

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

TAC

Document ID: 116217

Updated: 2015 年 11 月 25 日

Marcin Latosiewicz およびニコラス Darchis によって貢献される、Cisco TAC エンジニア。

 [PDF のダウンロード](#)

[印刷](#)

[フィードバック](#)

## 関連製品

- [ワイヤレス LAN \( WLAN \)](#)
- [Cisco Identity Services Engine](#)

## 目次

[はじめに](#)

[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](#)

[Webauth URL で外部 ISE をグローバルに設定して下さい](#)

[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 ポータルによるローカル 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推奨されます。

- ISE
- Cisco ワイヤレス LAN コントローラ ( 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くものです。

- ISE バージョン 1.4
- WLC バージョン 7.4

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## 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。

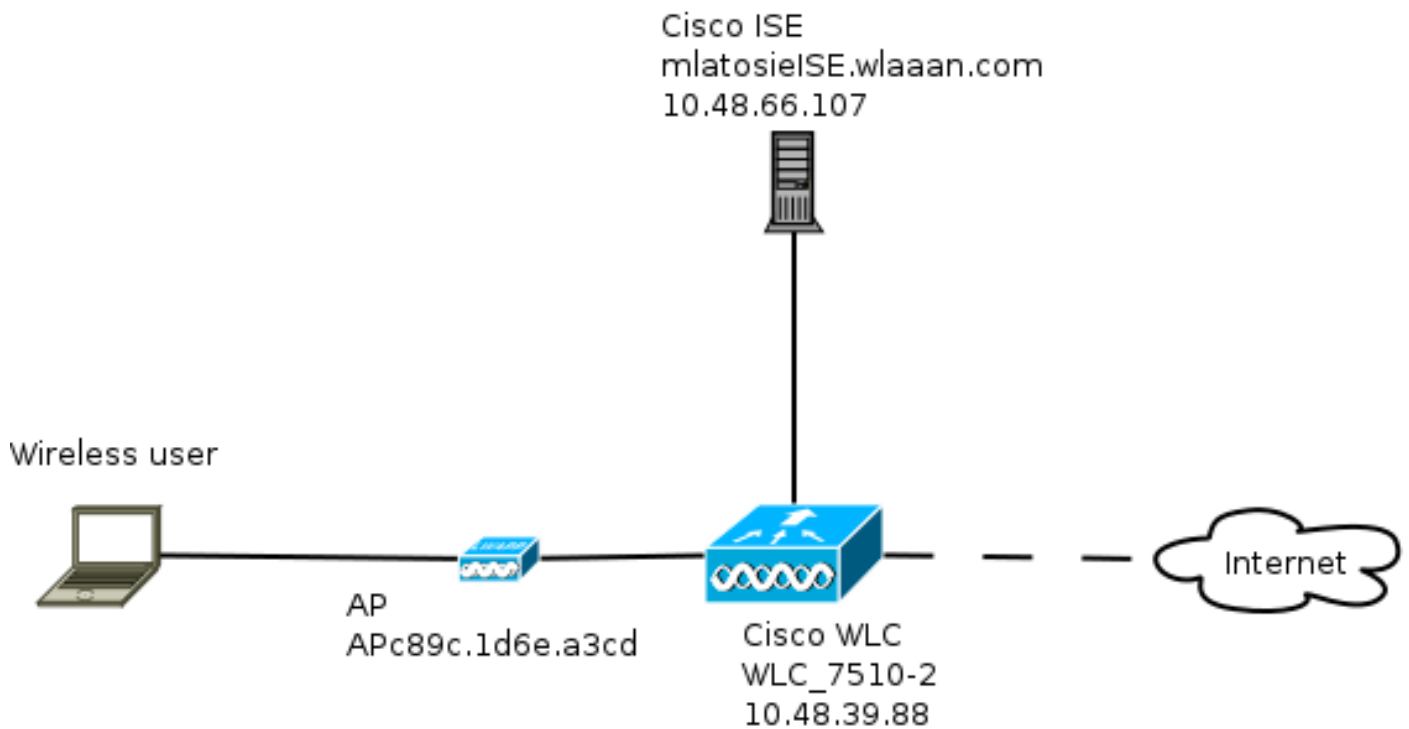
これらについて説明する前に、ここでは ISE による LWA プロセスの概要を示します。

### 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 要求を傍受し、それを 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 またはローカル設定によって提供されます。LWA が動作するためには、DNS 解決が正常に機能する必要があります。

