

# Konfigurationsbeispiel für die lokale Webauthentifizierung im Gastportal der Identity Services Engine

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[LWA-Prozess mit ISE-Gastportal](#)

[Netzwerkdiagramm](#)

[Konfigurationsvoraussetzungen](#)

[Konfigurieren des WLC](#)

[Konfigurieren Sie die externe ISE als Webauth-URL global.](#)

[Konfigurieren der Zugriffskontrolllisten \(ACLs\)](#)

[Konfigurieren Sie den Service Set Identifier \(SSID\) für LWA.](#)

[Konfigurieren der ISE](#)

[Definieren des Netzwerkgeräts](#)

[Konfigurieren der Authentifizierungsrichtlinie](#)

[Konfigurieren der Autorisierungsrichtlinie und des -Ergebnisses](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie Local Web Authentication (LWA) mit dem Cisco Identity Services Engine (ISE)-Gastportal konfigurieren.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ISE
- Cisco Wireless LAN Controller (WLC)

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ISE Version 1.4
- WLC-Version 7.4

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Dieses Dokument beschreibt die Konfiguration von LWA. Cisco empfiehlt jedoch die Verwendung von Centralized Web Authentication (CWA) mit der ISE, wann immer dies möglich ist. Es gibt einige Szenarien, in denen LWA bevorzugt oder die einzige Option ist. Dies ist ein Konfigurationsbeispiel für diese Szenarien.

## Konfigurieren

LWA erfordert bestimmte Voraussetzungen und eine Hauptkonfiguration auf dem WLC sowie einige Änderungen, die für die ISE erforderlich sind.

Bevor diese behandelt werden, folgt eine Zusammenfassung des LWA-Prozesses mit der ISE.

### LWA-Prozess mit ISE-Gastportal

1. Der Browser versucht, eine Webseite abzurufen.
2. Der WLC fängt die HTTP(S)-Anfrage ab und leitet sie an die ISE um.  
Mehrere wichtige Informationen werden in diesem HTTP-Redirect-Header gespeichert. Hier ein Beispiel für die URL für die Umleitung:  
`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/`  
Aus der Beispiel-URL können Sie sehen, dass der Benutzer versucht hat, "yahoo.com" zu erreichen. Die URL enthält außerdem Informationen zum Namen des Wireless Local Area Network (WLAN) (mlatosie\_LWA) sowie zu den MAC-Adressen des Clients und Access Points (AP). Im Beispiel-URL ist 1.1.1.1 der WLC und mlatosieise.wlaaan.com der ISE-Server.
3. Dem Benutzer wird die Anmeldeseite für den ISE-Gast angezeigt, und er gibt den Benutzernamen und das Kennwort ein.
4. Die ISE führt die Authentifizierung anhand der konfigurierten Identitätssequenz durch.
5. Der Browser wird erneut umgeleitet. Diesmal sendet er Anmeldeinformationen an den WLC. Der Browser stellt den Benutzernamen und das Kennwort bereit, die der Benutzer ohne zusätzliche Interaktion durch den Benutzer in die ISE eingegeben hat. Im Folgenden finden Sie ein Beispiel für eine GET-Anforderung an den WLC.  
GET  
`/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0`

