Exemplo de Configuração de Autenticação da Web Local do Portal de Convidado do Identity Services Engine

Contents

Introduction

Este documento descreve como configurar a autenticação da Web local (LWA) com o portal de convidado do Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE
- Cisco Wireless LAN Controller (WLC)

Componentes Utilizados

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

- ISE versão 1.4
- WLC versão 7.4

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. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Este documento descreve a configuração do LWA. No entanto, a Cisco recomenda que você use a CWA (Centralized Web Authentication) com o ISE sempre que possível. Há alguns cenários em que o LWA é preferencial ou a única opção, portanto, este é um exemplo de configuração para esses cenários.

Configurar

O LWA requer determinados pré-requisitos e uma configuração principal na WLC, bem como algumas alterações necessárias no ISE.

Antes de abordá-las, aqui está um esboço do processo LWA com o ISE.

Processo LWA com o Portal de Convidado do ISE

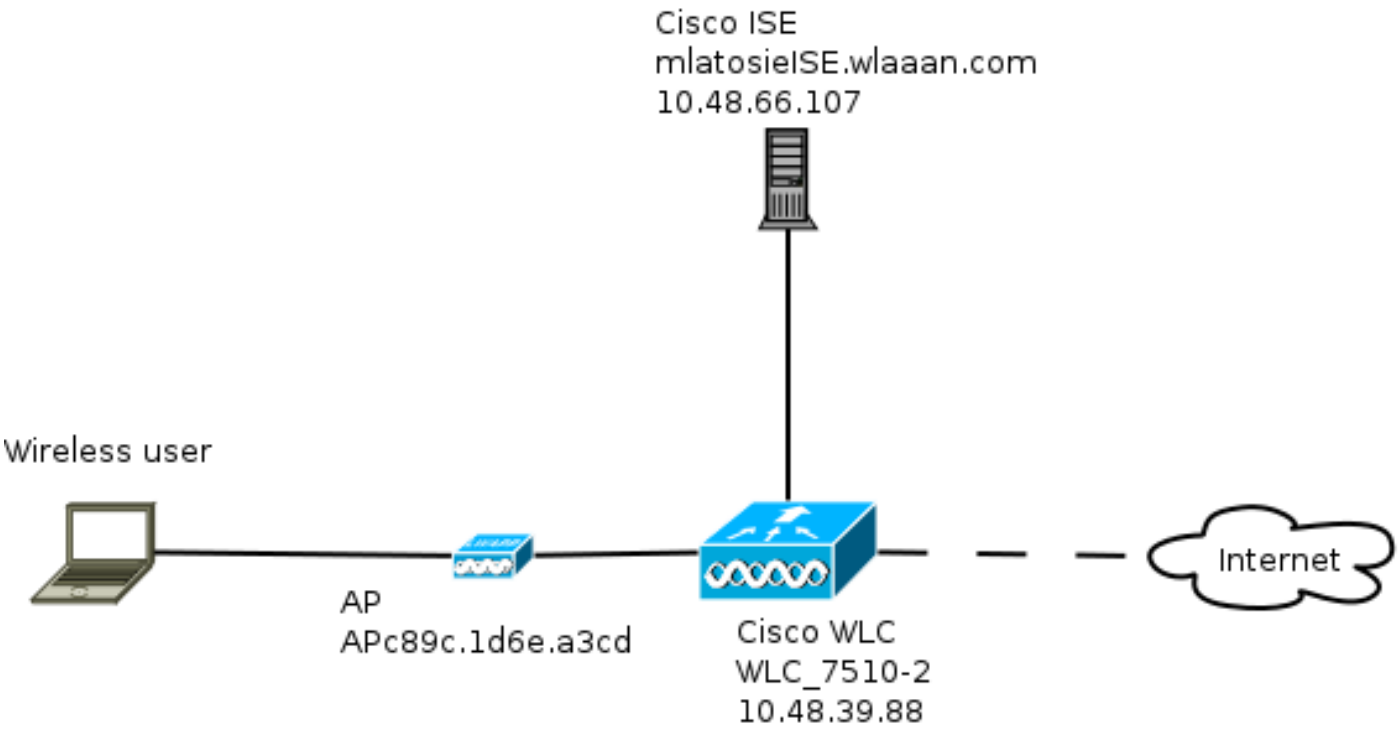
1. O navegador tenta buscar uma página da Web.
2. A WLC intercepta a solicitação HTTP(S) e a redireciona para o ISE.
   Várias informações importantes são armazenadas nesse cabeçalho de redirecionamento HTTP. Aqui está um exemplo do URL de redirecionamento:
   https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9#&ui-state=dialog?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/
   No exemplo de URL, você pode ver que o usuário tentou acessar "yahoo.com". O URL também contém informações sobre o nome da Rede Local Sem Fio (WLAN - Wireless Local Area Network) (mlatosie_LWA) e os endereços MAC do ponto de acesso e do cliente (AP).
   No exemplo de URL, **1.1.1.1** é a WLC, e **mlatosieise.wlaaan.com** é o servidor ISE.
3. O usuário recebe a página de login de convidado do ISE e digita o nome de usuário e a senha.
4. O ISE executa a autenticação em relação à sua sequência de identidade configurada.
5. O navegador é redirecionado novamente. Desta vez, ele envia credenciais para a WLC. O navegador fornece o nome de usuário e a senha que o usuário inseriu no ISE sem nenhuma interação adicional do usuário. Aqui está um exemplo de solicitação GET para a WLC.
   GET /login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
   Novamente, o URL original (**yahoo.com**), o nome de usuário (**mlatosie@cisco.com**) e a senha (**ityh**) estão incluídos.

