

Configurazione dell'autenticazione Web locale con autenticazione esterna

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Autenticazione Web](#)

[Tipi di autenticazione](#)

[Database per autenticazione](#)

[Autenticazione Web locale](#)

[Autenticazione Web locale con autenticazione esterna](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione dell'autenticazione Web locale con autenticazione esterna sulla CLI](#)

[Configurazione del server e del gruppo di server AAA](#)

[Configura autenticazione e autorizzazione locali](#)

[Configura mapping parametri](#)

[Configurazione dei parametri di sicurezza WLAN](#)

[Crea profilo criteri wireless](#)

[Crea un tag di criteri](#)

[Assegnazione di un tag di criterio a un punto di accesso](#)

[Configurazione dell'autenticazione Web locale con autenticazione esterna su WebUI](#)

[Configurazione AAA sui controller 9800 WLC](#)

[Configurazione WebAuth](#)

[Configurazione della WLAN](#)

[Configurazione del profilo di policy](#)

[Configurazione del tag di policy](#)

[Assegnazione di un tag di policy](#)

[Configurazione di ISE](#)

[Connetti client guest](#)

[Verifica](#)

[show wlan summary](#)

[Mostra configurazione mappa parametri](#)

[Mostra informazioni AAA](#)

[Risoluzione dei problemi](#)

[Problemi comuni](#)

[Debug condizionale, Radio Active Trace e Embedded Packet Capture](#)

[Esempio di tentativo riuscito](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione Web locale con autenticazione esterna su un WLC 9800 e ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione dei Wireless LAN Controller (WLC) 9800
- LAP (Lightweight Access Point)
- Come configurare e configurare un server Web esterno Identity Services Engine (ISE).
- Come configurare i server DHCP e DNS.

Componenti usati

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

- 9800-40 WLC Cisco IOS® XE, versione 17.18.4a con APSP1 e APSP2
- Identity Services Engine (ISE), versione 3.2.0.542
- Cisco® Wireless serie 9172I Wi-Fi 7 Access Point, versione 17.18.4.202

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.

Autenticazione Web

L'autenticazione Web è una funzione di protezione di livello 3 che consente agli utenti guest di accedere alla rete.

Questa funzionalità è progettata per fornire un accesso guest facile e sicuro agli SSID aperti, senza la necessità di configurare un profilo utente, e può inoltre funzionare con i metodi di sicurezza di layer 2.

Lo scopo dell'autenticazione Web è quello di consentire ai dispositivi non attendibili (guest) di accedere alla rete con privilegi di accesso limitati, tramite una WLAN guest configurabile con meccanismi di sicurezza e senza compromettere la sicurezza della rete. Affinché gli utenti guest possano accedere alla rete, è necessario che eseguano correttamente l'autenticazione, ovvero che forniscano le credenziali corrette o accettino i criteri di utilizzo accettabile per accedere alla rete.

L'autenticazione Web è un vantaggio per le aziende in quanto favorisce la fedeltà degli utenti, rende l'azienda conforme all'utilizzo di un disclaimer che l'utente ospite deve accettare e consente all'azienda di impegnarsi con i visitatori.

Per distribuire l'autenticazione Web, è necessario considerare la modalità di gestione del portale guest e dell'autenticazione. Esistono due metodi comuni:

- Autenticazione Web locale (LWA): Metodo di reindirizzamento degli utenti guest a un portale direttamente dal WLC. Il reindirizzamento e l'ACL pre-WebAuth sono configurati localmente sul WLC.
- Autenticazione Web centrale (CWA): Un metodo di reindirizzamento degli utenti guest in cui l'URL di reindirizzamento e l'ACL di reindirizzamento sono configurati centralmente su un server esterno (ad esempio ISE) e comunicati al WLC tramite RADIUS. Nell'autenticazione Web centrale, l'URL di reindirizzamento e l'ACL di reindirizzamento si trovano al centro su un server esterno (ad esempio RADIUS). Il server RADIUS è quello che gestisce l'autenticazione e invia istruzioni al WLC. In CWA, il WLC non richiede un certificato di autenticazione Web locale, è richiesto un solo certificato sul portale Web centrale e richiede un server di autenticazione centrale, come ISE. Per ulteriori informazioni su CWA, consultare il documento sulla [configurazione dell'autenticazione Web centrale \(CWA\) su Catalyst 9800 WLC e ISE](#).

In Autenticazione Web locale, il portale Web può essere presente sul WLC o su un server esterno. In LWA con autenticazione esterna, il portale Web è presente sul WLC. In LWA con server Web esterno, il portale Web è presente su un server esterno, ad esempio Cisco DNA Spaces. Un esempio di LWA con server Web esterno è descritto in dettaglio all'indirizzo: [Configurare DNA Spaces Captive Portal con Catalyst 9800 WLC](#).

Diagramma dei diversi metodi di autenticazione Web:

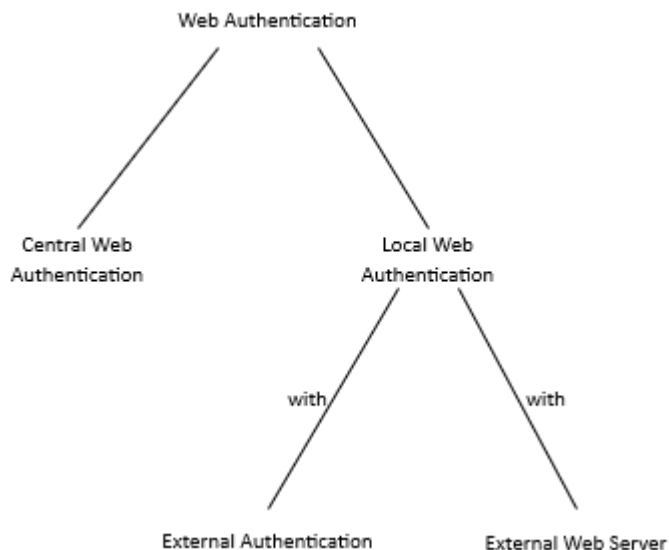


Diagramma dei diversi metodi di autenticazione Web



Nota: Se si distribuiscono Wi-Fi 7 AP con autenticazione Web su un WLC 9800, verificare di eseguire una versione di Cisco IOS XE consigliata, ad esempio 17.18.4a o successiva.

Tipi di autenticazione

Per autenticare l'utente guest sono disponibili quattro tipi di autenticazione:

- Webauth: Immettere nome utente e password.
- Consenso (web-passthrough): Accettare le CDS.
- Autypass: Autenticazione basata sull'indirizzo MAC del dispositivo utente guest.
- Webconsence: Combinazione di nome utente/password e accettazione di CDS.

webauth	authbypass	consent	webconsent
Username: Password: OK	Client connects to the SSID and gets an IP address, then the 9800 WLC checks if the MAC address is allowed to enter the network, if yes, it is moved to RUN state, if it is not it is not allowed to join. (It won't fall back to web authentication)	banner1 ☒ Accept ☐ Don't Accept OK	banner login ☒ Accept ☐ Don't Accept Username: Password: OK

Database per autenticazione

Le credenziali per l'autenticazione possono essere archiviate su un server LDAP, localmente sul WLC o sul server RADIUS.

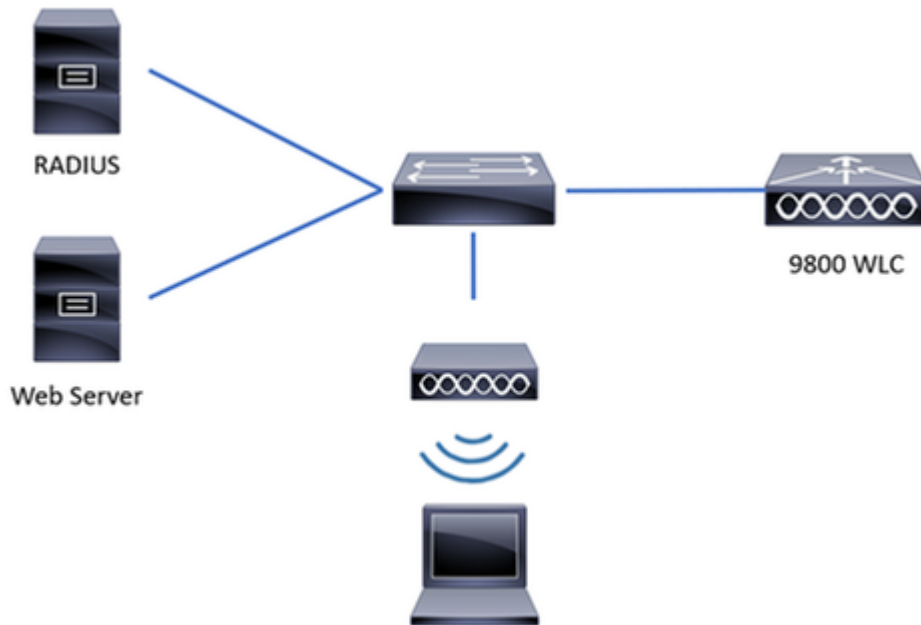
- Database locale: Le credenziali (nome utente e password) vengono archiviate localmente sul WLC.
- Database LDAP: Le credenziali vengono memorizzate nel database back-end LDAP. Il WLC esegue una query sul server LDAP per ottenere le credenziali di un utente specifico nel database.
- Database RADIUS: Le credenziali vengono archiviate nel database back-end RADIUS. Il WLC esegue una query sul server RADIUS per ottenere le credenziali di un utente specifico nel database.

Autenticazione Web locale

Nell'autenticazione Web locale l'utente guest viene reindirizzato a un portale Web direttamente dal WLC.

Il portale Web può trovarsi nel WLC o in un altro server. Ciò che rende locale è il fatto che l'URL di reindirizzamento e l'ACL che corrisponde al traffico devono essere sul WLC (non sulla posizione del portale Web). In LWA, quando un utente guest si connette alla WLAN guest, il WLC intercetta la connessione dall'utente guest e la reindirizza all'URL del portale Web, dove all'utente guest viene richiesto di eseguire l'autenticazione. Quando l'utente guest immette le credenziali (nome utente e password), il WLC le acquisisce. Il WLC autentica l'utente guest con un server LDAP, un server RADIUS o un database locale (database presente localmente sul WLC). Nel caso di un server RADIUS (un server esterno come ISE), può essere utilizzato non solo per memorizzare le credenziali, ma anche per fornire opzioni per la registrazione del dispositivo e l'autoprovisioning. Nel caso di un server Web esterno, ad esempio Cisco DNA Spaces, il portale Web è presente. In LWA c'è un certificato sul WLC e un altro sul portale web.

