

Configurazione dell'autenticazione 802.1X su Catalyst serie 9800 Wireless Controller

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione WLC](#)

[Configurazione AAA su 9800 WLC](#)

[Configurazione profilo WLAN](#)

[Configurazione del profilo di policy](#)

[Configurazione del tag di policy](#)

[Assegnazione tag criteri](#)

[Configurazione di ISE](#)

[Dichiarare il WLC su ISE](#)

[Creazione di un nuovo utente in ISE](#)

[Creazione del profilo di autorizzazione](#)

[Crea set di criteri](#)

[Crea criterio di autenticazione](#)

[Crea criterio di autorizzazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi sul WLC](#)

[Risoluzione dei problemi con ISE](#)

Introduzione

Questo documento descrive come configurare una WLAN con sicurezza 802.1X su un controller wireless Cisco Catalyst serie 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 802.1X

Componenti usati

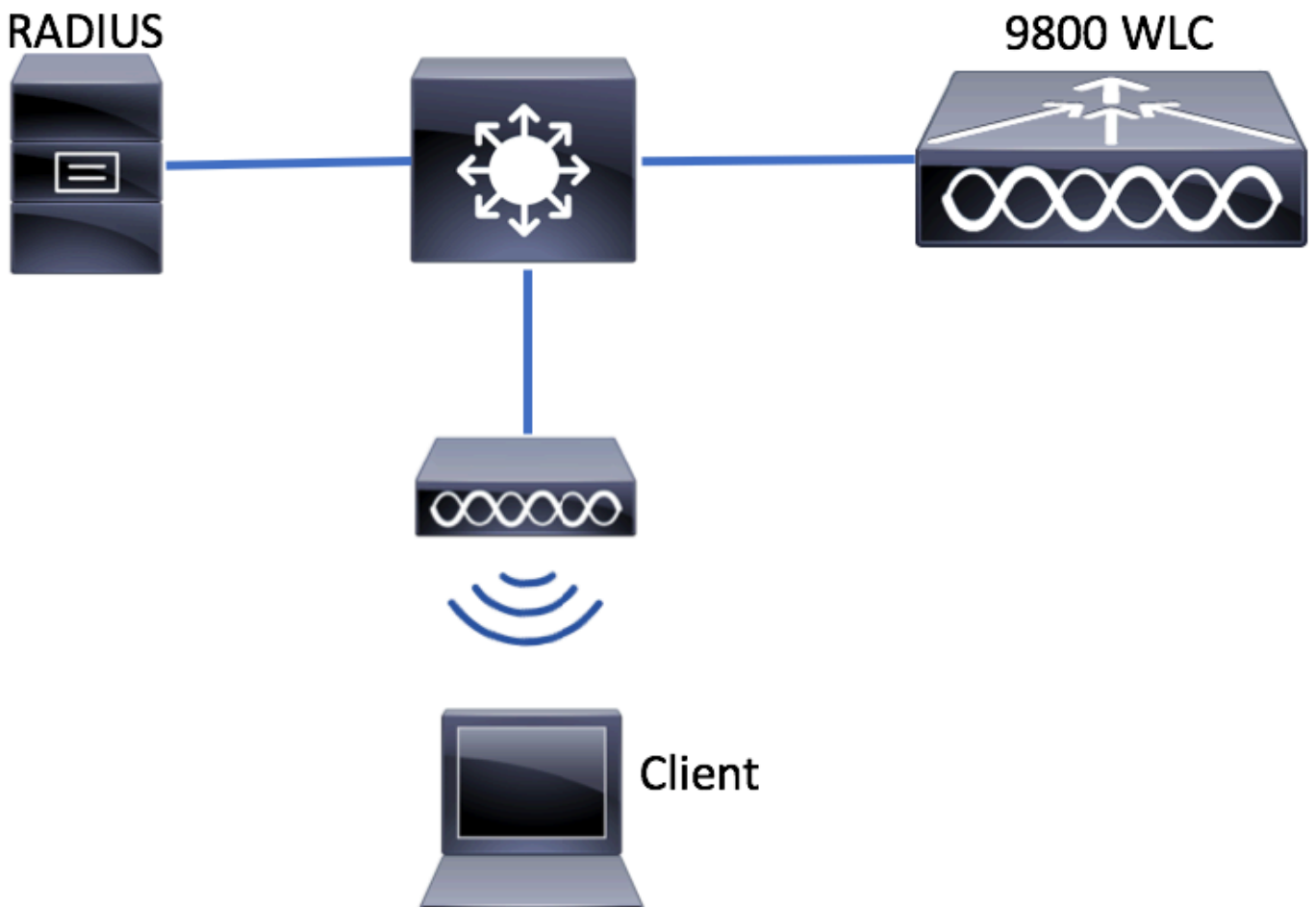
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst serie 9800 Wireless Controller (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

