

# Identity Services Engine ゲスト ポータルのローカル Web 認証の設定例

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ISE ゲスト ポータルでの LWA プロセス](#)

[ネットワーク図](#)

[設定要件](#)

[WLC の設定](#)

[外部ISEをWebauth URLとしてグローバルに設定する](#)

[アクセスコントロール リスト \( ACL \) の設定](#)

[LWA のサービス セット ID \( SSID \) の設定](#)

[ISE の設定](#)

[ネットワーク デバイスの定義](#)

[認証ポリシーの設定](#)

[許可ポリシーと許可結果の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco Identity Services Engine ( ISE ) のゲスト ポータルでローカル Web 認証 ( LWA ) を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ISE
- Cisco Wireless LAN Controller ( WLC )

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ISE バージョン 1.4
- WLC バージョン 7.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 背景説明

このドキュメントでは、LWA の設定について説明します。ただし、可能な限り ISE による中央集中型 Web 認証（CWA）を使用することを推奨します。一部のシナリオでは LWA が推奨または唯一のオプションとなるため、ここではそれらのシナリオの設定例を示します。

## 設定

LWA を使用するには、特定の前提条件、WLC での主要な設定、および ISE でのいくつかの変更が必要です。

これらについて説明する前に、ここでは ISE による LWA プロセスの概要を示します。

### ISE ゲスト ポータルでの LWA プロセス

1. ブラウザが Web ページを取得しようとします。
2. WLC は HTTP(S) 要求をインターセプトし、ISE にリダイレクトします。  
情報のいくつかの重要な部分が HTTP リダイレクト ヘッダーに格納されます。リダイレクト URL の例を次に示します。  
`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/`  
この URL 例から、ユーザが「yahoo.com」に到達しようとしたことがわかります。この URL には、ワイヤレス ローカル エリア ネットワーク（WLAN）の名前（mlatosie\_LWA）、およびクライアントとアクセスポイント（AP）の MAC アドレスに関する情報が含まれています。この URL 例では、1.1.1.1 が WLC であり、mlatosieise.wlaaan.com が ISE サーバです。
3. ISE のゲスト ログイン ページが表示され、ユーザがユーザ名とパスワードを入力します。
4. ISE は、設定済みの ID シーケンスに照らして認証を実行します。
5. ブラウザが再びリダイレクトします。今度は、WLC にクレデンシャルを送信します。ブラウザは、ユーザが ISE で入力したユーザ名とパスワードを追加のユーザ操作なしで提供します。WLC に対する GET 要求の例を次に示します。

