

# Configurar o CWA sem fio do ISE e os fluxos de hotspot com o AireOS e as WLCs de próxima geração

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar Unified 5508 WLC](#)

[Configuração global](#)

[Configure o identificador do conjunto de serviços \(SSID\) do convidado:](#)

[Configurar a ACL de redirecionamento](#)

[Redirecionamento para HTTPS](#)

[Failover agressivo](#)

[Desvio cativo](#)

[Configurar o 3850 NGWC convergente](#)

[Configuração global](#)

[configuração de SSID](#)

[Configuração de ACL de redirecionamento](#)

[Configuração da interface de linha de comando \(CLI\)](#)

[Configurar o ISE](#)

[Tarefas comuns de configuração do ISE](#)

[Caso de uso 1: CWA com autenticação de convidado em todas as conexões de usuário](#)

[Caso de uso 2: o CWA com o Device Registration impõe a autenticação do convidado uma vez por dia.](#)

[Caso de uso 3: Portal HostSpot](#)

[Verificar](#)

[Caso de uso 1](#)

[Caso de uso 2](#)

[Caso de uso 3](#)

[Switching local FlexConnect no AireOS](#)

[Cenário de Âncora Externa](#)

[Troubleshoot](#)

[Estados quebrados comuns no AireOS e no WLC de acesso convergente](#)

[WLC AireOS](#)

[NGWC](#)

[ISE](#)

[Informações Relacionadas](#)

# Introduction

Este documento descreve como configurar três casos de convidados no Identity Services Engine com Cisco AireOS e Controladores de LAN sem fio de próxima geração.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controladores de LAN sem fio da Cisco (acesso unificado e convergente)
- Identity services engine (ISE)

### Componentes Utilizados

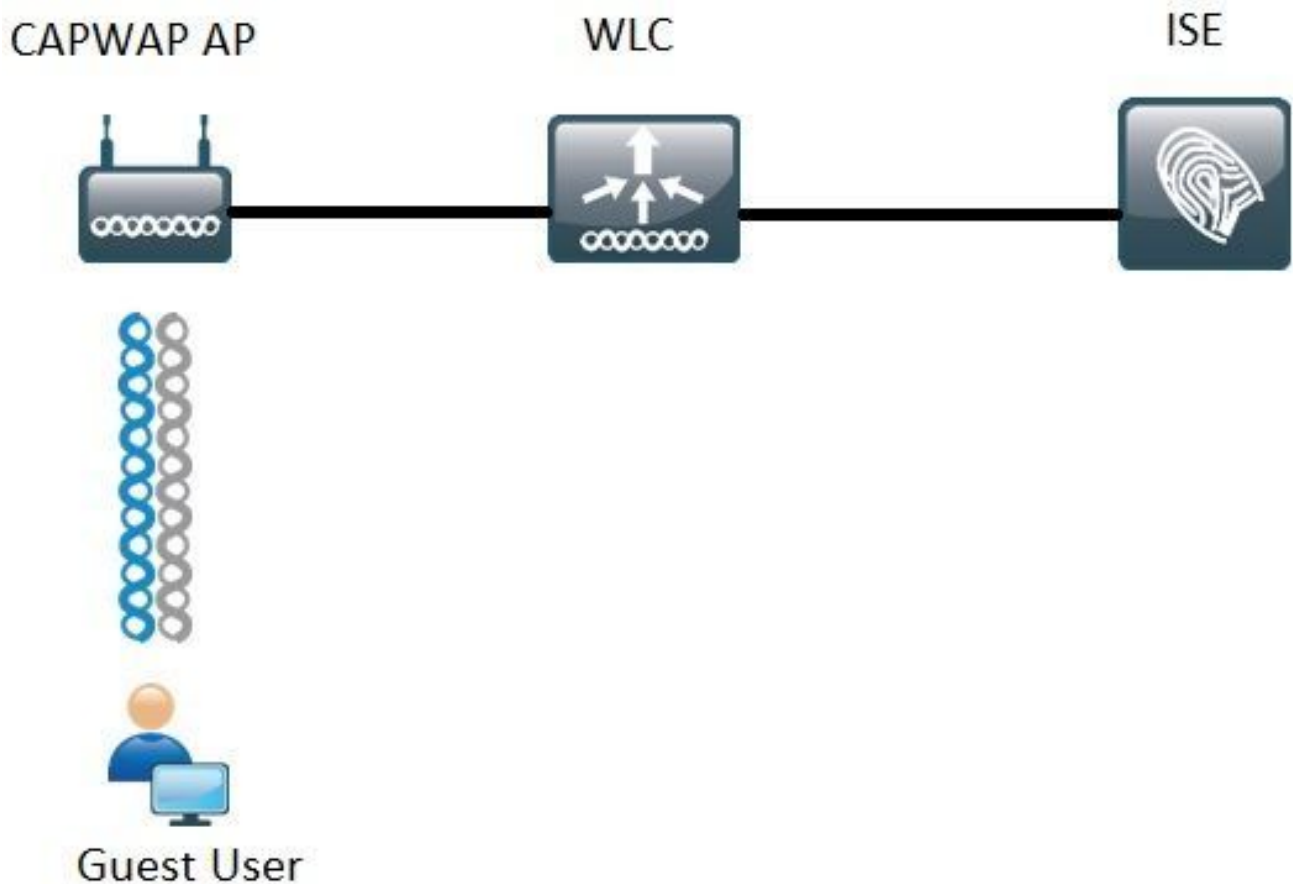
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Services Engine versão 2.1
- Controlador de LAN sem fio Cisco 5508 com 8.0.121.0
- Catalyst 3850 (WS-C3850-24P) do controlador sem fio de próxima geração com 03.06.04.E

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.

## Configurar

### Diagrama de Rede



As etapas abordadas neste documento descrevem a configuração típica em WLCs de acesso unificado e convergente para suportar qualquer fluxo de convidado com ISE.

## Configurar Unified 5508 WLC

Independentemente do caso de uso configurado no ISE, da perspectiva da WLC, tudo começa com um endpoint sem fio que se conecta a um SSID aberto com filtragem MAC habilitada (mais substituição de AAA e NAC RADIUS) que aponta para o ISE como o servidor de autenticação e contabilização. Isso garante que o ISE possa enviar dinamicamente os atributos necessários para a WLC para a aplicação bem-sucedida de um redirecionamento para o Portal de convidados do ISE.

### Configuração global

1. Adicione o ISE globalmente como um servidor de autenticação e contabilização.
  - Navegue para **Security > AAA > Authentication** e clique em **New**

**Security** | **RADIUS Authentication Servers > Edit**

**AAA**  
 General  
 RADIUS  
   Authentication  
   Accounting  
   Fallback  
   DNS  
   Downloaded AVP  
 TACACS+  
 LDAP  
 Local Net Users  
 MAC Filtering  
 Disabled Clients  
   User Login Policies  
   AP Policies  
   Password Policies  
 Local EAP  
 Advanced EAP  
 Priority Order  
 Certificate  
 Access Control Lists

Server Index	6
Server Address(Ipv4/Ipv6)	157.210
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

- Insira o IP do servidor ISE e o segredo compartilhado
- Certifique-se de que o **Server Status** e **Support for RFC 3676** (Change of Authorization or CoA support) estejam ambos definidos como **Enabled**.
- Sob o tempo limite do servidor por padrão, as WLCs AireOS têm 2 segundos. Dependendo das características da rede (latência, ISE e WLC em locais diferentes), pode ser vantajoso aumentar o tempo limite do servidor para pelo menos 5 segundos para evitar eventos de failover desnecessários.
- Clique em **Apply**.
- Se houver vários Policy Services Nodes (PSNs) para configurar, continue para criar entradas adicionais do servidor.

**Observação:** este exemplo de configuração específico inclui 2 instâncias do ISE

- Navegue para **Security > AAA > RADIUS > Accounting** e clique em **New**
- Insira o IP do servidor ISE e o segredo compartilhado
- Verifique se o Status do servidor está definido como **Habilitado**
- Aumente o tempo limite do servidor, se necessário (o padrão é 2 segundos).

## 2. Configuração de fallback.

No ambiente unificado, quando o tempo limite do servidor é acionado, a WLC passa para o próximo servidor configurado. O próximo na linha da WLAN. Se não houver nenhum outro disponível, a WLC selecionará o próximo na lista de servidores globais. Quando vários servidores são configurados no SSID (primário, secundário), uma vez que o failover ocorre, o WLC por padrão continua a enviar tráfego de autenticação e (ou) contabilidade permanentemente para a instância secundária, mesmo se o servidor primário estiver novamente on-line.

Para atenuar esse comportamento, habilite o fallback. Navegue até **Security > AAA > RADIUS > Fallback**. O comportamento padrão está desativado. A única maneira de se recuperar de um evento de servidor inativo requer intervenção administrativa (devolução global do status de administrador do servidor).

Para habilitar o fallback, você tem duas opções:

- **Passivo** - No modo passivo, se um servidor não responder à solicitação de autenticação da WLC, a WLC moverá o servidor para a fila inativa e definirá um temporizador (opção Intervalo em segundos). Quando o temporizador expira, a WLC move o servidor para a fila ativa, independentemente do status real dos servidores. Se a solicitação de autenticação resultar em um evento de tempo limite (o que significa que o servidor ainda está inativo), a entrada do servidor será movida novamente para a fila Inativo e o temporizador será acionado novamente. Se o servidor responder com êxito, ele permanecerá na fila Ativo. Os valores configuráveis aqui vão de 180 a 3600 segundos.
- **Ativo** - No modo ativo, quando um servidor não responde à solicitação de autenticação da WLC, a WLC marca o servidor como inativo e, em seguida, move o servidor para o pool de servidores não ativos e começa a enviar mensagens de sondagem periodicamente até que o servidor responda. Se o servidor responder, a WLC moverá o servidor inativo para o pool ativo e parará de enviar mensagens de sondagem.

Neste modo, a WLC exige que você insira um nome de usuário e um intervalo de sondagem em segundos (180 a 3600).

**Observação:** a sonda WLC não requer uma autenticação bem-sucedida. De qualquer forma, uma autenticação bem-sucedida ou com falha é considerada uma resposta do servidor que é suficiente para promover o servidor para a fila Ativa.

#### Configure o Service Set Identifier (SSID) do convidado:

- Navegue até a guia WLANs e, na opção Create New, clique em Go:



- Digite o nome do perfil e o nome SSID. Clique em Apply.
- Na guia General (Geral), selecione a interface ou o grupo de interface a ser usado (Guest VLAN).



- Em **Security** > Layer 2 > Layer 2 Security selecione None e ative Mac Filtering.



- Na guia **AAA Servers**, defina Authentication and Accounting servers como **enabled** e selecione seus servidores primário e secundário.



- **Atualização Provisória:** esta é uma configuração opcional que não adiciona nenhum benefício a este fluxo. Se preferir ativá-la, o WLC deverá executar o código 8.x ou superior:

**Desativado:** o recurso está completamente desativado.

**Habilitado com Intervalo 0:** A WLC envia atualizações de contabilização ao ISE toda vez que há uma alteração na entrada de MSCB (Mobile Station Control Block) do cliente ( ou seja, Atribuição ou alteração de endereço IPv4 ou IPv6, evento de roaming de cliente.) Nenhuma atualização periódica adicional é enviada.

