Exemplo de Configuração da Autenticação Central da Web no Acesso Convergente e no Acesso Unificado WLCs

Contents

Introduction

Este documento descreve como configurar a autenticação central da Web no controlador de LAN sem fio (WLC) de acesso convergido e também entre o WLC de acesso convergido e o Unified Access WLC (5760 e também entre 5760 e 5508).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Cisco WLC 5508, 5760, 3850
- Conhecimento básico do Identity Services Engine (ISE)
- Conhecimento básico de mobilidade sem fio
- Conhecimento básico de âncora de convidado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC 5760 com Cisco IOS® XE versão 3.3.3
- WLC 5508 que executa o Cisco Aironet OS versão 7.6
- Switch 3850 com Cisco IOS XE Release 3.3.3
- Cisco ISE que executa a versão 1.2

Configurar

> **Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.**

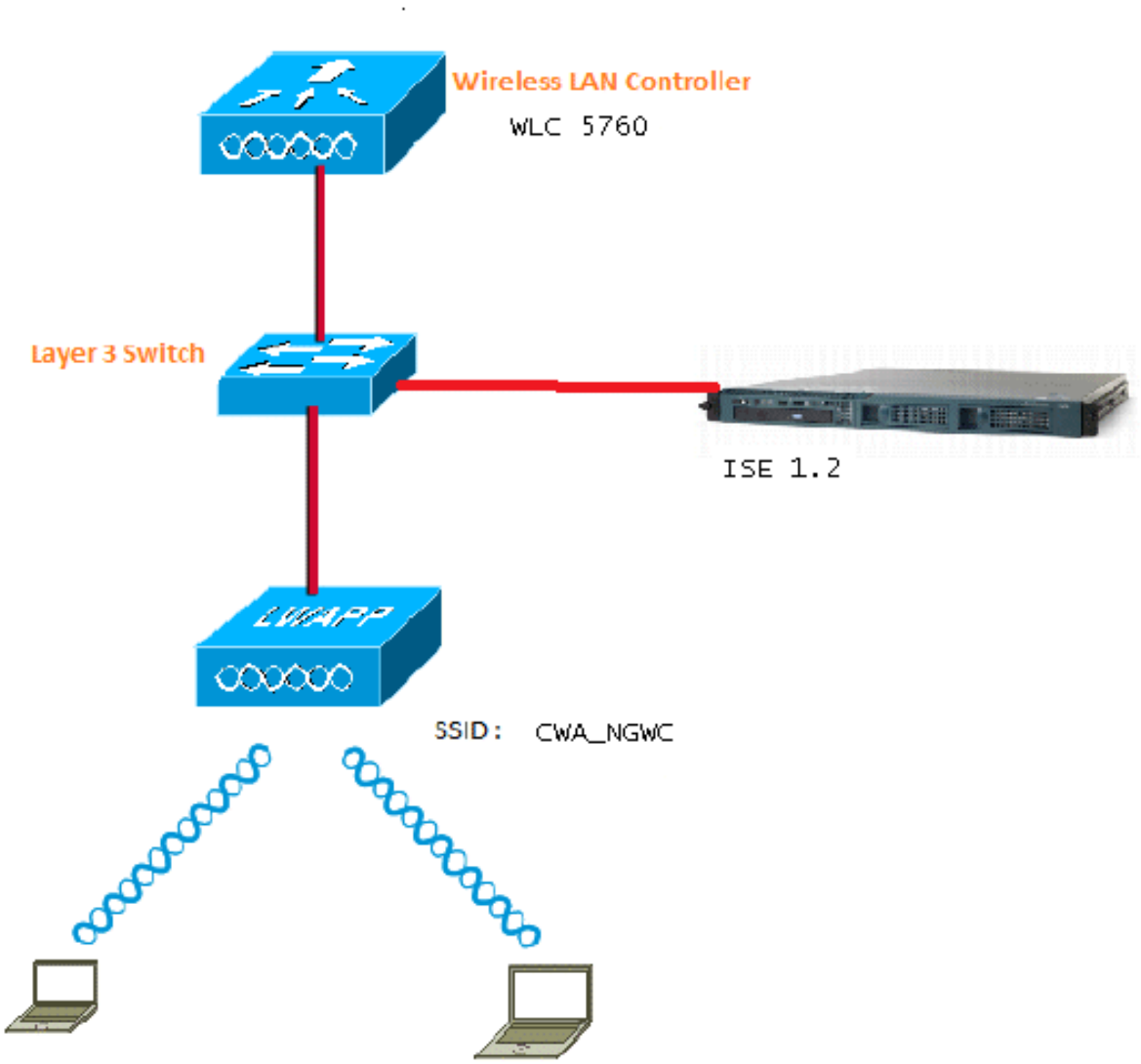
O fluxo inclui estas etapas:

1. O usuário se associa ao Service Set Identifier (SSID) de autenticação da Web, que é, na verdade, open+macfiltering e nenhuma segurança de Camada 3.
2. O usuário abre o navegador.
3. A WLC redireciona para o portal do convidado.
4. O usuário se autentica no portal.
5. O ISE envia uma Alteração de Autorização RADIUS (CoA - UDP Port 1700) para indicar ao controlador que o usuário é válido e, eventualmente, envia atributos RADIUS, como a Lista de Controle de Acesso (ACL).
6. O usuário é solicitado a tentar novamente a URL original.

A Cisco usa três configurações de implantação diferentes que cobrem todos os cenários diferentes para realizar a Autenticação da Web Central (CWA).

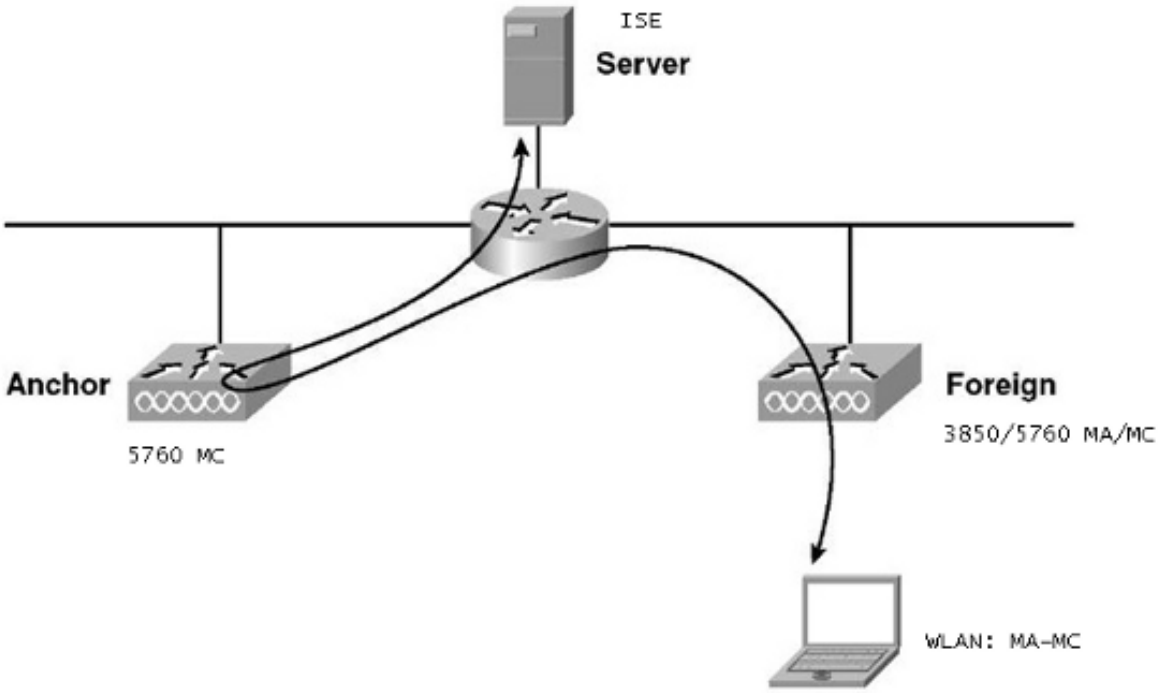
Topologia 1

A WLC 5760 atua como uma WLC autônoma e os access points terminam na mesma WLC 5760. Os clientes estão conectados à LAN sem fio (WLAN) e são autenticados no ISE.



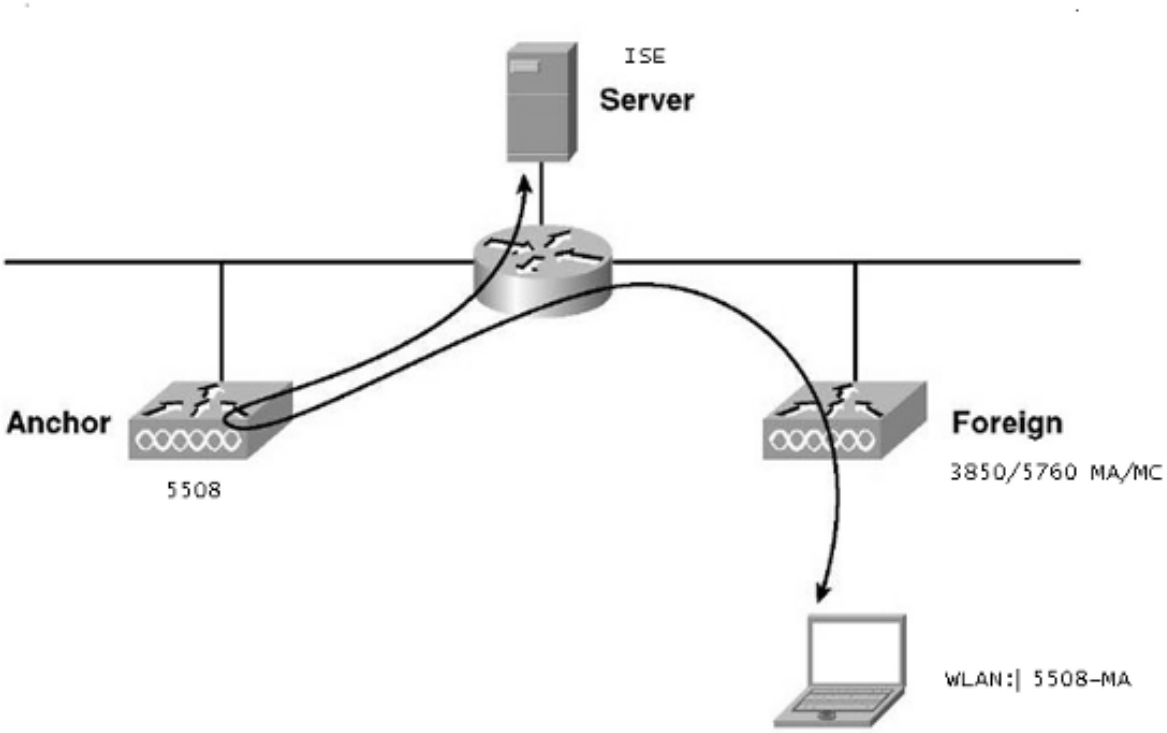
Topologia 2

Ancoragem de convidado entre a WLC de acesso convergente com uma que atua como um controlador de mobilidade e a outra que atua como um agente de mobilidade. O agente de mobilidade é a WLC externa e o controlador de mobilidade é a âncora.



Topologia 3

Ancoragem de convidado entre o Cisco Unified WLC 5508 e o Converged Access WLC 5760/3850 com um que atua como um controlador de mobilidade e o outro que atua como um agente de mobilidade. O agente de mobilidade/controlador de mobilidade é a WLC externa e o controlador de mobilidade 5508 é a âncora.



Observação: há muitas implantações em que o Anchor é o controlador de mobilidade e o WLC externo é o agente de mobilidade que obtém a licença de outro controlador de mobilidade. Nesse caso, a WLC externa tem apenas uma âncora e essa âncora é a que envia as políticas. A ancoragem dupla não é suportada e não funciona, pois não se espera que ela funcione dessa maneira.

Exemplo

A WLC 5508 atua como a Âncora e a WLC 5760 atua como o controlador de mobilidade para um Switch 3850 que atua como um agente de mobilidade. Para a WLAN externa de âncora, a WLC 5508 será a âncora para a WLAN externa 3850. Não há necessidade de configurar essa WLAN no WLC 5760. Se você apontar o Switch 3850 para a Âncora 5760 e, em seguida, desta WLC 5760 para a WLC 5508 como uma âncora dupla, ele não funcionará, pois isso se tornará uma âncora dupla e as políticas estarão na Âncora 5508.

Se você tiver uma configuração que inclua uma WLC 5508 como a Âncora, uma WLC 5760 como o controlador de mobilidade e um switch 3850 como o agente de mobilidade e uma WLC externa, a qualquer momento a Âncora do switch 3850 será a WLC 5760 ou a WLC 5508. Não pode ser o ao mesmo tempo e a âncora dupla não funciona.

Exemplo de configuração da topologia 1

Consulte a Topologia 1 para obter o diagrama e a explicação da rede.

