

Configurazione della verifica e della risoluzione dei problemi del guest cablato nel controller LAN wireless

Sommario

Introduzione

In questo documento viene descritto come configurare, verificare e risolvere i problemi relativi all'accesso guest cablato in 9800 e IRCM con autenticazione Web esterna.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

9800 WLC

AireOS WLC

Mobility Tunnel

ISE

Si presume che sia stato stabilito un tunnel di mobilità tra i due WLC prima di configurare l'accesso guest cablato.

Questo aspetto non rientra nell'ambito di questo esempio di configurazione. Per istruzioni dettagliate, fare riferimento al documento allegato intitolato [Configurazione delle topologie di mobilità su 9800](#)

Componenti usati

9800 WLC versione 17.12.1

5520 WLC versione 8.10.185.0

ISE versione 3.1.0.518

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Configurazione di Wired Guest su Catalyst 9800 ancorato a un altro Catalyst 9800

Esempio di rete



Topologia della rete

Configurazione su Foreign 9800 WLC

Configura mapping parametri Web

Passaggio 1: Passare a Configurazione > Sicurezza > Autenticazione Web, selezionare Globale, verificare l'indirizzo IP virtuale del controller e il mapping del trust point e verificare che il tipo sia impostato su webauth.

+ Add × Delete

Parameter Map Name

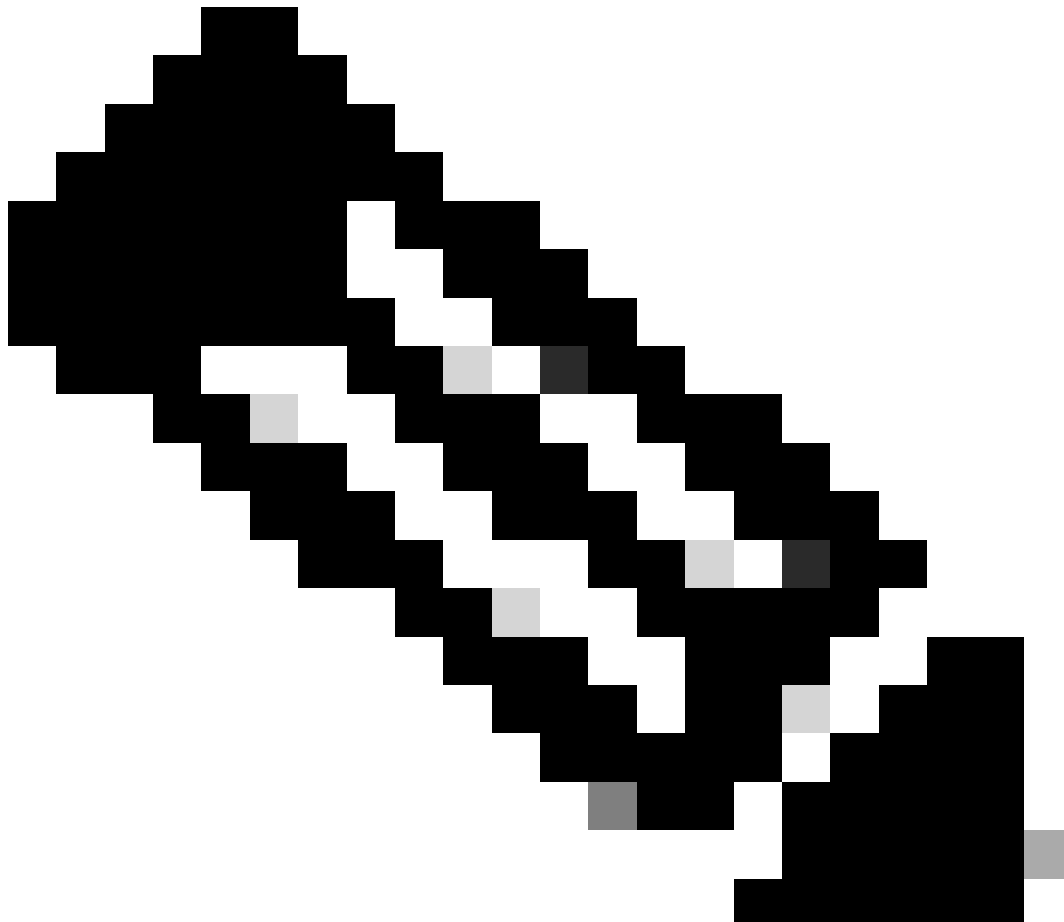
- global
- Web-Filter

1 10

General Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	XXXXXX:XX
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Mappa parametri globali



Nota: HTTP intercettazione autenticazione Web è un'impostazione facoltativa. Se è necessario il reindirizzamento HTTPS, è necessario abilitare l'opzione HTTPS di intercettazione autenticazione Web. Tuttavia, questa configurazione non è consigliata in quanto aumenta l'utilizzo della CPU.

Passaggio 2: nella scheda Avanzate, configurare l'URL della pagina Web esterna per il reindirizzamento del client. Impostare "Reindirizza URL per accesso" e "Reindirizza in caso di errore"; "Reindirizza in caso di esito positivo" è facoltativo. Dopo la configurazione, nel profilo Web Auth viene visualizzata un'anteprima dell'URL di reindirizzamento.

General **Advanced**

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

Scheda Avanzate

Configurazione dalla CLI

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable
```

trustpoint TP-self-signed-3915430211
webauth-http-enable

Nota: in questo scenario viene utilizzata la mappa dei parametri globale. Per configurare una mappa dei parametri Web personalizzata in base alle esigenze, selezionare Aggiungi e quindi impostare l'URL di reindirizzamento nella scheda Avanzate. Le impostazioni Trustpoint e IP virtuale vengono ereditate dal profilo globale.

Impostazioni AAA:

Fase 1. Creazione di un server Radius:

Selezionare Configurazione > Sicurezza > AAA, fare clic su "Aggiungi" nella sezione Server/Gruppo, quindi nella pagina "Crea server AAA Radius" immettere il nome del server, l'indirizzo IP e il segreto condiviso.

The screenshot displays the 'Create AAA Radius Server' configuration page. The breadcrumb navigation is 'Configuration > Security > AAA'. A '+ AAA Wizard' button is visible. The 'Servers / Groups' section is active, with a '+ Add' button highlighted in red. The 'Servers' tab is also highlighted in red. The configuration form includes the following fields:

- Name* (text input)
- Server Address* (text input with placeholder 'IPv4/IPv6/Hostname')
- PAC Key (checkbox, unchecked)
- Key Type (dropdown menu, 'Clear Text' selected)
- Key* (text input)
- Confirm Key* (text input)
- Auth Port (text input, '1812')
- Acct Port (text input, '1813')
- Server Timeout (seconds) (text input, '1-1000')
- Retry Count (text input, '0-100')
- Support for CoA (checkbox, checked, 'ENABLED')
- CoA Server Key Type (dropdown menu, 'Clear Text' selected)
- CoA Server Key (text input)
- Confirm CoA Server Key (text input)
- Automate Tester (checkbox, unchecked)

At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

Configurazione server Radius

Configurazione dalla CLI

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

Passaggio 2: Creare un gruppo di server RADIUS:

Selezionare "Aggiungi" nella sezione Gruppi di server per definire un gruppo di server e attivare o disattivare i server da includere nella configurazione del gruppo.

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

[Servers / Groups](#) [AAA Method List](#) [AAA Advanced](#)

[+ Add](#) [x Delete](#)

RADIUS

[Servers](#) [Server Groups](#)

Create AAA Radius Server Group

Name*	ISE-Group	! Name is required
Group Type	RADIUS	
MAC-Delimiter	none	
MAC-Filtering	none	
Dead-Time (mins)	5	
Load Balance	<input type="checkbox"/> DISABLED	
Source Interface VLAN ID	2074	

Available Servers

Assigned Servers

ISE-Auth

Configurazione dalla CLI

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2074
deadtime 5
```

Fase 3. Configurare l'elenco dei metodi AAA:

Passare alla scheda Elenco metodi AAA, selezionare Aggiungi in Autenticazione, definire un nome di elenco di metodi con Tipo come "accesso" e Tipo di gruppo come "Gruppo", quindi mappare il gruppo di server di autenticazione configurato nella sezione Gruppo di server assegnato.

The screenshot shows the Cisco configuration interface for AAA Method List. The breadcrumb navigation is Configuration > Security > AAA. The main menu includes Servers / Groups, AAA Method List (highlighted with a red box), and AAA Advanced. The left sidebar has Authentication (highlighted with a red box), Authorization, and Accounting. The main content area is titled 'Quick Setup: AAA Authentication' and contains the following fields:

- Method List Name*: ISE-List (highlighted with a red box)
- Type*: login (highlighted with a red box)
- Group Type: group (highlighted with a red box)
- Fallback to local:
- Available Server Groups: A list of server groups including undefined, Radius-Group, Test-group, test-group, undefined, and tacacs1.
- Assigned Server Groups: A list containing ISE-Group (highlighted with a red box).

Elenco dei metodi di autenticazione

Configurazione dalla CLI

```
aaa authentication login ISE-List group ISE-Group
```

Configura profilo criteri

Passaggio 1: Passare a Configurazione > Tag e profili > Criterio, assegnare un nome al nuovo profilo nella scheda Generale e abilitarlo utilizzando l'interruttore di stato.

Configuration > Tags & Profiles > Policy

+ Add × Delete Clone

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*	<input type="text" value="GuestLANPolicy"/>	WLAN Switching Policy	
Description	<input type="text" value="Enter Description"/>	Central Switching	<input checked="" type="checkbox"/> ENABLED
Status	<input checked="" type="checkbox"/> ENABLED	Central Authentication	<input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input checked="" type="checkbox"/> ENABLED
IP MAC Binding	<input checked="" type="checkbox"/> ENABLED	Flex NAT/PAT	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED		
CTS Policy			
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

Profilo criterio

Passaggio 2: Nella scheda Access Policies (Criteri di accesso), assegnare una vlan casuale quando il mapping della vlan è stato completato sul controller di ancoraggio. Nell'esempio, la vlan 1 è configurata

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 ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

Scheda Criteri di accesso

Passaggio 3: Nella scheda Mobility, impostare il controller di ancoraggio su Primary (1) e facoltativamente configurare i tunnel per la mobilità secondaria e terziaria per i requisiti di ridondanza

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 (3) Selected (1)

Anchor IP	Anchor Priority
 10.106.40.11 <input type="button" value="→"/>	 10.76.118.70 <input type="text" value="Primary (1)"/> ⓘ
 10.76.118.75 <input type="button" value="→"/>	
 10.76.118.74 <input type="button" value="→"/>	

Mappa della mobilità

Configurazione dalla CLI

```
wireless profile policy GuestLANPolicy
mobility anchor 10.76.118.70 priority 1
no shutdown
```

Configura profilo LAN guest

Passaggio 1: Passare a Configurazione > Wireless > LAN guest, selezionare Aggiungi, configurare un nome di profilo univoco, abilitare la VLAN cablata, immettere l'ID VLAN per gli utenti guest cablati e impostare lo stato del profilo su Abilitato.

General	Security
Profile Name*	Client Association Limit
Guest LAN ID*	Wired VLAN Status
mDNS Mode	Wired VLAN ID*
Status	

Guest-Profile

2000

1

ENABLE

Bridging

2024

ENABLE

Profilo LAN guest

Passaggio 2: nella scheda Sicurezza, abilitare Autenticazione Web, mappare la mappa dei parametri Autenticazione Web e selezionare il server Radius dall'elenco a discesa Autenticazione.

