

Configurazione di 9800 WLC e Aruba ClearPass - Accesso guest e FlexConnect

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Flusso del traffico per la distribuzione Enterprise guest CWA](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurazione dei parametri di Guest Wireless Access C9800](#)

[C9800 - Configurazione AAA per guest](#)

[C9800 - Configurazione dell'ACL di reindirizzamento](#)

[C9800 - Configurazione profilo WLAN guest](#)

[C9800 - Definizione profilo criteri guest](#)

[C9800 - Codice](#)

[C9800 - Profilo di join AP](#)

[C9800 - Flex Profile](#)

[C9800 - Tag sito](#)

[C9800 - Profilo RF](#)

[C9800 - Assegna tag all'access point](#)

[Configura istanza di Aruba CPPM](#)

[Configurazione iniziale di Aruba ClearPass Server](#)

[Richiedi licenza](#)

[Nome host server](#)

[Genera certificato server Web CPPM \(HTTPS\)](#)

[Definisci C9800 WLC come dispositivo di rete](#)

[Pagina portale guest e timer CoA](#)

[ClearPass - Configurazione CWA guest](#)

[Attributo metadati endpoint ClearPass: Allow-Guest-Internet](#)

[Configurazione criterio di imposizione riautenticazione ClearPass](#)

[Configurazione profilo di applicazione reindirizzamento portale guest ClearPass](#)

[Configurazione profilo di imposizione metadati ClearPass](#)

[Configurazione criteri di imposizione accesso a Internet guest ClearPass](#)

[Configurazione dei criteri di imposizione Post-AUP guest ClearPass](#)

[Configurazione del servizio di autenticazione MAB ClearPass](#)

[Configurazione servizio ClearPass Webauth](#)

[ClearPass - Accesso Web](#)

[Verifica - Autorizzazione CWA Guest](#)

[Appendice](#)

Introduzione

In questo documento viene descritta l'integrazione di Catalyst 9800 Wireless LAN Controller (WLC) con Aruba ClearPass per fornire SSID (Guest Wireless Service Set Identifier) che sfrutta l'autenticazione Web centrale (CWA) ai client wireless in una modalità di distribuzione Flexconnect del punto di accesso (AP).

L'autenticazione wireless degli utenti guest è supportata dal portale degli utenti guest mediante una pagina di criteri utente accettabili anonimi (AUP), ospitata in Aruba Clearpass in un segmento DMZ (Secure Demilitarized Zone).

Prerequisiti

In questa guida si presume che questi componenti siano stati configurati e verificati:

- Tutti i componenti pertinenti vengono sincronizzati con il protocollo NTP (Network Time Protocol) e verificati per verificare che abbiano l'ora corretta (necessaria per la convalida del certificato)
- Server DNS operativo (richiesto per i flussi di traffico guest, convalida CRL (Certificate Revocation List))
- Server DHCP operativo
- CA (Certification Authority) facoltativa (necessaria per firmare il portale guest CPPM)
- Catalyst 9800 WLC
- Aruba ClearPass Server (richiede licenza della piattaforma, licenza di accesso, licenza integrata)
- Vmware ESXi

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Distribuzione C9800 e nuovo modello di configurazione
- Switching Flexconnect su C9800
- Autenticazione CWA 9800 (fare riferimento a <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html>)

Componenti usati

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

- Cisco Catalyst C9800-L-C con 17.3.4c
- Cisco Catalyst C9130AX
- Aruba ClearPass, patch 6-8-0-109592 e 6.8-3
- Server MS Windows Active Directory (Criteri di gruppo configurati per il rilascio automatico di

certificati basati su computer agli endpoint gestiti) Server DHCP con opzione 43 e opzione 60 Server DNS Server NTP per sincronizzare l'ora di tutti i componenti La CA

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

Il diagramma fornisce i dettagli degli scambi di accesso Wifi guest prima che l'utente guest sia autorizzato ad accedere alla rete:

1. L'utente guest si associa alla Wifi guest in una sede remota.
2. La richiesta di accesso RADIUS iniziale viene inoltrata da C9800 al server RADIUS.
3. Il server cerca l'indirizzo MAC guest fornito nel database degli endpoint MAC locale. Se l'indirizzo MAC non viene trovato, il server risponde con un profilo MAB (MAC Authentication Bypass). Questa risposta RADIUS include:
 - ACL (Redirect Access Control List)
 - Reindirizzamento URL
4. Il client passa attraverso il processo di apprendimento IP in cui gli viene assegnato un indirizzo IP.
5. C9800 esegue la transizione del client guest (identificato dall'indirizzo MAC) allo stato 'Web Auth Pending'.
6. La maggior parte dei moderni sistemi operativi per dispositivi, in associazione con le WLAN guest, esegue una sorta di rilevamento di portale vincolato. L'esatto meccanismo di rilevamento dipende dall'implementazione specifica del sistema operativo. Il sistema operativo del client apre una finestra di dialogo a comparsa (pseudo browser) con una pagina reindirizzata da C9800 all'URL del portale guest ospitato dal server RADIUS fornito come parte della risposta di accesso e accettazione RADIUS.
7. L'utente guest accetta i termini e le condizioni nella schermata popup visualizzata. ClearPass imposta un flag per l'indirizzo MAC del client nel suo database di endpoint (DB) per indicare che il client ha completato un'autenticazione e avvia un Cambio di autorizzazione RADIUS (CoA), selezionando un'interfaccia basata sulla tabella di routing (se in ClearPass sono presenti più interfacce).
8. Il client guest WLC passa allo stato 'Esegui' e all'utente viene concesso l'accesso a Internet senza ulteriori reindirizzamenti.

Nota: Per il diagramma di flusso dello stato di Cisco 9800 Foreign, Anchor Wireless Controller con RADIUS e il portale guest ospitato esternamente, fare riferimento alla sezione Appendice di questo articolo.

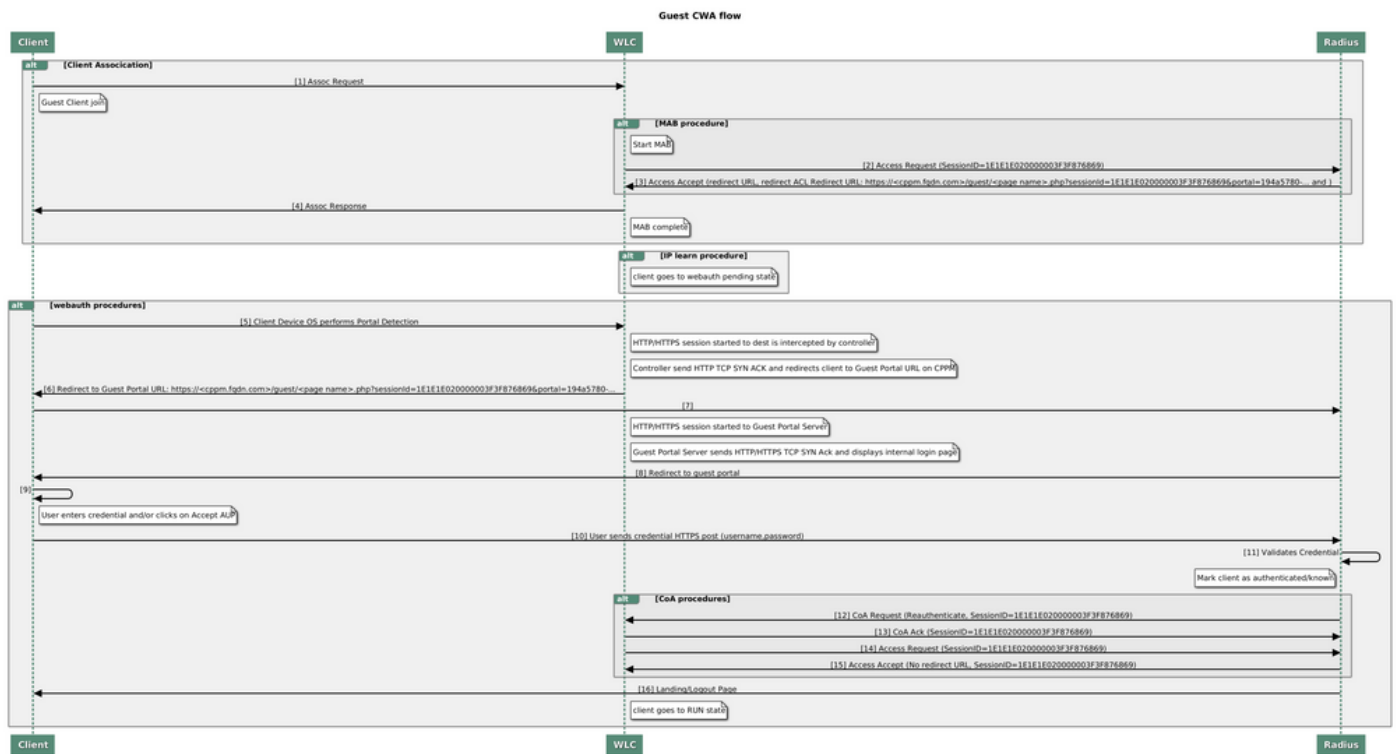


Diagramma di stato di Guest Central Web Authentication (CWA)

