Konfigurationsbeispiel für zentrale Web-Authentifizierung in WLCs mit konvergentem Zugriff und Unified Access

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die zentrale Webauthentifizierung auf dem Converged Access Wireless LAN Controller (WLC) sowie zwischen dem Converged Access WLC und dem Unified Access WLC (5760 sowie zwischen 5760 und 5508) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse des Cisco WLC 5508, 5760, 3850
- Grundkenntnisse der Identity Services Engine (ISE)
- Grundkenntnisse der Wireless-Mobilität
- Grundkenntnisse der Gastverankerung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Konfigurieren

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur für registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

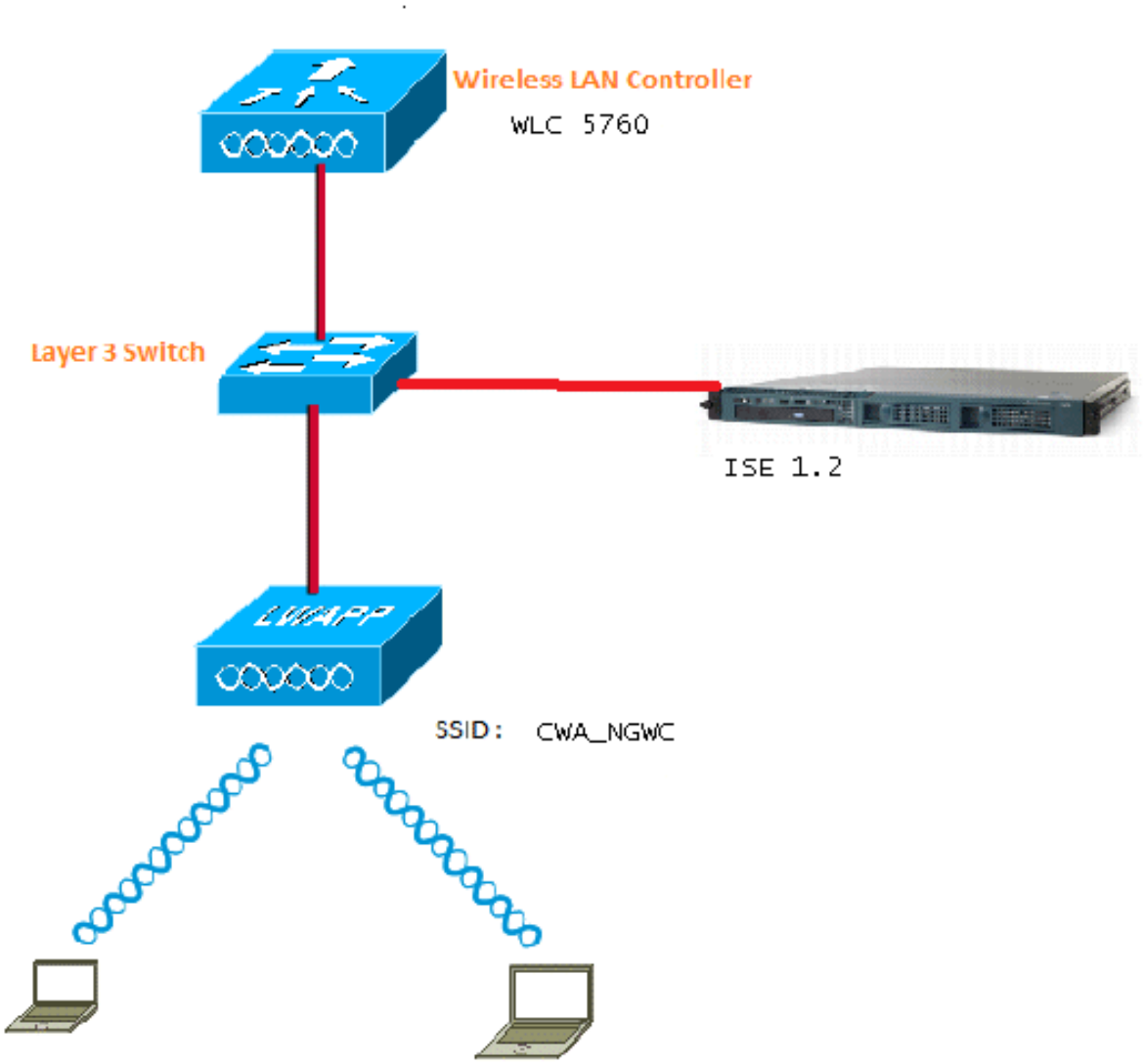
Der Fluss umfasst folgende Schritte:

1. Der Benutzer wird mit dem Service Set Identifier (SSID) für die Webauthentifizierung verknüpft, der offen+makfilter ist und keine Layer-3-Sicherheit bietet.
2. Der Benutzer öffnet den Browser.
3. Der WLC leitet zum Gastportal um.
4. Der Benutzer authentifiziert sich im Portal.
5. Die ISE sendet eine RADIUS-Autorisierungsänderung (CoA - UDP-Port 1700), um dem Controller die Gültigkeit des Benutzers anzuzeigen. Anschließend werden RADIUS-Attribute wie die Zugriffskontrollliste (Access Control List, ACL) übertragen.
6. Der Benutzer wird aufgefordert, die ursprüngliche URL erneut zu versuchen.

Cisco verwendet für die zentrale Webauthentifizierung (CWA) drei verschiedene Bereitstellungsszenarien, die alle Szenarien abdecken.

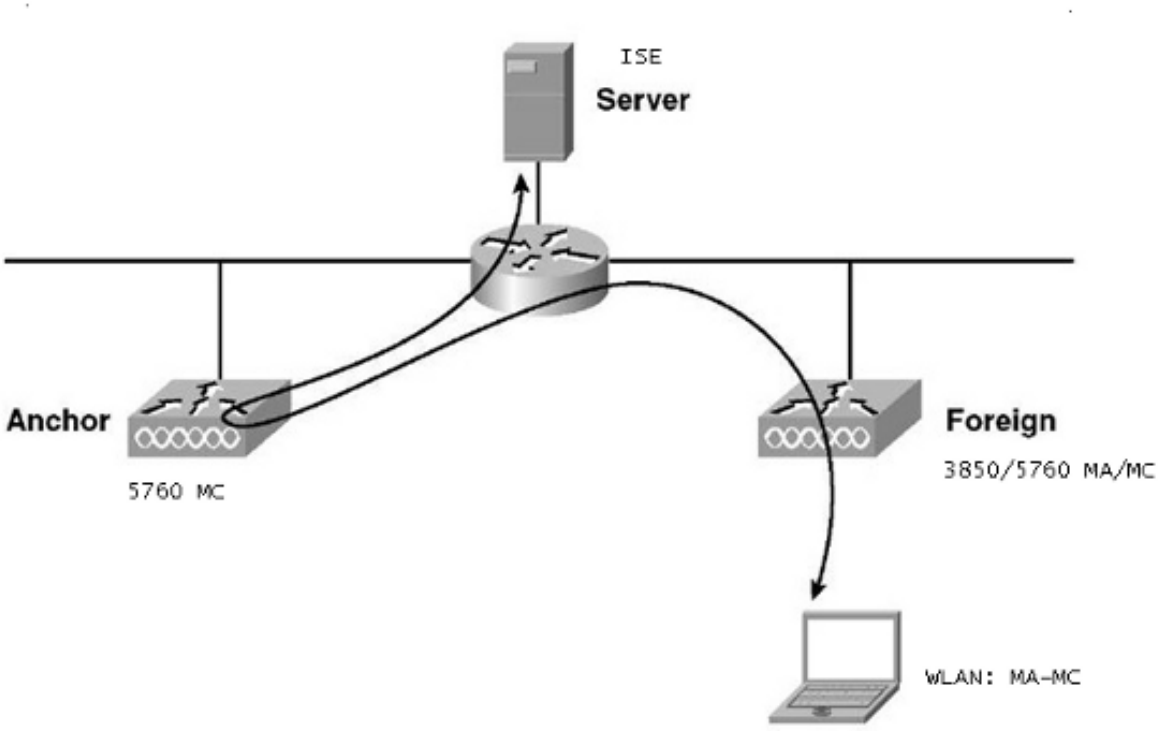
Topologie 1

Der 5760 WLC agiert als eigenständiger WLC, und die Access Points enden am selben 5760 WLC. Die Clients sind mit dem Wireless LAN (WLAN) verbunden und werden bei der ISE authentifiziert.



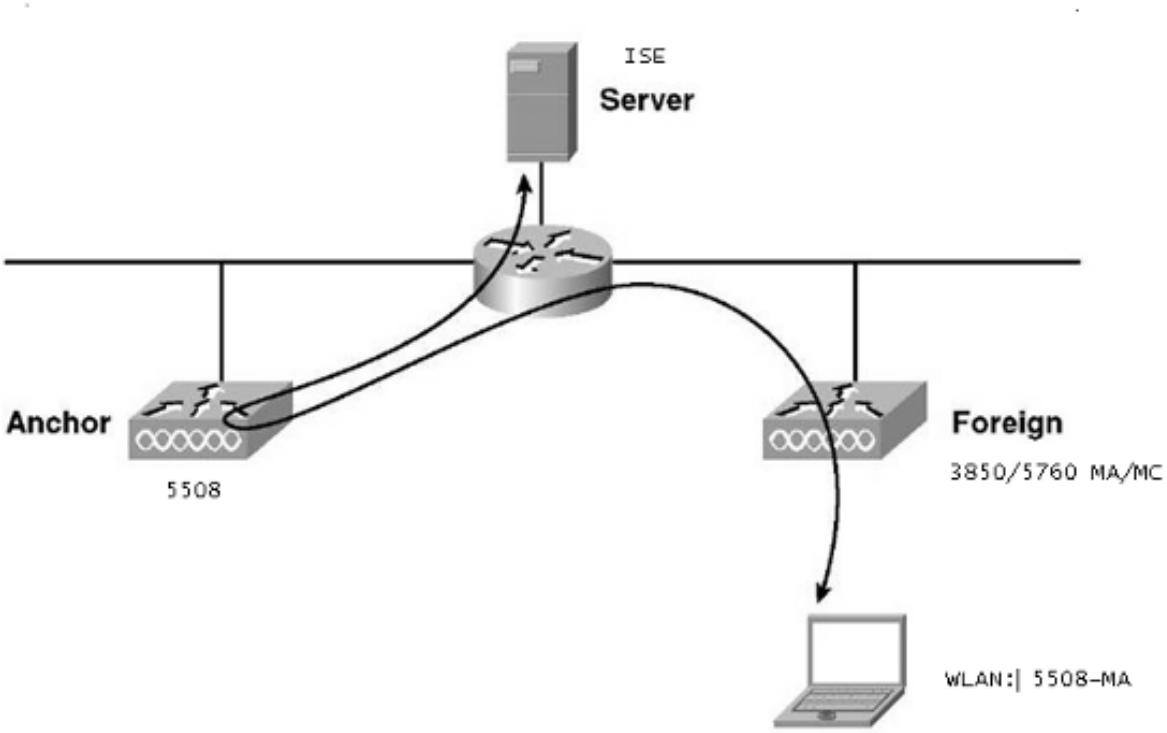
Topologie 2

Gastverankerung zwischen dem Converged Access WLC, wobei der eine als Mobility Controller und der andere als Mobility Agent fungiert Der Mobility Agent ist der ausländische WLC und der Mobility Controller der Anker.



Topologie 3

Gastverankerung zwischen dem Cisco Unified WLC 5508 und dem Converged Access WLC 5760/3850, wobei der eine als Mobility Controller und der andere als Mobility Agent fungiert Der Mobility Agent/Mobility Controller ist der ausländische WLC und der Mobility Controller 5508 der Anker.



Hinweis: In vielen Bereitstellungen ist Anchor der Mobility Controller und der Foreign WLC der Mobility Agent, der die Lizenz von einem anderen Mobility Controller bezieht. In diesem Fall hat der ausländische WLC nur einen Anker, und dieser Anker ist derjenige, der die Politik vorantreibt. Die doppelte Verankerung wird nicht unterstützt und funktioniert nicht, da von ihr nicht erwartet wird, dass sie auf diese Weise funktioniert.

Beispiel

Der WLC 5508 fungiert als Anker und der WLC 5760 als Mobility Controller für einen 3850 Switch, der als Mobility Agent fungiert. Für das Anker-Auslands-WLAN ist der WLC 5508 der Anker für das 3850-Auslands-WLAN. Auf dem WLC 5760 muss dieses WLAN gar nicht konfiguriert werden. Wenn Sie den 3850 Switch auf den 5760 Anchor und dann von diesem WLC 5760 auf den WLC 5508 als doppelten Anker zeigen, funktioniert das nicht, da dies zu doppelter Verankerung wird und die Richtlinien auf dem 5508 Anchor festgelegt sind.

Wenn Sie über eine Konfiguration verfügen, die einen WLC 5508 als Anker, einen WLC 5760 als Mobility Controller und einen 3850 Switch als Mobility Agent und einen ausländischen WLC umfasst, ist der Anker für den 3850-Switch zu jedem Zeitpunkt entweder der WLC 5760 oder der WLC C 5508 Es kann nicht gleichzeitig sein, und der doppelte Anker funktioniert nicht.

Konfigurationsbeispiel für Topologie 1

Netzwerkdiagramm und Erläuterung finden Sie in Topologie 1.

