

Identity Services Engine Guest Portal Local Web Authentication Configuration Example

Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Components Used](#)
- [Background Information](#)
- [Configure](#)
- [LWA Process with the ISE Guest Portal](#)
- [Network Diagram](#)
- [Configuration Prerequisites](#)
- [Configure the WLC](#)
- [Configure the External ISE as the Webauth URL Globally](#)
- [Configure the Access Control Lists \(ACLs\)](#)
- [Configure the Service Set Identifier \(SSID\) for LWA](#)
- [Configure the ISE](#)
- [Define the Network Device](#)
- [Configure the Authentication Policy](#)
- [Configure the Authorization Policy and Result](#)
- [Verify](#)
- [Troubleshoot](#)
- [Related Information](#)

Introduction

This document describes how to configure Local Web Authentication (LWA) with the Cisco Identity Services Engine (ISE) guest portal.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ISE
- Cisco Wireless LAN Controller (WLC)

Components Used

The information in this document is based on these software and hardware versions:

- ISE Version 1.4
- WLC Version 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.

Background Information

This document describes the configuration of LWA. However, Cisco recommends that you use Centralized Web Authentication (CWA) with the ISE whenever possible. There are a few scenarios where LWA is preferred or the only option, so this is a configuration example for those scenarios.

Configure

LWA requires certain prerequisites and a major configuration on the WLC as well as a few changes needed on the ISE.

Before those are covered, here is an outline of the LWA process with the ISE.

