

# 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[与ISE访客门户的LWA进程](#)

[网络图](#)

[配置前提](#)

[配置 WLC](#)

[配置外部ISE作为Webauth URL](#)

[配置访问控制列表\(ACL\)](#)

[配置LWA的服务集标识\(SSID\)](#)

[配置ISE](#)

[定义网络设备](#)

[配置验证策略](#)

[配置授权策略和结果](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文描述如何配置本地Web验证(LWA)与思科身份服务引擎(ISE)访客门户。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- ISE
- Cisco 无线局域网控制器 (WLC)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- ISE版本1.1

- WLC版本7.4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 背景信息

本文描述LWA的配置。然而，思科建议您以ISE使用集中化Web验证(CWA)若情况许可。有LWA更喜欢或唯一选择的一些个方案，因此这是那些方案的配置示例。

## 配置

LWA要求在ISE和一个主要配置在WLC以及一些更改需要的某些prerequisites。

在那些被覆盖前，这是LWA进程的概述与ISE的。

### 与ISE访客门户的LWA进程

1. 浏览器设法拿来网页。
2. WLC拦截HTTP请求并且重定向它对ISE。  
几个关键信息在该HTTP重定向报头存储。这是重定向URL的示例：  
`https://mlatosieise.wlaaan.com:8443/guestportal/Login.action?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/`  
从示例URL，您能看到用户设法到达“yahoo.com”。URL也包含关于无线局域网(WLAN)名称(mlatosie\_LWA)的信息和客户端和接入点(AP) MAC地址。在示例URL中，1.1.1.1是WLC，并且mlatosieise.wlaaan.com是ISE服务器。
3. 用户提交与ISE访客登录页并且输入用户名和密码。
4. ISE执行验证其已配置的标识顺序。
5. 再浏览器重定向。这时，它提交凭证对WLC。浏览器提供用户在ISE输入，不用从用户的任何另外的交互作用的用户名和密码。这是示例GET请求对WLC。  
GET  
`/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0`  
再次，原始URL (yahoo.com)，用户名(mlatosie@cisco.com)和密码(ityh)是包括的全部。  
**注意：**虽然URL可视在这里，实际请求在安全套接字协议层(SSL)提交，是由HTTPS表示的，并且是难拦截。
6. WLC使用RADIUS为了验证用户名和密码ISE并且允许访问。
7. 用户重定向到指定的门户。参考本文的“**配置外部ISE作为webauth URL**”部分欲知更多信息。

## 网络图

此图描述用于此示例的设备逻辑拓扑。

## 配置前提

为了使这种网络屏敏配置，客户端需要能获取：

- 默认路由
- 域名系统 (DNS) 服务器

所有这些可以带有DHCP或本地配置。

DNS解析需要适当地运作为了LWA能工作。

## 配置 WLC

### 配置外部ISE作为Webauth URL

在**安全> Web验证> Web登录**页下，您能访问此信息。

**注意：**此示例使用外部Webauth URL和从ISE版本1.1被采取了。如果有一个不同的版本，请参见配置指南为了了解应该配置什么。

### 配置访问控制列表(ACL)

为了使工作Web的验证，应该定义允许流量。

确定是否应该使用FlexConnect ACL或正常ACL。

FlexConnect AP使用使用集中化交换使用正常ACL的FlexConnect ACL，当AP时。

为了了解在什么模式特定AP操作，请导航到**Wireless>Access点**并且选择**AP名称> AP模式**下拉框。一典型的部署是**本地**或**FlexConnect**。

在**安全>访问控制列表**下，请选择**FlexConnect ACL**或**ACL**。

在本例中，所有UDP流量允许为了特别地允许DNS交换和流量到ISE (10.48.66.107)。

此示例使用FlexConnect，因此FlexConnect和标准ACL定义。

此行为在Cisco Bug ID [CSCue68065](#)描述关于WLC 7.4控制器。

### 配置LWA的服务集标识(SSID)

在**WLAN**下，请选择**WLAN ID**编辑。

### Web验证配置

应用在上一步定义的同样ACL并且启用Web验证。

**注意：**如果FlexConnect的使用本地交换功能，ACL映射在AP级别上需要被添加。这可以被找到在**Wireless>Access点**下。选择适当的**AP名称> FlexConnect >外部WebAuthentication ACL**。

;

## 验证、授权和统计(AAA)服务器配置

在本例中，验证和记帐服务器指向早先定义的ISE服务器。

**注意：**在高级选项卡。下的默认不需要被添附。

## 配置ISE

ISE配置包括几个步骤。

首先，请定义设备作为网络设备。

然后，请保证适应此交换的认证和授权规则存在。

### 定义网络设备

在**管理下->网络资源->网络设备**，填充这些字段：

- 设备名
- 设备的 IP 地址
- **验证设置>共享塞克雷**

### 配置验证策略

在**策略>验证下**，请添加一项新证书策略。

此示例使用这些参数：

- 名称：**WLC\_LWA\_Guests**
- 条件：**Airespace**：Airespace WLAN Id.此情况匹配WLAN ID 3，是WLAN mlatosie\_LWA ID在WLC以前定义。
- {可选}它允许不要求证书**Non\_Cert\_Auth**的身份验证协议，但是可以使用默认。
- **Guest\_Portal\_Sequence**，定义了用户是本地定义的客人身份的用户。

### 配置授权策略和结果

在**策略>授权下**，请定义一项新的策略。它可以是一个非常基本策略，例如：

此配置取决于ISE的整体配置。此示例有目的地简化。

## [验证](#)

在ISE，管理员能监控和排除故障会话在**操作>认证**下。

应该看到两个认证。第一验证是从ISE的访客门户。第二验证来自，访问请求WLC到ISE。

您能点击授权策略和验证策略选择的**验证详细报表**图标验证。

在WLC，管理员能监控客户端在**监视器>客户端**下。

这是适当地验证客户端的示例：

## **[故障排除](#)**

思科建议您通过客户端运行调试若情况许可。

通过CLI，这些调试提供有用的信息：

## **相关信息**

- [思科ISE 1.x配置指南](#)
- [思科WLC 7.x配置指南](#)
- [技术支持和文档 - Cisco Systems](#)