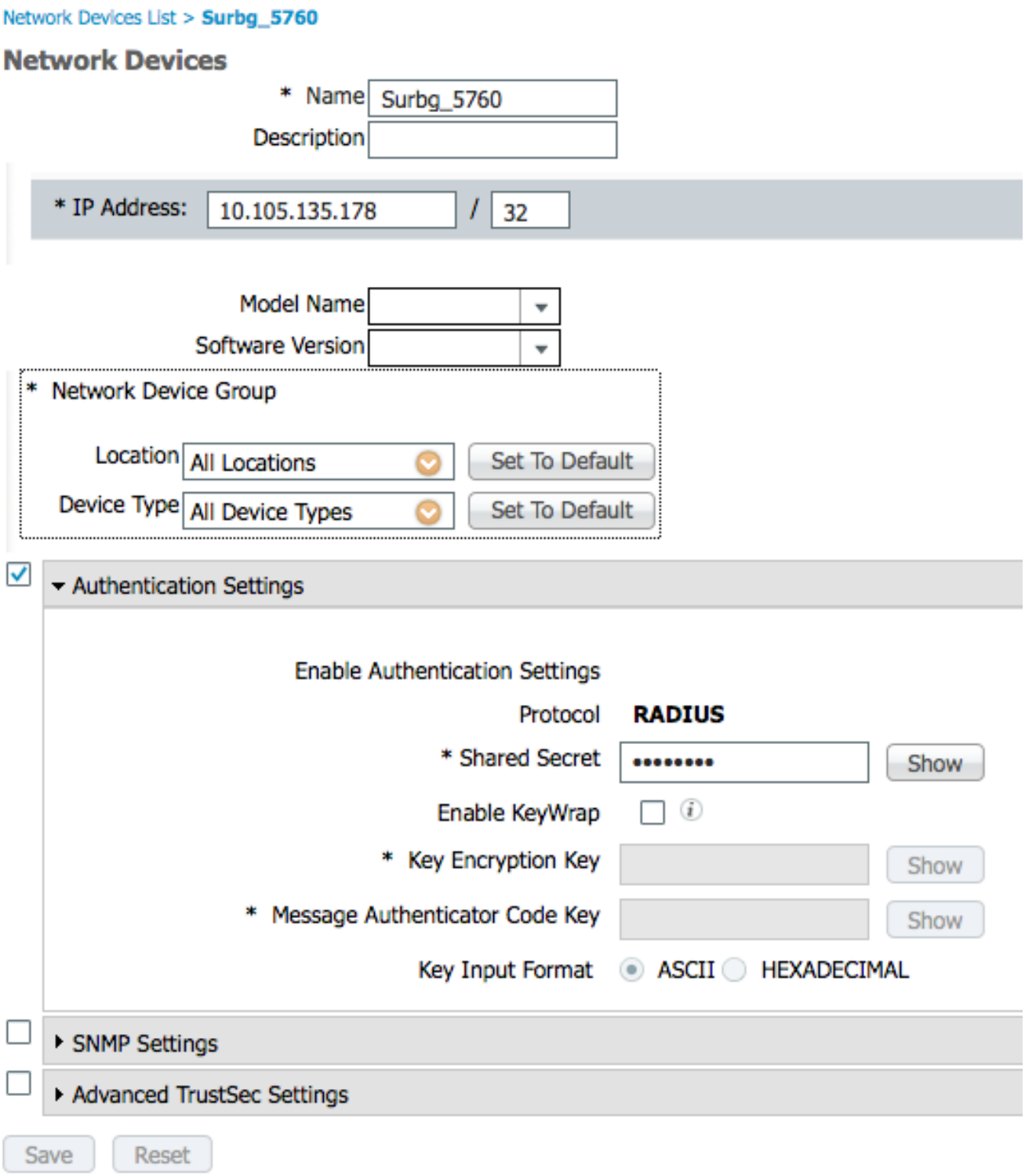
Die Konfiguration erfolgt in zwei Schritten:

1. Konfiguration auf der ISE.
2. Konfiguration auf dem WLC

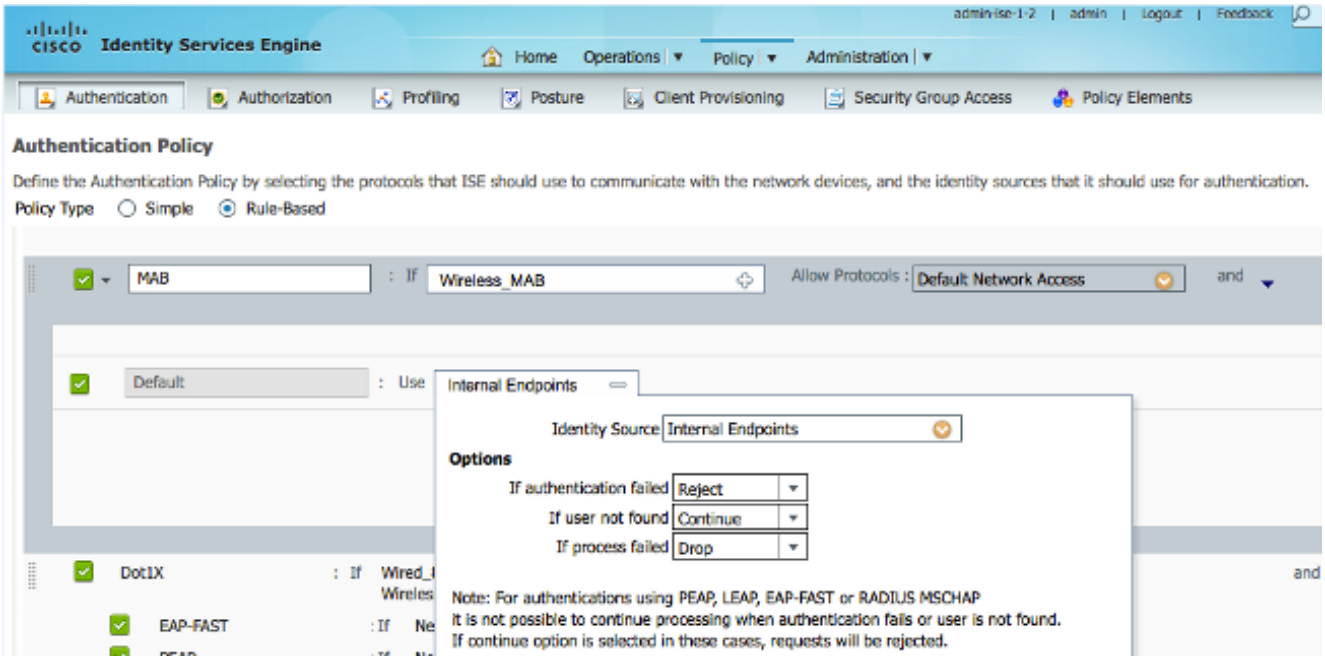
Der WLC 5760 fungiert als Standalone-WLC, und die Benutzer werden über die ISE authentifiziert.

Konfiguration auf der ISE

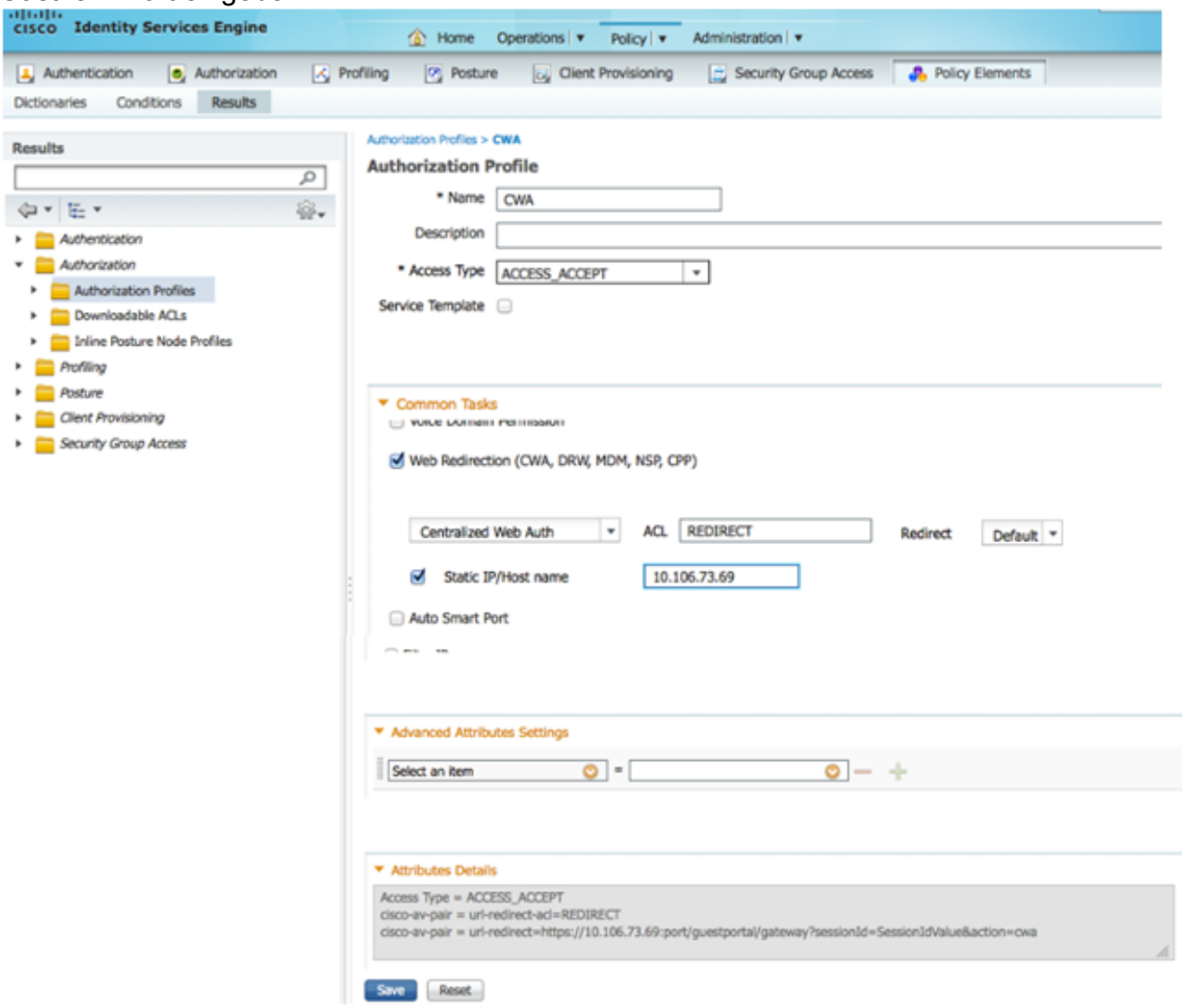
1. Wählen Sie **ISE GUI > Administration > Network Resource > Network Devices List > Add aus,** um den WLC als AAA-Client (Authentication, Authorization, and Accounting) zur ISE hinzuzufügen. Stellen Sie sicher, dass Sie auf dem WLC denselben gemeinsamen geheimen Schlüssel eingeben, der auf dem RADIUS-Server hinzugefügt wurde. **Hinweis**: Während Sie Anchor-Foreign bereitstellen, müssen Sie nur den Foreign WLC hinzufügen. Der Anker-WLC muss nicht der ISE als AAA-Client hinzugefügt werden. Dieselbe ISE-Konfiguration wird für alle anderen Bereitstellungsszenarien in diesem Dokument verwendet.



2. Wählen Sie in der ISE-GUI **Policy > Authentication > MAB > Edit** aus, um die Authentifizierungsrichtlinie zu erstellen. Die Authentifizierungsrichtlinie akzeptiert die MAC-Adresse des Clients, die auf interne Endpunkte verweist. Wählen Sie in der Liste Optionen folgende Optionen aus:Wählen Sie in der Dropdown-Liste Bei fehlgeschlagener Authentifizierung die Option **Ablehnen aus**.Wählen Sie in der Dropdown-Liste If user not found (Benutzer nicht gefunden) die Option **Continue (Weiter)**.Wählen Sie in der Dropdown-Liste Wenn der Prozess fehlgeschlagen ist die Option **Löschen aus**.Wenn Sie diese Optionen konfigurieren, wird der Client, bei dem die MAC-Autorisierung fehlschlägt, mit dem Gastportal
fortgefahren.

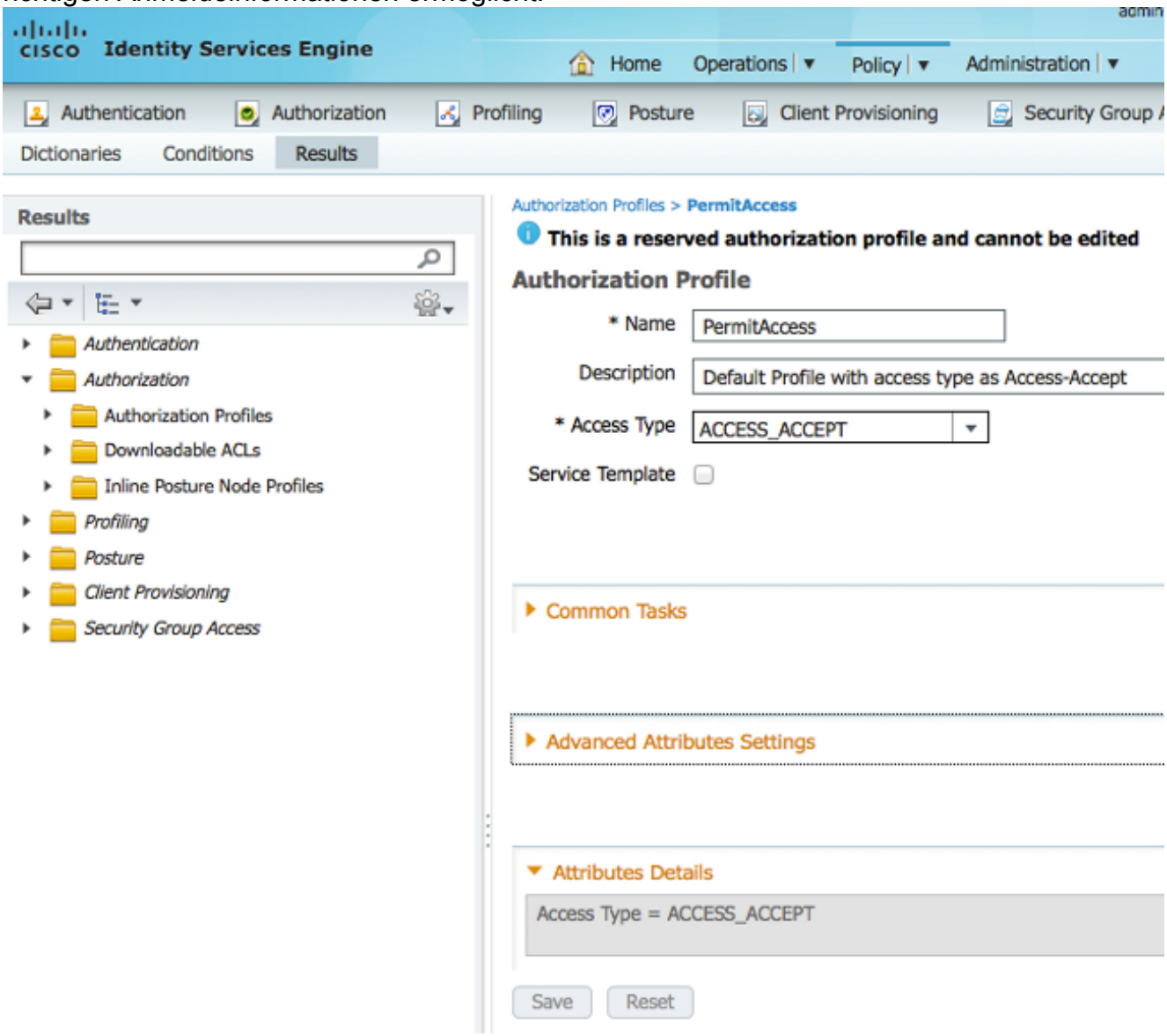


3. Wählen Sie in der ISE-GUI **Policy > Authorization > Results > Authorization Profiles > Add**. Geben Sie die Details ein, und klicken Sie auf **Speichern**, um das Autorisierungsprofil zu erstellen. Dieses Profil unterstützt die Clients dabei, nach der MAC-Authentifizierung zur Umleitungs-URL umgeleitet zu werden, über die die Clients den Gastbenutzernamen/das Gastkennwort eingeben.

