

# Configurazione dell'autenticazione Web centrale con ancoraggio su Catalyst 9800

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione di un Catalyst 9800 ancorato a un altro Catalyst 9800](#)

[Esempio di rete](#)

[Configurazione del server AAA su entrambi gli switch 9800](#)

[Configurazione delle WLAN sui WLC](#)

[Crea il profilo criteri e il tag criteri sul WLC esterno](#)

[Crea il profilo dei criteri nel WLC di ancoraggio](#)

[Reindirizza configurazione ACL su entrambi gli switch 9800](#)

[Configurare ISE](#)

[Configurazione di Catalyst 9800 ancorato a un WLC AireOS](#)

[Catalyst 9800 Configurazione esterna](#)

[Configurazioni AAA sull'ancoraggio AireOS WLC](#)

[Configurazione WLAN sul WLC di AireOS](#)

[Reindirizzamento dell'ACL sul WLC di AireOS](#)

[Configurare ISE](#)

[Differenze nella configurazione quando il WLC di AireOS è il dispositivo esterno e Catalyst 9800 è l'ancoraggio](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni sulla risoluzione dei problemi di Catalyst 9800](#)

[Dettagli client](#)

[Embedded Packet Capture](#)

[Tracce RadioActive](#)

[Informazioni sulla risoluzione dei problemi AireOS](#)

[Dettagli client](#)

[Debug dalla CLI](#)

[Riferimenti](#)

## Introduzione

In questo documento viene descritto come configurare e risolvere i problemi di un'autenticazione Web centrale (CWA) su Catalyst 9800 che punta a un altro controller WLC (Wireless LAN Controller) come ancoraggio per la mobilità, includendo la destinazione con AireOS o un altro WLC 9800.

# Prerequisiti

## Requisiti

Si consiglia di avere una conoscenza di base del WLC 9800, del WLC di AireOS e di Cisco ISE. Si presume che, prima di avviare la configurazione di ancoraggio di CWA, sia già stato aperto il tunnel di mobilità tra i due WLC. Non è compreso nell'ambito di questo esempio di configurazione. Per assistenza, consultare il documento "[Creazione di tunnel per la mobilità sui controller Catalyst 9800](#)"

## Componenti usati

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.

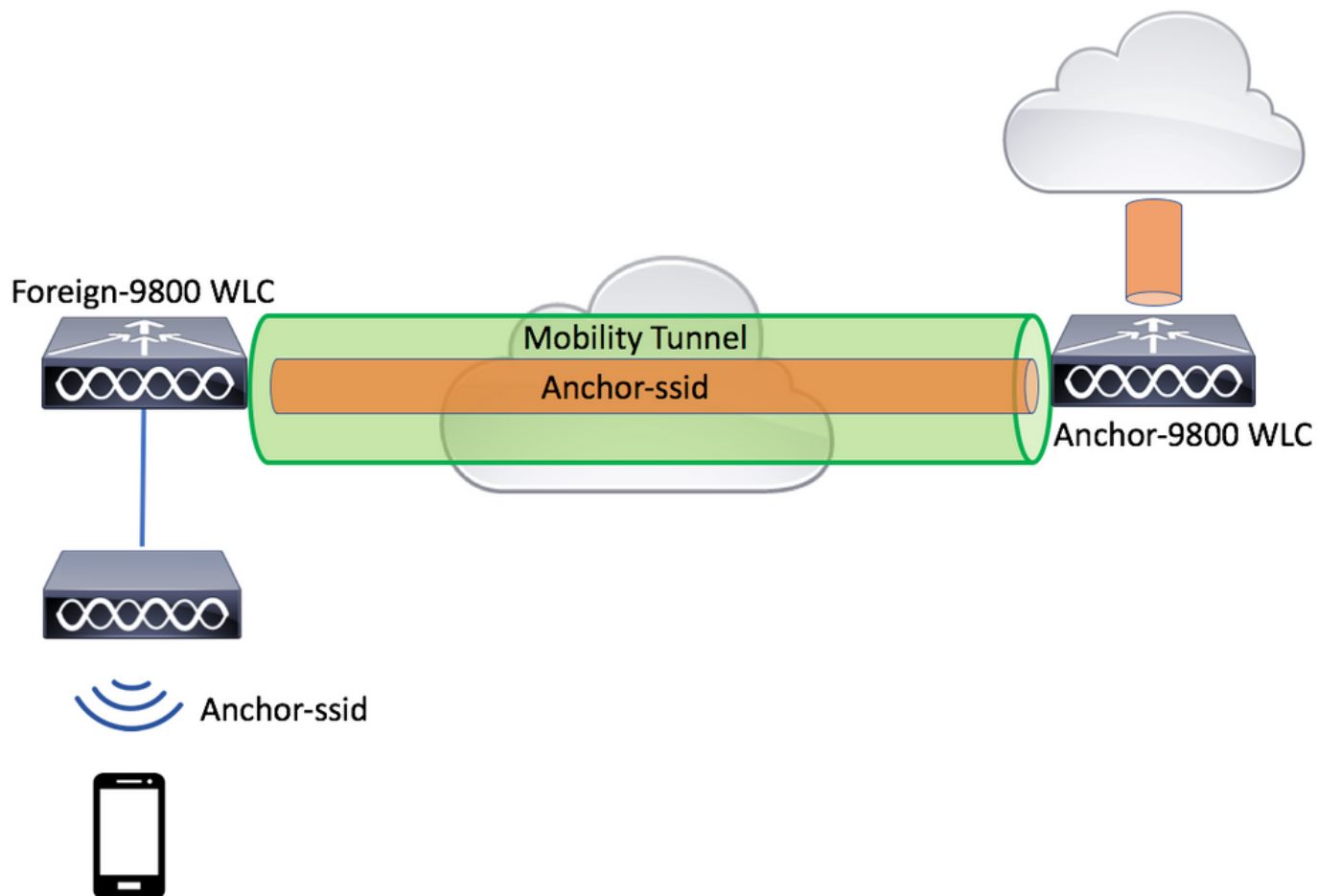
9800 17.2.1

Immagine 5520 8.5.164 IRCM

ISE 2.4

## Configurazione di un Catalyst 9800 ancorato a un altro Catalyst 9800

### Esempio di rete



## Configurazione del server AAA su entrambi gli switch 9800

Sia sull'ancora che sull'esterno è necessario aggiungere il server RADIUS e verificare che CoA sia abilitato. Questa operazione può essere eseguita nel menu `Configurazione>Sicurezza>AAA>Server/Gruppi>Server>` fare clic sul pulsante **Aggiungi**

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Welcome admin  
Last login Fri, May 15 2020 16:56:51 ...

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

+ Add

RADIUS

Servers

Server Groups

TACACS+

LDAP

Name Address Auth Port

### Create AAA Radius Server

Name\* CLUS-Server

Server Address\* X.X.X.X

PAC Key

Key Type Clear Text

Key\* .....

Confirm Key\* .....

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA **ENABLED**

Cancel Apply to Device

È ora necessario creare un gruppo di server e inserire in tale gruppo il server appena configurato. A tale scopo, selezionare **Configuration>Security>AAA>Servers/Groups>Server Groups>+Add**.

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add X Delete

RADIUS Servers Server Groups

TACACS+

LDAP

Create AAA Radius Server Group

Name\* CLUS-Server-Group

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 1-1440

Available Servers Assigned Servers

CLUS-Server

Cancel Apply to Device

Creare un elenco di metodi di **autorizzazione** (non è necessario un elenco di metodi di autenticazione per CWA) in cui il tipo è rete e il tipo di gruppo è gruppo. Aggiunge il gruppo di server dall'azione precedente all'elenco dei metodi.

Questa configurazione viene eseguita qui **Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is **Configuration > Security > AAA**. The main menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The current view is **AAA Method List** under the **Authorization** tab. A **+ Add** button is visible. The **Quick Setup: AAA Authorization** dialog box is open, showing the following configuration:

- Method List Name\*: CLUS-AuthZ-Meth-List
- Type\*: network
- Group Type: group
- Fallback to local:
- Authenticated:
- Available Server Groups: radius, ldap, tacacs+, ISE1
- Assigned Server Groups: CLUS-Server-Group

Buttons for **Cancel** and **Apply to Device** are at the bottom of the dialog.

