

Configurazione di ISE Wireless CWA e dei flussi di hotspot con AireOS e WLC di nuova generazione

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione di Unified 5508 WLC](#)

[Configurazione globale](#)

[Configurare l'SSID \(Service Set Identifier\) del guest:](#)

[Configurazione dell'ACL di reindirizzamento](#)

[Reindirizzamento HTTPS](#)

[Failover aggressivo](#)

[Bypass vincolato](#)

[Configurazione di Converged 3850 NGWC](#)

[Configurazione globale](#)

[Configurazione SSID](#)

[Configurazione degli ACL di reindirizzamento](#)

[Configurazione dell'interfaccia della riga di comando \(CLI\)](#)

[Configurare ISE](#)

[Attività comuni di configurazione ISE](#)

[Caso di utilizzo 1: CWA con autenticazione guest in ogni connessione utente](#)

[Caso di utilizzo 2: CWA con registrazione del dispositivo che impone l'autenticazione guest una volta al giorno.](#)

[Caso di utilizzo 3: portale HostSpot](#)

[Verifica](#)

[Caso di utilizzo 1](#)

[Caso di utilizzo 2](#)

[Caso di utilizzo 3](#)

[Switching locale FlexConnect in AireOS](#)

[Scenario di ancoraggio esterno](#)

[Risoluzione dei problemi](#)

[Stati di interruzione comuni su AireOS e Converged Access WLC](#)

[AireOS WLC](#)

[NGWC](#)

[ISE](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare tre richieste guest in Identity Services Engine con Cisco AireOS e Wireless LAN Controller di nuova generazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Wireless LAN Controller (accesso unificato e convergente)
- Identity Services Engine (ISE)

Componenti usati

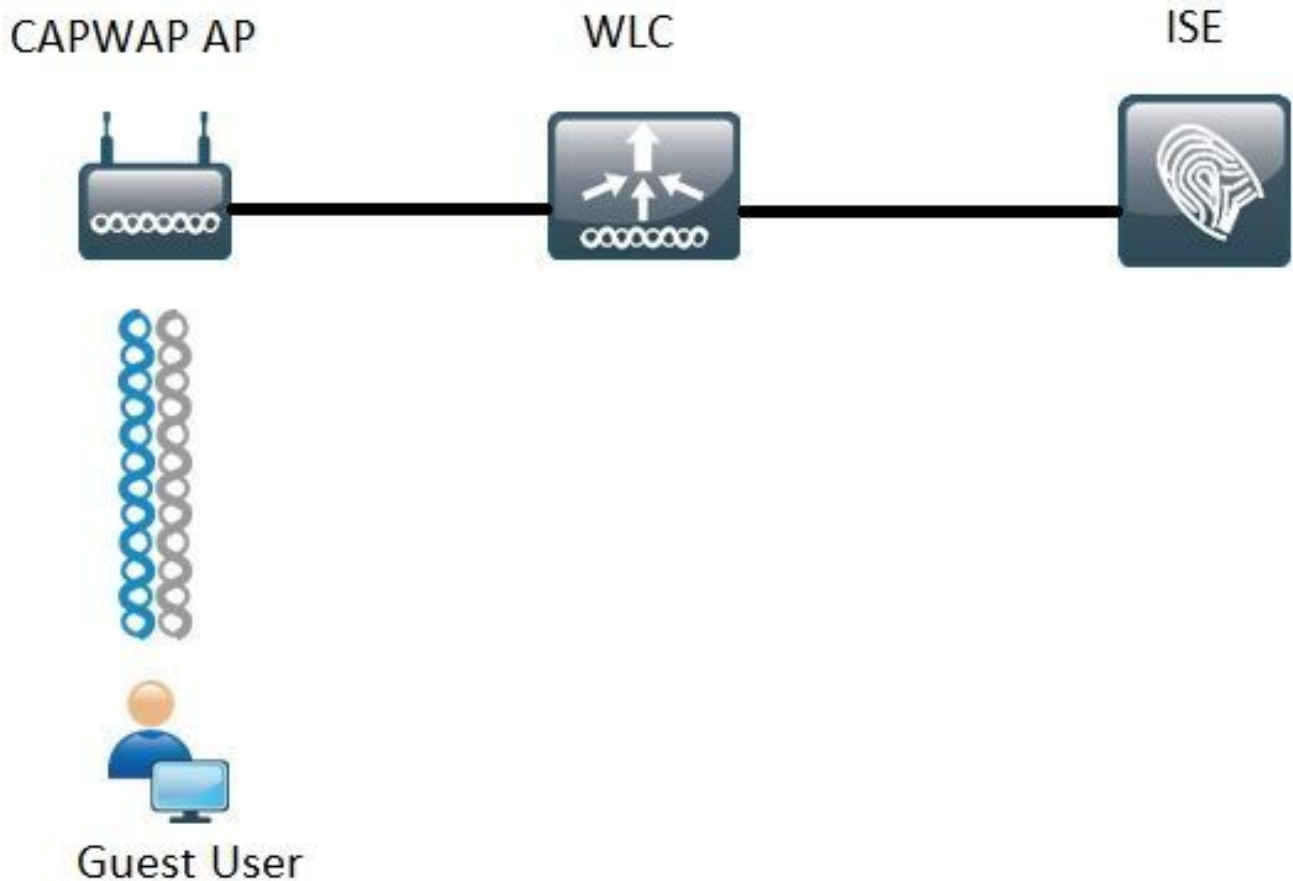
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Services Engine versione 2.1
- Controller LAN wireless Cisco 5508 con 8.0.121.0
- Next-Generation Wireless Controller (NGWC) catalyst 3850 (WS-C3850-24P) con 03.06.04.E

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

Configurazione

Esempio di rete



La procedura descritta in questo documento descrive la configurazione tipica sui WLC di accesso unificato e convergente per supportare qualsiasi flusso guest con ISE.

Configurazione di Unified 5508 WLC

Indipendentemente dallo Use Case configurato in ISE, dal punto di vista WLC tutto inizia con un endpoint wireless che si connette a un Open SSID con il filtro MAC abilitato (Plus AAA override e RADIUS NAC) che punta ad ISE come server di autenticazione e accounting. In questo modo, ISE può inviare dinamicamente gli attributi necessari al WLC per applicare correttamente un reindirizzamento al portale clienti di ISE.

Configurazione globale

1. Aggiungere ISE a livello globale come server di autenticazione e accounting.

- Selezionare **Sicurezza > AAA > Autenticazione** e fare clic su **Nuovo**



- Immettere l'IP del server ISE e il segreto condiviso
- Verificare che lo stato del server e il **supporto per la RFC 3676** (Modifica di autorizzazione o supporto CoA) siano entrambi impostati su **Abilitato**.
- In timeout server per impostazione predefinita, i WLC di AireOS hanno 2 secondi. In base alle caratteristiche della rete (latenza, ISE e WLC in luoghi diversi) può essere utile aumentare il timeout del server ad almeno 5 secondi per evitare eventi di failover non necessari.
- Fare clic su **Apply** (Applica).
- Se sono presenti più nodi di Servizi criteri (PSN, Policy Services Nodes) da configurare, procedere alla creazione di altre voci server.

Nota: questo particolare esempio di configurazione include 2 istanze ISE

- Selezionare **Sicurezza > AAA > RADIUS > Accounting** e fare clic su **Nuovo**
- Immettere l'indirizzo IP e il segreto condiviso del server ISE
- Verificare che lo stato del server sia impostato su Abilitato
- Aumentare il timeout del server se necessario (il valore predefinito è 2 secondi).

2. Configurazione fallback.

In un ambiente unificato, una volta attivato il timeout del server, il WLC passa al successivo server configurato. Prossima linea dalla WLAN. Se non sono disponibili altri server, il WLC seleziona quello successivo nell'elenco dei server globali. Quando più server sono configurati sul SSID (primario, secondario) una volta che si verifica il failover, per impostazione predefinita il WLC continua a inviare in modo permanente il traffico di autenticazione e/o accounting all'istanza secondaria anche se il server primario è di nuovo online.

Per mitigare questo comportamento, abilitare il fallback. Selezionare **Sicurezza > AAA > RADIUS > Fallback**. Il comportamento predefinito è disattivato. L'unico modo per eseguire il ripristino da un evento di inattività del server richiede l'intervento dell'amministratore, che a livello globale esegue il rimbalzo dello stato dell'amministratore del server.

Per abilitare il fallback, sono disponibili due opzioni:

- **Passivo:** in modalità passiva, se un server non risponde alla richiesta di autenticazione WLC,

il WLC sposta il server nella coda inattiva e imposta un timer (opzione Intervallo in secondi). Alla scadenza del timer, il WLC sposta il server nella coda attiva indipendentemente dallo stato effettivo dei server. Se la richiesta di autenticazione genera un evento di timeout, ovvero se il server è ancora inattivo, la voce relativa al server viene spostata nuovamente nella coda Inactive e il timer viene riattivato. Se il server risponde correttamente, rimane nella coda Attivo. I valori configurabili vanno da 180 a 3600 secondi.

- **Attivo:** in modalità attiva, quando un server non risponde alla richiesta di autenticazione WLC, il WLC contrassegna il server come inattivo, quindi lo sposta in un pool di server non attivo e avvia periodicamente l'invio di messaggi di richieste finché il server non risponde. Se il server risponde, il WLC sposta il server inattivo nel pool attivo e interrompe l'invio dei messaggi di richieste.

In questa modalità, il WLC richiede l'immissione di un nome utente e di un intervallo di prova in secondi (da 180 a 3600).

Nota: il probe WLC non richiede un'autenticazione riuscita. In entrambi i casi, le autenticazioni riuscite o non riuscite sono considerate una risposta del server sufficiente per innalzare il server alla coda Attiva.