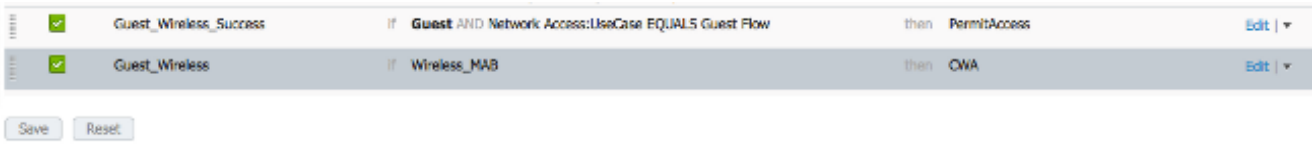


4. Wählen Sie in der ISE-GUI **Policy > Authorization > Results > Authorization Profiles > Add**

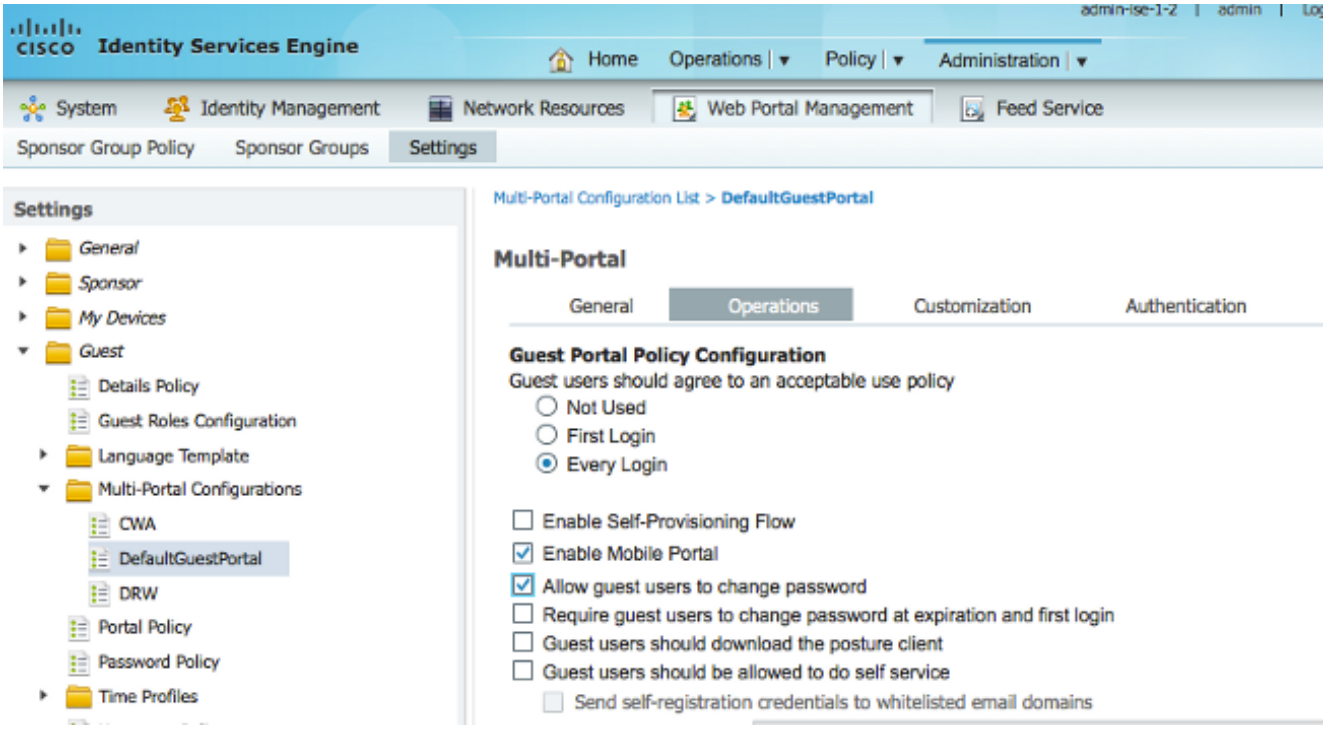
aus, um ein weiteres Autorisierungsprofil zu erstellen, das den Benutzern den Zugriff mit den richtigen Anmeldeinformationen ermöglicht.



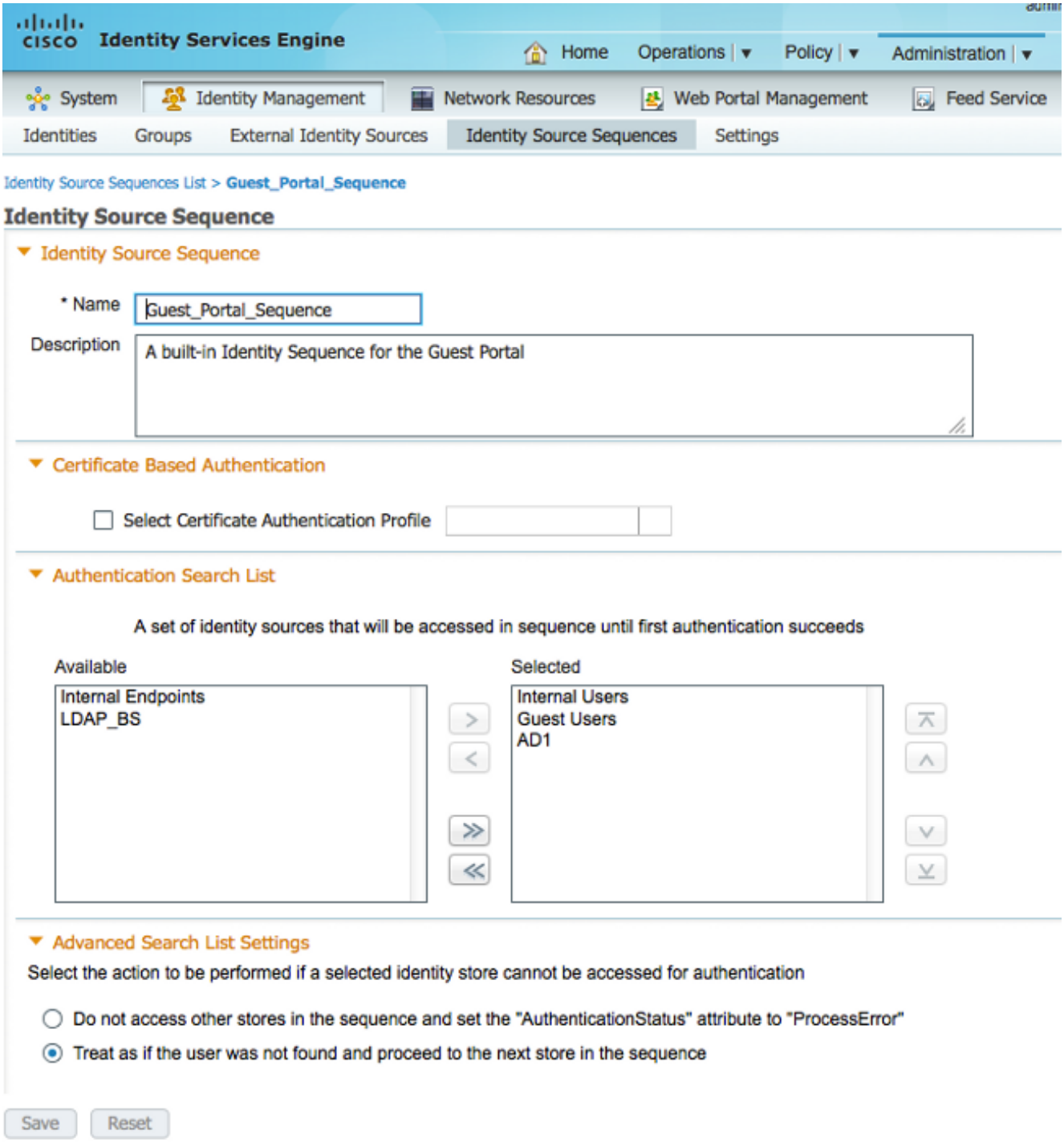
5. Erstellen der Autorisierungsrichtlinien Die Autorisierungsrichtlinie "Guest_Wireless" überträgt die URL für die Umleitung und die ACL für die Umleitung an die Clientsitzung. Das Profil, das hier verschoben wird, ist der CWA, wie zuvor gezeigt.Die Autorisierungsrichtlinie "Guest_Wireless-Success" gewährt vollständigen Zugriff auf einen Gastbenutzer, der über das Gastportal erfolgreich authentifiziert wurde. Nachdem der Benutzer im Gastportal erfolgreich authentifiziert wurde, sendet der WLC eine dynamische Autorisierung. Dadurch wird die Client-Sitzung mit dem Attribut 'Network Access:Use EQUALS Guest Flow' erneut authentifiziert.Die endgültigen Autorisierungsrichtlinien sehen wie folgt aus:



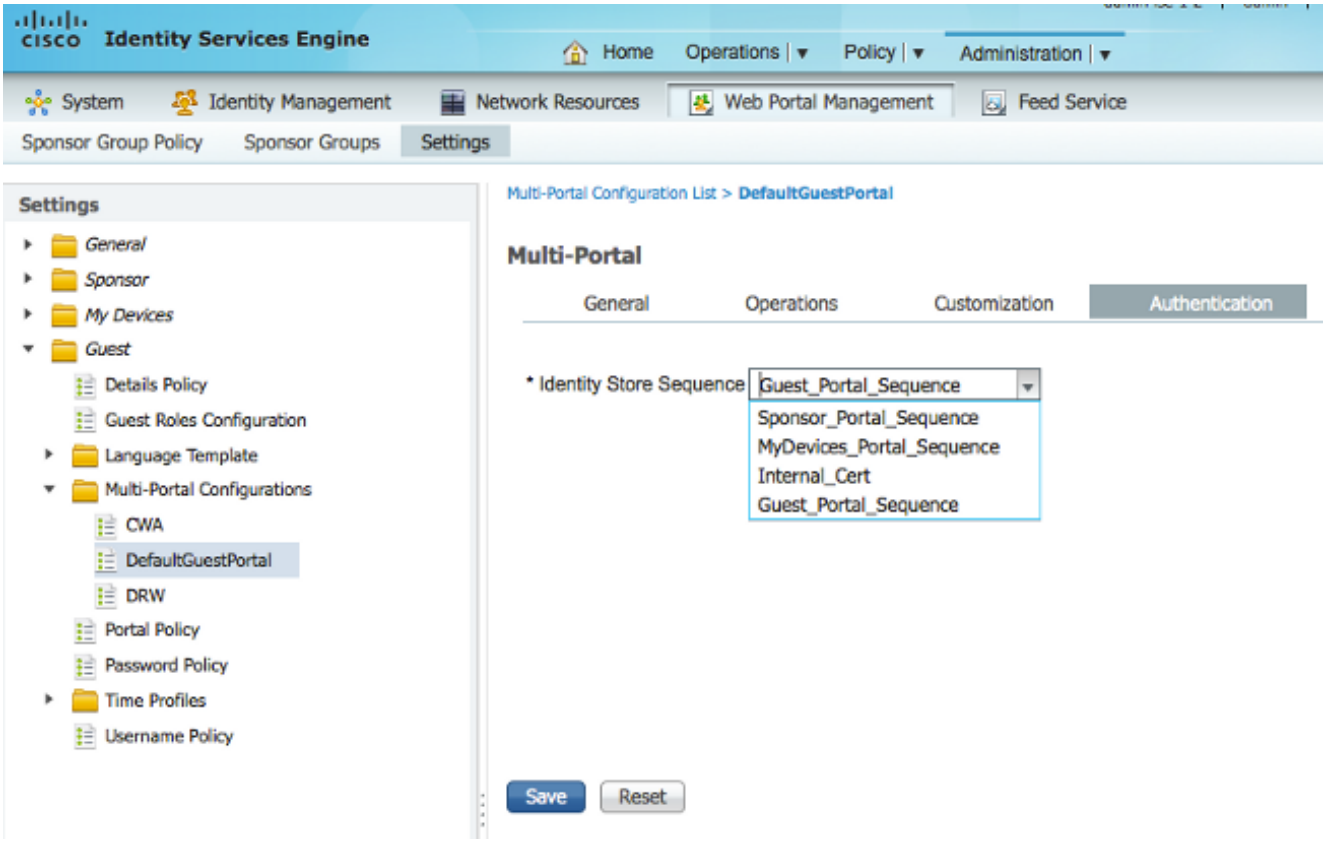
6. Optional: In diesem Fall werden standardmäßige Multiportal-Konfigurationen verwendet. Abhängig von den Anforderungen kann dasselbe in der GUI geändert werden. Wählen Sie in der ISE-GUI **Administration > Web Portal management > Multi Portal Configurations > DefaultGuestPortal**
aus.



Die Guest_Portal_sequence wird erstellt, die die internen, Guest- und AD-Benutzer unterstützt.



7. Wählen Sie in der ISE-GUI **Guest > Multi-Portal Configurations > DefaultGuestPortal aus**. Wählen Sie in der Dropdown-Liste Identify Store Sequence (Speichersequenz identifizieren) die Option **Guest_Portal_Sequence aus**.