L'immagine rappresenta la topologia generica di LWA:



Topologia generica di LWA

Dispositivi nella topologia di rete di LWA:

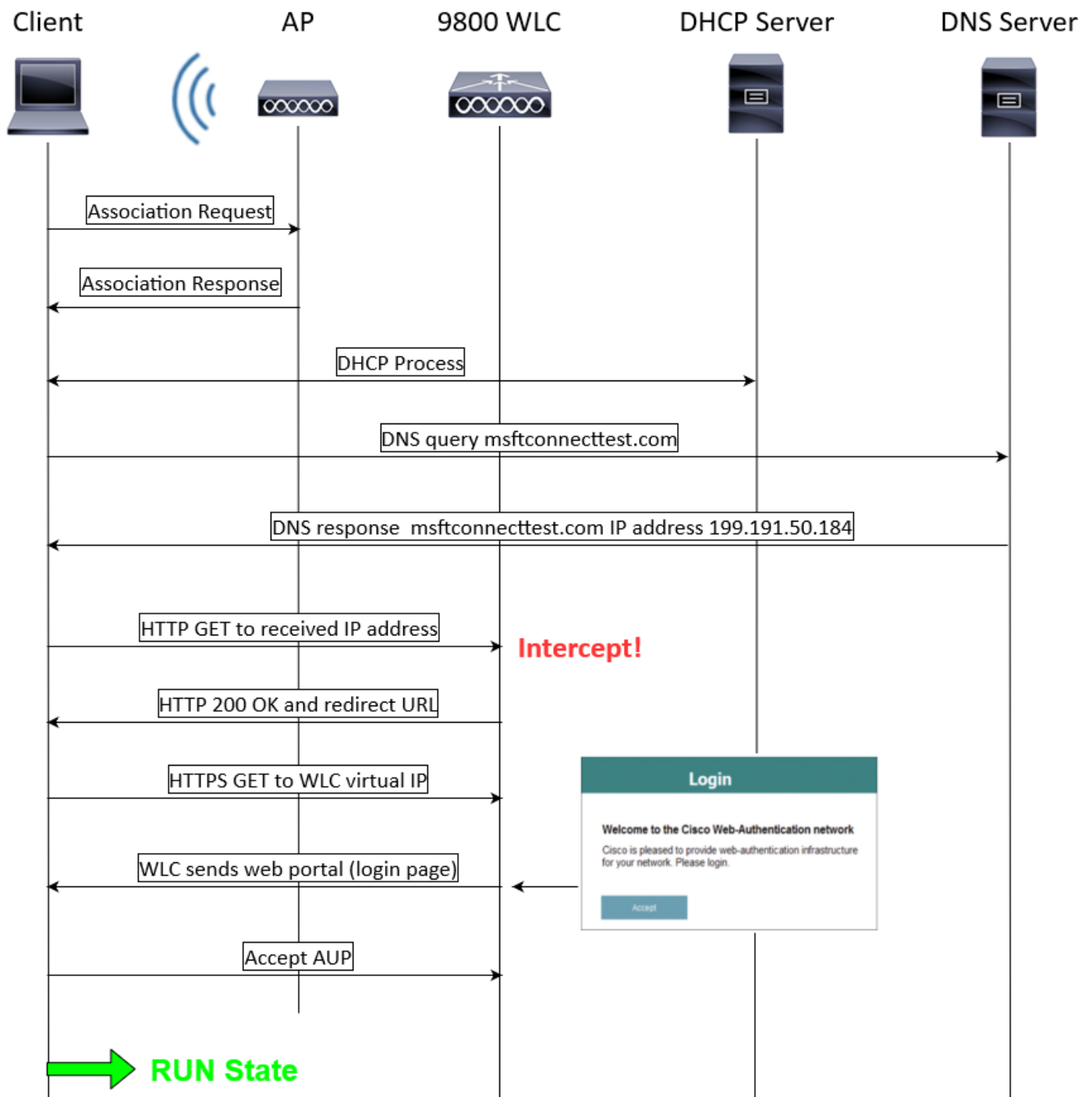
- Client: Invia le richieste al server DHCP e DNS, richiede l'accesso alla WLAN guest e risponde alle richieste del WLC.
- Access Point: Collegata a uno switch, trasmette la WLAN guest e fornisce la connessione wireless ai dispositivi degli utenti guest. Consente inoltre l'invio di pacchetti DHCP e DNS prima dell'autenticazione dell'utente guest (prima di immettere credenziali valide).
- WLC: Gestisce i punti di accesso e i client. Il WLC ospita l'URL di reindirizzamento e l'ACL che corrisponde al traffico. Intercetta le richieste HTTP degli utenti guest e le reindirizza a un portale Web (pagina di accesso) in cui gli utenti guest devono eseguire l'autenticazione. Acquisisce le credenziali e autentica gli utenti guest e invia richieste di accesso a un server esterno, a un server LDAP o a un database locale per confermare la validità delle credenziali.
- Server di autenticazione: Risponde alle richieste di accesso provenienti dal WLC con access accept/reject. Il server di autenticazione convalida le credenziali dell'utente guest e avvisa il WLC se le credenziali sono valide o meno. Se le credenziali sono valide, l'utente guest è autorizzato ad accedere alla rete (il server di autenticazione fornisce opzioni per la registrazione del dispositivo e l'autoprovisioning). Se le credenziali non sono valide, l'utente guest non potrà accedere alla rete.

LWA:

- L'utente guest viene associato a un punto di accesso che trasmette la WLAN guest.
- L'utente guest esegue il processo DHCP per ottenere un indirizzo IP.
- L'utente guest desidera eseguire un controllo della connettività Internet al portale vincolato. Se si tratta di un dispositivo Apple, prova il portale captive Apple; se si tratta di un dispositivo

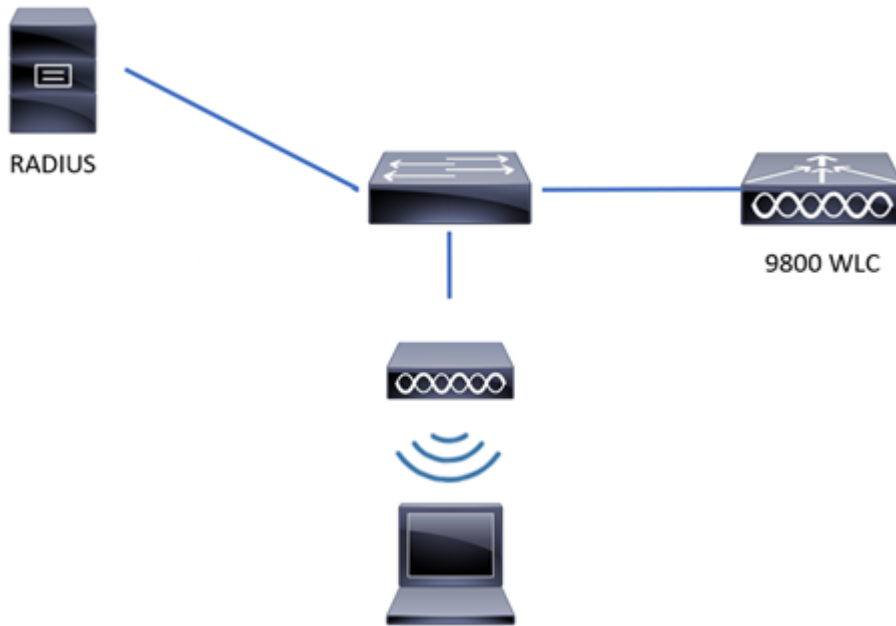
Android prova il portale captive Android; se si tratta di un dispositivo Windows, prova a utilizzare il portale di prova di Windows connect.

- L'utente guest invia una query DNS per richiedere l'indirizzo IP del portale vincolato. Il server DNS risponde alla query con l'indirizzo IP corrispondente.
- L'utente guest invia un messaggio HTTP GET all'indirizzo IP del portale captive.
- Il WLC intercetta il messaggio e risponde all'utente guest con HTTP 200 OK e l'URL di reindirizzamento.
- L'utente guest invia un messaggio GET HTTPS all'IP virtuale del WLC e il WLC risponde con il portale Web.
- All'utente guest viene richiesto di immettere le credenziali di autenticazione nel portale Web.
- Il portale Web reindirizza l'utente al WLC con le credenziali fornite (se viene utilizzato un portale Web esterno).
- Il WLC autentica l'utente guest tramite un database locale oppure invia una query al server RADIUS o LDAP per confermare se le credenziali sono corrette (se il tipo di autenticazione è webconsence o webauth).
- Se le credenziali sono corrette, il WLC autentica l'utente guest e passa allo stato RUN. Se le credenziali sono errate, il WLC elimina l'utente guest.
- Il WLC reindirizza il client all'URL originale immesso nel browser Web.



