

# 身份服务引擎访客门户本地Web身份验证配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[ISE访客门户的LWA流程](#)

[网络图](#)

[配置前提](#)

[配置 WLC](#)

[将外部ISE配置为全局Webauth URL](#)

[配置访问控制列表\(ACL\)](#)

[配置LWA的服务集标识符\(SSID\)](#)

[配置ISE](#)

[定义网络设备](#)

[配置身份验证策略](#)

[配置授权策略和结果](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文档介绍如何使用思科身份服务引擎(ISE)访客门户配置本地Web身份验证(LWA)。

## 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1.4

- 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

本文档介绍LWA的配置。但是，思科建议尽可能将集中式Web身份验证(CWA)与ISE配合使用。有一些情况是首选LWA或唯一选项，因此这是这些情况的配置示例。

## 配置

LWA要求在WLC上执行某些预要求和主要配置，以及在ISE上执行一些更改。

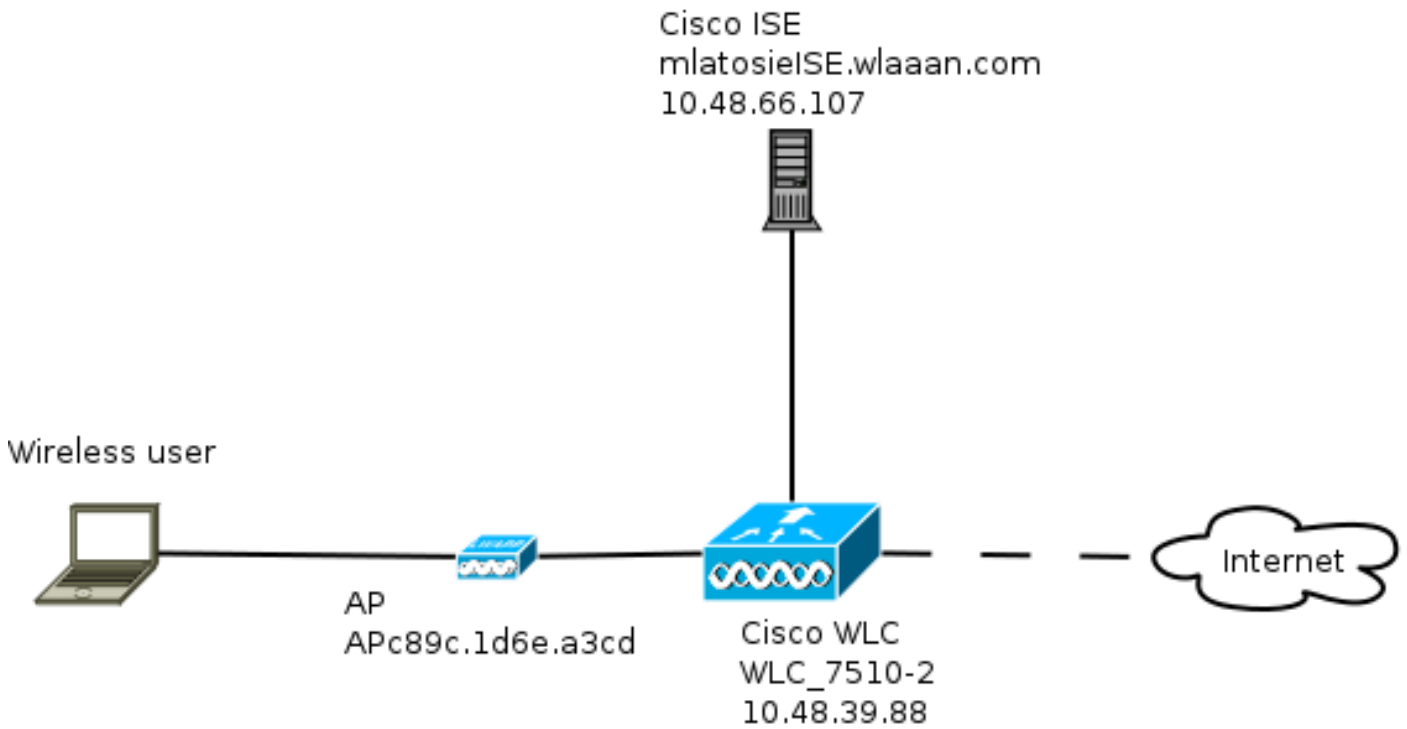
在涵盖这些内容之前，以下是ISE的LWA流程的概要。

### ISE访客门户的LWA流程

1. 浏览器尝试获取网页。
2. WLC拦截HTTP(S)请求并将其重定向到ISE。  
该HTTP重定向报头中存储了若干关键信息。以下是重定向URL的示例：  
`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/`  
从示例URL中，您可以看到用户尝试访问“yahoo.com”。该URL还包含有关无线局域网(WLAN)名称(mlatosie\_LWA)以及客户端和接入点(AP)MAC地址的信息。在示例URL中，1.1.1.1是WLC，mlatosies.wlaaan.com是ISE服务器。
3. 用户将显示ISE访客登录页面并输入用户名和密码。
4. ISE根据其配置的身份序列执行身份验证。
5. 浏览器再次重定向。这次，它会向WLC提交凭证。浏览器提供用户在ISE中输入的用户名和密码，无需用户进行任何其他交互。以下是WLC的GET请求示例。  
GET  
`/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0`  
同样，原始URL(yahoo.com)、用户名(mlatosie@cisco.com)和密码(ityh)都包括在内。  
**注意：**虽然URL在此处可见，但实际请求是通过安全套接字层(SSL)提交的，由HTTPS表示，且难以拦截。
6. WLC使用RADIUS来根据ISE验证该用户名和密码并允许访问。
7. 用户被重定向到指定的门户。有关详细信息，请参阅本文档的“将外部ISE配置为webauth URL”部分。