Konfiguration auf dem WLC

1. Definieren Sie den ISE Radius-Server auf dem WLC 5760.
2. Konfigurieren des RADIUS-Servers, der Servergruppe und der Methodenliste mithilfe der 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. Konfigurieren des WLAN mithilfe der CLI

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

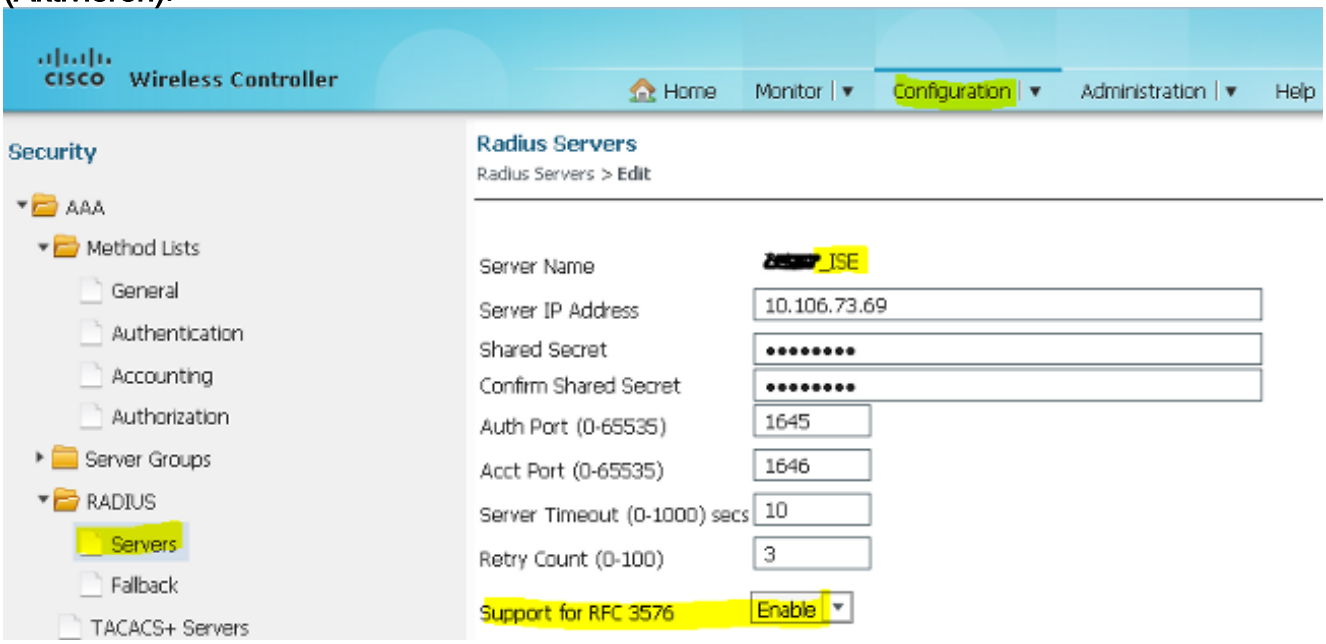
```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

4. Konfigurieren der Umleitungszugriffskontrolllisten mithilfe der CLI Hierbei handelt es sich um die URL-Umleitungs-ACL, die von der ISE als AAA-Überschreibung zurückgegeben wird, zusammen mit der Umleitungs-URL für die Gastportal-Umleitung. Es handelt sich um eine direkte ACL, die derzeit auf der Unified Architecture verwendet wird. Hierbei handelt es sich um eine Punkt-ACL, eine Art umgekehrte ACL, die Sie normalerweise für eine einheitliche Architektur verwenden würden. Sie müssen den Zugriff auf DHCP, den DHCP-Server, DNS, den DNS-Server und den ISE-Server blockieren. Geben Sie nur www, 443 und 8443 nach Bedarf ein. Dieses ISE-Gastportal verwendet den Port 8443, und die Umleitung funktioniert weiterhin mit der hier gezeigten ACL. Hier ist ICMP aktiviert, aber basierend auf den Sicherheitsregeln können Sie es entweder ablehnen oder zulassen.

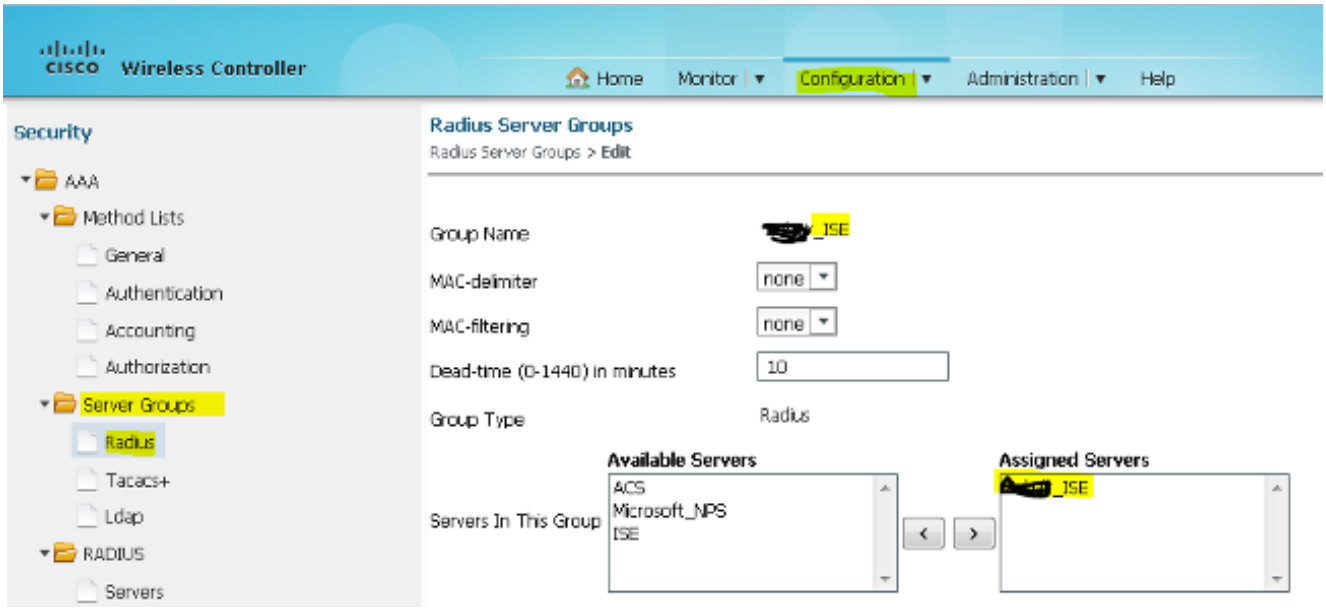
```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

Vorsicht: Wenn Sie HTTPS aktivieren, kann dies aufgrund der Skalierbarkeit zu hohen CPU-Problemen führen. Aktivieren Sie diese Option nur, wenn sie vom Cisco Designteam empfohlen wird.

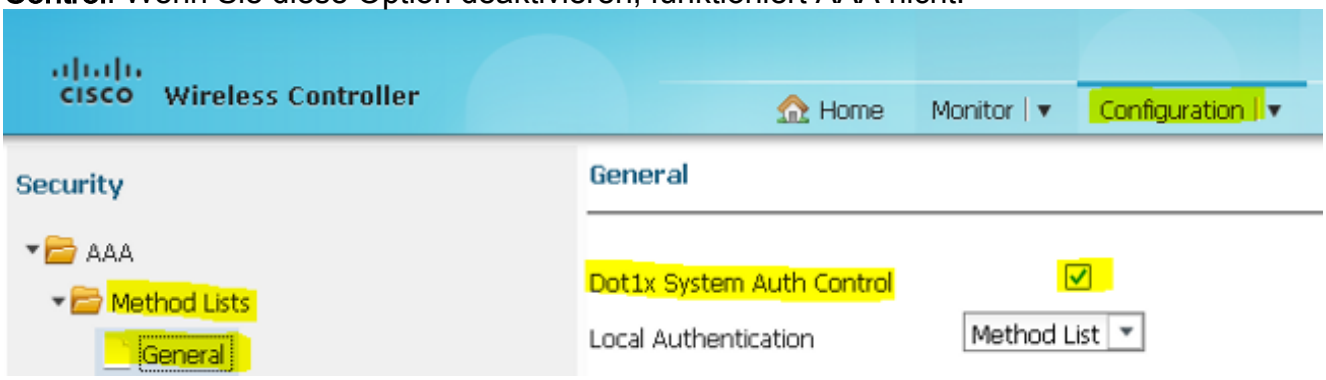
5. Wählen Sie in der Wireless Controller-GUI **AAA > RADIUS > Servers (AAA > RADIUS > Server) aus**. Konfigurieren des RADIUS-Servers, der Servergruppe und der Methodenliste in der GUI Füllen Sie alle Parameter aus, und stellen Sie sicher, dass der hier konfigurierte Shared Secret mit dem auf der ISE für dieses Gerät konfigurierten übereinstimmt. Wählen Sie in der Dropdown-Liste Support für RFC 3576 die Option **Enable (Aktivieren)**.



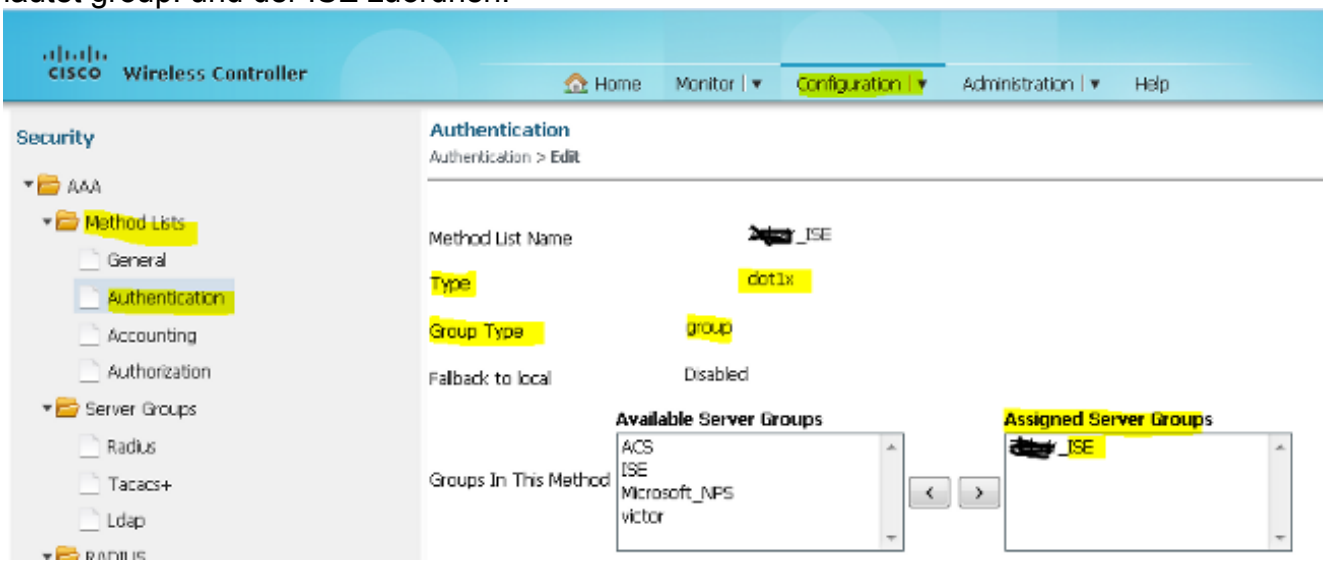
6. Wählen Sie in der Wireless Controller-GUI **AAA > Server Groups > Radius aus**. Fügen Sie den zuvor erstellten RADIUS-Server den Servergruppen hinzu.



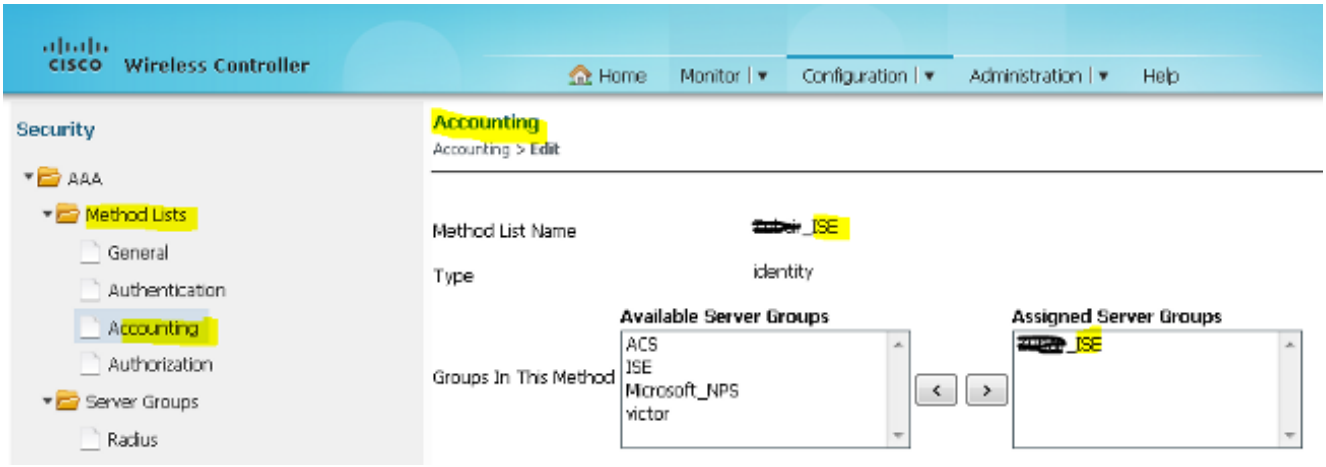
7. Wählen Sie in der Wireless Controller-GUI **AAA > Method Lists > General (AAA > Methodenlisten > Allgemein)**. Aktivieren Sie das Kontrollkästchen **Dot1x System Auth Control**. Wenn Sie diese Option deaktivieren, funktioniert AAA nicht.



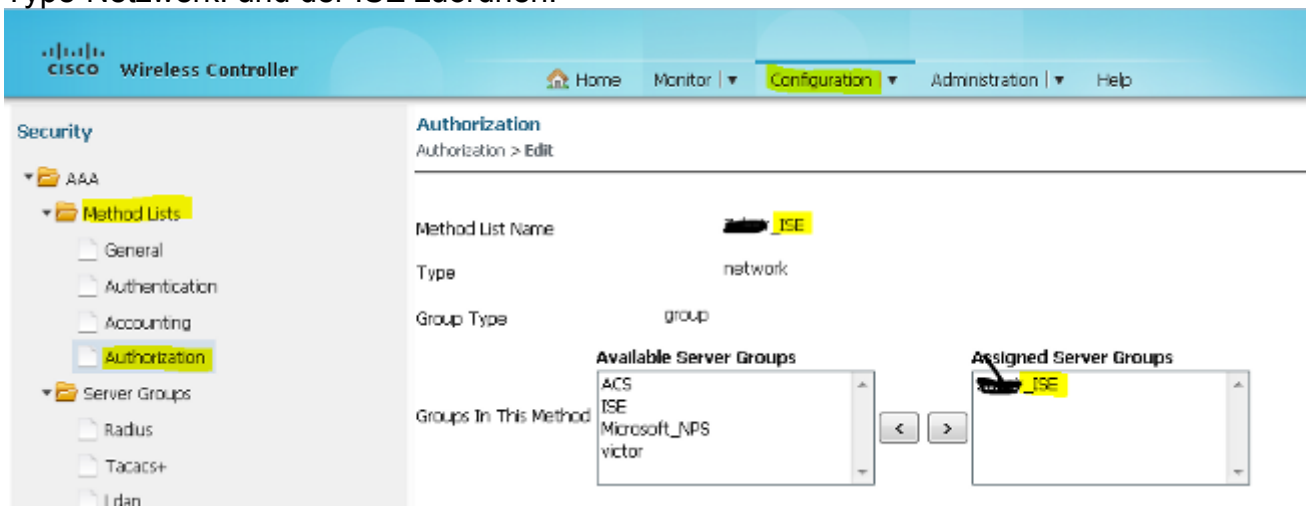
8. Wählen Sie in der Wireless Controller-GUI **AAA > Method Lists > Authentication aus**. Erstellen Sie eine Liste der Authentifizierungsmethoden für den Typ dot1X. Der Gruppentyp lautet group. und der ISE zuordnen.