Flusso del traffico per la distribuzione Enterprise guest CWA

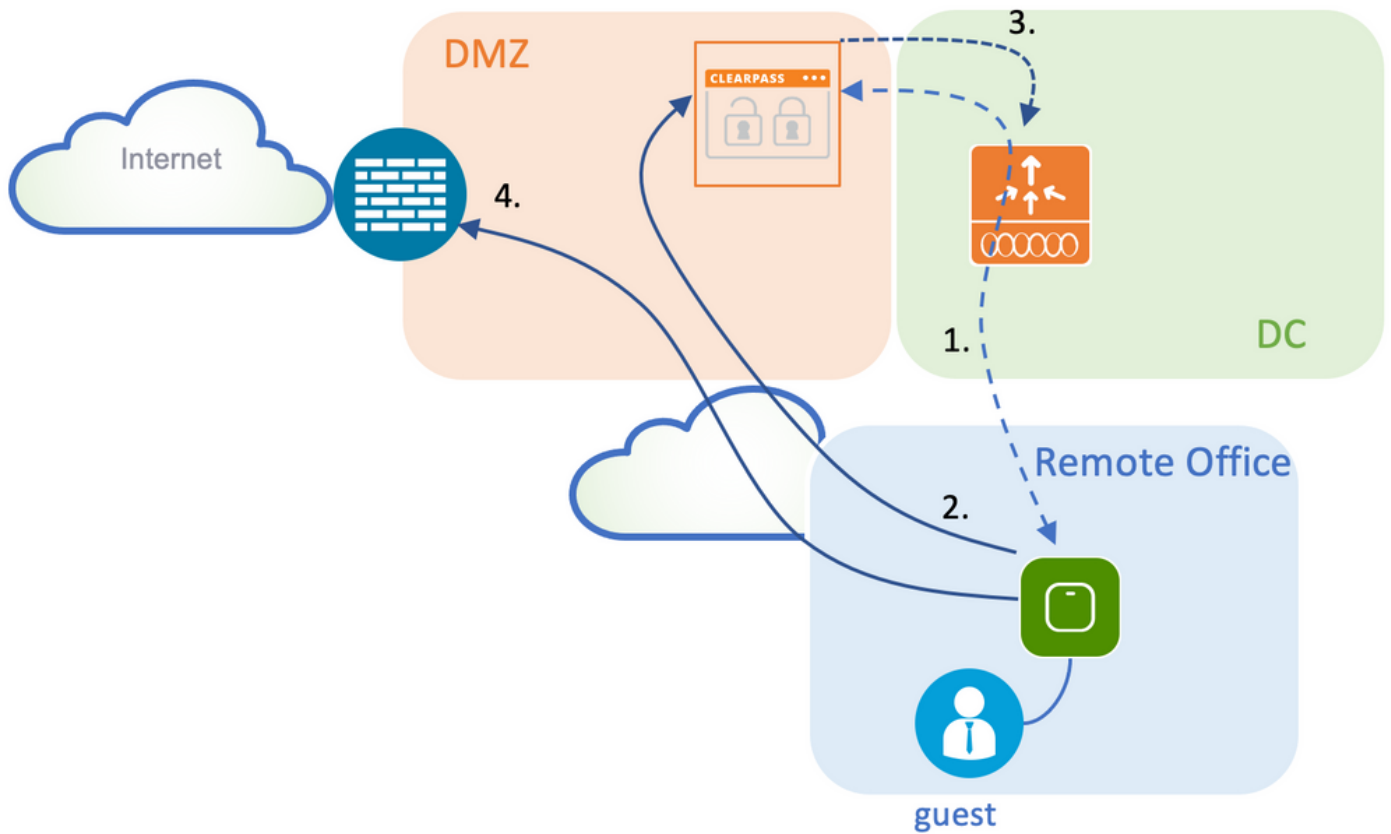
In un'installazione aziendale tipica con più filiali, ogni filiale è configurata per fornire un accesso segmentato e sicuro ai guest tramite un portale guest una volta che il guest accetta il contratto di licenza.

In questo esempio di configurazione, 9800 CWA viene utilizzato per l'accesso guest tramite l'integrazione in un'istanza ClearPass separata, implementata esclusivamente per gli utenti guest nella DMZ protetta della rete.

Gli ospiti devono accettare i termini e le condizioni stabiliti nel portale pop-up di consenso Web fornito dal server DMZ ClearPass. In questo esempio di configurazione viene illustrato il metodo di accesso guest anonimo, ovvero non è necessario immettere nome utente e password guest per l'autenticazione al portale guest.

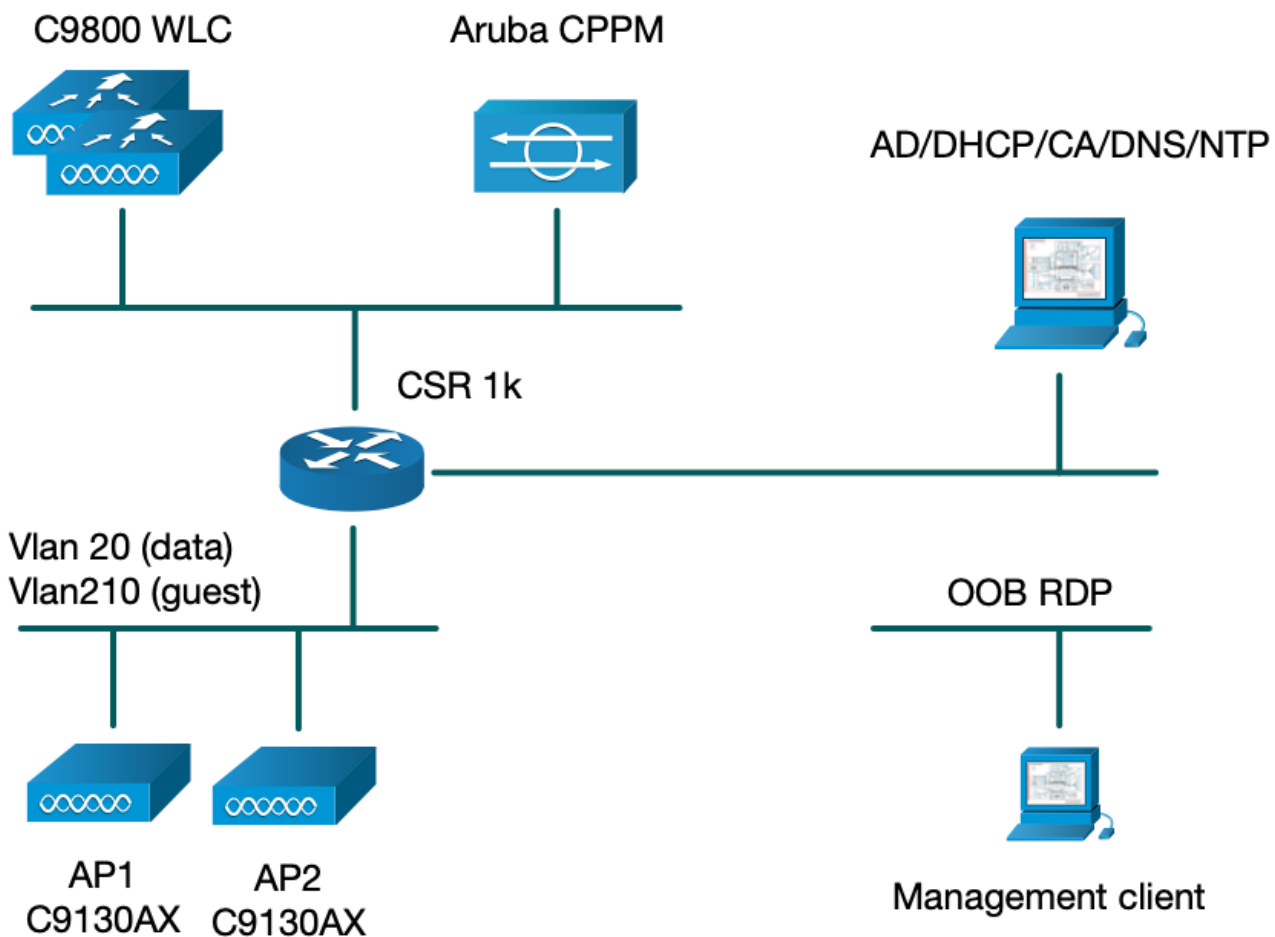
Il flusso del traffico che corrisponde a questa distribuzione è mostrato nell'immagine:

1. RAGGIO - Fase MAB
2. Reindirizzamento dell'URL del client guest al portale guest
3. Dopo l'accettazione da parte degli utenti guest del contratto di licenza sul portale per gli utenti guest, il certificato di riautenticazione RADIUS CoA viene rilasciato da CPPM a 9800 WLC
4. Agli ospiti è consentito l'accesso a Internet



Esempio di rete

Nota: Ai fini delle demo di laboratorio, viene utilizzata un'istanza singola o combinata del server Aruba CPPM per servire le funzioni del server di accesso alla rete (NAS) Guest e Corp SSID. L'implementazione di best practice suggerisce istanze NAS indipendenti.