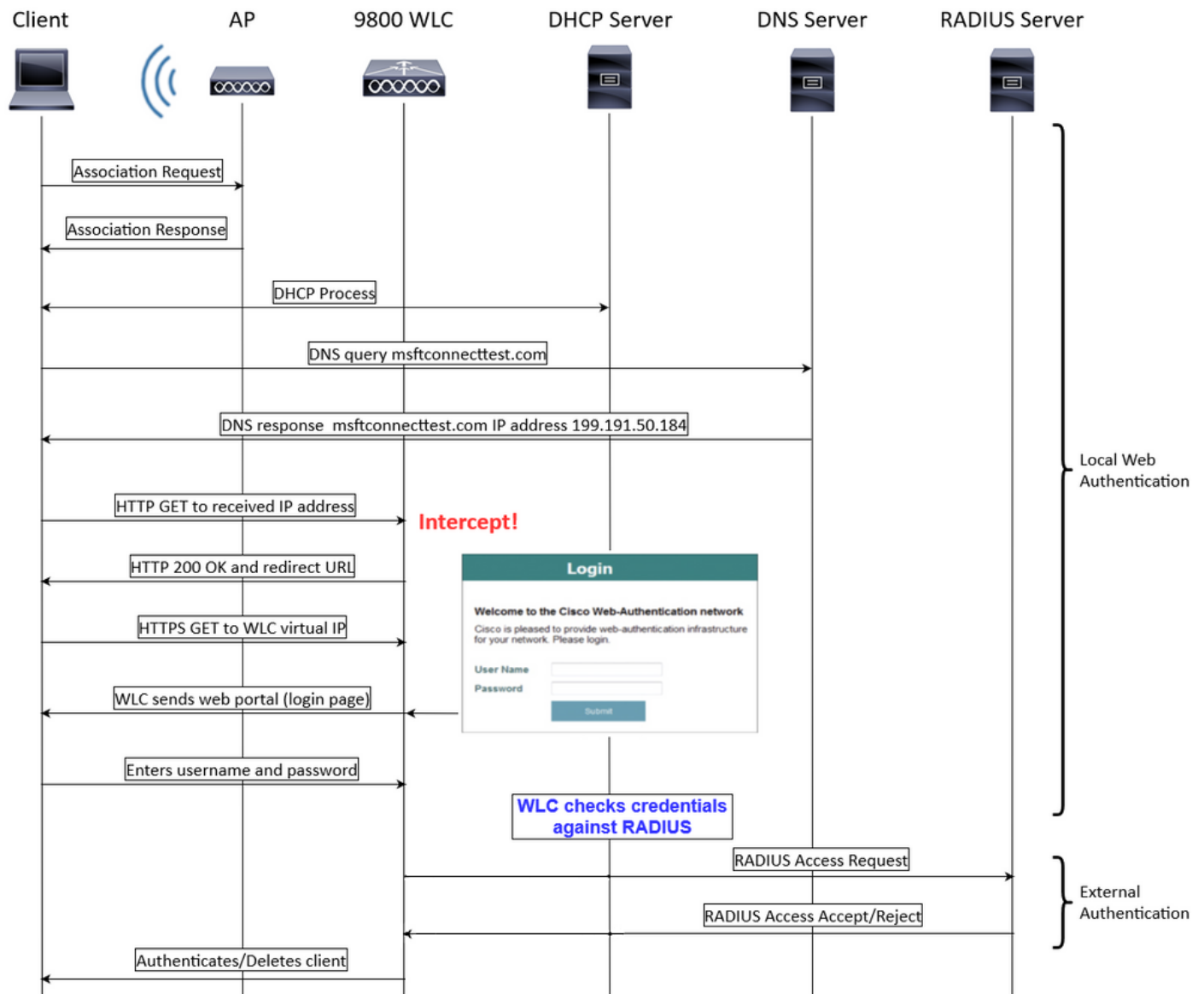
Flusso LWA

Autenticazione Web locale con autenticazione esterna



Topologia generica di LWA-EA

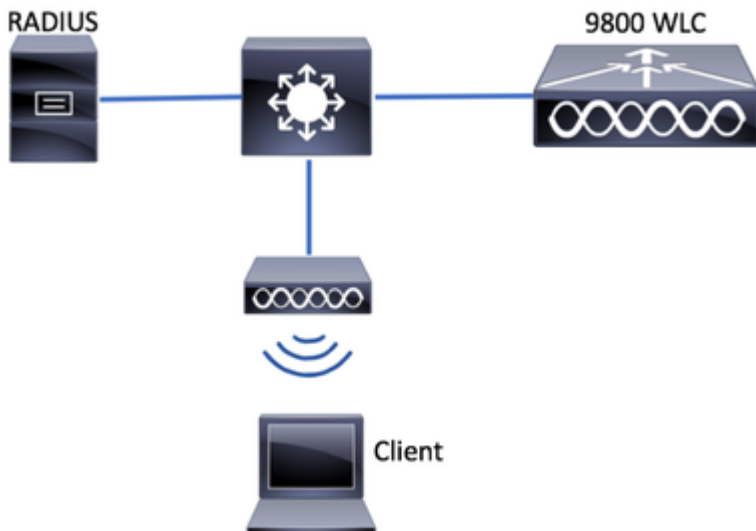
LWA-EA è un metodo di LWA in cui il portale Web e l'URL di reindirizzamento si trovano sul WLC e le credenziali sono archiviate su un server esterno, ad esempio ISE. Il WLC acquisisce le credenziali e autentica il client tramite un server RADIUS esterno. Quando un utente guest immette le credenziali, il WLC le confronta con RADIUS, invia una richiesta di accesso RADIUS e riceve un'accettazione/rifiuto di accesso RADIUS dal server RADIUS. Quindi, se le credenziali sono corrette, l'utente guest passa allo stato RUN. Se le credenziali non sono corrette, l'utente guest viene eliminato dal WLC.



Flusso LWA-EA

Configurazione

Esempio di rete



Esempio di rete



Nota: In questo esempio di configurazione vengono considerate solo la commutazione e l'autenticazione a livello centrale. La configurazione della commutazione locale flessibile prevede requisiti leggermente diversi per la configurazione dell'autenticazione Web.

Configurazione dell'autenticazione Web locale con autenticazione esterna sulla CLI

Configurazione del server e del gruppo di server AAA

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4 <ip address> auth-port 1812 acct-port 1813
9800WLC(config-radius-server)#key cisco
9800WLC(config-radius-server)#exit
9800WLC(config)#aaa group server radius RADIUSGROUP
9800WLC(config-sg-radius)#server name RADIUS
9800WLC(config-sg-radius)#end
```

Configura autenticazione e autorizzazione locali

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
```

```
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint <trustpoint name>
9800WLC(config-params-parameter-map)#end
```

Configurazione dei parametri di sicurezza WLAN

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Crea profilo criteri wireless

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan <vlan name>
9800WLC(config-wireless-policy)#no shutdown
9800WLC(config-wireless-policy)#end
```

Crea un tag di criteri

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
```

```
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

Assegnazione di un tag di criterio a un punto di accesso

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap <MAC address>
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
9800WLC(config-ap-tag)#end
```

Per completare la configurazione sul lato ISE, passare alla sezione Configurazione ISE.

Configurazione dell'autenticazione Web locale con autenticazione esterna su WebUI

Configurazione AAA sui controller 9800 WLC

Passaggio 1. Aggiungere il server ISE alla configurazione WLC 9800.

Passare a Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Server > + Aggiungi e immettere le informazioni sul server RADIUS come mostrato nell'immagine:

Create AAA Radius Server

General

RadSec

Show Me How >

Name*	RADIUS	Support for CoA ⓘ	ENABLED ☒
Server Address*	192.0.2.30	CoA Server Key Type	Clear Text ▼
PAC Key	☐	CoA Server Key ⓘ	
Key Type	Clear Text ▼	Confirm CoA Server Key	
Key* ⓘ		VRF	
Confirm Key*		Automate Tester	☐
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

Cancel

Apply to Device

Configurazione AAA sui controller 9800 WLC

Passaggio 2. Aggiungere il gruppo di server RADIUS.

Passare a Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Gruppo server > +
Aggiungi e immettere le informazioni sul gruppo di server RADIUS:

Create AAA Radius Server Group

Name*

RADIUSGROUP

Group Type

RADIUS

Show Me How >

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Load Balance

☐ DISABLED

IPv4 Source Interface

Search or Select

i

IPv4 VRF

Search or Select

IPv6 Source Interface

Search or Select

i

IPv6 VRF

Search or Select

Available Servers

Assigned Servers

>

<

>>

<<

RADIUS

Cancel

Apply to Device

Aggiungere il gruppo di server RADIUS

Passaggio 3. Creare un elenco di metodi di autenticazione.

Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione > +
Aggiungi:

Quick Setup: AAA Authentication

Method List Name*

LWA_AUTHENTICATION

Type*

login

Group Type

group

Fallback to local

☐

Available Server Groups

radius
ldap
tacacs+

>
<
>>
<<

Assigned Server Groups

RADIUSGROUP

^
^
v
v

Cancel

Apply to Device

Creazione di un elenco di metodi di autenticazione

Passaggio 4. Creare un elenco dei metodi di autorizzazione.

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

Quick Setup: AAA Authorization

Method List Name*

LWA_AUTHORIZATION

Type*

network

i

Group Type

group

i

Fallback to local

☐

Authenticated

☐

Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

RADIUSGROUP

Cancel

Apply to Device

Creare un elenco di metodi di autorizzazione

Configurazione WebAuth

Creare o modificare una mappa dei parametri. Selezionare il tipo come webauth, l'indirizzo IPv4 virtuale deve essere un indirizzo non utilizzato nella rete per evitare conflitti di indirizzi IP e aggiungere un Trustpoint.

Passare a Configurazione > Sicurezza > Autenticazione Web > + Aggiungi o selezionare una mappa dei parametri:

Configuration > Security > Web Auth

+ Add - Delete

Parameter Map Name

global

1 10

Edit Web Auth Parameter

General Advanced

Parameter-map Name: global

Banner Title:

Banner Type: ☒ None ☐ Banner Text ☐ File Name

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☐

Disable Cisco Logo: ☐

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-94747...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::XX

Web Auth intercept HTTPs: ☐

Enable HTTP server for Web Auth: ☐

Disable HTTP secure server for Web Auth: ☐

Cancel Update & Apply

Configurazione WebAuth

Configurazione della WLAN

Passaggio 1. Creare la WLAN.

Selezionare Configuration > Tags & Profiles > WLANs > + Add (Configurazione > Tag e profili > WLAN > +Aggiungi) e configurare la rete secondo necessità.

Add WLAN

General Security Advanced

Profile Name*: LWA_EA

SSID*: LWA_EA

WLAN ID*: 1

Status: ENABLED

Broadcast SSID: ENABLED

Wi-Fi 6E Compatibility: 1/2 requirements met

Wi-Fi 7 Compatibility: 0/3 requirements met 0/3 bands enabled

Radio Policy ⓘ

Show slot configuration

6 GHz Status: ENABLED ⓘ

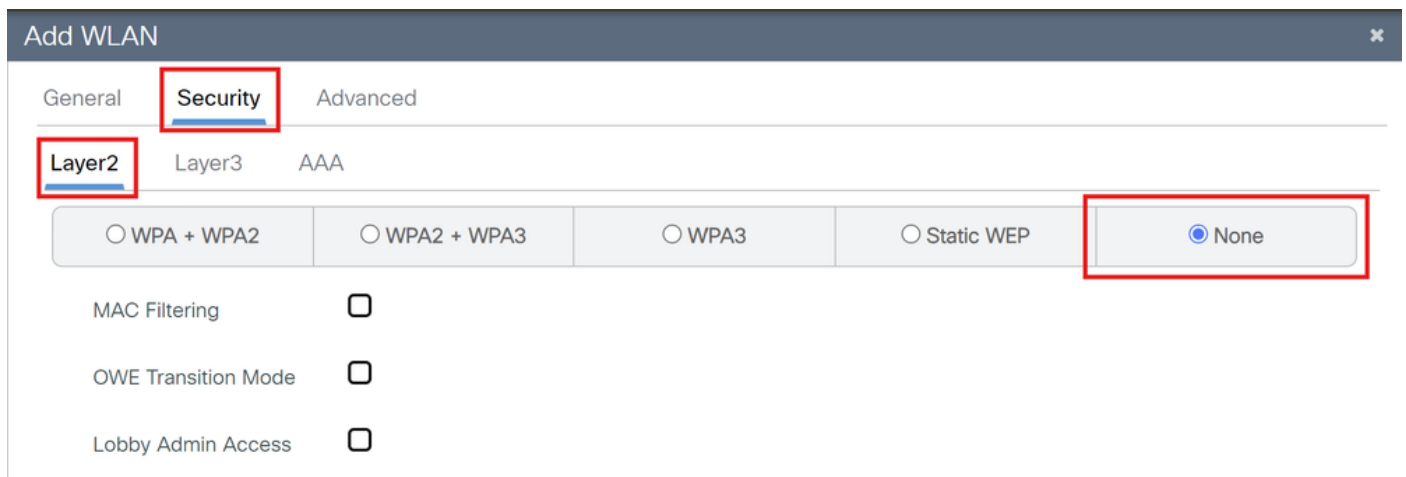
5 GHz Status: ENABLED

2.4 GHz Status: ENABLED

802.11b/g Policy: 802.11b/g

Creazione della WLAN

Passaggio 2. Passare a Protezione > Layer 2 e in Modalità di protezione Layer 2 selezionare Nessuno.