Edit Guest LAN Profile

General

Security

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List



Scheda Sicurezza LAN guest

Configurazione dalla CLI

```
guest-lan profile-name Guest-Profile 1 wired-vlan 2024
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

MAPPA LAN guest

Selezionare Configurazione > Wireless > LAN guest.

Nella sezione di configurazione Guest LAN MAP, selezionare Add e mappare il profilo della policy e il profilo della LAN guest

Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map: GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page 0 - 0 of 0 items	

Profile Name	Guest-Profile
Policy Name	GuestLANPolicy
<input type="button" value="Save"/>	
<input type="button" value="Cancel"/>	

MAPPA LAN guest

Configurazione dalla CLI

```
wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy
```

Configurazione su Anchor 9800 WLC

Configura mapping parametri Web

Passaggio 1: Passare a Configurazione > Sicurezza > Autenticazione Web, selezionare Globale, verificare l'indirizzo IP virtuale del controller e il mapping del trust point e verificare che il tipo sia impostato su webauth.

Configuration > Security > Web Auth

+ Add × Delete

Parameter Map Name

- global
- Web-Filter

1 10

Edit Web Auth Parameter

General Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	XXXXXX:XX
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Passaggio 2: nella scheda Avanzate, configurare l'URL della pagina Web esterna per il reindirizzamento del client. Impostare "Reindirizza URL per accesso" e "Reindirizza in caso di errore"; "Reindirizza in caso di esito positivo" è facoltativo.

Dopo la configurazione, nel profilo Web Auth viene visualizzata un'anteprima dell'URL di reindirizzamento.

General **Advanced**

i Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

Scheda Avanzate

Configurazione dalla CLI

```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 intercept-https-enable.
 trustpoint TP-self-signed-3915430211
 webauth-http-enable
```

Impostazioni AAA:

Fase 1. Creazione di un server Radius:

Selezionare Configurazione > Sicurezza > AAA, fare clic su Aggiungi nella sezione Server/Gruppo, quindi nella pagina "Crea server AAA Radius" immettere il nome del server, l'indirizzo IP e il segreto condiviso.

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Add' button is highlighted with a red box. The 'Servers' tab is also highlighted with a red box. The form contains the following fields and options:

- Name* (text input)
- Server Address* (text input, placeholder: IPv4/IPv6/Hostname)
- PAC Key (checkbox, unchecked)
- Key Type (dropdown menu, value: Clear Text)
- Key* (text input)
- Confirm Key* (text input)
- Auth Port (text input, value: 1812)
- Acct Port (text input, value: 1813)
- Server Timeout (seconds) (text input, value: 1-1000)
- Retry Count (text input, value: 0-100)
- Support for CoA (checkbox, checked, value: ENABLED)
- CoA Server Key Type (dropdown menu, value: Clear Text)
- CoA Server Key (text input)
- Confirm CoA Server Key (text input)
- Automate Tester (checkbox, unchecked)

Buttons: Cancel, Apply to Device

Configurazione server Radius

Configurazione dalla CLI

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

Passaggio 2: Creare un gruppo di server RADIUS:

Selezionare Aggiungi nella sezione Gruppi di server per definire un gruppo di server e attivare o disattivare i server da includere nella configurazione del gruppo.

Name*	ISE-Group
Group Type	RADIUS

MAC-Delimiter	none ▼
---------------	--------

MAC-Filtering	none ▼
---------------	--------

Dead-Time (mins)	5
------------------	---

Load Balance	<input type="checkbox"/> DISABLED
--------------	-----------------------------------

Source Interface VLAN ID	2081 ▼ 
--------------------------	--

Available Servers

Assigned Servers

--



ISE-Auth

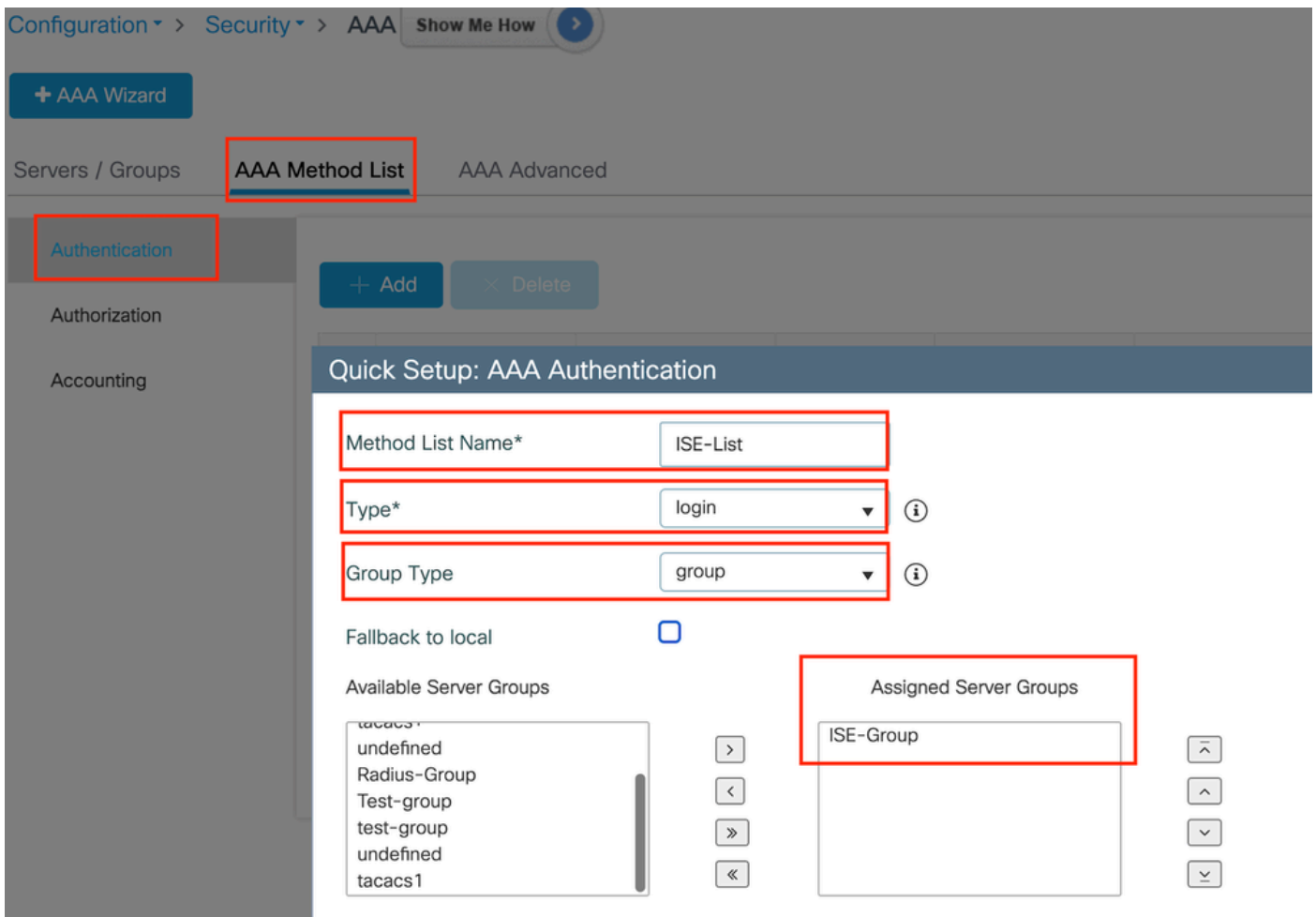
Gruppo raggio di ancoraggio

Configurazione dalla CLI

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2081
deadtime 5
```

Fase 3. Configurare l'elenco dei metodi AAA:

Passare alla scheda Elenco metodi AAA, selezionare Add in Authentication, definire un nome di elenco di metodi con Type come "login" e Group come "Group", quindi mappare il gruppo di server di autenticazione configurato nella sezione Assigned Server Group.



Elenco dei metodi di autenticazione

Configurazione dalla CLI

```
aaa authentication login ISE-List group ISE-Group
```

Configura profilo criteri

Passaggio 1: Passare a Configurazione > Tag e profili > Criteri, configurare il profilo dei criteri con lo stesso nome del controller esterno e abilitare il profilo.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*	GuestLANPolicy
Description	Enter Description
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
IP MAC Binding	ENABLED <input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED
CTS Policy	
Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

WLAN Switching Policy

Central Switching	ENABLED <input checked="" type="checkbox"/>
Central Authentication	ENABLED <input checked="" type="checkbox"/>
Central DHCP	ENABLED <input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/> DISABLED

Profilo criteri di ancoraggio

Passaggio 2: In Criteri di accesso, mappare la vlan del client cablato dall'elenco a discesa

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select

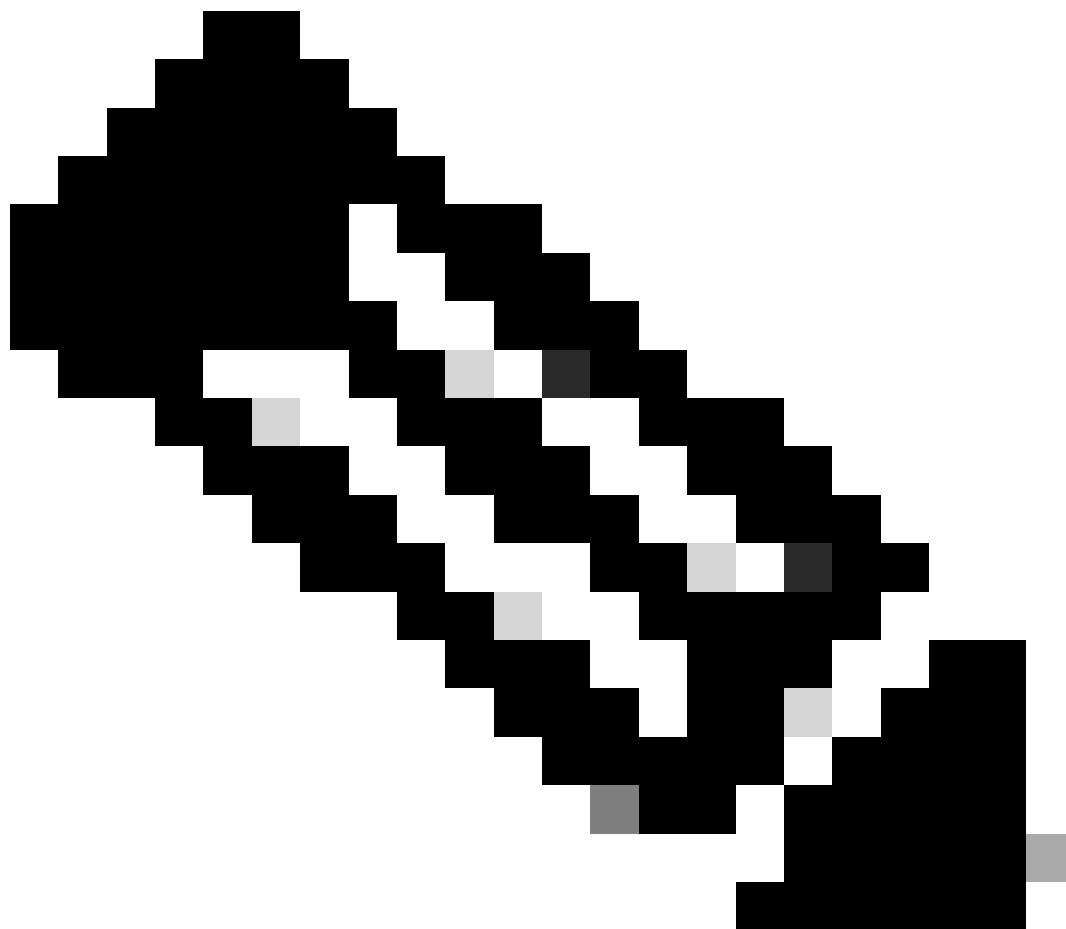


VLAN

VLAN/VLAN Group

VLAN2024





Nota: la configurazione del profilo dei criteri deve corrispondere sui controller esterno e di ancoraggio, ad eccezione della VLAN.

Passo 3: sotto la scheda Mobilità, casella di controllo Esporta ancoraggio.

Mobility Anchors

Export Anchor



Static IP Mobility



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 (2)

Selected (0)

Anchor IP

Anchor IP

Anchor IP



Nota: questa configurazione designa il controller WLC (Wireless LAN Controller) 9800 come WLC di ancoraggio per qualsiasi WLAN associata al profilo criteri specificato. Quando un WLC esterno 9800 reindirizza i client al WLC di ancoraggio, fornisce i dettagli sulla WLAN e sul profilo delle policy assegnato al client. In questo modo il WLC di ancoraggio può applicare il Profilo criteri locale appropriato in base alle informazioni ricevute.