Note: Embora a URL esteja visível aqui, a solicitação real é enviada pela SSL (Secure Sockets Layer), indicada pelo HTTPS, e é difícil de interceptar.

6. A WLC usa RADIUS para autenticar esse nome de usuário e senha em relação ao ISE e permitir o acesso.
7. O usuário é redirecionado para o portal especificado. Consulte a seção **"Configurar o ISE externo como o URL da Web"** deste documento para obter mais informações.

Diagrama de Rede

Esta figura descreve a topologia lógica dos dispositivos usados neste exemplo.



Pré-requisitos de configuração

Para que o processo LWA funcione corretamente, um cliente precisa obter:

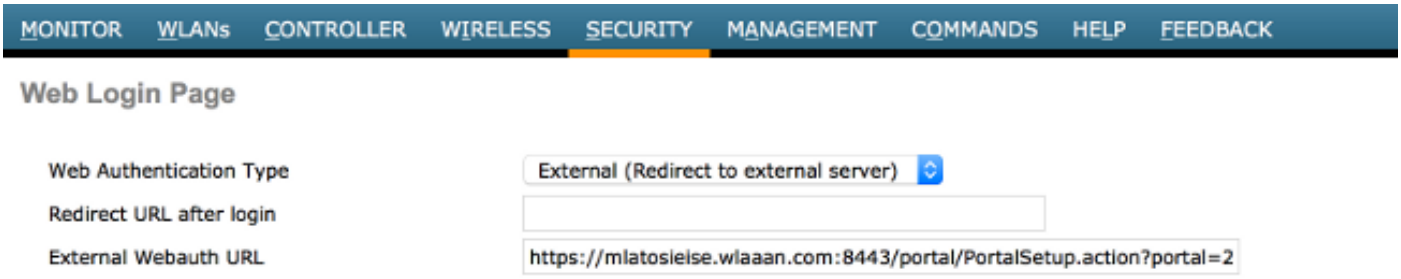
- Configuração de endereço IP e máscara de rede
- Rota padrão
- Servidor do Sistema de Nomes de Domínio (DNS)

Todos eles podem ser fornecidos com DHCP ou com a configuração local. A resolução DNS precisa funcionar corretamente para que o LWA funcione.