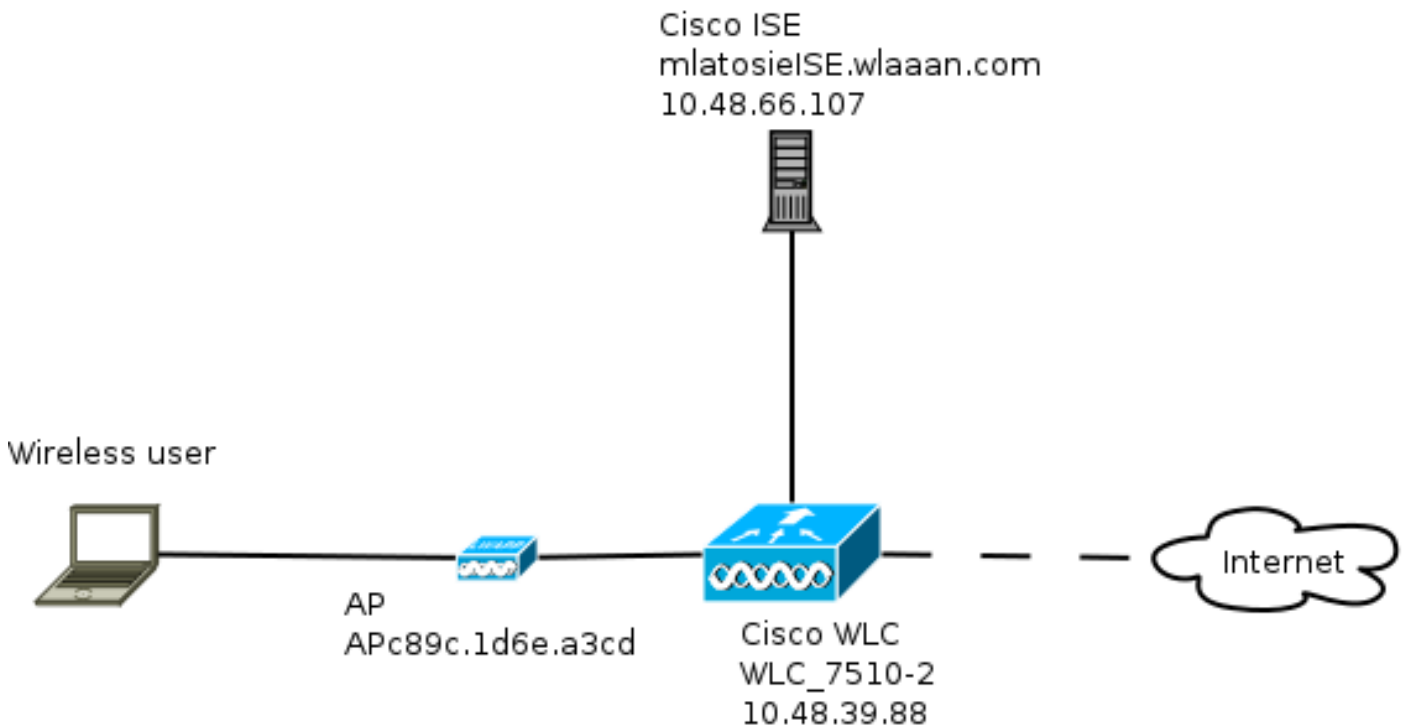
LWA Process with the ISE Guest Portal

1. The browser tries to fetch a web page.
2. The WLC intercepts the HTTP(S) request and redirects it to the ISE.
Several key pieces of information are stored in that HTTP redirect header. Here is an example of the redirect 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/`
From the example URL, you can see that the user tried to reach "yahoo.com." The URL also contains information about the Wireless Local Area Network (WLAN) name (mlatosie_LWA), and the client and access point (AP) MAC addresses. In the example URL, **1.1.1.1** is the WLC, and **mlatosieise.wlaaan.com** is the ISE server.
3. The user is presented with the ISE guest login page and enters the username and password.
4. The ISE performs authentication against its configured identity sequence.
5. The browser redirects again. This time, it submits credentials to the WLC. The browser provides the username and password that the user entered in the ISE without any additional interaction from the user. Here is an example GET request to the WLC.
GET
`/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0`
Again, the original URL (**yahoo.com**), the username (**mlatosie@cisco.com**), and the password (**ityh**) are all included.
Note: Although the URL is visible here, the actual request is submitted over Secure Sockets Layer (SSL), which is indicated by HTTPS, and is hard to intercept.
6. The WLC uses RADIUS in order to authenticate that username and password against the ISE and allows access.

7. The user is redirected to the specified portal. Refer to the "**Configure external ISE as the webauth URL**" section of this document for more information.

Network Diagram

This figure describes the logical topology of devices used in this example.



Configuration Prerequisites

For the LWA process to work properly, a client needs to be able to obtain the:

- IP address and netmask configuration
- Default route
- Domain Name System (DNS) server

All of these can be provided with DHCP or the local configuration. The DNS resolution needs to work properly in order for the LWA to work.

Configure the WLC

Configure the External ISE as the Webauth URL Globally

Under **Security > Web Auth > Web Login Page**, you can access this information.

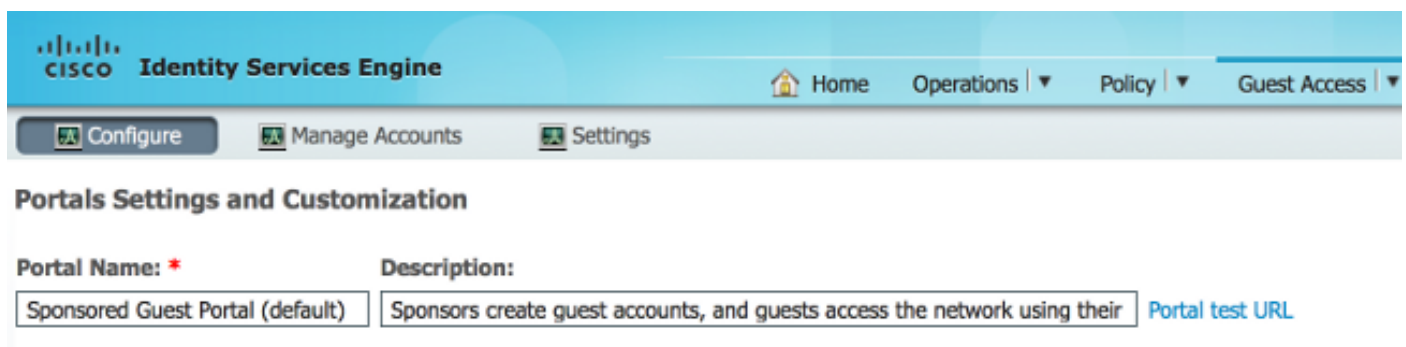
Web Login Page

Web Authentication Type	External (Redirect to external server) 
Redirect URL after login	<input type="text"/>
External Webauth URL	<input type="text" value="https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=2"/>

Note: This example uses an External Webauth URL and was taken from ISE Version 1.4. If you have a different version, consult the configuration guide in order to understand what should be configured.

It is also possible to configure this setting per-WLAN. It is then in the specific WLAN security settings. Those override the global setting.

In order to find out the correct URL for your specific portal, choose **ISE > Guest Policy > Configure > your specific portal**. Right-click the link from "portal test URL" and choose **copy link location**.



The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes "Home", "Operations", "Policy", and "Guest Access". Below the navigation bar are tabs for "Configure", "Manage Accounts", and "Settings". The main content area is titled "Portals Settings and Customization". It features two input fields: "Portal Name: *" with the value "Sponsored Guest Portal (default)" and "Description:" with the value "Sponsors create guest accounts, and guests access the network using their Portal test URL".

In this example, the full URL is:

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

Configure the Access Control Lists (ACLs)

For web authentication to work, the allowed traffic should be defined. Determine whether FlexConnect ACLs or normal ACLs should be used. FlexConnect APs use FlexConnect ACLs, while APs that use centralized switching use normal ACLs.

In order to understand in what mode a particular AP operates, choose **Wireless > Access points** and choose the **AP name > AP Mode** drop-down box. A typical deployment is either **local** or **FlexConnect**.

Under **Security > Access Control Lists**, choose either **FlexConnect ACLs** or **ACLs**. In this example, all UDP traffic was permitted in order to specifically allow DNS exchange and traffic to the 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	<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"/>

This example uses FlexConnect, so **both** FlexConnect and standard ACLs are defined.