GET

```
/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
```

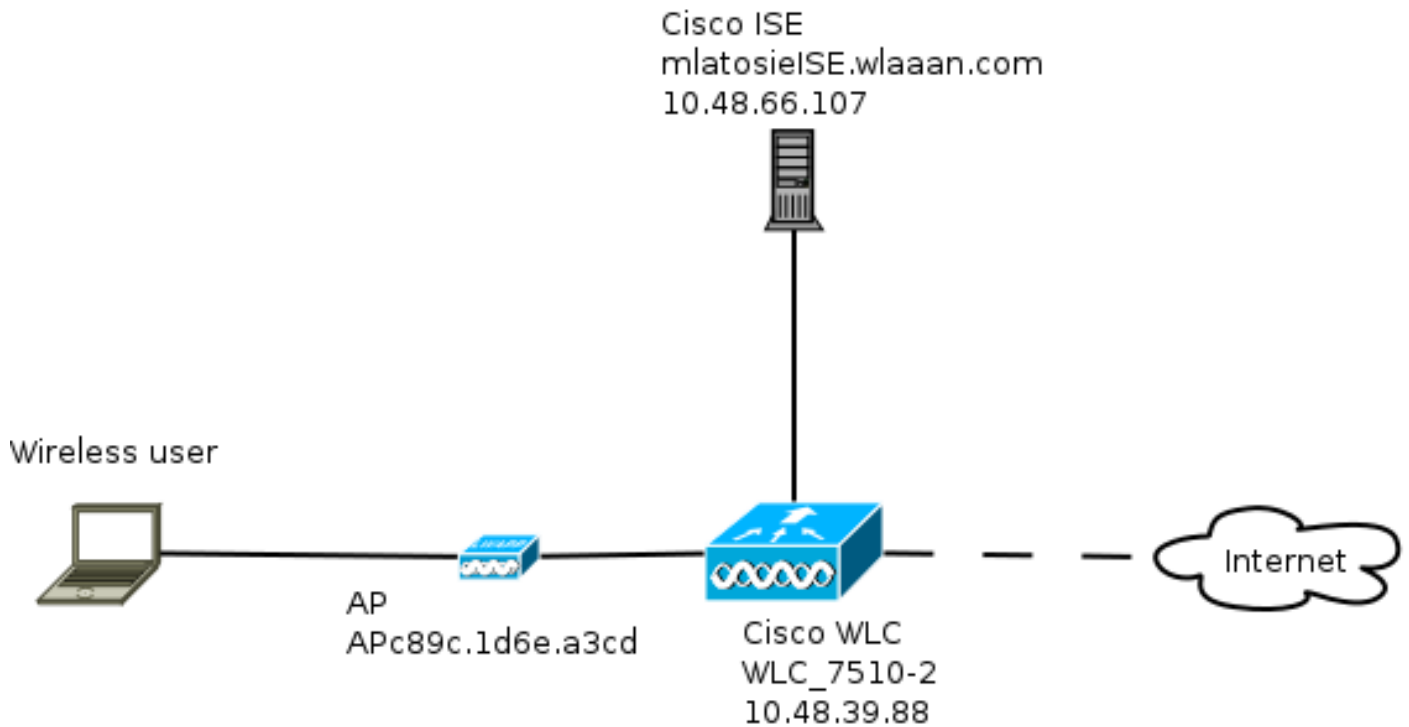
ここにも、元の URL（yahoo.com）、ユーザ名（mlatosie@cisco.com）、およびパスワード（ityh）のすべてが含まれています。

注：ここでは URL を表示していますが、実際の要求は HTTPS で示される Secure Sockets Layer（SSL）を介して送信されるため、傍受は困難です。

6. WLC は、RADIUS を使用してこのユーザ名とパスワードを ISE に対して認証し、アクセスを許可します。
7. ユーザが指定されたポータルにリダイレクトされます。詳細については、このドキュメントの「WebAuth URL としての外部 ISE の設定」の項を参照してください。