**Habilitado com um Intervalo Provisório configurado:** Neste modo, o WLC envia notificações ao ISE quando as entradas de MSCB do cliente são alteradas e também envia notificações de contabilidade periódica adicionais no intervalo configurado (independentemente de quaisquer alterações).

- Na guia Advanced (Avançado), selecione **Allow AAA Override** e, em **NAC state**, selecione **RADIUS NAC**. Isso garante que a WLC aplique todos os pares de valores de atributo (AVPs) que vêm do ISE.
- Navegue até a guia SSID geral e defina o status do SSID como **Enabled (Habilitado)**

WLANs > Edit 'Guest'



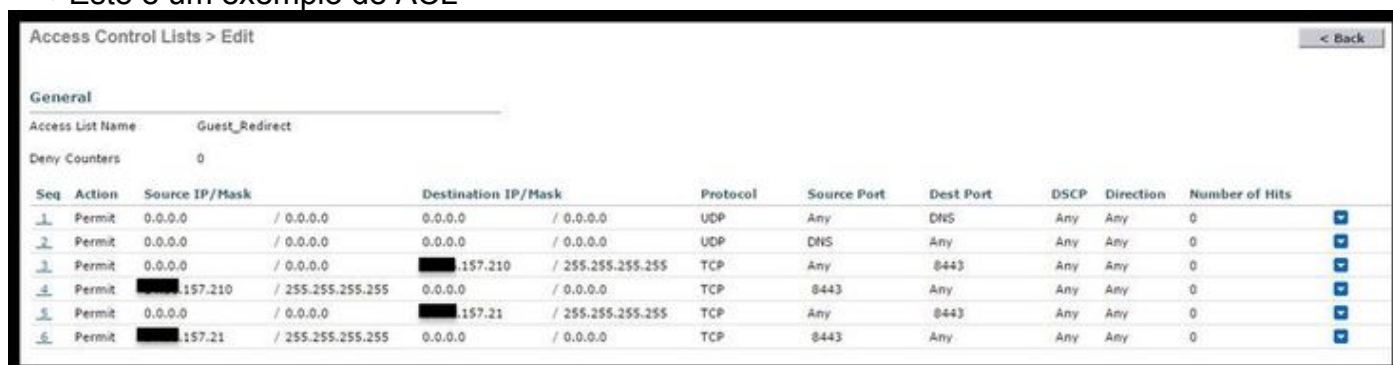
Field	Value
Profile Name	Guest
Type	WLAN
SSID	Guest
Status	<input checked="" type="checkbox"/> Enabled

- Aplique as alterações.

## Configurar a ACL de redirecionamento

Essa ACL é referenciada pelo ISE e determina por qual tráfego é redirecionado e por qual tráfego é permitido.

- Vá para a guia **Segurança > Listas de controle de acesso** e clique em **Novo**
- Este é um exemplo de ACL



Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	157.210 / 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	157.210 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	157.21 / 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	157.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0

Essa ACL deve permitir acesso de e para serviços DNS e nós ISE na porta TCP 8443. Há uma negação implícita na parte inferior que significa que o restante do tráfego é redirecionado para a URL do Portal do convidado do ISE.

## Redirecionamento para HTTPS

Este recurso é suportado nas versões 8.0.x e superiores do AireOS, mas é desativado por padrão. Para habilitar o suporte a HTTPS, vá para **Gerenciamento de WLC > HTTP-HTTPS > Redirecionamento de HTTPS** e defina-o como **Habilitado** ou aplique este comando na CLI:

```
(Cisco Controller) >config network web-auth https-redirect enable
```

## Avisos de certificado após o redirecionamento para HTTPS ser habilitado

Após a habilitação de https-redirect, o usuário poderá ter problemas de confiança de certificado durante o redirecionamento. Isso é visto mesmo se houver um certificado encadeado válido no controlador e mesmo se esse certificado for assinado por uma autoridade de certificação confiável de terceiros. O motivo é que o certificado instalado na WLC é emitido para seu nome de host ou endereço IP da interface virtual. Quando o cliente tenta <https://cisco.com>, o navegador espera que o certificado seja emitido para cisco.com. No entanto, para que a WLC possa interceptar o GET emitido pelo cliente, ela primeiro precisa estabelecer a sessão HTTPS para a qual a WLC apresenta seu Certificado de Interface Virtual durante a fase de handshake SSL. Isso faz com que o navegador exiba um aviso, pois o certificado apresentado durante o handshake SSL não foi emitido para o site original que o cliente está tentando acessar (por exemplo, cisco.com, em oposição ao nome de host da interface Virtual do WLC). Você pode ver mensagens de erro de certificado diferentes em navegadores diferentes, mas todas se relacionam ao mesmo problema.

## Failover agressivo

Esse recurso é habilitado por padrão nas WLCs do AireOS. Quando o failover agressivo é habilitado, a WLC marca o servidor AAA como não respondente e ele se move para o próximo servidor AAA configurado após um evento de timeout de RADIUS afetar um cliente.

Quando o recurso é desabilitado, a WLC faz failover para o próximo servidor somente se o evento de timeout RADIUS ocorrer com pelo menos 3 sessões de cliente. Este recurso pode ser desativado por este comando (nenhuma reinicialização é necessária para este comando):

```
(Cisco Controller) >config radius aggressive-failover disable
```

Para verificar o status atual do recurso:

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

## Desvio cativo

Os endpoints que oferecem suporte a um mecanismo CNA (Captive Network Assistant) para descobrir um portal cativo e iniciar automaticamente uma página de logon geralmente fazem isso por meio de um pseudonavegador em uma janela controlada, enquanto outros endpoints iniciam um navegador totalmente compatível para disparar isso. Para endpoints em que o CNA inicia um pseudonavegador, isso pode interromper o fluxo quando redirecionado para um portal cativo do ISE. Isso normalmente afeta dispositivos Apple IOS e tem efeitos especialmente negativos em fluxos que exigem registro de dispositivo, VLAN DHCP-Release, verificação de conformidade.



Dependa da complexidade do fluxo em uso. Pode ser recomendado ativar o desvio cativo. Nesse cenário, a WLC ignora o mecanismo de descoberta do portal CNA e o cliente precisa abrir um navegador para iniciar o processo de redirecionamento.

Verifique o status do recurso:

```
(Cisco Controller) >show network summary
```

```
Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disabled
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

Para ativar esse recurso, digite este comando:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.
```

You must reset system for this setting to take effect.

A WLC alerta o usuário de que, para que as alterações entrem em vigor, é necessário reiniciar o sistema.

Neste ponto, um **show network summary** mostra o recurso como habilitado, mas para que as alterações entrem em vigor, a WLC precisa ser reiniciada.

## Configurar o 3850 NGWC convergente

### Configuração global

#### 1. Adicionar o ISE globalmente como um servidor de autenticação e contabilização

- Navegue até **Configuration > Security > RADIUS > Servers** e clique em **New**
- Insira o **endereço IP do servidor do ISE**, o **segredo compartilhado**, o **tempo limite do servidor** e a **Contagem de repetições** que reflita suas condições ambientais.
- Certifique-se de que o **suporte para RFC 3570** (suporte a CoA) esteja habilitado.
- Repita o processo para adicionar uma entrada do servidor secundário.

### RADIUS Servers

Radius Servers > **New**

---

Server Name

Server IP Address

Shared Secret

Confirm Shared Secret

Auth Port (0-65535)

Acct Port (0-65535)

Server Timeout (1-1000)secs

Retry Count (0-100)

Support for RFC 3576  ▾

## 2. Criar grupo de servidores do ISE

- Navegue até **Configuration > Security > Server Groups** e clique em **New**
- Atribua um nome ao grupo e insira um valor de **Dead-time** em minutos. Este é o tempo que o controlador mantém o servidor na fila Inativo antes de ser promovido novamente para a lista de servidores ativos.
- Na lista Servidores disponíveis, adicione-os à coluna Servidores atribuídos.

### Radius Server Group

Radius Server Group > **New**

---

Name

MAC-delimiter  ▾

MAC-filtering  ▾

Dead-time (0-1440) in minutes

Group Type

Servers In This Group

**Available Servers**

< >

**Assigned Servers**

ISE2

ISE1

## 3. Ativar globalmente o Dot1x

- Navegue para **Configuration > AAA > Method Lists > General** e habilite **Dot1x system Auth**

## Control

The screenshot shows the 'General' configuration page for 'Dot1x System Auth Control'. The 'Dot1x System Auth Control' checkbox is checked and highlighted with a yellow border. Below it, the 'Local Authentication' and 'Local Authorization' dropdown menus are both set to 'None'.

### 4. Configurar Listas de Métodos

- Navegue até **Configuration > AAA > Method Lists > Authentication** e crie uma nova Method List. Nesse caso, é Tipo Dot1x e Grupo ISE\_Group (grupo criado na etapa anterior). Em seguida, pressione **Aplicar**

The screenshot shows the 'Authentication > New' configuration page. The 'Method List Name' is 'ISE\_Method'. The 'Type' is 'dot1x' (selected with a radio button). The 'Group Type' is 'group' (selected with a radio button). The 'Fallback to local' checkbox is unchecked. Under 'Available Server Groups', there are no groups listed. Under 'Assigned Server Groups', 'ISE\_Group' is listed. Navigation arrows are visible between the two group lists.

- Faça o mesmo para contabilidade (**Configuração > AAA > Listas de métodos > contabilidade**) e autorização (**Configuração > AAA > Listas de métodos > Autorização**). Eles devem se parecer com isso

The screenshot shows the 'Accounting > New' configuration page. The 'Method List Name' is 'ISE\_Method'. The 'Type' is 'identity' (selected with a radio button). Under 'Available Server Groups', there are no groups listed. Under 'Assigned Server Groups', 'ISE\_Group' is listed. Navigation arrows are visible between the two group lists.

**Authorization**  
Authorization > New

Method List Name:

Type:  network  exec  credential-download

Group Type:  group  local

Available Server Groups:

Assigned Server Groups:

Groups In This Method:

## 5. Crie o método de filtro MAC de autorização.

Isso é chamado posteriormente nas configurações de SSID.

- Navegue para **Configuration > AAA > Method Lists > Authorization** e clique em **New**.
- Insira o nome da lista de métodos. Escolha **Type = Network** e **Group Type Group**.
- Adicione ISE\_Group ao campo Grupos de servidores atribuídos.

