

Configurazione del richiedente 802.1X per i punti di accesso con controller 9800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione del LAP come supplicant 802.1x](#)

[Se L'AP È Già Stato Aggiunto Al WLC:](#)

[Se L'Access Point Non È Ancora Stato Aggiunto A Un WLC:](#)

[Configurazione dello switch](#)

[Configurazione del server ISE](#)

[Verifica](#)

[Verifica il tipo di autenticazione](#)

[Verifica della porta dello switch 802.1x](#)

[Risoluzione dei problemi](#)

[Riferimenti](#)

Introduzione

In questo documento viene descritto come configurare un Cisco Access Point (AP) come supplicant 802.1x da autorizzare su una porta switch su un server RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Wireless Lan Controller (WLC) e LAP (Lightweight Access Point).
- 802.1x su switch Cisco e ISE
- Protocollo EAP (Extensible Authentication Protocol)
- RADIUS (Remote Authentication Dial-In User Service)

Componenti usati

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

- WS-C3560CX, Cisco IOS® XE, 15.2(3r)E2
- C9800-CL-K9, Cisco IOS® XE, 17.6.5
- ISE 3.0
- AIR-CAP3702
- AIR-AP3802

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

In questa configurazione, il punto di accesso (AP) agisce come supplicant 802.1x ed è autenticato dallo switch sull'ISE con il metodo EAP-FAST.

Dopo aver configurato la porta per l'autenticazione 802.1X, lo switch non consente il passaggio di traffico diverso dal traffico 802.1X attraverso la porta fino a quando il dispositivo connesso alla porta non viene autenticato correttamente.

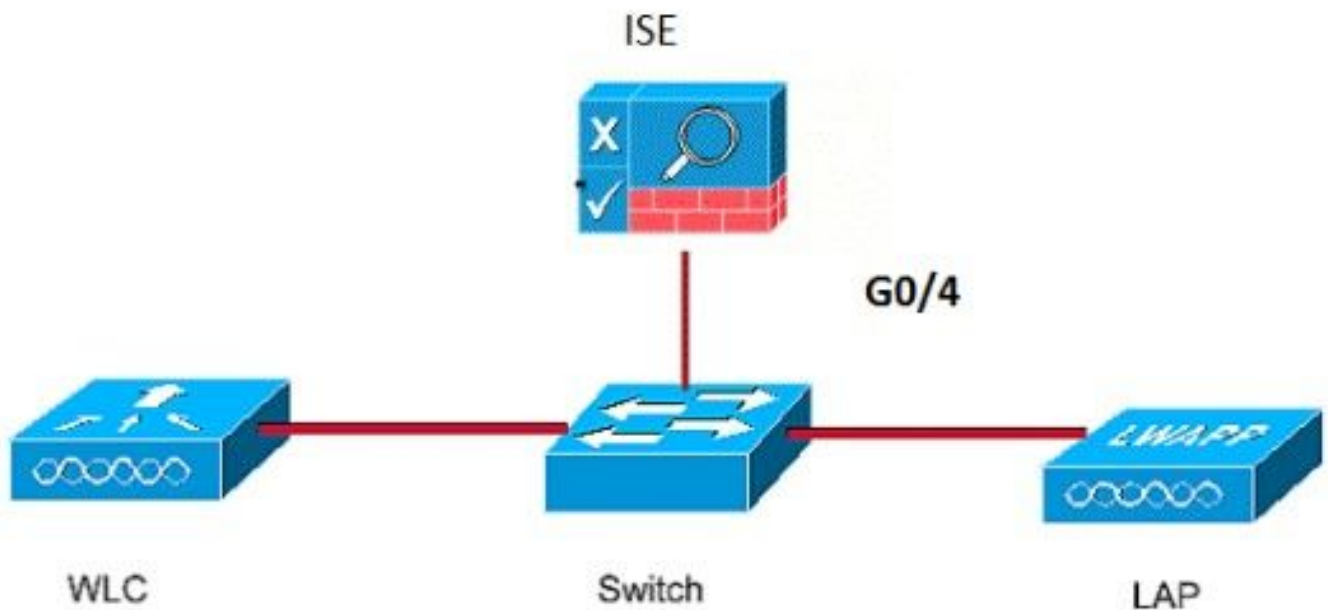
Un access point può essere autenticato prima di essere aggiunto a un WLC o dopo essere stato aggiunto a un WLC, nel qual caso, configurare 802.1X sullo switch dopo che il LAP si è unito al WLC.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Il documento usa la seguente configurazione di rete:



