

Configurazione dell'elenco di autorizzazioni dei Wireless Controller Catalyst 9800 AP

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Elenco autorizzazioni AP MAC - Locale](#)

[Elenco autorizzazioni punto di accesso MAC - Server RADIUS esterno](#)

[Configurazione 9800 WLC](#)

[Configurazione ISE](#)

[Configurare ISE per autenticare l'indirizzo MAC come endpoint](#)

[Configurare ISE per autenticare l'indirizzo MAC come nome utente/password](#)

[Criteri di autorizzazione per autenticare gli access point](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Riferimenti](#)

Introduzione

In questo documento viene descritto come configurare i criteri di autenticazione di Catalyst 9800 Wireless LAN Controller Access Point (AP).

Premesse

Per autorizzare un punto di accesso, l'indirizzo MAC Ethernet del punto di accesso deve essere autorizzato per il database locale con controller LAN wireless 9800 o per un server RADIUS (Remote Authentication Dial-In User Service) esterno.

Questa funzione garantisce che solo i punti di accesso autorizzati possano unirsi a un controller LAN wireless Catalyst 9800. Questo documento non copre il caso di access point mesh (serie 1500) che richiedono una voce del filtro mac per collegarsi al controller ma non tracciano il flusso tipico di autorizzazione degli access point (vedere riferimenti).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 9800 WLC
- Accesso CLI (Command Line Interface) ai controller wireless

Componenti usati

9800 WLC v17.3

AP 1810W

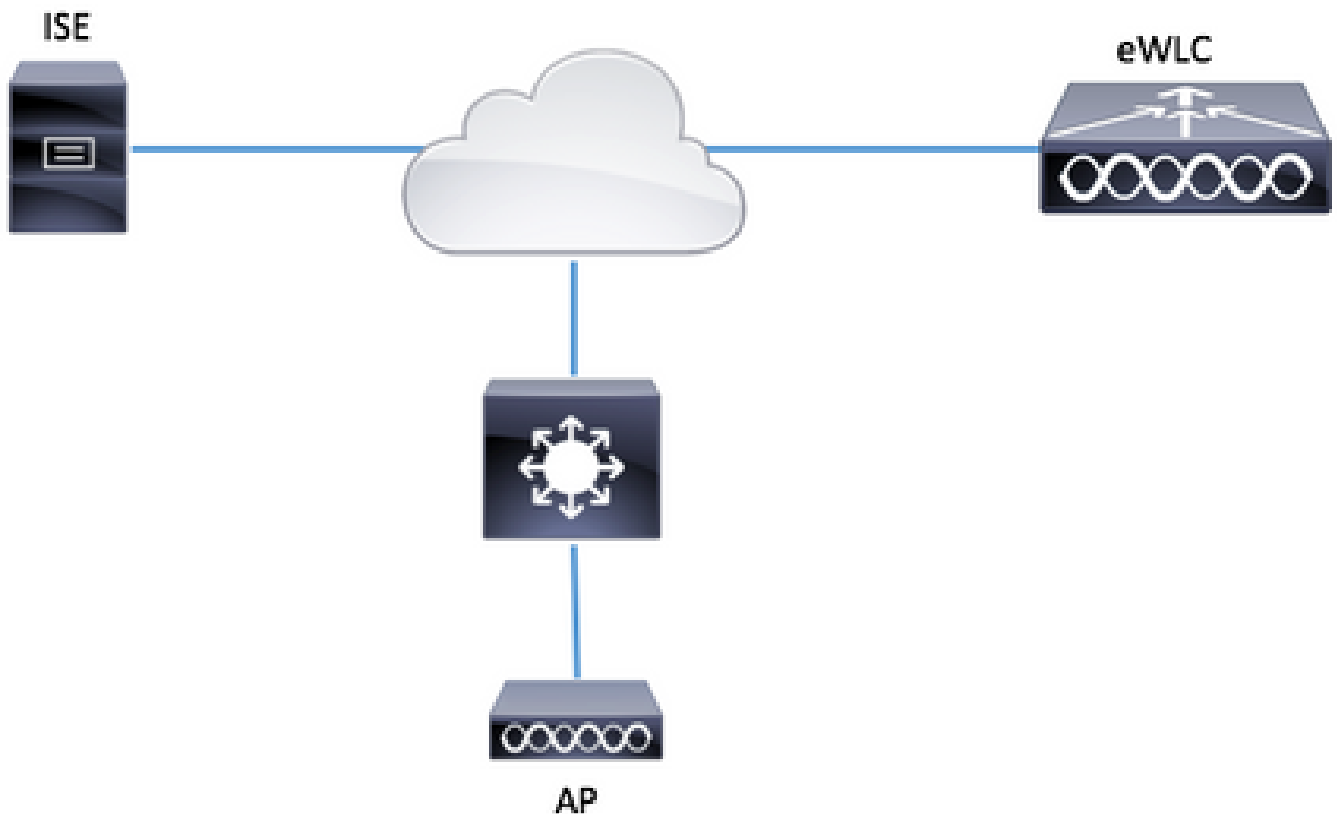
AP 1700

Identity Service Engine (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



Configurazioni

Elenco autorizzazioni AP MAC - Locale

L'indirizzo MAC degli access point autorizzati viene archiviato localmente nel WLC del 9800.

