802.1x WLAN + Mobility Express(ME)8.2および ISE 2.1でのVLANオーバーライド

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 設定 ネットワーク図 設定 ME の設定 ISE で ME を宣言する ISE で新しいユーザの作成 認証ルールの作成 認証ルールの作成 エンド デバイスの設定 確認 MEの認証プロセス ISE の認証プロセス

概要

このドキュメントは、Wi-Fi Protected Access 2(WPA2)エンタープライズ セキュリティを備え た WLAN(ワイヤレス LAN)を Mobility Express コントローラおよび外部 Remote Authentication Dial-In User Service(RADIUS)サーバで設定する方法について説明します。 Identity Service Engine(ISE)は外部 RADIUS サーバの例として使用されます。

このガイドで使用される Extensible Authentication Protocol(EAP; 拡張可能認証プロトコル)は Protected Extensible Authentication Protocol(PEAP)です。 また、クライアントは特定の VLANに割り当てられます(デフォルトではWLANに割り当てられているVLAN以外)。

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。

- 802.1x
- PEAP
- 認証局(CA)
- •証明書

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。

MEv8.2

ISE v2.1

Windows 10 ラップトップ

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、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

設定

ネットワーク図



設定

一般的な手順は以下のとおりです。

- 1. ME でサービス セット識別子(SSID)を作成し、ME 上で RADIUS サーバ(この例では ISE)を宣言する
- 2. RADIUS サーバ(ISE)で ME を宣言する
- 3. ISE の認証ルールの作成
- 4. ISE の認可ルールの作成
- 5. エンドポイントの設定

ME の設定

RADIUS サーバと ME 間の通信を可能にするには、RADIUS サーバを ME に登録し、その逆も登録する必要があります。この手順は RADIUS サーバを ME に登録する方法を示します。

ステップ1:MEのGUIを開き、 [Wireless Settings] > [WLANs] > [Add new WLAN]



ステップ2:WLAN の名前を選択します。

Add Ne	ew WLAN		×
General	WLAN Security	VLAN & Firewall	QoS
	WLAN Id	3	•
	Profile Name *	me-ise	
	SSID *	me-ise	
	Admin State	Enabled	•
	Radio Policy	ALL	•
			pply 🛞 Cancel

ステップ3: [WLAN Security] でセキュリティの設定を指定します。

[WPA2-Enterprise] を選択し、[Authentication Server] には [External RADIUS] を選択します。編 集オプションをクリックして RADIUS の IP アドレスを追加し、[Shared Secret] **キーを決めます** 。



Add New	WLAN		×
General W	'LAN Security	VLAN & Firewall	QoS
Authentic	Security ation Server	WPA2 Enterprise External Radius	•
 (*) (*)	Radius IP 🔺 a.b.c.d I Please	Radius Port 1812 e enter valid IPv4 add	Shared Secret
External Radiu all WLANs	s configuration a	pplies to 📿 A	pply 🛞 Cancel

<a.b.c.d>は、RADIUS サーバに対応しています。

ステップ4:SSIDへのVLANの割り当て。

SSID を AP の VLAN に割り当てる必要がある場合は、この手順はスキップできます。

特定の VLAN(AP の VLAN 以外)にこの SSID のユーザを割り当てるには、[Use VLAN Tagging] **を有効にし、目的の VLAN ID** を割り当てます。

Add New WLAN	×				
General WLAN Security	VLAN & Firewall QoS				
Use VLAN Tagging	Yes				
VLAN ID *	2400 🔹				
Enable Firewall	No				
VLAN and Firewall configuration apply to all WLANs					

注: VLAN タギングを使用する場合は、アクセス ポイントに接続されたスイッチ ポートが トランク ポートとして設定され、AP VLAN がネイティブに設定されていることを確認しま す。

ステップ 5 : [Apply] をクリックして、設定を終了します。

Add New WLAN	×				
General WLAN Security	VLAN & Firewall QoS				
Use VLAN Tagging	Yes				
VLAN ID *	2400 🔹				
Enable Firewall	No 🔻				
VLAN and Firewall configuration apply to all WLANs					