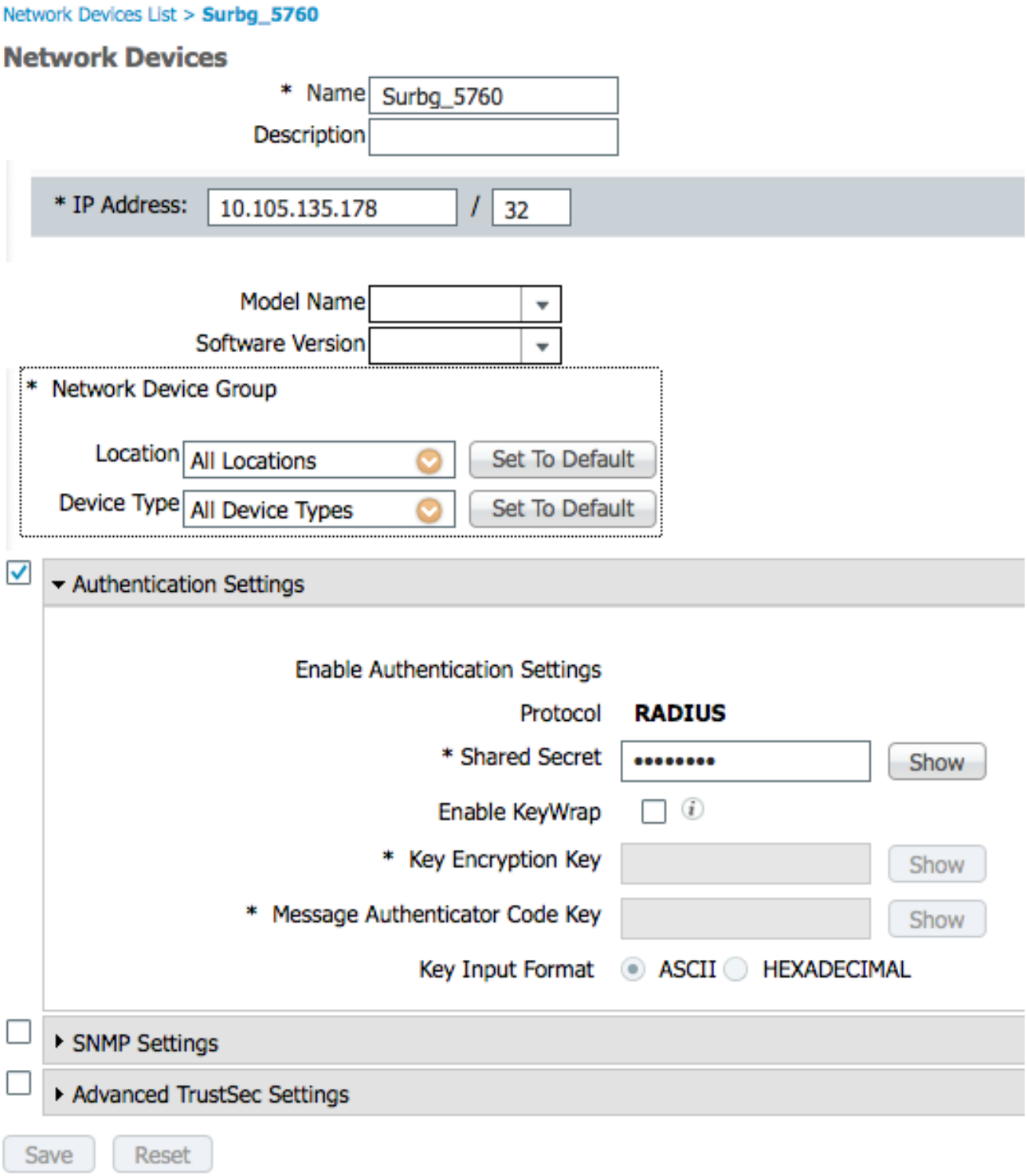
A configuração é um processo de duas etapas:

1. Configuração no ISE.
2. Configuração na WLC.

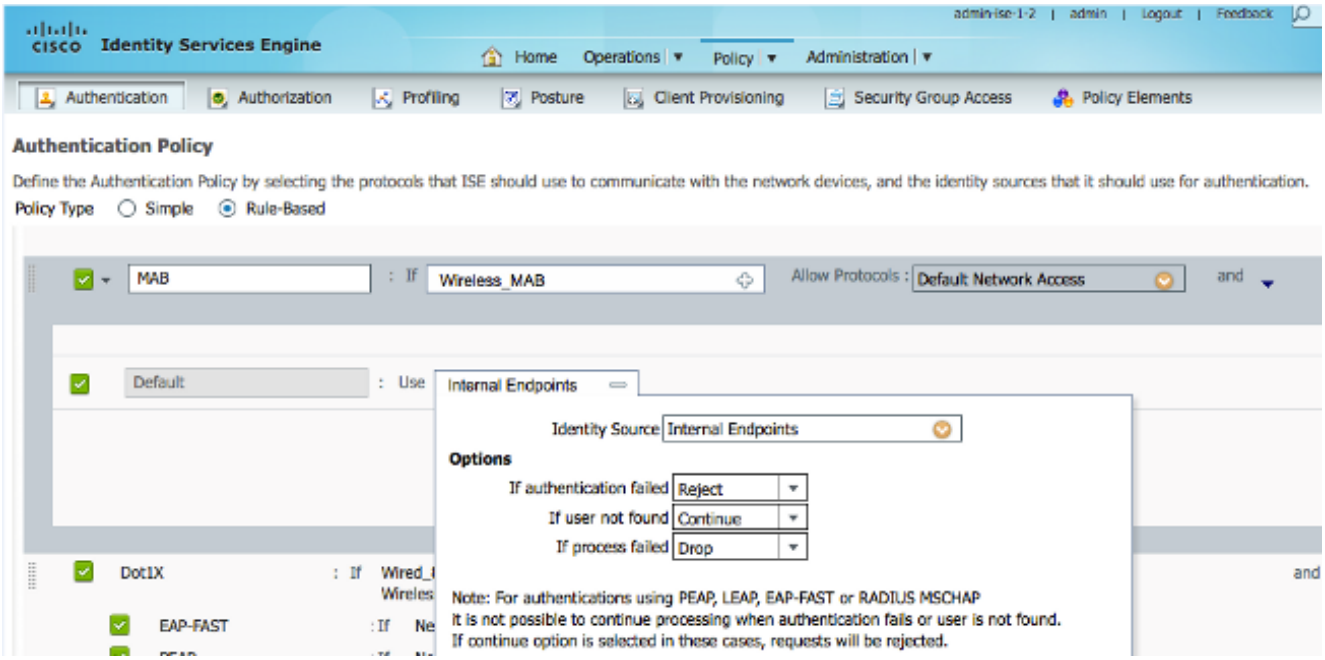
A WLC 5760 atua como uma WLC independente e os usuários são autenticados no ISE.

Configuração no ISE

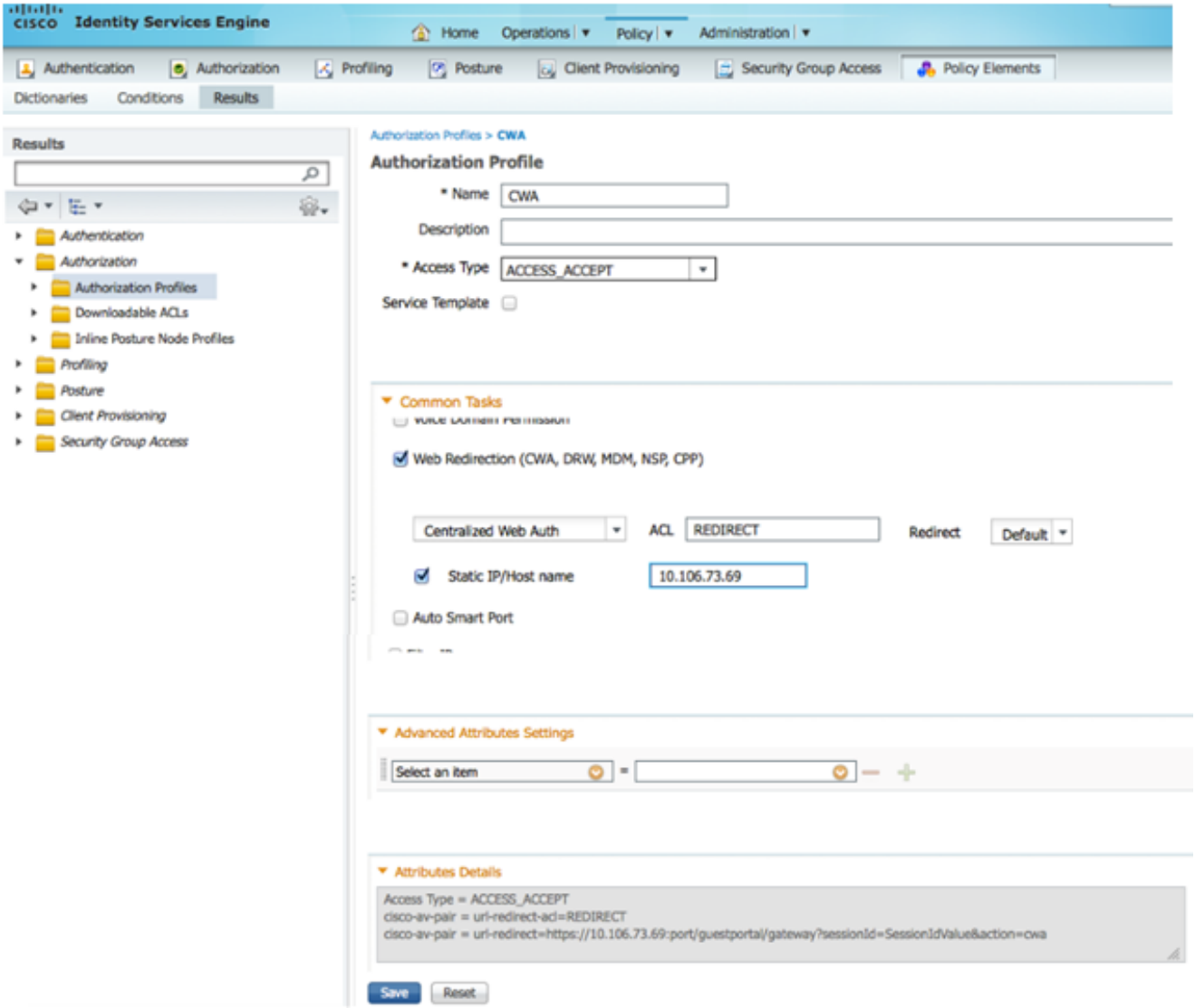
1. Escolha **ISE GUI > Administration > Network Resource > Network Devices List > Add** para adicionar a WLC no ISE como o cliente AAA (Authentication, Authorization, and Accounting). Certifique-se de inserir o mesmo segredo compartilhado na WLC que é adicionado no servidor RADIUS. **Observação**: ao implantar a Anchor-Foreign, você só precisa adicionar a WLC externa. Não há necessidade de adicionar o Anchor WLC no ISE como um cliente AAA. A mesma configuração do ISE é usada para todos os outros cenários de implantação neste
documento.



2. Na GUI do ISE, escolha **Policy > Authentication > MAB > Edit** para criar a política de autenticação. A política de autenticação aceita o endereço MAC do cliente, que aponta para endpoints internos. Escolha estas seleções na lista Opções:Na lista suspensa Se a autenticação falhou, escolha **Rejeitar**.Na lista suspensa Se o usuário não for encontrado, escolha **Continuar**.Na lista suspensa Se o processo falhou, escolha **Eliminar**.Quando você configura com essas opções, o cliente com falha na autorização MAC prossegue com o portal do
convidado.

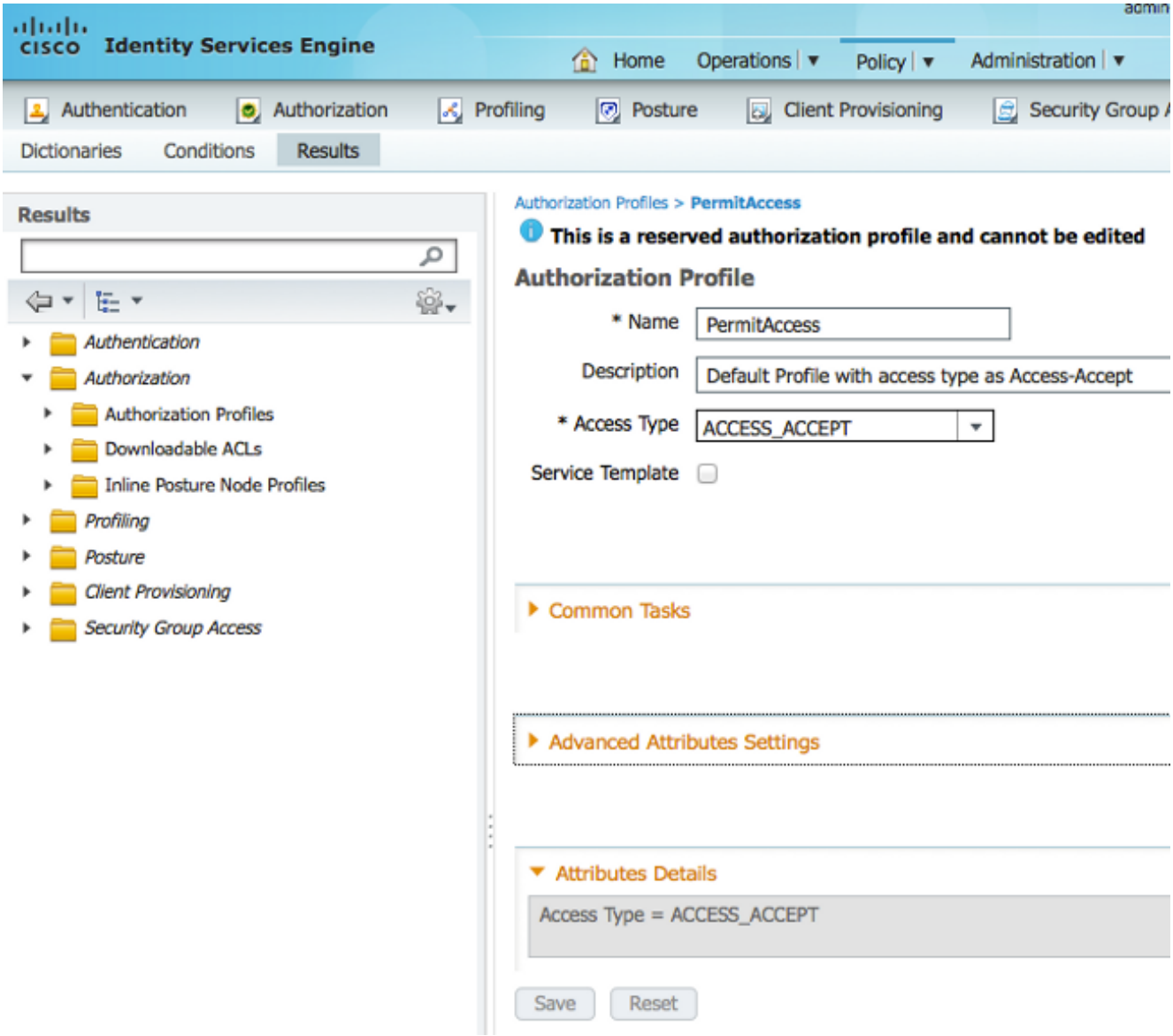


3. Na GUI do ISE, escolha **Policy > Authorization > Results > Authorization Profiles > Add**. Preencha os detalhes e clique em **Save** para criar o perfil de autorização. Esse perfil ajuda os clientes a serem redirecionados para o URL de redirecionamento após a autenticação MAC, onde os clientes inserem o nome de usuário/senha do convidado.

