WIN-	DESTINA 3E2O2T1QD0U.my	FION SER\ domain.lo	/ER ocal
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 				
	< Previous	Next >	Configure	Cancel	I

web登録サービスの設定

ステップ 14:SCEPサービスが正常に動作していることを確認するには、 <u>http://<serverip>/certsrv/mscep/mscep.dll</u>にアクセスします。

Network Device Enrollment Servic ×	+	L_		X
← → C ③ No seguro 172	.16.80.8/certsrv/mscep/mscep.dll	☆	۲	:
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 <u>http://Chuu-Win12/CertSrv/mscep_admin</u>

For more information see Using Network Device Enrollment Service.

SCEPポータルの検証

ステップ 15:

デフォルトでは、Windows Serverは、Microsoft SCEP(MSCEP)に登録する前に、動的チャレンジ パスワードを使用してクライアントおよびエンドポイントの要求を認証します。これには、管理 者アカウントがWeb GUIを参照して要求ごとにオンデマンドパスワードを生成する必要がありま す(パスワードは要求内に含める必要があります)。コントローラは、サーバに送信する要求に このパスワードを含めることはできません。この機能を削除するには、NDESサーバのレジスト リキーを変更する必要があります。

レジストリエディタを開き、StartメニューでRegeditを検索します。

Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePasswordの順に移動します。

EnforcePasswordの値を0に変更します。すでに0の場合は、そのままにしておきます。

۵¢		Registry Editor		_ 🗆 X
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
——————————————————————————————————————		(Default)	REG SZ	(value not set)
		8 EnforcePassword	REG_DWORD	0x0000000 (0)
		(
- OID	Ξ			
- Protect	_			
- Providers				
- Services				
Data Assess				
DataAccess				
Device Association Framework				
Device Association Flamework				R
DES				
DirectDraw				
DirectInput				
DirectPlay8				
DirectPlayNATHelp	$\overline{}$			
< III >		<	Ш	>
Computer\HKEY_LOCAL_MACHINE\	SOFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword

Enforcepassword値の設定

証明書テンプレートとレジストリの設定

証明書および証明書に関連付けられたキーは、CAサーバ内のアプリケーションポリシーで定義さ れたさまざまな目的で、複数のシナリオで使用できます。アプリケーションポリシーは、証明書 の拡張キー使用法(EKU)フィールドに保存されます。このフィールドは、オーセンティケータに よって解析され、クライアントが目的の目的で使用していることを確認します。適切なアプリケ ーションポリシーがWLCとAPの証明書に確実に統合されるようにするには、適切な証明書テンプ レートを作成し、NDESレジストリにマッピングします。

ステップ1: Start > Administrative Tools > Certification Authorityの順に移動します。

ステップ 2: CA Serverフォルダツリーを展開し、Certificate Templatesフォルダを右クリックして、Manageを選択します。

ステップ 3: Users証明書テンプレートを右クリックし、コンテキストメニューからDuplicate Templateを選択します。

ステップ4:Generalタブに移動し、必要に応じてテンプレート名と有効期間を変更し、他のすべ

▲ 注意:有効期間を変更する場合は、認証局ルート証明書の有効期間を超えないようにしてく ださい。

Properties of New Template

Х

Subject Name	Subject Name Serv			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	l period: weeks ∽	
Do not automatic Directory	Active Dir ally reenro	rectory oll if a dupli	cate certificate e	xists in Active
ОК		Cancel	Apply	Help

ステップ 5: Subject Nameタブに移動し、Supply in the requestが選択されていることを確認しま す。ポップアップが表示され、ユーザが証明書に署名するために管理者の承認を必要としていな いことを示し、OKを選択します。

Properties of New Template				
Compatibility General Request Handling Cryptography Key Attestation				
Superseded Ter	Extensions Securi		Security	
Subject Name Server Issuance Requirements			equirements	
Use subject information from existing certificates for autoenrollment renewal requests (*)				
 Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. 				

