Configurar o CWA com APs FlexConnect em uma WLC com ISE

Contents

Introduction

Este documento descreve como configurar a autenticação central da Web com pontos de acesso (APs) FlexConnect em uma controladora Wireless LAN (WLC) com Identity Services Engine (ISE) no modo de switching local.

Observação importante: neste momento, a autenticação local nos FlexAPs não é suportada para este cenário.

Outros documentos nesta série

- Exemplo de Configuração da Autenticação Central da Web com um Switch e um Identity Services Engine
- Exemplo de configuração da autenticação da Web central no WLC e no ISE

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco Identity Services Engine (ISE), versão 1.2.1
- Wireless LAN Controller Software, Versão - 7.4.100.0

Configurar

Há vários métodos para configurar a autenticação central da Web na controladora Wireless LAN (WLC). O primeiro método é a autenticação da Web local, na qual a WLC redireciona o tráfego HTTP para um servidor interno ou externo, onde o usuário é solicitado a se autenticar. Em seguida, a WLC busca as credenciais (enviadas de volta por meio de uma solicitação HTTP GET no caso de um servidor externo) e faz uma autenticação RADIUS. No caso de um usuário convidado, um servidor externo (como o Identity Service Engine (ISE) ou o NAC Guest Server (NGS)) é necessário, pois o portal fornece recursos como registro e autoprovisionamento de dispositivos. Esse processo inclui estas etapas:

1. O usuário se associa ao SSID de autenticação da Web.
2. O usuário abre o navegador.
3. A WLC é redirecionada para o portal do convidado (como ISE ou NGS) assim que uma URL é inserida.
4. O usuário se autentica no portal.
5. O portal do convidado redireciona de volta para a WLC com as credenciais inseridas.
6. A WLC autentica o usuário convidado via RADIUS.
7. A WLC redireciona de volta para a URL original.

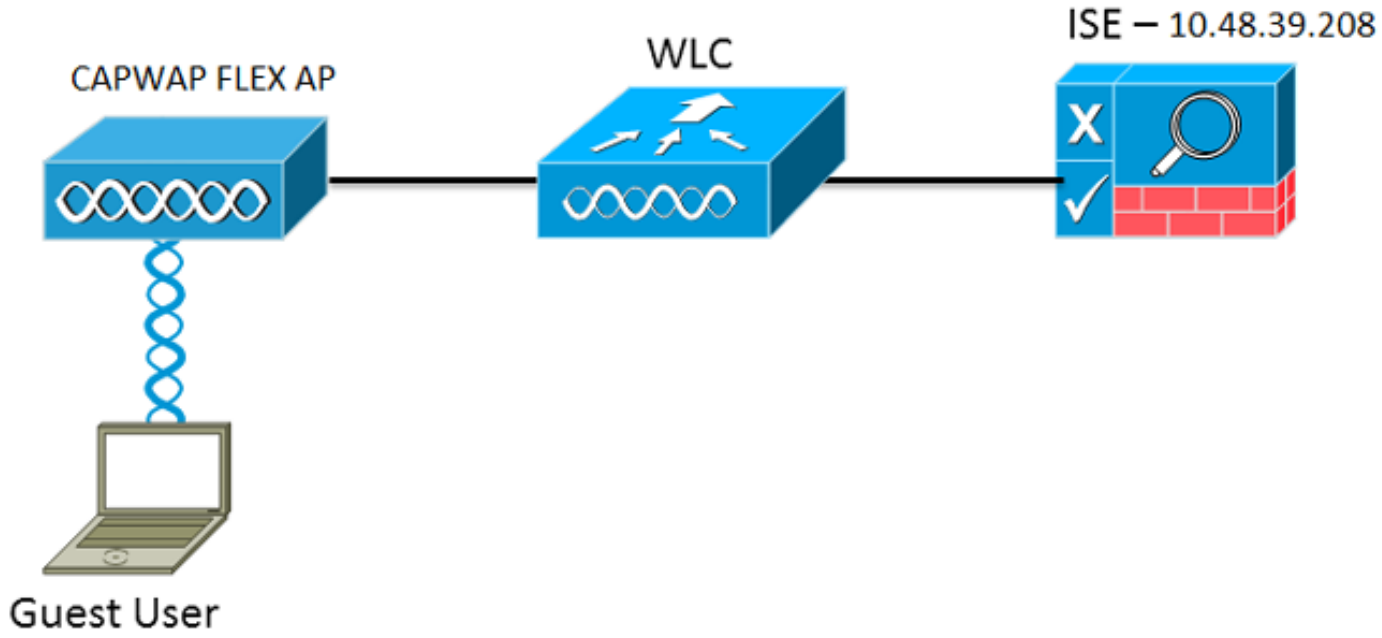
Esse processo inclui muito redirecionamento. A nova abordagem é usar a autenticação central da Web que funciona com ISE (versões posteriores à 1.1) e WLC (versões posteriores à 7.2). Esse processo inclui estas etapas:

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

Esta seção descreve as etapas necessárias para configurar a autenticação central da Web em WLC e ISE.

Diagrama de Rede

Essa configuração utiliza esta configuração de rede:

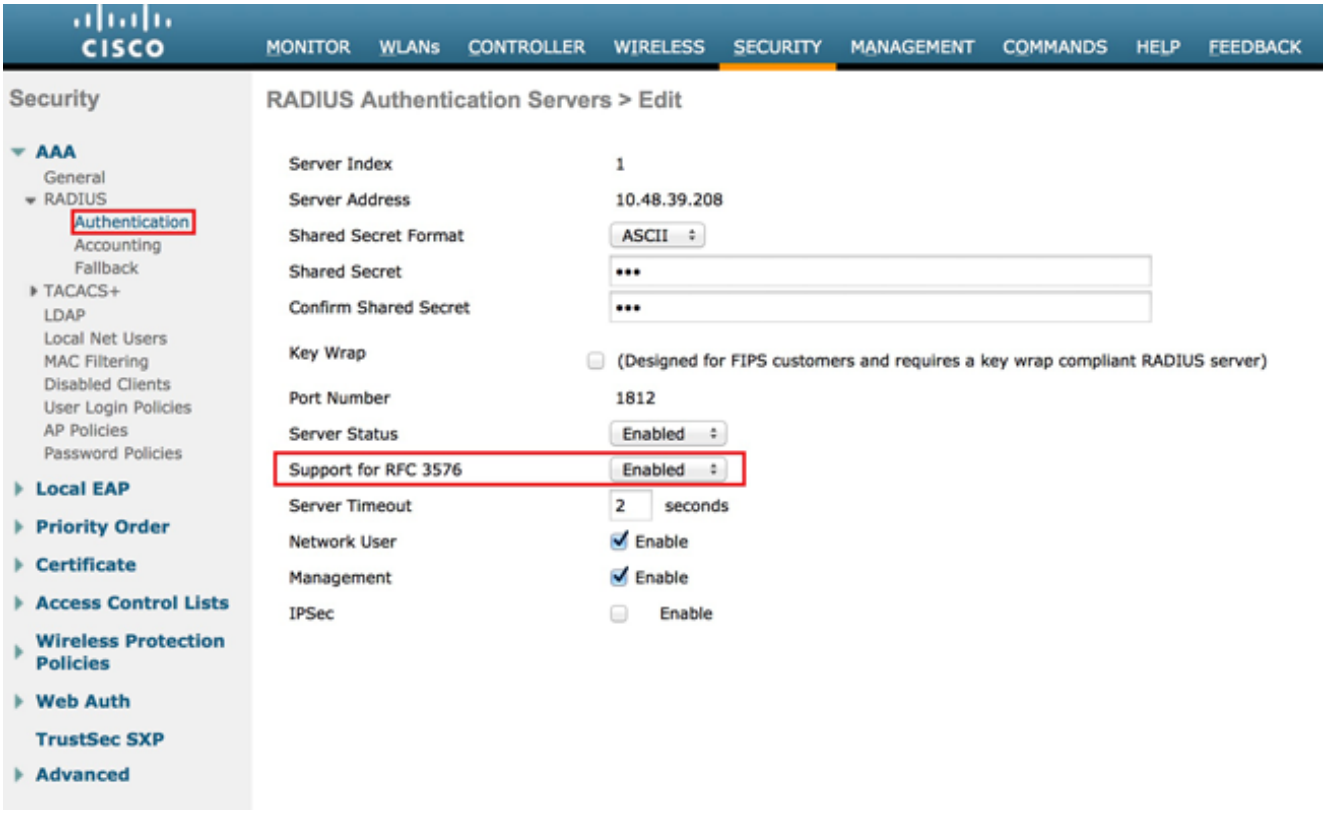


Configuração de WLC

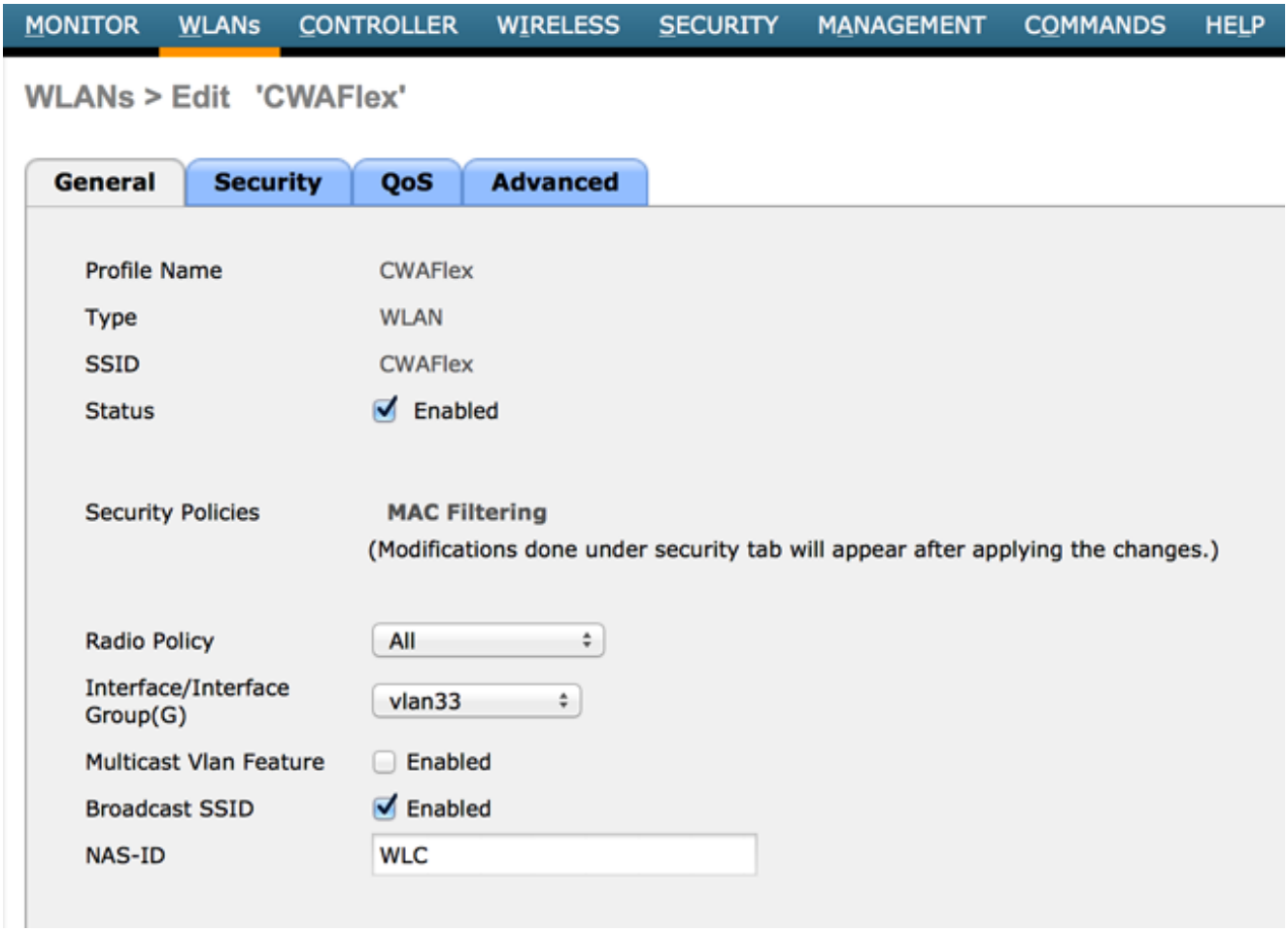
A configuração da WLC é bastante direta. Um "truque?" é usado (igual ao dos switches) para obter o URL de autenticação dinâmica do ISE. (Como ele usa CoA, uma sessão precisa ser criada, pois o ID da sessão faz parte do URL.) O SSID é configurado para usar a filtragem MAC e o ISE é configurado para retornar uma mensagem de aceitação de acesso mesmo que o endereço MAC não seja encontrado, de modo que ele envie a URL de redirecionamento para todos os usuários.

Além disso, o Network Admission Control (NAC) RADIUS e a Substituição de AAA devem ser habilitados. O NAC RADIUS permite que o ISE envie uma solicitação de CoA que indica que o usuário está autenticado e pode acessar a rede. Também é usado para avaliação de postura, em que o ISE altera o perfil do usuário com base no resultado da postura.

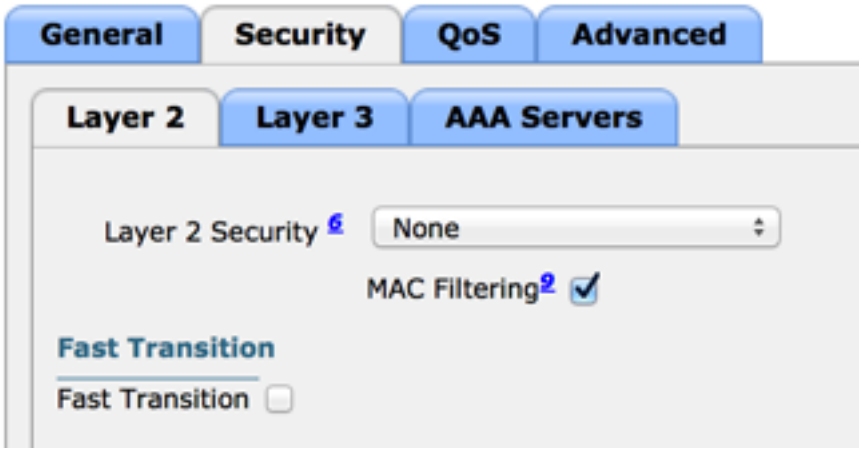
1. Certifique-se de que o servidor RADIUS tenha RFC3576 (CoA) habilitado, que é o padrão.



2. Crie uma nova WLAN. Este exemplo cria uma nova WLAN chamada *CWAFlex* e a atribui à vlan33. (Observe que ela não terá muito efeito, já que o access point está no modo de switching local.)

