

# Exemple de configuration de l'authentification Web centrale sur l'accès convergé et les WLC Unified Access

## Table des matières

[Introduction](#)  
[Conditions préalables](#)  
[Exigences](#)  
[Composants utilisés](#)  
[Configurer](#)  
[Topologie 1](#)  
[Topologie 2](#)  
[Topologie 3](#)  
[Exemple](#)  
[Exemple de configuration de la topologie 1](#)  
[Configuration sur l'ISE](#)  
[Configuration sur le WLC](#)  
[Exemple de configuration de la topologie 2](#)  
[Configuration sur l'ISE](#)  
[Configuration sur le WLC](#)  
[Exemple de configuration de la topologie 3](#)  
[Configuration sur l'ISE](#)  
[Configuration sur le WLC](#)  
[Vérifier](#)  
[Dépannage](#)

## Introduction

Ce document décrit comment configurer l'authentification Web centrale sur le contrôleur LAN sans fil d'accès convergé (WLC) et aussi entre le WLC d'accès convergé et le WLC d'accès unifié (5760 et aussi entre 5760 et 5508).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base des WLC Cisco 5508, 5760 et 3850
- Connaissances de base d'Identity Services Engine (ISE)
- Connaissances de base sur la mobilité sans fil
- Connaissances de base de l'ancrage invité

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC 5760 qui exécute Cisco IOS® XE version 3.3.3
- WLC 5508 qui exécute Cisco Aironet OS version 7.6
- Commutateur 3850 qui exécute Cisco IOS XE version 3.3.3
- Cisco ISE qui exécute la version 1.2

## Configurer

**Remarque :** utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

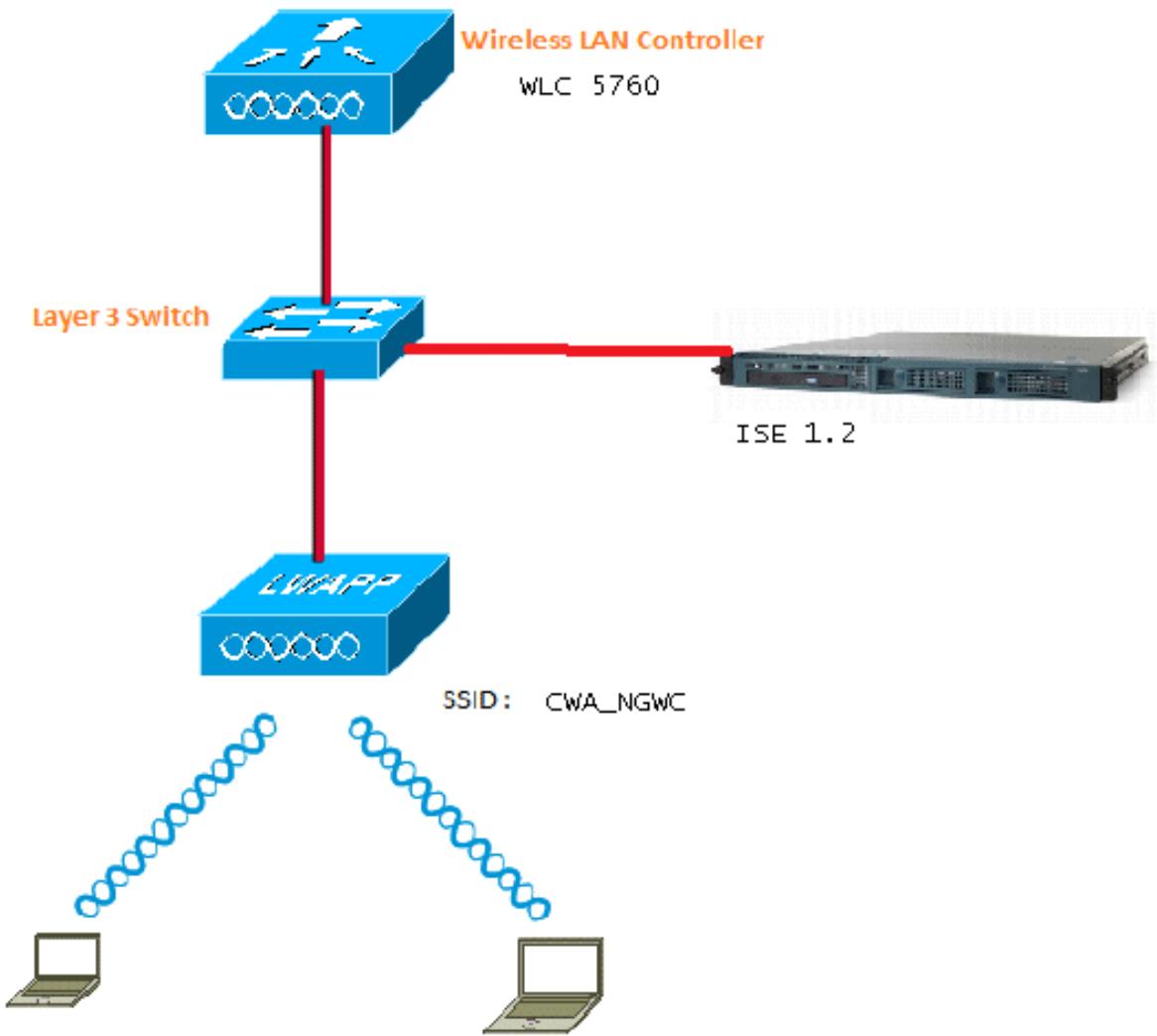
Le flux comprend les étapes suivantes :

1. L'utilisateur s'associe à l'identifiant SSID (Service Set Identifier) d'authentification Web, qui est en fait open+macfilter et n'offre aucune sécurité de couche 3.
2. L'utilisateur ouvre le navigateur.
3. Le WLC redirige vers le portail invité.
4. L'utilisateur s'authentifie sur le portail.
5. L'ISE envoie un changement d'autorisation RADIUS (CoA - Port UDP 1700) afin d'indiquer au contrôleur que l'utilisateur est valide, et finit par pousser les attributs RADIUS tels que la liste de contrôle d'accès (ACL).
6. L'utilisateur est invité à réessayer l'URL d'origine.

Cisco utilise trois configurations de déploiement différentes qui couvrent tous les différents scénarios pour réaliser l'authentification Web centrale (CWA).

