Esempio di configurazione dell'autenticazione Web centrale su WLC di accesso convergente e ad accesso unificato

Sommario

Introduzione

Questo documento descrive come configurare l'autenticazione Web centrale sul controller WLC (Converged Access Wireless LAN Controller) e anche tra il WLC ad accesso convergente e il WLC ad accesso unificato (5760 e anche tra 5760 e 5508).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Cisco WLC 5508, 5760, 3850
- Conoscenze base di Identity Services Engine (ISE)
- Conoscenze base di mobilità wireless
- Conoscenze base di ancoraggio ospiti

Componenti usati

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

- WLC 5760 con Cisco IOS® XE release 3.3.3
- WLC 5508 con Cisco Aironet OS release 7.6
- Switch 3850 con Cisco IOS XE release 3.3.3
- Cisco ISE con release 1.2

Configurazione

> **Nota**: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

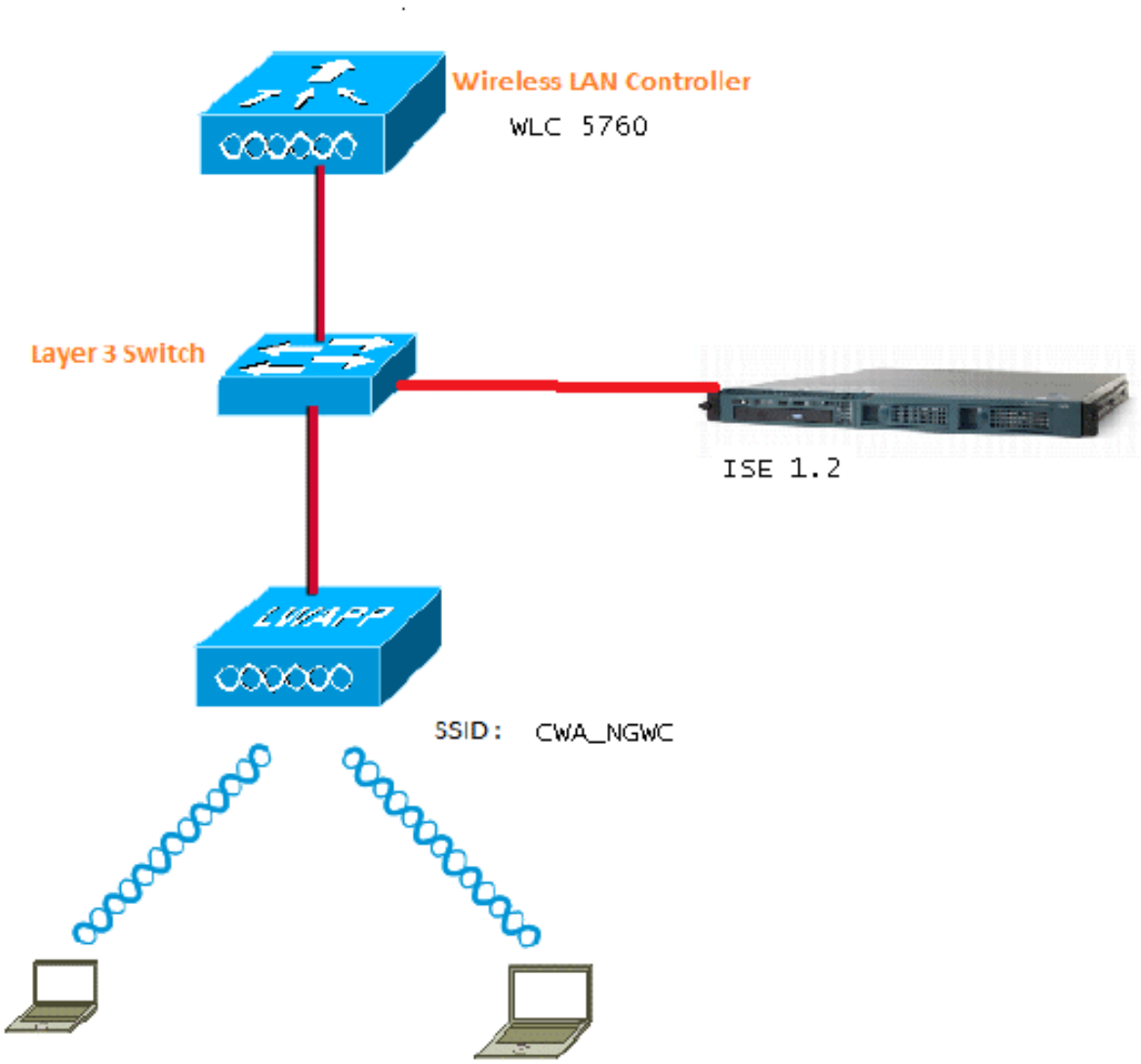
Il flusso include i passi riportati di seguito.

1. L'utente viene associato all'SSID (Service Set Identifier) dell'autenticazione Web, che in realtà è open+macfiltering senza protezione di livello 3.
2. Verrà aperto il browser.
3. Il WLC reindirizza al portale guest.
4. L'utente esegue l'autenticazione nel portale.
5. L'ISE invia una richiesta di modifica dell'autorizzazione RADIUS (CoA - UDP Port 1700) per segnalare al controller che l'utente è valido e infine spinge gli attributi RADIUS come l'Access Control List (ACL).
6. All'utente viene richiesto di riprovare l'URL originale.

Cisco utilizza tre diverse impostazioni di distribuzione che coprono tutti i diversi scenari per eseguire Central Web Authentication (CWA).

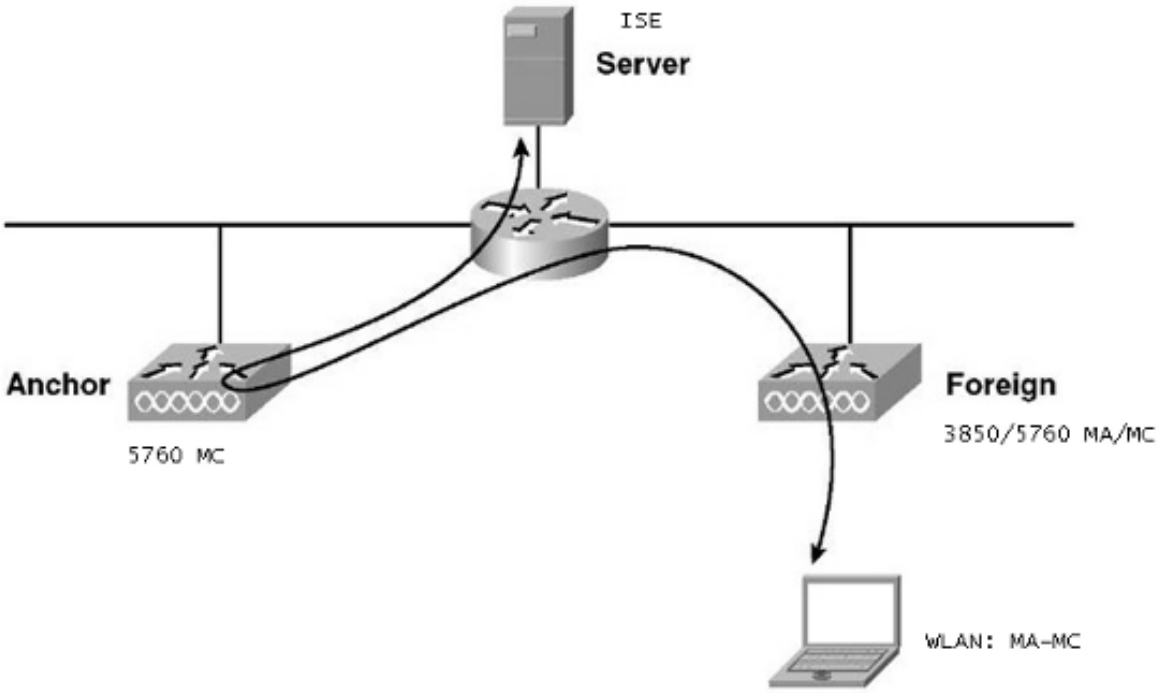
Topologia 1

Il 5760 WLC funziona come WLC standalone e i punti di accesso terminano sullo stesso 5760 WLC. I client sono connessi a una LAN wireless (WLAN) e sono autenticati all'ISE.



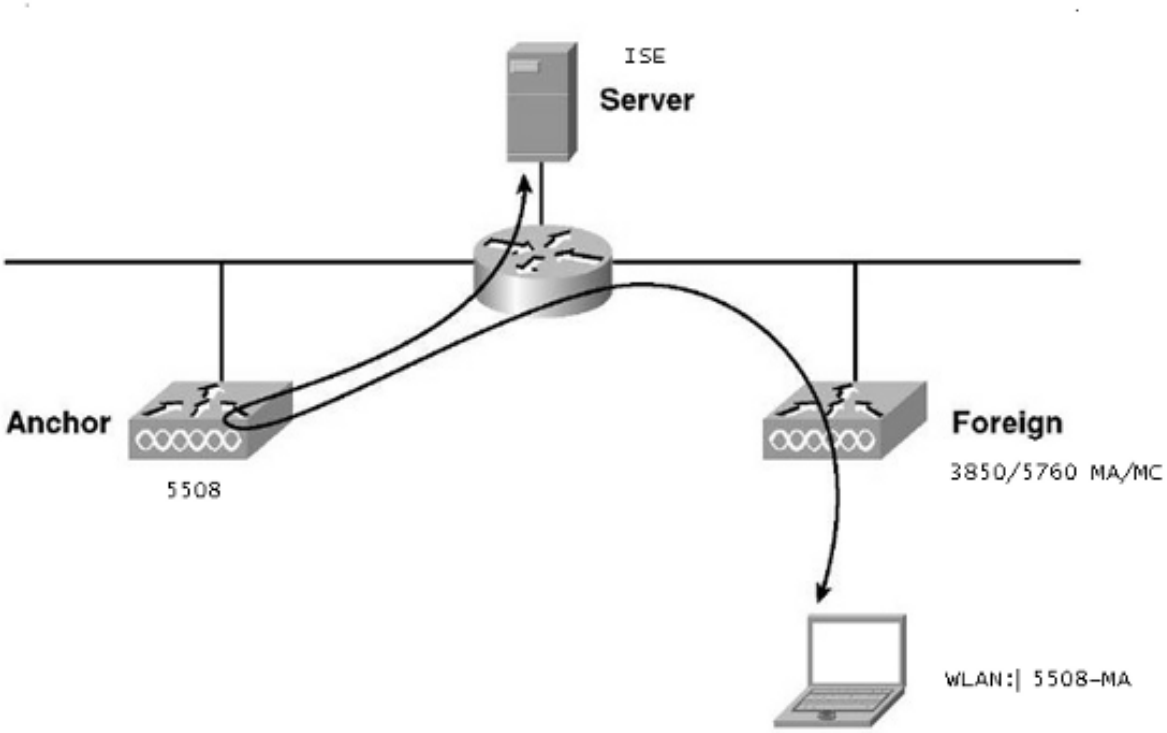
Topologia 2

Ancoraggio guest tra il WLC ad accesso convergente con uno che agisce come controller di mobilità e l'altro come agente di mobilità. L'agente di mobilità è il WLC esterno e il controller di mobilità è l'ancoraggio.



Topologia 3

Ancoraggio guest tra Cisco Unified WLC 5508 e Converged Access WLC 5760/3850 con uno che funge da controller di mobilità e l'altro da agente di mobilità. Il Mobility Agent/Mobility Controller è il WLC esterno e il Mobility Controller 5508 è l'ancoraggio.



Nota: ci sono molte implementazioni in cui l'ancora è il controller di mobilità e il WLC esterno è l'agente di mobilità che ottiene la licenza da un altro controller di mobilità. In questo caso, il WLC straniero ha un solo Anchor e quello Anchor è quello che spinge le politiche. Il doppio ancoraggio non è supportato e non funziona perché non dovrebbe funzionare in questo modo.

Esempio

Il WLC 5508 funge da ancoraggio e il WLC 5760 da controller di mobilità per uno switch 3850 funziona come agente di mobilità. Per la WLAN esterna di ancoraggio, la WLC 5508 sarà l'ancoraggio della WLAN esterna 3850. Non è necessario configurare tale WLAN sul WLC 5760. Se si punta lo switch 3850 all'ancoraggio 5760 e quindi si passa dal WLC 5760 al WLC 5508 come doppio ancoraggio, non funzionerà in quanto questo diventa doppio ancoraggio e le policy si trovano sull'ancoraggio 5508.

Se si dispone di una configurazione che include un WLC 5508 come ancoraggio, un WLC 5760 come controller di mobilità e uno switch 3850 come agente di mobilità e WLC esterno, in un qualsiasi momento l'ancoraggio per lo switch 3850 sarà il WLC 5760 o il WLC 5508. Non può essere contemporaneamente e il doppio ancoraggio non funziona.

Esempio di configurazione della topologia 1

Vedere Topologia 1 per il diagramma di rete e la spiegazione.

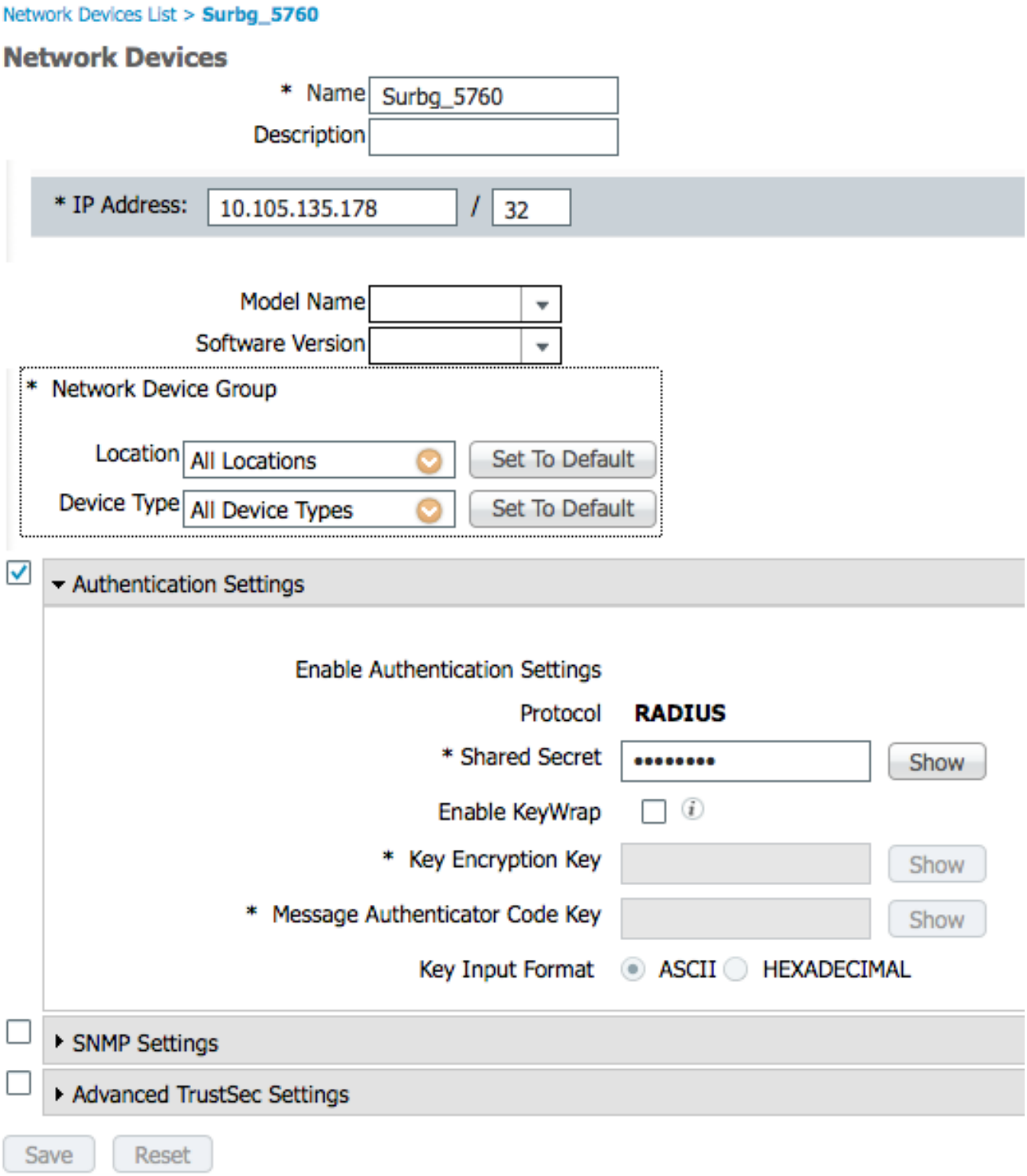
La configurazione è un processo in due passaggi:

1. sull'ISE.
2. Configurazione sul WLC.

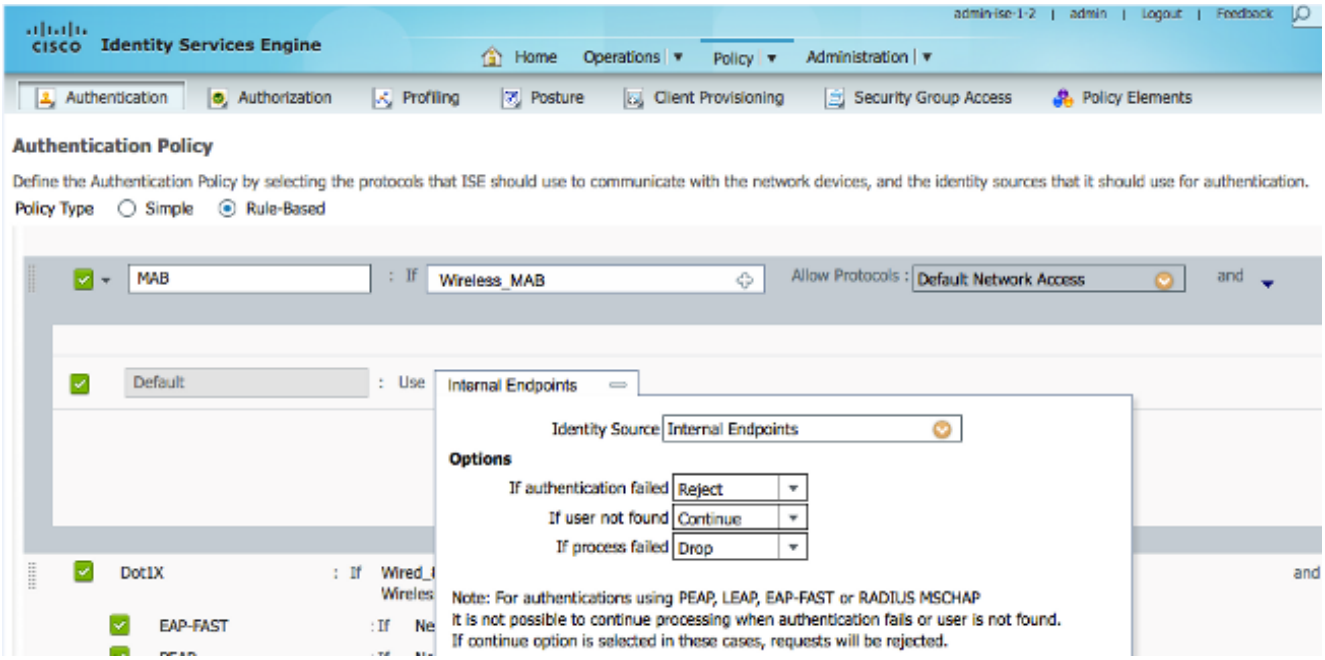
Il WLC 5760 funziona come WLC standalone e gli utenti vengono autenticati all'ISE.

