

Configurazione del SSID di autenticazione MAC sui controller wireless Catalyst 9800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisito](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione AAA su 9800 WLC](#)

[Autenticazione dei client con il server esterno](#)

[Autenticazione locale dei client](#)

[Configurazione della WLAN](#)

[Configurazione del profilo di policy](#)

[Configurazione del tag di policy](#)

[Assegnazione tag criteri](#)

[Registra localmente l'indirizzo MAC sul WLC per l'autenticazione locale](#)

[Immettere l'indirizzo MAC nel database degli endpoint ISE](#)

[Creare una regola di autenticazione](#)

[Creazione regola di autorizzazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Debug condizionale e traccia Radioactive \(RA\)](#)

Introduzione

Questo documento descrive come configurare una rete WLAN (Wireless Local Area Network) con sicurezza dell'autenticazione MAC su Cisco Catalyst 9800 WLC.

Prerequisiti

Requisito

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Indirizzo MAC
- Cisco Catalyst serie 9800 Wireless Controller
- Identity Service Engine (ISE)

Componenti usati

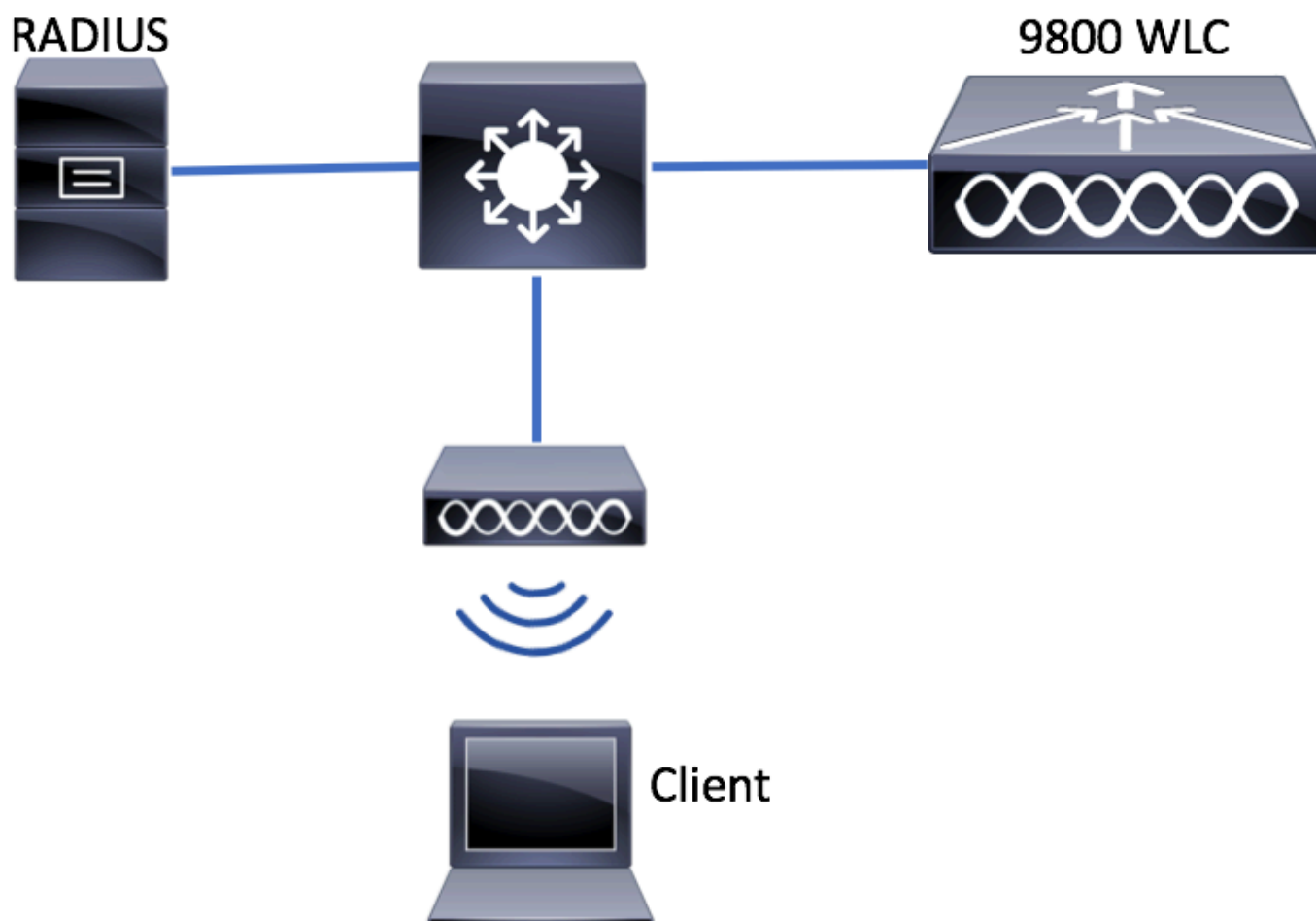
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS® XE Gibraltar v16.12
- ISE v2.2