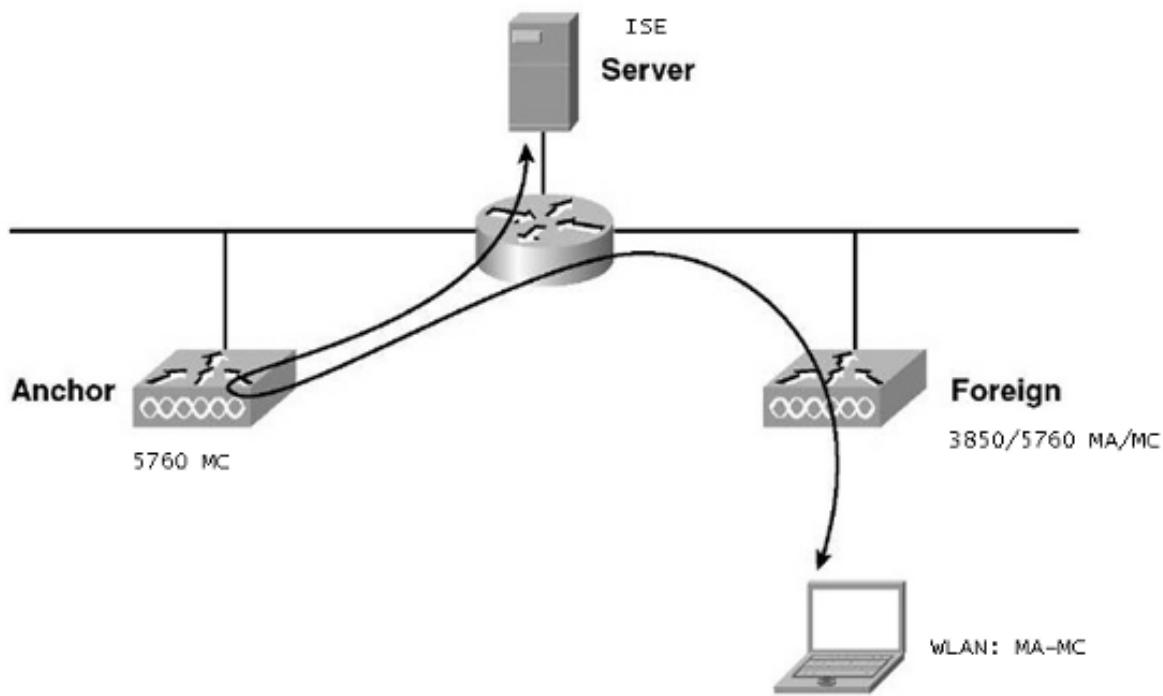
## Topologie 1

Le WLC 5760 agit comme un WLC autonome et les points d'accès se terminent sur le même WLC 5760. Les clients sont connectés à un réseau local sans fil (WLAN) et sont authentifiés auprès de l'ISE.



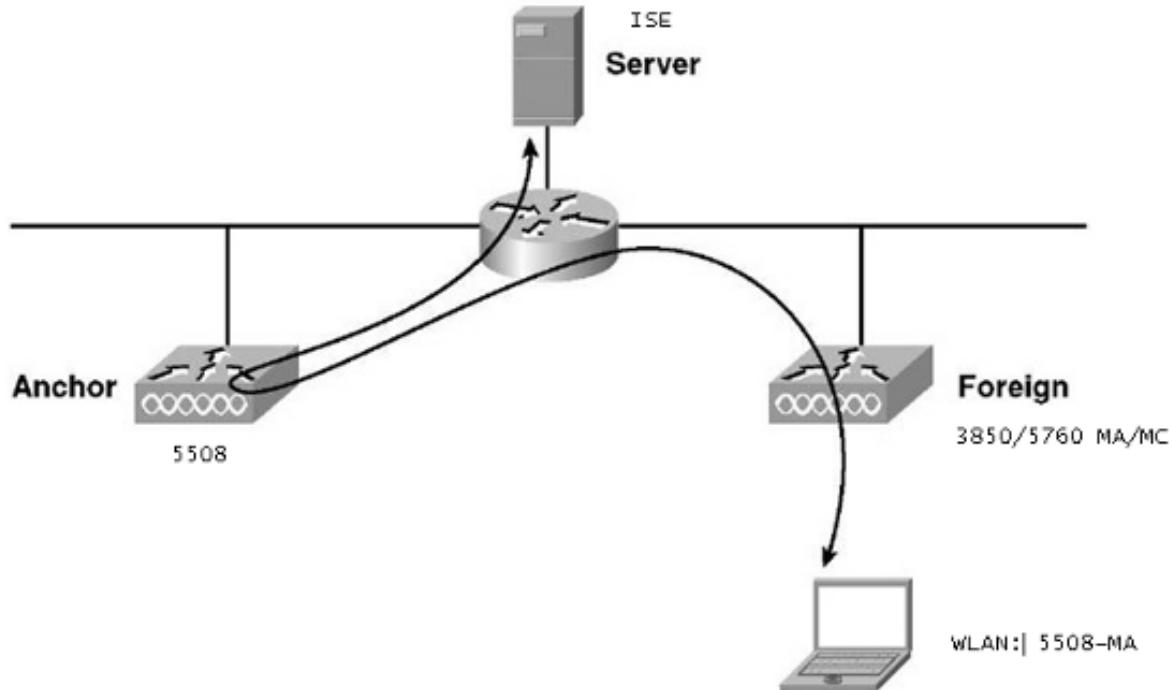
## Topologie 2

Ancrage invité entre le WLC d'accès convergé avec un contrôleur de mobilité et un agent de mobilité. L'agent de mobilité est le WLC étranger et le contrôleur de mobilité est l'ancre.



### Topologie 3

Ancrage invité entre le WLC Cisco Unified 5508 et le WLC d'accès convergé 5760/3850 avec un contrôleur de mobilité et un agent de mobilité. Le contrôleur de mobilité/agent de mobilité est le WLC étranger et le contrôleur de mobilité 5508 est l'ancre.



**Remarque :** dans de nombreux déploiements, l'ancre est le contrôleur de mobilité et le WLC étranger est l'agent de mobilité qui obtient la licence d'un autre contrôleur de mobilité. Dans ce cas, le WLC étranger n'a qu'une seule ancre et cette ancre est celle qui pousse les politiques. Le double ancrage n'est pas pris en charge et ne fonctionne pas, car il n'est pas censé fonctionner de cette manière.

