

# Configurazione dei filtri MAC con i controller WLC (Wireless LAN Controller) AireOS

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Filtro indirizzi MAC \(autenticazione MAC\) sui WLC](#)

[Configurazione dell'autenticazione MAC locale sui WLC](#)

[Configurazione di una WLAN e abilitazione del filtro MAC](#)

[Configurare il database locale sul WLC con gli indirizzi MAC del client](#)

[Configurazione dell'autenticazione MAC con un server RADIUS](#)

[Configurazione di una WLAN e abilitazione del filtro MAC](#)

[Configurazione del server RADIUS con gli indirizzi MAC del client](#)

[Usare la CLI per configurare il filtro MAC sul WLC](#)

[Configurazione di un timeout per i client disabilitati](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene spiegato come configurare i filtri MAC sui Wireless LAN Controller (WLC).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di LAP e WLC Cisco
- Soluzioni Cisco Unified Wireless Security

### Componenti usati

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

hardware:

- Cisco 4400 WLC con software versione 5.2.178.0
- Cisco serie 1230AG LAP
- scheda client wireless 802.11 a/b/g con firmware 4.4
- Aironet Desktop Utility (ADU) versione 4.4

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.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

## Premesse

In questo documento viene descritto come configurare i filtri MAC con i controller WLC (Wireless LAN Controller) con un esempio di configurazione. In questo documento viene spiegato inoltre come autorizzare gli access point LAP (Lightweight Access Point) in un server AAA.

## Filtro indirizzi MAC (autenticazione MAC) sui WLC

Quando si crea un filtro di indirizzi MAC sui WLC, agli utenti viene concesso o negato l'accesso alla rete WLAN in base all'indirizzo MAC del client che utilizzano.

I WLC supportano due tipi di autenticazione MAC:

- Autenticazione MAC locale
- Autenticazione MAC utilizzata con un server RADIUS

Con l'autenticazione MAC locale, gli indirizzi MAC degli utenti vengono archiviati in un database sul WLC. Quando un utente tenta di accedere alla WLAN configurata per il filtro MAC, l'indirizzo MAC del client viene convalidato in base al database locale sul WLC e il client ottiene l'accesso alla WLAN se l'autenticazione ha esito positivo.

Per impostazione predefinita, il database locale WLC supporta fino a 512 voci utente.

Il database locale degli utenti può contenere un massimo di 2048 voci. Il database locale memorizza le voci per questi elementi:

- Utenti di gestione locale, che includono ambasciatori della lobby

- Utenti della rete locale, inclusi gli utenti guest
- Voci filtro MAC
- Voci dell'elenco di esclusione
- Voci dell'elenco di autorizzazione dei punti di accesso

Tutti questi tipi di utenti non possono superare le dimensioni del database configurate.

Per aumentare il numero del database locale, usare questo comando dalla CLI:

```
<#root>  
  
<Cisco Controller>  
  
config database size ?  
  
<count>          Enter the maximum number of entries (512-2048)
```

In alternativa, è possibile eseguire l'autenticazione dell'indirizzo MAC anche con un server RADIUS. L'unica differenza consiste nel fatto che il database degli indirizzi MAC degli utenti viene archiviato nel server RADIUS anziché nel WLC. Quando un database utente viene archiviato su un server RADIUS, il WLC inoltra l'indirizzo MAC del client al server RADIUS per la convalida del client. Il server RADIUS convalida quindi l'indirizzo MAC in base al database di cui dispone. Se l'autenticazione del client ha esito positivo, al client viene concesso l'accesso alla WLAN. È possibile utilizzare qualsiasi server RADIUS che supporta l'autenticazione dell'indirizzo MAC.