Configurazione dalla CLI

```
wireless profile policy GuestLANPolicy
  mobility anchor
  vlan VLAN2024
  no shutdown
```

Configura profilo LAN guest

Fase 1. Passare a Configurazione > Wireless > LAN guest, quindi selezionare Aggiungi per creare e configurare il profilo LAN guest. Verificare che il nome del profilo corrisponda a quello del controller esterno. Notare che la VLAN cablata deve essere disabilitata sul controller di ancoraggio.

Configuration > Wireless > Guest LAN

> Guest LAN Configuration

+ Add × Delete

Add Guest LAN Profile

General Security

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	ENABLE <input checked="" type="checkbox"/>		

Profilo LAN guest

Passaggio 2: nelle impostazioni di protezione, abilitare Web Auth, quindi configurare la mappa dei parametri Web Auth e l'elenco di autenticazione.

Edit Guest LAN Profile

General

Security

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

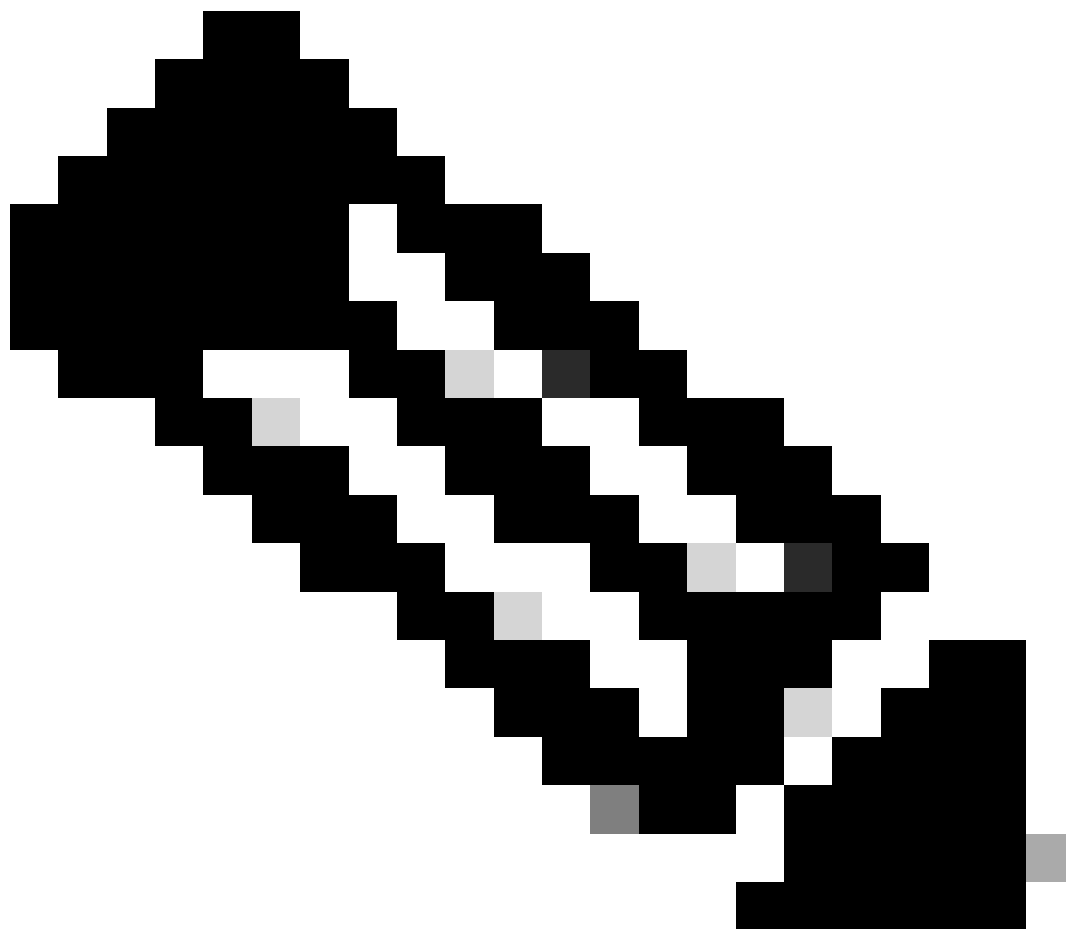
global



Authentication List

ISE-List





Nota: la configurazione del profilo LAN guest deve essere identica tra i controller esterno e di ancoraggio, ad eccezione dello stato della VLAN cablata

Configurazione dalla CLI

```
guest-lan profile-name Guest-Profile 1
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

MAPPA LAN guest

Fase 1. Passare a Configurazione > Wireless > LAN guest. Nella sezione Configurazione mappe LAN guest, selezionare Add e mappare il profilo criteri al profilo LAN guest.

> Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map : GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page 0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save Cancel

MAPPA LAN guest

wireless guest-lan map GuestMap
guest-lan Guest-Profile policy GuestLANPolicy

Configurazione di Wired Guest su Catalyst 9800 ancorato al controller AireOS 5520



Topologia della rete

Configurazione su Foreign 9800 WLC

Configura mapping parametri Web

Passo 1: passare a Configurazione > Sicurezza > Autenticazione Web e selezionare Globale. Verificare che l'indirizzo IP virtuale del controller e il trust point siano mappati correttamente nel profilo, con il tipo impostato su webauth.

General	Advanced		
Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3... ▼
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth ▼	Virtual IPv6 Address	x::x::x::x
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

Mappa parametri Web

Passaggio 2: nella scheda Avanzate, specificare l'URL della pagina Web esterna a cui reindirizzare i client. Configurare l'URL di reindirizzamento per Login e Redirect On-Failure. L'impostazione Reindirizza se riuscito è una configurazione facoltativa.

Preview of the Redirect URL:

```
http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>
```

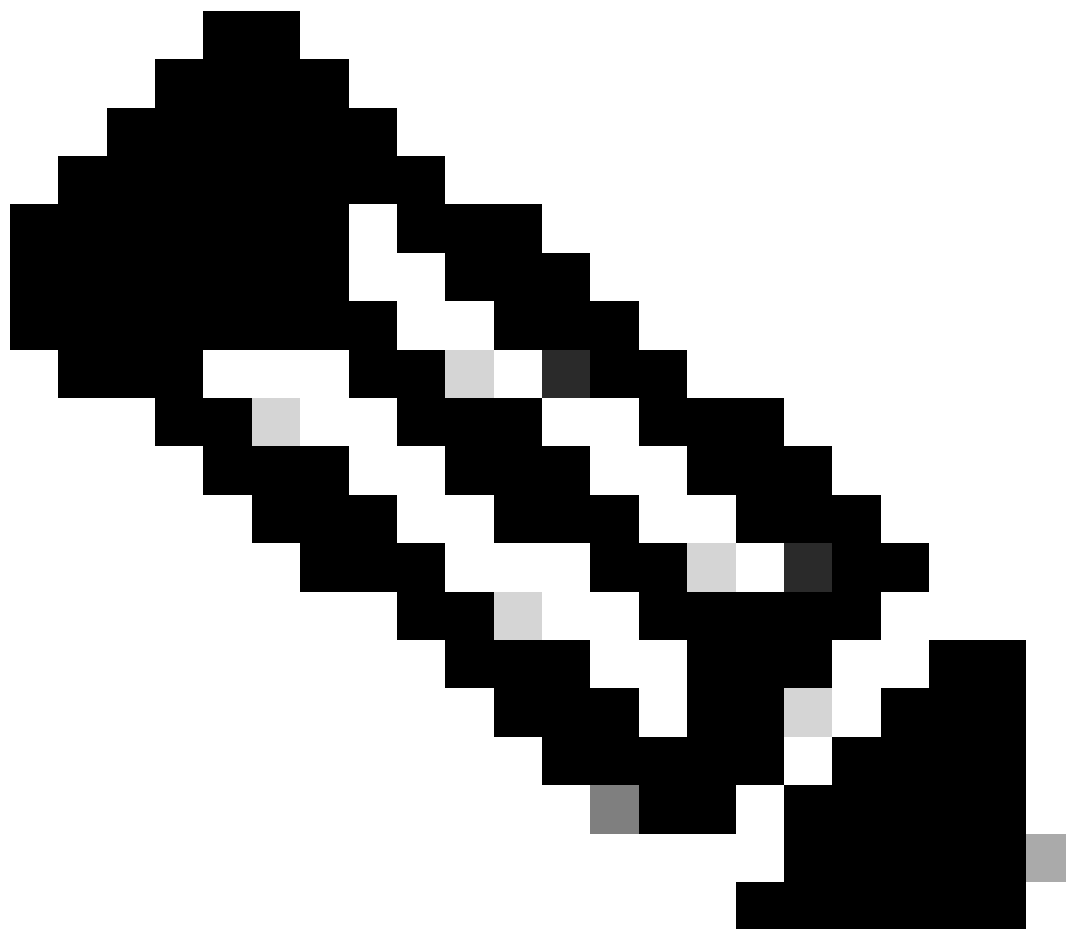
Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X::X"/>

Scheda Avanzate

Configurazione dalla CLI

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Nota: per la configurazione AAA, fare riferimento ai dettagli di configurazione forniti nella sezione "" per il WLC esterno di 9800.

Configura profilo criteri

Fase 1. Passare a Configurazione > Tag e profili > Criterio. Selezionare Aggiungi, e nella scheda Generale, fornire un nome per il profilo e abilitare l'interruttore di stato.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Guest

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Profilo criteri

Fase 2. Nella scheda Access Policies (Criteri di accesso), assegnare una VLAN casuale.

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 ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

Criteri di accesso

Passaggio 3: nella scheda Mobility, attivare il controller di ancoraggio e impostarne la priorità su Primary (1)

Mobility Anchors

Export Anchor



Static IP Mobility



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)



Anchor IP

 10.76.6.156 

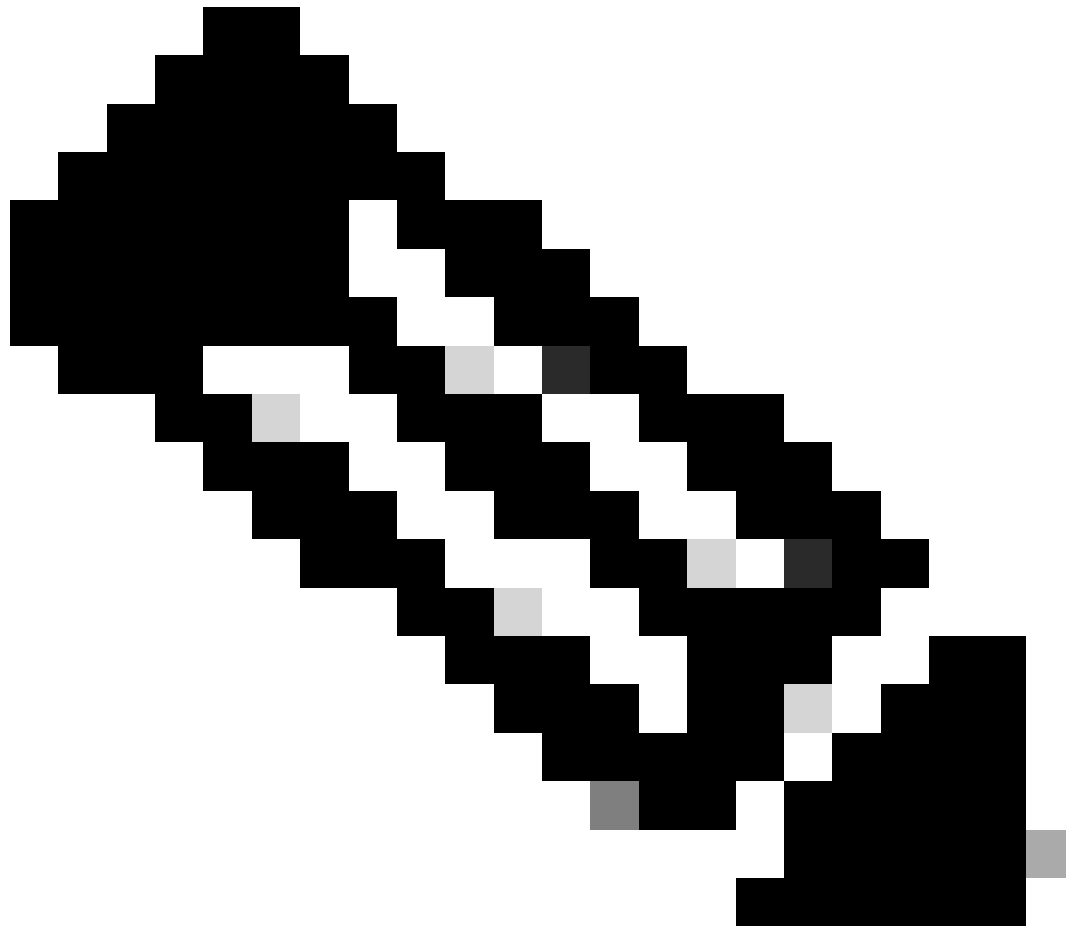
Selected (1)

Anchor IP

Anchor Priority

 10.76.118.74	Primary (1) 
--	---

Scheda Mobilità



Nota: il profilo Policy del WLC esterno 9800 deve corrispondere al profilo LAN guest dello switch 5520 Anchor WLC, ad eccezione della configurazione vlan

Configurazione dalla CLI