Configurazione sull'ISE

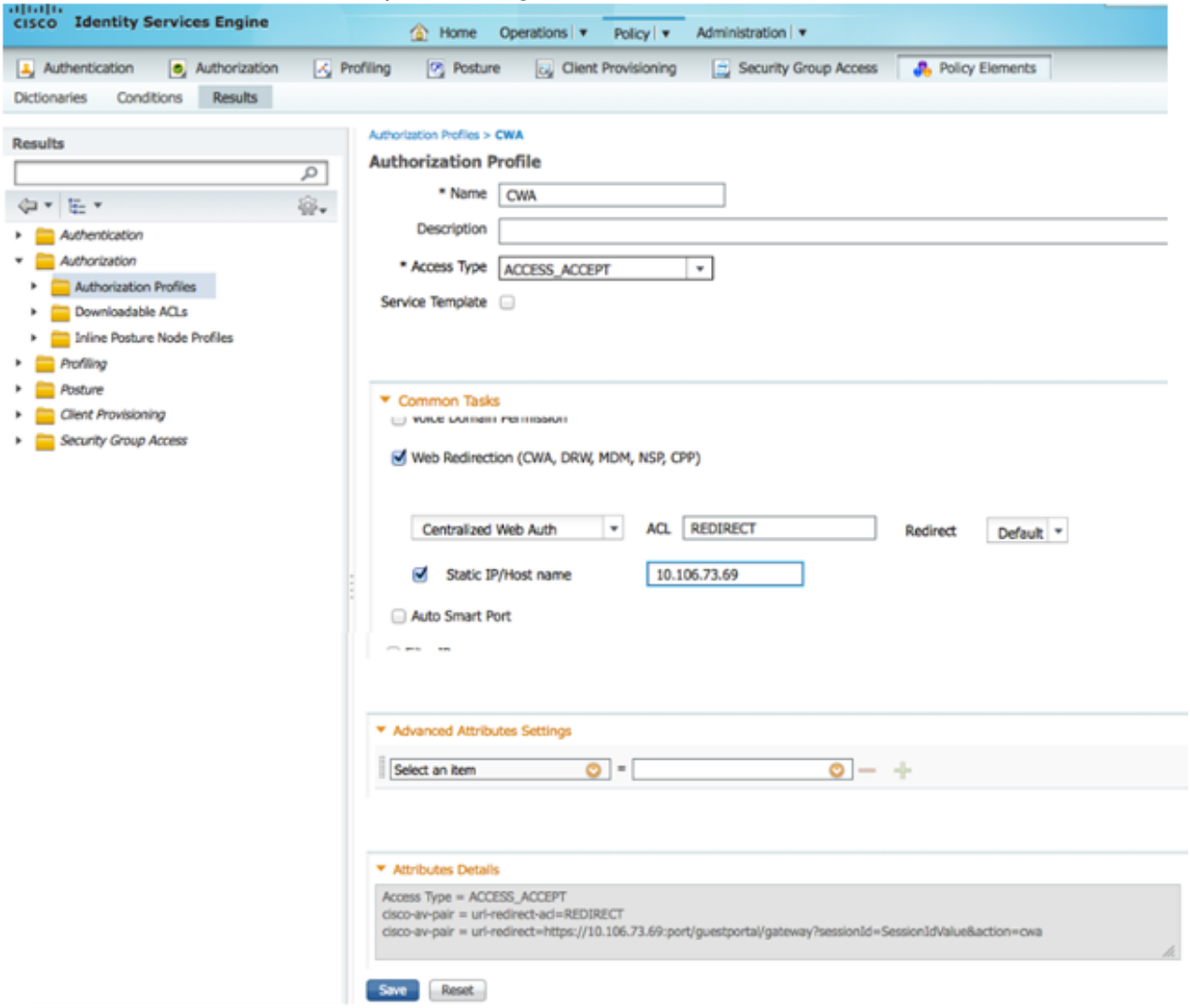
1. Scegliere **ISE GUI > Administration > Network Resource > Network Devices List > Add** per aggiungere il WLC sull'ISE come client di autenticazione, autorizzazione e accounting (AAA). Assicurarsi di immettere lo stesso segreto condiviso nel WLC aggiunto al server RADIUS.
   Nota: durante la distribuzione di Anchor-Foreign, è sufficiente aggiungere il WLC esterno. Non è necessario aggiungere il WLC di ancoraggio sull'ISE come client AAA. La stessa configurazione ISE viene utilizzata per tutti gli altri scenari di implementazione illustrati nel presente
   documento.



2. Dalla GUI di ISE, scegliere **Policy > Authentication > MAB > Edit (Policy > Autenticazione > MAB > Modifica)** per creare la policy di autenticazione. Il criterio di autenticazione accetta l'indirizzo MAC del client che punta agli endpoint interni. Nell'elenco Opzioni selezionare le opzioni seguenti:Dall'elenco a discesa Se l'autenticazione non è riuscita, scegliere **Rifiuta**.Dall'elenco a discesa Se l'utente non è stato trovato, scegliere **Continua**.Dall'elenco a discesa Se il processo non è riuscito, scegliere **Elimina**.Quando si esegue la configurazione con queste opzioni, il client che non ha ottenuto l'autorizzazione MAC procede con il portale guest.

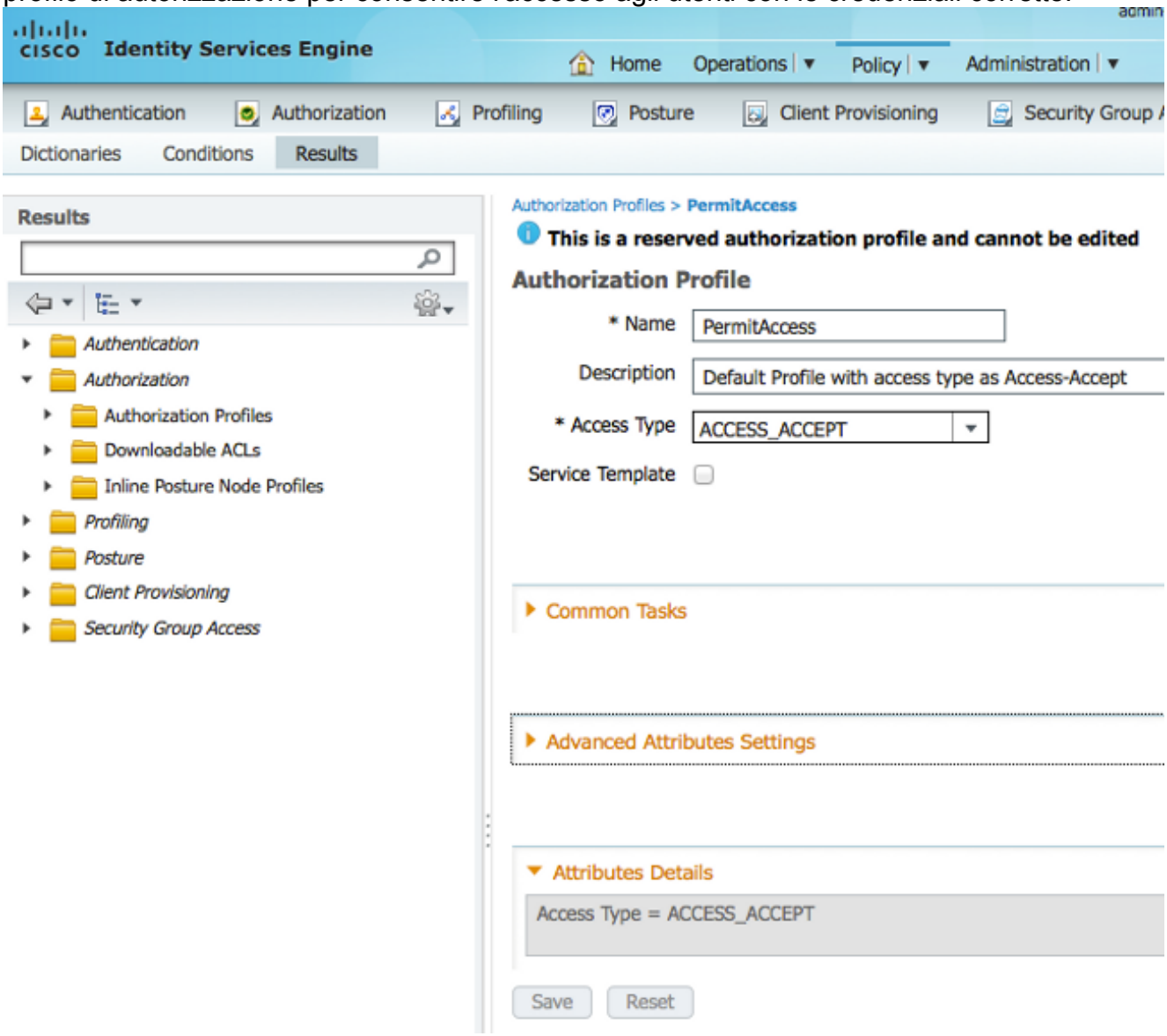


3. Dalla GUI di ISE, scegliere **Policy > Authorization > Results > Authorization Profiles > Add** (Policy > Autorizzazione > Risultati > Profili di autorizzazione > Aggiungi). Immettere i dettagli e fare clic su **Salva** per creare il profilo di autorizzazione. Questo profilo consente ai client di essere reindirizzati all'URL di reindirizzamento dopo l'autenticazione MAC, in cui i client immettono il nome utente e la password guest.

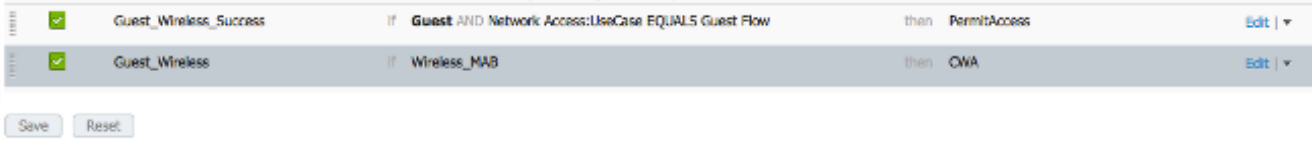


4. Dalla GUI di ISE, scegliere **Policy > Authorization > Results > Authorization Profiles > Add**

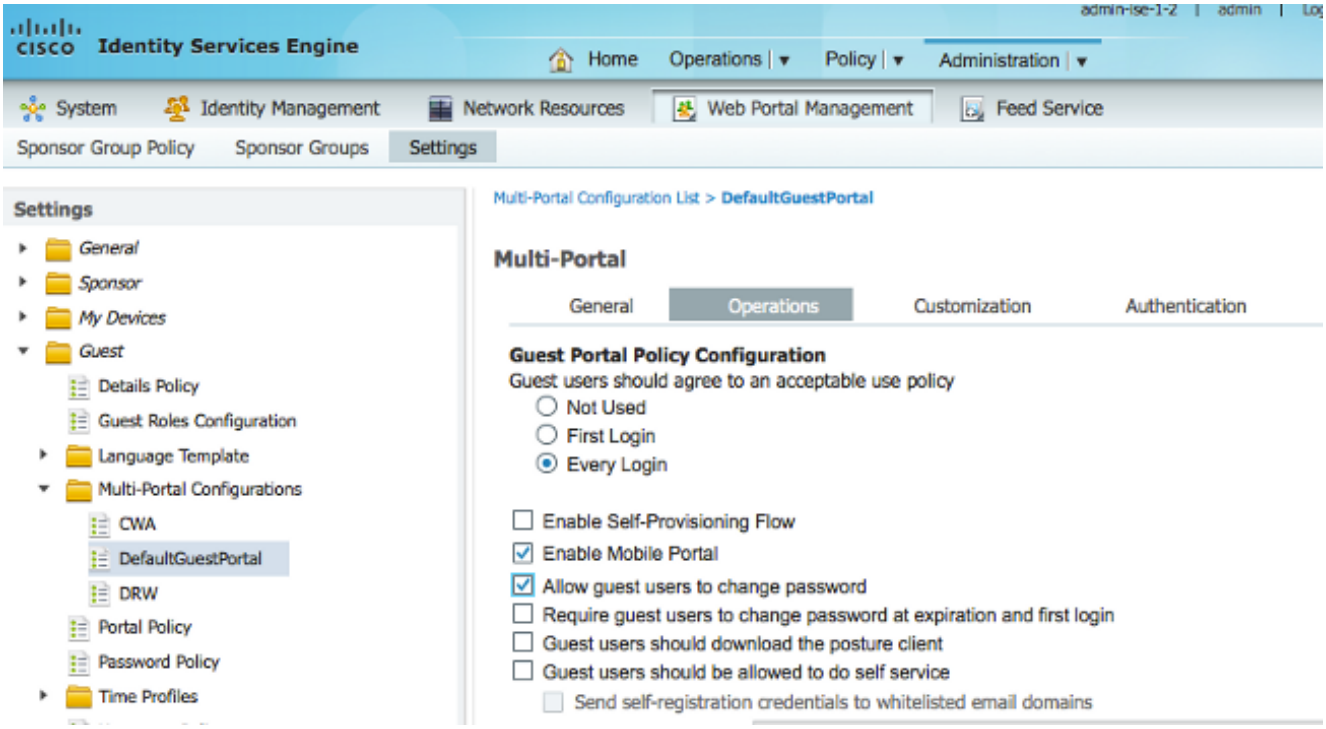
(Policy > Autorizzazione > Risultati > Profili di autorizzazione > Aggiungi) per creare un altro profilo di autorizzazione per consentire l'accesso agli utenti con le credenziali corrette.



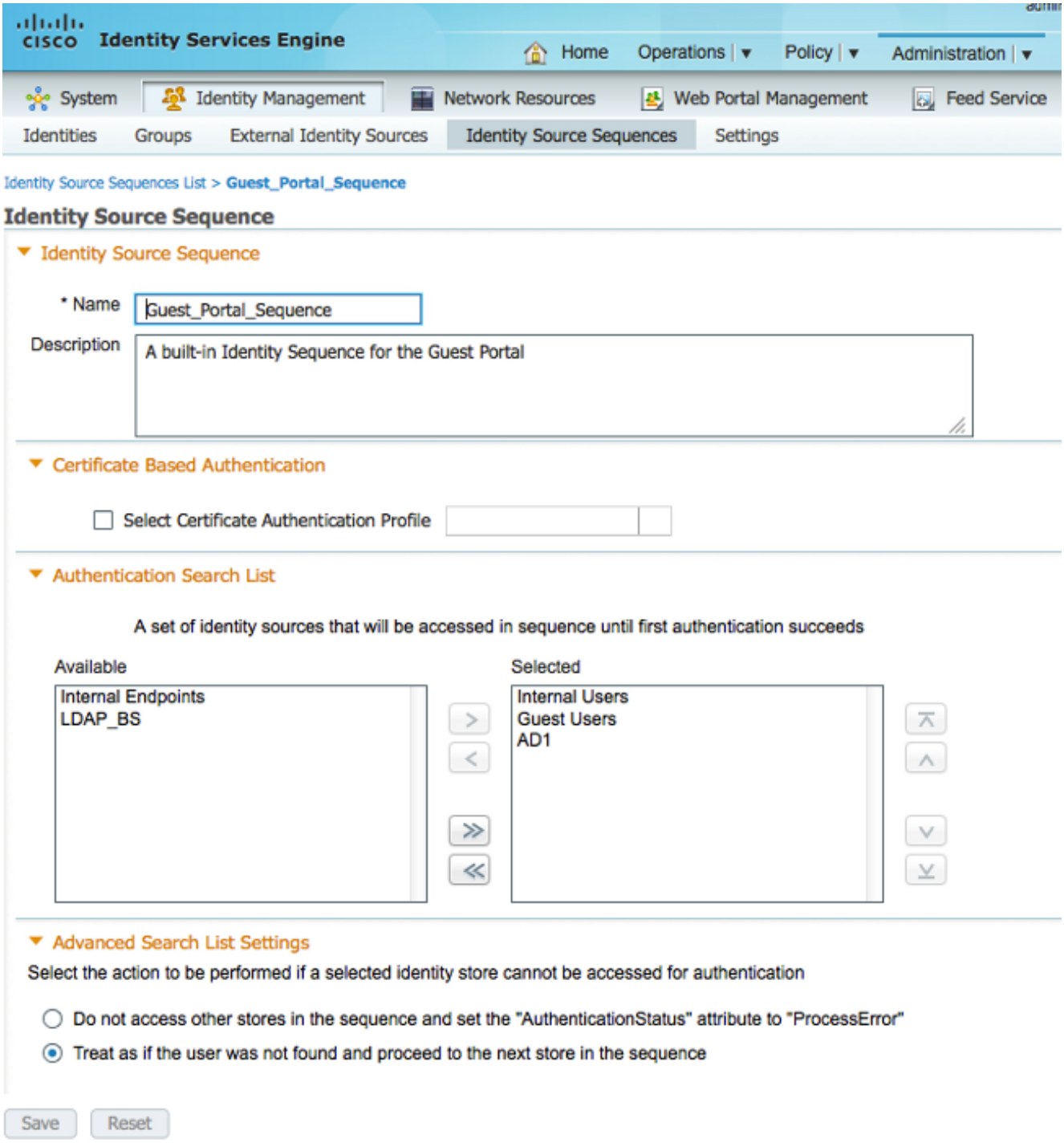
5. Creare i criteri di autorizzazione. Il criterio di autorizzazione 'Guest_Wireless' invia l'URL di reindirizzamento e l'ACL di reindirizzamento alla sessione client. Il profilo spostato qui è il CWA, come mostrato in precedenza.Il criterio di autorizzazione 'Guest_Wireless-Success' fornisce accesso completo a un utente guest autenticato tramite il portale guest. Dopo che l'utente è stato autenticato correttamente sul portale guest, l'autorizzazione dinamica viene inviata dal WLC. In questo modo la sessione client viene riautenticata con l'attributo 'Network Access:Usecase EQUALS Guest Flow'.I criteri di autorizzazione finali sono i seguenti:



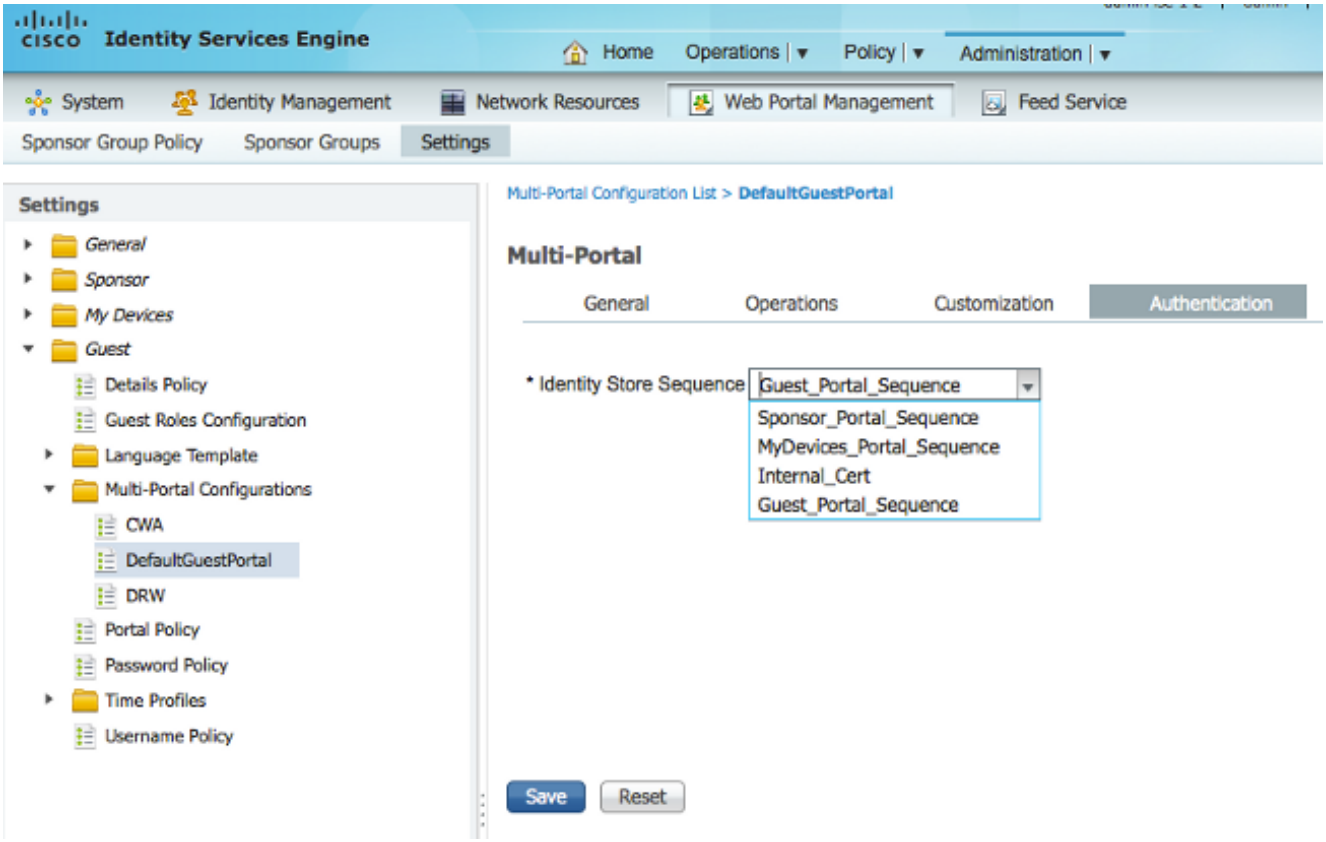
6. Facoltativo: in questo caso vengono utilizzate le configurazioni multiportale predefinite. In base ai requisiti, lo stesso può essere modificato nella GUI. Dalla GUI di ISE, scegliere **Amministrazione > Gestione portale Web > Configurazioni multi-portale > DefaultGuestPortal**.



Viene creata la sequenza Guest_Portal_sequence che consente agli utenti Internal, Guest e AD.



7. Dalla GUI di ISE, scegliere **Guest > Multi-Portal Configurations > DefaultGuestPortal**. Dall'elenco a discesa Identifica sequenza punto vendita, scegliere **Guest_Portal_Sequence**.



Configurazione sul WLC

1. Definire il server ISE Radius sul WLC 5760.
2. Configurare il server RADIUS, il gruppo di server e l'elenco dei metodi con la CLI.

```
dot1x system-auth-control

radius server ISE
address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
server name ISE
deadtime 10

aaa authentication dot1x ISE group ISE
aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
!

aaa server radius dynamic-author
client 10.106.73.69 server-key Cisco123
auth-type any
```

3. Configurare la WLAN con la CLI.

```
wlan CWA_NGWC 10 CWA_NGWC
 aaa-override
accounting-list ISE
client vlan VLAN0012
no exclusionlist
mac-filtering MACFILTER
nac
```

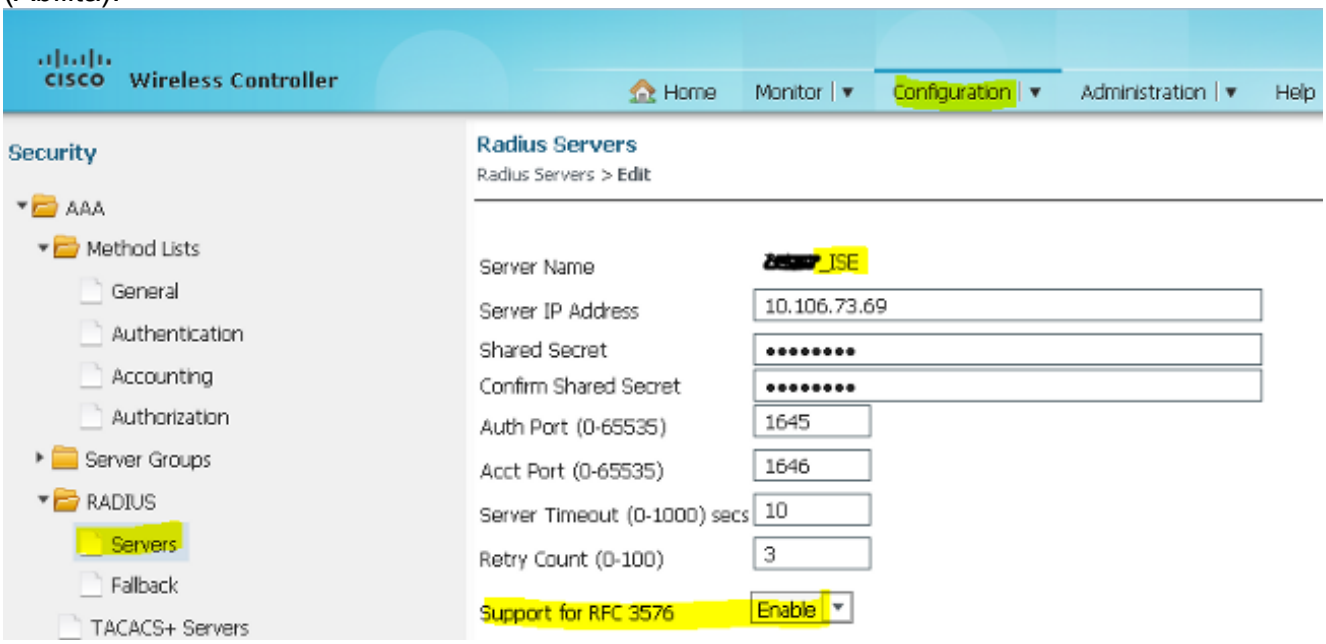
```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

4. Configurare gli ACL di reindirizzamento con la CLI. Questo è l'ACL di reindirizzamento URL restituito da ISE come override AAA insieme all'URL di reindirizzamento per il reindirizzamento del portale guest. Si tratta di un ACL diretto che viene attualmente utilizzato sull'architettura unificata. Questo è un ACL 'punt', una sorta di ACL inverso che normalmente usereste per l'architettura unificata. È necessario bloccare l'accesso a DHCP, al server DHCP, a DNS, al server DNS e al server ISE. Consentire solo www, 443 e 8443 in base alle esigenze. Questo portale guest ISE utilizza la porta 8443 e il reindirizzamento funziona ancora con l'ACL mostrato di seguito. In questo caso, l'ICMP è abilitato, ma in base alle regole di sicurezza è possibile negarlo o autorizzarlo.

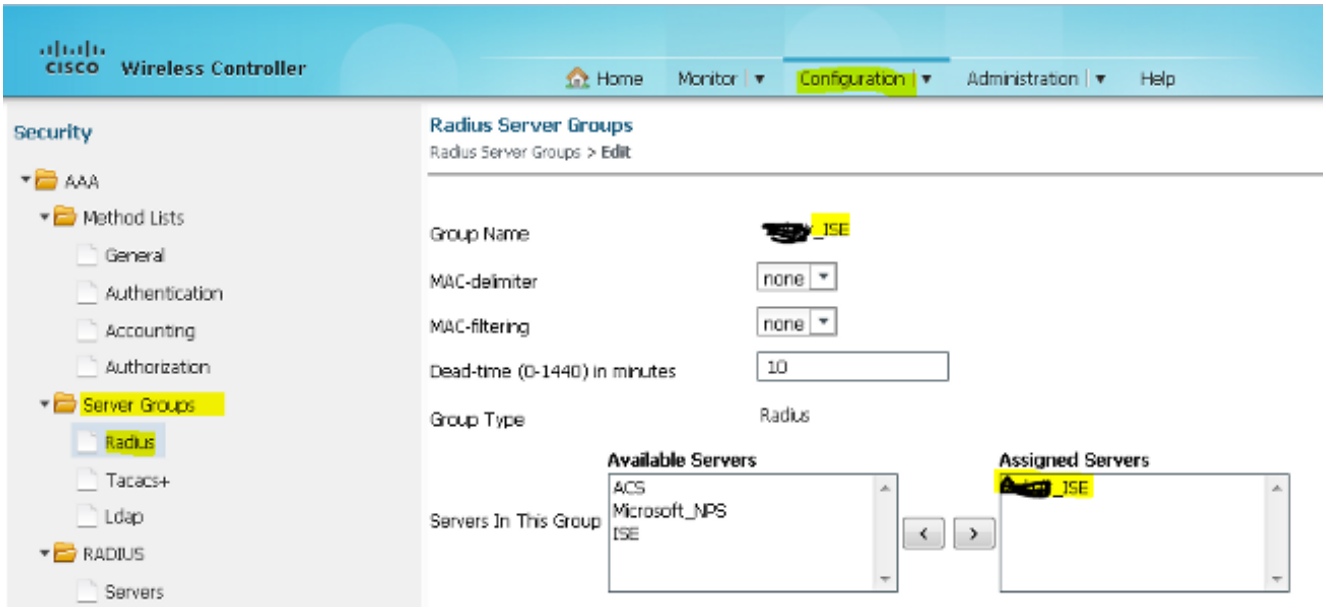
```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

Attenzione: l'abilitazione del protocollo HTTPS potrebbe causare problemi elevati alla CPU dovuti alla scalabilità. Non abilitare questa funzionalità a meno che non sia consigliata dal team di progettazione Cisco.

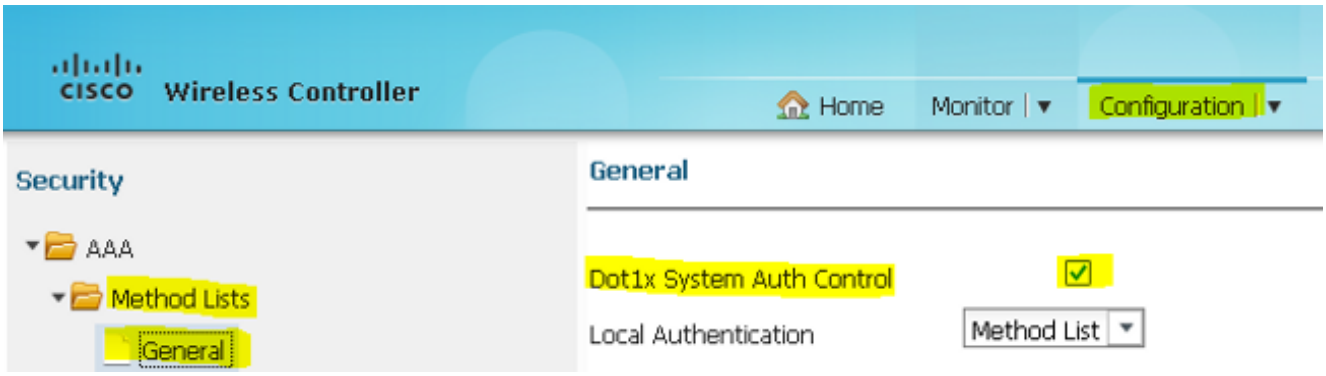
5. Dalla GUI del controller wireless, scegliere **AAA > RADIUS > Server**. Configurare il server RADIUS, il gruppo di server e l'elenco di metodi nella GUI. Specificare tutti i parametri e verificare che il segreto condiviso configurato qui corrisponda a quello configurato sull'ISE per questo dispositivo. Dall'elenco a discesa Support for RFC 3576 (Supporto per RFC 3576), scegliere **Enable**
(Abilita).



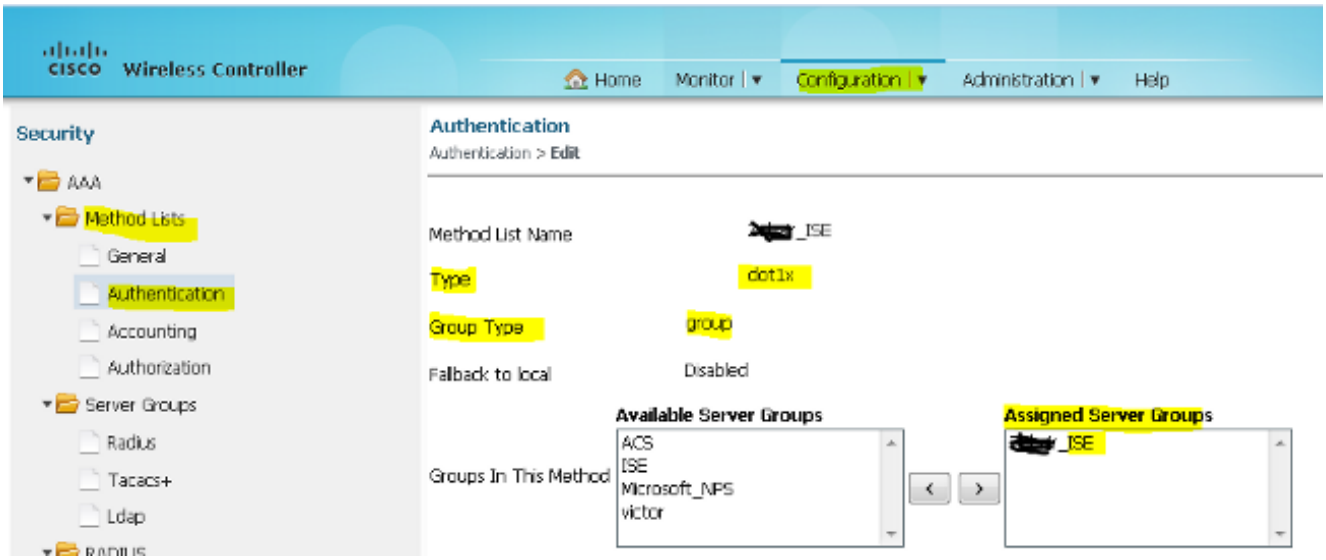
6. Dalla GUI del controller wireless, scegliere **AAA > Gruppi di server > Radius**. Aggiungere il server RADIUS creato in precedenza ai gruppi di server.



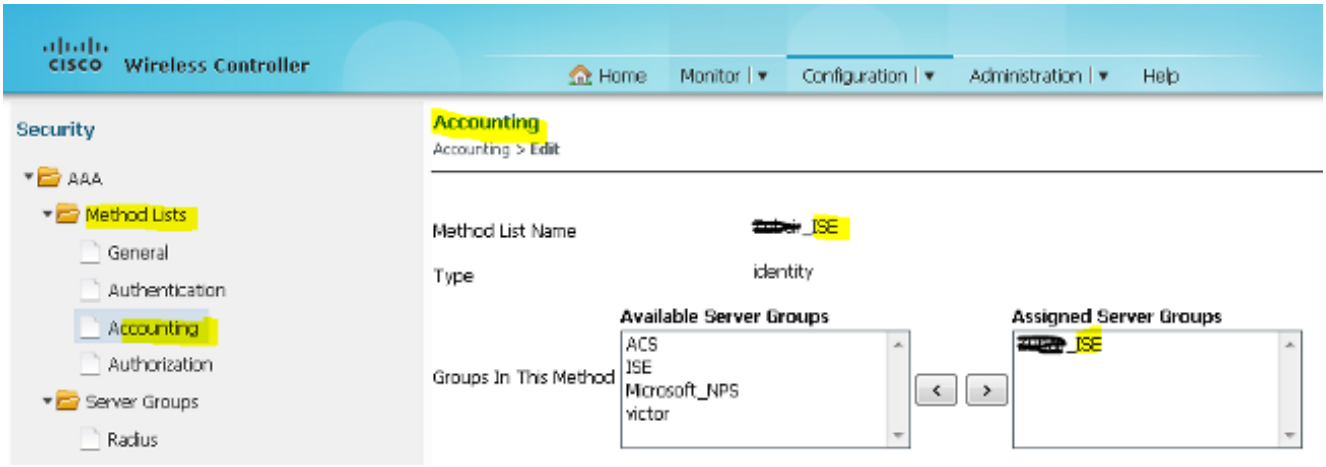
7. Dalla GUI del controller wireless, scegliere **AAA > Elenchi di metodi > Generale**. Selezionare la casella di controllo **Dot1x System Auth Control**. Se si disabilita questa opzione, il processo AAA non funzionerà.