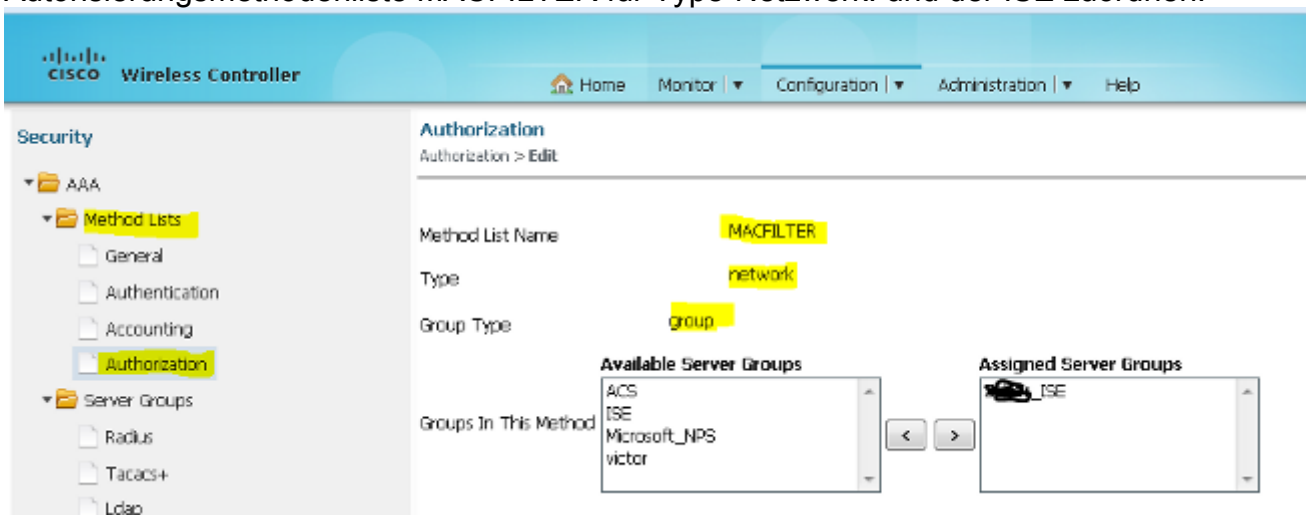
9. Wählen Sie in der Wireless Controller-GUI **AAA > Method Lists > Accounting aus**. Erstellen Sie eine Buchungsmethodenliste für die Typidentität. und der ISE zuordnen.



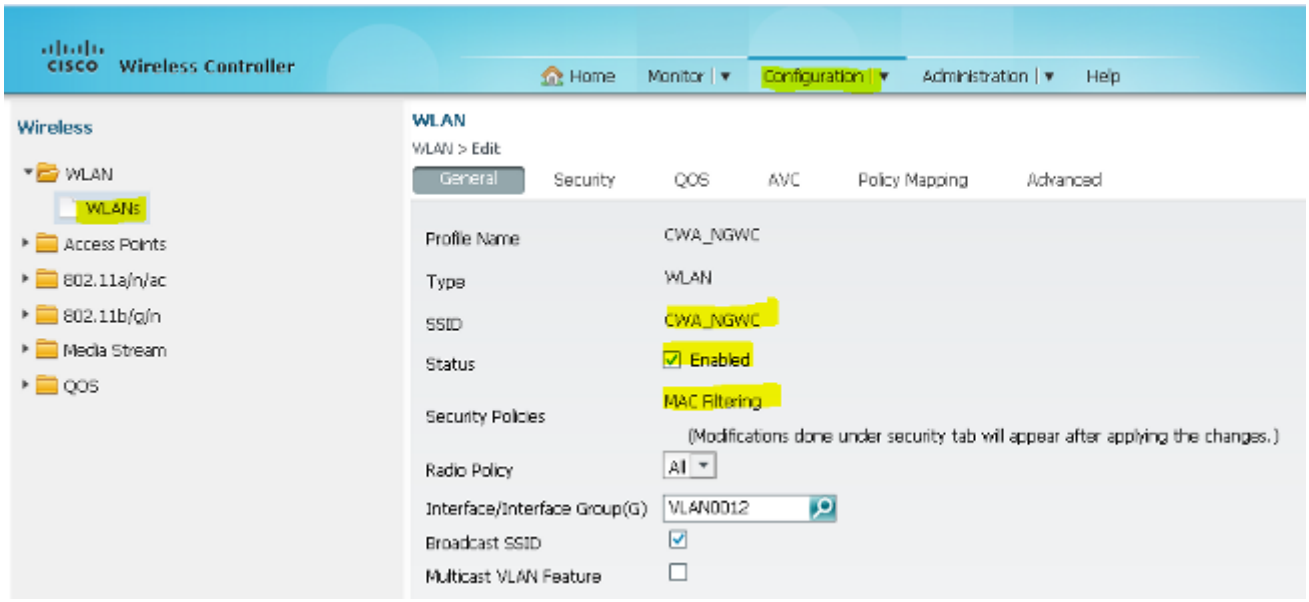
10. Wählen Sie in der Wireless Controller-GUI **AAA > Method Lists > Authorization (AAA > Methodenlisten > Autorisierung)**. Erstellen Sie eine Liste der Autorisierungsmethoden für Type-Netzwerk. und der ISE zuordnen.



11. Optional, da es auch MAC für die Fehlerunterstützung gibt. Erstellen Sie eine Autorisierungsmethodenliste MACFILTER für Type-Netzwerk. und der ISE zuordnen.

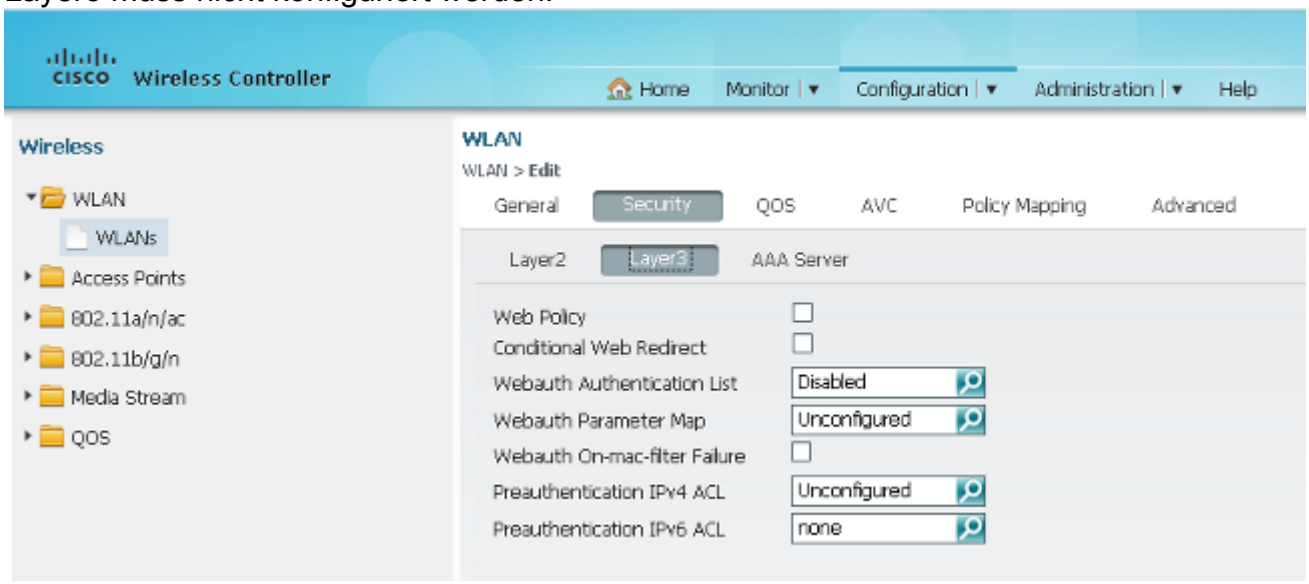


12. Wählen Sie in der Wireless Controller-GUI **WLAN > WLANs aus**. Erstellen Sie eine neue Konfiguration mit den hier gezeigten Parametern.

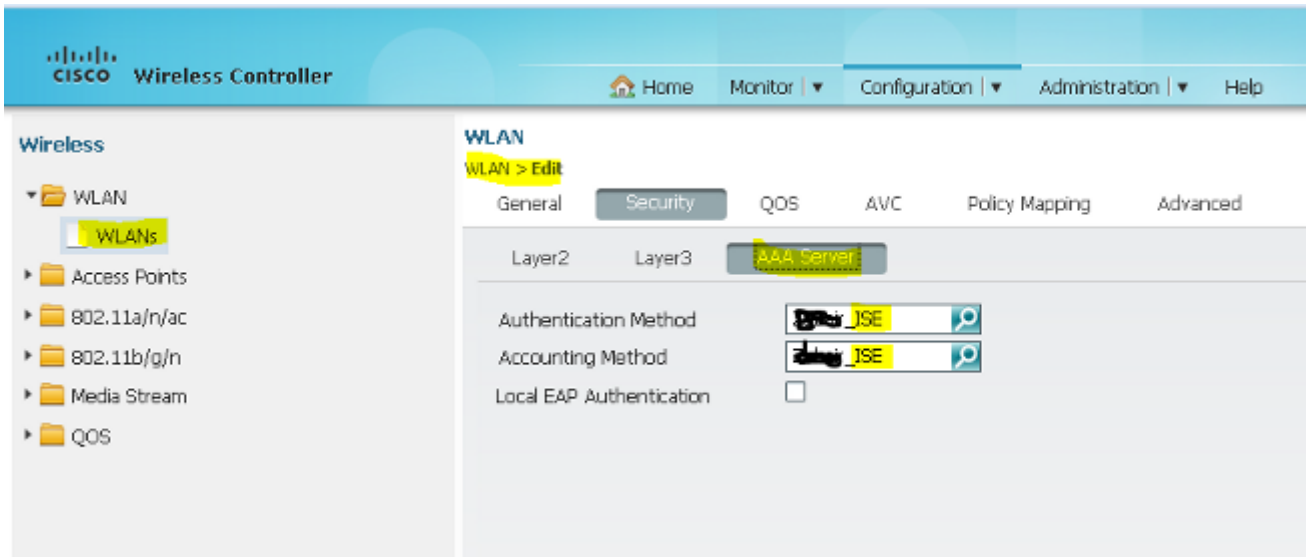


13. Wählen Sie **Security > Layer2 aus**. Geben Sie in das Feld MAC Filtering (MAC-Filterung) **MACFILTER ein**.

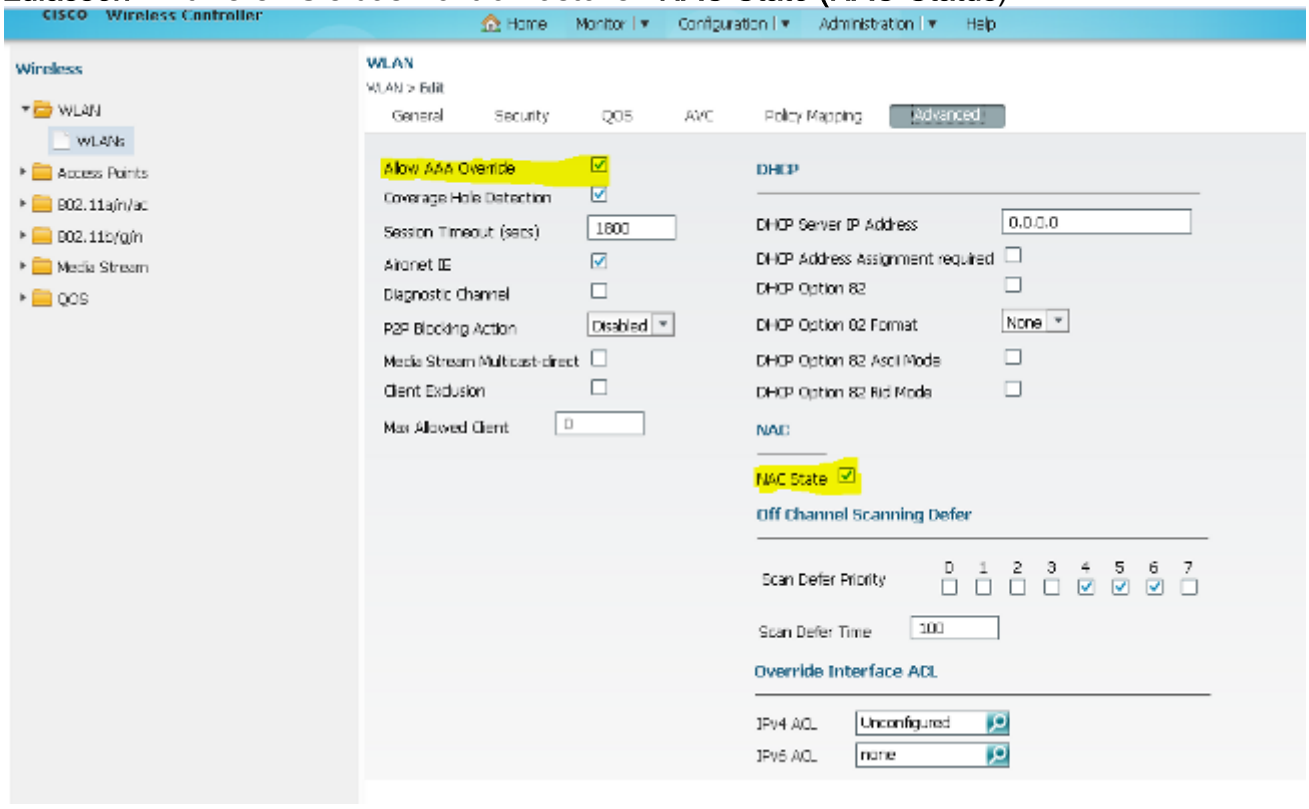
14. Layer3 muss nicht konfiguriert werden.