Configurare il SSID (Service Set Identifier):

- Passare alla scheda WLAN e in Crea nuova opzione fare clic su **Vai**:



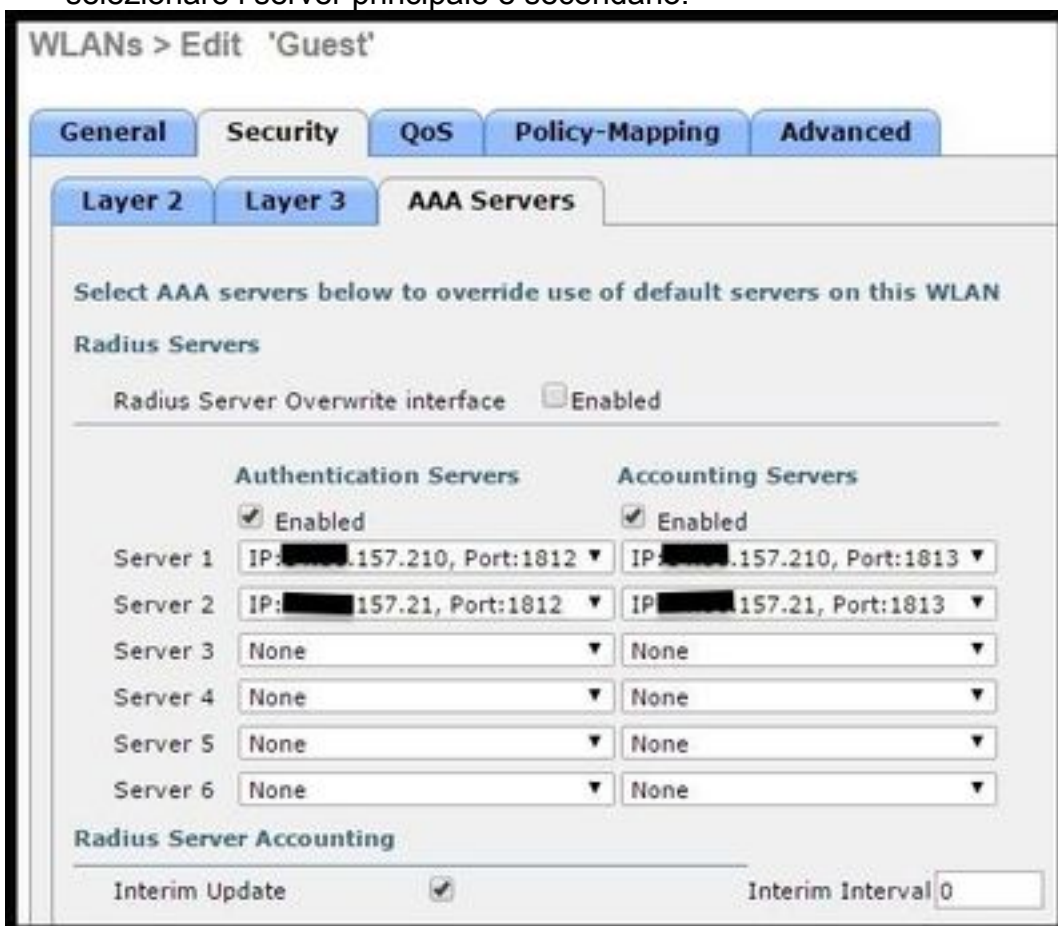
- Immettere il nome del profilo e il nome SSID. Fare clic su **Apply** (Applica).
- Nella scheda General (Generale), selezionare l'interfaccia o il gruppo di interfacce da usare (VLAN guest).



- In **Protezione > Livello 2 > Protezione di livello 2** selezionare **Nessuna** e abilitare il filtro **Mac** casella di controllo.



- Nella scheda **Server AAA** impostare i server di autenticazione e accounting su **abilitato** e selezionare i server principale e secondario.



- **Aggiornamento provvisorio:** si tratta di una configurazione facoltativa che non aggiunge vantaggi al flusso. Se si preferisce abilitarlo, il WLC deve eseguire il codice 8.x o superiore:
Disabilitato: la funzione è completamente disabilitata.

Abilitato con intervallo 0: il WLC invia aggiornamenti di accounting ad ISE ogni volta che viene modificata la voce MSCB (Mobile Station Control Block) del client (ad esempio. Assegnazione o modifica dell'indirizzo IPv4 o IPv6, evento di roaming client.) Non vengono inviati ulteriori aggiornamenti periodici.

Abilitato con un intervallo provvisorio configurato: in questa modalità il WLC invia notifiche ad ISE in caso di modifiche alle voci MSCB del client e invia inoltre notifiche di accounting periodiche aggiuntive all'intervallo configurato (indipendentemente da eventuali modifiche).

- In Advanced Tab Enable **Allow AAA Override (Consenti sostituzione AAA)** e Under **NAC state (Stato NAC)** selezionare **RADIUS NAC**. Ciò garantisce che il WLC applichi qualsiasi coppia di valori di attributo (AVP) proveniente dall'ISE.
- Passare alla scheda Generale SSID e impostare lo stato SSID su **Abilitato**

WLANs > Edit 'Guest'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	Guest			
Type	WLAN			
SSID	Guest			
Status	<input checked="" type="checkbox"/> Enabled			

- **Applicare** le modifiche.

Configurazione dell'ACL di reindirizzamento

ISE fa riferimento a questo ACL, che determina il traffico da reindirizzare e il traffico da attraversare.

- Selezionare **Security Tab > Access Control Lists** e fare clic su **New**
- Questo è un esempio di ACL

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	157.210 / 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	157.210 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	157.21 / 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	157.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0

Questo ACL deve consentire l'accesso da e verso i servizi DNS e i nodi ISE tramite la porta TCP 8443. In basso è presente una negazione implicita che indica che il resto del traffico viene reindirizzato all'URL del portale per gli utenti guest di ISE.

Reindirizzamento HTTPS

Questa funzione è supportata in AireOS versione 8.0.x e successive ma è disattivata per impostazione predefinita. Per abilitare il supporto HTTPS, passare a **Gestione WLC > HTTP-HTTPS > Reindirizzamento HTTPS** e impostarlo su **Enabled** o applicare questo comando nella CLI:

```
(Cisco Controller) >config network web-auth https-redirect enable
```

Avvisi certificato dopo l'abilitazione del reindirizzamento HTTPS

Dopo l'abilitazione di https-redirect, l'utente può riscontrare problemi di attendibilità del certificato durante il reindirizzamento. Ciò si verifica anche se è presente un certificato concatenato valido sul controller e anche se il certificato è firmato da un'Autorità di certificazione attendibile di terze parti. Il motivo è che il certificato installato sul WLC viene rilasciato al relativo nome host o indirizzo IP dell'interfaccia virtuale. Quando il client tenta di eseguire <https://cisco.com>, il browser si aspetta che il certificato venga rilasciato a cisco.com. Tuttavia, per essere in grado di intercettare il GET emesso dal client, il WLC deve prima stabilire la sessione HTTPS per cui presenta il certificato dell'interfaccia virtuale durante la fase di handshake SSL. In questo modo il browser visualizza un avviso poiché il certificato presentato durante l'handshake SSL non è stato rilasciato al sito Web originale a cui il client sta tentando di accedere (ad esempio, cisco.com opposto al nome host dell'interfaccia virtuale WLC). È possibile visualizzare diversi messaggi di errore relativi ai certificati in browser diversi, ma tutti sono correlati allo stesso problema.

Failover aggressivo

Questa funzione è abilitata per impostazione predefinita nei WLC di AireOS. Quando il failover aggressivo è abilitato, il WLC contrassegna il server AAA come non rispondente e si sposta sul successivo server AAA configurato dopo che un evento di timeout RADIUS ha influito su un client.

Quando la funzionalità è disabilitata, il WLC esegue il failover sul server successivo solo se l'evento di timeout RADIUS si verifica con almeno 3 sessioni client. Questa funzionalità può essere disabilitata da questo comando (per questo comando non è richiesto il riavvio):

```
(Cisco Controller) >config radius aggressive-failover disable
```

Per verificare lo stato corrente della feature:

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

Bypass vincolato

Gli endpoint che supportano un meccanismo CNA (Captive Network Assistant) per l'individuazione di un portale separato e l'avvio automatico di una pagina di accesso in genere lo eseguono tramite uno pseudo browser in una finestra controllata, mentre gli altri endpoint avviano un browser completamente funzionante per attivare questa funzionalità. Per gli endpoint in cui la CNA avvia uno pseudo-browser, il flusso può essere interrotto quando reindirizzato a ISE captive portal. Questo problema riguarda in genere i dispositivi Apple IOS e ha effetti particolarmente negativi nei flussi che richiedono la registrazione del dispositivo, la release DHCP della VLAN, il controllo della conformità.

In funzione della complessità del flusso in uso, si consiglia di abilitare il bypass vincolato. In questo scenario, il WLC ignora il meccanismo di rilevamento del portale CNA e il client deve aprire un browser per avviare il processo di reindirizzamento.

Verificate lo stato della feature:

```
(Cisco Controller) >show network summary
```

```
Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disabled
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

Per abilitare questa funzione, digitare questo comando:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.
```

You must reset system for this setting to take effect.

Il WLC avvisa l'utente che per rendere effettive le modifiche è necessario un reset-system (riavvio).

A questo punto, un **riepilogo della visualizzazione della rete** mostra che la funzione è abilitata, ma per rendere effettive le modifiche è necessario riavviare il WLC.

Configurazione di Converged 3850 NGWC

Configurazione globale

1. Aggiungere ISE a livello globale come server di autenticazione e accounting

- Selezionare **Configurazione > Protezione > RADIUS > Server** e fare clic su **Nuovo**
- Immettere l'**indirizzo IP** del server ISE, il **segreto condiviso**, il **timeout del server** e il conteggio **dei tentativi** che riflettono le condizioni ambientali.
- Verificare che il **supporto per RFC 3570** (supporto CoA) sia abilitato.
- Ripetere la procedura per aggiungere una voce Server secondario.

RADIUS Servers

Radius Servers > **New**

Server Name

Server IP Address

Shared Secret

Confirm Shared Secret

Auth Port (0-65535)

Acct Port (0-65535)

Server Timeout (1-1000)secs

Retry Count (0-100)

Support for RFC 3576 ▾

2. Creare il gruppo di server ISE

- Selezionare **Configurazione > Protezione > Gruppi di server** e fare clic su **Nuovo**
- Assegnate un nome al gruppo e immettete un valore per il **tempo morto** in minuti. Si tratta dell'intervallo di tempo durante il quale il controller mantiene il server nella coda Inattivo prima di essere promosso di nuovo all'elenco dei server attivi.
- Dall'elenco Server disponibili, aggiungerli alla colonna Server assegnati.

Radius Server Group

Radius Server Group > **New**

Name

MAC-delimiter ▾

MAC-filtering ▾

Dead-time (0-1440) in minutes

Group Type

Servers In This Group

Available Servers

< >

Assigned Servers

ISE2

ISE1

3. Abilitazione globale punto1x

- Selezionare **Configurazione > AAA > Elenchi metodi > Generale** e abilitare **Controllo**

autenticazione sistema Dot1x

The screenshot shows the 'General' configuration page for 'Dot1x System Auth Control'. The 'Dot1x System Auth Control' checkbox is checked and highlighted with a yellow border. Below it, the 'Local Authentication' and 'Local Authorization' dropdown menus are both set to 'None'.

4. Configurazione degli elenchi di metodi

- Passare a **Configurazione > AAA > Elenchi metodi > Autenticazione** e creare un nuovo elenco di metodi. In questo caso si tratta del tipo Dot1x e del gruppo ISE_Group (gruppo creato nel passaggio precedente). Quindi fare clic su **Applica**

The screenshot shows the 'Authentication > New' configuration page. The 'Method List Name' is 'ISE_Method'. The 'Type' is 'dot1x' (selected with a radio button). The 'Group Type' is 'group' (selected with a radio button). The 'Fallback to local' checkbox is unchecked. The 'Available Server Groups' list is empty, and the 'Assigned Server Groups' list contains 'ISE_Group'. Navigation arrows are visible between the two lists.

- Eseguire la stessa operazione per l'accounting (**Configurazione > AAA > Elenchi metodi > Accounting**) e per l'autorizzazione (**Configurazione > AAA > Elenchi metodi > Autorizzazione**). Devono avere questo aspetto

The screenshot shows the 'Accounting > New' configuration page. The 'Method List Name' is 'ISE_Method'. The 'Type' is 'identity' (selected with a radio button). The 'Available Server Groups' list is empty, and the 'Assigned Server Groups' list contains 'ISE_Group'. Navigation arrows are visible between the two lists.

Authorization
Authorization > New

Method List Name:

Type: network exec credential-download

Group Type: group local

Available Server Groups: [Empty list]

Assigned Server Groups: ISE_Group

5. Creare il metodo di filtro MAC dell'autorizzazione.

Questa chiamata viene effettuata dalle impostazioni SSID in seguito.