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 AAA sui controller 9800 WLC

Autenticazione dei client con il server esterno

GUI:

Leggere i punti 1-3 della sezione 'Configurazione AAA su 9800 WLC' da questo collegamento:

[Configurazione AAA su WLC serie 9800](#)

Passaggio 4. Creare un metodo di rete di autorizzazione.

Individuate [Configuration > Security > AAA > AAA Method List > Authorization > +](#) Adde create l'oggetto.

The screenshot shows the Cisco WLC configuration interface. On the left is a navigation menu with 'Configuration' highlighted. The main area is titled 'Authentication Authorization and Accounting' and has 'AAA Method List' selected. Under the 'Authorization' sub-tab, there is a '+ Add' button and a 'Delete' button. Below these is a table with columns for 'Name' and 'Type'.

The 'Quick Setup: AAA Authorization' dialog box is shown. It contains the following fields and options:

- Method List Name***: AuthZ-method-name
- Type***: network
- Group Type**: group
- Fallback to local**:
- Available Server Groups**: radius, ldap, tacacs+
- Assigned Server Groups**: ISE-KCG-grp
- Buttons**: Cancel, Save & Apply to Device

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 authorization network <AuthZ-method-name> group <radius-grp-name>

```

Autenticazione locale dei client

Creare un metodo di rete di autorizzazione locale.

Individuate [Configuration > Security > AAA > AAA Method List > Authorization > + Add](#) create l'oggetto.

The screenshot shows the Cisco ISE GUI for 'Authentication Authorization and Accounting'. The left sidebar has 'Configuration' highlighted. The main area shows 'AAA Method List' selected in the top navigation, and 'Authorization' selected in the sub-navigation. A '+ Add' button is highlighted in a red box, indicating the next step in the process.

The screenshot shows the 'Quick Setup: AAA Authorization' dialog box. The 'Method List Name*' field is set to 'AuthZ-local', 'Type*' is set to 'network', and 'Group Type' is set to 'local'. The 'Available Server Groups' list includes 'radius', 'ldap', 'tacacs+', and 'ISE-KCG-grp'. The 'Assigned Server Groups' list is empty. The 'Save & Apply to Device' button is highlighted in a red box.

CLI:

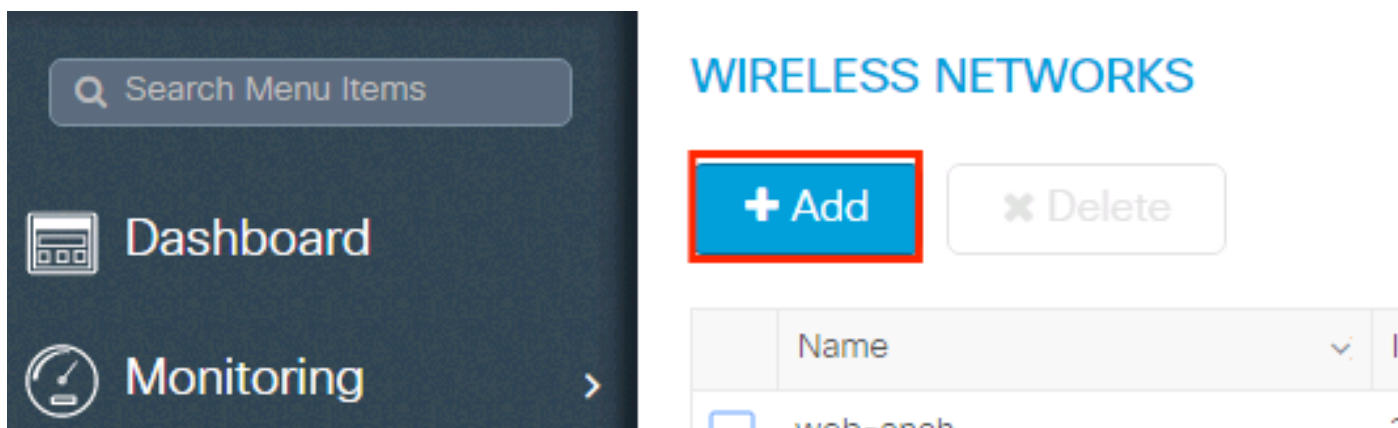
```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