ステップ6:オプションで、VLANオーバーライドを受け入れるようにWLANを設定します。

WLANでAAAオーバーライドを有効にし、必要なVLANを追加します。そのためには、ME管理インターフェイスへのCLIセッションを開き、次のコマンドを発行する必要があります。

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
ISE で ME を宣言する
```

ステップ1: ISE コンソールを開き、[Administration] > [Network Resources] > [Network Devices] > [Add] **に移動します。**

ellado Identity Serv	ices Engine Hom	e 🔹 🕨 Context Vi	sibility 🔹 🕨 Operati	ons 🔹 🕨 Policy	✓ Administration	→ Worl
▶ System ▶ Identi	ity Management 🛛 🕶 Netw	ork Resources	Device Portal Mana	agement pxGr	rid Services 🔹 🕨 Feed S	ervice (
▼Network Devices	Network Device Groups	Network Device	e Profiles External	RADIUS Servers	RADIUS Server Sequ	Jences
	Ø					
Network devices	Ne	twork Devices				
Default Device	1	Edit 🕂 Add 🗅	Duplicate	🚯 Export 👻 🌘	Generate PAC	ete 🔻

ステップ2:情報を入力します。

任意でモデル名、ソフトウェア バージョン、説明を指定し、デバイス タイプ、場所、WLC に基

a.b.c.d は ME の IP アドレスに対応します。

Network Devices List > New Network Device Network Devices
* Name WLC-name
Description optional description
*IP Address: a.b.c.d / 32
* Device Profile 🛛 🚽 🕀
Model Name wic-model
Software Version wlc-software 🍷
* Network Device Group
Device Type WLCs-2504 Set To Default
WLCs W/ Ca
← RADIUS Authentication Settings
Enable Authentication Settings
Protocol RADIUS
* Shared Secret Show
Enable KeyWrap 🗌 👔
* Key Encryption Key Show
* Message Authenticator Code Key Show
Key Input Format 💿 ASCII 🔵 HEXADECIMAL
CoA Port 1700 Set To Default

ネットワーク デバイス グループに関する詳細については以下のリンクを参照してください。

ISE で新しいユーザの作成

ステップ1: [Administration] > [Identity Management] > [Identities] > [Users] > [Add]を選択します。

disco Identi	ty Services Engine	Home	Context Visibility	Operations	Policy	 Administration
▶ System	■Identity Management	Network	Resources 🔹 🕨 Devi	ce Portal Managemei	nt pxGrid 8	System
◄ Identities	Groups External Ide	ntity Sources	Identity Source Se	quences 🔹 🕨 Setting	IS	Deployment Licensing
Users	C C	Netwo	rk Access Users			Certificates Logging Maintenance
Latest Manual	Network Scan Res	🥖 Edit	🕂 Add 🔢 Change	Status 👻 🎲 Import	🕞 Export 👻	Upgrade Backup & Restor
		Sta	tus Name	•	Description	Admin Access
		🍰 Lo	ading			Settings
						Identity Managem
					_	Identities

ステップ2:情報を入力します。

この例でこのユーザは ALL_ACCOUNTS と呼ばれるグループに属していますが、必要に応じて調整できます。

Network Access Users List > New Network Access User	
Network Access User	
* Name user1	
Status 🔽 Enabled 👻	
▼ Passwords	
Password Type: Internal Users 🔹	
Password	Re-Enter Passw
* Login Password	•••••
Enable Password	
 User Information 	
First Name	
Last Name	
 Account Options 	
Description	
Change password on next login	
 Account Disable Policy 	
Disable account if date exceeds 2017-01-21	
 User Groups 	
ALL_ACCOUNTS (default) 📀 🛖 🕂	
Submit Cancel	

認証ルールの作成

認証ルールはユーザのクレデンシャルが正しいか検証(ユーザ本当に本人かどうかの確認)し、 それに使用する許可されている認証方法を制限するのに使用されます。 ステップ1: ナビゲート [Policy] > [Authentication] に移動します。



ステップ2:新しい認証ルールを挿入してください。

[Policy] > [Authentication] > [Insert] を選択して、下または上に新しい行を挿入します。

dials. Identity Services Engine Home ♦ Context Visibility ♦ Operati	ons <mark>▼Policy</mark> → Administration → Work Centers Li					
Authentication Authorization Profiling Posture Client Provisioning + Pol	icy Elements					
ting the protocols that ISE should use to communicate with the network devices, and the ide system > Backup & Restore > Policy Export Page ed	entity sources that it should use for authentication.					
: If Wired_MAB OR Insert new row above Insert new row above Insert new row below Insert new row below						
: If Wired_802.1X OR IC_Protocols and	Duplicate above Duplicate below Delete					

ステップ3:必要な情報を入力します。

この認証ルールの例は、[Default Network Access] **の一覧に記載されたすべてのプロトコルを許可** します。この場合、Wireless 802.1x クライアント向けで Calling-Station-ID が *ise-ssid* で終了す る認証要求に適用されます。