## Exemple

Le WLC 5508 agit en tant qu'ancre et le WLC 5760 en tant que contrôleur de mobilité pour un commutateur 3850 qui agit en tant qu'agent de mobilité. Pour le WLAN étranger d'ancrage, le WLC 5508 sera l'ancrage du WLAN étranger 3850. Il n'est pas du tout nécessaire de configurer ce WLAN sur le WLC 5760. Si vous pointez le commutateur 3850 vers l'ancre 5760, puis de ce WLC 5760 vers le WLC 5508 en tant qu'ancre double, cela ne fonctionnera pas car cela devient une ancre double et les politiques sont sur l'ancre 5508.

Si vous disposez d'une configuration qui inclut un WLC 5508 en tant qu'ancre, un WLC 5760 en tant que contrôleur de mobilité et un commutateur 3850 en tant qu'agent de mobilité et WLC étranger, alors à tout moment l'ancre du commutateur 3850 sera soit le WLC 5760 soit le WLC 5508. Il ne peut pas être à la fois le et le double ancrage ne fonctionne pas.

## Exemple de configuration de la topologie 1

Reportez-vous à la [topologie 1](#) pour le schéma et l'explication du réseau.

La configuration est un processus en deux étapes :

1. Configuration sur ISE.
2. Configuration sur le WLC.

Le WLC 5760 agit comme un WLC autonome et les utilisateurs sont authentifiés auprès de l'ISE.

## Configuration sur l'ISE

1. Choisissez **ISE GUI > Administration > Network Resource > Network Devices List > Add** afin d'ajouter le WLC sur l'ISE en tant que client AAA (Authentication, Authorization, and Accounting). Assurez-vous que vous entrez le même secret partagé sur le WLC qui est ajouté sur le serveur RADIUS. **Remarque :** lorsque vous déployez Anchor-Foreign, il vous suffit d'ajouter le WLC étranger. Il n'est pas nécessaire d'ajouter le WLC d'ancrage sur l'ISE comme client AAA. La même configuration ISE est utilisée pour tous les autres scénarios de déploiement de ce document.

## Network Devices

* Name	<input type="text" value="Surbg_5760"/>
Description	<input type="text"/>
* IP Address: <input type="text" value="10.105.135.178"/> / <input type="text" value="32"/>	
Model Name <input type="text"/>	
Software Version <input type="text"/>	
* Network Device Group	
Location	<input type="text" value="All Locations"/> <input type="button" value="Set To Default"/>
Device Type	<input type="text" value="All Device Types"/> <input type="button" value="Set To Default"/>
<input checked="" type="checkbox"/> <input type="button" value="Authentication Settings"/>	
Enable Authentication Settings	
Protocol	<b>RADIUS</b>
* Shared Secret	<input type="text" value="*****"/> <input type="button" value="Show"/>
Enable KeyWrap	<input type="checkbox"/> <input type="button" value="i"/>
* Key Encryption Key	<input type="text"/> <input type="button" value="Show"/>
* Message Authenticator Code Key	<input type="text"/> <input type="button" value="Show"/>
Key Input Format	<input type="radio"/> ASCII <input type="radio"/> HEXADECIMAL
<input type="checkbox"/> <input type="button" value="SNMP Settings"/>	
<input type="checkbox"/> <input type="button" value="Advanced TrustSec Settings"/>	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

2. Dans l'interface utilisateur graphique d'ISE, choisissez **Policy > Authentication > MAB > Edit** afin de créer la stratégie d'authentification. La stratégie d'authentification accepte l'adresse MAC du client, qui pointe vers les points d'extrémité internes. Choisissez ces sélections dans la liste Options :Dans la liste déroulante If authentication failed, sélectionnez **Reject**.Dans la liste déroulante Si l'utilisateur est introuvable, sélectionnez **Continuer**.Dans la liste déroulante Si le processus a échoué, sélectionnez **Abandonner**.Lorsque vous configurez avec ces options, le client qui échoue l'autorisation MAC poursuit avec le portail invité.

3. Dans l'interface utilisateur graphique d'ISE, choisissez **Policy > Authorization > Results > Authorization Profiles > Add**. Complétez les détails et cliquez sur **Save** afin de créer le profil d'autorisation. Ce profil aide les clients à être redirigés vers l'URL de redirection après l'authentification MAC, où les clients entrent le nom d'utilisateur/mot de passe invité.

4. Dans l'interface utilisateur graphique d'ISE, choisissez **Policy > Authorization > Results > Authorization Profiles > Add** afin de créer un autre profil d'autorisation pour permettre l'accès

aux utilisateurs avec les informations d'identification correctes.

The screenshot shows the ISE web interface with the following details:

- Authorization Profiles > PermitAccess**
- Authorization Profile**
  - \* Name: PermitAccess
  - Description: Default Profile with access type as Access-Accept
  - \* Access Type: ACCESS\_ACCEPT
  - Service Template:
- Common Tasks**
- Advanced Attributes Settings**
- Attributes Details**
  - Access Type = ACCESS\_ACCEPT

Buttons at the bottom: Save, Reset.

5. Créez les stratégies d'autorisation. La stratégie d'autorisation « Guest\_Wireless » transmet l'URL de redirection et la liste de contrôle d'accès de redirection à la session client. Le profil poussé ici est le CWA, comme indiqué précédemment. La stratégie d'autorisation « Guest\_Wireless-Sucess » donne un accès complet à un utilisateur invité qui a été authentifié avec succès via le portail invité. Une fois que l'utilisateur est authentifié avec succès sur le portail invité, l'autorisation dynamique est envoyée par le WLC. Cette opération authentifie à nouveau la session client avec l'attribut « Accès réseau : l'utilisation est égale au flux invité ». Les politiques d'autorisation finales ressemblent à :

<input checked="" type="checkbox"/> Guest_Wireless_Success	If Guest AND Network Access:UseCase EQUALS Guest Flow	then PermitAccess	Edit   ▾
<input checked="" type="checkbox"/> Guest_Wireless	If Wireless_MAB	then OWA	Edit   ▾

Buttons at the bottom: Save, Reset.

6. Facultatif : dans ce cas, les configurations multiportails par défaut sont utilisées. En fonction de la configuration requise, la même configuration peut être modifiée dans l'interface utilisateur graphique. Dans l'interface utilisateur graphique d'ISE, choisissez **Administration > Web Portal management > Multi Portal Configurations > DefaultGuestPortal**.