The screenshot shows the 'Add WLAN' configuration window. The 'Security' tab is selected, and the 'Layer2' mode is chosen. The 'None' option for protection is selected, and the 'MAC Filtering', 'OWE Transition Mode', and 'Lobby Admin Access' checkboxes are unchecked.

General	Security	Advanced
Layer2	Layer3	AAA
☐ WPA + WPA2 ☐ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☒ None		
MAC Filtering ☐		
OWE Transition Mode ☐		
Lobby Admin Access ☐		

Creazione della protezione WLAN

Passaggio 3. Passare a Sicurezza > Layer 3 e selezionare la casella di spunta Criteri Web, in Mappa parametri autenticazione Web selezionare il nome del parametro e in Elenco autenticazione selezionare l'elenco di autenticazione creato in precedenza.

Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

Web Policy

☒

Show Advanced Settings >>>

Web Auth Parameter Map

global

Authentication List

LWA_AUTHENTIC...

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Cancel

Apply to Device

Creazione dell'elenco di autenticazione WLAN

La WLAN è visualizzata nell'elenco WLAN:

Configuration > Tags & Profiles > WLANs

+ Add

× Delete

Clone

Enable WLAN

Disable WLAN

WLAN Wizard

Selected WLANs : 0

☐	Status	Name	ID	SSID	2.4/5 GHz Security	6 GHz Security
☐		LWA_EA	1	LWA_EA	[open],[Web Auth]	

1

10

1 - 1 of 1 items

WLAN creata

Configurazione del profilo di policy

All'interno di un profilo di policy, è possibile selezionare la VLAN che assegna i client, tra le altre impostazioni.

È possibile usare il profilo di policy predefinito oppure crearne uno nuovo.

Passaggio 1. Creare un nuovo Policy Profile (Profilo di policy).

Passare a Configurazione > Tag e profili > Criterio e configurare il profilo dei criteri predefinito o crearne uno nuovo.

Verificare che il profilo sia abilitato.

Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

POLICY_PROFILE

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Crea un nuovo profilo criteri

Passaggio 2. Selezionare la VLAN.

Selezionare la scheda Access Policies (Policy di accesso) e selezionare il nome della VLAN dal menu a discesa o immettere manualmente l'ID VLAN.

Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General
Access Policies
QOS and AVC
Mobility
Advanced

RADIUS Profiling
☐

HTTP TLV Caching
☐

DHCP TLV Caching
☐

WLAN Local Profiling

Global State of Device Classification
Disabled ⓘ

Local Subscriber Policy Name
Search or Select

VLAN

VLAN/VLAN Group
VLAN1432 x ⓘ

Multicast VLAN
Enter Multicast VLAN

WLAN ACL

IPv4 ACL
Search or Select

IPv6 ACL
Search or Select

URL Filters ⓘ

Pre Auth
Search or Select

Post Auth
Search or Select

Cancel
Apply to Device

Selezionare la VLAN

Configurazione del tag di policy

Il tag di policy permette di collegare l'SSID al profilo di policy. È possibile creare un nuovo tag o utilizzare il tag predefinito.

Selezionare Configuration > Tags & Profiles > Tags > Policy (Configurazione > Tag e profili > Tag > Policy) e aggiungere una nuova policy se necessario, come mostrato nell'immagine.

Seleziona + Aggiungi:

Add Policy Tag

Name*
POLICY_TAG

Description
Enter Description

WLAN-POLICY Maps : 0

+ Add
Delete

WLAN Profile	Policy Profile
No records available.	

10 items per page
0 - 0 of 0 items

Configurazione del tag di policy

Associare il profilo WLAN al profilo di policy desiderato:

Add Policy Tag

+ Add
Delete

WLAN Profile	Policy Profile
No records available.	

10 items per page
0 - 0 of 0 items

Map WLAN and Policy

WLAN Profile*
LWA_EA
Policy Profile*
POLICY_PRO...

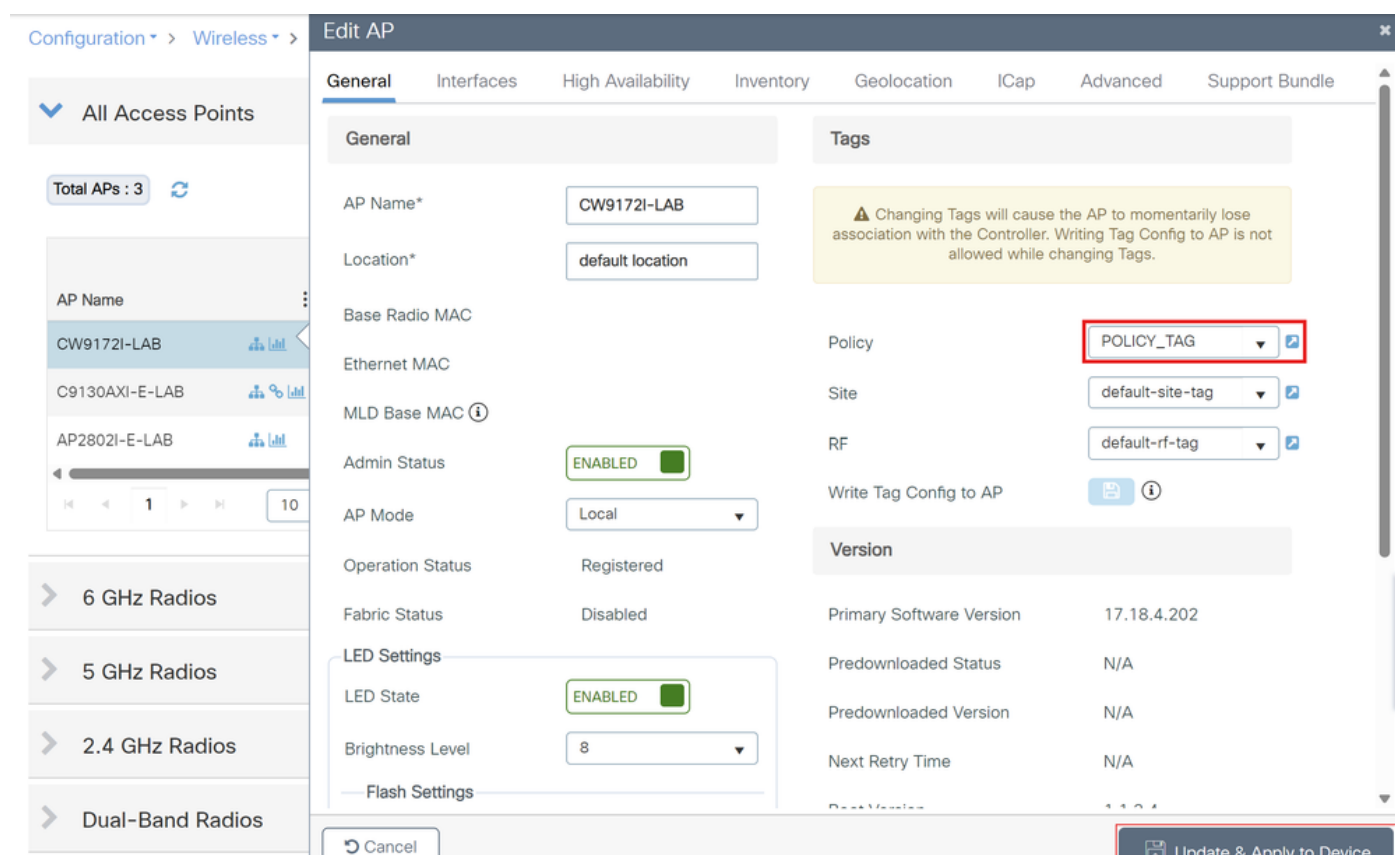
Cancel
Apply to Device

Configurazione del tag di policy

Assegnazione di un tag di policy

Assegnare il tag di policy agli access point desiderati.

Per assegnare il tag a un access point, selezionare Configuration > Wireless > Access Points > AP Name > General Tags (Configurazione > Wireless > Access point > Nome access point > Tag generali), effettuare le opportune assegnazioni, quindi fare clic su Update & Apply to Device (Aggiorna e applica al dispositivo).

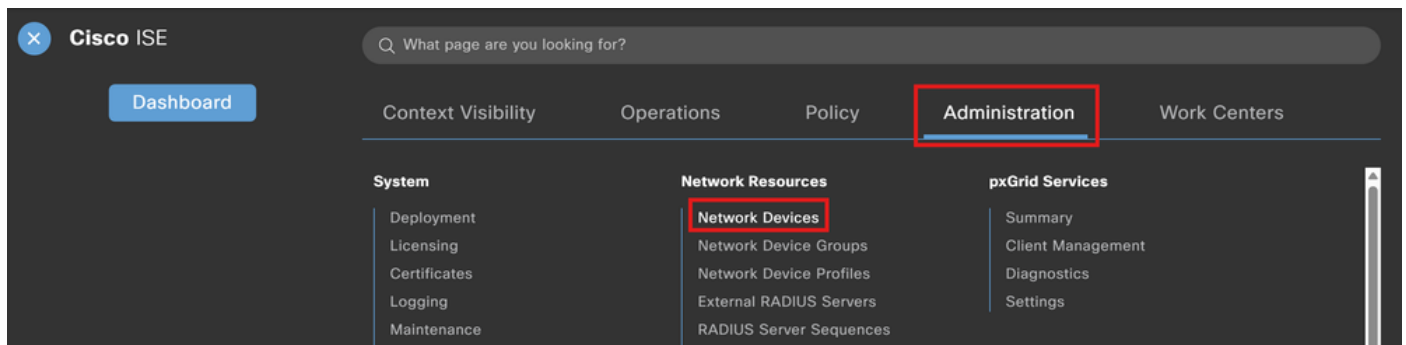


Assegnazione di un tag di policy

Configurazione di ISE

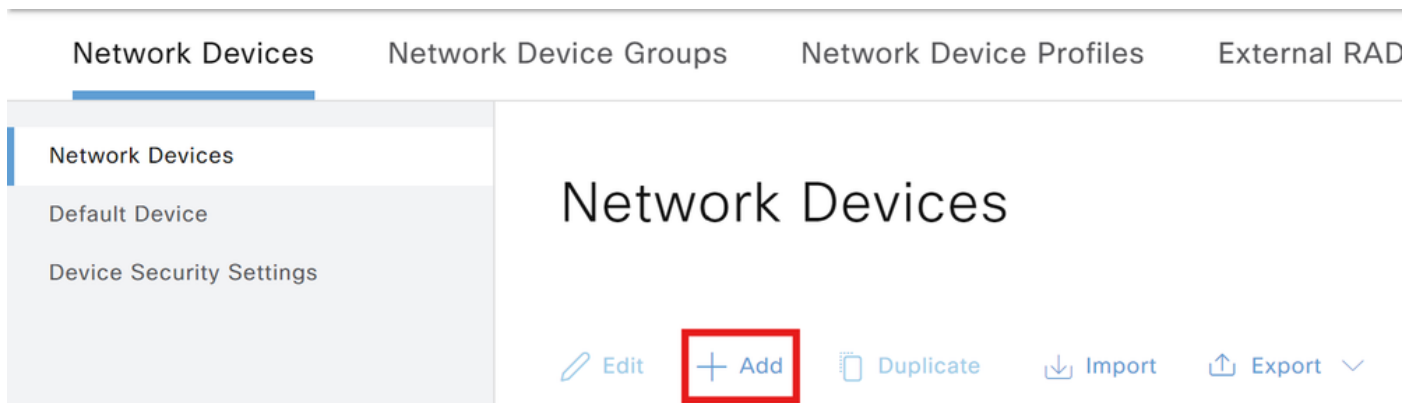
Aggiunta di controller 9800 WLC a ISE

Passaggio 1. Accedere a Administration > Network Resources > Network Devices (Amministrazione > Risorse di rete > Dispositivi di rete) come mostrato nell'immagine.