diado Identity:	Services Engine	Home 🕨	Context Visibility	 Operations 	▼Policy	 Administration 	Work Centers	
Authentication	Authorization	Profiling Posture	Client Provisionin	g 🔹 🕨 Policy Ele	ments			
Authentication Define the Auther For Policy Export Policy Type	n Policy Itication Policy by s go to Administration Simple () Rule-	electing the protocols n > System > Backup -Based	s that ISE should use & Restore > Policy E	to communicate xport Page	with the netv	vork devices, and the i	dentity sources that it st	nould use for authentica
Ø 🗹 🕶	Rule name	: If	Wireless_802.1X A	ND Select Attribu	ite 🔍 A	low Protocols : Defau	It Network Access	ond —
	Default	: U:	Condition Na	inne [1X 📀 A ci	orary Description andition to m Radius:Cal	atch 802.1X based au ed-Sta 📀 🛛 Ends	thentication request	AND - AND

また、この認証ルールに一致するクライアントのアイデンティティ ソースを選択します。この例 では、*内部ユーザを使用します。*

Rule name : If Wireless_802.1X AND Radius:Call 🗇 Allow Protocols : Default N	Network Access 📀 and .
Image: Contract of the processing when authentication fails of the processing whence and the processing when authentication	dentity Source List
	DenyAccess Guest Users Guest_Portal_Sequence IdnetitySequence_JUST_Internal Internal Endpoints Internal Users

完了したら、[Done] と [Save] をクリックします。

Rule name	: If Wireless_802.1X AND Radius:Cal	Allow Protocols : Default Network Acces	is 📀 and 🕳	Done
Default	: Use 🛛 Internal Users 💠			Actions 👻
Save				

許可されるプロトコルのポリシーに関する詳細については以下のリンクを参照してください。

<u>許可されるプロトコル サービス(Allowed Protocols Service)</u>

アイデンティティ ソースに関する詳細については以下のリンクを参照してください。

<u>ユーザ ID グループの作成</u>

認証ルールの作成

認証ルールはクライアントがネットワークに接続するかどうかの判断基準になります。

ステップ1: [Policy] > [Authorization] へ移動します。

es Engine	e Home	► 0	ontext Visibility	•	Operations	▼Policy	 Administration 	► We	ork Centers
norization	Profiling Po	osture	Client Provision	ing	Policy Ele	Authentic	ation		Authorization
						Profiling		F	Posture
V Policy by co dministratio	onfiguring rules on > System > B	based) Jackup (on identity groups & Restore ≻ Policy	and/ Expo	or other condi ort Page	Client Pro	wisioning	F	Policy Elements Dictionaries Conditions Results

ステップ2:新規ルールを追加します。[Policy] > [Authorization] > [Insert New Rule Above/Below] **に進みます。**

altala cisco	Identity	Services Engine	e Home	 Context Visibility 	 Operations 		Administration	• Work Centers	License \
Authe	entication	Authorization	Profiling Post	ture Client Provisioning	 Policy Eleme 	ents			
diaurina ri	ules hased	on identity arouns a	and/or other cor	ditions. Drag and drop ru	les to change the	order			
> System	> Backup 8	Restore > Policy E	xport Page	anono, orag ana arop ra	to to onange the				
*									
		Conditions (i	identity groups	and other conditions)			Permissions		
									Insert New Rule Above
									Insert New Rule Below
									Duplicate Above
									Duplicate Below

ステップ3:情報を入力します。

まずルールの名前とユーザを保存する ID グループを選択します。この例では、ユーザは *ALL_ACCOUNTS のグループに保存されます。*

	Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
e e		NameAuthZrule	if Any Dind Condition(s)	💠 then AuthZ Pr 💠
	2	That .	if \$ 2	
	~	Minetes Table 1817 645-3	if ["ng Any 💽 🚽	less Acusto
	~	Profiled Cases and Larma	if C:)5)5
	~	Francis Mon Chen (P. Pistnak)	if Non	ي پنج
	Ø	Compliant_Devices_Auch.co	if Mat	efault) (default)
	0	Employas JEAP THE	if 114r GuestType_Contract	tor (default)
	0	Shipleyes Ophoenline	if (Mireless, 800.11/ AND EAP-MSCHAPV2) U ALL_ACCOUNTS (d	efault) CP_Options (2010) SMICH.
				1.6.10

次に、承認プロセスがこのルールに当てはまるように、その他の条件を選択します。この例では、802.1x Wireless を使用した場合、承認プロセスはこのルールに当てはまり、局 ID は *ise- ssid* で終了します。

Status	Rule Name	Conditions (identity groups	and other conditions)	Permissions	
1	NameAuthZrule	if AL 💠 and	Wireless_802.1X AND Radius:Call	😑 then AuthZ Pr 💠	
		15	💾 Add All Conditions Below to Librar	у	
