

Exemplo de configuração local da autenticação da Web do portal do convidado do Identity Services Engine



ID do Documento: 116217

Atualizado em: novembro 25, 2015

Contribuído por Marcin Latosiewicz e por Nicolas Darchis, engenheiros de TAC da Cisco.



[Transferência PDF](#)

[Imprimir](#)

[Feedback](#)

Produtos Relacionados

- [Wireless LAN \(WLAN\)](#)
- [Cisco Identity Services Engine](#)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Processo LWA com o portal do convidado ISE](#)

[Diagrama de Rede](#)

[Pré-requisito de configuração](#)

[Configurar o WLC](#)

[Configurar o ISE externo como o Webauth URL globalmente](#)

[Configurar o Access Control Lists \(ACLs\)](#)

[Configurar o Service Set Identifier \(SSID\) para LWA](#)

[Configurar o ISE](#)

[Defina o dispositivo de rede](#)

[Configurar a política de autenticação](#)

[Configurar a política e o resultado da autorização](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

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

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE
- Controlador de LAN do Cisco Wireless (WLC)

Componentes Utilizados

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

- Versão 1.4 ISE
- Versão 7.4 WLC

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve a configuração de LWA. Contudo, Cisco recomenda que você use a autenticação da Web centralizada (CWA) com o ISE sempre que possível. Há algumas encenações onde LWA é preferido ou a única opção, assim que este é um exemplo de configuração para aquelas encenações.

Configurar

LWA exige determinados prerequisites e uma configuração principal no WLC assim como algumas mudanças necessários no ISE.

Antes que aqueles estejam cobertos, está aqui um esboço do processo LWA com o ISE.

Processo LWA com o portal do convidado ISE

1. As tentativas do navegador para buscar um página da web.
2. O WLC intercepta o pedido do HTTP e reorienta-o ao ISE.
Diversas partes principal de informação são armazenadas nesse HTTP reorientam o encabeçamento. Está aqui um exemplo da reorientação URL:
`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/`
Do exemplo URL, você pode ver que o usuário tentou alcançar “yahoo.com.” A URL igualmente contém a informação sobre o nome do Wireless Local Area Network (WLAN) (mlatosie_LWA), e o cliente e os endereços do Access Point (AP) MAC. No exemplo URL, 1.1.1.1 é o WLC, e mlatosieise.wlaaan.com é o server ISE.
3. O usuário é apresentado com a página de login do convidado ISE e incorpora o nome de usuário e senha.
4. O ISE executa a autenticação contra sua sequência configurada da identidade.
5. O navegador reorienta outra vez. Esta vez, submete credenciais ao WLC. O navegador fornece o nome de usuário e senha que o usuário incorporou ao ISE sem nenhuma interação adicional do usuário. Está aqui um pedido do exemplo GET ao WLC.
GET
`/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0`
Além disso, todos a URL original (**yahoo.com**), o username (**mlatosie@cisco.com**), e a senha (**ityh**) são incluídos.
Note: Embora a URL seja visível aqui, o pedido real é submetido sobre o secure sockets layer (SSL), que é indicado pelo HTTPS, e é duro de interceptar.
6. O WLC usa o RAIO a fim autenticar que nome de usuário e senha contra o ISE e permite o acesso.
7. O usuário é reorientado ao portal especificado. Refira “**configuram o ISE externo como a seção do webauth a URL**” deste documento para mais informação.

Diagrama de Rede

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

Pré-requisito de configuração

Para que o processo LWA trabalhe corretamente, um cliente precisa de poder obter:

- Configuração do endereço IP de Um ou Mais Servidores Cisco ICM NT e do netmask
- Rota padrão
- Server do Domain Name System (DNS)

Toda a estes pode ser fornecida com o DHCP ou a configuração local. A resolução de DNS precisa de trabalhar corretamente para que o LWA trabalhe.

Configurar o WLC

Configurar o ISE externo como o Webauth URL globalmente

Sob o **AUTH da Segurança > da Web > a página de login da Web**, você pode alcançar esta informação.

Note: Este exemplo usa um Webauth externo URL e foi tomado da versão 1.4 ISE. Se você tem uma versão diferente, consulte o manual de configuração a fim compreender o que deve ser configurado.

É igualmente possível configurar este por-WLAN de ajuste. Está então nos ajustes específicos da Segurança de WLAN. Aqueles cancelam a configuração global.

A fim encontrar a URL correta para seu portal específico, escolha **ISE > política do convidado > configuram > seu portal específico**. Clicar com o botão direito o link “do teste portal URL” e escolha o **lugar do link da cópia**.

