

Configurazione verifica e risoluzione dei problemi autenticazione Web su filtro Mac non riuscito

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configura parametri Web](#)

[Configura profilo criteri](#)

[Configura profilo WLAN](#)

[Configurare le impostazioni AAA:](#)

[Configurazione di ISE:](#)

[Verifica](#)

[Configurazione controller](#)

[Stato criteri client sul controller](#)

[Risoluzione dei problemi](#)

[Raccolta traccia radioattiva](#)

[Acquisizioni pacchetti incorporati:](#)

[Articolo correlato](#)

Introduzione

In questo documento viene descritto come configurare, risolvere i problemi e verificare l'autenticazione Web locale con la funzione "Mac Filter Failure" usando ISE per l'autenticazione esterna.

Prerequisiti

Configurazione di ISE per l'autenticazione MAC

Credenziali utente valide configurate su ISE/Active Directory

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

Nozioni di base per spostarsi nell'interfaccia utente Web del controller

Configurazione di criteri, profili WLAN e tag di criteri

Configurazione delle policy di servizio su ISE

Componenti usati

9800 WLC versione 17.12.2

AP C9120 AXI

switch 9300

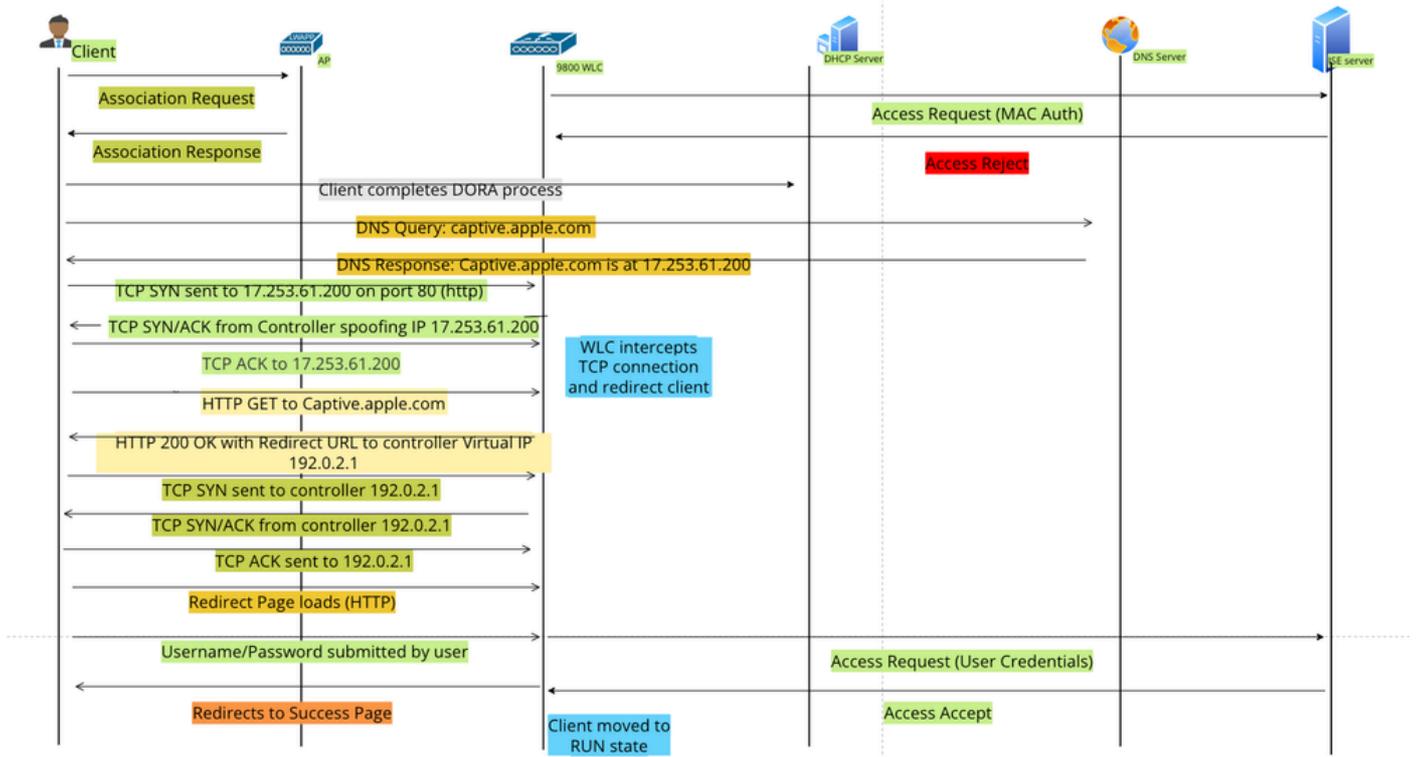
ISE versione 3.1.0.518

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.

Premesse

La funzione "On Mac Failure Filter" (Filtro in caso di guasto del sistema) dell'autenticazione Web funge da meccanismo di fallback negli ambienti WLAN che utilizzano sia l'autenticazione MAC che l'autenticazione Web.