CISCO Identity Services Engine

Home Operations | Policy | Administration |

System Identity Management Network Resources Web Portal Management Feed Service

Sponsor Group Policy Sponsor Groups Settings

Multi-Portal Configuration List > DefaultGuestPortal

**Multi-Portal**

General Operations Customization Authentication

**Guest Portal Policy Configuration**

Guest users should agree to an acceptable use policy

Not Used  
 First Login  
 Every Login

Enable Self-Provisioning Flow  
 Enable Mobile Portal  
 Allow guest users to change password  
 Require guest users to change password at expiration and first login  
 Guest users should download the posture client  
 Guest users should be allowed to do self service  
 Send self-registration credentials to whitelisted email domains

Settings

- General
- Sponsor
- My Devices
- Guest**
  - Details Policy
  - Guest Roles Configuration
  - Language Template
  - Multi-Portal Configurations**
    - CWA
    - DefaultGuestPortal**
    - DRW
    - Portal Policy
    - Password Policy
  - Time Profiles

La séquence Guest\_Portal\_sequence est créée pour autoriser les utilisateurs internes, invités et Active Directory.

**CISCO Identity Services Engine**

Home Operations | Policy | Administration |

System Identity Management Network Resources Web Portal Management Feed Service

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences List > Guest\_Portal\_Sequence

### Identity Source Sequence

▼ Identity Source Sequence

\* Name: Guest\_Portal\_Sequence

Description: A built-in Identity Sequence for the Guest Portal

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints LDAP_BS	Internal Users Guest Users AD1

▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"  
 Treat as if the user was not found and proceed to the next store in the sequence

**Save** **Reset**

7. Dans l'interface utilisateur graphique d'ISE, choisissez **Guest > Multi-Portal Configurations > DefaultGuestPortal**. Dans la liste déroulante Identifier la séquence de stockage, sélectionnez **Guest\_Portal\_Sequence**.

## Configuration sur le WLC

1. Définissez le serveur ISE Radius sur le WLC 5760.
2. Configurez le serveur RADIUS, le groupe de serveurs et la liste de méthodes avec l'interface de ligne de commande.

```
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. Configurez le WLAN avec l'interface de ligne de commande.

```
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. Configurez les listes de contrôle d'accès Redirect avec CLI. Il s'agit de l'url-redirect-acl retournée par ISE comme remplacement AAA avec l'URL de redirection pour la redirection du portail invité. Il s'agit d'une liste de contrôle d'accès directe actuellement utilisée sur l'architecture Unified. Il s'agit d'une liste de contrôle d'accès « punt » qui est une sorte de liste de contrôle d'accès inverse que vous utiliseriez normalement pour l'architecture Unified. Vous devez bloquer l'accès au serveur DHCP, au serveur DNS, au serveur DNS, au serveur DNS et au serveur ISE. Autorisez uniquement www, 443 et 8443 si nécessaire. Ce portail invité ISE utilise le port 8443 et la redirection fonctionne toujours avec la liste de contrôle d'accès présentée ici. ICMP est ici activé, mais en fonction des règles de sécurité, vous pouvez soit refuser, soit autoriser.

```

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

```

**Attention :** lorsque vous activez HTTPS, cela peut entraîner des problèmes de CPU élevés en raison de l'évolutivité. N'activez pas cette option, sauf recommandation de l'équipe de conception Cisco.

5. Dans l'interface graphique du contrôleur sans fil, choisissez **AAA > RADIUS > Servers**. Configurez le serveur RADIUS, le groupe de serveurs et la liste de méthodes dans l'interface utilisateur graphique. Renseignez tous les paramètres et assurez-vous que le secret partagé configuré ici correspond à celui configuré sur l'ISE pour ce périphérique. Dans la liste déroulante Support for RFC 3576, sélectionnez **Enable**.

The screenshot shows the Cisco Wireless Controller configuration interface. The top navigation bar includes Home, Monitor, Configuration (which is highlighted), Administration, and Help. The left sidebar has a tree view with nodes like AAA, Method Lists, Server Groups, RADIUS (with Servers selected), Fallback, and TACACS+ Servers. The main content area is titled "Radius Servers" under "Radius Servers > Edit". It contains the following fields:

Server Name	ISE
Server IP Address	10.106.73.69
Shared Secret	*****
Confirm Shared Secret	*****
Auth Port (0-65535)	1645
Acct Port (0-65535)	1646
Server Timeout (0-1000) secs	10
Retry Count (0-100)	3
Support for RFC 3576	Enable

6. Dans l'interface graphique du contrôleur sans fil, choisissez **AAA > Server Groups > Radius**.

Ajoutez le serveur RADIUS précédemment créé aux groupes de serveurs.

The screenshot shows the 'Radius Server Groups' configuration page. On the left, the navigation tree under 'Security' includes 'AAA', 'Method Lists' (with 'General' selected), 'Server Groups' (with 'Radius' selected), and 'RADIUS'. The main panel displays 'Radius Server Groups > Edit' for a group named 'ISE'. The 'Group Type' is set to 'Radius'. Under 'Available Servers', 'ISE' is listed. Under 'Assigned Servers', 'ISE' is also listed. Buttons for moving servers between lists are visible.

7. Dans l'interface graphique du contrôleur sans fil, choisissez AAA > Method Lists > General. Cochez la case Dot1x System Auth Control. Si vous désactivez cette option, AAA ne fonctionne pas.

The screenshot shows the 'General' method list configuration. Under 'AAA > Method Lists > General', the 'Dot1x System Auth Control' checkbox is checked. Other options like 'Local Authentication' and 'Method List' dropdown are also shown.

8. Dans l'interface graphique du contrôleur sans fil, choisissez AAA > Method Lists > Authentication. Créez une liste de méthodes d'authentification pour Type dot1X. Le type de groupe est groupe. Mappez-le à l'ISE.

The screenshot shows the 'Authentication' method list configuration. Under 'AAA > Method Lists > Authentication', a new method list 'dot1x\_ISE' is created for 'Type dot1x' and 'Group Type group'. The 'Fallback to local' option is disabled. Under 'Groups In This Method', 'ISE' is listed in the 'Available Server Groups' list and assigned to the 'Assigned Server Groups' list.

9. Dans l'interface graphique du contrôleur sans fil, choisissez AAA > Method Lists > Accounting. Créez une liste de méthodes de comptabilisation pour l'identité de type. Mappez-le à l'ISE.

The screenshot shows the Cisco Wireless Controller interface under the 'Security' section. In the left sidebar, 'Method Lists' is selected. On the right, the 'Accounting' tab is active, showing a configuration for a method list named 'ISE'. The 'Type' is set to 'identity'. The 'Available Server Groups' list contains 'ACS', 'ISE', 'Microsoft\_NPS', and 'victor'. The 'Assigned Server Groups' list contains 'ISE'. Navigation buttons '<' and '>' are between the two lists.