要求への入力

手順 6: Extensionsタブに移動し、Application Policiesオプションを選択して、Edit...ボタンを選 択します。Client AuthenticationがApplication Policiesウィンドウにあることを確認します。そう でない場合は、Addを選択して追加します。

Properties of New Template							
Compatibility	General	Request	Request Handling Cryptography Key Attestatio				
Subject N	lame	Ser	ver	Issuance R	lequirements		
Supersec	ded Templa	tes	Exte	nsions	Security		
To modify an	extension,	select it,	and then c	lick Edit.			
Extensions in Applicati	ion Policies	bis templa	te:				
Edit Application Policies Extension							
An application policy defines how a certificate can be used.							
Application policies: Client Authentication Encrypting File System Secure Email							

内線番号の確認

手順 7: Securityタブに移動し、Enable SCEP Services in the Windows Serverのステップ6で定義 したサービスアカウントにテンプレートのFull Control権限が付与されていることを確認し、 ApplyおよびOKを選択します。

Properties of New Template

X

Subject I	Name	Serve	er	Issuance R	equirements
Superse	ded Templa	tes	Exte	nsions	Security
Smill or light names:					
	tionted Llar				
R Adminis	strator	15			
S. Domain	1 Admins (C	HUU-DOM	AIN\Dom	ain Admins)	
Se Domain	users (CH	UU-DOMAI	N\Domai	n Users)	
Se Enterpr	rise Admins	(CHUU-DO	MAIN\En	terprise Admins)	
					_
				Add	Remove
Permissions	for Administ	trator		Allow	Denv
Full Contr	ol			~	
Read				~	
Write				~	
				-	
Enroll				L	
Enroll Autoenrol	I			 Image: A start of the start of	
Enroll Autoenrol					
Enroll Autoenrol					
Enroll Autoenrol	l xermissions	or advance	d settings	s, click	Advanced
Enroll Autoenrol For special p Advanced.	l xermissions	or advance	d settings	s, click	Advanced
Enroll Autoenrol For special p Advanced.	l xermissions	or advance	d settings	s, click	Advanced
Enroll Autoenrol For special p Advanced.	ermissions	or advance	d settings	s, click	Advanced

ステップ 8 : Certification Authorityウィンドウに戻り、Certificate Templatesフォルダを右クリックして、New > Certificate Template to Issueを選択します。

ステップ 9:以前に作成した証明書テンプレート(この例では9800-LSC)を選択し、OKを選択 します。

◆ 注:新しく作成された証明書テンプレートは、すべてのサーバ間で複製する必要があるため、複数のサーバの展開にリストされるまでに時間がかかる場合があります。

Enable Certificate Templates				
elect one Certificate Template to lote: If a certificate template that formation about this template has Il of the certificate templates in th for more information, see <u>Cert</u>	enable on this Certification Authority. was recently created does not appear on this list, you may need to wait until been replicated to all domain controllers. e organization may not be available to your CA. <u>ifficate Template Concepts.</u>			
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>			
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 Response Signing	OCSP Signing	~		
	OK Canc	el		

テンプレートの選択

新しい証明書テンプレートがCertificate Templatesフォルダの内容にリストされます。

🧔 certsrv - [Cer	tification Authority (Local)\CHUU-WIN	V12-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, Server Authentic Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all></all>	

LSCの選択

ステップ 10 : Registry Editorウィンドウに戻り、Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEPの順に移動します。

ステップ 11EncryptionTemplate、GeneralPurposeTemplate、およびSignatureTemplateレジスト リを編集して、新しく作成された証明書テンプレートを指すようにします。



レジストリのテンプレートの変更

ステップ 12NDESサーバをリブートして、Certification Authorityウィンドウに戻り、サーバ名を 選択し、StopとPlayボタンを続けて選択します。

ت م	ertsrv - [Certification Authority (Local)\CHU	IU-WIN12-CA]	- D X
File Action View Help	▶ ■		
CHUU-WIN12-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates	Name Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates		

9800でのLSCの設定

WLCでAPのLSCを設定する手順を次に示します。

- 1. RSAキーを作成します。このキーは、後でPKIトラストポイントに使用されます。
- 2. トラストポイントを作成し、作成したRSAキーをマッピングします。
- APのLSCプロビジョニングを有効にし、トラストポイントをマッピングします。
 1. 加入しているすべてのAPでLSCを有効にします。
 - 2. プロビジョニングリストを使用して、選択したAPのLSCを有効にします。
- 4. ワイヤレス管理トラストポイントを変更し、LSCトラストポイントをポイントします。