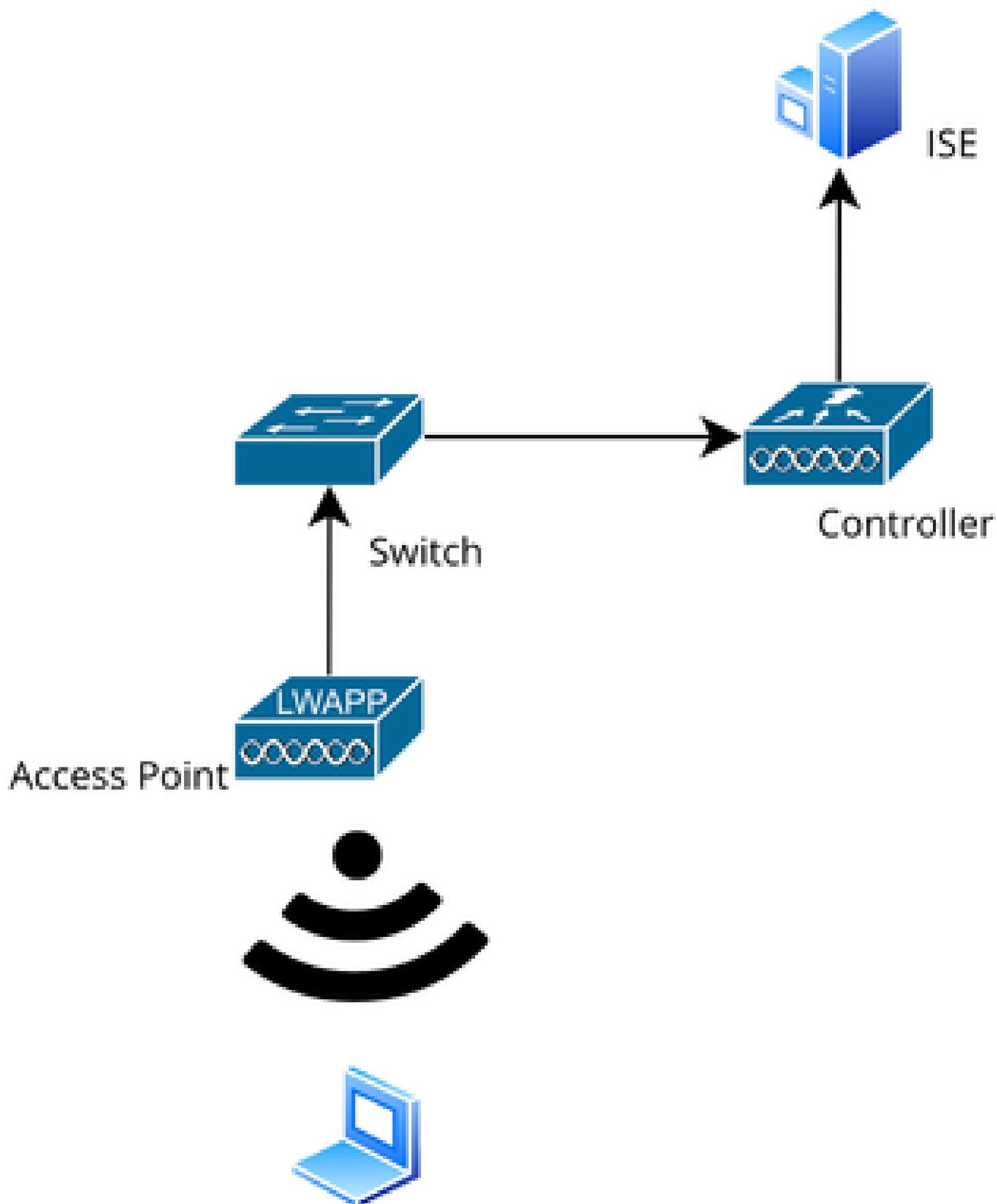
- Meccanismo di fallback: quando un client tenta di connettersi a una WLAN con filtro MAC su un server RADIUS esterno (ISE) o locale e non riesce ad autenticarsi, questa funzione avvia automaticamente un'autenticazione Web di layer 3.
- Autenticazione riuscita: se un client esegue l'autenticazione tramite il filtro MAC, l'autenticazione Web viene ignorata, consentendo al client di connettersi direttamente alla WLAN.
- Evitare le dissociazioni: questa funzione consente di evitare le dissociazioni che possono verificarsi a causa di errori di autenticazione del filtro MAC.



Flusso autenticazione Web

Configurazione

Esempio di rete



Topologia della rete

Configurazioni

Configura parametri Web

Passare a Configurazione > Sicurezza > Autenticazione Web e selezionare la mappa dei parametri globali

Verificare la configurazione di IP virtuale e Trustpoint dalla mappa dei parametri globali. Tutti i profili dei parametri di autenticazione Web personalizzati ereditano la configurazione dell'IP virtuale e del punto di trust dalla mappa dei parametri globali.

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
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"/>		
Sleeping Client Status	<input type="checkbox"/>		

Banner Configuration

Profilo parametro autenticazione Web globale

Passaggio 1: selezionare "Aggiungi" per creare una mappa dei parametri di autenticazione Web personalizzata. Immettere il nome del profilo e scegliere Tipo come "Webauth".

Configuration > Security > Web Auth

+ Add **× Delete**

Parameter Map Name

- global

Create Web Auth Parameter

Parameter-map Name*	Web-Filter
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth ▼

× Close **✓ Apply to Device**

Se i client ricevono anche un indirizzo IPv6, è necessario aggiungere anche un indirizzo IPv6 virtuale nella mappa dei parametri. Utilizzare un indirizzo IP nella documentazione 2001:db8::/32

Se i client hanno ottenuto un indirizzo IPv6, è possibile che tentino di ottenere il reindirizzamento dell'autenticazione Web HTTP in V6 e non in V4. Per questo motivo è necessario impostare anche l'IPv6 virtuale.

Configurazione dalla CLI:

```
parameter-map type webauth Web-Filter  
type webauth
```

Configura profilo criteri

Passaggio 1: Creare un profilo criteri

Selezionare Configurazione > Tag e profili > Criterio. Selezionare "Add". Nella scheda Generale, specificare un nome per il profilo e attivare o disattivare lo stato.

Configuration > Tags & Profiles > Policy

+ Add 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* Web-Filter-Policy

Description Enter Description

Status **ENABLED**

Passive Client DISABLED

IP MAC Binding **ENABLED**

Encrypted Traffic Analytics DISABLED

CTS Policy

WLAN Switching Policy

Central Switching **ENABLED**

Central Authentication **ENABLED**

Central DHCP **ENABLED**

Flex NAT/PAT DISABLED

Inline Tagging

SGACL Enforcement

Profilo criterio

Fase 2:

Nella scheda Access Policies (Criteri di accesso), selezionare la VLAN client dall'elenco a discesa della sezione VLAN.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name Search or Select ↕

VLAN

VLAN/VLAN Group VLAN2074 ⓘ

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 ↕

Scheda Criteri di accesso

Configurazione dalla CLI:

```
wireless profile policy Web-Filter-Policy  
vlan VLAN2074  
no shutdown
```

Configura profilo WLAN

Fase 1. Passare a Configurazione > Tag e profili > WLAN. Selezionare "Aggiungi" per creare un nuovo profilo. Definire un nome di profilo e un nome SSID e abilitare il campo di stato.