10. Dans l'interface graphique du contrôleur sans fil, choisissez AAA > Method Lists > Authorization. Créez une liste de méthodes d'autorisation pour le type réseau. Mappez-le à l'ISE.

The screenshot shows the Cisco Wireless Controller interface under the 'Security' section. In the left sidebar, 'Authorization' is selected under 'Method Lists'. On the right, the 'Authorization' tab is active, showing a configuration for a method list named 'ISE'. The 'Type' is set to 'network' and 'Group Type' is 'group'. The 'Available Server Groups' list contains 'ACS', 'ISE', 'Microsoft\_NPS', and 'victor'. The 'Assigned Server Groups' list contains 'ISE'. Navigation buttons '<' and '>' are between the two lists.

11. Facultatif, puisqu'il y a également une prise en charge MAC en cas de panne. Créez une liste de méthodes d'autorisation MACFILTER pour le réseau Type. Mappez-le à l'ISE.

The screenshot shows the Cisco Wireless Controller interface under the 'Security' section. In the left sidebar, 'Authorization' is selected under 'Method Lists'. On the right, the 'Authorization' tab is active, showing a configuration for a method list named 'MACFILTER'. The 'Type' is set to 'network' and 'Group Type' is 'group'. The 'Available Server Groups' list contains 'ACS', 'ISE', 'Microsoft\_NPS', and 'victor'. The 'Assigned Server Groups' list contains 'ISE'. Navigation buttons '<' and '>' are between the two lists.

12. Dans l'interface graphique du contrôleur sans fil, choisissez WLAN > WLANS. Créez une nouvelle configuration avec les paramètres affichés ici.

Cisco Wireless Controller

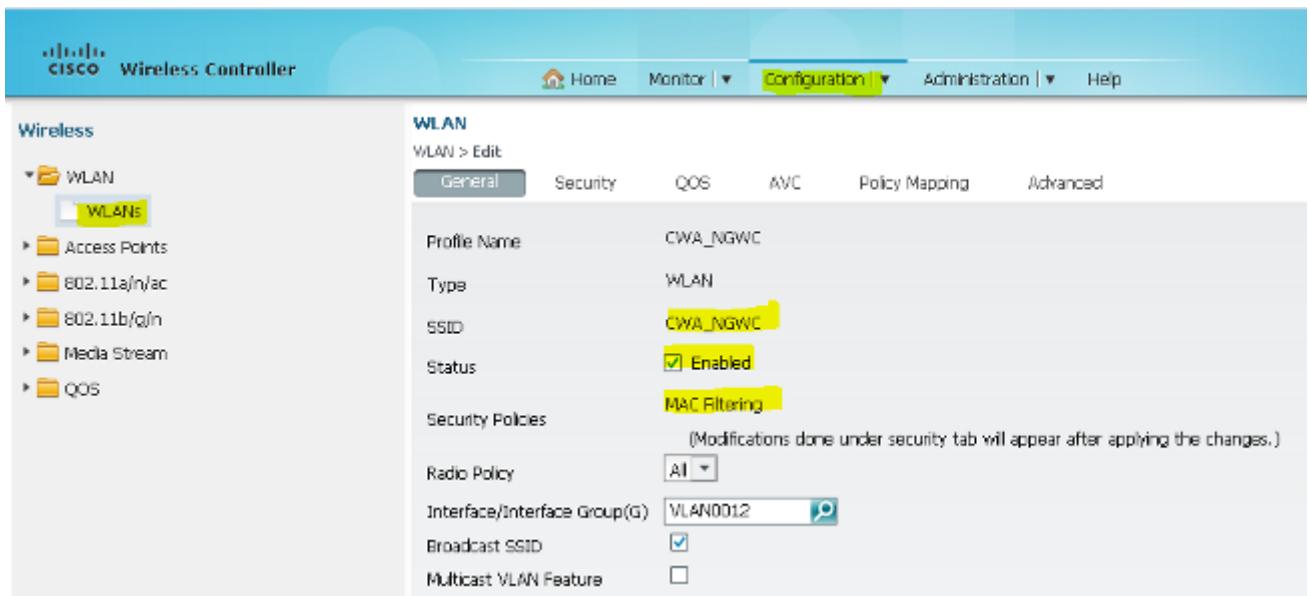
Home Monitor Configuration Administration Help

Wireless WLAN

WLAN > Edit

General Security QoS AVC Policy Mapping Advanced

Profile Name: CWA\_NGWC  
Type: WLAN  
SSID: CWA\_NGWC  
Status: Enabled  
Security Policies: MAC Filtering  
(Modifications done under security tab will appear after applying the changes.)  
Radio Policy: AI  
Interface/Interface Group(G): VLAN0012  
Broadcast SSID:   
Multicast VLAN Feature:



13. Choisissez **Security > Layer2**. Dans le champ MAC Filtering, saisissez **MACFILTER**.

Cisco Wireless Controller

Home Monitor Configuration Administration Help

Wireless WLAN

WLAN > Edit

General Security QoS AVC Policy Mapping Advanced

Layer2 Layer3 AAA Server

Layer 2 Security: None  
MAC Filtering: MACFILTER  
Fast Transition:   
Over the DS:   
Reassociation Timeout: 20