Configurazione

In questo esempio di configurazione, viene utilizzato un nuovo modello di configurazione su C9800 per creare i profili e i tag necessari per fornire accesso aziendale dot1x e accesso guest CWA alla filiale aziendale. La configurazione risultante è riepilogata in questa immagine:

AP
MAC: XXXX.XXXX.XXXX

Policy Tag: PT_CAN01

WLAN Profile: WP_Guest
SSID: Guest
Layer 2: Security None
Layer 2: MAC Filtering Enabled
Authz List: AAA_Authz-CPPM

Policy Profile: PP_Guest
Central Switching: Disabled
Central Auth: Enabled
Central DHCP: Disabled
Vlan: guest (21)
AAA Policy: Allow AAA Override Enabled
AAA Policy: NAC State Enabled
AAA Policy: NAC Type RADIUS
AAA Policy Accounting List: Guest_Accounting

Site Tag: ST_CAN01
Enable Local Site: Off

AP Join Profile: MyApProfile
NTP Server: 10.0.10.4

Flex Profile: FP_CAN01
Native Vlan 2
Policy ACL: CAPTIVE_PORTAL_REDIRECT,
ACL CWA: Enabled
VLAN: 21 (Guest)

RF Tag: Branch_RF

5GHz Band RF: Typical_Client_Density_rf_5gh

2GHz Band RF: Typical_Client_Density_rf_2gh

Configurazione dei parametri di Guest Wireless Access C9800

C9800 - Configurazione AAA per guest

Nota: Per quanto riguarda l'ID bug Cisco [CSCvh03827](#), verificare che i server di autenticazione, autorizzazione e accounting (AAA) definiti non abbiano un bilanciamento del carico, in quanto il meccanismo si basa sulla persistenza di SessionID in WLC per gli scambi ClearPass RADIUS.

Passaggio 1. Aggiungere i server DMZ Aruba ClearPass alla configurazione WLC del 9800 e creare un elenco di metodi di autenticazione. Selezionare **Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Server > +Aggiungi** e immettere le informazioni sui server RADIUS.

Create AAA Radius Server ✕

Name*	<input type="text" value="CPPM"/>
Server Address*	<input type="text" value="10.85.54.98"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Clear Text"/>
Key* (i)	<input type="text" value="....."/>
Confirm Key*	<input type="text" value="....."/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

↶ Cancel

📄 Apply to Device

Passaggio 2. Definire il gruppo di server AAA per i guest e assegnare il server configurato nel passaggio 1 a questo gruppo di server. Selezionare **Configurazione > Sicurezza > AAA > Server/Gruppi > RADIUS > Gruppi > +Aggiungi**.

Create AAA Radius Server Group ✕

Name*	<input type="text" value="AAA_Radius_CPPM "/>
Group Type	<input type="text" value="RADIUS"/>
MAC-Delimiter	<input type="text" value="none"/>
MAC-Filtering	<input type="text" value="none"/>
Dead-Time (mins)	<input type="text" value="5"/>
Source Interface VLAN ID	<input type="text" value="1"/>

Available Servers

Assigned Servers



CPPM



↶ Cancel

📄 Apply to Device

Passaggio 3. Definire un elenco di metodi di autorizzazione per l'accesso guest e mappare il gruppo di server creato nel passaggio 2. Passare a **Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione > +Aggiungi**. Selezionare **Tipo di rete**, quindi **Gruppo server AAA** configurato nel passaggio 2.

Quick Setup: AAA Authorization ✕

Method List Name*

Type* network (i)

Group Type (i)

Fallback to local

Authenticated

Available Server Groups Assigned Server Groups

radius ldap tacacs+	> < >> <<	AAA_Radius_CPPM	^ ^ v v
---------------------------	--------------------	-----------------	------------------

Passaggio 4. Creare un elenco di metodi contabili per l'accesso guest e mappare il gruppo di server creato nel passaggio 2. Passare a **Configurazione > Sicurezza > AAA > Elenco metodi AAA > Contabilità > +Aggiungi**. Selezionare **Type Identity** (Identità tipo) dal menu a discesa, quindi **AAA Server Group** (Gruppo server AAA) configurato nel passo 2.

Quick Setup: AAA Accounting ✕

Method List Name*

Type* identity (i)

Available Server Groups Assigned Server Groups

radius ldap tacacs+	> < >> <<	AAA_Radius_CPPM	^ ^ v v
---------------------------	--------------------	-----------------	------------------

L'ACL di reindirizzamento definisce il traffico che deve essere reindirizzato al portale guest rispetto a quello che può passare senza reindirizzamento. In questo caso, il rifiuto dell'ACL implica il bypass del reindirizzamento o del pass-through, mentre il rifiuto dell'autorizzazione implica il reindirizzamento al portale. Per ciascuna classe di traffico, è necessario considerare la direzione del traffico quando si creano le voci di controllo di accesso (ACE, Access Control Entries) e le voci di controllo di accesso (ACE, Access Control Entries) che corrispondono sia al traffico in entrata che al traffico in uscita.

Passare a **Configurazione > Sicurezza > ACL** e definire un nuovo ACL denominato **CAPTIVE_PORTAL_REDIRECT**. Configurare l'ACL con le seguenti ACE:

- ACE1: Consente al traffico ICMP (Internet Control Message Protocol) bidirezionale di ignorare il reindirizzamento ed è utilizzato principalmente per verificare la raggiungibilità.
- ACE10, ACE30: Consente il flusso del traffico DNS bidirezionale verso il server DNS 10.0.10.4 e non viene reindirizzato al portale. Per attivare il flusso guest sono necessarie una ricerca DNS e un'intercettazione per la risposta.
- ACE70, ACE80, ACE110, ACE120: Consente l'accesso HTTP e HTTPS al portale captive guest per la presentazione dell'utente al portale.
- ACE150: Tutto il traffico HTTP (porta UDP 80) viene reindirizzato.

Sequence ▲	Action ▼	Source IP ▼	Source Wildcard ▼	Destination IP ▼	Destination Wildcard ▼	Protocol ▼	Source Port ▼	Destination Port ▼
1	deny	any		any		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

C9800 - Configurazione profilo WLAN guest

Passaggio 1. Passare a **Configurazione > Tag e profili > Wireless > +Aggiungi**. Creare un nuovo profilo SSID WP_Guest, con la trasmissione di SSID 'Guest' a cui i client guest associano.

Add WLAN ✕

General Security Advanced

Profile Name*	<input type="text" value="WP_Guest"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="Guest"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="3"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Nella stessa finestra di dialogo **Aggiungi WLAN**, selezionare la scheda **Sicurezza > Layer 2**.

- Modalità di sicurezza layer 2: Nessuna

- Filtro MAC: Attivato

- Elenco autorizzazioni: AAA_Authz_CPPM dal menu a discesa (configurato al punto 3. come parte della configurazione AAA)

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input checked="" type="checkbox"/>	Fast Transition	<input type="text" value="Adaptive Enab..."/>
OWE Transition Mode	<input checked="" type="checkbox"/>	Over the DS	<input type="checkbox"/>
Transition Mode WLAN ID*	<input type="text" value="1-4096"/>	Reassociation Timeout	<input type="text" value="20"/>
Authorization List*	<input type="text" value="AAA_Authz_C"/>		

C9800 - Definizione profilo criteri guest

Dalla GUI del WLC di C9800, selezionare **Configurazione > Tag e profili > Criteri > +Aggiungi**.

Nome: P_Guest

Stato: Attivato

Switching centrale: Disattivato

Autenticazione centrale: Attivato

DHCP centrale: Disattivato

Associazione centrale: Disattivato

Add Policy Profile ✕

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

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	<input type="text" value="PP_Guest"/>	WLAN Switching Policy	
Description	<input type="text" value="Policy Profile for Guest"/>	Central Switching	<input type="checkbox"/> DISABLED
Status	<input checked="" type="checkbox"/> ENABLED	Central Authentication	<input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Central Association	<input type="checkbox"/> DISABLED
CTS Policy		Flex NAT/PAT	<input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

Add Policy Profile ✕

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General Access Policies QOS and AVC Mobility Advanced

Name*	PP_Guest	WLAN Switching Policy
Description	Profile for Branch Guest	Central Switching <input type="checkbox"/> DISABLED
Status	<input type="checkbox"/> DISABLED	Central Authentication ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP <input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Central Association <input type="checkbox"/> DISABLED
CTS Policy		Flex NAT/PAT <input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	2-65519	

Passare alla scheda **Criteri di accesso** nella stessa finestra di dialogo **Aggiungi profilo criterio**.

- Profilatura RADIUS: Attivato

- Gruppo VLAN/VLAN: 210 (ossia, la VLAN 210 è la VLAN locale guest a ciascuna postazione di succursale)

Nota: La VLAN guest per Flex non deve essere definita sul WLC 9800 in VLAN, nel numero di VLAN del tipo di gruppo VLAN/VLAN.

Difetto noto: l'ID bug Cisco [CSCvn48234](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvn48234) impedisce la trasmissione dell'SSID se la stessa VLAN guest Flex è definita in WLC e nel profilo Flex.

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

210 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

↶ Cancel

📄 Apply to Device

Nella stessa finestra di dialogo **Aggiungi profilo criterio**, passare alla scheda **Avanzate**.

- Consenti sostituzione AAA: Attivato
- Stato NAC: Attivato
- Tipo NAC: RAGGIO
- Elenco contabile: AAA_Accounting_CPPM (definito nel passaggio 4 come parte della configurazione AAA)

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

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

WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>
Guest LAN Session Timeout	<input type="checkbox"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

Show more >>>

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input checked="" type="checkbox"/>
NAC Type	<input type="text" value="RADIUS"/>
Policy Name	<input type="text" value="default-aaa-policy"/>
Accounting List	<input type="text" value="AAA_Accounting_"/>

Fabric Profile

mDNS Service Policy

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map [Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

Nota: Per abilitare il WLC C9800 per accettare i messaggi RADIUS CoA, è necessario lo stato 'NAC (Network Admission Control) - Abilita'.

