Override 802.1x WLAN + VLAN con Mobility Express (ME) 8.2 e ISE 2.1

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Configurazione Esempio di rete Configurazioni Configurazione su ME **Dichiaratemi ad ISE** Crea un nuovo utente su ISE Creare la regola di autenticazione Creare la regola di autorizzazione Configurazione del dispositivo terminale Verifica Processo di autenticazione in ME Processo di autenticazione su ISE

Introduzione

In questo documento viene descritto come configurare una WLAN (Wireless Local Area Network) con protezione aziendale Wi-Fi Protected Access 2 (WPA2) con un controller Mobility Express e un server esterno RADIUS (Remote Authentication Dial-In User Service). Identity Service Engine (ISE) è utilizzato come esempio di server RADIUS esterni.

Il protocollo EAP (Extensible Authentication Protocol) utilizzato in questa guida è PEAP (Protected Extensible Authentication Protocol). Inoltre, il client è assegnato a una VLAN specifica (diversa da quella assegnata alla WLAN per impostazione predefinita).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 802.1x
- PEAP
- CA (Certification Authority)
- Certificati

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

ME v8.2

ISE v2.1

Notebook Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazioni

Le fasi generali sono:

- 1. Creare il Service Set Identifier (SSID) in ME e dichiarare il server RADIUS (ISE in questo esempio) in ME
- 2. Dichiara ME su server RADIUS (ISE)
- 3. Crea la regola di autenticazione su ISE
- 4. Creare la regola di autorizzazione in ISE
- 5. Configurare l'endpoint

Configurazione su ME

Per consentire la comunicazione tra il server RADIUS e ME è necessario registrare il server RADIUS su ME e viceversa. In questo passaggio viene illustrato come registrare il server RADIUS su ME.

Passaggio 1. Aprire la GUI di ME e passare a Wireless Settings (Impostazioni wireless) > WLAN > Add new WLAN (Aggiungi nuova WLAN).



Passaggio 2. Selezionare un nome per la WLAN.

Add Ne	w WLAN		×
General	WLAN Security	VLAN & Firewall	QoS
	WLAN Id	3 •	
	Profile Name *	me-ise	
	SSID *	me-ise	
	Admin State	Enabled 🔹	
	Radio Policy	ALL .	
		🛛 📿 App	ly 🛞 Cancel

Passaggio 3. Specificare la configurazione di protezione nella scheda **Protezione WLAN**.

Scegliere **WPA2 Enterprise**, per il server di autenticazione scegliere **RAGGIO esterno**. Fare clic sull'opzione di modifica per aggiungere l'indirizzo IP del RADIUS e scegliere una chiave **segreta condivisa**.



Add N	ew WLAN	×
General	WLAN Security	VLAN & Firewall QoS
Authe	Security ntication Server	WPA2 Enterprise 🔹 External Radius 🔹
 ✓ ✓ 	Radius IP 🔺	Radius Port Shared Secret 1812 ••••••• e enter valid IPv4 address •••••••
External F all WLANs	Radius configuration a s	applies to 🛛 🖉 Apply 💌 Cancel

<a.b.c.d> corrisponde al server RADIUS.

Passaggio 4. Assegnare una VLAN all'SSID.

Se l'SSID deve essere assegnato alla VLAN dell'access point, questo passaggio può essere ignorato.

Per assegnare gli utenti per questo SSID a una VLAN specifica (diversa dalla VLAN dell'access point), abilitare **Use VLAN Tagging** e assegnare l'**ID VLAN** desiderato.

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				

Nota: Se si usa il tagging VLAN, verificare che la porta dello switch a cui è connesso il punto di accesso sia configurata come porta trunk e che la VLAN dell'access point sia configurata come nativa.

Passaggio 5. Fare clic su Apply (Applica) per completare la configurazione.

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				

Passaggio 6. Facoltativo, configurare la WLAN in modo che accetti l'override della VLAN.