Configurazione della WLAN

GUI:

Passaggio 1. Creare la WLAN.

Individuare [Configuration > Wireless > WLANs > + Add](#) e configurare la rete in base alle esigenze.



Passaggio 2. Immettere le informazioni sulla WLAN.

Add WLAN ✕

General
Security
Advanced

Profile Name*	<input type="text" value="mac-auth"/>	Radio Policy	<input type="text" value="All"/>
SSID	<input type="text" value="mac-auth"/>	Broadcast SSID	ENABLED <input checked="" type="checkbox"/>
WLAN ID*	<input type="text" value="3"/>		
Status	ENABLED <input checked="" type="checkbox"/>		

↶ Cancel

📄 Save & Apply to Device

Passaggio 3. Passare alla Security scheda e disabilitare Layer 2 Security Mode e abilitare MAC Filtering. Da Authorization List, scegliere il metodo di autorizzazione creato nel passo precedente. Quindi fate clic su Save & Apply to Device.

Add WLAN ✕

General
Security
Advanced

Layer2
Layer3
AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Fast Transition	<input type="text" value="Adaptive Enab..."/>
MAC Filtering	<input checked="" type="checkbox"/>	Over the DS	<input checked="" type="checkbox"/>
Authorization List*	<input type="text" value="AuthZ-method-name"/>	Reassociation Timeout	<input type="text" value="20"/>

↶ Cancel

📄 Save & Apply to Device

CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

Configurazione del profilo di policy

È necessario abilitare `aaa-override` nel profilo dei criteri per garantire il corretto funzionamento del filtro mac per SSID.

[Configurazione del profilo delle policy su 9800 WLC](#)

Configurazione del tag di policy

[Codice di matricola su 9800 WLC](#)

Assegnazione tag criteri

[Assegnazione codice su 9800 WLC](#)

Registra l'indirizzo MAC consentito.

Registra localmente l'indirizzo MAC sul WLC per l'autenticazione locale

Passare a `Configuration > Security > AAA > AAA Advanced > AP Authentication > + Add`.


The screenshot displays the Cisco WLC configuration interface for 'Authentication Authorization and Accounting'. The left sidebar shows the navigation menu with 'Configuration' highlighted. The main content area is titled 'Authentication Authorization and Accounting' and includes a '+ AAA Wizard' button. Below this, there are tabs for 'AAA Method List', 'Servers / Groups', and 'AAA Advanced', with 'AAA Advanced' selected. Under 'AAA Advanced', there are sections for 'RADIUS Fallback', 'Attribute List Name', 'AP Authentication', and 'Password Policy'. The 'AP Authentication' section is highlighted, and a '+ Add' button is visible. The 'AP Authentication' section shows a table with columns for 'MAC Address' and 'Serial Number'. The table contains two entries: 'aabbccdeeff' and 'e4b3187c3058'. A '+ Add' button and a 'x Delete' button are located above the table. The table also has a pagination control showing '10 items per page'.

Scrivere l'indirizzo MAC in lettere minuscole senza separatore e fare clic su `Save & Apply to Device`.

