

# Entender E Solucionar Problemas Da CWA (Central Web Authentication, Autenticação Da Web Central) Na Configuração De Âncora De Convidado

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Fluxo básico](#)

[Fluxo de Webauth Central para Tentativa de Conexão de Cliente Bem-Sucedida](#)

[Fluxo do Webauth Central quando o cliente é desconectado](#)

[Conta do cliente suspensa no ISE](#)

[Solucionar problemas da Web central na configuração da âncora do convidado](#)

[Cenário 1. O cliente está preso no estado START e não recebe o endereço IP](#)

[Cenário 2. O cliente não consegue obter o endereço IP](#)

[Cenário 3. O cliente não é redirecionado para a página da Web](#)

## Introduction

Este documento descreve como a webauth central funciona em uma configuração de âncora de convidado e alguns dos problemas comuns vistos em uma rede de produção e como eles podem ser corrigidos.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento sobre como configurar a web central no Wireless LAN Controller (WLC).

Este documento fornece etapas com relação à configuração da webauth central:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>

### Componentes Utilizados

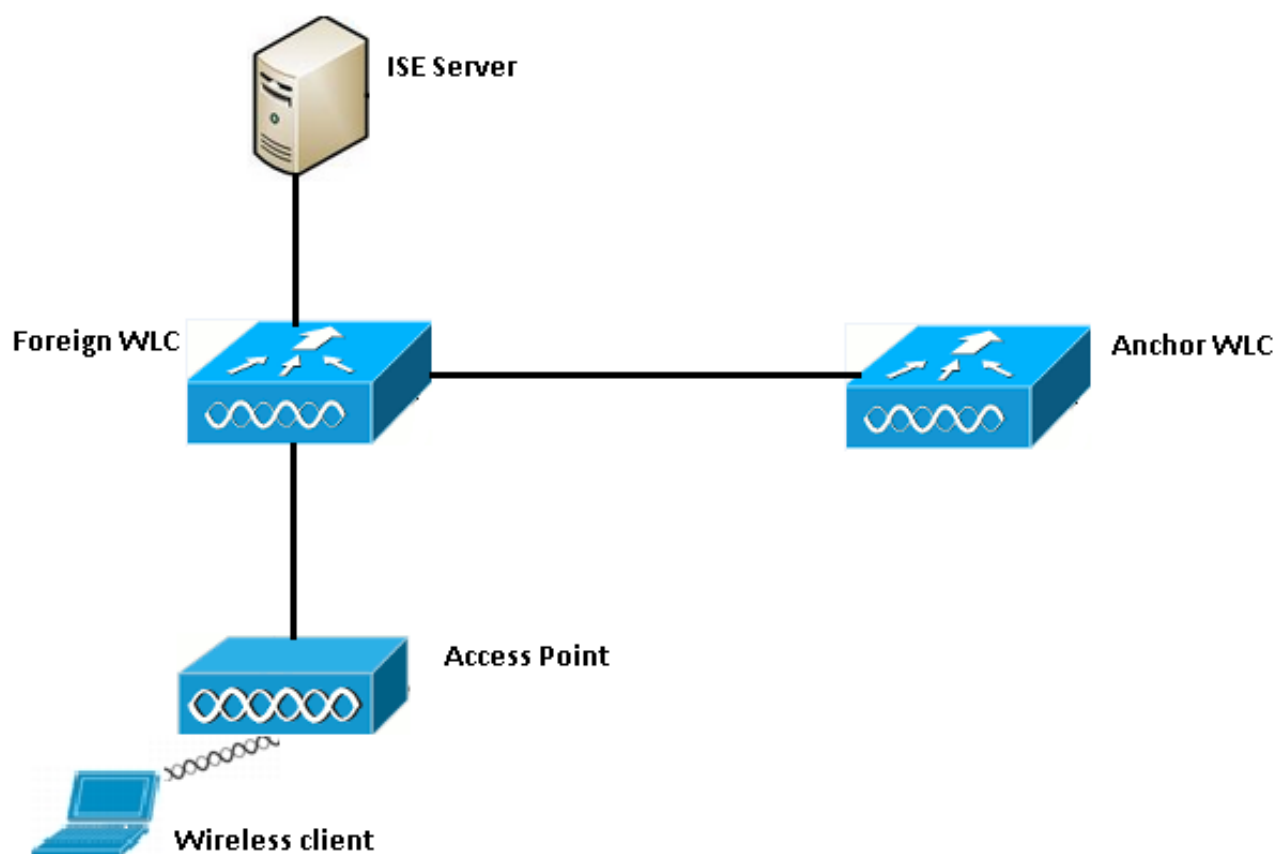
As informações neste documento são baseadas nestas versões de software e hardware:

- WLC 5508 executando a versão 7.6
- Identity Services Engine (ISE) executando a versão 1.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando

## Fluxo básico

Esta seção mostra o fluxo de trabalho básico do webauth central em uma configuração de âncora de convidado, como mostrado na imagem:



Etapa 1. O cliente inicia a conexão quando envia uma solicitação de associação.

Etapa 2. A WLC inicia o processo de autenticação MAC quando envia uma solicitação de autenticação ao servidor ISE configurado.

Etapa 3. Com base na política de autorização configurada no ISE, a mensagem Access-Accept é enviada de volta para a WLC com a URL de redirecionamento e redireciona entradas da Access Control List (ACL).

Etapa 4. A WLC externa envia uma resposta de associação ao cliente.

Etapa 5. Essas informações são passadas pela WLC estrangeira para a WLC âncora em mensagens de transferência de mobilidade. Você precisa garantir que as ACLs de redirecionamento estejam configuradas na âncora e nas WLCs externas.

Etapa 6. Neste estágio, o cliente passa para o estado Executar na WLC externa.

Passo 7. Quando o cliente inicia o web-auth com um URL no navegador, a âncora inicia o

processo de redirecionamento.

Etapa 8. Quando o cliente é autenticado com êxito, ele se move para o estado **RUN** na WLC âncora.

## Fluxo de Webauth Central para Tentativa de Conexão de Cliente Bem-Sucedida

Agora você pode analisar o fluxo básico descrito acima em detalhes quando passar pelas depurações. Essas depurações foram coletadas na âncora e na WLC externa para ajudar na sua análise:

```
debug client 00:17:7c:2f:b8:6e
debug aaa detail enable
debug mobility handoff enable
debug web-auth redirect enable mac 00:17:7c:2f:b8:6e
```

Estes detalhes são usados aqui:

```
WLAN name: CWA
WLAN ID: 5
IP address of anchor WLC: 10.105.132.141
IP address of foreign WLC: 10.105.132.160
Redirect ACL used: REDIRECT
Client MAC address: 00:17:7c:2f:b8:6e
New mobility architecture disabled
```

Etapa 1. O cliente inicia o processo de conexão quando envia uma solicitação de associação. Isso é visto no controlador externo:

```
*apfMsConnTask_6: May 08 12:10:35.897: 00:17:7c:2f:b8:6e Association received from mobile on
BSSID dc:a5:f4:ec:df:34
```

Etapa 2. A WLC vê que a LAN sem fio (WLAN) é mapeada para autenticação MAC e move o cliente para o status **AAA pendente**. Ele também inicia o processo de autenticação quando envia uma solicitação de autenticação ao ISE:

```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*aaaQueueReader: May 08 12:10:35.898: Callback.....0x10166e78
*aaaQueueReader: May 08 12:10:35.898: protocolType.....0x40000001
*aaaQueueReader: May 08 12:10:35.898:
proxyState.....00:17:7C:2F:B8:6E-00:00
```

Etapa 3. No ISE, o desvio da autenticação MAC é configurado e retorna o URL de redirecionamento e a ACL após a autenticação MAC. Você pode ver estes parâmetros enviados na resposta de autorização:

```
*radiusTransportThread: May 08 12:10:35.920: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:10:35.920: structureSize.....320
*radiusTransportThread: May 08 12:10:35.920: resultCode.....0
```

```

*radiusTransportThread: May 08 12:10:35.920:
protocolUsed.....0x00000001
*radiusTransportThread: May 08 12:10:35.920:
proxyState.....00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:10:35.920: Packet contains 5 AVPs:
*radiusTransportThread: May 08 12:10:35.920: AVP[01] User-
Name.....00-17-7C-2F-B8-6E (17 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[02]
State.....ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[03]
Class.....CACs:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/38
(54 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[04] Cisco / Url-Redirect-
Acl.....REDIRECT (8 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[05] Cisco / Url-
Redirect.....DATA (91 bytes)