(Facoltativo) Creare un elenco di metodi di accounting utilizzando lo stesso gruppo di server dell'elenco dei metodi di autorizzazione. È possibile creare l'elenco di accounting qui **Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation at the top reads "Configuration > Security > AAA". The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled "AAA Method List" and includes tabs for "Servers / Groups", "AAA Method List", and "AAA Advanced". Under the "AAA Method List" tab, there are sections for "Authentication", "Authorization", and "Accounting". The "Accounting" section is active, showing a "+ Add" button and a "- Delete" button. Below these is a table with columns for "Name", "Type", and "Group1". A "Quick Setup: AAA Accounting" dialog box is open, showing the following configuration: "Method List Name\*" is "CLUS-Acct-Meth-List"; "Type\*" is "identity"; "Available Server Groups" includes "radius", "ldap", "tacacs+", and "ISE1"; "Assigned Server Groups" includes "CLUS-Server-Group". At the bottom of the dialog are "Cancel" and "Apply to Device" buttons.

## Configurazione delle WLAN sui WLC

Creare e configurare le WLAN su entrambi i WLC. Le WLAN devono corrispondere su entrambi. Il tipo di protezione deve essere filtro MAC e deve essere applicato l'elenco dei metodi di autorizzazione del passaggio precedente. Questa configurazione viene eseguita in **Configurazione>Tag e profili>WLAN>+Aggiungi**

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
--------------------------	--------	------	----

Add WLAN

General Security Advanced

Profile Name\* CLUS-WLAN-Name

SSID\* CLUS-SSID

WLAN ID\* 2

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED

Cancel Apply to Device

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
--------------------------	--------	------	----

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None

MAC Filtering

OWE Transition Mode

Authorization List\* CLUS-AuthZ-Meth-l

Lobby Admin Access

Fast Transition Adaptive Enab...

Over the DS

Reassociation Timeout 20

Cancel Apply to Device

Crea il profilo criteri e il tag criteri sul WLC esterno



Passare all'interfaccia utente Web WLC esterna.

Per creare il profilo del criterio, passare a **Configurazione>Tag e profili>Criterio>+Aggiungi**

Quando si effettua l'ancoraggio, è necessario utilizzare la commutazione centrale.

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is **Configuration > Tags & Profiles > Policy**. The **+ Add** button is highlighted. The **Add Policy Profile** dialog box is open, showing the **General** tab. A warning message states: "Configuring in enabled state will result in loss of connectivity for clients associated with this profile." The **Name\*** field is set to "CLUS-Policy-Profile" and the **Description** is "Policy Profile for CLUS". The **Status** is set to **ENABLED**. The **WLAN Switching Policy** section has **Central Switching**, **Central Authentication**, **Central DHCP**, and **Central Association** all set to **ENABLED**. The **CTS Policy** section has **Inline Tagging** and **SGACL Enforcement** set to **DISABLED**, and the **Default SGT** is "2-65519". The **Flex NAT/PAT** is set to **DISABLED**. The **Apply to Device** button is visible at the bottom right.

Nella scheda "Avanzate", l'override AAA e il NAC RADIUS sono obbligatori per CWA. In questa finestra è inoltre possibile applicare l'elenco dei metodi contabili se si è scelto di crearne uno.

Configuration > Tags & Profiles > Policy

+ Add    × Delete

Status    Policy Profile Name    Description

### Add Policy Profile

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

**WLAN Timeout**

Session Timeout (sec)    1800

Idle Timeout (sec)    300

Idle Threshold (bytes)    0

Client Exclusion Timeout (sec)     60

Guest LAN Session Timeout   

**DHCP**

IPv4 DHCP Required   

DHCP Server IP Address   

Show more >>>

**AAA Policy**

Allow AAA Override   

NAC State   

NAC Type    RADIUS

Policy Name    default-aaa-policy

Accounting List    CLUS-Acct-Meth-

Fabric Profile     Search or Select

mDNS Service Policy    Search or Select

Hotspot Server    Search or Select

**User Private Network**

Status   

Drop Unicast   

**Umbrella**

Umbrella Parameter Map    Not Configured    Clear

Flex DHCP Option for DNS    **ENABLED**

DNS Traffic Redirect    **IGNORE**

**WLAN Flex Policy**

VLAN Central Switching   

Split MAC ACL    Search or Select

**Air Time Fairness Policies**

2.4 GHz Policy    Search or Select

Nella scheda "Mobilità" **NON** selezionare la casella di controllo "esporta ancoraggio", ma aggiungere il WLC all'elenco degli ancoraggi. Assicurarsi di selezionare "Apply to Device" (Applica al dispositivo). Come promemoria, si presume che tra i due controller sia già stato configurato un tunnel per la mobilità

Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > Policy

+ Add    × Delete

Status    Policy Profile Name    Description

### Add Policy Profile

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

**Mobility Anchors**

Export Anchor   

Static IP Mobility    **DISABLED**

Adding Mobility Anchors will cause the enabled VLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

**Available (0)**

Anchor IP    No anchors available

**Selected (1)**

Anchor IP	Anchor Priority
192.168.160.18	Primary (1)

Cancel    Apply to Device

Affinché gli access point possano utilizzare questo profilo, è necessario creare un tag di criterio e

applicarlo agli access point che si desidera utilizzare.

Per creare il tag di criterio, passare a **Configurazione>Tag e profili>Tag?Criterio>+Aggiungi**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation at the top reads "Configuration > Tags & Profiles > Tags". The "Policy" tab is selected, and the "+ Add" button is highlighted. A modal dialog titled "Add Policy Tag" is open, showing the following fields and actions:

- Name\***: CLUS-Policy-Tag
- Description**: Policy Tag for CLUS
- WLAN-POLICY Maps: 0** (expanded)
- + Add** and **× Delete** buttons
- WLAN Profile** dropdown: CLUS-WLAN-Name
- Policy Profile** dropdown: CLUS-Policy-Profile
- Map WLAN and Policy** section with "WLAN Profile\*" and "Policy Profile\*" dropdowns, both set to the selected values.
- ×** and **✓** buttons for the mapping.
- RLAN-POLICY Maps: 0** (collapsed)
- Cancel** and **Apply to Device** buttons at the bottom.

Per aggiungere questo valore a più access point contemporaneamente, selezionare **Configurazione>Installazione wireless>Avanzate>Avvia ora**. Fare clic sulle barre dei punti elenco accanto a "Tag AP" e aggiungere il tag agli AP selezionati.

Configuration > Wireless Setup > Advanced

+ Tag APs

Number of APs: 3  
Selected Number of APs: 3

AP Name	AP Model	AP MAC	AP Mode
<input checked="" type="checkbox"/> Jays2800	AIR-AP2802I-B-K9	002a.10f3.6b60	Local
<input checked="" type="checkbox"/> Jays3800	AIR-AP3802I-B-K9	70b3.1755.0520	Local
<input checked="" type="checkbox"/> AP0062.ec20.122c	AIR-CAP2702I-B-K9	cc16.7e6c.3cf0	Local

1 10 items per page

Tag APs

Tags

Policy:

Site:

RF:

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel Apply to Device

## Crea il profilo dei criteri nel WLC di ancoraggio

Andare all'interfaccia utente Web WLC di ancoraggio. Aggiungere il Profilo criterio sull'ancoraggio 9800 in **Configurazione>Tag e profili>Tag>Criterio>+Aggiungi**. Accertarsi che corrisponda al Profilo criteri effettuato sull'esterno, ad eccezione della scheda Mobilità e dell'elenco di contabilità.

Qui non aggiungete un ancoraggio ma selezionate la casella di controllo "Esporta ancoraggio". Non aggiungere qui l'elenco di accounting. Come promemoria, si presume che tra i due controller sia già stato configurato un tunnel per la mobilità

**Nota:** Non c'è motivo di associare questo profilo a una WLAN in un tag di criterio. In tal caso si creeranno problemi. Se si desidera utilizzare la stessa WLAN per gli access point su questo WLC, creare un altro profilo dei criteri per tale WLC.