- Selezionare **Configurazione > AAA > Elenchi metodi > Autorizzazione** e fare clic su **Nuovo**.
- Immettere il nome dell'elenco di metodi. Scegliere **Tipo = Rete** e **Gruppo di tipi**.
- Aggiungere ISE_Group al campo Gruppi di server assegnati.

Authorization
Authorization > New

Method List Name:

Type: network exec credential-download

Group Type: group local

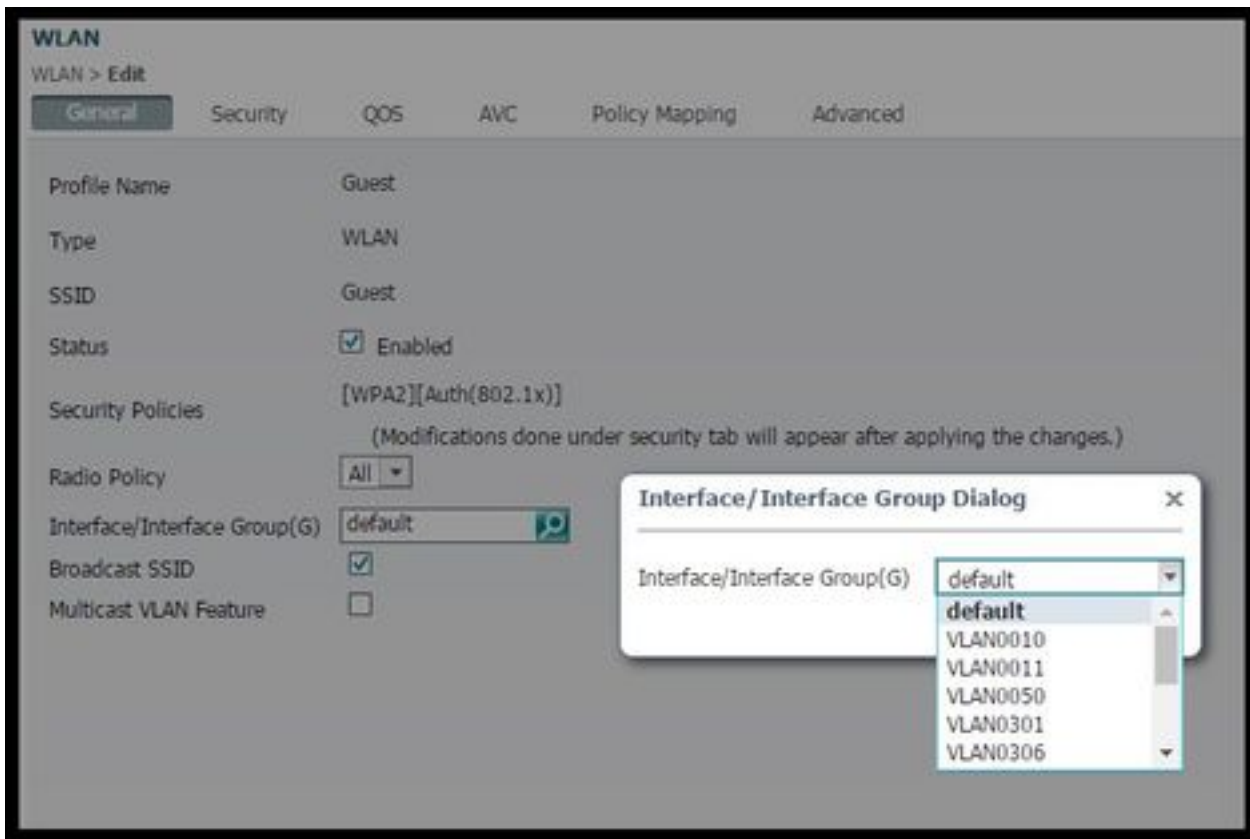
Available Server Groups: [Empty list]

Assigned Server Groups: ISE_Group

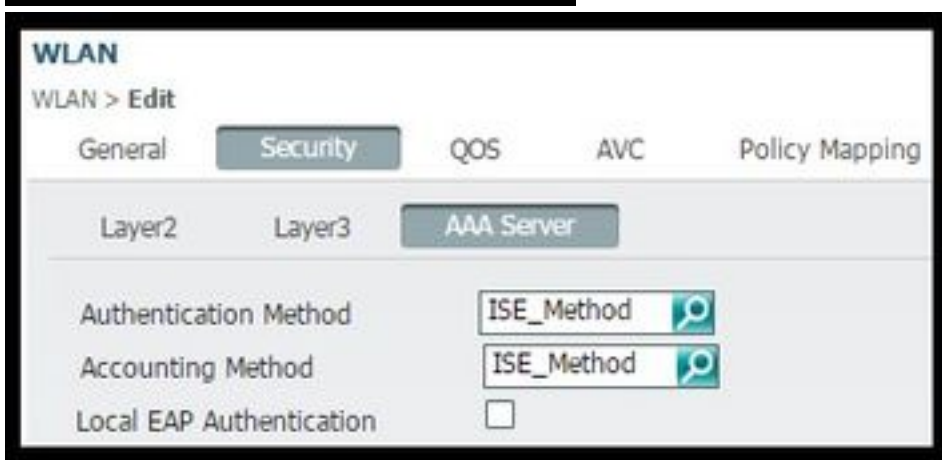
Configurazione SSID

1. Creare il SSID guest

- Selezionare **Configuration > Wireless > WLAN** (Configurazione > Wireless > WLAN), quindi fare clic su **New (Nuovo)**
- Immettete ID WLAN, SSID e Nome profilo e fate clic su **Applica (Apply)**.
- Selezionare l'interfaccia Guest VLAN Layer 3 nelle impostazioni SSID in **Interfaccia/Gruppo di interfacce**.



- In **Protezione > Livello 2** selezionare **Nessuno** e accanto a **Filtraggio Mac** immettere il Nome elenco del metodo di filtro Mac configurato in precedenza (MacFilterMethod).
- In **Sicurezza > scheda Server AAA** selezionare gli elenchi dei metodi di autenticazione e accounting (ISE_Method) appropriati.



- In Scheda **Avanzate**, abilitare **Consenti sostituzione AAA** e lo stato **NAC**. Le altre impostazioni devono essere regolate in base ai requisiti di distribuzione (timeout sessione, esclusione client, supporto per estensioni Aironet).

WLAN
WLAN > Edit

General Security QOS AVC Policy Mapping **Advanced**

Allow AAA Override
 Coverage Hole Detection
 Session Timeout (secs)
 Aironet IE
 Diagnostic Channel
 P2P Blocking Action
 Media Stream Multicast-direct
 Client Exclusion
 Timeout Value(secs)
 Max Allowed Client

DHCP

DHCP Server IP Address
 DHCP Address Assignment required
 DHCP Option 82
 DHCP Option 82 Format
 DHCP Option 82 Ascii Mode
 DHCP Option 82 Rid Mode

NAC

NAC State

- Passare alla scheda Generale e impostare lo stato su Abilitato. Quindi scegliere **Applica**.

Configurazione degli ACL di reindirizzamento

ISE fa riferimento a questo ACL più avanti in access-accept in risposta alla richiesta MAB iniziale. La NGWC la usa per stabilire quale traffico reindirizzare e quale traffico deve passare.

- Passare a **configurazione > sicurezza > ACL > Access Control Lists** e fare clic su **Aggiungi nuovo**.
- Selezionare Extended (Esteso) e immettere il nome dell'ACL.
- Nell'immagine viene mostrato un esempio di ACL di reindirizzamento tipico:

Access Control Lists
ACLs > ACL detail

Details :

Name: **Guest_Redirect**
 Type: **IPv4 Extended**

Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port
10	deny	icmp	any	any	-	-
20	deny	udp	any	any	-	eq 67
30	deny	udp	any	any	-	eq 68
40	deny	udp	any	any	-	eq 53
50	deny	tcp	any	████████.157.210	-	eq 8443
60	deny	tcp	any	████████.157.21	-	eq 8443
70	permit	tcp	any	any	-	eq 80
80	permit	tcp	any	any	-	eq 443

Nota: la riga 10 è facoltativa. Questa opzione viene in genere aggiunta per le proposte di risoluzione dei problemi. Questo ACL deve consentire l'accesso a DHCP, ai servizi DNS e

anche alle porte TCP 8443 (Nega ACE) dei server ISE. Il traffico HTTP e HTTPS viene reindirizzato (consenti ACE).

Configurazione dell'interfaccia della riga di comando (CLI)

tutte le configurazioni descritte nei passaggi precedenti possono essere applicate anche dalla CLI.

802.1x abilitato a livello globale

```
dot1x system-auth-control
```

Configurazione AAA globale

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
  client 172.16.157.210 server-key *****
  client 172.16.157.21 server-key *****
  auth-type any
!
radius server ISE1
  address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
radius server ISE2
  address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
!
aaa group server radius ISE_Group
  server name ISE2
  server name ISE1
  deadtime 10
  mac-delimiter colon
!
```

Configurazione della WLAN

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
mac-filtering MacFilterMethod
nac
no security wpa
```

```
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
no shutdown
```

Esempio di ACL di reindirizzamento

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
 10 deny icmp any any
 20 deny udp any any eq bootps
 30 deny udp any any eq bootpc
 40 deny udp any any eq domain
 50 deny tcp any host 172.16.157.210 eq 8443
 60 deny tcp any host 172.16.157.21 eq 8443
 70 permit tcp any any eq www
 80 permit tcp any any eq 443
```

Supporto HTTP e HTTPS