```

Você pode ver as mesmas informações nos registros do ISE. Navegue até **Operações >Autenticações** e clique em **Detalhes da sessão do cliente** conforme mostrado na imagem:

**Result**

User-Name	00-17-7C-2F-B8-6E
State	ReauthSession:0a6984a0000000045371b7c4
Class	CACS:0a6984a0000000045371b7c4:sid-ise-1-2/188796966/714
cisco-av-pair	url-redirect-acl=REDIRECT
cisco-av-pair	url-redirect=https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a0000000045371b7c4&action=cwa

Etapa 4. A WLC estrangeira então altera o estado para auth L2 concluída e envia a resposta da associação ao cliente.

**Note:** Com a autenticação MAC ativada, a resposta da associação não é enviada até que isso seja concluído.

```

*apfReceiveTask: May 08 12:10:35.921: 00:17:7c:2f:b8:6e 0.0.0.0 AUTHCHECK (2) Change state to
L2AUTHCOMPLETE (4)
*apfReceiveTask: May 08 12:10:35.922: 00:17:7c:2f:b8:6e Sending Assoc Response to station on
BSSID dc:a5:f4:ec:df:34 (status 0) ApVapId 5 Slot 0

```

Passo 5: O estrangeiro, então, inicia o processo de transferência para a âncora. Isso é visto na saída do comando debug mobility handoff:

```

*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Attempting anchor export for mobile
00:17:7c:2f:b8:6e
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export:
Client IP: 0.0.0.0, Anchor IP: 10.105.132.141
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e mmAnchorExportSend: Building
UrlRedirectPayload
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export: Sending url redirect acl
REDIRECT

```

Etapa 6. Você pode ver que o cliente entra no estado RUN na WLC externa. O status correto do cliente agora pode ser visto apenas na âncora. Aqui está um trecho do comando show client detail output coletado do exterior (somente informações relevantes são mostradas):

```
Client MAC Address..... 00:17:7c:2f:b8:6e
Client Username ..... 00-17-7C-2F-B8-6E
AP MAC Address..... dc:a5:f4:ec:df:30
BSSID..... dc:a5:f4:ec:df:34
IP Address..... Unknown
Gateway Address..... Unknown
Netmask..... Unknown
Mobility State..... Export Foreign
Mobility Anchor IP Address..... 10.105.132.141
Policy Manager State..... RUN
Policy Manager Rule Created..... Yes
AAA Override ACL Name..... REDIRECT
AAA URL
redirect.....https://10.106.73.98:8443/guestportal/gatewaysessionId=
0a6984a00000004c536bac7b&action=cwa
```

Passo 7. O controlador externo inicia uma solicitação de transferência com a âncora. Agora você pode ver as mensagens de transferência abaixo:

```
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Received Anchor Export request: from Switch
IP: 10.105.132.160
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv:, Mobility role is Unassoc
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv Ssid=cwa Security
Policy=0x42000
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv vapId= 5, Ssid=cwa
AnchorLocal=0x0
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e mmAnchorExportRcv:Url redirect
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e Url redirect ACL REDIRECT
```

A handoff acknowledgement message is also sent to the foreign and can be seen in the debugs on foreign:

```
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Received Anchor Export Ack for client from
Switch IP: 10.105.132.141
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Anchor Mac: d0:c2:82:e2:91:60, Old Foreign
Mac: 30:e4:db:1b:e0:a0 New Foreign Mac: 30:e4:db:1b:e0:a0
```