## Configurazione dell'autenticazione MAC locale sui WLC

Per configurare l'autenticazione MAC locale sui WLC:

1. [Configurare una WLAN e abilitare il filtro MAC.](#)
2. [Configurare il database locale sul WLC con gli indirizzi MAC del client.](#)



Nota: prima di configurare l'autenticazione MAC, è necessario configurare il WLC per il funzionamento di base e registrare i LAP sul WLC. In questo documento si presume che il WLC sia già configurato per il funzionamento di base e che i LAP siano registrati sul WLC. Se si è un nuovo utente e si desidera provare a configurare il WLC per il funzionamento di base con i LAP, fare riferimento alla sezione [Risoluzione dei problemi di un Lightweight Access Point che non riesce a collegarsi a un WLC.](#)

---



Nota: non è necessaria una configurazione speciale sul client wireless per supportare l'autenticazione MAC.

---

## Configurazione di una WLAN e abilitazione del filtro MAC

Per configurare una WLAN con il filtro MAC:

1. Per creare una WLAN, fare clic su WLAN dall'interfaccia utente del controller.

Viene visualizzata la finestra WLAN. In questa finestra sono elencate le WLAN configurate sul controller.

2. Per configurare una nuova WLAN, fare clic su New (Nuovo).

Nell'esempio, il nome della WLAN è MAC-WLAN e l'ID della WLAN è 1.

### WLANs > New

Type	WLAN
Profile Name	MAC-WLAN
SSID	MAC-WLAN
ID	1

Configurazione dell'abilitazione del filtro MAC per WLAN

3. Fare clic su Apply (Applica).
4. Nella finestra WLAN > Modifica, definire i parametri specifici della WLAN.

### WLANs > Edit

The screenshot shows the 'WLANs > Edit' configuration page. At the top, there are four tabs: 'General', 'Security', 'QoS', and 'Advanced'. The 'Security' tab is selected. Below the tabs, there are three sub-tabs: 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'Layer 2' sub-tab is selected. In the 'Layer 2 Security' section, there is a dropdown menu set to 'None' and a checked checkbox for 'MAC Filtering'. A red box highlights these two settings.

Definizione dei parametri

- a. In Protezione > Layer 2 > Criteri di sicurezza di Layer 2, selezionare la casella di controllo Filtro MAC.

In questo modo viene abilitata l'autenticazione MAC per la WLAN.

b. In Generale > Nome interfaccia , selezionare l'interfaccia a cui è mappata la WLAN.

Nell'esempio, la WLAN è mappata all'interfaccia di gestione.

c. Selezionare gli altri parametri, che dipendono dai requisiti di progettazione della WLAN.

d. Fare clic su Apply (Applica).

### WLANs > Edit

The screenshot shows the 'WLANs > Edit' configuration window with the 'Security' tab selected. The 'Status' is checked and set to 'Enabled'. Under 'Security Policies', 'MAC Filtering' is selected. The 'Interface' dropdown is set to 'management'. A note states: '(Modifications done under security tab will appear after applying th...'. Other visible settings include 'Profile Name: MAC-WLAN', 'Type: WLAN', 'SSID: MAC-WLAN', 'Radio Policy: All', and 'Broadcast SSID: Enabled'.

WLAN mappata sull'interfaccia

Il passaggio successivo è quello di configurare il database locale sul WLC con gli indirizzi MAC del client.

Per informazioni su come configurare le interfacce dinamiche (VLAN) sui WLC, fare riferimento agli [esempi di configurazione delle VLAN sui controller LAN wireless](#).

### Configurare il database locale sul WLC con gli indirizzi MAC del client

Per configurare il database locale con un indirizzo MAC client sul WLC:

1. Fare clic su Security (Sicurezza) nell'interfaccia utente del controller, quindi su MAC Filtering (Filtro MAC) dal menu a sinistra.

Viene visualizzata la finestra Filtro MAC.

## MAC Filtering

RADIUS Compatibility Mode

Cisco ACS

(In the Radius Access Request MAC address.)