```
3850#show run | inc http
ip http server
ip http secure-server
```

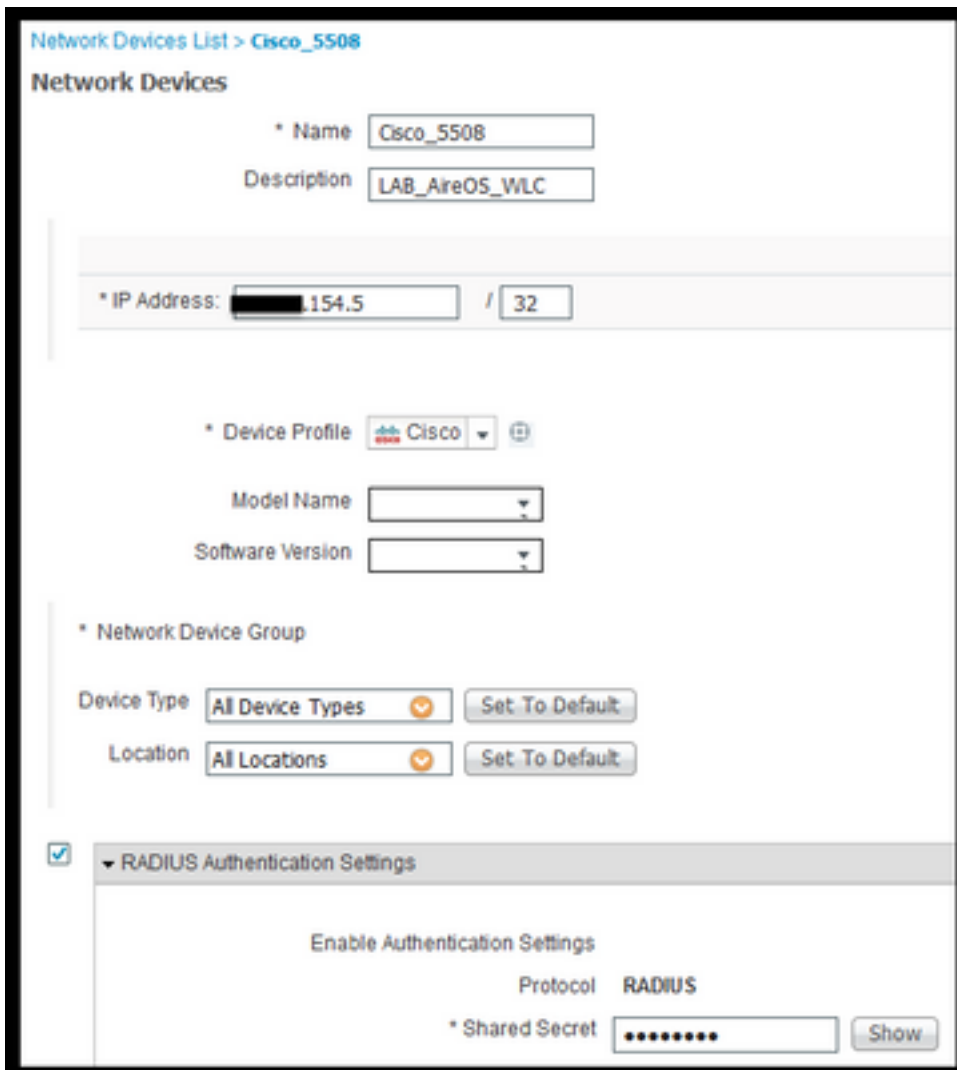
Nota: l'applicazione di un ACL per limitare l'accesso al WLC su HTTP ha effetto sul reindirizzamento.

Configurare ISE

In questa sezione viene descritta la configurazione richiesta per ISE in modo da supportare tutti gli utilizzi discussi in questo documento.

Attività comuni di configurazione ISE

1. Accedere a ISE e selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**, quindi fare clic su **Aggiungi**
2. Immettere il **Nome** associato al WLC e l'**indirizzo IP** del dispositivo.
3. Selezionare la casella **Impostazioni autenticazione RADIUS** e digitare il **segreto condiviso** configurato sul lato WLC. Quindi fare clic su **Invia**.

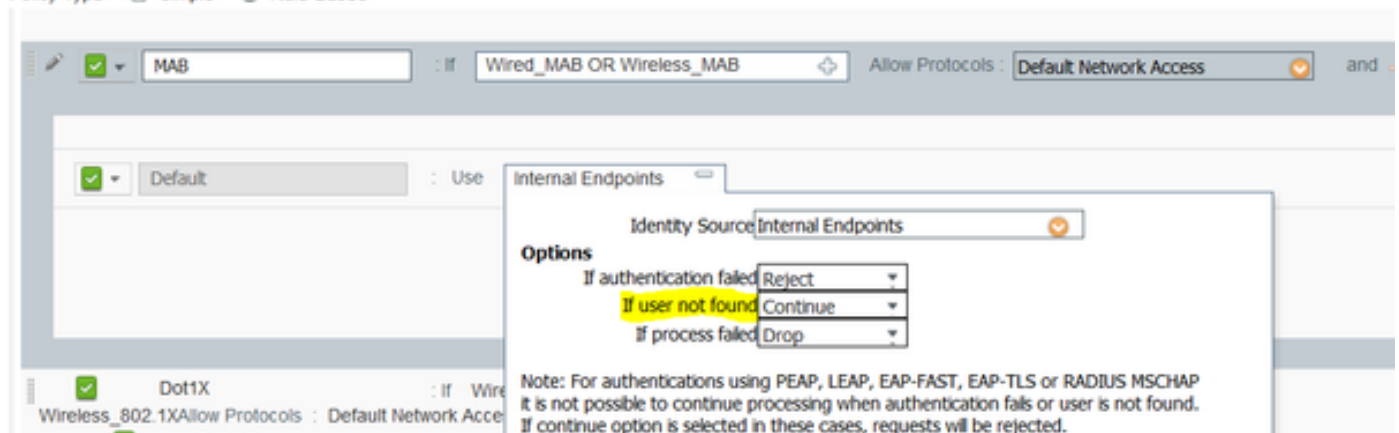


4. Passare a Criterio > Autenticazione e in MAB fare clic su Modifica e assicurarsi che in **Usa: Endpoint interni** l'opzione **Se l'utente non viene trovato** sia impostata su **Continua** (deve essere presente per impostazione predefinita).

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based



Caso di utilizzo 1: CWA con autenticazione guest in ogni connessione utente

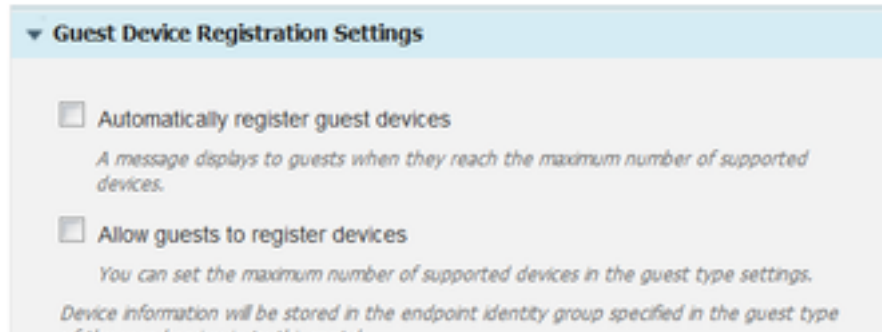
Panoramica sul flusso

1. L'utente wireless si connette al SSID guest.

2. WLC autentica l'endpoint in base al suo indirizzo MAC su ISE come server AAA.
 3. ISE torna indietro e accetta l'accesso con due coppie di valori di attributo (AVP): url-redirect e url-redirect-acl. Una volta che il WLC applica gli AVP alla sessione dell'endpoint, la stazione passa a DHCP-Required e, dopo aver acquisito un indirizzo IP, rimane in CENTRAL_WEB_AUTH. A questo punto, il WLC è pronto per avviare il reindirizzamento del traffico http / https del client.
 4. L'utente finale apre il browser Web e, una volta generato il traffico HTTP o HTTPS, il WLC reindirizza l'utente al portale guest ISE.
 5. Quando l'utente accede al portale guest, richiede di immettere le credenziali guest (create dallo sponsor in questo caso).
 6. Dopo la convalida delle credenziali, ISE visualizza la pagina AUP e, una volta accettato dal client, invia al WLC un messaggio di tipo Re-authentication di tipo CoA dinamico.
 7. Il WLC rielabora l'autenticazione del filtro MAC senza emettere un de-autenticato alla stazione mobile. Questa operazione deve essere eseguita senza problemi fino all'endpoint.
 8. Dopo che si è verificato l'evento di riautenticazione, ISE valuta nuovamente i criteri di autorizzazione e questa volta all'endpoint viene concesso un accesso con autorizzazione poiché si è verificato un precedente evento di autenticazione guest riuscito.
- Questo processo si ripete ogni volta che l'utente si connette al SSID.

Configurazione

1. Accedere ad ISE e selezionare **Work Center > Guest Access > Configure > Guest Portals > Select Sponsored Guest Portal** (o creare un nuovo portale di tipo Sponsored-Guest).
2. In **Guest Device Registration settings** deselezionare tutte le opzioni e fare clic su **Save**.



3. Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione**. Fare clic su **Add**.

4. Questo profilo viene propagato al WLC, all'**URL di reindirizzamento** e all'**ACL di reindirizzamento dell'URL** in risposta alla richiesta iniziale di bypass dell'autenticazione Mac (MAB).

- Una volta selezionato il reindirizzamento Web (CWA, MDM, NSP, CPP), selezionare Autenticazione Web centralizzata, quindi Digitare il nome dell'ACL di reindirizzamento nel campo **ACL** e in **Valore** selezionare il **portale guest sponsorizzato (predefinito)**(o qualsiasi altro portale specifico creato nei passaggi precedenti).

Il profilo deve essere simile a quello illustrato nella figura. Quindi fare clic su **Salva**.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) (i)

Centralized Web Auth ACL Value

Display Certificates Renewal Message

Static IP/Host name/FQDN

Dettagli attributo nella parte inferiore della pagina le coppie di valori di attributo (AVP) durante il push nel WLC

Attributes Details

```

Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-ac=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
    
