Configurazione dell'autenticazione 802.1X con PEAP, ISE 2.1 e WLC 8.3

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Esempio di rete
Configurazione
Dichiara server RADIUS su WLC
Crea SSID
Dichiarare WLC su ISE
Creazione di un nuovo utente in ISE
Crea regola di autenticazione
Creazione del profilo di autorizzazione
Crea regola di autorizzazione
Configurazione del dispositivo finale
Fine configurazione dispositivo - Installazione certificato autofirmato ISE
End Device Configuration - Creazione del profilo WLAN
Verifica
Processo di autenticazione su WLC
Processo di autenticazione su ISE
Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare una rete WLAN (Wireless Local Area Network) con sicurezza 802.1x e override della VLAN (Virtual Local Area Network).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 802.1x
- PEAP (Protected Extensible Authentication Protocol)
- CA (Certification Authority)
- Certificati

Componenti usati

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

- WLC v8.3.102.0
- Identity Service Engine (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.

Premesse

Quando si configura una WLAN con sicurezza 802.1x e VLAN, è possibile ignorare il protocollo EAP (Protected Extensible Authentication Protocol).

Configurazione

Esempio di rete



Configurazione

Le fasi generali sono le seguenti:

- 1. Dichiarare il server RADIUS su WLC e viceversa per consentire la comunicazione reciproca.
- 2. Creare I'SSID (Service Set Identifier) nel WLC.
- 3. Creare la regola di autenticazione in ISE.
- 4. Creare il profilo di autorizzazione su ISE.
- 5. Creare la regola di autorizzazione in ISE.
- 6. Configurare l'endpoint.

Dichiara server RADIUS su WLC

Per consentire la comunicazione tra il server RADIUS e il WLC, è necessario registrare il server RADIUS sul WLC e viceversa.

GUI:

Passaggio 1. Aprire la GUI del WLC e selezionare SECURITY > RADIUS > Authentication > New (SICUREZZA > RADIUS > Autenticazione > Nuovo), come mostrato nell'immagine.



Passaggio 2. Immettere le informazioni sul server RADIUS come mostrato nell'immagine.