C9800 - Codice

Dalla GUI di C9800, selezionare **Configurazione > Tag e profili > Tag > Criteri > +Aggiungi**.

-Nome: PT_CAN01

-Descrizione: Codice di matricola per il sito di succursale CAN01

Nella stessa finestra di dialogo **Add Policy Tag**, in **WLAN-POLICY MAPS**, fare clic su **+Add**, quindi mappare il profilo WLAN creato in precedenza a Policy Profile:

- Profilo WLAN: Ospite_PL
- Profilo delle politiche: P_Guest

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

➤ RLAN-POLICY Maps: 0

C9800 - Profilo di join AP

Dalla GUI del WLC di C9800, selezionare **Configurazione > Tag e profili > AP Join > +Aggiungi**.

-Nome: Profilo_AP_diramazione

- Server NTP: 10.0.10.4 (fare riferimento al diagramma della topologia lab). Server NTP utilizzato dagli access point nel branch per la sincronizzazione.

Add AP Join Profile ✕

General Client CAPWAP AP Management Security ICap QoS

Name*

Description

LED State

LAG Mode

NTP Server

GAS AP Rate Limit

Apphost


OfficeExtend AP Configuration

Local Access

Link Encryption

Rogue Detection

 Cancel

 Apply to Device

C9800 - Flex Profile

I profili e i tag sono modulari e possono essere riutilizzati per più siti.

Nel caso dell'implementazione di FlexConnect, se si utilizzano gli stessi ID VLAN in tutti i siti di succursale, è possibile riutilizzare lo stesso profilo flessibile.

Passaggio 1. Su un'interfaccia GUI WLC C9800, selezionare **Configurazione > Tag e profili > Flex > +Aggiungi**.

-Nome: FP_Branch

- ID VLAN nativo: 10 (richiesto solo se si dispone di una VLAN nativa non predefinita in cui si desidera disporre di un'interfaccia di gestione AP)

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name* Fallback Radio Shut

Description Flex Resilient

Native VLAN ID ARP Caching

HTTP Proxy Port Efficient Image Upgrade

HTTP-Proxy IP Address OfficeExtend AP

CTS Policy Join Minimum Latency

Inline Tagging IP Overlap

SGACL Enforcement mDNS Flex Profile

CTS Profile Name

Nella stessa finestra di dialogo **Aggiungi profilo Flex**, passare alla scheda **ACL criterio** e fare clic su **+Aggiungi**.

- Nome ACL: CAPTIVE_PORTAL_REDIRECT

- Central Web Auth: Attivato

In un'implementazione di Flexconnect, ogni access point gestito deve scaricare l'ACL di reindirizzamento localmente quando il reindirizzamento avviene sull'access point e non sul C9800.

Add Flex Profile ✕

General Local Authentication **Policy ACL** VLAN Umbrella

ACL Name	Central Web Auth	Pre Auth URL Filter
0	<input checked="" type="checkbox"/>	

10 items per page No items to display

ACL Name*

Central Web Auth

Pre Auth URL Filter

Nella stessa finestra di dialogo **Add Flex Profile**, passare alla scheda **VLAN** e fare clic su **+Add** (fare riferimento al diagramma della topologia lab).

- Nome VLAN: ospite

- ID VLAN: 210

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
<input type="checkbox"/> data	2	

1 10 items per page
1 - 1 of 1 items

VLAN Name*

VLAN Id*

ACL Name

✓ Save ↶ Cancel

↶ Cancel Apply to Device

C9800 - Tag sito

Sulla GUI del WLC 9800, selezionare **Configurazione > Tag e profili > Tag > Sito > Aggiungi**.

Nota: Creare un codice di matricola univoco per ogni sito remoto che deve supportare i due SSID wireless come descritto.

Esiste un mapping 1-1 tra una posizione geografica, un tag del sito e una configurazione Flex Profile.

A un sito di connessione flessibile deve essere associato un profilo di connessione flessibile. È possibile disporre di un massimo di 100 punti di accesso per ogni sito flex connect.

-Nome: ST_CAN01

- Profilo di join AP: Profilo_AP_diramazione

- Profilo Flex: FP_Branch

- Attiva sito locale: Disattivato

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel Apply to Device

C9800 - Profilo RF

Sulla GUI del WLC 9800, selezionare **Configurazione > Tag e profili > Tag > RF > Aggiungi**.

-Nome: Ramo_RF

- Profilo a radiofrequenza (RF) su banda 5 GHz: Typical_Client_Density_5gh (opzione definita dal sistema)

- Profilo RF su banda 2,4 GHz: Typical_Client_Density_2gh (opzione definita dal sistema)

The screenshot shows the 'Add RF Tag' configuration window. The fields are as follows:

Name*	Branch_RF
Description	Typical Branch RF
5 GHz Band RF Profile	Client_Density_rf_5gh
2.4 GHz Band RF Profile	Typical_Client_Densi

Buttons: Cancel, Apply to Device

C9800 - Assegna tag all'access point

Per assegnare tag definiti ai singoli access point nella distribuzione, sono disponibili due opzioni:

- Assegnazione basata sul nome AP, che sfrutta le regole regex che corrispondono ai pattern nel campo Nome AP (**Configura > Tag e profili > Tag > AP > Filtro**)

- Assegnazione basata sull'indirizzo MAC Ethernet AP (**Configurazione > Tag e profili > Tag > AP > Statico**)

Nell'implementazione di produzione con DNA Center, si consiglia di utilizzare DNAC e il flusso di lavoro PNP AP oppure un metodo di caricamento statico con valori delimitati da virgole (CSV) disponibile nel modello 9800 per evitare l'assegnazione manuale per punto di accesso. Selezionare **Configura > Tag e profili > Tag > AP > Statico > Aggiungi** (notare l'opzione **Carica file**).

- Indirizzo MAC AP: <AP_ETHERNET_MAC>

- Nome tag criteri: PT_CAN01

- Nome tag sito: ST_CAN01

- Nome tag RF: Ramo_RF

Nota: A partire dalla versione Cisco IOS®-XE 17.3.4c, il numero massimo di regole regex è 1000 per limitazione del controller. Se il numero di siti nella distribuzione supera questo numero, è necessario utilizzare l'assegnazione statica per MAC.

Associate Tags to AP



AP MAC Address*	aaaa.bbbb.cccc
Policy Tag Name	PT_CAN01
Site Tag Name	ST_CAN01
RF Tag Name	Branch_RF

Cancel

Apply to Device

Nota: In alternativa, per utilizzare il metodo di assegnazione dei tag basato su regex di nome AP, selezionare **Configura > Tag e profili > Tag > AP > Filtro > Aggiungi**.

-Nome: BR_CAN01

- Nome punto di accesso regex: BR-CAN01-.{7} (questa regola corrisponde alla convenzione del nome AP adottata nell'organizzazione. In questo esempio, i tag vengono assegnati ai punti di accesso che dispongono di un campo Nome punto di accesso contenente 'BR_CAN01-' seguito da sette caratteri qualsiasi.)

-Priority: 1

- Nome tag criteri: PT_CAN01 (come definito)

- Nome tag sito: ST_CAN01

- Nome tag RF: Ramo_RF

Associate Tags to AP



⚠ Rule "BR-CAN01" has this priority. Assigning it to the current rule will swap the priorities.

Rule Name*	BR_CAN01	Policy Tag Name	PT_CAN01	x	▼
AP name regex*	BR-CAN01-.{7}	Site Tag Name	ST_CAN01	x	▼
Active	YES	RF Tag Name	Branch_RF	x	▼
Priority*	1				

Cancel

Apply to Device

Configura istanza di Aruba CPPM

Per la configurazione di Aruba CPPM basata su procedure ottimali/produzione, contattare la risorsa locale HPE Aruba SE.

Configurazione iniziale di Aruba ClearPass Server

Aruba ClearPass viene implementato con il modello OVF (Open Virtualization Format) sul server ESXi <> che alloca queste risorse:

- Due CPU virtuali riservate
- 6 GB di RAM
- Disco da 80 GB (deve essere aggiunto manualmente dopo la distribuzione iniziale della VM prima che la macchina venga accesa)

Richiedi licenza

Applicare la licenza della piattaforma tramite: **Amministrazione > Server Manager > Licenze**.
Aggiungere **licenze di piattaforma, accesso e integrate**.

Nome host server

Passare a **Amministrazione > Server Manager > Configurazione server** e scegliere il server CPPM con il nuovo provisioning.

- Nome host: cppm

- FQDN: cppm.example.com

- Verifica dell'indirizzamento IP e del DNS della porta di gestione

Administration » Server Manager » Server Configuration - cppm

Server Configuration - cppm (10.85.54.98)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	cppm				
FQDN:	cppm.example.com				
Policy Manager Zone:	default				Manage F
Enable Performance Monitoring Display:	<input checked="" type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input checked="" type="checkbox"/> Enable Insight <input checked="" type="checkbox"/> Enable as Insight Master Current Master:cppm(10.85.54.98)				
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server				
Master Server in Zone:	Primary master				
Span Port:	-- None --				
		IPv4	IPv6	Action	
Management Port	IP Address	10.85.54.98		<input type="button" value="Configure"/>	
	Subnet Mask	255.255.255.224			
	Default Gateway	10.85.54.97			
Data/External Port	IP Address			<input type="button" value="Configure"/>	
	Subnet Mask				
	Default Gateway				
DNS Settings	Primary	10.85.54.122		<input type="button" value="Configure"/>	
	Secondary				
	Tertiary				
	DNS Caching	Disabled			

Genera certificato server Web CPPM (HTTPS)

Questo certificato viene utilizzato quando la pagina di ClearPass Guest Portal viene presentata tramite HTTPS ai client guest che si connettono alla Wifi guest in Branch.