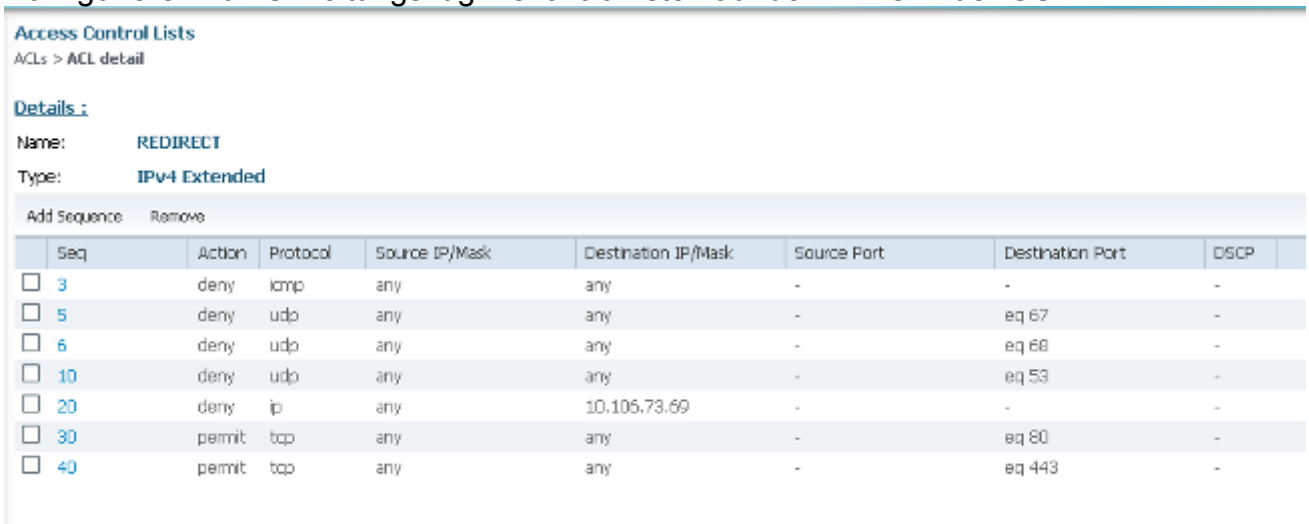
15. Wählen Sie **Security > AAA Server aus**. Wählen Sie in der Dropdown-Liste "Authentication Method" die Option **ISE aus**. Wählen Sie in der Dropdown-Liste "Accounting Method" die Option **ISE aus**.



16. Wählen Sie **Erweitert aus**. Aktivieren Sie das Kontrollkästchen **AAA-Außerkraftsetzung zulassen**. Aktivieren Sie das Kontrollkästchen **NAC State (NAC-Status)**.



17. Konfigurieren von Umleitungszugriffskontrolllisten auf dem WLC in der 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	-

Konfigurationsbeispiel für Topologie 2

Netzwerkdiagramm und Erläuterung finden Sie in Topologie 2.

Diese Konfiguration ist ebenfalls ein zweistufiger Prozess.

Konfiguration auf der ISE

Die Konfiguration auf der ISE ist mit der Konfiguration in Topologie 1 identisch.

Es ist nicht erforderlich, den Anker-Controller zur ISE hinzuzufügen. Sie müssen lediglich den ausländischen WLC zur ISE hinzufügen, den RADIUS-Server auf dem ausländischen WLC definieren und die Autorisierungsrichtlinie unter dem WLAN zuordnen. Auf dem Anker müssen Sie nur die MAC-Filterung aktivieren.

In diesem Konfigurationsbeispiel gibt es zwei WLC 5760-Geräte, die als Anchor Foreign (ausländischer Anker) agieren. Wenn Sie den WLC 5760 als Anker und den 3850 Switch als Anchor Foreign, den Mobility Agent, für einen anderen Mobility Controller verwenden möchten, ist dieselbe Konfiguration richtig. Es ist jedoch nicht erforderlich, das WLAN auf dem zweiten Mobility Controller zu konfigurieren, von dem der Switch der Serie 3850 die Lizenzen bezieht. Sie müssen lediglich den 3850 Switch auf den WLC 5760 verweisen, der als Anker fungiert.

Konfiguration auf dem WLC

1. Konfigurieren Sie auf dem Foreign-Server den ISE-Server mit der AAA-Methodenliste für AAA, und ordnen Sie das WLAN einer MAC-Filterautorisierung zu. **Hinweis**: Konfigurieren Sie die Umleitungszugriffskontrollliste auf Anker- und Fremd- sowie auf MAC-Filterung.

```
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. Konfigurieren von Umleitungszugriffskontrolllisten mithilfe der CLI Hierbei handelt es sich um die URL-Umleitungs-ACL, die von der ISE als AAA-Überschreibung zurückgegeben wird, zusammen mit der Umleitungs-URL für die Gastportal-Umleitung. Es handelt sich um eine direkte ACL, die derzeit auf der Unified Architecture verwendet wird. Hierbei handelt es sich um eine Punkt-ACL, eine Art umgekehrte ACL, die Sie normalerweise für eine einheitliche Architektur verwenden würden. Sie müssen den Zugriff auf DHCP, den DHCP-Server, DNS, den DNS-Server und den ISE-Server blockieren. Geben Sie nur www, 443 und 8443 nach Bedarf ein. Dieses ISE-Gastportal verwendet den Port 8443, und die Umleitung funktioniert weiterhin mit der hier gezeigten ACL. Hier ist ICMP aktiviert, aber basierend auf den Sicherheitsregeln können Sie es entweder ablehnen oder zulassen.

```
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
```

   Vorsicht: Wenn Sie HTTPS aktivieren, kann dies aufgrund der Skalierbarkeit zu hohen CPU-Problemen führen. Aktivieren Sie diese Option nur, wenn sie vom Cisco Designteam empfohlen wird.

3. Konfigurieren der Mobilität auf dem Anker

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

   Hinweis: Wenn Sie den gleichen Switch mit dem 3850 als Foreign (Fremd) konfigurieren, stellen Sie sicher, dass Sie die Switch-Peer-Gruppe auf dem Mobility Controller und umgekehrt auf dem Mobility Controller definieren. Konfigurieren Sie anschließend die oben genannten CWA-Konfigurationen auf dem 3850 Switch.

4. Konfiguration auf dem Anker. Auf dem Anker müssen keine ISE-Konfigurationen konfiguriert werden. Sie benötigen lediglich die WLAN-Konfiguration.

```
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. Konfigurieren der Mobilität auf dem Anker Definieren Sie den anderen WLC als Mobilitätsmitglied auf diesem WLC.

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

6. Konfigurieren von Umleitungszugriffskontrolllisten mithilfe der CLI Hierbei handelt es sich um

die URL-Umleitungs-ACL, die von der ISE als AAA-Überschreibung zurückgegeben wird, zusammen mit der Umleitungs-URL für die Gastportal-Umleitung. Es handelt sich um eine direkte ACL, die derzeit auf der Unified Architecture verwendet wird. Hierbei handelt es sich um eine Punkt-ACL, eine Art umgekehrte ACL, die Sie normalerweise für eine einheitliche Architektur verwenden würden. Sie müssen den Zugriff auf DHCP, den DHCP-Server, DNS, den DNS-Server und den ISE-Server blockieren. Geben Sie nur www, 443 und 8443 nach Bedarf ein. Dieses ISE-Gastportal verwendet den Port 8443, und die Umleitung funktioniert weiterhin mit der hier gezeigten ACL. Hier ist ICMP aktiviert, aber basierend auf den Sicherheitsregeln können Sie es entweder ablehnen oder zulassen.

```
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
```

Vorsicht: Wenn Sie HTTPS aktivieren, kann dies aufgrund der Skalierbarkeit zu hohen CPU-Problemen führen. Aktivieren Sie diese Option nur, wenn sie vom Cisco Designteam empfohlen wird.

Konfigurationsbeispiel für Topologie 3

Netzwerkdiagramm und Erläuterung finden Sie in Topologie 3.

Dies ist ebenfalls ein zweistufiger Prozess.

Konfiguration auf der ISE

Die Konfiguration auf der ISE ist mit der Konfiguration in Topologie 1 identisch.

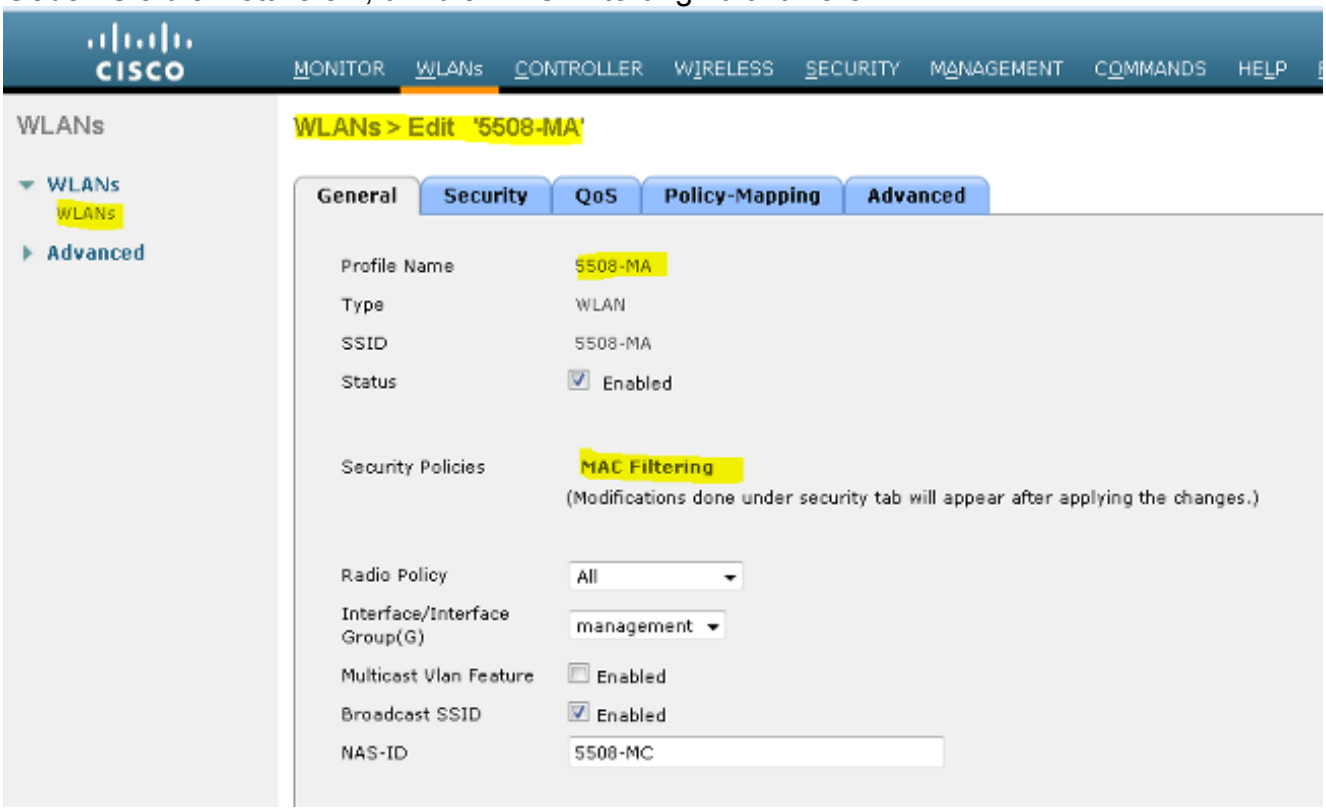
Es ist nicht erforderlich, den Anker-Controller zur ISE hinzuzufügen. Sie müssen lediglich den ausländischen WLC zur ISE hinzufügen, den RADIUS-Server auf dem ausländischen WLC definieren und die Autorisierungsrichtlinie unter dem WLAN zuordnen. Auf dem Anker müssen Sie nur die MAC-Filterung aktivieren.

In diesem Beispiel gibt es einen WLC 5508, der als Anker fungiert, und einen WLC 5760, der als ausländischer WLC fungiert. Wenn Sie einen WLC 5508 als Anker und einen Switch 3850 sowie einen Foreign WLC, einen Mobility Agent, für einen anderen Mobility Controller verwenden möchten, ist dieselbe Konfiguration richtig. Es ist jedoch nicht erforderlich, das WLAN auf dem zweiten Mobility Controller zu konfigurieren, von dem der Switch der Serie 3850 die Lizenzen bezieht. Sie müssen lediglich den 3850 Switch auf den 5508 WLC verweisen, der als Anker fungiert.