Configurar o WLC

Configure o ISE externo como a URL da Web globalmente

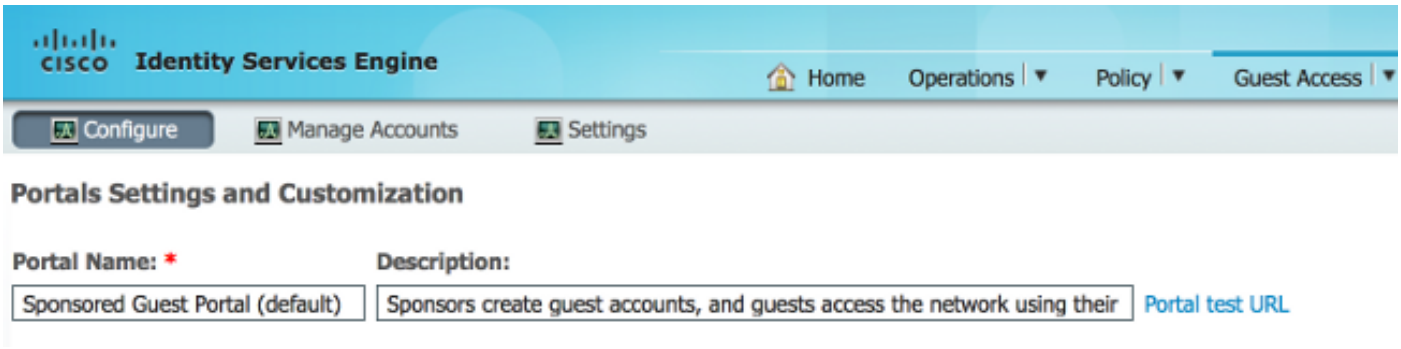
Em **Security > Web Auth > Web Login Page**, você pode acessar essas informações.



Note: Este exemplo usa um URL de Webauth Externo e foi extraído do ISE Versão 1.4. Se você tiver uma versão diferente, consulte o guia de configuração para entender o que deve ser configurado.

Também é possível configurar essa configuração por WLAN. Ela está nas configurações de segurança específicas da WLAN. Eles substituem a configuração global.

Para descobrir a URL correta para o seu portal específico, escolha **ISE > Guest Policy > Configure > your specific portal**. Clique com o botão direito do mouse no link "URL de teste do portal" e escolha **copiar local do link**.



Neste exemplo, o URL completo é: https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9

Configurar as listas de controle de acesso (ACLs)

Para que a autenticação da Web funcione, o tráfego permitido deve ser definido. Determine se as ACLs FlexConnect ou ACLs normais devem ser usadas. Os APs FlexConnect usam ACLs FlexConnect, enquanto os APs que usam comutação centralizada usam ACLs normais.

Para entender em que modo um AP específico opera, escolha **Wireless > Access points** e escolha a caixa suspensa **AP name > AP Mode**. Uma implantação típica é **local** ou **FlexConnect**.

Em **Segurança > Listas de Controle de Acesso,** escolha **ACLs FlexConnect** ou **ACLs**. Neste exemplo, todo o tráfego UDP foi permitido para permitir especificamente o intercâmbio e o tráfego de DNS para o ISE (10.48.66.107).

General

Access List Name FLEX_GUEST

Deny Counters 634752

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	Any	Any	Any	208398
2	Permit	10.48.66.107 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	32155
3	Permit	0.0.0.0 / 0.0.0.0	10.48.66.107 / 255.255.255.255	TCP	Any	Any	Any	Any	24532

Este exemplo usa o FlexConnect, então **tanto** o FlexConnect quanto as ACLs padrão são definidas.