Abilitare l'override AAA sulla WLAN e aggiungere le VLAN necessarie. A tale scopo, è necessario aprire una sessione CLI sull'interfaccia di gestione ME ed eseguire i seguenti comandi:

```
>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>
Dichiaratemi ad ISE
```

Passaggio 1. Aprire la console ISE e selezionare Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi.

elisio Identity Serv	rices Engine Hom	e 🔹 🕨 Context V	isibility 🔹 🕨 Operati	ons 🔹 🕨 Policy	 Administration 	→ Worl
▶ System → Ident	iity Management 🛛 🕶 Netw	ork Resources	Device Portal Man	agement pxGrid	d Services 🔹 🕨 Feed Se	ervice I
▼Network Devices	Network Device Groups	Network Devic	e Profiles External	RADIUS Servers	RADIUS Server Sequ	ences
	Ø					
Network devices	Ne	twork Devices				
Default Device	/	Edit 🕂 Add 🕞	Duplicate	Export 👻 🖸	Generate PAC	te 🔻

Passaggio 2. Immettere le informazioni.

Facoltativamente, è possibile specificare il nome del modello, la versione del software, la

descrizione e assegnare i gruppi di dispositivi di rete in base al tipo di dispositivo, alla posizione o ai WLC.

a.b.c.d corrisponde all'indirizzo IP dell'utente corrente.

Network Devices List > New Network Device Network Devices
* Name WLC-name
Description optional description
* IP Address: a.b.c.d / 32
* Device Profile 🛛 😹 Cisco 👻 🕀
Model Name
wic-software 🛬
* Network Device Group
Device Type WLCs-2504 📀 Set To Default
WI CS WI C
WECS Sec To Default
RADIUS Authentication Settings
Enable Authentication Settings
Protocol RADIUS
* Shared Secret Show
Enable KeyWrap 🔲 🕢
* Key Encryption Key Show
* Message Authenticator Code Key
Key Input Format ASCIL HEXADECIMAL
CoA Port 1700

Per ulteriori informazioni sui gruppi di dispositivi di rete, vedere questo collegamento:

ISE - Gruppi di dispositivi di rete

Crea un nuovo utente su ISE

Passaggio 1. Passare a Amministrazione > Gestione delle identità > Identità > Utenti > Aggiungi.

diale Identity Services Engine	Home	Context Visibility	Operations	▶ Policy	 Administration
► System	• Network F	Resources 🔹 🕨 Device	e Portal Managemer	nt pxGrid 8	System
■Identities Groups External Iden	itity Sources	Identity Source Seq	uences 🕨 Setting	s	Deployment Licensing
C Users	Networ	k Access Users			Certificates Logging Maintenance
Latest Manual Network Scan Res	/ Edit	+ Add 🔣 Change St	atus 👻 🕵 Import	Export -	Upgrade Backup & Restor
	Stat	ading		Description	Admin Access Settings
					Identity Managem

Passaggio 2. Immettere le informazioni.

In questo esempio l'utente appartiene a un gruppo denominato ALL_ACCOUNTS ma può essere adeguato in base alle esigenze.

Network Access Users List > New Network Access User	
Network Access User	
*Name user1	
Status 🔽 Enabled 👻	
Email	
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 Grouns	
Submit Cancel	

Creare la regola di autenticazione

Le regole di autenticazione vengono utilizzate per verificare se le credenziali degli utenti sono corrette, ovvero per verificare se l'utente è effettivamente l'utente a cui sono state assegnate, e

per limitare i metodi di autenticazione consentiti.

Passaggio 1. Naviga in Criteri > Autenticazione.



Passaggio 2. Inserire una nuova regola di autenticazione.

A tale scopo, passare a Criterio > Autenticazione > Inserisci nuova riga sopra/sotto.

diale Identity Services Engine	Home 🔸 Context Visibility	Operations → Policy	▶ Administration	▶ Work Centers	Li
Authentication Authorization Pr	Profiling Posture Client Provision	ning 🔹 Policy Elements			
ting the protocols that ISE should use to o system > Backup & Restore > Policy Expo ed	communicate with the network device nt Page	es, and the identity sources that i	t should use for auther	ntication.	
: If Wired_MAB OR _Protocols and :use Internal Endpoints					Insert new row above
: If Wired_802.1X OR IC_Protocols and					Duplicate below