+ Add × Delete Clone Enable WLAN Disable WLAN

Add WLAN

General Security Advanced

Profile Name* Mac_Filtering_Wlan

SSID* Mac_Filtering_Wlan

WLAN ID* 9

Status **ENABLED**

Broadcast SSID **ENABLED**

Radio Policy ⓘ

[Show slot configuration](#)

6 GHz

Status **ENABLED** ⓘ

- ✖ WPA3 Enabled
- ✔ Dot11ax Enabled

5 GHz

Status **ENABLED**

2.4 GHz

Status **ENABLED**

802.11b/g Policy 802.11b/g ▼

Profilo WLAN

Fase 2. Nella scheda Sicurezza, abilitare la casella di controllo "Mac Filtering" (Filtro Mac) e configurare il server RADIUS nell'elenco delle autorizzazioni (ISE o server locale). Questa configurazione utilizza ISE per l'autenticazione Mac e per l'autenticazione Web.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Authorization List*

network

OWE Transition Mode

Lobby Admin Access

Fast Transition

Status

Disabled

Over the DS

Reassociation Timeout *

20

Sicurezza WLAN layer 2

Passaggio 3: Passare a Protezione > Livello 3. Abilitare il criterio Web e associarlo al profilo Mappa parametri di autenticazione Web. Selezionare la casella di controllo "In caso di errore del filtro Mac" e scegliere il server RADIUS dall'elenco a discesa Autenticazione.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy

Web Auth Parameter Map

Web-Filter

Authentication List

ISE-List

For Local Login Method List to work, please make sure

<< Hide

On MAC Filter Failure

Splash Web Redirect

DISABLED

Preauthentication ACL

Scheda Protezione Layer3 WLAN

Configurazione dalla CLI

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
mac-filtering network
radio policy dot11 24ghz
radio policy dot11 5ghz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list ISE-List
security web-auth on-macfilter-failure
security web-auth parameter-map Web-Filter
no shutdown
```

Fase 4. Configurazione dei tag dei criteri, creazione del profilo WLAN e mappatura del profilo dei criteri

Selezionare Configurazione > Tag e profili > Tag > Criterio. Fare clic su "Aggiungi" per definire un nome per il tag di criterio. In Mappe WLAN-Policy, selezionare "Aggiungi" per mappare il profilo WLAN e Policy creato in precedenza.

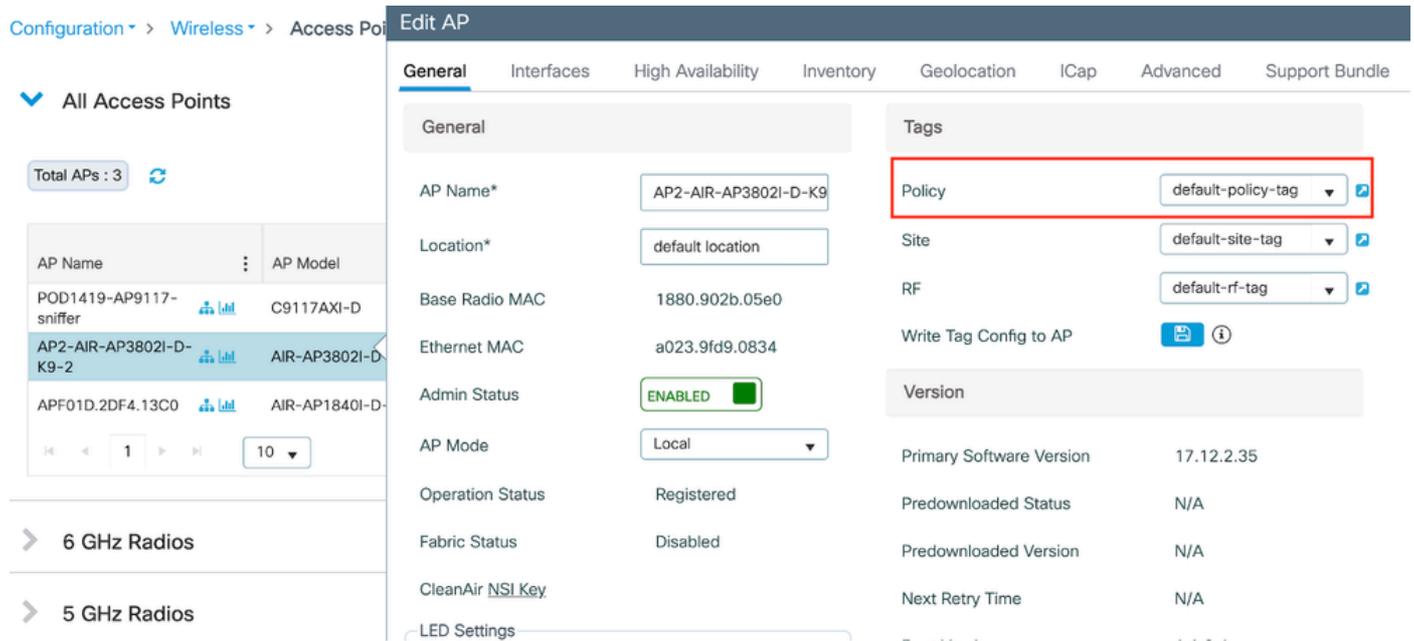
The screenshot displays the Cisco ISE configuration interface. At the top, there are tabs for 'Policy', 'Site', 'RF', and 'AP'. Below these tabs, there are three buttons: '+ Add', 'x Delete', and 'Clone'. The '+ Add' button is highlighted with a red box. Below this is a modal window titled 'Add Policy Tag'. Inside this modal, there are two input fields: 'Name*' with the value 'default-policy-tag' and 'Description' with the placeholder 'Enter Description'. Below the input fields, there is a section for 'WLAN-POLICY Maps: 0' with a blue checkmark icon and two buttons: '+ Add' and 'x Delete'. Below this section, there is a table with two columns: 'WLAN Profile' and 'Policy Profile'. The table is currently empty, showing '0' items and a 'No items to display' message. Below the table, there is a section titled 'Map WLAN and Policy' which is highlighted with a red box. This section contains two search/select dropdowns: 'WLAN Profile*' and 'Policy Profile*'. Below these dropdowns are two buttons: 'x' and a blue checkmark icon.

Mappa tag criteri

Configurazione dalla CLI:

```
wireless tag policy default-policy-tag
description "default policy-tag"
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

Passaggio 5: Passare a Configurazione > Wireless > Access Point. Selezionare il punto di accesso responsabile della trasmissione di questo SSID. Nel menu Modifica punto di accesso, assegnare il tag di criterio creato.