**Authorization**  
Authorization > New

Method List Name:

Type:  network  exec  credential-download

Group Type:  group  local

Available Server Groups:

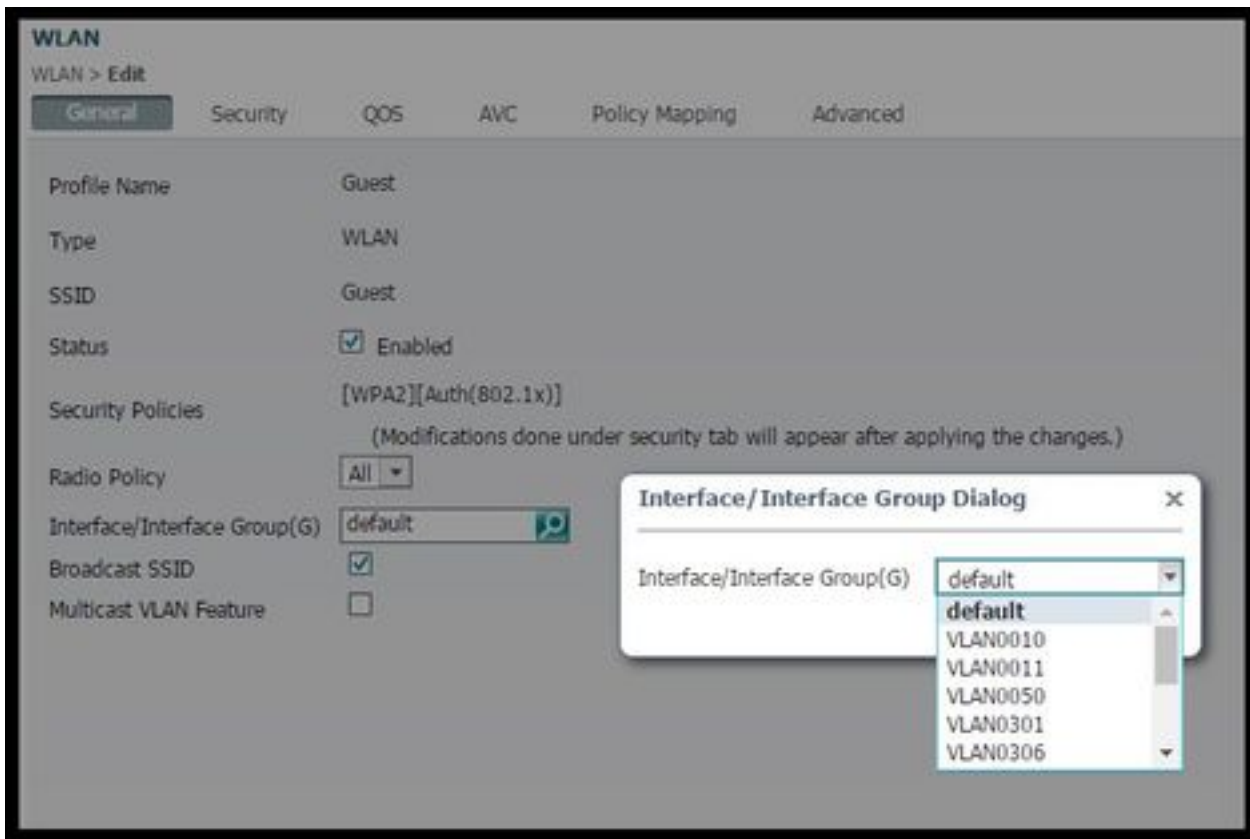
Assigned Server Groups:

Groups In This Method:

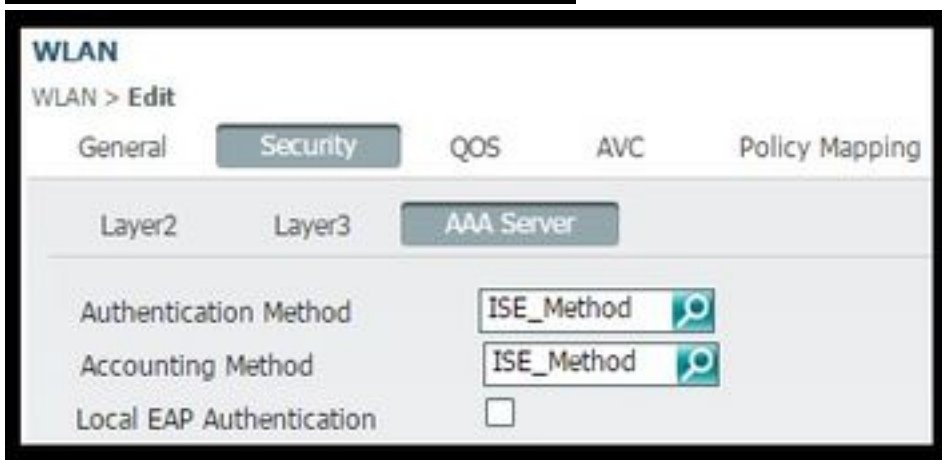
## configuração de SSID

### 1. Crie o SSID de Convidado

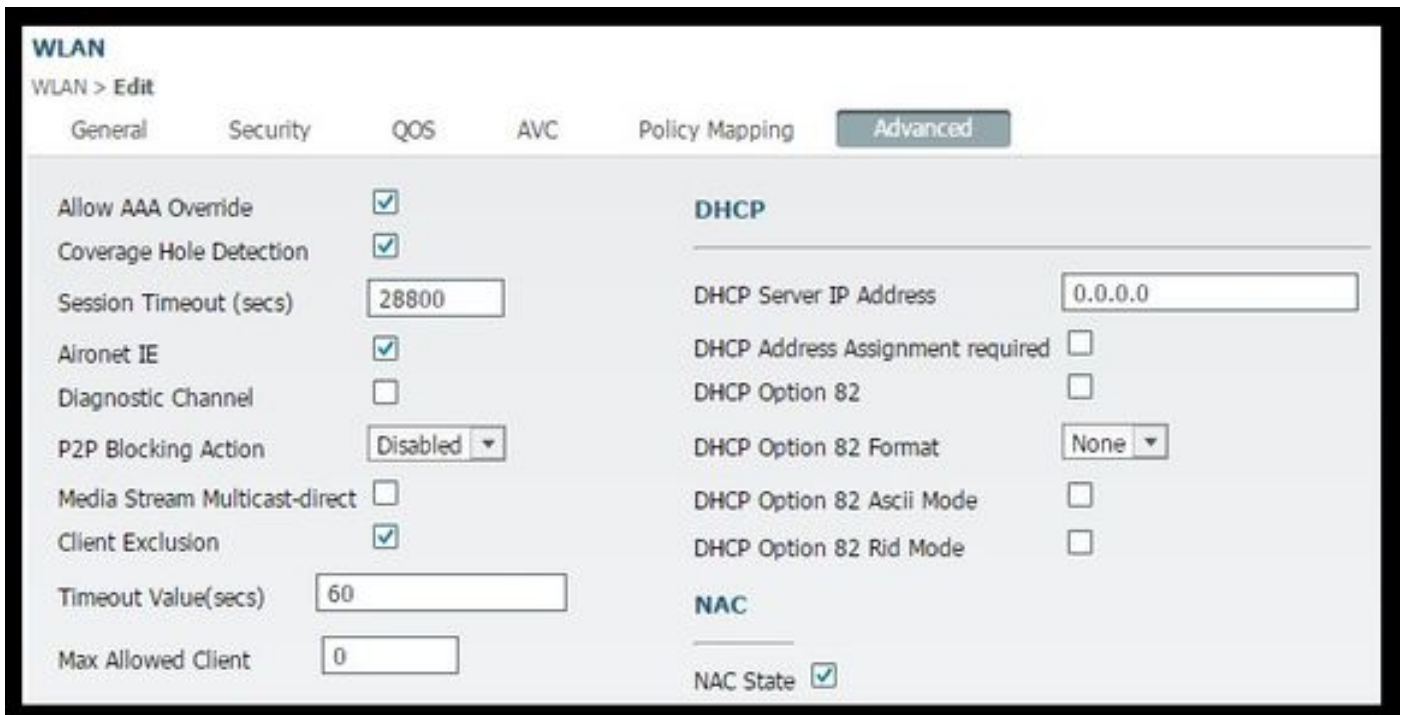
- Navegue até **Configuration > Wireless > WLANs** e clique em **New**
- Insira o ID da WLAN, o SSID e o nome do perfil e clique em **Apply (Aplicar)**.
- Quando estiver nas configurações de SSID em Interface / Interface Group, selecione a interface de Camada 3 da VLAN de convidado.



- Em **Security > Layer 2**, selecione **None** e, ao lado de **Mac Filtering**, insira o nome da lista de métodos de filtro Mac que você configurou anteriormente (MacFilterMethod).
- Na guia **Security > AAA Server**, selecione as listas apropriadas de métodos de autenticação e contabilização (ISE\_Method).



- Na guia **Advanced**, habilite **Allow AAA Override** e o **estado NAC**. O restante das configurações deve ser ajustado de acordo com cada requisito de implantação (tempo limite da sessão, Exclusão do cliente, Suporte para extensões Aironet).



- Navegue até a Guia Geral e defina o Status como Ativado. Em seguida, pressione **Aplicar**.

### Configuração de ACL de redirecionamento

Essa ACL é referenciada pelo ISE posteriormente no access-accept em resposta à solicitação MAB inicial. O NGWC a utiliza para determinar o tráfego a ser redirecionado e o tráfego pelo qual deve ser permitido.

- Navegue até **configuration > security > ACL > Access Control Lists** e clique em **Add New**.
- Selecione Extended e insira o nome da ACL.
- Esta figura mostra um exemplo de uma ACL de redirecionamento típica:



**Observação:** a linha 10 é opcional. Isso geralmente é adicionado para propostas de solução de problemas. Essa ACL deve permitir acesso ao DHCP, aos serviços DNS e também à

porta TCP 8443 (negar ACEs) dos servidores ISE. O tráfego HTTP e HTTPS é redirecionado (permitir ACEs).

## Configuração da interface de linha de comando (CLI)

Todas as configurações discutidas nas etapas anteriores também podem ser aplicadas através da CLI.

### 802.1x globalmente habilitado

```
dot1x system-auth-control
```

## Configuração global de AAA

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
  client 172.16.157.210 server-key *****
  client 172.16.157.21 server-key *****
  auth-type any
!
radius server ISE1
  address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
radius server ISE2
  address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
!
aaa group server radius ISE_Group
  server name ISE2
  server name ISE1
  deadtime 10
  mac-delimiter colon
!
```

## Configuração de WLAN

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
mac-filtering MacFilterMethod
nac
no security wpa
```

```
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
no shutdown
```

## Exemplo de ACL de redirecionamento

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
 10 deny icmp any any
 20 deny udp any any eq bootps
 30 deny udp any any eq bootpc
 40 deny udp any any eq domain
 50 deny tcp any host 172.16.157.210 eq 8443
 60 deny tcp any host 172.16.157.21 eq 8443
 70 permit tcp any any eq www
 80 permit tcp any any eq 443
```

## Suporte a HTTP e HTTPS