Passaggio 3. Inserire le informazioni necessarie

Questo esempio di regola di autenticazione consente di utilizzare tutti i protocolli elencati nell'elenco **Accesso alla rete predefinito**, applicabile alla richiesta di autenticazione per i client Wireless 802.1x e con ID stazione chiamata e terminante con *ise-ssid*.

the intervices Engine Home + C	Context Visibility ► Operations ▼Policy	Administration Work Centers
Authentication Authorization Profiling Posture	Client Provisioning	
Authentication Policy Define the Authentication Policy by selecting the protocols For Policy Export on to Administration > System > Backup	that ISE should use to communicate with the netw	vork devices, and the identity sources that it should use for authentica
Policy Type O Simple Rule-Based	a restore - Fondy Export Fuge	
if Rule name	Wireless_802.1X AND Select Attribute	llow Protocols : Default Network Access 📀 and 🕳
Default : Us	Add All Conditions Below to Library Condition Name Description Wireless_802.1X A condition to m Desting Call	AND AND AND AND AND AND AND AND AND AND AND

Scegliere inoltre l'origine Identità per i client che soddisfano questa regola di autenticazione. In questo esempio viene utilizzato *Utenti interni*

Rule name : If War	eless_802.1X AND Radius:Call	It Network Access 📀 and .
✓ Default : Use	Internal Users Identity Source Internal Users Options If authentication failed Reject If user not found Reject If user not found Reject If process failed Drop V Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or it is not possible to continue processing when authentication fails o If continue option is selected in these cases, requests will be reject	Identity Source List
		Tureural Ozeiz

Al termine, fate clic su Fatto (Done) e Salva (Save)

🖉 🖌 🗹 🗸 Rule name : If 🛛 Wireless_802.1X AND Radius:Cal 💠 Allow Protocols : Default Network Access 📀 and —	Done
Default : Use Internal Users 💠	Actions 👻
Save	

Per ulteriori informazioni su Consenti criteri protocolli, vedere questo collegamento:

Servizio Protocolli consentiti

Per ulteriori informazioni sulle origini di identità, vedere questo collegamento:

Crea un gruppo di identità utente

Creare la regola di autorizzazione

La regola di autorizzazione è quella incaricata di determinare se al client è consentito o meno connettersi alla rete

Passaggio 1. Passare a Criterio > Autorizzazione.

es Engine	e Home	► C	ontext Visibility	Operations	▼Policy	Administration	Work Centers
norization	Profiling Po	osture	Client Provisionin	g 🔹 🕨 Policy Ele	Authentic	ation	Authorization
					Profiling		Posture
V Policy by co dministratio plies	onfiguring rules on > System > E	based (Backup &	on identity groups a k Restore ≻ Policy E	nd/or other condi xport Page	Client Pro	wisioning	Policy Elements Dictionaries Conditions Results

Passaggio 2. Inserire una nuova regola. Passare a **Criterio > Autorizzazione > Inserisci nuova** regola sopra/sotto.

ditajn cisco	Identity S	Services Engine	Home	Context Visibility	Operations	* Policy	Administration	Work Centers	License V
Authe	entication	Authorization Pr	ofiling Postu	re Client Provisioning	Policy Eleme	ents			
riaurina ru	les based o	n identity groups an	d/or other cond	tions. Drag and drop ru	les to change the	order.			
> System	> Backup &	Restore > Policy Exp	oort Page						
*									
		A	171	1 - H			B 1		
		Conditions (id	entity groups ar	id other conditions)			Permissions		_
									Insert New Rule Above
									Insert New Rule Below
									Duplicate Above Duplicate Below

Passaggio 3. Immettere le informazioni.

Scegliere innanzitutto un nome per la regola e i gruppi di identità in cui è memorizzato l'utente. In questo esempio l'utente è memorizzato nel gruppo *ALL_ACCOUNTS*.