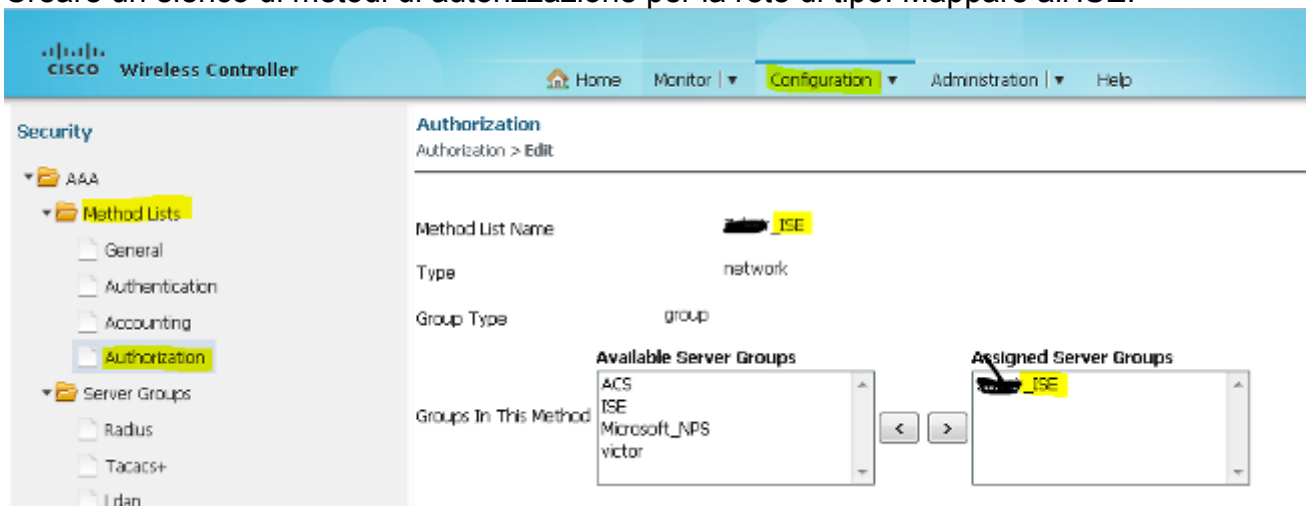
8. Dalla GUI del controller wireless, scegliere **AAA > Elenchi metodi > Autenticazione**. Creare un elenco di metodi di autenticazione per il tipo dot1X. Il tipo di gruppo è group. Mappare all'ISE.



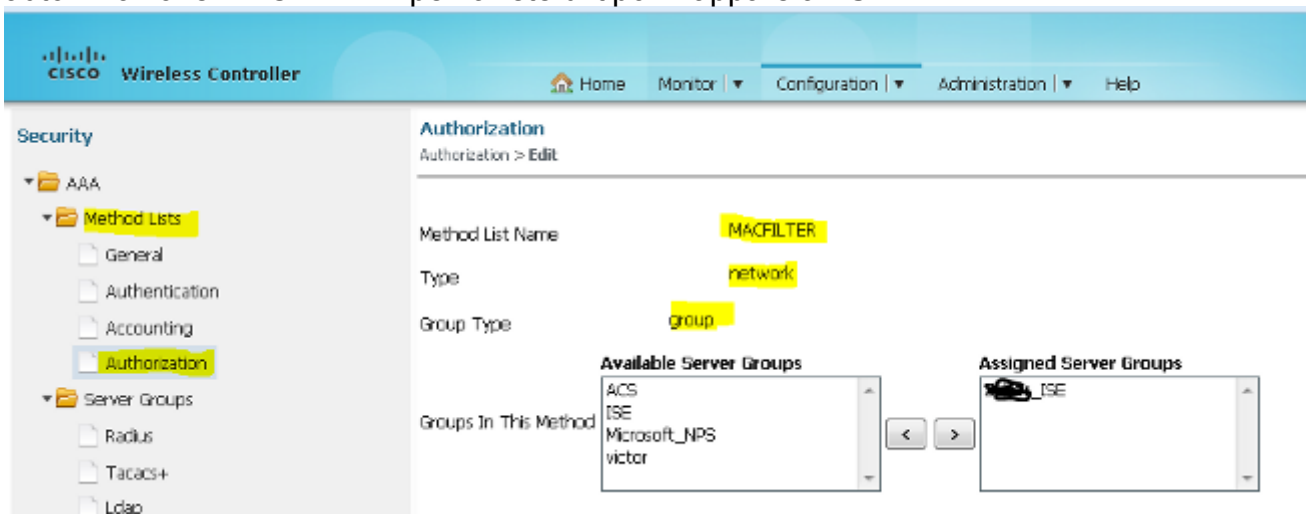
9. Dalla GUI del controller wireless, scegliere **AAA > Elenchi metodi > Accounting**. Creare un elenco di metodi di accounting per l'identità di tipo. Mappare all'ISE.



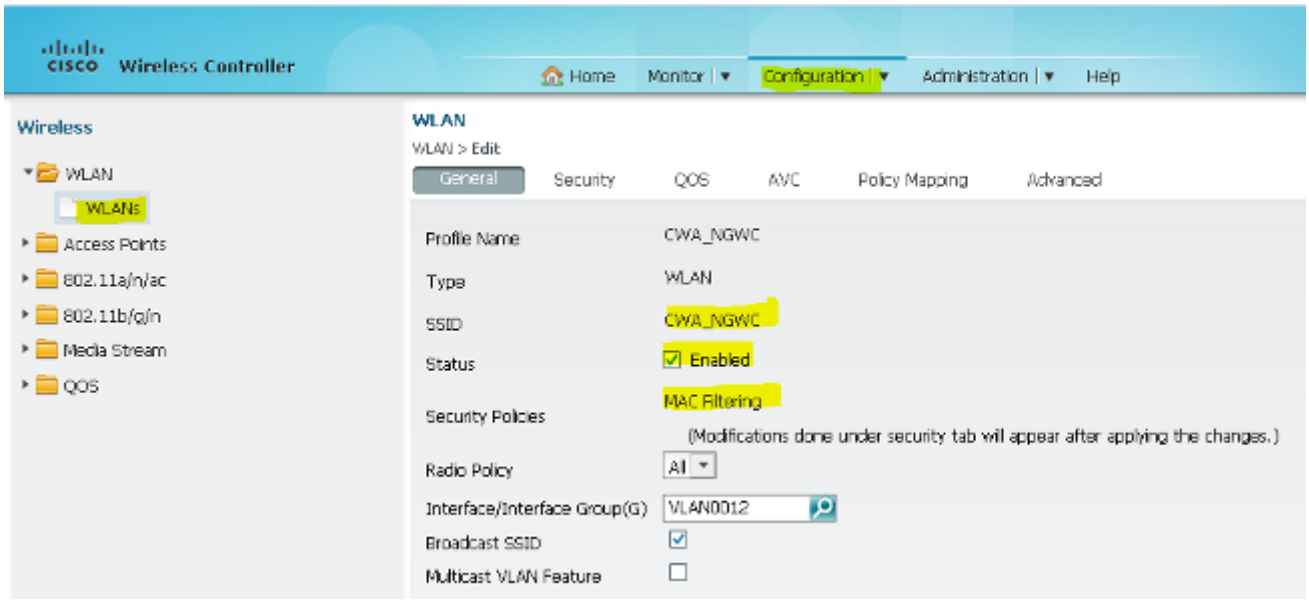
10. Dalla GUI del controller wireless, scegliere **AAA > Elenchi di metodi > Autorizzazione**. Creare un elenco di metodi di autorizzazione per la rete di tipo. Mappare all'ISE.



11. Opzionale, poiché esiste anche il supporto di errori MAC on. Creare un elenco di metodi di autorizzazione MACFILTER per la rete di tipo. Mappare all'ISE.

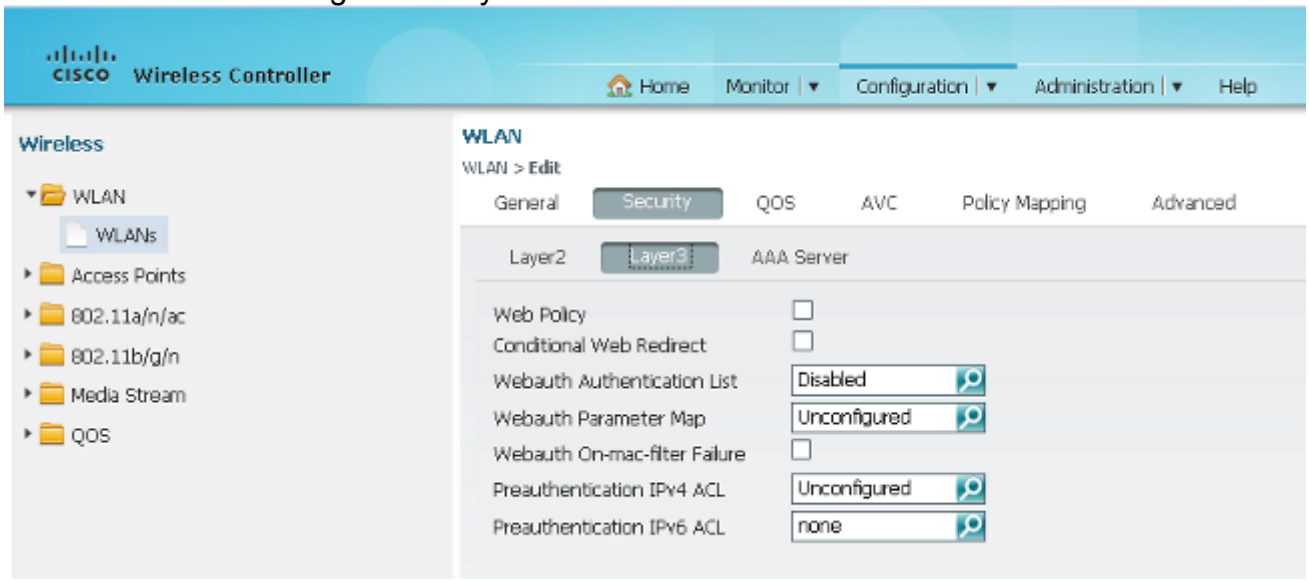


12. Dall'interfaccia utente del controller wireless, scegliere **WLAN > WLAN**. Create una nuova configurazione con i parametri mostrati di seguito.

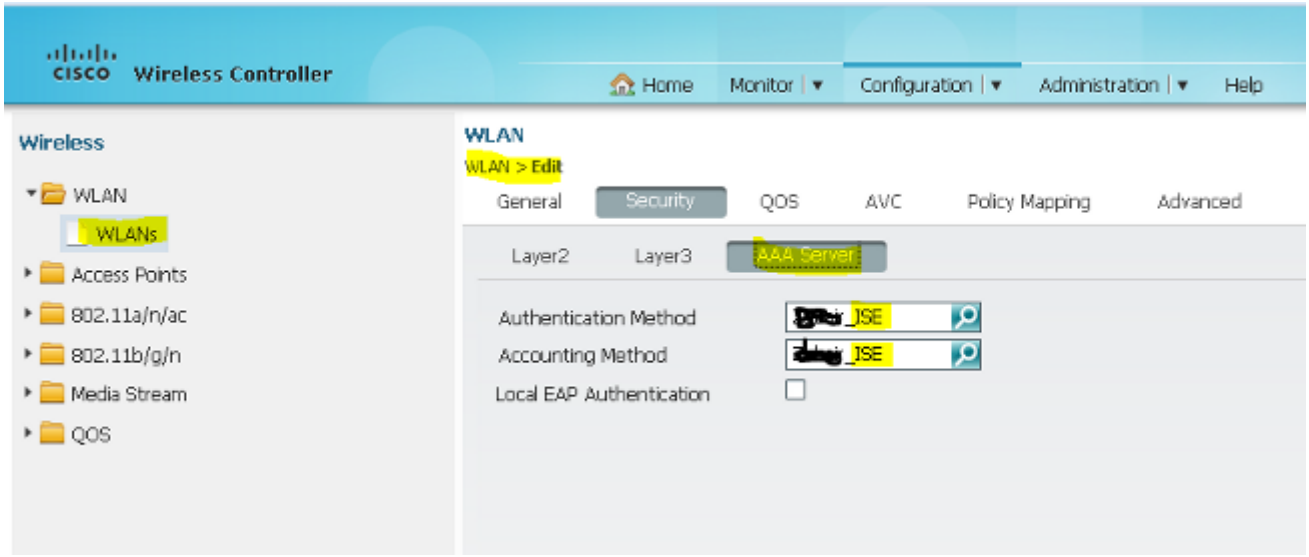


13. Scegliete **Sicurezza > Livello 2**. Nel campo Filtro MAC, immettere **MACFILTER**.

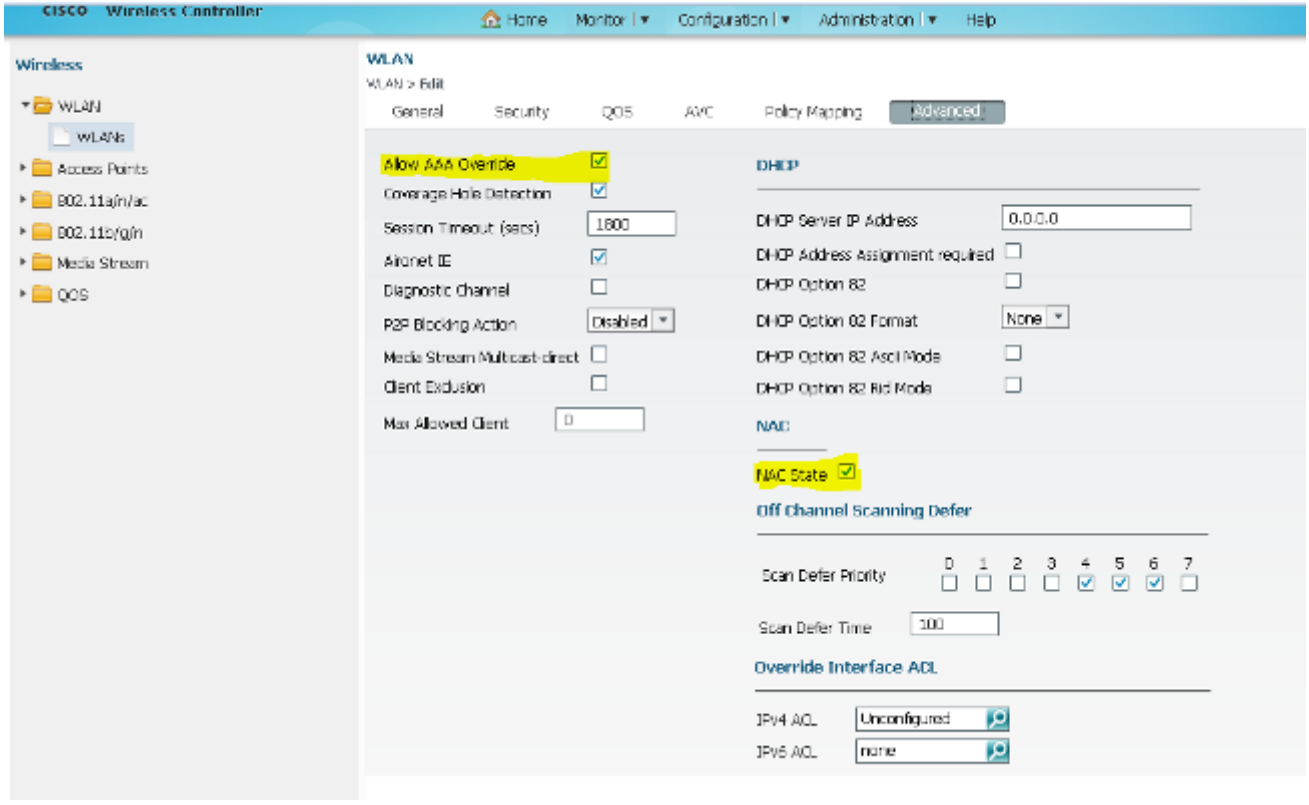
14. Non è necessario configurare il layer 3.



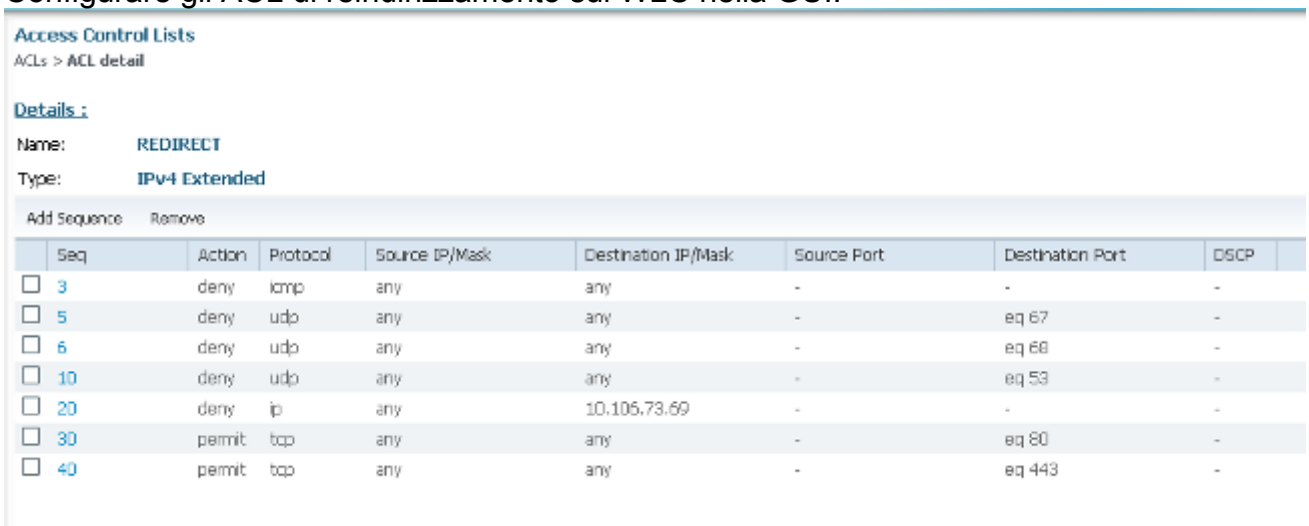
15. Scegliere **Sicurezza > Server AAA**. Dall'elenco a discesa Authentication Method (Metodo di autenticazione), selezionare **ISE**. Dall'elenco a discesa Metodo di accounting, scegliere **ISE**.