## 网络图

本图描述了本示例中使用的设备的逻辑拓扑。



## 配置前提

要使LWA流程正常工作，客户端需要能够获得：

- IP地址和网络掩码配置
- 默认路由
- 域名系统 (DNS) 服务器

所有这些都可以通过DHCP或本地配置提供。DNS解析需要正常工作，LWA才能正常工作。

## 配置 WLC

### 将外部ISE配置为全局Webauth URL

在Security > Web Auth > Web Login Page下，您可以访问此信息。

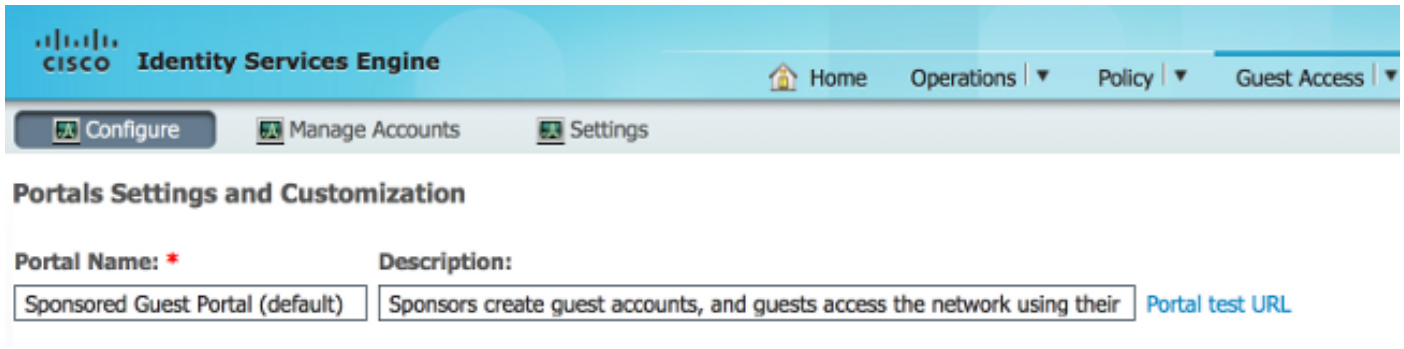
| MONITOR                  | WLANs   | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|--------------------------|---|------------|----------|----------|------------|----------|------|----------|
| <b>Web Login Page</b>    |   |            |          |          |            |          |      |          |
| Web Authentication Type  | External (Redirect to external server) <input type="button" value="v"/>                             |            |          |          |            |          |      |          |
| Redirect URL after login | <input type="text"/>  |            |          |          |            |          |      |          |
| External Webauth URL     | <input type="text" value="https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=2"/> |            |          |          |            |          |      |          |

**注意：**此示例使用外部Webauth URL，并取自ISE版本1.4。如果您有其他版本，请参阅配置指南以了解应配置的内容。

也可以按WLAN配置此设置。然后，它将处于特定WLAN安全设置中。这些设置会覆盖全局设置。

要查找特定门户的正确URL，请选择ISE > Guest Policy > Configure > Your specific portal。右键单

击“门户测试URL”中的链接，然后选择复制链接位置。



在本例中，完整URL为

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

### 配置访问控制列表(ACL)

要使Web身份验证有效，应定义允许的流量。确定应使用FlexConnect ACL还是普通ACL。FlexConnect AP使用FlexConnect ACL，而使用集中交换的AP使用普通ACL。

要了解特定AP在什么模式下运行，请选择Wireless > Access points，然后选择AP name > AP Mode下拉框。典型的部署是本地部署或FlexConnect。

在安全>访问控制列表下，选择FlexConnect ACL或ACL。在本示例中，允许所有UDP流量，以便明确允许DNS交换和流向ISE(10.48.66.107)的流量。

#### 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         | <input checked="" type="checkbox"/> |
| 2   | Permit | 10.48.66.107 / 255.255.255.255 | 0.0.0.0 / 0.0.0.0              | TCP      | Any         | Any       | Any  | Any       | 32155          | <input checked="" type="checkbox"/> |
| 3   | Permit | 0.0.0.0 / 0.0.0.0              | 10.48.66.107 / 255.255.255.255 | TCP      | Any         | Any       | Any  | Any       | 24532          | <input checked="" type="checkbox"/> |