		٩	Condition Name De	scription	AND -
			Wireless 802.1X 💟 Normalis	ed Radius:RadiusFlowType EQUALS Wireless802_1>	AND

最後にクライアントがネットワークに参加できる認証プロファイルを選択して [Done] 、[Save] **をクリックします。**

	Status	Rule Name	Conditions (identity	groups and other conditions)	Perm	nissions		
	-	NameAuthZrule	if AL <	and Wireless_802.1X AND Radius:Call	💠 then	PermitAc		Done
1	~							Edit 🕶
1						PermitAccess 💿 📼	÷	Edit 🕶
1						Standa	b	Edit 🕶
1	~						 - -	Edit 🕶
1	0					QL		Edit 🕶
1	0							Edit 🗸
	0					- C .		Edit I 🔻
-	0					1		Edit I 🗸
-	0					📿 Permi	Access	Edit I v
-								Edit I v
-		Default	if no matches, then	Denváccess				Editio
				en grievere				cuit •
Sa	ve Res	et						

オプションで、ワイヤレスクライアントを別のVLANに割り当てる新しい許可プロファイルを作 成します。

•		
(> -+	
	Standard	
	↓ ■ .	ŵ .
	😪 Blackhole_Wireless_Access	🎡 Add New Standard Profile

次の情報を入力します。

Add New Standard Pro	ile	_				×
Authorization Profile					^	
* Name	name-of-profile					
Description						
* Access Type	ACCESS_ACCEPT					
Network Device Profile	🗰 Cisco 💌 🕀					
Service Template						
Track Movement						
Passive Identity Tracking						
▼ Common Tasks						
DACL Name					^	
					- 11	
ACL (Filter-ID)						
M VLAN	Tag ID 1	Edit Tag ID/Name vlan-id			- 15	
Voice Domain Perm	ssion					
 Advanced Attribut 	es Settings					
					_	
Select an item	⊘ =	<u>o</u> - +				
 Attributes Details 	ACCEDT					
Tunnel-Private-Group-ID	= 1:vlan-id					
Tunnel-Medium-Type =	1:6					
<					×	1
					Save	incel

エンド デバイスの設定

PEAP/MS-CHAPv2 (Challenge Handshake Authentication Protocol バージョン 2 の Microsoft 版)を使用して 802.1x 認証で SSID と接続するように Windows 10 のラップトップを設定します。

この設定例で ISE は自己署名証明書を使用して認証を実行します。

Windows のマシンで WLAN プロファイルを作成するには、次の 2 つのオプションがあります。

- 1. ISE サーバを有効にし、信頼するようにマシンに自己署名証明書をインストールし、認証を 完成させる方法
- 2. RADIUS サーバの検証をバイパスし、認証に使用されるすべての RADIUS サーバを信頼す る方法(推奨されません)

これらのオプションの設定については、「<u>エンド デバイスの設定 - WLAN プロファイルの作成</u> <u>」ステップ 7 で説明しています。</u>

エンド デバイスの設定 - ISE 自己署名証明書のインストール

ステップ1:ISE から自己署名証明書をエクスポートします。

ISE にログインし、[Administration] > [System] > [Certificates] > [System Certificates] に移動しま す。

EAP 認証に使用した証明書を選択し、[Export] をクリックします。



必要な場所に証明書を保存します。この証明書は Windows マシンにインストールされます。

Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'					
	• Export Certificate Only				
	Export Certificate and Private Key				
*Private Key Password					
*Confirm Password					
Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.					
	Export				

ステップ2: Windows マシンに証明書をインストールします。

前にエクスポートした証明書をWindowsマシンにコピーし、ファイルの拡張子を.pemから.crtに 変更します。その後、ダブルクリックして[証明書のインストール]を選択**します。**

💀 Certificate	×
General Details Certification Path	
Certificate Information	
This CA Root certificate is not install this certificate in the Tu Authorities store.	trusted. To enable trust, rusted Root Certification
Issued to: EAP-SelfSigned	Certificate
Issued by: EAP-SelfSigned	Certificate
Valid from 23/11/2016 to	23/11/2018
Insta	I Certificate Issuer Statement
	ОК

インストール場所で [Local Machine] を選択し、[Next] をクリックします。

🔶 😸 Certificate Import Wizard	^
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location Current User Local Machine	
To continue, click Next.	
♥Next Cance	:1

[Place all certificates in the following store] を選択し、参照してから [Trusted Root Certification Authorities] を選択します。そのあと、[Next] をクリックします。

←	🚰 Certificate Import Wizard	^				
	Certificate Store Certificate stores are system areas where certificates are kept.					
	Windows can automatically select a certificate store, or you can specify a location for the certificate.					
	Automatically select the certificate store based on the type of certificate					
	Place all certificates in the following store Certificate store:					
	Trusted Root Certification Authorities Browse					
	Next Canc	el				

次に、[Finish] をクリックします。