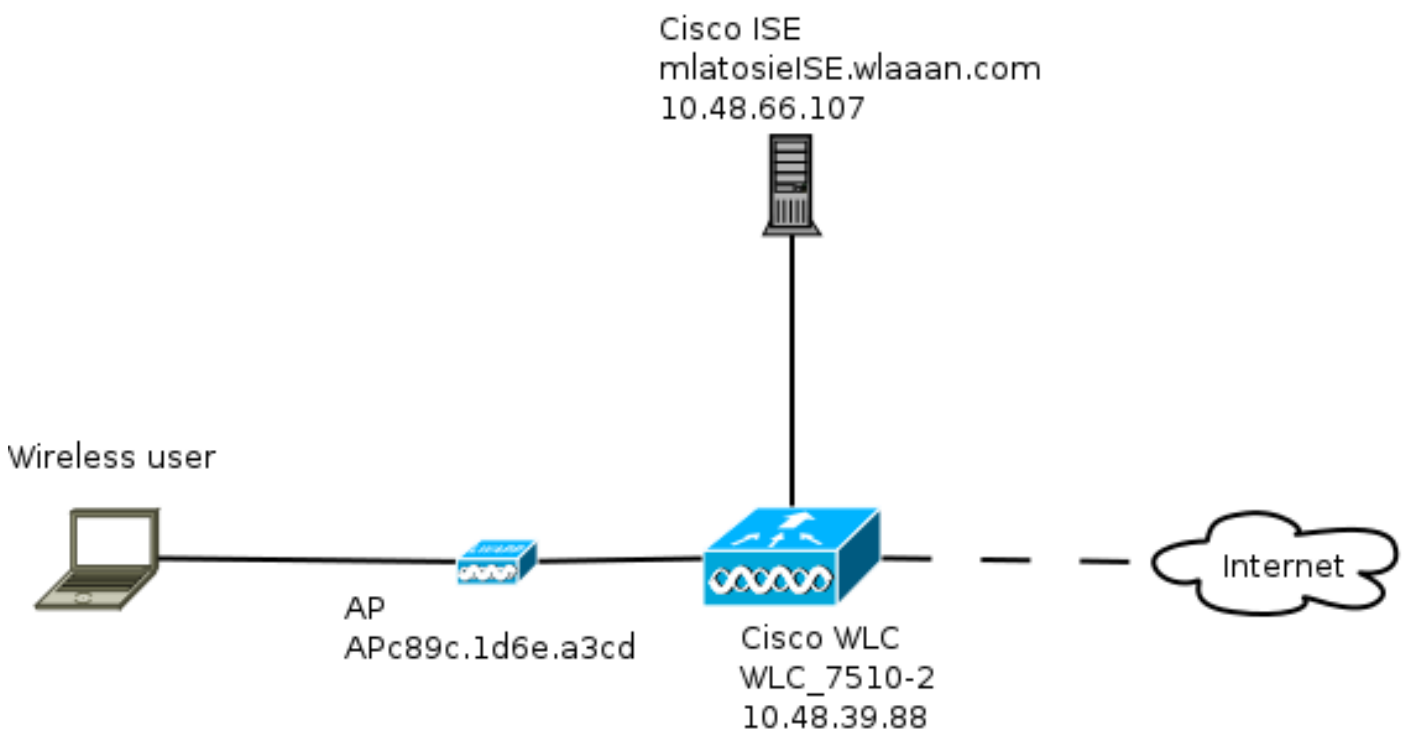
Auch hier sind die ursprüngliche URL (**yahoo.com**), der Benutzername (**mlatosie@cisco.com**) und das Kennwort (**ityh**) enthalten.

**Hinweis:** Obwohl die URL hier sichtbar ist, wird die eigentliche Anfrage über Secure Sockets Layer (SSL) gesendet, was durch HTTPS angegeben wird. Diese Anforderung ist schwer abzufangen.

6. Der WLC verwendet RADIUS, um diesen Benutzernamen und das Kennwort für die ISE zu authentifizieren und den Zugriff zuzulassen.
7. Der Benutzer wird zum angegebenen Portal umgeleitet. Weitere Informationen finden Sie im Abschnitt "**Externe ISE als Webauth-URL konfigurieren**" dieses Dokuments.

## Netzwerkdiagramm

Diese Abbildung beschreibt die logische Topologie der in diesem Beispiel verwendeten Geräte.



## Konfigurationsvoraussetzungen

Damit der LWA-Prozess ordnungsgemäß funktioniert, muss ein Client Folgendes erhalten:

- Konfiguration von IP-Adresse und Netzmaske
- Standardroute
- DNS-Server (Domain Name System)

All diese können mit DHCP oder der lokalen Konfiguration bereitgestellt werden. Die DNS-Auflösung muss ordnungsgemäß funktionieren, damit das LWA funktioniert.

## Konfigurieren des WLC

Konfigurieren Sie die externe ISE als Webauth-URL global.

Unter **Sicherheit > Webauthentifizierung > Webseite** können Sie auf diese Informationen zugreifen.

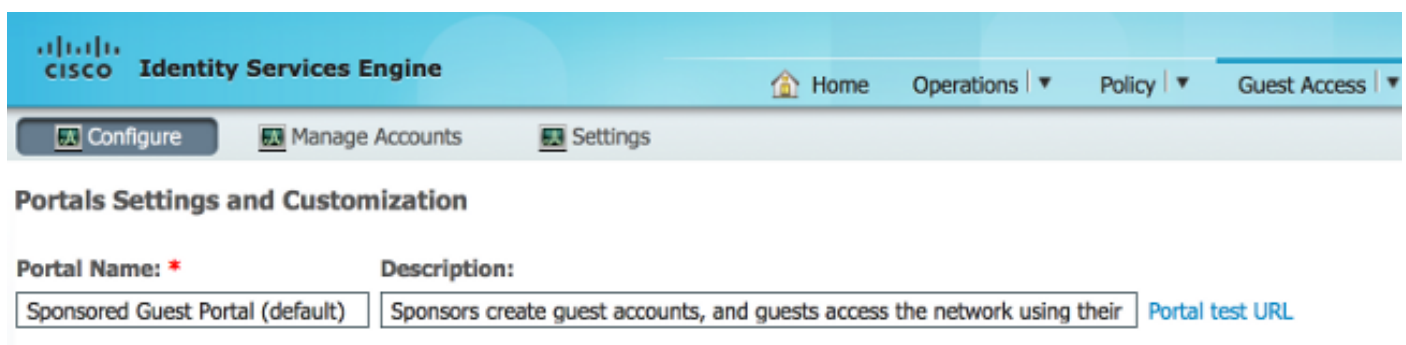
## Web Login Page

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"/>

**Hinweis:** In diesem Beispiel wird eine externe Webauth-URL verwendet, die aus ISE Version 1.4 stammt. Wenn Sie eine andere Version haben, lesen Sie im Konfigurationsleitfaden nach, welche Konfigurationen erforderlich sind.