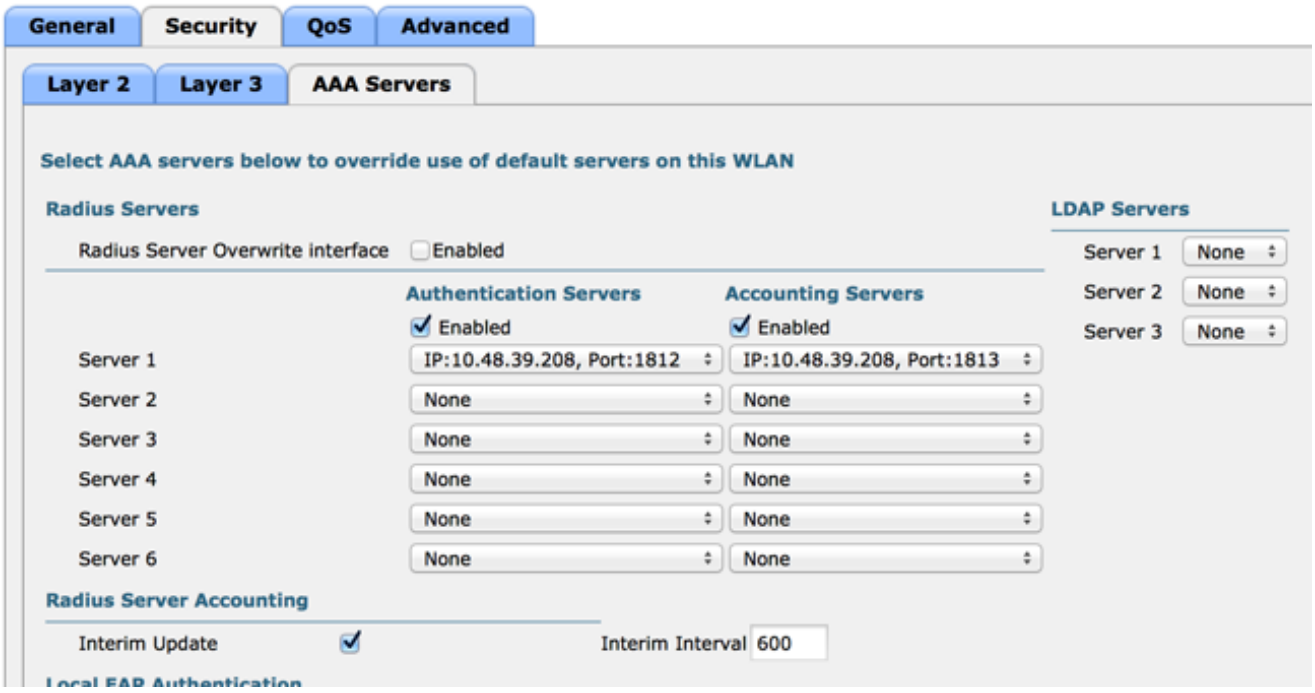


3. Na guia Security, ative a filtragem de endereços MAC como Layer 2 Security.

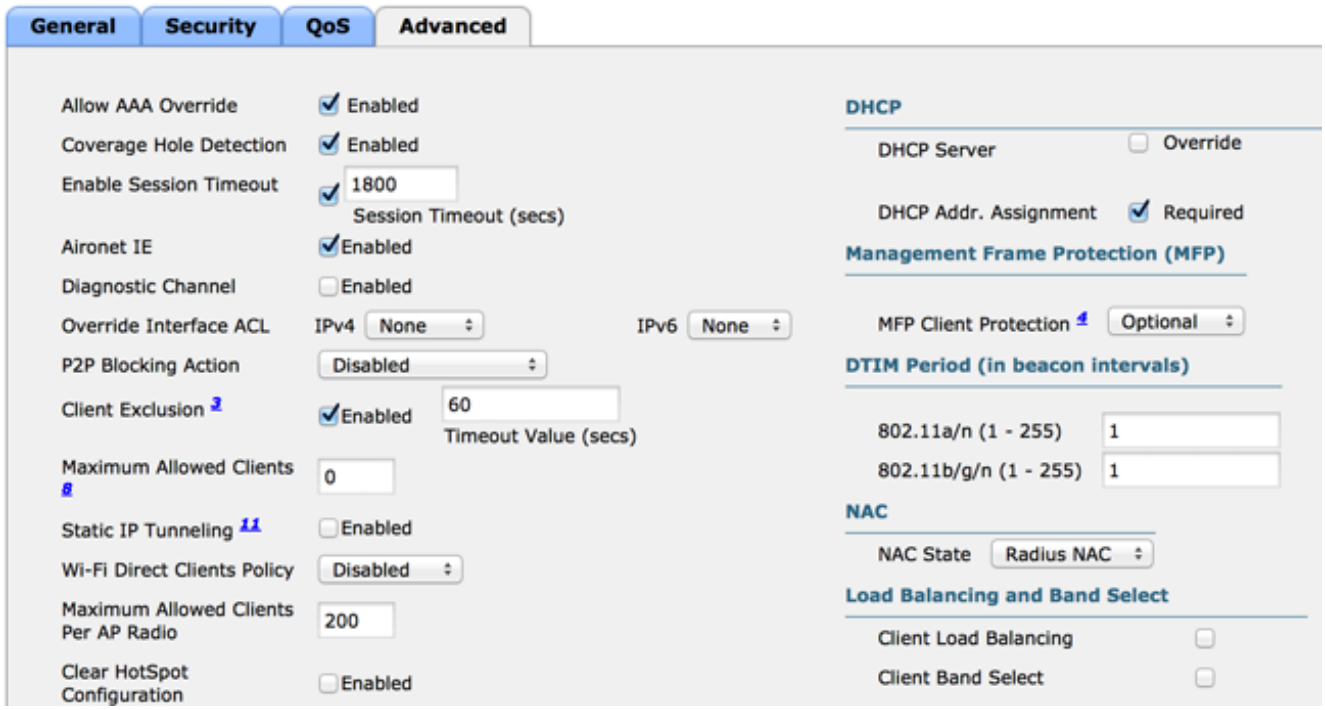


4. Na guia Layer 3, certifique-se de que a segurança esteja desativada. (Se a autenticação da Web estiver habilitada na Camada 3, a autenticação da Web local estará habilitada, não a autenticação da Web central.)

5. Na guia AAA Servers (Servidores AAA), selecione o servidor ISE como servidor radius para a WLAN. Opcionalmente, você pode selecioná-lo para contabilização para ter informações mais detalhadas sobre o ISE.



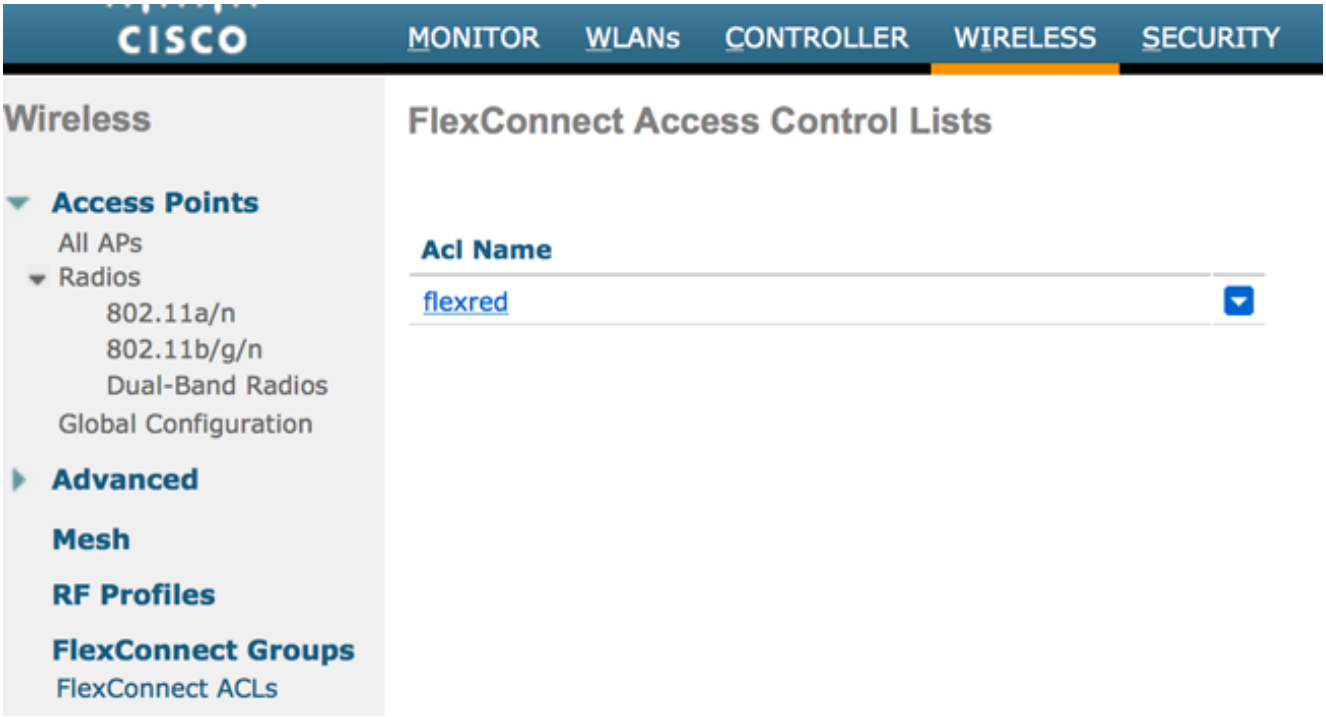
6. Na guia Advanced (Avançado), verifique se Allow AAA Override (Permitir substituição de AAA) está marcado e Radius NAC está selecionado para NAC State (Estado NAC).