÷	🛃 Certificate I	mport Wizard			×
	Comple	eting the Certific	ate Import Wizard		
	The certifica	ate will be imported after	you click Finish.		
	You have sr	pecified the following sett	ings:		
	Certificate	e Store Selected by User	Trusted Root Certification Authorities		
	Content		Certificate		
			Finish	Cance	1

最後に証明書のインストールを確認するには、[Yes] をクリックします。

Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Warning:

If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?



[OK] をクリックします。



エンド デバイスの設定:WLAN プロファイルの作成

ステップ1: [Start] アイコンを右クリックし、[Control Panel] を選択します。



ステップ 2: [Network and Internet] から [Network and Sharing Center] へ移動して、[Setup a new connection or network] をクリックします。

😫 Network and Sharing Center									
🔶 🔶 👻 🛧 💐 > Control Par	nel > Network and Internet > Network ar	nd Sharing Center							
Control Panel Home	View your basic network informa	ation and set up connections							
View your active networks Change adapter settings									
Change advanced sharing settings	Change advanced sharingcisco.comAccess type:InternetsettingsDomain networkConnections: Ethernet								
	Change your networking settings Set up a new connection or networking settings Set up a broadband, dial-up, or M Troubleshoot problems Diagnose and repair network proc	ork /PN connection; or set up a router or access point. oblems, or get troubleshooting information.							

ステップ 3 : [Manually connect to a wireless network] を選択し、[Next] をクリックします。

			_		Х
← 🐲	Set Up a Connection or Network				
Ch	oose a connection option				
	Connect to the Internet				
	Set up a broadband or dial-up connection to the Internet.				
-	Set up a new network				
4	Set up a new router or access point.				
	Manually connect to a wireless network				
-	Connect to a hidden network or create a new wireless profile.				
e	Connect to a workplace				
4	Set up a dial-up or VPN connection to your workplace.				
		Ne	avt	Cany	el
		INC	AL	Cant	.ei

ステップ 4:SSID の名前および WPA2-Enterprise のセキュリティタイプの情報を入力し、[Next] をクリックします。

				—		×
←	💐 Manually connect to a v	vireless network				
	Enter information fo	r the wireless network you want	t to add			
	Network name:	ise-ssid				
	Security type:	WPA2-Enterprise \vee				
	Encryption type:	AES 🗸				
	Security Key:	H	lide characte	rs		
	Start this connection	automatically				
	Connect even if the	network is not broadcasting				
	Warning: If you seled	t this option, your computer's privacy mig	ght be at risk	-		
			N	ext	Cano	:el

ステップ 5:WLAN プロファイルの設定をカスタマイズするには、[Change connection settings] を選択します。



ステップ 6 : [Security] タブに移動して [Settings] をクリックします。

ise-ssid Wireless Ne	twork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network aut	thentication method:		_	
Microsoft: Protected	EAP (PEAP) 🗸 🗸	Setting	js 🛛	
Remember my cre time I'm logged o	edentials for this connec n	tion each		
Advanced settings	•			
		ОК	Cance	el

ステップ7:RADIUS サーバが有効になっているかいないか選択します。

「はい」の場合は、「証明書を検証してサーバーのIDを確認する」を有効にし、「信頼できるル ート証明機関」のリストからISEの自己署名証明書を選択します。

その後、[Configure] を選択して [Automatically use my Windows logon name and password...] を 無効にし、[OK] をクリックします。

Protected EAP Properties	×								
When connecting:									
Verify the server's identity by validating the certificate									
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):									
Trusted Root Certification Authorities:									
Digging & Clobal Lines and Digging & Clobal Lines and	^								
EAP-SelfSignedCertificate									
 For Survey Deeple Configuration, St. Str. 199 L. S. Michaels, Letter work of the Str. Str. 200 E., S. S. Karler & C. S. Str. Str. Str. Str. 200 Construct Clabel 199 	~								
< >									
Notifications before connecting:									
Tell user if the server name or root certificate isn't specified	~								
