使用ISE内部CA在9800 WLC上配置EAP-TLS

目录

$\underline{\hat{n}}$
先决条件
使用的组件
EAP-TLS身份验证流程
EAP-TLS流程中的步骤
添加网络设备
验证内部CA
<u>添加身份验证方法</u>
<u>指定证书模板</u>
创建证书门户
添加内部用户
ISE证书调配门户和RADIUS策略配置
<u>9800 WLC配置</u>
<u>将ISE服务器添加到9800 WLC</u>
<u>在9800 WLC上添加服务器组</u>
在9800 WLC上配置AAA方法列表
<u>在9800 WLC上配置授权方法列表</u>
<u>在9800 WLC上创建策略配置文件</u>
在9800 WLC上创建WLAN
<u>在9800 WLC上使用策略配置文件映射WLAN</u>
<u>将策略标记映射到9800 WLC上的接入点</u>
安装完成后的WLC运行配置
为用户创建和下载证书
<u>Windows 10计算机上的证书安装</u>
<u>故障排除</u>
<u>参考</u>

简介

本文档介绍使用身份服务引擎的证书颁发机构对用户进行身份验证的EAP-TLS身份验证。

先决条件

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 无线控制器:运行17.09.04a的C9800-40-K9
- 思科ISE:运行版本3补丁4
- AP型号:C9130AXI-D
- 交换机: 9200-L-24P

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

大多数组织都有自己的CA向最终用户颁发证书以进行EAP-TLS身份验证。ISE包括一个内置证书颁 发机构,可用于生成用户在EAP-TLS身份验证中使用的证书。在无法使用完整CA的情况下,使用 ISE CA进行用户身份验证会更有优势。

本文档概述了有效使用ISE CA对无线用户进行身份验证所需的配置步骤。EAP-TLS身份验证流程

EAP-TLS身份验证流程



EAP-TLS身份验证流程

EAP-TLS流程中的步骤

- 1. 无线客户端与接入点(AP)关联。
- 2. 在此阶段, AP不允许数据传输并发送身份验证请求。
- 3. 客户端作为请求方,使用EAP-Response Identity进行响应。
- 4. 无线局域网控制器(WLC)将用户ID信息转发到身份验证服务器。
- 5. RADIUS服务器使用EAP-TLS启动数据包回复客户端。
- 6. EAP-TLS会话从此开始。
- 7. 客户端将EAP-Response发送回身份验证服务器,包括密码设置为NULL的client_hello握手消息。
- 8. 身份验证服务器使用访问质询数据包进行响应,该数据包包含:

TLS server_hello Handshake message Certificate Server_key_exchange Certificate request Server_hello_done

9.客户端回复的EAP-Response消息包括:

Certificate (for server validation) Client_key_exchange Certificate_verify (to verify server trust) Change_cipher_spec TLS finished

10.成功进行客户端身份验证后,RADIUS服务器将发送访问质询,内容包括:

Change_cipher_spec Handshake finished message

11.客户端验证哈希值以验证RADIUS服务器。

12.在TLS握手期间,从密钥动态派生新的加密密钥。

13. EAP-Success消息从服务器发送到身份验证器,然后发送到请求方。

14.启用EAP-TLS的无线客户端现在可以访问无线网络。

配置



实验室拓扑结构

配置

在本节中,我们将配置两个组件:ISE和9800 WLC。

ISE 配置

以下是ISE服务器的配置步骤。每个步骤都附带此部分中的屏幕截图,以提供可视指导。



ISE服务器配置步骤

添加网络设备

要添加无线LAN控制器(WLC)作为网络设备,请使用以下说明:

- 1. 导航到Administration > Network Resources > Network Devices。
- 2. 单击+Add图标启动添加WLC的过程。
- 3. 确保预共享密钥与WLC和ISE服务器匹配,以实现正确的通信。
- 4. 正确输入所有详细信息后,点击左下角的Submit保存配置

🔽 🗸 RADIUS Auth	entication Setting	gs							
RADIUS UDP Settings									
Protocol	RADIUS								
Shared Secret	<u></u>		Show						
Use Second Sha	Use Second Shared Secret (i)								
Se Se	cond Shared cret			Show					
CoA Port	1700		Set To Default						

```
添加网络设备
```

验证内部CA

要验证内部证书颁发机构(CA)设置,请执行以下步骤:

- 1. 转至Administration > System > Certificates > Certificate Authority > Internal CA Settings。
- 2. 确保已启用CA列以确认内部CA处于活动状态。