Passaggio 1. Creare un elenco di metodi di download delle credenziali di autorizzazione locale.

Selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione > +
Aggiungi

The screenshot shows the 'Authentication Authorization and Accounting' configuration page. The left sidebar has 'Configuration' highlighted. The main area shows 'AAA Method List' selected under 'Authorization'. A '+ Add' button is highlighted in the top right of the configuration area. Below it is a table with columns 'Name' and 'Type'.

Name	Type
<input type="checkbox"/> default	network
<input type="checkbox"/> AuthZ-Netw-ISE	network

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

- Method List Name*: AP-auth
- Type*: credential-download
- Group Type: local
- Available Server Groups: radius, ldap, tacacs+, ISE-KCG-grp, ISE-grp-name
- Assigned Server Groups: (empty)

Buttons at the bottom: Cancel, Save & Apply to Device.

Passaggio 2. Abilitare l'autorizzazione MAC AP.

Passare a Configurazione > Sicurezza > AAA > AAA Avanzate > Criteri PA. Abilitare Authorize APs against MAC e selezionare l'elenco dei metodi di autorizzazione creato nel passo 1.

+ AAA Wizard

AAA Method List Servers / Groups **AAA Advanced**

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC ENABLED

Authorize APs against Serial Number DISABLED

Authorization Method List AP-auth

Apply to Device

Passaggio 3. Aggiungere l'indirizzo MAC Ethernet AP.

Selezionare Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List **AAA Advanced**

Global Config

RADIUS Fallback

Attribute List Name

Device Authentication

AP Policy

Password Policy

AAA Interface

MAC Address Serial Number

+ Add × Delete

MAC Address


0 10 items per page

Quick Setup: MAC Filtering

MAC Address* 00:B0:E1:8C:49:E8

Attribute List Name None

Cancel Save & Apply to Device

 Nota: l'indirizzo MAC Ethernet AP deve essere in uno di questi formati quando viene immesso nell'interfaccia utente Web (xx:xx:xx:xx:xx (o) xxxx.xxxx.xxxx (o) xx-xx-xx-xx-xx-xx) nella versione 16.12. Nella versione 17.3, devono essere nel formato xxxxxxxxxxxx senza alcun separatore. Il formato CLI è sempre xxxxxxxxxxxx in qualsiasi versione (nella versione 16.12, l'interfaccia utente Web rimuove i separatori nella configurazione). l'ID bug Cisco [CSCv43870](https://cisco.com/cisco/webbugtool/bugdetails?bug=CSCv43870) consente di usare qualsiasi formato nella CLI o nell'interfaccia utente Web nelle versioni più recenti.

CLI:

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

Elenco autorizzazioni punto di accesso MAC - Server RADIUS esterno

Configurazione 9800 WLC

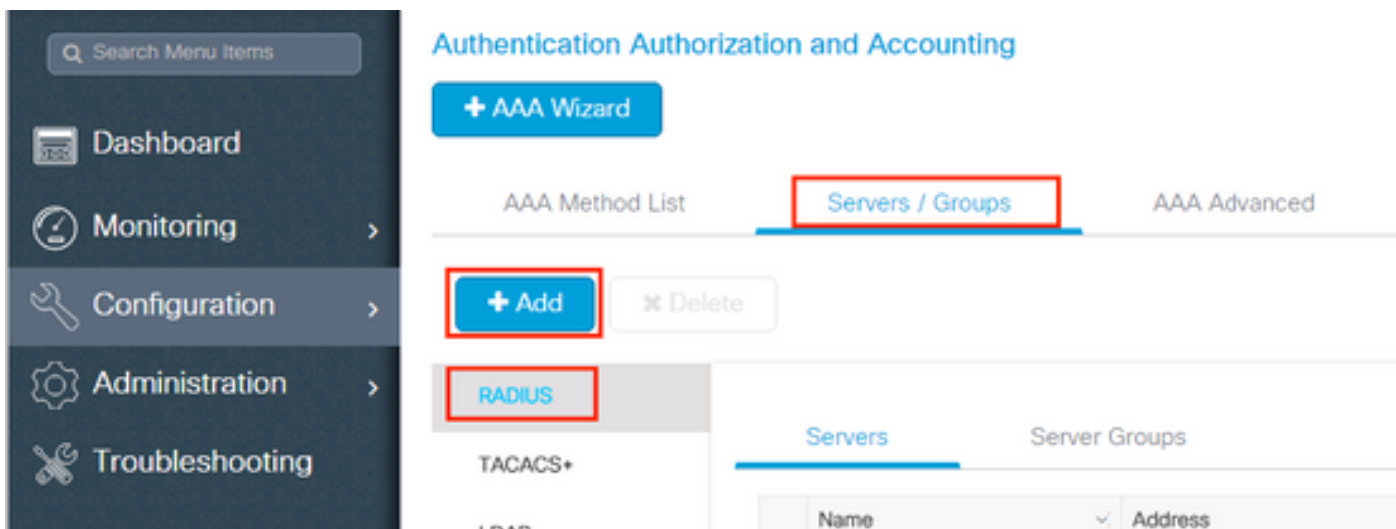
L'indirizzo MAC dei punti di accesso autorizzati viene memorizzato su un server RADIUS esterno, nell'esempio ISE.