Select Authentication Method:	_								
Secured password (EAP-MSCHAP v2) Configu	re								
✓ Enable Fast Reconnect									
Disconnect if server does not present cryptobinding TLV									
Enable Identity Privacy									
OK Can	el								

EAP MSCHAPv2 Properties						
When connecting:						
Automatically use my Windows logon name and password (and domain if any).						
OK Cancel						

ステップ8:ユーザクレデンシャルを設定します。

一度 [Security] **タブに戻って [Advanced settings]** を選択し、認証モードを [User authentication] として指定してユーザを認証するために ISE で設定されたクレデンシャルを保存します。

ise-ssid Wireless Network Properties $\qquad \qquad \qquad$							
Connection Security							
Security type:	WPA2-Enterprise		\sim				
Encryption type:	AES		\sim				
Choose a network aut	thentication method:						
Microsoft: Protected	EAP (PEAP)	Settin	gs				
Remember my cre time I'm logged o	edentials for this connect n	tion each					
Advanced settings							
		ОК	Cancel				

Advanced sett	ings		×						
802.1X settings	802.11 settings								
Specify a	uthentication mode:								
User aut	User authentication Save credentials								
Delet	e credentials for all users								
Enable si	ngle sign on for this network								
Perfo	rm immediately before user log	ion							
O Perfo	rm immediately after user logo	n							
Maximun	n delay (seconds):	10	*						
Allow sign o	additional dialogs to be display	ved during single							
This r and u	network uses separate virtual L user authentication	ANs for machine							
		ок	Cancel						

Windows Secu	rity	×
Save creder Saving your cre when you're no	ntials dentials allows your computer to connect to the network ot logged on (for example, to download updates).	:
.ı ı.ı ı. cısco	user1	
	OK Cancel	

確認

認証フローは WLC または ISE の観点から確認できます。

ME の認証プロセス

特定のユーザの認証プロセスをモニタするには、次のコマンドを実行します。

> debug client <mac-add-client>
認証の成功例(出力を一部省略しています):

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```

AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client *apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is *apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48) *apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3 *apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1 *spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45 *Dotlx_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47 *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries *Dot1x NW_MsqTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime. *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800 *Dotlx_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dotlx - moving mobile 08:74:02:77:13:45 into Connecting state *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1) *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: 08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253 *Dot1x NW MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800 *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2) *Dot1x NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16) *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent *Dot1x NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same. *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70) *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45 *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16) *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22) *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Starting key exchange to mobile