MAC Delimiter

No Delimiter

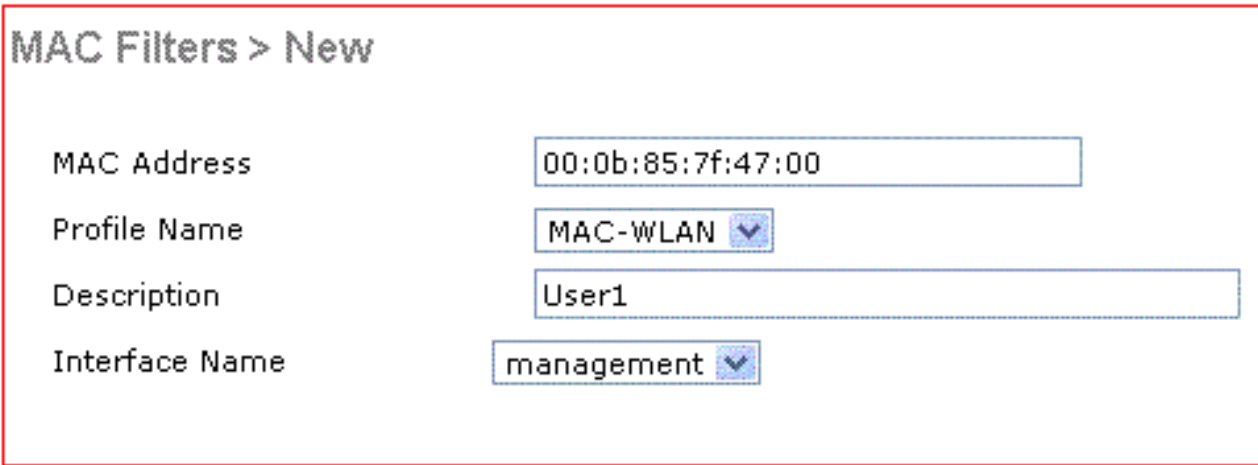
## Local MAC Filters

**MAC Address Profile Name Interface Description**

Finestra Filtro MAC

2. Per creare una voce relativa all'indirizzo MAC del database locale sul WLC, fare clic su New (Nuovo).
3. Nella finestra Filtri MAC > Nuovo , immettere l'indirizzo MAC, il nome del profilo, la descrizione e il nome dell'interfaccia per il client.

Di seguito è riportato un esempio:



**MAC Filters > New**

MAC Address	00:0b:85:7f:47:00
Profile Name	MAC-WLAN
Description	User1
Interface Name	management

Crea un database locale per l'indirizzo MAC

4. Fare clic su Apply (Applica).
5. Ripetere i passaggi da 2 a 4 per aggiungere altri client al database locale.

Ora, quando i client si connettono a questa WLAN, il WLC convalida l'indirizzo MAC dei client rispetto al database locale e, se la convalida ha esito positivo, il client ottiene l'accesso alla rete.



Nota: nell'esempio, è stato usato solo un filtro indirizzi MAC senza altri meccanismi di sicurezza di layer 2. Cisco consiglia di utilizzare l'autenticazione dell'indirizzo MAC con altri metodi di sicurezza di livello 2 o 3. Non è consigliabile utilizzare solo l'autenticazione dell'indirizzo MAC per proteggere la rete WLAN, in quanto non fornisce un meccanismo di sicurezza efficace.

## Configurazione dell'autenticazione MAC con un server RADIUS

Per configurare l'autenticazione MAC con un server RADIUS, utilizzare questi collegamenti. Nell'esempio, il server Cisco Secure ACS viene utilizzato come server RADIUS.

1. [Configurazione di una WLAN e abilitazione del filtro MAC](#)
2. [Configurazione del server RADIUS con gli indirizzi MAC del client](#)

### Configurazione di una WLAN e abilitazione del filtro MAC

Per configurare una WLAN con il filtro MAC:

1. Per creare una WLAN, fare clic su WLAN dall'interfaccia utente del controller.

Viene visualizzata la finestra WLAN. In questa finestra sono elencate le WLAN configurate sul controller.

2. Per configurare una nuova WLAN, fare clic su New (Nuovo).

Nell'esempio, il nome della WLAN è MAC-ACS-WLAN e l'ID della WLAN è 2.