AP LSC GUIの設定手順

ステップ1:Configuration > Security > PKI Management > Key Pair Generationの順に移動します。

- 1. Addをクリックし、適切な名前を付けます。
- 2. RSAキーサイズを追加します。
- key exportableオプションはオプションです。これは、キーをエクスポートする場合にのみ 必要です。
- 4. 生成の選択

Dashboard	Trustpoints CA Server	Key Pair	Generation Add Ce	ertificate Trustp	ool
Monitoring ;	+ Add	Key T	Key Y		
Configuration	TD_solf_signed_2147029136	DSA	No R Zeroize	Key Name*	AP-SCEP
Administration	9800-40.cisco.com	RSA	No a Zer	Key Type*	● RSA Key ○ EC Key
icensing	TP-self-signed- 2147029136.server	RSA	No 🖹 Zer	Modulus Size*	2048
	CISCO_IDEVID_SUDI	RSA	No 🗎 Zer	Iniodalido Olizo	
Troubleshooting	CISCO_IDEVID_SUDI_LEGACY	RSA	No 🗎 Zer	Key Exportable*	
	H ← 1 → H [10 🗸	1 - 5 of 5 items	D Cancel	✓ Generate

ステップ2: Configuration > Security > PKI Management > Trustpointsの順に移動します。

- 1. Addをクリックし、適切な名前を付けます。
- 2. 登録URL(URLは<u>http://10.106.35.61:80/certsrv/mscep/mscep.dll</u>)とその他の詳細を入力しま す。
- 3. ステップ1で作成したRSAキーペアを選択します。
- 4. Authenticateをクリックします。
- 5. Enroll trustpointをクリックし、パスワードを入力します。
- 6. Apply to Deviceをクリックします。

Q Search Menu Items	Configuration • > Set	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
© 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

ステップ3:Configuration > Wireless > Access Pointsの順に移動します。下にスクロールして、 LSC Provisionを選択します。

- 1. ステータスとしてenabledを選択します。これにより、このWLCに接続されているすべての APに対してLSCが有効になります。
- 2. ステップ2で作成したトラストポイント名を選択します。

必要に応じて残りの詳細を入力します。

Q. Search Menu Items	Configuration * > Wireless * > Access Points			
Teshboard	 All Access Points 			
Monitoring	Total APs : 1		Misconfigured APs Tag : 0 Country Code : 0	LSC Failback : 0 Select an Action +
🖏 Configuration 🔷 🔸	AP Name E AP Model E	Admin : Slots : Status Up Time : IP Address	Base Radio MAC : Ethernet MAC : Mod	i Power Derate i Operation i Config e Capable Status Status
(Ô) Administration →	AP0CD0-F89A-46E0 4 M C9117AXI-D	2 O days 0 hrs 26 10.105.101.168	d0ec.3579.0300 0cd0.189a.46e0 Loca	Yes Registered Healths
C Licensing	H 4 1 H H 10 V			1 - 1 of 1 access points
💥 Troubleshooting	> 6 GHz Radios			
	> 5 GHz Radios			
	> 2.4 GHz Radios			
	> Dual-Band Radios			
	> Country			
	✓ LSC Provision			
	Status	Enabled v	Subject Name Parameters	E Apply
	Trustpoint Name	Access_Point-MS # +	Country IN	
	Number of Join Attempts	3	State KA	
	Key Size	2048 •	City Bengaluru	
	Certificate chain status	Not Available	Organization TAC	
	Number of certificates on chein	0		