```
wireless profile policy Guest
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor 10.76.118.74 priority 1
no shutdown
```

Configura profilo LAN guest

Fase 1. Passare a Configurazione > Wireless > LAN guest e selezionare Add. Configurare un

nome di profilo univoco e abilitare la VLAN cablata, specificando l'ID VLAN dedicato agli utenti guest cablati. Infine, lo stato del profilo viene impostato su Abilitato (Enabled).

General

Security

Profile Name*	Guest	Client Association Limit	2000
Guest LAN ID*	2	Wired VLAN Status	ENABLE <input checked="" type="checkbox"/>
mDNS Mode	Bridging	Wired VLAN ID*	11
Status	ENABLE <input checked="" type="checkbox"/>		

Criteri LAN guest

Passaggio 2: nella scheda Sicurezza, abilitare Web Auth, mappare la mappa dei parametri Web Auth e selezionare il server RADIUS dall'elenco a discesa Autenticazione.

General

Security

Layer3

Web Auth

ENABLE

Web Auth Parameter Map

global

Authentication List

ISE-List

Scheda Protezione



Nota: il nome del profilo LAN guest deve essere lo stesso per il controller esterno 9800 e il controller di ancoraggio 5520

Configurazione dalla CLI

```
guest-lan profile-name Guest 2 wired-vlan 11
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

MAPPA LAN guest

Fase 1. Passare a Configurazione > Wireless > LAN guest. Nella sezione di configurazione Guest LAN MAP, selezionare Add (Aggiungi) e mappare il profilo criteri al profilo LAN guest.

Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map : GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page 0 - 0 of 0 items

Profile Name: Guest
Policy Name: Guest

Save Cancel

MAPPA LAN guest

Configurazione dalla CLI

```
wireless guest-lan map GuestMap  
guest-lan Guest policy Guest
```

Configurazione su Anchor 5520 WLC

Configura autenticazione Web

Passaggio 1: Passare a Protezione > Web Auth > Pagina di login Web. Impostare il tipo di autenticazione Web su Esterna (reindirizzamento su server esterno) e configurare l'URL di autenticazione Web esterno. L'opzione Reindirizza URL dopo l'accesso è facoltativa e può essere configurata se i client devono essere reindirizzati a una pagina dedicata dopo l'autenticazione.

Security > Web Login Page

Web Authentication Type: External (Redirect to external server)

Redirect URL after login: http://10.127.196.171/webauth/logout.html

Login Success Page Type: None

External Webauth URL: http://10.127.196.171/webauth/login.html

QrCode Scanning Bypass Timer: 0

QrCode Scanning Bypass Count: 0

Web Auth

Impostazioni autenticazione Web

Impostazioni AAA:

Fase 1. Configurare il server RADIUS

Selezionare Protezione > Raggio > Autenticazione > Nuovo.



Server Radius

Passaggio 2: configurare l'indirizzo IP e il segreto condiviso del server RADIUS sul controller. Impostare lo stato del server su Abilitato e selezionare la casella di controllo Utente in rete.

RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Configurazione server

Configura elenco di controllo di accesso

Passo 1: passare a Sicurezza > Lista di controllo di accesso e selezionare Nuovo. Creare un ACL

di preautenticazione che autorizzi il traffico verso il DNS e il server Web esterno.

The screenshot shows the Cisco ISE Security configuration page. The 'SECURITY' tab is highlighted in the top navigation bar. The left sidebar shows the 'Access Control Lists' menu item highlighted. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for an 'Access List Name' of 'Pre-Auth_ACL'. The 'Deny Counters' are set to 0. Below this is a table of access list entries:

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	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Elenco di accesso per autorizzare il traffico verso il server Web

Configura profilo LAN guest

Passaggio 1: Passare a WLAN > selezionare Crea nuovo.

Selezionare Type come Guest LAN e configurare lo stesso nome del profilo dei criteri del controller esterno 9800.

The screenshot shows the Cisco ISE WLANs configuration page. The 'WLANs' tab is highlighted in the top navigation bar. The 'Current Filter' is set to 'None'. A 'Create New' button with a dropdown arrow and a 'Go' button are highlighted with a red box. Below this is a table with columns: 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'.

Crea LAN guest

The screenshot shows the Cisco ISE WLANs configuration page in the 'New' form. The 'Type' dropdown is set to 'Guest LAN' and is highlighted with a red box. The 'Profile Name' field contains 'Guest' and the 'ID' dropdown is set to '2'. The 'Apply' button is highlighted with a red box.

Profilo LAN guest

Fase 2. Mappare le interfacce in entrata e in uscita sul profilo LAN guest.

In questo caso, l'interfaccia in ingresso è nessuna, in quanto è il tunnel EoIP del controller esterno.

L'interfaccia in uscita è la VLAN a cui il client cablato si connette fisicamente.

General **Security** **QoS** **Advanced**

Profile Name

Type Guest LAN

Status Enabled

Security Policies **Web-Auth**
(Modifications done under security tab will appear after applying the changes.)

Ingress Interface

Egress Interface

NAS-ID

Profilo LAN guest

Passaggio 3: nella scheda Sicurezza, selezionare Sicurezza di layer 3 come Autenticazione Web e mappare l'ACL di preautenticazione.

WLANs > Edit 'Guest'

General **Security** **QoS** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Layer 3 Security

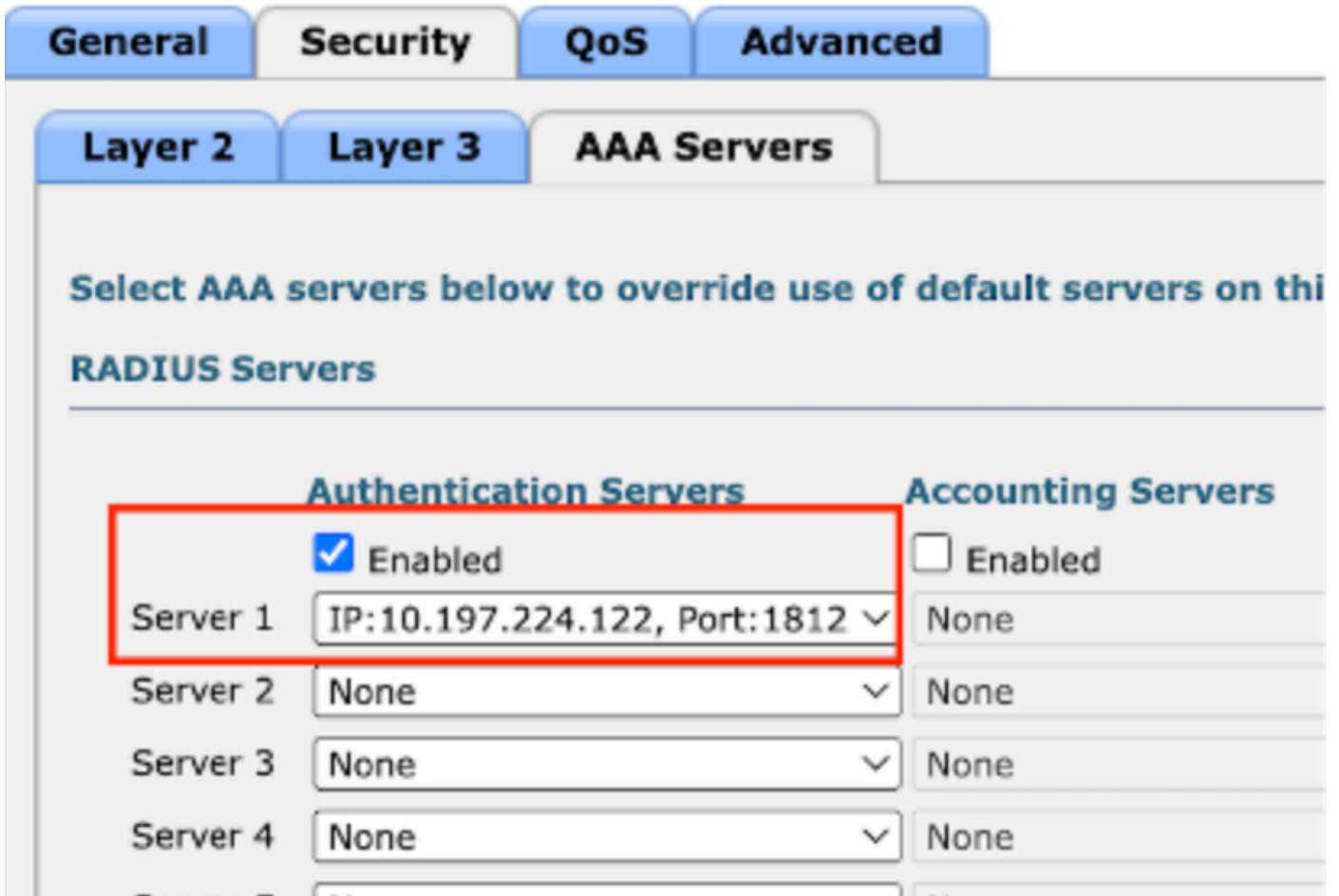
Preauthentication ACL IPv4 IPv6

Override Global Config²⁰ Enable

Scheda Sicurezza LAN guest

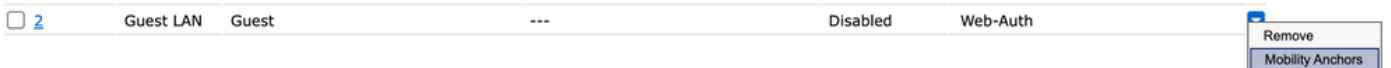
Passaggio 4: Passare a Sicurezza > Server AAA.

Selezionare l'elenco a discesa e mappare il server radius al profilo LAN guest.

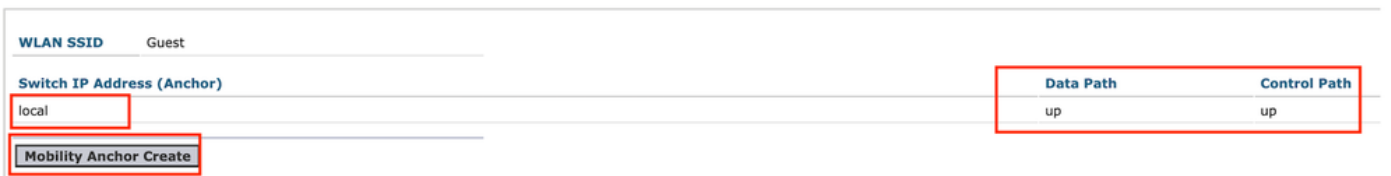


Mappare il server radius al profilo LAN guest

Fase 5. Passare alla WLAN. Posizionare il puntatore del mouse sull'icona a discesa del profilo LAN guest e selezionare Mobility Anchors.



Passaggio 6: selezionare Creazione ancoraggio di mobilità per configurare il controller come ancoraggio di esportazione per questo profilo LAN guest.