16. Scegliere **Avanzate**. Selezionare la casella di controllo **Consenti sostituzione AAA**. Selezionare la casella di controllo **Stato NAC**.



17. Configurare gli ACL di reindirizzamento sul WLC nella GUI.



Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP
3	deny	icmp	any	any	-	-	-
5	deny	udp	any	any	-	eq 67	-
6	deny	udp	any	any	-	eq 68	-
10	deny	udp	any	any	-	eq 53	-
20	deny	ip	any	10.105.73.69	-	-	-
30	permit	tcp	any	any	-	eq 80	-
40	permit	tcp	any	any	-	eq 443	-

Esempio di configurazione della topologia 2

Vedere Topologia 2 per il diagramma di rete e la spiegazione.

Anche questa configurazione prevede un processo in due fasi.

Configurazione sull'ISE

La configurazione sull'ISE è la stessa della configurazione della topologia 1.

Non è necessario aggiungere il Anchor Controller sull'ISE. È sufficiente aggiungere il WLC esterno sull'ISE, definire il server RADIUS sul WLC esterno e mappare i criteri di autorizzazione nella WLAN. Sul punto di ancoraggio è sufficiente abilitare il filtro MAC.

In questo esempio di configurazione, sono presenti due WLC 5760 che agiscono come dispositivi di ancoraggio esterni. Se si desidera utilizzare il WLC 5760 come dispositivo di ancoraggio e lo switch 3850 come dispositivo di ancoraggio esterno, ovvero l'agente di mobilità, su un altro controller di mobilità, la stessa configurazione è corretta. Tuttavia, non è necessario configurare la WLAN sul secondo controller di mobilità dal quale lo switch 3850 ottiene le licenze. È sufficiente puntare lo switch 3850 al WLC 5760 che funge da ancoraggio.

Configurazione sul WLC

1. Sul server esterno, configurare il server ISE con l'elenco dei metodi AAA per AAA e mappare la WLAN su un'autorizzazione per filtro MAC. **Nota**: configurare il reindirizzamento dell'ACL sia su Anchor che su Foreign e sul filtro MAC.

```
dot1x system-auth-control

radius server ISE
 address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
 server name ISE
 deadtime 10


aaa authentication dot1x ISE group ISE

aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
!

aaa server radius dynamic-author
 client 10.106.73.69 server-key Cisco123
 auth-type any

wlan MA-MC 11 MA-MC
 aaa-override
 accounting-list  ISE
 client vlan VLAN0012
```

```
 mac-filtering MACFILTER
 mobility anchor 10.105.135.244
nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

2. Configurare gli ACL di reindirizzamento con la CLI. Questo è l'ACL di reindirizzamento URL restituito da ISE come override AAA insieme all'URL di reindirizzamento per il reindirizzamento del portale guest. Si tratta di un ACL diretto che viene attualmente utilizzato sull'architettura unificata. Questo è un ACL 'punt', una sorta di ACL inverso che normalmente usereste per l'architettura unificata. È necessario bloccare l'accesso a DHCP, al server DHCP, a DNS, al server DNS e al server ISE. Consentire solo www, 443 e 8443 in base alle esigenze. Questo portale guest ISE utilizza la porta 8443 e il reindirizzamento funziona ancora con l'ACL mostrato di seguito. In questo caso, l'ICMP è abilitato, ma in base alle regole di sicurezza è possibile negarlo o autorizzarlo.

```
ip access-list extended REDIRECT
 deny icmp any any
deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

   Attenzione: l'abilitazione del protocollo HTTPS potrebbe causare problemi elevati alla CPU dovuti alla scalabilità. Non abilitare questa funzionalità a meno che non sia consigliata dal team di progettazione Cisco.

3. Configurare la mobilità sull'ancoraggio.

```
wireless mobility group member ip 10.105.135.244 public-ip 10.105.135.244 group surbg
```

   Nota: se si configura lo stesso switch con lo switch 3850 come dispositivo esterno, accertarsi di definire il gruppo di peer dello switch sul controller di mobilità e viceversa. Quindi, configurare le configurazioni CWA di cui sopra sullo switch 3850.

4. Configurazione sull'ancoraggio. Sull'ancora, non è necessario configurare alcuna configurazione ISE. È sufficiente la configurazione WLAN.

```
wlan MA-MC 6 MA-MC
 aaa-override
 client vlan VLAN0012
 mac-filtering MACFILTER
 mobility anchor
nac
 nbsp;no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
```

5. Configurare la mobilità sull'ancoraggio. Definire l'altro WLC come membro della mobilità su questo WLC.

```
wireless mobility group member ip 10.105.135.178 public-ip 10.105.135.178 group surbg
```

6. Configurare gli ACL di reindirizzamento con la CLI. Questo è l'ACL di reindirizzamento URL restituito da ISE come override AAA insieme all'URL di reindirizzamento per il reindirizzamento del portale guest. Si tratta di un ACL diretto che viene attualmente utilizzato sull'architettura unificata. Questo è un ACL 'punt', una sorta di ACL inverso che normalmente

usereste per l'architettura unificata. È necessario bloccare l'accesso a DHCP, al server DHCP, a DNS, al server DNS e al server ISE. Consentire solo www, 443 e 8443 in base alle esigenze. Questo portale guest ISE utilizza la porta 8443 e il reindirizzamento funziona ancora con l'ACL mostrato di seguito. In questo caso, l'ICMP è abilitato, ma in base alle regole di sicurezza è possibile negarlo o autorizzarlo.

```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
 deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

Attenzione: l'abilitazione del protocollo HTTPS potrebbe causare problemi elevati alla CPU dovuti alla scalabilità. Non abilitare questa funzionalità a meno che non sia consigliata dal team di progettazione Cisco.

Esempio di configurazione della topologia 3

Vedere Topologia 3 per il diagramma di rete e la spiegazione.

Si tratta inoltre di un processo in due fasi.

Configurazione sull'ISE

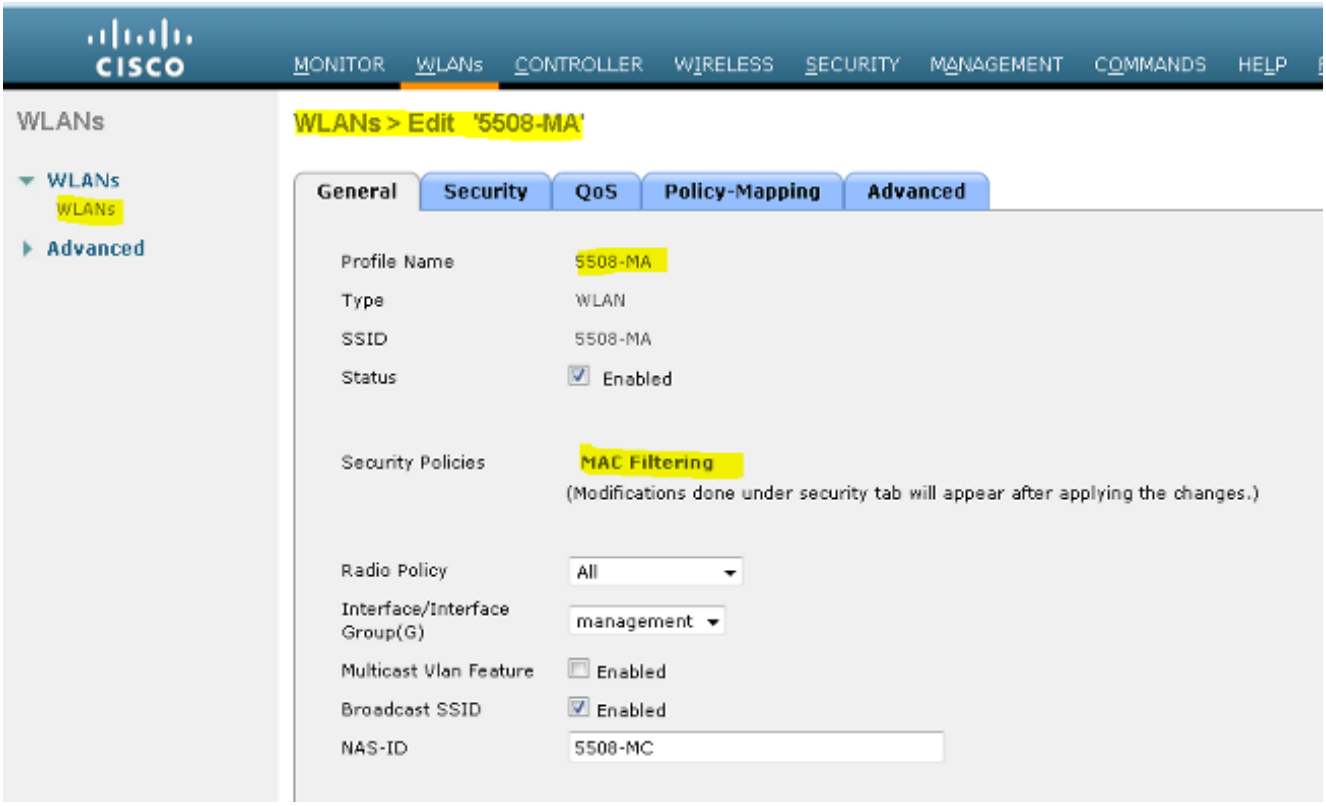
La configurazione sull'ISE è la stessa della configurazione della topologia 1.

Non è necessario aggiungere il Anchor Controller sull'ISE. È sufficiente aggiungere il WLC esterno sull'ISE, definire il server RADIUS sul WLC esterno e mappare i criteri di autorizzazione nella WLAN. Sul punto di ancoraggio è sufficiente abilitare il filtro MAC.

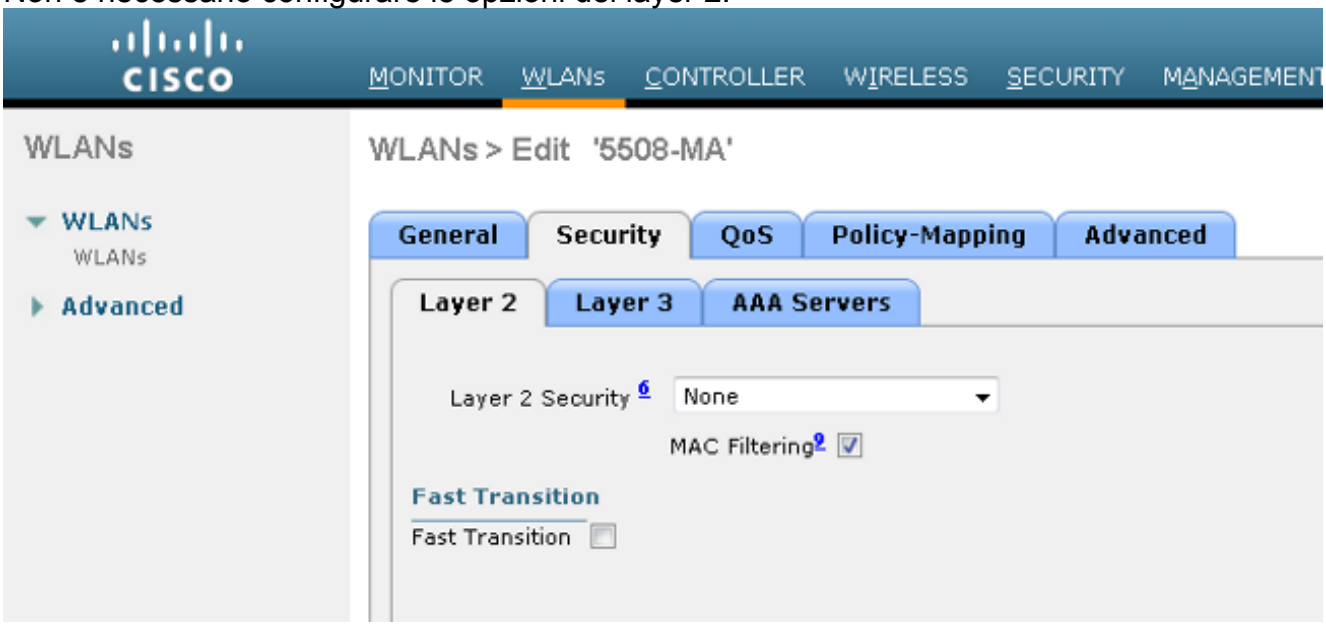
Nell'esempio, c'è un WLC 5508 che agisce come ancora e un WLC 5760 che agisce come WLC straniero. Se si desidera utilizzare un WLC 5508 come ancora e uno switch 3850 e un WLC esterno, che è un agente di mobilità, su un altro controller di mobilità, la stessa configurazione è corretta. Tuttavia, non è necessario configurare la WLAN sul secondo controller di mobilità dal quale lo switch 3850 ottiene le licenze. È sufficiente puntare lo switch 3850 al WLC 5508 che funge da ancoraggio.

Configurazione sul WLC

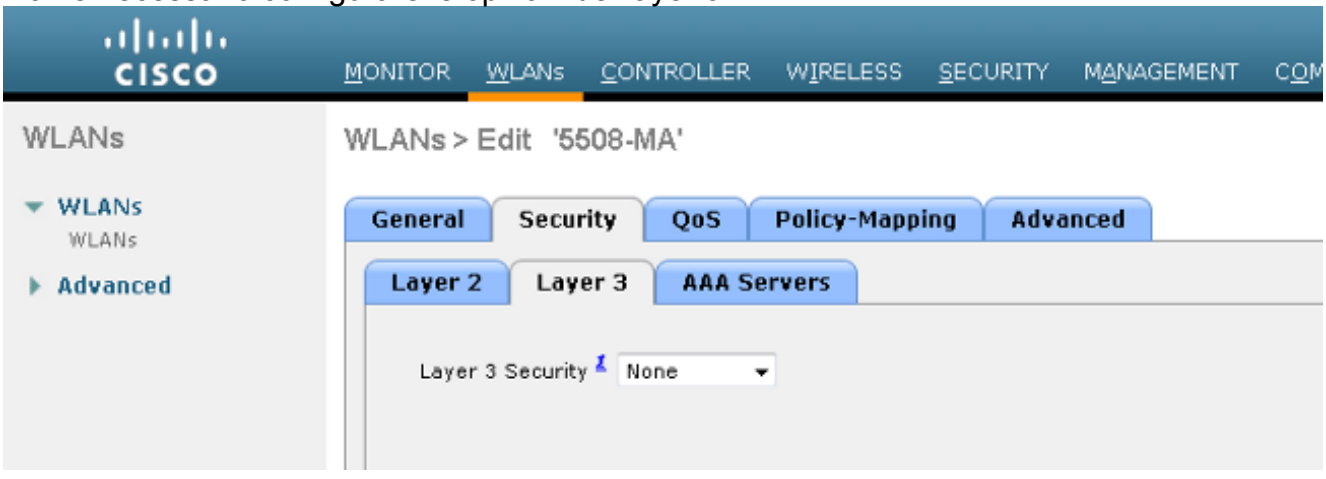
1. Sul WLC esterno, configurare il server ISE con l'elenco dei metodi AAA per AAA e mappare la WLAN su un'autorizzazione per filtro MAC. Questa operazione non è necessaria sull'ancora. **Nota**: configurare il reindirizzamento dell'ACL sul WLC di ancoraggio e esterno e sul filtro MAC.
2. Dalla GUI del WLC 5508, selezionare **WLAN > New** (WLAN > Nuovo) per configurare l'ancoraggio 5508. Completare i dettagli per abilitare il filtro MAC.



3. Non è necessario configurare le opzioni del layer 2.

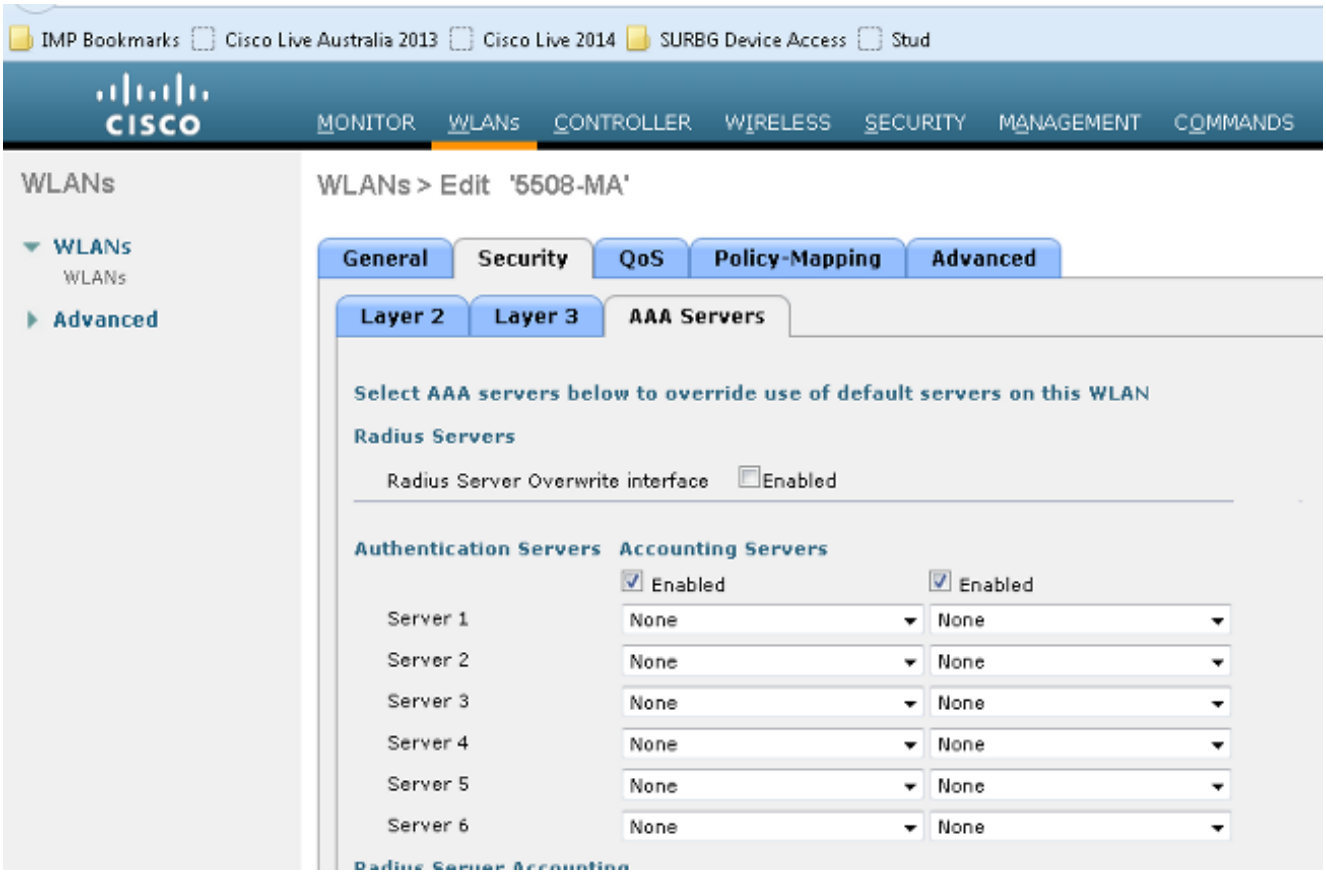


4. Non è necessario configurare le opzioni del layer 3.

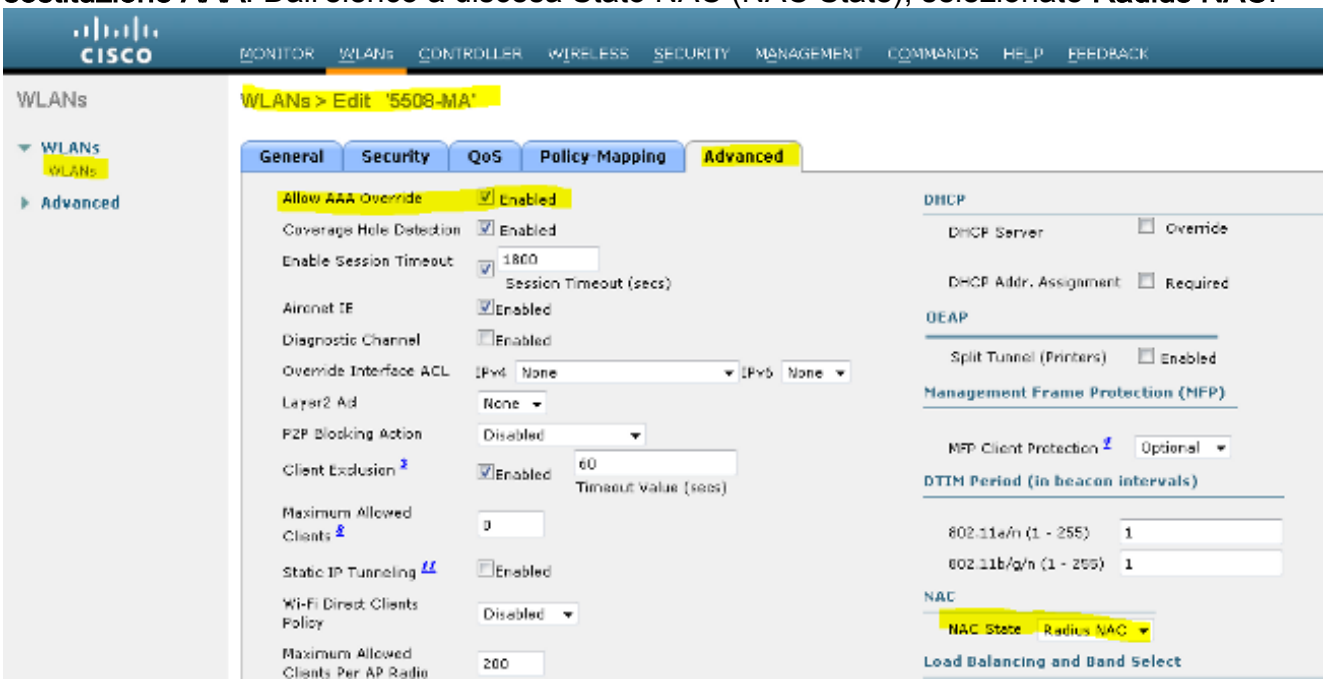


5. I server AAA devono essere disabilitati nel WLC di Anchor AireOS in modo che il CoA possa

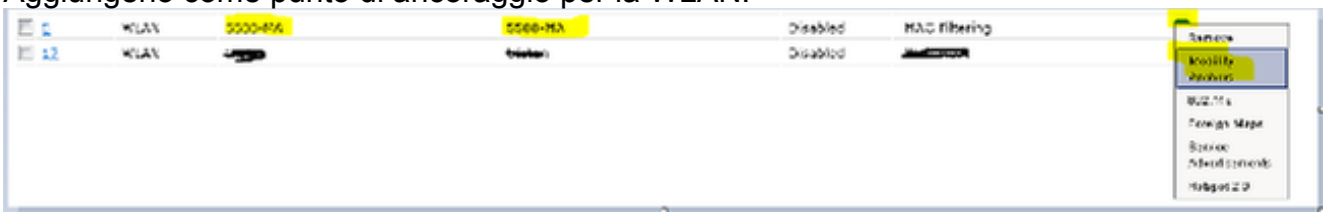
essere elaborato dalla NGWC straniera. I server AAA possono essere abilitati nel WLC di ancoraggio solo se non sono presenti server RADIUS configurati in: Sicurezza > AAA > RADIUS > Autenticazione



6. Scegliere **WLAN > WLAN > Modifica > Avanzate**. Selezionare la casella di controllo **Consenti sostituzione AAA**. Dall'elenco a discesa Stato NAC (NAC State), selezionate **Radius NAC**.

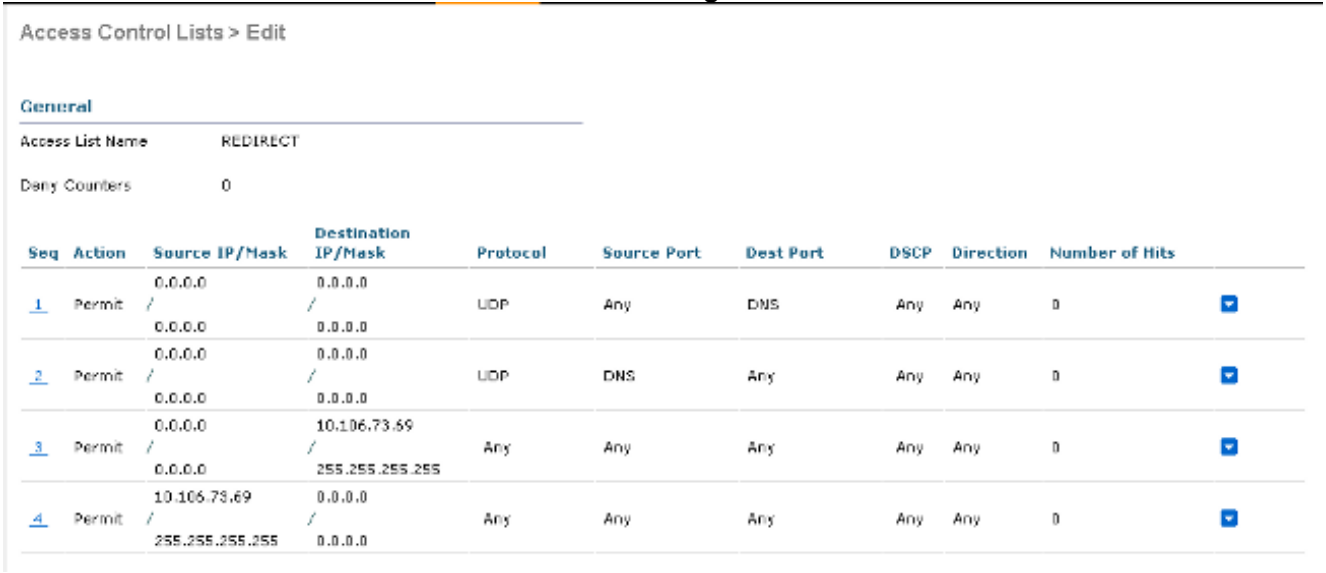


7. Aggiungerlo come punto di ancoraggio per la WLAN.

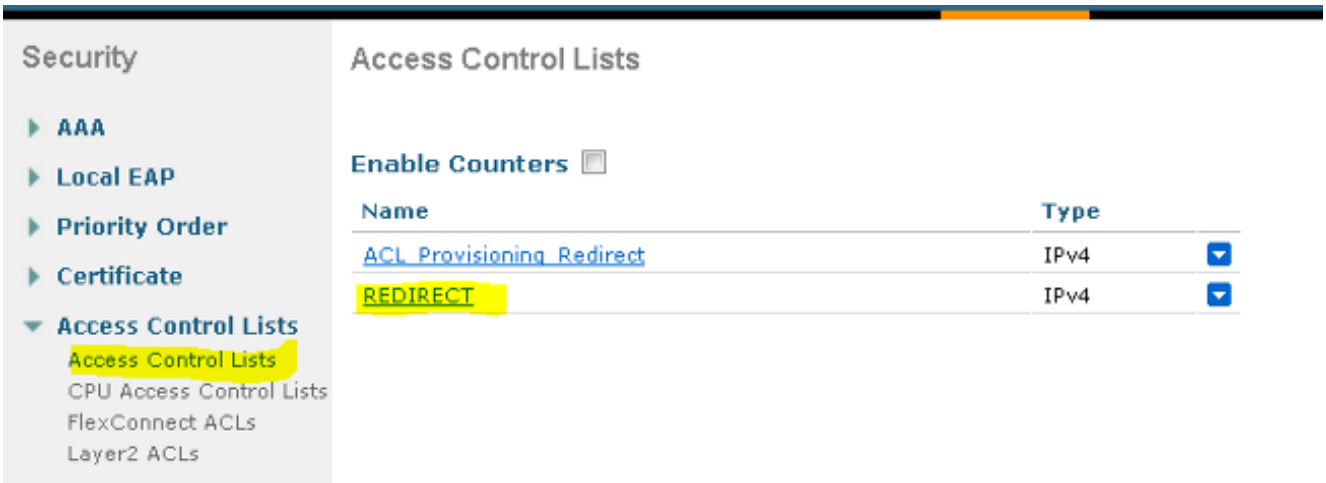


8. Dopo essere stato indirizzato a un server locale, è necessario eseguire questa operazione con Control e Data Path UP/UP.

9. Creare l'ACL di reindirizzamento sul WLC. Ciò nega DHCP e DNS. Consente HTTP/HTTP.



Di seguito viene riportato l'aspetto dell'ACL dopo la creazione.



10. Definire il server ISE RADIUS sul WLC 5760.
11. Configurare il server RADIUS, il gruppo di server e la lista metodi con la CLI.