Щ	Bookmarks	Deployment	Licensing	Certificates	Loggin	g Maintenance	Upgrade	e Health	Checks Backup &	
55	Dashboard	0								
망	Context Visibility	Certificate Mana	agement	Inter	nal CA	A Settings	🙏 For disaster	recovery it is re	commended to Export Internal	
×	Operations	Certificate Authority ~ Overview								
U	Policy	Issued Certific	cates	Host Na	ime ^	Personas		Role(s)	CA, EST & OCSP Re	
20	Administration	Certificate Au	thority Certificat	ise3gen	vc	Administration, Monito	ring, Poli	STANDAL	•	
alı.	Work Centers	Certificate Te	mplates							

验证内部CA

添加身份验证方法

导航到管理>身份管理>身份源序列。添加自定义身份序列以控制门户登录源。

Identities	Groups	External Identity	Sources	Identity Sour	ce Sequences	Settings
Identity S	iource Sequenc	es List > Allow_EMP_Cert				
ldentit	y Source S	equence				
∽ lde	ntity Sourc	e Sequence				
* Nam	1e	Allow_EMP_Cert				
Descr	iption					
∨ Ce	ertificate Ba	ased Authentication	ר Pre	loaded_Certific∽		
✓ Au	thenticatio	on Search List				
	A set of ide	ntity sources that will be	accessed	in sequence until fi	rst authentication	succeeds
	Identity Source Sequences List > Allow_EMP_Cert Identity Source Sequence * Name Allow_EMP_Cert Description			Selected		
	Identity Source Sequence Identity Source Sequence * Name Allow_EMP_Cert Description Select Certificate Authentication Profession Authentication Search List A set of identity sources that will Available Internal Endpoints Guest Users All_AD_Join_Points			Internal Users)	
	Guest Us	sers				
	All_AD_	Join_Points				
			$\overline{\langle}$			<

认证方法

指定证书模板

要指定证书模板,请执行以下步骤:

步骤1.导航到管理>System >证书>证书颁发机构>证书模板。

步骤2.点击+Add图标以创建新的证书模板:

2.1为模板提供ISE服务器的本地唯一名称。

2.2确保公用名(CN)设置为\$UserName\$。

2.3检验主题备用名称(SAN)是否已映射到MAC地址。

2.4 将SCEP RA配置文件设置为ISE内部CA。

2.5在extended key usage部分,启用客户端身份验证。

Certificate Management >	Edit Certificate Template	
Certificate Authority ~	* Name	EAP_Authentication_Certificate_Template
Issued Certificates	Description	This template will be used to issue certificates for EAP Authentication
Certificate Authority Certificat	Subject	2
Internal CA Settings	Common Name (CN)	\$UserName\$ 🕠
Certificate Templates	Organizational Unit (OU)	Example unit
	Organization (O)	Company name
	City (L)	City
	State (ST)	State
	Country (C)	us
	Subject Alternative Name (SAN)	
	Кеу Туре	RSA 🗸
	Key Size	2048 ~
	* SCEP RA Profile	ISE Internal CA
	Valid Period	730 Day(s) (Valid Range 1 - 3652)
	Extended Key Usage	Client Authentication Server Authentication

证书模板

创建证书门户

要创建用于生成客户端证书的证书门户,请执行以下步骤:

步骤1.导航到管理>设备门户管理>证书调配。

步骤2.单击创建,设置新的门户页面。

步骤3.为门户提供唯一名称,以便轻松识别它。

3.1.选择门户的端口号;将此设置为8443。

3.2.指定ISE侦听此门户的接口。

3.3.选择Certificate Group Tag作为默认门户证书组。

3.4.选择authentication method,指明用于验证登录此门户的身份库序列。

3.5.包括其成员可以访问门户的授权组。例如,如果您的用户属于此组,请选择Employee用户 组。

3.6.定义在"证书调配"(Certificate Provisioning)设置下允许的证书模板。

I I	Bookmarks	Blocked List	BYOD	Certificate Pro	visioning	Client Provisioning
5	Dashboard	Port	als Se	ttings and	Custor	nization
ц <mark>о</mark>	Context Visibility					
×	Operations	Portal Nar	ne:		Descri	iption:
Ø	Policy		RTIFICATE P	PORTAL		
a 0	Administration	Languag	e File			
កា	Work Centers	Portal tes	t URL			
?	Interactive Features	Portal B	ehavior and	I Flow Settings	Portal Page	e Customization



Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available	Chosen
Q ALL_ACCOUNTS (default) GROUP_ACCOUNTS (default) OWN_ACCOUNTS (default)	Employee
Choose all Fully qualified domain name (FODN):	Clear all

> Login Page Settings							
> Acceptable Use Policy (AUP) Page Settings							
> Post-Login Banner Pag	ge Settings						
> Change Password Settings							
✓ Certificate Portal Setting	ngs						
Certificate Templates: *	EAP_Authentication_Certificate_Template × 🧹						