Neste exemplo, a URL completa é:

<https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9>

Configurar o Access Control Lists (ACLs)

Para que a autenticação da Web trabalhe, o tráfego permitido deve ser definido. Determine se FlexConnect ACL ou ACL normais deve ser usado. FlexConnect AP usar FlexConnect ACL, quando os AP que usam o uso centralizado ACL normais do interruptor.

A fim compreender no que modo um AP particular opere, escolha o **Sem fio > os Access point** e escolha o **nome AP > a caixa suspensa do modo AP**. Uma implementação típica é **local** ou **FlexConnect**.

Sob a **Segurança > as listas de controle de acesso**, escolha **FlexConnect ACL** ou **ACL**. Neste exemplo, todo o tráfego UDP foi permitido a fim permitir especificamente a troca e o tráfego DNS ao ISE (10.48.66.107).

Este exemplo usa FlexConnect, assim que FlexConnect e o padrão ACL são definidos.

Este comportamento é documentado na identificação de bug Cisco [CSCue68065](#) no que diz respeito aos controladores WLC 7.4. Não se exige anymore em WLC 7.5 onde você não precisa somente um FlexACL e nenhum padrão ACL anymore

Configurar o Service Set Identifier (SSID) para LWA

Sob **WLAN**, escolha o **ID de WLAN** editar.

Configuração do AUTH da Web

Aplique os mesmos ACL que foram definidos na etapa precedente e permita a autenticação da Web.

Note: Se a característica do switching local de FlexConnect é usada, o mapeamento ACL precisa de ser adicionado no nível AP. Isto pode ser encontrado sob o **Sem fio > os Access point**. Escolha o nome apropriado > **FlexConnect AP > WebAuthentication externo ACL**.
;

Configuração do servidor do Authentication, Authorization, and Accounting (AAA)

Neste exemplo, a autenticação e os servidores de contabilidade apontam ao server precedente-definido ISE.

Note: Os padrões sob o **guia avançada** não precisam de ser adicionados.

Configurar o ISE

A configuração ISE consiste em diversas etapas.

Primeiramente, defina o dispositivo como um dispositivo de rede.

Então, assegure-se de que as regras da authentication e autorização que acomodam esta troca existam.

Defina o dispositivo de rede

Sob a **administração > recursos de rede > dispositivos de rede**, povoe estes campos:

- Nome de dispositivo
- Endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo
- **Ajustes da autenticação > segredo compartilhado**

Configurar a política de autenticação

Sob a **política > a autenticação**, adicionar uma política de autenticação nova.

Este exemplo usa estes parâmetros:

- Nome: **WLC_LWA_Guests**
- Condição: **Airespace: Airespace-WLAN-identificação**. Esta circunstância combina o ID de WLAN de 3, que é o ID do **mлатosie_LWA** WLAN que foi definido previamente no WLC.
- {opcional} permite os 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 local-definidos dos convidados.

Configurar a política e o resultado da autorização

Sob a **política > a autorização**, defina uma política nova. Pode ser muito uma política básica, como:

Esta configuração depende da configuração total do ISE. Este exemplo é simplificado purposefully.

Verificar

No ISE, os administradores podem monitorar e pesquisar defeitos sessões vivas sob **operações > autenticações**.

Duas autenticações devem ser consideradas. A primeira autenticação é do portal do convidado no ISE. A segunda autenticação vem como um pedido do acesso do WLC ao ISE.

Você pode clicar o ícone dos **relatórios de detalhes da autenticação** a fim verificar que políticas e políticas de autenticação da autorização foram escolhidas.

No WLC, um administrador pode monitorar clientes sob o **monitor > o cliente**.

Está aqui um exemplo de um cliente que autentique corretamente:

Troubleshooting

Cisco recomenda que você é executado debuga por meio do cliente sempre que possível.

Com o CLI, estes debugam fornecem a informação util:

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

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

```
debug aaa all enable
```

Informações Relacionadas

- [Manual de configuração de Cisco ISE 1.x](#)
- [Manual de configuração de Cisco WLC 7.x](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Era este documento útil? [Sim nenhum](#)

Obrigado para seu feedback.

[Abra um caso de suporte](#) (exige um [contrato de serviço Cisco](#).)

Cisco relacionado apoia discussões da comunidade

[Cisco apoia a comunidade](#) é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira [convenções dos dicas técnicas da Cisco](#) para obter informações sobre das convenções usadas neste documento.

Atualizado em: novembro 25, 2015

ID do Documento: 116217