```
dot1x system-auth-control

radius server ISE
 address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
 server name ISE
 deadtime 10

aaa authentication dot1x ISE group ISE
```

```
aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE

aaa accounting identity ISE start-stop group ISE

!

aaa server radius dynamic-author
 client 10.106.73.69 server-key Cisco123
 auth-type any
```

12. Configurare la WLAN dalla CLI.

```
wlan 5508-MA 15 5508-MA
 aaa-override
 accounting-list ISE
 client vlan VLAN0012
 mac-filtering MACFILTER
 mobility anchor 10.105.135.151
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 shutdown
```

13. Definire l'altro WLC come membro della mobilità su questo WLC.

```
wireless mobility group member ip 10.105.135.151public-ip 10.105.135.151 group Mobile-1
```

Nota: se si configura lo stesso switch con il WLC 3850 come dispositivo esterno, accertarsi di definire il gruppo di switch peer sul controller della mobilità e viceversa sul controller della mobilità. Configurare quindi le precedenti configurazioni CWA sul WLC 3850.

14. Configurare gli ACL di reindirizzamento con la CLI. Questo è l'ACL di reindirizzamento URL restituito da ISE come override AAA insieme all'URL di reindirizzamento per il reindirizzamento del portale guest. Si tratta di un ACL diretto che viene attualmente utilizzato sull'architettura unificata. Questo è un ACL 'punt', una sorta di ACL inverso che normalmente usereste per l'architettura unificata. È necessario bloccare l'accesso a DHCP, al server DHCP, a DNS, al server DNS e al server ISE. Consentire solo www, 443 e 8443 in base alle esigenze. Questo portale guest ISE utilizza la porta 8443 e il reindirizzamento funziona ancora con l'ACL mostrato di seguito. In questo caso, l'ICMP è abilitato, ma in base alle regole di sicurezza è possibile negarlo o autorizzarlo.

```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
 deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

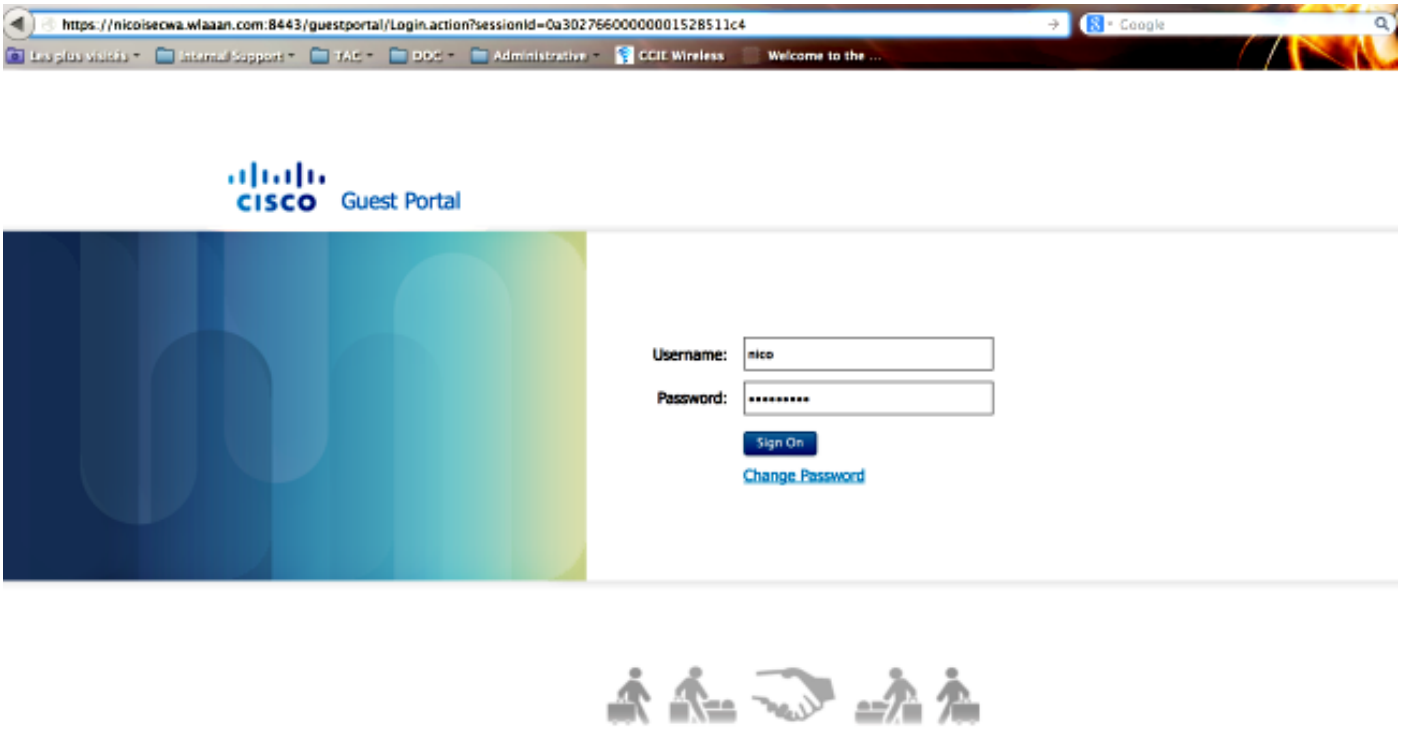
Attenzione: l'abilitazione del protocollo HTTPS potrebbe causare problemi elevati alla CPU dovuti alla scalabilità. Non abilitare questa funzionalità a meno che non sia consigliata dal team di progettazione Cisco.