Passaggio 1. Caricare il certificato della catena di pub della CA.

Passare a **Amministrazione > Certificati > Elenco scopi consentiti > Aggiungi**.

- Utilizzo: Abilita altri

View Certificate Details

Subject DN:	
Issuer DN:	
Issue Date/Time:	Dec 23, 2020 16:55:10 EST
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST
Validity Status:	Valid
Signature Algorithm:	SHA256WithRSAEncryption
Public Key Format:	X.509
Serial Number:	86452691282006080280068723651711271611
Enabled:	true
Usage:	<input checked="" type="checkbox"/> EAP <input checked="" type="checkbox"/> RadSec <input checked="" type="checkbox"/> Database <input checked="" type="checkbox"/> Others

Update **Disable** **Export** **Close**

Passaggio 2. Creare la richiesta di firma del certificato.

Selezionare **Amministrazione > Certificati > Archivio certificati > Certificati server > Utilizzo: Certificato server HTTPS**.

- Fare clic su **Create Certificate Signing Request**

- Nome comune: CPPM

- Organizzazione: **cppm.example.com**

Compilare il campo SAN (deve essere presente un nome comune nella SAN, nonché IP e altri

FQDN in base alle esigenze). Il formato è DNS: <fqdn1>,DNS:<fqdn2>,IP<ip1>.

Common Name (CN):	cppm
Organization (O):	Cisco
Organizational Unit (OU):	Engineering
Location (L):	Toronto
State (ST):	ON
Country (C):	CA
Subject Alternate Name (SAN):	DNS:cppm.example.com
Private Key Password:
Verify Private Key Password:
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512

Submit **Cancel**

Passaggio 3. Nella CA scelta, firmare il CSR del servizio HTTPS CPPM appena generato.

Passaggio 4. Passare a **Modello di certificato > Server Web > Importa certificato.**

- Tipo certificato: Certificato server

- Utilizzo: Certificato server HTTP

- File certificato: Individuare e selezionare il certificato del servizio HTTPS CPPM firmato dalla CA

Certificate Type:	Server Certificate
Server:	cppm
Usage:	HTTPS Server Certificate
Upload Method:	Upload Certificate and Use Saved Private Key
Certificate File:	Browse... No file selected.

Import **Cancel**

Definisci C9800 WLC come dispositivo di rete

Selezionare **Configurazione > Rete > Dispositivi > Aggiungi**.

-Nome: WLC_9800_Branch

- Indirizzo IP o subnet: 10.85.54.99 (fare riferimento al diagramma della topologia lab)

- Cisco condiviso RADIUS: <password RADIUS WLC>

- Nome fornitore: Cisco

- Abilitare l'autorizzazione dinamica RADIUS: 1700

Device	SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enforcement	Attributes
Name:	WLC_9800_Branch				
IP or Subnet Address:	10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)				
Description:	Cisco 9800 WLC for Branch Guest Wifi				
RADIUS Shared Secret:		Verify:	
TACACS+ Shared Secret:			Verify:		
Vendor Name:	Cisco				
Enable RADIUS Dynamic Authorization:	<input checked="" type="checkbox"/> Port: 1700				
Enable RadSec:	<input type="checkbox"/>				

Add **Cancel**

Pagina portale guest e timer CoA

È molto importante impostare i valori corretti del timer per tutta la configurazione. Se i timer non sono ottimizzati, è probabile che si verifichi un reindirizzamento ciclico del portale Web con il client non in 'Stato di esecuzione'.

Timer a cui prestare attenzione:

- Timer accesso Web portale: questo timer ritarda il reindirizzamento della pagina prima di consentire l'accesso alla pagina del portale guest per notificare al servizio CPPM la transizione dello stato, registrare il valore dell'attributo personalizzato 'Allow-Guest-Internet' dell'endpoint e attivare il processo CoA da CPPM a WLC. Passare a **Guest > Configurazione > Pagine > Accesso Web**.
 - Scegliere il nome del portale guest: Registrazione utente anonimo Lab (questa configurazione della pagina del portale per gli utenti guest è descritta in dettaglio)
 - Fare clic su **Modifica**
 - Ritardo accesso: 6 secondi

* Login Delay: 6 The time in seconds to delay while displaying the login message.

- Timer ritardo CoA ClearPass: Ciò ritarda la creazione dei messaggi CoA da ClearPass al WLC. Questa operazione è necessaria affinché CPPM esegua internamente la transizione

dello stato dell'endpoint client prima che il riconoscimento CoA (ACK) torni dal WLC. I test Lab mostrano i tempi di risposta al di sotto dei millisecondi dal WLC e, se il CPPM non ha completato l'aggiornamento degli attributi dell'endpoint, la nuova sessione RADIUS dal WLC corrisponde ai criteri di imposizione del servizio MAB non autenticato e al client viene assegnata di nuovo una pagina di reindirizzamento. Passare a **CPPM > Amministrazione > Server Manager > Configurazione server** e scegliere **Server CPPM > Parametri servizio**.

- Ritardo autorizzazione dinamica RADIUS (DM/CoA) - Impostato su 6 secondi

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation options like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Administration > Server Manager > Server Configuration - cppm' and 'Server Configuration - cppm (10.85.54.98)'. Under the 'Service Parameters' tab, a table lists various parameters. The 'RADIUS Dynamic Authorization (DM/CoA) Delay' parameter is highlighted in yellow and set to 6 seconds.

Parameter Name	Parameter Value
Ingress Event	
Batch Processing Interval	30 seconds
Command Control	
RADIUS Dynamic Authorization (DM/CoA) Delay	6 seconds
Enable SNMP Bounce Action	FALSE
Post Auth	
Number of request processing threads	20 threads
Lazy handler polling frequency	5 minutes
Eager handler polling frequency	30 seconds
Connection Timeout	10 seconds
Palo Alto User Identification Timeout	45 minutes

ClearPass - Configurazione CWA guest

La configurazione CWA ClearPass-side è composta da (3) punti/fasi di servizio:

Componente ClearPass	Tipo di servizio	Scopo
1. Responsabile delle politiche	Servizio: Autenticazione Mac	Se l'attributo personalizzato Allow-Guest-Internet = TRUE, consente l'accesso alla rete. In caso contrario, attiva Redirect e COA: Riautentica .
2. Guest	Accessi Web	Presenta la pagina di accesso anonimo AUP. Dopo l'autenticazione imposta l'attributo personalizzato Allow-Guest-Internet = TRUE.
3. Responsabile delle politiche	Servizio: Autenticazione basata sul Web	Aggiorna endpoint su noto . Imposta attributo personalizzato Allow-Guest-Internet = TRUE. CACAO: Riautentica

Attributo metadati endpoint ClearPass: Allow-Guest-Internet

Creare un attributo di metadati di tipo Boolean per tenere traccia dello stato dell'endpoint guest come transizioni client tra lo stato 'Webauth in sospeso' e lo stato 'Eseguiti':

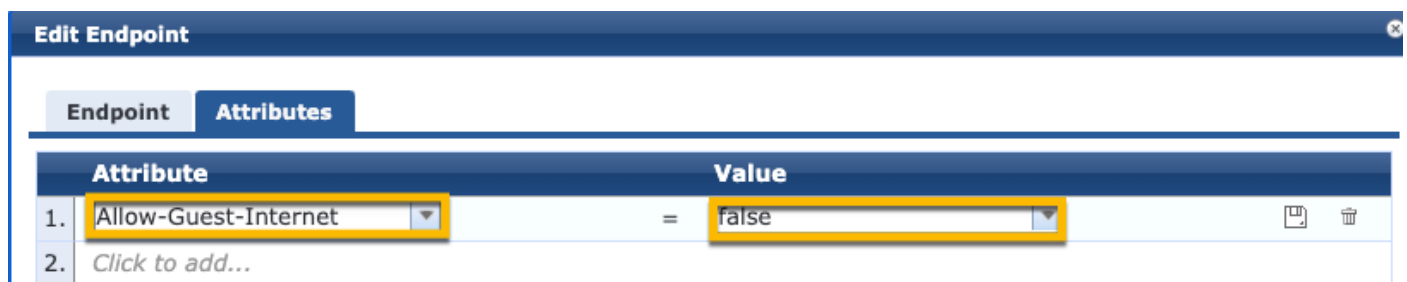
- I nuovi guest che si connettono a wifi hanno un attributo di metadati predefinito impostato su Allow-Guest-Internet=false. In base a questo attributo, l'autenticazione client passa attraverso il

servizio MAB

- Il client guest, quando si fa clic sul pulsante di accettazione AUP, ha il suo attributo metadati aggiornato su Allow-Guest-Internet=true. Il successivo MAB basato su questo attributo impostato su True consente l'accesso non reindirizzato a Internet

Selezionare ClearPass > Configuration > Endpoints, scegliere un endpoint dall'elenco, fare clic sulla scheda **Attributi**, aggiungere **Allow-Guest-Internet** con il valore **false** e **Save**.