Creazione ancoraggio di mobilità

Configurazione di Wired Guest su AireOS 5520 ancorato a Catalyst 9800



Topologia della rete

Configurazione su router esterno 5520 WLC

Configurazione interfaccia controller

Passo 1: passare a Controller > Interfacce > Nuovo. Configurare un nome di interfaccia, un ID VLAN e abilitare la LAN guest.

Il guest cablato richiede due interfacce dinamiche.

Creare innanzitutto un'interfaccia dinamica di layer 2 e designarla come LAN guest. Questa interfaccia funge da interfaccia in entrata per la LAN guest, in cui i client cablati si connettono fisicamente.

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANA'. The left sidebar lists various configuration categories, with 'Interfaces' highlighted in red. The main content area is titled 'Interfaces > Edit' and is divided into several sections:

- General Information:** Interface Name is 'wired-guest' (highlighted in red), and MAC Address is 'a0:e0:af:32:d9:ba'.
- Configuration:** 'Guest Lan' is checked (highlighted in red), and NAS-ID is 'none'.
- Physical Information:** Port Number is '1', Backup Port is '0', and Active Port is '1'.
- Interface Address:** VLAN Identifier is '2020' (highlighted in red), DHCP Proxy Mode is 'Global', and 'Enable DHCP Option 82' is unchecked.

Interfaccia in ingresso

Passo 2: passare a Controller > Interfacce > Nuovo. Configurare un nome di interfaccia, ossia l'ID VLAN.

La seconda interfaccia dinamica deve essere un'interfaccia di layer 3 sul controller. I client cablati ricevono l'indirizzo IP da questa subnet vlan. Questa interfaccia funge da interfaccia in uscita per il profilo LAN guest.

Controller

- General
- Icons
- Inventory
- Interfaces**
- Interface Groups
- Multicast
- ▶ Network Routes
- ▶ Fabric Configuration
- ▶ Redundancy
- ▶ Mobility Management
- Ports
- ▶ NTP
- ▶ CDP
- ▶ PMIPv6
- ▶ Tunneling
- ▶ IPv6
- ▶ mDNS
- ▶ Advanced
- Lawful Interception

Interfaces > Edit

General Information

Interface Name	vlan2024
MAC Address	a0:e0:af:32:d9:ba

Configuration

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	none

Physical Information

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address

VLAN Identifier	2024
IP Address	10.105.211.85
Netmask	255.255.255.128
Gateway	10.105.211.1

Interfaccia in uscita

Configurazione porta switch

Gli utenti guest cablati si connettono allo switch del livello di accesso. Queste porte designate devono essere configurate con la VLAN in cui è abilitata la LAN guest sul controller

Configurazione porta switch livello di accesso

interfaccia gigabit Ethernet <x/x/x>

descrizione Wired Guest Access

switchport access vlan 2020

accesso in modalità switchport

fine

Configurazione porta uplink del controller esterno

interfaccia TenGigabit Ethernet<x/x/x>

descrizione Porta trunk su WLC esterno

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081.2020

fine

Configurazione porta uplink controller di ancoraggio

interfaccia TenGigabit Ethernet<x/x/x>

descrizione Porta trunk per il WLC di ancoraggio

switchport mode trunk

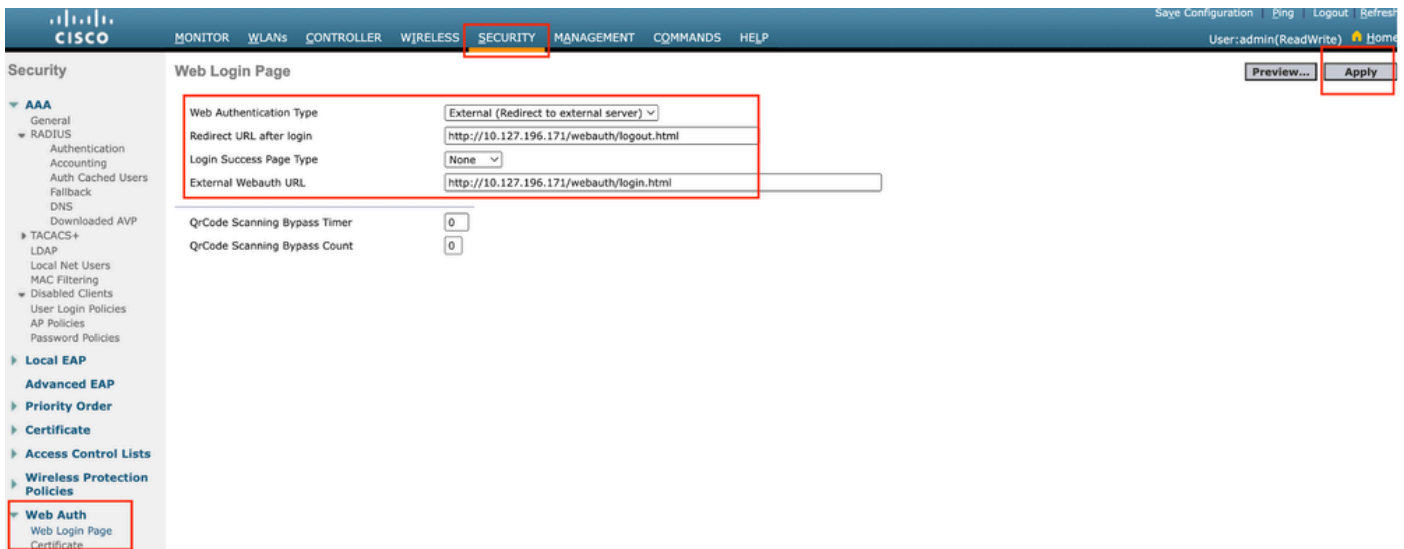
switchport trunk native vlan 2081

switchport trunk allowed vlan 2081.2024

fine

Configura autenticazione Web

Passaggio 1: Passare a Protezione > Web Auth > Pagina di login Web. Impostare il tipo di autenticazione Web su Esterna (reindirizzamento su server esterno) e configurare l'URL di autenticazione Web esterno. L'opzione Reindirizza URL dopo l'accesso è facoltativa e può essere configurata se i client devono essere reindirizzati a una pagina dedicata dopo l'autenticazione.

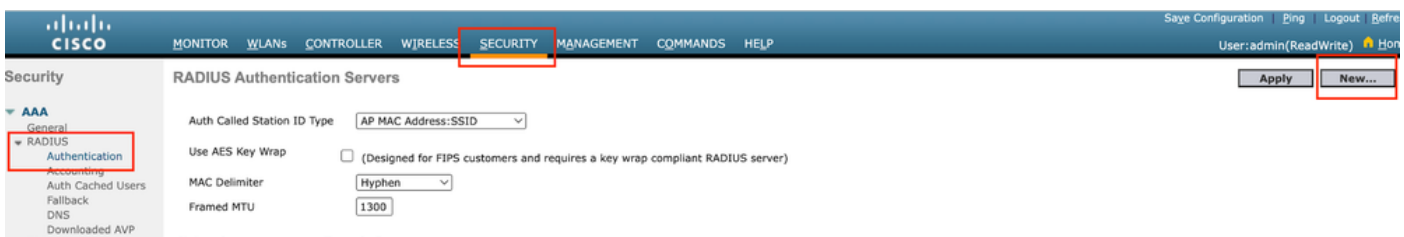


Impostazioni autenticazione Web

Impostazioni AAA:

Fase 1. Configurare il server RADIUS

Selezionare Protezione > Raggio > Autenticazione > Nuovo.



Server Radius

Passaggio 2: configurare l'indirizzo IP e il segreto condiviso del server RADIUS sul controller. Impostare lo stato del server su Abilitato e selezionare la casella di controllo Utente in rete.

RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Configurazione server

Configura elenco di controllo di accesso

Passo 1: passare a Sicurezza > Lista di controllo di accesso e selezionare Nuovo. Creare un ACL

di preautenticazione che autorizzi il traffico verso il DNS e il server Web esterno.

The screenshot shows the Cisco Meraki Security configuration page. The 'SECURITY' tab is highlighted in the top navigation bar. On the left sidebar, 'Access Control Lists' is selected. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for an 'Access List Name' of 'Pre-Auth_ACL'. The 'Deny Counters' are set to 0. Below this is a table of rules:

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	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Elenco di accesso per autorizzare il traffico verso il server Web

Configura profilo LAN guest

Fase 1. Passare a WLAN > Crea nuovo > Vai.

The screenshot shows the Cisco Meraki WLANs configuration page. The 'WLANs' tab is highlighted in the top navigation bar. Below the navigation bar, there is a 'Current Filter: None' section with links for '[Change Filter]' and '[Clear Filter]'. On the right side, there is a 'Create New' button with a dropdown arrow and a 'Go' button next to it.

Profilo LAN guest

Selezionare Tipo come LAN guest e configurare un nome di profilo. È necessario configurare lo stesso nome sul profilo criteri e sul profilo LAN guest del controller di ancoraggio 9800.

WLANs > New

Type

Guest LAN

Profile Name

Guest-Profile

ID

3

Profilo LAN guest

Fase 2. Nella scheda General (Generale), mappare l'interfaccia in entrata e in uscita sul profilo LAN guest.

L'interfaccia in ingresso è la vlan a cui si connettono fisicamente i client cablati.

L'interfaccia in uscita è la subnet vlan richiesta dai client per l'indirizzo IP.

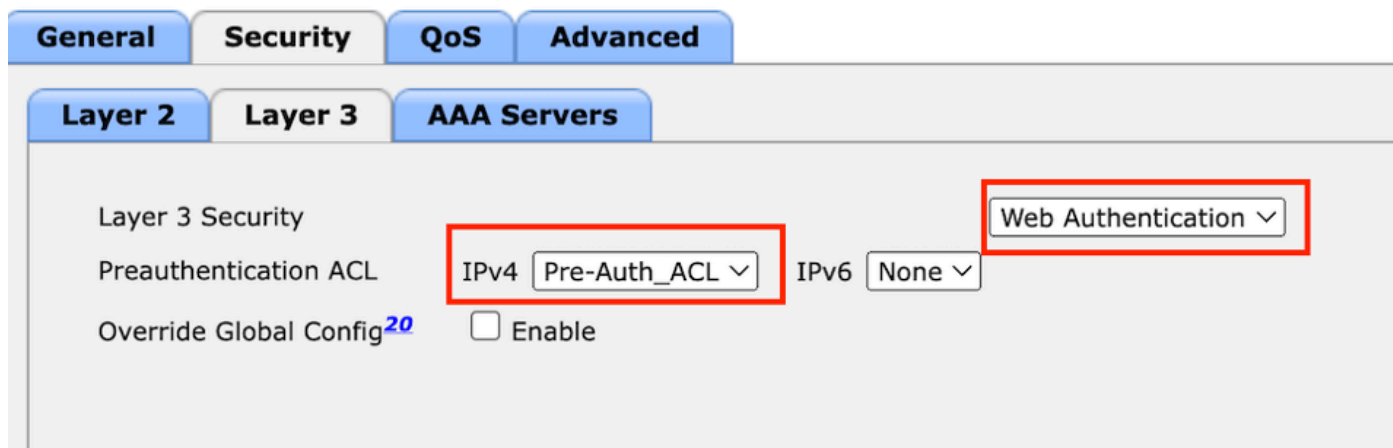
General	Security	QoS	Advanced
Profile Name	Guest-Profile		
Type	Guest LAN		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	Web-Auth (Modifications done under security tab will appear after applying th		
Ingress Interface	wired-guest		
Egress Interface	vlan2024		
NAS-ID	none		

Profilo LAN guest

Passaggio 3: Passare a Sicurezza > Layer 3.