#### WLANs > New

Type	WLAN
Profile Name	MAC-ACS-WLAN
SSID	MAC-ACS-WLAN
ID	2

Configurazione di una nuova WLAN Abilitazione del filtro MAC

3. Fare clic su Apply (Applica).
4. Nella finestra WLAN > Modifica, definire i parametri specifici della WLAN.
  - a. In Protezione > Layer 2 > Criteri di sicurezza di Layer 2, selezionare la casella di

controllo Filtro MAC.

In questo modo viene abilitata l'autenticazione MAC per la WLAN.

b. In Generale > Nome interfaccia , selezionare l'interfaccia a cui è mappata la WLAN.

c. In Protezione > Server AAA > Server RADIUS , selezionare il server RADIUS che può essere utilizzato per l'autenticazione MAC.

### WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:10.77.244.196, Port:1812	None
Server 2	None	None
Server 3	None	None

Enabled

Selezionare il server RADIUS da utilizzare per l'autenticazione MAC.

Nota: prima di selezionare il server RADIUS dalla finestra WLAN > Modifica, è necessario definire il server RADIUS nella finestra Sicurezza > Autenticazione Radius e abilitare il server RADIUS.

RADIUS Authentication Servers

Call Station ID Type: IP Address

Use AES Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.77.244.196	1812	Enabled	Enabled

Server di autenticazione Radius

d. Selezionare gli altri parametri, che dipendono dai requisiti di progettazione della WLAN.

e. Fare clic su Apply (Applica).



## WLANs > Edit

General	Security	QoS	Advanced
Profile Name	MAC-ACS-WLAN		
Type	WLAN		
SSID	MAC-ACS-WLAN		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	<b>MAC Filtering</b> (Modifications done under security tab will appear after applying the		
Radio Policy	All		
Interface	management		
Broadcast SSID	<input checked="" type="checkbox"/> Enabled		

Parametri dei requisiti di progettazione

5. Fare clic su Sicurezza > Filtro MAC.

6. Nella finestra Filtro MAC, scegliere il tipo di server RADIUS in Modalità compatibilità RADIUS.

In questo esempio viene utilizzato Cisco ACS.

7. Dal menu a discesa Delimitatore MAC, scegliete il delimitatore MAC.

In questo esempio vengono utilizzati i due punti (:) e (:): (:).

8. Fare clic su Apply (Applica).

### MAC Filtering

RADIUS Compatibility Mode	Cisco ACS	(In the Radius Access Request MAC address.)
MAC Delimiter	Colon	