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > Policy

+ Add - Delete

### Add Policy Profile

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

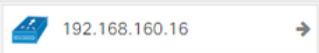
**Mobility Anchors**

Export Anchor

Static IP Mobility  DISABLED

*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (0)	
Anchor IP	Anchor IP	Anchor Priority
 192.168.160.16 →	Anchors not assigned	

Cancel Apply to Device

## Reindirizza configurazione ACL su entrambi gli switch 9800

Quindi, è necessario creare la configurazione dell'ACL di reindirizzamento su entrambi gli switch 9800. Le voci sull'indirizzo esterno non hanno importanza in quanto sarà il WLC di ancoraggio ad applicare l'ACL al traffico. L'unico requisito è che ci sia e che ci sia qualche entrata. Le voci sull'ancora devono "negare" l'accesso ad ISE sulla porta 8443 e "permettere" tutto il resto. Questo ACL viene applicato solo al traffico in entrata dal client, quindi non sono necessarie regole per il traffico di ritorno. DHCP e DNS possono passare senza voci nell'ACL.

Cisco Catalyst 9800-L Wireless Controller 17.2.1 Welcome admin  
Last login None

Configuration > Security > ACL

+ Add    × Delete    Associate Interfaces

### Add ACL Setup

ACL Name\*     ACL Type

Rules

Sequence\*     Action

Source Type

Destination Type

Protocol

Log     DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		192.168.160.99		tcp	None	eq 8443	None	Disabled
<input type="checkbox"/> 100	permit	any		any		ip	None	None	None	Disabled

10 items per page    1 - 2 of 2 items

Cancel    Apply to Device

## Configurare ISE

L'ultimo passaggio consiste nel configurare ISE per CWA. Le opzioni disponibili sono numerose, ma in questo esempio verranno mantenute le nozioni di base e verrà utilizzato il portale guest predefinito con registrazione automatica.

Ad ISE, è necessario creare un profilo di autorizzazione, un set di criteri con un criterio di autenticazione e un criterio di autorizzazione che utilizzi il profilo di autorizzazione, aggiungere lo switch 9800 (esterno) ad ISE come dispositivo di rete, quindi creare un nome utente e una password per accedere alla rete.

Per creare il profilo di autorizzazione, passare a **Criteri>Elementi dei criteri>Autorizzazione>Risultati>Profili di autorizzazione**, quindi fare clic su **Aggiungi**. Verificare che il tipo di accesso restituito sia "access\_accept", quindi impostare gli AVP (coppie attributo-valore) che si desidera inviare. Per CWA, l'ACL di reindirizzamento e l'URL di reindirizzamento sono obbligatori, ma è possibile anche inviare indietro elementi come l'ID VLAN e il timeout della sessione. È importante che il nome dell'ACL corrisponda al nome dell'ACL di reindirizzamento sull'host esterno e sull'host 9800.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > test

Authorization Profile

\* Name CLUS-AuthZ-Profile-ISE

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth ACL CLUS-ACL Value Self-Registered Guest Portal

È quindi necessario configurare un modo per applicare il profilo di autorizzazione appena creato ai clienti che utilizzano CWA. Per ottenere questo risultato, è possibile creare un set di criteri che ignori l'autenticazione quando si utilizza MAB e applichi il profilo di autorizzazione quando si utilizza il SSID inviato nell'ID stazione chiamato. Di nuovo, ci sono molti modi per farlo quindi se avete bisogno di qualcosa di più specifico o più sicuro, che bene, questo è solo il modo più semplice di farlo.

Per creare il set di criteri, selezionare **Policy>Set di criteri** e fare clic sul pulsante + sul lato sinistro della schermata. Assegnare un nome al nuovo set di criteri e assicurarsi che sia impostato su "accesso di rete predefinito" o su qualsiasi elenco di protocolli consentiti che consenta "Ricerca host processo" per MAB. Per controllare l'elenco di protocolli consentiti, selezionare Criteri>Elementi dei criteri>Risultati>Autenticazione>Protocolli consentiti. Fare clic sul segno + all'interno del nuovo set di criteri creato.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

License Warning

Click here to do visibility setup Do not show this again.

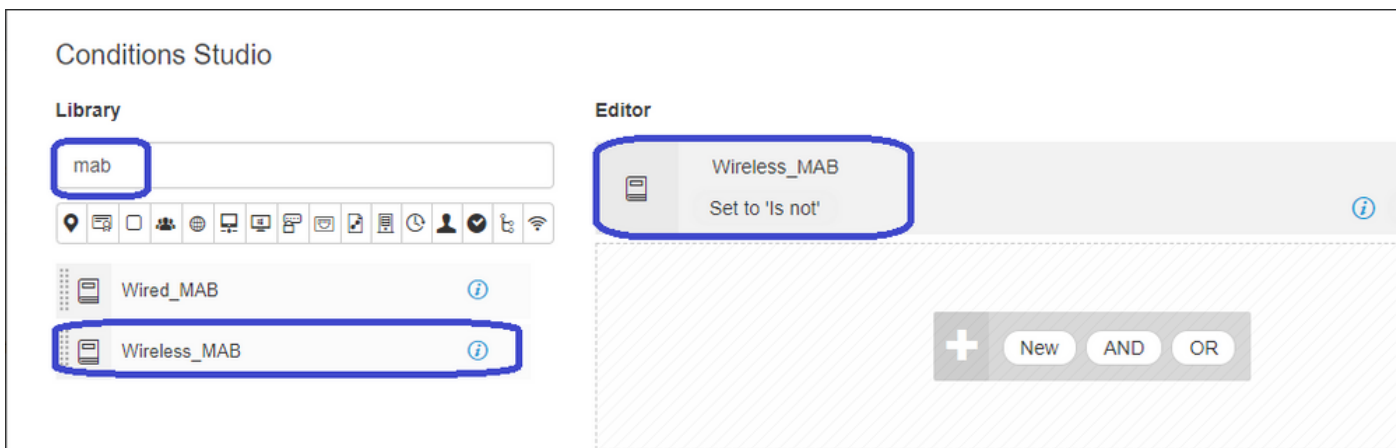
ResetAll Hitcounts Reset Save

Policy Sets

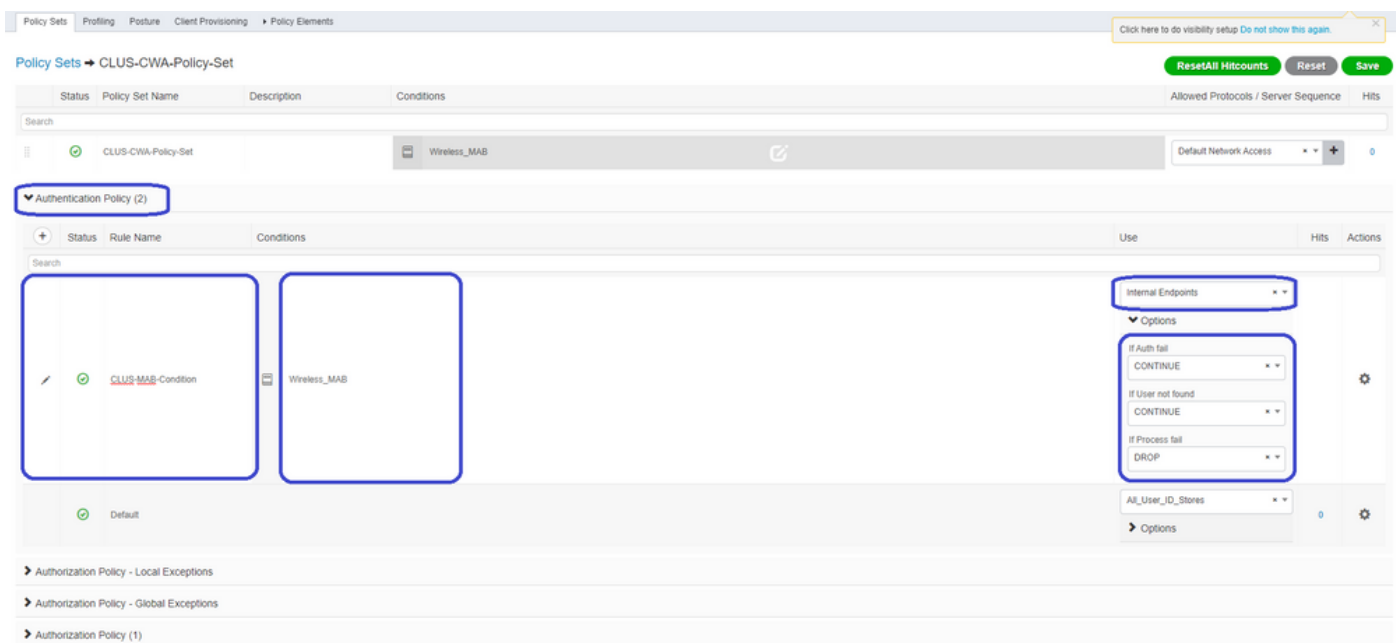
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	CLUS-AuthZ-Policy-Set			Default Network Access			
+	Default	Default policy set		Default Network Access	0		