Ad ISE, è possibile registrare l'indirizzo MAC degli access point come nome utente/password o come endpoint. Lungo i passaggi viene indicato come selezionare l'utilizzo di un modo o dell'altro.

GUI:

Passaggio 1. Dichiarare server RADIUS

Selezionare Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Server > + Aggiungi e immettere le informazioni sul server RADIUS.



Verificare che l'opzione Support for CoA (Supporto per CoA) sia abilitata se si pensa di usare in futuro l'autenticazione Web centralizzata o altro tipo di sicurezza che richieda una modifica di autorizzazione, o CoA (Change of Authorization).

Create AAA Radius Server

Name*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPv4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

Passaggio 2. Aggiungere il server RADIUS a un gruppo RADIUS

Selezionare Configurazione > Sicurezza > AAA > Server / Gruppi > RADIUS > Gruppi di server > + Aggiungi

Per fare in modo che ISE autentichi l'indirizzo MAC AP come nomi utente, lasciare MAC-Filtering impostato su none (nessuno).

Create AAA Radius Server Group



Name*

ISE-grp-name

Group Type

RADIUS

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

1-1440

Available Servers



Assigned Servers

ISE-icg

Cancel

Save & Apply to Device

Affinché ISE autentichi l'indirizzo MAC dell'access point come endpoint, modificare il filtro MAC in mac.

Create AAA Radius Server Group ✕

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers Assigned Servers

ISE-KCG

Passaggio 3. Creare un elenco di metodi per il download delle credenziali di autorizzazione.

Selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione > +
 Aggiungi

Search Menu Items

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

Authentication Authorization and Accounting

[+ AAA Wizard](#)

AAA Method List Servers / Groups AAA Advanced

General

Authentication

Authorization

Accounting

[+ Add](#)

	Name	Type
<input type="checkbox"/>	default	network
<input type="checkbox"/>	AuthZ-Netw-ISE	network

Quick Setup: AAA Authorization ✕

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups

radius
 ldap
 tacacs+
 ISE-KCG-grp

Assigned Server Groups

ISE-grp-name

Passaggio 4. Abilitare l'autorizzazione MAC AP.

Passare a Configurazione > Sicurezza > AAA > AAA Avanzate > Criteri PA. Abilitare Authorize APs against MAC e selezionare l'elenco dei metodi di autorizzazione creato nel passo 3.

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List
Servers / Groups
AAA Advanced

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC ENABLED

Authorize APs against Serial Number DISABLED

Authorization Method List

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 credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

Configurazione ISE

Passaggio 1. Per aggiungere 9800 WLC a ISE:

[Dichiarare 9800 WLC su ISE](#)

Scegliere questa opzione per configurare l'indirizzo MAC degli access point in base all'autenticazione con i passaggi richiesti:

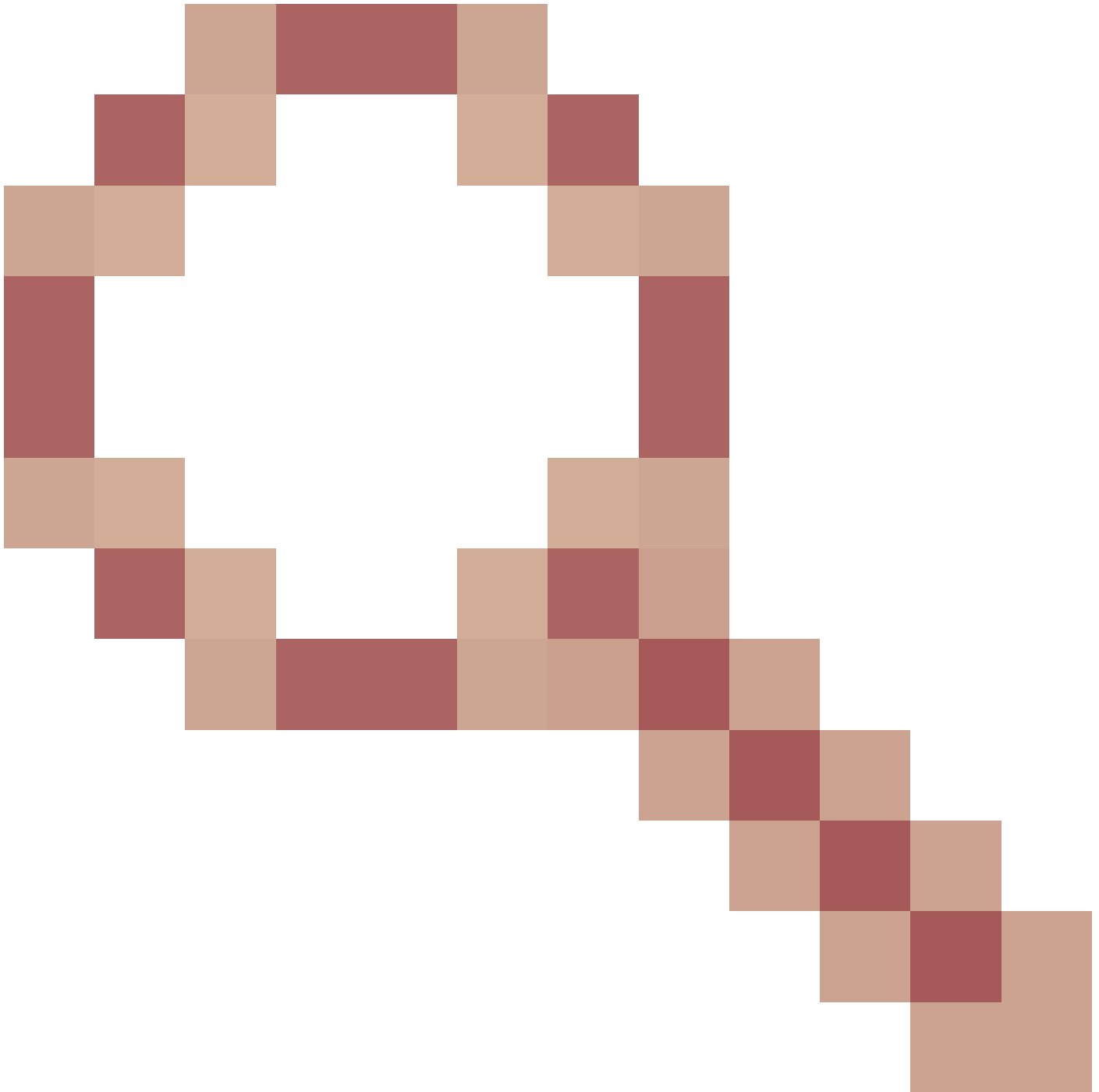
[Configurare ISE per autenticare l'indirizzo MAC come endpoint](#)

[Configurare ISE per autenticare l'indirizzo MAC come nome utente/password](#)

Configurare ISE per autenticare l'indirizzo MAC come endpoint

Passaggio 2. (Facoltativo) Creare un gruppo di identità per i punti di accesso

Poiché lo switch 9800 non invia l'attributo NAS-port-Type con autorizzazione AP (bug Cisco [IDCSCvy74904](#))



), ISE non riconosce un'autorizzazione AP come flusso di lavoro MAB e quindi non è possibile autenticare un access point se l'indirizzo MAC dell'access point è incluso nell'elenco degli endpoint a meno che non si modifichino i flussi di lavoro MAB in modo da non richiedere l'attributo NAS-PORT-type su ISE.

Selezionare Amministratore > Profilo dispositivo di rete e creare un nuovo profilo dispositivo. Abilitare RADIUS e aggiungere service-type=call-check per Wired MAB. È possibile copiare il resto dal profilo originale Cisco; l'idea è di non avere la condizione "nas-port-type" per il MAB cablato.