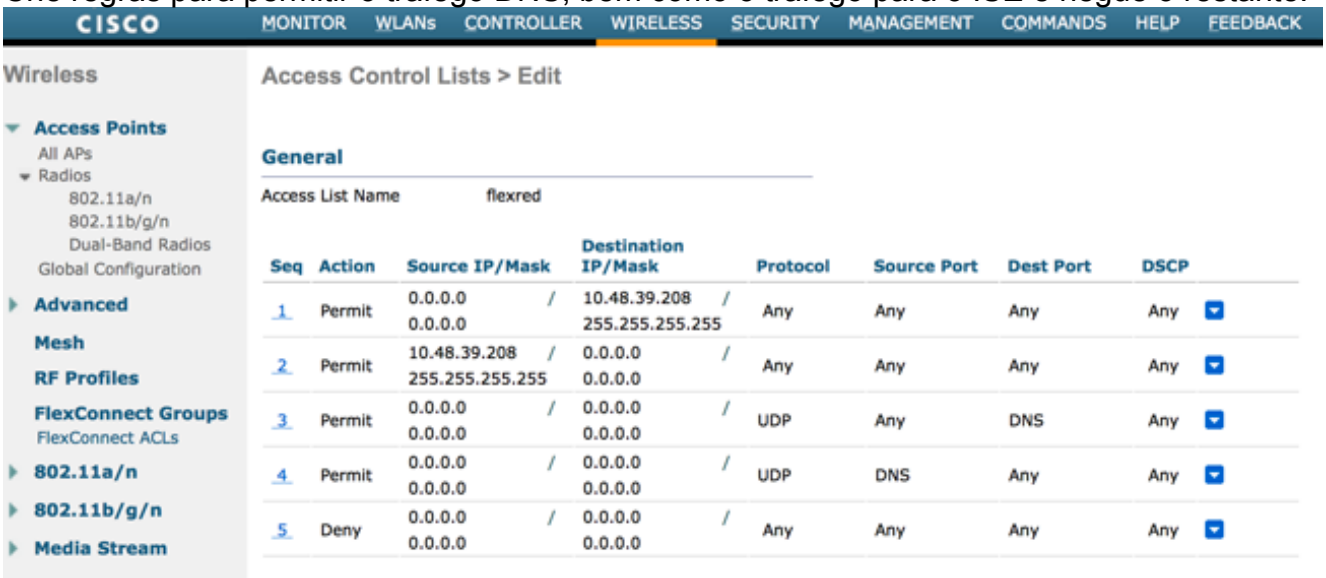
7. Crie uma ACL de redirecionamento.

Essa ACL é referenciada na mensagem Access-Accept do ISE e define qual tráfego deve ser redirecionado (negado pela ACL), bem como qual tráfego não deve ser redirecionado (permitido pela ACL). Basicamente, o DNS e o tráfego de/para o ISE precisam ser permitidos. **Observação**: um problema com os APs FlexConnect é que você deve criar uma ACL FlexConnect separada de sua ACL normal. Esse problema está documentado no Cisco Bug CSCue68065 e é corrigido na versão 7.5. Na WLC 7.5 e posterior, apenas uma FlexACL é necessária, e nenhuma ACL padrão é necessária. A WLC espera que a ACL de redirecionamento retornada pelo ISE seja uma ACL normal. No entanto, para garantir que

funcione, você precisa aplicar a mesma ACL que a ACL FlexConnect.
Este exemplo mostra como criar uma ACL FlexConnect chamada *flexred*:

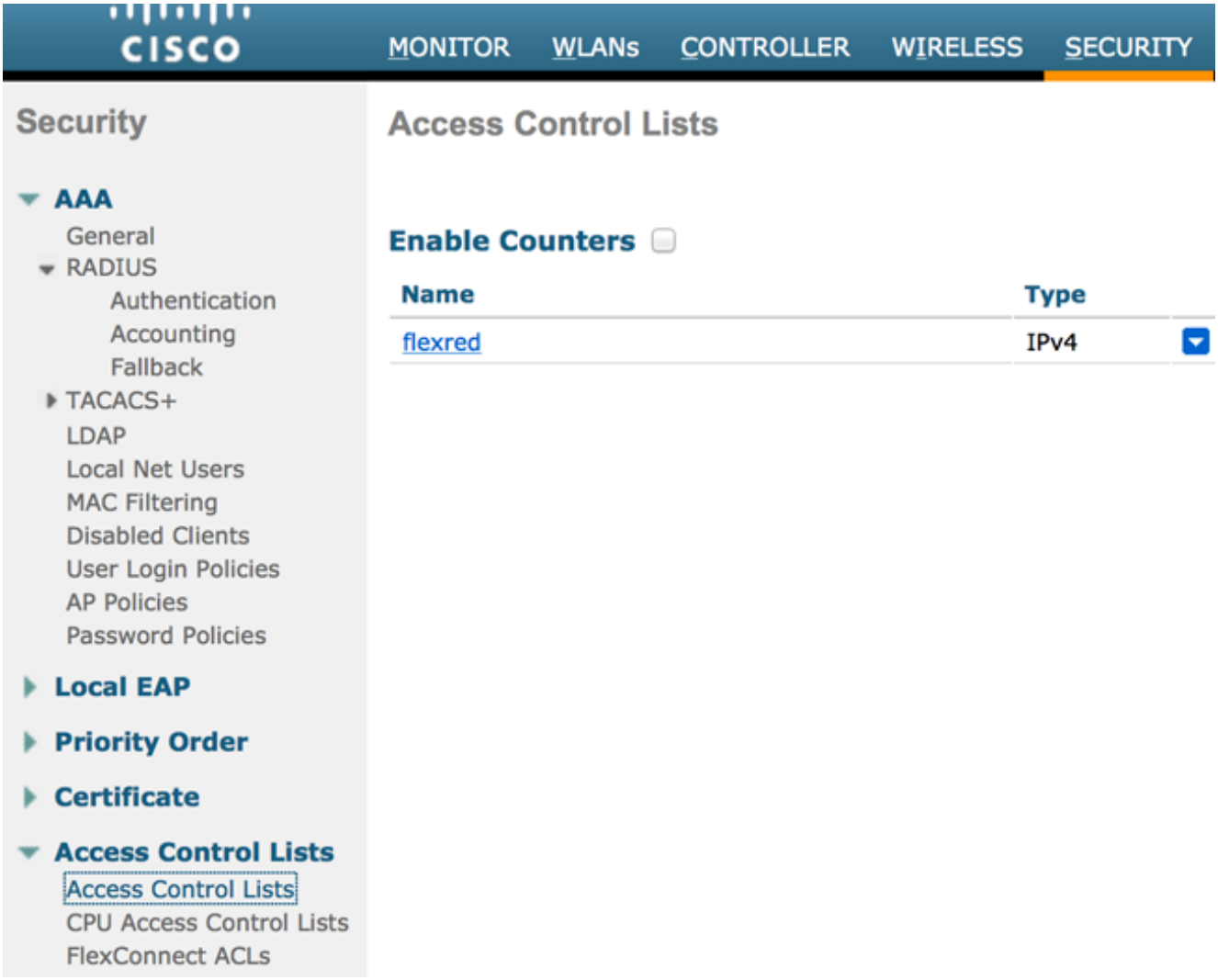


Crie regras para permitir o tráfego DNS, bem como o tráfego para o ISE e negue o restante.