Nota: È inoltre possibile modificare lo stesso endpoint ed eliminare questo attributo subito dopo. In questo passaggio viene semplicemente creato un campo nel database di metadati degli endpoint che può essere utilizzato nei criteri.



Configurazione criterio di imposizione riautenticazione ClearPass

Creare un profilo di imposizione assegnato al client guest subito dopo che il client ha accettato le CDS nella pagina Portale guest.

Passare a **ClearPass > Configurazione > Profili > Aggiungi**.

- Modello: Autorizzazione dinamica RADIUS

-Nome: Cisco_WLC_Guest_COA

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Dynamic Authorization	
Name:	Cisco_WLC_Guest_COA	
Description:		
Type:	RADIUS_CoA	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<input type="text"/>	Remove View Details Modify
	--Select--	

Raggio:IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station
Radius:Cisco	Cisco-AVPair	sottoscrittore:comando=riauter
Radius:Cisco	Cisco-AVPair	%{Radius:Cisco:AVPair:subscr audit-session-id}
Radius:Cisco	Cisco-AVPair	sottoscrittore:reauthenticate- type=last-type=last

Configurazione profilo di applicazione reindirizzamento portale guest ClearPass

Creare un profilo di imposizione da applicare al guest durante la fase MAB iniziale, quando l'indirizzo MAC non viene trovato nel database degli endpoint CPPM con 'Allow-Guest-Internet' impostato su **'true'**.

In questo modo, il WLC 9800 reindirizza il client guest al portale guest CPPM per l'autenticazione esterna.

Passare a **ClearPass > Applicazione > Profili > Aggiungi**.

-Nome: Cisco_Portal_Redirect

-Tipo: RAGGIO

-Azione: Accetta

Enforcement Profiles

Profile	Attributes	Summary
Template:	Aruba RADIUS Enforcement	
Name:	Cisco_Portal_Redirect	
Description:		
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<input type="text"/> <input type="text"/> <input type="text"/>	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>
	--Select--	

Profilo di applicazione reindirizzamento ClearPass

Nella stessa finestra di dialogo, nella scheda **Attributi**, configurare due Attributi in base a questa immagine:

Enforcement Profiles - Cisco_Portal_Redirect

Summary	Profile	Attributes
Type	Name	Value
1. Radius: Cisco	Cisco-AVPair	= url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
2. Radius: Cisco	Cisco-AVPair	= url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=%{Radius:IETF:NAS-IP-Address}

Attributi profilo di reindirizzamento ClearPass

L'attributo **url-redirect-acl** è impostato su **CAPTIVE-PORTAL-REDIRECT**, che è il nome dell'ACL creato su C9800.

Nota: Nel messaggio RADIUS viene passato solo il riferimento all'ACL, non il contenuto dell'ACL. È importante che il nome dell'ACL creato sul WLC 9800 corrisponda esattamente al valore di questo attributo RADIUS, come mostrato.

L'attributo **url-redirect** è composto da diversi parametri:

- **URL di destinazione** in cui è ospitato il portale guest, <https://cppm.example.com/guest/iaccept.php>
- **MAC client guest**, macro %{Connection:Client-Mac-Address-Hyphen}
- **Autenticator IP** (9800 WLC attiva il reindirizzamento), macro %{Radius:IETF:NAS-IP-Address}
- azione **cmd-login**

L'URL della pagina di login Web di ClearPass Guest viene visualizzato quando si passa a **CPPM > Guest > Configurazione > Pagine > Accessi Web > Modifica**.

In questo esempio, il nome della pagina del portale guest in CPPM viene definito come **inaccept**.

Nota: La procedura di configurazione della pagina Portale guest è descritta di seguito.

The screenshot shows the Aruba configuration interface. On the left is a navigation menu with categories: Guest, Devices, Onboard, Configuration (highlighted), Authentication, Content Manager, Guest Manager, Hotspot Manager, Pages (expanded to show Fields, Forms, List Views, Self-Registrations, Web Logins, and Web Pages), and Web Pages. The main content area shows the breadcrumb 'Home » Configuration » Pages » Web Logins' and the title 'Web Login (Lab Anonymous Guest Regist)'. Below the title is a subtitle: 'Use this form to make changes to the Web Login **Lab Anon**'. The form contains several fields: '* Name:' with the value 'Lab Anonymous Guest Registration' and a hint 'Enter a name for this web login page.'; 'Page Name:' with the value 'iaccept' (highlighted with a yellow box) and a hint 'Enter a page name for this web login. The web login will be accessible from "/guest/'; 'Description:' with a large empty text area and a hint 'Comments or descriptive text about the web l'; and '* Vendor Settings:' with the value 'Aruba Networks' and a hint 'Select a predefined group of settings suitable'.

Nota: Per i dispositivi Cisco, `audit_session_id` viene normalmente utilizzato, ma questa opzione non è supportata da altri fornitori.

Configurazione profilo di imposizione metadati ClearPass

Configurare Profilo di imposizione per aggiornare l'attributo dei metadati dell'endpoint utilizzato da CPPM per il monitoraggio della transizione dello stato.

Questo profilo viene applicato alla voce Guest Client MAC Address nel database degli endpoint e imposta l'argomento '**Allow-Guest-Internet**' su '**true**'.

Passare a **ClearPass > Applicazione > Profili > Aggiungi**.

- Modello: Applicazione aggiornamento entità ClearPass

-Tipo: Post_autenticazione

Enforcement Profiles

Profile	Attributes	Summary
Template:	ClearPass Entity Update Enforcement	
Name:	Make-Cisco-Guest-Valid	
Description:		
Type:	Post_Authentication	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<input type="text"/> <input type="text"/> <input type="text"/>	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>

Nella stessa finestra di dialogo, selezionare la scheda **Attributi**.

-Tipo: Endpoint

-Nome: Allow-Guest-Internet

Nota: Affinché questo nome venga visualizzato nel menu a discesa, è necessario definire manualmente questo campo per almeno un Endpoint come descritto nella procedura.

-Valore: vero

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Endpoint	Allow-Guest-Internet	= true
2. <i>Click to add...</i>		

Configurazione criteri di imposizione accesso a Internet guest ClearPass

Passare a **ClearPass > Applicazione > Criteri > Aggiungi**.

-Nome: Consenti guest WLC Cisco

- Tipo di applicazione: RAGGIO

- Profilo predefinito: Cisco_Portal_Redirect

Enforcement Policies

Enforcement Rules Summary

Name: WLC Cisco Guest Allow

Description:

Enforcement Type: RADIUS TACACS+ WEBAUTH (SNMP/Agent/CLI/CoA) Application Event

Default Profile: Cisco_Portal_Redirect **View Details** **Modify**

Nella stessa finestra di dialogo passare alla scheda **Regole** e fare clic su **Aggiungi regola**.

-Tipo: Endpoint

-Nome: Allow-Guest-Internet

- Operatore: UGUALE A



- Valore True

- Nomi profilo / Selezionare per aggiungere: [RADIUS] [Consenti accesso al profilo]

Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value	
1.	Endpoint	Allow-Guest-Internet	EQUALS	true	 
2.	Click to add...				

Enforcement Profiles

Profile Names: [RADIUS] [Allow Access Profile]

Move Up ↑
Move Down ↓
Remove

--Select to Add--

Save **Cancel**

Configurazione dei criteri di imposizione Post-AUP guest ClearPass

Passare a **ClearPass > Applicazione > Criteri > Aggiungi**.

-Nome: Policy di applicazione Cisco WLC Webauth

- Tipo di applicazione: WEBAUTH (SNMP/Agent/CLI/CoA)

- Profilo predefinito: [RADIUS_CoA] Cisco_Reauthenticate_Session

Enforcement Policies

Enforcement	Rules	Summary
Name:	Cisco WLC Webauth Enforcement Policy	
Description:		
Enforcement Type:	<input type="radio"/> RADIUS <input type="radio"/> TACACS+ <input checked="" type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event	
Default Profile:	[RADIUS_CoA] Cisco_Reauth	<input type="button" value="View Details"/> <input type="button" value="Modify"/>

Nella stessa finestra di dialogo passare a **Regole > Aggiungi**.

-Condizioni: Autenticazione

-Nome: Stato

- Operatore: UGUALE A

-Valore: Utente

- Nomi profilo: <aggiungi ogni>:

- [Post Authentication] [Update Endpoint Known]
- [Post-autenticazione] [Make-Cisco-Guest-Valid]
- [RADIUS_CoA] [Cisco_WLC_Guest_COA]

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Authentication	Status	EQUALS	User
2.	Click to add...		

Enforcement Profiles

Profile Names:	[Post Authentication] [Update Endpoint Known] [Post Authentication] Make-Cisco-Guest-Valid [RADIUS_CoA] Cisco_WLC_Guest_COA	<input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Remove"/>
	<input type="text" value="--Select to Add--"/>	

Nota: Se si verifica uno scenario con una finestra popup di pseudo browser di reindirizzamento del portale guest continuo, è indicativo del fatto che i timer CPPM richiedano delle modifiche o che i messaggi RADIUS CoA non vengano scambiati correttamente tra CPPM e 9800 WLC. Verificare questi siti.

- Passare a **CPPM > Monitoraggio > Monitoraggio in tempo reale > Access Tracker** e verificare che la voce del registro RADIUS contenga i dettagli di RADIUS CoA.