Mapping del tag dei criteri al punto di accesso

Configurare le impostazioni AAA:

Fase 1. Creazione di un server Radius:

Passare a Configurazione > Sicurezza > AAA. Fare clic sull'opzione "Aggiungi" nella sezione Server/Gruppo. Nella pagina "Crea server AAA Radius", immettere il nome del server, l'indirizzo IP e il segreto condiviso.

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

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

RADIUS **Servers** Server Groups

Create AAA Radius Server

Name*	<input type="text"/>	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	<input type="text" value="IPv4/IPv6/Hostname"/>	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	<input type="text"/>
Key Type	Clear Text ▼	Confirm CoA Server Key	<input type="text"/>
Key* ⓘ	<input type="text"/>	Automate Tester	<input type="checkbox"/>
Confirm Key*	<input type="text"/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		

Configurazione server

Configurazione dalla CLI

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

Fase 2. Creare un gruppo di server Radius:

Per definire un gruppo di server, selezionare l'opzione "Aggiungi" nella sezione Gruppi di server. Attiva/disattiva i server da includere nella stessa configurazione di gruppo.

Non è necessario impostare l'interfaccia di origine. Per impostazione predefinita, la 9800 utilizza la tabella di routing per definire l'interfaccia da utilizzare per raggiungere il server RADIUS e in genere utilizza il gateway predefinito.

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

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS

Servers **Server Groups**

TACACS

LDAP

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 DISABLED

Source Interface VLAN ID 2074

Available Servers Assigned Servers

ISE-Auth

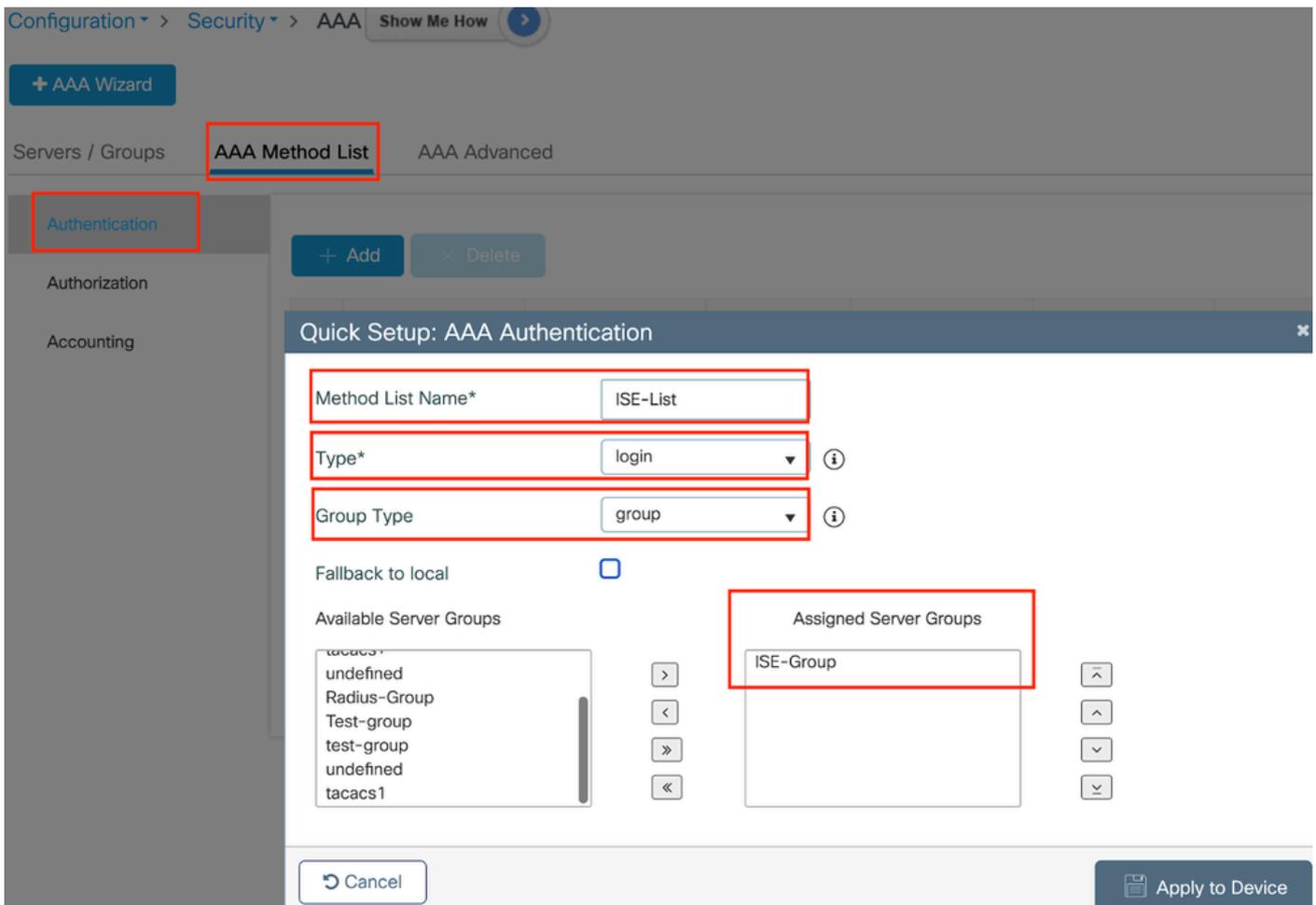
Gruppo server

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. In Autenticazione fare clic su Aggiungi. Definire un nome di elenco di metodi con Type come "login" e Group come "Group". Mappare il gruppo di server di autenticazione configurato nella sezione Gruppo di server assegnato.



Elenco dei metodi di autenticazione

Configurazione dalla CLI

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

Passare alla sezione Elenco metodi di autorizzazione e fare clic su "Aggiungi". Definire un nome di elenco di metodi e impostare il tipo su "network" con il tipo di gruppo "Group". Passare dal server RADIUS configurato alla sezione Gruppi di server assegnati.

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add × Delete

Quick Setup: AAA Authorization

Method List Name* network

Type* network i

Group Type group i

Fallback to local

Authenticated

Available Server Groups

tacacs1
undefined
Radius-Group
Test-group
test-group
undefined
tacacs1

Assigned Server Groups

ISE-Group

Elenco dei metodi di autorizzazione

Configurazione dalla CLI

```
aaa authorization network network group ISE-Group
```

Configurazione di ISE:

Aggiungere WLC come dispositivo di rete su ISE

Fase 1. Passare a Amministrazione > Dispositivi di rete e fare clic su Aggiungi. Immettere l'indirizzo IP, il nome host e il segreto condiviso del controller nelle impostazioni di autenticazione Radius

Network Devices

Name

Description

 IP Address * IP : / 32 

Aggiungi dispositivo di rete

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret

Show

Segreto condiviso

Fase 2. Creazione della voce utente

In Gestione delle identità > Identità, selezionare l'opzione Aggiungi.