Diese Einstellung kann auch pro WLAN konfiguriert werden. Anschließend werden die Sicherheitseinstellungen für das WLAN festgelegt. Diese überschreiben die globale Einstellung.

Um die richtige URL für Ihr Portal zu finden, wählen Sie **ISE > Guest Policy > Configure > your specific portal**. Klicken Sie mit der rechten Maustaste auf den Link von "Portal test URL", und wählen Sie **Copy Link Location** aus.



**Portals Settings and Customization**

Portal Name: \*  Description:  [Portal test URL](#)

In diesem Beispiel lautet die vollständige URL:

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

## Konfigurieren der Zugriffskontrolllisten (ACLs)

Damit die Webauthentifizierung funktioniert, muss der zulässige Datenverkehr definiert werden. Bestimmen Sie, ob FlexConnect-ACLs oder normale ACLs verwendet werden sollen. FlexConnect-APs verwenden FlexConnect-ACLs, während Access Points, die zentralisiertes Switching verwenden, normale ACLs verwenden.

Um zu erfahren, in welchem Modus ein bestimmter Access Point betrieben wird, wählen Sie **Wireless > Access Points** und wählen das Dropdown-Feld **AP name > AP Mode** aus. Eine typische Bereitstellung ist entweder **lokal** oder **FlexConnect**.

Wählen Sie unter **Security > Access Control Lists (Sicherheit > Zugriffskontrolllisten)** entweder **FlexConnect-ACLs** oder **ACLs** aus. In diesem Beispiel wurde der gesamte UDP-Datenverkehr zugelassen, um speziell DNS-Austausch und Datenverkehr zur ISE zuzulassen (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"/>

In diesem Beispiel wird FlexConnect verwendet, sodass **sowohl** FlexConnect als auch Standard-ACLs definiert sind.

Dieses Verhalten ist in der Cisco Bug-ID [CSCue68065](#) für WLC 7.4-Controller dokumentiert. Auf WLC 7.5 ist dies nicht mehr erforderlich, da Sie nur eine FlexACL und keine Standard-ACL mehr benötigen.

**Konfigurieren Sie den Service Set Identifier (SSID) für LWA.**

Wählen Sie unter **WLANs** die **WLAN-ID** aus, die bearbeitet werden soll.

## Web Auth-Konfiguration

Wenden Sie die gleichen Zugriffskontrolllisten an, die im vorherigen Schritt definiert wurden, und aktivieren Sie die Webauthentifizierung.

WLANs > Edit 'mlatosie\_LWA'

The screenshot shows the configuration page for 'mlatosie\_LWA' with the following settings:

- General tab selected
- Layer 3 Security: None
- Web Policy:  (checked)
- Authentication:  (selected)
- Passthrough:
- Conditional Web Redirect:
- Splash Page Web Redirect:
- On MAC Filter failure:  <sup>10</sup>
- Preauthentication ACL: IPv4: FLEX\_GUEST, IPv6: None, WebAuth FlexAcl: FLEX\_GUEST
- Over-ride Global Config:  Enable

**Hinweis:** Wenn die lokale Switching-Funktion von FlexConnect verwendet wird, muss die ACL-Zuordnung auf AP-Ebene hinzugefügt werden. Diese finden Sie unter **Wireless > Access Points**. Wählen Sie die entsprechenden **AP-Namen > FlexConnect > External Web Authentication ACLs** aus.

## 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

Serverkonfiguration für Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting - AAA)

In diesem Beispiel verweisen sowohl die Authentifizierungs- als auch die Accounting-Server auf den zuvor definierten 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			
<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"/>

**Hinweis:** Die Standardwerte unter der Registerkarte **Erweitert** müssen nicht angehängt werden.

## Konfigurieren der ISE

Die ISE-Konfiguration besteht aus mehreren Schritten.

Definieren Sie zuerst das Gerät als Netzwerkgerät.

Stellen Sie dann sicher, dass die Authentifizierungs- und Autorisierungsregeln für diesen Austausch vorhanden sind.