- In **9800 WLC**, selezionare **Risoluzione dei problemi > Packet Capture**, abilitare pcap sull'interfaccia in cui si prevede l'arrivo dei pacchetti RADIUS CoA e verificare che i messaggi

RADIUS CoA vengono ricevuti dal CPPM.

Configurazione del servizio di autenticazione MAB ClearPass

Il servizio corrisponde alla coppia di valori attributo (AV) Radius: Cisco | CiscoAVPair | cisco-wlan-ssid

Passare a **ClearPass > Configurazione > Servizi > Aggiungi**.

Scheda **Servizio**:

-Nome: GuestPortal - Autenticazione Mac

-Tipo: Autenticazione MAC

- Altre opzioni: Selezione autorizzazione, endpoint profilo

Aggiungi regola di abbinamento:

-Tipo: Raggio: Cisco

-Nome: Cisco-AVPair

- Operatore: UGUALE A

-Valore: cisco-wlan-ssid=Guest (corrispondere al nome SSID Guest configurato)

Nota: 'Guest' è il nome dell'SSID guest trasmesso da 9800 WLC.

Configuration » Services » Add

Services

Service Authentication Authorization Roles Enforcement Profiler Summary

Type: MAC Authentication

Name: GuestPortal - Mac Auth

Description: MAC-based Authentication Service

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value		
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)		
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)		
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}		
4.	Radius:Cisco	Cisco-AVPair	EQUALS	cisco-wlan-ssid=Guest		

Nella stessa finestra di dialogo, scegliere la scheda **Autenticazione**.

- Metodi di autenticazione: Rimuovi [MAC AUTH], Aggiungi [Allow All MAC AUTH]

- Origini autenticazione: [Repository di endpoint][Database SQL locale], [Repository utente guest][Database SQL locale]

aruba ClearPass Policy Manager

Configuration » Services » Edit - GuestPortal - Mac Auth

Services - GuestPortal - Mac Auth

Summary Service **Authentication** Authorization Roles Enforcement Profiler

Authentication Methods: [Allow All MAC AUTH]

Authentication Sources: [Endpoints Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB]

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Nella stessa finestra di dialogo, scegliere la scheda **Applicazione**.

- Politica di applicazione: Consenti guest WLC Cisco

Configuration » Services » Add

Services

Service Authentication Roles **Enforcement** Summary

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: WLC Cisco Guest Allow **Modify**

Enforcement Policy Details

Description:	MAB Enforcement Redirect
Default Profile:	Cisco_Portal_Redirect
Rules Evaluation Algorithm:	first-applicable

Conditions	Enforcement Profiles
1. (Endpoint:Allow-Guest-Internet EQUALS true)	[Allow Access Profile]

Nella stessa finestra di dialogo, scegliere la scheda **Applicazione**.

Configuration » Services » Add

Services

Service Authentication Authorization Roles Enforcement **Profiler** Summary

Endpoint Classification: Select the classification(s) after which an action must be triggered -

RADIUS CoA Action: Cisco_Reauthenticate_Session **View Details** **Modify**

Configurazione servizio ClearPass Webauth

Passare a **ClearPass > Applicazione > Criteri > Aggiungi**.

-Nome: Guest_Portal_Webauth

-Tipo: Autenticazione basata sul Web

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Type:	Web-based Authentication			
Name:	Guest			
Description:				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance			
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name			
1.	Host	CheckType		
2.	Click to add...			

Nella stessa finestra di dialogo, nella scheda **Applicazione**, il criterio di applicazione: Policy di applicazione Cisco WLC Webauth.

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	Cisco WLC Webauth Enforcement Policy Modify			Add New Enforcement Poli
Enforcement Policy Details				
Description:				
Default Profile:	Cisco_Reauthenticate_Session			
Rules Evaluation Algorithm:	first-applicable			
Conditions	Enforcement Profiles			
1. (Authentication:Status EQUALS User)	[Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session			

ClearPass - Accesso Web

Per la pagina Anonymous AUP Guest Portal, utilizzare un singolo nome utente senza campo password.

Il nome utente utilizzato deve avere i seguenti campi definiti/impostati:

nomeutente_auth | Autenticazione nome utente: | 1

Per impostare il campo 'username_auth' per un utente, è necessario che tale campo sia esposto nel modulo 'modifica utente'. Passare a **ClearPass > Guest > Configurazione > Pagine > Moduli**, quindi scegliere **create_user** form.

The screenshot shows the Aruba ClearPass Guest configuration interface. The left sidebar contains a navigation menu with categories like Guest, Devices, Onboard, and Configuration. Under Configuration, there are sub-items for Authentication, Content Manager, Guest Manager, Hotspot Manager, Pages, and Fields. The 'Forms' item is highlighted. The main content area shows a list of forms with columns for Name and Title. The 'create_user' form is selected and highlighted in blue. Below the list, there are action buttons: Edit, Edit Fields, Reset to Defaults, Duplicate, Show Usage, and Translations. The 'Edit Fields' button is highlighted with a yellow box.

Scegliere **nome_visitatore** (riga 20) e fare clic su **Inserisci dopo**.

Home » Configuration » Pages » Forms

Customize Form Fields (create_user)

Use this list view to modify the fields of the form **create_user**.

Rank	Field	Type	Label	Description
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	visitor_name	text	Guest's Name:	Name of the guest.

At the bottom of the table, there are action buttons: Edit, Edit Base Field, Remove, Insert Before, Insert After, and Disable Field. The 'Insert After' button is highlighted with a yellow box.

Customize Form Field (new)

Use this form to add a new field to the form **create_user**.

Form Field Editor	
* Field Name:	<input type="text" value="username_auth"/> <small>Select the field definition to attach to the form.</small>
Form Display Properties <small>These properties control the user interface displayed for this field.</small>	
Field:	<input checked="" type="checkbox"/> Enable this field <small>When checked, the field will be included as part of the form.</small>
* Rank:	<input type="text" value="22"/> <small>Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.</small>
* User Interface:	<input type="text" value="No user interface"/> <input type="button" value="Revert"/> <small>The kind of user interface element to use when entering or editing this field.</small>
Form Validation Properties <small>These properties control how the value of this field is checked.</small>	
Field Required:	<input type="checkbox"/> Field value must be supplied <small>Select this option if the field cannot be omitted or left blank.</small>
Initial Value:	<input type="text" value="1"/> <input type="button" value="Revert"/> <small>value to initialize this field with when the form is first displayed.</small>
* Validator:	<input type="text" value="IsValidBool"/> <small>The function used to validate the contents of a field.</small>
Validator Param:	<input type="text" value="(None)"/> <small>Optional name of field whose value will be supplied as the argument to a validator.</small>
Validator Argument:	<input type="text"/> <small>Optional value to supply as the argument to a validator.</small>
Validation Error:	<input type="text"/> <small>The error message to display if the field's value fails validation and the validator does not return an error message directly.</small>

Creare il nome utente da utilizzare dietro la pagina del portale guest AUP.

Passare a **CPPM > Guest > Guest > Gestisci account > Crea**.

- Nome ospite: Guest WiFi
- Nome della società: Cisco
- Indirizzo e-mail: guest@example.com
- Autenticazione nome utente: Consenti accesso guest solo con il nome utente: Attivato
- Attivazione account: Ora
- Scadenza account: L'account non scade
- Condizioni per l'utilizzo: Sono lo sponsor: Attivato

Create Guest Account

New guest account being created by **admin**.

Create New Guest Account	
* Guest's Name:	<input type="text" value="GuestWiFi"/> Name of the guest.
* Company Name:	<input type="text" value="Cisco"/> Company name of the guest.
* Email Address:	<input type="text" value="guest@example.com"/> The guest's email address. This will become their username to log into the network.
Username Authentication:	<input checked="" type="checkbox"/> Allow guest access using their username only Guests will require the login screen setup for username-based authentication as well.
Account Activation:	<input type="text" value="Now"/> Select an option for changing the activation time of this account.
Account Expiration:	<input type="text" value="Account will not expire"/> Select an option for changing the expiration time of this account.
* Account Role:	<input type="text" value="[Guest]"/> Role to assign to this account.
Password:	281355
Notes:	<input type="text"/>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the terms of use
<input type="button" value="Create"/>	

Crea modulo di accesso Web. Passare a **CPPM > Guest > Configurazione > Accessi Web**.

Gli attributi degli endpoint nella sezione post-autenticazione sono riportati di seguito.

username | Nome utente

nome_visitatore | Nome del visitatore

cn | Nome del visitatore

telefono_visitatore | Telefono visitatori

email | E-mail

posta | E-mail

nome_sponsor | Nome sponsor

e-mail_sponsor | E-mail dello sponsor

Allow-Guest-Internet | vero

- Guest
- Device
- Onboard
- Configuration
 - Authentication
 - Content Manager
 - Private Files
 - Public Files
 - Guest Manager
 - Hotspot Manager
- Pages
 - Fields
 - Forms
 - List Views
 - Self-Registrations
 - Web Logins
 - Web Pages
- Receipts
- SDS Services
- Translations

Administration

Web Login Editor

Name:

Page Name:

Description:

Vendor Settings:

Login Method:

Page Redirect:

Security Mode:

Auth Method:

Auto-Generate: Create a new anonymous account

Anonymous User:

- The account will be created without a session, first or expiration time, and with the Guest role (S-2). Enter a valid email address to use a specific username, or leave blank to randomly generate a username.