```

5. Passare a **Criterio > Autorizzazione** e inserire una nuova regola. Questa regola attiva il processo di reindirizzamento in risposta alla richiesta di autenticazione MAC iniziale dal WLC (in questo caso chiamata **Wireless_Guest_Redirect**).

6. In **Condizioni** scegliere **Seleziona condizione esistente da libreria**, quindi in **Nome condizione** selezionare **Condizione composta**. Selezionare una condizione composta predefinita denominata **Wireless_MAB**.

Nota: questa condizione è costituita da 2 attributi Radius previsti nella richiesta di accesso originata dal WLC (NAS-Port-Type= IEEE 802.11 <presente in tutte le richieste wireless> e Service-Type = Call Check< che fa riferimento a una richiesta specifica per un bypass di autenticazione mac>)

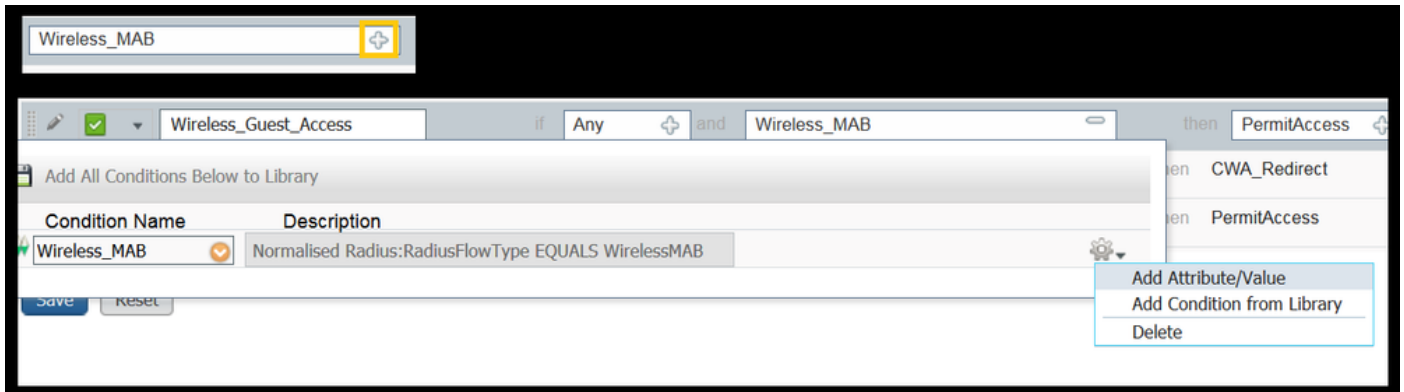
7. In Risultati, selezionare **Standard > CWA_Redirect** (profilo di autorizzazione creato nel passo precedente). Quindi fate clic su **Fatto (Done)** e **Salva (Save)**

Wireless_Guest_Redirect if Wireless_MAB then CWA_Redirect [Edit](#)

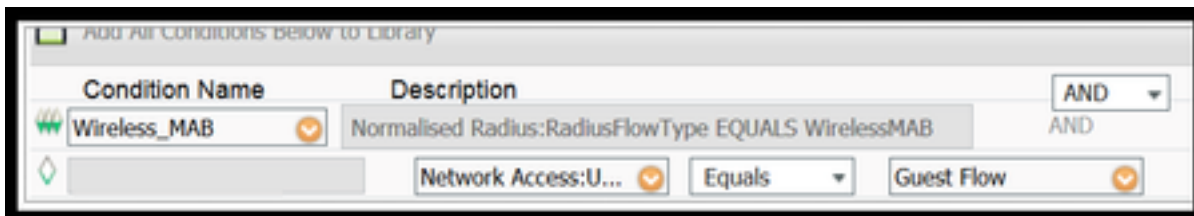
8. Passare alla fine della regola **CWA_Redirect** e fare clic sulla freccia accanto a **Modifica**. Quindi selezionare **duplicato**.

9. Modificare il nome come criterio che l'endpoint deve soddisfare una volta che la sessione è stata riautenticata sul CoA di ISE (in questo caso Wireless_Guest_Access).

10. Accanto alla condizione composta **Wireless_MAB** fare clic sul simbolo + per espandere le condizioni e alla fine della condizione **Wireless_MAB** fare clic su **Aggiungi attributo/valore**.



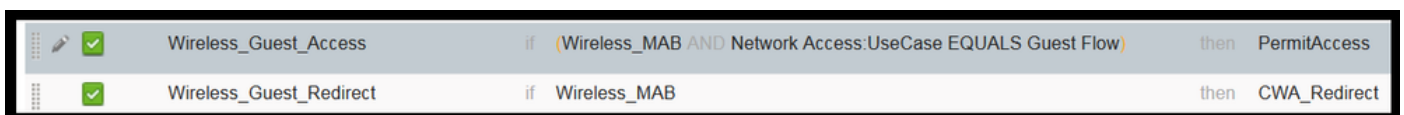
11. In "Seleziona attributo" scegliere **Accesso alla rete > UseCase uguale a Guest flow**



12. In **Autorizzazioni** selezionare **PermitAccess**. Quindi fate clic su **Fatto (Done)** e **Salva (Save)**



Le due politiche devono avere un aspetto simile al seguente:



Caso di utilizzo 2: CWA con registrazione del dispositivo che impone l'autenticazione guest una volta al giorno.

Panoramica sul flusso

1. L'utente wireless si connette al SSID guest.
2. WLC autentica l'endpoint in base al suo indirizzo MAC su ISE come server AAA.
3. ISE torna indietro e accetta l'accesso con due coppie di valori di attributo (AVP) (url-redirect e url-redirect-acl).
4. Una volta che il WLC applica gli AVP alla sessione dell'endpoint, la stazione passa a DHCP-Required e, dopo aver acquisito un indirizzo IP, rimane in CENTRAL_WEB_AUTH. A questo punto, il WLC è pronto per avviare il reindirizzamento del traffico http / https del client.
5. L'utente finale apre il browser Web e, una volta generato il traffico HTTP o HTTPS, il WLC reindirizza l'utente al portale guest ISE.
6. Quando l'utente accede al portale guest, gli viene richiesto di immettere le credenziali create

dallo sponsor.

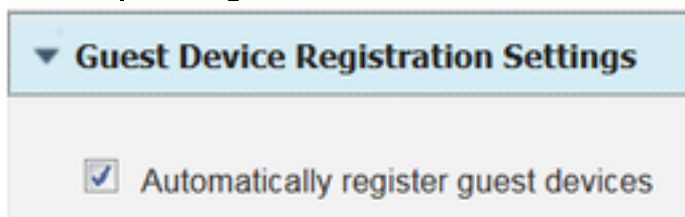
7. Alla convalida delle credenziali, ISE aggiunge l'endpoint a un Endpoint Identity Group (Device Registration) specifico (preconfigurato).
8. Viene visualizzata la pagina AUP e, una volta accettato dal client, viene eseguito il re-authentication di un tipo di CoA dinamico. Viene inviato al WLC.
9. Il WLC deve rielaborare l'autenticazione del filtro MAC senza emettere una richiesta di deautenticazione per la stazione mobile. Questa operazione deve essere eseguita senza problemi fino all'endpoint.
10. Una volta che si è verificato l'evento di riautenticazione, ISE valuta nuovamente le policy di autorizzazione. Questa volta, poiché l'endpoint è membro del gruppo di identità dell'endpoint appropriato, ISE restituisce un'autorizzazione di accesso senza restrizioni.
11. Poiché l'endpoint è stato registrato nel passaggio 6, ogni volta che l'utente ritorna, viene autorizzato sulla rete finché non viene rimosso manualmente da ISE oppure finché gli endpoint che soddisfano i criteri non vengono scaricati da un criterio di rimozione degli endpoint.

In questo scenario di laboratorio, l'autenticazione viene applicata una volta al giorno. Il trigger di riautenticazione è Criterio di rimozione degli endpoint che rimuove ogni giorno tutti gli endpoint del gruppo di identità degli endpoint utilizzato.

Nota: è possibile applicare l'evento di autenticazione guest in base al tempo trascorso dall'ultima accettazione AUP. Questa opzione può essere utile se è necessario imporre l'accesso come Guest più spesso di una volta al giorno (ad esempio ogni 4 ore).

Configurazione

1. All'ISE passare a **Centri di lavoro > Accesso guest > Configura > Portali guest > Seleziona portale guest sponsorizzato** (o crea un nuovo tipo di portale Sponsorizzato-Guest).
2. In **Guest Device Registration** settings verificare che l'opzione **Registra automaticamente i dispositivi guest** sia selezionata. Fare clic su **Salva**.



3. Passare a **Centro di lavoro > Accesso guest > Configura > Tipi di guest** o fare semplicemente clic sul collegamento specificato in Impostazioni di registrazione dei dispositivi guest nel portale.

▼ Guest Device Registration Settings

Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers > Guest Access > Configure > Guest Types](#)

4. Quando l'utente sponsor crea un account guest, gli assegna un tipo guest. Ogni singolo tipo di guest può avere un endpoint registrato che appartiene a un gruppo di identità degli endpoint diverso. Per assegnare il gruppo di identità degli endpoint a cui deve essere aggiunto il dispositivo, selezionare il tipo di guest utilizzato dallo sponsor per questi utenti guest (questo caso di utilizzo è basato su Settimanale (impostazione predefinita)).

5. Una volta nel tipo di guest, in **Opzioni di accesso** selezionare Gruppo endpoint dal menu a discesa **Gruppo identità endpoint per la registrazione del dispositivo guest**

Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration: ⓘ

6. Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione**. Fare clic su **Add**.

7. Questo profilo viene propagato al WLC, all'**URL di reindirizzamento** e all'**ACL di reindirizzamento dell'URL** in risposta alla richiesta iniziale di bypass dell'autenticazione Mac (MAB).

- Una volta selezionato il reindirizzamento Web (CWA, MDM, NSP, CPP), selezionare **Autenticazione Web centralizzata**, quindi digitare il nome dell'ACL di reindirizzamento nel campo **ACL** e in **Valore** selezionare il portale creato per questo flusso (CWA_DeviceRegistration).

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ Common Tasks

VLAN

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Centralized Web Auth ACL Value

8. Passare a **Criterio > Autorizzazione** e inserire una nuova regola. Questa regola attiva il processo di reindirizzamento in risposta alla richiesta di autenticazione MAC iniziale dal WLC (in questo caso chiamata **Wireless_Guest_Redirect**).

9. In **Condizioni** scegliere **Seleziona condizione esistente da libreria**, quindi in **nome condizione** selezionare **Condizione composta**. Selezionare una condizione composta predefinita denominata **Wireless_MAB**.

10. In **Risultati**, selezionare **Standard > CWA_DeviceRegistration** (profilo di autorizzazione creato nel passaggio precedente). Quindi fate clic su **Fatto (Done)** e **Salva (Save)**

Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

11. Duplicare il criterio sopra indicato, modificarne il nome in quanto si tratta del criterio raggiunto dall'endpoint dopo la restituzione dall'evento di riautenticazione (denominato **Wireless_Guest_Access**).

12. Nella casella **Dettagli gruppo di identità**, selezionare **Gruppo di identità endpoint** e selezionare il gruppo a cui si fa riferimento in Tipo ospite (Endpoint ospiti).

13. In **Risultati** selezionare **PermitAccess**. Fate clic su **Fatto (Done)** e **salvate** le modifiche.

Wireless_Guest_Access if GuestEndpoints AND Wireless_MAB then PermitAccess
 Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

14. Creare e rimuovere i criteri che cancellano giornalmente il gruppo GuestEndpoint.

- Passare a **Amministrazione > Gestione identità > Impostazioni > Rimozione endpoint**
- In **Purge** rules è necessario che sia presente una regola predefinita che attivi l'eliminazione di GuestEndpoints se il tempo trascorso è maggiore di 30 giorni.
- Modificare i criteri esistenti per GuestEndpoints o crearne uno nuovo, nel caso in cui sia stato rimosso il criterio predefinito. I criteri di rimozione vengono eseguiti ogni giorno a un'ora definita.


In questo caso, la condizione è Membri di GuestEndpoints con Giorni trascorsi inferiori a 1 giorno