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



Configurazione WLC

Configurazione AAA su 9800 WLC

GUI:

Passaggio 1. Dichiarare il server RADIUS. Passa a **Configuration > Security > AAA > Servers / Groups >**

RADIUS > Servers > + Add e immettere le informazioni sul server RADIUS.

The screenshot shows the 'Authentication Authorization and Accounting' configuration page. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area has three tabs: 'AAA Method List', 'Servers / Groups' (highlighted with a red box), and 'AAA Advanced'. Below the tabs, there are '+ Add' and 'Delete' buttons, with '+ Add' highlighted in red. Underneath, there are two sub-tabs: 'RADIUS' (highlighted in red) and 'TACACS+'. The 'RADIUS' sub-tab is active, showing a table with columns 'Name' and 'Address'. The table is currently empty.

verificare che il **supporto per CoA** sia abilitato se si intende utilizzare l'autenticazione Web centrale (o qualsiasi tipo di protezione che richieda la modifica dell'autorizzazione [CoA]) in futuro.

The screenshot shows the 'Create AAA Radius Server' form. The form has the following fields and options:

- Name*: ISE-kcg
- IPV4/IPv6 Server Address*: 172.16.0.11
- Shared Secret*:
- Confirm Shared Secret*:
- Auth Port: 1812
- Acct Port: 1813
- Server Timeout (seconds): 1-1000
- Retry Count: 0-100
- Support for CoA: ENABLED
- Clear PAC Key:
- Set New PAC Key:

At the bottom of the form, there are two buttons: 'Cancel' and 'Save & Apply to Device' (highlighted with a red box).

Passaggio 2. Aggiungere il server RADIUS a un gruppo RADIUS. Passa a **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. Assegnare un nome al gruppo e spostare il server creato in precedenza nell'elenco **Assigned Servers**.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Passaggio 3. Creare un elenco di metodi di autenticazione. Passa a **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.

Authentication Authorization and Accounting

Servers / Groups

General

Authorization

Name

Immettere le informazioni:

Quick Setup: AAA Authentication

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

CLI:

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Nota sul rilevamento di server inattivi AAA

Dopo aver configurato il server RADIUS, è possibile verificare se è considerato "ATTIVO":

```
#show aaa servers | s WNCN Platform State from WNCN (1) : current UP Platform State from WNCN
(2) : current UP Platform State from WNCN (3) : current UP Platform State from WNCN (4) :
current UP ...
```

È possibile configurare il **dead criteria**, nonché **deadtime** sul WLC, in particolare se si utilizzano più server RADIUS.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

Nota: la **dead criteria** Criteri utilizzati per contrassegnare un server RADIUS come inattivo. Si compone di: 1. Un timeout (in secondi) che rappresenta il periodo di tempo che deve trascorrere tra il momento in cui il controller ha ricevuto per ultimo un pacchetto valido dal