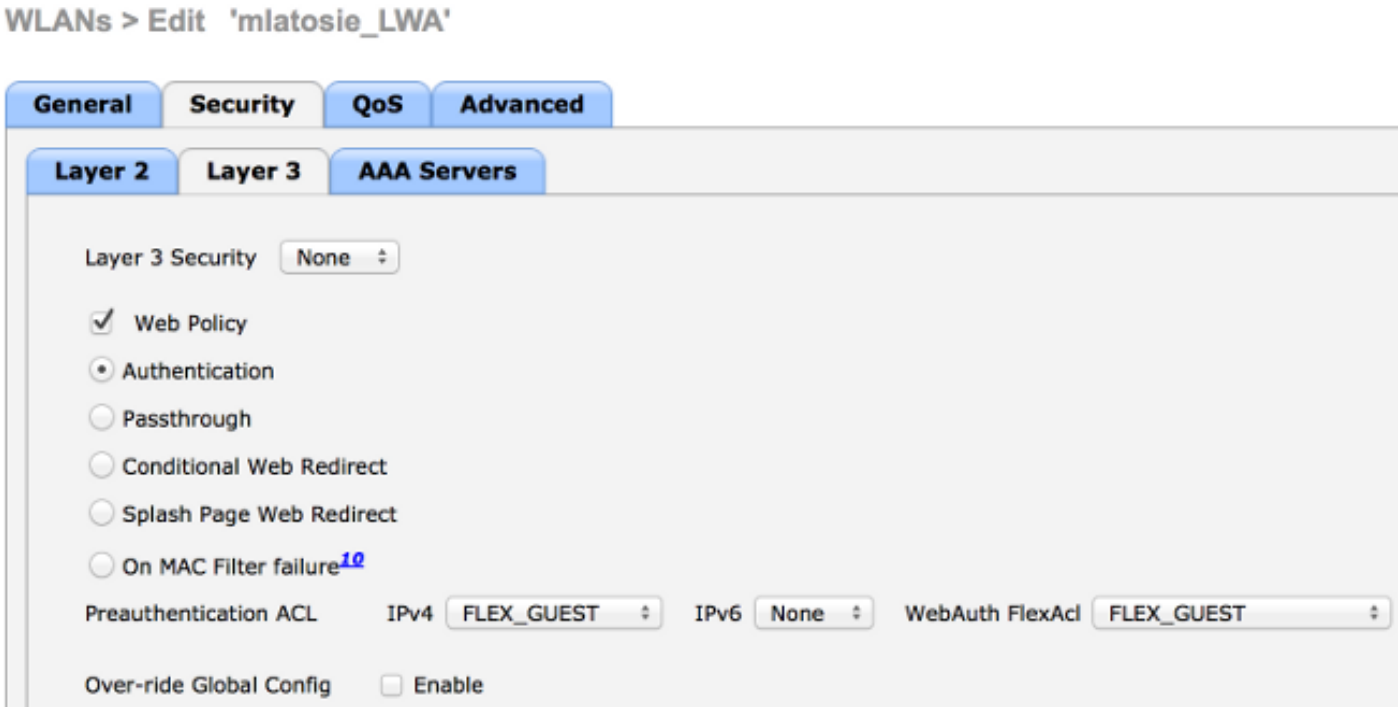
Esse comportamento é documentado no Cisco Bug ID CSCue68065 em relação aos controladores WLC 7.4. Ele não é mais necessário no WLC 7.5, onde você só precisa de uma FlexACL e não precisa mais de uma ACL padrão

Configurar o SSID (Service Set Identifier, Identificador do conjunto de serviços) para LWA