* Name

Description

Icon



[Change icon...](#)

[Set To Default](#)



Vendor

Supported Protocols

- RADIUS
- TACACS+
- TrustSec

RADIUS Dictionaries

Templates

[Expand All](#) / [Collapse All](#)

Authentication/Authorization

Flow Type Conditions

Wired MAB detected if the following condition(s) are met :

⋮ ▾ = ▾

Tornare alla voce relativa al dispositivo di rete per il modello 9800 e impostare il relativo profilo sul nuovo profilo del dispositivo creato.

Passare a Amministrazione > Gestione delle identità > Gruppi > Gruppi di identità degli endpoint > + Aggiungi.

Endpoint Identity Groups

Edit **Add** Delete

Name	Description
------	-------------

Scegliere un nome e fare clic su Invia.

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

Endpoint Identity Group

* Name

Description

Parent Group

Passaggio 3. Aggiungere l'indirizzo MAC Ethernet AP al relativo gruppo di identità dell'endpoint.

Selezionare Centri di lavoro > Accesso alla rete > Identità > Endpoint > +

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers' (highlighted with a red box). Below this, the 'Network Access' menu is expanded, showing 'Identities' (highlighted with a red box). The 'Endpoints' section is active, displaying a bar chart titled 'INACTIVE ENDPOINTS' with a count of 1. The x-axis is labeled 'Last Activity Date' and shows a date of 8/27. The y-axis ranges from 0 to 1. To the right, there is a section for 'AUTHENTICATED' endpoints, with a note 'disconnected: [1009]'. At the bottom, a table header is visible with columns for 'MAC Address', 'Status', 'IPv4 Address', and 'Username'. A red box highlights a '+' icon in the table's toolbar.

Immettere le informazioni necessarie.

Add Endpoint



General Attributes

Mac Address *

Description

Static Assignment

Policy Assignment

Static Group Assignment

Identity Group Assignment

Passaggio 4. Verificare che l'archivio identità utilizzato nella regola di autenticazione predefinita contenga gli endpoint interni.

A. Passare a Criterio > Autenticazione e prendere nota dell'archivio di identità.

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

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity source for each protocol. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)





Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MABAllow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1XAllow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores

B. Passare a Amministrazione > Gestione delle identità > Sequenze origini identità > Nome identità.

Identity Source Sequences

For Policy Export go to [Administration](#) > [System](#) > [Backup & Restore](#) > [Policy Export Page](#)

 Edit  Add  Duplicate  Delete

<input type="checkbox"/>	Name	Description	Identity
<input type="checkbox"/>	All_User_ID_Stores	A built-in Identity Sequence to include all User Identity Stores	Preload
<input type="checkbox"/>	Certificate_Request_Sequence	A built-in Identity Sequence for Certificate Request APIs	Internal
<input type="checkbox"/>	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal
<input type="checkbox"/>	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal
<input type="checkbox"/>	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal

C. Verificare che gli endpoint interni appartengano a tale endpoint. In caso contrario, aggiungerli.

Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
<input type="text" value="Internal Endpoints"/>	<input type="button" value=">"/>	<input type="text" value="Internal Users"/> <input type="text" value="All_AD_Join_Points"/> <input type="text" value="Guest Users"/>
	<input type="button" value="<"/>	<input type="button" value="↑"/>
	<input type="button" value="⇒"/>	<input type="button" value="↓"/>
	<input type="button" value="⇐"/>	<input type="button" value="↕"/>

▼ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Configurare ISE per autenticare l'indirizzo MAC come nome utente/password

Questo metodo non è consigliato in quanto richiede criteri per le password inferiori per consentire la stessa password del nome utente.

Tuttavia, può rappresentare una soluzione nel caso in cui non sia possibile modificare il profilo del dispositivo di rete

Passaggio 2. (Facoltativo) Creare un gruppo di identità per i punti di accesso

Passare a Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente > +
Aggiungi.

The screenshot shows the 'Identity Groups' sidebar on the left with 'User Identity Groups' selected. The main area is titled 'User Identity Groups' and contains a toolbar with 'Edit', '+ Add', 'Delete', 'Import', and 'Export' buttons. Below the toolbar is a table with columns 'Name' and 'Description'. The table contains one entry: 'ALL_ACCOUNTS (default)' with a description of 'Default ALL_'. The '+ Add' button is highlighted with a red box.

Scegliere un nome e fare clic su Invia.

User Identity Groups > New User Identity Group

Identity Group

* Name

Description

Passaggio 3. Verificare che i criteri password correnti consentano di aggiungere un indirizzo MAC come nome utente e password.

Passare a Amministrazione > Gestione identità > Impostazioni > Impostazioni autenticazione utente > Criteri password e verificare che almeno queste opzioni siano disabilitate:

Cisco Identity Services Engine Administration Settings

User Authentication Settings

Password Policy

Account Disable Policy

Minimum Length: 4 characters (Valid Range 4 to 127)

Password must not contain:

- User name or its characters in reverse order
- "cisco" or its characters in reverse order
- This word or its characters in reverse order:
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced with other characters ?