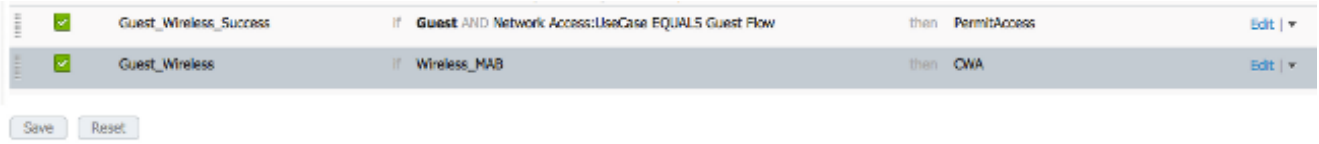


4. Na GUI do ISE, escolha **Policy > Authorization > Results > Authorization Profiles > Add** para criar outro perfil de autorização para permitir o acesso aos usuários com as credenciais

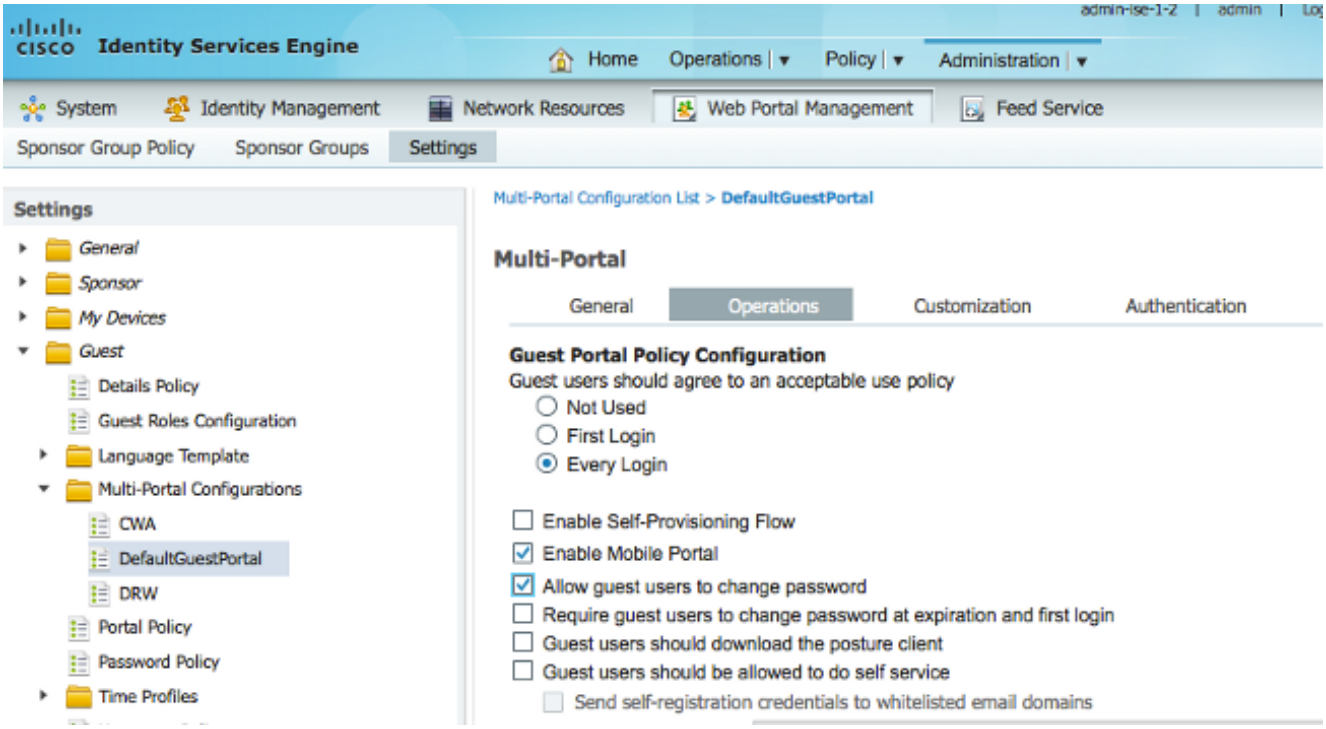
corretas.



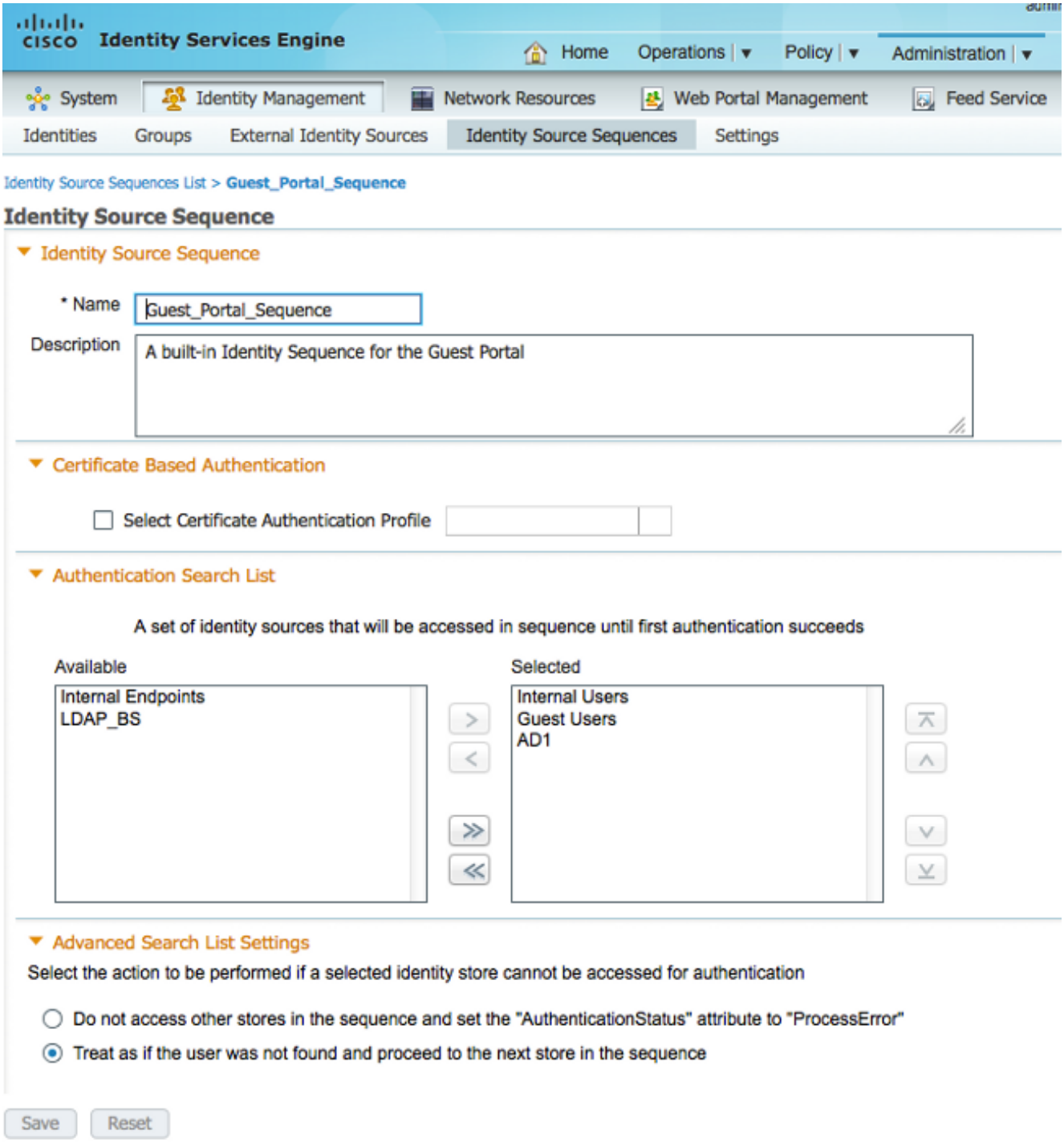
5. Crie as políticas de Autorização. A diretiva de autorização 'Guest_Wireless' envia a URL de redirecionamento e a ACL de redirecionamento para a sessão do cliente. O perfil enviado aqui é o CWA como mostrado anteriormente.A política de Autorização 'Guest_Wireless-Success' fornece acesso total a um usuário convidado que é autenticado com êxito por meio do portal do convidado. Depois que o usuário é autenticado com êxito no portal do convidado, a autorização dinâmica é enviada pela WLC. Isso autentica novamente a sessão do cliente com o atributo 'Acesso à rede:Usecase EQUALS Guest Flow'.As políticas de Autorização finais se parecem
com:



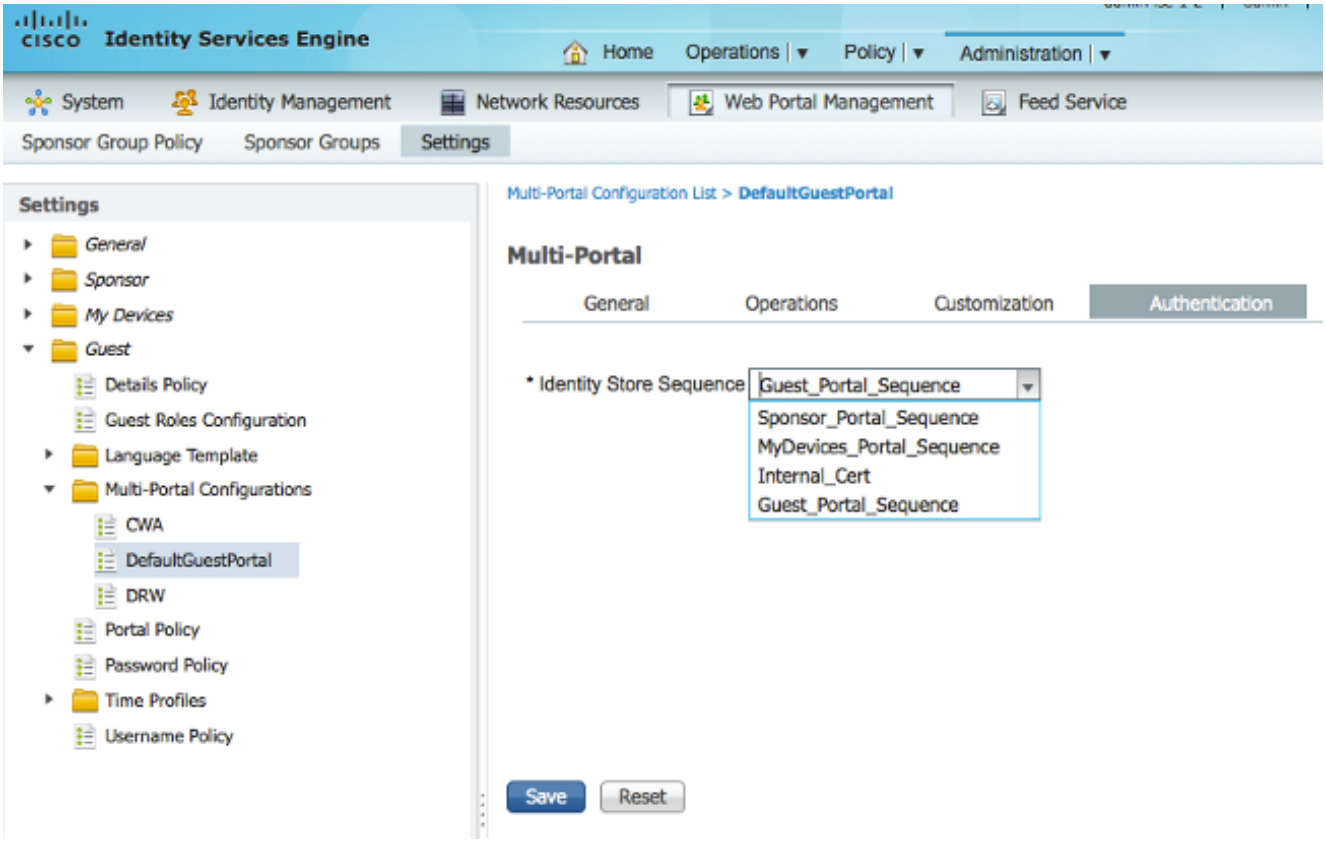
6. Opcional: nesse caso, são usadas configurações padrão de vários portais. Com base nos requisitos, o mesmo pode ser alterado na GUI. Na GUI do ISE, escolha **Administration > Web Portal management > Multi Portal Configurations > DefaultGuestPortal**.



A sequência_Portal_Convidado é criada para permitir usuários internos, convidados e do AD.



7. Na GUI do ISE, escolha **Guest > Multi-Portal Configurations > DefaultGuestPortal**. Na lista suspensa Identificar sequência de armazenamento, escolha **Guest_Portal_Sequence**.



Configuração na WLC

1. Defina o servidor ISE Radius no WLC 5760.
2. Configure o servidor RADIUS, o grupo de servidores e a lista de métodos com a 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. Configurar a WLAN com a CLI.