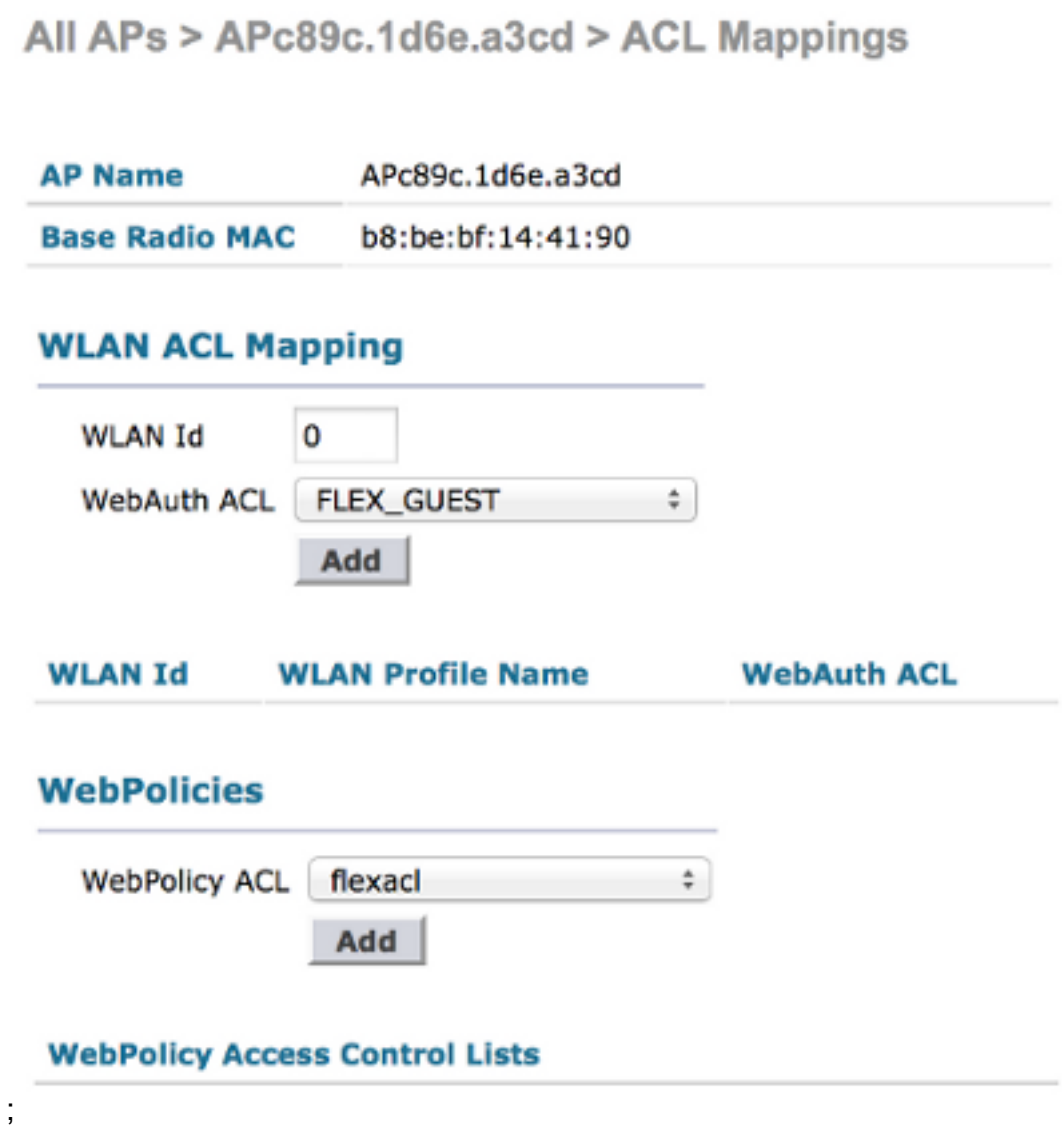
Em **WLANs,** escolha a **ID da WLAN** para editar.

Configuração do Web Auth

Aplique as mesmas ACLs definidas na etapa anterior e habilite a autenticação da Web.



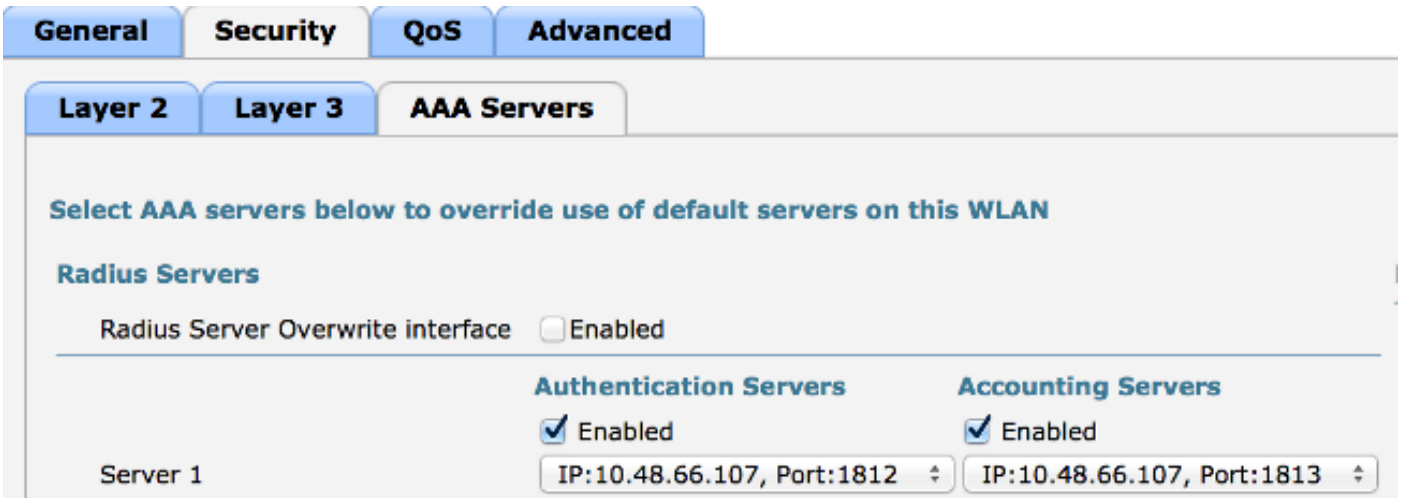
Note: Se o recurso de comutação local do FlexConnect for usado, o mapeamento da ACL precisará ser adicionado no nível do AP. Isso pode ser encontrado em **Wireless > Access Points.** Escolha o **nome do AP** apropriado **> FlexConnect > External WebAuthentication ACLs**.