证书门户配置

完成此设置后,您可以通过点击门户测试URL来测试门户。此操作将打开门户页面。

Portals Settings and Customization							
Portal Name:	Description:						
EMP CERTIFICATE PORTAL							
Language File							
Portal test URL							

测试门户页面URL

e	tps://10.106.32.31:8443/certprovportal/PortalSetup.action?portal=45aea9cb-29c8-4f73-98bb-63543bba423a										
	CISCO Certificate Provisioning Portal										
	Sign On Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you. Username: emp										
	Password:										
	Sign On										

门户页

添加内部用户

要创建通过证书门户进行身份验证的用户,请执行以下步骤:

- 1. 转至Administration > Identity Management > Identities > Users。
- 2. 单击选项将用户添加到系统。
- 3. 选择用户所属的User Identity Groups。在本例中,将用户分配到Employee组。

Identities	Groups	External	Identity S	ources	Identity Sour	ce Sequences	Settings				
Users Latest Manu	ial Network Scan H	Res	Netw	ork A	ccess U	sers					
			🖉 Edit	+ Add					✓ iDuplicate		
				Status	Username \land	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
	🗆 🔳 Ena			Enabled	1 emp				C	Employee	

添加内部用户

ISE证书调配门户和RADIUS策略配置

上一节介绍ISE证书调配门户的设置。现在,我们将ISE RADIUS策略集配置为允许用户身份验证。

- 1. 配置ISE RADIUS策略集
- 2. 导航到Policy > Policy Sets。
- 3. 点击加号(+)创建新的策略集。

在本示例中,设置一个简单的策略集,用于使用用户证书对用户进行身份验证。

Policy Sets		Reset	Reset Policyset Hit	counts		Save
Status Policy Set Name Description	Conditions	Allowed Protocols	/ Server Sequence	Hits	Actions	View
Q Search						
EMP Wireless 802.1x Auth	E Wreless_802.1X	. Default Network A			têr	
	Airespace-Airespace-Wian-Id EQUALS 17				ж.	

策略集

∼Auth	entication	Policy(2)					
٠	Status	Rule Name	Conditions		Use	Hits	Actions
C							
					Allow_EMP_Cert 🛛 🛛 🗸		
	•	Allow Certificate Authentication	F FAP-TLS		> Options		¢
					DenyAccess 🤕 🗸		
	0	Default			> Options		ŵ
> Auth	orization P	olicy - Local Exceptions					
> Auth	orization P	olicy - Globel Exceptions					
∽Auth	orization P	folicy(2)					
				Results			
\odot	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
C							
	۲	Authz Employee	E LAP-TLS	PermitAccess 0	Employees 🖉 +		¢
	۲	Default		DenyAccess 0			ŵ

显示身份验证和授权策略的策略集

9800 WLC配置

以下是9800 WLC的配置步骤。每个步骤都附带此部分中的屏幕截图,以提供可视指导。



WLC配置步骤

将ISE服务器添加到9800 WLC

- 1. 要将ISE服务器与9800无线局域网控制器(WLC)集成,请执行以下步骤:
- 2. 转至Configuration > Security > AAA。
- 3. 单击Add按钮以在WLC配置中包含ISE服务器。

Configuration * > Security * > AAA	Show Me How			
+ AAA Wizard				
Servers / Groups AAA Method List	AAA Advanced			
	Create AAA Radius Server			
+ Add × Delete	Name*	ISE3	Support for CoA ()	ENABLED
RADIUS	Server Address*	10.106.32.31	CoA Server Key Type	Clear Text 👻
TACACS+	PAC Key	0	CoA Server Key 🛞	
LDAP	Кеу Туре	Clear Text 👻	Confirm CoA Server Key	
	Key* (i)		Automate Tester	
	Confirm Key*			
	Auth Port	1812		
	Acct Port	1813		
	Server Timeout (seconds)	1-1000		
	Retry Count	0-100		

添加服务器后,它将显示在服务器列表中。

Servers / Groups	AAA Method Lis	t AAA Ad	Ivanced							
+ Add	< Delete									
RADIUS		Servers	Server Groups							
TACACS+										
1010			Name	Ŧ	Address	Ŧ	Auth Port	т	Acct Port	Ŧ
LDAP			ISE3		10.106.33.23		1812		1813	

显示Radius服务器

在9800 WLC上添加服务器组

要在9800无线LAN控制器上添加服务器组,请完成以下步骤:

- 1. 导航到Configuration > Security > AAA。
- 2. 单击Server Group选项卡,然后单击Add以创建新的服务器组。

Configuration * > Security * > AA	A Show Me How	Edit AAA Radius Server Gro	quo
+ AAA Wizard		Name*	ISE
Servers / Groups AAA Method Lis	t AAA Advanced	Group Type	RADIUS
		MAC-Delimiter	none v
+ Maa 🛛 🕆 Delete		MAC-Filtering	none 🔻
RADIUS	Servers Server Groups	Dead-Time (mins)	1-1440
TACACS+		Load Balance	DISABLED
LDAP	Name Y Server 1	Source Interface VLAN ID	2124 💌 💈
	N 4 1 > N 10 -	Available Servers	Assigned Servers
) ISE3
			S
			«