Default Dictionary ?

Custom Dictionary ? No file chosen

The newly added custom dictionary file will replace the existing custom dictionary file.

Password must contain at least one character of each of the selected types:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

Password History


- Password must be different from the previous 3 versions (Valid Range 1 to 10)
- Password change delta 3 characters (Valid Range 3 to 10)
- Cannot reuse password within 15 days (Valid Range 0 to 365)

Password Lifetime

Users can be required to periodically change password

- Disable user account after 60 days if password was not changed (valid range 1 to 3650)
- Display reminder 30 days prior to password expiration (valid range 1 to 3650)
- Lock/Suspend Account with Incorrect Login Attempts

- # 3 (Valid Range 3 to 20)
- Suspend account for 15 minutes (Valid Range 15 to 1440) Disable account

 Nota: è possibile disabilitare l'opzione Disabilita account utente dopo XX giorni se la password non è stata modificata. Poiché si tratta di un indirizzo MAC, la password non cambia mai.

Passaggio 4. Aggiungere l'indirizzo MAC Ethernet AP.

Selezionare Amministrazione > Gestione delle identità > Identità > Utenti > + Aggiungi








CISCO Identity Services Engine Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Administration

▶ System ▶ Identity Management ▶ Network Resources ▶ Device Portal Management pxGrid Services ▶ Feed Service

▶ Identities Groups External Identity Sources Identity Source Sequences ▶ Settings

Users

Latest Manual Network Scan Results

 Edit  Add  Change Status  Import  Export  Delete 

Status	Name	Description	First N
--------	------	-------------	---------

Immettere le informazioni necessarie.

▼ Network Access User

* Name

Status Enabled ▼

Email

▼ Passwords

Password Type: ▼

Password

Re-Enter Password

* 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 (yyyy-mm-dd)