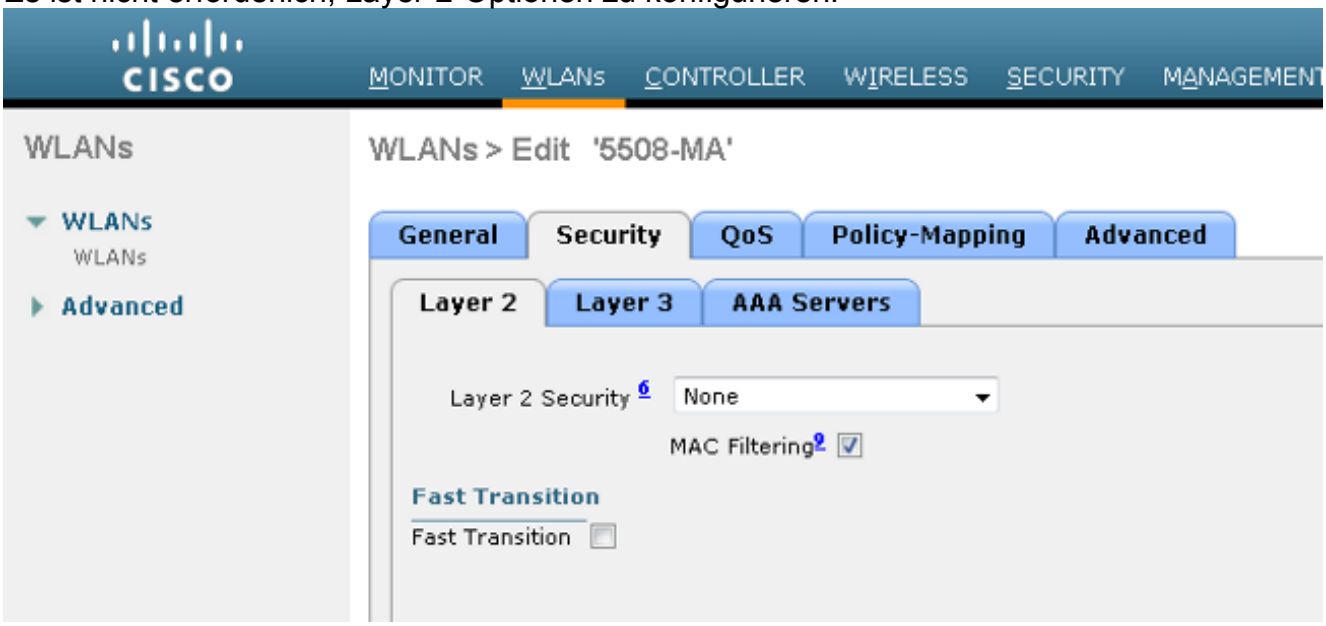
Konfiguration auf dem WLC

1. Konfigurieren Sie auf dem ausländischen WLC den ISE-Server mit der AAA-Methodenliste für AAA, und ordnen Sie das WLAN einer MAC-Filterautorisierung zu. Dies ist für den Anker nicht erforderlich. **Hinweis:** Konfigurieren Sie die Umleitungszugriffskontrollliste auf dem Anker- und Fremd-WLC sowie auf der MAC-Filterung.
2. Wählen Sie in der WLC 5508-GUI **WLANs > New** aus, um den Anchor 5508 zu konfigurieren.

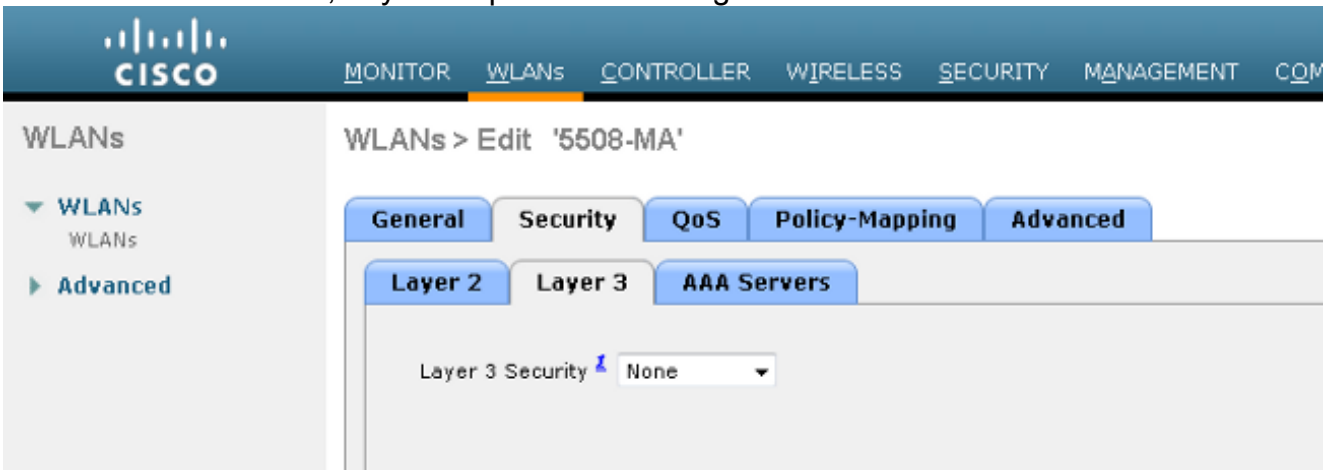
Geben Sie die Details ein, um die MAC-Filterung zu aktivieren.



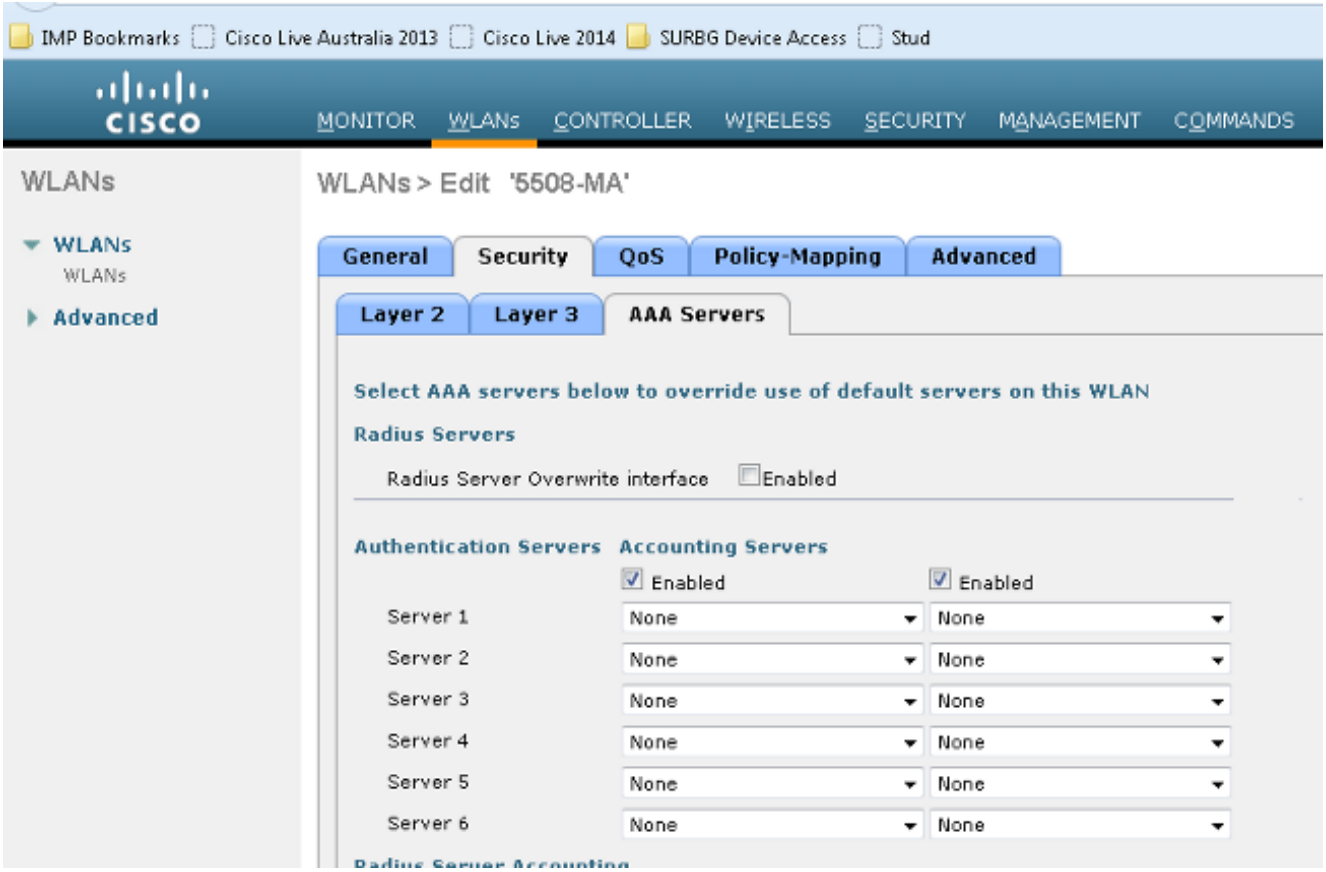
3. Es ist nicht erforderlich, Layer-2-Optionen zu konfigurieren.



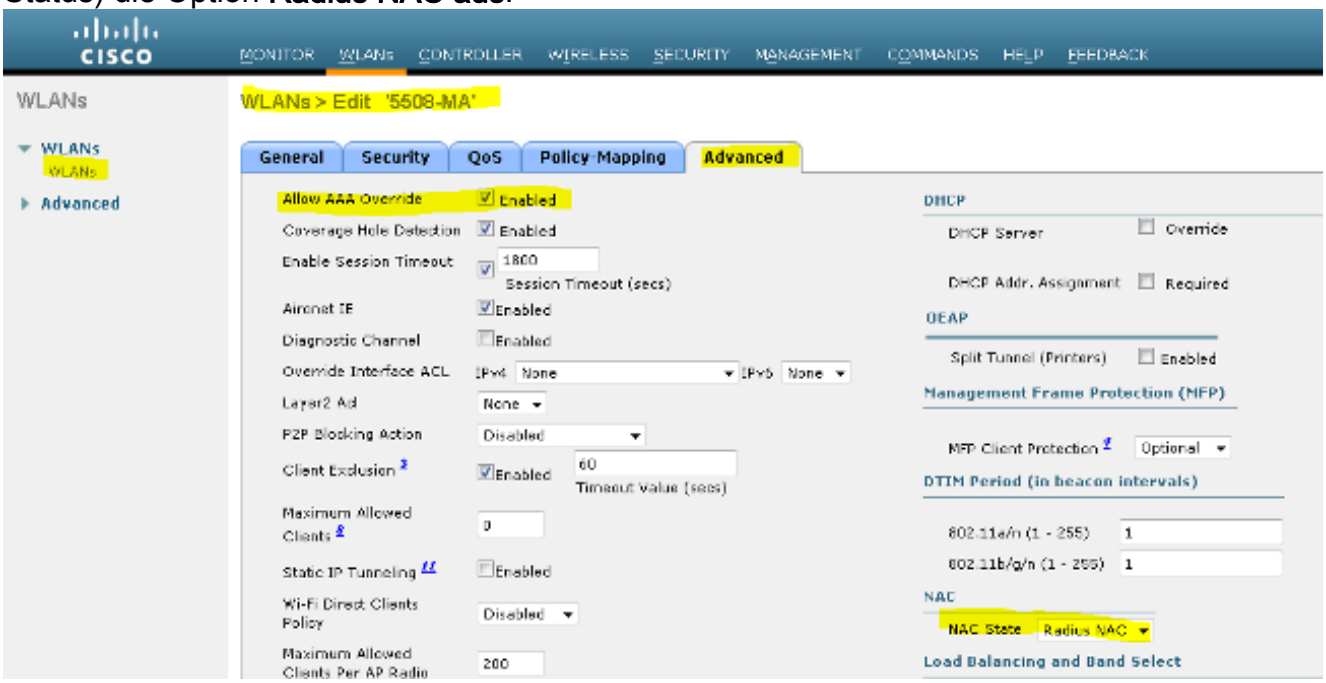
4. Es ist nicht erforderlich, Layer-3-Optionen zu konfigurieren.



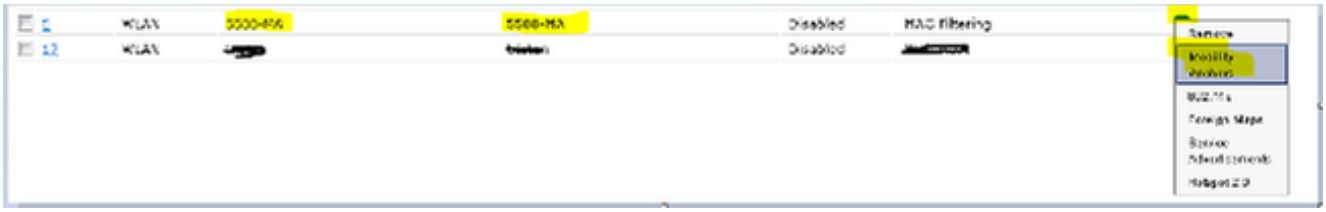
5. AAA-Server sollten im Anchor AireOS WLC deaktiviert werden, damit die CoA vom ausländischen NGWC verarbeitet werden kann. AAA-Server können im Anchor-WLC nur aktiviert werden, wenn keine RADIUS-Server konfiguriert sind unter: Security > AAA > RADIUS > Authentication



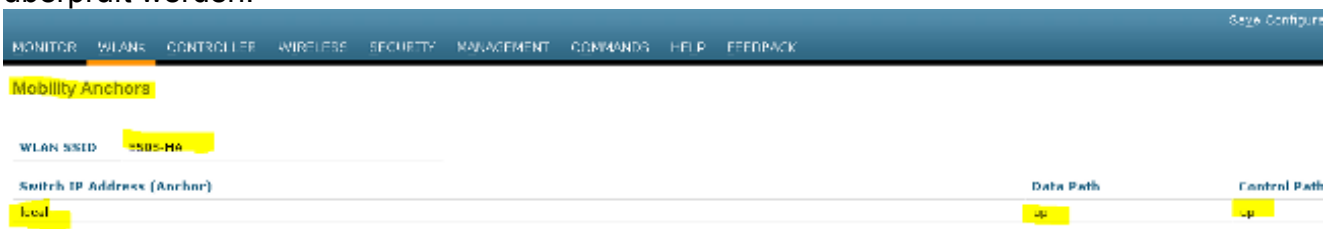
6. Wählen Sie **WLANs > WLANs > Edit > Advanced aus**. Aktivieren Sie das Kontrollkästchen **AAA-Außerkraftsetzung zulassen**. Wählen Sie in der Dropdown-Liste "NAC State" (NAC-Status) die Option **Radius NAC aus**.