LSCを有効にすると、APはWLC経由で証明書をダウンロードし、リブートします。APコンソー ルセッションで、次のようなスニペットが表示されます。

[*09/25/2023 10:03:28.0993]	
[+09/25/2023 10:03:28.7016]	
[+09/25/2023 10:03:28.7663]	writing new private key to '/tmp/lsc/priv_key'
[+09/25/2023 10:03:28.7666]	
[+09/25/2023 10:03:28.9212]	LSC_ENABLE: saving ROOT_CERT
[+09/25/2023 10:03:28.9212]	
[+09/25/2023 10:03:28.9293]	LSC_ENABLE: saving DEVICE_CERT
[+09/25/2023 10:03:28.9293]	
[+09/25/2023 10:03:28.9635]	LSC certs and private key verified
[+09/25/2023 10:03:28.9635]	
[+09/25/2023 10:03:29.4997]	LSC private key written to hardware TAM
[+09/25/2023 10:03:29.4997]	
[*09/25/2023 10:03:29.5526]	A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed

ステップ4:LSCを有効にすると、LSCトラストポイントと一致するようにワイヤレス管理証明書 を変更できます。これにより、APはLSC証明書を使用して加入し、WLCはAP加入にLSC証明書 を使用します。APの802.1X認証のみを行う場合、これはオプションの手順です。

1. Configuration > Interface > Wirelessの順に選択し、Management Interfaceをクリックします。

2. トラストポイントを、手順2で作成したトラストポイントに一致するように変更します。

これで、LSC GUIの設定の部分は終了です。APは、LSC証明書を使用してWLCに参加できる必要があります。

Q. Search Menu Items	Configuration * > Interface * > Wireless Edit Management Interface *
Dashboard	Add Changing the interface or trustpoint will cause APs to disconnect and disrupt clients.
	Interface Name T Interface Type T VLAN ID T IP Address T IP Netmask
(2) Monitoring →	Want01 Management 101 10.105.101.160 255.255.255. Montage Management I
Configuration	H < 1 > H 10 + Deers of a control of the control of
[ⓒ] Administration >	
(C) Licensing	NAI IMA(IMA) Server Address U.O.O.U
Y Troubleshooting	
	2 Cancel
	Update & Apply to Device

AP LSC CLIの設定手順

1.次のコマンドを使用してRSAキーを作成します。

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. PKIトラストポイントを作成し、RSAキーペアをマッピングします。登録URLと残りの詳細を 入力します。

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.コマンドcrypto pki authenticate <trustpoint>を使用して、PKIトラストポイントを認証し、CAサ ーバに登録します。パスワードプロンプトにパスワードを入力します。

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=9800-4
Serial-number: 5C000001400DD405D77E6FE7F00000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#

4. LSC証明書を使用してAP加入を設定します。

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.ワイヤレス管理トラストポイントを、上記で作成したトラストポイントと一致するように変更します。

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

AP LSCの検証

WLCで次のコマンドを実行して、LSCを確認します。

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





APがリロードされたら、AP CLIにログインし、次のコマンドを実行してLSC設定を確認します。

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

```
APOCD0.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:
```

AP0CD0.F89A.46E0#sho crypto	in LSC	
LSC: Enabled		
AP@CD@.F89A.46E@#sho capwap	cli config in	lsc
AP lsc enable	: 1	
AP lsc reboot cnt	: 0	
AP lsc max num of retry	: 10	
AP lsc mode	: 0×1	
AP lsc dtls fallback state	: 0	
AP0CD0.F89A.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

LSCプロビジョニングのトラブルシューティング

WLCまたはAPアップリンクスイッチポートからEPCキャプチャを取得して、APがCAPWAPトン ネルを形成するために使用している証明書を確認できます。DTLSトンネルが正常に構築されたか どうかをPCAPから確認します。



DTLSデバッグをAPおよびWLCで実行すると、証明書の問題を理解できます。

LSCを使用したAP有線802.1X認証

APは、同じLSC証明書を使用して自身を認証するように設定されています。APは802.1Xサプリ カントとして機能し、ISEサーバに対してスイッチによって認証されます。ISEサーバはバックエ ンドでADと通信します。



注:APアップリンクスイッチポートでdot1x認証を有効にすると、認証が通過するまで APはトラフィックを転送または受信できません。認証に失敗したAPを回復してAPにア クセスするには、APの有線スイッチポートでdot1x authを無効にします。

EAP-TLS認証のワークフローとメッセージ交換



AP有線802.1x認証の設定手順

- 1. CAPWAP DTLSとともにdot1xポート認証を有効にし、EAPタイプを選択します。
- 2. AP用のdot1xクレデンシャルを作成します。
- 3. スイッチポートでdot1xを有効にします。
- 4. 信頼できる証明書をRADIUSサーバにインストールします。