## ネットワーク図

この図は、この例で使用するデバイスの論理トポロジを示しています。



## 設定要件

LWA プロセスが正常に動作するには、クライアントが次の情報を取得できる必要があります。

- IP アドレスとネットマスクの設定
- デフォルト ルート
- ドメイン ネーム システム ( DNS ) サーバ

これらはすべてDHCPまたはローカル構成で提供できます。LWAが機能するには、DNS解決が正しく動作する必要があります。

## WLC の設定

### 外部ISEをWebauth URLとしてグローバルに設定する

[Security] > [Web Auth] > [Web Login Page] で、この情報にアクセスできます。

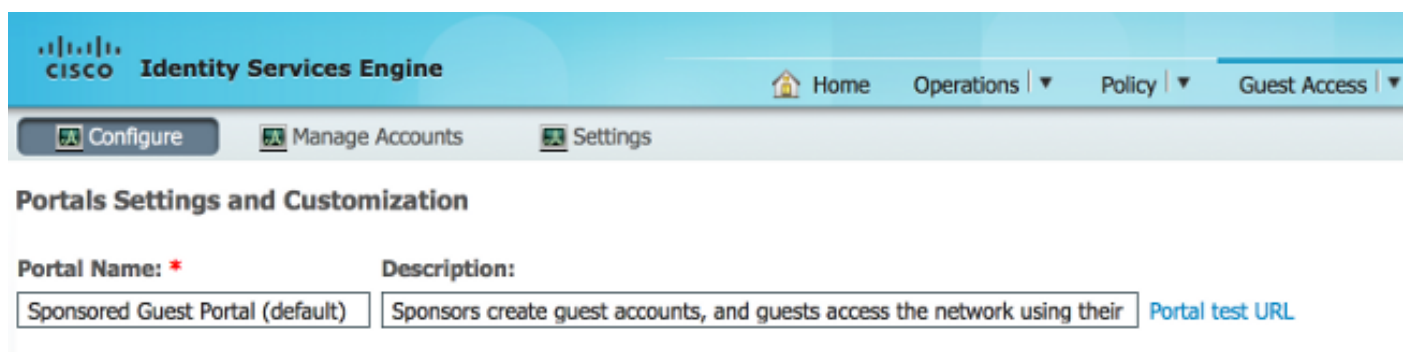
## Web Login Page

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"/>

注：この例では、外部Webauth URLを使用し、ISEバージョン1.4から取得したものです。別のバージョンを使用している場合は、設定ガイドを参照して、設定する必要のある内容を理解してください。

WLANごとにこの設定を設定することもできます。その後、特定のWLANセキュリティ設定に含まれます。これらはグローバル設定を上書きします。

特定のポータル正しいURLを見つけるには、[ISE] > [Guest Policy] > [Configure] > [your specific portal]の順に選択します。「ポータルテストURL」のリンクを右クリックし、「リンクの場所をコピー」を選択します。



The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Portals Settings and Customization. The main heading is "Portals Settings and Customization". Below this, there are 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".

この例では、完全なURLは次のとおりです。

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

## アクセスコントロール リスト ( ACL ) の設定

Web認証が機能するには、許可されたトラフィックを定義する必要があります。FlexConnect ACLと通常のACLのどちらを使用するかを決定してください。FlexConnect APはFlexConnect ACLを使用し、集中スイッチングを使用するAPは通常ACLを使用します。

特定のAPが動作するモードを理解するには、[Wireless] > [Access points]の順に選択し、[AP name] > [AP Mode]ドロップダウンボックスを選択します。一般的な展開は、[local] と [FlexConnect] のいずれかです。

[Security] > [Access Control Lists] で、[FlexConnect ACLs]または[ACLs]を選択します。この例では、すべてのUDPトラフィックが許可され、DNS交換とISE(10.48.66.107)へのトラフィックが具体的に許可されています。

## 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"/>

この例ではFlexConnectを使用するため、FlexConnectと標準ACLの両方が定義されています。

この動作は、WLC 7.4 コントローラに関する Cisco [Bug ID CSCue68065](#) に記述されています。FlexACLのみが必要で、標準ACLが不要になったWLC 7.5では不要になりました

## LWA のサービス セット ID ( SSID ) の設定

[WLAN] で、編集する [WLAN ID] を選択します。

## Web 認証設定

直前の手順で定義した ACL を適用し、Web 認証をイネーブルにします。

WLANs > Edit 'mlatosie\_LWA'

The screenshot shows the configuration page for 'mlatosie\_LWA' with the 'AAA Servers' tab selected. The 'Layer 3 Security' dropdown is set to 'None'. The 'Web Policy' checkbox is checked, and the 'Authentication' radio button is selected. The 'Preauthentication ACL' is set to 'FLEX\_GUEST' for both IPv4 and IPv6. The 'WebAuth FlexAcl' is also set to 'FLEX\_GUEST'. The 'Over-ride Global Config' checkbox is unchecked.