Reset Save

Per questo set di criteri ogni volta che MAB viene utilizzato in ISE passerà attraverso questo set di criteri. In seguito sarà possibile creare criteri di autorizzazione corrispondenti all'ID della stazione chiamata in modo da poter applicare risultati diversi a seconda della WLAN in uso. Questo processo è molto personalizzabile con molte cose su cui potete fare corrispondenza.



All'interno del set di regole, creare le regole. I criteri di autenticazione possono corrispondere nuovamente in MAB, ma è necessario modificare l'archivio ID per utilizzare gli endpoint interni ed è necessario modificare le opzioni per continuare l'autenticazione non riuscita e l'utente non trovato.



Una volta impostato il criterio di autenticazione, è necessario creare due regole nel criterio di autorizzazione. Questo criterio è simile a un ACL, quindi l'ordine deve avere la regola di post-autenticazione in primo piano e la regola di pre-autenticazione in secondo piano. La regola di post-autenticazione corrisponderà agli utenti che hanno già eseguito il flusso guest. Questo per dire che se hanno già firmato, andranno incontro a quella regola e si fermeranno lì. Se non hanno effettuato l'accesso, continueranno a scorrere l'elenco e raggiungeranno la regola di preautenticazione per ottenere il reindirizzamento. È consigliabile far corrispondere le regole dei criteri di autorizzazione con l'ID stazione chiamato che termina con l'SSID in modo che venga rilevato solo per le WLAN configurate a tale scopo.



Policy Sets → CLUS-CWA-Policy-Set Reset All Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

Authentication Policy (2)  
 Authorization Policy - Local Exceptions  
 Authorization Policy - Global Exceptions  
 Authorization Policy (4)

Status	Rule Name	Conditions	Results	Security Groups
✓	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth	Select from list
✓	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE	Select from list
✓	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA	Select from list
✓	Default		DenyAccess	Select from list

Ora che la policy è stata configurata, è necessario comunicare ad ISE le informazioni relative allo switch 9800 (esterno) in modo che ISE possa considerarlo un autenticatore. A tale scopo, selezionare **Admin>Network Resources>Network Device>+**. È necessario denominarlo, impostare l'indirizzo IP (o in questo caso l'intera subnet di amministrazione), abilitare RADIUS e impostare il segreto condiviso. Il segreto condiviso su ISE deve corrispondere al segreto condiviso su 9800 altrimenti questo processo non riuscirà. Dopo aver aggiunto la configurazione, fare clic sul pulsante di invio per salvarla.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device  
Device Security Settings

Network Devices List > JaysNet

Network Devices

\* Name: CLUS\_Net-Device

Description: [ ]

IP Address: \* IP: 192.168.160.0 / 24

\* Device Profile: Cisco

Model Name: [ ]  
Software Version: [ ]

\* Network Device Group

Location: All Locations [Set To Default]  
 IPSEC: No [Set To Default]  
 Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: [ ] [Show]

Use Second Shared Secret:  [ ] [Show]

CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings [ ]

Infine, è necessario aggiungere il nome utente e la password che il client immetterà nella pagina

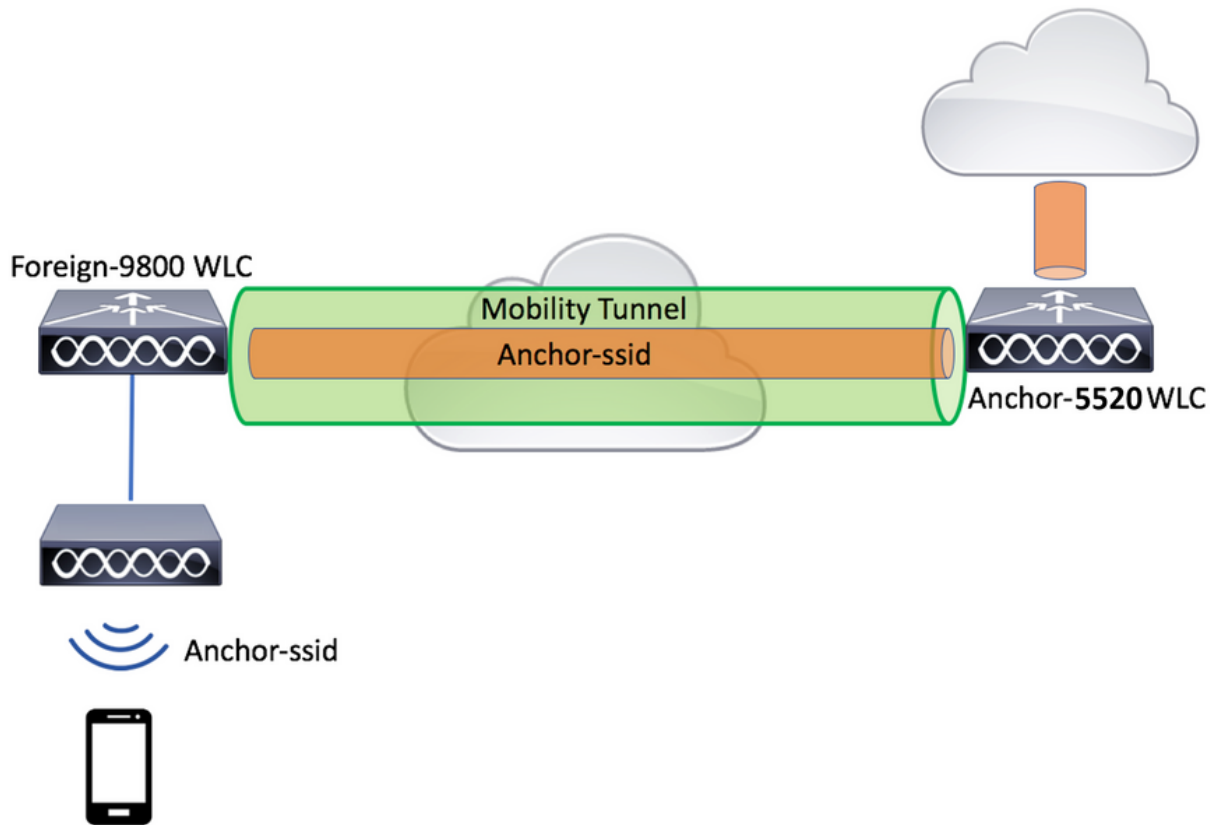
di login per verificare che abbia accesso alla rete. Questa operazione viene eseguita in **Amministrazione>Gestione delle identità>Identità>Utenti>+Aggiungi** e accertarsi di fare clic su Invia dopo averlo aggiunto. Come tutte le altre soluzioni ISE, anche questa è personalizzabile e non deve essere un utente memorizzato localmente, ma è la configurazione più semplice.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Identity Management' section is expanded to show 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Identities' section is further expanded to show 'Users'. The main content area is titled 'Network Access Users List > New Network Access User'. The form contains the following sections:

- Network Access User:** \* Name (CLUS-User), Status (Enabled), Email.
- Passwords:** Password Type (Internal Users), \* Login Password (\*\*\*\*\*), Re-Enter Password (\*\*\*\*\*), Enable Password.
- User Information:** First Name, Last Name.
- Account Options:** Description, Change password on next login (checkbox).
- Account Disable Policy:** Disable account if date exceeds (2020-07-17) (yyyy-mm-dd).
- User Groups:** Select an item (dropdown menu).