Configurare il nome utente e la password che il client deve utilizzare per l'autenticazione Web

✓ Network Access User

* Username

Status Enabled

Email

✓ Passwords

Password Type:

* Login Password

Aggiungi credenziali utente

Passo 3: passare ad Amministrazione > Gestione delle identità > Gruppi > Dispositivi registrati e fare clic su Aggiungi.

Immettere l'indirizzo MAC del dispositivo per creare una voce sul server.

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

- Endpoint Identity Groups
 - Blocked List
 - GuestEndpoints
 - Profiled
 - RegisteredDevices**
 - Unknown
 - User Identity Groups

Endpoint Identity Group List > RegisteredDevices

Endpoint Identity Group

* Name: RegisteredDevices

Description: Asset Registered Endpoints Identity Group

Parent Group

Save

Identity Group Endpoints Select

+ Add Remove

MAC Address Static Group Assignment Endpoint Profile

Aggiungi indirizzo MAC del dispositivo

Fase 4. Creazione dei criteri del servizio

Passare a Criterio > Set di criteri e selezionare "+" per creare un nuovo set di criteri

Questo set di criteri è per l'autenticazione Web dell'utente, in cui un nome utente e una password per il client vengono creati in Identity Management

Policy Sets → User-Webauth Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User-Webauth		Wireless_802.1X	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	0	Options

Criteri del servizio di autenticazione Web

Analogamente, creare un criterio del servizio MAB ed eseguire il mapping degli endpoint interni nei criteri di autenticazione.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Test-MAB		Normalised Radius-RadiusFlowType EQUALS WirelessMAB	Default Network Access	0

Authentication Policy (1)					
Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Endpoints	0	Options

Criteri del servizio di autenticazione MAB

Verifica

Configurazione controller

```
<#root>
```

```
show wireless tag policy detailed
```

```
default-policy-tag
```

```
Policy Tag Name : default-policy-tag
```

```
Description : default policy-tag
```

```
Number of WLAN-POLICY maps: 1
```

```
WLAN Profile Name Policy Name
```

```
-----
```

```
Mac_Filtering_Wlan
```

```
Web-Filter-Policy
```

```
<#root>
```

```
show wireless profile policy detailed
```

```
Web-Filter-Policy
```

```
Policy Profile Name :
```

```
Web-Filter-Policy
```

```
Description :
```

Status :
ENABLED
VLAN :
2074
Multicast VLAN : 0

<#root>

show wlan name

Mac_Filtering_Wlan

WLAN Profile Name :

Mac_Filtering_Wlan

=====
Identifier : 9
Description :
Network Name (SSID) :

Mac_Filtering_Wlan

Status :

Enabled

Broadcast SSID :

Enabled

Mac Filter Authorization list name :

network

Webauth On-mac-filter Failure :

Enabled

Webauth Authentication List Name :

ISE-List

Webauth Authorization List Name : Disabled

Webauth Parameter Map :

Web-Filter

<#root>

show parameter-map type webauth name Web-Filter

Parameter Map Name :

Web-Filter

Type :

webauth

Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window :

Enabled

Webauth success-window :

Enabled

Consent Email : Disabled
Activation Mode : Replace
Sleeping-Client : Disabled
Webauth login-auth-bypass:

<#root>

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 server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:

Enabled

HTTP secure server port:

443

show ap name AP2-AIR-AP3802I-D-K9-2 tag detail

Policy tag mapping

WLAN Profile Name	Policy Name	VLAN	Flex
Mac_Filtering_Wlan	Web-Filter-Policy	2074	ENAB

Stato criteri client sul controller

Passare alla sezione Dashboard > Client per confermare lo stato dei client connessi.
Il client è attualmente in stato di attesa di autenticazione Web

[Clients](#)
[Sleeping Clients](#)
[Excluded Clients](#)

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type
6c7e.67e3.6db9	10.76.6.150	fe80::10eb:ede2:23fe:75c3	AP2-AIR-AP3802I-D-K9-2	1	Mac_Filtering_Wlan	9	WLAN	Web Auth Pending	11ac	6c7e67e36db9	N/A

1 - 1 of 1 clients

Dettagli client

```
show wireless client summary
```

```
Number of Clients: 1
```

MAC Address	AP Name	Type	ID	State	Protocol	Method
6c7e.67e3.6db9	AP2-AIR-AP3802I-D-K9-2	WLAN	9	Webauth Pending	11ac	Web

```
<#root>
```

```
show wireless client mac-address 6c7e.67e3.6db9 detail
```

```
Client MAC Address :
```

```
6c7e.67e3.6db9
```

```
Client MAC Type : Universally Administered Address
```

```
Client DUID: NA
```

```
Client IPv4 Address :
```

```
10.76.6.150
```

```
Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
```

```
Client Username :
```

```
6c7e67e36db9
```

```
AP MAC Address : 1880.902b.05e0
```

```
AP Name: AP2-AIR-AP3802I-D-K9-2
```

```
AP slot : 1
```

```
Client State : Associated
```

```
Policy Profile :
```

```
Web-Filter-Policy
```

```
Flex Profile : N/A
```

Wireless LAN Id: 9
WLAN Profile Name:

Mac_Filtering_Wlan

Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :

Failed

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List

Method : Web Auth
Webauth State :

Get Redirect

Webauth Method :

Webauth

Dopo il completamento dell'autenticazione Web, lo stato di gestione dei criteri client passa a ESEGUI

<#root>

show wireless client mac-address 6c7e.67e3.6db9 detail

Client ACLs : None
Mac authentication : Failed
Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 131 seconds
Policy Type : N/A

Risoluzione dei problemi

La funzionalità della funzione Web Auth on MAC Failure si basa sulla capacità del controller di

attivare l'autenticazione Web in caso di errore MAB. Il nostro obiettivo principale è quello di raccogliere le tracce RA in modo efficiente dal controller per la risoluzione dei problemi e l'analisi.