Aggiunta di controller 9800 WLC a ISE

Passaggio 2. Fare clic su +Aggiungi.



Aggiungi dispositivi di rete

Facoltativamente, può essere un nome di modello, una versione software, una descrizione. Assegnare gruppi di dispositivi di rete in base al tipo di dispositivo, alla posizione o ai controller WLC.

Passaggio 3. Inserire le impostazioni del WLC 9800 come mostrato nell'immagine. Immettere la stessa chiave RADIUS definita al momento della creazione del server sul lato WLC. Quindi fare clic su Invia.

Network Devices

Name

9800-WLC

Description



IP Address



* IP :

192.0.2.20

/

32



Device Profile



Cisco



Model Name



Software Version



Network Device Group

Location

All Locations



[Set To Default](#)

IPSEC

Is IPSEC Device



[Set To Default](#)

Device Type

All Device Types



[Set To Default](#)



✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

.....

[Show](#)

Impostazioni 9800 WLC

Passaggio 4. Passare a Amministrazione > Risorse di rete > Dispositivi di rete, è possibile

visualizzare l'elenco dei dispositivi di rete.

Network Devices

Selected 0 Total 6  

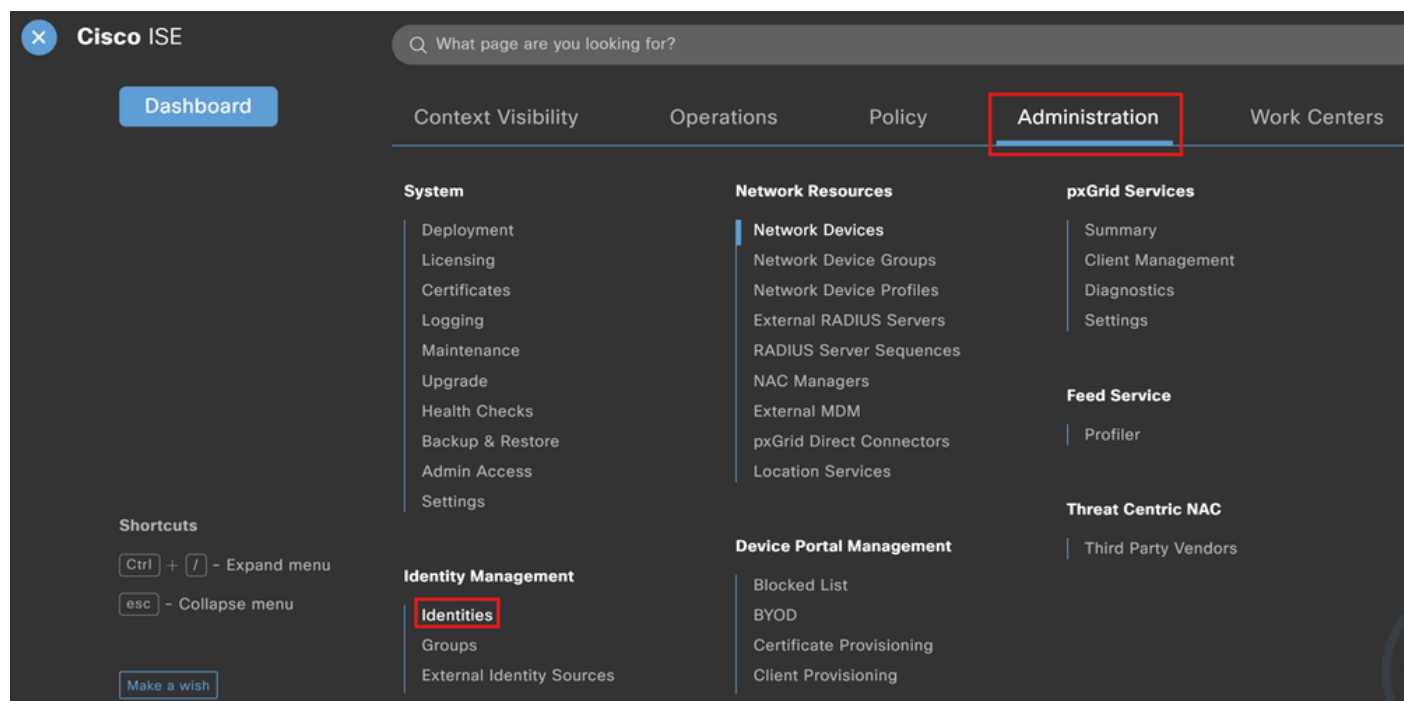
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

☐	Name	IP/Mask	Profile Name	Location	Type
☐	9800		 Cisco 	All Locations	All Device Types
☐	9800-2		 Cisco 	All Locations	All Device Types
☐	9800-40		 Cisco 	All Locations	All Device Types
☐	9800-WLC	192.0.2.20/32	 Cisco 	All Locations	All Device Types

Elenco dispositivi di rete

Creazione di un nuovo utente in ISE

Passaggio 1. Passare a Amministrazione > Gestione delle identità > Identità:



Cisco ISE

Dashboard Context Visibility Operations Policy **Administration** Work Centers

- System**
 - Deployment
 - Licensing
 - Certificates
 - Logging
 - Maintenance
 - Upgrade
 - Health Checks
 - Backup & Restore
 - Admin Access
 - Settings
- Network Resources**
 - Network Devices**
 - Network Device Groups
 - Network Device Profiles
 - External RADIUS Servers
 - RADIUS Server Sequences
 - NAC Managers
 - External MDM
 - pxGrid Direct Connectors
 - Location Services
 - Device Portal Management**
 - Blocked List
 - BYOD
 - Certificate Provisioning
 - Client Provisioning
- Identity Management**
 - Identities**
 - Groups
 - External Identity Sources
- pxGrid Services**
 - Summary
 - Client Management
 - Diagnostics
 - Settings
- Feed Service**
 - Profiler
- Threat Centric NAC**
 - Third Party Vendors

Shortcuts
Ctrl + **/** - Expand menu
esc - Collapse menu
Make a wish

Amministrazione ISE - Identità

Passaggio 2. Passare a Utenti e fare clic su +Aggiungi.

Users

Latest Manual Network Scan Res...

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#)

Status

Username ^

Description

First Name

Last Name

Em:

Aggiungi utente

Passaggio 3. Immettere il nome utente e la password per l'utente guest e fare clic su Sottometti.

[Network Access Users List](#) > [New Network Access User](#)

Network Access User

* Username

guest

Status

☒ Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

☒ With Expiration

Password will expire in 60 days

☐ Never Expires

Password

Re-Enter Password

* Login Password

[Generate Password](#)

i

Enable Password

[Generate Password](#)

i

Creazione di un nuovo utente in ISE

Passaggio 4. Passare a Amministrazione > Gestione delle identità > Identità > Utenti, per visualizzare l'elenco degli utenti.

Network Access Users

Edit

+ Add

Change Status

Import

Export

Delete

Duplicate

Status	Username	Descripti... ^	First Name	Last Name	Email Address	User Identity Groups	Admin
	Enabled	guest					

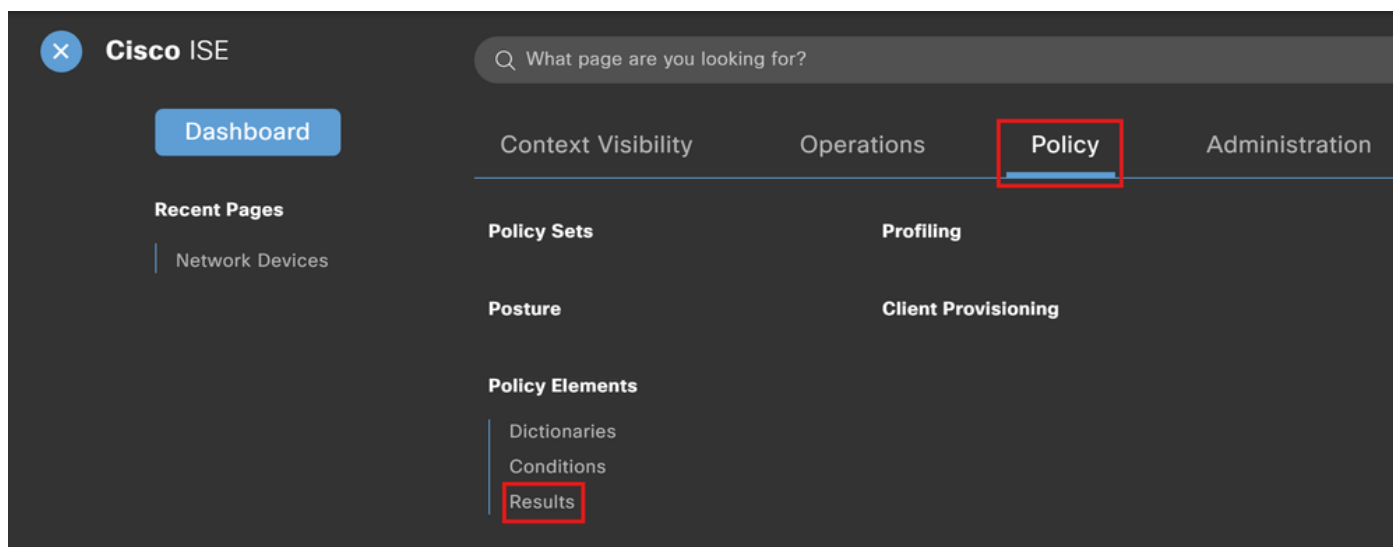
Elenco utenti di Accesso alla rete

Creazione del profilo di autorizzazione

Il profilo di policy è un insieme di parametri, come indirizzo MAC, credenziali, WLAN usata e altro, configurati per un client. È possibile configurare impostazioni specifiche come Virtual Local Area Network (VLAN), Access Control Lists (ACL), Uniform Resource Locator (URL) e così via.