The 'Submit' button is highlighted with a red box.

## Configurazione di Catalyst 9800 ancorato a un WLC AireOS



## Catalyst 9800 Configurazione esterna

Seguire la stessa procedura descritta in precedenza, ignorando la sezione "Creazione del profilo dei criteri sul WLC di ancoraggio".

## Configurazioni AAA sull'ancoraggio AireOS WLC

Aggiungere il server al WLC scegliendo **Security>AAA>RADIUS>Authentication>New** (Sicurezza>RADIUS>Autenticazione>Nuovo). Aggiungere l'indirizzo IP del server, il segreto condiviso e il supporto per CoA.

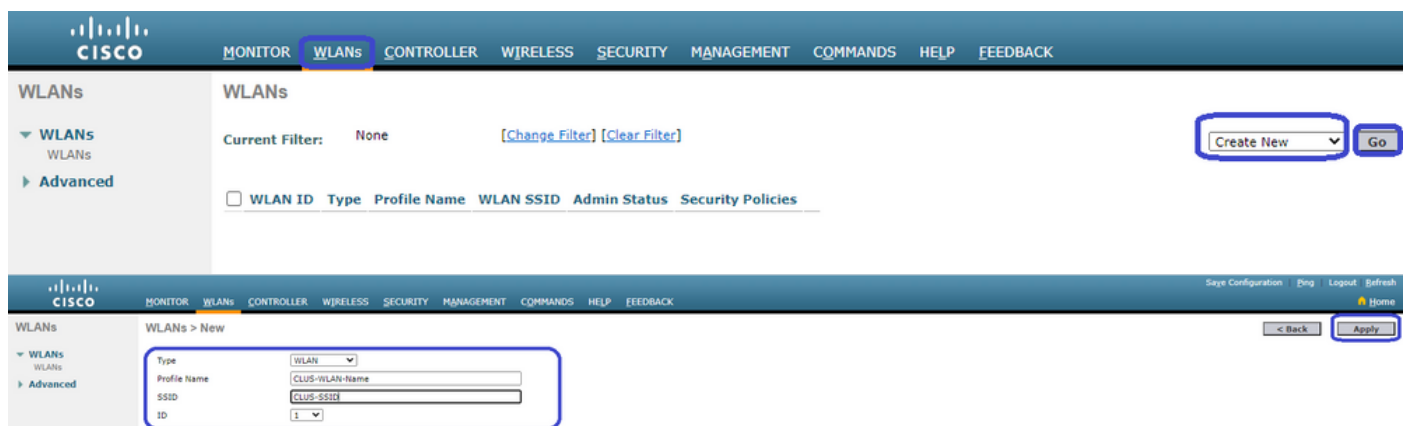
The top screenshot shows the 'RADIUS Authentication Servers' configuration page. The 'Auth Called Station ID Type' is set to 'AP MAC Address:SSID'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen' and the 'Framed MTU' is set to '1300'. Below these fields is a table with columns: Network User, Management, Tunnel Proxy, Server Index, Server Address(Ipv4/Ipv6), Port, IPSec, and Admin Status.

The bottom screenshot shows the 'RADIUS Authentication Servers > New' configuration page. The 'Server Index' is set to '1'. The 'Server IP Address(Ipv4/Ipv6)' is '192.168.160.99'. The 'Shared Secret Format' is 'ASCII'. The 'Shared Secret' and 'Confirm Shared Secret' fields are masked with asterisks. The 'Apply Cisco ISE Default settings' checkbox is checked. The 'Key Wrap' checkbox is unchecked. The 'Port Number' is '1812'. The 'Server Status' is 'Enabled'. The 'Support for CoA' is 'Enabled'. The 'Server Timeout' is '5 seconds'. The 'Network User' and 'Management' checkboxes are checked. The 'Management Retransmit Timeout' is '5 seconds'. The 'Tunnel Proxy', 'PAC Provisioning', and 'IPsec' checkboxes are unchecked.

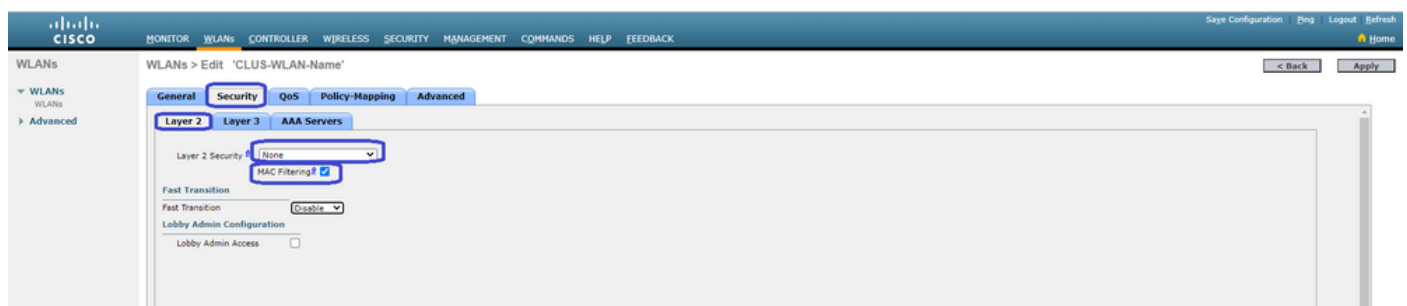
# Configurazione WLAN sul WLC di AireOS

Per creare la WLAN, selezionare **WLAN>Crea nuovo>Vai**.

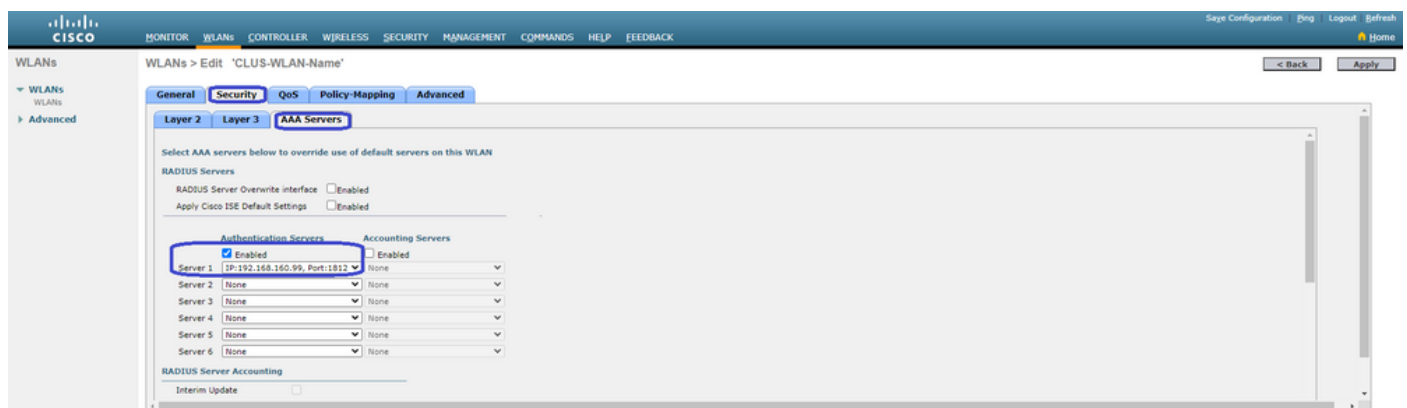
Configurare il nome del profilo, l'ID WLAN e l'SSID, quindi fare clic su "Apply" (Applica).