```
3850#show run | inc http
ip http server
ip http secure-server
```

**Observação:** se você aplicar uma ACL para restringir o acesso à WLC sobre HTTP, isso afetará o redirecionamento.

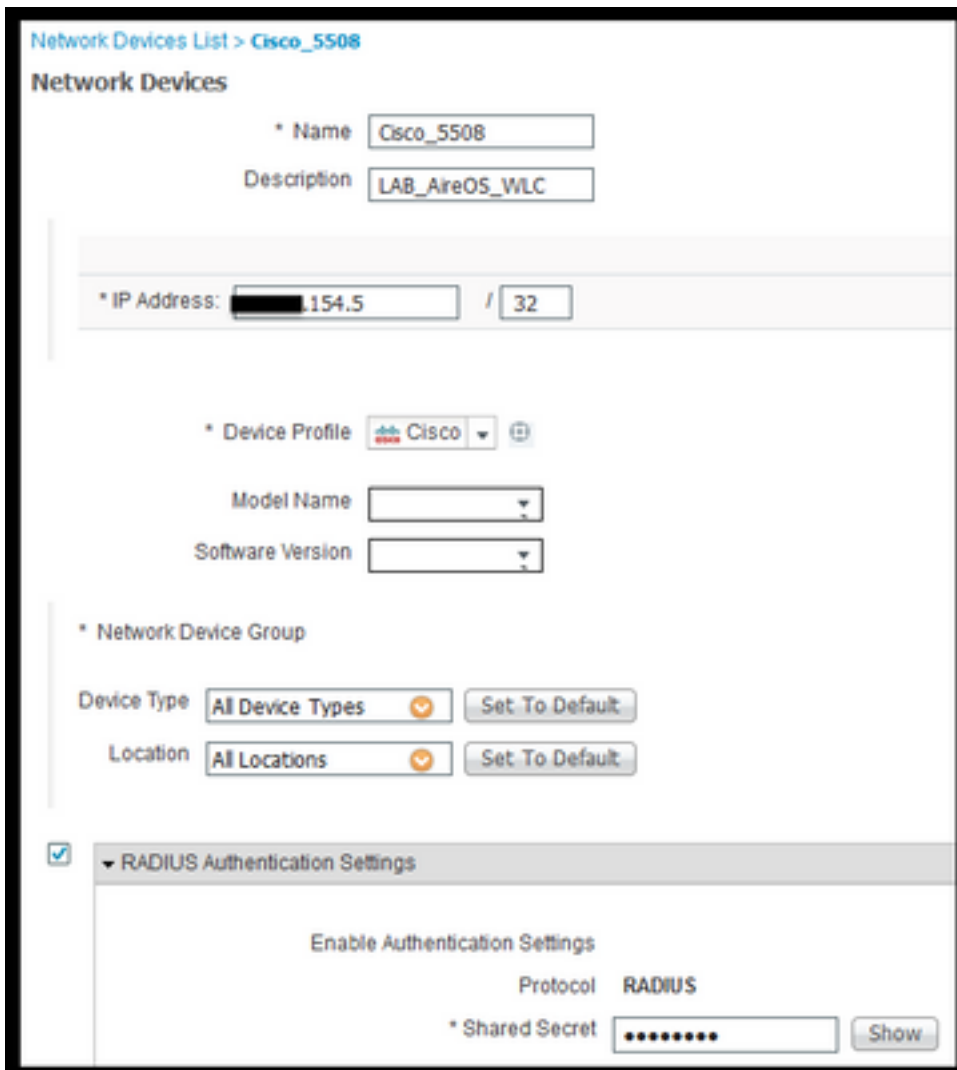
## Configurar o ISE

Esta seção descreve a configuração necessária no ISE para suportar todos os casos de uso discutidos neste documento.

### Tarefas comuns de configuração do ISE

1. Faça login no ISE, navegue até **Administration > Network Resources > Network Devices** e clique em **Add**
2. Insira o **Nome** associado à WLC e o **endereço IP** do dispositivo.
3. Marque a caixa **configurações de autenticação de RADIUS** e digite o **Shared Secret** configurado no lado da WLC. Em seguida, clique em **Enviar**.



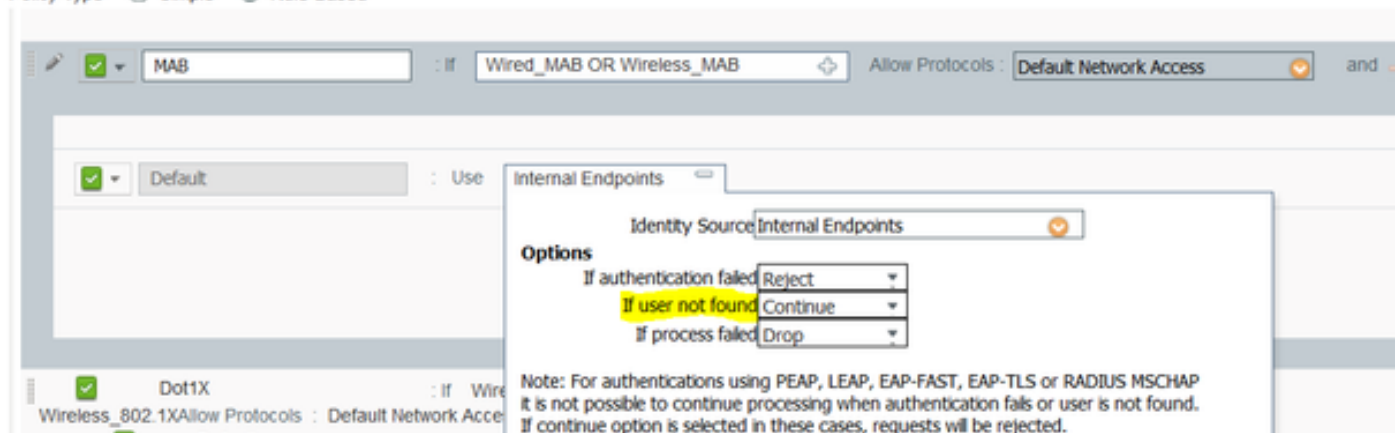


4. Navegue para Política > Autenticação e, em MAB, clique em Editar e certifique-se de que, em Usar: Pontos Finais Internos, a opção Se o usuário não for encontrado esteja definida como Continuar (Ela deve estar lá por padrão).

#### Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type  Simple  Rule-Based



Caso de uso 1: CWA com autenticação de convidado em todas as conexões de usuário

#### Visão geral do fluxo

1. O usuário sem fio se conecta ao SSID convidado.

2. A WLC autentica o endpoint com base em seu endereço MAC no ISE como servidor AAA.
3. O ISE retorna e acessa-aceita com dois AVPs (Attribute Value Pairs): url-redirect e url-redirect-acl. Quando a WLC aplica esses AVPs à sessão de endpoint, a estação faz a transição para DHCP-Required e, quando obtém um endereço IP, permanece em CENTRAL\_WEB\_AUTH. Nesta etapa, a WLC está pronta para iniciar o redirecionamento do tráfego http / https do cliente.
4. O usuário final abre o navegador da Web e uma vez que o tráfego HTTP ou HTTPS é gerado, a WLC redireciona o usuário para o portal de convidado do ISE.
5. Quando o usuário chega ao Portal do convidado, ele solicita que você insira as credenciais do convidado (criadas pelo patrocinador nesse caso).
6. Após a validação das credenciais, o ISE exibe a página AUP e, uma vez que o cliente aceita, um tipo de CoA dinâmico Re-authenticate é enviado para a WLC.
7. A WLC processa novamente a autenticação de filtragem MAC sem emitir uma desautenticação para a estação móvel. Isso deve ser perfeito para o endpoint.
8. Quando o evento de reautenticação acontece, o ISE reavalia as políticas de Autorização e, desta vez, o ponto final recebe um acesso de Permissão desde que houve um evento de autenticação de convidado bem-sucedido anterior.

Esse processo se repete toda vez que o usuário se conecta ao SSID.

## Configuração

1. Navegue até o ISE e navegue até **Centros de trabalho > Acesso de convidado > Configurar > Portais de convidado > Selecionar Portal de convidado patrocinado** (ou crie um novo tipo de portal Patrocinado-convidado).
2. Em **Guest Device Registration**, desmarque todas as opções e clique em **Save**.



3. Navegue até **Política > Elementos de Política > Resultados > Autorização > Perfis de Autorização**. Clique em **Add**.

4. Este perfil é enviado para a WLC através do **Redirect-URL** e do **Redirect-URL-ACL** em resposta à solicitação inicial de desvio de autenticação de Mac (MAB).

- Depois que o redirecionamento da Web (CWA, MDM, NSP, CPP) for verificado, selecione **Centralized Web Auth** e, em seguida, digite o nome da ACL de redirecionamento no campo **ACL** e, em **Value**, selecione o **Patrocinado Guest Portal(default)** (ou qualquer outro portal específico criado nas etapas anteriores).

O perfil deve ser semelhante ao desta imagem. Em seguida, clique em **Salvar**.

## Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

## Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) (i)

Centralized Web Auth  ACL  Value

Display Certificates Renewal Message

Static IP/Host name/FQDN

Detalhes do atributo na parte inferior da página os Pares de valor do atributo (AVPs) à medida que são enviados para a WLC

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-act=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
```

5. Navegue até **Política > Autorização** e insira uma nova regra. Essa regra é a que dispara o processo de redirecionamento em resposta à solicitação de autenticação MAC inicial da WLC. (Nesse caso, chamada **Wireless\_Guest\_Redirect**).

6. Em **Condições**, escolha **Selecionar Condição Existente na Biblioteca** e, em seguida, em **nome da condição**, selecione **Condição composta**. Selecione uma condição composta predefinida chamada **Wireless\_MAB**.

**Observação:** essa condição consiste em 2 atributos Radius esperados na solicitação de acesso originados da WLC (NAS-Port-Type= IEEE 802.11 <presente em todas as solicitações sem fio> e Service-Type = Call Check< que se refere a uma solicitação específica para um desvio de autenticação MAC> )

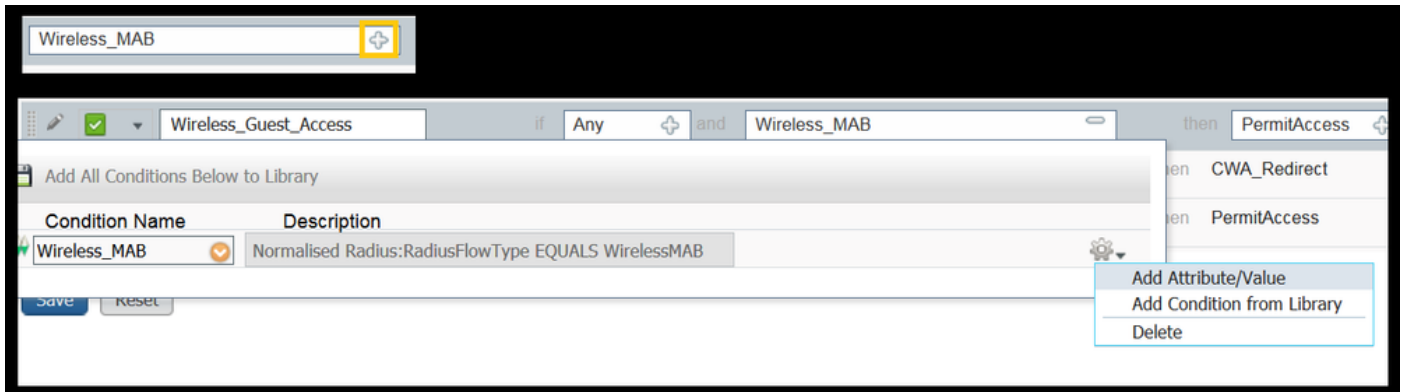
7. Em resultados, selecione **Padrão > CWA\_Redirect** (Perfil de autorização criado na etapa anterior). Em seguida, clique em **Concluído e Salvar**

Wireless\_Guest\_Redirect if Wireless\_MAB then CWA\_Redirect [Edit](#)

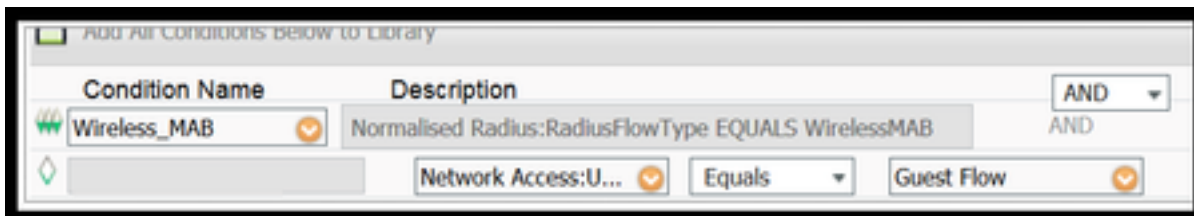
8. Navegue até o final da regra **CWA\_Redirect** e clique na seta ao lado de **Edit**. Em seguida, selecione **duplicar acima**.