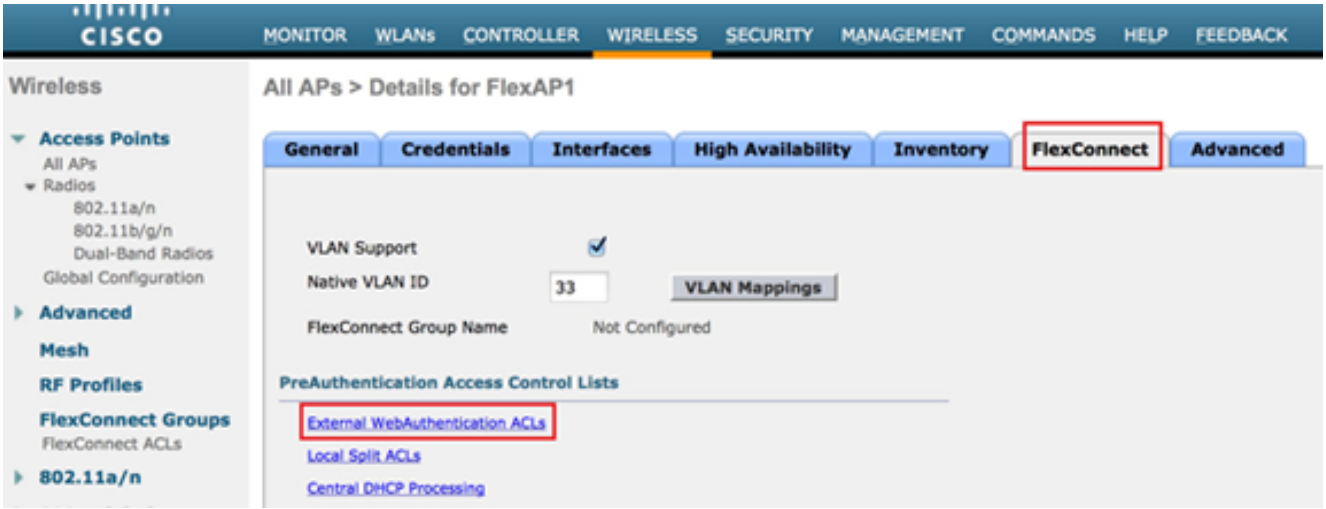
Se desejar a segurança máxima, você poderá permitir somente a porta 8443 em direção ao ISE. (Se estiver posturando, você deverá adicionar portas de postura típicas, como 8905.8906.8909.8910.)

(Somente no código anterior à versão 7.5 devido a CSCue68065) Escolha **Security > Access Control Lists** para criar uma ACL idêntica com o mesmo nome.



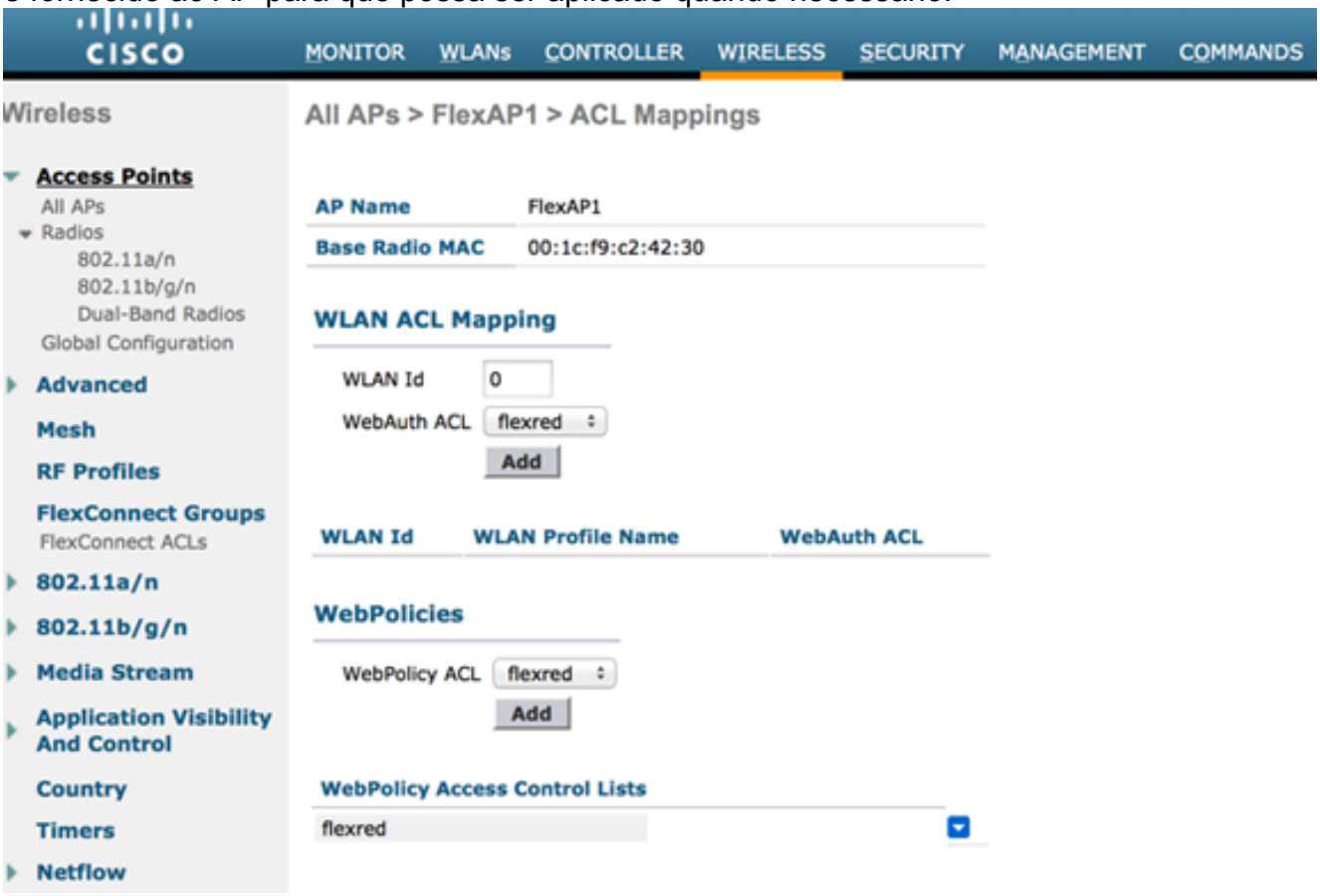
Prepare o AP FlexConnect específico. Observe que, para uma implantação maior, você normalmente usaria grupos FlexConnect e não executaria esses itens por AP por motivos de escalabilidade.

Clique em **Wireless** e selecione o ponto de acesso específico.Clique na guia **FlexConnect** e em **External Webauthentication ACLs**. (Antes da versão 7.4, essa opção era chamada de *políticas da Web*.)



Adicione a ACL (chamada *flexred* neste exemplo) à área de políticas da Web. Isso envia

previamente a ACL ao ponto de acesso. Ele ainda não foi aplicado, mas o conteúdo da ACL é fornecido ao AP para que possa ser aplicado quando necessário.



A configuração da WLC está concluída.