Quick Setup: MAC Filtering ✕

MAC Address*

Attribute List Name

 Nota: nelle versioni precedenti alla 17.3, l'interfaccia utente Web ha modificato qualsiasi formato MAC digitato nel formato 'nessun separatore' mostrato nella figura. Nella versione 17.3 e successive, l'interfaccia utente Web rispetta qualsiasi struttura immessa ed è pertanto essenziale non immettere alcun separatore. Miglioramento bug Cisco ID bug [CSCv43870](https://tools.cisco.com/bugcenter/bug/?bugID=CSCv43870) tiene traccia del supporto di diversi formati per l'autenticazione MAC.

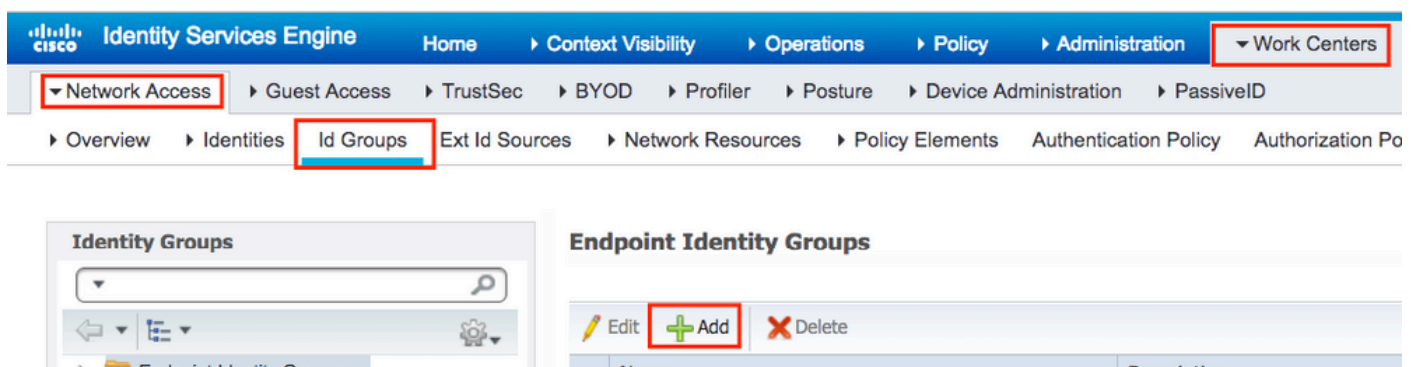
CLI:

```
# config t
# username <aabbccddeeff> mac
```

Immettere l'indirizzo MAC nel database degli endpoint ISE

Passaggio 1. (Facoltativo) Creare un nuovo gruppo di endpoint.

Passare a Work Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add.



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Work Centers' menu is expanded, showing 'Network Access', 'Guest Access', 'TrustSec', 'BYOD', 'Profiler', 'Posture', 'Device Administration', and 'PassiveID'. The 'Network Access' menu is further expanded to show 'Overview', 'Identities', 'Id Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements', 'Authentication Policy', and 'Authorization Po'. The 'Id Groups' menu item is highlighted. Below the navigation, the 'Endpoint Identity Groups' section is visible, featuring an 'Add' button (a green plus sign) and a 'Delete' button (a red X).

Identity Groups

Endpoint Identity Group List > **New Endpoint Group**

Endpoint Identity Group

* Name

Description

Parent Group

Passaggio 2. Passare a Work Centers > Network Access > Identities > Endpoints > +Add.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > **Work Centers**

Network Access > **Identities** > Id Groups > Ext Id Sources > Network Resources > Policy Elements > Authentication Policy > Authorization Policy > Troubleshoot

Endpoints

Network Access Users
Identity Source Sequences

INACTIVE ENDPOINTS

AUTHENTICATION STATUS

No data available

Last Activity Date

Change Authorization Clear Threats & Vulnerabilities Export Import

Add Endpoint ✕

▼ **General Attributes**

Mac Address *

Description

Static Assignment

Policy Assignment

Static Group Assignment

Identity Group Assignment

Configurazione di ISE

Aggiunta di controller 9800 WLC a ISE.

Leggi le istruzioni in questo link: [Declare WLC to ISE](#).

Creare una 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 che possono essere utilizzati dall'utente.

Passaggio 1. Passare a **Policy > Authentication** come mostrato nell'immagine.

Confermare che la regola MAB predefinita esiste sull'ISE.