将ISE服务器映射到Radius服务器组

在9800 WLC上配置AAA方法列表

创建服务器组后,按照以下步骤配置身份验证方法列表:

- 1. 导航到Configuration > Security > AAA > AAA Method List。
- 2. 在Authentication选项卡中,添加新的身份验证方法列表。
- 3. 将类型设置为dot1x。
- 4. 选择group作为组类型。
- 5. 包括您之前创建的ISE服务器组作为服务器组。

Configuration > Security > AA	Configuration * > Security * > AAA show Me How			Quick Setup: AAA Authentication			
+ AAA Wizard				Method List Name*	CERT_AUTH		
Servers / Groups AAA Method L	ist AAA Advanced			Туре*	dot1x 🔻 🗓		
				Group Type			
Authentication	– Arini – × Delete			Fallback to local	0		
Authorization				Available Server Groups	Assigned Server Groups		
Accounting	Name	т Туре 🛛 🕇	Group Type	radius			
	CERT_AUTH	dot1x	group	Idap tacacat			
					8		
					×.		

创建身份验证方法列表

在9800 WLC上配置授权方法列表

要设置授权方法列表,请执行以下步骤:

- 1. 导航到AAA Method List部分中的Authorization选项卡。
- 2. 单击Add创建新的授权方法列表。
- 3. 选择network作为类型。
- 4. 选择group作为组类型。
- 5. 包括ISE服务器组作为服务器组。

Configuration * > Security * > AAA show Me How			Quick Setup: AAA Authorization		
+ AAA Wizard				Method List Name*	CERT_AUTH
Servers / Groups AAA Method L	ist AAA Advanced			Type*	network 🔻 👔
				Group Type	
Authentication				Fallback to local	
Authorization		10		Authenticated	Π
Accounting	Name	ү Туре	T Group Type	Ausilable Server Creune	Assisted Secure Course
Accounting	CERT_AUTH	network	group	Available Server Groups	Assigned Server Groups
	H < 1 > H	10 🔻		radius Idap	
				tacacs+	1

添加授权方法列表

在9800 WLC上创建策略配置文件

完成RADIUS组配置后,继续创建策略配置文件:

- 1. 导航至配置 > 标签和配置文件 > 策略。
- 2. 单击Add创建新的策略配置文件。
- 3. 为策略配置文件选择适当的参数。在本例中,所有设备都处于中心状态,并且实验VLAN用作 客户端VLAN。



配置策略配置文件

Gen	eral	Access Policies	QOS and AV	/C	Mobility	Ad	/ance
ſ	radius p	rofiling					
I	HTTP TLV	Caching					
I	DHCP TLV	/ Caching					
	WLAN L	ocal Profiling					
()	Global Sta Classificat	ate of Device tion		Enabled	i)		
I	Local Sub	scriber Policy Nam	е	Searc	h or Select	•	
	VLAN						
, v	VLAN/VL4	AN Group		2124		•	
I	Multicast	VLAN		Enter	Multicast VLAN	1	

VLAN到策略的映射

配置RADIUS授权时,请确保在策略配置文件设置的高级选项卡中启用AAA Override选项。此设置 允许无线局域网控制器将基于RADIUS的授权策略应用于用户和设备。

Ge	eneral	Access Policies	QOS and AVC	Mobility	Advanced
	WLAN	Timeout			Fabric
	Session	Timeout (sec)	1800		Link-L
	ldle Tim	eout (sec)	300		mDNS Policy
	Idle Thr	eshold (bytes)	0		Hotspo
	Client E	xclusion Timeout (sec)	60		User I
	Guest L	AN Session Timeout			Status
	DHCP				Drop L
	IPv4 DH	ICP Required			DNS I
	DHCP S	Server IP Address			DNS L Param
S	how mor	re >>>			Flex D for DN
	AAA P	olicy			
	Allow A	AA Override			Flex D Redire

AAA覆盖

在9800 WLC上创建WLAN

要设置具有802.1x身份验证的新WLAN,请执行以下步骤:

- 1. 导航到配置>标签和配置文件> WLAN。
- 2. 单击Add以创建新的WLAN。
- 3. 选择第2层身份验证设置并启用802.1x身份验证。

Configuration * > Tags & Profiles * > WLANs	Edit WLAN	
+ Add × Delete Cione Enable WLAN Disable WLAN	General Security Advanced Add To Policy Tags	
Status V Name V ID	Layer2 Layer3 AAA	
C R-webeuth 10 C CERT-AUTH 17	O WPA + WPA2 • WPA2 + WPA3 • WPA3 • Static WEP • None MAC Filtering •	
	Libitry Admin Access WPA Parameters WPA2 Palicy GTK OSEN Policy GTK OSEN Policy WPA2 Encryption Adeptive Enable Acts(CCMP128) CCMP256 Policy Protected Management Frame Status PSK PMF Disabled SHA256 MPK Disabled MPSK Configuration Enable MPSK Inable MPSK	4

WLAN配置文件配置

Ģ	ieneral	Security	Advance	d Add To	Policy 7	Tags
	Layer2	Layer3	AAA			
	Authon	tiestics List		CEPT ALL	ru _	
	Autnen	tication List		CERT_AU		
	Local E	AP Authentica	ation			

WLAN配置文件到方法列表映射

在9800 WLC上使用策略配置文件映射WLAN

要将WLAN与策略配置文件关联,请执行以下步骤:

- 1. 导航到配置>标签和配置文件>标签。
- 2. 单击Add添加新标记。
- 3. 在WLAN-POLICY部分,将新创建的WLAN映射到相应的策略配置文件。



策略标签配置

将策略标记映射到9800 WLC上的接入点

要将策略标记分配给接入点(AP),请完成以下步骤:

- 1. 导航到配置>标签和配置文件>标签> AP。
- 2. 转到AP配置中的Static(静态)部分。
- 3. 点击要配置的特定AP。
- 4. 将您创建的策略标记分配到所选AP。

Policy Site RF	AP			▲ Changing Tags wil	I cause the AP to moment not all	arily lose a owed while	ssociation changing
Tag Source Static	Location Filter						
				AP MAC Address*	cc7f.75ae.1fc0		
Number of AP Tag mapping	gs selected : 0		Select File	Policy Tag Name	CERT_POLICY_TAG 🔻		
AP MAC Address	т	Policy Tag Name		Site Tag Name	default-site-tag 👻		
a4b4.392a.8dfc		default-policy-tag		RF Tag Name	default-rf-tag 🔹		
Cc7f.75ae.1fc0	10 👻	CERT_POLICY_TAG					

AP标记分配

安装完成后的WLC运行配置

wlan CERT-AUTH 17 CERT-AUTH

```
aaa group server radius ISE
server name ISE3
ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
client 10.106.32.31 server-key Cisco!123
!
wireless profile policy CERT-AUTH
aaa-override
ipv4 dhcp required
vlan 2124
no shutdown
wlan CERT-AUTH policy CERT-AUTH
```

security dot1x authentication-list CERT_AUTH
no shutdown
!
wireless tag policy CERT_POLICY_TAG
wlan CERT-AUTH policy CERT-AUTH

为用户创建和下载证书

要为用户创建和下载证书,请执行以下步骤:

1.让用户登录之前设置的证书门户。

Not Secure	https://10.106.32.31:8443/certprovportal/PortalSetup.action?portal=45aea9cb-29c8-4f73-98bb-63543bba423a
	Certificate Provisioning Portal
	Sign On
	Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you.
	Username:
	emp
	Password:
	Sign On

访问证书门户

2.接受可接受的使用政策(AUP)。 然后,ISE显示用于生成证书的页面。

3.选择Generate a single certificate(without a certificate signing request)。



of the date is not of the date is a set of the date	
I want to: *	
Generate a single certif	ıt a certificat 💿
Common Name (CN): *	
emp 2	
MAC Address: *	
242f.d0da.a563	
Choose Certificate Template: *	_3
EAP_Authentication_Certificate	_Template 💿
Description:	
Certificate Download Format: *	4
PKCS12 format, including certifica	te chain (… 💿
Certificate Password: * 5	Θ
Enter password to download and view/install t	he certificate
Confirm Password: *	
Generate	Reset

生成证书

要通过证书调配门户生成证书,请确保填写以下必填字段:

- CN:身份验证服务器使用客户端证书中Common Name字段中显示的值对用户进行身份验证。
 在Common Name字段中,输入用户名(用于登录证书调配门户)。
- MAC 地址:主题备用名称(SAN)是X.509扩展,允许将各种值与安全证书关联。思科ISE版本 2.0仅支持MAC地址。因此,在SAN/MAC地址字段中。
 - 证书模板:证书模板定义CA在验证请求和颁发证书时使用的字段集。公用名(CN)等字段
 用于验证请求(CN必须与用户名匹配)。CA在颁发证书时使用其他字段。
- 证书密码:您需要证书密码来保护您的证书。必须提供证书密码才能查看证书的内容并在设备 上导入证书。
- 您的密码必须符合以下规则:
- 密码必须至少包含1个大写字母、1个小写字母和1个数字