Verifica

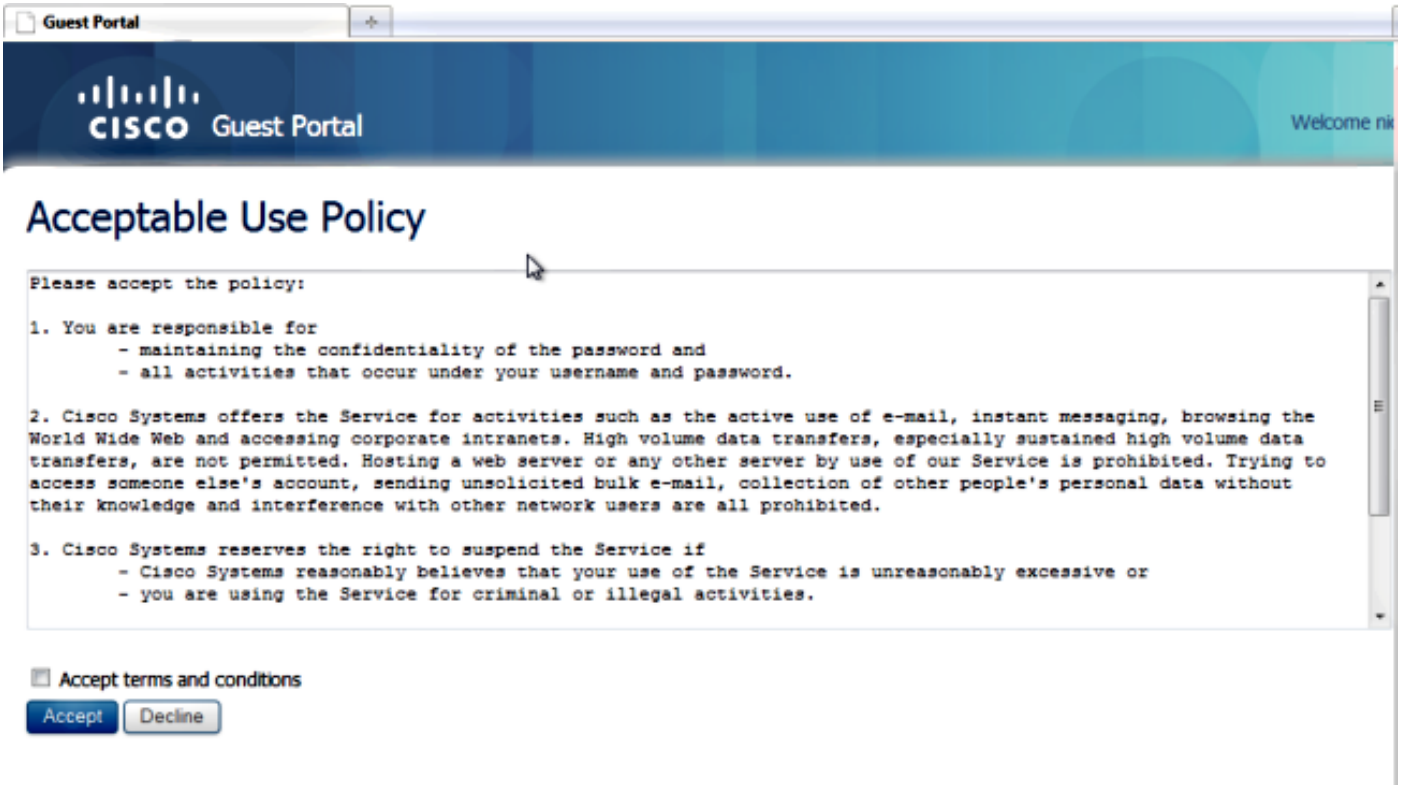
Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

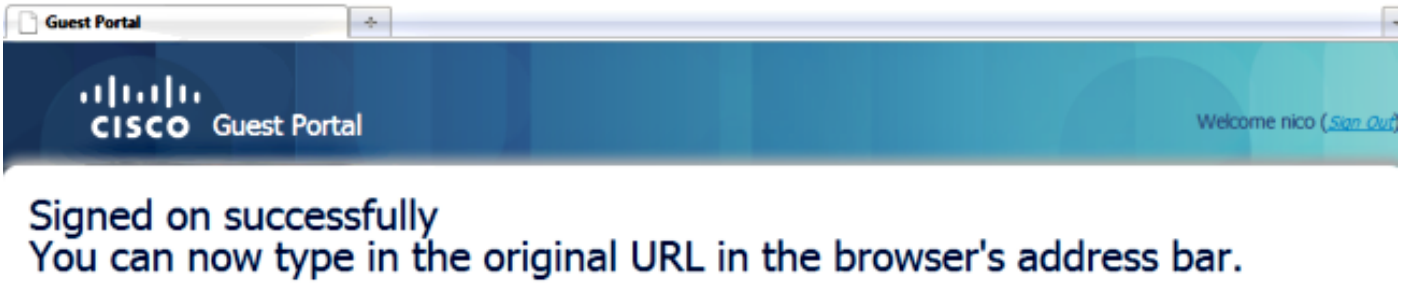
Connettere il client all'SSID configurato. Dopo aver ricevuto l'indirizzo IP e quando il client passa allo stato Web auth Required, aprire il browser. Immettere le credenziali client nel portale.



Dopo aver completato l'autenticazione, selezionare la casella di controllo **Accetta termini e condizioni**. Fare clic su **Accetta**.

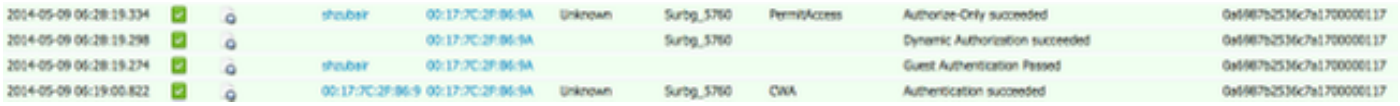


Verrà visualizzato un messaggio di conferma e sarà possibile accedere a Internet.



You can now type in the original URL in the browser's address bar.

Sull'ISE, il flusso del client ha questo aspetto:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

> **Nota**: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

Sul WLC di Converged Access, è consigliabile eseguire le tracce anziché i debug. Sul WLC di Aironet OS 5508, è sufficiente immettere **debug client <mac client>** e **debug web-auth redirect enable mac <mac client>**.

```
set trace group-wireless-client level debug
set trace group-wireless-secure level debug

set trace group-wireless-client filter mac 0017.7c2f.b69a
set trace group-wireless-secure filter mac 0017.7c2f.b69a
```

Alcuni difetti noti di Cisco IOS-XE e del sistema operativo Aironet sono inclusi nell'ID bug Cisco CSCun38344.

Di seguito viene riportato l'aspetto del flusso CWA riuscito sulle tracce:

```
[05/09/14 13:13:15.951 IST 63d7 8151] 0017.7c2f.b69a Association received from mobile
on AP c8f9.f983.4260
[05/09/14 13:13:15.951 IST 63d8 8151] 0017.7c2f.b69a qos upstream policy is unknown
and downstream policy is unknown
```

[05/09/14 13:13:15.951 IST 63e0 8151] 0017.7c2f.b69a Applying site-specific IPv6 override for station 0017.7c2f.b69a - vapId 15, site 'default-group', interface 'VLAN0012'
[05/09/14 13:13:15.951 IST 63e1 8151] 0017.7c2f.b69a Applying local bridging Interface Policy for station 0017.7c2f.b69a - vlan 12, interface 'VLAN0012'
[05/09/14 13:13:15.951 IST 63e2 8151] 0017.7c2f.b69a
**** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:15.951 IST 63e3 8151] 0017.7c2f.b69a *** **Client State = START** instance = 1 instance Name POLICY_PROFILING_80211_ASSOC, OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null

[05/09/14 13:13:15.951 IST 63eb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER
[05/09/14 13:13:15.951 IST 63ec 8151] 0017.7c2f.b69a AAAS: auth request sent
05/09/14 13:13:15.951 IST 63ed 8151] 0017.7c2f.b69a apfProcessAssocReq (apf_80211.c:6149) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from Idle to AAA Pending

[05/09/14 13:13:15.951 IST 63ee 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1
[05/09/14 13:13:15.951 IST 63ef 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station: (callerId: 20) in 10 seconds
[05/09/14 13:13:15.951 IST 63f0 211] **Parsed CLID MAC Address = 0:23:124:47:182:154**
[05/09/14 13:13:15.951 IST 63f1 211] AAA SRV(00000118): process author req
[05/09/14 13:13:15.951 IST 63f2 211] **AAA SRV(00000118): Author method=SERVER_GROUP Zubair_ISE**
[05/09/14 13:13:16.015 IST 63f3 220] AAA SRV(00000118): protocol reply PASS for Authorization
[05/09/14 13:13:16.015 IST 63f4 220] AAA SRV(00000118): Return Authorization status=PASS
[05/09/14 13:13:16.015 IST 63f5 8151] 0017.7c2f.b69a AAAS: received response, cid=266
[05/09/14 13:13:16.015 IST 63f6 8151] 0017.7c2f.b69a AAAS: deleting context, cid=266
[05/09/14 13:13:16.015 IST 63f7 8151] 0017.7c2f.b69a Not comparing because the ACLs have not been sent yet.
[05/09/14 13:13:16.015 IST 63f8 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1, epmSendAclDone 0
[05/09/14 13:13:16.015 IST 63f9 8151] 0017.7c2f.b69a
client incoming attribute size are 193
[05/09/14 13:13:16.015 IST 63fa 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0 uniqueId=280
[05/09/14 13:13:16.015 IST 63fb 8151] 0017.7c2f.b69a AAA Override Url-Redirect 'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa' set
[05/09/14 13:13:16.015 IST 63fc 8151] **0017.7c2f.b69a Redirect URL received for client from RADIUS. for redirection.**
[05/09/14 13:13:16.015 IST 63fd 8151] 0017.7c2f.b69a Setting AAA Override Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:16.015 IST 63fe 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:16.015 IST 63ff 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State START

[05/09/14 13:13:16.015 IST 6400 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a
[05/09/14 13:13:16.015 IST 6401 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station
[05/09/14 13:13:16.015 IST 6402 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:16.015 IST 6403 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:16.015 IST 6404 8151] 0017.7c2f.b69a Local Policy: Applying override policy
[05/09/14 13:13:16.015 IST 6405 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---
[05/09/14 13:13:16.015 IST 6406 8151] 0017.7c2f.b69a Local Policy: Before

```
Applying WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and
apfMsTimeout is 1800

[05/09/14 13:13:16.015 IST 6407 8151] 0017.7c2f.b69a Local Policy:Setting
Interface name e VLAN0012

[05/09/14 13:13:16.015 IST 6408 8151] 0017.7c2f.b69a Local Policy:Setting local
bridging VLAN  name VLAN0012 and VLAN ID  12

[05/09/14 13:13:16.015 IST 6409 8151] 0017.7c2f.b69a Applying WLAN ACL
policies to client
[05/09/14 13:13:16.015 IST 640a 8151] 0017.7c2f.b69a No Interface ACL
used for Wireless client in WCM(NGWC)
[05/09/14 13:13:16.015 IST 640b 8151] 0017.7c2f.b69a apfApplyWlanPolicy:
Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:16.015 IST 640c 8151] 0017.7c2f.b69a Local Policy: After
Applying WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and
apfMsTimeout is 1800

[05/09/14 13:13:16.015 IST 641a 8151] 0017.7c2f.b69a WCDB_ADD: Platform
ID allocated successfully ID:259
[05/09/14 13:13:16.015 IST 641b 8151] 0017.7c2f.b69a WCDB_ADD: Adding
opt82 len 0
[05/09/14 13:13:16.015 IST 641c 8151] 0017.7c2f.b69a WCDB_ADD: ssid
5508-MA bssid c8f9.f983.4260 vlan 12 auth=ASSOCIATION(0)
wlan(ap-group/global) 15/15 client 0 assoc 1 mob=Unassoc(0) radio 0
m_vlan 12 ip 0.0.0.0 src 0x506c800000000f dst 0x0 cid 0x47ad4000000145
glob rsc id 259dhcpsrv  0.0.0
[05/09/14 13:13:16.015 IST 641d 8151] 0017.7c2f.b69a Change state to
AUTHCHECK (2) last state START (0)

[05/09/14 13:13:16.015 IST 641e 8151] 0017.7c2f.b69a Change state to
L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

[05/09/14 13:13:16.015 IST 641f 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:16.015 IST 6420 8151] 0017.7c2f.b69a WCDB_LLM: NoRun Prev Mob 0,
Curr Mob 0 llmReq 1, return False
[05/09/14 13:13:16.015 IST 6421 207] [WCDB] ==Add event: type Regular Wireless client
(0017.7c2f.b69a) client id (0x47ad4000000145) client index (259) vlan (12)
auth_state (ASSOCIATION) mob_state (INIT)
[05/09/14 13:13:16.015 IST 6422 207] [WCDB] ===intf src/dst (0x506c800000000f)/(0x0)
radio_id (0) p2p_state (P2P_BLOCKING_DISABLE) switch/asic (1/0)
[05/09/14 13:13:16.015 IST 6423 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=L2_AUTH(1)
vlan 12 radio 0 client_id 0x47ad4000000145 mobility=Unassoc(0) src_int
0x506c800000000f dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip  0.0.0.0
ip_learn_type 0
[05/09/14 13:13:16.015 IST 6424 8151] 0017.7c2f.b69a WCDB_CHANGE: In L2 auth
but l2ack waiting lfag not set,so set
[05/09/14 13:13:16.015 IST 6425 8151] 0017.7c2f.b69a Not Using WMM Compliance code
qosCap 00
[05/09/14 13:13:16.016 IST 6426 8151] 0017.7c2f.b69a Change state to DHCP_REQD (7)
last state L2AUTHCOMPLETE (4)


[05/09/14 13:13:16.016 IST 6434 8151] 0017.7c2f.b69a Sending Assoc Response to
station on BSSID  c8f9.f983.4260  (status 0) ApVapId 15 Slot 0
[05/09/14 13:13:16.016 IST 6435 8151] 0017.7c2f.b69a apfProcessRadiusAssocResp
(apf_80211.c:2316) Changing state for mobile  0017.7c2f.b69a  on AP
c8f9.f983.4260  from Associated to Associated

[05/09/14 13:13:16.016 IST 6436 8151] 0017.7c2f.b69a 1XA: Session Push for
Non-dot1x wireless client
[05/09/14 13:13:16.016 IST 6437 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
to Push wireless session for client  47ad4000000145 uid 280
```

```
[05/09/14 13:13:16.016 IST 6438 8151] 0017.7c2f.b69a Session Push for
wireless client

[05/09/14 13:13:16.016 IST 6439 8151] 0017.7c2f.b69a Session Manager Call
Client 47ad4000000145, uid 280, capwap id 506c800000000f,Flag 1 Audit-Session
ID 0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:16.016 IST 643a 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2] Session start request from Client[1] for
0017.7c2f.b69a (method: No method, method list: none, aaa id:
0x00000118) - session-push,  policy
[05/09/14 13:13:16.016 IST 643b 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2]  - client iif_id: 47AD4000000145, session ID:
0a6987b2536c871300000118 for 0017.7c2f.b69a
[05/09/14 13:13:16.016 IST 643c 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of auth-domain for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 643d 243] ACCESS-CORE-SM-CLIENT-DOT11-ERR:
[0017.7c2f.b69a, Ca2] Invalid client authorization notification: NO method
[05/09/14 13:13:16.017 IST 643e 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-profile-name for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 643f 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-device-name for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6440 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of
dc-device-class-tag for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6441 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-certainty-metric for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6442 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-opaque for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6443 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-protocol-map for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6444 22] [WCDB] wcdb_ffcp_add_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (CREATE) return code (0)
[05/09/14 13:13:16.017 IST 6445 22] [WCDB] wcdb_send_add_notify_callback_event:
Notifying other features about client add
[05/09/14 13:13:16.017 IST 6446 22] [WCDB] wcdb_sisf_client_add_notify:
Notifying SISF of DEASSOC to DOWN any old entry for 0017.7c2f.b69a
[05/09/14 13:13:16.017 IST 6447 22] [WCDB] wcdb_sisf_client_add_notify:
Notifying SISF of new Association for 0017.7c2f.b69a
[05/09/14 13:13:16.017 IST 6448 8151] 0017.7c2f.b69a WCDB SPI response msg handler
client code 0 mob state 0
[05/09/14 13:13:16.017 IST 6449 8151] 0017.7c2f.b69a WcdbClientUpdate: L2 Auth ACK
from WCDB
[05/09/14 13:13:16.017 IST 644a 8151] 0017.7c2f.b69a WCDB_L2ACK: wcdbAckRecvdFlag
updated
[05/09/14 13:13:16.017 IST 644b 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:16.017 IST 644c 8151] 0017.7c2f.b69a WCDB_CHANGE: Suppressing SPI
(Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 12 client_id
0x47ad4000000145 mob=Unassoc(0) ackflag 2 dropd 1
[05/09/14 13:13:18.796 IST 644d 8151] 0017.7c2f.b69a Local Policy:
apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from apfMsSumOverride
[05/09/14 13:13:18.802 IST 644e 8151] 0017.7c2f.b69a Applying post-handoff policy
for station  0017.7c2f.b69a  - valid mask 0x0

[05/09/14 13:13:18.802 IST 644f 8151] 0017.7c2f.b69a     QOS Level: -1, DSCP: -1,
dot1p: -1, Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
 --More--
```

```
[05/09/14 13:13:18.802 IST 6450 8151] 0017.7c2f.b69a     Session: -1,
User session: -1, User elapsed -1
   Interface: N/A ACL: N/A Qos Pol Down   Qos Pol Up

[05/09/14 13:13:18.802 IST 6451 8151] 0017.7c2f.b69a Local Policy: At the start of
apfApplyOverride2. Client State DHCP_REQD

[05/09/14 13:13:18.802 IST 6452 8151] 0017.7c2f.b69a Applying new AAA override for
station  0017.7c2f.b69a
[05/09/14 13:13:18.802 IST 6453 8151] 0017.7c2f.b69a Local Policy: Applying new AAA
override for station
[05/09/14 13:13:18.802 IST 6454 8151] 0017.7c2f.b69a Override Values: source: 16,
valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1
[05/09/14 13:13:18.802 IST 6455 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1,
dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:18.802 IST 6456 8151] 0017.7c2f.b69a Local Policy: Applying
override policy
[05/09/14 13:13:18.802 IST 6457 8151] 0017.7c2f.b69a Clearing Dhcp state for
station  ---
[05/09/14 13:13:18.802 IST 6458 8151] 0017.7c2f.b69a Local Policy: Before Applying
WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 6459 8151] 0017.7c2f.b69a Local Policy:Setting Interface
name e VLAN0012

[05/09/14 13:13:18.802 IST 645a 8151] 0017.7c2f.b69a Local Policy:Setting local
bridging VLAN  name VLAN0012 and VLAN ID  12

[05/09/14 13:13:18.802 IST 645b 8151] 0017.7c2f.b69a Applying WLAN ACL policies
to client
[05/09/14 13:13:18.802 IST 645c 8151] 0017.7c2f.b69a No Interface ACL used for
Wireless client in WCM(NGWC)
[05/09/14 13:13:18.802 IST 645d 8151] 0017.7c2f.b69a apfApplyWlanPolicy:
Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:18.802 IST 645e 8151] 0017.7c2f.b69a Local Policy: After
Applying WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and
apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 645f 8151] 0017.7c2f.b69a Local Policy: After Applying
Site Override  policy AccessVLAN = 12 and SessionTimeout  is 1800 and
apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 6460 8151] 0017.7c2f.b69a Inserting AAA Override struct
for mobile MAC:  0017.7c2f.b69a , source 16

[05/09/14 13:13:18.802 IST 6461 8151] 0017.7c2f.b69a Inserting new RADIUS override
into chain for station  0017.7c2f.b69a
[05/09/14 13:13:18.802 IST 6462 8151] 0017.7c2f.b69a Override Values: source: 16,
valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1
[05/09/14 13:13:18.802 IST 6463 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1,
dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:18.802 IST 6464 8151] 0017.7c2f.b69a Local Policy: After ovr
check continuation
[05/09/14 13:13:18.802 IST 6465 8151] 0017.7c2f.b69a Local Policy:
apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from
apfMsSumOverride
[05/09/14 13:13:18.802 IST 6466 8151] 0017.7c2f.b69a Local Policy: Calling
applyLocalProfilingPolicyAction from Override2

[05/09/14 13:13:18.802 IST 6467 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****
```

```
[05/09/14 13:13:18.802 IST 6468 8151] 0017.7c2f.b69a *** Client State =
DHCP_REQD instance = 2 instance Name POLICY_PROFILING_L2_AUTH,
OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0,
userRole=(null)

[05/09/14 13:13:18.802 IST 6469 8151] 0017.7c2f.b69a     Local Profiling Values :
isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,applyPolicyAtRun= 0
[05/09/14 13:13:18.802 IST 646a 8151] 0017.7c2f.b69a          ipv4ACL = [],
ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[05/09/14 13:13:18.802 IST 646b 8151] 0017.7c2f.b69a Local Policy: At the End
AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 646c 8151] 0017.7c2f.b69a apfMsRunStateInc
[05/09/14 13:13:18.802 IST 646d 8151] 0017.7c2f.b69a Session Update for Non-dot1x client

[05/09/14 13:13:18.802 IST 646e 8151] 0017.7c2f.b69a 1XA: Session Push for Non-dot1x
wireless client
[05/09/14 13:13:18.802 IST 646f 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr to Push
wireless session for client  47ad4000000145 uid 280
 --More--
[05/09/14 13:13:18.802 IST 6470 8151] 0017.7c2f.b69a Session Update for Pushed Sessions

[05/09/14 13:13:18.802 IST 6471 8151] 0017.7c2f.b69a Session Manager Call Client
47ad4000000145, uid 280, capwap id 506c800000000f,Flag 0 Audit-Session ID
0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:18.802 IST 6472 8151] 0017.7c2f.b69a Change state to RUN (20) last
state DHCP_REQD (7)

[05/09/14 13:13:18.802 IST 6473 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:18.802 IST 6474 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0 curr
Mob State 3 llReq flag 1
[05/09/14 13:13:18.802 IST 6475 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0
currMob State 3 afd action 1
[05/09/14 13:13:18.802 IST 6476 8151] 0017.7c2f.b69a WCDB_LLM: pl handle 259 vlan_id
12 auth RUN(4) mobility 3 client_id 0x47ad4000000145 src_interface 0x506c800000000f
dst_interface 0x75e18000000143 client_type 0 p2p_type 1 bssid c8f9.f983.4260 radio_id
0 wgbid 0000.0000.0000
[05/09/14 13:13:18.802 IST 6477 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan
12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f
dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 1 ip  0.0.0.0
ip_learn_type 0
[05/09/14 13:13:18.802 IST 6478 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2] Session update from Client[1] for 0017.7c2f.b69a,
ID list 0x00000000, policy
[05/09/14 13:13:18.802 IST 6479 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:18.802 IST 647a 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3
curr Mob State 3 llReq flag 0
[05/09/14 13:13:18.802 IST 647b 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4)
vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int
0x506c800000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0
ip  0.0.0.0 ip_learn_type 0
[05/09/14 13:13:18.802 IST 647c 8151] 0017.7c2f.b69a AAAS: creating accounting start
record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:18.802 IST 647d 8151] 0017.7c2f.b69a AAAS: initialised accounting
start request, uid=280 passthrough=1
[05/09/14 13:13:18.802 IST 647e 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:18.803 IST 647f 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state
(L2_AUTH_DONE->RUN) mob_st<truncated>
[05/09/14 13:13:18.803 IST 6480 207] [WCDB] ===intf src/dst
(0x506c800000000f->0x506c800000000f)/(0x0->0x75e18000000143)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6
```

```
(<truncated>
[05/09/14 13:13:18.803 IST 6481 207] [WCDB] Foreign client add. Final llm
notified = false
[05/09/14 13:13:18.803 IST 6482 207] [WCDB] wcdb_client_mcast_update_notify:
No mcast action reqd
[05/09/14 13:13:18.803 IST 6483 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:13:18.803 IST 6484 207] [WCDB] wcdb_client_state_change_notify:
update flags = 0x3
[05/09/14 13:13:18.803 IST 6485 8151] 0017.7c2f.b69a aaa attribute list length is 79
[05/09/14 13:13:18.803 IST 6486 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF: [0017.7c2f.b69a]
WCDB RUN notification for 0017.7c2f.b69a
[05/09/14 13:13:18.803 IST 6487 8151] 0017.7c2f.b69a Sending SPI
spi_epm_epm_session_create successfull
[05/09/14 13:13:18.803 IST 6488 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20
mmRole ExpForeign !!!
[05/09/14 13:13:18.803 IST 6489 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20 mmRole
ExpForeign, updating wcdb not needed
[05/09/14 13:13:18.803 IST 648a 8151] 0017.7c2f.b69a Tclas Plumb needed: 0
[05/09/14 13:13:18.803 IST 648b 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:18.803 IST 648c 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN)
mob_st<truncated>
[05/09/14 13:13:18.803 IST 648d 207] [WCDB] ===intf src/dst
(0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false)
addr v4/v6 (<truncated>
[05/09/14 13:13:18.803 IST 648e 207] [WCDB] wcdb_client_mcast_update_notify:
No mcast action reqd
[05/09/14 13:13:18.803 IST 648f 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:13:18.803 IST 6490 207] [WCDB] wcdb_client_state_change_notify:
update flags = 0x2
[05/09/14 13:13:18.803 IST 6491 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0017.7c2f.b69a] WCDB RUN notification for 0017.7c2f.b69a
[05/09/14 13:13:18.803 IST 6492 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:18.803 IST 6493 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (UPDATE) return code (0)
[05/09/14 13:13:18.803 IST 6494 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (UPDATE) return code (0)
[05/09/14 13:13:18.803 IST 6495 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2]
Delay add/update sync of iif-id for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:18.803 IST 6496 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2]
Delay add/update sync of audit-session-id for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:18.803 IST 6497 8151] 0017.7c2f.b69a Received session_create_response
for client handle 20175213735969093
[05/09/14 13:13:18.803 IST 6498 8151] 0017.7c2f.b69a Received session_create_response
with EPM session handle 4261413136
[05/09/14 13:13:18.803 IST 6499 8151] 0017.7c2f.b69a Splash Page redirect client
or posture client
 --More--
[05/09/14 13:13:18.803 IST 649a 8151] 0017.7c2f.b69a REDIRECT ACL present in the
attribute list
[05/09/14 13:13:18.803 IST 649b 8151] 0017.7c2f.b69a Setting AAA Override
Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:18.803 IST 649c 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl
'REDIRECT'
[05/09/14 13:13:18.803 IST 649d 8151] 0017.7c2f.b69a AAA Override Url-Redirect
'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa'
set
[05/09/14 13:13:18.803 IST 649e 8151] 0017.7c2f.b69a  Wireless Client mobility role
is not ExportAnchor/Local. Hence we are not sending request to EPM
```