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

有关WLC 7.4控制器，此行为记录在Cisco Bug ID CSCue68065中。在WLC 7.5中，您不再需要FlexACL，不再需要标准ACL

### 配置LWA的服务集标识符(SSID)

在WLANs下，选择要编辑的WLAN ID。

### 网络身份验证配置

应用上一步中定义的同ACL并启用Web身份验证。

Layer 3 Security

Web Policy  
 Authentication  
 Passthrough  
 Conditional Web Redirect  
 Splash Page Web Redirect  
 On MAC Filter failure<sup>10</sup>

Preauthentication ACL IPv4  IPv6  WebAuth FlexAcl

Over-ride Global Config  Enable

注意：如果使用FlexConnect的本地交换功能，则需要在AP级别添加ACL映射。这可在 Wireless > Access Points 下找到。选择适当的AP Name > FlexConnect > External WebAuthentication ACL。

### All APs > APc89c.1d6e.a3cd > ACL Mappings

|                       |                   |
|-----------------------|-------------------|
| <b>AP Name</b>        | APc89c.1d6e.a3cd  |
| <b>Base Radio MAC</b> | b8:be:bf:14:41:90 |

#### WLAN ACL Mapping

WLAN Id   
 WebAuth ACL

| WLAN Id | WLAN Profile Name | WebAuth ACL |
|---------|-------------------|-------------|
|---------|-------------------|-------------|

#### WebPolicies

WebPolicy ACL

#### WebPolicy Access Control Lists

;

## 身份验证、授权和记帐(AAA)服务器配置

在本例中，身份验证和记帐服务器都指向之前定义的ISE服务器。

| Radius Servers                    |   |
|-----------------------------------|---|
| Radius Server Overwrite interface | <input type="checkbox"/> Enabled            |
|                                   | <b>Authentication Servers</b>               |
|                                   | <input checked="" type="checkbox"/> Enabled |
|                                   | <b>Accounting Servers</b>                   |
|                                   | <input checked="" type="checkbox"/> Enabled |
| Server 1                          | IP:10.48.66.107, Port:1812                  |
|                                   | IP:10.48.66.107, Port:1813                  |

注意：无需附加“高级”选项卡下的默认值。

## 配置ISE

ISE配置包括几个步骤。

首先，将设备定义为网络设备。

然后，确保包含此交换的身份验证和授权规则存在。

### 定义网络设备

在**管理>网络资源>网络设备**下，填写以下字段：

- 设备名
- 设备的 IP 地址
- **身份验证设置>共享密钥**

## Network Devices

\* Name

Description

\* IP Address:  /

Model Name

Software Version

\* Network Device Group

WLC

Location

Device Type

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

## 配置身份验证策略

在**策略>身份验证**下，添加新的身份验证策略。

本示例使用以下参数：

- 名称：**WLC\_LWA\_Guests**
- 条件：**Airespace:Airespace-Wlan-Id**。此条件与WLAN ID 3匹配，该WLAN ID是WLC上先前定义的WLAN mlatosie\_LWA的ID。
- {可选}它允许不需要证书Non\_Cert\_Auth的身份验证协议，但可以使用默认值。
- Guest\_Portal\_Sequence，它定义用户是本地定义的访客户户。

: If  allow protocols  and...

: if  use

## 配置授权策略和结果

在“策略”>“授权”下定义新策略。它可以是非常基本的策略，例如：

此配置取决于ISE的整体配置。此示例有目的地进行了简化。

## 验证

在ISE上，管理员可以在Operations > Authentications下监控实时会话并对其进行故障排除。

应该看到两个身份验证。第一个身份验证来自ISE上的访客门户。第二个身份验证作为从WLC到ISE的访问请求。

|                           |   |  |                    |            |              |                |                             |
|---------------------------|---|--|--------------------|------------|--------------|----------------|-----------------------------|
| May 15,13 02:04:02.589 PM | ✓ |  | mlatosie@cisco.com | WLC_7510-2 | PermitAccess | ActivatedGuest | Authentication succeeded    |
| May 15,13 02:03:59.819 PM | ✓ |  | mlatosie@cisco.com |            |              | ActivatedGuest | Guest Authentication Passed |

您可以单击Authentication Detail Report图标以验证选择了哪些授权策略和身份验证策略。

在WLC上，管理员可以在“监控”>“客户端”下监控客户端。

以下是正确进行身份验证的客户端示例：

|                   |                  |              |              |                    |          |            |     |   |    |
|-------------------|------------------|--------------|--------------|--------------------|----------|------------|-----|---|----|
| 28:cf:e9:13:47:cb | APc89c.1d6e.a3cd | mlatosie_LWA | mlatosie_LWA | mlatosie@cisco.com | 802.11bn | Associated | Yes | 1 | No |
|-------------------|------------------|--------------|--------------|--------------------|----------|------------|-----|---|----|

## 故障排除

思科建议尽可能通过客户端运行调试。

通过CLI，这些调试提供有用信息：

```
debug client MA:CA:DD:RE:SS
debug web-auth redirect enable macMA:CA:DD:RE:SS
debug aaa all enable
```

## 相关信息

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