;

Autenticação, autorização e configuração do servidor de contabilidade (AAA)

Neste exemplo, os servidores de autenticação e tarifação apontam para o servidor ISE definido anteriormente.



Note: Os padrões na guia **Avançado** não precisam ser acrescentados.

Configurar o ISE

A configuração do ISE consiste em várias etapas.

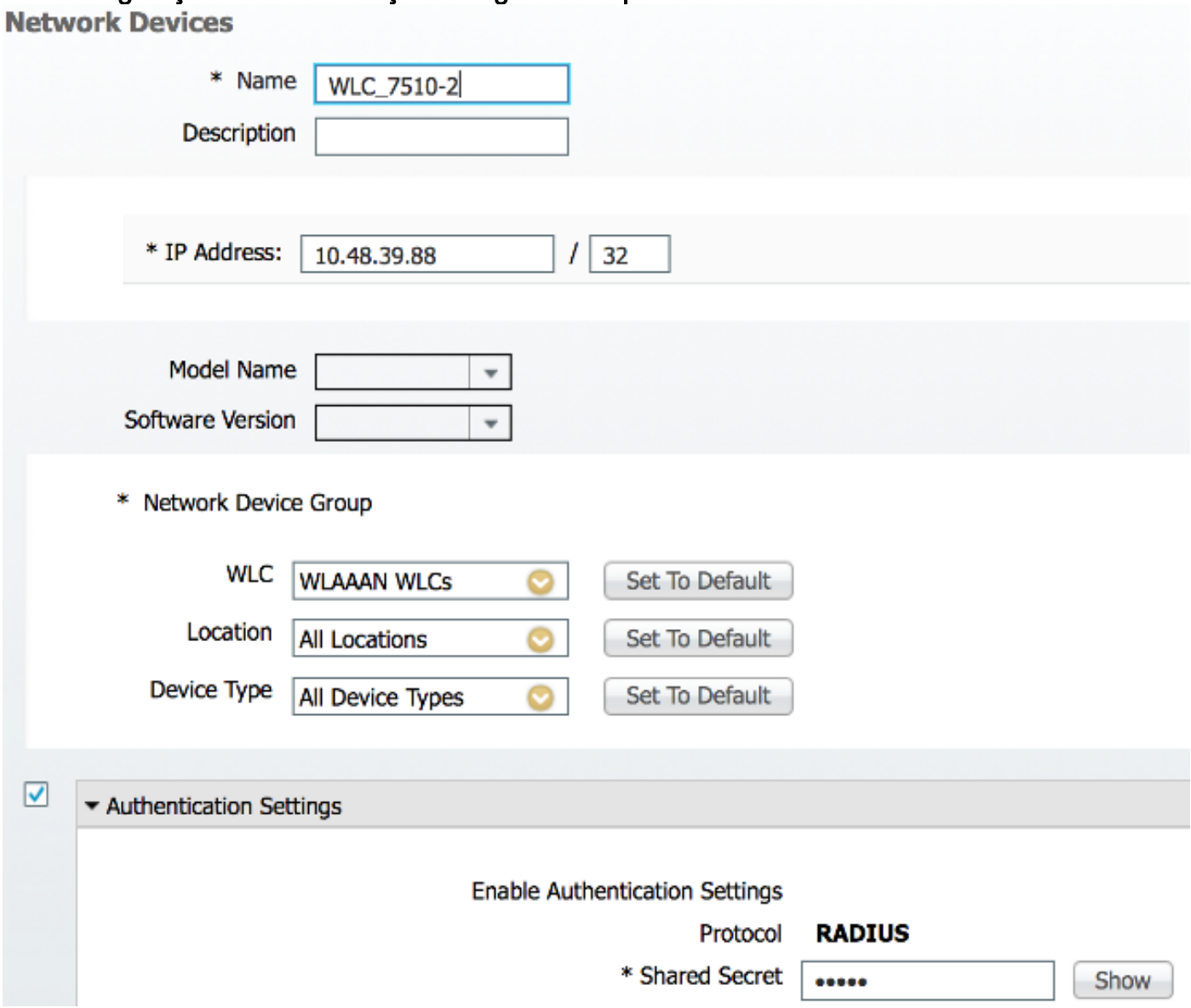
Primeiro, defina o dispositivo como um dispositivo de rede.