14. Il n'est pas nécessaire de configurer la couche 3.

Cisco Wireless Controller

Home Monitor Configuration Administration Help

Wireless WLAN

WLAN > Edit

General Security QoS AVC Policy Mapping Advanced

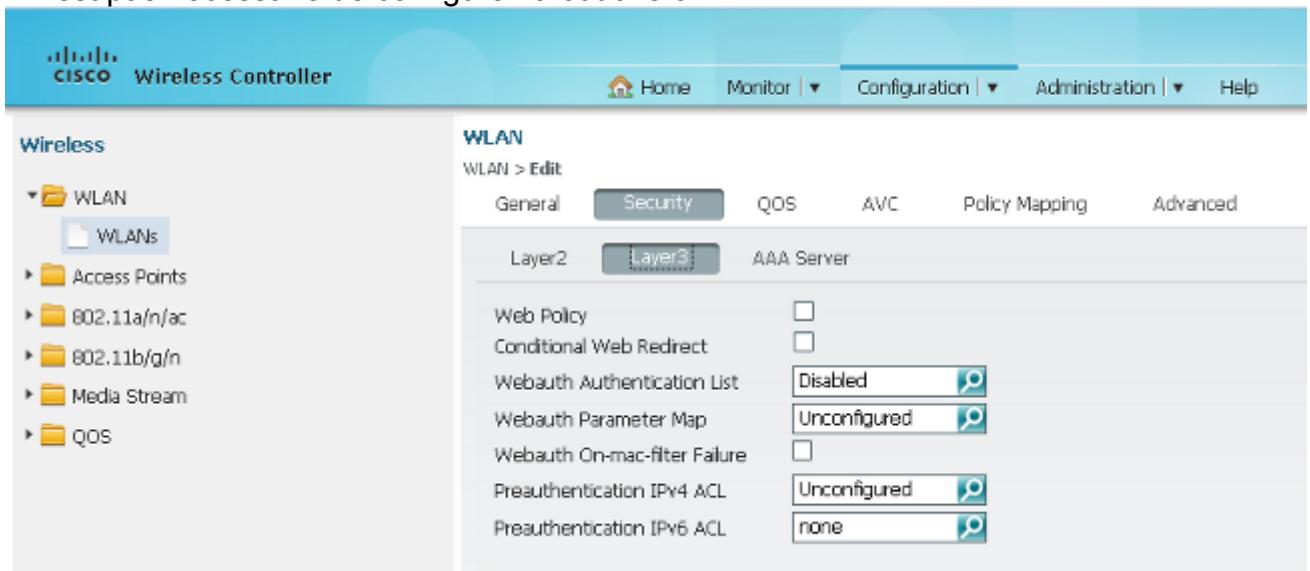
Layer2 Layer3 AAA Server

Web Policy:   
Conditional Web Redirect:   
Webauth Authentication List: Disabled

Webauth Parameter Map: Unconfigured

Webauth On-mac-filter Failure:   
Preattentation IPv4 ACL: Unconfigured

Preattentation IPv6 ACL: none



15. Choisissez **Security > AAA Server**. Dans la liste déroulante Authentication Method, sélectionnez **ISE**. Dans la liste déroulante Méthode de comptabilisation, sélectionnez **ISE**.

16. Sélectionnez Avancé. Cochez la case Allow AAA Override. Cochez la case État NAC.

17. Configurez les ACL de redirection sur le WLC dans l'interface graphique utilisateur.

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	-

## Exemple de configuration de la topologie 2

Reportez-vous à la [topologie 2](#) pour le schéma et l'explication du réseau.

Cette configuration est également un processus en deux étapes.

## Configuration sur l'ISE

La configuration sur l'ISE est la même que celle de la topologie 1.

Il n'est pas nécessaire d'ajouter le contrôleur d'ancrage sur l'ISE. Il vous suffit d'ajouter le WLC étranger sur l'ISE, de définir le serveur RADIUS sur le WLC étranger et de mapper la stratégie d'autorisation sous le WLAN. Sur l'ancre, il vous suffit d'activer le filtrage MAC.

Dans cet exemple de configuration, il y a deux WLC 5760 qui agissent comme un Anchor Foreign. Si vous souhaitez utiliser le WLC 5760 comme point d'ancrage et le commutateur 3850 comme point d'ancrage étranger, qui est l'agent de mobilité, vers un autre contrôleur de mobilité, alors la même configuration est correcte. Cependant, il n'est pas nécessaire de configurer le WLAN sur le deuxième contrôleur de mobilité vers lequel le commutateur 3850 obtient les licences. Il vous suffit de pointer le commutateur 3850 vers le WLC 5760 qui agit comme l'ancre.

## Configuration sur le WLC

- Sur le routeur Foreign, configurez le serveur ISE avec la liste de méthodes AAA pour AAA et mappez le WLAN à une autorisation de filtre MAC. **Remarque** : configurez la liste de contrôle d'accès de redirection sur les filtres Anchor et Foreign, ainsi que 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. Configurez les listes de contrôle d'accès Redirect avec CLI. Il s'agit de l'url-redirect-acl retournée par ISE comme remplacement AAA avec l'URL de redirection pour la redirection du portail invité. Il s'agit d'une liste de contrôle d'accès directe actuellement utilisée sur l'architecture Unified. Il s'agit d'une liste de contrôle d'accès « punt » qui est une sorte de liste de contrôle d'accès inverse que vous utiliseriez normalement pour l'architecture Unified. Vous devez bloquer l'accès au serveur DHCP, au serveur DNS, au serveur DNS et au serveur ISE. Autorisez uniquement www, 443 et 8443 si nécessaire. Ce portail invité ISE utilise le port 8443 et la redirection fonctionne toujours avec la liste de contrôle d'accès présentée ici. ICMP est ici activé, mais en fonction des règles de sécurité, vous pouvez soit refuser, soit autoriser.

```

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

```

**Attention :** lorsque vous activez HTTPS, cela peut entraîner des problèmes de CPU élevés en raison de l'évolutivité. N'activez pas cette option, sauf recommandation de l'équipe de conception Cisco.

3. Configurer la mobilité sur l'ancre

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

**Remarque :** si vous configurez la même chose avec le commutateur 3850 comme étranger, assurez-vous que vous définissez le groupe d'homologues de commutateur sur le contrôleur de mobilité et vice-versa sur le contrôleur de mobilité. Configurez ensuite les configurations CWA ci-dessus sur le commutateur 3850.

4. Configuration sur l'ancre. Sur l'ancre, il n'est pas nécessaire de configurer des configurations ISE. Vous avez juste besoin de la configuration 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. Configurer la mobilité sur l'ancre Définissez l'autre WLC comme membre de mobilité sur ce WLC.

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

6. Configurez les listes de contrôle d'accès Redirect avec CLI. Il s'agit de l'url-redirect-acl retournée par ISE comme remplacement AAA avec l'URL de redirection pour la redirection du portail invité. Il s'agit d'une liste de contrôle d'accès directe actuellement utilisée sur l'architecture Unified. Il s'agit d'une liste de contrôle d'accès « punt » qui est une sorte de

liste de contrôle d'accès inverse que vous utiliseriez normalement pour l'architecture Unified. Vous devez bloquer l'accès au serveur DHCP, au serveur DNS, au serveur DNS et au serveur ISE. Autorisez uniquement www, 443 et 8443 si nécessaire. Ce portail invité ISE utilise le port 8443 et la redirection fonctionne toujours avec la liste de contrôle d'accès présentée ici. ICMP est ici activé, mais en fonction des règles de sécurité, vous pouvez soit refuser, soit autoriser.

```
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
```

**Attention :** lorsque vous activez HTTPS, cela peut entraîner des problèmes de CPU élevés en raison de l'évolutivité. N'activez pas cette option, sauf recommandation de l'équipe de conception Cisco.

## Exemple de configuration de la topologie 3

Reportez-vous à la [topologie 3](#) pour le schéma et l'explication du réseau.