Identity Services Engine | Home | Context Visibility | Operations | **Policy** | Adm

Summary | Endpoints | Guests | Vulnerability | Threat | +

Authentication

Profiling

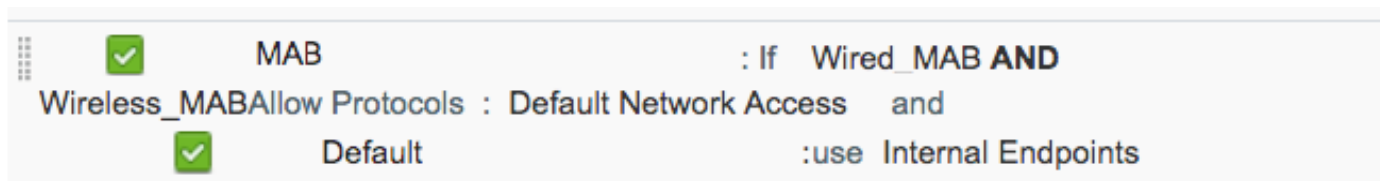
Client Provisioning

METRICS

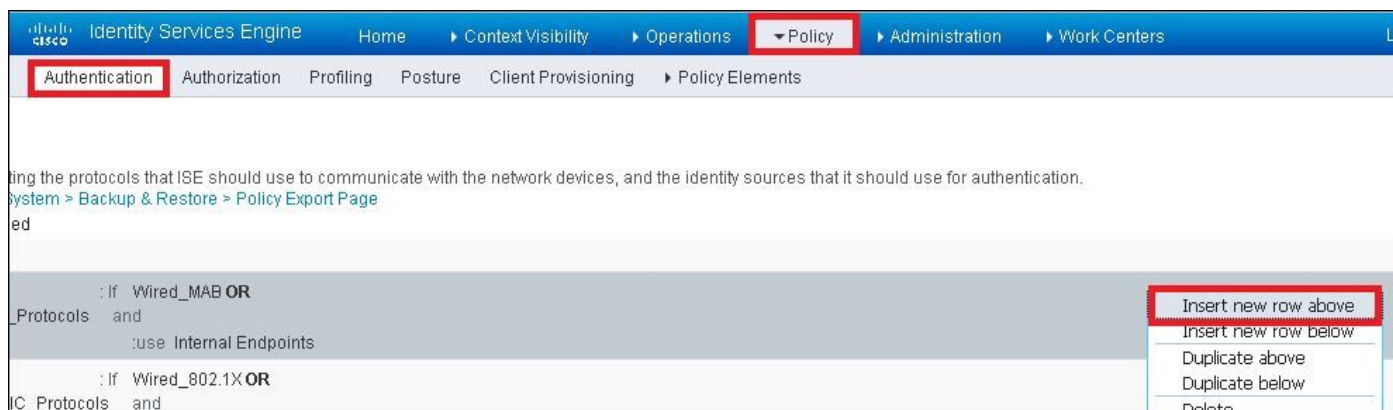
Total Endpoints ⓘ

Active Endpoi

Passaggio 2. Verificare che la regola di autenticazione predefinita per MAB esista già:



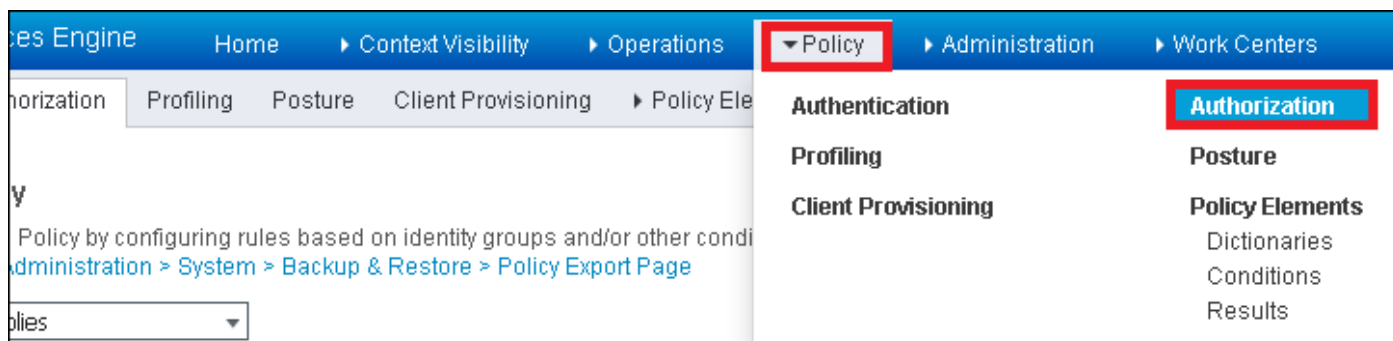
In caso contrario, è possibile aggiungerne uno nuovo facendo clic su **Insert new row above**.