Raccolta 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:

Assicurarsi che tutti i debug condizionali siano disabilitati

```
clear platform condition all
```

Abilita 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 nel 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.

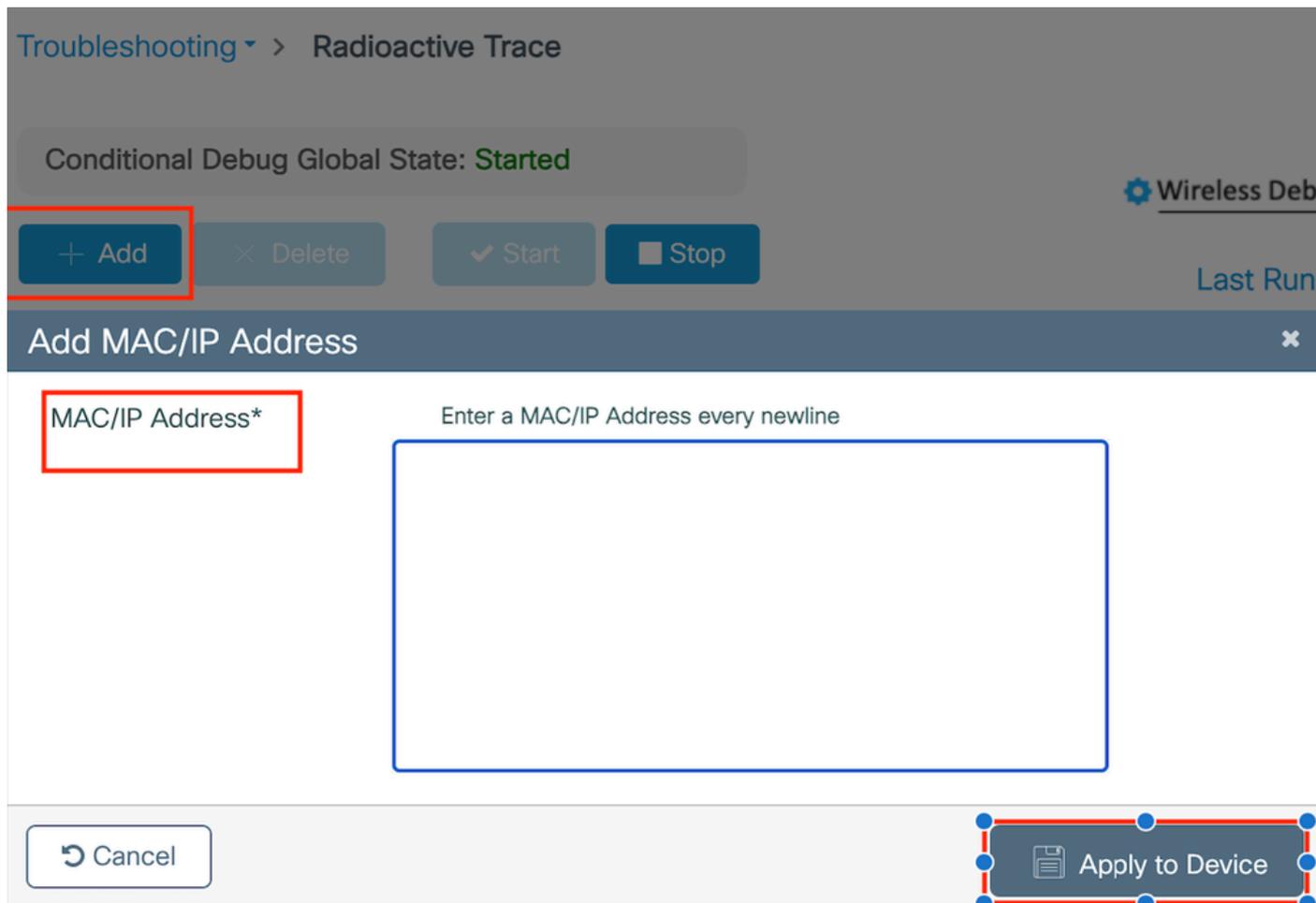
```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

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,

Passo 1: passare a Risoluzione dei problemi > Traccia radioattiva. Selezionare l'opzione per aggiungere una nuova voce, quindi immettere l'indirizzo MAC del client nella scheda Add MAC/IP Address (Aggiungi indirizzo MAC/IP).



traccia Radioactive

Acquisizioni pacchetti incorporati:

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.

+ Add × Delete

Create Packet Capture

Capture Name* TestPCap

Filter* any

Monitor Control Plane

Inner Filter Protocol DHCP

Inner Filter MAC

Buffer Size (MB)* 100

Limit by* Duration 3600 secs ≈ 1.00 hour

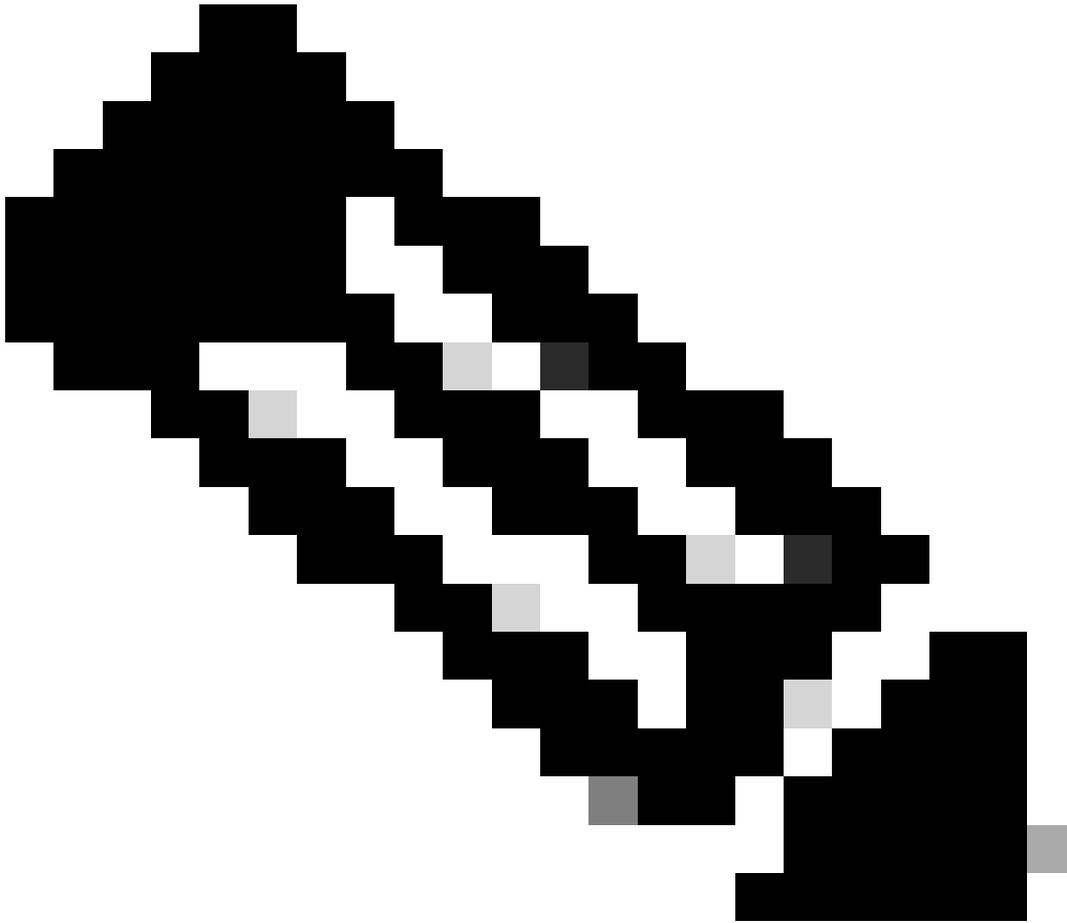
Available (12) Search

- Tw0/0/1
- Tw0/0/2
- Tw0/0/3
- Te0/1/0

Selected (1)