Caso di utilizzo 3: portale HostSpot

Panoramica sul flusso

1. L'utente wireless si connette al SSID guest.
2. WLC autentica l'endpoint in base al suo indirizzo MAC utilizzando ISE come server AAA.
3. ISE restituisce un access-accept con due coppie di valori di attributo (AVP): url-redirect e url-redirect-acl.
4. Una volta che il WLC applica gli AVP alla sessione dell'endpoint, la stazione passa a DHCP-Required e, dopo aver acquisito un indirizzo IP, rimane in CENTRAL_WEB_AUTH. In questa fase, il WLC è pronto a reindirizzare il traffico http / https del client.
5. L'utente finale apre il browser Web e, una volta generato il traffico HTTP o HTTPS, il WLC reindirizza l'utente al portale ISE HotSpot.
6. Una volta nel portale, all'utente viene richiesto di accettare le Regole d'uso accettabili.
7. ISE aggiunge l'indirizzo MAC dell'endpoint (ID endpoint) nel gruppo Endpoint Identity configurato.
8. Il PSN (Policy Services Node) che elabora la richiesta emette un comando **Admin-Reset** di tipo CoA dinamico sul WLC.
9. Al termine dell'elaborazione del CoA in entrata, il WLC emette una richiesta di deautenticazione per il client (la connessione viene interrotta per il tempo necessario al client per tornare).
10. Dopo la riconnessione del client, viene creata una nuova sessione che non garantisce la continuità della sessione sul lato ISE. Significa che l'autenticazione viene elaborata come un nuovo thread.
11. Poiché l'endpoint viene aggiunto al gruppo di identità dell'endpoint configurato ed esiste un criterio di autorizzazione che verifica se l'endpoint fa parte di tale gruppo, la nuova autenticazione corrisponde a questo criterio. Il risultato è l'accesso completo alla rete Guest.
12. L'utente non deve accettare di nuovo le CDS a meno che l'oggetto identità dell'endpoint non venga eliminato dal database ISE come risultato di un criterio di rimozione degli endpoint.

Configurazione

1. Crea un nuovo gruppo di identità degli endpoint in cui spostare i dispositivi alla registrazione. Passare a **Centri di lavoro > Accesso guest > Gruppi di identità > Gruppi di identità degli endpoint** e fare clic su  .
- Immettere il nome di un gruppo (in questo caso HotSpot_Endpoints). Aggiungere una descrizione e non è necessario alcun gruppo padre.

Endpoint Identity Group List > HotSpot_Endpoints

Endpoint Identity Group

* Name

Description

Parent Group

2. Passare a **Centri di lavoro > Accesso guest > Configura > Portali guest > seleziona Portale hotspot (impostazione predefinita).**

3. Espandere Impostazioni portale e in Gruppo identità endpoint selezionare il gruppo **HotSpot_Endpoints** in **Gruppo identità endpoint**. Le periferiche registrate vengono inviate al gruppo specificato.

Endpoint

Identity *Configure endpoint identity groups at:*

group: * [Work Centers > Guest Access > Identity Groups](#)

4. **Salvare** le modifiche.

5. Creare il profilo di autorizzazione che chiama il portale HotSpot all'autenticazione MAB originata dal WLC.

- Passare a **Criterio > Elementi criteri > Risultati > autorizzazione > Profili di autorizzazione** e crearne uno (HotSpotRedirect).
- Una volta selezionato il **reindirizzamento Web (CWA, MDM, NSP, CPP)**, selezionare **Area sensibile**, quindi digitare il nome dell'ACL di reindirizzamento nel campo ACL (Guest_Redirect) e come valore selezionare il portale corretto (**Portale area sensibile (impostazione predefinita)**).

Add New Standard Profile

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Hot Spot: ACL: Value:

Static IP/Host name/FQDN

Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = url-redirect-ad=Guest_Redirect
 cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw

6. Creare i criteri di autorizzazione che attivano il risultato HotSpotRedirect su richiesta MAB iniziale da parte di WLC.

- Passare a **Criterio > Autorizzazione** e inserire una nuova regola. Questa regola attiva il processo di reindirizzamento in risposta alla richiesta di autenticazione MAC iniziale dal WLC (in questo caso chiamata **Wireless_HotSpot_Redirect**).
- In **Condizioni** scegliere **Seleziona condizione esistente da libreria**, quindi in **nome condizione** selezionare **Condizione composta**
- In **Risultati**, selezionare **Standard > HotSpotRedirect** (profilo di autorizzazione creato nel passaggio precedente). Quindi fate clic su **Fatto (Done)** e **Salva (Save)**

7. Creare il secondo criterio di autorizzazione.

- Duplicare il criterio precedente, modificarne il nome in quanto si tratta del criterio raggiunto dall'endpoint dopo la restituzione dall'evento di riautenticazione (denominato **Wireless_HotSpot_Access**).
- Nella casella **Dettagli gruppo di identità** selezionare **Gruppo di identità endpoint**, quindi il gruppo creato in precedenza (**HotSpot_Endpoints**).
- In **Risultati** selezionare **PermitAccess**. Fate clic su **Fatto (Done)** e **salvate** le modifiche.

<input checked="" type="checkbox"/>	Wireless_HotSpot_Access	if HotSpot_Endpoints AND Wireless_MAB	then PermitAccess
<input checked="" type="checkbox"/>	Wireless_HotSpot_Redirect	if Wireless_MAB	then HotSpotRedirect

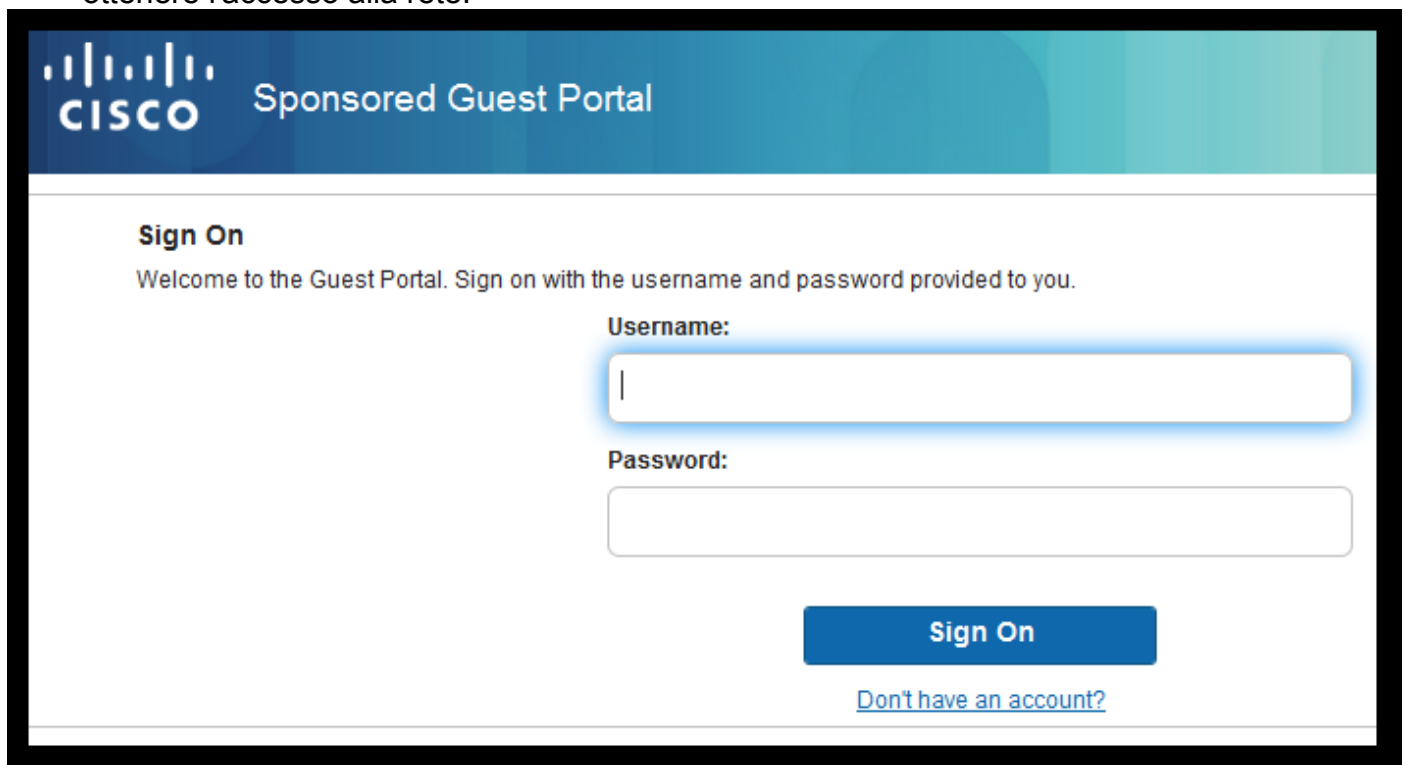
8. Configurare i criteri di rimozione per la cancellazione degli endpoint con un tempo trascorso superiore a 5 giorni.

- Passare a **Amministrazione > Gestione delle identità > Impostazioni > Rimozione endpoint** e in **Regole di rimozione** crearne una nuova.
- In **Dettagli gruppo di identità** selezionare **Gruppo di identità endpoint > HotSpot_Endpoints**
- In **condizioni** fare clic su **Crea nuova condizione (opzione avanzata)**.
- In **Seleziona attributo** scegliere **ENDPOINTPURGE : ElapsedDays** **MAGGIORE DI 5** giorni

Verifica

Caso di utilizzo 1

1. L'utente si connette al SSID guest.
2. Apre il browser e, non appena viene generato il traffico HTTP, viene visualizzato il portale guest.
3. Una volta che l'utente guest ha eseguito l'autenticazione e ha accettato le CDS, viene visualizzata una pagina di operazione riuscita.
4. Viene inviato un CoA di riautenticazione (trasparente per il client).
5. La sessione dell'endpoint viene riautenticata con accesso completo alla rete.
6. Qualsiasi connessione guest successiva deve passare l'autenticazione guest prima di ottenere l'accesso alla rete.



The screenshot shows the Cisco Sponsored Guest Portal Sign On page. The header features the Cisco logo and the text "Sponsored Guest Portal". Below the header, the page is titled "Sign On" and includes a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". A blue "Sign On" button is positioned below the password field. At the bottom, there is a link that says "Don't have an account?".



Sponsored Guest Portal

Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



Sponsored Guest Portal

Success

You now have Internet access through this network.

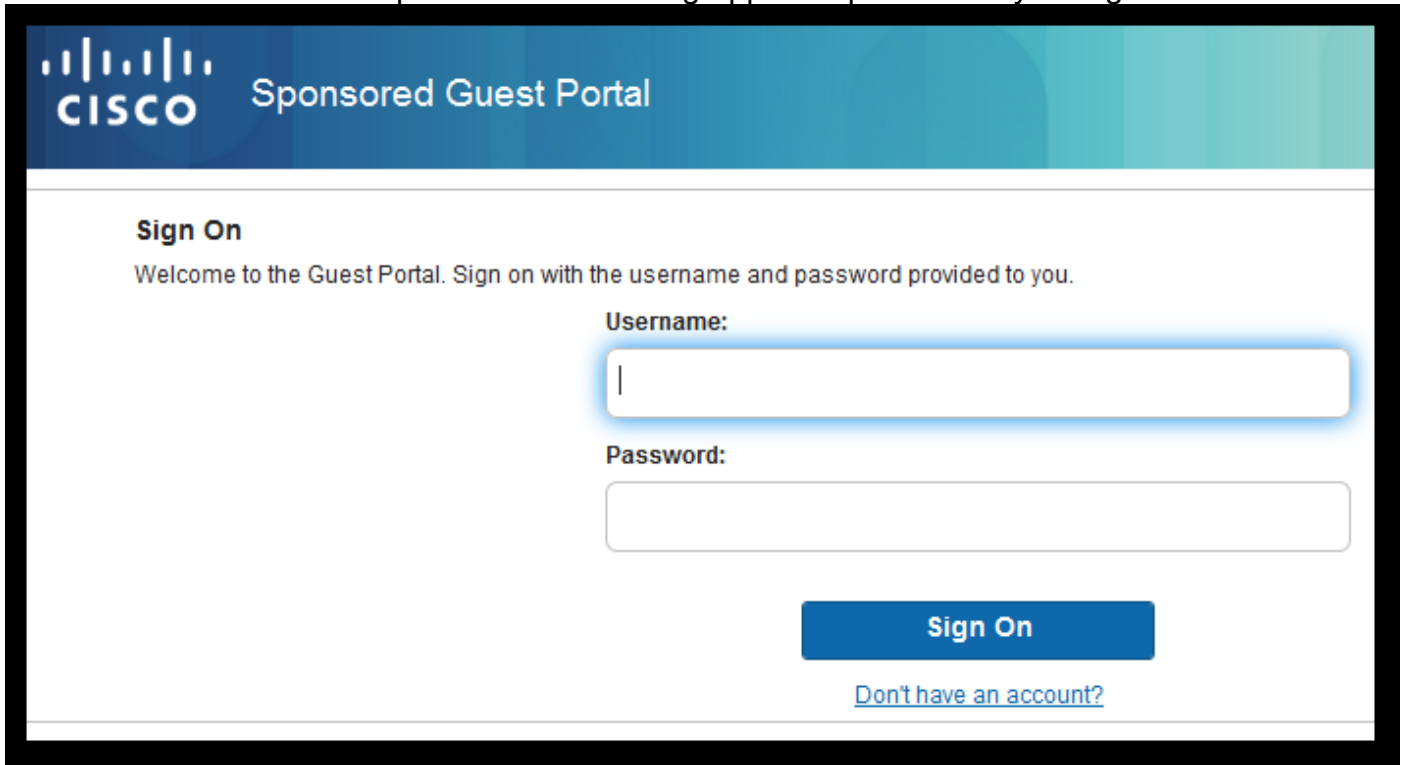
Flusso dai log ISE RADIUS Live:

1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Accounting Start
1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Re-Authentication Event
	68:7F:74:72:18:2E					← CoA Event
1001	68:7F:74:72:18:2E					← Guest Authentication Event
68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	← Initial MAB request

Caso di utilizzo 2

1. L'utente si connette al SSID guest.
2. Apre il browser e, non appena viene generato il traffico HTTP, viene visualizzato il portale guest.

3. Una volta che l'utente guest esegue l'autenticazione e accetta le CDS, il dispositivo viene registrato.
4. Viene visualizzata una pagina che indica la riuscita dell'operazione e viene inviata una nuova autenticazione CoA (trasparente per il client).
5. La sessione dell'endpoint viene riautenticata con accesso completo alla rete.
6. Qualsiasi connessione guest successiva è consentita senza applicare l'autenticazione guest, a condizione che l'endpoint sia ancora nel gruppo Endpoint Identity configurato.



The image shows a screenshot of the Cisco Sponsored Guest Portal. At the top, there is a blue header with the Cisco logo on the left and the text "Sponsored Guest Portal" on the right. Below the header, the page is titled "Sign On" in bold. Underneath the title, there is a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." The form contains two input fields: "Username:" and "Password:". The "Username:" field is currently empty and has a blue glow effect around it. Below the "Password:" field, there is a blue "Sign On" button. At the bottom of the form, there is a blue link that says "Don't have an account?".



Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

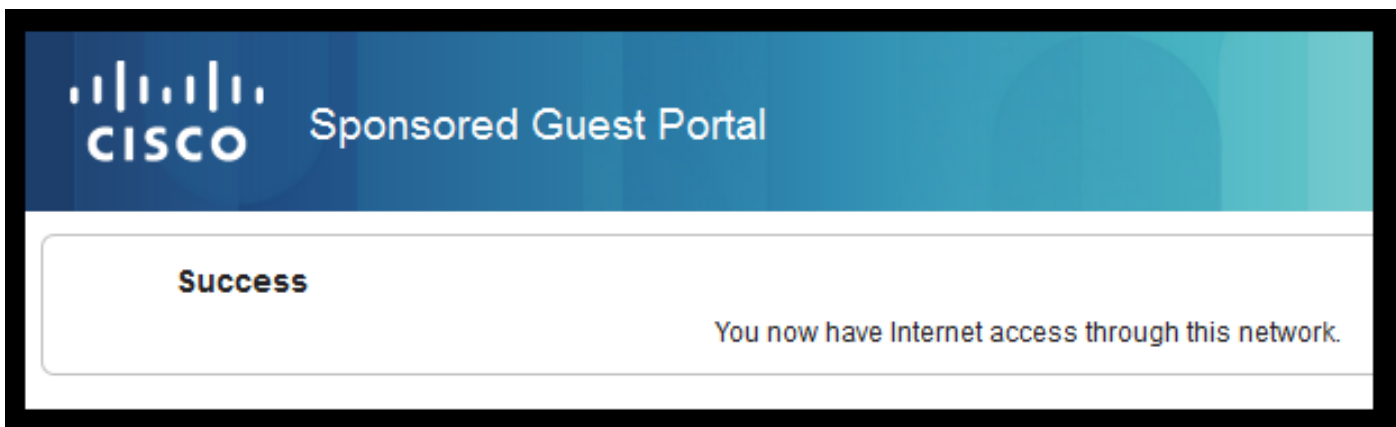


Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue



Flusso dai log ISE RADIUS Live:

Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
●		68:7F:74:72:1...	68:7F:74:72:1...	PermitAccess	
✓		68:7F:74:72:1...	68:7F:74:72:1...	PermitAccess	GuestEndpoints
✓		hfr592	68:7F:74:72:1...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
✓			68:7F:74:72:1...		
✓		hfr592	68:7F:74:72:1...		GuestType_Contractor (default)
✓		68:7F:74:72:1...	68:7F:74:72:1...	CWA_DeviceRegistration	Profiled

Accounting Start

Subsequent MAB request(no redirect to guest portal)

Re-Authentication Event

CoA Reauth Event

Guest Authentication and Device Registration

Initial MAB request

Caso di utilizzo 3

1. L'utente si connette al SSID guest.
2. Apre il browser e, non appena viene generato il traffico HTTP, viene visualizzata una pagina AUP.
3. Una volta che l'utente guest ha accettato l'AUP, il dispositivo viene registrato.
4. Viene visualizzata una pagina che indica la riuscita dell'operazione e viene inviato il comando Admin-Reset CoA (trasparente per il client).
5. L'endpoint si riconnette con accesso completo alla rete.
6. Qualsiasi connessione guest successiva è consentita senza applicare l'accettazione AUP (a meno che non sia configurato diversamente) per tutto il tempo in cui l'endpoint rimane nel gruppo Endpoint Identity configurato.



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline



Connection Successful

You have successfully connected to the network.

Switching locale FlexConnect in AireOS

Quando la commutazione locale di FlexConnect è configurata, l'amministratore di rete deve verificare che:

- L'ACL di reindirizzamento è configurato come ACL FlexConnect.
- L'ACL di reindirizzamento è stato applicato come criterio in entrambi i modi attraverso l'access point stesso in scheda **FlexConnect > ACL di autenticazione Web esterni > Criteri > Seleziona ACL di reindirizzamento e fare clic su Applica**

All APs > Details for aaa-ap-3

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID 301 **VLAN Mappings**

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

External WebAuthentication ACLs

Local Split ACLs

Central DHCP Processing

Layer2 ACLs

Policies

Policy ACL CWA_Redirect **Add**

Policy Access Control Lists

CWA_Redirect

In alternativa, aggiungendo l'ACL per i criteri al gruppo FlexConnect appartiene a (**Wireless > Gruppi FlexConnect > Selezionare il gruppo corretto > Mapping ACL > Criteri** Selezionare l'ACL di reindirizzamento e fare clic su Aggiungi)

FlexConnect Groups > Edit 'test'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping **Policies**

Policies

Policy ACL CWA_Redirect **Add**

Policy Access Control Lists

CWA_Redirect

TOR_Redirect

L'aggiunta di ACL basati su criteri attiva il WLC per eseguire il push dell'ACL configurato agli AP membri del gruppo FlexConnect. Se non si esegue questa operazione, si verifica un problema di reindirizzamento Web.

Scenario di ancoraggio esterno

Negli scenari di ancoraggio automatico (Foreign-Anchor) è importante evidenziare i seguenti fatti:

- È necessario definire l'ACL di reindirizzamento sul WLC esterno e su quello di ancoraggio. Anche quando viene applicata solo sull'ancora.
- L'autenticazione di layer 2 è sempre gestita dal WLC esterno. Ciò è fondamentale durante le fasi di progettazione (anche per la risoluzione dei problemi), in quanto tutto il traffico di autenticazione e accounting RADIUS si verifica tra ISE e il WLC esterno.
- Una volta applicati gli AVP di reindirizzamento alla sessione client, il WLC esterno aggiorna la sessione client nell'ancoraggio tramite un messaggio di handoff della mobilità.
- A questo punto, il WLC di ancoraggio inizia a imporre il reindirizzamento usando il Redirect-ACL che è stato preconfigurato.
- È necessario disattivare completamente l'accounting sull'SSID WLC di ancoraggio per evitare aggiornamenti dell'accounting verso ISE (che fanno riferimento allo stesso evento di autenticazione) provenienti sia dall'ancoraggio che dall'esterno.
- Gli ACL basati su URL non sono supportati negli scenari di ancoraggio esterno.

Risoluzione dei problemi

Stati di interruzione comuni su AireOS e Converged Access WLC

1. Il client non è in grado di partecipare al SSID guest

Un messaggio "**show client detailed xx:xx:xx:xx:xx**" indica che il client è bloccato in **START**. In genere questo è un indicatore del WLC che non è in grado di applicare un attributo restituito dal server AAA.

Verificare che il nome dell'ACL di reindirizzamento predefinito da ISE corrisponda esattamente al nome dell'ACL predefinito sul WLC.

Lo stesso principio si applica a qualsiasi altro attributo configurato per ISE per il push al WLC (VLAN ID, nomi interfaccia, Airespace-ACL). Il client deve quindi passare a DHCP e quindi a CENTRAL_WEB_AUTH.

2. Gli AVP di reindirizzamento vengono applicati alla sessione del client ma il reindirizzamento non funziona

Verificare che lo stato del gestore dei criteri del client sia CENTRAL_WEB_AUTH con un indirizzo IP valido allineato all'interfaccia dinamica configurata per l'SSID e che gli attributi Redirect ACL e URL-Redirect vengano applicati alla sessione del client.

ACL di reindirizzamento

Nei WLC di AireOS, l'ACL di reindirizzamento deve consentire esplicitamente il traffico che non deve essere reindirizzato, come DNS e ISE sulla porta TCP 8443 in entrambe le direzioni e l'implicito rifiuto dell'indirizzo IP any attiva il reindirizzamento del resto del traffico.

In Accesso convergente la logica è opposta. Nega reindirizzamento ACE ignorato mentre Consenti ACE attiva il reindirizzamento. Per questo motivo, si consiglia di autorizzare

esplicitamente le porte TCP 80 e 443.

Verificare l'accesso all'ISE sulla porta 8443 dalla VLAN guest. Se dal punto di vista della configurazione tutto sembra buono, il modo più semplice per procedere è catturare un'immagine dietro la scheda wireless del client e verificare dove si interrompe il reindirizzamento.

- La risoluzione DNS avviene?
- L'handshake a 3 vie TCP è stato completato sulla pagina richiesta?
- Il WLC restituisce un'azione di reindirizzamento dopo l'avvio del comando GET da parte del client?
- L'handshake TCP a 3 vie con ISE over 8443 è stato completato?

3. Il client non è in grado di accedere alla rete dopo che ISE ha inserito una modifica alla VLAN alla fine del flusso guest

Una volta che il client ha acquisito un indirizzo IP all'inizio del flusso (stato di pre-reindirizzamento), se una modifica della VLAN viene disattivata dopo l'autenticazione Guest (riautenticazione post CoA), l'unico modo per forzare un rilascio/rinnovo DHCP nel flusso Guest (senza agente di postura) è tramite un'applet Java che nei dispositivi mobili non funziona.

In questo modo, il client rimane bloccato nella VLAN X con un indirizzo IP della VLAN Y. È necessario tenerne conto durante la pianificazione della soluzione.

4. ISE visualizza il messaggio "HTTP 500 Internal error, Radius session not found" (Errore interno HTTP 500, sessione Radius non trovata) nel browser del client guest durante il reindirizzamento

Questo in genere è un indicatore della perdita di sessione su ISE (sessione terminata). Il motivo più comune è la configurazione dell'accounting sul WLC di ancoraggio quando è stato distribuito Foreign-Anchor. Per risolvere questo problema, disabilitare l'accounting sull'ancoraggio e lasciare l'autenticazione e l'accounting dell'handle esterno.

5. Il client si disconnette e rimane disconnesso o si connette a un SSID diverso dopo aver accettato le CDS nel portale HotSpot di ISE.

Questa condizione può essere rilevata in HotSpot a causa del cambiamento dinamico di autorizzazione (CoA) coinvolto in questo flusso (CoA Admin Reset) che determina il rilascio di un'autorizzazione alla stazione wireless da parte del WLC. La maggior parte degli endpoint wireless non ha problemi a tornare all'SSID dopo la deautenticazione, ma in alcuni casi il client si connette a un altro SSID preferito in risposta all'evento di deautenticazione. L'ISE o il WLC non permettono di evitare questa condizione, in quanto spetta al client wireless attenersi all'SSID originale o connettersi a un altro SSID disponibile (preferito).

In questo caso, l'utente wireless deve riconnettersi manualmente all'SSID HotSpot.

AireOS WLC