Etapa 8. Em seguida, o controlador âncora move o cliente para o estado DHCP necessário. Quando o cliente obtém um endereço IP, o controlador continua a processar e mover o cliente para o estado necessário da webauth central. Você pode ver o mesmo na saída show client detail coletada na âncora:

```
Client MAC Address..... 00:17:7c:2f:b8:6e
AP MAC Address..... 00:00:00:00:00:00
Client State..... Associated
Wireless LAN Id..... 5
IP Address..... 10.105.132.254
Mobility State..... Export Anchor
Mobility Foreign IP Address..... 10.105.132.160
Policy Manager State..... CENTRAL_WEB_AUTH
AAA Override ACL Name..... REDIRECT
AAA URL redirect.....
```

https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a0000004c536bac7b&action=cwa

Etapa 9. A WLC externa inicia simultaneamente o processo de contabilização quando move o cliente para o estado de execução. Ele envia a mensagem de início da contabilidade para o ISE:

```
*aaaQueueReader: May 08 12:10:38.803: AccountingMessage Accounting Start: 0x2b6c0a78
*aaaQueueReader: May 08 12:10:38.803: Packet contains 16 AVPs:
*aaaQueueReader: May 08 12:10:38.803: AVP[01] User-Name.....00-17-7C-
2F-B8-6E (17 bytes)
```

**Note:** A contabilização só precisa ser configurada na WLC externa.

Etapa 10. Em seguida, o usuário inicia o processo de redirecionamento de aut da Web inserindo um URL no navegador. Você pode ver as depurações relevantes no controlador de âncora:

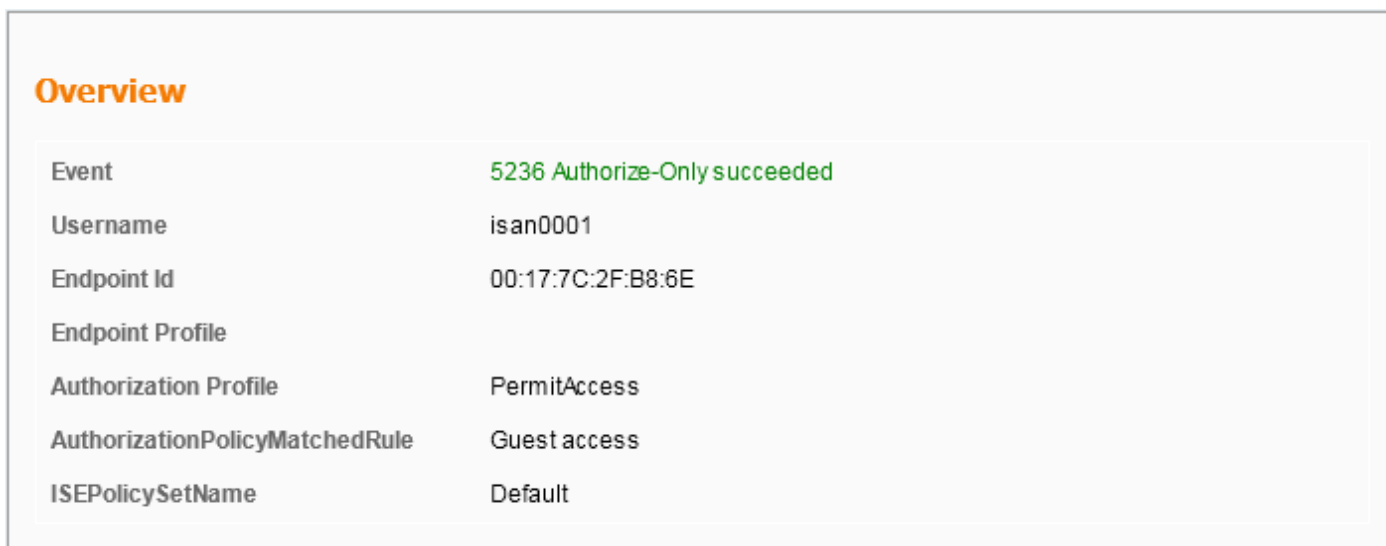
```
*webauthRedirect: May 08 05:53:05.927: 0:17:7c:2f:b8:6e- received connection
*webauthRedirect: May 08 05:53:05.928: captive-bypass detection disabled, Not checking for wispr
in HTTP GET, client mac=0:17:7c:2f:b8:6e
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e: Client configured with AAA overridden
redirect URL
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a0000004c536bac7b&action=cwa
```