9. Modifique o nome, pois essa é a política à qual o endpoint corresponde quando a sessão é reautenticada no CoA do ISE (nesse caso, Wireless\_Guest\_Access).

10. Ao lado da condição composta **Wireless\_MAB**, clique no símbolo + para expandir as condições e, ao final da condição **Wireless\_MAB**, clique em **Adicionar Atributo/Valor**.



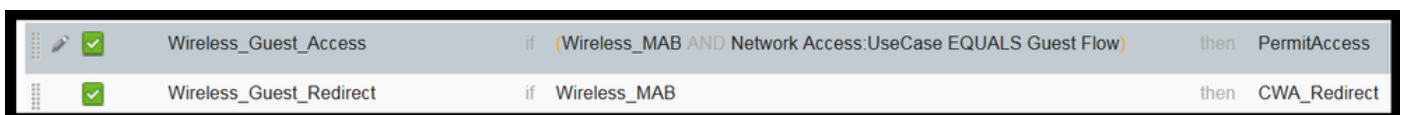
11. Em "Selecionar atributo", escolha **Acesso à rede > Caso de uso igual ao fluxo do convidado**



12. Em **Permissions**, selecione **PermitAccess**. Em seguida, clique em **Concluído** e **Salvar**



As duas políticas devem ser semelhantes a esta:



**Caso de uso 2: o CWA com o Device Registration impõe a autenticação do convidado uma vez por dia.**

### Visão geral do fluxo

1. O usuário sem fio se conecta ao SSID convidado.
2. A WLC autentica o endpoint com base em seu endereço MAC no ISE como servidor AAA.
3. O ISE retorna e acessa-aceita com dois Pares de Valores de Atributos (AVPs) ( url-redirect e url-redirect-acl).
4. Quando a WLC aplica esses AVPs à sessão de endpoint, a estação faz a transição para DHCP-Required e, quando obtém um endereço IP, permanece em CENTRAL\_WEB\_AUTH. Nesta etapa, a WLC está pronta para iniciar o redirecionamento do tráfego http / https do cliente.
5. O usuário final abre o navegador da Web e uma vez que o tráfego HTTP ou HTTPS é gerado, a WLC redireciona o usuário para o portal de convidado do ISE.

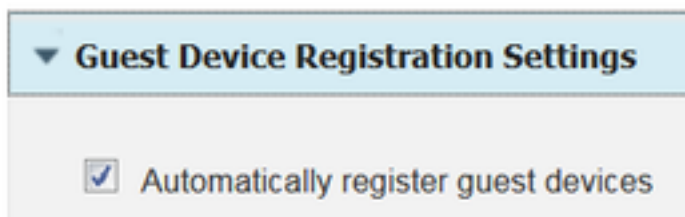
6. Quando o usuário chega ao Portal do convidado, ele é solicitado a inserir credenciais criadas pelo patrocinador.
7. Mediante validação de credenciais, o ISE adiciona esse endpoint a um grupo de identidade de endpoint específico (pré-configurado) (registro de dispositivo).
8. A página AUP é exibida e, uma vez que o cliente aceite, um tipo de CoA dinâmico é Re-authenticate. É enviado para a WLC.
9. A WLC processará novamente a autenticação de filtragem MAC sem emitir uma desautenticação para a estação móvel. Isso deve ser perfeito para o endpoint.
10. Quando o evento de reautenticação ocorre, o ISE reavalia as políticas de autorização. Desta vez, como o ponto final é membro do grupo de identidade de ponto final correto, o ISE retorna uma aceitação de acesso sem restrições.
11. Como o ponto de extremidade foi registrado na etapa 6, sempre que o usuário voltar, ele terá permissão na rede até que seja removido manualmente do ISE, ou uma Política de Limpeza de Ponto de Extremidade será executada, liberando os pontos de extremidade que atenderem aos critérios.

Neste cenário de laboratório, a autenticação é aplicada uma vez por dia. O gatilho de reautenticação é a Política de Limpeza de Ponto de Extremidade que remove todos os pontos de extremidade do Grupo de Identidade de Ponto de Extremidade usado todos os dias.

**Observação:** é possível aplicar o evento de autenticação de convidado com base no tempo decorrido desde a última aceitação AUP. Isso pode ser uma opção se você precisar aplicar o Logon de convidado com mais frequência do que uma vez por dia (por exemplo, a cada 4 horas).

## Configuração

1. No ISE, navegue para **Centros de trabalho > Acesso de convidado > Configurar > Portais de convidado > Selecionar Portal de convidado patrocinado** (ou crie um novo tipo de portal Patrocinado-Convidado).
2. Em **Guest Device Registration**, verifique se a opção **Registrar dispositivos convidados automaticamente** está marcada. Click **Save**.



3. Navegue para **Centro de trabalho > Acesso de convidado > Configurar > Tipos de convidado** ou apenas clique no atalho especificado em Configurações de registro do dispositivo de convidado no portal.

## ▼ Guest Device Registration Settings

Automatically register guest devices

*A message displays to guests when they reach the maximum number of supported devices.*

Allow guests to register devices

*You can set the maximum number of supported devices in the guest type settings.*

*Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.*

*Configure guest types at:*

[Work Centers > Guest Access > Configure > Guest Types](#)

4. Quando o Usuário Patrocinador cria uma conta de convidado, ele atribui um tipo de convidado a ela. Cada Tipo de Convidado individual pode ter um ponto de extremidade registrado que pertence a um Grupo de Identidade de Ponto de Extremidade diferente. Para atribuir o Grupo de Identidade de Ponto de Extremidade ao qual o dispositivo deve ser adicionado, selecione o Tipo de Convidado que o patrocinador usa para esses usuários convidados (esse caso de uso baseia-se em Semanal (padrão)).

5. Uma vez no tipo de convidado, em **Opções de Login** selecione o Grupo de Endpoint no menu suspenso **Grupo de Identidade de Endpoint para registro de dispositivo de convidado**

Maximum devices guests can register:  (1-999)

Endpoint identity group for guest device registration:  ⓘ

6. Navegue até **Política > Elementos de Política > Resultados > Autorização > Perfis de Autorização**. Clique em Add.

7. Este perfil é enviado para a WLC através do **Redirect-URL** e do **Redirect-URL-ACL** em resposta à solicitação inicial de desvio de autenticação de Mac (MAB).

- Depois que o redirecionamento da Web (CWA, MDM, NSP, CPP) for verificado, selecione **Autenticação da Web centralizada**, em seguida, digite o nome da ACL de redirecionamento no campo **ACL** e, em Valor, selecione o portal criado para esse fluxo (CWA\_DeviceRegistration).

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

---

▼ Common Tasks

VLAN

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Centralized Web Auth  ACL  Value

8. Navegue até **Política > Autorização** e insira uma nova regra. Essa regra é a que dispara o processo de redirecionamento em resposta à solicitação de autenticação MAC inicial da WLC. (Nesse caso, chamada **Wireless\_Guest\_Redirect**).

9. Em **Condições**, escolha **Selecionar Condição Existente na Biblioteca** e, em seguida, em **nome da condição**, selecione **Condição composta**. Selecione uma condição composta predefinida chamada **Wireless\_MAB**.

10. Em Results, selecione **Standard > CWA\_DeviceRegistration** (perfil de autorização criado na etapa anterior). Em seguida, clique em **Concluído e Salvar**

Wireless\_Guest\_Redirect if Wireless\_MAB then CWA\_DeviceRegistration

11. Duplique a política acima, modifique seu nome, pois esta é a política atingida pelo ponto final após retornar do evento de reautenticação (chamado **Wireless\_Guest\_Access**).

12. Na caixa **Identity Group Details**, selecione **Endpoint Identity Group** e selecione o grupo ao qual você fez referência em Guest Type(GuestEndpoints).

13. Em Resultados, selecione **PermitAccess**. Clique em **Concluído e Salvar** as alterações.

Wireless\_Guest\_Access if GuestEndpoints AND Wireless\_MAB then PermitAccess  
 Wireless\_Guest\_Redirect if Wireless\_MAB then CWA\_DeviceRegistration

14. Crie uma política de limpeza de ponto de extremidade que limpe o Grupo de Pontos de Extremidade do Convidado diariamente.

- Navegue até **Administração > Gerenciamento de identidades > Configurações > Expurgação de endpoint**
- Em **Purge** rules, deve haver uma que acione a exclusão de GuestEndpoints se o tempo decorrido for maior que 30 dias.
- Modifique a política existente para GuestEndpoints ou crie uma nova (caso o padrão tenha sido removido). Observe que as políticas de expurgação são executadas todos os dias em um horário definido.


Nesse caso, a condição é Membros de GuestEndpoints com Dias Decorridos menos de 1 dia

### Caso de uso 3: Portal HostSpot

#### Visão geral do fluxo

1. O usuário sem fio se conecta ao SSID convidado.
2. A WLC autentica o endpoint com base em seu endereço MAC usando o ISE como servidor AAA.
3. O ISE retorna um access-accept com dois Pares de Valores de Atributo (AVPs): url-redirect e url-redirect-acl.
4. Quando a WLC aplica esses AVPs à sessão de endpoint, a estação faz a transição para DHCP-Required e, quando obtém um endereço IP, permanece em CENTRAL\_WEB\_AUTH. Nesta etapa, a WLC está pronta para redirecionar o tráfego http / https do cliente.
5. O usuário final abre o navegador da Web e uma vez que o tráfego HTTP ou HTTPS é gerado, a WLC redireciona o usuário para o ISE HotSpot Portal.
6. Uma vez no portal, o usuário é solicitado a aceitar uma Política de uso aceitável.
7. O ISE adiciona o endereço MAC do ponto final (ID do ponto final) ao grupo de identidade do ponto final configurado.
8. O Policy Services Node (PSN) que processa a solicitação emite um tipo de CoA dinâmico **Admin-Reset** para o WLC.
9. Quando a WLC termina de processar o CoA de entrada, ela emite uma desautenticação para o cliente (a conexão é perdida pelo tempo que leva para o cliente voltar).
10. Depois que o cliente se reconecta, uma nova sessão é criada para que não haja continuidade de sessão no ISE. Isso significa que a autenticação é processada como um novo thread.
11. Como o ponto final é adicionado ao grupo de identidade do ponto final configurado e há uma política de autorização que verifica se o ponto final faz parte desse grupo, a nova autenticação corresponde a essa política. O resultado é acesso total à rede de convidado.
12. O usuário não deve ter que aceitar a AUP novamente, a menos que o Objeto de Identidade de Ponto de Extremidade seja removido do banco de dados do ISE como resultado de uma política de limpeza de ponto de extremidade.

#### Configuração

1. Crie um Novo Grupo de Identidade de Ponto de Extremidade para mover esses dispositivos após o registro. Navegue até **Centros de trabalho > Acesso de convidado > Grupos de identidade > Grupos de identidade de endpoint** e clique em  .
- Digite um nome de grupo (neste caso, HotSpot\_Endpoints). Adicione uma descrição e nenhum grupo pai será necessário.