Configurazione del LAP come supplicant 802.1x

Se L'AP È Già Stato Aggiunto Al WLC:

Configurare il tipo di autenticazione 802.1x e il tipo di autenticazione AP LSC (Locally Significant Certificate):

Passaggio 1. Passare a Configurazione > Tag e profili > AP Join > Nella pagina AP Join Profile, fare clic su Add per aggiungere un nuovo profilo di join o modificarne il nome.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration page for AP Join profiles. The page title is "Cisco Catalyst 9800-CL Wireless Controller 17.5.1". The navigation path is "Configuration > Tags & Profiles > AP Join". There are two buttons: "+ Add" and "x Delete". Below the buttons is a table with columns "AP Join Profile Name" and "Description".

AP Join Profile Name	Description
<input type="checkbox"/> test	
<input type="checkbox"/> Dot1x	
<input type="checkbox"/> Split-Tunnel	
<input type="checkbox"/> default-ap-profile	default ap profile

At the bottom of the table, there is a pagination control showing "1" items per page and a dropdown menu for "10" items per page.

Passaggio 2. Nella pagina Profilo di join AP, da AP > Generale, passare alla sezione Configurazione autenticazione EAP AP. Dall'elenco a discesa Tipo EAP, scegliere il tipo EAP come EAP-FAST, EAP-TLS o EAP-PEAP per configurare il tipo di autenticazione dot1x. EAP-FAST è l'unico tipo di autenticazione che utilizza solo nome utente e password ed è il più semplice

da configurare. PEAP e EAP-TLS richiedono il provisioning dei certificati sui punti di accesso tramite il flusso di lavoro LSC (vedere la sezione Riferimenti).

The screenshot shows the 'Edit AP Join Profile' configuration window with the 'AP' tab selected. The 'AP EAP Auth Configuration' section is highlighted with a blue box. The configuration includes:

- Power Over Ethernet:** Switch Flag, Power Injector State, Power Injector Type (Unknown), and Injector Switch MAC (00:00:00:00:00:00).
- Client Statistics Reporting Interval:** 5 GHz (sec) and 2.4 GHz (sec) both set to 90.
- Extended Module:** Enable checkbox.
- Mesh:** Profile Name set to mesh-profile.
- AP EAP Auth Configuration:** EAP Type dropdown menu showing EAP-FAST, EAP-TLS, and EAP-PEAP options.

Buttons at the bottom include 'Cancel' and 'Update & Apply to Device'.

Passaggio 3. Dall'elenco a discesa Tipo di autorizzazione AP, scegliere il tipo come CAPWAP DTLS + o CAPWAP DTLS > Fare clic su Aggiorna e applica a dispositivo.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

AP EAP Auth Configuration

EAP Type

AP Authorization Type

- CAPWAP DTLS
- CAPWAP DTLS + DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

Extended Module

Enable

Mesh

Profile Name [Clear](#)

Configurare il nome utente e la password 802.1x:

Passaggio 1. Da Gestione > Credenziali > Immettere il nome utente e la password dot1x > Scegliere il tipo di password 802.1x appropriato > Fare clic su Aggiorna e applica al dispositivo

Edit AP Join Profile ✕

General Client CAPWAP AP **Management** Security ICap QoS

Device User **Credentials** CDP Interface

Dot1x Credentials

Dot1x Username	<input type="text" value="Dot1x"/>
Dot1x Password	<input type="password" value="••••••••"/>
Dot1x Password Type	<input type="text" value="clear"/>

Se L'Access Point Non È Ancora Stato Aggiunto A Un WLC:

Collegare la console al LAP per impostare le credenziali e usare i seguenti comandi CLI: (per i Cisco IOS e Cheetah OS® AP)

CLI:

```
<#root>
```

```
LAP#
```

```
debug capwap console cli
```

```
LAP#
```

```
capwap ap dot1x username <username> password <password>
```

Per Cancellare Le Credenziali Dot1x Sull'Access Point (Se Necessario)

Per i Cisco IOS® AP, ricaricare il punto di accesso:

CLI:

```
<#root>
```

```
LAP#
```

```
clear capwap ap dot1x
```

Per i Cisco COS AP, ricaricare il punto di accesso:

CLI:

```
<#root>
```

```
LAP#
```

```
capwap ap dot1x disable
```

Configurazione dello switch

Abilitare dot1x sullo switch a livello globale e aggiungere il server ISE allo switch.