。 密码的长度必须介于8到15个字符之间

◎ 允许的字符包括A-Z、a-z、0-9、_、#

填写所有字段后,选择Generate以创建和下载证书。

Windows 10计算机上的证书安装

要在Windows 10计算机上安装证书,请按以下步骤打开Microsoft管理控制台(MMC):



注意:这些说明可能因您的Windows设置而异,因此建议参阅Microsoft文档以了解具体的 详细信息。

- 1. 单击Start,然后单击Run。
- 2. 在"Run(运行)"框中键入mmc,然后按Enter。Microsoft管理控制台打开。
- 3. 添加证书管理单元:
- 4. 转到文件>添加/删除管理单元。
- 5. 选择Add,然后选择Certificates,然后单击Add。

6. 选择Computer Account,然后选择Local Computer,然后单击Finish。

这些步骤允许您管理本地计算机上的证书。

🌇 Console1 - [Console Root]	- 🗆 X
🚪 File Action View Favorites Window Help	_ & ×
Console Root	Actions
Add of hemove shap-ins	Console Root
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.	More Actions
Available snap-ins: Selected enap-ins:	
Snap-in Vendor ^ Edit Extensions	1
ActiveX Control Microsoft Cor Remove	1
Certificates Microsoft Cor	
Component Services Microsoft Cor Move Up	()
Computer Managem Microsoft Cor Move Down	
The bence manager microsoft and Add >	
Event Viewer Microsoft Cor	
Folder Microsoft Cor	
Group Policy Object Microsoft Cor	
UP Security Monitor Microsoft Cor	
UP Security Policy M Microsoft Cor	
Link to Web Address Microsoft Cor	
Uescription:	
The Certificates shap-in allows you to browse the contents or the certificate stores for yourself, a service, or a computer.	
OK Cancel	
Line and Lin	щ
	1

Windows MMC控制台

步骤1.导入证书:

1.1.单击菜单中的Action。

1.2.转到所有任务,然后选择导入。

1.3.按照提示查找并选择计算机上存储的证书文件。

← 😺 Certificate Import Wizard

File to Import

Specify the file you want to import.

C: \Users \admin \Desktop \en	np-2025-01-06_08-30-59\emp_C4-E9-0 Browse
Note: More than one certific	ate can be stored in a single file in the following formats:
Personal Information Exc	hange-PKCS #12 (.PFX,.P12)
Cryptographic Message S	yntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certif	icate Store (.SST)

导入证书

在证书导入过程中,系统会提示您输入在门户上生成证书时创建的密码。请确保准确输入此密码以 成功导入证书并将其安装在计算机上。

I	Private key protection To maintain security, the private key was protected with a password.
	Turne the energy of fac the entropy have
	Type the password for the private key.
	Password:
	••••••
	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	Protect private key using virtualized-based security(Non-exportable)
	I Include all extended preparties

输入证书密码

步骤2.将证书移动到适当的文件夹:

2.1.打开Microsoft Management Console(MMC),然后导航到Certificates(Local Computer)> Personal文件夹。

2.2.检查证书并确定其类型(例如,根CA、中间CA或个人)。

2.3. 将每个证书移动到相应的存储区:

2.4.根CA证书:转到受信任的根证书颁发机构。

2.5.中间CA证书:转到中级证书颁发机构。

					×
🔶 🦻 Certifi	cate Import Wizard				
Certificat	te Store				
Cert	ificate stores are system	areas where certificate	s are kep	ot.	
Wind the o	lows can automatically se certificate.	ect a certificate store,	or you c	an specify a location f	or
(Automatically select the	e certificate store based	d on the t	type of certificate	
(Place all certificates in t	the following store			
	Certificate store:				
	Personal			Browse	
					_
				Next	Cancel
在个人文件夹中存储证	 :书				
Console Root V 🗊 Certificates (Local Computer)	Issued To	Issued By Certificate Services Node CA - ise3genvc	Expiration Date 1/3/2035	Intended Purposes	Friendly Name Statu EndpointSubCA
 Personal Certificates Trusted Root Certification 	Certificate Services Node CA - ise3genvc Certificate Services Root CA - ise3genvc	Certificate Services Root CA - ise3genvc Certificate Services Root CA - ise3genvc	1/3/2035 1/3/2035	<all></all>	certificate_nodeCA certificate
Certificates Enterprise Trust Intermediate Certification Aut	t⊯emp Gisa3genvc.lab.local t	centricate services triapoint Sub CA - ise3genvc ise3genvcJab.local	1/3/2027	Client Authentication Server Authentication, Client Authentication	emp_C4-t5-0A-00 Self-Signed

在其存储中移动证书

连接Windows计算机

将证书移动到正确的存储区后,请使用以下步骤连接到WLAN:

1. 单击系统托盘中的network图标查看可用的无线网络。

- 2. 查找并单击要连接的WLAN的名称。
- 3. 单击Connect并继续执行任何其他提示,以使用证书进行身份验证来完成连接过程。



连接到无线网络

在与WLAN的连接过程中出现提示时,选择Connect using a certificate(使用证书进行连接)选项。

٩//	CERT-AUTH Secured						
	Enter your user name and password						
	User name						
	Password						
[Connect using a certificate						
	OK	Cancel					

使用证书作为凭证

这使您能够使用证书成功连接到无线网络。

C:\>netsh wlan show interface 200% There is 1 interface on the system: : Wi-Fi 3 Name : TP-Link Wireless USB Adapter Description : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea GUID Physical address : 24:2f:d0:da:a5:63 State : connected SSID : CERT-AUTH BSSID : a4:88:73:9e:8d:af Network type : Infrastructure Radio type : 802.11ac Authentication : WPA2-Enterprise Cipher : CCMP Connection mode : Profile Channel : 36 Receive rate (Mbps) : 360 Transmit rate (Mbps) : 360 Signal : 100% Profile : CERT-AUTH

Hosted network status : Not available

C:\>netsh wlan show profiles CERT-AUTH | find "Smart" EAP type : Microsoft: Smart Card or other certificate

验证无线配置文件

验证

验证WLC是否正在广播WLAN:

<#root>

POD6_9800#show wlan summ Number of WLANs: 2 ID Profile Name SSID Status Security

17

CERT-AUTH

CERT-AUTH

UP [WPA2][802.1x][AES]

验证WLC上的AP是否打开:

确保AP正在广播WLAN:

<#root>

POD6_9800#show ap name AP1 wlan dot11 24ghz Slot id : 0 WLAN ID BSSID

17 a488.739e.8da0

POD6_9800#show ap name AP1 wlan dot11 5ghz Slot id : 1 WLAN ID BSSID

17

a488.739e.8daf

使用EAP-TLS连接的客户端:

<#root>

POD6_9800#show wire cli summ Number of Clients: 1 MAC Address AP Name Type ID State Protocol Method Role

242f.dOda.a563 AP1 WLAN

17

IP Learn 11ac

Dot1x

Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN

Wireless LAN Network Name (SSID): CERT-AUTH

BSSID : a488.739e.8daf

EAP Type : EAP-TLS

VLAN : 2124 Multicast VLAN : 0

Cisco Radius ISE实时日志:

⊖ 🖒 Reset Repeat Counts 止 Export		⊥ Export To ∨					
	Status	Details	Identity	Endpoint ID	Authentication Policy	Authoriz	Authoriz If
			Identity	Endpoint ID	Authentication Policy	Authorizatic	Authorizatic I
	٠	G			EMP Wireless 802.1x Auth >> Allow Certificate Authenti	EMP Wirel	PermitAcc
		6			EMP Wireless 802.1x Auth >> Allow Certificate Authenti	EMP Wirel	PermitAcc

ISE Radius实时日志

详细身份验证类型:

Authentication Details

Source Timestamp	2025-01-08 11:58:21.055
Received Timestamp	2025-01-08 11:58:21.055
Policy Server	ise3genvc
Event	5200 Authentication succeeded
Username	emp
Endpoint Id	24:2F:D0:DA:A5:63
Calling Station Id	24-2f-d0-da-a5-63
Endpoint Profile	TP-LINK-Device
Identity Group	User Identity Groups:Employee,Profiled
Audit Session Id	4D084E0A0000007E46F0C6F7
Authentication Method	dot1x
Authentication Method Authentication Protocol	dot1x EAP-TLS
Authentication Method Authentication Protocol Service Type	dot1x EAP-TLS Framed
Authentication Method Authentication Protocol Service Type Network Device	dot1x EAP-TLS Framed Iab-9800
Authentication Method Authentication Protocol Service Type Network Device Device Type	dot1x EAP-TLS Framed Iab-9800 All Device Types
Authentication Method Authentication Protocol Service Type Network Device Device Type Location	dot1x EAP-TLS Framed lab-9800 All Device Types All Locations
Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address	dot1x EAP-TLS Framed Iab-9800 All Device Types All Locations 10.78.8.77
Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address NAS Port Type	dot1x EAP-TLS Framed lab-9800 All Device Types All Locations 10.78.8.77 Wireless - IEEE 802.11
Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address NAS Port Type Authorization Profile	dot1x EAP-TLS Framed lab-9800 All Device Types All Locations 10.78.8.77 Wireless - IEEE 802.11 PermitAccess

ISE详细日志

显示EAP-TLS数据包的WLC EPC捕获:

	зар					X 🖘 🔹 +	
No.	Time	Source	Destination	Protocol	Length	Info	
	65 17:36	:58 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity	
	68 17:36	:58 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity	
	69 17:36	:58 TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity	
	70 17:36	:58 TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity	
	73 17:36	:58 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)	
	74 17:36	:58 TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello	
	78 17:36	:58 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)	
	79 17:36	:58 TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)	
	83 17:36	:58 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)	
	84 17:36	:58 TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)	
	87 17:36	:58 Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done	
	95 17:36	:58 TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)	
	100 17:36	:58 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)	
	102 17:36	:58 TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)	
	107 17:36	:58 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)	
	109 17:36	:59 TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)	
	114 17:36	:59 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)	
	115 17:36	:59 TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Messag	je
	118 17:36	:59 Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message	
	119 17:36	:59 TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)	
	126 17:36	:59 Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	, Success	

显示EAP事务的WLC捕获

- •数据包编号87对应于文档开头所述的EAP-TLS流中的步骤8。
- •数据包编号115对应于文档开头所述的EAP-TLS流中的步骤9。
- 数据包编号118对应于文档开头所述的EAP-TLS流中的步骤10。

显示客户端连接的无线活动(RA)跟踪:此RA跟踪经过过滤,可显示身份验证事务的一些相关行。

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655](调试)发送 加密DTLS消息。目的IP 10.78.8.78[5256],长499

2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655](信息)RADIUS发送访问请求 到10.106.33.23 1812 id 0/25,len 390

2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655](信息)从id 1812/25 10.106.33.23 0、Access-Challens、len 123接收的RADIUS

2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP,负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]收到的EAPOL数据包 — 版本1,EAPOL类型EAP,负载长度204,EAP类型= EAP-TLS

2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655](信息)RADIUS发送访问请求 到10.106.33.23 1812 id 0/26,len 663

2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655](信息)从id 1812/26 10.106.33.23 0、Access-Challens、len 1135接收的RADIUS

2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP,负载长度1012,EAP类型= EAP-TLS

2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP,负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655](信息)RADIUS Send Access-Request to 10.106.33.23 1812 id 0/27, len 465

2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655](信息)从id 1812/27 10.106.33.23 0、Access-Challens、len 1131接收的RADIUS

2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP,负载长度1008,EAP类型= EAP-TLS 2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP,负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655](信息)RADIUS发送访问请求 到10.106.33.23 1812 id 0/28,len 465

2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655](信息)从id 1812/28 10.106.33.23 0、Access-Challens、len 275接收的RADIUS

2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP,负载长度158,EAP类型= EAP-TLS

2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP,负载长度1492,EAP类型= EAP-TLS

2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655](信息)RADIUS发送访问请求 到10.106.33.23 1812 id 0/29,len 1961

2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655](信息)从id 1812/29 10.106.33.23 0、Access-Challens、len 123接收的RADIUS

2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP,负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP,负载长度1492,EAP类型= EAP-TLS

2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655](信息)RADIUS发送访问请求 到10.106.33.23 1812 id 0/30,len 1961

2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655](信息)从id 1812/30 10.106.33.23 0、Access-Challens、len 123接收的RADIUS

2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP,负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP,负载长度1492,EAP类型= EAP-TLS

2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655](信息)RADIUS发送访问请求 到10.106.33.23 1812 id 0/31,len 1961

2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655](信息)从id 1812/31 10.106.33.23 0、Access-Challens、len 123接收的RADIUS

2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP,负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655](信息)[242f.d0da.a563 capwap_90800005]收到的EAPOL数据包 — 版本1,EAPOL类型EAP,负载长度247,EAP类型= EAP-TLS

2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655](信息)RADIUS发送访问请求 到10.106.33.23 1812 id 0/32,len 706

2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655](信息)从id 1812/32

10.106.33.23 0、Access-Challens、len 174接收的RADIUS 2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP,负载长度57,EAP类型= EAP-TLS 2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]收到的EAPOL数据包 — 版本1,EAPOL类型EAP,负载长度6,EAP类型= EAP-TLS 2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/33, len 465 2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/33 10.106.33.23 0、Access-Accept、len 324接收的RADIUS 2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]已引发eap方法EAP-TLS的身份更新事件

故障排除

除典型的无线802.1x故障排除步骤外,没有针对此问题的具体故障排除步骤:

- 1. 执行客户端RA跟踪调试以检查身份验证过程。
- 2. 执行WLC EPC捕获以检查客户端、WLC和RADIUS服务器之间的数据包。
- 3. 检查ISE实时日志以验证请求是否与正确的策略匹配。
- 4. 在Windows终端上验证证书安装正确且存在整个信任链。

参考

- <u>证书调配门户常见问题解答, 版本3.2</u>
- <u>了解ISE内部证书颁发机构服务</u>
- <u>了解并配置WLC和ISE的EAP-TLS</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。