APの有線802.1x認証GUI設定

- 1. AP加入プロファイルに移動し、プロファイルをクリックします。
 - 1. AP > Generalの順にクリックします。「CAPWAP DTLS + dot1x port auth」として EAPタイプとAP認証タイプを選択します。
 - 2. Management > Credentialsの順に移動し、AP dot1x authのユーザ名とパスワードを作成します。

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 Clent CAPWAP AP Management Security	x ICap QoS
Dashboard	AP Join Profile Name	T Des	General Power Management Hyperlocation AP Statistics Power Over Ethernet Clies	nt Statistics Reporting Interval
Configuration	APQ_test tonSto APQ_stor-Fir-APs		Switch Flag 5 GH Power Injector State 2.4 0	z (sec) 90 Hz (sec) 90
Clicensing Troubleshooting	APG_db-FF-APs APG_db-FF-APs APG_fb-FF-APs APG_7b-FF-APs		Power Injector Type Unknown Exte Injector Switch MAC 0000.0000 Enable	nded Module
	APG_BUH-Fir-APs APG_110+-Fir-APs APG_110+-Fir-APs		AP EAP Auth Configuration Mes EAP Type EAP-TLS Profil AP Authorization Type CAPNAP DTLS + DOTe.	h e Name default-mesh-pro v @ Clear
Work Me Through 1	APO_1200+PH-APs H ← 1 2 3 → ₩ 10 -		CAPVAP DTLS + DOT's port auth CAPVAP DTLS Dot's port auth	
			"D Cancel	👸 Update & Apply to Device

Cisco Cat	talyst 9800-40 Wireless Controller	Welcome admin 🛛 🐐 🌾 🛕 🖹 🏟 🔞 🕢 🗯 Search Alts and Chems 🔍 🛛 🜌 Feedback 🖉 🦗
Q. Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile ×
Dashboard	+ Add X Delete	General Cillent CAPWAP AP Management Security ICap QoS Device User Credentials CDP Interface
C Marine and	AP Join Profile Name	Y Des
(2) Monitoring >	ap-auth	Dot1x Credentials
🗞 Configuration 🔹 🔹	APG_test	Dot1x Username ap-wired-user
(C) Administration	testSite	Dot1x Password
C Licensing	APG_3rd-Fir-APs ADG_Ath_Eir-APs	Dot1x Password Type clear +
and coversing	APG 6th-Fk-APs	
W Troubleshooting	APQ_7th-Fk-APs	
	APG_8th-Fk-APs	
	APG_11th-Fir-APs	
	APG_12th-Fir-APs	
waik the Through 1	H < 1 2 3 + H 10 +	
		Cancel

APの有線802.1x認証のCLI設定

CLIからAPのdot1xを有効にするには、次のコマンドを使用します。これは、特定の参加プロファ イルを使用しているAPの有線認証のみを有効にします。

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

AP有線802.1x認証スイッチの設定

このスイッチ設定は、ラボでAP有線認証を有効にするために使用されます。設計に基づいて異な る設定を行うことができます。

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

RADIUSサーバ証明書のインストール

認証は、(サプリカントとして機能している)APとRADIUSサーバの間で行われます。両方が互 いの証明書を信頼する必要があります。APにRADIUSサーバ証明書を信頼させる唯一の方法は、 AP証明書を発行したSCEP CAによって発行された証明書をRADIUSサーバで使用させることです 。

ISEで、Administration > Certificates > Generate Certificate Signing Requestsの順に選択します