CLI:

```
<#root>
```

```
Enable
```

```
Configure terminal
```

```
aaa new-model
```

```
aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius
```

```
dot1x system-auth-control
```

```
Radius-server host <ISE IP address> auth-port <port> acct-port <port>  
key 7 <server key>
```

Configurare la porta dello switch AP.

CLI:

```
<#root>
```

```
configure terminal
```

```
interface GigabitEthernet</>  
switchport access vlan <>  
switchport mode access  
authentication order dot1x  
authentication port-control auto  
dot1x pae authenticator  
spanning-tree portfast edge
```


```
end
```

Se l'access point è in modalità Flex Connect, ossia in modalità locale, è necessario eseguire una configurazione aggiuntiva sull'interfaccia dello switch per consentire la presenza di più indirizzi MAC sulla porta, poiché il traffico del client viene rilasciato al livello dell'access point:

```
<#root>
```

```
authentication host-mode multi-host
```

Nota: indica che il lettore prende nota. Le note contengono utili suggerimenti o riferimenti a materiale non trattato nel documento.

 Nota: la modalità multi-host autentica il primo indirizzo MAC e consente un numero illimitato di altri indirizzi MAC. Abilitare la modalità host sulle porte dello switch se l'access point connesso è stato configurato con la modalità di commutazione locale. Consente al traffico del client di passare alla porta dello switch. Se si desidera un percorso del traffico protetto, abilitare dot1x sulla WLAN per proteggere i dati client

Configurazione del server ISE

Passaggio 1. Aggiungere lo switch come dispositivo di rete sul server ISE. Passare a Amministrazione > Risorse di rete > Dispositivi di rete > Fare clic su Aggiungi > Immettere il nome del dispositivo, l'indirizzo IP, abilitare le impostazioni di autenticazione RADIUS, Specificare il valore segreto condiviso, la porta COA (o lasciarla come predefinita) > Invia.

The screenshot displays the Cisco ISE Administration interface. At the top, the 'Administration - Network Resources' breadcrumb is highlighted with a red box. The 'Network Devices' menu item in the left sidebar is also highlighted with a red box. The main content area shows the 'New Network Device' configuration page. The 'RADIUS Authentication Settings' section is highlighted with a red box, indicating the current configuration step. This section includes the following fields and options:

- Protocol: RADIUS
- Shared Secret: [Redacted] (with a 'Show' button)
- Use Second Shared Secret: (with a 'Show' button)
- CoA Port: 1700 (with a 'Set To Default' button)
- RADIUS DTLS Settings: (with a 'Show' button)
- DTLS Required: (with a 'Show' button)
- Shared Secret: radius/dtls (with a 'Show' button)

Passaggio 2. Aggiungere le credenziali dell'access point ad ISE. Passare a Amministrazione > Gestione delle identità > Identità > Utenti e fare clic sul pulsante Aggiungi per aggiungere un utente. Immettere le credenziali configurate nel profilo di aggiunta all'access point sul WLC. Si noti che l'utente viene inserito nel gruppo predefinito, ma può essere regolato in base alle proprie esigenze.

The screenshot shows the Cisco ISE Administration console for Identity Management. The 'Identities' tab is active. Under 'Network Access User', the 'Name' is set to 'dot1x' and the status is 'Enabled'. In the 'Passwords' section, the 'Login Password' field is highlighted with a red box, and there are two 'Generate Password' buttons. The 'User Groups' section shows 'ALL_ACCOUNTS (default)' as the selected group.

Passaggio 3. Su ISE, configurare i criteri di autenticazione e autorizzazione. Andare a Criterio > Set di criteri e selezionare il set di criteri da configurare e la freccia blu a destra. In questo caso, viene utilizzato il set di criteri predefinito, ma è possibile personalizzarlo in base al requisito.

The screenshot shows the 'Policy - Policy Sets' section of the Cisco ISE Administration console. A table lists policy sets, with one entry 'Default' (Default policy set) highlighted. The right-side action menu for this entry is highlighted with a red box, showing a blue arrow icon. Buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save' are visible at the top and bottom of the interface.

Configurare quindi i criteri di autenticazione e di autorizzazione. Le policy mostrate qui sono le policy predefinite create sul server ISE, ma possono essere adattate e personalizzate secondo le vostre esigenze.