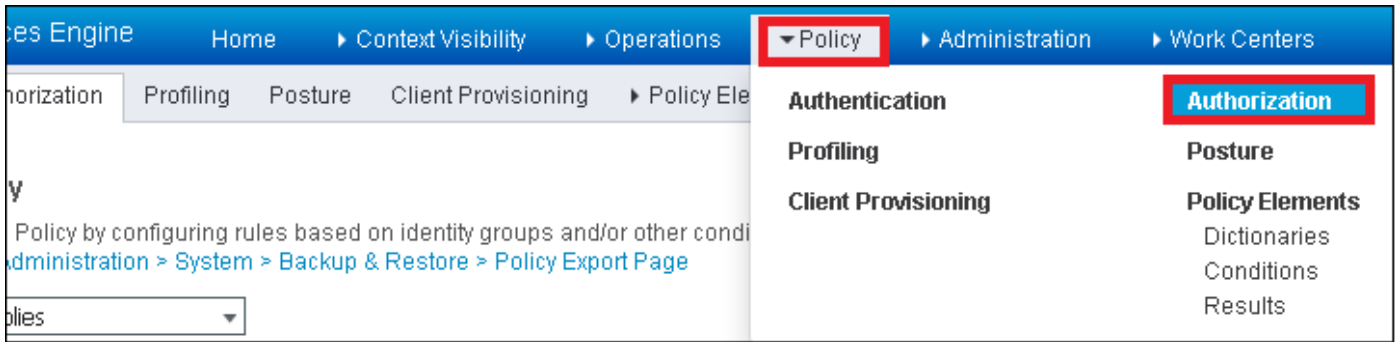
▼ User Groups

- +

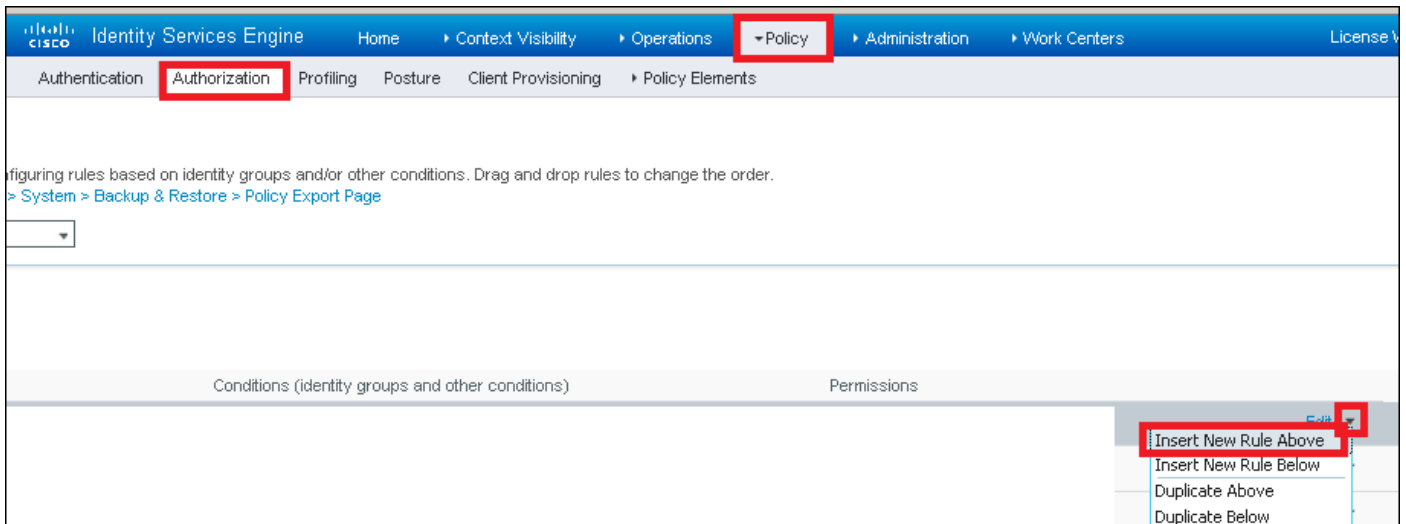
 Nota: Name e Login Passwordfield devono corrispondere all'indirizzo MAC Ethernet dell'access point, in lettere minuscole e senza separatori.

Criteria di autorizzazione per autenticare gli access point

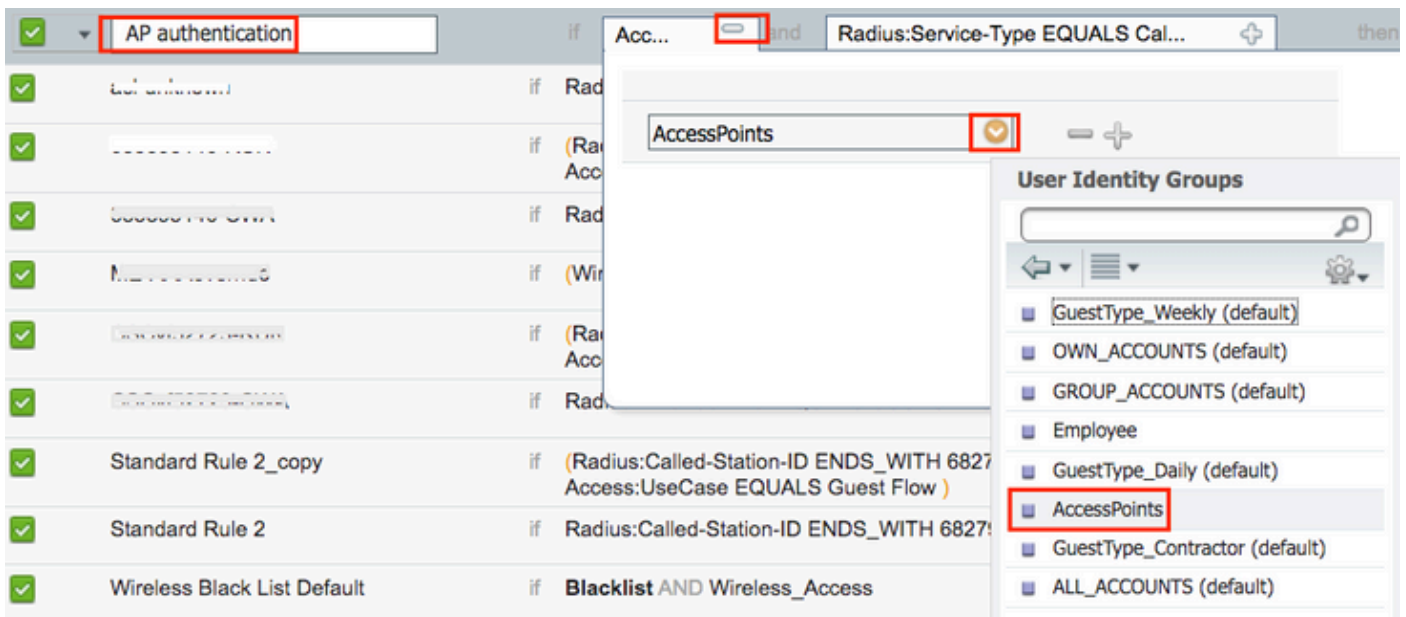
Passare a Criterio > Autorizzazione come mostrato nell'immagine.



Inserite una nuova regola come mostrato nell'immagine.