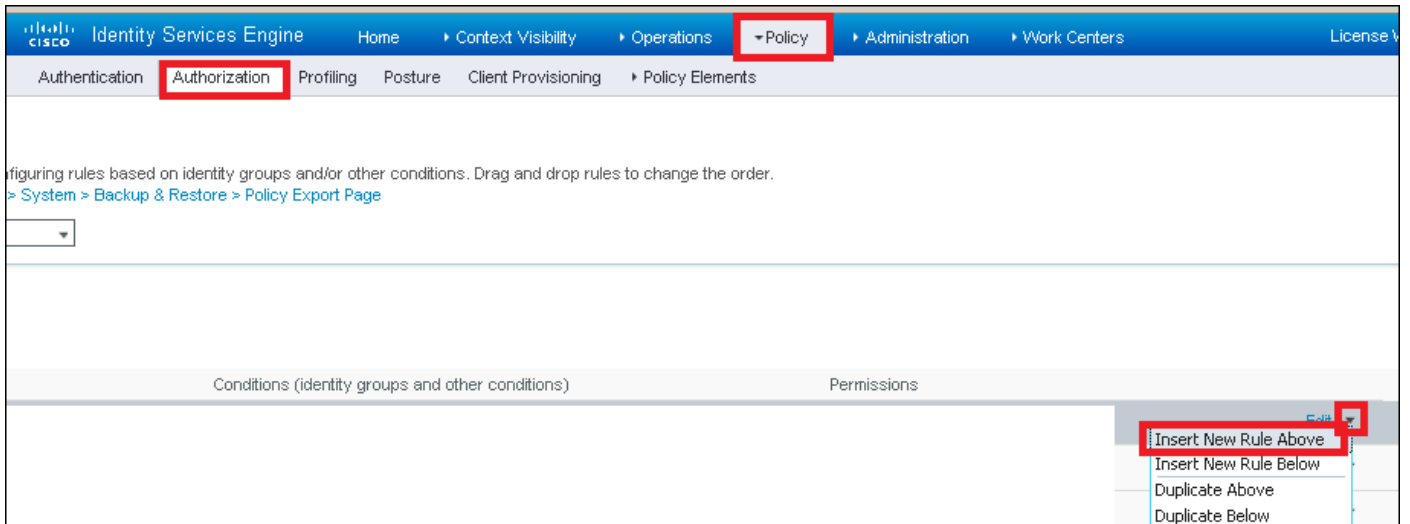
Creazione regola di autorizzazione

La regola di autorizzazione permette di stabilire quali autorizzazioni (ovvero quale profilo di autorizzazione) vengono applicate al client.

Passaggio 1. Passare a **Policy > Authorization** come mostrato nell'immagine.