Etapa 11. Também podemos ver que a parte de autenticação no processo de webauth é tratada na WLC externa e não na âncora. Você pode ver o mesmo nas saídas de debug AAA no estrangeiro:

```
*aaaQueueReader: May 08 12:11:11.537: AuthenticationRequest: 0x2b6c0a78
*aaaQueueReader: May 08 12:11:11.537: Callback.....0x10166e78
*aaaQueueReader: May 08 12:11:11.537: protocolType.....0x40000001
*aaaQueueReader: May 08 12:11:11.537:
proxyState.....00:17:7C:2F:B8:6E-00:00
*aaaQueueReader: May 08 12:11:11.537: Packet contains 12 AVPs (not shown)
Authorization response from ISE:
*radiusTransportThread: May 08 12:11:11.552: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:11:11.552: structureSize.....252
*radiusTransportThread: May 08 12:11:11.552: resultCode.....0
*radiusTransportThread: May 08 12:11:11.552:
protocolUsed.....0x00000001
*radiusTransportThread: May 08 12:11:11.552:
proxyState.....00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:11:11.552: Packet contains 6 AVPs:
*radiusTransportThread: May 08 12:11:11.552: AVP[01] User-
Name.....isan0001 (8 bytes) -----> (Username used for web
authentication)
*radiusTransportThread: May 08 12:11:11.552: AVP[02]
State.....ReauthSession:0a6984a0000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[03]
Class.....CACs:0a6984a0000004c536bac7b:sid-ise-1-2/188796966/40
(54 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[04] Session-
Timeout.....0x00006e28 (28200) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[05] Termination-
Action.....0x00000000 (0) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[06] Message-
```

Authenticator.....DATA (16 bytes)

O mesmo pode ser verificado no ISE, como mostrado na imagem:



The screenshot shows the 'Overview' section of an ISE event. The event is '5236 Authorize-Only succeeded'. The details are as follows:

Field	Value
Event	5236 Authorize-Only succeeded
Username	isan0001
Endpoint Id	00:17:7C:2F:B8:6E
Endpoint Profile	
Authorization Profile	PermitAccess
AuthorizationPolicyMatchedRule	Guest access
ISEPolicySetName	Default

Etapa 12. Essas informações são passadas para a WLC âncora. Esse handshake não é claramente visível nas depurações e você pode fazer isso pela âncora que aplica uma política de transferência de post como mostrado aqui:

```
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Received Anchor Export policy update, valid mask 0x900:
Qos Level: 0, DSCP: 0, dot1p: 0 Interface Name: , IPv4 ACL Name:
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Applying post-handoff policy for station 00:17:7c:2f:b8:6e - valid mask 0x900
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e QOS Level: -1, DSCP: -1, dot1p: -1, Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Session: 0, User session: 28200, User elapsed 1
Interface: N/A, IPv4 ACL: N/A, IPv6 ACL: N/A.
```

A melhor maneira de verificar se a autenticação está completa é verificar os registros passados no ISE e coletar a saída de show client detail no controlador que deve mostrar o cliente no estado RUN como mostrado aqui:

```
Client MAC Address..... 00:17:7c:2f:b8:6e
Client State..... Associated
Client NAC OOB State..... Access
Wireless LAN Id..... 5
IP Address..... 10.105.132.254
Mobility State..... Export Anchor
Mobility Foreign IP Address..... 10.105.132.160
Policy Manager State..... RUN
```

Outra verificação importante é o fato de que a âncora envia um Protocolo de Resolução de Endereço (ARP - Address Resolution Protocol) gratuito após a autenticação bem-sucedida:

```
*pemReceiveTask: May 08 05:53:23.343: 00:17:7c:2f:b8:6e Sending a gratuitous ARP for 10.105.132.254, VLAN Id 20480
```

A partir daqui, o cliente é livre para enviar todos os tipos de tráfego encaminhado pelo controlador de âncora.