Selezionare innanzitutto un nome per la regola e il gruppo di identità in cui è memorizzato il punto di accesso (AccessPoint). Selezionare Gruppi identità utente se si è deciso di autenticare l'indirizzo MAC come password del nome utente o Gruppi identità endpoint se si sceglie di autenticare l'indirizzo MAC AP come endpoint.



In seguito, selezionare altre condizioni che fanno rientrare il processo di autorizzazione in questa regola. Nell'esempio, il processo di autorizzazione raggiunge questa regola se utilizza il tipo di

servizio Controllo delle chiamate e la richiesta di autenticazione proviene dall'indirizzo IP 10.88.173.52.

The screenshot shows a configuration window with a header bar containing 'Radius:Service-Type EQUALS Cal...' and 'then AuthZ Pr...'. Below the header is a section titled 'Add All Conditions Below to Library'. The main area contains a table with two rows of conditions. The first row has a diamond icon, a text input field, 'Radius:Service-Type' with a dropdown arrow, 'Equals' with a dropdown arrow, 'Call Check' with a dropdown arrow, and 'AND'. The second row has a diamond icon, a text input field, 'Radius:NAS-IP-Ad...' with a dropdown arrow, 'Equals' with a dropdown arrow, '10.88.173.52' with a dropdown arrow, and a gear icon.

Infine, selezionare il profilo di autorizzazione assegnato ai client che hanno raggiunto la regola, fare clic su Annulla e salvarlo come mostrato nell'immagine.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	AP authentication	if AccessPoints AND (Radius:Service-Type EQUALS Call Check AND Radius:NAS-IP-Address EQUALS 10.88.173.52)	then PermitAccess

Nota: gli access point già aggiunti al controller non perdono l'associazione. Se, tuttavia, dopo l'abilitazione dell'elenco di autorizzazioni, la comunicazione con il controller viene interrotta e si tenta di eseguire il join, viene eseguito il processo di autenticazione. Se gli indirizzi MAC non sono elencati localmente o nel server RADIUS, non sarà possibile eseguire il join al controller.

Verifica

Verifica se 9800 WLC ha abilitato l'elenco di autenticazione AP

```
<#root>
```

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled  
Authorize APs against Serial Num : Enabled  
Authorization Method List : <auth-list-name>
```

Verificare la configurazione del raggio:

```
<#root>
```

```
#
```

```
show run aaa
```

Risoluzione dei problemi

WLC 9800 offre funzionalità di traccia ALWAYS-ON. In questo modo, tutti gli errori correlati al join dell'access point, i messaggi di avviso e di livello di avviso vengono registrati costantemente ed è possibile visualizzare i registri di un evento imprevisto o di una condizione di errore dopo che si è verificato.



Nota: il volume dei log generati varia all'indietro da alcune ore a diversi giorni.

Per visualizzare le tracce raccolte per impostazione predefinita dal protocollo 9800 WLC, è possibile connettersi al protocollo 9800 WLC tramite SSH/Telnet attenendosi alla seguente procedura (accertarsi di registrare la sessione in un file di testo).

Passaggio 1. Controllare l'ora corrente del controller in modo da poter tenere traccia dei log nel tempo che intercorre tra il momento 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. In questo modo è possibile visualizzare rapidamente lo stato di integrità del sistema ed eventuali errori.

```
# 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 Trace 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). Ciò aumenta le dimensioni dei log. Pertanto, si consiglia di cancellare tutte le condizioni quando non si effettua attivamente il debug.

Passaggio 4. Si supponga che l'indirizzo MAC in fase di test non sia stato elencato come condizione nel passaggio 3, raccogliere le tracce del livello di avviso always on per l'indirizzo MAC radio 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 dei livelli di debug per tutti i processi che interagiscono con la condizione specificata (in questo caso l'indirizzo MAC del client).


Passaggio 5. Accertarsi 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.

Questo comando avvia il monitoraggio dell'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 <aaa.bbbb.ccc> per ogni indirizzo MAC.

 Nota: l'output dell'attività del client nella sessione terminale non viene visualizzato, in quanto tutto viene memorizzato internamente nel buffer 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>
```

Una volta trascorso il tempo di monitoraggio o interrotto il debug wireless, il controller 9800 WLC 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 la traccia RA .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 del livello di debug. non è necessario eseguire di nuovo il

debug del client, in quanto vengono forniti solo ulteriori dettagli sui 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. Contattare Cisco TAC per analizzare queste tracce.

È possibile copiare il file ra-internal-FILENAME.txt su un server esterno o visualizzare l'output 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.

Riferimenti

[Unisci punti di accesso mesh a 9800 WLC](#)

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).