Endpoint Identity Group List > HotSpot\_Endpoints

### Endpoint Identity Group

\* Name

Description

Parent Group

2. Navegue até **Centros de trabalho > Acesso de convidado > Configurar > Portais de convidado > selecione Portal de hotspot (padrão)**.

3. Expanda Configurações do Portal e, em Grupo de Identidade do Ponto Final, selecione o grupo **HotSpot\_Endpoints** em **Grupo de Identidade do Ponto Final**. Envie os dispositivos registrados para o grupo especificado.

Endpoint

Identity *Configure endpoint identity groups at:*

group: \* [Work Centers > Guest Access > Identity Groups](#)

4. **Salve** as alterações.

5. Crie o perfil de Autorização que aciona o Portal HotSpot na autenticação MAB originada pela WLC.

- Navegue para **Política > Elementos de política > Resultados > autorização > Perfis de autorização** e crie um (HotSpotRedirect).
- Depois que o **redirecionamento da Web (CWA, MDM, NSP, CPP)** for marcado, selecione **Hot Spot** e digite o nome da ACL de redirecionamento no campo ACL (Guest\_Redirect) e, como um valor, selecione o portal correto (**Hotspot Portal ( padrão )**).

**Add New Standard Profile**

**Authorization Profile**

\* Name:

Description:

\* Access Type:

Network Device Profile:

---

**Common Tasks**

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Hot Spot:     ACL:     Value:

Static IP/Host name/FQDN

---

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
 cisco-av-pair = url-redirect-ad=Guest\_Redirect  
 cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw

6. Crie a Política de Autorização que dispara o resultado HotSpotRedirect na solicitação MAB inicial da WLC.

- Navegue até **Política > Autorização** e insira uma nova regra. Essa regra é a que dispara o processo de redirecionamento em resposta à solicitação de autenticação MAC inicial da WLC. (Nesse caso, chamada **Wireless\_HotSpot\_Redirect**).
- Em **Condições**, escolha **Selecionar condição existente da biblioteca**, em seguida, em **nome da condição** selecione **Condição composta**
- Em **Results**, selecione **Standard > HotSpotRedirect** (Perfil de autorização criado na etapa anterior). Em seguida, clique em **Concluído e Salvar**

7. Crie a segunda Política de Autorização.

- Duplique a política acima e modifique seu nome, pois esta é a política atingida pelo ponto final após retornar do evento de reautenticação (chamado **Wireless\_HotSpot\_Access**).
- Na caixa **Identity Group Details**, selecione **Endpoint Identity Group** e o grupo criado anteriormente (**HotSpot\_Endpoints**).
- Em **Resultados**, selecione **PermitAccess**. Clique em **Concluído e Salvar** as alterações.

✓	Wireless_HotSpot_Access	if	HotSpot_Endpoints AND Wireless_MAB	then	PermitAccess
✓	Wireless_HotSpot_Redirect	if	Wireless_MAB	then	HotSpotRedirect

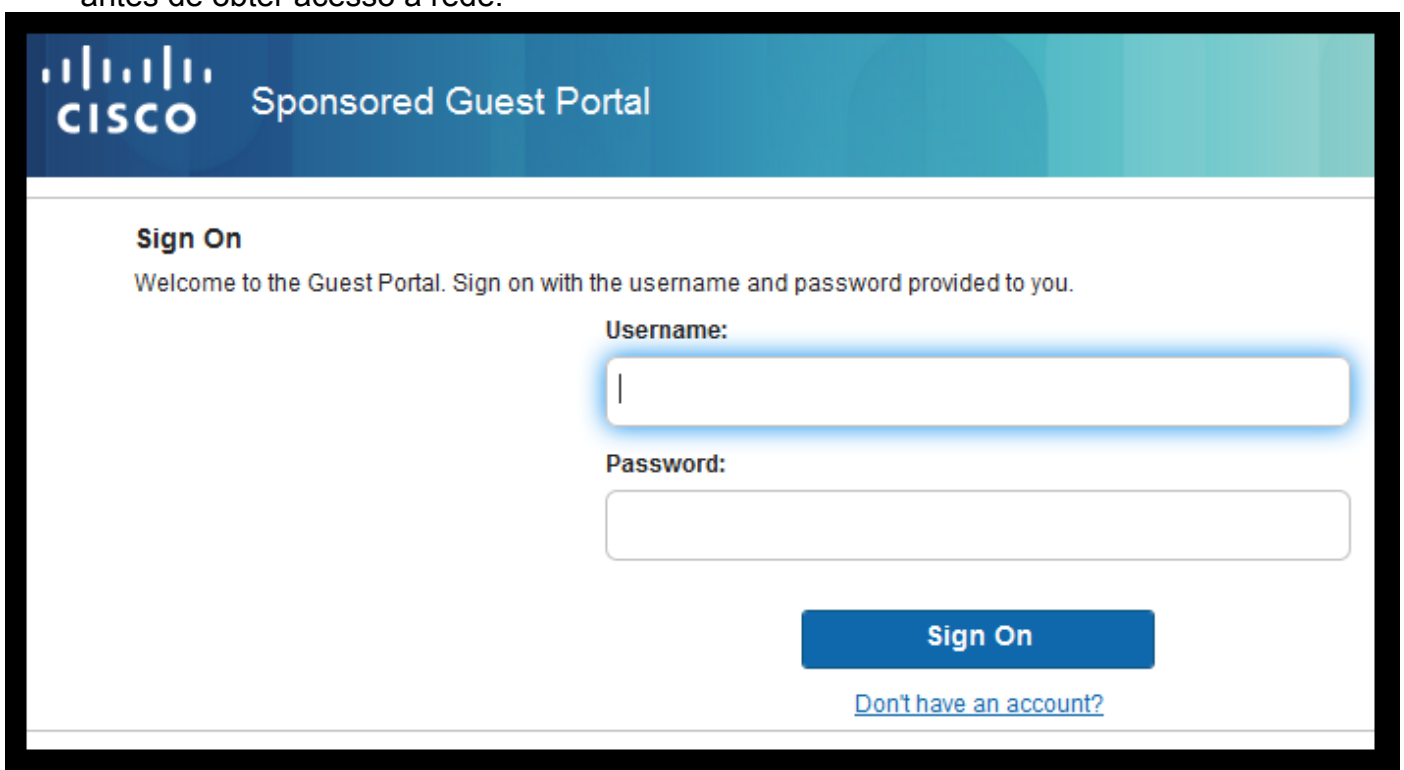
8. Configure a política de expurgação que apaga pontos finais com um Tempo decorrido maior que 5 dias.

- Navegue até **Administração > Gerenciamento de identidades > Configurações > Expurgação de endpoint** e, em Regras de expurgação, crie um novo.
- Na caixa **Identity Group Details**, selecione **Endpoint Identity Group > HotSpot\_Endpoints**
- Em **condições**, clique em **Criar nova condição (opção avançada)**.
- Em **Selecionar atributo**, escolha **ENDPOINTPURGE : ElapsedDays GREATER THAN 5 dias**

## Verificar

### Caso de uso 1

1. O usuário se conecta ao SSID convidado.
2. Ele abre o navegador e assim que o tráfego HTTP é gerado, o portal do convidado é exibido.
3. Depois que o usuário convidado autentica e aceita a AUP, uma página de sucesso é exibida.
4. Um CoA autenticado novamente é enviado (transparente para o cliente).
5. A sessão de endpoint é reautenticada com acesso total à rede.
6. Qualquer conexão de convidado subsequente deve passar pela autenticação de convidado antes de obter acesso à rede.



The screenshot shows the Cisco Sponsored Guest Portal Sign On page. The header features the Cisco logo and the text "Sponsored Guest Portal". Below the header, the page is titled "Sign On" and includes a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". A blue "Sign On" button is located below the password field. At the bottom, there is a link that says "Don't have an account?".



## Sponsored Guest Portal

### Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



## Sponsored Guest Portal

Success

You now have Internet access through this network.

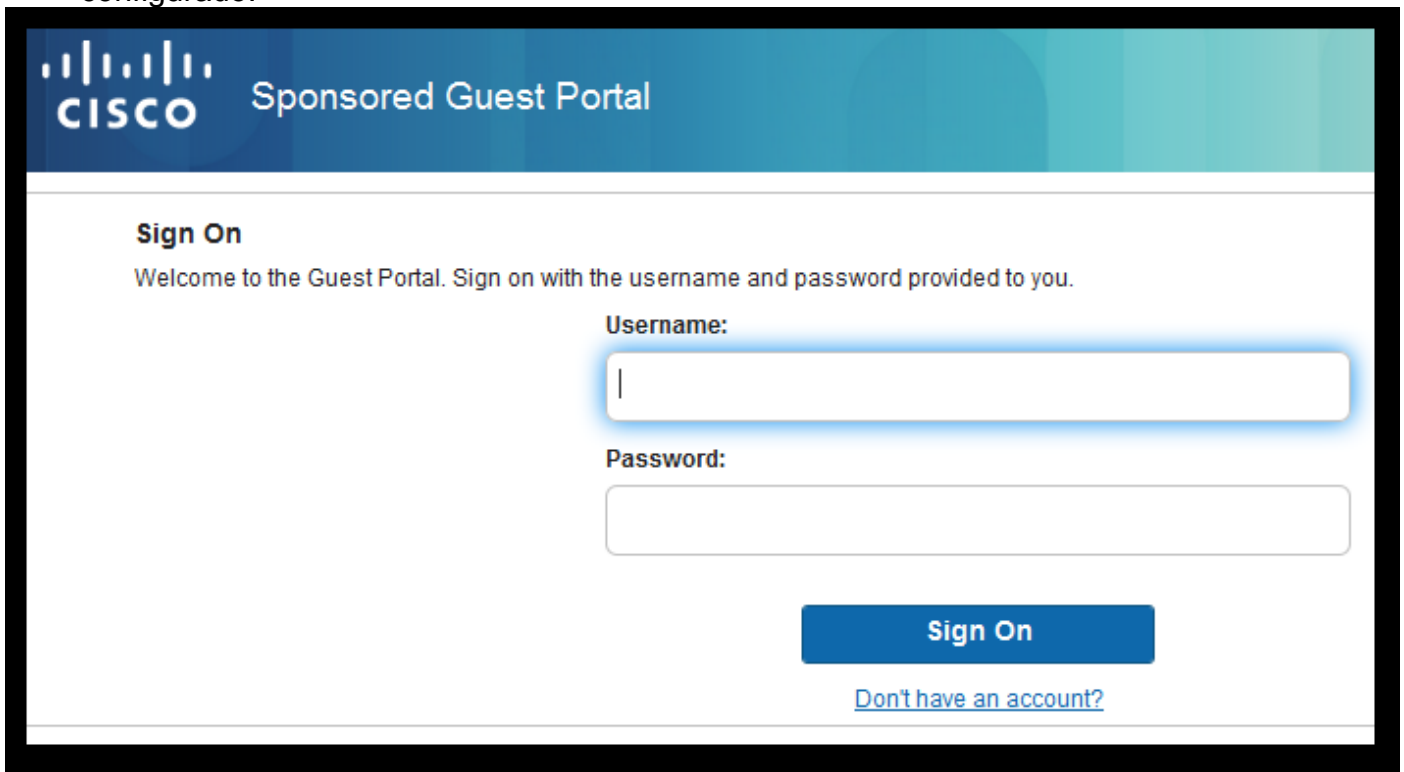
Fluxo dos logs do ISE RADIUS Live:

1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	Accounting Start
1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	Re-Authentication Event
	68:7F:74:72:18:2E					CoA Event
1001	68:7F:74:72:18:2E					Guest Authentication Event
68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	Initial MAB request

## Caso de uso 2

1. O usuário se conecta ao SSID convidado.
2. Ele abre o navegador e assim que o tráfego HTTP é gerado, o portal do convidado é exibido.
3. Depois que o usuário convidado autentica e aceita a AUP, o dispositivo é registrado.