Present CAPTCHA: Enable displaying the Aruba Captive Network Assistant

Custom Form: Provide a custom login form

Custom Labels: Override the default labels and error messages

Pre-Auth Check: Require the username and password should be checked before proceeding to the NAS authentication

Pre-Auth Error:

Terms: Requires a Terms and Conditions confirmation

Terms Label:

Terms Text:

Terms Layout:

Terms Error:

CAPTCHA:

Log In Label:

Translations: Skip automatic translation handling

Default Destination:

- Default URL:
- Override Destination: Force default destination for all clients

Login Page:

- Skin:
- Title:
- Header HTML:


```
[www_anonregwelcome]
<div>
<div style = "margin">
<div style = "background-color: #E6F2FF">
<div>
<div style = "float: right">
<div style = "clear: both">
</div>
</div>
</div>
</div>
</div>
</div>
</div>
</pre>

```
- HTML content displayed before the login form:


```
[www_saml_login]
Contact a staff member if you are experiencing
difficulty logging in.
</pre>

```

Login Delay:

Advertising Services:

- Enable advertising content on the login page: Enable Advertising Services content

Cloud Identity:

- Enabled: Enable logins with cloud identity / social network credentials

Multi-Factor Authentication:

- Provider:

Network Login Access:

- Allowed Access:
- Denied Access:

Deasy Behavior:

Post-Authentication:

- Health Check: Requires a successful OnGuard health check
- Update Endpoint: Mark the user's MAC address as a known endpoint
- Advanced: Customize attributes stored with the endpoint
- Endpoint Attribute:
 - Attributes:

Verifica - Autorizzazione CWA Guest

In CPPM, passare a **Monitoraggio attivo > Access Tracker**.

Nuovo utente Guest che connette e attiva il servizio MAB.

Scheda **Riepilogo**:

The screenshot shows the 'Request Details' window with the 'Summary' tab selected. The window has a dark blue header with the title 'Request Details' and a close button. Below the header are four tabs: 'Summary', 'Input', 'Output', and 'RADIUS CoA'. The 'Summary' tab contains a table of request details. Several fields are highlighted with yellow boxes: 'Login Status: ACCEPT', 'Username: d43b047a647b', 'Access Device IP/Port: 10.85.54.99:73120 (WLC_9800_Branch / Cisco)', 'Service: Guest SSID - GuestPortal - Mac Auth', and 'Enforcement Profiles: Cisco_Portal_Redirect'. Below the table is a section titled 'Policies Used -' with a table of policy details. At the bottom of the window is a navigation bar with a record count 'Showing 8 of 1-8 records', and five buttons: 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

Summary	Input	Output	RADIUS CoA
Login Status:		ACCEPT	
Session Identifier:		R0000471a-01-6282a110	
Date and Time:		May 16, 2022 15:08:00 EDT	
End-Host Identifier:		d4-3b-04-7a-64-7b (Computer / Windows / Windows)	
Username:		d43b047a647b	
Access Device IP/Port:		10.85.54.99:73120 (WLC_9800_Branch / Cisco)	
Access Device Name:		wlc01	
System Posture Status:		UNKNOWN (100)	

Policies Used -	
Service:	Guest SSID - GuestPortal - Mac Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository]
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	Cisco_Portal_Redirect

Showing 8 of 1-8 records | Change Status | Show Configuration | Export | Show Logs | Close

Nella stessa finestra di dialogo passare alla scheda **Input**.

Request Details

Summary Input Output RADIUS CoA

Username: d43b047a647b

End-Host Identifier: d4-3b-04-7a-64-7b (Computer / Windows / Windows)

Access Device IP/Port: 10.85.54.99:73120 (WLC_9800_Branch / Cisco)

RADIUS Request

Radius:Airespace:Airespace-Wlan-Id	4
Radius:Cisco:Cisco-AVPair	audit-session-id=6336550A00006227CE452457
Radius:Cisco:Cisco-AVPair	cisco-wlan-ssid=Guest
Radius:Cisco:Cisco-AVPair	client-iif-id=1728058392
Radius:Cisco:Cisco-AVPair	method=mab
Radius:Cisco:Cisco-AVPair	service-type=Call Check
Radius:Cisco:Cisco-AVPair	vlan-id=21
Radius:Cisco:Cisco-AVPair	wlan-profile-name=WP_Guest
Radius:IETF:Called-Station-Id	14-16-9d-df-16-20:Guest
Radius:IETF:Calling-Station-Id	d4-3b-04-7a-64-7b

◀ ◀ Showing 8 of 1-8 records ▶ ▶ Change Status Show Configuration Export Show Logs Close

Nella stessa finestra di dialogo passare alla scheda **Output**.

Request Details

Summary Input Output RADIUS CoA

Enforcement Profiles: Cisco_Portal_Redirect

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

RADIUS Response

Radius:Cisco:Cisco-AVPair	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
Radius:Cisco:Cisco-AVPair	url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b-04-7a-64-7b&switchip=10.85.54.99

◀ ◀ Showing 8 of 1-8 records ▶ ▶ Change Status Show Configuration Export Show Logs Close

Appendice

A scopo di riferimento, qui è presentato un diagramma di flusso dello stato per le interazioni di

controller di ancoraggio, esterni e Cisco 9800 con server RADIUS e portale guest ospitato esternamente.

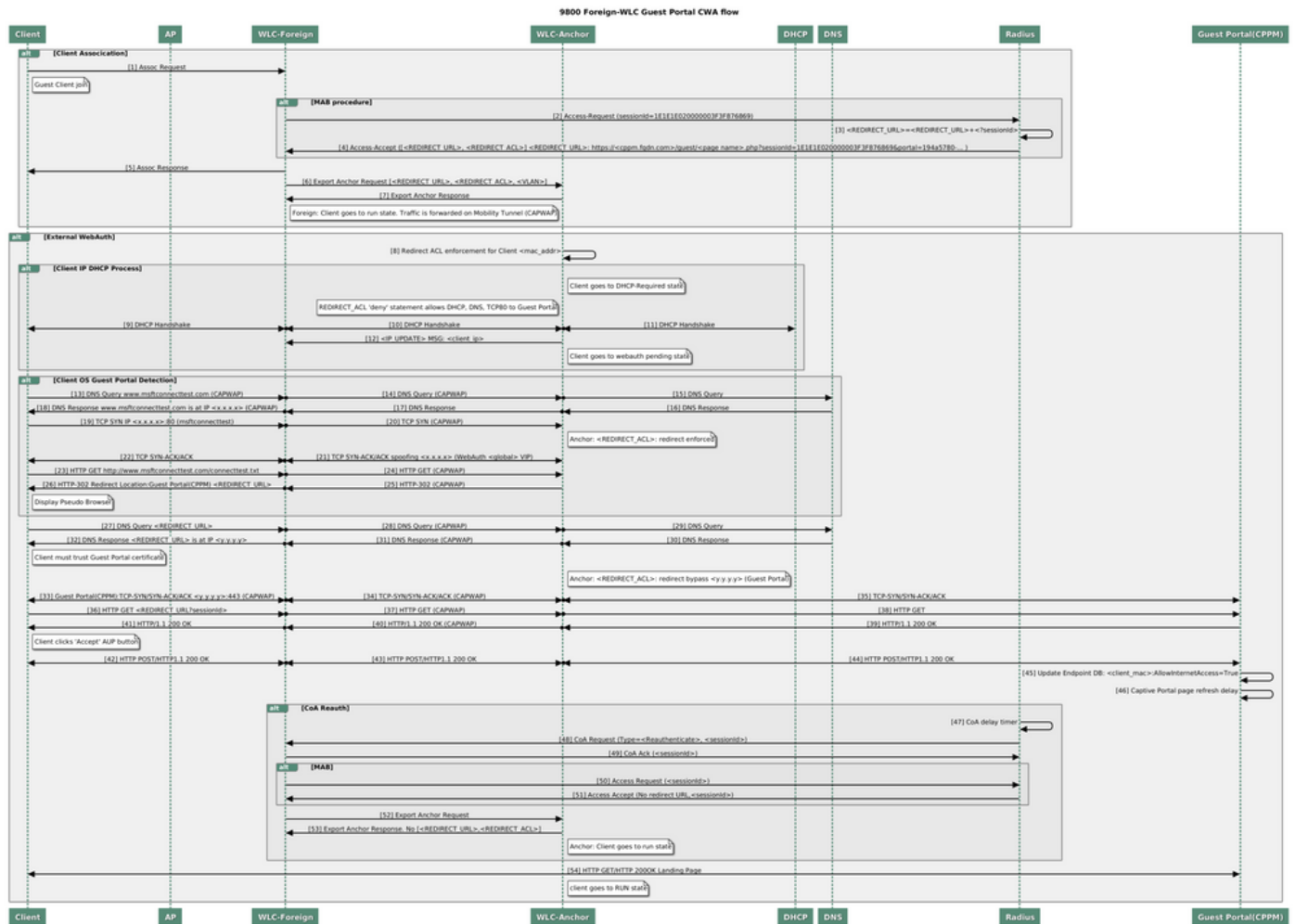


Diagramma di stato dell'autenticazione Web centrale guest con WLC ancorato

Informazioni correlate

- [Guida alle best practice per l'installazione di Cisco 9800](#)
- [Informazioni sul modello di configurazione dei controller wireless Catalyst 9800](#)
- [Informazioni su FlexConnect su Catalyst 9800 Wireless Controller](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).