	Status	Rule Name	Соп	ditions (identity groups and other conditions)	Permissions	
1		NameAuthZrule		Any Pland Condition(s)	then AuthZ Pr	. ¢
	~	75.5	f Vi			
	~	Minetes Thank and deep a	f Ela	Any Ol -+		less Acuma
		Profiled Ciscolary Lauris	f Ci	User Identity Groups	C	s
	~	Francis Mon Cheo (R.Phones	f Nor	↓	•	ગણ્યુલ
	0	Compliant_Devices_Authors	f (Na	GuestType_Daily(default) GuestType_Weekly(default)		
	0	Employes JEAP THE	f (114 1845	GuestType_Contractor (default)		NE
1	0	Employee Ophoending	f (031	EAP-MSCHAPV2 ALL_ACCOUNTS (default)	07_05/2×1	0.0.9200
	-					

In seguito scegliere altre condizioni che fanno rientrare il processo di autorizzazione in questa regola. In questo esempio il processo di autorizzazione rileva questa regola se utilizza una connessione wireless 802.1x e viene chiamato ID stazione e termina con *ise-ssid*.

	Status	Rule Name	Conditions (identity groups a	and other conditions)	Permissions	
0	-	NameAuthZrule	if AL 💠 and	Wireless_802.1X AND Radius:Call	😑 then AuthZ Pr 💠	
1	~		S	💾 Add All Conditions Below to Librar	У	
	~		<i>۵</i> ,	Condition Name De	escription	AND -
				Wireless 802.1X 📀 Normali	sed Radius:RadiusFlowType EQUALS Wireless802_1>	AND
1	<u>~</u>		e			

Infine, scegliere il profilo di autorizzazione che consente ai client di connettersi alla rete, fare clic su **Fine** e **Salva**.

	Status	Rule Name	Conditions (ider	tity groups and other conditions))	Permi	issions		
	-	NameAuthZrule	if AL		ND Radius:Call	💠 then	PermitAc		Done
1	<u>~</u>								Edit 🕶
1						1	PermitAccess		Edit 🕶
1								Standard	Edit 🕶
1	<u>~</u>								Edit -
1	0							€ E	Edit 🕶
1	0								Edit 🕶
1	0								Edit 🕶
1	0								Edit 🕶
1	0							PermitAccess	Edit -
1									Edit 🕶
	~	Default	if no matches, the	DenyAccess					Edit 🕶
	_								
Sa	ve Res	et							

Facoltativamente, creare un nuovo profilo di autorizzazione che assegni il client wireless a una VLAN diversa:

•		
6) — ÷	
	Standard	
	⟨= • ≡ •	د <u>ن</u> ي -
	😪 Blackhole_Wireless_Access	🎡 Add New Standard Profile

Immettere le informazioni:

Add New Standard Pro	file		1
Authorization Profile		í	ì .
* Name	e name-of-profile		
Description			
* Access Type	access_accept		
Network Device Profile	the Cisco 🔹 🕀		
Service Template			
Track Movement			
Passive Identity Tracking	9 D 0		
▼ Common Tasks			
DACL Name		^	
		- 84	
ACL (Filter-ID)			
_			
🗹 VLAN	Tag ID 1 Edit Tag IDName Van-id		
Voice Domain Perm	nission		
		Ŷ	
 Advanced Attribut 	tes Settings		
Select an item			
 Attributes Details 			
Access Type = ACCESS Tunnel-Private-Group-ID Tunnel-Type = 1:13 Tunnel-Medium-Type =	LACEPT D = 1:vbn-id 1:6		
americanite type -			
C		>	
		Save	ance

Configurazione del dispositivo terminale

Configurare un portatile Windows 10 per la connessione a un SSID con autenticazione 802.1x utilizzando PEAP/MS-CHAPv2 (versione Microsoft del protocollo Challenge-Handshake Authentication versione 2).

In questo esempio di configurazione, ISE utilizza il proprio certificato autofirmato per eseguire l'autenticazione.

Per creare il profilo WLAN sul computer Windows, sono disponibili due opzioni:

- 1. Installa il certificato autofirmato nel computer per convalidare e considerare attendibile il server ISE per completare l'autenticazione
- 2. Ignora la convalida del server RADIUS e considera attendibile qualsiasi server RADIUS utilizzato per eseguire l'autenticazione (scelta non consigliata, in quanto può diventare un problema di sicurezza)

La configurazione di queste opzioni è spiegata in <u>Configurazione del dispositivo terminale -</u> <u>Creazione del profilo WLAN - Passaggio 7</u>.