Selezionare Sicurezza di livello 3 come Autenticazione Web ed eseguire il mapping dell'ACL di

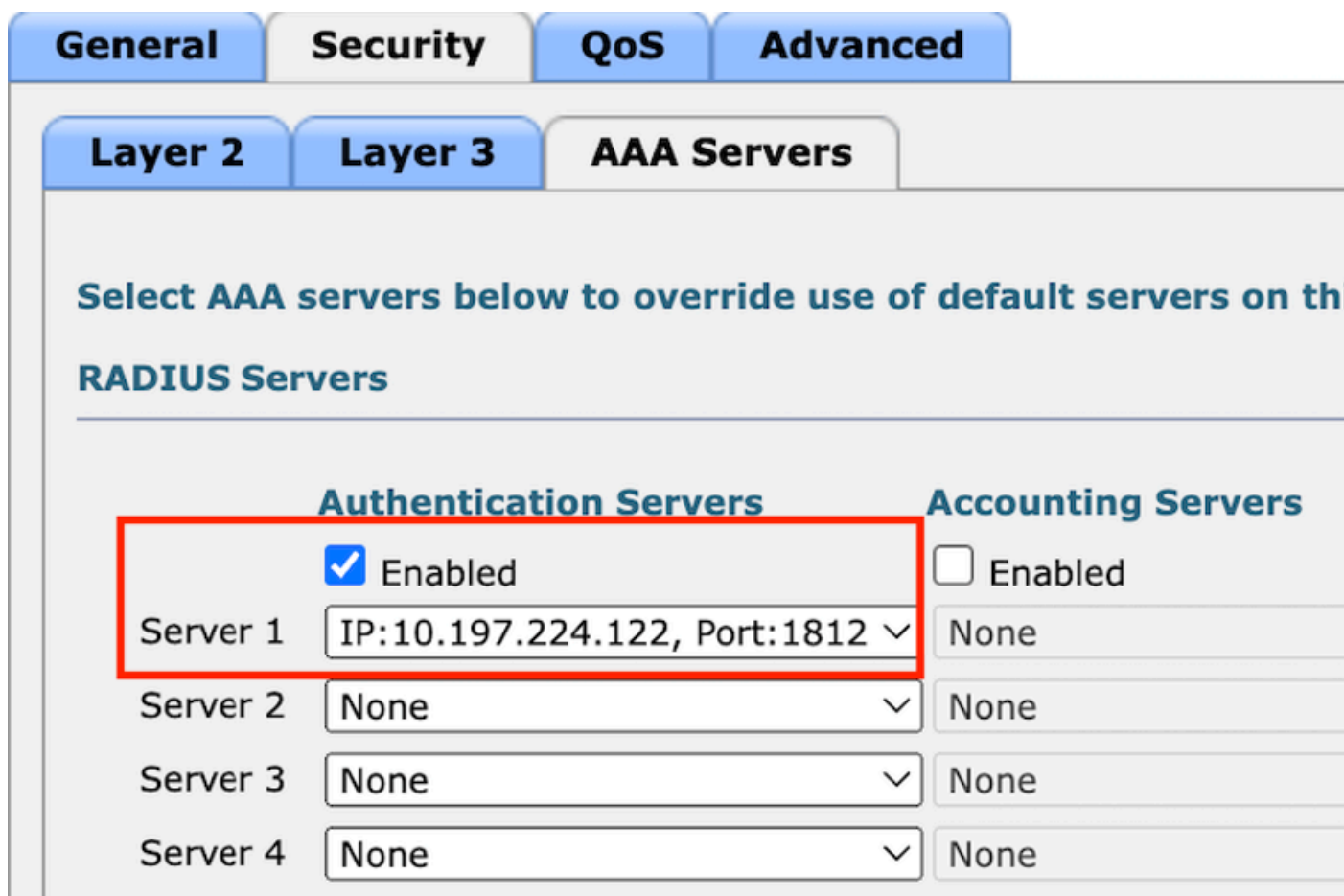
preautenticazione.



Scheda Protezione di livello 3

Fase 4:

Nella scheda Server AAA, mappare il server Radius e selezionare la casella di controllo Abilitato.



Mappatura dei server radius al profilo LAN guest

Fase 5. Passare alla pagina WLAN e passare il mouse sull'icona a discesa del profilo LAN guest e selezionare Mobility Anchors.

General

Advanced

Parameter-map Name Maximum HTTP connections Init-State Timeout(secs) Type Captive Bypass Portal Disable Success Window Disable Logout Window Disable Cisco Logo Sleeping Client Status Sleeping Client Timeout (minutes) Virtual IPv4 Address Trustpoint Virtual IPv4 Hostname Virtual IPv6 Address Web Auth intercept HTTPs Enable HTTP server for Web Auth Disable HTTP secure server for Web Auth **Banner Configuration**Banner Title Banner Type None Banner Text Read From File

Mappa parametri Web

Passaggio 2: nella scheda Avanzate, specificare l'URL della pagina Web esterna a cui reindirizzare i client. Configurare l'URL di reindirizzamento per Login e Redirect On-Failure. L'impostazione Reindirizza se riuscito è una configurazione facoltativa.

Preview of the Redirect URL:

```
http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>
```

Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X::X"/>

Scheda Avanzate

Configurazione dalla CLI

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Nota: per la configurazione AAA, consultare i dettagli della configurazione forniti nella sezione "Configure Wired Guest on Catalyst 9800 ancorato a un altro Catalyst 9800" per il WLC esterno di 9800.

Configura profilo criteri

Fase 1. Passare a Configurazione > Tag e profili > Criterio. Configurare il profilo dei criteri con lo stesso nome utilizzato per il profilo LAN guest del controller esterno.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Profilo criterio

Passaggio 2: Nella scheda Access Policies (Criteri di accesso), mappare la vlan del client cablato dall'elenco a discesa

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local ProfilingGlobal State of Device
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select

**VLAN**

VLAN/VLAN Group

VLAN2024



Multicast VLAN

Enter Multicast VLAN

Criteri di accesso

Passaggio 3: Nella scheda Mobilità, selezionare la casella di controllo Esporta ancoraggio.

Mobility Anchors

Export Anchor



Static IP Mobility



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

Scheda Mobility

Configurazione dalla CLI

```
wireless profile policy Guest-Profile
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor
vlan VLAN2024
no shutdown
```

Configura profilo LAN guest

Fase 1. Passare a Configurazione > Wireless > LAN guest e selezionare Aggiungi per configurare il profilo LAN guest e disabilitare lo stato della VLAN cablata.

Il nome del profilo LAN guest sull'ancoraggio deve essere uguale al profilo LAN guest sul WLC esterno.

General Security

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	ENABLE <input checked="" type="checkbox"/>		

Profilo LAN guest

Fase 2. Nella scheda Protezione, abilitare Autenticazione Web. Selezionare la mappa dei parametri Autenticazione Web e l'elenco Autenticazione dall'elenco a discesa

Edit Guest LAN Profile

General Security

Layer3

Web Auth	ENABLE <input checked="" type="checkbox"/>
Web Auth Parameter Map	global
Authentication List	ISE-List

Scheda Sicurezza LAN guest

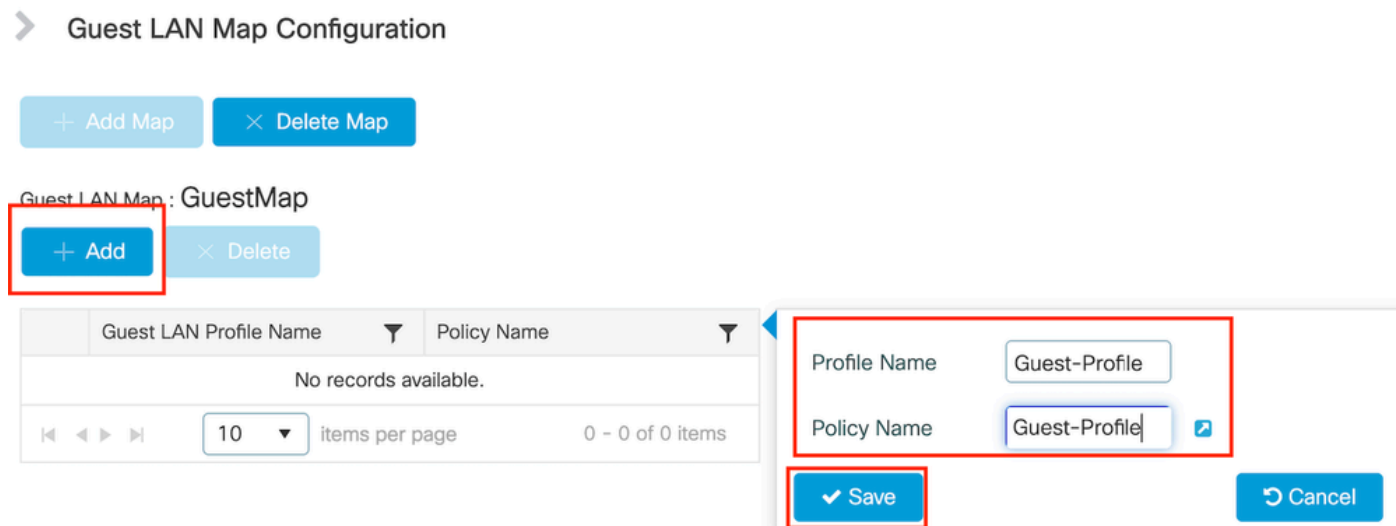
Configurazione dalla CLI

```
guest-lan profile-name Guest-Profile 1
```

```
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

MAPPA LAN guest

Fase 1. Passare a Configurazione > Wireless > LAN guest. Nella sezione di configurazione Guest LAN MAP, selezionare Add (Aggiungi) e mappare il profilo criteri al profilo LAN guest.



MAPPA LAN guest

Verifica

Convalida configurazione controller

riepilogo lan guest #show

GLAN	GLAN Profile Name	Status
1	Guest-Profile	UP
2	Guest	UP

#show guest-lan id 1

<#root>

```
Guest-LAN Profile Name      : Guest
=====
Guest-LAN ID                : 2
Wired-Vlan                  :
11
Status                       :
```

Enabled

Number of Active Clients : 0
Max Associated Clients : 2000
Security
 WebAuth :

Enabled

 Webauth Parameter Map : global
 Webauth Authentication List :

ISE-List

 Webauth Authorization List : Not configured
mDNS Gateway Status : Bridge

#show parameter-map, tipo webauth global

<#root>

Parameter Map Name : global
Type :

webauth

Redirect:
 For Login :

http://10.127.196.171/webauth/login.html

 On Success :

http://10.127.196.171/webauth/logout.html

 On Failure :

http://10.127.196.171/webauth/failed.html

 Portal ipv4 :

10.127.196.171

 Virtual-ipv4 :

192.0.2.1

#show parameter-map type webauth name <nome profilo> (se viene utilizzato un profilo di parametro Web personalizzato)

riepilogo di #show wireless guest-lan-map

GLAN Profile Name	Policy Name
Guest	Guest

riepilogo mobilità wireless #show

IP	Public Ip	MAC Address
10.76.118.70	10.76.118.70	f4bd.9e59.314b

#show ip http server status

HTTP server status: Enabled
HTTP server port: 80
HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local

HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server trustpoint: TP-self-signed-3010594951

>mostra riepilogo lan guest

Number of Guest LANs..... 1

GLAN ID	GLAN Profile Name	Status	Interface Name
2	Guest	Enabled	wired-vlan-11

>show guest-lan 2

Guest LAN Identifier..... 2
Profile Name..... Guest
Status..... Enabled
Interface..... wired-vlan-11

Radius Servers
Authentication..... 10.197.224.122 1812 *
Web Based Authentication..... Enabled
Web Authentication Timeout..... 300
IPv4 ACL..... Pre-Auth_ACL

Mobility Anchor List

GLAN ID	IP Address	Status
2	10.76.118.74	Up

>mostra tutto web personalizzato

```
Radius Authentication Method..... PAP
Cisco Logo..... Enabled
CustomLogo..... None
Custom Title..... None
Custom Message..... None
Custom Redirect URL..... http://10.127.196.171/webauth/logout.html
Web Authentication Login Success Page Mode..... None
Web Authentication Type..... External
Logout-popup..... Enabled
External Web Authentication URL..... http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer..... 0
QR Code Scanning Bypass Count..... 0
```

>show custom-web guest-lan 2