Configuração do ISE

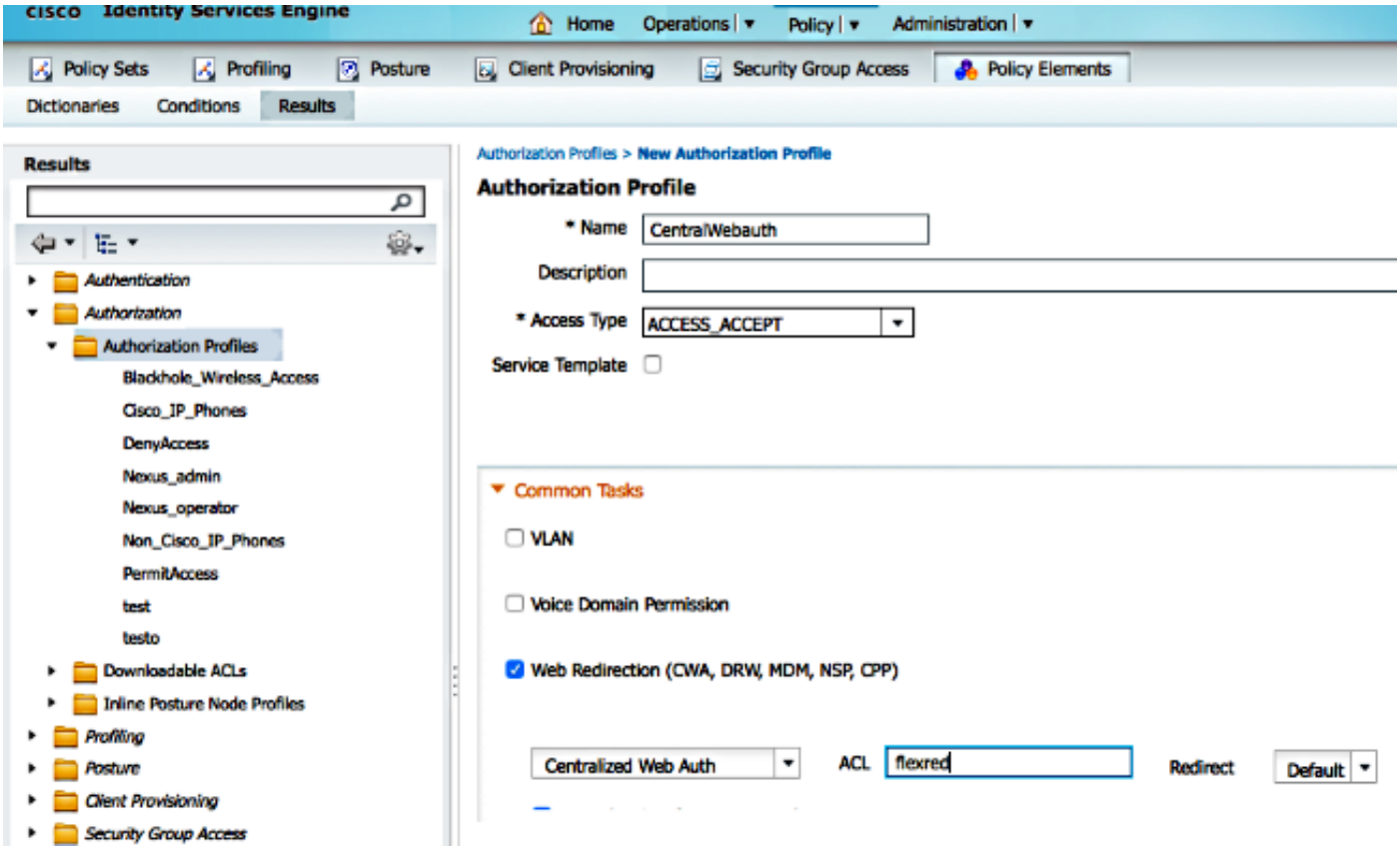
Criar o Perfil de Autorização

Conclua estas etapas para criar o perfil de autorização:

1. Clique em **Policy** e, em seguida, clique em **Policy Elements**.
2. Clique em **Results**.
3. Expanda **Authorization** e clique em **Authorization profile**.
4. Clique no botão **Add** para criar um novo perfil de autorização para webauth central.
5. No campo **Name**, insira um nome para o perfil. Este exemplo usa *CentralWebauth*.
6. Escolha **ACCESS_ACCEPT** na lista suspensa Tipo de acesso.
7. Marque a caixa de seleção **Autenticação da Web** e escolha **Autenticação da Web centralizada** na lista suspensa.
8. No campo ACL, insira o nome da ACL na WLC que define o tráfego que será redirecionado. Este exemplo usa *flexred*.
9. Escolha **Default** na lista suspensa Redirect.

O atributo Redirecionar define se o ISE vê o portal da Web padrão ou um portal da Web

personalizado que o administrador do ISE criou. Por exemplo, a ACL *flexred* neste exemplo dispara um redirecionamento no tráfego HTTP do cliente para qualquer lugar.

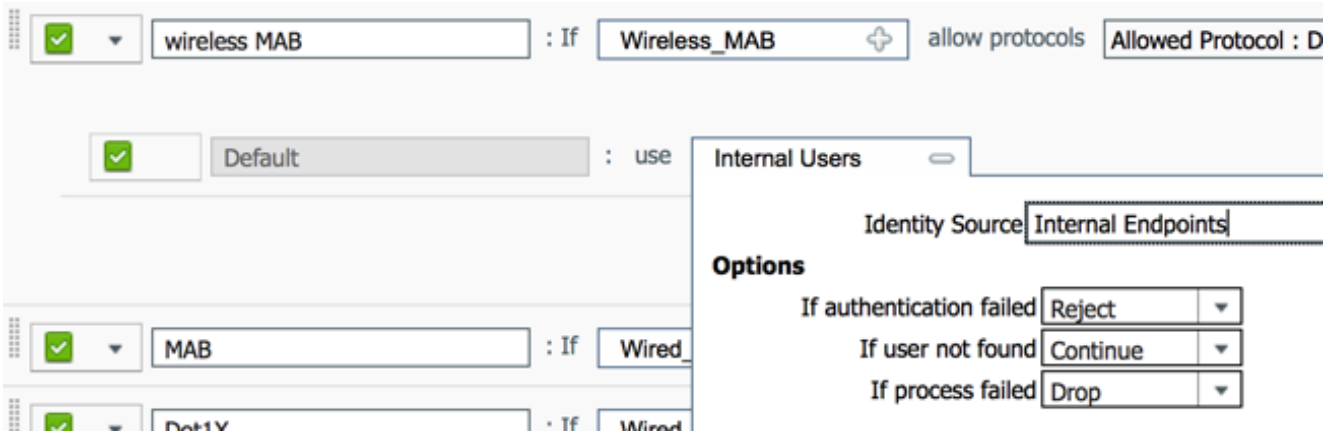


Criar uma Regra de Autenticação

Conclua estas etapas para usar o perfil de autenticação para criar a regra de autenticação:

1. No menu Policy (Diretiva), clique em **Authentication**. Esta imagem mostra um exemplo de como configurar a regra de política de autenticação. Neste exemplo, é configurada uma regra que será acionada quando a filtragem de MAC for detectada.

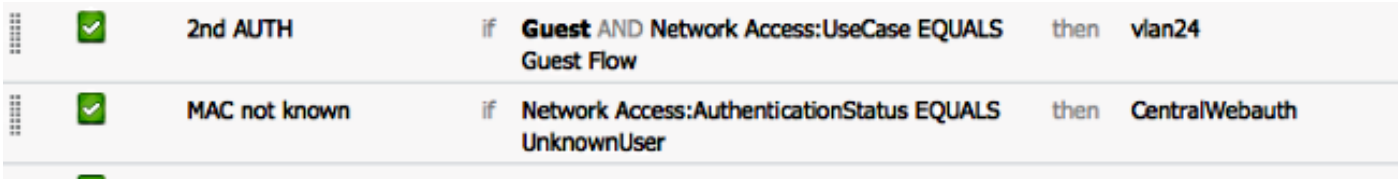
2. Digite um nome para a regra de autenticação. Este exemplo usa *Wireless mab*.
3. Selecione o ícone de adição (**+**) no campo Condição If.
4. Escolha **Compound condition** e, em seguida, **Wireless_MAB**.
5. Escolha "Default network access" (Acesso padrão à rede) como protocolo permitido.
6. Clique na seta localizada ao lado de **e ...** para expandir ainda mais a regra.
7. Clique no ícone **+** no campo Origem da identidade e escolha **Pontos finais internos**.
8. Escolha **Continue** na lista suspensa If user not found.



Esta opção permite que um dispositivo seja autenticado (através de webauth) mesmo que seu endereço MAC não seja conhecido. Os clientes Dot1x ainda podem se autenticar com suas credenciais e não devem se preocupar com esta configuração.