This behavior is documented in Cisco Bug ID [CSCue68065](#) with regard to WLC 7.4 controllers. It is not required anymore on WLC 7.5 where you only need a FlexACL and no standard ACL anymore

Configure the Service Set Identifier (SSID) for LWA

Under **WLANs**, choose the **WLAN ID** to edit.

Web Auth Configuration

Apply the same ACLs which were defined in the previous step and enable web authentication.

WLANs > Edit 'mlatosie_LWA'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security None

Web Policy

Authentication

Passthrough

Conditional Web Redirect

Splash Page Web Redirect

On MAC Filter failure¹⁰

Preauthentication ACL IPv4 FLEX_GUEST IPv6 None WebAuth FlexAcl FLEX_GUEST

Over-ride Global Config Enable

Note: If FlexConnect's local switching feature is used, ACL mapping needs to be added on the AP level. This can be found under **Wireless > Access Points**. Choose the appropriate **AP Name > FlexConnect > External WebAuthentication ACLs**.

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

AP Name APc89c.1d6e.a3cd
Base Radio MAC 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

Authentication, Authorization, and Accounting (AAA) Server Configuration

In this example, both the authentication and accounting servers point to the previously-defined ISE server.

General	Security	QoS	Advanced
Layer 2	Layer 3	AAA Servers	
Select AAA servers below to override use of default servers on this WLAN			
Radius Servers			
Radius Server Overwrite interface <input type="checkbox"/> Enabled			
		Authentication Servers	Accounting Servers
		<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 1		<input type="text" value="IP:10.48.66.107, Port:1812"/>	<input type="text" value="IP:10.48.66.107, Port:1813"/>

Note: The defaults under the **Advanced** tab do not need to be appended.

Configure the ISE

The ISE configuration consists of several steps.

First, define the device as a network device.

Then, ensure that the authentication and authorization rules that accommodate this exchange exist.

Define the Network Device

Under **Administration > Network Resources > Network Devices**, populate these fields:

- Device name
- Device IP address
- **Authentication Settings > Shared Secret**

Network Devices

* Name
Description

* IP Address: /

Model Name
Software Version

* Network Device Group

WLC
Location
Device Type



Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

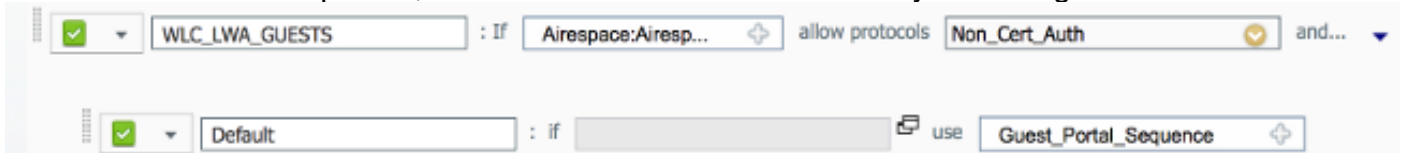
* Shared Secret

Configure the Authentication Policy

Under **Policy > Authentication**, add a new authentication policy.

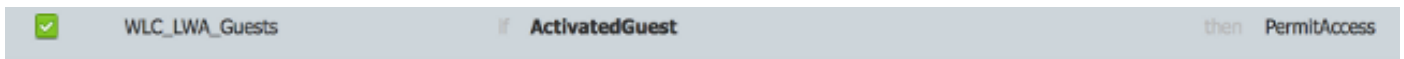
This example uses these parameters:

- Name: **WLC_LWA_Guests**
- Condition: **Airespace:Airespace-Wlan-Id**. This condition matches the WLAN ID of 3, which is the ID of the WLAN **mlatosie_LWA** that was previously defined on the WLC.
- {optional} It allows authentication protocols that do not require the certificate **Non_Cert_Auth**, but the defaults can be used.
- **Guest_Portal_Sequence**, which defines that users are locally-defined guests users.



Configure the Authorization Policy and Result

Under **Policy > Authorization**, define a new policy. It can be a very basic policy, such as:



This configuration depends on the overall configuration of the ISE. This example is purposefully simplified.

Verify

On the ISE, administrators can monitor and troubleshoot live sessions under **Operations > Authentications**.

Two authentications should be seen. The first authentication is from the guest portal on the ISE. The second authentication comes as an access request from the WLC to the ISE.

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

You can click the **Authentication Detail Report** icon in order to verify which authorization policies and authentication policies were chosen.

On the WLC, an administrator can monitor clients under **Monitor > Client**.

Here is an example of a client that authenticated properly:

28:cf:e9:13:47:db	AP:c80c:1d6e:a3cd	mlatosie_LWA	mlatosie_LWA	mlatosie@cisco.com	802.11bn	Associated	Yes	1	No
-------------------	-------------------	--------------	--------------	--------------------	----------	------------	-----	---	----

Troubleshoot

Cisco recommends that you run debugs by means of the client whenever possible.

Through the CLI, these debugs provide useful information:

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



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

```
debug aaa all enable
```

Related Information

- [Cisco ISE 1.x Configuration Guide](#)
- [Cisco WLC 7.x Configuration Guide](#)
- [Technical Support & Documentation - Cisco Systems](#)