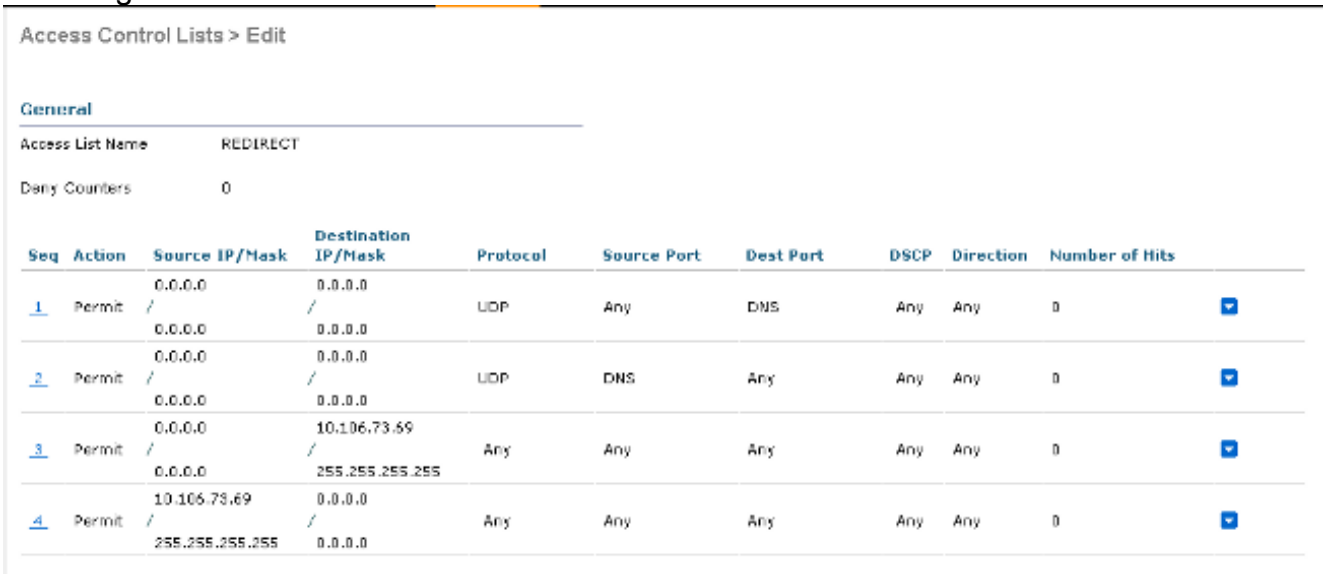
7. Fügen Sie dies als Auslöser für das WLAN hinzu.



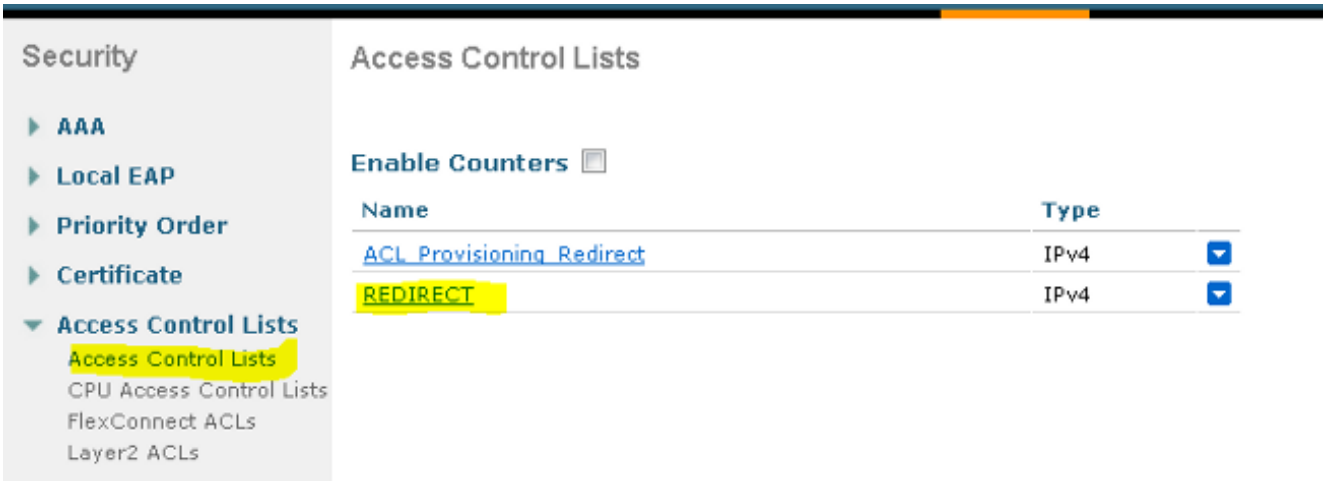
8. Nachdem auf "Lokal" gezeigt wurde, sollte dies mit "Control" und "Data Path UP/UP" überprüft werden.



9. Erstellen Sie die Umleitungszugriffskontrollliste auf dem WLC. Dadurch werden DHCP und DNS abgelehnt. Er lässt HTTP/HTTPs zu.



So sieht es aus, wenn die ACL erstellt wurde.



10. Definieren Sie den ISE RADIUS-Server auf dem WLC 5760.
11. Konfigurieren von RADIUS-Server, Servergruppe und Methodenliste mithilfe der 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. Konfigurieren des WLAN über die 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. Definieren Sie den anderen WLC als Mobilitätsmitglied auf diesem WLC.

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

Hinweis: Wenn Sie den gleichen Switch mit dem WLC 3850 als Foreign (Fremd) konfigurieren, stellen Sie sicher, dass Sie die Switch-Peer-Gruppe auf dem Mobility Controller und umgekehrt auf dem Mobility Controller definieren. Konfigurieren Sie anschließend die vorherigen CWA-Konfigurationen auf dem WLC 3850.

14. Konfigurieren von Umleitungszugriffskontrolllisten mithilfe der CLI Hierbei handelt es sich um die URL-Umleitungs-ACL, die von der ISE als AAA-Überschreibung zurückgegeben wird, zusammen mit der Umleitungs-URL für die Gastportal-Umleitung. Es handelt sich um eine direkte ACL, die derzeit auf der Unified Architecture verwendet wird. Hierbei handelt es sich um eine Punkt-ACL, eine Art umgekehrte ACL, die Sie normalerweise für eine einheitliche Architektur verwenden würden. Sie müssen den Zugriff auf DHCP, den DHCP-Server, DNS, den DNS-Server und den ISE-Server blockieren. Geben Sie nur www, 443 und 8443 nach Bedarf ein. Dieses ISE-Gastportal verwendet den Port 8443, und die Umleitung funktioniert weiterhin mit der hier gezeigten ACL. Hier ist ICMP aktiviert, aber basierend auf den Sicherheitsregeln können Sie es entweder ablehnen oder zulassen.

```
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
```

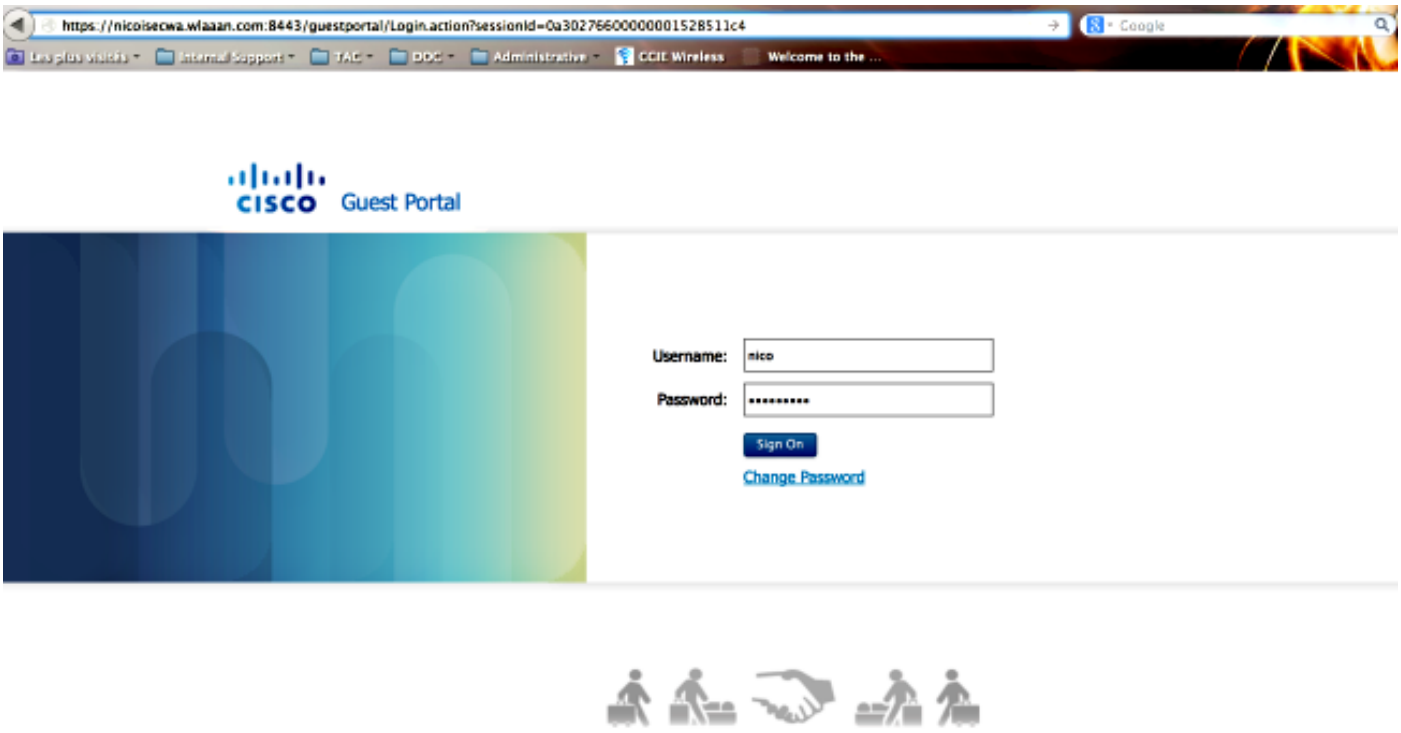
Vorsicht: Wenn Sie HTTPS aktivieren, kann dies aufgrund der Skalierbarkeit zu hohen CPU-Problemen führen. Aktivieren Sie diese Option nur, wenn sie vom Cisco Designteam empfohlen wird.

Überprüfung

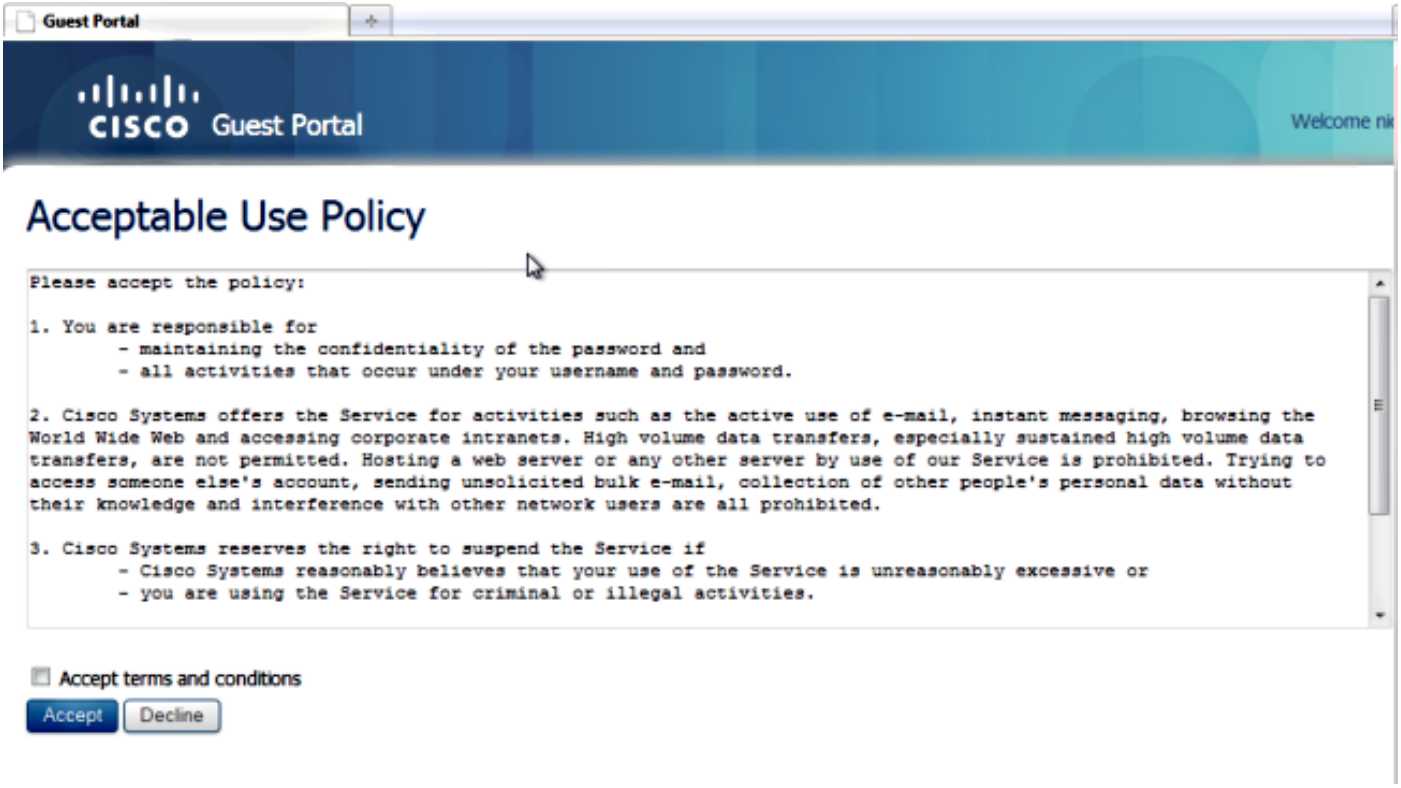
Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Verbinden des Clients mit der konfigurierten SSID Sobald Sie die IP-Adresse erhalten und der Client in den Status Web-Authentifizierung erforderlich wechselt, öffnen Sie den Browser. Geben Sie Ihre Client-Anmeldeinformationen im Portal ein.

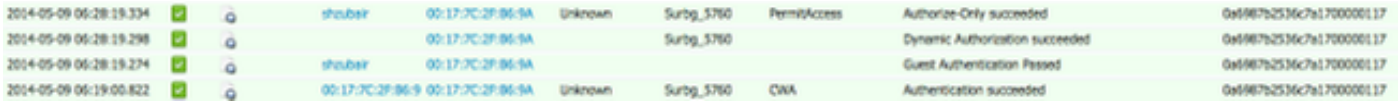


Aktivieren Sie nach erfolgreicher Authentifizierung das Kontrollkästchen **Geschäftsbedingungen akzeptieren**. Klicken Sie auf **Accept** (Akzeptieren).



Sie erhalten eine Bestätigungsmeldung und können nun auf das Internet zugreifen.

Auf der ISE sieht der Client-Fluss folgendermaßen aus:



Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Das Output Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Hinweis: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug-**Befehle verwenden.

Für den WLC mit konvergentem Zugriff wird empfohlen, Traces anstelle von Debugs auszuführen. Auf dem Aironet OS 5508 WLC müssen Sie nur den **Debug-Client <client mac>** eingeben und **den Web-Auth-Redirect-Enable-Mac <client mac>debuggen**.

```
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
```

Einige bekannte Fehler auf dem Cisco IOS-XE und dem Aironet OS sind in der Cisco Bug-ID CSCun3834 enthalten.

So sieht der erfolgreiche CWA-Flow auf den Traces aus:

```
[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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.