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

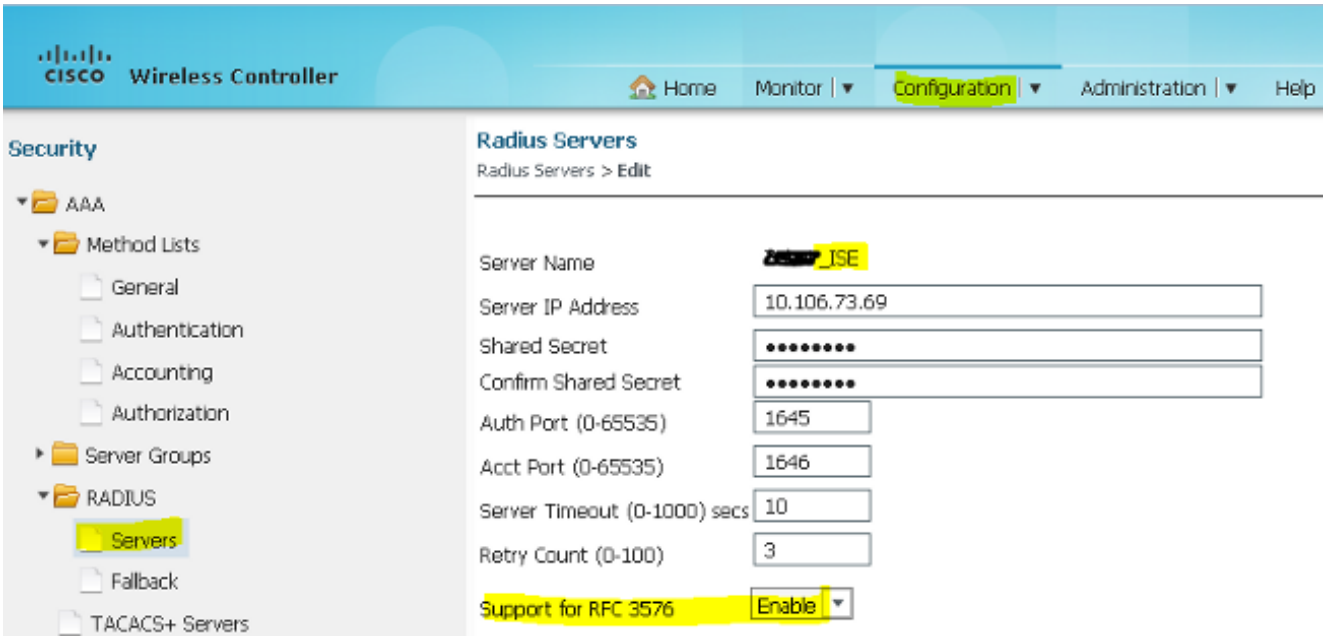
```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

4. Configure as ACLs de redirecionamento com a CLI. Esta é a url-redirect-acl que o ISE retorna como uma substituição de AAA junto com a URL de redirecionamento para o redirecionamento do portal convidado. É uma ACL direta usada atualmente na arquitetura unificada. Essa é uma ACL "punt", que é uma ACL reversa que você usaria normalmente para a arquitetura unificada. Você precisa bloquear o acesso ao DHCP, ao servidor DHCP, ao DNS, ao servidor DNS e ao servidor ISE. Permitir somente www, 443 e 8443 conforme necessário. Este portal de convidado do ISE usa a porta 8443 e o redirecionamento ainda funciona com a ACL mostrada aqui. Aqui, o ICMP é ativado, mas com base nas regras de segurança, você pode negar ou permitir.

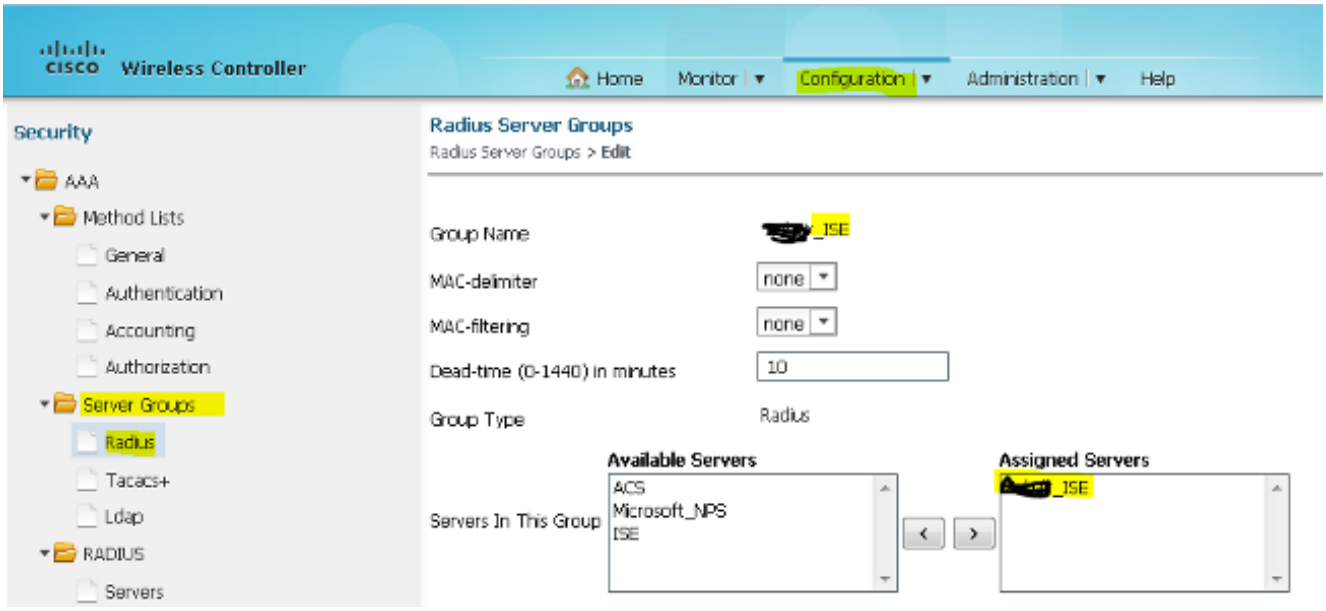
```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

Cuidado: quando você habilita o HTTPS, ele pode causar alguns problemas de alta utilização da CPU devido à escalabilidade. Não ative essa opção, a menos que ela seja recomendada pela equipe de projeto da Cisco.

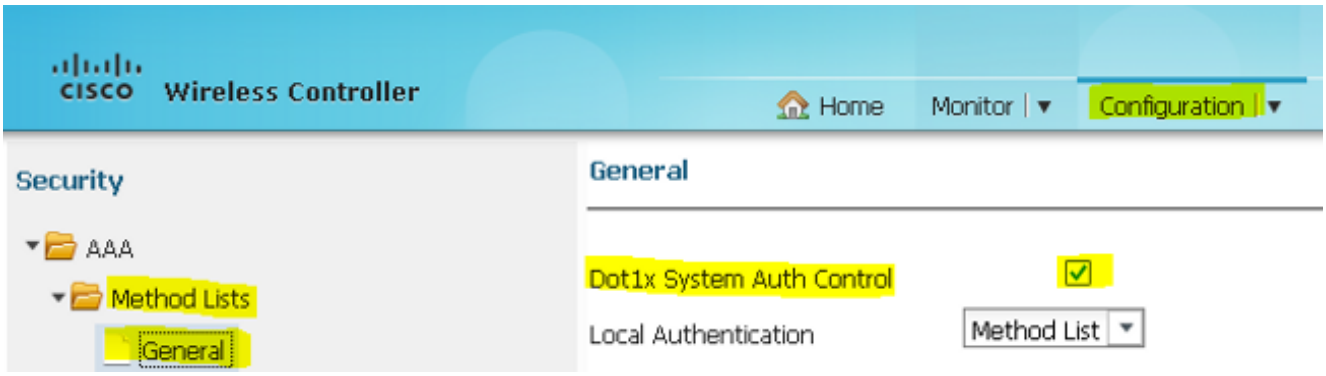
5. Na GUI do controlador sem fio, escolha **AAA > RADIUS > Servers**. Configure o servidor RADIUS, o grupo de servidores e a lista de métodos na GUI. Preencha todos os parâmetros e verifique se o segredo compartilhado configurado aqui corresponde ao configurado no ISE para este dispositivo. Na lista suspensa Suporte para RFC 3576, selecione **Habilitar**.



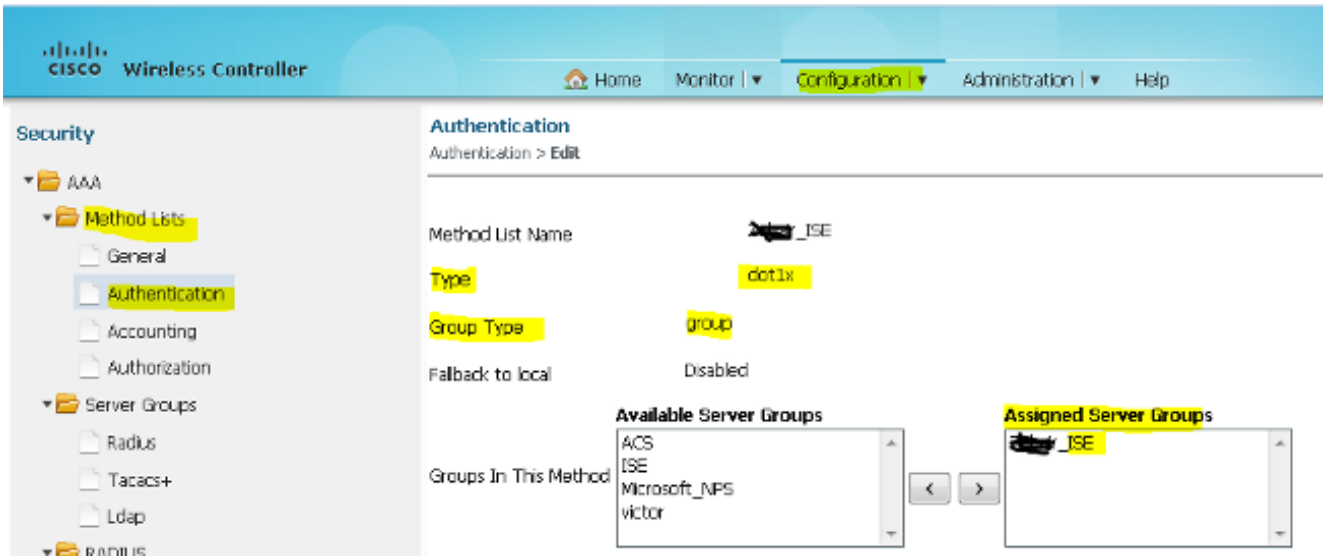
6. Na GUI do controlador sem fio, escolha **AAA > Server Groups > Radius**. Adicione o servidor RADIUS criado anteriormente aos grupos de servidores.



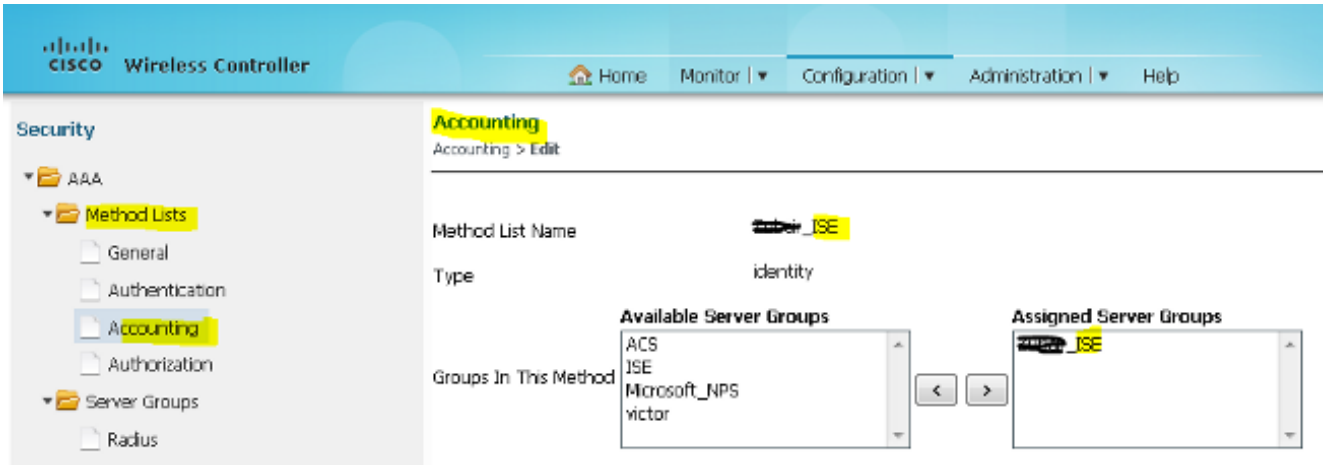
7. Na GUI do controlador sem fio, escolha **AAA > Listas de métodos > Geral**. Marque a caixa de seleção **Dot1x System Auth Control**. Se você desabilitar essa opção, AAA não funcionará.