Il s'agit également d'un processus en deux étapes.

### Configuration sur l'ISE

La configuration sur l'ISE est la même que celle de la topologie 1.

Il n'est pas nécessaire d'ajouter le contrôleur d'ancrage sur l'ISE. Il vous suffit d'ajouter le WLC étranger sur l'ISE, de définir le serveur RADIUS sur le WLC étranger et de mapper la stratégie d'autorisation sous le WLAN. Sur l'ancre, il vous suffit d'activer le filtrage MAC.

Dans cet exemple, il y a un WLC 5508 qui agit en tant qu'ancre et un WLC 5760 qui agit en tant que WLC étranger. Si vous voulez utiliser un WLC 5508 comme ancre et un commutateur 3850 et un WLC étranger, qui est un agent de mobilité, vers un autre contrôleur de mobilité, alors la même configuration est correcte. Cependant, il n'est pas nécessaire de configurer le WLAN sur le deuxième contrôleur de mobilité vers lequel le commutateur 3850 obtient les licences. Il vous suffit de pointer le commutateur 3850 vers le WLC 5508 qui agit comme point d'ancrage.

### Configuration sur le WLC

1. Sur le WLC étranger, configurez le serveur ISE avec la liste de méthodes AAA pour AAA et mappez le WLAN à une autorisation de filtre MAC. Ce n'est pas nécessaire sur l'ancre.  
**Remarque :** configurez la liste de contrôle d'accès de redirection sur les WLC ancre et étranger, ainsi que le filtrage MAC.
2. Dans l'interface graphique du WLC 5508, choisissez **WLANs > New** afin de configurer l'Anchor 5508. Complétez les détails afin d'activer le filtrage MAC.

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar has a tree view with WLANS expanded, showing WLANS and Advanced. The main content area is titled 'WLANS > Edit '5508-MA''. It shows the 'General' tab selected, with tabs for Security, QoS, Policy-Mapping, and Advanced also present. The General tab displays the following configuration:

Profile Name	5508-MA
Type	WLAN
SSID	5508-MA
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	MAC Filtering
(Modifications done under security tab will appear after applying the changes.)	
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	5508-MC

3. Il n'est pas nécessaire de configurer les options de couche 2.

The screenshot shows the Cisco WLC interface. The top navigation bar includes MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The left sidebar has a tree view with WLANS expanded, showing WLANS and Advanced. The main content area is titled 'WLANS > Edit '5508-MA''. It shows the 'Policy-Mapping' tab selected, with tabs for General, Security, QoS, and Advanced also present. The Policy-Mapping tab displays the following configuration:

Layer 2 Security	None
MAC Filtering	<input checked="" type="checkbox"/>
Fast Transition	<input type="checkbox"/>

4. Il n'est pas nécessaire de configurer les options de couche 3.

The screenshot shows the Cisco WLC interface. The top navigation bar includes MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COM. The left sidebar has a tree view with WLANS expanded, showing WLANS and Advanced. The main content area is titled 'WLANS > Edit '5508-MA''. It shows the 'General' tab selected, with tabs for Security, QoS, Policy-Mapping, and Advanced also present. The General tab displays the following configuration:

Layer 3 Security	None
------------------	------

5. Les serveurs AAA doivent être désactivés dans le WLC Anchor AireOS pour que la CoA soit

traitée par le NGWC étranger. Les serveurs AAA ne peuvent être activés dans le WLC d'ancre que si aucun serveur RADIUS n'est configuré sous : Security > AAA > RADIUS > Authentication

- Choisissez WLANS > WLANS > Edit > Advanced. Cochez la case Allow AAA Override. Dans la liste déroulante État NAC, sélectionnez NAC Radius.

- Ajoutez-le comme point d'ancre du WLAN.

8. Une fois qu'il est désigné local, il doit le vérifier avec Control and Data Path UP/UP.

The screenshot shows the 'Mobility Anchors' section of the WLC interface. It displays a table with one row for 'Local'. The 'WLAN SSID' is set to '802.11n'. The 'Source IP Address (Anchor)' is 'Local'. The 'Data Path' and 'Control Path' both show a green 'Up' status. The 'Edit' button is highlighted in yellow.

9. Créez la liste de contrôle d'accès Redirect sur le WLC. DHCP et DNS sont refusés. Il autorise les protocoles HTTP/HTTP.

The screenshot shows the 'Access Control Lists > Edit' page. Under the 'General' tab, the 'Access List Name' is 'REDIRECT'. The table below lists four rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
<u>1</u>	Permit	/0.0.0.0	/0.0.0.0	UDP	Any	DNS	Any	Any	0
		0.0.0.0	0.0.0.0						
<u>2</u>	Permit	/0.0.0.0	/0.0.0.0	UDP	DNS	Any	Any	Any	0
		0.0.0.0	0.0.0.0						
<u>3</u>	Permit	/0.0.0.0	10.106.73.69	Any	Any	Any	Any	Any	0
		0.0.0.0	255.255.255.255						
<u>4</u>	Permit	/10.106.73.69	/0.0.0.0	Any	Any	Any	Any	Any	0
		255.255.255.255	0.0.0.0						

Voici comment il se comporte après la création de la liste de contrôle d'accès.

The screenshot shows the 'Security > Access Control Lists' page. On the left, under 'Access Control Lists', 'Access Control Lists' is selected. In the main pane, 'Enable Counters' is checked. A table shows two entries:

Name	Type
ACL_Provisioning_Redirect	IPv4
REDIRECT	IPv4

10. Définissez le serveur RADIUS ISE sur le WLC 5760.

11. Configurez le serveur RADIUS, le groupe de serveurs et la liste de méthodes avec l'interface de ligne de commande.

```
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. Configurez le WLAN à partir de l'interface 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. Définissez l'autre WLC comme membre de mobilité sur ce WLC.

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

**Remarque :** si vous configurez le même avec le WLC 3850 comme Foreign, alors assurez-vous de définir le groupe d'homologues de commutateur sur le contrôleur de mobilité et vice-versa sur le contrôleur de mobilité. Configurez ensuite les configurations CWA précédentes sur le WLC 3850.

14. Configurez les listes de contrôle d'accès Redirect avec CLI. Il s'agit de l'url-redirect-acl renvoyée par ISE comme remplacement AAA avec l'URL de redirection pour la redirection du portail invité. Il s'agit d'une liste de contrôle d'accès directe actuellement utilisée sur l'architecture Unified. Il s'agit d'une liste de contrôle d'accès « punt » qui est une sorte de liste de contrôle d'accès inverse que vous utiliseriez normalement pour l'architecture Unified. Vous devez bloquer l'accès au serveur DHCP, au serveur DNS, au serveur DNS et au serveur ISE. Autorisez uniquement www, 443 et 8443 si nécessaire. Ce portail invité ISE utilise le port 8443 et la redirection fonctionne toujours avec la liste de contrôle d'accès présentée ici. ICMP est ici activé, mais en fonction des règles de sécurité, vous pouvez soit refuser, soit autoriser.