- Tw0/0/0

Acquisizione dei pacchetti integrata



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

Selezionare Start 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	<input type="button" value="Start"/>

Avvia acquisizione

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

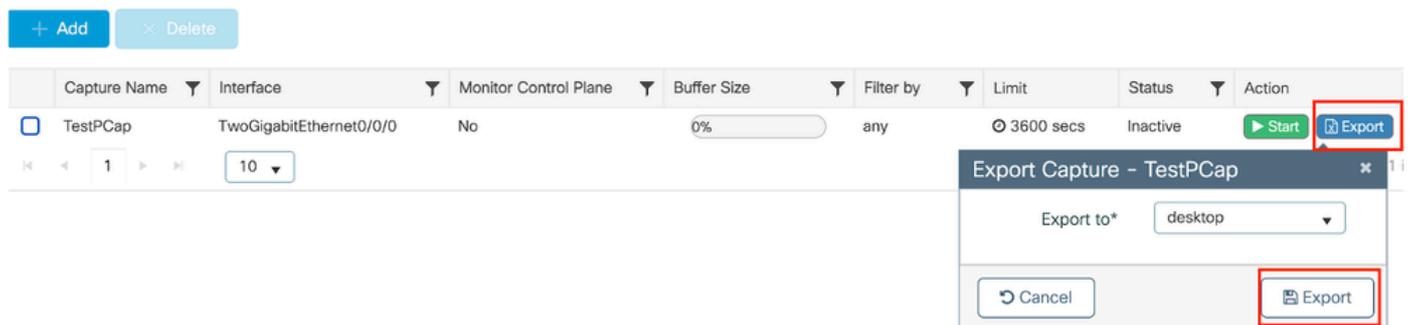
Packet Size to capture: 0 (no limit)

Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

Esporta acquisizione pacchetti su server TFTP esterno

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



Esporta acquisizione pacchetti

Scenario di esempio durante l'autenticazione MAC riuscita, un dispositivo client si connette alla rete, il relativo indirizzo MAC viene convalidato dal server RADIUS tramite criteri configurati e, dopo la verifica, il dispositivo di accesso alla rete concede l'accesso, consentendo la connettività di rete.

Una volta che il client si associa, il controller invia una richiesta di accesso al server ISE,

Nome utente è l'indirizzo MAC del client, poiché è l'autenticazione MAB

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
```