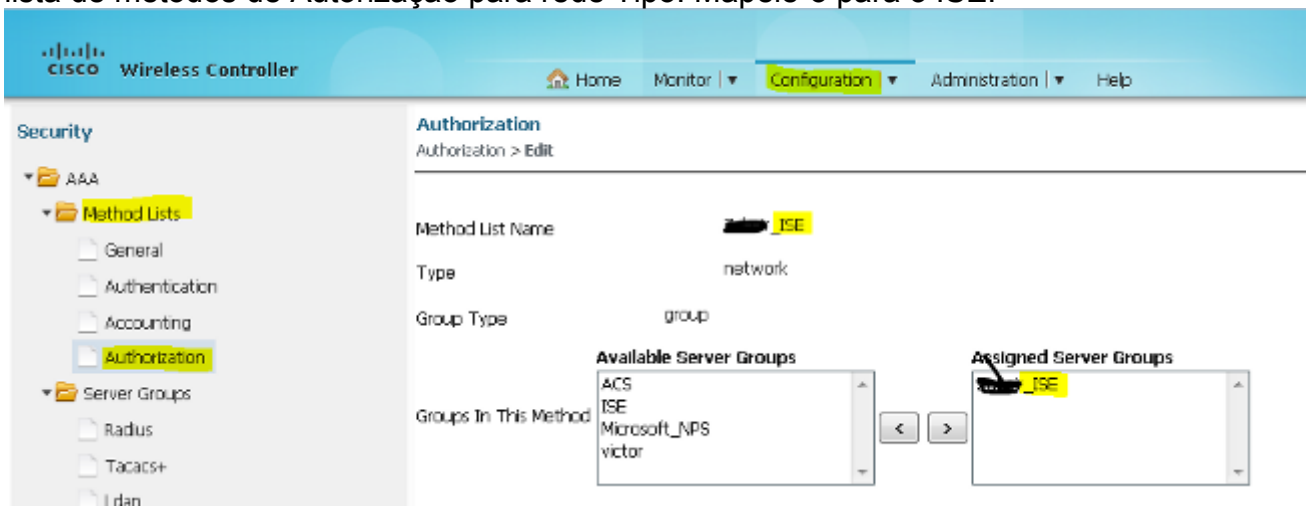
8. Na GUI do controlador sem fio, escolha **AAA > Listas de métodos > Autenticação**. Crie uma lista de Método de autenticação para o Tipo dot1X. O Tipo de grupo é group. Mapeie-o para o ISE.



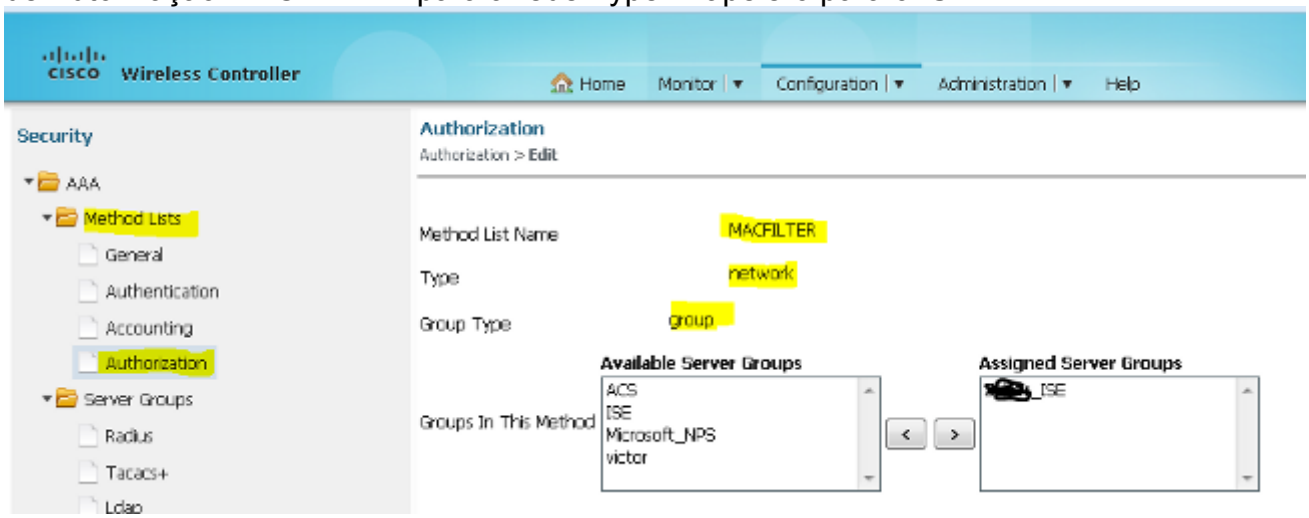
9. Na GUI do controlador sem fio, escolha **AAA > Listas de métodos > Contabilidade**. Crie uma lista de métodos Contábeis para a identidade Tipo. Mapeie-o para o ISE.



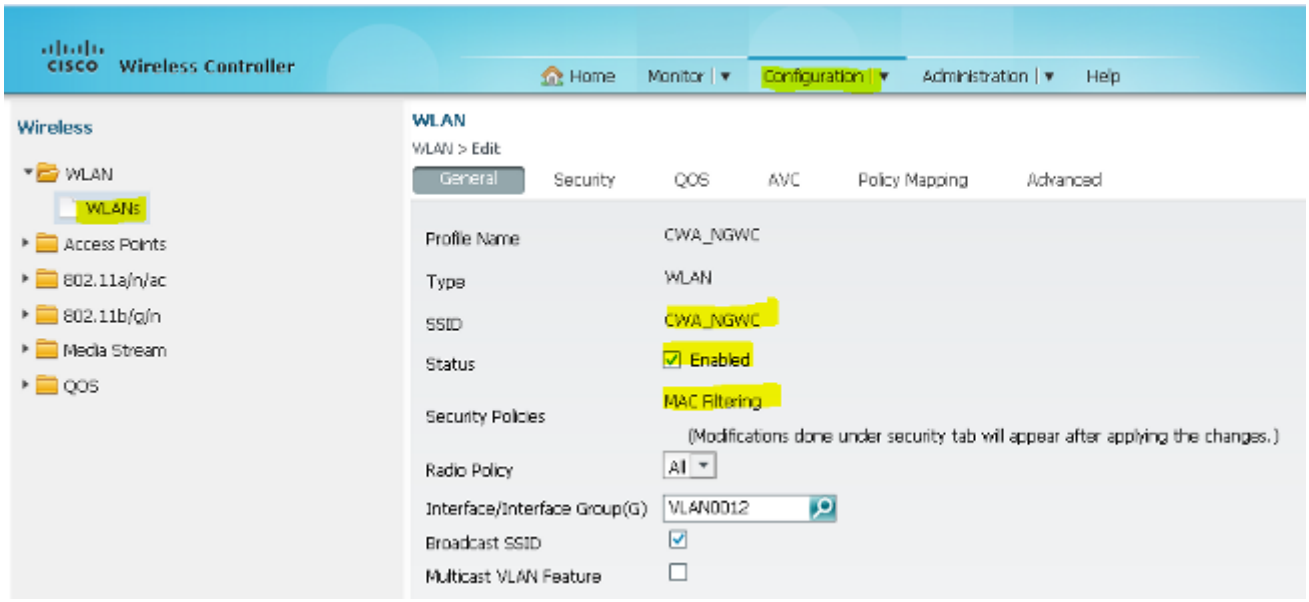
10. Na GUI do controlador sem fio, escolha **AAA > Listas de métodos > Autorização**. Crie uma lista de métodos de Autorização para rede Tipo. Mapeie-o para o ISE.



11. Opcional, já que também há suporte a MAC em caso de falha. Crie uma lista de métodos de Autorização MACFILTER para a rede Type. Mapeie-o para o ISE.

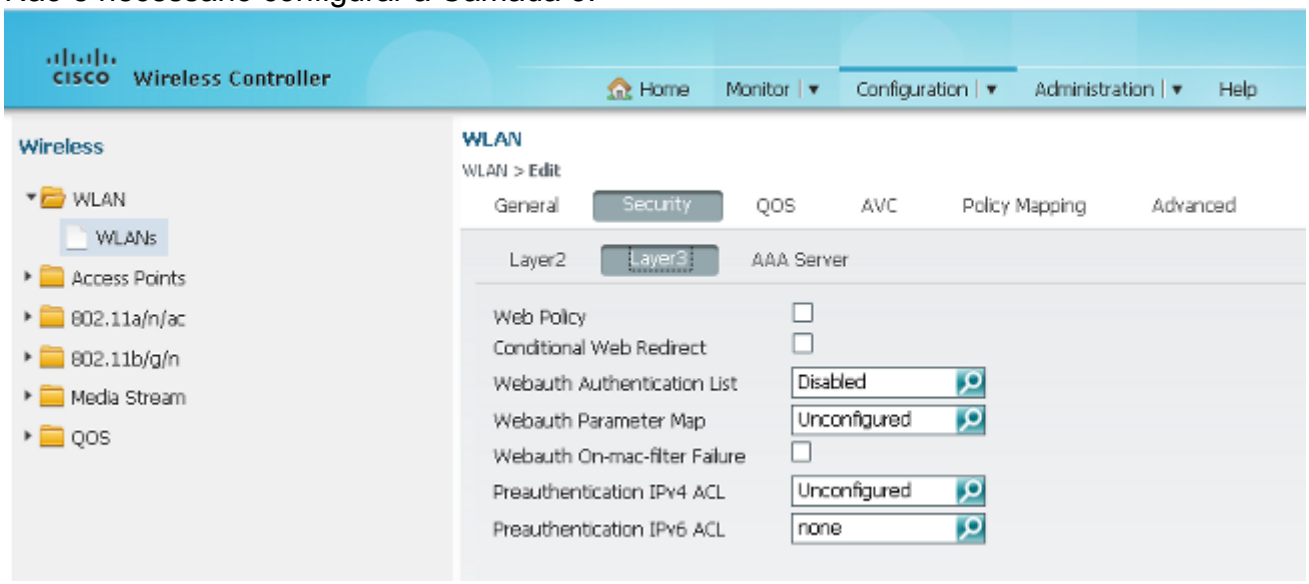


12. Na GUI do controlador sem fio, escolha **WLAN > WLANs**. Crie uma nova configuração com os parâmetros mostrados aqui.

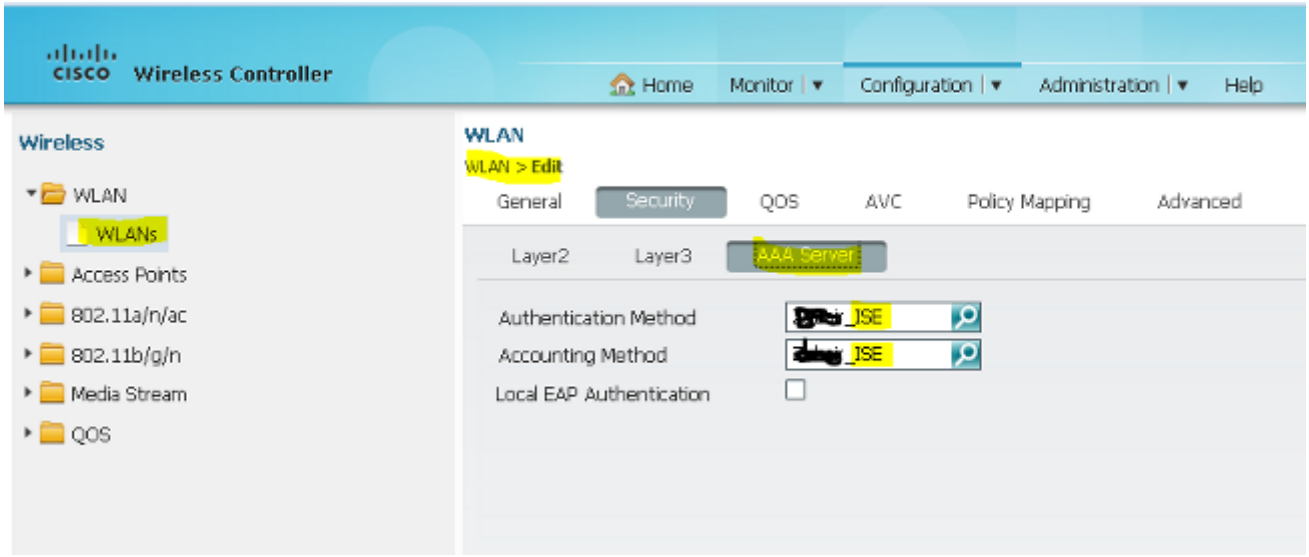


13. Escolha **Security > Layer2**. No campo MAC Filtering (Filtragem de MAC), digite **MACFILTER**.

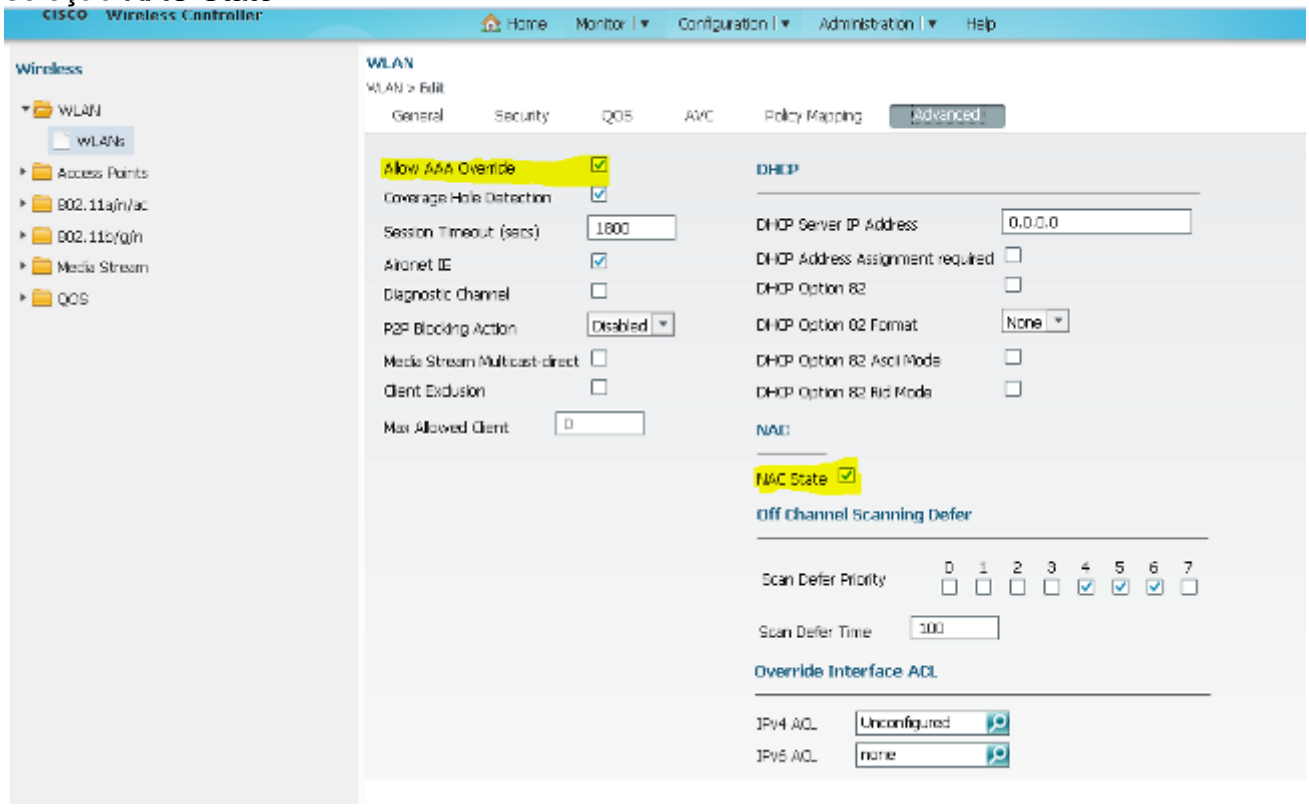
14. Não é necessário configurar a Camada 3.