Scegliere il tipo di server RADIUS

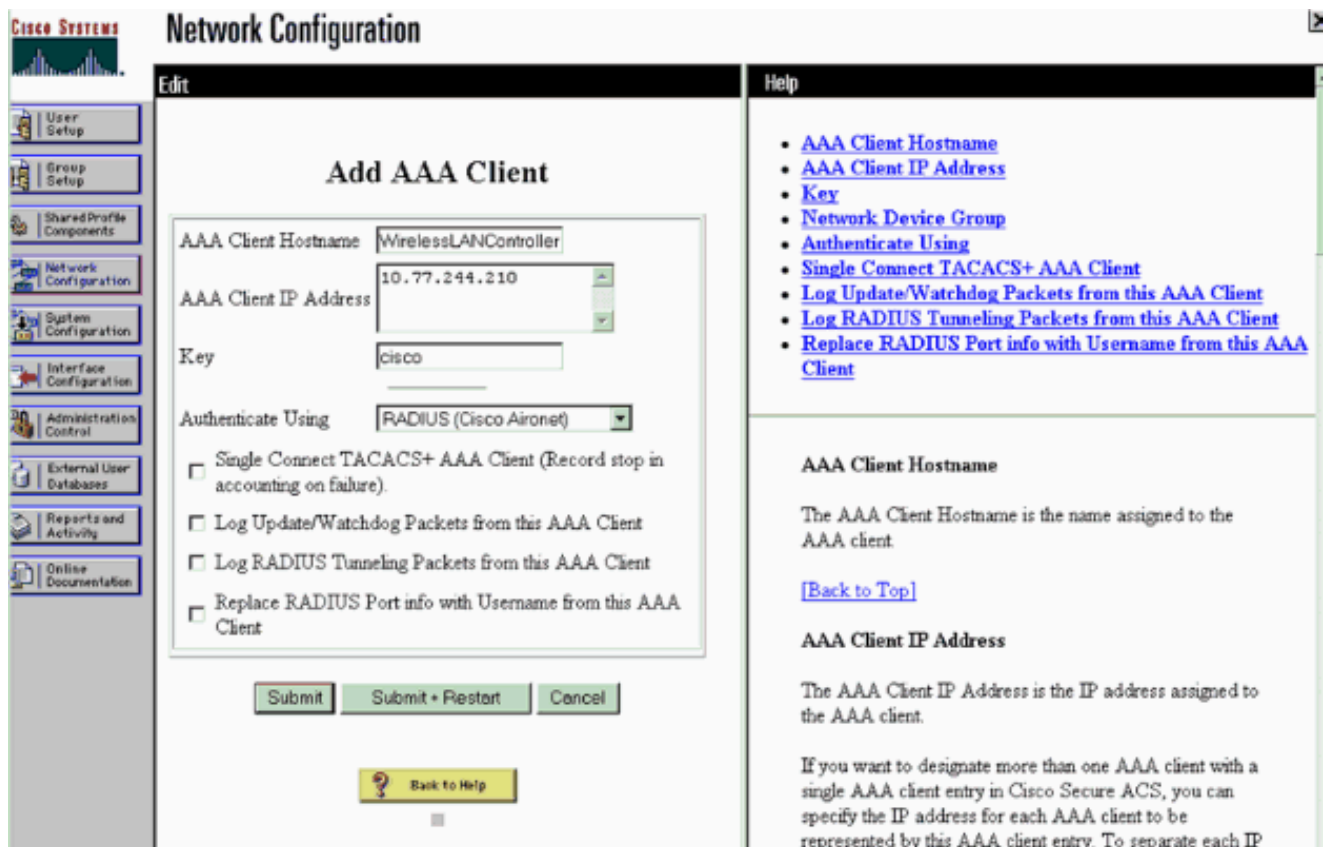
Il passaggio successivo consiste nel configurare il server ACS con gli indirizzi MAC del client.

## Configurazione del server RADIUS con gli indirizzi MAC del client

Per aggiungere un indirizzo MAC ad ACS:

1. Definire il WLC come client AAA sul server ACS. Fare clic su Network Configuration (Configurazione di rete) dall'interfaccia utente di ACS.
2. Quando viene visualizzata la finestra Configurazione di rete, definire il nome del WLC, l'indirizzo IP, il segreto condiviso e il metodo di autenticazione (RADIUS Cisco Aironet o RADIUS Airespace).

Per altri server di autenticazione non ACS, consultare la documentazione del produttore.



The screenshot shows the 'Network Configuration' page in Cisco ACS. The main content area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname: WirelessLANController
- AAA Client IP Address: 10.77.244.210
- Key: cisco
- Authenticate Using: RADIUS (Cisco Aironet)

Below the fields are four checkboxes:

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom of the form are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'. Below these is a 'Back to Help' button.

The right-hand side of the page has a 'Help' section with a list of links:

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

Below the links are two sections of explanatory text:

**AAA Client Hostname**  
The AAA Client Hostname is the name assigned to the AAA client.  
[\[Back to Top\]](#)

**AAA Client IP Address**  
The AAA Client IP Address is the IP address assigned to the AAA client.  
If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP

Aggiungere un client AAA



Nota: la chiave segreta condivisa configurata sul WLC e sul server ACS devono corrispondere. Il segreto condiviso fa distinzione tra maiuscole e minuscole.

3. Dal menu principale di ACS, fare clic su User Setup .
4. Nella casella di testo Utente, immettere l'indirizzo MAC da aggiungere al database utenti.