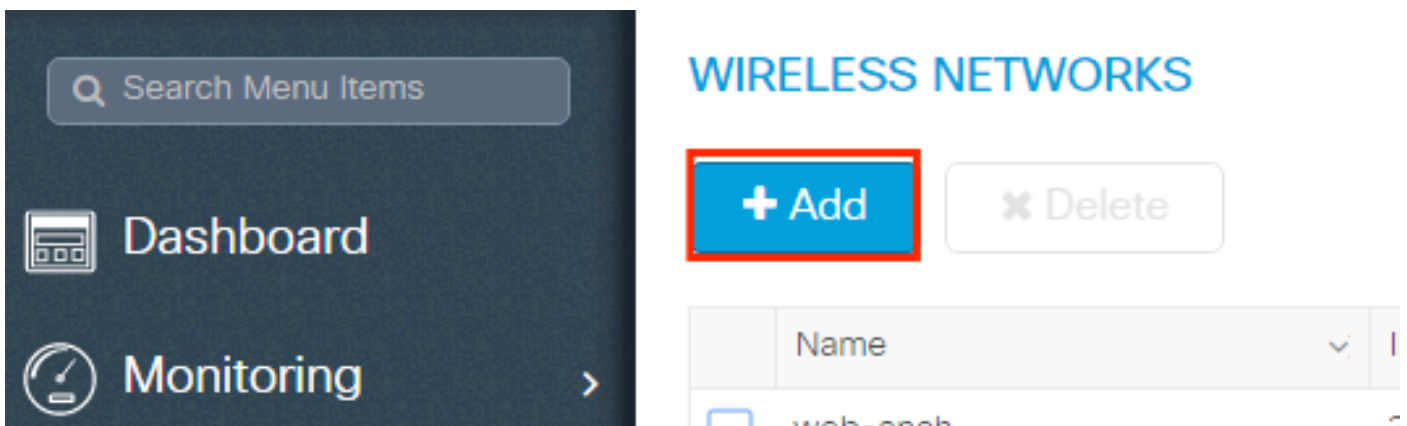
server RADIUS e il momento in cui il server viene contrassegnato come inattivo. 2. Un contatore, che rappresenta il numero di timeout consecutivi che devono verificarsi sul controller prima che il server RADIUS venga contrassegnato come inattivo.

Nota: la *deadtime* specifica il periodo di tempo (in minuti) durante il quale il server rimane nello stato inattivo dopo che i criteri inattivo lo contrassegnano come inattivo. Alla scadenza del tempo di inattività, il controller contrassegna il server come ATTIVO (ALIVE) e notifica ai client registrati la modifica dello stato. Se il server è ancora irraggiungibile dopo che lo stato è contrassegnato come ATTIVO e se i criteri non attivi sono soddisfatti, il server viene nuovamente contrassegnato come non attivo per l'intervallo di tempo morto.

Configurazione profilo WLAN

GUI:

Passaggio 1. Creare la WLAN. Selezionare **Configurazione > Wireless > WLAN > + Aggiungi** e configura la rete come necessario.



Passaggio 2. Immettere le informazioni sulla WLAN

Add WLAN ✕

General	Security	Advanced
Profile Name*	<input type="text" value="prof-name"/>	Radio Policy <input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID <input checked="" type="checkbox"/>
WLAN ID*	<input type="text" value="1"/>	
Status	<input checked="" type="checkbox"/>	

Passaggio 3. Passare alla Scheda **Protezione** e selezionare il metodo di protezione necessario. In questo caso, **WPA2 + 802.1x**.

Add WLAN ✕

General	Security	Advanced
	Layer2	Layer3
	Layer 2 Security Mode <input type="text" value="WPA + WPA2"/>	AAA
	MAC Filtering <input type="checkbox"/>	Fast Transition <input type="text" value="Adaptive Enab..."/>
	Protected Management Frame	Over the DS <input checked="" type="checkbox"/>
	PMF <input type="text" value="Disabled"/>	Reassociation Timeout <input type="text" value="20"/>
	WPA Parameters	
	WPA Policy <input type="checkbox"/>	

Add WLAN

PMF Disabled

WPA Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

Cancel Save & Apply to Device

Passaggio 4. Dal **Security > AAA** selezionare il metodo di autenticazione creato nel passaggio 3 dalla sezione AAA Configuration on 9800 WLC.

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List list-name

Local EAP Authentication

Cancel Save & Apply to Device

CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```


Configurazione del profilo di policy

All'interno di un profilo di policy è possibile decidere a quale VLAN assegnare ai client, tra le altre impostazioni (come Access Controls List [ACLs], Quality of Service [QoS], Mobility Anchor, Timer e così via).

È possibile utilizzare il profilo dei criteri predefinito oppure creare un nuovo profilo.

GUI:

Passare a **Configurazione > Tag e profili > Profilo criterio** e configurare il **profilo predefinito-criterio** o crearne uno nuovo.

Policy Profile

+ Add

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

1 10 items per page

Verificare che il profilo sia abilitato.

Inoltre, se il punto di accesso è in modalità locale, verificare che nel profilo della policy siano attivate le opzioni **Cambio centrale** e **Autenticazione centrale**.

Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*

Description

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

Selezionare la VLAN a cui assegnare i client nella scheda **Criteri di accesso**.