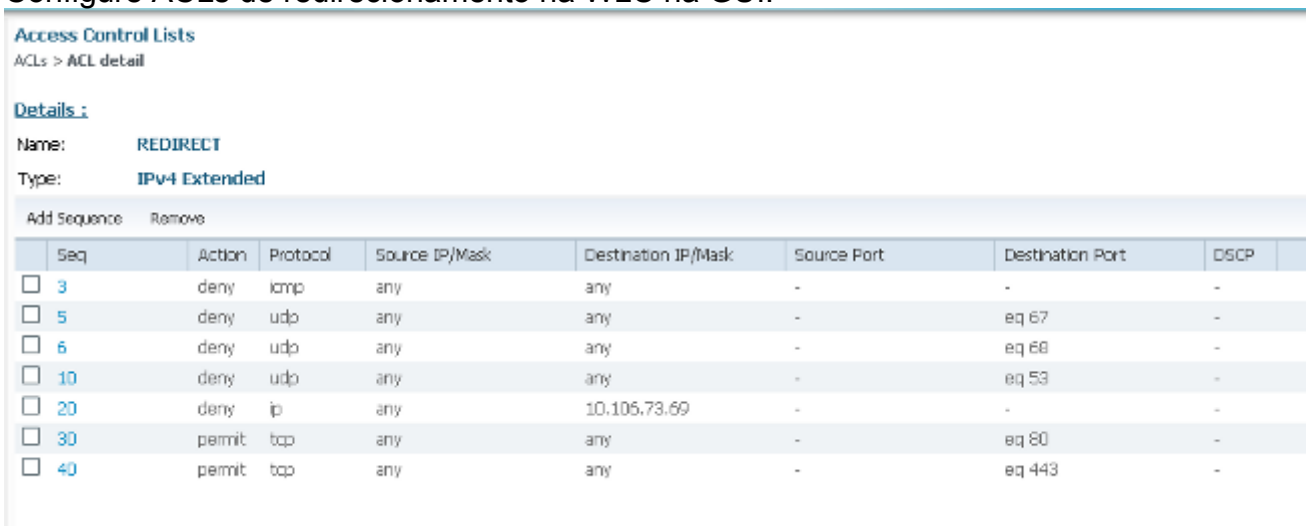
15. Selecione **Security > AAA Server**. Na lista suspensa Método de autenticação, escolha **ISE**. Na lista suspensa Método de contabilização, escolha **ISE**.



16. Escolha **Advanced**. Marque a caixa de seleção **Allow AAA Override**. Marque a caixa de seleção **NAC State**.



17. Configure ACLs de redirecionamento na WLC na 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	-

Exemplo de Configuração da Topologia 2

Consulte a Topologia 2 para obter o diagrama e a explicação da rede.

Essa configuração também é um processo de duas etapas.

Configuração no ISE

A configuração no ISE é a mesma da configuração da Topologia 1.

Não há necessidade de adicionar o controlador de âncora no ISE. Basta adicionar a WLC externa no ISE, definir o servidor RADIUS na WLC externa e mapear a política de autorização na WLAN. Na âncora, basta habilitar a filtragem de endereços MAC.

Neste exemplo de configuração, há duas WLC 5760s que atuam como uma Âncora Externa. Caso você queira usar a WLC 5760 como uma âncora e o switch 3850 como Âncora Externa, que é o Agente de Mobilidade, para outro Controlador de Mobilidade, a mesma configuração está correta. No entanto, não há necessidade de configurar a WLAN no segundo controlador de mobilidade do qual o Switch 3850 obtém as licenças. Você só precisa apontar o Switch 3850 para o WLC 5760 que atua como a Âncora.

Configuração na WLC

1. No roteador externo, configure o servidor ISE com a lista de Método AAA para AAA e mapeie a WLAN para uma autorização de filtro MAC. **Observação**: configure a ACL de redirecionamento tanto na âncora quanto na externa e também na filtragem 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. Configure ACLs de redirecionamento com a CLI. Esta é a url-redirect-acl que o ISE retorna como uma substituição de AAA junto com a URL de redirecionamento para o redirecionamento do portal convidado. É uma ACL direta usada atualmente na arquitetura unificada. Essa é uma ACL "punt", que é uma ACL reversa que você usaria normalmente para a arquitetura unificada. Você precisa bloquear o acesso ao DHCP, ao servidor DHCP, ao DNS, ao servidor DNS e ao servidor ISE. Permitir somente www, 443 e 8443 conforme necessário. Este portal de convidado do ISE usa a porta 8443 e o redirecionamento ainda funciona com a ACL mostrada aqui. Aqui, o ICMP é ativado, mas com base nas regras de segurança, você pode negar ou permitir.

```
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
```

   Cuidado: quando você habilita o HTTPS, ele pode causar alguns problemas de alta utilização da CPU devido à escalabilidade. Não ative essa opção, a menos que ela seja recomendada pela equipe de projeto da Cisco.

3. Configure a mobilidade na âncora.

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

   Observação: se você configurar o mesmo com o Switch 3850 como o Externo, certifique-se de definir o grupo de peer do Switch no Controlador de mobilidade e vice-versa no Controlador de mobilidade. Em seguida, configure as configurações do CWA acima no Switch 3850.

4. Configuração na âncora. Na âncora, não há necessidade de configurar nenhuma configuração do ISE. Você só precisa da configuração da 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. Configure a mobilidade na âncora. Defina a outra WLC como o membro Mobility nessa WLC.

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

6. Configure ACLs de redirecionamento com a CLI. Esta é a url-redirect-acl que o ISE retorna como uma substituição de AAA junto com a URL de redirecionamento para o redirecionamento do portal convidado. É uma ACL direta usada atualmente na arquitetura unificada. Essa é uma ACL "punt", que é uma ACL reversa que você usaria normalmente

para a arquitetura unificada. Você precisa bloquear o acesso ao DHCP, ao servidor DHCP, ao DNS, ao servidor DNS e ao servidor ISE. Permitir somente www, 443 e 8443 conforme necessário. Este portal de convidado do ISE usa a porta 8443 e o redirecionamento ainda funciona com a ACL mostrada aqui. Aqui, o ICMP é ativado, mas com base nas regras de segurança, você pode negar ou permitir.

```
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
```

Cuidado: quando você habilita o HTTPS, ele pode causar alguns problemas de alta utilização da CPU devido à escalabilidade. Não ative essa opção, a menos que ela seja recomendada pela equipe de projeto da Cisco.

Exemplo de Configuração da Topologia 3

Consulte a Topologia 3 para obter o diagrama e a explicação da rede.

Esse também é um processo de duas etapas.

Configuração no ISE

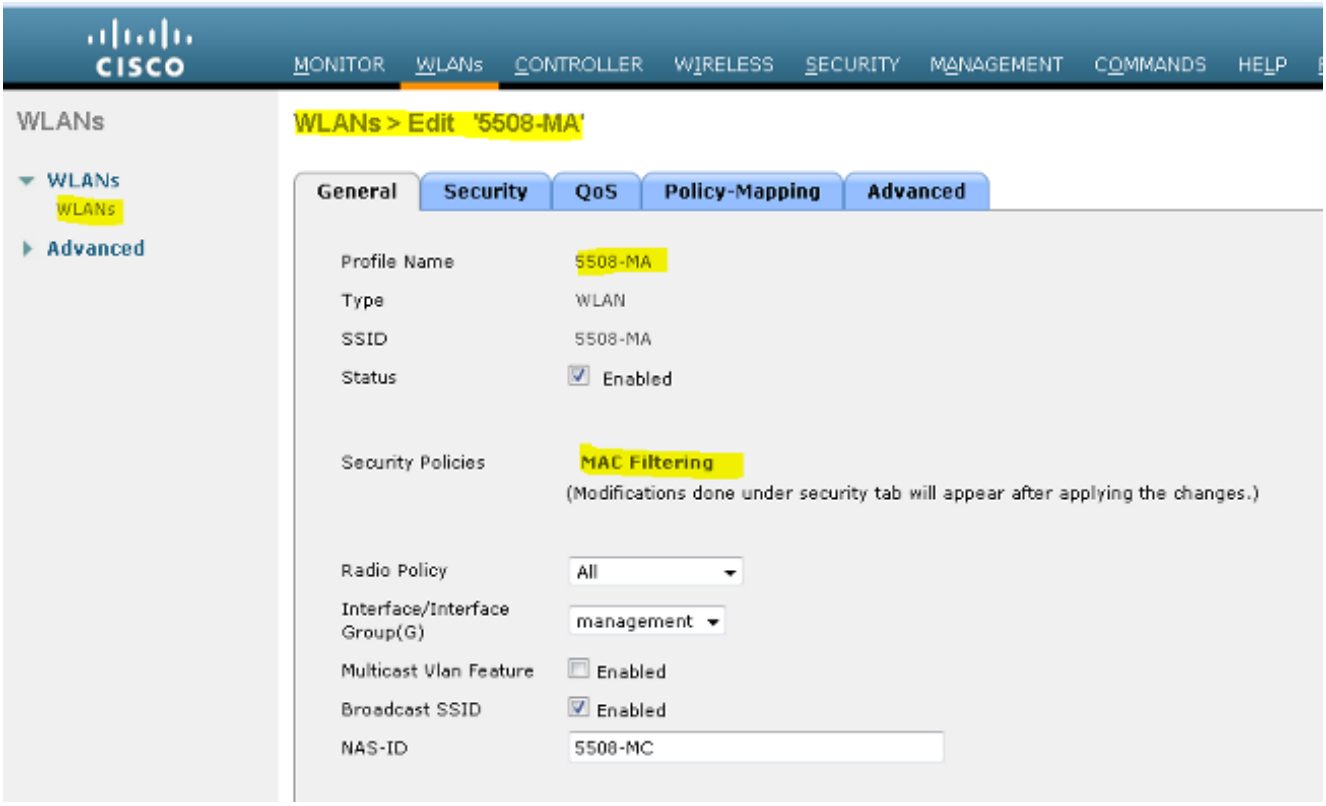
A configuração no ISE é a mesma da configuração da topologia 1.

Não há necessidade de adicionar o controlador de âncora no ISE. Basta adicionar a WLC externa no ISE, definir o servidor RADIUS na WLC externa e mapear a política de autorização na WLAN. Na âncora, basta habilitar a filtragem de endereços MAC.

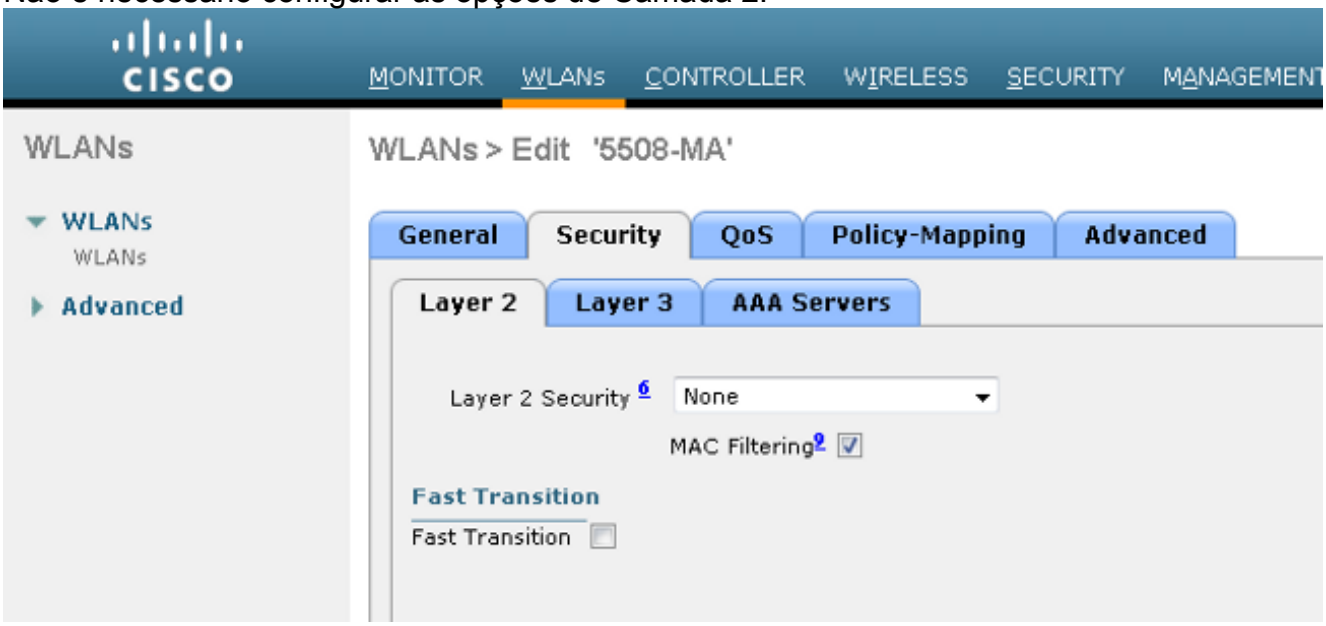
Neste exemplo, há uma WLC 5508 que atua como uma âncora e uma WLC 5760 que atua como uma WLC externa. Se você quiser usar uma WLC 5508 como uma âncora e um switch 3850 e uma WLC externa, que é um agente de mobilidade, para outro controlador de mobilidade, a mesma configuração estará correta. No entanto, não há necessidade de configurar a WLAN no segundo controlador de mobilidade do qual o Switch 3850 obtém as licenças. Você só precisa apontar o Switch 3850 para a WLC 5508 que atua como a âncora.