CSRを生成し、フィールドにISEノードの情報を入力します。

Cisco ISE

Administration · System

Certificate Management 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 • Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication Certificate Periodic Check Se • EAP Authentication	
Certificate Management 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 Authentication - Server Authentication	
System Certificate 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 Authentication	
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 Authentication - Server Authentication	
OCSP Client Profile • Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication Certificate Signing Requests • Admin - Server Authentication Certificate Periodic Check Se • EAP Authentication - Server Authentication D19 Extension • Extension	
Certificate Signing Requests • Admin - Server Authentication Certificate Periodic Check Se • EAP Authentication - Server Authentication	
Certificate Periodic Check Se EAP Authentication - Server Authentication - DTI & Automatication - DTI & Automatication - DTI & Automatication - Server Authentication -	
 DTLS Authentication - Securit Authentication 	
Disadi Laurente de la constructione de la	
Portal - Server Automitication Portal - Server Automitication	
SAML - SAML Signing Certificate SAML - SAML Signing Certificate	
ISE Messaging Service - Generate a Signing Certificate or generate a brand new Messaging Certificate.	
Data Connect Corntlicate - 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	
ISE99 ISE99HEAP Authentication	
Subject	
Common Name (CN)	
ardina ()	
Organizational Unit (OU)	
Oranaitation (O)	
G G	
City (L)	
State (ST)	

生成されたテキストは、エクスポートしたり、テキストとしてコピー&ペーストしたりできます 。

Windows CA IPアドレスに移動し、URLに/certsrv/を追加します

Request a certificateをクリックします

← → C ▲ Non sécurisé | 192.168.1.98/certsrv/
 Microsoft Active Directory Certificate Services - mydomain-WIN-3E2O2T1QD0U-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services Documentation</u>.

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>

Submit a certificate request by using a base-64をクリックします

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: Create and submit a request to this CA.

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.

CSRテキストをテキストボックスに貼り付けます。Webサーバ証明書テンプレートを選択します

← C ▲ Non sécurisé 192.168.1.98/certsrv/certrqxt.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 certificate request (CMC or PKCS #10 or PKCS #7):
Certificate Template: (No templates found!) >
Additional Attributes:
Attributes

その後、Certificate Signing Requestメニューに戻り、Bind certificateをクリックして、この証明 書をISEにインストールできます。その後、Windows Cから取得した証明書をアップロードでき ます。

■ 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 >	Eriendly Name Certificate Subject Key Length Portal gro Timestamp A Host
	☑ ISE99#EAP Authentication CN=ISE99.mydomain.local 4096 Mon, 30 Oct 2023 ISE99

AP有線802.1x認証の検証

コンソールからAPにアクセスし、次のコマンドを実行します。

#show ap authentication status

Ap認証が有効になっていない:

ap authを有効にした後のAPからのコンソールログ:

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が正常に認証されました:



WLCの検証:

9800-40#sho ap name AP0CD0.F89A.46E0 config general begin Certificate				
AP Certificate Expiry-time	: \$9/25/2024 65:48:23			
AP Certificate Issuer common-	Tance : Samars-Gov-B : Default			
Certificate status	: Available			
LSC fallback status Issuer certificate hash	: No 5 (11255bc69f565af537bc59297f453593e432e1b			
Certificate expiry time AP 802.1x LSC Status	: 09/25/2024 06:48:23			
Certificate status	: Available 6.11256/s62455.sf37hs50207f451503n412n15			
Certificate expiry time	9(1)57/00/4_06/48/173			
AP LSC authentication state	: CAPHAP-DILS and 802.1X authentication			

認証に成功した後のswitchportインターフェイスのステータス:

Switch#sho authenticati Interface	on sessions inte MAC Address	rface gi Method	gabitEth Domain	Status Fg	Session ID
Gi1/0/2	0cd0.f89a.46e0	dot1x	DATA	Auth	9765690A000005CCEED0FBF

次に、認証が成功したことを示すAPコンソールログの例を示します。

```
[*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]
```

802.1X認証のトラブルシューティング

APアップリンクでPCAPを取得し、RADIUS認証を確認します。認証に成功した場合のスニペットを次に示します。



認証をキャプチャするISEからのTCPdump collect。



認証中に問題が確認された場合は、APの有線アップリンクとISE側からの同時パケットキャプチャが必要になります。

APのdebugコマンド:

#debug ap authentication packet

関連情報

- シスコテクニカルサポートおよびダウンロード
- <u>AireOSを使用するAPでの802.1Xの設定</u>
- ・ <u>LSC用の9800コンフィギュレーションガイド</u>
- ・ <u>9800のLSC設定例</u>
- <u>9800上のAP用の802.1Xの設定</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。