注：FlexConnect のローカル スイッチング機能を使用する場合は、ACL のマッピングを AP レベルで追加する必要があります。これは、[Wireless] > [Access Points] にあります。適切な [AP Name] > [FlexConnect] > [External WebAuthentication ACLs] を選択します。

## 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

## 認証、認可、およびアカウントティング (AAA) のサーバ設定

この例では、認証サーバとアカウントティングサーバの両方が、以前に定義した ISE サーバを指しています。

General	Security	QoS	Advanced
Layer 2	Layer 3	AAA Servers	
Select AAA servers below to override use of default servers on this WLAN			
<b>Radius Servers</b>			
Radius Server Overwrite interface <input type="checkbox"/> Enabled			
		<b>Authentication Servers</b>	<b>Accounting Servers</b>
		<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"/>

注：[Advanced] タブのデフォルトを追加する必要はありません。

## ISE の設定

ISE の設定は複数の手順で構成されます。

まず、デバイスをネットワーク デバイスとして定義します。

次に、この交換に対応する認証ルールと許可ルールが存在することを確認します。

### ネットワーク デバイスの定義

[Administration] > [Network Resources] > [Network Devices] で、次のフィールドに値を入力します。

- デバイス名
- デバイスの IP アドレス
- [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**

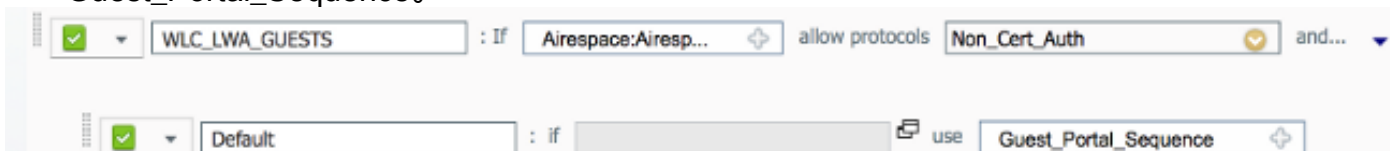
\* Shared Secret

### 認証ポリシーの設定

[Policy] > [Authentication] で、新しい認証ポリシーを追加します。

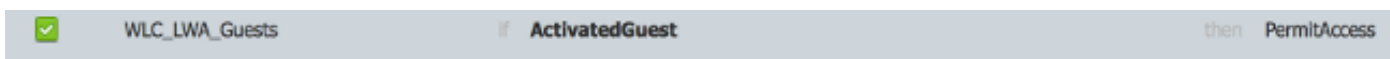
この例では、次のパラメータを使用します。

- [Name] : WLC\_LWA\_Guests
- 条件 : Airespace:Airespace-Wlan-Id。この条件は、WLCで以前に定義されたWLAN mlatosie\_LWAのIDである3のWLAN IDと一致します。
- ( オプション ) 証明書 Non\_Cert\_Auth を必要としない認証プロトコルを許可しますが、デフォルトを使用できます。
- ユーザがローカルに定義されたゲスト ユーザであることを定義する Guest\_Portal\_Sequence。



## 許可ポリシーと許可結果の設定

[Policy] > [Authorization] で、新しいポリシーを定義します。次のような非常に基本的なポリシーでかまいません。



この設定は、ISE の全体的な設定によって異なります。この例では、意図的に簡単にしています。

## 確認

管理者は、ISE の [Operations] > [Authentications] でライブ セッションの監視とトラブルシューティングを行うことができます。

2つの認証を確認する必要があります。1つ目の認証は、ISE のゲスト ポータルで行われます。2つ目の認証は、WLC から ISE へのアクセス要求として行われます。

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

[Authentication Detail Report]アイコンをクリックして、選択された認可ポリシーと認証ポリシーを確認できます。

管理者は、WLC の [Monitor] > [Client] でクライアントを監視できます。

正常に認証されたクライアントの例を次に示します。

28:cf:e9:13:47:cb	AP:89c.1d6e.a3cd	mlatosie_LWA	mlatosie_LWA	mlatosie@cisco.com	802.11bn	Associated	Yes	1	No
-------------------	------------------	--------------	--------------	--------------------	----------	------------	-----	---	----

## トラブルシューティング

可能な限り、クライアントでデバッグを実行することを推奨します。

これらのデバッグでは、CLI を介して有用な情報が提供されます。



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

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

```
debug aaa all enable
```

## 関連情報

- [Cisco ISE 1.xコンフィギュレーションガイド](#)
- [Cisco WLC 7.xコンフィギュレーションガイド](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)