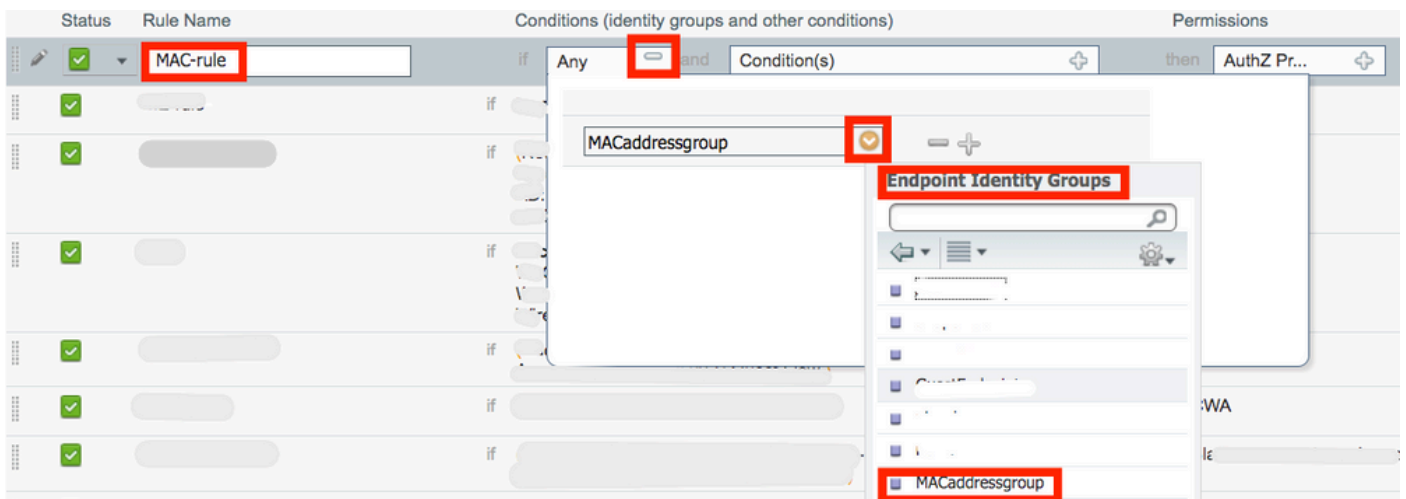


Passaggio 2. Inserite una nuova regola come mostrato nell'immagine.

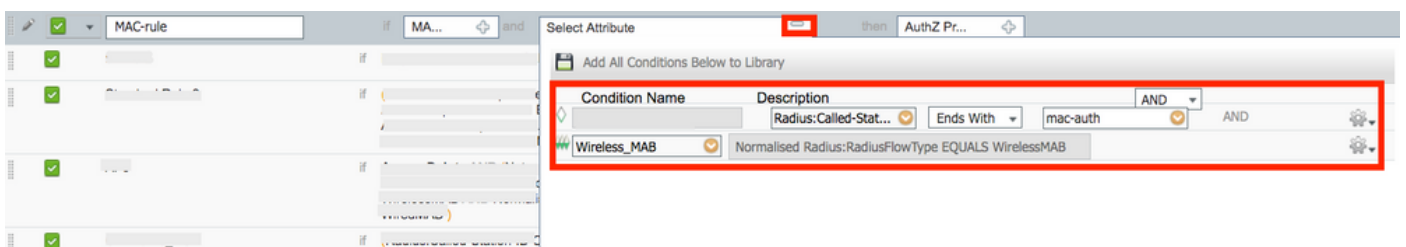


Passaggio 3. Immettere i valori.

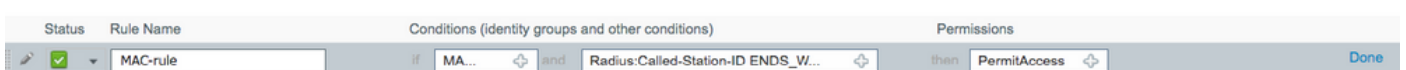
Innanzitutto, scegliete un nome per la regola e il gruppo di identità in cui è memorizzato il punto finale (MACaddressgroup), come mostrato nell'immagine.



In seguito, scegliere altre condizioni che fanno il processo di autorizzazione per rientrare in questa regola. In questo esempio, il processo di autorizzazione raggiunge questa regola se utilizza il servizio MAB wireless e il relativo ID stazione chiamato (il nome dell'SSID) termina con mac-auth come mostrato nell'immagine.



Infine, scegliere il profilo di autorizzazione assegnato, in questo caso, PermitAccess ai client che hanno eseguito la regola. Fare clic Done e salvarlo.




Verifica

Usare questi comandi per verificare la configurazione corrente:

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Risoluzione dei problemi

WLC 9800 offre funzionalità di traccia ALWAYS-ON. In questo modo, tutti gli errori, gli avvisi e i messaggi relativi alla connettività del client vengono registrati costantemente ed è possibile visualizzare i registri relativi a un evento imprevisto o a una condizione di errore dopo che si è verificato.

 Nota: anche se dipende dal volume di log generati, è possibile tornare indietro di alcune ore a diversi giorni.