Fine configurazione dispositivo - Installa certificato autofirmato ISE

Passaggio 1. Esportare il certificato autofirmato da ISE.

Accedere ad ISE e selezionare Amministrazione > Sistema > Certificati > Certificati di sistema.

Selezionare quindi il certificato utilizzato per l'autenticazione EAP e fare clic su Esporta.



Salvare il certificato nella posizione desiderata. Il certificato è installato nel computer Windows.

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 ke	у.
Export	:el

Passaggio 2. Installare il certificato nel computer Windows.

Copiare il certificato esportato in precedenza nel computer Windows, modificare l'estensione del file da .pem a .crt, dopo che il doppio clic su di esso e selezionare **Installa certificato...**.

👼 Certificate	×			
General Details Certification Path				
Certificate Information				
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.				
Issued to: EAP-SelfSignedCertificate	,			
Issued by: EAP-SelfSignedCertificate	,			
Valid from 23/11/2016 to 23/11/2	018			
Install Certificat	e Issuer Statement			
	ОК			

Scegliere di installarlo nel computer locale, quindi fare clic su Avanti.

🔶 😸 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 Occal Machine	
To continue, click Next.	
	_
Sext Cance	1

Selezionare Colloca tutti i certificati nel seguente archivio, quindi individuare e scegliere Autorità di certificazione radice attendibili. Quindi, fare clic su Next (Avanti).

🚰 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.	
O 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 Cano	el
	Certificate Import Wizard Certificate Store Certificate stores are system areas where certificates are kept. Mindows 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 store. Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse

Quindi fare clic su Fine.

🗲 🛭 🛃 Certificate Import Wizard	^
Completing the Certificate I	mport Wizard
The certificate will be imported after you clic	k Finish.
You have specified the following settings:	
Certificate Store Selected by User Trustee	d Root Certification Authorities
Content Certific	ate
	Finish Cancel

Alla fine fare clic su Sì per confermare l'installazione del certificato.

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?



Infine fare clic su OK.



Fine configurazione dispositivo - Creazione del profilo WLAN

Passaggio 1. Fare clic con il pulsante destro del mouse sull'icona **Start** e selezionare **Pannello di** controllo.

	Programs and Features
	Mobility Center
	Power Options
	Event Viewer
	System
	Device Manager
	Network Connections
	Disk Management
	Computer Management
	Command Prompt
	Command Prompt (Admin)
	Task Manager
	Control Panel
	File Explorer
	Search
	Run
	Shut down or sign out
	Desktop
E	א נון 📮 Downi 👽 Networ 👳 א

Passaggio 2. Passare a **Rete e Internet**, quindi a **Centro connessioni di rete e condivisione** e fare clic su **Configura nuova connessione o rete.**

🔩 Network and Sharing Center									
← → ✓ ↑ 💐 > Control Panel > Network and Internet > Network and Sharing Center									
Control Panel Home View your basic network information and set up connections									
Change adapter settings	View your active networks								
Change advanced sharing settings	cisco.com Domain network	Access type: Internet Connections: <i>Iternet</i>							
	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connection Troubleshoot problems Diagnose and repair network problems, or get	on; or set up a router or access point. t troubleshooting information.							

Passaggio 3. Selezionare Connetti manualmente a una rete wireless e fare clic su Avanti.

	_		\times
🔶 🛬 Set Up a Connection or Network			
Choose a connection option			
Connect to the Internet			
Set up a broadband or dial-up connection to the Internet.			
Set up a new network			
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.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
	Next	Can	cel

Passaggio 4. Immettere le informazioni con il nome del SSID e il tipo di protezione WPA2-Enterprise e fare clic su **Avanti**.

				—		×
←	💐 Manually connect to a v	vireless network				
	Enter information for	r the wireless network	you want to add			
	Network name:	ise-ssid				
	Security type:	WPA2-Enterprise	\sim			
	Encryption type:	AES	\sim			
	Security Key:		Hide charac	ters		
	Start this connection	automatically				
	Connect even if the r	network is not broadcasting				
	Warning: If you seled	t this option, your computer's	privacy might be at ri	sk.		
				Next	Cano	cel

Passaggio 5. Selezionare **Change connection settings** per personalizzare la configurazione del profilo WLAN.