Criar uma Regra de Autorização

Agora há várias regras a serem configuradas na política de autorização. Quando o PC é associado, ele passa pela filtragem de MAC; presume-se que o endereço MAC não seja conhecido, portanto, o webauth e a ACL são retornados. Esta regra *MAC desconhecido* é mostrada na imagem abaixo e é configurada nesta seção.



Conclua estas etapas para criar a regra de autorização:

1. Crie uma nova regra e insira um nome. Este exemplo usa *MAC desconhecido*.
2. Clique no ícone de mais (**+**) no campo de condição e escolha criar uma nova condição.
3. Expanda a lista suspensa **expressão**.
4. Escolha **Acesso à rede** e expanda-o.
5. Clique em **AuthenticationStatus** e escolha o operador **Equals**.
6. Escolha **UnknownUser** no campo do lado direito.
7. Na página Autorização geral, escolha **CentralWebauth** (Perfil de autorização) no campo à direita da palavra then.Essa etapa permite que o ISE continue mesmo que o usuário (ou o MAC) não seja conhecido.Usuários desconhecidos agora são apresentados com a página Login. No entanto, depois que elas inserem suas credenciais, são apresentadas novamente com uma solicitação de autenticação no ISE; portanto, outra regra deve ser configurada com uma condição que é atendida se o usuário for um usuário convidado. Neste exemplo, *If UseridentityGroup equals Guest* é usado e supõe-se que todos os convidados pertencem a este grupo.
8. Clique no botão de ações localizado no final da regra *MAC desconhecido* e escolha inserir uma nova regra acima.**Observação:** é muito importante que essa nova regra venha antes da regra *MAC not known*.

9. Insira **2nd AUTH** no campo de nome.
10. Selecione um grupo de identidade como condição. Este exemplo escolheu **Guest**.

11. No campo Condição, clique no ícone de adição (**+**) e escolha criar uma nova condição.

12. Escolha **Network Access** e clique em **UseCase**.

13. Escolha **Equals** como o operador.

14. Escolha **GuestFlow** como o operando direito. Isso significa que você capturará os usuários que acabaram de fazer logon na página da Web e voltarão após uma Alteração de Autorização (a parte do fluxo de convidados da regra) e somente se eles pertencerem ao grupo de identidade do convidado.

15. Na página de autorização, clique no ícone de adição (**+**) (localizado ao lado de *then*) para escolher um resultado para sua regra.

    Neste exemplo, um perfil pré-configurado (vlan34) é atribuído; essa configuração não é mostrada neste documento.

    Você pode escolher uma opção **Permit Access** ou criar um perfil personalizado para retornar a VLAN ou os atributos desejados.

Observação importante: no ISE versão 1.3, dependendo do tipo de autenticação da Web, o caso de uso "Fluxo de convidado" pode não ser mais encontrado. A regra de autorização teria então que conter o grupo de usuários convidado como a única condição possível.

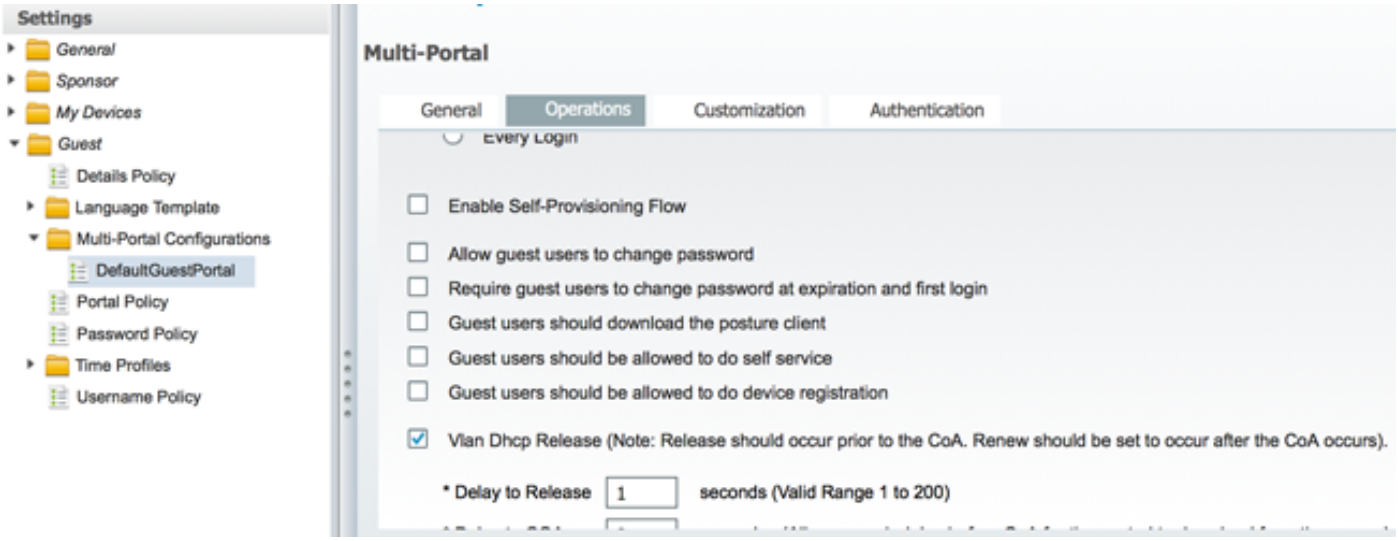
Habilitar a Renovação de IP (Opcional)

Se você atribuir uma VLAN, a etapa final é que o PC cliente renove seu endereço IP. Essa etapa é realizada pelo portal de convidado para clientes Windows. Se você não definiu uma VLAN para a *regra 2nd AUTH* anteriormente, ignore esta etapa.

Observe que nos APs FlexConnect, a VLAN precisa pré-existir no próprio AP. Portanto, se isso não acontecer, você pode criar um mapeamento VLAN-ACL no próprio AP ou no grupo flex onde você não aplica nenhuma ACL para a nova VLAN que deseja criar. Na verdade, isso cria uma VLAN (sem ACL).

Se você atribuiu uma VLAN, siga estas etapas para habilitar a renovação de IP:

1. Clique em **Administração** e em **Gerenciamento de convidados**.
2. Clique em **Settings**.
3. Expanda **Guest** e, em seguida, expanda **Multi-Portal Configuration**.
4. Clique em **DefaultGuestPortal** ou no nome de um portal personalizado que você possa ter criado.
5. Clique na caixa de seleção **Vlan DHCP Release**.**Observação:** essa opção funciona apenas para clientes Windows.



Fluxo de tráfico

Pode parecer difícil entender qual tráfego é enviado para onde nesse cenário. Aqui está uma revisão rápida:

- O cliente envia uma solicitação de associação pelo ar para o SSID.
- A WLC manipula a autenticação de filtragem MAC com o ISE (onde recebe os atributos de redirecionamento).
- O cliente só recebe uma resposta assoc depois que a filtragem MAC é concluída.
- O cliente envia uma solicitação DHCP, que é **LOCALMENTE** comutado pelo ponto de acesso para obter um endereço IP do local remoto.
- No estado Central_webauth, o tráfego marcado para deny na ACL de redirecionamento (portanto, o HTTP normalmente) é **CENTRALMENTE** comutado. Portanto, não é o AP que faz o redirecionamento, mas a WLC; por exemplo, quando o cliente solicita qualquer site, o AP envia isso para a WLC encapsulada no CAPWAP e a WLC falsifica esse endereço IP do site e redireciona para o ISE.
- O cliente é redirecionado para a URL de redirecionamento do ISE. Isso é **LOCALMENTE** novamente (porque ele acessa permit na ACL de redirecionamento flexível).
- Uma vez no estado RUN, o tráfego é comutado localmente.