[05/09/14 13:13:20.445 IST 649f 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 0.0.0.0
ip_learn_type 0 deleted ipv4 0.0.0.0
[05/09/14 13:13:20.446 IST 64a0 207] [WCDB] wcdb_foreign_client_ip_addr_update:
Foreign client (0017.7c2f.b69a) ip addr update received.
[05/09/14 13:13:20.446 IST 64a1 207] [WCDB] SISF Update: IPV6 Addr[0] :
fe80::6c1a:b253:d711:c7f
[05/09/14 13:13:20.446 IST 64a2 207] [WCDB] SISF Update : Binding delete status
for V6: = 0
[05/09/14 13:13:20.446 IST 64a3 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:20.448 IST 64a4 8151] 0017.7c2f.b69a MS got the IP,
resetting the Reassociation Count 0 for client
[05/09/14 13:13:20.448 IST 64a5 8151] 0017.7c2f.b69a AAAS: creating accounting interim
record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:20.449 IST 64a6 8151] 0017.7c2f.b69a AAAS: initialised accounting
interim request, uid=280 passthrough=1
[05/09/14 13:13:20.449 IST 64a7 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:20.449 IST 64a8 8151] 0017.7c2f.b69a Guest User() assigned IP Address
(10.105.135.190)
[05/09/14 13:13:20.449 IST 64a9 8151] 0017.7c2f.b69a Assigning Address 10.105.135.190
to mobile
[05/09/14 13:13:20.449 IST 64aa 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4
10.105.135.190 ip_learn_type DHCP deleted ipv4 0.0.0.0
[05/09/14 13:13:20.449 IST 64ab 8151] 0017.7c2f.b69a AAAS: creating accounting
interim record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:20.449 IST 64ac 8151] 0017.7c2f.b69a AAAS: initialised accounting
interim request, uid=280 **passthrough=1**
[05/09/14 13:13:20.449 IST 64ad 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:20.449 IST 64ae 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20
mmRole ExpForeign !!!
[05/09/14 13:13:20.449 IST 64af 207] [WCDB] wcdb_foreign_client_ip_addr_update: Foreign
client (0017.7c2f.b69a) ip addr update received.
[05/09/14 13:13:20.449 IST 64b0 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20
mmRole ExpForeign, updating wcdb not needed
[05/09/14 13:13:20.449 IST 64b1 8151] 0017.7c2f.b69a Tclas Plumb needed: 0
[05/09/14 13:13:20.449 IST 64b2 207] [WCDB] SISF Update: IPV6 Addr[0] :
fe80::6c1a:b253:d711:c7f
[05/09/14 13:13:20.449 IST 64b3 207] [WCDB] SISF Update : Binding delete status for V6: = 0
[05/09/14 13:13:20.449 IST 64b4 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF
to remove assoc in Foreign
[05/09/14 13:13:20.449 IST 64b5 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay
add/update sync of addr for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:49.429 IST 64b6 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
Session authz update requested cmd 5, mac 0017.7c2f.b69a, attr-list 0x0 for Client[1]
[05/09/14 13:13:49.430 IST 64b7 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
Session authz update request sent to Client[1]
[05/09/14 13:13:49.430 IST 64b8 8151] 0017.7c2f.b69a 1XA: Processing update request from
dot1x. COA type 5
[05/09/14 13:13:49.430 IST 64b9 8151] 0017.7c2f.b69a AAAS: authorization init, uid=280,
context=268
[05/09/14 13:13:49.430 IST 64ba 8151] 0017.7c2f.b69a AAAS: initialised auth request,
uinque id=280, context id = 268, context reqHandle 0xfefc172c
[05/09/14 13:13:49.430 IST 64bb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request
for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER
[05/09/14 13:13:49.430 IST 64bc 8151] 0017.7c2f.b69a AAAS: auth request sent
[05/09/14 13:13:49.430 IST 64bd 8151] 0017.7c2f.b69a processing COA type 5
 was successful
[05/09/14 13:13:49.430 IST 64be 8151] 0017.7c2f.b69a processing COA type 5
 was successful
[05/09/14 13:13:49.430 IST 64bf 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
Session authz update response received for Client[1]
[05/09/14 13:13:49.430 IST 64c0 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[05/09/14 13:13:49.430 IST 64c1 211] AAA SRV(00000118): process author req
[05/09/14 13:13:49.430 IST 64c2 211] AAA SRV(00000118): **Author method=SERVER_GROUP**

Zubair_ISE

```
[05/09/14 13:13:49.430 IST 64c3 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[05/09/14 13:13:49.430 IST 64c4 211]  AAA SRV(00000000): process response req
[05/09/14 13:13:49.469 IST 64c5 220] AAA SRV(00000118): protocol reply PASS for
Authorization
[05/09/14 13:13:49.469 IST 64c6 220] AAA SRV(00000118): Return Authorization status=PASS
[05/09/14 13:13:49.469 IST 64c7 8151] 0017.7c2f.b69a AAAS: received response, cid=268
[05/09/14 13:13:49.469 IST 64c8 8151] 0017.7c2f.b69a AAAS: deleting context, cid=268
[05/09/14 13:13:49.469 IST 64c9 8151] 0017.7c2f.b69a Not comparing because the ACLs
have not been sent yet.
[05/09/14 13:13:49.469 IST 64ca 8151] 0017.7c2f.b69a Final flag values are,
epmSendAcl 1, epmSendAclDone 0
[05/09/14 13:13:49.469 IST 64cb 8151] 0017.7c2f.b69a
client incoming attribute size are 77
 --More--
[05/09/14 13:13:49.469 IST 64cc 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0
uniqueId=280
[05/09/14 13:13:49.469 IST 64cd 8151] 0017.7c2f.b69a Local Policy: At the start of
apfApplyOverride2. Client State RUN

[05/09/14 13:13:49.469 IST 64ce 8151] 0017.7c2f.b69a Applying new AAA override for
station  0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64cf 8151] 0017.7c2f.b69a Local Policy: Applying new AAA
override for station
[05/09/14 13:13:49.469 IST 64d0 8151] 0017.7c2f.b69a Override Values: source: 2,
valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:49.469 IST 64d1 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC:
-1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:49.469 IST 64d2 8151] 0017.7c2f.b69a Local Policy: Applying override policy
[05/09/14 13:13:49.469 IST 64d3 8151] 0017.7c2f.b69a Clearing Dhcp state for station  ---
[05/09/14 13:13:49.469 IST 64d4 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN
policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64d5 8151] 0017.7c2f.b69a Local Policy:Setting Interface name
e VLAN0012

[05/09/14 13:13:49.469 IST 64d6 8151] 0017.7c2f.b69a Local Policy:Setting local bridging
VLAN  name VLAN0012 and VLAN ID  12

[05/09/14 13:13:49.469 IST 64d7 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client
[05/09/14 13:13:49.469 IST 64d8 8151] 0017.7c2f.b69a No Interface ACL used for Wireless
client in WCM(NGWC)
[05/09/14 13:13:49.469 IST 64d9 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the
ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:49.469 IST 64da 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN
policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64db 8151] 0017.7c2f.b69a Local Policy: After Applying Site
Override  policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64dc 8151] 0017.7c2f.b69a Inserting AAA Override struct for mobile
   MAC:  0017.7c2f.b69a , source 2

[05/09/14 13:13:49.469 IST 64dd 8151] 0017.7c2f.b69a Inserting new RADIUS override into
chain for station  0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64de 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits:
0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:49.469 IST 64df 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC:
-1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:49.469 IST 64e0 8151] 0017.7c2f.b69a Local Policy: After ovr check
continuation
[05/09/14 13:13:49.469 IST 64e1 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c
apfMsSumOverride 447  Returning fail from apfMsSumOverride
[05/09/14 13:13:49.469 IST 64e2 8151] 0017.7c2f.b69a Local Policy: Calling
```

```
applyLocalProfilingPolicyAction from Override2

[05/09/14 13:13:49.469 IST 64e3 8151] 0017.7c2f.b69a
**** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:49.469 IST 64e4 8151] 0017.7c2f.b69a *** Client State = RUN instance = 2
instance Name POLICY_PROFILING_L2_AUTH, OverrideEnable = 1 deviceTypeLen=0,
deviceType=(null), userRoleLen=0, userRole=(null)

[05/09/14 13:13:49.469 IST 64e5 8151] 0017.7c2f.b69a     Local Profiling Values :
isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,applyPolicyAtRun= 0
[05/09/14 13:13:49.469 IST 64e6 8151] 0017.7c2f.b69a          ipv4ACL = [],
ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[05/09/14 13:13:49.469 IST 64e7 8151] 0017.7c2f.b69a Local Policy: At the End AccessVLAN
= 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64e8 8151] 0017.7c2f.b69a In >= L2AUTH_COMPLETE for station
0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64e9 8151] 0017.7c2f.b69a AAAS: creating accounting interim
record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:49.469 IST 64ea 8151] 0017.7c2f.b69a AAAS: initialised accounting interim
request, uid=280 passthrough=1
[05/09/14 13:13:49.469 IST 64eb 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:49.469 IST 64ec 8151] 0017.7c2f.b69a Not Using WMM Compliance code qosCap 00
[05/09/14 13:13:49.469 IST 64ed 8151] 0017.7c2f.b69a In SPI call for >= L2AUTH_COMPLETE
for station  0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64ee 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:49.469 IST 64ef 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3 curr Mob
State 3 llReq flag 0
[05/09/14 13:13:49.469 IST 64f0 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 12
radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f
dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0 ip  10.105.135.190
ip_learn_type DHCP
 --More--
[05/09/14 13:13:49.469 IST 64f1 8151] 0017.7c2f.b69a apfMsAssoStateInc
[05/09/14 13:13:49.469 IST 64f2 8151] 0017.7c2f.b69a apfPemAddUser2 (apf_policy.c:197)
Changing state for mobile  0017.7c2f.b69a  on AP  c8f9.f983.4260  from AAA Pending to
Associated

[05/09/14 13:13:49.469 IST 64f3 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1
[05/09/14 13:13:49.469 IST 64f4 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station:
 (callerId: 49) in 1800 seconds
[05/09/14 13:13:49.469 IST 64f5 8151] 0017.7c2f.b69a Ms Timeout = 1800,
Session Timeout = 1800

[05/09/14 13:13:49.469 IST 64f6 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN)
mob_st<truncated>
[05/09/14 13:13:49.469 IST 64f7 207] [WCDB] ===intf src/dst
(0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143) radio/bssid
(0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (<truncated>
[05/09/14 13:13:49.469 IST 64f8 207] [WCDB] wcdb_client_mcast_update_notify: No mcast
action reqd
[05/09/14 13:13:49.469 IST 64f9 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify client
(0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:15:47.411 IST 650a 8151] 0017.7c2f.b69a Acct-interim update sent for
station 0017.7c2f.b69a
[05/09/14 13:16:38.431 IST 650b 8151] 0017.7c2f.b69a
Client stats update: Time now in sec 1399621598, Last Acct Msg Sent at 1399621547 sec
```

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).