Per visualizzare le tracce raccolte per impostazione predefinita dal 9800 WLC, è possibile connettersi al 9800 WLC tramite SSH/Telnet e leggere i seguenti passaggi (verificare di aver registrato la sessione su un file di testo).

Passaggio 1. Controllare l'ora corrente del controller in modo da poter tenere traccia dei registri dall'ora precedente a quella in cui si è verificato il problema.

```
# show clock
```

Passaggio 2. Raccogliere syslog dal buffer del controller o dal syslog esterno in base alla configurazione del sistema. Questo fornisce una rapida panoramica dello stato e degli eventuali errori del sistema.

```
# show logging
```

Passaggio 3. Verificare se sono abilitate le condizioni di debug.


```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address _____ Port
-----|-----
```

 Nota: se nell'elenco è presente una condizione, le tracce vengono registrate a livello di debug per tutti i processi che soddisfano le condizioni abilitate (indirizzo MAC, indirizzo IP e così via). In questo modo si aumenta il volume dei registri. È pertanto consigliabile cancellare tutte le condizioni quando non si esegue il debug attivo.

Passaggio 4. Se l'indirizzo MAC sottoposto al test non è stato elencato come condizione nel Passaggio 3., raccogliere le tracce del livello di notifica sempre attive per l'indirizzo MAC specifico.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

È possibile visualizzare il contenuto della sessione oppure copiare il file su un server TFTP esterno.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Debug condizionale e traccia Radioactive (RA)

Se le tracce sempre attive non forniscono informazioni sufficienti per determinare il trigger del problema in esame, è possibile abilitare il debug condizionale e acquisire la traccia Radio attiva (RA), che fornisce le tracce a livello di debug per tutti i processi che interagiscono con la condizione specificata (in questo caso l'indirizzo MAC del client). Per abilitare il debug condizionale, leggere i passaggi seguenti.

Passaggio 5. Verificare che non vi siano condizioni di debug abilitate.

```
# clear platform condition all
```

Passaggio 6. Abilitare la condizione di debug per l'indirizzo MAC del client wireless che si desidera monitorare.

Questi comandi iniziano a monitorare l'indirizzo MAC fornito per 30 minuti (1800 secondi). È possibile aumentare questo tempo fino a 2085978494 secondi.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```



Nota: Per monitorare più client alla volta, eseguire il comando `debug wireless mac` per indirizzo MAC.



Nota: non si visualizza l'output dell'attività del client nella sessione terminale, in quanto tutto viene memorizzato internamente per essere visualizzato successivamente.

Passaggio 7. Riprodurre il problema o il comportamento che si desidera monitorare.

Passaggio 8. Interrompere i debug se il problema viene riprodotto prima che il tempo di monitoraggio predefinito o configurato sia attivo.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Allo scadere del tempo di monitoraggio o dopo aver interrotto il debug wireless, il WLC 9800 genera un file locale con il nome: `ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

Passaggio 9. Recuperare il file dell'attività dell'indirizzo MAC. È possibile copiare il file `ra_trace.log` su un server esterno o visualizzare l'output direttamente sullo schermo.

Controllare il nome del file delle tracce RA:

```
# dir bootflash: | inc ra_trace
```

Copiare il file su un server esterno:


```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

Visualizzare il contenuto:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Passaggio 10. Se la causa principale non è ancora ovvia, raccogliere i log interni che offrono una visualizzazione più dettagliata dei log a livello di debug. non è necessario eseguire di nuovo il debug del client, in quanto è sufficiente esaminare in dettaglio i log di debug già raccolti e archiviati internamente.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file r
```

 Nota: questo output del comando restituisce tracce per tutti i livelli di registrazione per tutti i processi ed è piuttosto voluminoso. Coinvolgere Cisco TAC per analizzare queste tracce.

È possibile copiare il file `ra-internal-FILENAME.txt` su un server esterno oppure visualizzarlo direttamente sullo schermo.

Copiare il file su un server esterno:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Visualizzare il contenuto:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Passaggio 11. Rimuovere le condizioni di debug.

```
# clear platform condition all
```



Nota: assicurarsi di rimuovere sempre le condizioni di debug dopo una sessione di risoluzione dei problemi.

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).