## User Setup

**Select**

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

User:

List users beginning with letter/number:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9			

**Help**

- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, add users, and delete users in the database.

### User Setup and External User Databases

Before Cisco Secure ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

**Note:** User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the


Immettere l'indirizzo MAC



Nota: l'indirizzo MAC deve essere esattamente uguale a quello inviato dal WLC per il nome utente e la password. Se l'autenticazione ha esito negativo, controllare il log dei tentativi non riusciti per verificare in che modo il WLC segnala l'indirizzo MAC. Non tagliare e incollare l'indirizzo MAC, in quanto ciò può introdurre caratteri fantasma.

5. Nella finestra User Setup, immettere l'indirizzo MAC nella casella di testo Secure-PAP password.

Immettere l'indirizzo MAC nel campo Password Secure-PAP

 **Nota:** l'indirizzo MAC deve essere esattamente uguale a quello inviato dal WLC per il nome utente e la password. Se l'autenticazione ha esito negativo, controllare il log dei tentativi non riusciti per verificare in che modo l'access point riporta il MAC. Non tagliare e incollare l'indirizzo MAC, in quanto ciò può introdurre caratteri fantasma.

6. Fare clic su Invia.

7. Ripetere i passaggi da 2 a 5 per aggiungere altri utenti al database ACS.

Quando i client si connettono a questa WLAN, il WLC passa le credenziali al server ACS. Il server ACS convalida le credenziali rispetto al database ACS. Se l'indirizzo MAC del client è presente nel database, il server RADIUS ACS restituisce al WLC un messaggio di autenticazione riuscito e al client può essere concesso l'accesso alla WLAN.

## Usare la CLI per configurare il filtro MAC sul WLC

In questo documento veniva descritto in precedenza come usare l'interfaccia GUI del WLC per configurare i filtri MAC. È possibile anche usare la CLI per configurare i filtri MAC sul WLC. Per configurare il filtro MAC sul WLC:

- Per abilitare il filtro MAC, usare il comando `config wlan mac-filtering enable wlan_id`. Per verificare che il filtro MAC sia abilitato per la WLAN, immettere il comando `show wlan`.

- config macfilter add, comando:

Il comando config macfilter add consente di aggiungere un macfilter, un'interfaccia, una descrizione e così via.

Usare il comando config macfilter add per creare una voce del filtro MAC sul controller Cisco Wireless LAN. Utilizzare questo comando per aggiungere un client localmente a una LAN wireless sul controller Cisco Wireless LAN. Questo filtro ignora il processo di autenticazione RADIUS.

```
<#root>
```

```
config macfilter add
```

```
<MAC_address> <WLAN_id> <Interface_name> <description> <IP_address>
```

### Esempio

Immettere un mapping statico tra indirizzi MAC e IP. Questa operazione può essere effettuata per supportare un client passivo, ossia un client che non utilizza il protocollo DHCP e non trasmette pacchetti IP non richiesti.

```
<#root>
```

```
(Cisco Controller) >
```

```
config macfilter add
```

```
00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

- config macfilter indirizzo-ip, comando

Il comando config macfilter ip-address consente di mappare un filtro MAC a un indirizzo IP. Utilizzare questo comando per configurare un indirizzo IP nel database del filtro MAC locale:

```
<#root>
```

```
config macfilter ip-address
```

```
<MAC_address> <IP_address>
```

### Esempio

```
<#root>
```

```
(Cisco Controller) >
config macfilter ip-address

00:E0:77:31:A3:55 10.92.125.51
```

## Configurazione di un timeout per i client disabilitati

È possibile configurare un timeout per i client disabilitati. I client che non eseguono l'autenticazione per tre volte durante i tentativi di associazione vengono automaticamente disattivati da ulteriori tentativi di associazione. Alla scadenza del periodo di timeout, il client può riprovare a eseguire l'autenticazione finché non associa o non supera l'autenticazione e viene escluso di nuovo. Immettere il comando `config wlan excluionlist wlan_id timeout` per configurare il timeout per i client disabilitati. Il valore di timeout può essere compreso tra 1 e 65535 secondi oppure è possibile immettere 0 per disabilitare il client in modo permanente.

## Verifica

Per verificare se il filtro MAC è configurato correttamente:

- `show macfilter summary`: visualizza un riepilogo di tutte le voci di filtro MAC.
- `show macfilter detail < indirizzo MAC client >`: visualizzazione dettagliata di una voce di filtro MAC.

Di seguito è riportato un esempio del comando `show macfilter summary`:

```
<#root>
```

```
(Cisco Controller) >
show macfilter summary
```

```
MAC Filter RADIUS Compatibility mode..... Cisco ACS
MAC Filter Delimiter..... None
```

```
Local Mac Filter Table
```

MAC Address	WLAN Id	Description
00:40:96:ac:e6:57	1	Guest

```
(Cisco Controller) >
```

Di seguito è riportato un esempio del comando `show macfilter detail`:

<#root>

(Cisco Controller) >


```
show macfilter detail 00:40:96:ac:e6:57
```

```
MAC Address..... 00:40:96:ac:e6:57
WLAN Identifier..... 1
Interface Name..... mac-client
Description..... Guest
```

## Risoluzione dei problemi

Per risolvere i problemi relativi alla configurazione, è possibile utilizzare i seguenti comandi:

---

 Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

---

- debug aaa all enable: fornisce il debug di tutti i messaggi AAA.
- debug mac addr <Client-MAC-address xx:xx:xx:xx:xx:xx>: per configurare il debug MAC, usare il comando debug maccommand.

Di seguito è riportato un esempio del comando debug aaa all enable:

<#root>

```
Wed May 23 11:13:55 2007:
Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007:
User 004096ace657 authenticated
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57
Returning AAA Error 'Success' (0)
                        for mobile 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: AuthorizationResponse: 0xbadff97c
Wed May 23 11:13:55 2007:     structureSize.....76
Wed May 23 11:13:55 2007:     resultCode.....0
Wed May 23 11:13:55 2007:     protocolUsed.....0x00000008
Wed May 23 11:13:55 2007:     proxyState.....
                        00:40:96:AC:E6:57-00:00
Wed May 23 11:13:55 2007:     Packet contains 2 AVPs:
Wed May 23 11:13:55 2007:         AVP[01] Service-Type.....
                        0x0000000a (10) (4 bytes)
Wed May 23 11:13:55 2007:         AVP[02] Airespace / Interface-Name.....
                        staff-vlan (10 bytes)
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[0]: attribute 6
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[1]: attribute 5
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Applying new AAA override for
                        station 00:40:96:ac:e6:57
```

```
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
source: 2, valid bits: 0x200 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC:
-1, rTimeBurstC: -1 vlanIfName: 'mac-client'
```

Quando un client wireless non è presente nel database degli indirizzi MAC sul WLC (database locale) o sul server RADIUS cerca di associarsi alla WLAN, il client può essere escluso. Di seguito è riportato un esempio del comando debug aaa all enable per un'autenticazione MAC non riuscita:

<#root>

```
Wed May 23 11:05:06 2007:
Unable to find requested user entry for 004096ace657

Wed May 23 11:05:06 2007: AuthenticationRequest: 0xa620e50
Wed May 23 11:05:06 2007: Callback.....0x807e724
Wed May 23 11:05:06 2007: protocolType.....0x00000001
Wed May 23 11:05:06 2007: proxyState.....
00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 14 AVPs (not shown)
Wed May 23 11:05:06 2007: 00:40:96:ac:e6:57