```
Guest LAN Status..... Enabled
Web Security Policy..... Web Based Authentication
WebAuth Type..... External
Global Status..... Enabled
```

Convalida stato criteri client

Su Foreign,

riepilogo client wireless #show

Lo stato di gestione dei criteri client nel controller esterno viene ESEGUITO dopo la corretta associazione del client.

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	N/A			

GLAN 1

Run

802.3

Web Auth

Export Foreign

>show client detail a0ce.c8c3.a9b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username N/A
Client Webauth Username N/A
Client State..... Associated
User Authenticated by None
Client User Group.....
Client NAC OOB State..... Access
guest-lan..... 1
Wireless LAN Profile Name..... Guest-Profile
Mobility State.....

Export Foreign

Mobility Anchor IP Address.....
10.76.118.70

Security Policy Completed.....

Yes

Policy Manager State.....

RUN

Pre-auth IPv4 ACL Name..... Pre-Auth_ACL
EAP Type..... Unknown
Interface.....

wired-guest-egress

VLAN..... 2024
Quarantine VLAN..... 0

Su ancoraggio,

La transizione dello stato del client deve essere monitorata sul controller di ancoraggio.

Stato di Gestione criteri client in attesa di autenticazione Web.

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	10.76.6.156			

GLAN 1

Webauth Pending

802.3

Web Auth

Export Anchor

Una volta eseguita l'autenticazione del client, lo stato di gestione dei criteri passa allo stato RUN.

MAC Address	AP Name	Type ID	State	Protocol	Method
a0ce.c8c3.a9b5	10.76.6.156	GLAN 1	Run	802.3	Web

dettaglio #show wireless client mac-address a0ce.c8c3.a9b5

<#root>

Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :

10.105.211.69

Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
GLAN Id: 1
GLAN Name: Guest-Profile

Mobility:

Foreign IP Address :

10.76.118.74

Point of Attachment : 0xA0000003
Point of Presence : 0
Move Count : 1
Mobility Role :

Export Anchor

Mobility Roam Type :

L3 Requested

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 35 seconds

VLAN : VLAN2024

Session Manager:

Point of Attachment : mobility_a0000003
IIF ID : 0xA0000003
Authorized : FALSE
Session timeout : 28800
Common Session ID: 4a764c0a0000008ea0285466

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State :

Login

Webauth Method :

Webauth

Server Policies:

Resultant Policies:

URL Redirect ACL :

WA-v4-int-10.127.196.171

Preauth ACL :

WA-sec-10.127.196.171

VLAN Name : VLAN2024

VLAN :

2024

Absolute-Timer : 28800

Il client passa allo stato RUN dopo la corretta autenticazione Web.

visualizzare i dettagli dell'indirizzo mac del client wireless a0ce.c8c3.a9b5

<#root>

Client MAC Address : a0ce.c8c3.a9b5

Client MAC Type : Universally Administered Address

Client DUID: NA

Client IPv4 Address :

10.105.211.69

Client Username :

testuser

Client State : Associated

Policy Profile : Guest-Profile

Flex Profile : N/A

Guest Lan:

GLAN Id: 1

GLAN Name: Guest-Profile

Wireless LAN Network Name (SSID) : N/A

BSSID : N/A

Connected For : 81 seconds

Protocol : 802.3

Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 81 seconds

VLAN : VLAN2024

Last Tried Aaa Server Details:

Server IP :

10.197.224.122

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Resultant Policies:

URL Redirect ACL :

IP-Adm-V4-LOGOUT-ACL

VLAN Name : VLAN2024

VLAN :

2024

Absolute-Timer : 28800

>show client detail a0:ce:c8:c3:a9:b5

<#root>

```

Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username ..... N/A
Client Webauth Username ..... N/A
Client State..... Associated
Wireless LAN Profile Name..... Guest
WLAN Profile check for roaming..... Disabled
Hotspot (802.11u)..... Not Supported
Connected For ..... 90 secs
IP Address..... 10.105.211.75
Gateway Address..... 10.105.211.1
Netmask..... 255.255.255.128
Mobility State.....

```

Export Anchor

Mobility Foreign IP Address.....

10.76.118.70

Security Policy Completed..... No

Policy Manager State.....

WEBAUTH_REQD

Pre-auth IPv4 ACL Name.....

Pre-Auth_ACLPre-auth

IPv4 ACL Applied Status..... Yes
Pre-auth IPv4 ACL Applied Status.....

Yes

Dopo l'autenticazione, il client passa allo stato RUN.

<#root>

show client detail a0:ce:c8:c3:a9:b5
Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username

testuser

Client Webauth Username

testuser

Client State.....

Associated

User Authenticated by

RADIUS Server

Client User Group..... testuser
Client NAC OOB State..... Access
Connected For 37 secs
IP Address.....

10.105.211.75

Gateway Address..... 10.105.211.1
Netmask..... 255.255.255.128
Mobility State.....

Export Anchor

Mobility Foreign IP Address..... 10.76.118.70
Security Policy Completed..... Yes
Policy Manager State.....

RUN

Pre-auth IPv4 ACL Name..... Pre-Auth_ACL
Pre-auth IPv4 ACL Applied Status..... Yes
EAP Type..... Unknown
Interface.....

wired-vlan-11

VLAN.....

11

Quarantine VLAN..... 0

Risoluzione dei problemi

Debug del controller AireOS

Abilita debug client

```
>debug client <H.H.H>
```

Per verificare se il debug è abilitato

```
>mostra debug
```

Per disabilitare il debug

```
debug disable-all
```

9800 Traccia radioattiva

Attivare Radio Active Tracing per generare le tracce di debug del client per l'indirizzo MAC specificato nella CLI.

Passaggi per l'attivazione della traccia radioattiva:

Accertarsi che tutti i debug condizionali siano disabilitati.

```
clear platform condition all
```

Abilita il debug per l'indirizzo MAC specificato.

```
debug wireless mac <H.H.H> monitor-time <Time in seconds>
```

Dopo aver riprodotto il problema, disabilitare il debug per arrestare la raccolta di traccia dell'Autorità registrazione.

```
no debug wireless mac <H.H.H>
```

Una volta arrestata la traccia dell'Autorità registrazione, il file di debug viene generato nella memoria bootflash del controller.

```
show bootflash: | include ra_trace
2728      179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

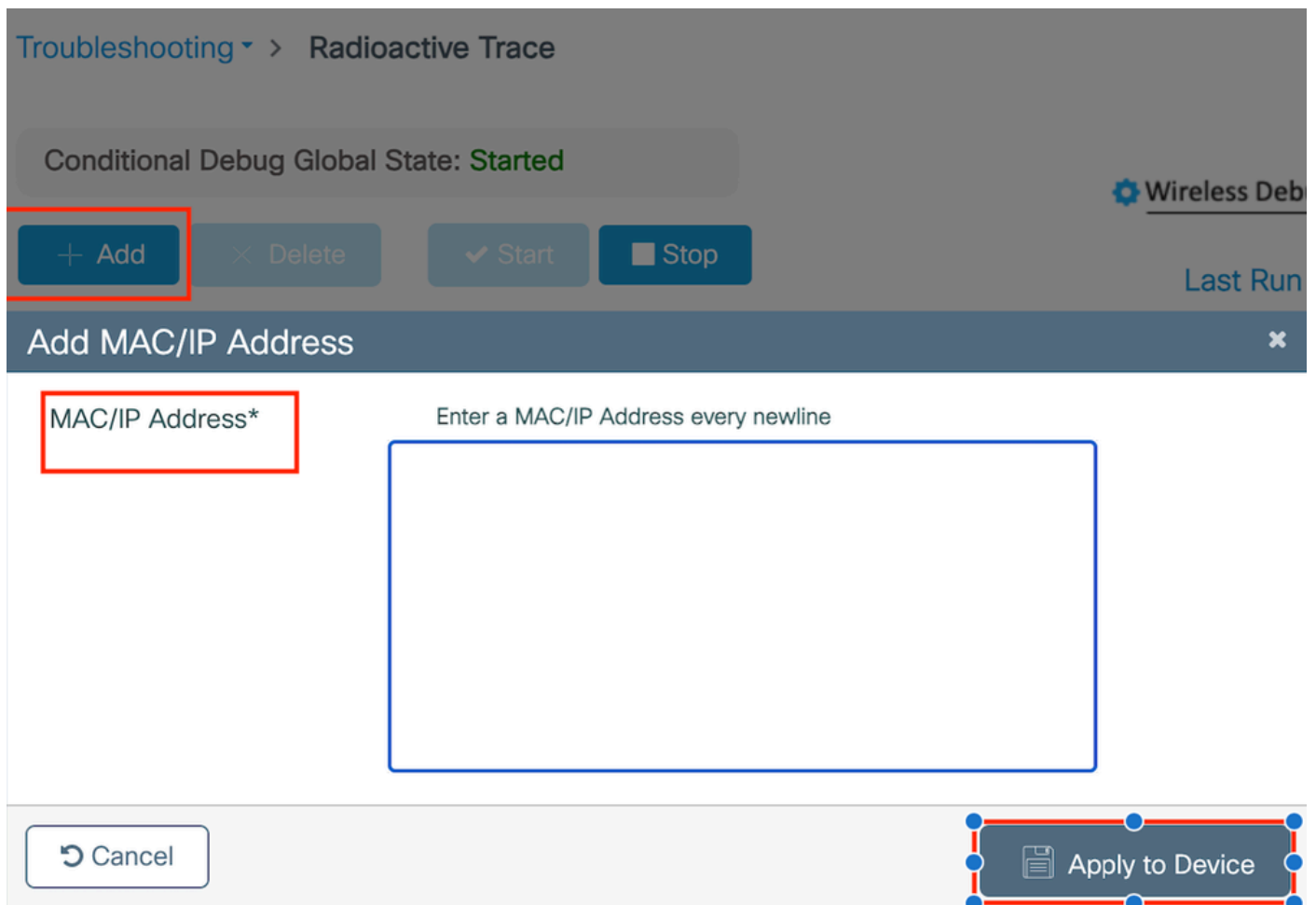
Copiare il file su un server esterno.

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

Visualizzare il registro di debug:

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

Abilitare la traccia dell'Agente di registrazione nella GUI,



Abilita traccia Autorità registrazione su WebUI

Embedded Packet Capture

Selezionare Risoluzione dei problemi > Acquisizione pacchetti. Immettere il nome di acquisizione e specificare l'indirizzo MAC del client come indirizzo MAC del filtro interno. Impostare la

dimensione del buffer su 100 e scegliere l'interfaccia uplink per monitorare i pacchetti in entrata e in uscita.

Troubleshooting > Packet Capture

+ Add × Delete

Create Packet Capture ×

Capture Name*

Filter*

Monitor Control Plane

Inner Filter Protocol DHCP

Inner Filter MAC

Buffer Size (MB)*

Limit by* secs ~ 1.00 hour

Available (12)

<input type="checkbox"/> Tw0/0/1	→
<input checked="" type="checkbox"/> Tw0/0/2	→
<input checked="" type="checkbox"/> Tw0/0/3	→
<input type="checkbox"/> Te0/1/0	→

Selected (1)

<input checked="" type="checkbox"/> Tw0/0/0	←
---	---

Embedded Packet Capture



Nota: selezionare l'opzione "Controlla traffico" per visualizzare il traffico reindirizzato alla CPU del sistema e reinserito nel piano dati.

Passare a Risoluzione dei problemi > Acquisizione pacchetti e selezionare Inizia per acquisire i pacchetti.