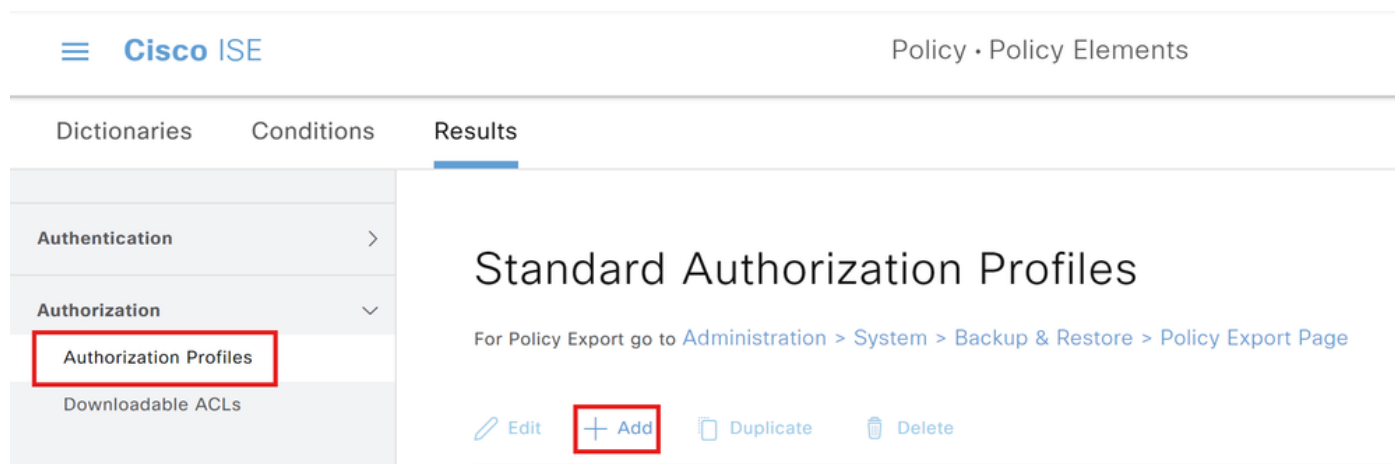
Questi passaggi mostrano come creare il profilo di autorizzazione necessario per reindirizzare il client al portale di autenticazione. Tenere presente che nelle versioni recenti di ISE esiste già un profilo di autorizzazione Cisco_Webauth. Qui è possibile modificarlo per cambiare il nome dell'ACL di reindirizzamento in modo che corrisponda a quello configurato nel WLC.

Passaggio 1. Passare a Criterio > Elementi criteri > Risultati.



Politica ISE - Risultati

Passaggio 2. Passare a Autorizzazione > Profili di autorizzazione. Per creare il profilo di autorizzazione, fare clic su +Aggiungi.



The screenshot shows the Cisco ISE interface. At the top, there's a navigation bar with 'Cisco ISE' and 'Policy • Policy Elements'. Below this, there are tabs for 'Dictionaries', 'Conditions', and 'Results'. The 'Results' tab is active. On the left, there's a sidebar with 'Authentication', 'Authorization', and 'Downloadable ACLs'. 'Authorization' is expanded, and 'Authorization Profiles' is highlighted with a red box. The main content area is titled 'Standard Authorization Profiles' and includes a link for 'Policy Export'. Below the title, there are buttons for 'Edit', '+ Add' (highlighted with a red box), 'Duplicate', and 'Delete'.

Aggiungi profilo di autorizzazione

Passaggio 3. Creare il profilo di autorizzazione LWA_EA_AUTHORIZATION. Il valore di Dettagli attributi deve essere Access Type=ACCESS_ACCEPT. Fare clic su Invia.

[Authorization Profiles](#) > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile 

Service Template ☐

Track Movement ☐ 

Agentless Posture ☐ 

Passive Identity Tracking ☐ 

Creazione del profilo di autorizzazione

Passaggio 4. Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione. È possibile visualizzare i profili di autorizzazione.

Dictionaries

Conditions

Results

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Standard Authorization Profiles

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

Edit

+ Add

Duplicate

Delete

☐	Name	Profile
☐	9800-admin-priv	Cisco
☐	9800-helpdeskuser-priv	Cisco
☐	AuthZ-Guest	Cisco
☐	AuthZ_Guest-Redirect	Cisco
☐	AuthZ_Mobile	Cisco
☐	Block_Wireless_Access	Cisco
☐	Cisco_IP_Phones	Cisco
☐	Cisco_Temporal_Onboard	Cisco
☐	Cisco_WebAuth	Cisco
☐	LWA_EA_AUTHORIZATION	Cisco

Elenco profili di autorizzazione

Configurazione della regola di autenticazione

Passaggio 1. Andare a Policy > Policy Sets (Policy > Set di policy).

Cisco ISE

Dashboard

Recent Pages

Results

Policy Sets

Identities

Network Devices

Q What page are you looking for?

Context Visibility

Operations

Policy

Administration

Policy Sets

Posture

Policy Elements

Dictionaries

Conditions

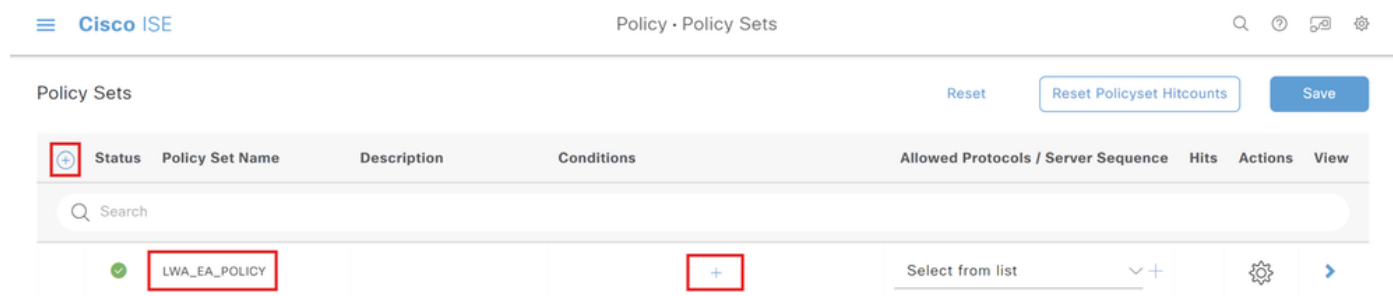
Results

Profiling

Client Provisioning

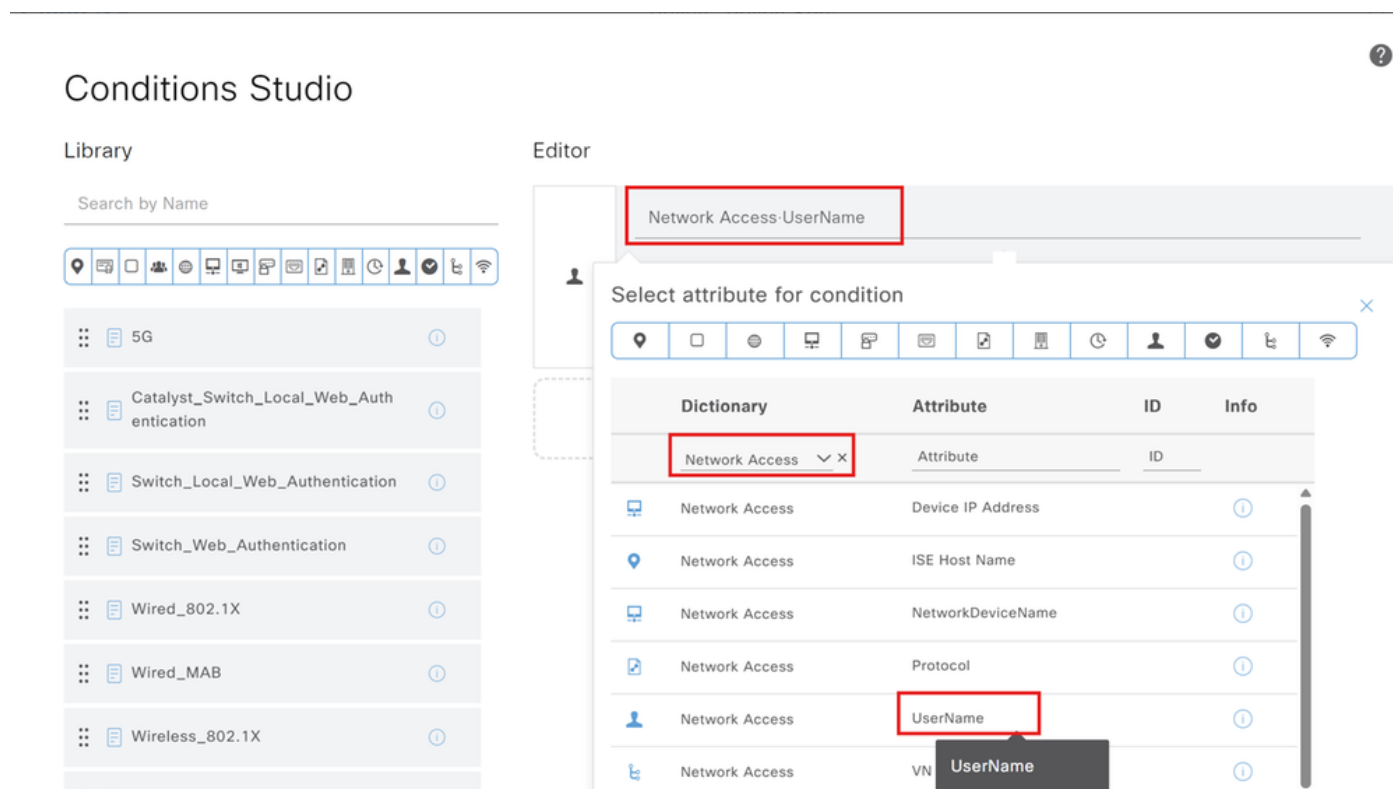
Policy ISE - Set di policy

Passaggio 2. Selezionare il segno + e digitare il nome del set di criteri LWA_EA_POLICY. Fare clic sulla colonna Condizioni.