_								
R	ADIUS Authentication Serve	ers > New						
	Server Index (Priority)	2 ~	_					
	Server IP Address(Ipv4/Ipv6)	a.b.c.d						
	Shared Secret Format	ASCII 🗸						
	Shared Secret	•••••						
	Confirm Shared Secret	•••••						
	Key Wrap	(Designed fo)	r FIPS customers and requires a key wrap compliant RADIUS server)					
	Port Number	1812						
	Server Status	Enabled \sim						
	Support for CoA	Disabled $\!$						
	Server Timeout	10 seconds	5					
	Network User	🗹 Enable						
	Management	🗹 Enable						
	Management Retransmit Timeout	2 seconds						
	IPSec	Enable						

```
CLI:
```

```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

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

Crea SSID

GUI:

Passaggio 1. Aprire la GUI del WLC e selezionare WLAN > Create New > Go (WLAN > Crea nuovo > Vai), come mostrato nell'immagine.

،، ،،، ،، cısco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
WLANs	WLANs									
WLANS WLANS WLANS Advanced	Current Filt	ter: Not	ne [<u>Cha</u>	nge Filter] [Cl	<u>ear Filter]</u>		[Create N	lew V	ìo

Passaggio 2. Scegliere un nome per il SSID e il profilo, quindi fare clic su Apply (Applica) come mostrato nell'immagine.

Ν	/LANs > New		< Back	Apply
	Туре	WLAN V		
	Profile Name	profile-name		
	SSID	SSID-name		
	ID	2 ~		

CLI:

> config wlan create <id> <profile-name> <ssid-name>

Passaggio 3. Assegnare il server RADIUS alla WLAN.

CLI:

> config wlan radius_server auth add <wlan-id> <radius-index>

GUI:

Passare a Sicurezza > Server AAA e scegliere il server RADIUS desiderato, quindi fare clic su Applica come mostrato nell'immagine.

WLANs > Edit 'ise-prof'	< Back	Apply
General Security QoS Policy-Mapping Advanced		
Layer 2 Layer 3 AAA Servers		
		^
Select AAA servers below to override use of default servers on this WLAN		
RADIUS Servers		
RADIUS Server Overwrite interface		
Authentication Servers Accounting Servers EAP Parameters		
Enabled Enable		
Server 1 IP:172.16.15.8, Port:1812 V None V		
Server 2 None V None V		
Server 3 None V None V		
Server 4 None V None V		
Server 5 None V None V		
Server 6 None V None V		
RADIUS Server Accounting		
Interim Update 🗹 Interim Interval 0 Seconds		×
	2	>

Passaggio 4. Abilitare Consenti sostituzione AAA e, facoltativamente, aumentare il timeout della sessione

CLI:

> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>

GUI:

Selezionare WLAN > ID WLAN > Avanzate e abilitare Consenti sostituzione AAA. Facoltativamente, specificare il timeout della sessione come mostrato nell'immagine.

WLANs > Edit 'ise-pr	of'			< Back	
General Security	QoS Policy-Mapping	Advanced			
	_				^
Allow AAA Override	🗹 Enabled	DHCP			
Coverage Hole Detection	🗹 Enabled	DHC	P Server	Override	
Enable Session Timeout	Session Timeou (secs)	DHC Assi	P Addr. gnment	Required	
Aironet IE	Enabled	OEAP			
Diagnostic Channel <u>18</u>	Enabled	Spli	t Tunnel	Enabled	
Override Interface ACL	IPv4 None 🗸	IPv6 None 😪 Manage	ement Frame Prot	ection (MFP)	
Layer2 Ad	None 🗸				
URL ACL	None 🗸	MFP	Client Protection d	🖞 Optional 🗸	
P2P Blocking Action	Disabled \lor	DTIM P	eriod (in beacon in	itervals)	
Client Exclusion 🛂	Enabled 60 Timeout Value (secs)	802	.11a/n (1 - 255)	1	
Maximum Allowed Clients 🗳	0	802. NAC	.11b/g/n (1 - 255)	1	
Static IP Tunneling	□	NAC	State None	V	>

Passaggio 5. Abilitare la WLAN.

CLI:

> config wlan enable <wlan-id>

GUI:

Selezionare WLAN > ID WLAN > Generale e abilitare l'SSID come mostrato nell'immagine.

WLANs>Edit 'ise-p	prof'	< Back	Apply
General Securit	y QoS Policy-Mapping Advanced		
Profile Name Type SSID Status	ise-prof WLAN ise-ssid C Enabled		
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)		
Radio Policy Interface/Interface Group(G) Multicast Vlan Feature Broadcast SSID NAS-ID	All management Enabled Fnabled none		

Dichiarare WLC su ISE

Passaggio 1. Aprire la console ISE e selezionare Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi, come mostrato nell'immagine.

dialo Identity Serv	rices Engine – _H	Home 💦 🕨 Context \	∕isibility ► Operati	ons 🕨 Policy	 Administration 	► Worl
▶ System → Ident	ity Management 🔽	Network Resources	Device Portal Mana	agement pxGrid S	Services 🔹 🕨 Feed Se	ervice I
✓ Network Devices	Network Device Gro	oups Network Devic	e Profiles External !	RADIUS Servers	RADIUS Server Sequi	ences
	ġ					
Network devices		Network Devices	3			
Default Device						
		/ Edit 🕂 Add 🖸	Duplicate	🚯 Export 👻 🙆 G	enerate PAC XDele	te 🔻

Passaggio 2. Immettere i valori.

Facoltativamente, può corrispondere a un nome di modello, una versione del software, una descrizione e l'assegnazione di gruppi di dispositivi di rete in base al tipo di dispositivo, alla posizione o ai WLC.

a.b.c.d corrisponde all'interfaccia WLC che invia l'autenticazione richiesta. Per impostazione predefinita, si tratta dell'interfaccia di gestione, come illustrato nell'immagine.

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-model 🝷						
Software Version w/c-software						
me solemate 2						
* Network Device Group						
Set To Default						
Location All Locations 📀 Set To Default						
WLCs 😡 📀 Set To Default						
✓ 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						

Per ulteriori informazioni sui gruppi di dispositivi di rete:

Passaggio 1. Passare a Amministrazione > Gestione delle identità > Identità > Utenti > Aggiungi come mostrato nell'immagine.

dialo Identity Services Engine	Home	d Visibility 🔹 🕨 Op	erations	▶ Policy	 Administration
System ▼Identity Management	• Network Resources	Device Portal	Managemer	nt pxGrid 8	System
◄Identities Groups External Iden	tity Sources Identity	Source Sequences	▶ Setting	s	Deployment Licensing
C Users	Network Access	s Users			Certificates Logging Maintenance
Latest Manual Network Scan Res	/ Edit Add	🔀 Change Status 👻	() Import	Export -	Upgrade Backup & Restor Admin Access
	Loading	Name		Description	Settings
					Identity Managem

Passaggio 2. Immettere le informazioni.

In questo esempio, l'utente appartiene a un gruppo denominato ALL_ACCOUNTS, ma può essere regolato in base alle esigenze, come mostrato nell'immagine.

Network Access Users List > New Network Access User							
Network Access User							
* Name user1							
Status 🗾 Enable	d 💌						
Email							
 Passwords 							
Password Type:	Internal Users	×					
	Password		Re-Enter Passw				
* Login Password	•••••		•••••				
Enable Password							
👻 User Informati	on						
First Name							
Last Name							
Account Optio	ns						
	Description						
Change password on next login 🔲							
Account Disable Policy							
Disable accourt	nt if date exceeds	2017-01-21					

2. Ignorare la convalida del server RADIUS e considerare 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 Configurazione del dispositivo terminale -Creazione del profilo WLAN - Passaggio 7.

Fine configurazione dispositivo - Installazione certificato autofirmato ISE

Passaggio 1. Esporta certificato autofirmato.

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

Scegliere quindi il certificato utilizzato per l'autenticazione EAP e fare clic su Esporta, come mostrato nell'immagine.



Salvare il certificato nella posizione desiderata. Tale certificato deve essere installato nel computer Windows come illustrato nell'immagine.

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 o	of the private key.				
	Export Cancel				

Passaggio 2. Installare il certificato nel computer Windows.

Copiare il certificato esportato da ISE nel computer Windows, modificare l'estensione del file da .pem a .crt, quindi fare doppio clic per installarlo come mostrato nell'immagine.

🐱 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 23/11/2018	
Install Cartificate	
and/our-concentered booker beatering	
OK	

Passaggio 3. Selezionare Installa nel computer locale e fare clic su Avanti, come mostrato

÷	F 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	
	To continue, dick Next.	
	Sext Cance	

Passaggio 4. Selezionare Colloca tutti i certificati nell'archivio, quindi individuare e selezionare Autorità di certificazione radice attendibili. Quindi, fare clic su Next (Avanti) come mostrato nell'immagine.

← 🖉 Certificate Import Wizard	×
Certificate Stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location the certificate.	n for
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	Cancel