ISE invia il messaggio Access-Accept perché è disponibile una voce utente valida

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

Transizione dello stato dei criteri client in autenticazione Mac completata

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29 Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

Il client è in stato di apprendimento IP dopo l'autenticazione MAB riuscita

```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d29
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

Stato di Client Policy Manager aggiornato a RUN, l'autenticazione Web viene ignorata per il client che completa l'autenticazione MAB

2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD

Verifica tramite Embedded Packet Capture

Time	Source	Destination	Length	Protocol	Info
02:42:52.710961	10.76.6.156	10.197.224.122		RADIUS	Access-Request id=0
02:42:52.778951	10.197.224.122	10.76.6.156		RADIUS	Access-Accept id=0

Frame 53: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0x0 (0)
Length: 422
Authenticator: 19c6635633a7e6b6f30070b02a7f753c
[The response to this request is in frame 54]
Attribute Value Pairs
> AVP: t=User-Name(1) l=14 val=6c7e67b72d29
> AVP: t=User-Password(2) l=18 val=Encrypted
> AVP: t=Service-Type(6) l=6 val=Call-Check(10)
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
> AVP: t=Framed-MTU(12) l=6 val=1485

Pacchetto Radius

Esempio di errore di autenticazione MAC per un dispositivo client

Autenticazione Mac avviata per un client dopo l'associazione

2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Success
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cli
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]

ISE invierebbe un messaggio di rifiuto dell'accesso poiché questa voce relativa al dispositivo non è presente in ISE

2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000

Autenticazione Web avviata per il dispositivo client a causa di un errore MAB

2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cli

Dopo che il client ha avviato una richiesta HTTP GET, l'URL di reindirizzamento viene inviato al dispositivo client quando la sessione TCP corrispondente viene oggetto di spoofing da parte del controller.

2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6

Il client avvia una richiesta HTTP Get all'URL di reindirizzamento e, una volta che la pagina ha caricato le credenziali di login, le invia.

Il controller invia una richiesta di accesso ad ISE

Questa è un'autenticazione Web, in quanto viene osservato un nome utente valido nel pacchetto Access-Accept

2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco

Access-Accept ricevuto da ISE

2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato

Autenticazione Web completata e transizione dello stato client allo stato RUN

2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db

Verifica tramite acquisizioni EPC

Il client completa l'handshake TCP con l'indirizzo IP virtuale del controller e carica la pagina del portale di reindirizzamento. Una volta che l'utente ha inviato nome utente e password, possiamo osservare una richiesta di accesso radius dall'indirizzo IP di gestione del controller.

Dopo l'autenticazione, la sessione TCP del client viene chiusa e sul controller il client passa allo stato RUN.

15649	08:52:51.122979	10.76.6.150	192.0.2.1	TCP	58832 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=4022788869 TSecr=0 SACK_PERM
15650	08:52:51.123986	192.0.2.1	10.76.6.150	TCP	443 → 58832 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3313564363 TSecr=402
15651	08:52:51.125985	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=4022788871 TSecr=3313564363
15652	08:52:51.126992	10.76.6.150	192.0.2.1	512	TLSv1.2 Client Hello
15653	08:52:51.126992	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313564366 TSecr=4022788871
15654	08:52:51.126992	192.0.2.1	10.76.6.150	85,1,64	TLSv1.2 Server Hello, Change Cipher Spec, Encrypted Handshake Message
15655	08:52:51.129982	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=518 Ack=166 Win=131008 Len=0 TSval=4022788876 TSecr=3313564367
15656	08:52:51.129982	10.76.6.150	192.0.2.1	1,64	TLSv1.2 Change Cipher Spec, Encrypted Handshake Message
15657	08:52:51.130989	10.76.6.150	192.0.2.1	640	TLSv1.2 Application Data
15658	08:52:51.130989	10.76.6.150	192.0.2.1	160	TLSv1.2 Application Data
15659	08:52:51.130989	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64000 Len=0 TSval=3313564371 TSecr=4022788876
15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3
15665	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment o
15666	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1114 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment i
15667	08:52:51.191976	192.0.2.1	10.76.6.150	2496	TLSv1.2 Application Data
15668	08:52:51.192983	192.0.2.1	10.76.6.150	48	TLSv1.2 Encrypted Alert
15673	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2667 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15674	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2721 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15675	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58832 → 443 [ACK] Seq=1403 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=331356
15676	08:52:51.197987	10.76.6.150	192.0.2.1	48	TLSv1.2 Encrypted Alert
15677	08:52:51.197987	10.76.6.150	192.0.2.1	TCP	58832 → 443 [FIN, ACK] Seq=1456 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15678	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0
15679	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0

Flusso TCP con pacchetto radius

15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3

Frame 15660: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol

Code: Access-Request (1)
Packet identifier: 0x3 (3)
Length: 457
Authenticator: fd400f7e3567dc5a63cfefaeaf379eaa
[\[The response to this request is in frame 15663\]](#)
Attribute Value Pairs
AVP: t=Calling-Station-Id(31) l=19 val=6c-7e-67-e3-6d-b9
AVP: t=User-Name(1) l=10 val=testuser
AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
AVP: t=Framed-IP-Address(8) l=6 val=10.76.6.150
AVP: t=Message-Authenticator(30) l=16 val=501b124c30216efd5973086d99f3a185
> AVP: t=Service-Type(6) l=6 val=Dialog-Framed-User(5)
> AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
> AVP: t=User-Password(2) l=18 val=Encrypted

Pacchetto Radius inviato ad ISE con credenziali utente

L'acquisizione wireshark sul lato client per verificare il traffico del client viene reindirizzata alla pagina del portale e convalidata l'handshake TCP per l'indirizzo IP virtuale/server Web del controller

Time	Source	Destination	Length	Protocol	Info
105	08:51:34.203945	10.76.6.150	10.76.6.145	HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
108	08:51:34.206602	10.76.6.150	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)
234	08:51:39.028084	10.76.6.150	7.7.7.7	HTTP	GET / HTTP/1.1
236	08:51:39.031420	7.7.7.7	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)

Frame 108: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface en0, id 0
 Ethernet II, Src: Cisco_34:90:e7 (6c:5e:3b:34:90:e7), Dst: Apple_e3:6d:b9 (6c:7e:67:e3:6d:b9)
 Internet Protocol Version 4, Src: 10.76.6.145, Dst: 10.76.6.150
 Transmission Control Protocol, Src Port: 80, Dst Port: 58811, Seq: 1, Ack: 107, Len: 637

Hypertext Transfer Protocol

Line-based text data: text/html (9 lines)

```
<HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8" name="viewport" content="width=device-width, initial-scale=1">\n
<HEAD>\n
<TITLE> Web Authentication Redirect</TITLE>\n
<META http-equiv="Cache-control" content="no-cache">\n
<META http-equiv="Pragma" content="no-cache">\n
<META http-equiv="Expires" content="-1">\n
<META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://10.76.6.145/auth/discovery?architecture=9">\n
</HEAD>\n
</HTML>
```

Acquisizione sul lato client per convalidare l'URL di reindirizzamento

Il client stabilisce l'handshake TCP all'indirizzo IP virtuale del controller

Time	Source	Destination	Length	Protocol	Info
115	08:51:34.208377	10.76.6.150	192.0.2.1	TCP	58812 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_PERM
117	08:51:34.211190	192.0.2.1	10.76.6.150	TCP	443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSecr=0
118	08:51:34.211275	10.76.6.150	192.0.2.1	TCP	58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120	08:51:34.212673	10.76.6.150	192.0.2.1	512	TLSv1.2 Client Hello
122	08:51:34.217896	192.0.2.1	10.76.6.150	TCP	443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124	08:51:34.220834	192.0.2.1	10.76.6.150	89,830	TLSv1.2 Server Hello, Certificate
125	08:51:34.220835	192.0.2.1	10.76.6.150	7834	TLSv1.2 Server Key Exchange, Server Hello Done

Handshake TCP tra il client e il server Web

La sessione viene chiusa dopo l'autenticazione Web,

144	08:51:34.235915	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=0
145	08:51:34.235996	10.76.6.150	192.0.2.1	52	TLSv1.2 Encrypted Alert
146	08:51:34.236029	10.76.6.150	192.0.2.1	TCP	58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147	08:51:34.238965	192.0.2.1	10.76.6.150	52	TLSv1.2 Encrypted Alert
148	08:51:34.238966	192.0.2.1	10.76.6.150	TCP	443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655

Sessione TCP chiusa dopo il completamento dell'autenticazione Web del client

Articolo correlato

[Comprendere i debug wireless e la raccolta dei log sui controller LAN wireless Catalyst 9800](#)

[Autenticazione basata su Web su 9800](#)

[Configura autenticazione Web locale su 9800](#)

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).