Configurazione della regola di autenticazione

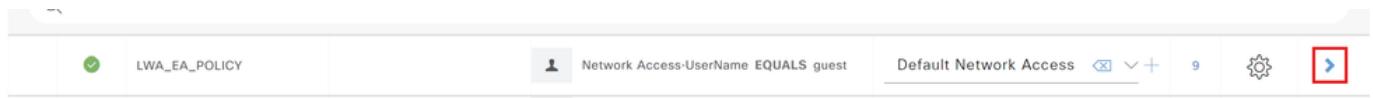
Passaggio 3. In Dizionario selezionare Accesso alla rete. In Attributo selezionare Nome utente.



Accesso alla rete per i dizionari

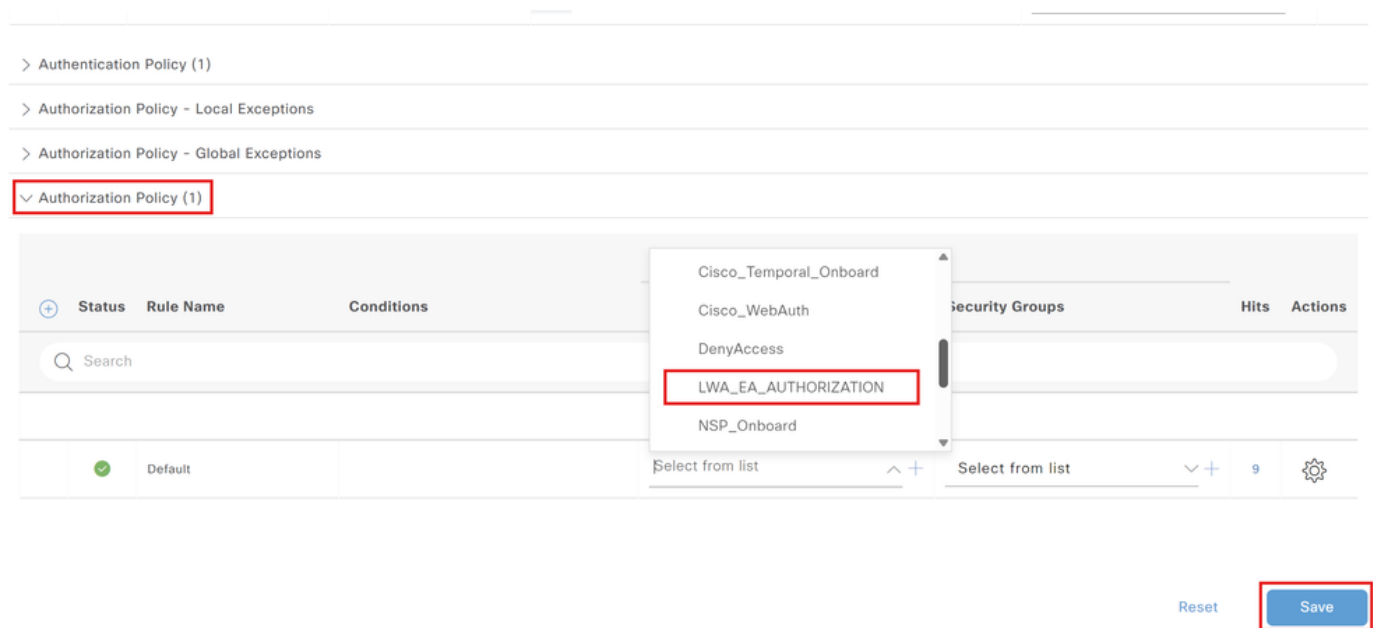
Passaggio 4. Impostare Uguale a e digitare guest nella casella di testo (il nome utente definito in Amministrazione > Gestione delle identità > Identità > Utenti). Per salvare le modifiche, fare clic su Salva.

Passaggio 1. Andare a Policy > Policy Sets (Policy > Set di policy). Fare clic sull'icona a forma di freccia del set di criteri creato.



Freccia

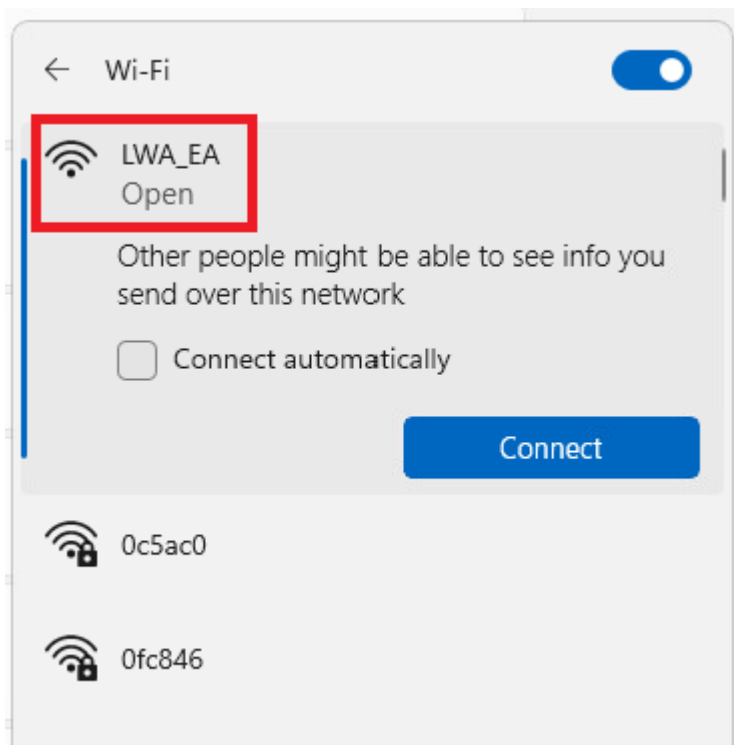
Passaggio 2. Nella stessa pagina di impostazione dei criteri, espandere Criteri di autorizzazione come mostrato nell'immagine. Nella colonna Profili eliminare DenyAccess e aggiungere LWA_EA_AUTHORIZATION. Per salvare le modifiche, fare clic su Salva.



Criteri di autorizzazione

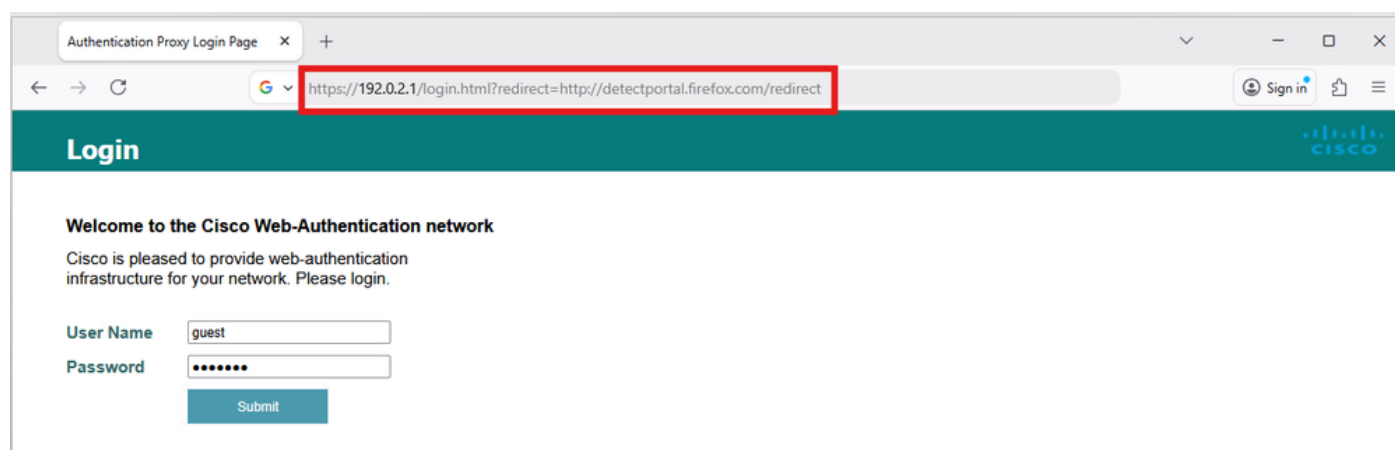
Connetti client guest

Passaggio 1. Sul computer/telefono, passare alle reti Wi-Fi, individuare il SSID LWA_EA e selezionare Connetti.



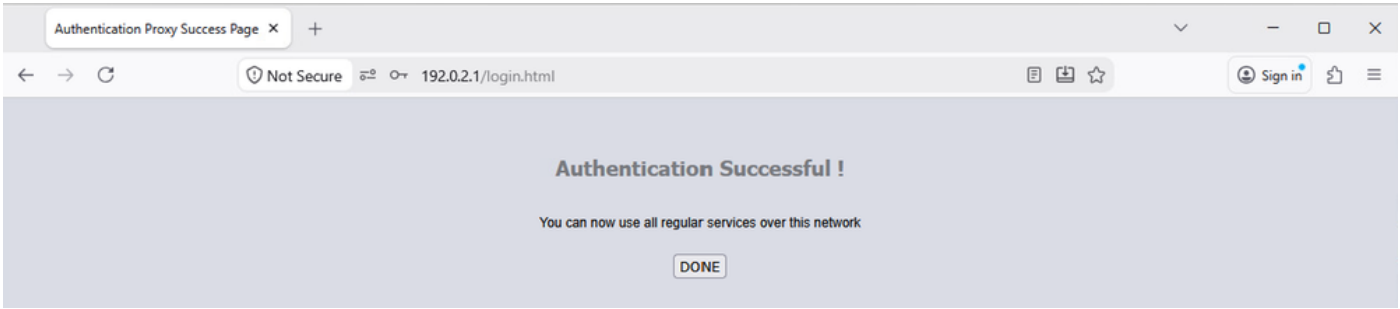
Connetti client guest

Passaggio 2. Viene visualizzata una finestra del browser, con la pagina di login. L'URL di reindirizzamento si trova nella casella URL ed è necessario digitare il Nome utente e la Password per accedere alla rete. Quindi selezionare Invia.



Pagina di accesso con URL di reindirizzamento

Se le credenziali sono corrette, viene visualizzata la pagina Autenticazione riuscita:



Pagina Autenticazione riuscita: Login

 **Nota:** L'URL presentato è stato fornito dal WLC. Contiene l'IP virtuale del WLC e il reindirizzamento per l'URL di prova di Windows Connect.

Passaggio 3. Passare a Operazioni > RADIUS > Live Log. È possibile visualizzare il dispositivo client autenticato, insieme ai relativi criteri di autenticazione e autorizzazione.

Cisco ISE

Operations - RADIUS

Live Logs

Live Sessions

Misconfigured Supplicants0

Misconfigured Network Devices0

RADIUS Drops0

Client Stopped Responding0

Repeat Counter2

RefreshNever

ShowLatest 20 records

WithinLast 3 hours

Reset Repeat Counts

Export To

Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
				Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Sep 18, 2026 10:00:26.1...			2	guest	08-BE-AC:...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...
Sep 18, 2026 09:54:58.3...				guest	08-BE-AC:...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...
Sep 18, 2026 09:41:04.9...				guest	08-BE-AC:...	Unknown	LWA_EA_POLICY >> Default	LWA_EA_POLICY >> Default	LWA_EA_AUTHORIZATION	10.14.32.109,...