Passaggio 5. Quindi, fare clic su Finish (Fine) come mostrato nell'immagine.

← 🧬 Certi	ficate Import Wizard			×
Co	mpleting the Certific	ate Import Wizard		
The	certificate will be imported after	you click Finish.		
You	have specified the following sett	ings:		
Ce	rtificate Store Selected by User	Trusted Root Certification Authorities		
Co	rtert	Certificate		
		Finish	Cancel	
				_

Passaggio 6. Confermare l'installazione del certificato. Fare clic su Yes (Sì) come illustrato nell'immagine.

Security W	arning	×
L C C C C C C C C C C C C C C C C C C C	You are about to install a certificate from a certification authority CA) claiming to represent: CAP-SelfSignedCertificate Vindows cannot validate that the certificate is actually from EAP-SelfSignedCertificate". You should confirm its origin by ontacting "EAP-SelfSignedCertificate". The following number will ssist you in this process:	
Vi lf ai u a	Varning: f you install this root certificate, Windows will automatically trust ny certificate issued by this CA. Installing a certificate with an inconfirmed thumbprint is a security risk. If you click "Yes" you ocknowledge this risk.	
	Yes No	

Passaggio 7. Infine, fare clic su OK come mostrato nell'immagine.



End Device Configuration - Creazione del profilo WLAN

Passaggio 1. Fare clic con il pulsante destro del mouse sull'icona Start e selezionare Pannello di controllo, come mostrato nell'immagine.

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

ALL REPORTS



Passaggio 3. Selezionare Connetti manualmente a una rete wireless, quindi fare clic su Avanti come mostrato nell'immagine.

		-		×
<i>(</i>	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 modern network of create a new wreters prome.			
	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, come mostrato nell'immagine.

			-		Х
←	🐓 Manually connect to a v	vireless network			
	Enter information fo	r the wireless network you want to add	1		
		(treated			
	Network name:	154-351G			
	Security type:	WPA2-Enterprise ~			
	Formation tune:	ATC			
	Cici ypolori type.	AD			
	Security Key:	Hide chara	ters		
	Start this connection	automatically			
	Connect even if the	network is not broadcasting			
	Warning: If you sele	ct this option, your computer's privacy might be at i	fisk.		
		_			_
			Next	Cani	oel .

Passaggio 5. Per personalizzare la configurazione del profilo WLAN, selezionare Change connection settings (Cambia impostazioni di connessione)come mostrato nell'immagine.



Passaggio 6. Passare alla scheda Protezione e fare clic su Impostazioni come mostrato nell'immagine.

ise-ssid Wireless Ne	twork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network aut	hentication method:			
Microsoft: Protected	EAP (PEAP) 🛛 🗸	Setting	js	
Remember my credentials for this connection each				
time I'm logged on				
Advanced settings				
				_
		OK	Cancel	

Passaggio 7. Selezionare 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 radice attendibili selezionare il certificato autofirmato ISE.

Quindi selezionare Configure and disable Automatically use my Windows logon name and password..., quindi fare clic su OK come mostrato nelle immagini.

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:	
 Equila V Cichai Interna. Equila 1985: Assessments infinite dat. Entrance infinite 	
EAP-SelfSignedCertificate	
End Advanced international over the control of the start of the s	
Notifications before connecting:	
Tell user if the server name or root certificate isn't specified $\qquad \qquad \qquad$	
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) Configure.	
Enable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV	
Enable Identity Privacy	
OK Cancel	

Una volta tornata 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 come mostrato nelle immagini.

ise-ssid Wireless Ne	twork Properties			×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network aut	hentication method:			
Microsoft: Protected E	EAP (PEAP) 🛛 🗸	Setting	ps.	
Remember my cre time I'm logged or	dentials for this connect	tion each		
Advanced settings				
		ок	Cano	el

Advanced settings	×
802.1X settings 802.11 settings	
Specify authentication mode:	
User authentication Save credentials	
Delete credentials for all users	
Enable single sign on for this network	
Perform immediately before user logon	
 Perform immediately after user logon 	
Maximum delay (seconds): 10 *	
Allow additional dialogs to be displayed during single sign on	
This network uses separate virtual LANs for machine and user authentication	
OK Cano	el

Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

ahaha	user1
cisco	******
	OK Cancel

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

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

Processo di autenticazione su WLC

Per monitorare il processo di autenticazione per un utente specifico, eseguire i comandi seguenti:

> debug client <mac-add-client> > debug dot1x event enable > debug dot1x aaa enable

Esempio di autenticazione riuscita (alcuni output sono stati omessi):

<#root> *apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00 thread:1a5cc288 *apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00 *apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobil

X

*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override *apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for s *apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities: 60 *apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as none4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication 11w Capable *apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b *apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID: (16) *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mo *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache f *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0) *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2) *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP ru *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing sta *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId *apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session *apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00: *spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP *spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4: *spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mob *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime. *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from m *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authent *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) fo *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mo *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) fo *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 6
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Found an interface name: 'vlan2404' corresponds to interface name received: vlan2404

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intg *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mol *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

MAC: e4:b3:18:7c:30:58, source 4 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overrie *Dot1x_NW_MsgTask_0: Nov 24

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name: 'vlan2404' corresponds to interface name received

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobi *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got f *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for statio *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for statio *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cac *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: New PMKID: (16) *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for stati *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can ta *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:3 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is d *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: Including PMKID in M1 (16) [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: M1 - Key Data: (22) *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: [0016] cd fd a0 8a c4 39 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticati *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

e4:b3:18:7c:30:58