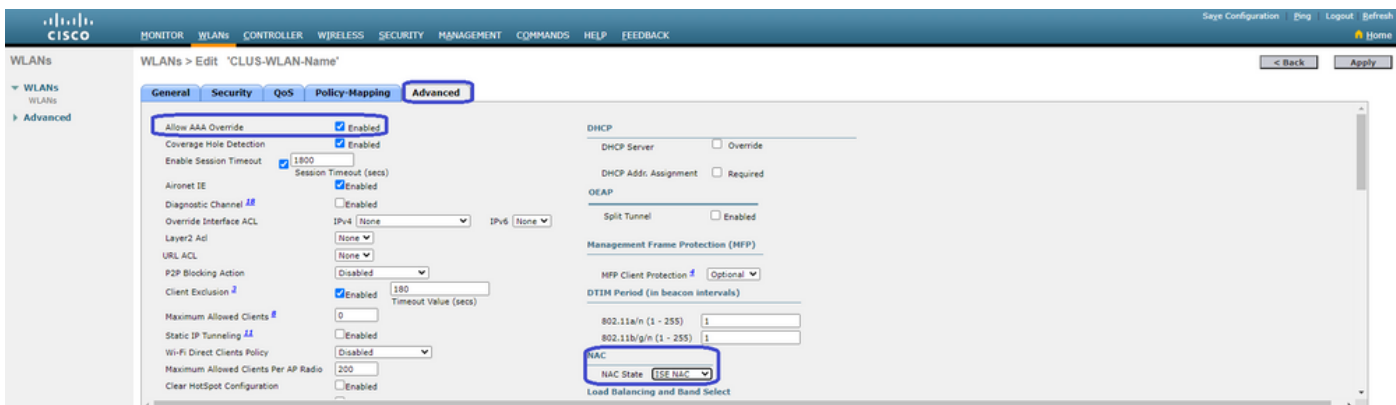
Viene visualizzata la configurazione WLAN. Nella scheda "Generale" è possibile aggiungere l'interfaccia che si desidera venga utilizzata dai client se non si intende configurare ISE per l'invio negli AVP. Quindi, andare alla scheda **Sicurezza>Layer2** e verificare che la configurazione di "Sicurezza Layer 2" utilizzata sul 9800 corrisponda a quella di "Filtro MAC".



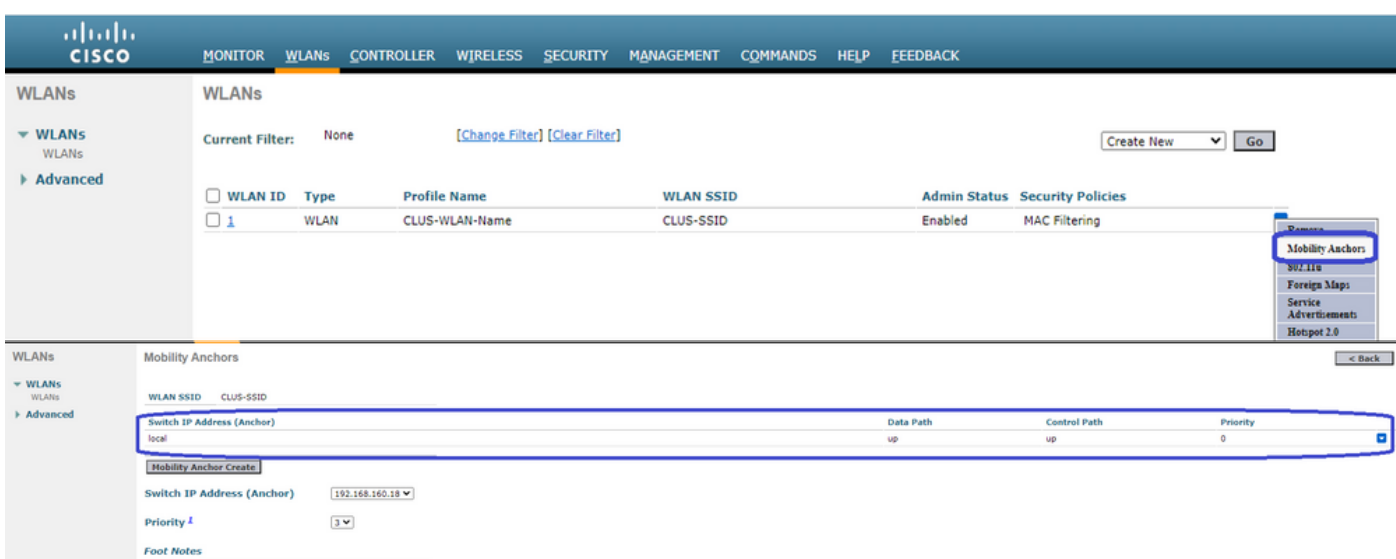
Passare quindi alla scheda **Security>AAA Servers** (Server AAA di sicurezza) e impostare il server ISE come "Authentication Servers" (Server di autenticazione). **Non** impostare alcun valore per i "Server di accounting". Deselezionare la casella di controllo "Abilita" per l'accounting.



Mentre le configurazioni WLAN sono ancora configurate, passare alla scheda "Avanzate" e abilitare "Consenti sostituzione AAA", nonché modificare "Stato NAC" in "ISE NAC"



L'ultima cosa è ancorarla a se stessa. Per farlo, tornare alla pagina **WLAN** e passare il mouse sulla casella blu a destra di **WLAN>Mobility Anchors**. Impostare "Switch IP Address (Anchor)" (Indirizzo IP switch (Anchor)) su local (Locale) e premere il pulsante "Mobility Anchor Create" (Creazione ancoraggio mobilità). Dovrebbe quindi apparire con priorità 0 ancorata locale.



## Reindirizzamento dell'ACL sul WLC di AireOS

Questa è la configurazione finale richiesta sul WLC di AireOS. Per creare il reindirizzamento dell'ACL, selezionare **Protezione>Access Control Lists>Access Control Lists>New**. Immettere il nome dell'ACL (che deve corrispondere a quello inviato negli AVP) e premere "Apply".



Fare clic sul nome dell'ACL appena creato. Fare clic sul pulsante "Aggiungi nuova regola". A differenza del controller 9800, sul WLC di AireOS, è possibile configurare un'istruzione di autorizzazione per il traffico che può raggiungere ISE senza essere reindirizzato. DHCP e DNS sono consentiti per impostazione predefinita.

The screenshot shows the Cisco ISE Security configuration page. The left sidebar contains a navigation menu with categories like AAA, RADIUS, Local EAP, and Access Control Lists. The main content area is titled "Access Control Lists > Edit" and shows the configuration for an ACL named "CLUS-ACL".

**General**

Access List Name: CLUS-ACL  
Deny Counters: 5

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	192.168.160.99 / 255.255.255.255	TCP	Any	8443	Any	Any	273
2	Permit	192.168.160.99 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	566

## Configurare ISE

L'ultimo passaggio consiste nel configurare ISE per CWA. Le opzioni disponibili sono numerose, ma in questo esempio verranno mantenute le nozioni di base e verrà utilizzato il portale guest predefinito con registrazione automatica.

Ad ISE, è necessario creare un profilo di autorizzazione, un set di criteri con un criterio di autenticazione e un criterio di autorizzazione che utilizzi il profilo di autorizzazione, aggiungere lo switch 9800 (esterno) ad ISE come dispositivo di rete, quindi creare un nome utente e una password per accedere alla rete.

Per creare il profilo di autorizzazione, selezionare **Criterio>Elementi dei criteri>Autorizzazione>Risultati>Profili di autorizzazione>+Aggiungi**. Verificare che il tipo di accesso restituito sia "access\_accept", quindi impostare gli AVP (coppie attributo-valore) che si desidera inviare. Per CWA, l'ACL di reindirizzamento e l'URL di reindirizzamento sono obbligatori, ma è possibile anche inviare indietro elementi come l'ID VLAN e il timeout della sessione. È importante che il nome dell'ACL corrisponda al nome dell'ACL di reindirizzamento sul WLC esterno e su quello di ancoraggio.

The screenshot shows the Cisco ISE Identity Services Engine configuration page. The left sidebar contains a navigation menu with categories like Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled "Authorization Profiles > test" and shows the configuration for an Authorization Profile named "CLUS-AuthZ-Profile-ISE".