Last Updated: Fri Sep 18 2026 11:00:54 GMT+0100 (Hora de verão da Europa Ocidental)

Records Shown: 3

Log dinamici Radius

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Show WLAN Summary

<#root>

9800WLC#show wlan summary

Number of WLANs: 1

ID Profile Name SSID Status 2.4GHz/5GHz Security

1 LWA_EA LWA_EA UP [open],[Web Auth]

9800WLC#

show wlan name LWA_EA

WLAN Profile Name : LWA_EA

=====

Identifier : 1

Description :

Network Name (SSID) : LWA_EA

Status : Enabled

Broadcast SSID : Enabled

Advertise-Apname : Disabled

Universal AP Admin : Disabled

(...)

Accounting list name :

802.1x authentication list name : Disabled

802.1x authorization list name : Disabled

Security

Web Based Authentication : Enabled

OWE Transition Mode : Disabled

Conditional Web Redirect : Disabled

Splash-Page Web Redirect : Disabled

Webauth On-mac-filter Failure : Disabled

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

(...)

Security-2.4GHz/5GHz

802.11 Authentication : Open System

Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OSEN : Disabled
PMF Support : Disabled
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)

Show Parameter Map Configuration

9800WLC#show running-config | section parameter-map type webauth global

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint TP-self-signed-123456
```

Show AAA Information

<#root>

9800WLC#show aaa method-lists authentication

authen queue=AAA_ML_AUTHEN_LOGIN

name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
(...)
```

9800WLC#show aaa method-lists authorization

```
author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
```

name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
author queue=AAA_ML_AUTHOR_CONN
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
(...)
```

9800WLC#show aaa servers

RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS

State: current UP, duration 8421s, previous duration 0s

Dead: total time 0s, count 0

Platform State from SMD: current UP, duration 8421s, previous duration 0s

SMD Platform Dead: total time 0s, count 0

Platform State from WNCN (0) : current UP

(...)

Risoluzione dei problemi

Problemi comuni

Di seguito sono riportate alcune guide per la risoluzione dei problemi di autenticazione Web, ad esempio:

- Gli utenti non possono eseguire l'autenticazione.
- Problemi relativi ai certificati.
- L'URL di reindirizzamento non funziona.
- Gli utenti guest non possono connettersi alla rete WLAN guest.
- Gli utenti non ottengono un indirizzo IP.
- Il reindirizzamento alla pagina di accesso dell'autenticazione Web non riesce.
- Dopo l'autenticazione, gli utenti guest non riescono ad accedere a Internet.

Queste guide descrivono in dettaglio i passaggi per la risoluzione dei problemi:

- [Risoluzione dei problemi comuni di autenticazione Web](#)
- [Altre situazioni da risolvere](#)

Debug condizionale, Radio Active Trace e Embedded Packet Capture

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). Per abilitare il debug condizionale, seguire la procedura descritta nella guida [Debug condizionale e traccia RadioActive](#).

È inoltre possibile raccogliere dati EPC (Embedded Packet Capture). EPC è una funzione di acquisizione dei pacchetti che consente di visualizzare i pacchetti destinati a, originati da e

passanti per i WLC Catalyst 9800, ossia DHCP, DNS, HTTP GET in LWA. Queste clip possono essere esportate per l'analisi offline con Wireshark. Per ulteriori informazioni, consultare il documento sull'[acquisizione integrata dei pacchetti](#).

Esempio di tentativo riuscito

Questo è l'output di RA_traces per un tentativo riuscito di identificare ciascuna delle fasi del processo di associazione/autenticazione, durante la connessione a un SSID guest con server RADIUS.

Associazione/autenticazione 802.11:

```
[client-orch-sm] [1762]: Nota: MAC: 08be.ac3f Associazione ricevuta. BSSID cc70.edcf.552f, WLAN LWA_EA, slot 1 AP 2ce3.8eb4, CW9172I-LAB
[client-orch-sm] [1762]: (debug) MAC: 08be.ac3f: ricevuta richiesta di associazione dot11. Elaborazione avviata, SSID: LWA_EA, profilo criteri: POLICY_PROFILE, nome punto di accesso: CW9172I-LAB, Indirizzo Mac Ap: 2ce3.8eb4BSSID MAC0000.0000.0000ID WLAN: 1RSSI: -49, SNR: 46
[stato-orch-client] [17062]: Nota: MAC: 08be.ac3f Transizione dello stato del client: S_CO_INIT -> S_CO_ASSOCIATING
[convalida11] [17062]: (info): MAC: 08be.ac3f Dot11 ie convalida le velocità di ext/supp. Convalida superata per tariffe supportate radio_type 2
[convalida11] [17062]: (info): MAC: 08be.ac3f WiFi diretto: Dot11 convalida IP2P IE. IP2P IE non presente.
[dot11] [17062]: (debug) MAC: 08be.ac3f dot11 invia risposta di associazione. Risposta associazione di frame con resp_status_code: 0
[dot11] [17062]: (debug) MAC: 08be.ac3f Dot11 Informazioni sulla capacità byte1 1, byte2: 11
[dot11-frame] [17062]: (info): MAC: 08be.ac3f WiFi diretto: ignorare la compilazione di Assoc Resp con P2P IE: Criteri diretti Wi-Fi disabilitati
[dot11] [17062]: (info): MAC: 08be.ac3f dot11 invia risposta di associazione. Invio risposta assoc di lunghezza: 130 con resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS
[dot11] [17062]: Nota: MAC: 08be.ac3f Associazione riuscita. RAID 1, roaming = False, WGB = False, 11r = False, 11w = False, roaming veloce = False
[dot11] [17062]: (info): MAC: 08be.ac3f DOT11 transizione di stato: S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [1762]: (debug) MAC: L'associazione di 08be.ac3f Station Dot11 ha esito positivo.
```

Processo di apprendimento IP:

```
[stato-orch-client] [17062]: Nota: MAC: 08be.ac3f Transizione dello stato del client: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [17062]: (info): MAC: 08be.ac3f Transizione dello stato di apprendimento IP: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: (info): MAC: 08be.ac3f Transizione dello stato dell'interfaccia di autenticazione client: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[client-iplearn] [17062]: Nota: MAC: 08be.ac3f Client IP info riuscito. Metodo: IP DHCP: 10.14.32.109
[client-iplearn] [17062]: (info): MAC: 08be.ac3f Transizione dello stato di apprendimento IP: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
[client-orch-sm] [1762]: (debug) MAC: 08be.ac3f Ha ricevuto una risposta di apprendimento IP. metodo: IPLEARN_METHOD_DHCP
```

Autenticazione di livello 3:

```
[client-orch-sm] [1762]: (debug) MAC: 08be.ac3f Autenticazione L3 attivata. stato = 0x0, Operazione riuscita
[stato-orch-client] [17062]: Nota: MAC: 08be.ac3f Transizione dello stato del client: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: Nota: MAC: Autenticazione L3 08be.ac3f avviata. LWA
```

[client-auth] [17062]: (info): MAC: 08be.ac3f Transizione dello stato dell'interfaccia di autenticazione client: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]GET ricevuto quando è in stato LOGIN

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Richiesta HTTP GET

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Parse GET, src [10.14.32.109] dst [10.107.221.82] url [<http://firefox.detect.portal/>]

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Lettura completa: parse_request restituito 8

[webauth-io] [17062] (info): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 LETTURA stato IO -> SCRITTURA

[webauth-io] [17062] (info): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO -> LETTURA

[webauth-io] [17062] (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO stato NEW -> READING

[webauth-io] [17062] (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Evento Read, Message ready

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]POST rcvd quando in stato LOGIN

Autenticazione di livello 3 completata. Spostare il client nello stato RUN:

[auth-mgr] [1762]: (info): [08be.ac3f:capwap_90000004] Ricevuto guest nome utente per il client 08be.ac3f

[auth-mgr] [1762]: (info): [08be.ac3f:capwap_90000004] ricezione notifica aggiunta/modifica gestione autenticazione per attr auth-domain(954)

[auth-mgr] [1762]: (info): [08be.ac3f:capwap_90000004] Metodo webauth che modifica lo stato da 'In esecuzione' a 'Autenticazione riuscita'

[auth-mgr] [1762]: (info): [08be.ac3f:capwap_90000004] Modifica dello stato del contesto da 'In esecuzione' a 'Autenticazione riuscita'

[auth-mgr] [1762]: (info): [08be.ac3f:capwap_90000004] ricezione notifica aggiunta/modifica auth mgr attr per il metodo attr(757)

[auth-mgr] [1762]: (info): [08be.ac3f:capwap_90000004] Generato evento AUTHZ_SUCCESS (1)

[auth-mgr] [1762]: (info): [08be.ac3f:capwap_90000004] Modifica dello stato del contesto da 'Autenticazione riuscita' a 'Autorizzazione riuscita'

[webauth-acl] [1762]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Applicazione dell'ACL di disconnessione IPv4 tramite SVM, nome: IP-Adm-V4-LOGOUT-ACL, priorità: 51, IIF-ID: 0

[webauth-sess] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Mappa-param utilizzata: globale

[webauth-state] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Mappa-param utilizzata: globale

[webauth-state] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Stato AUTHC_SUCCESS -> AUTHZ

[pagina-web] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Invio della pagina WebAuth riuscita

[webauth-io] [17062] (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO stato AUTHENTICATING -> SCRITTURA

[webauth-io] [17062] (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO -> FINE

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Remove IO ctx and close socket, id [99000029]

[client-auth] [17062]: Nota: MAC: Autenticazione L3 08be.ac3f riuscita. ACL:[]

[client-auth] [17062]: (info): MAC: 08be.ac3f Transizione dello stato dell'interfaccia di autenticazione client: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.48.39.243]56538/219 Remove IO ctx and close socket, id [D7000028]

[errmsg] [17062] (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Voce del nome utente (guest) unita al ssid (LWA_EA) per il dispositivo con MAC: 08be.ac3f
[aaa-attr-inf] [17062]: (info): [Attributo applicato: bsn-vlan-interface-name 0 "VLAN0039"]
[aaa-attr-inf] [17062]: (info): [Attributo applicato: timeout 0 1800 (0x708)]
[aaa-attr-inf] [17062]: (info): [Attributo applicato: url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]
[ewlc-qos-client] [17062]: (info): MAC: 08be.ac3f Gestore stato esecuzione QoS client
[rog-proxy-capwap] [1762]: (debug) Notifica stato di ESECUZIONE client gestito: 08be.ac3f
[stato-orch-client] [17062]: Nota: MAC: 08be.ac3f Transizione dello stato del client:
S_CO_L3_AUTH_IN_PROGRESS -> ESEGUI_CO

Informazioni correlate

- [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).