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45 *Dot1x NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45 *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dotlx - moving mobile 08:74:02:77:13:45 into Authenticated state *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK_START state (message 2) from mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!! *Dot1x NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!! *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0..... *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 of ac 04 01 00 00 of ac 04 01 00 00 Of *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 *Dot1x NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45 *Dot1x NW MsqTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45 state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45 *Dotlx NW MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3) *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce : *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload: *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0 *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224 *Dot1x NW_MsqTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1 *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload. *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00 *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name: *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4) *Dotlx_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6623, Adding TMP rule *Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule type = Airespace AP - Learn IP address

08:74:02:77:13:45, data packets will be dropped

on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0 IPv4 ACL ID = 255, IPv *apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role update request from Unassociated to Local Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136 *apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from Mobility-Incomplete to Mobility-Complete, mobility role=Local, client state=APF_MS_STATE_ASSOCIATED *apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6261, Adding TMP rule *apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule type = Airespace AP - Learn IP address on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0 IPv4 ACL ID = 255, *apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255) *pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0 *pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0 *apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB ip_learn_type 1, add_or_delete 1 *apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0 *apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug: regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller apf_ms.c:3593) *apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0 *apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB ip_learn_type 1, add_or_delete 1 *apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state to RUN (20) last state DHCP_REQD (7) デバッグ クライアントの出力を簡単に読むための手段として、 ワイヤレス デバッグ アナライザ ツールを使用します。

<u> ワイヤレス デバッグ アナライザ</u>

ISE の認証プロセス

[Operations] > [RADIUS] > [Live Logs] に移動してどの認証ポリシーと認可ポリシー、認証プロフ アイルがユーザに割り当てられているか確認できます。

altalta cisco	Identi	ty Service:	s Engine	Home	+ Cont	ext Visibility	- Operation	s Policy	 Administra 	ation 🔸	Work Centers		License
▼RA	DIUS	TC-NAC Liv	e Logs	+ TACACS	Reports	In Troublesh	noot 🕨 Adapti	ve Network Con	trol				
Live	Logs	Live Sessio	ns										
Misconfigured Supplicants Misconfigured Network RADIUS Drops O Client Stopped Responding							ing Repea						
OR	lefresh	🗢 Reset	Repeat Co	ounts ∠E	ixport To 🕶		0			Refresh	Never	Sho	w Latest 20 record:
	Time	Sta	Details	lde	Endpoin	nt ID I	Endpoint	Authenticatio	on Policy	Autho	orization Polic	y Autho	rization Profiles
	No	1	Q	user1	08:74:02:	77:13:45	Apple-Device	Default >> Rule	:name >> Defau	it Defaul	t >> NameAuthZ	rule PermitA	Access

もっと詳細の認証プロセスを見るには、[Details] をクリックします。