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start

Avvia acquisizione pacchetto

Configurazione dalla CLI

```
monitor capture TestPCap inner mac <H.H.H>  
monitor capture TestPCap buffer size 100  
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
```

```
monitor capture TestPCap start
```

<Reproduce the issue>

```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap
```

Status Information for Capture TestPCap

Target Type:

Interface: TwoGigabitEthernet0/0/0, Direction: BOTH

Status : Inactive

Filter Details:

Capture all packets

Inner Filter Details:

Mac: 6c7e.67e3.6db9

Continuous capture: disabled

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 100

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 3600

Packet Size to capture: 0 (no limit)

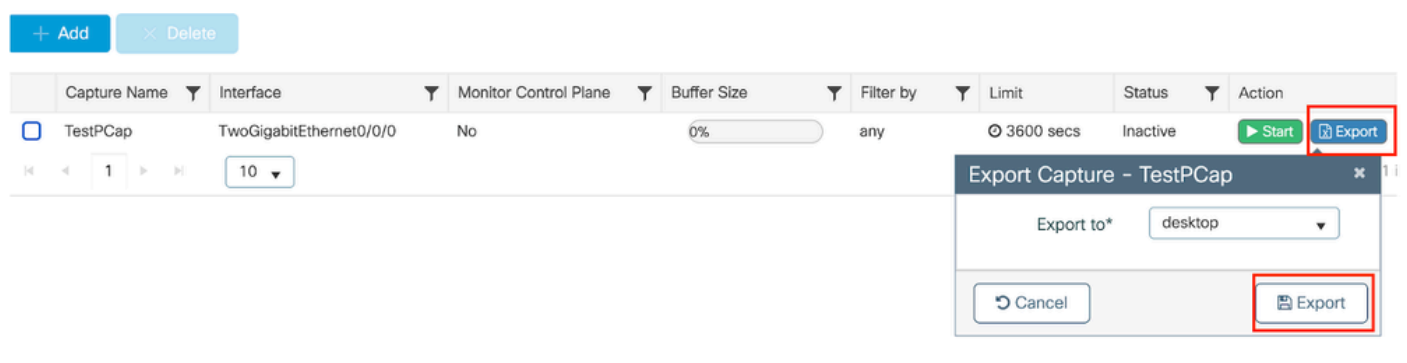
Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

Esporta l'acquisizione dei pacchetti sul server TFTP esterno.

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```

Passare a Risoluzione dei problemi > Acquisizione pacchetti e selezionare Esporta per scaricare il file di acquisizione sul computer locale.



Scarica EPC

Frammenti di log di lavoro

Registro di debug del client AireOS Foreign Controller

Pacchetto cablato ricevuto dal client cablato

*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5 Wired Guest packet from 10.105.211.69 on mobi1

Richiesta di ancoraggio di esportazione compilazione controller esterno

*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3:

*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM

*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0

Il controller esterno invia una richiesta di ancoraggio di esportazione al controller di ancoraggio.

*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70

Il controller di ancoraggio invia conferma per la richiesta di ancoraggio per il client

*Dot1x_NW_MsgTask_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile a0:ce:c8:c3:

Il ruolo di mobilità per i client nel controller esterno è aggiornato per l'esportazione.

*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) mobility role update requ
Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70

Il client è passato allo stato RUN.

*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mobilit

*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId:

*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state

9800 Traccia radioattiva del controller esterno

Il client viene associato al controller.

2024/07/15 04:10:29.087608331 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

Individuazione mobilità in corso dopo l'associazione.

2024/07/15 04:10:29.091585813 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

Dopo l'elaborazione dell'individuazione di Mobility, il tipo di roaming client viene aggiornato a L3 richiesto.

2024/07/15 04:10:29.091664605 {wncd_x_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM

2024/07/15 04:10:29.091693445 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t

Il controller esterno sta inviando la richiesta di ancoraggio di esportazione al WLC di ancoraggio.

2024/07/15 04:10:32.093245394 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex

2024/07/15 04:10:32.093253788 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo

2024/07/15 04:10:32.093274405 {mobilityd_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For

L'esportazione della risposta di ancoraggio viene ricevuta dal controller di ancoraggio e la vlan viene applicata dal profilo utente.

2024/07/15 04:10:32.106775213 {mobilityd_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:32.106811183 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex

2024/07/15 04:10:32.107183692 {wncd_x_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An

2024/07/15 04:10:32.107247304 {wncd_x_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr

2024/07/15 04:10:32.107250258 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:

Una volta elaborata la richiesta di esportazione dell'ancoraggio, il ruolo di mobilità del client viene aggiornato in Esporta esterno.

2024/07/15 04:10:32.107490972 {wncd_x_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce

2024/07/15 04:10:32.107502336 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili

2024/07/15 04:10:32.107533732 {wncd_x_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20

2024/07/15 04:10:32.107592251 {wncd_x_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobili

Il client passa allo stato di apprendimento IP.

```
2024/07/15 04:10:32.108210365 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 04:10:32.108293096 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5
```

Dopo l'apprendimento da parte dell'IP, il client passa allo stato RUN sul WLC esterno.

```
2024/07/15 04:10:32.108521618 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
```

Registro di debug del client del controller di ancoraggio AireOS

Esporta richiesta di ancoraggio restituita dal controller esterno.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:c
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv Ssid=Guest useProfileNa
```

Al client viene applicata la VLAN di bridging locale.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) po
```

Il ruolo di mobilità viene aggiornato in Esporta ancoraggio e stato client in stato di transistoning associato.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 0.0.0.0 START (0) mobility role update requ
Peer = 10.76.118.70, Old Anchor = 0.0.0.0, New Anchor = 10.76.118.74
Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
add client MAC a0:ce:c8:c3:a9:b5 IP 10.76.1
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
Sent message to add a0:ce:c8:c3:a9:b5 on mer
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm_listen.c:7933) Changi
```

La mobilità è stata completata, lo stato del client è associato e il ruolo di mobilità è Export Anchor.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mob
```

L'indirizzo IP del client viene appreso sul controller e lo stato viene convertito da DHCP richiesto a Web auth required.

```
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dtlArpSetType: Changing ARP Type from 0 ---> 1 for
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP_REQD (7) Change state to WEBAUTH
```

È in corso la formulazione dell'URL Webauth aggiungendo l'URL di reindirizzamento esterno e l'indirizzo IP virtuale del controller.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch_url, redirect URL is now http://
```

Sono stati aggiunti l'indirizzo MAC del client e la WLAN all'URL.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client_mac , redirect URL is now http:/
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127.
```

URL finale dopo l'analisi di HTTP GET per l'host 10.105.211.1

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser host is 10.105.211.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.
```

L'URL di reindirizzamento viene inviato al client nel pacchetto di risposta 200 OK.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send_data =HTTP/1.1 200 OK
Location:http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&client_mac=a0
```

Il client stabilisce una connessione TCP con l'host URL di reindirizzamento. Una volta che i client hanno inviato il nome utente e la password di login sul portale, il controller invia una richiesta radius al server radius

Una volta che il controller riceve un messaggio di accettazione dell'accesso, il client chiude la sessione TCP e passa allo stato RUN.

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe

*aaaQueueReader: May 28 10:46:59:077: AVP[01] User-Name.....testuser
*aaaQueueReader: May 28 10:46:59:077: AVP[03] Calling-Station-Id.....a0-ce-c8
*aaaQueueReader: May 28 10:46:59:077: AVP[04] Nas-Port.....0x000000
*aaaQueueReader: May 28 10:46:59:077: AVP[05] Nas-Ip-Address.....0x0a4c76
*aaaQueueReader: May 28 10:46:59:077: AVP[06] NAS-Identifier.....POD1586-

*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Access-Accept received from RADIUS serv

*Dot1x_NW_MsgTask_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c

*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state
```

9800 Anchor controller radioactive trace

Messaggio di annuncio mobilità per il client dal controller esterno.

```
2024/07/15 15:10:20.614677358 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Re
```

Richiesta di ancoraggio di esportazione ricevuta dal controller esterno durante l'associazione del client per la quale la risposta di ancoraggio di esportazione viene inviata dal controller di ancoraggio che può essere verificata nella traccia RA del controller esterno.

```
2024/07/15 15:10:22.615246594 {mobilityd_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5
```

Il client viene spostato allo stato di associazione e il ruolo di mobilità viene trasferito all'ancoraggio di esportazione.

```
2024/07/15 15:10:22.616156811 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b5
```

```
2024/07/15 15:10:22.627358367 {wncd_x_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

```
2024/07/15 15:10:22.627462963 {wncd_x_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5 Client da
```

```
2024/07/15 15:10:22.627490485 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex
```

```
2024/07/15 15:10:22.627494963 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo
```

L'apprendimento IP è completato, l'IP del client è stato appreso tramite ARP.

```
2024/07/15 15:10:22.628124206 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:23.627064171 {wncd_x_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m
2024/07/15 15:10:24.469704913 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470527056 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470587596 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470613094 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
```

Stato dei criteri client in attesa di autenticazione Web.

```
2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5 Cli
```

Handshake TCP falsificato dal controller. Quando il client invia un GET HTTP, viene inviato un frame di risposta 200 OK che contiene l'URL di reindirizzamento.

Il client deve stabilire un handshake TCP con l'URL di reindirizzamento e caricare la pagina.

```
2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123082753 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
```

Quando il client invia le credenziali di accesso nella pagina del portale Web, un pacchetto di richiesta di accesso viene inviato al server radius per l'autenticazione.

```
2024/07/15 15:12:04.281076844 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t
2024/07/15 15:12:04.281087672 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator e3 01
2024/07/15 15:12:04.281093278 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Calling-Station-Id
2024/07/15 15:12:04.281097034 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
2024/07/15 15:12:04.281148298 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Cisco AVpair
```

L'autorizzazione di accesso viene ricevuta dal server radius. Webauth ha esito positivo.

```
2024/07/15 15:12:04.683597101 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812
2024/07/15 15:12:04.683607762 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator 52 3e
2024/07/15 15:12:04.683614780 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
```

L'autenticazione è riuscita e lo stato dei criteri client è impostato su RUN.

```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs
2024/07/15 15:12:04.691064276 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
```

Analisi dell'acquisizione dei pacchetti integrata

No.	Time	Source	Destination	Length	Protocol	Info
804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)

> Frame 806: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)
> Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb)
> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.76.6.156
> User Datagram Protocol, Src Port: 16667, Dst Port: 16667
> Control And Provisioning of Wireless Access Points - Data
> Ethernet II, Src: Cisco_34:90:d4 (6c:5e:3b:34:90:d4), Dst: CeLink_c3:a9:b5 (a0:ce:c8:c3:a9:b5)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4095
> Internet Protocol Version 4, Src: 10.105.211.1, Dst: 10.105.211.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 54351, Seq: 1, Ack: 108, Len: 743
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n\r\nLocation: http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://10.105.211.1/auth/discovery?architecture=9\r\n\r\nContent-Type: text/html\r\n\r\nContent-Length: 527\r\n\r\n\r\n[HTTP response 1/1]
[Time since request: 0.000000000 seconds]
[Request in frame: 804]
[Request URI: http://10.105.211.1/auth/discovery?architecture=9]
File Data: 527 bytes

Il client viene reindirizzato alla pagina del portale

La sessione viene chiusa dopo la ricezione dell'URL di reindirizzamento.

804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
805	15:10:24.826953	10.105.211.1	10.105.211.69		TCP	80 → 54351 [ACK] Seq=1 Ack=108 Win=65152 Len=0 TSval=2124108437 TSecr=2231352500
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)
807	15:10:24.826953	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=108 Ack=744 Win=131008 Len=0 TSval=2231352500 TSecr=2124108437
812	15:10:24.835955	10.105.211.69	10.105.211.1		TCP	54351 → 80 [FIN, ACK] Seq=108 Ack=744 Win=131072 Len=0 TSval=2231352510 TSecr=2124108437
813	15:10:24.836947	10.105.211.1	10.105.211.69		TCP	80 → 54351 [FIN, ACK] Seq=744 Ack=109 Win=65152 Len=0 TSval=2124108447 TSecr=2231352510
814	15:10:24.836947	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=109 Ack=745 Win=131072 Len=0 TSval=2231352510 TSecr=2124108447

La sessione TCP viene chiusa dopo la ricezione dell'URL di reindirizzamento

Il client avvia l'handshake TCP a 3 vie all'host dell'URL di reindirizzamento e invia una richiesta HTTP GET.

Una volta caricata la pagina, le credenziali di accesso vengono inviate sul portale, il controller invia una richiesta di accesso al server radius per autenticare il client.

Una volta completata l'autenticazione, la sessione TCP sul server Web viene chiusa e sul controller viene eseguita la transizione dello stato di gestione dei criteri del client su RUN.

Articolo correlato

[Configurazione della funzione WLAN Anchor Mobility su Catalyst 9800](#)

[Esempio di configurazione di Wired Guest Access mediante i controller AireOS](#)

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).