```
(Cisco Controller) >debug client
```

Debug del client imposta su DEBUG un set di componenti coinvolti nelle modifiche apportate al computer dello stato del client.

```
(Cisco Controller) >show debug
```

```
MAC Addr 1..... AA:AA:AA:AA:AA:AA
```

Debug Flags Enabled:

```
dhcp packet enabled.  
dot11 mobile enabled.  
dot11 state enabled  
dot1x events enabled.  
dot1x states enabled.  
mobility client handoff enabled.  
pem events enabled.  
pem state enabled.  
802.11r event debug enabled.  
802.11w event debug enabled.  
CCKM client debug enabled.
```

Debug dei componenti AAA

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

Questo può influire sulle risorse a seconda della quantità di utenti che si connettono tramite MAB o SSID Dot1X. Questi componenti a livello di DEBUG registrano le transazioni AAA tra WLC e ISE e stampano i pacchetti RADIUS sullo schermo.

Questa operazione è critica se ISE non è in grado di fornire gli attributi previsti o se il WLC non li elabora correttamente.

reindirizzamento Web-Auth

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

Questa opzione può essere utilizzata per verificare che il WLC stia attivando correttamente il reindirizzamento. Questo è un esempio di come deve apparire il reindirizzamento dai debug:

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a050000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a050000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430  
  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is  
HTTP/1.1 200 OK  
Location:  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a050000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-0050
```

NGWC

Debug del client imposta su DEBUG un set di componenti coinvolti nelle modifiche apportate al computer dello stato del client.

```
3850#debug client mac-address <client MAC>
```

Questo componente stampa i pacchetti RADIUS (Authentication and Accounting) sullo schermo. Ciò è utile quando è necessario verificare che ISE fornisca gli AVP corretti e che il CoA sia inviato ed elaborato correttamente.

```
3850#debug radius
```

Verranno eseguite tutte le transizioni AAA (autenticazione, autorizzazione e accounting) quando sono coinvolti client wireless. Ciò è fondamentale per verificare che WLC analizzi correttamente gli AVP e li applichi alla sessione client.

```
3850#debug aaa wireless all
```

Ciò può essere attivato quando si sospetta un problema di reindirizzamento sulla NGWC.

```
3850#debug epm plugin redirect all
```

```
3850#debug ip http transactions
```

```
3850#debug ip http url
```

ISE

Registri RADIUS Live

Verificare che la richiesta MAB iniziale sia stata elaborata correttamente in ISE e che ISE rimandi indietro gli attributi previsti. Passare a **Operazioni > RADIUS > Live Log** e filtrare l'output utilizzando l'indirizzo MAC del client in **ID endpoint**. Una volta trovato l'evento di autenticazione, fare clic sui dettagli e verificare i risultati inseriti come parte dell'accettazione.



Result

UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

TCPDump

Questa funzione può essere utilizzata quando è necessario uno scambio di pacchetti RADIUS più approfondito tra ISE e WLC. In questo modo è possibile dimostrare che ISE invia gli attributi corretti nell'access-accept senza dover abilitare i debug sul lato WLC. Per avviare un'acquisizione utilizzando TCDDump, selezionare **Operazioni > Risoluzione dei problemi > Strumenti di diagnostica > Strumenti generali > TCPDump**.

Questo è un esempio di un flusso corretto acquisito tramite TCPump

Source	Destination	Protocol	Length	Info
154.5	157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
157.13	154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
154.5	157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
157.13	154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
157.13	154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
154.5	157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
154.5	157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
157.13	154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

Di seguito sono elencati gli AVP inviati in risposta alla richiesta MAB iniziale (secondo pacchetto nello screenshot riportato sopra).

RADIUS Protocol

```
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: f1eaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
  AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
  AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
  AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
  AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
  AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=189 t=Cisco-AVPair(1): url-
```

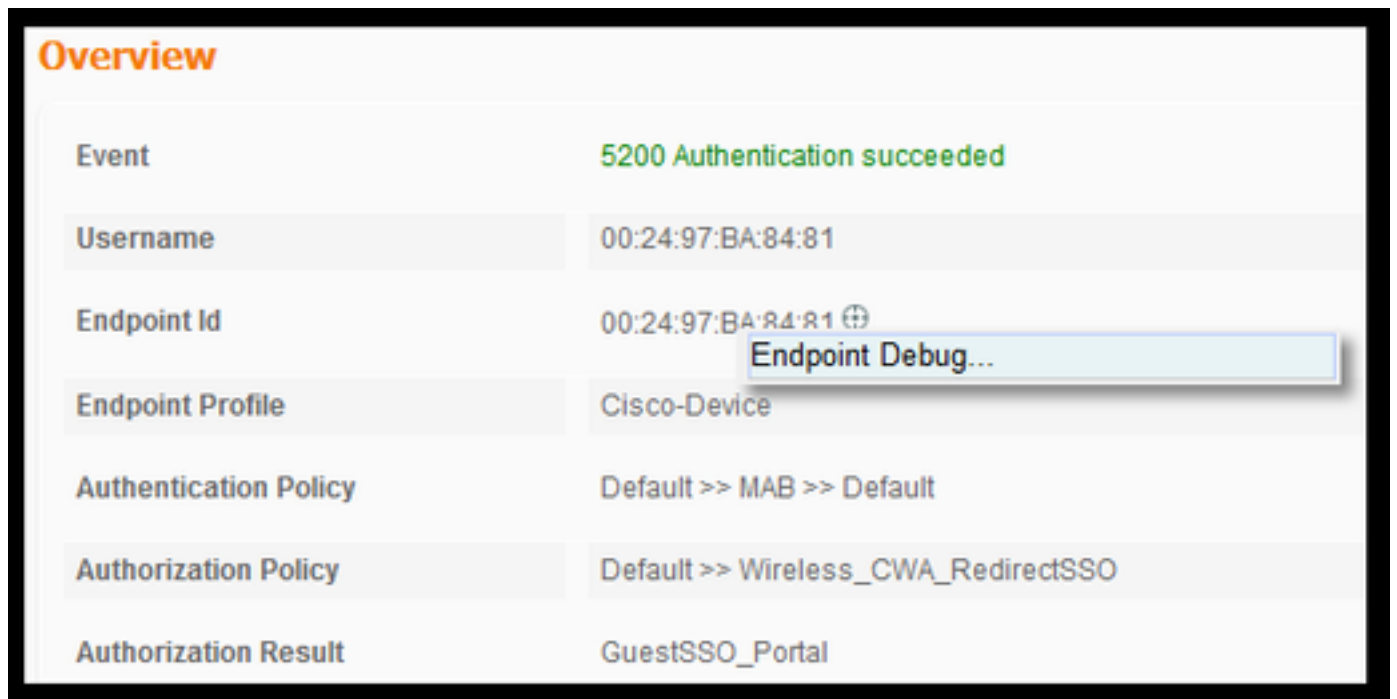
redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a050000aa05565e1c9&portal=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622

AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)

Debug degli endpoint:

Per approfondire i processi ISE che richiedono decisioni sulle policy, selezione del portale, autenticazione guest e CoA, il modo più semplice per risolvere il problema è abilitare i **debug degli endpoint**, senza dover impostare i componenti completi a livello di debug.

Per attivare questa opzione, selezionare **Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Strumenti generali > Debug di EndPoint**.

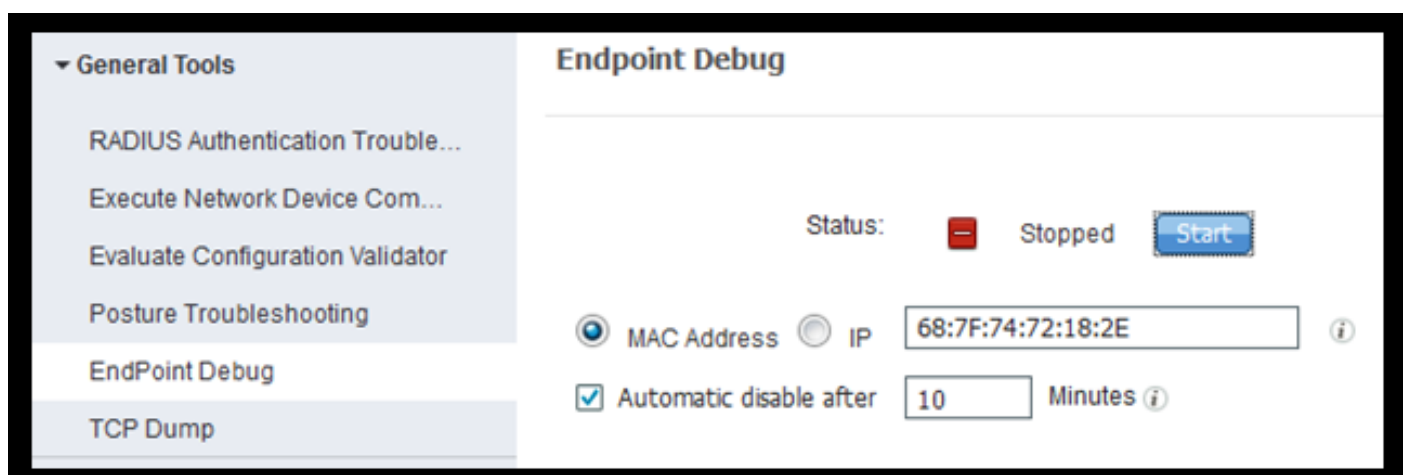


The screenshot shows the 'Overview' page in the ISE GUI. It displays the following information:

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81 ⓘ
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

A context menu is open over the 'Endpoint Id' field, showing the option 'Endpoint Debug...'. The entire screenshot is framed with a thick black border.

Nella pagina Debug endpoint, immettere l'indirizzo MAC dell'endpoint e fare clic su Avvia quando si è pronti a ricreare il problema.




The screenshot shows the 'Endpoint Debug' configuration page in the ISE GUI. On the left is a sidebar with 'General Tools' expanded, showing options like 'RADIUS Authentication Trouble...', 'Execute Network Device Com...', 'Evaluate Configuration Validator', 'Posture Troubleshooting', 'EndPoint Debug', and 'TCP Dump'. The main area is titled 'Endpoint Debug' and contains:


- Status: Stopped (with a red stop icon and a 'Start' button)
- MAC Address (selected) or IP: 68:7F:74:72:18:2E (with an info icon)
- Automatic disable after: 10 Minutes (with an info icon)


The entire screenshot is framed with a thick black border.

Dopo aver interrotto il debug, fare clic sul collegamento che identifica l'ID dell'endpoint per scaricare l'output del debug.

Endpoint Debug

Status:  Processing ...

MAC Address IP 

Automatic disable after Minutes 

Selected 0 | Total 1

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input type="checkbox"/>	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

Informazioni correlate

[Compilazioni AireOS consigliate TAC](#)

[Guida alla configurazione di Cisco Wireless Controller, versione 8.0.](#)

[Guida per l'amministratore di Cisco Identity Services Engine, versione 2.1](#)

[Configurazione wireless NGWC universale con Identity Services Engine](#)

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).