**Authorization Profile**

\* Name: CLUS-AuthZ-Profile-ISE  
Description:   
\* Access Type: ACCESS\_ACCEPT  
Network Device Profile: Cisco  
Service Template:   
Track Movement:   
Passive Identity Tracking:

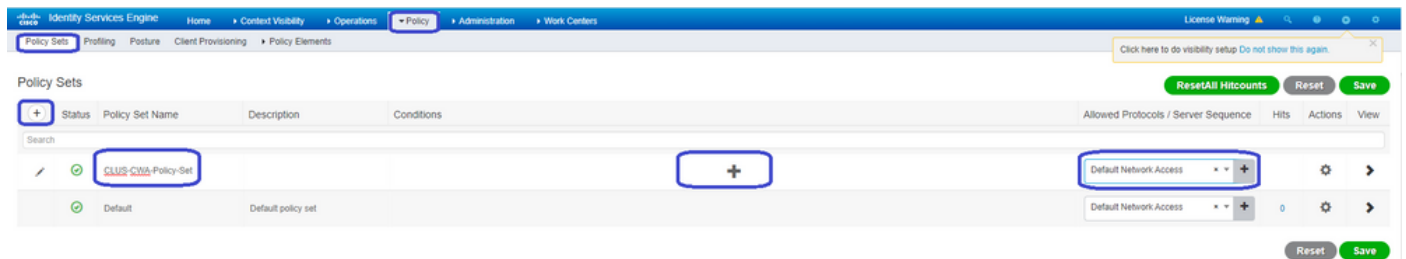
**Common Tasks**

Voice Domain Permission  
 Web Redirection (CWA, MDM, NSP, CPP)  
Centralized Web Auth:  ACL:  Value:

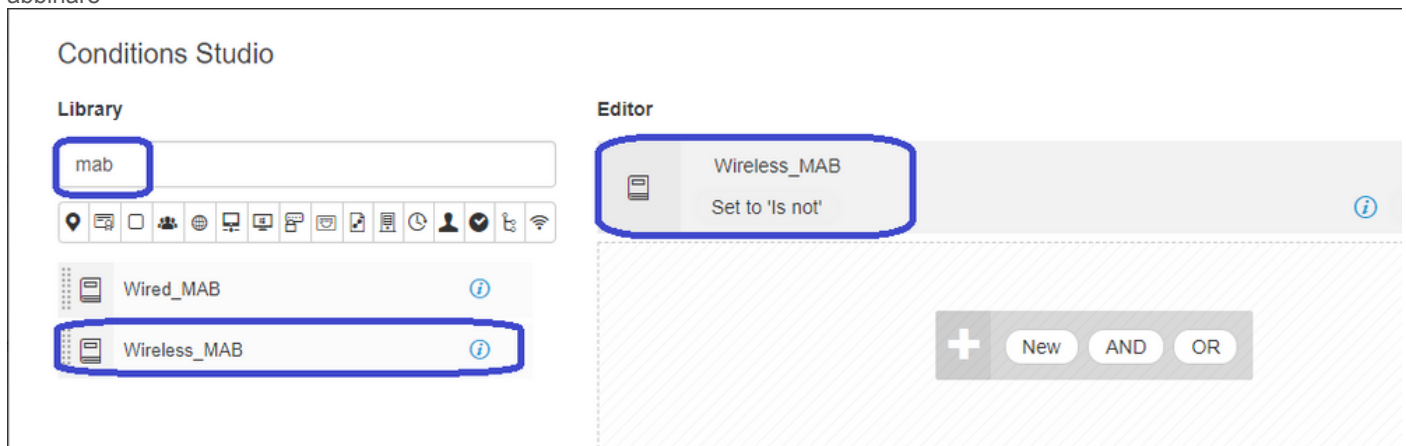
È quindi necessario configurare un modo per applicare il profilo di autorizzazione appena creato ai client che utilizzano CWA. Per

ottenere questo risultato, è possibile creare un set di criteri che ignori l'autenticazione quando si utilizza MAB e applichi il profilo di autorizzazione quando si utilizza il SSID inviato nell'ID stazione chiamato. Di nuovo, ci sono molti modi per farlo quindi se avete bisogno di qualcosa di più specifico o più sicuro, che bene, questo è solo il modo più semplice di farlo.

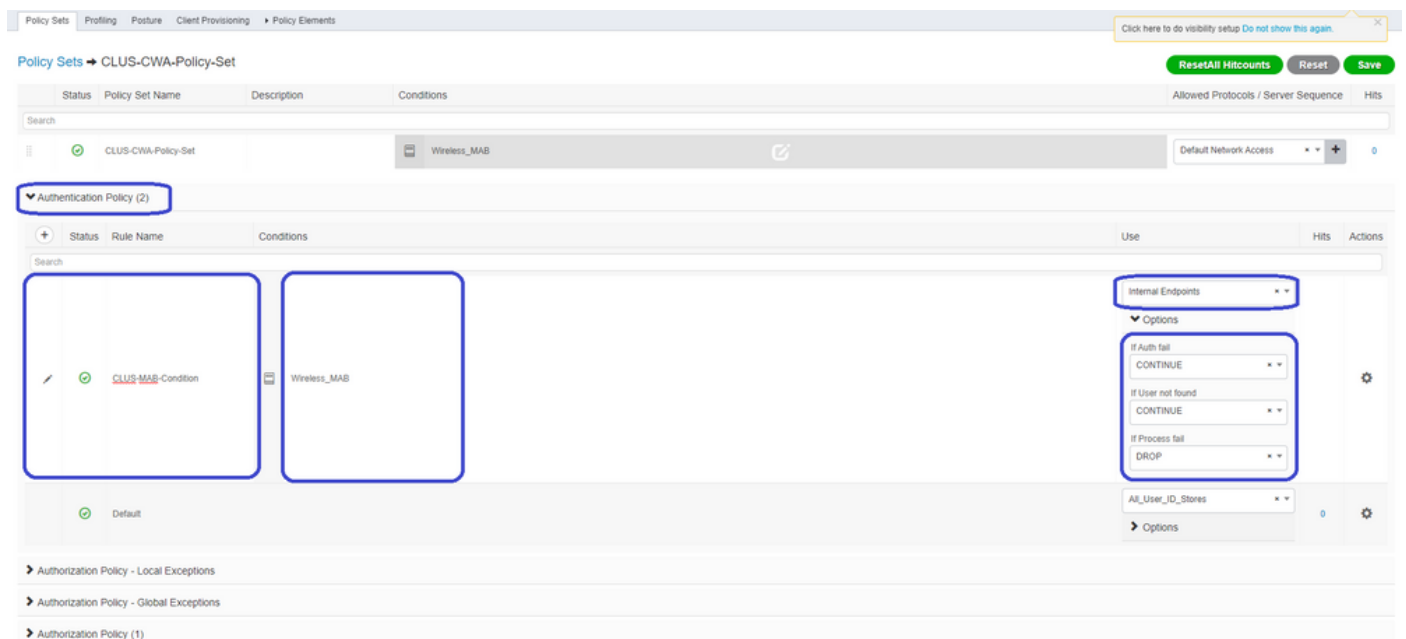
Per creare il set di criteri, andare **aCriteri>Set di criteri** e fare clic sul pulsante + nella parte sinistra della schermata. Assegnare un nome al nuovo set di criteri e assicurarsi che sia impostato su "accesso di rete predefinito" o su qualsiasi elenco di protocolli consentiti che consenta "Ricerca host processo" per MAB. Per controllare l'elenco di protocolli consentiti, selezionare Criteri>Elementi dei criteri>Risultati>Autenticazione>Protocolli consentiti. Fare clic sul segno + all'interno del nuovo set di criteri creato.



Per questo set di criteri ogni volta che MAB viene utilizzato in ISE passerà attraverso questo set di criteri. In seguito sarà possibile creare criteri di autorizzazione corrispondenti all'ID della stazione chiamata in modo da poter applicare risultati diversi a seconda della WLAN in uso. Questo processo è molto personalizzabile con molte cose su cui potete abbinare



All'interno del set di regole, creare le regole. I criteri di autenticazione possono corrispondere nuovamente in MAB, ma è necessario modificare l'archivio ID per utilizzare gli endpoint interni ed è necessario modificare le opzioni per continuare l'autenticazione non riuscita e l'utente non trovato.