```
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:1
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL-Key from mobile e4:b3:18:7c:
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Reusing invalid EAPOL-Key from mobile e4:b3:18:7c:
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Key Desc Version FT - 0
*Dotlx_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

from mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4 *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Bufer for mobile e4: *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc *Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc

e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                              Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                                ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58
                                                              Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile L
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:
```

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
type = Airespace AP - Learn IP address
on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mo
*spamApTask2: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0

*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update require Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3 *apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobility

```
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Ad
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobi
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 w
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:
e4:b3:18:7c:30:58 172.16.0.151 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 quale criterio di autenticazione, criterio di autorizzazione e profilo di autorizzazione sono stati assegnati all'utente.

Per ulteriori informazioni, fare clic su Details (Dettagli) per visualizzare un processo di autenticazione più dettagliato, come mostrato nell'immagine.

atoto Id	Jentity S	Services	Engine	Home	Conte:	xt Visibility	+ Operation:	s Policy	 Administra 	ation 🔸	Work Centers		License
▼RADIU	JS TC-	-NAC Live	Logs	+ TACACS	Reports	Troubleshood	ot 🔹 Adapti	ve Network Contr	ol				
Live Log	gs Live	e Sessions	5										
		Misconfigured Supplicants			ants	Misconfigured Network Devices O		¢ R	RADIUS Drops 🛛		Client Stopped Responding		ng Repea
										Refresh	Never	Show	Latest 20 records
🔿 Refresh 🛛 💿 Reset Repeat Counts 🛛 🛃 Export To 👻													
Т	ïme S	Sta [Details	lde	Endpoint	ID Er	ndpoint	Authentication	n Policy	Autho	orization Polic	y Authori	zation Profiles
N	lo	1	à	user1	08:74:02:7	7:13:45 Ap	ple-Device	Default >> Rule r	name >> Defau	ilt Defaul	lt >> NameAuthZ	irule PermitAc	cessVLAN2404

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).