Returning AAA Error 'No Server' (-7)
for mobile 00:40:96:ac:e6:57

Wed May 23 11:05:06 2007: AuthorizationResponse: 0xbadff7e4
Wed May 23 11:05:06 2007: structureSize.....28
Wed May 23 11:05:06 2007: resultCode.....-7
Wed May 23 11:05:06 2007: protocolUsed.....0xffffffff
Wed May 23 11:05:06 2007: proxyState.....
00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 0 AVPs:
```

Errore: i client wireless che tentano di eseguire l'autenticazione tramite l'indirizzo MAC vengono rifiutati. Il rapporto Autenticazione non riuscita mostra errori interni

Quando si utilizza ACS 4.1 su un server Microsoft Windows 2003 Enterprise, i client che tentano di eseguire l'autenticazione tramite l'indirizzo MAC vengono rifiutati. Questo si verifica quando un client AAA invia il valore dell'attributo Service-Type=10 al server AAA. a causa dell'ID bug Cisco [CSCsh62641](#). I client AAA interessati da questo bug includono WLC e switch che usano MAC Authentication Bypass.

Le soluzioni sono:

- Effettuare il downgrade ad ACS 4.0.
- o
- Aggiungere gli indirizzi MAC da autenticare a Protezione accesso alla rete nella tabella degli indirizzi MAC del database ACS interno.



Errore: impossibile aggiungere un filtro MAC con l'interfaccia utente grafica del WLC

La causa può essere un ID bug Cisco [CSCsj98722](#). Il bug è stato risolto nella versione 4.2 del codice. Se si eseguono versioni precedenti alla 4.2, è possibile aggiornare il firmware alla 4.2 o utilizzare queste due soluzioni per risolvere il problema.

- Usare la CLI per configurare il filtro MAC con questo comando:

```
<#root>  
  
config macfilter add  
  
  <MAC_address> <WLAN_id> <Interface_name>
```

- Dalla GUI Web del controller, selezionare Any WLAN (Qualsiasi WLAN) nella scheda Security (Sicurezza), quindi immettere l'indirizzo MAC da filtrare.

Errore: client invisibile all'utente non in stato di esecuzione

Se DHCP richiesto non è configurato sul controller, i punti di accesso apprenderanno l'indirizzo IP dei client wireless quando questi invieranno il primo pacchetto IP o ARP. Se i client wireless sono dispositivi passivi, ad esempio dispositivi che non avviano una comunicazione, gli access point non saranno in grado di conoscere l'indirizzo IP dei dispositivi wireless. Di conseguenza, il controller attende dieci secondi prima che il client invii un pacchetto IP. Se il pacchetto non risponde dal client, il controller scarta qualsiasi pacchetto ai client wireless passivi. Questo problema è documentato nell'ID bug Cisco [CSCsq46427](#).



Nota: solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interni.

---

Come soluzione consigliata per dispositivi passivi quali stampanti, pompe PLC wireless e così via, è necessario impostare la WLAN per il filtro MAC e controllare l'override dell'AAA per consentire il collegamento di questi dispositivi.

È possibile creare un filtro indirizzi MAC sul controller che mappa l'indirizzo MAC del dispositivo wireless a un indirizzo IP.



Nota: è necessario abilitare il filtro degli indirizzi MAC nella configurazione WLAN per la sicurezza di layer 2. Inoltre, è necessario che l'opzione `Allow AAA Override` sia abilitata nelle impostazioni avanzate della configurazione WLAN.

---

Dalla CLI, immettere questo comando per creare il filtro indirizzi MAC:

```
config macfilter add <STA MAC addr> <WLAN_id> <Interface_name> <description> <STA IP address>
```

Di seguito è riportato un esempio:

```
<#root>
```

```
(Cisco Controller) >
```

```
config macfilter add 00:01:02:03:04:05 1 my_interface "Zebra Printer" 192.168.1.1
```

## Informazioni correlate

- [Esempio di configurazione di ACL sui Wireless LAN Controller](#)
- [Esempi di configurazione dell'autenticazione sui controller LAN wireless](#)
- [Esempio di configurazione delle VLAN nei Wireless LAN Controller](#)
- [Guida alla configurazione di Cisco Wireless LAN Controller, avviso di ritiro versione 4.1](#)
- [Pagina di supporto per la tecnologia wireless](#)
- [Supporto tecnico Cisco e download](#)

## 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).