4. Uma página de sucesso é exibida e um CoA de reautenticação é enviado (transparente para o cliente).
5. A sessão de endpoint é reautenticada com acesso total à rede.
6. Qualquer conexão gust 9s subsequente permitida sem a aplicação da autenticação de convidado, desde que o ponto final ainda esteja no grupo de Identidade de Ponto Final configurado.



The screenshot shows the Cisco Sponsored Guest Portal Sign On page. The header features the Cisco logo and the text "Sponsored Guest Portal". Below the header, the page is titled "Sign On" and includes a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". A blue "Sign On" button is located below the password field, and a link "Don't have an account?" is positioned below the button.

**CISCO** Sponsored Guest Portal

**Sign On**

Welcome to the Guest Portal. Sign on with the username and password provided to you.

**Username:**

**Password:**

**Sign On**

[Don't have an account?](#)



### Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

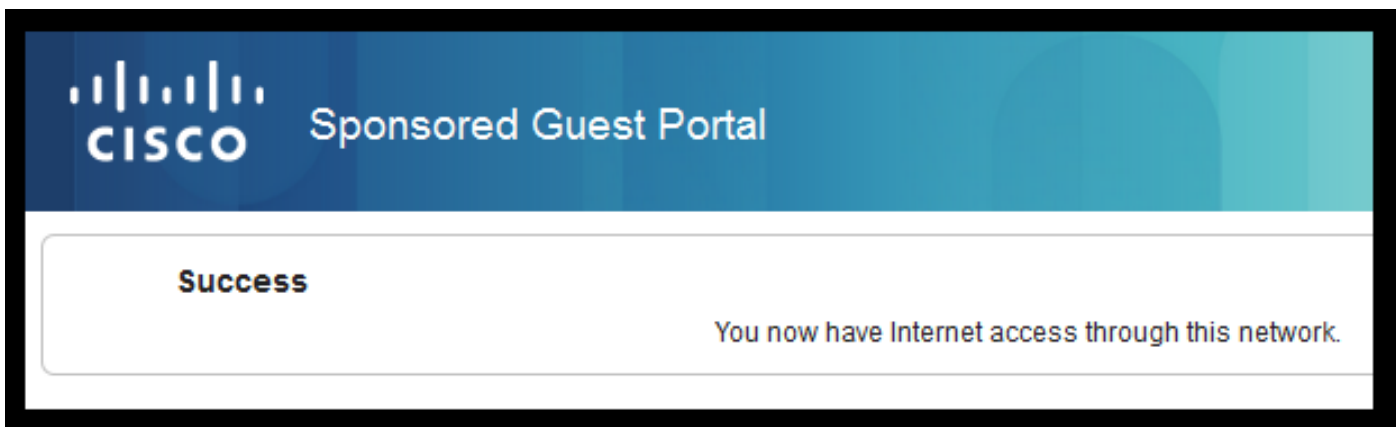


### Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue



Fluxo dos logs do ISE RADIUS Live:

Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
●		68:7F:74:72:1...	68:7F:74:72:...	PermitAccess	
✓		68:7F:74:72:1...	68:7F:74:72:...	PermitAccess	GuestEndpoints
✓		hfr592	68:7F:74:72:...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
✓			68:7F:74:72:...		
✓		hfr592	68:7F:74:72:...		GuestType_Contractor (default)
✓		68:7F:74:72:1...	68:7F:74:72:...	CWA_DeviceRegistration	Profiled

Accounting Start  
Subsequent MAB request( no redirect to guest portal)  
Re-Authentication Event  
CoA Reauth Event  
Guest Authentication and Device Registration  
Initial MAB request

### Caso de uso 3

1. O usuário se conecta ao SSID convidado.
2. Ele abre o navegador e assim que o tráfego HTTP é gerado, uma página AUP é exibida.
3. Quando o usuário convidado aceitar a AUP, o dispositivo será registrado.
4. Uma página de sucesso é exibida e um CoA de redefinição de administrador é enviado (transparente para o cliente).
5. O endpoint se reconecta com acesso total à rede.
6. Qualquer conexão gust subsequente é permitida sem impor a aceitação de AUP (a menos que seja configurado de outra forma) enquanto o ponto final permanecer no grupo de Identidade de Ponto Final configurado.



### Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline



**Connection Successful**

You have successfully connected to the network.

## Switching local FlexConnect no AireOS

Quando o switching local do FlexConnect é configurado, o administrador de rede precisa garantir que:

- A ACL de redirecionamento está configurada como uma ACL FlexConnect.
- A ACL de redirecionamento foi aplicada como uma política por meio do próprio AP na guia **FlexConnect > External WebAuthentication ACLs > Policies** > Selecione Redirect ACL e clique em **Apply**



All APs > Details for aaa-ap-3

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID 301 **VLAN Mappings**

FlexConnect Group Name Not Configured

**PreAuthentication Access Control Lists**

**External WebAuthentication ACLs**

Local Split ACLs

Central DHCP Processing

Layer2 ACLs

---

**Policies**

Policy ACL CWA\_Redirect **Add**

**Policy Access Control Lists**

CWA\_Redirect

Ou adicionando a ACL de política ao grupo FlexConnect pertence a (Wireless > FlexConnect Groups > Selecione o grupo correto > Mapeamento de ACL > Políticas Selecione a ACL de redirecionamento e clique em Adicionar)

FlexConnect Groups > Edit 'test'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping **Policies**

**Policies**

Policy ACL CWA\_Redirect **Add**

**Policy Access Control Lists**

CWA\_Redirect

TOR\_Redirect

A adição da ACL de política aciona a WLC para enviar a ACL configurada para os membros do AP do grupo FlexConnect. Deixar de fazer isso resulta em um problema de redirecionamento da Web.

## Cenário de Âncora Externa

Em cenários de âncora automática (Foreign-Anchor), é importante destacar estes fatos:

- A ACL de redirecionamento precisa ser definida na WLC Externa e de âncora. Mesmo quando só é aplicada na Âncora.
- A autenticação da camada 2 é sempre tratada pela WLC externa. Isso é crítico durante as fases de projeto (também para a solução de problemas ), pois todo o tráfego de autenticação e tarifação do RADIUS ocorre entre o ISE e a WLC externa.
- Depois que os AVPs de redirecionamento são aplicados à sessão do cliente, a WLC externa atualiza a sessão do cliente na âncora por meio de uma mensagem de handoff de mobilidade.
- Neste ponto, a WLC de âncora começa a aplicar o redirecionamento usando o Redirect-ACL que foi pré-configurado.
- A contabilização deve ser completamente desativada no SSID da WLC Âncora para evitar atualizações de contabilização no ISE (referenciando o mesmo evento de autenticação) vindas tanto da Âncora quanto da Externa.
- As ACLs baseadas em URL não são suportadas em cenários Foreign-Anchor.

## Troubleshoot

### Estados quebrados comuns no AireOS e no WLC de acesso convergente

#### 1. O cliente não consegue ingressar no SSID de convidado

Um "**show client detailed xx:xx:xx:xx:xx:xx**" revela que o cliente está preso em **START**. Geralmente, isso é um indicador de que a WLC não pode aplicar um atributo retornado pelo servidor AAA.

Verifique se o nome da ACL de redirecionamento enviado pelo ISE corresponde exatamente ao nome da ACL predefinida na WLC.

O mesmo princípio se aplica a qualquer outro atributo que você configurou no ISE para enviar para a WLC (VLAN IDs, Nomes de interface, Airespace-ACLs). O cliente deve fazer a transição para DHCP e, em seguida, **CENTRAL\_WEB\_AUTH**.

#### 2. Os AVPs de redirecionamento são aplicados à sessão do cliente, mas o redirecionamento não está funcionando

Verifique se o estado do gerenciador de políticas do cliente é **CENTRAL\_WEB\_AUTH** com um endereço IP válido alinhado à interface dinâmica configurada para o SSID e também se os atributos Redirect ACL e URL-Redirect estão aplicados à sessão do cliente.

### Redirecionar ACL

Nas WLCs do AireOS, a ACL de redirecionamento deve permitir explicitamente o tráfego que não deve ser redirecionado, como DNS e ISE na porta TCP 8443 em ambas as direções e o deny ip any any implícito aciona o restante do tráfego a ser redirecionado.

No acesso convergido, a lógica é oposta. Negar ACEs ignora o redirecionamento enquanto

permitir ACEs aciona o redirecionamento. É por isso que é recomendável permitir explicitamente as portas TCP 80 e 443.

Verifique o acesso ao ISE pela porta 8443 da VLAN convidada. Se tudo parecer bom do ponto de vista da configuração, a maneira mais fácil de seguir em frente é capturar o adaptador sem fio do cliente e verificar onde o redirecionamento é interrompido.

- A resolução DNS acontece?
- O handshake triplo TCP foi concluído na página solicitada?
- A WLC retorna uma ação de redirecionamento depois que o cliente inicia o GET?
- O handshake triplo do TCP em relação ao ISE no 8443 foi concluído?

### **3. O cliente não consegue acessar a rede depois que o ISE enviou uma alteração de VLAN ao final do fluxo de convidado**

Uma vez que o cliente pegou um endereço IP no início do fluxo (estado Pre Redirect), se uma alteração de VLAN for empurrada para baixo depois que a autenticação de convidado acontecer (pós-autenticação de CoA re-autenticar), a única maneira de forçar uma liberação/renovação de DHCP no fluxo de convidado (sem agente de postura) é através de um miniaplicativo java que em dispositivos móveis não funciona.

Isso deixa o cliente com o buraco negro na VLAN X com um endereço IP da VLAN Y. Isso deve ser considerado durante o planejamento da solução.

### **4. O ISE mostra a mensagem "HTTP 500 Erro interno, sessão Radius não encontrada" no navegador do cliente convidado durante o redirecionamento**

Isso geralmente é um indicador de perda de sessão no ISE (a sessão foi encerrada). O motivo mais comum para isso é a contabilização configurada na WLC Âncora quando a Âncora Externa foi implantada. Para corrigir isso, desabilite a contabilização na Âncora e deixe a Autenticação e Contabilização de identificador estrangeiro.

### **5. O cliente se desconecta e permanece desconectado ou se conecta a um SSID diferente após aceitar AUP no portal HotSpot do ISE.**

Isso pode ser esperado no HotSpot devido à alteração dinâmica de autorização (CoA) envolvida nesse fluxo (CoA Admin Reset) que faz com que a WLC emita um deauth para a estação sem fio. A maioria dos endpoints sem fio não tem problemas para retornar ao SSID após a ocorrência da desautenticação, mas em alguns casos o cliente se conecta a outro SSID preferencial em resposta ao evento de desautenticação. Nada pode ser feito do ISE ou da WLC para impedir isso, pois depende do cliente sem fio aderir ao SSID original ou conectar-se a outro SSID disponível (preferencial).