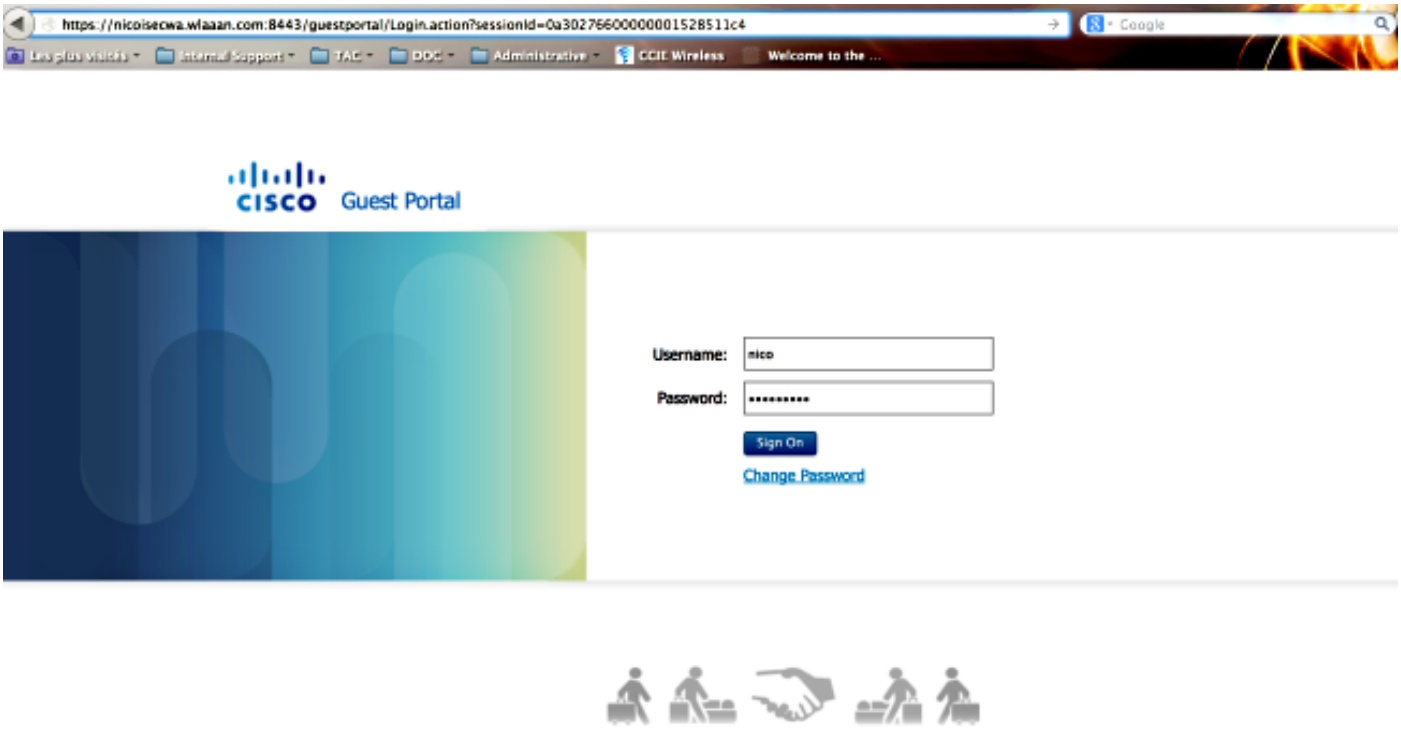
Verificar

Quando o usuário estiver associado ao SSID, a autorização será exibida na página do ISE.

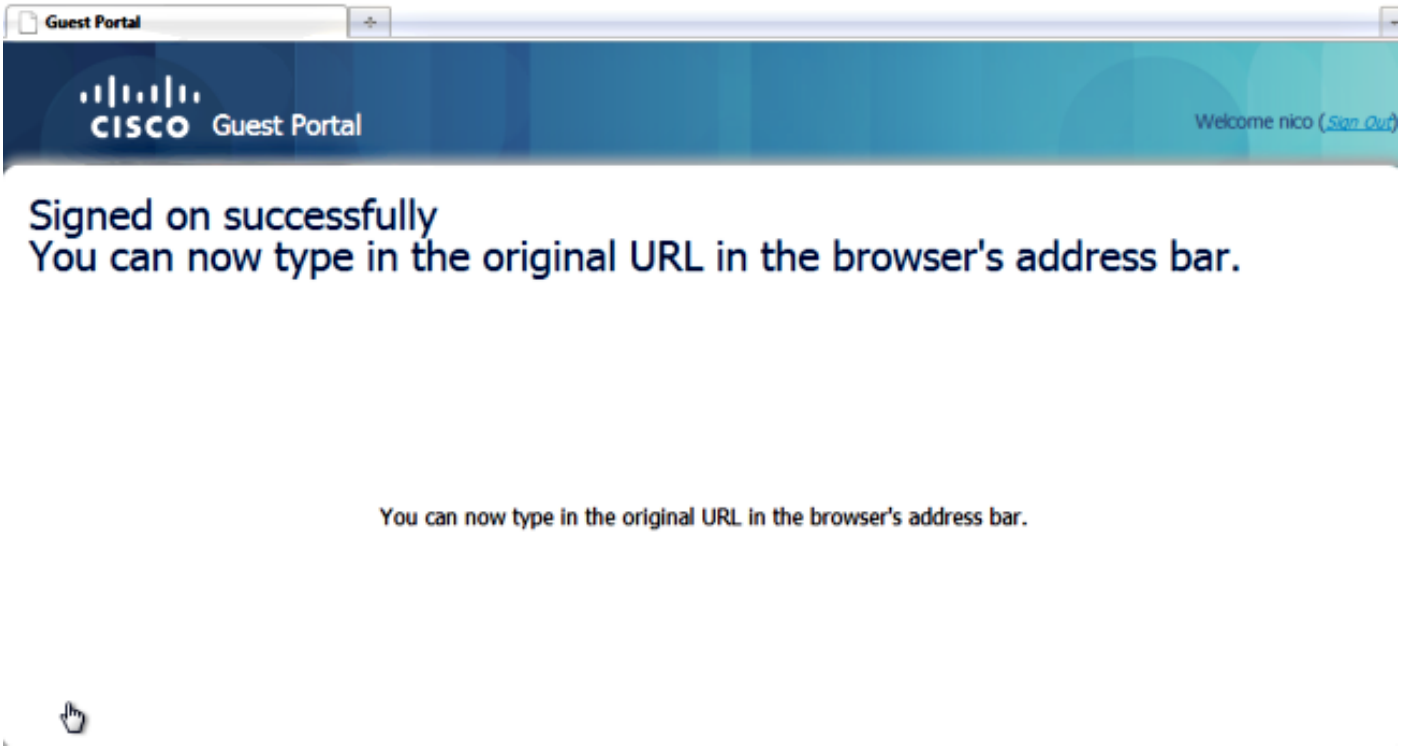
Apr 09,13 11:49:27.179 AM	✓		Nico	00:13:10:21:70:13	nicowlc	vlan34	Guest	NotApplicable	
Apr 09,13 11:49:27.174 AM	✓				nicowlc				Dynamic Author...
Apr 09,13 11:48:58.372 AM	✓		Nico	00:13:10:21:70:13			Guest		Guest Authentic..
Apr 09,13 11:47:19.475 AM	✓		00:13:10:21:70:13	00:13:10:21:70:13	nicowlc	CentralWebauth		Pending	Authentication ...

De baixo para cima, você pode ver a autenticação de filtragem de endereços MAC que retorna os atributos do CWA. A seguir está o login do portal com o nome de usuário. O ISE envia um CoA para a WLC e a última autenticação é uma autenticação de filtragem MAC da camada 2 no lado da WLC, mas o ISE lembra do cliente e do nome de usuário e aplica a VLAN necessária que configuramos neste exemplo.

Quando qualquer endereço é aberto no cliente, o navegador é redirecionado para o ISE. Verifique se o DNS (Domain Name System) está configurado corretamente.



O acesso à rede é concedido depois que o usuário aceita as políticas.



No controlador, o estado do Policy Manager e o estado do NAC RADIUS mudam de *POSTURE_REQD* para *RUN*.

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.