Configuração na WLC

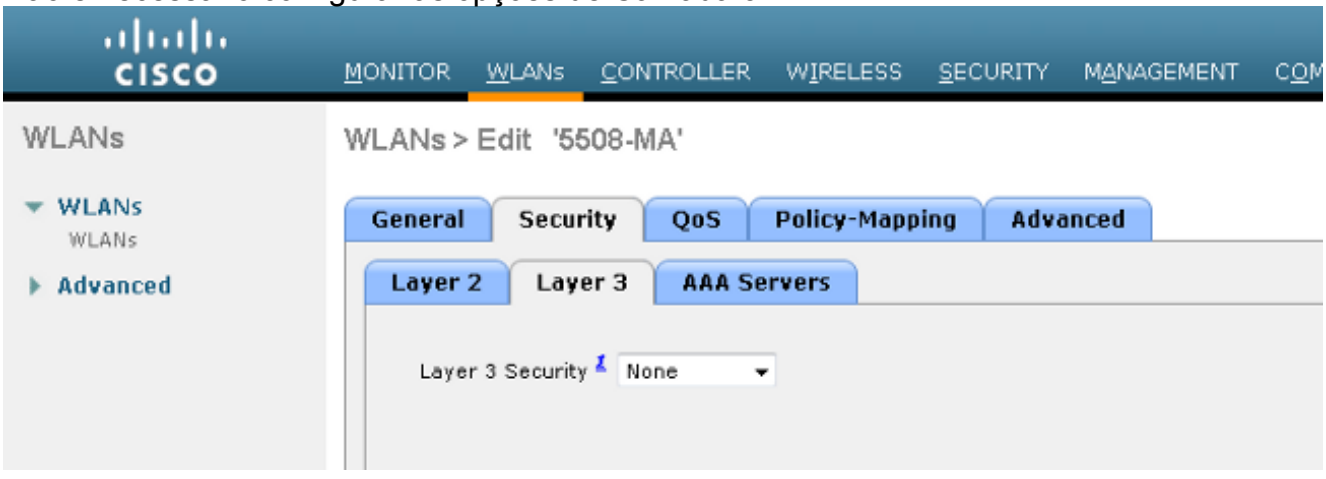
1. Na WLC externa, configure o servidor ISE com a lista de Método AAA para AAA e mapeie a WLAN para uma autorização de filtro MAC. Isso não é necessário na âncora. **Observação**: Configure a ACL de redirecionamento nas WLC Âncora e Externa e também na filtragem de MAC.
2. Na GUI do WLC 5508, escolha **WLANs > New** para configurar o Anchor 5508. Preencha os detalhes para habilitar a filtragem MAC.



3. Não é necessário configurar as opções de Camada 2.

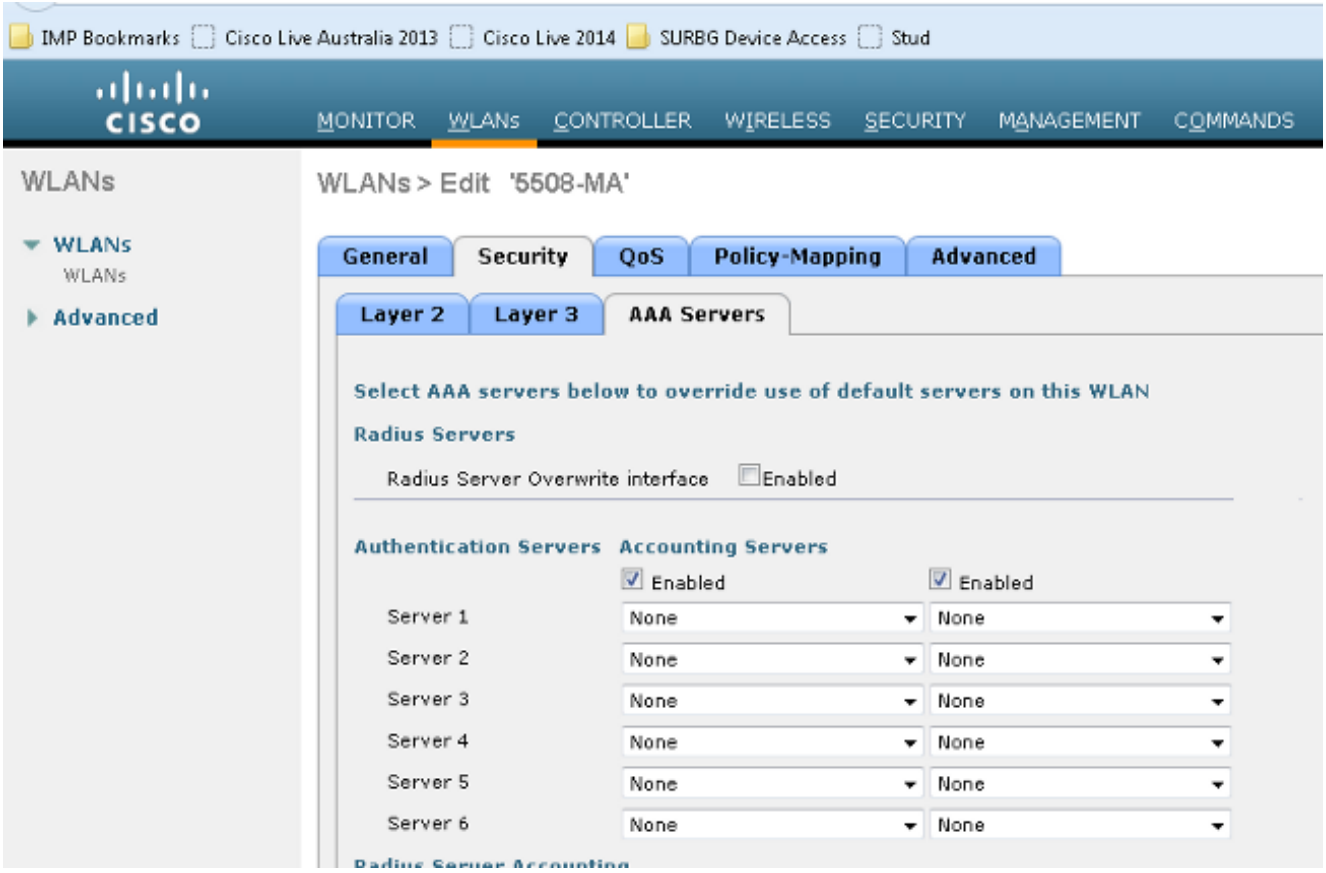


4. Não é necessário configurar as opções de Camada 3.

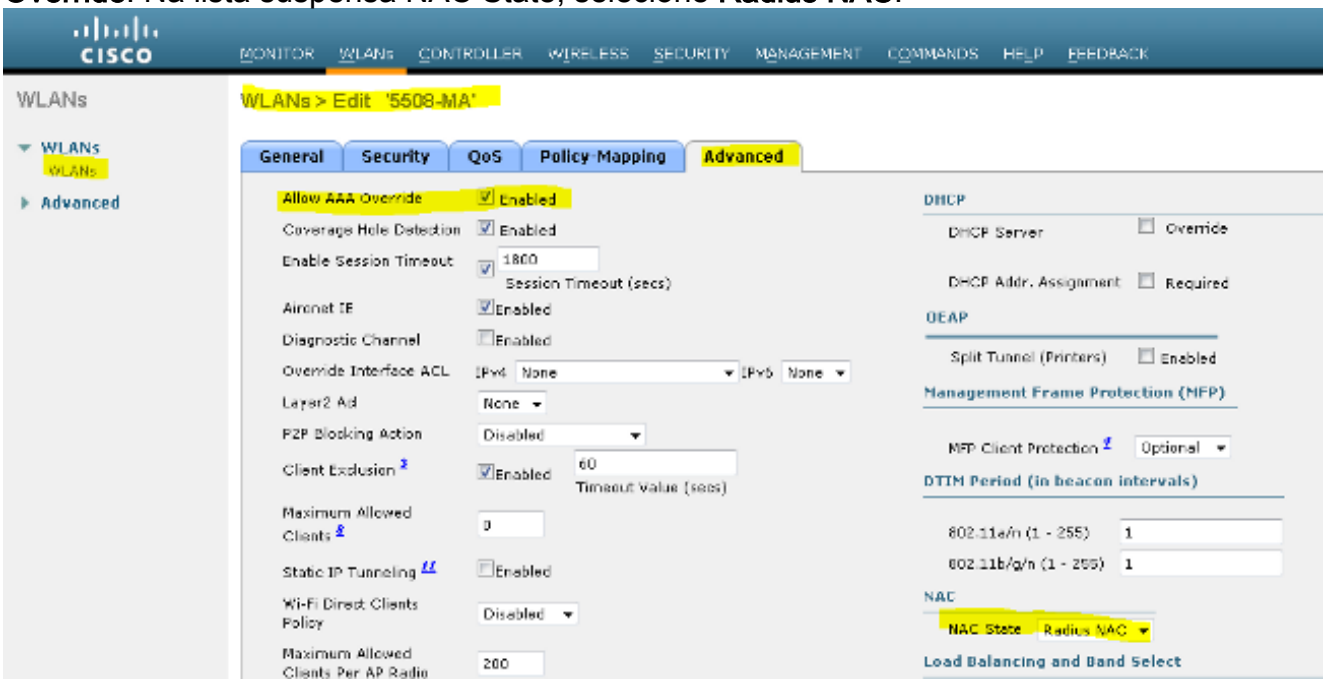


5. Os servidores AAA devem ser desabilitados no WLC Anchor AireOS para que o CoA seja

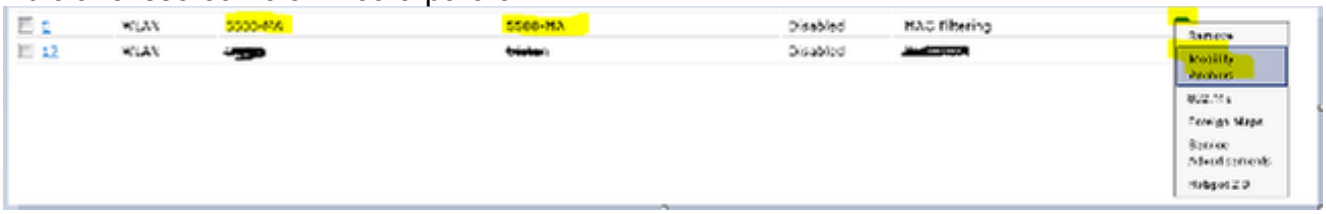
processado pelo NGWC estrangeiro. Os servidores AAA só poderão ser habilitados na WLC Anchor se não houver servidores RADIUS configurados em: Security > AAA > RADIUS > Authentication



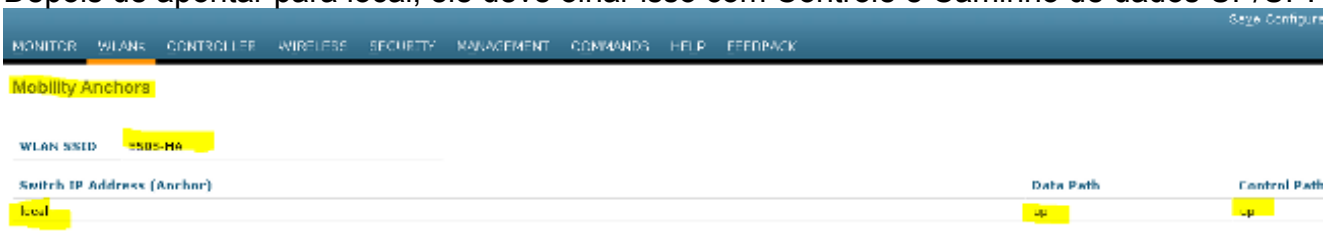
6. Escolha **WLANs > WLANs > Edit > Advanced**. Marque a caixa de seleção **Allow AAA Override**. Na lista suspensa NAC State, selecione **Radius NAC**.