## Fluxo do Webauth Central quando o cliente é desconectado

Quando uma entrada de cliente precisa ser removida da WLC devido a um tempo limite de sessão/ocioso ou quando removemos manualmente o cliente da WLC, estas etapas ocorrem:

A WLC externa envia uma mensagem de cancelamento de autenticação ao cliente e a agenda para exclusão:

```
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e apfMsExpireMobileStation (apf_ms.c:6634)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Associated to
Disassociated
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:6728)
```

Em seguida, ele envia uma mensagem de relatório radius stop para informar ao servidor ISE que a sessão de autenticação do cliente terminou:

```
*aaaQueueReader: May 08 12:19:21.199: AccountingMessage Accounting Stop: 0x2b6d5684
*aaaQueueReader: May 08 12:19:21.199: Packet contains 24 AVPs:
*aaaQueueReader: May 08 12:19:21.199: AVP[01] User-Name.....00-17-7C-
2F-B8-6E (17 bytes)
```

Ele também envia uma mensagem de transferência de mobilidade para a WLC âncora para informá-la de encerrar a sessão do cliente. Isso pode ser visto nas depurações de mobilidade na WLC âncora:

```
*mmListen: May 08 06:01:32.907: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 08 06:01:32.907: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e 10.105.132.254 RUN (20) mobility role
update request from Export Anchor to Handoff
Peer = 10.105.132.160, Old Anchor = 10.105.132.141, New Anchor = 0.0.0.0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e apfMmProcessCloseResponse (apf_mm.c:647)
Expiring Mobile!
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Mobility Response: IP 0.0.0.0 code
Anchor Close (5), reason Normal disconnect (0), PEM State DHCP_REQD, Role Handoff(6)
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Deleting mobile on AP
00:00:00:00:00:00(0)
```

## Conta do cliente suspensa no ISE

O ISE tem a capacidade de suspender uma conta de usuário convidado que sinaliza ao WLC para encerrar a sessão do cliente. Isso é útil para administradores que não precisam verificar a qual WLC o cliente está conectado e simplesmente encerrar a sessão. Agora você pode ver o que acontece quando a conta de usuário convidado é suspensa/expirada no ISE:

O servidor ISE envia uma mensagem de alteração de autorização ao controlador externo, indicando que a conexão do cliente precisa ser removida. Isso pode ser visto nas saídas de depuração:

```
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8 :6e apfMsDeleteByMscb
```



Scheduling mobile for deletion with deleteReason 6, reason Code 252

```
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8:6e Scheduling deletion of Mobile Station: (callerId: 30) in 1 seconds
```

A WLC externa envia uma mensagem de cancelamento de autenticação ao cliente:

```
*apfReceiveTask: May 13 02:01:54.303: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:5921)
```

Ele também envia uma mensagem de parada de contabilidade ao servidor de contabilidade para encerrar a sessão de autenticação do cliente em seu lado:

```
*aaaQueueReader: May 13 02:01:54.303: AccountingMessage Accounting Stop: 0x2b6d2 c7c
*aaaQueueReader: May 13 02:01:54.303: Packet contains 23 AVPs:
*aaaQueueReader: May 13 02:01:54.303: AVP[01] User-Name.....
.....00177c2fb86e (12 bytes)
```

Uma mensagem de transferência também é enviada para a WLC âncora para encerrar a sessão do cliente. Você pode ver isso na WLC âncora:

```
*mmListen: May 12 19:42:52.871: 00:17:7c:2f:b8:6e Received Handoff End request for client from Switch IP: 10.105.132.160
*apfReceiveTask: May 12 19:42:52.872: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
```

## Solucionar problemas da Web central na configuração da âncora do convidado

Agora, vamos analisar alguns dos problemas comuns observados quando você usa o CWA e o que pode ser feito para corrigi-lo.

### Cenário 1. O cliente está preso no estado START e não recebe o endereço IP

Em um cenário de web central, já que a autenticação MAC está habilitada, as respostas de associação são enviadas após a conclusão de uma autenticação MAC. Nesse caso, se houver uma falha de comunicação entre a WLC e o servidor radius ou se houver um erro de configuração no servidor radius que faça com que ele envie rejeitos de acesso, você poderá ver o cliente preso em um loop de associação onde ele repetidamente recebe uma rejeição de associação. Há também uma chance de o cliente ser excluído também se a exclusão do cliente estiver habilitada.