Em seguida, assegure-se de que as regras de autenticação e autorização que acomodam essa troca existam.

Definir o dispositivo de rede

Em **Administration > Network Resources > Network Devices**, preencha estes campos:

- Nome de dispositivo
- Endereço IP do dispositivo
- **Configurações de autenticação > Segredo compartilhado**

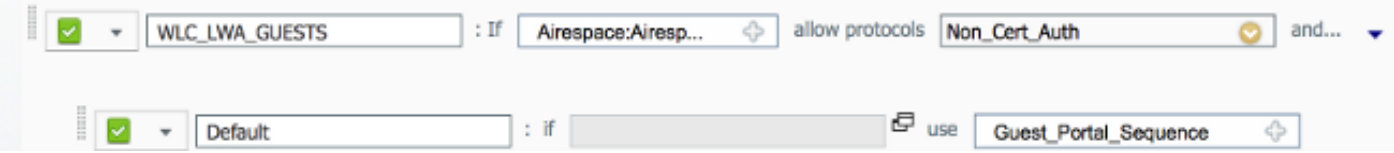


Configurar a política de autenticação

Em **Política > Autenticação**, adicione uma nova política de autenticação.

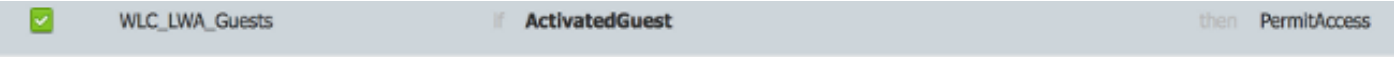
Este exemplo usa estes parâmetros:

- Nome: **WLC_LWA_Guests**
- Condição: **Airespace:Airespace-Wlan-Id.** Essa condição corresponde ao ID da WLAN 3, que é o ID do WLAN **mlatosie_LWA** que foi definido anteriormente na WLC.
- {opcional} Permite protocolos de autenticação que não exigem o certificado **Non_Cert_Auth**, mas os padrões podem ser usados.
- Guest_Portal_Sequence, que define que os usuários são usuários convidados definidos localmente.



Configurar a política de autorização e o resultado

Em **Política > Autorização,** defina uma nova política. Pode ser uma política muito básica, como:

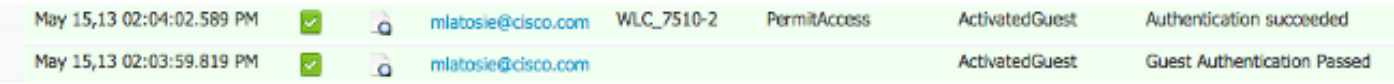


Essa configuração depende da configuração geral do ISE. Este exemplo é propositalmente simplificado.

Verificar

No ISE, os administradores podem monitorar e solucionar problemas de sessões ao vivo em **Operações > Autenticações**.

Duas autenticações devem ser vistas. A primeira autenticação é do portal do convidado no ISE. A segunda autenticação vem como uma solicitação de acesso da WLC ao ISE.



Você pode clicar no ícone **Authentication Detail Report** para verificar quais políticas de autorização e de autenticação foram escolhidas.

Na WLC, um administrador pode monitorar clientes em **Monitor > Client**.

Aqui está um exemplo de um cliente que foi autenticado corretamente:

Troubleshoot

A Cisco recomenda que você execute depurações por meio do cliente sempre que possível.

Através da CLI, essas depurações fornecem informações úteis:

```
debug client MA:CA:DD:RE:SS

debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable
```

Informações Relacionadas

- Guia de configuração do Cisco ISE 1.x
- Guia de configuração do Cisco WLC 7.x
- Suporte Técnico e Documentação - Cisco Systems