## WLC の設定

Webauth URL で外部 ISE をグローバルに設定して下さい

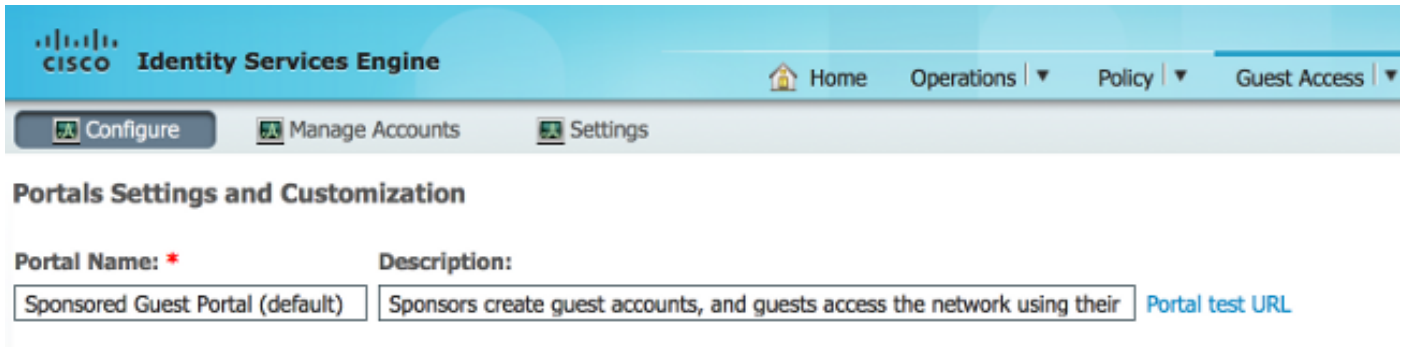
[Security] > [Web Auth] > [Web Login Page] で、この情報にアクセスできます。

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: この例は外部 Webauth URL を使用し、ISE バージョン 1.4 から奪取されました。バージョンが異なる場合は、必要な設定内容を理解するため、コンフィギュレーション ガイドを参照してください。

この設定毎 WLAN を設定することもまた可能性のあるです。それは特定の WLAN セキュリティ設定にそれからあります。それはグローバルな設定を無効にします。

特定のポータルのための正しい URL を調べるために、ISE > ゲスト ポリシー > 設定します > 仕様ポータル選択して下さい。「門脈テスト URL」からのリンクを右クリックし、リンク位置を『Copy』を選択して下さい。



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 認証が動作するためには、許可するトラフィックを定義する必要があります。FlexConnect ACL と標準 ACL のどちらを使用する必要があるかを決定します。FlexConnect AP は FlexConnect ACL を使用しますが、中央集中型スイッチングを使用する AP は標準 ACL を使用します。

どんなでモードを特定の AP が操作するか理解するために、> アクセス ポイント 『Wireless』 を選択し、AP 名前 > APモード ドロップダウン ボックスを選択して下さい。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、DNS 交換と ISE ( 10.48.66.107 ) へのトラフィックを特に許可するため、すべての UDP トラフィックが許可されています。

### 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"/>

この例は FlexConnect を使用します、従って FlexConnect および標準 ACL は両方定義されます。

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 および標準 ACL だけをもう必要としないところで WLC 7.5 でそれがもう必要となります。

せん

## 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 AAA Servers, specifically the 'AAA Servers' tab. The 'Layer 3 Security' dropdown is set to 'None'. The 'Web Policy' section has several radio button options: 'Web Policy' (checked), 'Authentication', 'Passthrough', 'Conditional Web Redirect', 'Splash Page Web Redirect', and 'On MAC Filter failure' (with a link '10'). The 'Preauthentication ACL' section has three dropdown menus: 'IPv4' set to 'FLEX\_GUEST', 'IPv6' set to 'None', and 'WebAuth FlexAcl' 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、およびアカウントिंग (AAA) のサーバ設定

この例では、認証サーバとアカウントिंग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 > ネットワークリソース > ネットワークデバイスの下で、これらのフィールドにデータ入力して下さい:

- 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。

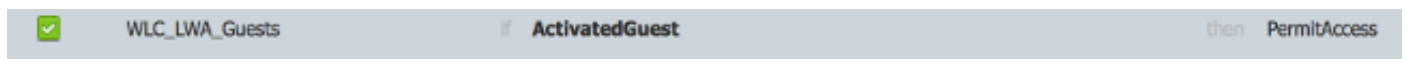
この例では、次のパラメータを使用します。

- [Name] : WLC\_LWA\_Guests
- [Condition] : Airespace: Airespace-Wlan-Id。この条件は WLAN ID の 3 と一致します。これは、以前に WLC に定義した WLAN mlatosie\_LWA の ID です。
- ( 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

どの許可ポリシーおよび認証 ポリシーが選択されたか確認するために認証 Detail レポート アイコンをクリックできます。

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:db	AP:80c.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](#)

このドキュメントは有用でしたか。 [はい いいえ](#)

フィードバックいただき、ありがとうございました。

[サポート ケースのオープン](#) ( [シスコ サービス契約< ts generic='1' nval='P%1,2%%'が必要ですか](#) )。

## Cisco サポート コミュニティ - 特集対話

[Cisco サポート コミュニティ](#)では、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

Updated: 2015 年 11 月 25 日

Document ID: 116217