Una volta impostato il criterio di autenticazione, è necessario creare due regole nel criterio di autorizzazione. Questo criterio è



simile a un ACL, quindi l'ordine deve avere la regola di post-autenticazione in primo piano e la regola di pre-autenticazione in secondo piano. La regola di post-autenticazione corrisponderà agli utenti che hanno già eseguito il flusso guest. Questo per dire che se hanno già firmato, andranno incontro a quella regola e si fermeranno lì. Se non hanno effettuato l'accesso, continueranno a scorrere l'elenco e raggiungeranno la regola di preautenticazione per ottenere il reindirizzamento. È consigliabile far corrispondere le regole dei criteri di autorizzazione con l'ID stazione chiamato che termina con l'SSID in modo che venga rilevato solo per le WLAN configurate a tale scopo.

Policy Sets → CLUS-CWA-Policy-Set Reset All Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
🟢	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

Authentication Policy (2)  
Authorization Policy - Local Exceptions  
Authorization Policy - Global Exceptions  
Authorization Policy (4)

Status	Rule Name	Conditions	Results	Security Groups
🟢	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth	Select from list
🟢	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE	Select from list
🟢	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA	Select from list
🟢	Default		DenyAccess	Select from list

Ora che la policy è stata configurata, è necessario comunicare ad ISE le informazioni relative allo switch 9800 (esterno) in modo che ISE possa considerarlo un autenticatore. Questa operazione può essere eseguita alle **Admin>Risorse di rete>Dispositivo di rete>+** È necessario denominarlo, impostare l'indirizzo IP (o in questo caso l'intera subnet di amministrazione), abilitare RADIUS e impostare il segreto condiviso. Il segreto condiviso su ISE deve corrispondere al segreto condiviso su 9800 altrimenti questo processo non riuscirà. Dopo aver aggiunto la configurazione, fare clic sul pulsante di invio per salvarla.



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows the navigation tree with 'Network Devices' selected. The main configuration area is titled 'Network Devices List > JaysNet' and 'Network Devices'. The configuration fields are as follows:

- \* Name: CLUS\_Net-Device
- Description: [Empty]
- IP Address: 192.168.160.0
- Subnet: 24
- \* Device Profile: Cisco
- Model Name: [Empty]
- Software Version: [Empty]
- \* Network Device Group:
  - Location: All Locations
  - IPSEC: No
  - Device Type: All Device Types
- RADIUS Authentication Settings
  - RADIUS UDP Settings
    - Protocol: RADIUS
    - Shared Secret: [Masked]
    - Use Second Shared Secret:
    - CoA Port: 1700
  - RADIUS DTLS Settings: [Empty]

Infine, è necessario aggiungere il nome utente e la password che il client immetterà nella pagina di login per verificare che abbia accesso alla rete. Questa operazione viene eseguita in **Amministrazione > Gestione delle identità > Identità > Utenti > +Aggiungi** assicurarsi di premere invio dopo averlo aggiunto. Come tutte le altre soluzioni ISE, anche questa è personalizzabile e non deve essere un utente memorizzato localmente, ma è la configurazione più semplice.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The 'Identities' section is selected, and the 'Users' sub-section is active. The main content area displays the 'New Network Access User' configuration form. The form includes fields for Name (CLUS-User), Status (Enabled), Email, Password Type (Internal Users), Login Password, Re-Enter Password, User Information (First Name, Last Name), Account Options (Description, Change password on next login), Account Disable Policy (Disable account if date exceeds 2020-07-17), and User Groups (Select an item). The 'Submit' button is highlighted.

## Differenze nella configurazione quando il WLC di AireOS è il dispositivo esterno e Catalyst 9800 è l'ancoraggio

Se si desidera che il WLC di AireOS sia il controller esterno, la configurazione è la stessa di quella precedente, con solo due differenze.

1. Poiché l'accounting AAA non viene mai eseguito sull'ancoraggio, lo switch 9800 non avrebbe un elenco di metodi di accounting e il WLC di AireOS avrebbe l'accounting abilitato e indirizzato all'ISE.
2. L'AireOS dovrebbe ancorarsi al 9800 invece che a se stesso. Nel Profilo criterio, per 9800 non viene selezionato un ancoraggio ma viene selezionata la casella di controllo "Ancoraggio esportazione".
3. È importante notare che quando i WLC di AireOS esportano il client sullo switch 9800, non esiste il concetto di profili delle policy, viene inviato solo il nome del profilo WLAN. Pertanto, il router 9800 applicherà il nome del profilo WLAN inviato da AireOS sia al nome del profilo WLAN che al nome del profilo della policy. Ciò detto, quando si esegue l'ancoraggio da un WLC AireOS a un WLC 9800, il nome del profilo WLAN su entrambi i WLC e il nome del profilo delle policy su 9800, devono corrispondere tutti.

# Verifica

Per verificare le configurazioni sul WLC 9800, eseguire i comandi

- AAA

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- Profilo criterio

```
Show wireless profile policy detailed <profile name>
```

- Tag criteri

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- Verificare che la mobilità sia attiva con l'ancoraggio

```
Show wireless mobility summary
```

Per verificare le configurazioni sul WLC di AireOS, eseguire i comandi

- AAA

```
Show radius summary
```

Nota: RFC3576 è la configurazione CoA

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- Verificare che la mobilità sia compatibile con le

```
Show mobility summary
```

## Risoluzione dei problemi

L'aspetto della risoluzione dei problemi varia a seconda del punto del processo in cui il client si arresta. Ad esempio, se il WLC non riceve mai una risposta da ISE su MAB, il client rimane bloccato in "Policy Manager State: Associazione" e non verrebbe esportato nell'ancora. In questa

situazione, si potrebbero risolvere i problemi solo sull'esterno e si potrebbe raccogliere una traccia RA e un pacchetto di acquisizione per il traffico tra il WLC e ISE. Un altro esempio potrebbe essere che il MAB è stato superato ma il client non riceve il reindirizzamento. In questo caso, è necessario assicurarsi che l'utente straniero abbia ricevuto il reindirizzamento negli AVP e lo abbia applicato al client. Inoltre, è necessario controllare l'ancoraggio per verificare che il client sia presente con l'ACL corretto. L'ambito della risoluzione dei problemi non è compreso nella progettazione di questo documento tecnico (vedere i riferimenti per le linee guida generali per la risoluzione dei problemi di un client).

Per ulteriori informazioni sulla risoluzione dei problemi relativi a CWA sul WLC 9800, visita il sito Cisco Live! presentazione DGTL-TSCENT-404

## Informazioni sulla risoluzione dei problemi di Catalyst 9800

### Dettagli client

```
show wireless client mac-address
```

Qui è possibile esaminare "Policy Manager State", "Session Manager>Auth Method", "Mobility Role".

Queste informazioni sono disponibili anche nella GUI in Monitoraggio > Client

### Embedded Packet Capture

Dalla CLI, il comando avvia *#monitor capture <nome acquisizione>* quindi le opzioni seguono.

Dalla GUI, selezionare Troubleshoot>Packet Capture>+Add

### Tracce RadioActive

Dalla CLI

```
debug wireless mac/ip
```

Utilizzare la forma no del comando per arrestarlo. Verrà registrato in un file in bootflash denominato "ra\_trace", quindi sull'indirizzo MAC o IP del client e sulla data e l'ora.

Dalla GUI, selezionare Troubleshoot>Radioactive Trace>+Add. Aggiungere l'indirizzo MAC o IP del client, fare clic su apply, quindi fare clic su start. Dopo aver eseguito il processo più volte, arrestare la traccia, generare il registro e scaricarlo nel dispositivo.

## Informazioni sulla risoluzione dei problemi AireOS

### Dettagli client

Dalla CLI, *visualizzare i dettagli del client <mac client>*

Dalla GUI Monitor>Client

## Debug dalla CLI

*Debug client*

*Debug mobility handoff*

*Debug mobility config*

## Riferimenti

[Creazione di tunnel per la mobilità con controller 9800](#)

[Debug wireless e raccolta log su 9800](#)