		—		×
~	💐 Manually connect to a wireless network			
	Successfully added ise-ssid			
	\rightarrow Change connection settings			
	Open the connection properties so that I can change the settings.			
			Clo	5.A
			CIU	50

Passaggio 6. Passare alla scheda Protezione e fare clic su Impostazioni.

ise-ssid Wireless N	etwork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network au	thentication method:		_	
Microsoft: Protected	EAP (PEAP)	Settin	gs	
Remember my cr time I'm logged o	edentials for this connector	tion each		
Advanced setting	s			
		ОК	Can	cel

Passaggio 7. Scegliere se il server RADIUS è convalidato o meno.

In caso affermativo, abilitare Verifica dell'identità del server convalidando il certificato e dall'elenco Autorità di certificazione fonti attendibili selezionare il certificato autofirmato ISE.

Quindi selezionare **Configure** and disable **Automatically use my Windows logon name and password...**, quindi fare clic su **OK**

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:									
Eggille & Clobel Line and	^								
EAP-SelfSignedCertificate									
 Fortunet Road Contribution for the fortune Low Science Contribution (1977) Sup (1977) E., Contribution (1972) State Science Lag Contribution (1972) 	~								
< >									
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								
C Enable Fast Reconnect									
Disconnect if server does not present cryptobinding TLV									
Enable Identity Privacy									
OK Cano	el								

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

Una volta tornati alla scheda **Sicurezza**, selezionare **Impostazioni avanzate**, specificare la modalità di autenticazione come **Autenticazione utente** e salvare le credenziali configurate su ISE per autenticare l'utente.

ise-ssid Wireless Network Properties X								
Connection Security								
Security type:	WPA2-Enterprise		\sim					
Encryption type:	AES		\sim					
Choose a network au	thentication method:		_					
Microsoft: Protected	EAP (PEAP) 🗸 🗸	Settin	igs					
Remember my cro time I'm logged o	edentials for this connect n	ion each						
	_							
Advanced settings	5							
		ок	Cancel					

Advanced sett	ings		×
802.1X settings	802.11 settings		
Specify a	uthentication mode:		
User aut	hentication $$	Save credent	tials
Delete	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 on	ed during single	
This r and u	network uses separate virtual L ser authentication	ANs for machine	
		ОК	Cancel

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

Verifica

Il flusso di autenticazione può essere verificato dal WLC o dalla prospettiva ISE.

Processo di autenticazione in ME

Eseguire questo comando per monitorare il processo di autenticazione per un utente specifico:

> debug client <mac-add-client>
Esempio di autenticazione riuscita (alcuni output sono stati omessi):

```
*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 00.00.00.00.00.00.00.00 *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)

Per leggere facilmente gli output dei client di debug, usare lo strumento Wireless debug analyzer.

Wireless Debug Analyzer

Processo di autenticazione su ISE

Passare a **Operazioni > RADIUS > Live Log** per verificare il criterio di autenticazione, il criterio di autorizzazione e il profilo di autorizzazione assegnati all'utente.

diala cisco	Identi	ty Service	s Engine	Home	♦ Context V	'isibility	•Operations	Policy ■	• Administra	ation 🔸	Work Centers		License
▼RA	DIUS	TC-NAC Liv	ve Logs	+ TACACS	Reports + Tr	roubleshoot	 Adaptive 	Network Cont	rol				
Live I	Logs	Live Sessio	ons										
Misconfigured Supplica		ants Mi	isconfigure Device O	d Network s	ą	ADIUS Drops	Ø	Client Stopp	ed Responding • 4 • channel	g Repea			
C Refresh						Latest 20 record.							
	Time	Sta	Details	lde	Endpoint ID	Endp	ooint 🛛 A	Authenticatio	n Policy	Autho	orization Policy	/ Authoriz	ation Profiles
	No	0	à	user1	08:74:02:77:13	3:45 Apple	-Device D)efault >> Rule	name ≻> Defau	ilt Defaul	t >> NameAuthZr	ule PermitAco	ess

Per ulteriori informazioni, fare clic su **Details** (Dettagli) per visualizzare un processo di autenticazione più dettagliato.