```

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

```

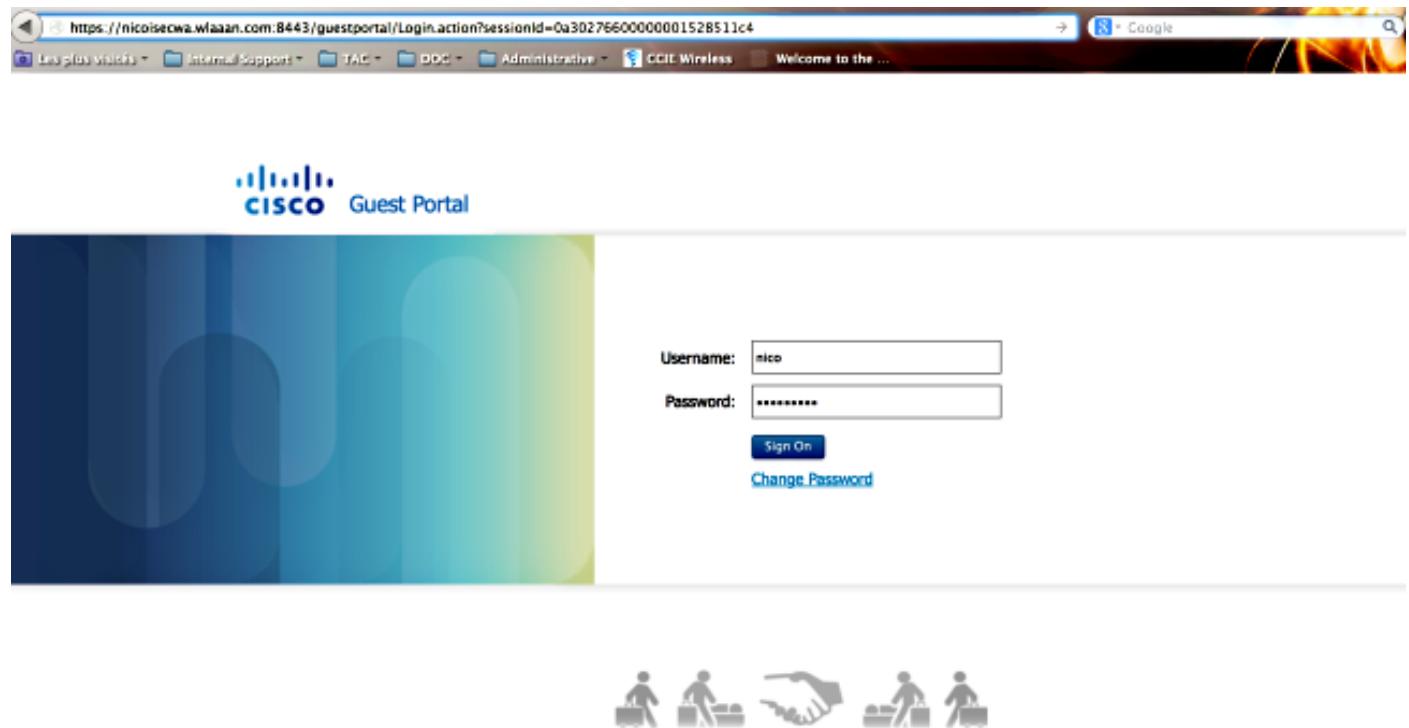
**Attention :** lorsque vous activez HTTPS, cela peut entraîner des problèmes de CPU élevés en raison de l'évolutivité. N'activez pas cette option, sauf recommandation de l'équipe de conception Cisco.

## Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Connectez le client au SSID configuré. Une fois que vous avez reçu l'adresse IP et que le client passe à l'état d'authentification Web requise, ouvrez le navigateur. Saisissez vos informations d'identification client dans le portail.



Une fois l'authentification réussie, cochez la case **Accepter les conditions générales**. Cliquez sur **Accepter**.

 Guest Portal

Welcome nico

## Acceptable Use Policy

Please accept the policy:

1. You are responsible for  
- maintaining the confidentiality of the password and  
- all activities that occur under your username and password.

2. 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.

3. 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.

Accept terms and conditions

Vous recevrez un message de confirmation et pourrez désormais naviguer sur Internet.

 Guest Portal

Welcome nico ([Sign Out](#))

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

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

Sur l'ISE, le flux client ressemble à ceci :

2014-05-09 06:28:19.334	<input checked="" type="checkbox"/>		shubar	00:17:7C:2F:86:9A	Unknown	Surbg_5760	PermitAccess	Authorize-Only succeeded	0x987b2536c7a1700000117
2014-05-09 06:28:19.298	<input checked="" type="checkbox"/>			00:17:7C:2F:86:9A		Surbg_5760		Dynamic Authorization succeeded	0x987b2536c7a1700000117
2014-05-09 06:28:19.274	<input checked="" type="checkbox"/>		shubar	00:17:7C:2F:86:9A				Guest Authentication Passed	0x987b2536c7a1700000117
2014-05-09 06:19.00.822	<input checked="" type="checkbox"/>			00:17:7C:2F:86:9	00:17:7C:2F:86:9A	Unknown	CWA	Authentication succeeded	0x987b2536c7a1700000117

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

**Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.**

Sur le WLC d'accès convergé, il est recommandé d'exécuter des traces au lieu de débogages. Sur le WLC Aironet OS 5508, il vous suffit d'entrer **debug client <client mac>** et **debug web-auth redirect enable mac <client mac>**.

```
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
```

Certains défauts connus sur le Cisco IOS-XE et le système d'exploitation Aironet sont inclus dans l'ID de bogue Cisco [CSCun3834](#).

Voici à quoi ressemble le flux CWA réussi sur les traces :

```
[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 received 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 wlan 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: wcdbAckRecvFlag
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, wlanIfName: , 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 received 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 wlan\_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) wlan
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
0x506c80000000f 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) wlan (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
(0x506c80000000f->0x506c80000000f)/(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) wlan (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
(0x506c80000000f->0x506c80000000f)/(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, unique 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, wlanIfName: , 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 received 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**

## À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.