Edit Policy Profile

General | **Access Policies** | QOS and AVC | Mobility | Advanced

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Se si intende avere gli attributi ISE restituiti nell'assegnazione Access-Accept come VLAN, abilitare l'override AAA nell'assegnazione **Advanced** scheda:

Edit Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)	<input style="width: 90%;" type="text" value="1800"/>
Idle Timeout (sec)	<input style="width: 90%;" type="text" value="300"/>
Idle Threshold (bytes)	<input style="width: 90%;" type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input style="width: 90%;" type="text" value="60"/>

DHCP

IPv4 DHCP Required	<input checked="" type="checkbox"/>
DHCP Server IP Address	<input style="width: 90%;" type="text"/>

Show more >>>

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	<input style="width: 90%;" type="text" value="default-aaa-policy"/> ✕ ▼

Fabric Profile	<input type="checkbox"/> <input style="width: 90%;" type="text" value="Search or Select"/> ▼
Umbrella Parameter Map	<input style="width: 90%;" type="text" value="Not Configured"/> ▼
mDNS Service Policy	<input style="width: 90%;" type="text" value="default-mdns-service"/> ▼ Clear

WLAN Flex Policy

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	<input style="width: 90%;" type="text" value="Search or Select"/> ▼

Air Time Fairness Policies

2.4 GHz Policy	<input style="width: 90%;" type="text" value="Search or Select"/> ▼
5 GHz Policy	<input style="width: 90%;" type="text" value="Search or Select"/> ▼

Cancel
Update & Apply to Device

CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

Configurazione del tag di policy

Il tag dei criteri viene utilizzato per collegare l'SSID al profilo dei criteri. È possibile creare un nuovo tag o utilizzare il tag predefinito.

Nota: il tag default-policy-tag mappa automaticamente qualsiasi SSID con ID WLAN compreso tra 1 e 16 al profilo default-policy-profile. Non può essere né modificata né eliminata. Se si dispone di una WLAN con ID 17 o superiore, non è possibile utilizzare il tag default-policy.

GUI:

Passa a **Configugation > Tags & Profiles > Tags > Policy** e aggiungerne uno nuovo, se necessario.

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting

Manage Tags

Policy Site RF AP

+ Add **✕ Delete**

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

Associare il profilo WLAN al profilo di policy desiderato.

Add Policy Tag

Name* PolicyTagName

Description Enter Description

+ Add **✕ Delete**

WLAN Profile	Policy Profile
No items to display	

0 10 items per page

Cancel Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◀ 0 ▶ ▶	10 items per page
No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

✕ ✓

↶ Cancel Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◀ 1 ▶ ▶	10 items per page
1 - 1 of 1 items	

↶ Cancel Save & Apply to Device

CLI:

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Assegnazione tag criteri

Assegnare il tag di policy agli access point desiderati.

GUI:

Per assegnare il tag a un punto di accesso, passare a **Configuration > Wireless > Access Points > AP Name > General Tags**, assegnare il tag di criterio appropriato e fare clic su **Update & Apply to Device**.

The screenshot shows the 'Edit AP' configuration page with the following details:

- General Tab:** AP Name* (AP3802-02-WS), Location* (default location), Base Radio MAC (00:42:68:c6:41:20), Ethernet MAC (00:42:68:a0:d0:22), Admin Status (Enabled), AP Mode (Local), Operation Status (Registered), Fabric Status (Disabled).
- Version Section:** Primary Software Version (10.0.200.50), Predownloaded Status (N/A), Predownloaded Version (N/A), Next Retry Time (N/A), Boot Version (1.0.0), IOS Version (10.0.200.52), Mini IOS Version (0.0.0.0).
- IP Config Section:** IP Address (172.16.0.207), Static IP (checkbox).
- Time Statistics Section:** Up Time (9 days 1 hrs 17 mins 24 secs), Controller Associated Time (0 days 3 hrs 26 mins 41 secs), Controller Association Latency (8 days 21 hrs 50 mins 33 secs).
- Tags Section:** Policy (default-policy-tag), Site (default-site-tag), RF (default-rf-tag).
- Buttons:** Cancel (left), Update & Apply to Device (right).

Nota: quando si modifica il tag di policy su un access point, l'associazione viene interrotta al WLC 9800 e si unisce nuovamente qualche istante dopo.

Per assegnare lo stesso tag criteri a più access point, passare a **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

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).