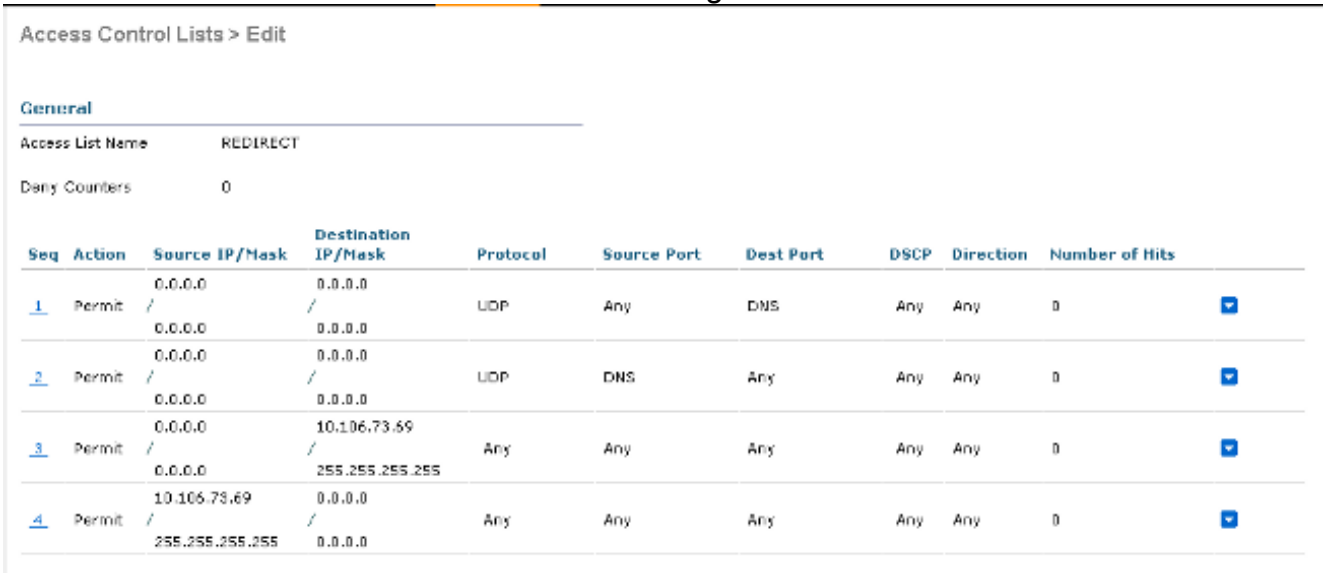
7. Adicione isso como a Âncora para a WLAN.



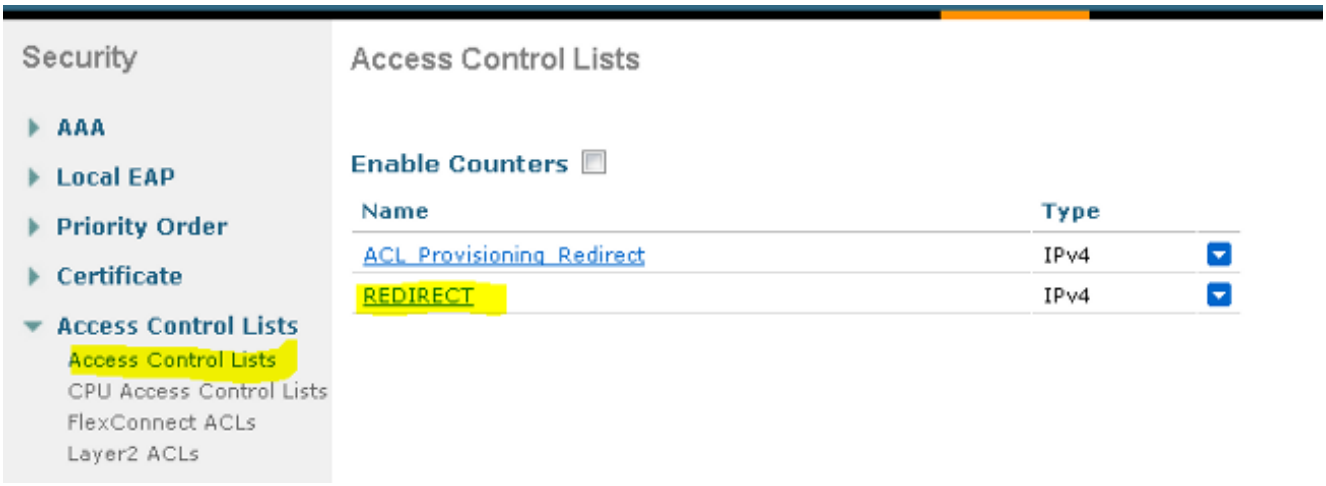
8. Depois de apontar para local, ele deve olhar isso com Controle e Caminho de dados UP/UP.



9. Crie a ACL de redirecionamento na WLC. Isso nega DHCP e DNS. Permite HTTP/HTTPs.



Esta é a aparência após a criação da ACL.



10. Defina o servidor ISE RADIUS no WLC 5760.
11. Configure o servidor RADIUS, o grupo de servidores e a lista de métodos com a 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. Configure a WLAN a partir da 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. Defina a outra WLC como o membro Mobility nessa WLC.

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

Observação: se você configurar o mesmo com o WLC 3850 como o Externo, certifique-se de definir o grupo de peer do Switch no controlador de mobilidade e vice-versa no controlador de mobilidade. Em seguida, configure as configurações anteriores do CWA no WLC 3850.

14. Configure ACLs de redirecionamento com a CLI. Esta é a url-redirect-acl que o ISE retorna como uma substituição de AAA junto com a URL de redirecionamento para o redirecionamento do portal convidado. É uma ACL direta usada atualmente na arquitetura unificada. Essa é uma ACL "punt", que é uma ACL reversa que você usaria normalmente para a arquitetura unificada. Você precisa bloquear o acesso ao DHCP, ao servidor DHCP, ao DNS, ao servidor DNS e ao servidor ISE. Permitir somente www, 443 e 8443 conforme necessário. Este portal de convidado do ISE usa a porta 8443 e o redirecionamento ainda funciona com a ACL mostrada aqui. Aqui, o ICMP é ativado, mas com base nas regras de segurança, você pode negar ou permitir.

```
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
```

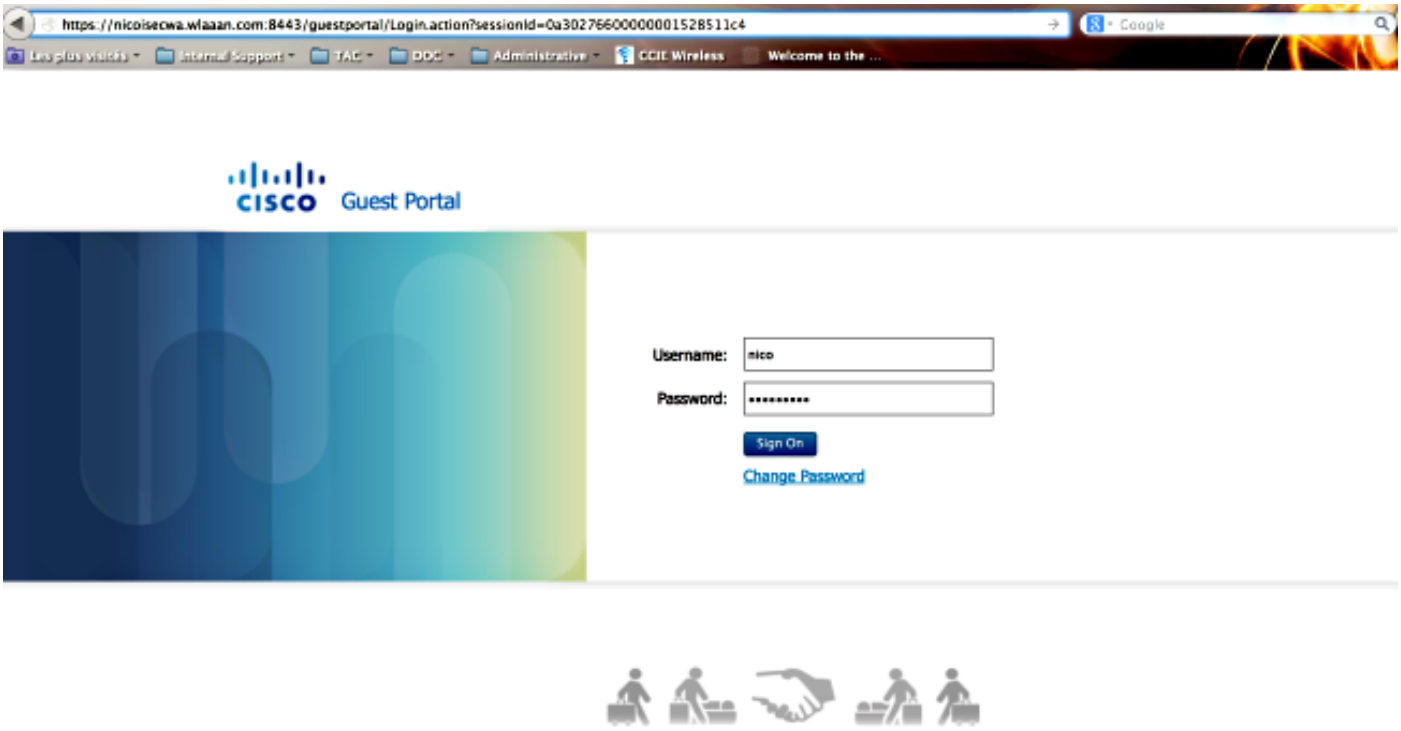
Cuidado: quando você habilita o HTTPS, ele pode causar alguns problemas de alta utilização da CPU devido à escalabilidade. Não ative essa opção, a menos que ela seja recomendada pela equipe de projeto da Cisco.

Verificar

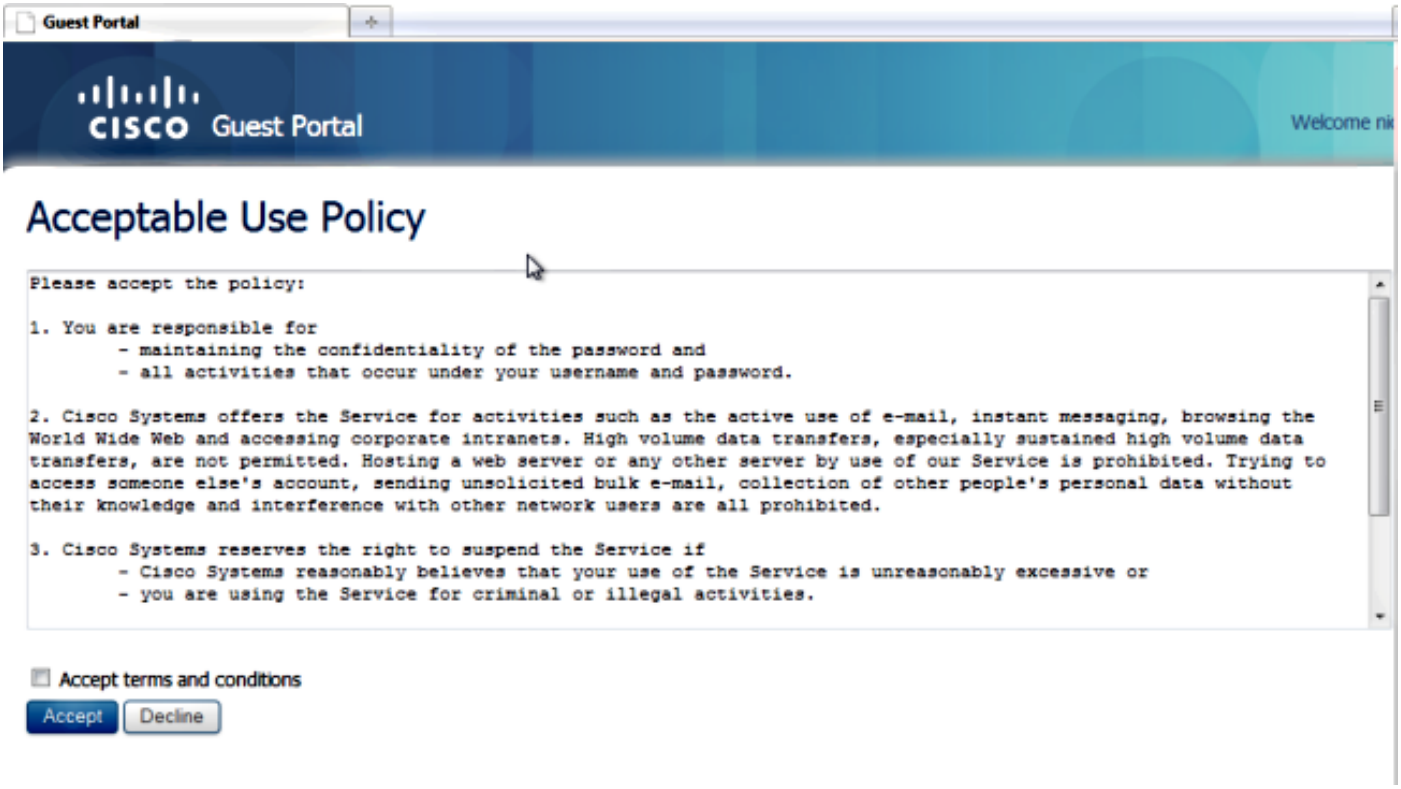
Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Conecte o cliente ao SSID configurado. Quando você receber o endereço IP e quando o cliente entrar no estado de autenticação da Web obrigatória, abra o navegador. Insira as credenciais do cliente no portal.

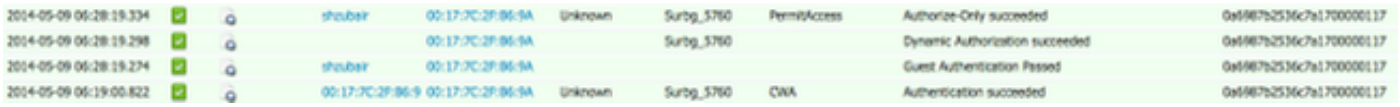


Após a autenticação bem-sucedida, marque a caixa de seleção **Aceitar termos e condições**. Clique em **Aceitar**.



Você receberá uma mensagem de confirmação e agora poderá navegar na Internet.

No ISE, o fluxo do cliente é semelhante a este:



Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

> **Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.**

Na WLC de acesso convergido, é recomendável executar rastreamentos em vez de depurações. No Aironet OS 5508 WLC, basta inserir **debug client <client mac>** e **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
```

Alguns defeitos conhecidos no Cisco IOS-XE e no Aironet OS estão incluídos no bug da Cisco ID CSCun38344.

Esta é a aparência do fluxo bem-sucedido do CWA nos rastreamentos:

```
[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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.