### Definieren des Netzwerkgeräts

Füllen Sie unter **Administration > Network Resources > Network Devices** (Verwaltung > Netzwerkressourcen > Netzwerkgeräte) die folgenden Felder aus:

- Gerätename
- Geräte-IP-Adresse
- **Authentifizierungseinstellungen > Freigegebener geheim**

#### Network Devices

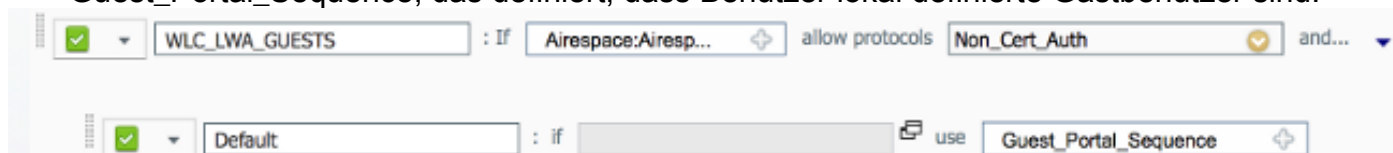
* Name	<input type="text" value="WLC_7510-2"/>
Description	<input type="text"/>
* IP Address:	<input type="text" value="10.48.39.88"/> / <input type="text" value="32"/>
Model Name	<input type="text"/>
Software Version	<input type="text"/>
* Network Device Group	
WLC	<input type="text" value="WLAAAN WLCs"/> <input type="button" value="Set To Default"/>
Location	<input type="text" value="All Locations"/> <input type="button" value="Set To Default"/>
Device Type	<input type="text" value="All Device Types"/> <input type="button" value="Set To Default"/>
<input checked="" type="checkbox"/>	▼ Authentication Settings
Enable Authentication Settings	
Protocol	<b>RADIUS</b>
* Shared Secret	<input type="text" value="*****"/> <input type="button" value="Show"/>

### Konfigurieren der Authentifizierungsrichtlinie

Fügen Sie unter **Policy > Authentication** (Richtlinien > Authentifizierung) eine neue Authentifizierungsrichtlinie hinzu.

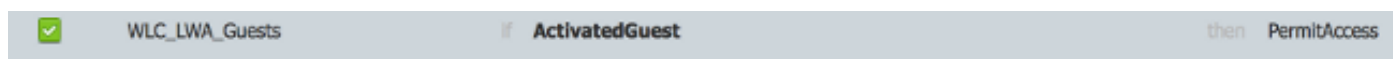
In diesem Beispiel werden folgende Parameter verwendet:

- Name: **WLC\_LWA\_Gäste**
- Bedingung: **Airespace:Airespace-Wlan-Id**. Diese Bedingung entspricht der WLAN-ID von 3, d. h. der ID des WLAN **mlatosie\_LWA**, die zuvor auf dem WLC definiert wurde.
- {optional} Es erlaubt Authentifizierungsprotokolle, die das Zertifikat **Non\_Cert\_Auth** nicht benötigen, aber die Standardwerte können verwendet werden.
- **Guest\_Portal\_Sequence**, das definiert, dass Benutzer lokal definierte Gastbenutzer sind.



## Konfigurieren der Autorisierungsrichtlinie und des -Ergebnisses

Definieren Sie unter **Richtlinien > Autorisierung** eine neue Richtlinie. Es kann sich um eine sehr grundlegende Richtlinie handeln, z. B.:



Diese Konfiguration hängt von der allgemeinen Konfiguration der ISE ab. Dieses Beispiel wurde gezielt vereinfacht.

## Überprüfen

Auf der ISE können Administratoren Live-Sitzungen unter **Betrieb > Authentifizierung** überwachen und Fehler beheben.

Zwei Authentifizierungen sollten sichtbar sein. Die erste Authentifizierung erfolgt über das Gastportal der ISE. Die zweite Authentifizierung erfolgt als Zugriffsanforderung vom WLC an die 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

Sie können auf das Symbol **Authentifizierungsdetail Report** klicken, um zu überprüfen, welche Autorisierungsrichtlinien und Authentifizierungsrichtlinien ausgewählt wurden.

Auf dem WLC kann ein Administrator Clients unter **Monitor > Client** überwachen.

Hier ein Beispiel für einen ordnungsgemäß authentifizierten Client:

28:cf:e9:13:47:db	AP:c89c:1d6e:a3cd	mlatosie_LWA	mlatosie_LWA	mlatosie@cisco.com	802.11bn	Associated	Yes	1	No
-------------------	-------------------	--------------	--------------	--------------------	----------	------------	-----	---	----

## Fehlerbehebung

Cisco empfiehlt, das Debuggen möglichst mithilfe des Clients auszuführen.



Über die CLI stellen diese Debugger nützliche Informationen bereit:

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

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

```
debug aaa all enable
```

## Zugehörige Informationen

- [Cisco ISE 1.x - Konfigurationsleitfaden](#)
- [Cisco WLC 7.x - Konfigurationsleitfaden](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)