Nesse caso, o usuário sem fio deve se conectar manualmente de volta ao SSID HotSpot.

## **WLC AireOS**

```
(Cisco Controller) >debug client
```

Depurar conjuntos de clientes para DEPURAR um conjunto de componentes envolvidos nas alterações da Máquina de Estado do Cliente.

```
(Cisco Controller) >show debug
```

```
MAC Addr 1..... AA:AA:AA:AA:AA:AA
```

Debug Flags Enabled:

```
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  mobility client handoff enabled.
  pem events enabled.
  pem state enabled.
  802.11r event debug enabled.
  802.11w event debug enabled.
  CCKM client debug enabled.
```

## Depurar componentes AAA

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

Isso pode afetar os recursos, dependendo da quantidade de usuários que se conectam através do MAB ou do Dot1X SSID. Esses componentes no nível de DEPURAÇÃO registram transações AAA entre WLC e ISE e imprimem os pacotes RADIUS na tela.

Isso é essencial se você perceber que o ISE não pode fornecer os atributos esperados ou se a WLC não os processar corretamente.

## Redirecionamento de Autenticação da Web

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

Isso pode ser usado para verificar se a WLC está disparando o redirecionamento com êxito. Este é um exemplo de como o redirecionamento deve parecer a partir de depurações:

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is
HTTP/1.1 200 OK
Location:
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-0050
```

## NGWC

Depurar conjuntos de clientes para DEPURAR um conjunto de componentes envolvidos nas alterações da Máquina de Estado do Cliente.

```
3850#debug client mac-address <client MAC>
```

Este componente imprime os pacotes RADIUS (Autenticação e Contabilização) na tela. Isso é útil quando você precisa verificar se o ISE fornece os AVPs corretos e também para verificar se o CoA foi enviado e processado corretamente.

```
3850#debug radius
```

Todas as transições de AAA (autenticação, autorização e contabilização) serão realizadas onde os clientes sem fio estiverem envolvidos. Isso é crítico para verificar se o WLC analisa corretamente os AVPs e os aplica à sessão do cliente.

```
3850#debug aaa wireless all
```

Isso pode ser ativado quando você suspeita de um problema de redirecionamento no NGWC.

```
3850#debug epm plugin redirect all
```

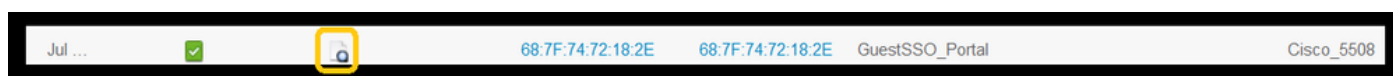
```
3850#debug ip http transactions
```

```
3850#debug ip http url
```

## ISE

### Logs ao vivo do RADIUS

Verifique se a solicitação MAB inicial foi processada corretamente no ISE e se o ISE envia de volta os atributos esperados. Navegue até **Operations > RADIUS > Live logs** e filtre a saída usando o MAC do cliente em **Endpoint ID**. Quando o evento de autenticação for encontrado, clique nos detalhes e verifique os Resultados enviados como parte da aceitação.



## Result

UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

## TCPDump

Esse recurso pode ser usado quando for necessária uma análise mais detalhada da troca de pacotes RADIUS entre o ISE e a WLC. Dessa forma, você pode provar que o ISE envia os atributos corretos no access-accept sem a necessidade de habilitar depurações no lado da WLC. Para iniciar uma captura usando o TCDDump, navegue para **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCPDump**.

Este é um exemplo de um fluxo correto capturado através do TCPDump

Source	Destination	Protocol	Length	Info
154.5	157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
157.13	154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
154.5	157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
157.13	154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
157.13	154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
154.5	157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
154.5	157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
157.13	154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

Aqui estão os AVPs enviados em resposta à solicitação MAB inicial (segundo pacote na captura de tela acima).

### RADIUS Protocol

```
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: f1eaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
  AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
  AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
  AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
  AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
  AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=189 t=Cisco-AVPair(1): url-
```

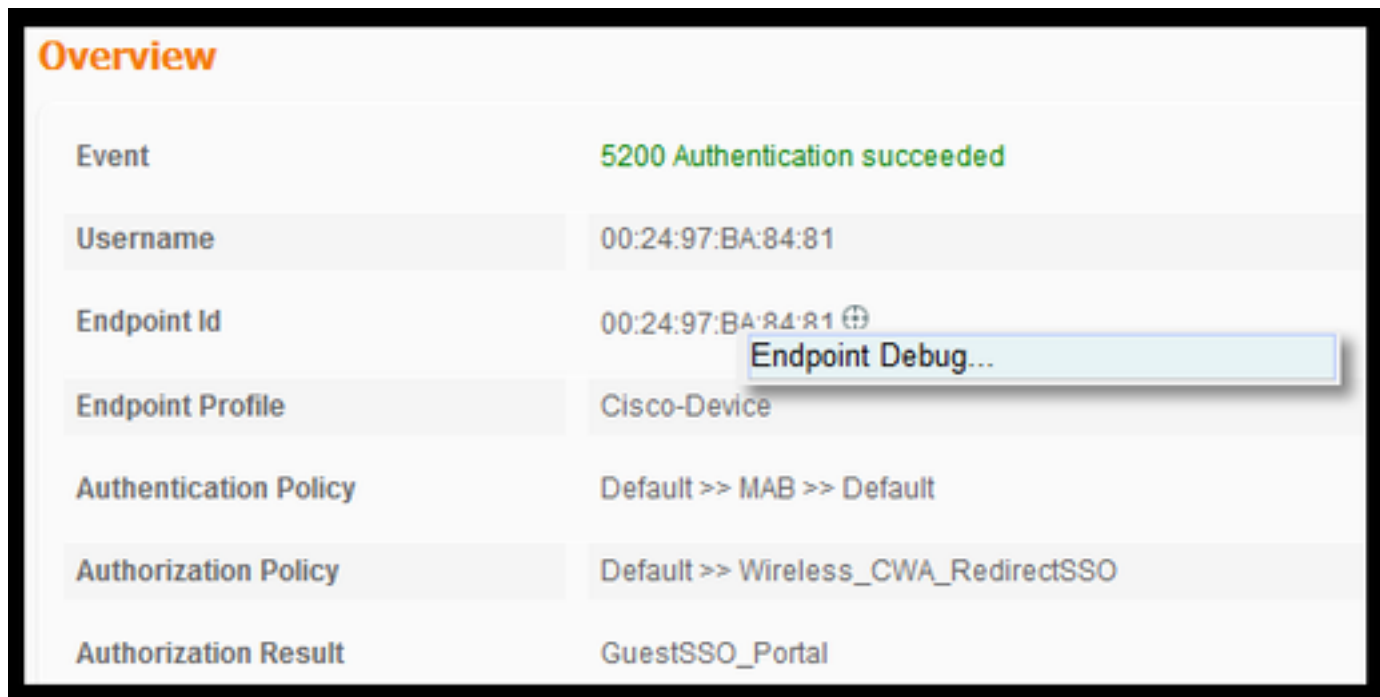
redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a050000aa05565e1c9&portal=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622

AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)

## Depurações de ponto final:

Se você precisar se aprofundar nos processos do ISE que envolvem decisões de política, seleção de portal, autenticação de convidado, tratamento de CoA a maneira mais fácil de abordar isso é habilitar **depurações de endpoint** em vez de ter que definir componentes completos para o nível de depuração.

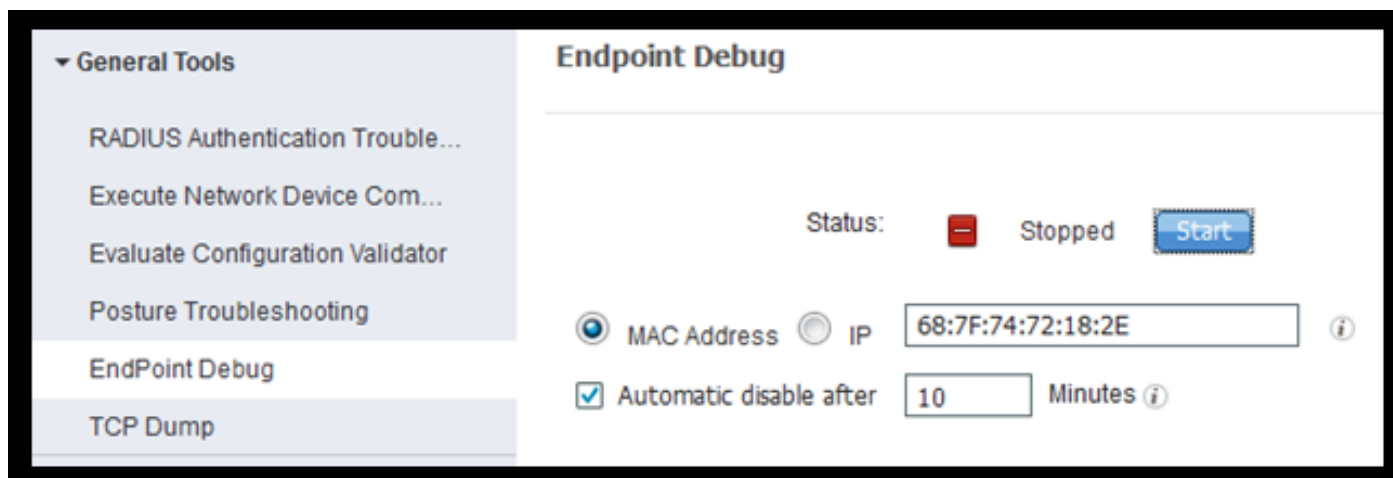
Para habilitar isso, navegue até **Operações > Solução de problemas > Ferramentas de diagnóstico > Ferramentas gerais > Depuração de endpoint**.



The screenshot shows the 'Overview' page in the ISE interface. It displays the following information:

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81 <a href="#">Endpoint Debug...</a>
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

Na página de depuração do endpoint, insira o endereço MAC do endpoint e clique em iniciar quando estiver pronto para recriar o problema.





The screenshot shows the 'Endpoint Debug' configuration page. On the left, there is a sidebar with 'General Tools' expanded, showing options like 'RADIUS Authentication Trouble...', 'Execute Network Device Com...', 'Evaluate Configuration Validator', 'Posture Troubleshooting', 'EndPoint Debug', and 'TCP Dump'. The main area is titled 'Endpoint Debug' and contains the following settings:


- Status: - Stopped [Start](#)
- MAC Address  IP
- Automatic disable after  Minutes [i](#)

Quando a depuração for interrompida, clique no link que identifica o ID do ponto final para fazer o download da saída da depuração.

### Endpoint Debug

Status:  Processing ...

MAC Address  IP  

Automatic disable after  Minutes 

---

Selected 0 | Total 1

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input type="checkbox"/>	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

## Informações Relacionadas

[Compilações AireOS recomendadas pelo TAC](#)

[Guia de Configuração do Cisco Wireless Controller Release 8.0.](#)

[Guia do Administrador do Cisco Identity Services Engine, Versão 2.1](#)

[Configuração sem fio NGWC universal com mecanismo de serviços de identidade](#)



## 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.