Nell'esempio, la configurazione può essere tradotta nel modo seguente: "Se si utilizza il cavo 802.1X e l'utente è noto sul server ISE, si consente l'accesso agli utenti per i quali l'autenticazione è riuscita". L'access point viene quindi autorizzato sul server ISE.

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	6	⚙️
●	Default		All_User_ID_Stores > Options	0	⚙️

Authorization Policy (12)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess x	Select from list	6	⚙️
●	Default		DenyAccess x	Select from list	0	⚙️

Passaggio 4. Verificare che nei protocolli consentiti per Accesso di rete predefinito sia consentito EAP-FAST. Passare a Criterio > Elementi criterio > Autenticazione > Risultati > Protocolli consentiti > Accesso di rete predefinito > Abilita EAP-TLS > Salva.

Cisco ISE Policy · Policy Elements

Results

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

- Process Host Lookup

Authentication Protocols

- Allow PAP/ASCII
- Allow CHAP
- Allow MS-CHAPv1
- Allow MS-CHAPv2
- Allow EAP-MD5
- Allow EAP-TLS

Expand Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 90 % of Time To Live has expired

- Allow LEAP
- Allow PEAP
- Allow EAP-FAST
- Allow EAP-TTLS
- Allow TEAP

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verifica il tipo di autenticazione

Il comando show visualizza le informazioni di autenticazione di un profilo AP:

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

Esempio:

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
...
Dot1x EAP Method     : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE    : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

Verifica della porta dello switch 802.1x

Il comando show visualizza lo stato di autenticazione 802.1x sulla porta dello switch:

CLI:

```
Switch# show dot1x all
```

Esempio di output:

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout          = 0
SuppTimeout            = 30
ReAuthMax              = 2
MaxReq                 = 2
TxPeriod               = 30
```

Verificare se la porta è stata autenticata o meno

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

Esempio di output:

```
Dot1x Info for GigabitEthernet0/8
```

```
-----  
PAE = AUTHENTICATOR  
QuietPeriod = 60  
ServerTimeout = 0  
SuppTimeout = 30  
ReAuthMax = 2  
MaxReq = 2  
TxPeriod = 30
```

```
Dot1x Authenticator Client List
```

```
-----  
EAP Method = FAST  
Supplicant = f4db.e67e.dd16  
Session ID = 0A30279E00000BB7411A6BC4  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE  
ED  
Auth BEND SM State = IDLE
```

Dalla CLI:

```
Switch#show authentication sessions
```

Esempio di output:

Interface	MAC Address	Method	Domain	Status	Fg	Session ID
Gi0/8	f4db.e67e.dd16	dot1x	DATA	Auth		0A30279E00000BB7411A6BC4

In ISE, scegliere Operations > Radius Livelogs e confermare che l'autenticazione sia stata eseguita correttamente e che sia stato premuto il profilo di autorizzazione corretto.

Cisco ISE Operations - RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 1 Client Stopped Responding 0 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization Policy	Authorization Pr...	IP Address	Network De...	Device P
Nov 28, 2022 08:39:49.7...	✓	🔍		dot1x	A4-53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	nschyns-SW-...	FastEther...		
Nov 28, 2022 08:33:34.4...	✓	🔍		dot1x	A4-53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	PermitAccess			

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

1. Immettere il comando ping per verificare se il server ISE è raggiungibile dallo switch.
2. Verificare che lo switch sia configurato come client AAA sul server ISE.
3. Verificare che il segreto condiviso sia lo stesso tra lo switch e il server ISE.
4. Verificare se EAP-FAST è abilitato sul server ISE.
5. Verificare che le credenziali 802.1x siano configurate per il LAP e che siano le stesse sul server ISE.

Nota: il nome utente e la password fanno distinzione tra maiuscole e minuscole.

6. Se l'autenticazione non riesce, immettere i seguenti comandi sullo switch: debug dot1x e debug authentication.

Notare che i Cisco IOS based access point (802.11ac wave 1) non supportano TLS versione 1.1 e 1.2. Ciò può causare un problema se il server ISE o RADIUS è configurato in modo da consentire solo l'autenticazione TLS 1.2 interna 802.1X.

Riferimenti

[Configurazione di 802.1X sui punti di accesso con PEAP e EAP-TLS](#)

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).