A acessibilidade do servidor radius pode ser verificada com o comando **test aaa radius** disponível no código 8.2 e acima.

O link de referência abaixo mostra como usar isso:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html>

### Cenário 2. O cliente não consegue obter o endereço IP

Há alguns motivos pelos quais um cliente pode falhar ao obter um endereço IP em uma configuração de âncora de convidado CWA.

- A configuração do SSID na âncora e externa não corresponde

É ideal ter a mesma configuração de SSID entre a âncora e as WLCs externas. Alguns dos aspectos para os quais uma verificação rigorosa é feita são configuração de segurança L2/L3, configuração de DHCP e parâmetros de substituição AAA. Caso isso não seja o mesmo, uma transferência para a âncora falha e você pode ver essas mensagens nas depurações de âncora:

```
DHCP dropping packet due to ongoing mobility handshake exchange, (siaddr 0.0.0.0, mobility state = 'apfMsMmAnchorExportRequested')
```

Para atenuar isso, você precisa garantir que a configuração do SSID seja a mesma âncora e externa.

- **O túnel de mobilidade entre as WLCs âncora e externa está inoperante/oscilante**

Todo o tráfego do cliente é enviado em um túnel de dados de mobilidade que usa o protocolo IP 97. Se o túnel de mobilidade não estiver ativado, você poderá ver que o handoff não foi concluído e que o cliente não se move para o estado RUN no estrangeiro. O status do túnel de mobilidade precisa ser mostrado como **UP** e pode ser visto em **Controller > Mobility Management > Mobility Groups** como mostrado na imagem.

Local Mobility Group	Anchor	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status
		80:e0:1d:23:ee:00	10.106.32.10	Anchor	0.0.0.0	Up
		00:f2:8b:2d:62:8b	10.106.32.119	Foreign	0.0.0.0	Up

Se houver apenas um controlador mapeado como membro (estrangeiro ou âncora), você também poderá verificar as estatísticas globais de mobilidade em **Monitor > Statistics > Mobility Statistics**.

- **A ACL de redirecionamento não está configurada na âncora ou nos controladores externos:**

Quando o nome da ACL de redirecionamento enviada pelo servidor radius não corresponde ao que está configurado na WLC externa, mesmo que a autenticação MAC esteja concluída, o cliente é rejeitado e não prossegue para o DHCP. Não é obrigatório configurar as regras individuais da ACL à medida que o tráfego do cliente é encerrado na âncora. Desde que haja uma ACL criada com o mesmo nome da ACL de redirecionamento, o cliente é entregue à âncora. A âncora precisa ter o nome da ACL e as regras configuradas corretamente para que o cliente mude para o estado necessário da webauth.

### Cenário 3. O cliente não é redirecionado para a página da Web

Há novamente alguns motivos diferentes pelos quais uma página da webauth pode não ser exibida. Alguns dos problemas comuns do lado da WLC são abordados aqui:

- **Problemas do servidor DNS**

Os problemas de alcance/configuração incorreta do servidor DNS são uma das razões mais comuns pelas quais os clientes não conseguem ser redirecionados. Isso também pode ser difícil de capturar, pois não é exibido em nenhum registro ou depuração de WLC. O usuário precisa verificar se a configuração do servidor DNS enviada do servidor DHCP está correta e se está acessível do cliente sem fio. Uma simples pesquisa de DNS do cliente inoperante é a maneira mais fácil de verificar isso.

- **Gateway padrão inalcançável quando você usa o servidor DHCP interno na âncora:**

Quando você usa servidores DHCP internos, é importante garantir que a configuração do gateway padrão esteja correta e que a VLAN seja permitida na porta do switch que se conecta à WLC âncora. Caso contrário, o cliente recebe um endereço IP, mas não poderá acessar nada. Você pode verificar o endereço MAC do gateway na tabela ARP do cliente. É uma maneira rápida de verificar a conectividade L2 ao gateway e se ele está acessível.